

IBM Security QRadar  
7.4.3

*Guide d'administration*



**Remarque**

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 457.

---

# Table des matières

<b>Introduction.....</b>	<b>xiii</b>
<b>Chapitre 1. Nouveautés pour les administrateurs.....</b>	<b>1</b>
Nouvelles fonctions et améliorations dans QRadar 7.4.3.....	1
Nouvelles fonctions et améliorations dans QRadar 7.4.2.....	2
Nouvelles fonctions et améliorations dans QRadar 7.4.1.....	4
Nouvelles fonctions et améliorations dans QRadar V7.4.0.....	4
<b>Chapitre 2. Administration QRadar.....</b>	<b>7</b>
Fonctions de votre produit IBM QRadar.....	7
Navigateurs Web pris en charge.....	8
<b>Chapitre 3. Gestion des utilisateurs.....</b>	<b>11</b>
Rôles utilisateur.....	11
Création d'un rôle utilisateur.....	11
Modification d'un rôle utilisateur.....	15
Suppression d'un rôle utilisateur.....	16
Profils de sécurité.....	16
Priorité d'autorisation.....	17
Création d'un profil de sécurité.....	17
Modification d'un profil de sécurité.....	18
Duplication d'un profil de sécurité.....	19
Suppression d'un profil de sécurité.....	19
Comptes utilisateur.....	20
Affichage et modification des informations relatives à l'utilisateur en cours.....	20
Affichage de l'historique des connexions utilisateur.....	21
Création d'un compte d'utilisateur.....	21
Modification d'un compte utilisateur.....	22
Désactivation d'un compte utilisateur.....	23
Suppression d'un compte utilisateur.....	23
Suppression de recherches sauvegardées d'un utilisateur supprimé.....	24
Déverrouillage des comptes utilisateur verrouillés.....	24
Déverrouillage des comptes verrouillés.....	24
Authentification de l'utilisateur.....	25
Modification des mots de passe utilisateur QRadar.....	26
Configuration du délai d'attente d'inactivité pour un utilisateur.....	26
Instructions d'authentification externes.....	27
Configuration de l'authentification d'utilisateur.....	28
Configuration de l'authentification RADIUS.....	29
Configuration de l'authentification TACACS.....	30
Configuration de l'authentification par Active Directory.....	31
Authentification LDAP.....	32
Authentification unique à l'ouverture de session.....	41
<b>Chapitre 4. Gestion des licences.....</b>	<b>49</b>
Capacité de traitement des événements et des flux.....	49
Pool de licences partagé.....	50
Dimensionnement des capacités.....	51
Octroi de licence incrémentiel.....	51
Événements internes.....	52

Gestion des salves.....	52
Exemple : pointe de données entrantes.....	52
Téléchargement d'une clé de licence.....	54
Allocation d'une clé de licence à un hôte.....	55
Distribution de la capacité d'événement et de flux.....	55
Affichage des détails de la licence.....	56
Suppression de licences.....	57
Exportation des informations de licence.....	58

## **Chapitre 5. Gestion de systèmes..... 59**

Informations sur la santé du système.....	59
Types de composant QRadar.....	59
Noeuds de données.....	61
Rééquilibrage des données après l'ajout d'un nœud de données.....	61
Affichage de la progression du rééquilibrage des données.....	63
Sauvegarde de toutes les données d'événement sur un dispositif Noeud de données.....	63
Archivage du contenu Noeud de données.....	64
Gestion de l'interface réseau.....	64
Configuration des interfaces réseau.....	64
Temps système QRadar.....	66
Configuration de l'heure système.....	67
Réseaux NAT activé.....	68
Configuration d'un groupe NAT.....	68
Modification du statut NAT pour un hôte géré.....	69
Gestion des hôtes hors site.....	70
Configuration d'une source hors site.....	70
Configuration d'une cible hors site.....	71
Génération de clés publiques pour les produits QRadar.....	71
Transfert de flux filtrés.....	72
Exemple : transmission d'événements et de flux normalisés.....	72
Hôtes gérés.....	74
Remarques sur la largeur de bande pour les hôtes gérés.....	75
Chiffrement.....	76
Ajout d'un hôte géré.....	76
Ajout d'un hôte géré IPv4-only dans un environnement à deux piles.....	78
Configuration d'un hôte géré.....	79
Retrait d'un hôte géré.....	80
Configuration de votre pare-feu local.....	80
Ajout d'un serveur de messagerie.....	81
Modifications de configuration dans votre environnement QRadar.....	81
Modifications qui ont une incidence sur la collecte d'événements.....	82
Configuration de Collecteur d'événements.....	82
Déploiement des modifications.....	84
Redémarrage du service de collecte d'événements.....	84
Arrêt d'un système.....	84
Redémarrage d'un système.....	85
Collecte des fichiers journaux.....	85
Modification du mot de passe racine sur votre console QRadar.....	86
Réinitialisation du module SIM.....	86

## **Chapitre 6. QRadar des tâches de configuration.....87**

Hiérarchie du réseau.....	87
Instructions pour la définition de votre hiérarchie de réseau.....	87
Valeurs CIDR acceptables.....	88
Définition de votre hiérarchie réseau.....	90
Mises à jour automatiques.....	91
Affichage des mises à jour en attente.....	92

Configuration des paramètres de mise à jour automatique.....	94
Configuration des mises à jour derrière un serveur proxy qui utilise l'interception SSL ou TLS.....	95
Planification d'une mise à jour.....	95
Suppression des mises à jour planifiées.....	96
Recherche de nouvelles mises à jour.....	96
Installation manuelle des mises à jour automatiques.....	96
Affichage de l'historique des mises à jour.....	97
Restauration de mises à jour masquées.....	97
Affichage du journal des mises à jour automatiques.....	97
Mises à jour manuelles.....	97
Configuration d'un serveur de mises à jour.....	98
Configuration de la console QRadar en tant que serveur de mise à jour.....	99
Téléchargement des mises à jour du serveur de mises à jour.....	100
Configuration des paramètres système.....	100
Personnalisation du menu contextuel.....	101
Amélioration du menu contextuel pour les colonnes d'événements et de flux.....	102
Présentation des valeurs de conservation des actifs.....	104
Ajout ou édition d'un message de connexion QRadar.....	106
Activation et configuration de la visualisation des performances des règles.....	106
Certificats de serveur IF-MAP.....	109
Configuration du certificat de serveur IF-MAP pour l'authentification de base.....	109
Configuration du certificat de serveur IF-MAP pour l'authentification mutuelle.....	109
Certificats SSL.....	110
Connexions SSL entre les composants QRadar.....	111
Création d'une demande de signature de certificat SSL avec clés RSA 2048 bits.....	111
Création d'une demande de signature de certificat SSL multidomaine (SAN).....	112
Utilisation de certificats signés par une autorité de certification interne.....	113
Installation d'un nouveau certificat SSL.....	113
Rétablissement de certificats générés par l'autorité de certification locale QRadar.....	115
Adressage IPv6 dans les déploiements QRadar.....	115
Exemples de règles iptables avancées.....	117
Configuration des règles iptables.....	118
Conservation des données.....	119
Configuration des compartiments de conservation.....	120
Gestion de la séquence de compartiment de conservation.....	122
Activation et désactivation d'un compartiment de conservation.....	122
Suppression d'un compartiment de conservation.....	122
Notifications système.....	123
Configuration des notifications par courrier électronique d'événements et de flux.....	123
Configuration des notifications par courrier électronique de violation personnalisée.....	127
Motif de fermeture d'infraction personnalisée.....	129
Ajout d'un motif de fermeture d'infraction personnalisé.....	130
Édition de la raison de fermeture de l'infraction personnalisée.....	130
Suppression d'une raison de fermeture d'infraction personnalisée.....	130
Configuration d'une propriété d'actif personnalisée.....	131
Gestion de l'index.....	131
Activation des index.....	132
Activation de l'indexation de charge pour optimiser les temps de recherche.....	132
Configuration de la période de conservation des index de charge.....	133
Restrictions visant à empêcher les recherches à forte intensité de ressources.....	134
Types de restrictions de ressources.....	134
Restrictions de ressources dans les environnements répartis.....	135
Configuration des restrictions de ressources.....	136
Hôtes d'application.....	137
Installation d'un hôte d'application.....	138
Modification de l'emplacement d'exécution des applications.....	139
Migration depuis un noeud d'application vers un hôte d'application.....	140
Suppression d'un hôte d'application.....	143

Vérification de l'intégrité des journaux des événements et des flux.....	143
Activation du réadressage calculé de journal.....	144
Ajout d'actions personnalisées.....	145
Test de votre action personnalisée.....	147
Transmission de paramètres à un script d'action personnalisé.....	147
Gestion des vues de données agrégées.....	149
Accès à une base de données GLOBALVIEW.....	150
<b>Chapitre 7. Traitement des données d'événement dans QRadar.....</b>	<b>153</b>
Présentation de DSM Editor.....	153
Propriétés dans l'éditeur DSM.....	155
Configuration des propriétés dans l'éditeur DSM.....	156
Référencement des chaînes de capture à l'aide des zones de chaîne de format.....	156
Regex pour les journaux bien structurés.....	157
Regex pour les journaux de langue naturelle.....	158
Expressions au format JSON pour les données structurées.....	158
Expressions de chemin de clé JSON.....	159
Expressions au format LEEF pour les données structurées.....	161
Expressions au format CEF pour les données structurées.....	162
Expressions dans le format Pair de valeur de nom pour les données structurées.....	163
Expressions dans le format de liste générique pour les données structurées.....	163
Expressions au format XML pour les données structurées.....	164
Ouverture de l'éditeur DSM.....	164
Configuration d'un type de source de journal.....	165
Configuration de la détection automatique des propriétés pour les types de source de journal.....	165
Configuration de la détection automatique des sources de journal pour les types de source de journal.....	166
Configuration des paramètres DSM pour les types de source de journal.....	167
Types de source de journal personnalisés.....	168
Création d'un type de source de journal personnalisé pour analyser les événements.....	168
Définitions de propriétés personnalisées dans l'éditeur DSM.....	169
Création d'une propriété personnalisée.....	170
Expressions.....	172
Sélection.....	174
Mappage d'événement.....	174
Propriétés d'identité pour les mappages d'événements.....	174
Création d'une mappe d'événements et d'une catégorisation.....	175
Exportation de contenus à partir de l'éditeur DSM.....	175
Exportation du contenu en tant que package.....	176
Exportation de contenu pour une propriété personnalisée unique.....	176
<b>Chapitre 8. Utilisation des données de référence dans QRadar.....</b>	<b>179</b>
Types d'ensembles de données de référence.....	179
Présentation des jeux de références.....	181
Ajout, édition et suppression d'ensembles de références.....	181
Affichage des contenus d'un ensemble de référence.....	183
Ajout d'éléments à un ensemble de référence.....	184
Exportation d'éléments depuis un ensemble de référence.....	185
Suppression d'éléments dans un ensemble de référence.....	186
Création de collections de données de référence à l'aide de la ligne de commande.....	186
Référence de commande pour les utilitaires de données de référence.....	188
Création de collections de données de référence avec les API.....	190
Exemples de recueil de données de référence.....	193
Suivi des comptes utilisateur arrivés à expiration.....	193
Intégration de données dynamiques à partir de sources externes.....	194
<b>Chapitre 9. Configuration de la source d'informations utilisateur.....</b>	<b>195</b>

Présentation de la source d'informations utilisateur.....	195
source d'informations utilisateur.....	195
Collections de données de référence pour les informations utilisateur.....	196
Exemple de flux d'intégration.....	197
Présentation de la configuration de la source d'informations utilisateur et de la tâche de gestion.....	197
Configuration du serveur Tivoli Directory Integrator.....	198
Création et gestion de la source d'informations utilisateur.....	200
Création d'une source d'informations utilisateur.....	200
Extraction des sources d'informations utilisateur.....	201
Édition d'une source d'informations utilisateur.....	201
Suppression d'une source d'informations utilisateur.....	202
Collecte d'informations utilisateur.....	202
<b>Chapitre 10. Intégration d'IBM X-Force.....</b>	<b>205</b>
Flux X-Force Threat Intelligence.....	205
Activation du flux X-Force Threat Intelligence.....	205
Mise à jour des données X-Force dans un serveur proxy.....	205
Empêcher les données X-Force de télécharger des données localement.....	206
Extension de contenu IBM QRadar Security Threat Monitoring.....	207
Installation de l'application IBM QRadar Security Threat Monitoring Content Extension.....	207
IBM X-Force Exchange plug-in pour QRadar.....	208
Installation du plug-in IBM X-Force Exchange.....	208
<b>Chapitre 11. Gestion des services autorisés.....</b>	<b>211</b>
Affichage des services autorisés.....	211
Ajout d'un service autorisé.....	211
Révocation des services autorisés.....	212
<b>Chapitre 12. Sauvegarde et récupération.....</b>	<b>213</b>
Sauvegarde des configurations et des données QRadar.....	214
Planification de la sauvegarde nocturne.....	214
Création d'une archive de sauvegarde de configuration à la demande.....	217
Création d'une notification par courrier électronique pour une sauvegarde ayant échoué.....	217
Gérer les archives de sauvegarde existantes.....	220
Importation d'une archive de sauvegarde.....	220
Suppression d'une archive de sauvegarde.....	221
Restauration des données et des configurations QRadar.....	221
Restauration d'une archive de sauvegarde.....	222
Restauration d'une archive de sauvegarde créée sur un autre système QRadar.....	225
Restauration des données de.....	227
Vérification des données restaurées.....	228
Extraction des fichiers de sauvegarde manquants sur le disque.....	229
Les fichiers WinCollect ne sont pas restaurés lors d'une restauration de configuration.....	229
Applications de sauvegarde et de restauration.....	230
Sauvegarde et restauration d'applications.....	230
Sauvegarde et restauration de données d'application.....	231
Redondance des données et reprise dans les déploiements QRadar.....	232
QRadar Console Principal et sauvegarde QRadar Console.....	233
Événement et transfert de flux d'un centre de données principal vers un autre centre de données.....	234
Équilibrage de charge des événements et des flux entre deux sites.....	237
Restauration des données de configuration depuis le serveur principal vers le système QRadar Console secondaire.....	237
Redondance des données d'événement et de flux.....	238
Sauvegarde et restauration de QRadar Analyst Workflow.....	240

<b>Chapitre 13. Sources de flux.....</b>	<b>241</b>
Types de sources de flux.....	241
Ajout ou édition d'une source de flux.....	242
Transmission de paquets à QRadar Packet Capture.....	243
Activation et désactivation d'une source de flux.....	244
Suppression d'une source de flux.....	245
Alias de source de flux.....	245
Ajout d'un alias de source de flux.....	245
Suppression d'un alias de source de flux.....	245
Correction des horodatages de flux.....	246
<b>Chapitre 14. Configuration des réseaux et services distants.....</b>	<b>247</b>
Groupes de réseaux distants par défaut.....	247
Groupes de services distants par défaut.....	248
Instructions pour les ressources réseau.....	249
Gestion des objets de réseaux distants.....	249
Gestion des objets de services distants.....	250
<b>Chapitre 15. Reconnaissance des serveurs.....</b>	<b>251</b>
Reconnaissance des serveurs.....	251
<b>Chapitre 16. Segmentation de domaine.....</b>	<b>253</b>
Adresses IP de chevauchement.....	253
Balisage et définition de domaine.....	254
Création de domaines.....	257
Création de domaines pour les flux de réseau local virtuel.....	258
Privilèges de domaine dérivés des profils de sécurité.....	260
Règles et infractions spécifiques au domaine.....	261
Exemple : affectations de privilèges de domaine basées sur des propriétés personnalisées.....	264
<b>Chapitre 17. Gestion à service partagé.....</b>	<b>267</b>
Rôles utilisateur.....	267
Domaines et sources de journal.....	268
Mettre en place un nouveau titulaire.....	269
Surveillance de l'utilisation de la licence.....	270
Détection d'événements et de flux supprimés.....	272
Gestion des règles dans les déploiements multilocataires.....	272
Restriction des fonctions d'activité de journal pour les utilisateurs locataires.....	273
Mises à jour de la hiérarchie de réseau dans un déploiement multilocataires.....	273
Règles de conservation des locataires.....	274
<b>Chapitre 18. Gestion des actifs.....</b>	<b>275</b>
Sources des données d'actif.....	275
Flux des données d'actifs entrantes.....	276
Mises à jour des données d'actifs.....	278
Règles d'exclusion de rapprochement d'actifs.....	278
Fusion d'actifs.....	279
Identification des écarts de croissance d'actifs.....	280
Notifications système indiquant des écarts de croissance d'actifs.....	281
Exemple : comment les erreurs de configuration pour extensions de source de journal peuvent causer des écarts de croissance d'actifs.....	281
Traitement des problèmes des profils d'actifs qui dépassent le seuil de taille normale.....	281
De nouvelles données d'actifs sont ajoutées aux listes noires d'actifs.....	282
Prévention des écarts de croissance d'actifs.....	283
Données d'actif périmées.....	283



Listes noires et listes blanches d'actifs.....	284
Optimisation des paramètres de conservation du profileur d'actifs.....	288
Optimisation du nombre d'adresses IP autorisées pour un seul actif.....	289
Optimisation du nombre d'adresses MAC autorisées pour un seul actif.....	290
Recherches d'exclusion d'identité.....	290
Optimisation avancée des règles d'exclusion de rapprochement des actifs.....	292
Exemple : règles d'exclusion d'actifs ajustées pour exclure des adresses IP de la liste noire.....	294
Nettoyer les données d'actif après les écarts de croissance.....	294
Suppression d'actifs non valides.....	295
Suppression d'entrées de liste noire.....	295

## **Chapitre 19. Configuration de QRadar pour réacheminer des données à d'autres systèmes..... 297**

Ajout de destinations de réacheminement.....	297
Configuration des profils de transfert.....	299
Configuration des règles de routage pour réacheminer des données.....	299
Options de routage pour les règles.....	301
Configuration des règles de routage pour utiliser le magasin de données QRadar.....	302
Utilisation de règles personnalisées et de réponses de règle pour transmettre des données.....	303
Affichage des destinations de transfert.....	304
Affichage et gestion des destinations de transfert.....	304
Affichage et gestion des règles de routage.....	305

## **Chapitre 20. Magasin d'événements et transmission..... 307**

Affichage de la liste de planification de stockage et de réacheminement.....	307
Création d'un planning de stockage et de réacheminement.....	310
Édition d'une planification de magasin et de réacheminement.....	311
Suppression d'un planning de stockage et retransmission.....	311

## **Chapitre 21. Contenu de sécurité..... 313**

Types de contenu de sécurité.....	313
Méthodes d'importation et d'exportation de contenu.....	314
Exportation de tous les contenus personnalisés.....	314
Exportation de tous les contenus personnalisés d'un type spécifique.....	315
Recherche d'éléments de contenu spécifiques à exporter.....	317
Exportation d'un élément de contenu personnalisé unique.....	319
Exportation d'éléments de contenu personnalisés de types différents.....	320
Installation des extensions à l'aide d'extensions Management.....	322
Désinstallation d'une extension de contenu.....	323
Importation de contenu à l'aide du script de gestion de contenu.....	324
Mise à jour du contenu à l'aide du script de gestion de contenu.....	325
Identificateurs de type de contenu pour l'exportation de contenu personnalisé.....	326
Paramètres de script de gestion de contenu.....	327

## **Chapitre 22. Configuration des alertes SNMP..... 331**

Personnalisation des informations d'alerte SNMP envoyées à un autre système.....	331
Personnalisation de la sortie d'alerte SNMP.....	332
Ajout d'une alerte SNMP personnalisée à QRadar.....	334
Envoi d'alertes SNMP à un hôte spécifique.....	335

## **Chapitre 23. Protection des données sensibles..... 337**

Comment fonctionne le brouillage des données ?.....	337
Profils de brouillage de données.....	338
Expressions de brouillage de données.....	338
Scénario : brouiller les noms d'utilisateur.....	339
Création d'un profil de débrouillage des données.....	340

Création d'expressions de brouillage de données.....	341
Débrouillage des données pour qu'elles puissent être affichées dans la console.....	341
Éditer ou désactiver des expressions de brouillage créées dans les versions précédentes.....	342
<b>Chapitre 24. Fichiers journaux.....</b>	<b>345</b>
Journaux d'audit.....	345
Affichage du fichier journal d'audit.....	345
Création de rapports à partir de recherches de journaux d'audit dans QRadar.....	346
Actions consignées.....	347
<b>Chapitre 25. Catégories d'événement.....</b>	<b>353</b>
Catégories d'événements de haut niveau.....	353
Recon.....	355
DoS.....	356
Authentification.....	360
Accès.....	369
Exploitation.....	372
Logiciel malveillant.....	374
Activité suspecte.....	376
Système.....	381
Politique.....	386
Inconnu.....	388
CRE.....	388
Utilisation potentielle.....	389
Flux.....	390
Défini par l'utilisateur.....	392
Audit SIM.....	396
Découverte d'hôte VIS.....	397
Application.....	397
Audit.....	424
Risque.....	428
Audit Risk Manager.....	430
Contrôle.....	430
Profileur d'actif.....	433
Sense.....	438
<b>Chapitre 26. Ports et serveurs courants utilisés par QRadar.....</b>	<b>441</b>
Utilisation du port QRadar.....	441
Affichage des associations de ports IMQ.....	450
Recherche des ports utilisés par QRadar.....	451
Serveurs QRadar publics.....	451
Conteneurs de Docker et interfaces réseau.....	452
<b>Chapitre 27. API RESTful.....</b>	<b>455</b>
Accès à la page de documentation interactive de l'API.....	455
<b>Remarques.....</b>	<b>457</b>
Marques.....	458
Dispositions pour la documentation du produit.....	459
Déclaration de confidentialité en ligne d'IBM.....	459
Règlement général sur la protection des données (RGPD).....	460
<b>Glossaire.....</b>	<b>461</b>
A.....	461
B.....	461
C.....	462
D.....	462

E.....	463
F.....	463
G.....	464
H.....	464
I.....	464
K.....	465
L.....	465
M.....	465
N.....	466
O.....	466
P.....	466
Q.....	467
R.....	467
S.....	468
T.....	469
V.....	469
W.....	469

<b>Index.....</b>	<b>471</b>
-------------------	------------



# Introduction à l'administration des produits QRadar

---

Les administrateurs utilisent IBM® QRadar SIEM pour gérer les tableaux de bord, les infractions, l'activité des journaux, l'activité réseau, les actifs et les rapports.

## Utilisateurs concernés

Ce guide est destiné à tous les utilisateurs QRadar SIEM responsables de l'investigation et de la gestion de la sécurité du réseau. Ce guide suppose que vous disposez d'un accès QRadar SIEM et d'une connaissance de votre réseau d'entreprise et de vos technologies de réseau.

## Documentation technique

Pour rechercher la documentation produit IBM QRadar sur le Web, y compris toute la documentation traduite, accédez à [IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) (<http://www.ibm.com/support/knowledgecenter/SS42VS/welcome>).

Pour plus d'informations sur l'accès à d'autres documents techniques dans la bibliothèque de produits QRadar, voir la [note technique relative à l'accès à la documentation IBM](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) ([www.ibm.com/support/docview.wss?rs=0&uid=swg21614644](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)).

## Contactez le service clients

Pour savoir comment contacter le service clients, consultez la [note technique relative au service de support et aux téléchargements](http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

## Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention, la détection et la réponse aux accès non autorisés au sein comme à l'extérieur de votre entreprise. Un accès non autorisé peut se traduire par la modification, la destruction, ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Non. Aucun produit ou service informatique ne doit être considéré comme parfaitement sûr et aucun produit, service ou mesure de sécurité ne peut être totalement efficace contre une utilisation inappropriée ou un accès non autorisé. Les systèmes et les produits IBM sont conçus pour s'intégrer à une approche de sécurité complète, ce qui implique nécessairement des procédures opérationnelles supplémentaires, et ils peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITÉ DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITÉ DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

### Remarque :

Diverses lois et réglementations peuvent régir l'utilisation de ce Logiciel, y compris celles relatives à la confidentialité, à la protection des données, à l'emploi, aux communications électroniques et à l'archivage. IBM QRadar ne peut être utilisé qu'à des fins légales et de façon légale. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le Détenteur de la Licence déclare qu'il obtiendra ou a obtenu tous les accords, droits ou licences nécessaires à l'utilisation légale d'IBM QRadar.



# Chapitre 1. Nouveautés pour les administrateurs

Découvrez les nouvelles fonctions et fonctionnalités qui vous permettent de configurer et d'administrer votre déploiement IBM QRadar.

## Nouvelles fonctions et améliorations dans QRadar 7.4.3

Les nouvelles fonctions et améliorations suivantes permettent aux administrateurs de gérer plus facilement leur déploiement IBM QRadar 7.4.3.

Pour afficher la liste de toutes les nouvelles fonctions de cette édition, consultez le document *Nouveautés* sur le [Centre de connaissances IBM](http://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pdf_launch.html) (www.ibm.com/support/knowledgecenter/SS42VS\_latest/com.ibm.qradar.doc/c\_pdf\_launch.html).

### Seuil de taille de lot du nettoyage des actifs

Dans QRadar 7.4.3, vous pouvez ajuster le nombre d'actifs à partir duquel un lot d'actifs est nettoyé. Vous pouvez configurer cette valeur si le nombre d'actifs peut dépasser la durée maximale autorisée par le pool de connexions à la base de données. En général, si l'agent de nettoyage des actifs ne rencontre pas de problème de pool de connexions, vous n'avez pas besoin de modifier cette valeur de configuration.

Entrez le nombre dans la zone **Nombre d'adresses MAC autorisées pour un actif unique** de la fenêtre **Configuration du profileur d'actif**.

Figure 1. Fenêtre Configuration du profileur d'actif

Asset Profiler Configuration	
<b>Asset Profile Settings</b>	
Asset Profile Retention Period	Use Advanced
Enable DNS Lookups for Host Identity	True
Enable WINS Lookups for Host Identity	True
Enable Real-Time DNS Lookups for Asset Profiles	True
<b>Asset Profiler Configuration</b>	
Asset Profiler Audit Events Per Minute Threshold	6,000
Number of Grey List Ports Per Asset	100
Enable Identity Profiling	True
Enable Client Application Profiling	True
Enable Open Port Profiling	True
Number of IPs Allowed for a Single Asset	96
Number of MAC Addresses Allowed for a Single Asset	10
Unified Asset Name	NetBIOS Name
Enable IP Reconciliation Blacklisting	True
Asset Identity Coalescing	15 minutes
<input type="checkbox"/> Coalesce Ownership Changes	
<b>Asset Profiler Retention Configuration</b>	
Asset Cleanup Batch Size Threshold	1,000
Clean Entire Asset	False
Retain Assets with Vulnerabilities	False

### Les jetons de service autorisés ne sont plus visibles après la création

Lorsque vous créez un jeton de service autorisé, le jeton s'affiche dans la boîte de dialogue **Service autorisé créé avec succès**. À partir de QRadar 7.4.3, le jeton de service autorisé ne peut pas être à nouveau visible après la fermeture de la boîte de dialogue **Service autorisé créé avec succès**. Copiez le jeton dans un emplacement sécurisé avant de fermer la boîte de dialogue.

## Services autorisés avec des configurations non valides

Lorsque vous effectuez une mise à niveau vers QRadar 7.4.3 ou une version ultérieure, tous les services autorisés avec le droit "Administrateur système" arrivent à expiration, sauf s'ils sont affectés au profil de sécurité "Admin".

Pour réactiver un service autorisé expiré après une mise à niveau, vous devez mettre à jour le rôle utilisateur et le profil de sécurité du service autorisé à une combinaison valide et réinitialiser la date d'expiration.

1. Dans l'onglet **Admin**, cliquez sur **Authorized Services**.
2. Sélectionnez le service autorisé à réactiver.
3. Cliquez sur **Editer le nom du service autorisé**
4. Affectez un rôle utilisateur et une combinaison de profil de sécurité valides.
5. Définissez la date d'expiration du service autorisé à une date ultérieure ou supprimez la date d'expiration si vous ne souhaitez pas que le service autorisé expire.

## Fichiers journaux chiffrés

Vous pouvez désormais définir vos propres mots de passe pour les fichiers journaux chiffrés. Lorsque vous envoyez des fichiers journaux chiffrés au service clients IBM, vous devez également fournir un mot de passe pour que les fichiers journaux soient déchiffrés.

Dans les versions antérieures, vous n'étiez pas capable de définir un mot de passe et les fichiers journaux étaient uniquement déchiffrés par le service clients IBM.

## Nouveau protocole de destination de réacheminement

IBM QRadar 7.4.3 inclut un nouveau protocole de destination de réacheminement **TCP sur TLS 1.1 et supérieur** qui garantit une connexion plus sécurisée à l'hôte de réacheminement.

Avec le nouveau protocole, vous pouvez confirmer que l'hôte de destination correspond au *nom usuel* ou au *nom secondaire du sujet* du certificat présenté par le serveur destination.

Lorsque vous configurez la destination de réacheminement, vous pouvez activer l'authentification du client et utiliser l'application QRadar Certificate Management pour télécharger le certificat client que vous souhaitez utiliser pour l'authentification.

## Noms de fichier de certificat SAML

Lorsque vous sélectionnez le certificat QRadar\_SAML sous **Certificat de signature et de chiffrement**, les noms de fichier des fichiers CRL de l'autorité de certification racine et de l'autorité de certification racine QRadar sont modifiés.

- **vault-qrd\_ca.pem** est remplacé par **root-qradar-ca\_ca**
- **vault-qrd\_ca.crl** est remplacé par **root-qradar-ca\_ca.crl**

**Important :** Vous devez reconfigurer SAML après la mise à jour vers QRadar 7.4.3.

## Nouvelles fonctions et améliorations dans QRadar 7.4.2

---

Les nouvelles fonctions et améliorations suivantes permettent aux administrateurs de gérer plus facilement leur déploiement IBM QRadar 7.4.2.

Pour afficher la liste de toutes les nouvelles fonctions de cette édition, consultez le document *Nouveautés* sur le [Centre de connaissances IBM](http://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pdf_launch.html) ([www.ibm.com/support/knowledgecenter/SS42VS\\_latest/com.ibm.qradar.doc/c\\_pdf\\_launch.html](http://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pdf_launch.html)).



## Modification du nombre d'adresses MAC autorisées pour un actif

Dans QRadar 7.4.2, vous pouvez modifier le nombre d'adresses MAC autorisées pour un seul actif. Dans les versions précédentes de QRadar, les administrateurs ne pouvaient pas modifier ce nombre. Un message d'erreur indiquait alors que le nombre d'adresses MAC était trop élevé pour l'actif. Entrez le nombre souhaité dans la zone **Nombre d'adresses MAC autorisées pour un actif unique** dans la fenêtre **Configuration du profileur d'actif**.

Si vous avez des utilisateurs qui se connectent à partir de plusieurs points d'accès sans fil, ou plusieurs utilisateurs qui se connectent à distance via un réseau privé virtuel, vous pouvez définir le nombre d'adresses MAC autorisées pour l'actif de la même façon que pour les adresses IP.

Figure 2. Fenêtre Configuration du profileur d'actif

Asset Profiler Configuration	
Asset Profile Settings	
Asset Profile Retention Period	Use Advanced
Enable DNS Lookups for Host Identity	True
Enable WINS Lookups for Host Identity	True
Enable Real-Time DNS Lookups for Asset Profiles	True
Asset Profiler Configuration	
Asset Profiler Audit Events Per Minute Threshold	6,000
Number of Grey List Ports Per Asset	100
Enable Identity Profiling	True
Enable Client Application Profiling	True
Enable Open Port Profiling	True
Number of IPs Allowed for a Single Asset	75
<b>Number of MAC Addresses Allowed for a Single Asset</b>	<b>10</b>
Unified Asset Name	NetBIOS Name
Enable IP Reconciliation Blacklisting	True
Asset Identity Coalescing	15 minutes <input type="checkbox"/> Coalesce Ownership Changes
Asset Profiler Retention Configuration	
Clean Entire Asset	False
Retain Assets with Vulnerabilities	False

Ensure that the **Asset Profile Retention Period** is set to **Use Advanced**, otherwise any of the the following retention periods that you select will not be applied.

## Génération d'expression régulière pour l'analyse des propriétés d'événement

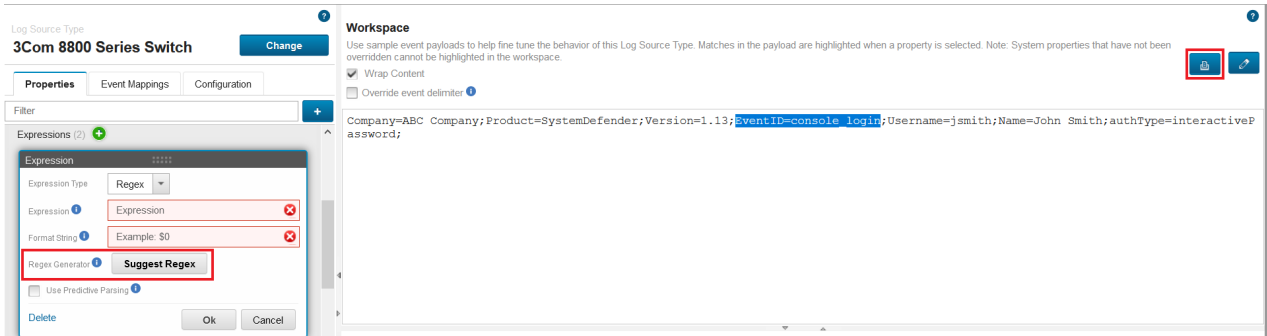
QRadar 7.4.2 peut suggérer des expressions régulières (regex) lorsque vous entrez des données d'événement dans l'**Espace de travail**. Si vous n'êtes pas habitué à créer des expressions régulières, utilisez cette fonction pour cela.


Mettez en évidence le texte que vous souhaitez capturer puis dans l'onglet **Propriétés**, cliquez sur **Suggérer une expression régulière**. L'expression suggérée s'affiche dans la zone **Expression**. Vous pouvez également cliquer sur le bouton **Expression régulière** dans l'**Espace de travail** puis sélectionner la propriété pour laquelle créer une expression. Si QRadar ne peut pas générer d'expression régulière adaptée à votre exemple de données, un message système s'affiche.

**Conseil :** Le générateur d'expression régulière est particulièrement adapté pour les zones des contenus d'événement bien structurés. Si le contenu se compose de données complexes (langage naturel ou événements non structurés), le générateur d'expression régulière peut ne pas pouvoir l'analyser et ne renvoie alors pas de résultat.

La figure suivante présente comment vous pouvez générer votre expression régulière en utilisant le bouton **Suggérer une expression régulière** dans l'onglet **Propriétés** ou le bouton **Expression régulière** dans l'**Espace de travail**.

Figure 3. Bouton Suggérer une expression régulière



 [En savoir plus sur l'espace de travail de l'éditeur DSM...](#)

## Nouvelles fonctions et améliorations dans QRadar 7.4.1

Les nouvelles fonctions et améliorations suivantes permettent aux administrateurs de gérer plus facilement leur déploiement IBM QRadar 7.4.1.

Pour afficher la liste de toutes les nouvelles fonctions de cette édition, consultez le document *Nouveautés* sur le Centre de connaissances IBM ([www.ibm.com/support/knowledgecenter/SS42VS\\_latest/com.ibm.qradar.doc/c\\_pdf\\_launch.html](http://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pdf_launch.html)).

## Nouvelles fonctions et améliorations dans QRadar V7.4.0

Les nouvelles fonctions et améliorations suivantes permettent aux administrateurs de gérer plus facilement leur déploiement IBM QRadar V7.4.0.

Pour afficher la liste de toutes les nouvelles fonctions de cette édition, consultez le document *Nouveautés* sur Centre de connaissances IBM ([www.ibm.com/support/knowledgecenter/SS42VS\\_7.4.0/com.ibm.qradar.doc/c\\_pdf\\_launch.html](http://www.ibm.com/support/knowledgecenter/SS42VS_7.4.0/com.ibm.qradar.doc/c_pdf_launch.html)).


### Configuration des notifications système globales

Les notifications système globales sont désormais locales, ce qui fait qu'elles sont spécifiques à l'hôte et plus utiles. Par conséquent, les seuils sont désormais définis automatiquement par QRadar et la section des notifications système globales de l'onglet Admin a été retirée.

### Serveur de messagerie sécurisé

Envoyez un e-mail pour distribuer des alertes, des rapports, des notifications et des messages d'événement à des serveurs de messagerie nécessitant une authentification.

Vous pouvez configurer un serveur de messagerie pour l'ensemble de votre déploiement QRadar ou plusieurs serveurs de messagerie.

 [En savoir plus sur la configuration du serveur de messagerie sécurisé...](#)

### Prise en charge du paramètre DSM dans l'éditeur DSM

Dans QRadar 7.4.0, si votre type de source de journal contient des paramètres DSM, vous pouvez utiliser l'éditeur DSM pour configurer ces derniers. Activez l'option **Afficher la configuration des paramètres DSM** pour afficher et modifier les paramètres DSM.

## Juniper Steel-Belted Radius

[Change](#)

Properties

Event Mappings

**Configuration**

### DSM Parameters Configuration

#### Display DSM Parameters Configuration

If there are any DSM Parameters for this log source type, enable this option to view and edit those DSM Parameters.



#### Event Collector

Default

The Default parameter set applies to all instances of this DSM in the deployment which do not have an Event Collector-specific override. To set different parameter values for this DSM for a specific Event Collector select it from the list and override the Default settings.

#### User Field

User-Name

Customize JunipserSBR DSM to fields mapping

#### Full Name Field

Full-Name

Customize JunipserSBR DSM to fields mapping

#### Source IP Field

Source-IP-Add

Customize JunipserSBR DSM to fields mapping

#### Source Port Field

Source-UDP-F

Customize JunipserSBR DSM to fields mapping

#### Destination IP Field

Customize JunipserSBR DSM to fields mapping

#### Destination Port Field

Target-UDP-Pc

Customize JunipserSBR DSM to fields mapping

[En savoir plus sur la configuration des paramètres DSM dans l'éditeur DSM...](#)

## Lancement du tunnel inverse

Le tunnel SSH entre deux hôtes gérés peut désormais être lancé à partir de l'hôte distant plutôt qu'à partir de l'hôte local. Par exemple, vous disposez d'une connexion entre un processeur d'événement dans un environnement sécurisé et un collecteur d'événements se trouvant en dehors de l'environnement sécurisé. Vous disposez également d'une règle de pare-feu qui vous empêche d'avoir un hôte en dehors de l'environnement sécurisé qui est connecté à un hôte dans l'environnement sécurisé. Dans QRadar 7.4.0, vous pouvez changer l'hôte qui crée le tunnel pour que la connexion soit établie à partir du processeur d'événement en cochant la case Déclenchement du tunnel distant pour le collecteur d'événements.

[En savoir plus sur l'initiation du tunnel inversé...](#)

## Gestion améliorée de l'horodatage de flux

Deux nouveaux paramètres de configuration fournissent davantage de contrôle sur la gestion des horodatages de flux lorsque Netflow V9 commence à envoyer des enregistrements avec des valeurs de disponibilité système dépassée. Les nouveaux paramètres éliminent le besoin de réinitialisation lors de la première et de la dernière période de commutation.

Les nouvelles options de configuration et valeurs par défaut sont présentées ici :

- NORMALISE\_OVERFLOWED\_UPTIMES=YES
- UPTIME\_OVERFLOW\_THRESHOLD\_MSEC=86400000

Les horodatages sont corrigés lorsque la valeur de disponibilité du système est inférieure à la première et à la dernière période de paquets commutés de plus de la valeur spécifiée dans la configuration UPTIME\_OVERFLOW\_THRESHOLD\_MSEC. Les horodatages sont corrigés sur la base de l'hypothèse que la disponibilité du système correspondait à peu près à la valeur 32 bits maximale.

 [En savoir plus sur la gestion des horodatages de flux...](#)

## Chapitre 2. Administration QRadar

En tant qu'administrateur IBM QRadar, vous disposez d'une variété d'outils pour vous aider à configurer et gérer votre déploiement QRadar.

Par exemple, à l'aide des outils de l'onglet **Admin**, vous pouvez effectuer les tâches suivantes :

- Déployer et gérer des hôtes et des licences QRadar.
- Configurer les comptes utilisateur et l'authentification.
- Créer une hiérarchie de réseau.
- Configurer les domaines et configurez un environnement multi-locataires.
- Définir et gérer les sources de données de flux et de journal.
- Gérer la conservation des données QRadar.
- Gérer les actifs et les données de référence.
- Planifier des sauvegardes régulières de la configuration et des données QRadar.
- Surveiller la santé du système des hôtes gérés.

### Fonctions de votre produit IBM QRadar

La documentation du produit IBM QRadar décrit des fonctionnalités, notamment les infractions, les flux, les actifs et la corrélation d'historique, qui ne sont pas toujours disponibles dans les produits QRadar. Selon le produit que vous utilisez, certaines des fonctionnalités décrites peuvent ne pas être disponibles dans votre déploiement.

#### IBM QRadar Log Manager

QRadar Log Manager est une solution de base haute performance et évolutive pour la collecte, l'analyse, le stockage et la génération de rapports sur de grands volumes de données de journaux d'événements réseau et sécurité.

#### IBM QRadar SIEM

QRadar SIEM est une offre avancée qui inclut la gamme complète de fonctions de renseignement de sécurité pour les déploiements sur site. Elle consolide les données de flux de source de journal et de réseau provenant de milliers d'actifs, d'unités, de noeuds finaux et d'applications répartis au sein de votre réseau, puis réalise immédiatement des activités de normalisation et de corrélation sur les données brutes de manière à distinguer les menaces réelles des faux positifs.

#### IBM QRadar on Cloud

QRadar on Cloud fournit des professionnel de la sécurité IBM pour gérer l'infrastructure, pendant que vos analystes de sécurité effectuent les tâches de détection et de gestion des menaces. Vous pouvez protéger votre réseau et respecter les exigences de surveillance et de production de rapports avec un coût total de possession réduit.

### Fonctions des produits QRadar

Consultez le tableau suivant pour comparer les fonctions de chaque produit QRadar.

Fonctions	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Fonctions d'administration complètes	Oui	Non	Oui
Prend en charge les déploiements hébergés	Non	Oui	Non

Tableau 1. Comparaison des fonctions de QRadar (suite)

Fonctions	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
Tableaux de bords personnalisables	Oui	Oui	Oui
Moteur de règles personnalisé	Oui	Oui	Oui
Gestion des événement réseau et des événements de sécurité	Oui	Oui	Oui
Gestion des hôtes et des journaux d'application	Oui	Oui	Oui
Alertes basées sur les seuils	Oui	Oui	Oui
Modèles de conformité	Oui	Oui	Oui
Archivage des données	Oui	Oui	Oui
Intégration de flux de réputation IP IBM Security X-Force Threat Intelligence	Oui	Oui	Oui
Déploiements WinCollect autonomes	Oui	Oui	Oui
Déploiements WinCollect gérés	Oui	Non	Oui
Surveillance de l'activité réseau	Oui	Oui	Non
Profilage d'actif	Oui	Oui	Non <sup>1</sup>
Gestion des infractions	Oui	Oui	Non
Capture et analyse du flux réseau	Oui	Oui	Non
Corrélation d'historique	Oui	Oui	Non
Intégration de QRadar Network Insights	Oui	Oui	Non
Intégration de QRadar Vulnerability Manager	Oui	Oui	Oui
Intégration de QRadar Risk Manager	Oui	Non	Non
Intégration de QRadar Incident Forensics	Oui	Non	Non
Scanners d'évaluation des vulnérabilités	Oui	Oui	Oui
<sup>1</sup> QRadar Log Manager n'effectue un suivi des données d'actif que si QRadar Vulnerability Manager est installé.			

Certains documents, tels que le *Guide d'administration* et le *Guide d'utilisation*, sont communs à plusieurs produits et peuvent décrire des fonctions qui ne sont pas disponibles dans votre déploiement. Par exemple, les utilisateurs d'IBM QRadar on Cloud ne disposent pas des fonctions d'administration complètes décrites dans le manuel *IBM QRadar Administration Guide*.

## Navigateurs Web pris en charge

Pour que les fonctions des produits IBM QRadar fonctionnent correctement, vous devez utiliser un navigateur Web pris en charge.

Le tableau ci-après répertorie les versions de navigateurs Web pris en charge.

Tableau 2. Navigateurs Web pris en charge par les produits QRadar

<b>Navigateur Web</b>	<b>Versions prises en charge</b>
64 bits Mozilla Firefox	60 Extended Support Release et versions ultérieures
Microsoft Edge 64 bits	38.14393 et versions ultérieures
64 bits Google Chrome	Dernière version disponible

Le navigateur Web Microsoft Internet Explorer n'est plus pris en charge sur QRadar 7.4.0 ou les versions ultérieures.

### **Exceptions et certificats de sécurité**

Si vous utilisez le navigateur Web Mozilla Firefox, vous devez ajouter une exception à Mozilla Firefox pour pouvoir vous connecter à QRadar. Pour plus d'informations, voir la documentation de votre navigateur Web Mozilla Firefox.

### **Accès à l'application Web**

Lorsque vous utilisez QRadar, utilisez les options de navigation disponibles dans QRadar Console au lieu du bouton **Retour** de votre navigateur.





---

## Chapitre 3. Gestion des utilisateurs

Vous définissez les rôles utilisateur, les profils de sécurité et les comptes utilisateur pour contrôler qui a accès à IBM QRadar, les tâches qu'ils peuvent effectuer et les données auxquelles ils ont accès.

Lors de la configuration initiale de QRadar, utilisez la fonction **Gestion des utilisateurs** dans l'onglet **Admin** pour configurer et gérer les comptes utilisateur pour tous les utilisateurs qui ont besoin d'accéder à QRadar.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Rôles utilisateur

Un rôle utilisateur définit les fonctions accessibles à un utilisateur dans IBM QRadar.

Au cours de l'installation, quatre rôles utilisateur par défaut sont définis : **Admin**, **Tous**, **WinCollect** et **Désactivé**.

Avant d'ajouter des comptes utilisateur, vous devez créer les rôles utilisateur pour répondre aux exigences d'autorisation de vos utilisateurs.

## Création d'un rôle utilisateur

Créez des rôles utilisateur pour gérer les fonctions accessibles à un utilisateur dans IBM QRadar.

### Pourquoi et quand exécuter cette tâche

Par défaut, votre système fournit un rôle d'administrateur par défaut, qui permet d'accéder à toutes les zones de QRadar. Les utilisateurs affectés à un rôle d'administrateur ne peuvent pas modifier leur propre compte. Cette restriction s'applique au rôle utilisateur Admin par défaut. Un autre utilisateur d'administration doit effectuer des modifications de compte.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Rôles utilisateur**.
2. Dans la barre d'outils, cliquez sur **Nouveau**.
3. Dans la zone **Nom de rôle utilisateur**, entrez un nom unique pour ce rôle utilisateur.
4. Sélectionnez les droits que vous souhaitez affecter au rôle utilisateur.

Les droits d'accès visibles dans la fenêtre **Gestion des rôles utilisateur** dépendent des composants QRadar installés.

<i>Tableau 3. Droits d'accès aux fenêtres</i> <b>Gestion des rôles utilisateur</b>	
<b>Autorisation</b>	<b>Description</b>
<b>Admin</b>	<p>Accorde l'accès administratif à l'interface utilisateur. Vous pouvez accorder des droits d'administration spécifiques.</p> <p>Les utilisateurs disposant des droits d'accès <b>Administrateur système</b> peuvent accéder à toutes les zones de l'interface utilisateur. Les utilisateurs qui disposent de cet accès ne peuvent pas éditer d'autres comptes administrateur.</p> <p><b>Gestionnaire d'administration</b> Permet aux utilisateurs de créer et d'éditer d'autres comptes administrateur.</p> <p><b>Configuration de réseaux distants et de services</b> Accorde aux utilisateurs l'accès à l'icône Réseaux et services distants dans l'onglet <b>Admin</b>.</p> <p><b>Administrateur système</b> Permet aux utilisateurs d'accéder à toutes les zones de l'interface utilisateur. Les utilisateurs disposant de cet accès ne peuvent pas modifier d'autres comptes administrateur.</p>
<b>Administration déléguée</b>	<p>Permet aux utilisateurs d'effectuer des fonctions d'administration limitées. Dans un environnement à plusieurs titulaires, les utilisateurs titulaires dotés des droits <b>Administration déléguée</b> peuvent uniquement afficher les données de leur propre environnement titulaire. Si vous affectez d'autres droits d'administration qui ne font pas partie de <b>Administration déléguée</b>, les utilisateurs locataires peuvent voir des données pour tous les locataires.</p>
<b>Infractions</b>	<p>Accorde l'accès administratif à toutes les fonctions de l'onglet <b>Offenses</b>.</p> <p>Les utilisateurs doivent disposer d'un accès administrateur pour créer ou éditer un groupe de recherche dans l'onglet <b>Offenses</b>.</p> <p>Les rôles utilisateur doivent disposer du droit <b>Gestion des règles personnalisées</b> pour créer et éditer des règles personnalisées.</p>

Tableau 3. Droits d'accès aux fenêtres **Gestion des rôles utilisateur** (suite)

Autorisation	Description
<p><b>Activité du journal</b></p>	<p>Accorde l'accès aux fonctions dans l'onglet <b>Activité de journal</b>. Vous pouvez également accorder des droits spécifiques :</p> <p><b>Gestion des règles personnalisées</b> Accorde le droit de créer ou d'éditer des règles affichées dans l'onglet <b>Activité de journal</b></p> <p><b>Gérer les séries temporelles</b> Accorde le droit de configurer et d'afficher les graphiques de données de série temporelle.</p> <p><b>Propriétés d'événement définies par l'utilisateur</b> Accorde le droit de créer des propriétés d'événement personnalisées.</p> <p><b>Afficher les règles personnalisées</b> Accorde le droit d'afficher des règles personnalisées. S'il est accordé à un rôle utilisateur qui ne dispose pas également des droits <b>Gestion des règles personnalisées</b>, le rôle utilisateur ne peut pas créer ou modifier de règles personnalisées.</p>
<p><b>Activité réseau</b></p>	<p>Accorde l'accès à toutes les fonctions de l'onglet <b>Activité réseau</b>. Vous pouvez accorder un accès spécifique aux droits suivants :</p> <p><b>Gestion des règles personnalisées</b> Accorde le droit de créer ou d'éditer des règles affichées dans l'onglet <b>Activité réseau</b>.</p> <p><b>Gérer les séries temporelles</b> Accorde le droit de configurer et d'afficher les graphiques de données de série temporelle.</p> <p><b>Propriétés de flux définies par l'utilisateur</b> Accorde le droit de créer des propriétés de flux personnalisées.</p> <p><b>Afficher les règles personnalisées</b> Accorde le droit d'afficher des règles personnalisées. Si le rôle utilisateur ne dispose pas également des droits d'accès <b>Gestion des règles personnalisées</b>, le rôle utilisateur ne peut pas créer ou modifier de règles personnalisées.</p> <p><b>Afficher le contenu du flux</b> Accorde le droit de visualiser la charge source et la charge de destination dans les détails des données de flux.</p>

Tableau 3. Droits d'accès aux fenêtres <b>Gestion des rôles utilisateur</b> (suite)	
Autorisation	Description
<b>Actifs</b>	<p>Cette autorisation s'affiche uniquement si IBM QRadar Vulnerability Manager est installé sur votre système.</p> <p>Accorde l'accès à la fonction dans l'onglet <b>Actifs</b>. Vous pouvez accorder des droits spécifiques :</p> <p><b>Exécution des analyses VA</b> Accorde la permission d'effectuer des analyses d'évaluation de la vulnérabilité. Pour plus d'informations sur l'évaluation de la vulnérabilité, voir le <i>Guide d'évaluation de gestion de la vulnérabilité</i>.</p> <p><b>Supprimer les vulnérabilités</b> Accorde le droit de supprimer les vulnérabilités des actifs.</p> <p><b>Reconnaissance de serveur</b> Accorde le droit de reconnaître les serveurs.</p> <p><b>Afficher les données VA</b> Accorde la permission aux données d'évaluation de la vulnérabilité. Pour plus d'informations sur l'évaluation de la vulnérabilité, voir le <i>Guide d'évaluation de gestion de la vulnérabilité</i>.</p>
<b>Rapports</b>	<p>Accorde le droit d'accéder à toutes les fonctions de l'onglet <b>Rapports</b>.</p> <p><b>Distribuer les rapports par courrier électronique</b> Accorde la permission de distribuer des rapports par courrier électronique.</p> <p><b>Gestion des modèles</b> Accorde le droit d'éditer des modèles de rapport.</p>
<b>Risk Manager</b>	Accorde aux utilisateurs la permission d'accéder aux fonctions QRadar Risk Manager . QRadar Risk Manager doit être activé.
<b>Gestionnaire de vulnérabilités</b>	<p>Accorde le droit d'accès à la fonction QRadar Vulnerability Manager . QRadar Vulnerability Manager doit être activé.</p> <p>Pour plus d'informations, voir <i>IBM QRadar Vulnerability Manager - Guide d'utilisation</i>.</p>
<b>Analyse légale</b>	<p>Accorde le droit d'accès aux fonctions QRadar Incident Forensics.</p> <p><b>Créer des cas dans l'incident d'analyse légale</b> Accorde le droit de créer des dossiers pour les ensembles de documents importés et les fichiers pcap.</p>
<b>Extensions du menu de clic droit IP</b>	Accorde le droit d'accès aux options ajoutées au menu contextuel.

Tableau 3. Droits d'accès aux fenêtres <b>Gestion des rôles utilisateur</b> (suite)	
Autorisation	Description
<b>Configuration de la plateforme</b>	<p>Accorde le droit d'accès aux services <b>Configuration de la plateforme</b>.</p> <p><b>Notifications système de déconnexion</b> Accorde le droit de masquer les notifications système à partir de l'onglet <b>Messages</b>.</p> <p><b>Afficher les données de référence</b> Accorde le droit d'afficher les données de référence lorsqu'elles sont disponibles dans les résultats de la recherche.</p> <p><b>Afficher les notifications système</b> Accorde le droit d'afficher les notifications système à partir de l'onglet <b>Messages</b>.</p>
<b>Gestion des sources de journal QRadar</b>	Accorde le droit d'accès à l'application QRadar Log Source Management.
<b>Pulse - Tableau de bord</b>	Accorde la permission aux tableaux de bord de l'application IBM QRadar Pulse.
<b>Pulse - Threat Globe</b>	Accorde le droit d'accès au tableau de bord Threat Globe dans l'application IBM QRadar Pulse.
<b>Assistant QRadar</b>	Accorde le droit d'accès à l'application IBM QRadar Assistant.
<b>Utilisation QRadar Case Manager</b>	Accorde le droit d'accès à l'application QRadar Use Case Manager.

5. Dans la zone **Tableaux de bord**, sélectionnez les tableaux de bord auxquels vous souhaitez que le rôle utilisateur ait accès, puis cliquez sur **Ajouter**.

**Remarque :** Un tableau de bord n'affiche aucune information lorsque le rôle utilisateur n'est pas autorisé à afficher les données du tableau de bord. Si un utilisateur modifie les tableaux de bord affichés, ceux qui sont définis pour le rôle utilisateur s'affichent lors de la connexion suivante.

6. Cliquez sur **Sauvegarder** et fermez la fenêtre **Gestion des rôles utilisateur**.
7. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Modification d'un rôle utilisateur

Vous pouvez éditer un rôle existant pour modifier les droits affectés au rôle.

### Pourquoi et quand exécuter cette tâche

Pour localiser rapidement le rôle utilisateur que vous souhaitez éditer dans la fenêtre **Gestion des rôles utilisateur**, vous pouvez entrer un nom de rôle dans la zone de texte **Type à filtrer**.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Rôles utilisateur**.
2. Dans la sous-fenêtre de gauche de la fenêtre **Gestion des rôles utilisateur**, sélectionnez le rôle utilisateur que vous souhaitez modifier.
3. Dans la sous-fenêtre de droite, mettez à jour les autorisations si nécessaire.
4. Modifiez les options **Tableaux de bord** pour le rôle utilisateur si nécessaire.
5. Cliquez sur **Sauvegarder**.

6. Fermez la fenêtre **Gestion des rôles utilisateur**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Suppression d'un rôle utilisateur

Si un rôle utilisateur n'est plus requis, vous pouvez supprimer le rôle utilisateur.

### Pourquoi et quand exécuter cette tâche

Si des comptes utilisateur sont affectés au rôle utilisateur que vous souhaitez supprimer, vous devez réaffecter les comptes utilisateur à un autre rôle utilisateur. Le système détecte automatiquement cette condition et vous invite à mettre à jour les comptes utilisateur.

Vous pouvez rapidement localiser le rôle utilisateur que vous souhaitez supprimer dans la fenêtre **Gestion des rôles utilisateur**. Entrez un nom de rôle dans la zone de texte **Type à filtrer** située au-dessus du panneau de gauche.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Rôles utilisateur**.
2. Dans la sous-fenêtre de gauche de la fenêtre **Gestion des rôles utilisateur**, sélectionnez le rôle que vous souhaitez supprimer.
3. Dans la barre d'outils, cliquez sur **Supprimer**.
4. Cliquez sur **OK**.
  - Si des comptes utilisateur sont affectés à ce rôle utilisateur, la fenêtre **Des utilisateurs sont affectés à ce rôle utilisateur** s'ouvre. Passez à l'étape 7.
  - Si aucun compte utilisateur n'est affecté à ce rôle, le rôle utilisateur est supprimé. Passez à l'étape 8.
5. Réaffectez les comptes utilisateur répertoriés à un autre rôle utilisateur :
  - a) Dans la zone de liste **Rôle utilisateur à affecter**, sélectionnez un rôle utilisateur.
  - b) Cliquez sur **Confirmer**.
6. Fermez la fenêtre **Gestion des rôles utilisateur**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Profils de sécurité

---

Les profils de sécurité définissent les réseaux, les sources de journal et les domaines auxquels un utilisateur peut accéder.

QRadar inclut un profil de sécurité par défaut pour les administrateurs. Le profil de sécurité **Admin** inclut l'accès à tous les réseaux, sources de journal et domaines.

Avant d'ajouter des comptes utilisateur, vous devez créer des profils de sécurité supplémentaires pour répondre aux exigences d'accès spécifiques de vos utilisateurs.

### Domaines

Les profils de sécurité doivent être mis à jour avec un domaine associé. Vous devez définir des domaines dans la fenêtre **Gestion des domaines** pour que l'onglet **Domaines** apparaisse dans la fenêtre **Gestion du profil de sécurité**. Les restrictions de niveau domaine ne sont pas appliquées tant que la sécurité n'a pas été mise à jour et que les modifications n'ont pas été déployées.

Les affectations de domaine ont la priorité sur tous les paramètres des onglets **Priorité de droit**, **Réseaux** et **Sources de journal**.

Si le domaine est affecté à un titulaire, le nom du titulaire apparaît entre crochets en regard du nom de domaine dans la fenêtre **Domaines affectés**.

## Priorité d'autorisation

La priorité des droits détermine les composants de profil de sécurité à prendre en compte lorsque le système affiche des événements dans l'onglet **Activité de journal** et des flux dans l'onglet **Activité réseau**.

Choisissez parmi les restrictions suivantes lorsque vous créez un profil de sécurité :

- **Aucune restriction** - Cette option ne place pas les restrictions sur les événements affichés dans l'onglet **Activité de journal** et les flux affichés dans l'onglet **Activité réseau**.
- **Réseau uniquement** - Cette option limite l'utilisateur à afficher uniquement les événements et les flux associés aux réseaux spécifiés dans ce profil de sécurité.
- **Sources de journal uniquement** - Cette option limite l'utilisateur à afficher uniquement les événements associés aux sources de journal spécifiées dans ce profil de sécurité.
- **Réseaux et sources de journal** - Cette option permet à l'utilisateur de visualiser uniquement les événements et les flux associés aux sources de journal et aux réseaux spécifiés dans ce profil de sécurité.

Par exemple, si le profil de sécurité autorise l'accès aux événements à partir d'une source de journal, mais que le réseau de destination est restreint, l'événement ne s'affiche pas dans l'onglet **Activité de journal**. L'événement doit correspondre aux deux exigences.

- **Réseaux OU Sources de journal** - Cette option permet à l'utilisateur d'afficher les événements et les flux associés aux sources de journal ou aux réseaux spécifiés dans ce profil de sécurité.

Par exemple, si un profil de sécurité permet d'accéder aux événements depuis une source de journal mais que le réseau de destination est restreint, l'événement apparaît sous l'onglet **Activité du journal** si la priorité de droit est définie sur **Réseaux OU Sources de journal**. Si la priorité de droit est définie sur **Réseaux ET Sources de journal**, l'événement n'apparaît pas sous l'onglet **Activité du journal**.

## Droits de priorité pour les données de violation

Les profils de sécurité utilisent automatiquement le droit **Réseaux OU Sources de journal** lorsque des données de violation sont affichées. Par exemple, si une violation a une adresse IP de destination que votre profil de sécurité vous autorise à voir, mais que le profil de sécurité n'accorde pas de droits à l'adresse IP source, la fenêtre **Récapitulatif des violations** affiche à la fois la destination et les adresses IP source.

## Création d'un profil de sécurité

Pour ajouter des comptes utilisateur, vous devez d'abord créer des profils de sécurité pour répondre aux besoins d'accès spécifiques de vos utilisateurs.

### Pourquoi et quand exécuter cette tâche

IBM QRadar SIEM inclut un profil de sécurité par défaut pour les administrateurs. Le profil de sécurité d'administration inclut l'accès à tous les réseaux, sources de journal et domaines.

Pour sélectionner plusieurs éléments dans la fenêtre **Gestion des profils de sécurité**, maintenez la touche Contrôle pendant que vous sélectionnez chaque réseau ou groupe de réseau que vous souhaitez ajouter.

Si une fois que vous avez ajouté des réseaux, vous souhaitez supprimer un ou plusieurs sources de journal ou domaines avant de sauvegarder la configuration, vous pouvez sélectionner l'élément et cliquer sur l'icône **Supprimer**. Pour supprimer tous les éléments, cliquez sur **Supprimer tout**.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Profils de sécurité**.
2. Dans la barre d'outils **Fenêtre Gestion des profils de sécurité**, cliquez sur **Nouveau**.

3. Configurez les paramètres suivants :
  - a) Dans la zone **Nom du profil de sécurité**, entrez un nom unique pour le profil de sécurité. Le nom du profil de sécurité doit répondre aux exigences suivantes : minimum de 3 caractères et maximum de 30 caractères.
  - b) **Facultatif** Entrez une description du profil de sécurité. Le nombre maximal de caractères est 255.
4. Cliquez sur l'onglet **Préséance des autorisations**.
5. Dans le panneau des paramètres de préséance d'autorisations, sélectionnez une option de préséance d'autorisations. Voir «[Priorité d'autorisation](#)», à la page 17.
6. Configurez les réseaux que vous désirez affecter au profil de sécurité :
  - a) Cliquez sur l'onglet **Réseaux**.
  - b) Dans l'arborescence de navigation du panneau gauche de l'onglet **Réseaux**, sélectionnez le réseau auquel ce profil de sécurité doit avoir accès.
  - c) Cliquez sur l'icône **Ajouter (>)** pour ajouter le réseau au panneau Réseaux affectés.
  - d) Répétez cette opération pour chaque réseau que vous désirez ajouter.
7. Configurez les sources de journal que vous désirez affecter au profil de sécurité :
  - a) Cliquez sur l'onglet **Sources de journal**.
  - b) Dans l'arborescence de navigation du panneau gauche, sélectionnez le groupe de sources de journal ou la source de journal auquel ce profil de sécurité doit avoir accès.
  - c) Cliquez sur l'icône **Ajouter (>)** pour ajouter la source de journal au panneau Sources de journal affectées.
  - d) Répétez cette opération pour chaque source de journal que vous désirez ajouter.
8. Configurez les domaines que vous souhaitez affecter au profil de sécurité :

Les domaines doivent être configurés avant l'apparition de l'onglet **Domaines**.

  - a) Cliquez sur l'onglet **Domaines**.
  - b) Dans l'arborescence de navigation du panneau gauche, sélectionnez le domaine auquel vous voulez que ce profil de sécurité ait accès.
  - c) Cliquez sur l'icône **Ajouter (>)** pour ajouter le domaine à la sous-fenêtre Domaines affectés.
  - d) Répétez l'opération pour chaque domaine à ajouter.
9. Cliquez sur **Sauvegarder**.

**Remarque** : Les sources de journal qui sont affectées au profil de sécurité doivent correspondre. Si les sources de journal et les domaines ne correspondent pas, vous ne pouvez pas enregistrer le profil de sécurité.
10. Fermez la fenêtre **Gestion du profil de sécurité**.
11. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Modification d'un profil de sécurité

Vous pouvez éditer un profil de sécurité existant pour mettre à jour les réseaux et les sources de journal auxquels un utilisateur peut accéder et la priorité d'autorisation.

### Pourquoi et quand exécuter cette tâche

Pour localiser rapidement le profil de sécurité que vous souhaitez éditer dans la fenêtre **Gestion des profils de sécurité**, entrez le nom du profil de sécurité dans la zone de texte **Type à filtrer**.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Profils de sécurité**.
2. Dans la sous-fenêtre de gauche, sélectionnez le profil de sécurité que vous souhaitez modifier.



3. Dans la barre d'outils, cliquez sur **Editer**.
4. Mettez à jour les paramètres si nécessaire.
5. Cliquez sur **Sauvegarder**.
6. Si la fenêtre **Le profil de sécurité a des données de série temporelle** s'ouvre, sélectionnez l'une des options suivantes :

Option	Description
<b>Conserver les anciennes données et sauvegarder</b>	Sélectionnez cette option pour conserver les données de série temporelle précédemment cumulées. Si vous choisissez cette option, les utilisateurs disposant de ce profil de sécurité peuvent voir les données précédentes qu'ils ne sont plus autorisés à voir lorsqu'ils affichent des graphiques de série temporelle.
<b>Masquer les anciennes données et sauvegarder</b>	Sélectionnez cette option pour masquer les données de série temporelle. Si vous choisissez cette option, l'accumulation des données de série temporelle redémarre après le déploiement des modifications de configuration.

7. Fermez la fenêtre **Gestion du profil de sécurité**.
8. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Duplication d'un profil de sécurité

Si vous souhaitez créer un nouveau profil de sécurité qui correspond étroitement à un profil de sécurité existant, vous pouvez dupliquer le profil de sécurité existant, puis modifier les paramètres.

### Pourquoi et quand exécuter cette tâche

Pour localiser rapidement le profil de sécurité que vous souhaitez dupliquer dans la fenêtre **Gestion des profils de sécurité**, entrez le nom du profil de sécurité dans la zone de texte **Type à filtrer**.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Profils de sécurité**.
2. Dans la sous-fenêtre de gauche, sélectionnez le profil de sécurité à dupliquer.
3. Dans la barre d'outils, cliquez sur **Dupliquer**.
4. Dans la fenêtre **Confirmation**, entrez un nom unique pour le profil de sécurité dupliquée.
5. Cliquez sur **OK**.
6. Mettez à jour les paramètres si nécessaire.
7. Fermez la fenêtre **Gestion du profil de sécurité**.
8. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Suppression d'un profil de sécurité

Si un profil de sécurité n'est plus requis, vous pouvez supprimer le profil de sécurité.

### Pourquoi et quand exécuter cette tâche

Si des comptes utilisateur sont affectés aux profils de sécurité que vous souhaitez supprimer, vous devez réaffecter les comptes utilisateur à un autre profil de sécurité. IBM QRadar détecte automatiquement cette condition et vous invite à mettre à jour les comptes utilisateur.

Pour localiser rapidement le profil de sécurité que vous souhaitez supprimer dans la fenêtre **Gestion des profils de sécurité**, entrez le nom du profil de sécurité dans la zone de texte **Type à filtrer**.

## Procédure

1. Dans l'onglet **Admin**, cliquez sur **Profils de sécurité**.
2. Dans la sous-fenêtre de gauche, sélectionnez le profil de sécurité à supprimer.
3. Dans la barre d'outils, cliquez sur **Supprimer**.
4. Cliquez sur **OK**.
  - Si des comptes utilisateur sont affectés à ce profil de sécurité, la fenêtre **Les utilisateurs sont affectés à ce profil de sécurité** s'ouvre. Accédez à «[Suppression d'un rôle utilisateur](#)», à la page 16.
  - Si aucun compte utilisateur n'est affecté à ce profil de sécurité, le profil de sécurité est supprimé. Accédez à «[Suppression d'un rôle utilisateur](#)», à la page 16.
5. Réaffectez les comptes utilisateur répertoriés à un autre profil de sécurité :
  - a) Dans la zone de liste **Profil de sécurité utilisateur à affecter**, sélectionnez un profil de sécurité.
  - b) Cliquez sur **Confirmer**.
6. Fermez la fenêtre **Gestion du profil de sécurité**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Comptes utilisateur

Le compte utilisateur définit le nom d'utilisateur unique utilisé pour se connecter à IBM QRadar et spécifie le rôle utilisateur, le profil de sécurité et les affectations de locataire auxquels l'utilisateur est affecté.

Lors de la configuration initiale de votre système, vous devez créer des comptes utilisateur pour chaque utilisateur qui a besoin d'accéder à QRadar.

## Affichage et modification des informations relatives à l'utilisateur en cours

Vous pouvez afficher et modifier les informations de compte de l'utilisateur en cours via l'interface du produit principal.

### Procédure

1. Cliquez sur l'icône de l'utilisateur en haut à droite de l'interface du produit principal.
2. Cliquez sur **Préférences utilisateur**.
3. Mettez à jour les détails de l'utilisateur configurable.

Paramètre	Description
<b>Messagerie électronique</b>	Entrez une adresse e-mail à associer à cet utilisateur. L'adresse ne peut pas contenir plus de 255 caractères et ne doit contenir aucun espace.
<b>Mot de passe actuel</b>	Entrez votre mot de passe actuel.
<b>Nouveau mot de passe</b>	Entrez un nouveau mot de passe qui permettra à l'utilisateur d'obtenir l'accès. Le mot de passe doit respecter la longueur minimale ainsi que les exigences de complexité imposées par la politique sur les mots de passe.
<b>Confirmer le nouveau mot de passe</b>	Entrez une seconde fois le nouveau mot de passe.
<b>Environnement local</b>	Sélectionnez une langue préférée dans la liste.

Paramètre	Description
<b>Activer les notifications en incrustation</b>	Lorsque cette option est activée, les messages de notification système s'affichent. Pour désactiver les notifications système, définissez la valeur off.

4. Cliquez sur **Sauvegarder**.

## Affichage de l'historique des connexions utilisateur

Vous pouvez afficher l'historique de connexion des utilisateurs pour déterminer s'il y a eu un accès non autorisé à leur compte. Vous pouvez activer et désactiver le suivi des tentatives de connexion et spécifier la période de conservation pour le suivi des tentatives de connexion.

### Pourquoi et quand exécuter cette tâche

Si vous activez l'affichage de l'historique de connexion, une fenêtre **Historique de connexion** affiche la date, l'heure et l'adresse IP de la dernière connexion réussie, ainsi que le nombre de tentatives de connexion infructueuses d'un utilisateur depuis la dernière connexion réussie.

Si vous spécifiez une période de conservation pour le suivi des tentatives de connexion, QRadar conserve l'historique de connexion pour le nombre de jours sélectionné.

Lorsque vous modifiez la période de conservation de la connexion, elle prend effet pour un utilisateur lors de sa connexion suivante. Par exemple, si vous modifiez la durée de conservation de la connexion de 14 jours à 7 jours, tout administrateur continue d'afficher 14 jours d'historique de connexion pour tout utilisateur qui n'est pas connecté depuis la modification.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres d'authentification généraux**.
3. Activez **Afficher l'historique de connexion**.
4. Définissez la zone **Conservation de l'historique de connexion (en jours)** sur le nombre de jours de conservation de l'historique des tentatives de connexion d'un utilisateur.

**Remarque :** La valeur par défaut n'est pas une valeur, qui conserve tous les historiques de connexion.

5. Cliquez sur **Save Settings**.
6. Fermez la fenêtre **Authentification**.

## Création d'un compte d'utilisateur

Lorsque vous créez un nouveau compte utilisateur, vous devez attribuer à l'utilisateur des données d'identification, un rôle utilisateur et un profil de sécurité. Les rôles utilisateur définissent les actions que l'utilisateur est autorisé à effectuer. Les profils de sécurité définissent à quelles données l'utilisateur est autorisé à accéder.

### Avant de commencer

Avant de créer un compte utilisateur, vous devez vérifier que le rôle utilisateur et le profil de sécurité requis ont été créés.

### Pourquoi et quand exécuter cette tâche

Vous pouvez créer plusieurs comptes utilisateur incluant des privilèges d'administration ; cependant, tout rôle utilisateur ayant des privilèges d'administrateur gestionnaire peut créer d'autres comptes utilisateur administratif.

## Procédure

1. Dans l'onglet **Admin**, cliquez sur **Utilisateurs**.  
La fenêtre **Gestion des utilisateurs** s'ouvre.
2. Cliquez sur **Ajouter**.
3. Entrez des valeurs pour les paramètres suivants :

Paramètre	Description
Nom d'utilisateur	Entrez un nom d'utilisateur unique pour le nouvel utilisateur. Le nom d'utilisateur doit contenir entre 1 et 60 caractères.
Description de l'utilisateur	Entrez une description pour l'utilisateur. La description ne peut pas contenir plus de 2048 caractères.
E-mail	Entrez une adresse e-mail à associer à cet utilisateur. L'adresse ne peut pas contenir plus de 255 caractères et ne doit contenir aucun espace.
Nouveau mot de passe	Entrez un nouveau mot de passe qui permettra à l'utilisateur d'obtenir l'accès. Le mot de passe doit respecter la longueur minimale ainsi que les exigences de complexité imposées par la politique sur les mots de passe.
Confirmer le nouveau mot de passe	Entrez une seconde fois le nouveau mot de passe.
Rôle utilisateur	Sélectionnez un rôle pour cet utilisateur dans la liste.
Profil de sécurité	Sélectionnez un profil de sécurité pour cet utilisateur dans la liste.
Remplacer le délai d'inactivité du système	Activez ce paramètre pour configurer le seuil d'inactivité du compte utilisateur.

4. Cliquez sur **Sauvegarder**.
5. Fermez la fenêtre **Gestion des utilisateurs**.
6. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Modification d'un compte utilisateur

Vous pouvez modifier les informations de compte pour l'utilisateur en cours via l'interface du produit principal. Pour localiser rapidement le compte utilisateur que vous souhaitez éditer dans la fenêtre **Gestion des utilisateurs**, entrez le nom de l'utilisateur dans la zone de texte **Rechercher un utilisateur** de la barre d'outils.

## Procédure

1. Dans l'onglet **Admin**, cliquez sur **Utilisateurs**.
2. Dans la fenêtre **Gestion des utilisateurs**, sélectionnez l'utilisateur que vous souhaitez modifier.  
Vous pouvez utiliser le **Filtre avancé** pour rechercher par Rôle utilisateur ou par Profil de sécurité.
3. Dans la fenêtre **Détails de l'utilisateur**, cliquez sur **Éditer**.
4. Éditez les informations de compte de l'utilisateur.
5. Cliquez sur **Sauvegarder**.
6. Fermez la fenêtre **Gestion des utilisateurs**.

7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Désactivation d'un compte utilisateur

Vous pouvez désactiver un compte utilisateur pour empêcher un utilisateur d'accéder à QRadar. L'option de désactivation d'un compte utilisateur révoque temporairement l'accès d'un utilisateur sans supprimer le compte.

### Pourquoi et quand exécuter cette tâche

Si l'utilisateur avec le compte désactivé tente de se connecter, un message les informe que le nom d'utilisateur et le mot de passe ne sont plus valides. Les éléments qu'ils ont créés, tels que les recherches sauvegardées et les rapports, restent associés à l'utilisateur.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Utilisateurs**.
2. Dans la fenêtre **Gestion des utilisateurs**, sélectionnez le compte utilisateur que vous souhaitez désactiver.  
Vous pouvez utiliser le **Filtre avancé** pour rechercher par Rôle utilisateur ou par Profil de sécurité.
3. Cliquez sur **Editer**.
4. Dans la fenêtre **Détails de l'utilisateur**, sélectionnez **Désactivé** dans la liste **Rôle utilisateur**.
5. Cliquez sur **Sauvegarder**.
6. Fermez la fenêtre **Gestion des utilisateurs**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Suppression d'un compte utilisateur

Si un compte utilisateur n'est plus nécessaire, vous pouvez supprimer le compte utilisateur. Une fois que vous avez supprimé un utilisateur, l'utilisateur n'a plus accès à l'interface utilisateur. Si l'utilisateur tente de se connecter, un message s'affiche pour informer l'utilisateur que le nom d'utilisateur et le mot de passe ne sont plus valides.

### Pourquoi et quand exécuter cette tâche

Pour localiser rapidement le compte utilisateur que vous souhaitez supprimer dans la fenêtre **Gestion des utilisateurs**, entrez le nom d'utilisateur dans la zone de texte **Rechercher**.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Utilisateurs**.
2. Dans la fenêtre **Gestion des utilisateurs**, sélectionnez l'utilisateur que vous souhaitez supprimer.  
Vous pouvez utiliser le **Filtre avancé** pour rechercher par Rôle utilisateur ou par Profil de sécurité.
3. Dans la fenêtre **Détails de l'utilisateur**, cliquez sur **Supprimer**.  
Une recherche pour les personnes à charge commence.
4. Dans la fenêtre **Dépendants trouvés**, cliquez sur **Supprimer** ou **Réaffecter** dépendants.
5. Lorsque l'utilisateur ne possède pas de dépendants, cliquez sur **Supprimer un utilisateur**.
6. Dans la fenêtre **Confirmation de suppression**, cliquez sur **Supprimer > OK**.
7. Cliquez sur **Supprimer**.
8. Fermez la fenêtre **Gestion des utilisateurs**.
9. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Suppression de recherches sauvegardées d'un utilisateur supprimé

Si les recherches sauvegardées d'un utilisateur supprimé ne sont plus nécessaires, vous pouvez supprimer les recherches.

### Pourquoi et quand exécuter cette tâche

Les recherches sauvegardées créées par un utilisateur supprimé restent associées à l'utilisateur jusqu'à ce que vous supprimiez les recherches.

### Procédure

1. Dans l'onglet **Activité de journal** ou **Activité réseau**, cliquez sur **Rechercher** > **Gérer les résultats de la recherche**.
2. Cliquez sur la colonne **Statut** pour trier les recherches sauvegardées.
3. Sélectionnez les recherches sauvegardées dont le statut est "ERREUR !", Puis cliquez sur **Supprimer**.

## Déverrouillage des comptes utilisateur verrouillés

Nouveautés de la version 7.4.1 Un utilisateur disposant de droits d'accès de l'utilisateur root peut déverrouiller des comptes utilisateur qui sont verrouillés sur IBM QRadar.

### Pourquoi et quand exécuter cette tâche

Un compte utilisateur peut être verrouillé sur QRadar s'il y a trop de tentatives de connexion infructueuses pour ce compte.

### Procédure

1. À l'aide de SSH, connectez-vous à votre système en tant qu'utilisateur racine.
2. Déverrouillage de comptes utilisateur spécifiques ou de tous les comptes utilisateur.
  - Déverrouillez des comptes utilisateur spécifiques en entrant la commande suivante :

```
/opt/qradar/bin/runjava.sh  
com.ibm.si.security_model.authentication.AuthenticationLockoutCommandLineTool --remove-  
account <user_account1> <user_account2> <user_account3>
```

- Déverrouillez tous les comptes utilisateur en entrant la commande suivante :

```
/opt/qradar/bin/runjava.sh  
com.ibm.si.security_model.authentication.AuthenticationLockoutCommandLineTool --remove-  
all-accounts
```

## Déverrouillage des comptes verrouillés

Nouveautés de la version 7.4.1 Un utilisateur disposant de droits d'accès de l'utilisateur root peut déverrouiller des hôtes qui sont verrouillés par IBM QRadar.

### Pourquoi et quand exécuter cette tâche

Un hôte peut être bloqué de QRadar s'il y a trop de tentatives de connexion infructueuses de cet hôte.

### Procédure

1. À l'aide de SSH, connectez-vous à votre système en tant qu'utilisateur racine.
2. Déverrouillage des hôtes spécifiques ou de tous les hôtes utilisateur.
  - Déverrouillez des hôtes spécifiques en entrant la commande suivante :

```
/opt/qradar/bin/runjava.sh
com.ibm.si.security_model.authentication.AuthenticationLockoutCommandLineTool --remove-ip
<host_IP_address1> <host_IP_address2> <host_IP_address3>
```

- Déverrouillez tous les hôtes en entrant la commande suivante :

```
/opt/qradar/bin/runjava.sh
com.ibm.si.security_model.authentication.AuthenticationLockoutCommandLineTool --remove-
all-ips
```

## Authentification de l'utilisateur

Lorsque l'authentification est configurée et qu'un utilisateur entre un nom d'utilisateur et un mot de passe non valides, un message s'affiche pour indiquer que la connexion n'est pas valide.

Si l'utilisateur tente d'accéder plusieurs fois au système avec des informations non valides, l'utilisateur doit attendre la durée configurée avant de pouvoir tenter d'accéder à nouveau au système. Vous pouvez configurer les paramètres de la console pour déterminer le nombre maximal d'échecs de connexion et d'autres paramètres associés.

IBM QRadar prend en charge les types d'authentification suivants :

- **Authentification du système** - Les utilisateurs sont authentifiés localement. L'authentification système est le type d'authentification par défaut.
- **Authentification RADIUS** - Les utilisateurs sont authentifiés par un serveur RADIUS (Remote Authentication Dial-in User Service). Lorsqu'un utilisateur tente de se connecter, QRadar chiffre le mot de passe uniquement et transmet le nom d'utilisateur et le mot de passe au serveur RADIUS pour l'authentification.
- **Authentification TACACS** - Les utilisateurs sont authentifiés par un serveur TACACS (Terminal Access Controller Access Control System). Lorsqu'un utilisateur tente de se connecter, QRadar chiffre le nom d'utilisateur et le mot de passe et transmet ces informations au serveur TACACS pour l'authentification. L'authentification TACACS utilise Cisco Secure ACS Express comme serveur TACACS. QRadar prend en charge le Cisco Sécurisé ACS Express 4.3.
- **Fonctions supprimées dans la version 7.4.2 Microsoft Active Directory** - Les utilisateurs sont authentifiés par un serveur LDAP (Lightweight Directory Access Protocol) qui utilise Kerberos.
- **LDAP** - Les utilisateurs sont authentifiés par un serveur LDAP.
- **Authentification de connexion unique SAML** - Les utilisateurs peuvent facilement intégrer QRadar à votre serveur d'identité d'entreprise pour fournir une connexion unique et éliminer la nécessité de gérer les utilisateurs locaux QRadar. Les utilisateurs authentifiés sur votre serveur d'identité peuvent s'authentifier automatiquement auprès de QRadar. Ils n'ont pas besoin de se rappeler des mots de passe séparés ou de saisir des données d'identification chaque fois qu'ils accèdent à QRadar.

### Liste de contrôle des prérequis pour les fournisseurs d'authentification externes

Avant de configurer un type d'authentification externe, vous devez effectuer les tâches suivantes :

- \_\_\_ • Configurez le serveur d'authentification avant de configurer l'authentification dans QRadar. Pour plus d'informations, voir la documentation de votre fournisseur.
- \_\_\_ • Vérifiez que le serveur dispose des comptes utilisateur et des niveaux de privilèges appropriés pour communiquer avec QRadar. Pour plus d'informations, voir la documentation de votre fournisseur.
- \_\_\_ • Vérifiez que l'heure du serveur d'authentification est synchronisée avec l'heure du serveur QRadar.
- \_\_\_ • Assurez-vous que tous les utilisateurs disposent de comptes utilisateur et de rôles appropriés pour permettre l'authentification avec les serveurs du fournisseur.

#### Concepts associés

[Temps système QRadar](#)

[«Authentification unique à l'ouverture de session», à la page 41](#)

Le langage SAML (Security Assertion Markup Language) est un cadre d'authentification et d'autorisation entre un fournisseur de services (SP) et un fournisseur d'identité (PDI) où l'authentification est échangée à l'aide de documents XML signés numériquement. Le fournisseur de services accepte de faire confiance au fournisseur d'identité pour authentifier les utilisateurs. En retour, le fournisseur d'identité génère une assertion d'authentification, ce qui indique qu'un utilisateur a été authentifié.


## Modification des mots de passe utilisateur QRadar

IBM QRadar modifie occasionnellement la règle de mot de passe pour qu'elle soit conforme aux normes de sécurité en vigueur. Lorsque la règle de mot de passe est mise à jour, les utilisateurs qui ont des mots de passe locaux sont invités à mettre à jour leur mot de passe la première fois qu'ils se connectent après la mise à niveau. Dans un très petit nombre de situations, il se peut que certains utilisateurs ne soient pas invités à modifier leur mot de passe après la mise à niveau, et vous devrez les modifier pour eux.

Pour modifier les mots de passe utilisateur SIEM, procédez comme suit :

1. Dans l'onglet **Admin**, cliquez sur **Utilisateurs**.
2. Sélectionnez un utilisateur dans la liste et cliquez sur **Éditer**.
3. Dans la sous-fenêtre **Détails de l'utilisateur**, entrez le nouveau mot de passe de l'utilisateur, puis cliquez sur **Sauvegarder**.

Pour modifier les mots de passe utilisateur PCAP, procédez comme suit :

1. Dans l'onglet **Admin**, cliquez sur **Gestion du système et de la licence**.
2. Sélectionnez **Vue Systèmes** dans la liste **Afficher**.
3. Mettez en évidence votre périphérique QRadar Incident Forensics.
4. Dans le menu **Actions de déploiement**, cliquez sur **Editer l'hôte**.
5. Cliquez sur l'icône **Gestion des composants** .
6. Dans la fenêtre PCAP Device Management, entrez de nouveau ou modifiez le mot de passe de connexion de l'utilisateur et cliquez sur **Sauvegarder**.
7. Dans l'onglet **Admin**, cliquez sur **Avancé** > **Déployer la configuration complète** pour que les modifications prennent effet.

Pour modifier les mots de passe utilisateur FTP, procédez comme suit :

1. Cliquez sur l'onglet **Admin**, puis sur **Droits utilisateur Forensics**.
2. Sélectionnez un utilisateur dans la liste **Utilisateurs** à gauche de la fenêtre.
3. Dans la sous-fenêtre **Éditer l'utilisateur**, cochez la case **Activer l'accès FTP**.
4. Entrez ou modifiez le mot de passe de l'utilisateur.
5. Sous **Cas affectés**, cliquez sur **Enregistrer l'utilisateur**.

## Configuration du délai d'attente d'inactivité pour un utilisateur

Si vous avez des utilisateurs qui ont besoin de plus longues périodes d'inactivité avant de se déconnecter du système, vous pouvez configurer individuellement leur seuil d'inactivité.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Utilisateurs**.
2. Sélectionnez un utilisateur dans la liste et cliquez sur **Éditer**.
3. Dans le volet **Détails de l'utilisateur**, activez le paramètre **Remplacer le délai d'inactivité du système**.
4. Entrez le nombre de minutes d'inactivité avant la déconnexion de l'utilisateur, puis cliquez sur **Sauvegarder**.



## Instructions d'authentification externes

Vous pouvez configurer un fournisseur d'authentification externe pour permettre à IBM QRadar d'authentifier les utilisateurs sans que QRadar stocke les mots de passe localement pour ces utilisateurs.



**Avertissement :** Vous ne pouvez pas configurer plusieurs fournisseurs d'authentification externes pour QRadar à la fois. Si vous avez configuré un fournisseur d'authentification externe et que vous avez configuré un autre fournisseur d'authentification externe, la configuration du premier fournisseur d'authentification externe est supprimée.

Lorsque vous choisissez d'utiliser un fournisseur d'authentification externe, considérez ces points :

- Vérifiez que votre fournisseur externe est digne de confiance car vous déléguez une décision de sécurité importante à ce fournisseur externe. Un fournisseur compromis peut autoriser l'accès à votre système QRadar à des parties inattendues.
- Vérifiez que la connexion au fournisseur externe est sécurisée. Choisissez uniquement des protocoles de communication sécurisés, en utilisant LDAPS au lieu de LDAP, par exemple.
- Déterminez si vous souhaitez activer une fonction de secours d'authentification locale si le fournisseur externe n'est pas disponible. Si le fournisseur externe est compromis, il peut être utilisé comme un refus d'accès.
- La décision de configurer un fournisseur d'authentification externe s'applique à tous les utilisateurs QRadar administrateurs et non-administrateurs. Il n'existe pas d'"utilisateur local uniquement" dans QRadar.
- Si vous activez l'approvisionnement automatique des comptes QRadar, un fournisseur compromis peut être utilisé pour forcer la création d'un compte QRadar voyous, alors utilisez la prudence lorsque vous combinez ces fonctions.
- Les utilisateurs QRadar qui n'ont pas d'entrée dans le fournisseur externe dépendent de la fonction de secours pour vérifier le mot de passe local. Un fournisseur d'authentification externe compromis peut être utilisé pour créer un "Ombre" pour un compte QRadar existant, en fournissant un autre mot de passe pour l'authentification.

### Fonction de secours sur l'authentification locale

Chaque utilisateur non administrateur peut être configuré pour une fonction de secours d'authentification locale. La fonction de secours d'authentification locale est désactivée par défaut. Si cette option est activée, un utilisateur QRadar non administrateur peut accéder au système en utilisant le mot de passe stocké localement même si le fournisseur externe n'est pas disponible ou si le mot de passe du fournisseur externe est verrouillé ou est inconnu de l'utilisateur. Cela signifie également qu'un administrateur QRadar voyous peut modifier le mot de passe stocké localement et se connecter en tant qu'utilisateur, afin de vous assurer que vos administrateurs QRadar sont dignes de confiance. C'est également le cas si un fournisseur d'authentification externe n'est pas configuré.

Le compte administrateur par défaut, nommé `Admin`, est toujours configuré pour les fonctions de secours d'authentification locales par défaut. Cela empêche l'utilisateur administratif d'être verrouillé sur le système, mais signifie également que vous devez vous assurer que le fournisseur d'authentification externe configuré possède l'entrée correcte pour l'utilisateur `Admin` et que le mot de passe est uniquement connu de l'administrateur QRadar autorisé. Si vous ne pouvez pas conserver le contrôle de l'entrée d'administration dans le fournisseur d'authentification externe, désactivez le compte `Admin` dans QRadar pour empêcher les utilisateurs non autorisés de se connecter à QRadar en tant que `Admin`. Lorsque vous activez l'approvisionnement automatique, par exemple lorsque vous utilisez l'authentification de groupe LDAP, tout compte utilisateur correspondant à la requête LDAP est créé ou réactivé avec les rôles appropriés tels qu'ils sont mappés. Pour éviter cela, désactivez l'approvisionnement automatique à l'aide de LDAP local.

Pour les autres utilisateurs QRadar privilégiés (utilisateurs disposant du rôle administrateur), vous pouvez choisir, par utilisateur, si vous souhaitez activer les fonctions de secours d'authentification locales. Le paramètre `ENABLE_FALLBACK_ALL_ADMINS` (désactivé par défaut) peut être utilisé pour forcer tous les utilisateurs privilégiés à utiliser les fonctions de secours d'authentification locales. Si une fonction de

secours d'authentification locale est configurée, les mêmes remarques s'appliquent que pour le compte Admin.

Lorsque vous configurez un fournisseur d'authentification externe et que vous créez un nouvel utilisateur, cet utilisateur n'a pas automatiquement un mot de passe local défini pour QRadar. Si un utilisateur a besoin d'un mot de passe local, vous devez configurer les fonctions d'authentification locales pour cet utilisateur. La fonction de secours d'authentification locale permet à un utilisateur d'authentifier localement si l'authentification externe échoue pour une raison quelconque, y compris des mots de passe non valides. Les utilisateurs de fonctions de secours peuvent alors accéder à QRadar quel que soit l'état de l'authentification externe.

Même si la fonction de secours d'authentification locale est activée pour un compte utilisateur, QRadar tente d'abord d'authentifier l'utilisateur dans le module d'authentification externe avant de tenter une authentification locale. En cas d'échec de l'authentification externe, QRadar tente automatiquement de s'authentifier localement si la fonction d'authentification locale est activée pour cet utilisateur. Les comptes utilisateur ne peuvent pas être configurés uniquement pour s'authentifier localement lorsqu'un fournisseur d'authentification externe est configuré. Pour cette raison, il est important que tous les comptes utilisateur QRadar correspondent à un compte de fournisseur d'authentification externe du même nom associé au même utilisateur autorisé.

Vérifiez que le fournisseur d'authentification externe est digne de confiance, car cette configuration dépasse une décision de sécurité et un administrateur d'authentification peut autoriser l'accès non autorisé à votre système QRadar. Faites de cette connexion sécurisée, à l'aide de la version sécurisée des protocoles (par exemple en utilisant LDAPS plutôt que LDAP).

L'authentification locale de secours n'est pas disponible avec l'authentification SAML. Aucun utilisateur ne peut s'authentifier localement lorsque vous utilisez l'authentification SAML.

Lors de la délocalisation des utilisateurs, désactivez la fonction de secours d'authentification locale pour cet utilisateur avant de retirer son accès d'authentification du fournisseur d'authentification externe.

## Configuration de l'authentification d'utilisateur

Vous pouvez configurer l'authentification locale sur votre système IBM QRadar. Vous pouvez spécifier la longueur, la complexité et les exigences d'expiration pour les mots de passe locaux.

### Pourquoi et quand exécuter cette tâche

Les règles sur les mots de passe d'authentification locale s'appliquent aux mots de passe locaux pour les administrateurs. Les règles s'appliquent également aux utilisateurs non administrateurs si aucune authentification externe n'est configurée.

Lorsque les règles sur les mots de passe d'authentification locale sont mises à jour, les utilisateurs sont invités à modifier leur mot de passe s'ils se connectent avec un mot de passe qui ne répond pas aux nouvelles exigences.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Facultatif : Dans la liste **Module d'authentification**, sélectionnez **Authentification du système**.

L'authentification système est le module d'authentification par défaut. Si vous effectuez une modification à partir d'un autre module d'authentification, vous devez déployer QRadar avant de procéder aux étapes suivantes.

4. Cliquez sur **Sauvegarder le module d'authentification**.
5. Cliquez sur **Home**.
6. Cliquez sur **Configuration de stratégie de mot de passe local**.
7. Sélectionnez les paramètres de complexité du mot de passe pour l'authentification locale.

## En savoir plus sur les paramètres de complexité du mot de passe :

Paramètre de complexité du mot de passe	Description
<b>Longueur minimale du mot de passe</b>	Spécifie le nombre minimum de caractères qui doivent figurer dans un mot de passe. <b>Important :</b> Pour assurer une sécurité adéquate, les mots de passe doivent contenir au moins 8 caractères.
<b>Utiliser les règles de complexité</b>	Requiert que les mots de passe répondent à un certain nombre de règles de complexité, telles que la présence de majuscules, minuscules, caractères spéciaux ou de chiffres.
<b>Nombre de règles requises</b>	Nombre de règles de complexité que chaque mot de passe doit respecter. Doit être compris entre un et le nombre de règles de complexité activées. Par exemple, si les quatre règles de complexité sont activées et que chaque mot de passe doit répondre à trois d'entre elles, entrez 3.
<b>Contenir un caractère majuscule</b>	Exige que les mots de passe contiennent au moins un caractère majuscule.
<b>Contenir un caractère minuscule</b>	Exige que les mots de passe contiennent au moins un caractère minuscule.
<b>Contenir un chiffre</b>	Exige que les mots de passe contiennent au moins un chiffre.
<b>Contenir un caractère spécial</b>	Requiert que les mots de passe contiennent au moins un espace ou un autre caractère qui n'est ni une lettre ni un nombre (par exemple, "\$%&'()*,-./:;<=>?@[ \ ] _ `   ~).
<b>Ne pas contenir de caractère se répétant</b>	N'autorise pas plus de deux caractères se répétant. Par exemple, abbc est autorisé contrairement à abbbc.
<b>Historique des mots de passe</b>	Empêche la réutilisation des mots de passe pendant un certain nombre de jours. Le nombre de jours est calculé selon le <b>Nombre de mots de passe uniques</b> multiplié par <b>Nombre de jours avant expiration du mot de passe</b> .
<b>Nombre de mots de passe uniques</b>	Ce paramètre s'affiche lorsque <b>Historique des mots de passe</b> est sélectionné. Nombre de changements de mot de passe avant qu'un mot de passe précédent puisse être réutilisé.
<b>Nombre de jours avant expiration du mot de passe</b>	Ce paramètre s'affiche lorsque <b>Historique des mots de passe</b> est sélectionné. Nombre de jours avant qu'un mot de passe puisse être changé.

8. Cliquez sur **Mettre à jour les règles sur les mots de passe**.

## Configuration de l'authentification RADIUS

Vous pouvez configurer l'authentification RADIUS sur votre système IBM QRadar.

## Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **Authentification RADIUS**.
4. Configurez les paramètres suivants :
  - a) Dans la zone **Serveur RADIUS**, entrez le nom d'hôte ou l'adresse IP du serveur RADIUS.
  - b) Dans la zone **Port RADIUS**, entrez le port du serveur RADIUS.
  - c) Dans la zone de liste **Type d'authentification**, sélectionnez le type d'authentification que vous souhaitez effectuer.

Choisissez parmi les options suivantes :

### **CHAP, protocole**

Le protocole CHAP (Challenge Handshake Authentication Protocol) établit une connexion PPP (Point-to-Point Protocol) entre l'utilisateur et le serveur.

### **MSCHAP**

Le protocole MSCHAP (Microsoft Challenge Handshake Authentication Protocol) authentifie des postes de travail Windows distants.

### **protocole d'authentification par mot de passe**

Le protocole PAP (Password Authentication Protocol) échange du texte en clair entre l'utilisateur et le serveur.

- d) Dans la zone **Secret partagé**, entrez le secret partagé utilisé par QRadar pour chiffrer les mots de passe RADIUS pour la transmission au serveur RADIUS.
5. Cliquez sur **Sauvegarder le module d'authentification**.

## Configuration de l'authentification TACACS

Vous pouvez configurer l'authentification TACACS sur votre système IBM QRadar.

## Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **Authentification TACACS**.
4. Configurez les paramètres suivants :
  - a) Dans la zone **Serveur TACACS**, entrez le nom d'hôte ou l'adresse IP du serveur TACACS.
  - b) Dans la zone **Port TACACS**, entrez le port du serveur TACACS.
  - c) Dans la zone de liste **Type d'authentification**, sélectionnez le type d'authentification que vous souhaitez effectuer.

Choisissez parmi les options suivantes :

Option	Description
ASCII	Le protocole ASCII envoie le nom d'utilisateur et le mot de passe sous la forme d'un texte en clair.
protocole d'authentification par mot de passe	Le protocole PAP (Password Authentication Protocol) échange du texte en clair entre l'utilisateur et le serveur. PAP est le type d'authentification par défaut.
CHAP, protocole	Le protocole CHAP (Challenge Handshake Authentication Protocol) établit une connexion PPP (Point-to-Point Protocol) entre l'utilisateur et le serveur.
MSCHAP	Le protocole MSCHAP (Microsoft Challenge Handshake Authentication Protocol) authentifie des postes de travail Windows distants.

d) Dans la zone **Secret partagé**, entrez le secret partagé utilisé par QRadar pour chiffrer les mots de passe TACACS pour la transmission au serveur TACACS.

5. Cliquez sur **Sauvegarder le module d'authentification**.

### Que faire ensuite

Pour l'authentification d'utilisateur TACACS, vous devez créer un compte utilisateur QRadar local identique au compte TACACS sur le serveur d'authentification.

## Configuration de l'authentification par Active Directory

Fonctions supprimées dans la version 7.4.2 Vous pouvez configurer l'authentification Microsoft Active Directory sur votre système IBM QRadar.

### Pourquoi et quand exécuter cette tâche

**Important :** Depuis QRadar 7.4.2, vous ne pouvez plus utiliser l'authentification Active Directory (AD) basée sur Kerberos. Pour plus d'informations, voir <https://www.ibm.com/support/pages/node/6253911>.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **Active Directory**.
4. Cliquez sur **Ajouter** et configurez les paramètres du référentiel Active Directory.

Le tableau suivant décrit les paramètres à configurer :

## Paramètres LDAP

Paramètre	Description
ID référentiel	<p>Le Repository ID est un identificateur ou un alias qui représente de manière unique le serveur qui est entré dans la zone <b>URL du serveur</b> et le domaine à partir de la zone <b>Domaine</b>. Utilisez l'ID du référentiel lorsque vous entrez vos détails de connexion.</p> <p>Par exemple, vous pouvez utiliser AD_1 pour représenter server_A sur Domain_A dans un référentiel Active Directory et AD_2 pour représenter server_B sur Domain_A dans votre second référentiel.</p>
URL du serveur	<p>URL qui est utilisée pour la connexion au serveur LDAP. Par exemple, tapez ldaps://nom_hôte:port.</p> <p><b>Remarque :</b> Si vous spécifiez une connexion LDAP sécurisée, le mot de passe sera chiffré, mais le nom d'utilisateur sera passé en clair.</p>
Contexte	Contexte que vous souhaitez utiliser ; par exemple, DC=QRADAR, DC=INC.
Domaine	Domaine que vous souhaitez utiliser, par exemple: qradar.inc.

5. Entrez le nom d'utilisateur et le mot de passe que vous utilisez pour vous authentifier auprès du référentiel.

6. Pour tester la connectivité au référentiel, cliquez sur **Tester la connexion**.

**Remarque :** Lorsque vous activez Active Directory, vérifiez que le port 88 est ouvert pour permettre les connexions Kerberos à partir de QRadar Console.

7. Pour éditer ou retirer un référentiel, sélectionnez-le et cliquez sur **Editer** ou **Retirer**.

8. Cliquez sur **Sauvegarder**.

Les utilisateurs peuvent se connecter à l'aide des formats de connexion Domain\user ou Repository\_ID\user.

La demande de connexion qui utilise Repository\_ID\user est tentée sur un serveur spécifique lié à un domaine spécifique. Par exemple, Server A sous Domain A, qui est plus spécifique que le format de demande de connexion Domain\user.

La demande de connexion qui utilise le format Domain\user est tentée sur des serveurs qui sont liés au domaine spécifié jusqu'à ce qu'une connexion réussie soit atteinte. Par exemple il pourrait y avoir plusieurs serveurs sur un domaine spécifique.

**Remarque :** Pour l'authentification d'utilisateur Active Directory, vous devez créer un compte utilisateur QRadar local identique au compte Active Directory (AD) sur le serveur d'authentification.

9. Sur la page **Admin**, cliquez sur **Déployer les modifications**.

## Authentification LDAP

Vous pouvez configurer IBM QRadar pour qu'il utilise les fournisseurs LDAP (Lightweight Directory Access Protocol) pris en charge pour l'authentification et l'autorisation des utilisateurs.

QRadar lit les informations sur les utilisateurs et les rôles à partir du serveur LDAP, sur la base des critères d'autorisation que vous avez définis.

Dans les environnements géographiquement dispersés, les performances peuvent être affectées négativement si le serveur LDAP et la console QRadar ne sont pas géographiquement proches les uns des autres. Par exemple, les attributs utilisateur peuvent prendre beaucoup de temps à remplir si la console QRadar est en Amérique du Nord et si le serveur LDAP est en Europe.

Vous pouvez utiliser l'authentification LDAP avec un serveur Active Directory.

## Configuration de l'authentification LDAP

Vous pouvez configurer l'authentification LDAP sur votre système IBM QRadar.

### Avant de commencer

Si vous envisagez d'utiliser le chiffrement SSL ou d'utiliser l'authentification TLS avec votre serveur LDAP, vous devez importer le certificat SSL ou TLS du serveur LDAP vers le répertoire `/opt/qradar/conf/trusted_certificates` de votre console QRadar. Pour plus d'informations sur la configuration des certificats, voir «[Configuration des certificats SSL ou TLS](#)», à la page 38.

Si vous utilisez l'autorisation de groupe, vous devez configurer un rôle utilisateur ou un profil de sécurité QRadar sur la console QRadar pour chaque groupe LDAP utilisé par QRadar. Chaque rôle utilisateur ou profil de sécurité QRadar doit avoir au moins un groupe **Accepter**. Le mappage des noms de groupe aux rôles d'utilisateur et aux profils de sécurité est sensible à la casse.

### Pourquoi et quand exécuter cette tâche

*Authentification* établit une preuve d'identité pour tout utilisateur qui tente de se connecter au serveur QRadar. Lorsqu'un utilisateur se connecte, le nom d'utilisateur et le mot de passe sont envoyés à l'annuaire LDAP pour vérifier si les données d'identification sont correctes. Pour envoyer ces informations en toute sécurité, configurez la connexion au serveur LDAP pour utiliser le chiffrement SSL (Secure Socket Layer) ou TLS (Transport Layer Security).

L'*autorisation* est le processus de détermination des droits d'accès d'un utilisateur. Les utilisateurs sont autorisés à effectuer des tâches en fonction de leurs attributions de rôle. Vous devez disposer d'une connexion de liaison valide au serveur LDAP avant de pouvoir sélectionner les paramètres d'autorisation.

Le nom distinctif de base de l'utilisateur est l'emplacement des requêtes QRadar et des utilisateurs. Activez les droits d'accès aux requêtes pour permettre à vos utilisateurs d'interroger le nom distinctif de base de l'utilisateur.

Les valeurs d'attribut utilisateur sont sensibles à la casse. Le mappage des noms de groupe aux rôles d'utilisateur et aux profils de sécurité est également sensible à la casse.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **LDAP**.
4. Cliquez sur **Ajouter** et définissez les paramètres de configuration de base.

Il existe trois types de configuration et chacun comporte des exigences spécifiques pour les paramètres **URL du serveur**, **connexion SSL** et **authentification TLS** :

#### LDAP sécurisé (LDAPS)

Le paramètre **URL du serveur** doit utiliser `ldaps://` comme protocole et spécifier un port LDAP chiffré (généralement 636). Par exemple `ldaps://ldap1.example.com:636`

Si vous utilisez le catalogue global car vous utilisez plusieurs domaines, utilisez le port 3269. Par exemple `ldaps://ldap1.example.com:3269`

Le paramètre **Connexion SSL** doit être défini sur "Vrai" et le paramètre **Authentification TLS** doit être défini sur "Faux".

#### LDAP avec StartTLS

Le paramètre **URL du serveur** doit utiliser `ldap://` comme protocole et spécifier un port LDAP non chiffré qui prend en charge l'option StartTLS (généralement 389). Par exemple `ldap://ldap1.example.com:389`

Le paramètre **Connexion SSL** doit être défini sur "Faux" et **Authentification TLS** doit être défini sur "Vrai".

TLS 1.2 utilisant StartTLS n'est pas le même que le port SSL LDAP.

L'authentification TLS ne prend pas en charge les références, de sorte que les références doivent être définies sur "ignorer", et le serveur LDAP doit inclure une structure complète pour la recherche.

### Non chiffré

Une configuration LDAP non chiffrée n'est pas recommandée.

Le paramètre **URL du serveur** doit utiliser le protocole ldap:// et spécifier un port non chiffré (généralement 389). Par exemple ldap://ldap1.example.com:389

Le paramètre **Connexion SSL** et le paramètre **Authentification TLS** doivent tous deux être définis sur "Faux".

Tableau 5. Paramètres de configuration de base LDAP

Paramètre	Description																		
ID référentiel	<p>L'<b>ID de référentiel</b> est un alias pour le nom distinctif de base utilisateur (nom distinctif) que vous utilisez lorsque vous entrez vos détails de connexion pour éviter d'avoir à saisir une chaîne longue. Si votre réseau inclut plusieurs référentiels, vous pouvez placer le nom distinctif de base de l'utilisateur avant le nom d'utilisateur ou utiliser l'ID référentiel, qui est plus court.</p> <p>Par exemple, le nom distinctif de base de l'utilisateur est : CN=Users, DC=IBM, DC=com. Vous créez un ID de référentiel tel que UsersIBM qui est un alias pour le nom distinctif de base de l'utilisateur.</p> <p>Vous pouvez entrer l'ID de référentiel abrégé UsersIBM au lieu de saisir l'exemple suivant d'un nom distinctif de base d'utilisateur complet CN=Users, DC=IBM, DC=com</p> <p>Voici un exemple de configuration de l'ID de référentiel à utiliser en tant qu'alias du nom distinctif de base de l'utilisateur.</p> <div data-bbox="586 1073 1469 1591" style="border: 2px solid black; padding: 10px;"> <p style="text-align: center;"><b>Add LDAP Repository</b></p> <hr/> <p><b>Basic Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Repository ID</td> <td style="border: 1px solid gray; padding: 2px;">UsersIBM</td> <td rowspan="7" style="vertical-align: middle; text-align: center;"> <b>Alias for User Base DN</b> </td> </tr> <tr> <td>Server URL</td> <td style="border: 1px solid gray; padding: 2px;"></td> </tr> <tr> <td>SSL Connection</td> <td style="border: 1px solid gray; padding: 2px;">true ▼</td> </tr> <tr> <td>TLS Authentication</td> <td style="border: 1px solid gray; padding: 2px;">true ▼</td> </tr> <tr> <td>Search Entire Base</td> <td style="border: 1px solid gray; padding: 2px;">true ▼</td> </tr> <tr> <td>LDAP User Field</td> <td style="border: 1px solid gray; padding: 2px;"></td> </tr> <tr> <td>User Base DN</td> <td style="border: 1px solid gray; padding: 2px;">CN=Users,DC=IBM,dc=com</td> </tr> <tr> <td>Referral</td> <td style="border: 1px solid gray; padding: 2px;">ignore ▼</td> <td></td> </tr> </table> <p><b>Connection Settings</b></p> </div>	Repository ID	UsersIBM	<b>Alias for User Base DN</b>	Server URL		SSL Connection	true ▼	TLS Authentication	true ▼	Search Entire Base	true ▼	LDAP User Field		User Base DN	CN=Users,DC=IBM,dc=com	Referral	ignore ▼	
Repository ID	UsersIBM	<b>Alias for User Base DN</b>																	
Server URL																			
SSL Connection	true ▼																		
TLS Authentication	true ▼																		
Search Entire Base	true ▼																		
LDAP User Field																			
User Base DN	CN=Users,DC=IBM,dc=com																		
Referral	ignore ▼																		

Figure 4. Référentiel LDAP

Lorsque vous entrez votre nom d'utilisateur sur la page de connexion, vous pouvez entrer l'ID référentiel UsersIBM\*<username>* au lieu de saisir le nom distinctif de base utilisateur complet.

**Remarque :** L'ID de référentiel et le nom distinctif de base de l'utilisateur doivent être uniques.



Paramètre	Description
Rechercher dans toute la base	Sélectionnez <b>True</b> afin d'effectuer la recherche dans tous les sous-répertoires du nom de répertoire (DN) spécifié.  Sélectionnez <b>False</b> pour rechercher uniquement dans le contenu immédiat du nom de répertoire de base La recherche n'est pas effectuée dans les sous-répertoires. Cette recherche est plus rapide qu'une recherche qui recherche tous les répertoires.
Zone Utilisateur LDAP	Identificateur de zone utilisateur sur lequel vous voulez effectuer la recherche.  Vous pouvez spécifier plusieurs zones utilisateur dans une liste de valeurs séparées par des virgules afin de permettre aux utilisateurs de s'authentifier avec plusieurs zones. Par exemple, si vous indiquez <b>uid,mailid</b> , un utilisateur peut être authentifié en fournissant son ID utilisateur ou son ID de courrier.
Nom distinctif (DN) de base d'utilisateur	Nom distinctif du noeud sur lequel doit démarrer la recherche d'un utilisateur. Le <b>Nom distinctif (DN) de base d'utilisateur</b> devient l'emplacement de départ pour le chargement des utilisateurs. A des fins de performance, assurez-vous que le <b>Nom distinctif (DN) de base d'utilisateur</b> est aussi spécifique que possible.  Par exemple, si tous vos comptes utilisateur se trouvent sur le serveur d'annuaire dans le dossier Utilisateurs et que votre nom de domaine est <code>ibm.com</code> , la valeur de nom distinctif de base de l'utilisateur est <code>Cn = Utilisateurs, dc = ibm, dc = com</code> .
Référence	Sélectionnez <b>Ignorer</b> ou <b>Suivre</b> afin d'indiquer comment les références sont traitées.

5. Sous **Paramètres de connexion**, sélectionnez le type de connexion de liaison.

Type de connexion de liaison	Description
Liaison anonyme	Utilisez une liaison anonyme pour créer une session avec le serveur d'annuaire LDAP qui ne nécessite pas que vous fournissiez des informations d'authentification.
Liaison authentifiée	Utilisez la liaison authentifiée lorsque vous souhaitez que la session exige un nom d'utilisateur et un mot de passe valides. Une liaison authentifiée réussie autorise l'utilisateur authentifié à lire la liste des utilisateurs et des rôles dans l'annuaire LDAP pendant la session. Pour renforcer la sécurité, assurez-vous que l'ID utilisateur utilisé pour la connexion de liaison ne dispose pas des autorisations pour réaliser une autre action que la lecture de l'annuaire LDAP.  Fournissez le <b>Nom distinctif de connexion</b> et le <b>Mot de passe</b> . Par exemple, si le nom de connexion est <code>admin</code> et le domaine <code>ibm.com</code> , le <b>nom distinctif de connexion</b> est <code>cn=admin,dc=ibm,dc=com</code> .

6. Cliquez sur **Tester la connexion** pour tester les informations de connexion.

Vous devez fournir des informations utilisateur pour vous authentifier sur les attributs utilisateur que vous avez spécifiés dans **Zone utilisateur LDAP**. Si vous avez spécifié plusieurs valeurs dans

**Zone utilisateur LDAP**, vous devez fournir des informations utilisateur pour vous authentifier sur le premier attribut spécifié.

**Remarque :** La fonction **Tester la connexion** teste la capacité de QRadar à lire l'annuaire LDAP, et non pas si vous pouvez vous connecter au répertoire.

7. Sélectionnez la méthode d'autorisation à utiliser.

Paramètre de la méthode d'autorisation	Description
Local	La combinaison nom d'utilisateur et mot de passe est vérifiée pour chaque utilisateur qui se connecte, mais aucune information d'autorisation n'est échangée entre le serveur LDAP et le serveur QRadar. Si vous choisissez l'autorisation <b>locale</b> , vous devez créer chaque utilisateur sur la console QRadar.
Attributs utilisateur	Choisissez <b>Attributs utilisateur</b> lorsque vous souhaitez indiquer quels attributs de rôle utilisateur et de profil de sécurité peuvent être utilisés afin de déterminer les niveaux d'autorisation.  Vous devez spécifier à la fois un attribut de rôle d'utilisateur et un attribut de profil de sécurité. Les attributs que vous pouvez utiliser sont extraits du serveur LDAP, en fonction de vos paramètres de connexion. Les valeurs d'attribut utilisateur sont sensibles à la casse.

Tableau 7. Méthodes d'autorisation LDAP (suite)	
Paramètre de la méthode d'autorisation	Description
Basée sur le groupe	<p>Choisissez <b>Basée sur le groupe</b> lorsque vous souhaitez que les utilisateurs héritent des droits d'accès basés sur les rôles après authentification auprès du serveur LDAP. Le mappage des noms de groupe aux rôles d'utilisateur et aux profils de sécurité est sensible à la casse.</p> <p><b>Nom distinctif de base de groupe</b> Indique le noeud de départ dans l'annuaire LDAP pour le chargement des groupes. Par exemple, si tous vos groupes se trouvent sur le serveur d'annuaire dans le dossier Groupes et que votre nom de domaine est <code>ibm.com</code>, la valeur <b>DN de base de groupe</b> peut être <code>Cn = Groupes, dc = ibm, dc = com</code>.</p> <p><b>Limite de requête activée</b> Définit une limite sur le nombre de groupes retournés.</p> <p><b>Limite de résultat de requête</b> Nombre maximal de groupes retournés par la requête. Par défaut, l'affichage des résultats de la requête se limite uniquement aux 1000 premiers résultats.</p> <p><b>Par membre</b> Sélectionnez <b>Par membre</b> afin de rechercher des groupes à partir de membres de groupe. Dans la <b>Zone Membre de groupe</b>, indiquez l'attribut LDAP qui est utilisé pour définir l'appartenance au groupe d'utilisateurs. Par exemple, si le groupe utilise l'attribut <code>memberUid</code> pour déterminer l'appartenance au groupe, entrez <code>memberUid</code> dans la <b>Zone Membre de groupe</b>.</p> <p><b>Par requête</b> Sélectionnez <b>Par requête</b> pour rechercher des groupes par l'exécution d'une requête. Vous fournissez des informations sur la requête dans les zones de texte <b>Zone Membre de groupe</b> et <b>Zone Requête de groupe</b>. Par exemple, pour rechercher tous les groupes ayant au moins un attribut <code>memberUid</code> et dont la valeur <code>cn</code> commence par la lettre "S", entrez <code>Uid membre</code> dans le <b>Champ Membre de Groupe</b> et entrez <code>cn=s*</code> dans le <b>Champ Requête de Groupe</b>.</p>

8. Si vous avez spécifié une autorisation basée sur un groupe, cliquez sur **Charger les groupes**, puis sur le signe plus (+) ou moins (-) pour ajouter ou retirer des groupes de privilèges.

Les options de privilège de rôle utilisateur contrôlent les composants QRadar auxquels l'utilisateur a accès. Les options de privilège de profil de sécurité contrôlent les données QRadar accessibles à chaque utilisateur.

**Remarque :** Les limites de requête peuvent être définies en sélectionnant la case à cocher **Limite de requête activée** ou les limites peuvent être définies sur le serveur LDAP. Dans ce dernier cas, vous recevrez peut-être un message indiquant que la limite de requête est activée même si vous n'avez pas sélectionné la case à cocher **Limite de requête activée**.

9. Cliquez sur **Sauvegarder**.
10. Cliquez sur **Gérer la synchronisation** pour échanger des informations d'authentification et d'autorisation entre le serveur LDAP et la console QRadar.

- a) Si vous configurez la connexion LDAP pour la première fois, cliquez sur **Exécuter une synchronisation maintenant** pour synchroniser les données.
  - b) Spécifiez la fréquence pour la synchronisation automatique.
  - c) Cliquez sur **Fermer**.
11. Répétez les étapes pour ajouter d'autres serveurs LDAP, puis cliquez sur **Sauvegarder le module d'authentification** lorsque vous avez terminé.

## Synchronisation des données avec un serveur LDAP

Vous pouvez synchroniser manuellement les données entre le serveur IBM QRadar et le serveur d'authentification LDAP.

### Pourquoi et quand exécuter cette tâche

Si vous utilisez une autorisation basée sur des attributs ou des groupes d'utilisateurs, les informations des utilisateurs sont importées automatiquement du serveur LDAP sur la console QRadar.

Chaque groupe configuré sur le serveur LDAP doit comporter un rôle d'utilisateur ou un profil de sécurité configuré dans la console QRadar. Pour chaque groupe correspondant, les utilisateurs sont importés et des autorisations basées sur ce rôle d'utilisateur ou ce profil de sécurité leur sont affectées.

**Remarque :** Si vous exécutez manuellement la synchronisation, les nouvelles données ne sont pas importées. Les utilisateurs LDAP ne sont importés que lorsque vous vous connectez pour la première fois à QRadar.

Par défaut, la synchronisation a lieu toutes les 24 heures. Le délai de synchronisation dépend de l'heure de la dernière exécution. Par exemple, si vous exécutez manuellement la synchronisation à 23 h 45 et que vous définissez l'intervalle de synchronisation sur 8 heures, la synchronisation suivante aura lieu à 7 h 45. Si les autorisations d'accès changent pour un utilisateur connecté lors de la synchronisation, la session n'est plus valide. L'utilisateur est redirigé vers l'écran de connexion pour la demande suivante.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **LDAP**.
4. Sélectionnez **Gérer la synchronisation** > **Exécuter une synchronisation maintenant**.

## Configuration des certificats SSL ou TLS

Si vous utilisez un serveur d'annuaire LDAP pour l'authentification des utilisateurs et que vous souhaitez activer le chiffrement SSL ou l'authentification TLS, vous devez configurer votre certificat SSL ou TLS. L'authentification LDAP de QRadar utilise TLS 1.2.

### Procédure

1. À l'aide de SSH, connectez-vous à votre système en tant qu'utilisateur racine.
2. Entrez la commande suivante pour créer le répertoire `/opt/qradar/conf/trusted_certificates/` :

```
mkdir -p /opt/qradar/conf/trusted_certificates
```

3. Copiez le certificat SSL ou TLS du serveur LDAP vers le répertoire `/opt/qradar/conf/trusted_certificates` de votre système.
4. Vérifiez que l'extension de nom de fichier de certificat est `.cert`, ce qui indique que le certificat est digne de confiance.  
Le système QRadar charge uniquement les fichiers `.cert`.

## Affichage du texte de l'infobulle pour les informations LDAP

Vous créez un fichier de configuration des propriétés LDAP pour afficher les informations utilisateur LDAP en tant que texte d'infobulle. Ce fichier de configuration interroge la base de données LDAP pour les informations utilisateur LDAP associées aux événements, les violations, ou aux actifs (si disponibles).

### Avant de commencer

Le serveur Web doit être redémarré après la création des propriétés LDAP. Envisagez de planifier cette tâche au cours d'une fenêtre de maintenance lorsqu'aucun utilisateur actif n'est connecté au système.

### Pourquoi et quand exécuter cette tâche

L'exemple suivant répertorie les propriétés que vous pouvez ajouter à un fichier de configuration `ldap.properties`.

```
ldap.url=ldap://LDAPserver.example.com:389
ldap.authentication=simple
ldap.userName=user.name
ldap.password=your.encrypted.password
ldap.basedn=0=IBM,C=US
ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))
ldap.attributes.displayName=Name
ldap.attributes.email=Email
ldap.attributes.employeeID=EmployeeID
ldap.attributes.department=Department
```

### Procédure

1. Utilisez SSH pour vous connecter à IBM QRadar en tant qu'utilisateur racine.
2. Pour obtenir un mot de passe utilisateur LDAP chiffré, exécutez le script **Perl** suivant :

```
perl -I /opt/qradar/lib/Q1/ -e 'print "Password: ";my $password = <>;
$password =~ s/\n$//;use auCrypto; print Q1::auCrypto::encrypt ($password)'
```
3. Utilisez un éditeur de texte pour créer le fichier de configuration `/opt/qradar/conf/ldap.properties`.
4. Indiquez les informations d'emplacement et d'authentification pour accéder au serveur LDAP distant.
  - a) Indiquez l'URL du serveur LDAP et le numéro de port.

Utilisez `ldaps://` ou `ldap://` pour vous connecter au serveur distant, par exemple, `ldap.url=ldaps://LDAPserver.example.com:389`.
  - b) Entrez la méthode d'authentification utilisée pour accéder au serveur LDAP.

Les administrateurs peuvent utiliser la méthode d'authentification simple, par exemple, `ldap.authentication=simple`.
  - c) Entrez le nom d'utilisateur disposant des droits d'accès au serveur LDAP.


Par exemple, `ldap.userName=user.name`.
  - d) Pour vous authentifier auprès du serveur LDAP distant, entrez le mot de passe de l'utilisateur LDAP chiffré pour l'utilisateur.

Par exemple, `ldap.password=password`.
  - e) Entrez le nom distinctif de base utilisé pour rechercher les utilisateurs sur le serveur LDAP.

Par exemple, `ldap.basedn=BaseDN`.
  - f) Entrez une valeur à utiliser pour le filtre de paramètres de recherche dans LDAP.

Par exemple, dans QRadar, lorsque vous survolez `ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))`, la valeur `%USER%` est remplacée par le nom d'utilisateur.
5. Entrez un ou plusieurs attributs à afficher dans le texte de l'infobulle.

Vous devez inclure au moins un attribut LDAP. Chaque valeur doit utiliser ce format :  
`ldap.attributes.AttributeName=Descriptive text to show in UI.`

6. Vérifiez qu'il existe un droit de lecture pour le fichier de configuration `ldap.properties`.
7. Ouvrez une session QRadar en tant qu'administrateur.
8. Dans le menu de navigation () , cliquez sur **Admin**.
9. Cliquez sur **Avancé** > **Redémarrer le serveur Web**.

## Résultats

Les administrateurs peuvent survoler la zone **Nom d'utilisateur** de l'onglet **Activité de journal** Et onglet **Offenses** ou survoler la zone **Dernier utilisateur** dans l'onglet **Actifs** (si disponible) pour afficher plus d'informations sur l'utilisateur LDAP.

## Référentiels LDAP multiples

Vous pouvez configurer IBM QRadar pour mapper des entrées de plusieurs référentiels LDAP dans un référentiel virtuel unique.

**Remarque :** Si vous configurez le même compte utilisateur dans plusieurs serveurs LDAP, quel que soit le **Nom distinctif de base utilisateur** configuré, un utilisateur peut s'authentifier sur le serveur LDAP. Lorsqu'ils s'authentifient, l'utilisateur est autorisé à accéder au même compte QRadar.

Si plusieurs référentiels sont configurés, lorsqu'un utilisateur se connecte, il doit spécifier le référentiel à utiliser pour l'authentification. Ils doivent indiquer le chemin d'accès complet au référentiel et au nom de domaine dans la zone du nom d'utilisateur. Par exemple, si `Archive_1` est configuré pour utiliser le domaine `ibm.com` et que `Archive_2` est configuré pour utiliser le domaine `ibm.ca.com`, les informations de connexion peuvent ressembler à ces exemples :

- `OU=User Accounts,OU=PHX,DC=qcorpaa,DC=aa,DC=ibm.com\<username>`
- `OU=Office,OU=User Accounts,DC=qcorpaa,DC=aa,DC=ibm.ca.com\<username>`

Pour un exemple utilisant des ID d'archive, si l'ID d'archive de `Archive_1` est `UsersIBM` et que l'ID d'archive de `Archive_2` est `UsersIBMca`, les informations de connexion peuvent ressembler à ces exemples :

- `UsersIBM\<username>`
- `UsersIBMca\<username>`

Les informations utilisateur sont automatiquement importées à partir du serveur LDAP pour les référentiels qui utilisent des attributs d'utilisateur ou l'autorisation de groupes. Pour les référentiels qui utilisent l'autorisation locale, vous devez créer des utilisateurs directement sur le système QRadar.

## Exemple : Configuration d'accès le moins privilégié et configuration

Accorder aux utilisateurs le minimum d'accès dont ils ont besoin pour accomplir leurs tâches quotidiennes.

Vous pouvez affecter des privilèges différents pour les données IBM QRadar et les fonctions QRadar. Vous pouvez effectuer cette affectation en spécifiant des groupes d'acceptation et de refus différents pour les profils de sécurité et les rôles utilisateur. Les groupes d'acceptation affectent des privilèges et les groupes de refus restreignent les privilèges.

Examinons un exemple. Votre entreprise a embauché un groupe d'étudiants stagiaires. John est dans sa dernière année d'un programme spécialisé de cybersécurité à l'université locale. On lui a demandé de surveiller et d'examiner les vulnérabilités des réseaux connus et de préparer un plan d'assainissement fondé sur les résultats. Les informations sur les vulnérabilités du réseau de l'entreprise sont confidentielles.

En tant qu'administrateur QRadar, vous devez vous assurer que les stagiaires ont un accès limité aux données et aux systèmes. La plupart des stagiaires doivent se voir refuser l'accès à IBM QRadar

Vulnerability Manager, mais l'affectation spéciale de John exige qu'il ait cet accès. La politique de votre organisation est que les stagiaires étudiants n'ont jamais accès à l'API QRadar.

Le tableau suivant indique que John doit être membre des groupes **company.interns** et **qvm.interns** pour avoir accès à IBM QRadar Risk Manager et QRadar Vulnerability Manager.

*Tableau 8. Groupes de privilèges de rôle utilisateur*

Rôle utilisateur	Accepter	Refuser
Admin	<b>qradar.admin</b>	<b>company.firedemployees</b>
QVM	<b>qradar.qvm</b> <b>qvm.interns</b>	<b>company.firedemployees</b> <b>qradar.qrm</b> <b>company.interns</b>
QRM	<b>qradar.qrm</b> <b>company.interns</b>	<b>company.firedemployees</b>

Le tableau suivant indique que le profil de sécurité pour **qvm.interns** limite John à l'accès à l'API QRadar .

*Tableau 9. Groupes de privilèges du profil de sécurité*

Profil de sécurité	Accepter	Refuser
QVM	<b>qradar.secprofile.qvm</b>	<b>company.firedemployees</b>
API	<b>qradar.secprofile.qvm.api</b>	<b>company.firedemployees</b> <b>qradar.secprofile.qvm.interns</b>

## Authentification unique à l'ouverture de session

Le langage SAML (Security Assertion Markup Language) est un cadre d'authentification et d'autorisation entre un fournisseur de services (SP) et un fournisseur d'identité (PDI) où l'authentification est échangée à l'aide de documents XML signés numériquement. Le fournisseur de services accepte de faire confiance au fournisseur d'identité pour authentifier les utilisateurs. En retour, le fournisseur d'identité génère une assertion d'authentification, ce qui indique qu'un utilisateur a été authentifié.

En utilisant la fonction d'authentification SAML, vous pouvez facilement intégrer QRadar à votre serveur d'identité d'entreprise pour fournir une connexion unique et éliminer la nécessité de gérer les utilisateurs locaux QRadar. Les utilisateurs authentifiés sur votre serveur d'identité peuvent s'authentifier automatiquement auprès de QRadar. Ils n'ont pas besoin de se rappeler des mots de passe séparés ou de saisir des données d'identification chaque fois qu'ils accèdent à QRadar.

QRadar est entièrement compatible avec le profil de connexion unique Web SAML 2.0 en tant que fournisseur de services. Il prend en charge la connexion unique SP et la connexion unique à l'initiative IDP.

## Configuration de l'authentification SAML

Vous pouvez configurer IBM QRadar pour utiliser la structure de connexion unique SAML (Security Assertion Markup Language) 2.0 pour l'authentification et l'autorisation des utilisateurs.

### Avant de commencer

Pour terminer la configuration SAML dans QRadar, vous devez générer un fichier de métadonnées XML sur votre serveur de fournisseur d'identité (SAML).

## Pourquoi et quand exécuter cette tâche

Procédez comme suit pour configurer l'authentification SAML sur votre hôte QRadar. Une fois cette tâche terminée, vous devez configurer le fournisseur d'identité pour qu'il fonctionne avec QRadar.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **SAML 2.0**.
4. Dans la section **Configuration du fournisseur d'identité**, cliquez sur **Sélectionner un fichier de métadonnées**, accédez au fichier de métadonnées XML créé par votre fournisseur d'identité, puis cliquez sur **Ouvrir**.
5. Dans la section **Configuration du fournisseur de services**, entrez l'URL **ID d'entité**.
6. Sélectionnez un **Format NameID** :
  - Non spécifié (valeur par défaut)
  - Persistant
  - Adresse e-mail
  - Nom de sujet de certificat X509
  - Nom de domaine Windows
  - Kerberos

**Conseil** : Utilisez **Non spécifié** sauf si votre fournisseur d'identité ne le prend pas en charge.

7. Sélectionnez le **Protocole de liaison de demande** :
  - HTTP-POST
  - HTTP-Redirect
8. Sélectionnez **Oui** pour **Demande d'assertion signée**, sauf si le périphérique auquel vous vous connectez ne prend pas en charge les assertions signées.



**Avertissement** : La sélection de **Non** entraîne une communication non authentifiée avec le dispositif SAML et n'est pas recommandée, car elle permet à un attaquant basé sur un réseau non authentifié d'accéder aux ressources protégées.

9. Si vous souhaitez que l'assertion renvoyée par le Fournisseur d'Identité soit chiffrée en utilisant un certificat QRadar, sélectionnez **Oui** pour **une Demande d'Assertion Chiffrée**.

**Remarque** : L'activation du chiffrement requiert «[Installation des fichiers de règles JCE SDK sans restriction](#)», à la page 45.

10. Si vous souhaitez signer la demande d'authentification à l'aide d'un certificat QRadar, sélectionnez **Oui** pour **Signer la demande d'authentification**.
11. Si vous souhaitez déconnecter automatiquement les utilisateurs du fournisseur d'identité lorsqu'ils se déconnectent de QRadar, sélectionnez **Oui** pour **Activer la déconnexion unique initiée par le fournisseur de services**.

**Conseil** : Cette option n'est disponible que s'il est pris en charge par votre fournisseur d'identité.

12. Utilisez l'une des méthodes suivantes pour configurer un certificat pour la signature et le déchiffrement :

Option	Description
<b>Utiliser le certificat QRadar_SAML fourni</b>	Utilisez les liens de l'infobulle pour télécharger les fichiers CA racine, CRL de CA racine, CA intermédiaire et CRL intermédiaire du certificat, qui doivent être téléchargés dans le magasin de certificats sécurisé du serveur Identity Provider.



Option	Description
<b>Ajouter un certificat de signataire</b>	Cliquez sur <b>Ajouter</b> et suivez les instructions de cette rubrique pour ajouter un certificat personnalisé : « <a href="#">Importation d'un nouveau certificat pour la signature et le déchiffrement</a> », à la page 43
<b>Renouveler ou mettre à jour un certificat existant</b>	Cliquez sur <b>Renouveler</b> pour renouveler le certificat QRadar_SAML s'il est arrivé à expiration ou expire bientôt. Cliquez sur <b>Mettre à jour</b> pour mettre à jour un certificat personnalisé qui est arrivé à expiration ou qui va bientôt arriver à expiration. L'affichage de ces options varie selon le certificat que vous utilisez.

13. Sélectionnez l'une des méthodes suivantes pour autoriser les utilisateurs :

Option	Description
<b>Local</b>	Vous devez créer des utilisateurs QRadar locaux et configurer leurs rôles et profils de sécurité dans <b>Gestionnaire d'utilisateurs</b> .
<b>Attributs utilisateur</b>	QRadar utilise les attributs fournis dans les assertions SAML pour créer automatiquement des utilisateurs locaux lors des demandes d'authentification. Les rôles et les profils de sécurité sont affectés en fonction de la valeur de l'attribut de rôle et de l'attribut de profil de sécurité. Ces attributs doivent être fournis dans les assertions et les rôles et les profils de sécurité doivent exister dans QRadar. Les noms d'utilisateur, les rôles utilisateur et les profils de sécurité sont sensibles à la casse.  <b>Remarque :</b> Lorsque vous utilisez un rôle avec des fonctions d'administration, la valeur de l'attribut de profil de sécurité doit être <i>Admin</i> .  <b>Conseil :</b> Dans un environnement à plusieurs niveaux, vous devez configurer l'attribut <i>Locataire</i> et affecter des utilisateurs aux locataires. Si l'attribut locataire n'est pas fourni, l'utilisateur créé n'est affecté à aucun titulaire.

14. Cliquez sur **Sauvegarder le module d'authentification**.

Le fichier de métadonnées SAML QRadar est automatiquement téléchargé.

15. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Que faire ensuite

Si vous avez sélectionné l'autorisation **Locale**, accédez à [Chapitre 3, «Gestion des utilisateurs»](#), à la page 11 pour créer des utilisateurs locaux. Si vous avez sélectionné **Attributs utilisateur**, créez des rôles, des profils de sécurité et des locataires au besoin, puis déployez.

Après avoir configuré QRadar, vous devez configurer votre fournisseur d'identité à l'aide du fichier de métadonnées XML sauvegardé.

## Importation d'un nouveau certificat pour la signature et le déchiffrement

La fonction QRadar SAML 2.0 dispose d'options permettant d'utiliser un certificat x509 autre que le certificat QRadar\_SAML fourni pour la signature et le chiffrement.

### Procédure

1. Pour **Certificat de signature et de chiffrement**, cliquez sur **Ajouter**.
2. Dans la fenêtre **Importer un nouveau certificat**, entrez **Nom convivial** pour le certificat.
3. Cliquez sur **Parcourir** pour sélectionner un **Fichier de clés privées**, puis sur **Ouvrir**.
4. Cliquez sur **Parcourir** pour sélectionner un **Fichier de certificat**, puis sur **Ouvrir**.
5. Si le certificat à télécharger possède une autorité de certification intermédiaire, cliquez sur **Parcourir** pour sélectionner **Fichier CA intermédiaire**, puis cliquez sur **Ouvrir**.

6. Si l'autorité de certification racine du certificat n'est pas une autorité de certification racine commune préinstallée avec le système d'exploitation, cliquez sur **Parcourir** pour sélectionner **Fichier CA racine**, puis cliquez sur **Ouvrir**.
7. Cliquez sur **Télécharger** pour télécharger le certificat.

## Configuration de SAML avec Microsoft Active Directory Federation Services

Une fois que vous avez configuré SAML dans QRadar, vous pouvez configurer votre fournisseur d'identité à l'aide du fichier de métadonnées XML que vous avez créé au cours de ce processus. Cet exemple inclut des instructions de configuration de Microsoft Active Directory Federation Services (AD FS) pour communiquer avec QRadar à l'aide du cadre de connexion unique SAML 2.0.

### Avant de commencer

Pour configurer le serveur AD FS, vous devez d'abord configurer SAML dans QRadar. Copiez ensuite le fichier de métadonnées XML QRadar SAML que vous avez créé au cours de ce processus vers un emplacement accessible au serveur AD FS.

### Procédure

1. Dans la console AD FS Management, sélectionnez le dossier **Relying Party Trusts**.
2. Dans la barre d'options latérale **Actions**, cliquez sur Standard **Relying Party Trust**, puis sur **Démarrer**.  
L'assistant **Add Relying Party Trust** s'ouvre.
3. Dans la fenêtre **Sélectionner une source de données**, sélectionnez **Importer des données sur la partie de confiance à partir d'un fichier**, accédez au fichier de métadonnées XML SAML QRadar et cliquez sur **Ouvrir**.
4. Cliquez sur **Suivant**.
5. Entrez un **Nom d'affichage** et ajoutez **Notes**, puis cliquez sur **Suivant**.
6. Sélectionnez une règle de contrôle d'accès et cliquez sur **Suivant**.
7. Configurez les options supplémentaires dont vous avez besoin, puis cliquez sur **Suivant**.
8. Cliquez sur **Fermer**.
9. Dans le dossier **Relying Party Trusts**, sélectionnez la nouvelle fiducie que vous avez créée, puis cliquez sur **éditer la règle d'émission des demandes d'indemnisation**.
10. Cliquez sur **Ajouter une règle**.
11. Sélectionnez **Envoi d'attributs LDAP en tant que revendications** dans le menu **Modèle de règle d'indemnisation**, puis cliquez sur **Suivant**.
12. Entrez **Nom de la règle de réclamation** et sélectionnez **Magasin d'attributs**.
13. Sélectionnez les attributs à envoyer dans l'assertion, mappela à la **Type de demande sortante** appropriée, puis cliquez sur **Terminer**.
14. Cliquez sur **Ajouter une règle**.
15. Sélectionnez **Transformer une demande d'indemnisation à venir** dans le menu **Modèle de règle d'indemnisation**, puis cliquez sur **Suivant**.
16. Configurez les options suivantes :
  - nom de règle de demande
  - Type de demande de réclamation entrant-valeur UPN
  - Type de réclamation sortante en tant que NameID
  - Format NameID sortant
17. Sélectionnez **Transmettre toutes les valeurs de réclamation**, puis cliquez sur **Terminer**.
18. Si vous avez configuré QRadar pour utiliser le certificat QRadar\_SAML fourni pour SAML, copiez les fichiers de CA racine, CA intermédiaire et CRL précédemment téléchargés dans un répertoire du

serveur Windows. Ouvrez ensuite une fenêtre de ligne de commande en tant qu'administrateur sur le système d'exploitation Windows et entrez les commandes suivantes :

```
certutil -addstore -f ROOT <local_path>root-qradar-ca_ca
certutil -addstore -f CA <local_path>QRadarSAML_ca.crt
certutil -addstore -f ROOT <local_path>QRadarSAML_ca.crl
certutil -addstore -f Root <local_path>root-qradar-ca_ca.crl
```

Les fichiers se trouvent dans /opt/qradar/ca/www.

## Installation des fichiers de règles JCE SDK sans restriction

L'utilisation de la technologie de chiffrement est contrôlée par le droit américain. IBM Java Solution Developer Kits (SDKs) inclut des fichiers de règles de juridiction solides mais limités. Pour prendre en charge les assertions SAML chiffrées, avec IBM QRadar, vous devez d'abord obtenir les fichiers de règles JCE (Java Cryptography Extension) de juridiction illimitée.

### Procédure

1. Téléchargez les fichiers de règles JCE (Java Cryptography Extension) sans restriction à partir d'ici : [https://www.ibm.com/support/knowledgecenter/SSYKE2\\_8.0.0/com.ibm.java.security.component.80.doc/security-component/sdkpolicyfiles.html](https://www.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/sdkpolicyfiles.html)
2. Décompresser le fichier compressé.  
Sélectionnez les fichiers JAR suivants dans le dossier sans restriction :
  - local\_policy.jar
  - US\_export\_policy.jar
3. Placez les fichiers dans le répertoire suivant sur votre QRadar Console :  
/store/configservices/staging/globalconfig/java\_security
4. Dans l'onglet Admin, cliquez sur **Déployer les modifications**.
5. Cliquez sur **Paramètres avancés** > **Redémarrer le serveur Web**.

## Traitement des incidents d'authentification SAML

Utilisez les informations suivantes pour identifier et résoudre les erreurs et les problèmes lors de l'utilisation de SAML 2.0 avec QRadar.

### Échec de la connexion ou de la déconnexion

En cas d'échec d'une connexion unique ou d'une déconnexion unique, vérifiez que les métadonnées SAML QRadar que vous avez téléchargées vers le fournisseur d'identité correspondent aux dernières métadonnées déployées sur <https://<yourqradarserverhostname>/console/SAMLMetadata>. Vérifiez également que vous avez téléchargé l'autorité de certification racine, l'autorité de certification racine CA, le CA intermédiaire, les fichiers CRL du CA intermédiaire de votre certificat sélectionné à l'emplacement approprié des magasins de certificats du serveur de personnes déplacées. Lorsque le certificat QRadar\_SAML fourni est utilisé, vous pouvez télécharger ces fichiers à l'adresse suivante :

```
http://<yourqradarserverhostname>:9381/root-qradar-ca_ca
http://<yourqradarserverhostname>:9381/QRadarSAML_ca.crt
http://<yourqradarserverhostname>:9381/root-qradar-ca_ca.crl
http://<yourqradarserverhostname>:9381/QRadarSAML_ca.crl
```

**Remarque :** Si vous utilisez le certificat QRadar\_SAML fourni, les étapes ci-dessus sont requises après la restauration de QRadar à partir d'une sauvegarde.

### Compte non autorisé

Certaines questions de configuration peuvent générer cette erreur :

Ce compte n'est pas autorisé à accéder à QRadar.  
Déconnectez-vous de votre fournisseur d'identité SAML et utilisez un compte autorisé pour vous connecter.

Si vous utilisez l'autorisation **Locale**, vérifiez que l'**ID de nom** dans l'assertion SAML correspond à un nom d'utilisateur QRadar existant et que l'utilisateur est déployé.

Si vous utilisez l'autorisation **Attribut utilisateur**, vérifiez que l'assertion SAML contient l'attribut de rôle configuré et le profil de sécurité avec des valeurs correspondant à un profil de rôle et de sécurité déployé existant dans QRadar. Lorsque vous utilisez un rôle avec des fonctions d'administration, la valeur de l'attribut de profil de sécurité doit être *Admin*. Si l'assertion contient un attribut locataire dans un environnement multilocation, vérifiez que la valeur de l'attribut correspond à un titulaire existant dans QRadar.

## Fichiers journaux

Vous pouvez diagnostiquer plusieurs autres problèmes à l'aide des journaux du serveur Identity Provider et du journal `/var/log/qradar.error`.

## Restaurer la connexion au système pour l'investigation

Pour étudier les problèmes avec SAML 2.0, vous pouvez restaurer QRadar pour utiliser la connexion par défaut du système.

Copiez le contenu de `/opt/qradar/conf/templates/login.conf` dans `/opt/qradar/conf/login.conf`

Sinon, éditez le fichier `/opt/qradar/conf/login.conf` et modifiez

```
ModuleClass=com.q11labs.uiframeworks.auth.configuration.SamlLoginConfiguration
```

à

```
ModuleClass=com.q11labs.uiframeworks.auth.configuration.LocalPasswordLoginConfiguration
```

Effacez le cache du navigateur et connectez-vous en tant qu'administrateur. Une fois votre investigation terminée, modifiez à nouveau l'attribut par `SAMLLoginModule` et supprimez à nouveau le cache du navigateur.

## Impossible d'accéder à la console QRadar après la connexion avec un fournisseur d'identité

Vérifiez que le nom d'hôte de la console QRadar peut être résolu par le serveur DNS local. Vérifiez également que votre ordinateur peut accéder à la console QRadar en utilisant le nom d'hôte.

## Échec de connexion ou de déconnexion sur le serveur IDP

Consultez les journaux du serveur IDP pour déterminer si les erreurs sont causées par des erreurs dans les vérifications de révocation de la LCR. Si tel est le cas, importez les LCR de certificats QRadar\_SAML sur le serveur IDP ou assurez-vous que le serveur de personnes déplacées peut atteindre la console QRadar à l'aide d'une connexion HTTP.

## Le certificat du fournisseur d'identité est arrivé à expiration

Lorsque le certificat du fichier de métadonnées des fournisseurs d'identité est arrivé à expiration, vous ne pouvez pas vous connecter à QRadar et l'erreur suivante apparaît dans le fichier `/var/log/qradar.error` :

```
com.q11labs.uiframeworks.auth.saml.metadata.DefaultMetadataServiceImpl:  
[ERROR] NotAfter: <date>  
java.security.cert.CertificateExpiredException: NotAfter:
```

Pour résoudre ce problème, demandez à votre fournisseur d'identité de mettre à jour le certificat dans le fichier de métadonnées, puis reconfigurez SAML dans QRadar pour utiliser le nouveau fichier de métadonnées IDP.

## Le certificat QRadar\_SAML est arrivé à expiration

Une notification système QRadar s'affiche lorsque le certificat QRadar\_SAML est sur le point d'expirer. Avant l'expiration du certificat, vous devez le renouveler.

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **SAML 2.0**.
4. Cliquez sur **Renouveler** pour renouveler le certificat QRadar\_SAML.
5. Cliquez sur **Sauvegarder le module d'authentification**.

Le fichier de métadonnées SAML QRadar est automatiquement téléchargé.

6. Cliquez sur les liens de l'infobulle pour télécharger l'autorité de certification racine et le certificat d'autorité de certification intermédiaire QRadar, ainsi que les fichiers CRL.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.
8. Envoyez les fichiers suivants à votre serveur IDP pour déployer les modifications.
  - Fichier de métadonnées QRadar
  - Certificat CA racine QRadar
  - Certificat CA intermédiaire QRadar
  - Fichiers CRL

## Le certificat tiers est arrivé à expiration

Vous n'êtes pas obligé d'utiliser le certificat QRadar\_SAML fourni avec QRadar; vous pouvez utiliser votre propre certificat tiers. Lorsque le certificat est sur le point d'expirer, une notification système QRadar est affichée.

Avant l'expiration du certificat tiers, vous devez mettre à jour le certificat existant ou ajouter un nouveau certificat.

1. Dans l'onglet **Admin**, cliquez sur **Authentification**.
2. Cliquez sur **Paramètres du module d'authentification**.
3. Dans la liste **Module d'authentification**, sélectionnez **SAML 2.0**.
4. Cliquez sur **Ajouter** ou sur **Mettre à jour**.
5. Cliquez sur **Sauvegarder le module d'authentification**.

Le fichier de métadonnées SAML QRadar est automatiquement téléchargé.

6. Cliquez sur les liens de l'infobulle pour télécharger le certificat CA racine et CA intermédiaire QRadar, ainsi que les fichiers CRL du certificat.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.
8. Envoyez les fichiers suivants à votre serveur IDP pour déployer les modifications.
  - Fichier de métadonnées QRadar
  - Certificat CA racine QRadar
  - Certificat CA intermédiaire QRadar
  - Fichiers CRL



---

## Chapitre 4. Gestion des licences

Les clés de licence vous permettent d'obtenir des produits IBM QRadar spécifiques et de contrôler l'événement et la capacité de flux pour votre déploiement QRadar. Vous pouvez ajouter des licences à votre déploiement pour activer d'autres produits QRadar, tels que QRadar Vulnerability Manager.

Lorsque vous installez QRadar, la clé de licence par défaut est temporaire et vous donne accès au système pendant 35 jours à partir de la date d'installation. Le courrier électronique que vous avez reçu de IBM lorsque vous avez acheté QRadar contient vos clés de licences permanentes. Ces clés de licence étendent les fonctions de votre dispositif ; vous devez les appliquer avant l'expiration de la licence par défaut.

Pour appliquer une clé de licence au système, procédez comme suit :

1. Obtenez la clé de licence. Pour obtenir de nouvelles clés de licence, ou des clés de licence mises à jour, contactez votre ingénieur commercial.
2. Téléchargez la clé de licence.
3. Allouez la licence à un système.
4. Déployez la configuration complète.

Une fois que vous avez appliqué les clés de licence à QRadar, Redistribuer les taux EPS et FPM pour garantir que chacun des hôtes gérés dispose de la capacité suffisante pour gérer le volume moyen du trafic réseau, et qu'il dispose encore de suffisamment d'EPS et de FPM pour gérer efficacement une pointe de données. Il n'est pas nécessaire de déployer les modifications après la redistribution de la capacité EPS et FPM.

### Expiration de la licence

La capacité de traitement du système est mesurée par le volume d'événements et de flux que QRadar peut traiter en temps réel. Cette capacité peut être limitée par le matériel du dispositif ou les clés de licence. La clé de licence temporaire autorise 5 000 événements par seconde (EPS) sur QRadar Console et 10 000 EPS sur chaque hôte géré. Le taux FPM de la licence temporaire est de 200 000 sur QRadar Console et sur les hôtes gérés.

Lorsqu'une licence expire, QRadar continue de traiter les événements et s'écoule jusqu'aux limites de capacité sous licence. Si la capacité EPS et FPM de la licence expirée a été allouée à un hôte, le pool de licences partagées risque d'entrer dans un déficit et de bloquer les fonctions de QRadar sur les onglets **Activité réseau** et **Activité de journal**.

Lorsque QRadar n'est pas autorisé à gérer le volume de données réseau entrantes, vous pouvez ajouter une licence ayant plus de capacité d'événement ou de flux.

#### Concepts associés

Fonctions de votre produit IBM QRadar

Gestion de systèmes

IBM QRadar dispose d'une architecture modulaire qui prend en charge les déploiements de tailles et de topologies variables.

#### Information associée

QRadar : À propos des limites EPS & FPM

---

## Capacité de traitement des événements et des flux

La capacité d'un déploiement est mesurée par le nombre d'événements par seconde (EPS) et les flux par minute (FPM) que IBM QRadar peut collecter, normaliser et corréliser en temps réel. La capacité d'événement et de flux est définie par les licences qui sont téléchargées sur le système.

Chaque hôte de votre déploiement QRadar doit disposer de suffisamment de capacité d'événement et de flux pour s'assurer que QRadar peut gérer les pics de données entrants. La plupart des pics de données entrants sont temporaires, mais si vous recevez continuellement des notifications système indiquant que le système a dépassé la capacité de licence, vous pouvez remplacer une licence existante par une licence ayant plus de capacité EPS ou FPM.

### **Concepts associés**

#### Gestion des salves

IBM QRadar utilise la gestion des rafales pour s'assurer qu'aucune donnée n'est perdue lorsque le système dépasse les événements alloués par seconde (EPS) ou les limites de licence de flux par minute (FPM).

### **Tâches associées**

Distribution de la capacité d'événement et de flux

## **Pool de licences partagé**

Le débit d'EPS (événements par seconde) et de FPM (flux par minute) défini par chaque licence est combiné dans un pool de licences partagé. A partir du pool de licences partagé, vous pouvez répartir la capacité de traitement sur tout hôte d'un déploiement spécifique ou géré par une console, quel que soit l'hôte auquel la licence d'origine est affectée.

En ajustant l'allocation du pool de licences partagé, vous garantissez que la capacité de flux et d'événements est répartie en fonction de la charge de travail réseau et que chaque hôte QRadar dispose de suffisamment d'EPS et de FPM pour gérer efficacement les périodes de pointe.

Dans les déploiements dotés de dispositifs de collecte d'événements et de processeurs d'événements distincts, le collecteur d'événements hérite du débit d'EPS du processeur d'événements auquel il est associé. Pour augmenter la capacité du collecteur d'événements, allouez davantage d'EPS du pool de licences partagé au processeur d'événements parent.

### **Contributions au pool de licences**

Une licence qui inclut à la fois la capacité d'événements et de flux peut ne pas contribuer au pool de licences partagé en matière d'EPS et de FPM. Les contributions au pool de licences dépendent du type de dispositif auquel la licence est allouée. Par exemple, lorsque vous appliquez une licence à un processeur d'événements 16xx, seuls les EPS sont ajoutés au pool de licences. La même licence, lorsqu'elle est appliquée à un processeur de flux 17xx, contribue au pool de licences uniquement avec des FPM. L'application de la licence à un processeur d'événements/de flux 18xx ajoute à la fois des EPS et des FPM au pool. A l'exception des licences logicielles pour les collecteurs d'événements ou de flux, toutes les licences logicielles ajoutent les EPS et les FPM au pool de licences partagé, quel que soit le type de dispositif auquel la licence est attribuée.

A partir du QRadar V7.3.2, vous pouvez acquérir des incréments d'EPS/flux empilables plutôt que remplacer la licence existante de la console ou d'autres hôtes gérés lorsque vous devez augmenter les seuils d'événement ou de flux globaux de votre déploiement. Une fois les licences téléchargées et déployées, la capacité d'événement/flux peut ensuite être réallouée via Gestion du pool de licences.

### **Dépassement des limites de capacité de traitement sous licence**

Le pool de licences est suralloué lorsque les EPS et FPM combinés, alloués aux hôtes gérés, dépassent les EPS et les FPM qui se trouvent dans le pool de licences partagé. Lorsque le pool de licences est suralloué, la fenêtre **Gestion du pool de licences** affiche une valeur négative pour les EPS et les FPM, et le graphique d'allocation devient rouge. QRadar bloque les fonctionnalités sur les onglets **Activité réseau** et **Activité du journal**, y compris la possibilité d'afficher des événements et des flux à partir de la liste **Messages** de la barre d'outils QRadar principale.

Pour activer les fonctionnalités bloquées, réduisez les EPS et les FPM que vous avez alloués aux hôtes gérés dans votre déploiement. Si les licences existantes ne disposent pas d'une capacité de flux et d'événements suffisante pour gérer le volume de données du réseau, téléchargez une nouvelle licence d'une capacité suffisante en EPS ou FPM pour résoudre le déficit du pool de licences partagé.



## Licences ayant expiré

Lorsqu'une licence arrive à expiration, QRadar continue de traiter les événements et les flux au débit alloué.

Si la capacité en EPS et en FPM de la licence arrivée à expiration a été allouée à un hôte, les ressources partagées dans le pool de licences risquent d'afficher un déficit et d'entraîner QRadar à bloquer les fonctionnalités des onglets **Activité réseau** et **Activité du journal**.

## Dimensionnement des capacités

La meilleure façon de traiter les pics de données est de s'assurer que votre déploiement dispose de suffisamment d'événements par seconde (EPS) et de flux par minute (FPM) pour équilibrer les périodes de pointe des données entrantes. L'objectif est d'allouer EPS et FPM de manière à ce que l'hôte dispose d'une capacité suffisante pour traiter les pics de données de manière efficace, mais ne dispose pas de grandes quantités de BPA en veille et de FPM.

Lorsque le serveur EPS ou FPM qui est alloué à partir du pool de licences est très proche de la moyenne EPS ou FPM pour le dispositif, le système est susceptible d'accumuler des données dans une file d'attente temporaire à traiter ultérieurement. Plus les données qui s'accumulent dans la file d'attente temporaire, également appelées file d'attente de traitement en rafale, prennent plus de temps QRadar pour traiter l'arriéré. Par exemple, un hôte QRadar avec un taux alloué de 10 000 EPS prend plus de temps pour vider la file d'attente de traitement des rafales lorsque le taux d'EPS moyen de l'hôte est de 9 500, par rapport à un système où le taux d'EPS moyen est de 7 000.

Les infractions ne sont pas générées tant que les données n'ont pas été traitées par le dispositif, de sorte qu'il est important de réduire le nombre de fois que QRadar ajoute des données à la file d'attente de traitement des rafales. En s'assurant que chaque hôte géré dispose de la capacité suffisante pour traiter des rafales de données courtes, vous réduirez le temps nécessaire à QRadar pour traiter la file d'attente, en veillant à ce que les infractions soient créées lorsqu'un événement se produit.

Lorsque le système dépasse de façon continue la capacité de traitement allouée, vous ne pouvez pas résoudre le problème en augmentant la taille de la file d'attente. Les données excédentaires sont ajoutées à la fin de la file d'attente de traitement en rafale où elles doivent attendre d'être traitées. Plus la file d'attente est grande, plus les événements en file d'attente doivent être traités par le dispositif.

### Concepts associés

Exemple : pointe de données entrantes

Chaque matin, entre 8 heures et 9 heures, le réseau d'une entreprise connaît une pointe de données lorsque les employés se connectent et commencent à utiliser les ressources réseau.

## Octroi de licence incrémentiel

L'octroi de licence incrémentiel rationalise le processus de distribution de licence et vous permet de gagner du temps et d'épargner vos efforts car vous n'avez pas besoin de licences séparées pour chaque dispositif. Achetez des augmentations de capacité mensuelles qui peuvent être appliquées à votre déploiement, sans courir le risque que ces clés temporaires puissent arrêter l'ensemble du système lorsqu'elles expirent. Maintenant, vous pouvez ajouter d'autres flux et événements à la licence de la console et redistribuer à votre pool d'appareils comme vous le voyez. Utilisez votre budget opérationnel pour ajouter de la capacité aux licences perpétuelles sur une base temporaire pour les projets à court terme, comme l'intégration réseau, la réorganisation et le test des cas d'utilisation.

Avec une licence incrémentielle, vous pouvez désormais acquérir des incréments d'EPS/Flow empilables au lieu de remplacer la licence de console existante ou d'autres hôtes gérés lorsque vous avez besoin d'augmenter les seuils d'événement ou de flux généraux de votre déploiement. Une fois les licences téléchargées et déployées, la capacité d'événement/flux peut ensuite être réallouée via Gestion du pool de licences. Par exemple, supposons que vous disposez d'un élément 3105 All-in-One avec 1 000 EPS sur une clé perpétuelle. Vous travaillez sur un projet de six mois dans lequel plusieurs sources de journal doivent être intégrées pendant une période temporaire. Auparavant, ce projet aurait pour effet de dépasser la limite de 1 000 EPS pour les volumes EPS. Avec la nouvelle fonctionnalité de licence incrémentielle, vous pouvez acheter 2500 EPS de plus pour seulement 6 mois. IBM fournit une clé de

licence qui augmente progressivement le serveur EPS de 1000 à 3500 pour la période de 6 mois. À la fin de la période de 6 mois, les 2500 EPS supplémentaires expirant, mais les 1000 EPS d'origine restent opérationnels, sans intervention supplémentaire de la prise en charge ou de la distribution des produits.

## Événements internes

Les dispositifs IBM QRadar génèrent un petit nombre d'événements internes lorsqu'ils communiquent entre eux au fur et à mesure qu'ils traitent des données.

Pour vous assurer que les événements internes ne sont pas comptés sur la capacité allouée, le système renvoie automatiquement tous les événements internes au pool de licences immédiatement après leur génération.

## Gestion des salves

---

IBM QRadar utilise la gestion des rafales pour s'assurer qu'aucune donnée n'est perdue lorsque le système dépasse les événements alloués par seconde (EPS) ou les limites de licence de flux par minute (FPM).

Lorsque QRadar reçoit une pointe de données qui lui permet de dépasser les limites EPS et FPM allouées, les événements et flux supplémentaires sont déplacés vers une file d'attente temporaire à traiter lorsque le débit de données entrant ralentit. Lorsque la gestion des rafales est déclenchée, une notification système vous avertit que le dispositif a dépassé la limite de licence EPS ou FPM.

L'arriéré dans la file d'attente temporaire est traité dans l'ordre où les événements ou les flux ont été reçus. Les données plus anciennes au début de la file d'attente sont traitées avant les données les plus récentes à la fin de la file d'attente. La vitesse à laquelle la file d'attente se vide ou se remplit est affectée par plusieurs facteurs, notamment le volume et la durée de la pointe de données, la capacité du dispositif et la taille de la charge.

Les appareils matériels peuvent normalement gérer des taux de rafale d'au moins 50% supérieurs à ceux de la fonction EPS et FPM du dispositif, et peuvent stocker jusqu'à 5GB dans la file d'attente temporaire. La capacité réelle dépend de la charge du système. Les machines virtuelles peuvent obtenir des résultats similaires si la machine virtuelle est correctement dimensionnée et qu'elle répond aux exigences de performance.

Le taux de reprise en rafale correspond à la différence entre le taux alloué et le taux entrant. Lorsque le volume de données entrantes ralentit, le système traite l'arriéré des événements ou des flux dans la file d'attente aussi rapidement que le taux de récupération le permet. Plus le taux de récupération est faible, plus il faut de temps pour vider la file d'attente.

### Concepts associés

[Capacité de traitement des événements et des flux](#)

### Tâches associées

[Distribution de la capacité d'événement et de flux](#)

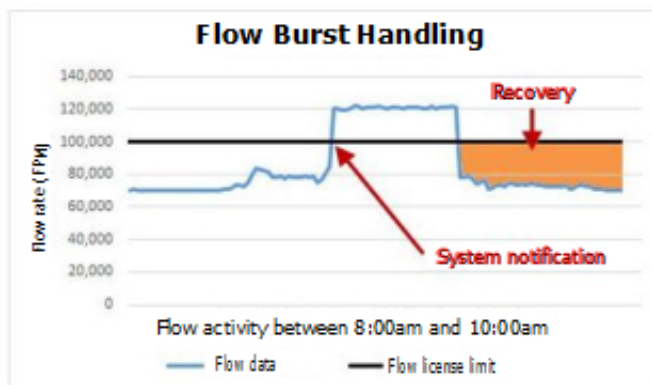
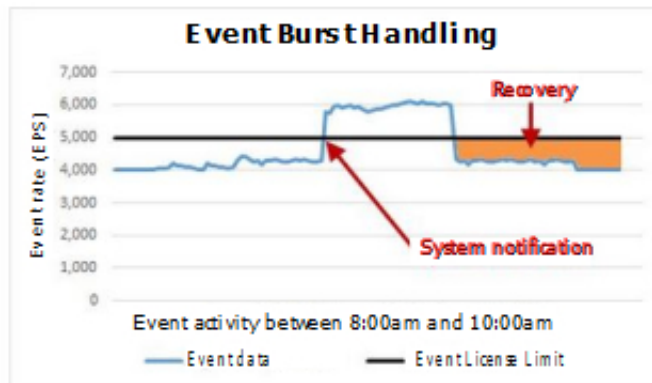
## Exemple : pointe de données entrantes

Chaque matin, entre 8 heures et 9 heures, le réseau d'une entreprise connaît une pointe de données lorsque les employés se connectent et commencent à utiliser les ressources réseau.

Le déploiement de l'entreprise inclut un dispositif QRadar 1828 Event / Flow Processor qui est alloué 5 000 événements par seconde (EPS) et 100 000 flux par minute (FPM). La capacité moyenne de ce dispositif est de 4 000 EPS et de 70 000 FPM.

Pendant le pic de données, qui atteint son maximum vers 9h du matin, le dispositif reçoit régulièrement jusqu'à 6 000 EPS et 120.000 FPM. QRadar déplace automatiquement les événements et flux supplémentaires (1 000 EPS et 20 000 FPM) vers la file d'attente de traitement des rafales, et génère une notification système pour avertir l'administrateur que le dispositif a dépassé la capacité allouée.

Les images suivantes montrent une fenêtre de deux heures lorsque l'événement entrant et les données de flux dépassent la capacité sous licence, ce qui déclenche une notification système et une période de reprise après le retour à la normale du volume de données.



Le taux de récupération correspond à la différence entre le volume EPS ou FPM alloué et le débit actuel des données entrantes. Dans cet exemple, lorsque l'événement et les débits reviennent à la normale, le taux de récupération est de 1 000 EPS et de 30 000 FPM.

5,000 licensed events - 4,000 incoming events = 1,000 EPS recovery rate  
 100,000 licensed flows - 70,000 incoming flows = 30,000 FPM recovery rate

Les infractions ne sont pas générées tant que les données n'ont pas été traitées par le dispositif, de sorte qu'il est important d'allouer suffisamment d'EPS et de FPM au dispositif pour s'assurer qu'il peut récupérer rapidement à partir d'une pointe de données.

### Concepts associés

#### Dimensionnement des capacités

La meilleure façon de traiter les pics de données est de s'assurer que votre déploiement dispose de suffisamment d'événements par seconde (EPS) et de flux par minute (FPM) pour équilibrer les périodes de pointe des données entrantes. L'objectif est d'allouer EPS et FPM de manière à ce que l'hôte dispose d'une capacité suffisante pour traiter les pics de données de manière efficace, mais ne dispose pas de grandes quantités de BPA en veille et de FPM.

### Tâches associées

Distribution de la capacité d'événement et de flux

## Téléchargement d'une clé de licence

---

Les clés de licence déterminent vos droits sur les produits et les fonctions IBM QRadar ainsi que la capacité du système pour le traitement des événements et des flux.

### Avant de commencer

Si vous avez besoin d'aide pour obtenir une nouvelle clé de licence ou une clé de licence mise à jour, contactez votre ingénieur commercial local.

### Pourquoi et quand exécuter cette tâche

Vous devez télécharger une clé de licence lorsque vous effectuez les tâches suivantes :

- Mise à jour d'une licence de console QRadar arrivée à expiration
- Augmentation des limites d'événements par minute (EPS) ou de flux par minute (FPM)
- Ajout d'un produit QRadar à votre déploiement, tel que IBM QRadar Vulnerability Manager


A partir de QRadar V7.3.0, vous n'avez pas besoin de télécharger une nouvelle licence lorsque vous ajoutez un processeur d'événements ou un processeur de flux à votre déploiement. Une licence de dispositif perpétuelle, ou permanente, est automatiquement affectée aux processeurs d'événement et de flux, et vous pouvez allouer des EPS ou FPM du pool de licences au dispositif.

A partir du QRadar V7.3.2, vous pouvez acquérir des incréments d'EPS/flux empilables plutôt que remplacer la licence existante de la console ou d'autres hôtes gérés lorsque vous devez augmenter les seuils d'événement ou de flux globaux de votre déploiement. Une fois les licences téléchargées et déployées, la capacité d'événement/flux peut ensuite être réallouée via Gestion du pool de licences.

Si la clé de licence de votre console QRadar Console arrive à expiration, vous êtes automatiquement dirigé vers la fenêtre **Gestion du système et de la licence** lorsque vous vous connectez. Vous devez télécharger une clé de licence pour pouvoir continuer.

Si un système d'hôte géré dispose d'une clé de licence arrivée à expiration, un message s'affiche lorsque vous vous connectez et indique qu'un hôte géré nécessite une nouvelle clé de licence. Utilisez la fenêtre **Gestion du système et de la licence** pour mettre à jour la clé de licence. Si le pool de licences n'est pas suralloué, supprimez la clé arrivée à expiration et allouez des EPS ou FPM du pool de licences à l'hôte géré.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la barre d'outils, cliquez sur **Télécharger la licence**.
4. Dans la boîte de dialogue, cliquez sur **Sélectionner le fichier**.
5. Sélectionnez la clé de licence, puis cliquez sur **Ouvrir**.
6. Cliquez sur **Télécharger**, puis sur **Confirmer**.

### Résultats

La licence est téléchargée sur votre console QRadar Console et s'affiche dans la fenêtre **Gestion du système et de la licence**.

Par défaut, la plupart des licences ne sont pas automatiquement allouées à un hôte QRadar. Cependant, le système alloue automatiquement toutes les clés QRadar Vulnerability Manager, QRadar Risk Manager et QRadar Incident Forensics à la console QRadar.

**Remarque :** Les licences incrémentielles qui étendent la capacité en nombre d'événements et de flux sont automatiquement allouées à la console.

## Que faire ensuite

Allouez la licence à un système.

### Information associée

[Gestion des licences dans QRadar SIEM](#)

## Allocation d'une clé de licence à un hôte

---

Allouez une clé de licence à un hôte IBM QRadar lorsque vous souhaitez remplacer une licence existante, ajouter de nouveaux produits QRadar ou augmenter la capacité d'événement ou de flux dans le pool de licences partagé.

### Avant de commencer


Vous devez [télécharger une clé de licence](#).

### Pourquoi et quand exécuter cette tâche

Vous pouvez allouer plusieurs licences à une console QRadar. Par exemple, vous pouvez allouer des clés de licence qui ajoutent IBM QRadar Risk Manager et QRadar Vulnerability Manager à votre console QRadar.

Vous ne pouvez pas rétablir une clé de licence après l'avoir ajoutée à un hôte QRadar. Si vous allouez par erreur une licence à un hôte, vous devez déployer la modification, puis supprimer la licence du système. Une fois la licence supprimée, vous pouvez la télécharger à nouveau, puis la réallouer. Lorsqu'elle est réallouée à l'hôte approprié, vous devez déployer à nouveau les modifications.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Licences**.
4. Sélectionnez la licence, puis cliquez sur **Allouer un système à la licence**.

**Conseil :** Lorsque vous sélectionnez **Système** dans la liste **Afficher**, le libellé devient **Allocate License to a System**.

5. Pour filtrer la liste des licences, entrez un mot clé dans la zone de recherche.
6. Dans la fenêtre **Allocate a System to a License**, sélectionnez l'hôte auquel vous souhaitez allouer la licence, puis cliquez sur **Allocate System to License**.

## Distribution de la capacité d'événement et de flux

---

Utilisez la fenêtre **Gestion des pools de licences** pour vous assurer que les événements par seconde (EPS) et les flux par minute (FPM) auxquels vous avez droit sont entièrement utilisés. Vérifiez également que IBM QRadar est configuré pour gérer des rafales périodiques de données sans supprimer d'événements ou de flux, ou avoir des EPS et FPM inutilisés excessifs.


### Avant de commencer

Vérifiez que le pool de licences dispose de suffisamment d'EPS ou de FPM non alloués. Si le serveur EPS ou FPM du pool de licences est entièrement alloué, redistribuez les allocations.

### Pourquoi et quand exécuter cette tâche

Une allocation adéquate de la capacité EPS et FPM est importante pour garantir que QRadar traite tous les événements et flux en temps opportun. L'objectif est d'allouer EPS et FPM de façon à ce que l'hôte ait une capacité suffisante pour traiter efficacement les pics de données, sans avoir une capacité EPS et FPM en veille excessive.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Licences**.
4. Cliquez sur **Gestion des pools de licences** et déplacez la souris sur les graphiques circulaires pour afficher la capacité totale du déploiement.
5. Dans la table **Allocations de licence**, consultez les données pour déterminer si le dispositif a suffisamment d'événements et de capacité de flux pour couvrir les EPS et FPM moyens, et qu'il reste suffisamment à gauche pour couvrir les volumes de pointe.

### En savoir plus sur la révision des données d'événement et de capacité de flux :

- Les colonnes **Allocation EPS** et **Allocation FPM** affichent la capacité affectée à chaque processeur QRadar ou à chaque console QRadar.
  - Les colonnes **Moyenne EPS** et **MPF moyenne** indiquent le nombre moyen d'événements et de flux traités par l'hôte QRadar au cours des 30 derniers jours.
  - Cliquez sur le nom d'hôte pour afficher les détails des taux de pic EPS et FPM des 30 derniers jours.
6. Pour modifier le taux EPS ou FPM alloué pour l'hôte QRadar, cliquez sur l'icône d'édition.
  7. Mettez à jour la zone **EPS alloga** ou **Allocated FPM**, puis cliquez sur **Sauvegarder**.
- Les attributions révisées de SPE et de FPM sont validées par rapport à ces critères :

- L'allocation EPS doit être un multiple de 100, et l'allocation FPM doit être un multiple de 5 000.
- Le serveur EPS ou FPM alloué ne peut pas entraîner la surallocation du pool de licences.
- La fonction EPS ou FPM allouée ne peut pas dépasser les limites matérielles du type d'appliance.

Si vos modifications ne sont pas correctement allouées, cliquez sur **Admin > Avancé > Redémarrer les services de collecte d'événements**.

Si le problème persiste, cliquez sur **Admin > Avancé > Déployer la configuration complète**. S'il existe des messages d'avertissement de SourceMonitor dans les journaux QRadar, cliquez sur **Admin > Avancé > Redémarrer les services de collecte d'événements**. Un déploiement complet entraîne l'arrêt de la collecte d'événements pendant plusieurs minutes.

### Concepts associés

Exemple : pointe de données entrantes

Chaque matin, entre 8 heures et 9 heures, le réseau d'une entreprise connaît une pointe de données lorsque les employés se connectent et commencent à utiliser les ressources réseau.

Gestion des salves

IBM QRadar utilise la gestion des rafales pour s'assurer qu'aucune donnée n'est perdue lorsque le système dépasse les événements alloués par seconde (EPS) ou les limites de licence de flux par minute (FPM).

Capacité de traitement des événements et des flux

## Affichage des détails de la licence

---


Affichez les détails de la licence pour afficher des informations telles que le statut, l'expiration et les limites de débit d'événements et de flux pour chaque licence qui est téléchargée sur le système.

### Pourquoi et quand exécuter cette tâche

Les licences qui ne sont pas encore allouées à un hôte apparaissent en haut du tableau **Licence**. Chaque hôte du déploiement dispose d'une ligne récapitulative, qui est affichée en gras. Les zones **Limite de taux d'événements** et **Limite de débit** de la ligne récapitulative indiquent les EPS et FPM qui sont alloués à l'hôte. Si l'hôte ne dispose d'aucun EPS ou FPM alloué, **N/A** est affiché dans les colonnes **Limite de taux d'événements** et **Limite de débit**.

Les licences allouées à un hôte QRadar apparaissent sous la forme d'une ligne enfant, imbriquée sous la ligne récapitulative de l'hôte QRadar. Pour les dispositifs QRadar Console et Processeur de flux et d'événement, la ligne enfant affiche les dates de capacité et d'expiration de la partie EPS et FPM de la licence. Avant de gérer les licences, sélectionnez la ligne qui correspond à la licence individuelle.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Licences**.
4. Pour afficher des informations détaillées sur un hôte ou une licence spécifique, sélectionnez la ligne imbriquée, puis cliquez sur **Actions > Afficher la licence**.

Etat	Description
<b>Non alloué</b>	La licence est téléchargée mais n'est pas allouée à un hôte QRadar. Les EPS et FPM de la licence ne contribuent pas au pool de licences.
<b>Non déployé</b>	La licence est allouée à un hôte QRadar, mais n'est pas déployée. La licence n'est pas encore active dans votre déploiement. Les EPS et FPM sont inclus dans le pool de licences.
<b>Déployé</b>	La licence est allouée et active dans votre déploiement. Les EPS et FPM sont inclus dans le pool de licences.

## Suppression de licences


Supprimez une licence si vous l'avez attribuée par erreur au mauvais hôte QRadar. Supprimez également une licence expirée pour empêcher IBM QRadar de générer des notifications système quotidiennes relatives à la licence expirée.

### Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas supprimer une licence si elle entraîne la sur allocation du pool de licences. QRadar valide que le pool de licences dispose d'une capacité EPS et FPM non allouée suffisante pour couvrir la perte de capacité lorsque la licence est supprimée. Par exemple, si vous souhaitez supprimer une licence dont l'EPS est associé à 2 500, le pool de licences doit avoir au moins 2 500 EPS qui n'ont pas été alloués à un hôte QRadar.

Si le pool de licences ne dispose pas de suffisamment de EPS et FPM non alloués pour couvrir le déficit, vous devez ajuster les allocations EPS et FPM pour vous assurer que le pool n'est pas suralloué lorsque vous supprimez la licence.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Licences**.
4. Dans le tableau hôte, sélectionnez la ligne enfant imbriquée qui contient la licence que vous souhaitez supprimer.
5. Cliquez sur **Actions > Supprimer la licence**.

La **date d'expiration de la licence** affiche **Perpétuelle** avec une **Limite de taux d'événements** et une **Limite de débit** de 0.


## Exportation des informations de licence

---

Pour l'audit, exportez des informations sur les clés de licence installées sur votre système vers un fichier .xml externe.

Vous ne pouvez pas utiliser le fichier .xml pour déplacer des licences vers un autre système. Utilisez-le uniquement pour afficher des informations détaillées sur les clés de licence individuelles.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Licences**.
4. Dans le menu **Actions**, sélectionnez **Licences d'exportation**.
5. Enregistrez le fichier localement et cliquez sur **OK**.



---

## Chapitre 5. Gestion de systèmes

IBM QRadar dispose d'une architecture modulaire qui prend en charge les déploiements de tailles et de topologies variables.

Dans un déploiement à un seul hôte, tous les composants logiciels s'exécutent sur un seul dispositif et QRadar Console fournit l'interface utilisateur, les vues d'événements et de flux en temps réel, les rapports, les violations, les informations sur les actifs et les fonctions d'administration.

Pour l'échelle QRadar, vous pouvez ajouter des hôtes gérés sans console au déploiement. Pour chaque hôte géré, vous pouvez configurer un type de composant spécifique, tel que des collecteurs, des processeurs et des noeuds de données. Vous profitez ainsi pleinement des atouts de l'environnement distribué et de sa plus grande souplesse de gestion de la collecte et du traitement des données.

### Concepts associés

#### Gestion des licences

Les clés de licence vous permettent d'obtenir des produits IBM QRadar spécifiques et de contrôler l'événement et la capacité de flux pour votre déploiement QRadar. Vous pouvez ajouter des licences à votre déploiement pour activer d'autres produits QRadar, tels que QRadar Vulnerability Manager.

#### Fonctions de votre produit IBM QRadar

---

## Informations sur la santé du système

L'application Deployment Intelligence QRadar est une application de surveillance puissante qui regroupe les données de santé d'historique pour chaque hôte géré de votre déploiement. Utilisez l'application pour surveiller la santé de votre déploiement QRadar.

La **Présentation du statut de l'hôte** sur le tableau de bord QRadar Deployment Intelligence affiche l'état de chaque dispositif (actif, de secours, hors ligne ou inconnu) et le nombre de notifications pour chaque hôte, le nom d'hôte et le type de dispositif, l'utilisation du disque, le statut et le temps modifié. À partir de **Présentation du statut de l'hôte**, vous pouvez explorer en aval pour afficher des informations plus visuelles sur le statut de l'hôte géré, y compris les débits d'événements et de flux, les notifications système et les informations sur le disque.

Pour vous aider à résoudre les incidents liés à votre déploiement, utilisez la fonction **Obtenir les journaux** pour collecter des fichiers journaux à partir de QRadar Console et de tout autre hôte géré dans votre déploiement.

L'application QRadar Deployment Intelligence est disponible sur IBM Security App Exchange. Vous devez installer l'application, puis créer un jeton de service autorisé pour permettre à l'application d'utiliser l'API QRadar pour demander des données à partir des hôtes gérés.

L'application QRadar Deployment Intelligence utilise des mesures de santé QRadar pour surveiller votre déploiement. Les mesures de santé sont des événements système légers et essentiels qui ne sont pas pris en compte par rapport à votre licence.

---

## Types de composant QRadar

Chaque dispositif IBM QRadar ajouté au déploiement comporte des composants configurables qui indiquent la façon dont l'hôte géré se comporte dans QRadar.

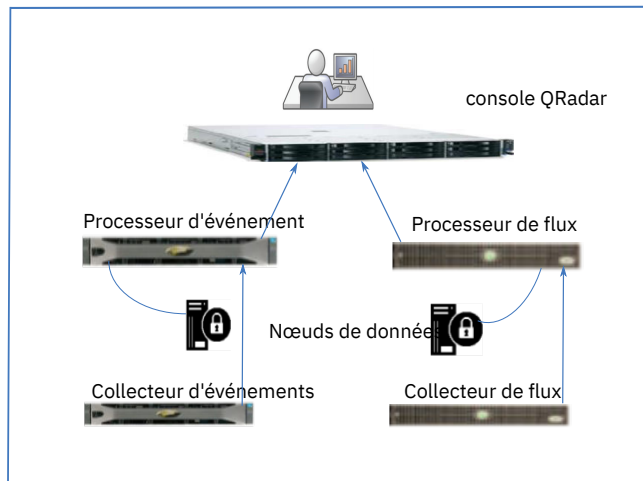


Figure 5. Composants d'événement et de flux QRadar

## QRadar Console

QRadar Console fournit l'interface du produit QRadar, les vues d'événements et de flux en temps réel, les rapports, les infractions, les informations sur les actifs et les fonctions d'administration. Dans les environnements répartis, QRadar Console est utilisé pour gérer les autres composants du déploiement.

## Collecteur d'événements

Collecteur d'événements collecte des événements à partir de sources de journal locales et éloignées et normalise les données d'événement brutes pour qu'elles puissent être utilisées par QRadar. Pour conserver les ressources système, Collecteur d'événements regroupe des événements identiques et envoie les données à processeur d'événements.

## processeur d'événements

Le processeur d'événements traite les événements collectés à partir d'un ou de plusieurs composants Collecteur d'événements. Si les événements sont mis en correspondance avec les règles personnalisées définies sur la console, processeur d'événements suit l'action définie dans la réponse de règle.

Chaque processeur d'événements dispose d'un espace de stockage local. Les données d'événement sont stockées sur le processeur ou peuvent être stockées sur un Noeud de données.

## QRadar QFlow Collector

QRadar QFlow Collector collecte les flux de réseau à partir d'unités sur votre réseau. Les flux actifs et enregistrés sont inclus, tels que les points réseau, les ports d'intervalle, NetFlow et les journaux de flux QRadar.

**Restriction :** QRadar Log Manager ne prend pas en charge la collecte de flux.

## processeur de flux

Le processeur de flux traite les flux provenant d'un ou de plusieurs dispositifs QRadar QFlow Collector. Le dispositif processeur de flux peut également collecter des flux réseau externes tels que NetFlow, J-Flow et sFlow directement depuis des routeurs sur votre réseau.

processeurs de flux inclut un processeur de bord et une mémoire interne pour les données de flux.

## Noeud de données

Le Noeud de données reçoit des événements de sécurité et des flux provenant des processeurs d'événements et de flux, et stocke les données sur le disque.

Noeud de données est toujours connecté à un processeur d'événements ou à un processeur de flux.

## Appareils source et cible hors site

Un dispositif hors site est un dispositif QRadar qui ne fait pas partie du déploiement surveillé par QRadar Console.

Un dispositif source externe transmet des données normalisées à un Collecteur d'événements. Vous pouvez configurer une source externe pour chiffrer les données avant de les transférer.

Un dispositif cible hors site reçoit des données d'événement ou de flux normalisées provenant de n'importe quel Collecteur d'événements ou de tout processeur de votre déploiement.

Les versions ultérieures des systèmes QRadar peuvent recevoir des données de versions antérieures de systèmes QRadar, mais les versions antérieures ne peuvent pas recevoir de données des versions ultérieures. Pour éviter les incidents, mettez à niveau tous les récepteurs avant de mettre à niveau les expéditeurs.

## Noeuds de données

---

Un nœud de données est un dispositif que vous pouvez ajouter à vos processeurs d'événements et de flux pour augmenter la capacité de stockage et améliorer les performances de recherche. Vous pouvez ajouter un nombre illimité de nœuds de données à votre déploiement IBM QRadar et ils peuvent être ajoutés à tout moment. Chaque nœud de données peut être connecté à un seul processeur, mais un processeur peut prendre en charge plusieurs nœuds de données.

Pour plus d'informations sur la planification de votre déploiement, voir le *IBM QRadar - Guide d'architecture et de déploiement*.

## Rééquilibrage des données après l'ajout d'un nœud de données

Lorsque vous ajoutez un nœud de données, IBM QRadar rééquilibre les données pour améliorer la recherche et les performances globales du système.

Le rééquilibrage des données inclut la décompression de données plus anciennes et le déplacement de données sur l'unité de stockage d'origine pour la répartir uniformément sur tous les périphériques connectés.

Par exemple, votre déploiement dispose d'un processeur d'événements qui reçoit 20 000 événements par seconde (EPS). Lorsque vous ajoutez des nœuds de données, QRadar distribue automatiquement les événements dans le processeur d'événements et tous les nœuds de données qui y sont disponibles. Si vous ajoutez trois nœuds de données, le processeur d'événements stocke 5 000 EPS et envoie 5000 EPS à chacun des nœuds de données connectés. Le processeur d'événements traite toujours tous les événements, mais les nœuds de données fournissent davantage de capacités de stockage, d'indexation et de recherche pour améliorer les performances globales.

## Comment rééquilibrer le travail ?

Les membres de cluster se composent d'un processeur d'événements et d'un ou plusieurs nœuds de données. Les données peuvent se déplacer entre les membres du cluster dans n'importe quelle direction. Les données se déplacent entre les membres du cluster de manière transactionnelle par des dossiers horaires. Une heure de données est le plus petit bloc de données qui se déplace. Si un fichier d'un dossier horaire n'est pas copié, la totalité de la transaction est annulée.

Le rééquilibrage ne fusionne pas les dossiers horaires. Par exemple, si un dossier horaire existe sur la destination, le rééquilibrage ne déplace pas les données du même dossier horaire des autres membres du cluster. Avant le rééquilibrage, le cluster détermine sa cible. La cible est le pourcentage d'espace libre que le rééquilibrage tente d'atteindre sur tous les membres du cluster. La cible ne tient pas compte de l'espace libre absolu en gigaoctets, elle ne tient compte que du pourcentage.

Les membres qui ont un pourcentage plus élevé d'espace libre sont des cibles. Une fois que le cluster a déterminé sa cible, les membres dont le pourcentage d'espace libre est inférieur à la cible deviennent des sources. Chaque source se connecte et envoie des données à chaque destination. Certains composants de votre déploiement QRadar peuvent redémarrer et provoquer l'échec du processus de rééquilibrage. Le rééquilibrage se redémarre et se poursuit d'où il n'a pas abouti. Lorsque le rééquilibrage redémarre, il le fait avec un délai d'attente croissant (5 minutes, 10 minutes, 30 minutes, etc.) pour éviter un trop grand nombre de tentatives ayant échoué lors du déploiement complet ou de la maintenance. Rééquilibrage total entre les processus Ariel sur les membres du cluster.

## Comment fonctionne la diffusion ?

La diffusion distribue les données entrantes du processeur d'événements parmi tous les membres du cluster. La diffusion fonctionne avec des événements et des flux et n'est pas liée au plus petit bloc horaire. Par exemple, une heure d'événements est diffusée sur tous les clusters dans le même dossier horaire.

La diffusion distribue des événements et s'écoule proportionnellement à la quantité d'espace disponible en pourcentage sur le membre du cluster. Le traitement des données déplace les données séquentiellement vers les hôtes de cluster en mode round-robin en fonction du pourcentage d'espace libre.

En cas d'erreurs ou de problèmes de connectivité, la diffusion tente de déplacer les données vers le membre suivant du cluster. Si elle échoue, elle stocke les données localement sur le processeur d'événements de sorte qu'aucune donnée ne soit perdue. Les données sont réparties entre le processus d'ecs-ep (source) et plusieurs processus de nœud de données (destinations) sur le nœud de données.

## Comment les données existantes sont-elles transférées entre le processeur d'événements (source) et le nœud de données (cible) ?

Lorsque vous ajoutez un nœud de données, QRadar calcule un espace cible. L'espace cible correspond à la quantité d'espace disponible sur le processeur d'événements, plus la quantité d'espace disponible sur les nœuds de données, divisée par la quantité totale de processeurs d'événements et de nœuds de données. Par exemple, vous disposez d'un processeur d'événements et de deux nœuds de données. Si le processeur d'événements dispose de 60% d'espace libre et que les deux nœuds de données ont 100 % d'espace libre, l'espace cible est de 86,6 % ( $60 + 100 + 100 / 3$ ). Lorsque la cible est définie, les données sont déplacées dans des blocs d'une heure à la fois, jusqu'à ce que l'espace cible soit atteint (86,6 % dans cet exemple) sur tous les hôtes de cluster.

## Comment les nouvelles données sont-elles transférées entre le processeur d'événements (source) et le nœud de données (cible) ?

Lorsque l'équilibrage initial est terminé, QRadar diffuse de nouvelles données sur les processeurs d'événements et les nœuds de données, en fonction de la quantité d'espace disponible. Par exemple, si un processeur d'événements dispose d'un espace libre de 25 % et qu'un nœud de données dispose de 40 % d'espace libre, le nœud de données reçoit 40 événements, tandis que le PE reçoit 25 événements jusqu'à ce que les deux dispositifs aient approximativement la même quantité d'espace disponible.

## Quand l'équilibrage est-il terminé ?


Le processus d'équilibrage est terminé lorsque toutes les données source sont traitées ou lorsque les contraintes d'espace cible sont atteintes.

## Affichage de la progression du rééquilibrage des données

Lorsque vous ajoutez un nœud de données, IBM QRadar redistribue automatiquement les données pour l'équilibrer sur les volumes de stockage de votre déploiement.

Les améliorations de performances de recherche ne sont réalisées qu'une fois le rééquilibrage des données terminé. Vous pouvez afficher la progression du rééquilibrage des données, ainsi que des données telles que le pourcentage d'espace disque utilisé.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Dans le tableau hôte, sélectionnez l'hôte géré sur lequel vous souhaitez afficher des informations supplémentaires.
  - Pour afficher des informations sur le cluster d'hôtes gérés, sélectionnez l'hôte de niveau supérieur.
  - Pour afficher des informations sur un nœud de données spécifique, sélectionnez le nœud de données.
5. Dans le menu **Actions**, cliquez sur **Afficher et gérer le système**.
6. Cliquez sur l'onglet **Distribution des données de sécurité** pour afficher la progression du rééquilibrage des données et la capacité du dispositif Noeud de données.



**Remarque :** Vous pouvez également afficher des informations sur la progression du rééquilibrage des noeuds de données dans la barre d'état de déploiement de l'onglet **Admin**.

## Sauvegarde de toutes les données d'événement sur un dispositif Noeud de données

Pour améliorer les performances d'un processeur d'événements, configurez IBM QRadar pour enregistrer toutes les données d'événement sur un dispositif Noeud de données. Avec cette configuration, le processeur d'événements traite uniquement les événements ; il ne stocke pas les données d'événement localement.

Un processeur d'événements configuré pour uniquement les événements de processus enregistre toujours des données d'événement localement lorsqu'aucun appareil Noeud de données actif n'est disponible. Lorsqu'un dispositif Noeud de données devient disponible, QRadar transfère le plus de données possible du processeur d'événements vers Noeud de données.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez processeur d'événements dans la table hôte et dans le menu **Actions de déploiement**, cliquez sur **Éditer l'hôte**.
5. Cliquez sur l'icône des paramètres **Gestion des composants** () .
6. Sous **Processeur d'événements**, dans la zone **Mode du processeur d'événement**, sélectionnez **Traitement-Uniquement**.

7. Cliquez sur **Sauvegarder**, puis sur **Sauvegarder** à nouveau.
8. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.



## Archivage du contenu Noeud de données

Configurez un dispositif Noeud de données pour utiliser le mode **Archive** quand vous voulez que le Noeud de données fournisse un accès en ligne aux données historiques sans affecter le stockage pour les données entrantes.

En mode **Archiver**, le dispositif ne reçoit pas de nouvelles données, mais les données existantes sont sauvegardées.

**Important** : Aucune politique de conservation des événements n'est appliquée sur le dispositif Noeud de données en mode **Archiver**.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez le dispositif Noeud de données dans le tableau hôte et, dans le menu **Actions de déploiement**, cliquez sur **Éditer l'hôte**.
5. Cliquez sur l'icône des paramètres **Gestion des composants** ().
6. Dans la zone **Mode noeud de données**, sélectionnez **Archiver**, puis cliquez sur **Sauvegarder**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

### Que faire ensuite

Pour reprendre le stockage des données sur le dispositif Noeud de données, redéfinissez le mode sur **Actif**.

## Gestion de l'interface réseau

---

En plus de l'interface de gestion par défaut, vous pouvez ajouter des interfaces réseau supplémentaires à vos dispositifs IBM QRadar pour fournir une connectivité réseau alternative.

Utilisez des interfaces réseau supplémentaires aux fins suivantes :

- Fournissez une connexion croisée dédiée entre homologues à haute disponibilité (HA). Vous configurez une connexion croisée lors de la configuration à haute disponibilité.
- Fournissez une interface de collecte de données dédiée pour les événements entrants ou les sources de flux externes. Les sources de données TCP doivent se trouver dans le même sous-réseau que l'interface de collecte de données.
- Augmentez la bande passante et ajoutez la tolérance aux pannes par des interfaces de liaison.

Utilisez une carte d'interface réseau régulière pour :

- Collecte de données (logs/flows (flux NetFlow/s))
- Interface utilisateur Web
- Sauvegarde / restauration (non limitée à iSCSI mais peut être NFS)

**Remarque** : Les configurations WinCollect connectées à un port non géré ne sont pas prises en charge.

## Configuration des interfaces réseau

Utilisez des liaisons pour accroître la bande passante disponible ou la tolérance aux pannes de vos dispositifs IBM QRadar en associant au moins 2 interfaces réseau dans un canal unique.


## Avant de commencer

**Remarque :** L'interface de gestion du réseau QRadar, y compris les options de liaison, sont configurées uniquement à l'invite shell UNIX lors de l'installation et de la configuration.

Configurez l'interface de gestion sur une console QRadar Console avant d'ajouter un hôte géré. Pour plus de détails sur la configuration de l'interface de gestion, voir "Configuring bonded management interfaces" dans le manuel *IBM QRadar - Guide d'installation*.

Vous ne pouvez pas lier une interface esclave existante. Vous ne pouvez lier des interfaces de gestion que depuis une invite shell. Vous pouvez lier des croisements depuis l'écran de configuration **Haute disponibilité**.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans le menu **Afficher**, cliquez sur **Systèmes**.
4. Sélectionnez l'hôte pour lequel vous désirez configurer des interfaces réseau.
5. Cliquez sur **Actions** > **Afficher et gérer le système**, puis sur l'onglet **Interfaces réseau**.
6. Pour éditer une interface réseau, procédez comme suit :
  - a) Sélectionnez le dispositif que vous souhaitez éditer, puis cliquez sur **Editer**.
  - b) Dans la liste **Rôle**, sélectionnez le rôle du dispositif :
    - Choisissez **Régulier** lorsque l'unité est utilisée pour :
      - Collecte de données (logs/flows (flux NetFlow/s))
      - Interface utilisateur Web
      - Sauvegarde / restauration (non limitée à iSCSI mais peut être NFS)Cette interface doit disposer d'une adresse IP. Le sous-réseau de l'interface ne peut pas être le même sous-réseau utilisé par l'interface de gestion.
    - Choisissez **Moniteur** si le dispositif est un collecteur IBM QRadar QFlow Collector utilisé pour la collecte de paquets. Cette interface ne requiert pas une adresse IP.
    - Choisissez **Désactivé** si vous voulez éviter que le dispositif soit utilisé pour une connexion réseau.
  - c) Pour appliquer la configuration au noeud haute disponibilité actif, cliquez sur **Appliquer cette configuration d'interface et cette adresse IP au noeud haute disponibilités actif**.
  - d) Cliquez sur **Sauvegarder**.
7. Pour créer une interface réseau liée, procédez comme suit :

Vous pouvez lier au moins deux interfaces ayant un rôle standard ou moniteur. Vous ne pouvez lier que des interfaces affectées au même rôle.

  - a) Sélectionnez le dispositif et cliquez sur **Lié**.
  - b) Entrez l'adresse IP et de masque de réseau.
  - c) Pour appliquer la configuration au noeud haute disponibilité actif, cliquez sur **Appliquer cette configuration d'interface et cette adresse IP au noeud haute disponibilités actif**.

**Remarque :** En sélectionnant cette option, vous maintenez l'interface active sur le noeud haute disponibilité actif entre les deux. Vous pouvez utiliser cette option sur une interface qui est utilisée pour recevoir des données entrantes, comme les messages syslog ou les enregistrements de données netflow. Cette option fait migrer les données entre le noeud principal et le noeud secondaire (selon celui qui est actif).
  - d) Entrez une option de liaison. L'option de liaison par défaut qui est configurée sur cette interface est mode=4.

**Remarque :**

Les interfaces liées prennent en charge divers modes d'opération, en fonction des capacités du commutateur auquel elles sont connectées. Le tableau suivant décrit les modes de liaison pris en charge que vous pouvez utiliser.

Modes de liaison	Nom de la liaison	Description
mode=1	Sauvegarde active	Un seul esclave est actif. Un autre esclave devient actif lorsque celui-ci échoue.
mode=4	802.3ad	Utilise le protocole LACP (Link Aggregation Control Protocol) pour créer des groupes d'agrégation partageant les paramètres de duplex et de vitesse.

Pour plus d'informations sur la configuration d'options de liaison spécifiques, consultez la documentation du système d'exploitation spécifique au fournisseur.

- e) Cliquez sur **Ajouter** et sélectionnez l'interface que vous voulez ajouter en tant qu'esclave, puis cliquez sur **OK**.
  - f) Cliquez sur **Sauvegarder** pour créer votre interface liée.
8. Pour fractionner une interface liée en plusieurs interfaces simples, sélectionnez le dispositif lié, puis cliquez sur **Non lié**.

## Que faire ensuite

Si la connexion ne fonctionne pas lorsque vous configurez vos paramètres d'interface de stockage, utilisez SSH pour vous connecter à l'hôte et recherchez dans le fichier journal `/var/log/message` des erreurs d'interface réseau.

Vous pouvez également essayer de définir le paramètre sur `mode=1` ou vous pouvez déconnecter physiquement toutes les connexions Ethernet sauf une dans le groupe d'interface liée. Si cette solution fonctionne, vérifiez que votre infrastructure de commutateur prend en charge le mode que vous tentez d'utiliser. Les commutateurs ne prennent pas toujours en charge `mode=4`.

## Temps système QRadar

Lorsque votre déploiement s'étend sur plusieurs fuseaux horaires, configurez tous les dispositifs pour qu'ils utilisent le même fuseau horaire que la console IBM QRadar. Vous pouvez également configurer tous les dispositifs pour utiliser l'heure GMT (Greenwich Mean Time).

Configurez l'heure du système IBM QRadar depuis l'interface utilisateur QRadar. Vous pouvez configurer l'heure manuellement ou en configurant les serveurs NTP (Network Time Protocol) pour conserver l'heure système.

L'heure est automatiquement synchronisée entre le QRadar Console et les hôtes gérés.

### Incidents causés par des fuseaux horaires mal appariés

Pour vous assurer que les recherches et les fonctions liées aux données fonctionnent correctement, tous les dispositifs doivent synchroniser les paramètres de temps avec le dispositif QRadar Console. Lorsque les paramètres de fuseau horaire sont incohérents, vous pouvez voir des résultats incohérents entre les recherches QRadar et les données de rapport.

Le service Accumulateur s'exécute sur tous les dispositifs dotés d'une mémoire locale pour créer des accumulations minute par minute ainsi que des cumuls horaires et quotidiens. QRadar utilise les données cumulées dans les rapports et les graphiques de série temporelle. Lorsque les fuseaux horaires sont mal appariés dans un déploiement distribué, les graphiques de rapports et de séries temporelles peuvent afficher des résultats incohérents par rapport aux résultats de la requête AQL en raison de la manière dont les données cumulées sont agrégées.



Les recherches QRadar s'exécutent sur des données stockées dans les bases de données Ariel, qui utilisent une structure de date (AAAA/MM/JJ/MM/HH/MM) pour stocker les fichiers sur le disque. La modification du fuseau horaire après l'écriture des données sur le disque perturbe la séquence de nommage des fichiers dans les bases de données Ariel et peut entraîner des problèmes d'intégrité des données.

### Concepts associés


#### Authentification de l'utilisateur

Lorsque l'authentification est configurée et qu'un utilisateur entre un nom d'utilisateur et un mot de passe non valides, un message s'affiche pour indiquer que la connexion n'est pas valide.

## Configuration de l'heure système

Configurez l'heure système sur votre QRadar Console en la définissant manuellement ou en utilisant des serveurs NTP pour la gérer. QRadar synchronise l'heure QRadar Console avec les hôtes gérés de votre déploiement.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez l'hôte pour lequel vous souhaitez configurer les paramètres d'heure système.
5. Dans le menu **Actions**, cliquez sur **Afficher et gérer le système**.
6. Cliquez sur l'onglet **Heure système**.
7. Pour configurer l'heure sur la QRadar Console, procédez comme suit :
  - a) Dans la liste **Fuseau horaire**, sélectionnez le fuseau horaire qui s'applique à la QRadar Console.
  - b) Pour configurer manuellement l'heure, cliquez sur **Définir l'heure manuellement** : puis définissez la date et l'heure de la console.

**Remarque** : Si vous définissez l'heure système en indiquant une date à venir concernée par le changement d'heure d'été, l'heure définie est ajustée d'une heure. Par exemple, le 4 juillet 2016 aux Etats-Unis, vous définissez la date du 16 décembre 2016 et l'heure 20:00. L'heure définie ignore le changement d'heure d'été et est modifiée en 19:00.
  - c) Pour gérer l'heure en utilisant des serveurs NTP, procédez comme suit :
    - i) Cliquez sur **Définir les serveurs NTP** puis sur **Ajouter plus**.
    - ii) Dans la zone **Adresse du serveur 1**, entrez une adresse IP ou un nom d'hôte pour le serveur NTP. Les noms d'hôte sont résolus par un serveur DNS.
8. Pour configurer l'heure sur un hôte géré, dans la liste **Fuseau horaire**, sélectionnez le fuseau horaire qui s'applique à l'hôte.

Sur un hôte géré, vous ne pouvez configurer que le fuseau horaire. L'heure système est synchronisée avec QRadar Console, mais si l'hôte géré est dans un autre fuseau horaire, vous pouvez choisir celui-ci.
9. Cliquez sur **Sauvegarder**.
10. Cliquez sur **OK** pour accepter le redémarrage des services, ou sur **Annuler** pour annuler les modifications.

La collecte de données pour les événements et les flux s'arrête jusqu'à ce que les services `hostcontext` et `tomcat` soient redémarrés.

### Que faire ensuite

L'heure définie sur un système VMware peut être perdue lors du redémarrage du système. Pour empêcher toute perte de changement d'heure, vous pouvez désactiver la synchronisation d'heure sur

le périphérique virtuel en modifiant le fichier de configuration de la machine virtuelle et en ajoutant les lignes suivantes aux propriétés de synchronisation :

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

Le fichier .vmx se trouve généralement dans le répertoire dans lequel vous avez créé la machine virtuelle. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

## Réseaux NAT activé

---

La conversion d'adresses réseau (NAT) convertit une adresse IP d'un réseau en une autre adresse IP sur un autre réseau. Cette fonctionnalité fournit une sécurité accrue pour votre déploiement IBM QRadar, car les demandes sont gérées via le processus de conversion et les adresses IP internes sont masquées. Avec la conversion NAT, les ordinateurs situés sur un réseau interne privé sont convertis via un périphérique réseau, généralement un pare-feu, et peuvent communiquer avec l'Internet public sur ce réseau. Utilisez NAT pour mapper des adresses IP internes individuelles vers des adresses IP externes individuelles.

QRadar La configuration NAT nécessite une conversion d'adresses réseau statique et n'autorise qu'une seule adresse IP publique par hôte géré.

Tout hôte QRadar ne faisant pas partie du même groupe NAT que son homologue, ou appartenant à un autre groupe NAT, est configuré pour utiliser l'adresse IP publique de cet hôte pour l'atteindre. Par exemple, lorsque vous configurez une adresse IP publique sur la QRadar Console, tout hôte situé dans le même groupe NAT utilise l'adresse IP privée de la QRadar Console pour communiquer. Tout hôte géré situé dans un autre groupe NAT utilise l'adresse IP publique de la QRadar Console pour communiquer.

Si vous disposez d'un hôte dans l'un de ces emplacements de groupe NAT qui ne nécessite pas de conversion externe, entrez l'adresse IP privée dans les zones **Private IP** et **Public IP**. Les systèmes situés dans des emplacements distants avec un groupe NAT différent de celui de la console nécessitent toujours une adresse IP externe et une conversion NAT car ils doivent pouvoir établir des connexions avec la console. Seuls les hôtes situés dans le même groupe NAT que la console peuvent utiliser les mêmes adresses IP publiques et privées.

## Configuration d'un groupe NAT

Configurez un groupe NAT (Network Address Translation) pour limiter le nombre d'adresses IP publiques requises par vos hôtes gérés IBM QRadar pour communiquer avec Internet.

### Avant de commencer


Vérifiez que le réseau NAT activé utilise la conversion NAT statique.


### Pourquoi et quand exécuter cette tâche

Il est important de terminer la configuration NAT pour chaque hôte géré de votre déploiement avant de déployer les modifications. Après le déploiement, les hôtes gérés qui ne sont pas NAT activé risquent de ne pas pouvoir communiquer avec QRadar Console.

QRadar peut prendre en charge plusieurs réseaux NAT lorsque l'adresse IP publique de QRadar Console est la même dans chaque réseau.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.

3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Pour configurer un groupe NAT pour QRadar Console, procédez comme suit :
  - a) Sélectionnez le dispositif QRadar Console dans la table hôte.
  - b) Dans le menu **Actions de déploiement**, cliquez sur **Editer l'hôte**.
  - c) Cochez la case **Traduction d'adresse réseau**.
  - d) Dans la liste **Groupe NAT**, sélectionnez le groupe NAT auquel appartient la console ou cliquez sur l'icône de paramètres () pour créer un nouveau groupe NAT.
  - e) Dans la zone **IP publique**, entrez l'adresse IP publique de la console, puis cliquez sur **Sauvegarder**.
5. Configurez chaque hôte géré sur le même réseau pour utiliser le même groupe NAT que QRadar Console.
  - a) Sélectionnez le dispositif hôte géré dans le tableau hôte.
  - b) Dans le menu **Actions de déploiement**, cliquez sur **Editer l'hôte**.
  - c) Cochez la case **Traduction d'adresse réseau**.
  - d) Dans la liste **Groupe NAT**, sélectionnez le groupe NAT auquel appartient le QRadar Console.
  - e) Dans la zone **IP public**, entrez l'adresse IP publique de l'hôte géré.

**Remarque :** À moins qu'un collecteur d'événements ne se connecte à un hôte géré qui utilise NAT, configurez l'hôte géré pour qu'il utilise la même adresse IP publique et l'adresse IP privée.
  - f) Cliquez sur **Sauvegarder**.
6. Sous l'onglet **Admin**, sélectionnez **Avancé > Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Que faire ensuite

Pour résoudre les problèmes de communication entre QRadar Console et les hôtes qui ne sont pas NAT activé après le déploiement, éditez les règles iptables pour l'hôte géré afin de configurer le pare-feu local afin de permettre à QRadar Console d'accéder à l'hôte géré.

## Modification du statut NAT pour un hôte géré

Configurez un hôte géré pour qu'il utilise la conversion d'adresses réseau (NAT) pour qu'il puisse communiquer avec le QRadar Console et les autres hôtes gérés du même réseau.


### Avant de commencer

Vérifiez que le réseau NAT activé utilise la conversion NAT statique.

Le QRadar Console et tous les hôtes gérés du même réseau doivent être membres du même groupe NAT.

Pour modifier l'état NAT d'un hôte géré, veillez à mettre à jour la configuration de l'hôte géré dans IBM QRadar avant de mettre à jour l'unité. La mise à jour de la configuration empêche l'hôte de devenir inaccessible et garantit que vous pouvez continuer à déployer des modifications sur cet hôte.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur l'icône **Gestion des systèmes et des licences**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez l'hôte dans la table d'hôtes et dans le menu **Actions de déploiement**, cliquez sur **Editer l'hôte**.

5. Pour désactiver la conversion NAT, désélectionnez la case à cocher **Traduction d'adresse réseau**.
6. Pour activer NAT, procédez comme suit :
  - a) Cochez la case **Traduction d'adresse réseau**.
  - b) Dans la liste **Groupe NAT**, sélectionnez le groupe auquel appartient l'hôte géré.
  - c) Dans la zone **IP publique**, entrez l'adresse IP publique que l'hôte géré utilise pour communiquer avec d'autres hôtes dans un autre groupe NAT.
7. Cliquez sur **Sauvegarder**.
8. Sous l'onglet **Admin**, sélectionnez **Avancé > Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Que faire ensuite

Si vous avez activé NAT, vous devrez peut-être mettre à jour la configuration du pare-feu pour l'hôte géré avec lequel vous souhaitez communiquer. Pour plus d'informations, voir [«Configuration de votre pare-feu local»](#), à la page 80.

## Gestion des hôtes hors site

---

Un hôte hors site est un dispositif QRadar qui ne peut pas être accédé via QRadar Console dans votre déploiement actuel. Vous pouvez configurer un hôte hors site pour transférer des données vers ou pour recevoir des données à partir de votre déploiement QRadar.


## Configuration d'une source hors site

Pour transférer des données d'événement et de flux vers un Collecteur d'événements dans un autre déploiement, configurez le déploiement cible afin d'inclure une source externe de sorte qu'il sache quel ordinateur envoie les données.

### Pourquoi et quand exécuter cette tâche

Pour éviter les erreurs de connexion, lorsque vous configurez des composants source et cible hors site, déployez d'abord la console IBM QRadar avec la source externe. Déployez ensuite le fichier QRadar Console avec la cible hors site.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Dans le menu **Actions de déploiement**, cliquez sur **Gérer les sources hors site**.
5. Cliquez sur **Ajouter** et configurez les paramètres.

Le nom peut comporter jusqu'à 20 caractères et peut inclure des traits de soulignement ou des traits d'union.

6. Cliquez sur **Sauvegarder**.
7. Cliquez sur **Gérer les connexions** pour indiquer quels hôtes QRadar vous souhaitez recevoir les données.

L'hôte doit disposer d'un Collecteur d'événements pour recevoir les données.

8. Répétez les étapes pour configurer toutes les sources hors site que vous souhaitez configurer.
9. Déployez les modifications et redémarrez le service de collecte d'événements.


## Configuration d'une cible hors site

Pour transférer des données d'événement et de flux vers une Collecteur d'événements dans un autre déploiement, configurez le déploiement source de sorte qu'il inclut une cible hors site de sorte qu'il sache à quel ordinateur envoyer les données.

### Avant de commencer

Vous devez connaître les ports d'écoute du dispositif cible hors site. Par défaut, le port d'écoute des événements est 32004 et 32000 pour les flux.


Pour rechercher le port d'écoute sur le dispositif cible, procédez comme suit :

1. Dans le déploiement cible, cliquez sur l'icône **Gestion des systèmes et des licences**.
2. Sélectionnez l'hôte et cliquez sur **Actions de déploiement > Éditer l'hôte**.
3. Cliquez sur l'icône des paramètres **Gestion des composants**  et recherchez les ports dans les zones **Port d'écoute du transfert d'événement** et **Port d'écoute de transfert de flux**.

### Pourquoi et quand exécuter cette tâche

Pour éviter les erreurs de connexion, lorsque vous configurez des composants source et cible hors site, déployez d'abord la console IBM QRadar avec la source externe. Déployez ensuite le fichier QRadar Console avec la cible hors site.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Dans le menu **Actions de déploiement**, cliquez sur **Gérer les cibles hors site**.
5. Cliquez sur **Ajouter** et configurez les paramètres.

Le nom peut comporter jusqu'à 20 caractères et peut inclure des traits de soulignement ou des traits d'union. Le port par défaut pour l'écoute des événements est 32004 et 32000 pour les flux.

**Remarque :** Si la cible hors site est un hôte géré avec des connexions hôte chiffrées vers sa console, le port 22 pour SSH s'ouvre, quel que soit le port sélectionné dans l'interface utilisateur.

6. Cliquez sur **Sauvegarder**.
7. Cliquez sur **Gérer les connexions** pour indiquer quels hôtes QRadar vous souhaitez recevoir les données.

Seuls les hôtes ayant un Collecteur d'événements sont affichés dans la liste.

8. Répétez les étapes pour configurer toutes les cibles hors site que vous souhaitez configurer.
9. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Génération de clés publiques pour les produits QRadar

Pour transférer des événements normalisés dans IBM QRadar, vous devez copier le fichier de clés publiques, `/root/.ssh/id_rsa.pub`, de la source externe vers la cible hors site.

Si la source externe et la cible hors site se trouvent sur des systèmes distincts, la clé publique est générée automatiquement. Si la source et la cible hors site sont toutes deux sur un système tout-en-un, la clé publique n'est pas générée automatiquement. Vous devez générer manuellement la clé publique.

### Procédure

Pour générer manuellement la clé publique, procédez comme suit :

1. Utilisez SSH pour vous connecter à votre système comme utilisateur root.

2. Pour générer la clé publique, entrez la commande suivante :

```
opt/qradar/bin/ssh-key-generating
```


3. Appuyez sur la touche Entrée.

La paire de clés publiques et privées est générée et enregistrée dans le dossier `/root/.ssh/id_rsa`.

## Transfert de flux filtrés

Vous pouvez configurer la transmission des flux filtrés. Vous pouvez utiliser des flux filtrés pour fractionner le transfert de flux sur plusieurs boîtes et pour acheminer des flux spécifiques pour des investigations spécifiques.

### Procédure

1. Sur le système cible, définissez le système source comme source externe.
  - a) Dans le menu de navigation () , cliquez sur **Admin**.
  - b) Cliquez sur **Gestion des systèmes et des licences > Actions de déploiement > Gérer les sources hors site**.
  - c) Ajoutez l'adresse IP du système source et sélectionnez **Recevoir les événements** et/ou **Flux de réception**.
  - d) Sélectionnez **Gérer les connexions** et sélectionnez l'hôte qui s'attend à recevoir la connexion hors site.
  - e) Cliquez sur **Sauvegarder**.
  - f) Sélectionnez **Déployer la configuration complète** dans le menu **Avancé** pour que les modifications prennent effet.
2. Sur le système source, définissez la destination de transfert, l'adresse IP et le numéro de port.
  - a) Cliquez sur **Menu principal > Admin**.
  - b) Cliquez sur **Transfert de destinations > Ajouter**.
  - c) Définissez l'adresse IP du système cible et du port de destination.
  - d) Entrez 32000 pour le numéro de port sur le système source. Le port 32000 est utilisé pour le transfert de flux.
  - e) Sélectionnez **Normalisé** dans la liste **Format d'événement**.
3. Configurez les règles de routage.
  - a) Cliquez sur **Menu principal > Admin**.
  - b) Cliquez sur **Règles de routage > Ajouter**.
  - c) Sélectionnez le flux que vous souhaitez éditer.

**Remarque :** Les règles transmettent des flux qui sont basés sur des violations ou basés sur des informations CRE lorsque **Transfert hors ligne** est sélectionné dans la page Règles de routage.

Les flux filtrés sur l'écran **Règles de routage** sont transmis.

## Exemple : transmission d'événements et de flux normalisés

Pour transférer des événements et des flux normalisés, configurez le déploiement cible afin d'inclure une source externe de sorte qu'il sache quel ordinateur envoie les données. Configurez le déploiement source pour inclure une cible hors site de sorte qu'il sache à quel ordinateur envoyer les données.

### Pourquoi et quand exécuter cette tâche

Le diagramme suivant illustre le transfert des données d'événement et de flux entre les déploiements.

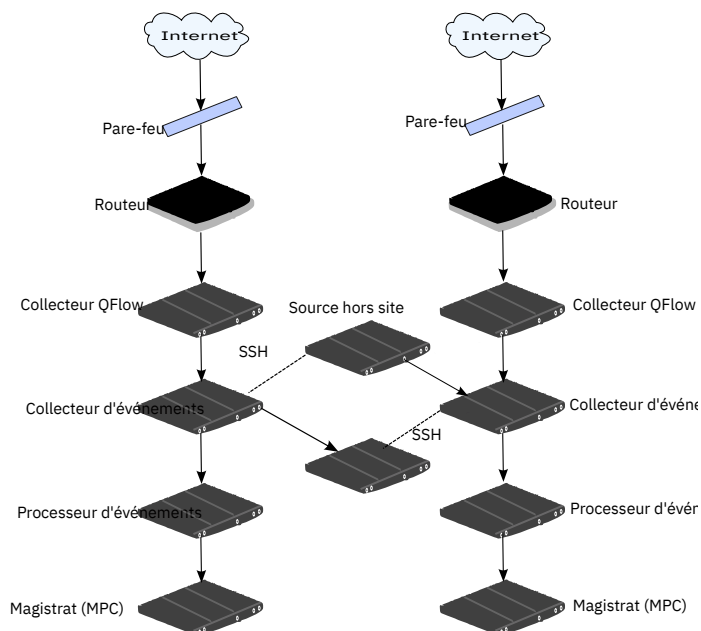


Figure 6. Transfert de données entre les déploiements à l'aide de SSH

Si la source ou la cible hors site est un système tout-en-un, la clé publique n'est pas générée automatiquement ; par conséquent, vous devez générer manuellement la clé publique. Pour plus d'informations, voir «Génération de clés publiques pour les produits QRadar», à la page 71.

## Procédure

Pour transférer des événements et des flux normalisés depuis le déploiement A vers le déploiement B :

1. Configurez une cible hors site dans le déploiement A.

La configuration cible hors site inclut l'adresse IP de Collecteur d'événements dans le déploiement B qui reçoit les données.

2. Configurez une source hors site dans le déploiement B.

La configuration source hors site inclut l'adresse IP et le numéro de port de Collecteur d'événements dans le déploiement A qui envoie les données.

3. Pour transférer des données chiffrées, vous devez activer le chiffrement à la fois sur la source externe et sur la cible hors site.

Pour garantir un accès approprié, la clé publique SSH du système source (déploiement A) doit être disponible pour le système cible (déploiement B). Par exemple, pour activer le chiffrement entre le déploiement A et le déploiement B, procédez comme suit :

4. Créez des clés ssh à l'aide de la commande **ssh-keygen -1 -t rsa** et appuyez sur Entrée lorsque vous êtes invité à indiquer le répertoire et le mot de passe composé.

Par défaut, le fichier `id_rsa.pub` est stocké dans le répertoire `/root/.ssh`.

5. Copiez le fichier `id_rsa.pub` dans le répertoire `/root/.ssh` sur Collecteur d'événements et sur QRadar Console dans le système source (déploiement A).

6. Renommez le fichier en `authorized_keys`.

Vérifiez que le système source est configuré avec les droits appropriés pour envoyer des données d'événement et de flux au système cible.

7. Si vous n'avez pas utilisé la commande **chmod 600 authorized\_key** pour affecter des privilèges de propriétaire `rw` au fichier et au répertoire parent, utilisez la commande **ssh-copy-id** avec le paramètre `-i` pour indiquer que le fichier d'identité `/root/.ssh/id_rsa.pub` doit être utilisé.

Par exemple, entrez la commande suivante pour ajouter des entrées ou créer un fichier `authorized_keys` sur la console cible avec les droits appropriés. Cette commande ne vérifie pas les entrées en double.

```
ssh-copy-id -i root@10.100.133.80
```

8. Configurez le système source pour vous assurer que la transmission des événements et des flux n'est pas interrompue par d'autres activités de configuration, telles que l'ajout d'un hôte géré à l'une des consoles.

Par exemple, si un hôte géré est ajouté à une console qui envoie des événements, un fichier `authorized_keys` doit exister dans le répertoire `/root/.ssh` sur l'hôte géré. Si ce n'est pas le cas, l'ajout d'un hôte géré échoue. Ce fichier est obligatoire, que le chiffrement soit utilisé entre l'hôte géré et la console.

9. Sous QRadar Console dans le système source (déploiement A), créez un fichier `ssh_keys_created` sous `/opt/qradar/conf`.
10. Remplacez le propriétaire et le groupe par **Personne** et le droit **775** pour vous assurer que le fichier peut être sauvegardé et restauré correctement.

```
chown nobody:nobody /opt/qradar/conf/ssh_keys_created
chmod 775 /opt/qradar/conf/ssh_keys_created
```

11. Pour éviter les erreurs de connexion, déployez les modifications dans le système cible (déploiement B) avant de déployer les modifications dans le système source (déploiement A).

## Que faire ensuite

Si vous mettez à jour la configuration Collecteur d'événements ou les ports de surveillance, vous devez mettre à jour manuellement la configuration de la source externe et de la cible hors site pour maintenir la connexion entre les deux déploiements.

Si vous souhaitez déconnecter le système source (déploiement A), vous devez supprimer les connexions des deux déploiements. Supprimez la cible hors site du système source (déploiement A), puis supprimez la source hors site du système cible (déploiement B).

## Hôtes gérés

---

Pour plus de flexibilité sur la collecte de données et le traitement des événements et des flux, générer un déploiement IBM QRadar réparti en ajoutant des hôtes gérés sans console, tels que des collecteurs, des processeurs et des nœuds de données.

Pour plus d'informations sur la planification et la génération de votre environnement QRadar, voir le *IBM QRadar - Guide d'architecture et de déploiement*.

### Compatibilité logicielle requise

Les versions logicielles de tous les dispositifs QRadar de votre déploiement doivent être au même niveau de version et de groupe de correctifs. Les déploiements qui utilisent des versions différentes de logiciels ne sont pas pris en charge car les environnements logiciels mixtes peuvent empêcher les règles de tirer, empêcher la création ou la mise à jour des violations ou provoquer des erreurs dans les résultats de la recherche.

Lorsqu'un hôte géré utilise une version de logiciel différente de la console QRadar, il se peut que vous puissiez afficher les composants qui ont déjà été affectés à l'hôte, mais vous ne pouvez pas configurer le composant, ni ajouter ou affecter de nouveaux composants.

### Configuration requise pour le protocole Internet (IP)

Le tableau suivant décrit les différentes combinaisons de protocoles IP qui sont prises en charge lorsque vous ajoutez des hôtes gérés sans console.



Tableau 12. Combinaisons de protocoles IP prises en charge sur des hôtes gérés sans console

Hôtes gérés	Console QRadar (IPv6, unique)	Console QRadar (IPv6, HA)	Console QRadar (pile en double, simple)	Console QRadar (pile-à-pile, HA)
IPv4, unique	Non	Non	Oui*	Non
IPv4, HA	Non	Non	Non	Non
IPv6, unique	Oui	Oui	Oui	Non
IPv6, HA	Oui	Oui	Oui	Non

**Restriction :** \*Par défaut, vous ne pouvez pas ajouter un hôte géré IPv4-only à une console à deux piles. Vous devez exécuter un script pour activer un hôte géré IPv4 uniquement. Pour plus d'informations, voir [Ajout d'un hôte géré IPv4-only dans un environnement à deux piles](#).

Une console à deux piles prend en charge IPv4 et IPv6. La liste suivante décrit les conditions que vous devez respecter dans les environnements à deux piles :

- Vous pouvez ajouter des hôtes gérés IPv6 à une console à deux piles ou à une console IPv6-only.
- Vous pouvez ajouter uniquement des hôtes gérés IPv4 à une console à deux piles.
- N'ajoutez pas d'hôte géré à une console à deux piles configurée pour HA.
- N'ajoutez pas d'hôte géré IPv4 qui ne se trouve pas dans une paire de haute disponibilité sur une console IPv6-only ou sur une console à deux piles qui se trouve dans une paire à haute disponibilité.

**Important :** IBM ne prend pas en charge les configurations suivantes :

- Ajout d'un hôte géré à une console à deux piles configurée pour l'HA
- Ajout d'un hôte géré IPv4 qui ne se trouve pas dans une paire de haute disponibilité sur une console IPv6-only
- Ajout d'un hôte géré IPv4 qui n'est pas dans une paire à haute disponibilité vers une console à deux piles qui se trouve dans une paire à haute disponibilité

## Remarques sur la largeur de bande pour les hôtes gérés

Pour pouvoir répliquer les données d'état et de configuration, vérifiez que vous disposez au minimum d'une bande passante de 100 Mbits/s entre la console IBM QRadar et tous les hôtes gérés. Une bande passante plus large est requise si vous devez effectuer des recherches dans les journaux et l'activité réseau et que votre nombre d'événements par seconde (EPS) dépasse 10000 événements.

Un collecteur Collecteur d'événements configuré pour stocker les données et les transmettre à un processeur d'événements lance la transmission en fonction du planning que vous avez défini. Vérifiez que vous disposez d'une largeur de bande suffisante pour la quantité de données collectée, pour permettre au dispositif de respecter le rythme planifié.

Utilisez les méthodes suivantes pour réduire les limitations liées à la bande passante entre les centres de données :

### Traitez et envoyez les données aux hôtes du centre de données principal.

Concevez votre déploiement de manière à traiter et à envoyer les données au fur et à mesure de leur collecte aux hôtes du centre de données principal sur lequel réside la console. De la sorte, toutes les demandes de recherche de l'utilisateur interrogent les données sur le centre de données local au lieu d'attendre leur réacheminement depuis des sites distants.

Vous pouvez déployer un collecteur d'événements de stockage et de réacheminement, tel qu'un dispositif QRadar 15XX physique ou virtuel, sur les emplacements distants pour contrôler les pics de données au sein du réseau. La bande de données est utilisée sur les emplacements distants et recherche des données produites dans le centre de données principal, et non pas à un emplacement distant.

## **N'effectuez pas de recherches impliquant de grands volumes de données sur des connexions à bande passante limitée**

Empêchez les utilisateurs d'effectuer des recherches impliquant des grands volumes de données sur des liens dont la bande passante est limitée. La définition de filtres détaillés sur les recherches limite la quantité de données extraites des emplacements distants, et la bande passante nécessaire pour renvoyer les résultats.

## **Chiffrement**

Pour assurer un transfert de données sécurisé entre chacun des dispositifs de votre environnement, IBM QRadar dispose d'un support de chiffrement intégré qui utilise OpenSSH. Le chiffrement se produit entre les hôtes gérés ; par conséquent, vous devez avoir au moins un hôte géré avant de pouvoir activer le chiffrement.

Lorsque le chiffrement est activé, un tunnel sécurisé est créé sur le client qui lance la connexion, à l'aide d'une connexion de protocole SSH. Lorsque vous activez le chiffrement sur un hôte géré, un tunnel SSH est créé pour toutes les applications client sur l'hôte géré. Lorsque vous activez le chiffrement sur un hôte non géré par la Console, les tunnels de chiffrement sont automatiquement créés pour les bases de données et autres connexions de services de support à la Console. Pour vous assurer que toutes les données entre les hôtes gérés sont chiffrées, activez le chiffrement.

Par exemple, avec le chiffrement activé sur un processeur d'événements, la connexion entre le processeur d'événements et Collecteur d'événements est chiffrée et la connexion entre le processeur d'événements et Magistrat est chiffrée.

Le tunnel SSH entre deux hôtes gérés peut être lancé à partir de l'hôte distant à la place de l'hôte local. Par exemple, si vous disposez d'une connexion d'un environnement processeur d'événements dans un environnement sécurisé à un environnement Collecteur d'événements qui se trouve en dehors de l'environnement sécurisé et que vous disposez d'une règle de pare-feu qui vous empêcherait d'avoir un hôte en dehors de l'environnement sécurisé se connectant à un hôte dans l'environnement sécurisé, vous pouvez changer l'hôte qui crée le tunnel de sorte que la connexion soit établie à partir de processeur d'événements en sélectionnant la case à cocher **Initiation du tunnel distant** pour Collecteur d'événements.

Vous ne pouvez pas inverser les tunnels de votre console vers les hôtes gérés.

### **Tâches associées**

«Configuration d'un hôte géré», à la page 79

### **Information associée**

[QRadar : vérification de la connectivité SSH à l'hôte géré cible](#)

## **Ajout d'un hôte géré**

Ajoutez des hôtes gérés, tels que des collecteurs d'événements et de flux, des processeurs d'événements et de flux et des noeuds de données, pour répartir les activités de collecte et de traitement des données sur votre déploiement de IBM QRadar.

### **Avant de commencer**

Vérifiez que l'hôte géré est au même niveau de version et de groupe de correctifs IBM QRadar que la console QRadar Console que vous utilisez pour le gérer.

Si vous souhaitez activer la conversion d'adresses réseau statique (NAT) pour un hôte géré, le réseau doit utiliser une conversion NAT statique. Pour plus d'informations, voir «Réseaux NAT activé», à la page 68.

Activez le chiffrement de l'hôte géré pour fournir le chiffrement entre les hôtes.

### **Pourquoi et quand exécuter cette tâche**

Le tableau suivant décrit les composants que vous pouvez connecter :

Tableau 13. Connexions de composant prises en charge


Connexion source	Connexion cible	Description
QRadar QFlow Collector	Collecteur d'événements	Vous ne pouvez connecter un collecteur IBM QRadar QFlow Collector qu'à un Collecteur d'événements. Le nombre de connexions n'est pas limité.  Vous ne pouvez pas connecter de collecteur QRadar QFlow Collector au Collecteur d'événements sur un dispositif 15xx.
Collecteur d'événements	processeur d'événements	Vous ne pouvez connecter un collecteur Collecteur d'événements qu'à un seul processeur d'événements.  Vous pouvez connecter un Collecteur d'événements d'un système non console à un processeur d'événements sur le même système.  Un Collecteur d'événements d'une console ne peut être connecté qu'à un processeur d'événements d'une console. Il n'est pas possible de retirer cette connexion.
processeur d'événements	processeur d'événements	Vous ne pouvez pas connecter un processeur d'événements de console à un processeur d'événements d'un système non console.  Vous pouvez connecter un processeur d'événements d'un système non console à un autre processeur d'événements de console ou d'un système non console, mais pas aux deux en même temps.  Lorsqu'un hôte géré d'un système non console est ajouté, le processeur d'événements du système non console est connecté au processeur d'événements de la console.
Noeud de données	processeur d'événements	Vous ne pouvez connecter un noeud de données qu'à un processeur d'événements ou de flux. Vous pouvez connecter plusieurs Noeuds de données au même processeur pour créer un cluster de stockage.
Collecteur d'événements	Cible hors site	Le nombre de connexions n'est pas limité.
Source hors site	Collecteur d'événements	Le nombre de connexions n'est pas limité.  Un Collecteur d'événements qui est connecté à un dispositif d'événements uniquement ne peut pas recevoir de connexion hors site depuis le matériel système sur lequel la fonction <b>Recevoir des flux</b> est activée.  Un Collecteur d'événements connecté à un dispositif uniquement QFlow ne peut pas recevoir de connexion hors site provenant d'un système distant sur lequel la fonction <b>Recevoir des flux</b> est activée.

Si vous avez configuré IBM QRadar Incident Forensics dans votre déploiement, vous pouvez ajouter un hôte géré QRadar Incident Forensics. Pour plus d'informations, voir *IBM QRadar Incident Forensics - Guide d'installation*.

Si vous avez configuré IBM QRadar Vulnerability Manager dans votre déploiement, vous pouvez ajouter des scanners de vulnérabilités et un processeur de vulnérabilité. Pour plus d'informations, voir *IBM QRadar Vulnerability Manager - Guide d'utilisation*.

Si vous avez configuré IBM QRadar Risk Manager dans votre déploiement, vous pouvez ajouter un hôte géré. Pour plus d'informations, voir *IBM QRadar Risk Manager - Guide d'installation*.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Dans le menu **Actions de déploiement**, cliquez sur **Ajouter l'hôte**.
5. Configurez les paramètres de l'hôte géré en fournissant l'adresse IP fixe, le mot de passe root pour accéder au shell du système d'exploitation sur le dispositif.
6. Cliquez sur **Ajouter**.
7. Facultatif : Sélectionnez **Actions de déploiement** > **Afficher le déploiement** pour afficher les visualisations de votre déploiement. Vous pouvez télécharger une image PNG ou un fichier Microsoft Visio (2010) VDX de visualisation de votre déploiement.
8. Sous l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Ajout d'un hôte géré IPv4-only dans un environnement à deux piles

Pour ajouter un hôte géré IPv4-only à une console à deux piles, vous devez exécuter des scripts pour préparer l'hôte géré et la console avant de pouvoir ajouter l'hôte géré à la console.

### Pourquoi et quand exécuter cette tâche

Une console à double pile est une console qui prend en charge IPv4 et IPv6. Vous ne pouvez pas ajouter un hôte géré IPv4-only à un déploiement High Availability (HA) QRadar.

Tableau 14. Combinaisons de protocoles IP prises en charge sur des hôtes gérés sans console

Hôtes gérés	Console QRadar (IPv6, unique)	Console QRadar (IPv6, HA)	Console QRadar (pile en double, simple)	Console QRadar (pile-à-pile, HA)
IPv4, unique	Non	Non	Oui*	Non
IPv4, HA	Non	Non	Non	Non
IPv6, unique	Oui	Oui	Oui	Non
IPv6, HA	Oui	Oui	Oui	Non

## Procédure

1. Pour activer votre QRadar Console pour un déploiement à deux piles, entrez la commande suivante :

```
/opt/qradar/bin/setup_v6v4_console.sh ip=<IPv4_address_of_the_Console> netmask=<netmask> gateway=<gateway>
```

Cet exemple suppose que l'adresse IPv4 de la console est 192.0.2.2, que le masque de sous-réseau est 255.255.255.0 et que la passerelle est 192.0.2.1.

```
/opt/qradar/bin/setup_v6v4_console.sh ip=192.0.2.2 netmask=255.255.255.0 gateway=192.0.2.1
```

2. Pour autoriser l'ajout d'un hôte géré IPv4-only à votre déploiement, entrez la commande suivante sur la console :

```
/opt/qradar/bin/add_v6v4_host.sh host=<IP_address_of_the_managed_host>
```

Cet exemple suppose que l'adresse IPv4 de l'hôte géré est 192.0.2.3.

```
/opt/qradar/bin/add_v6v4_host.sh host=192.0.2.3
```

3. Ajoutez l'hôte géré IPv4-only au déploiement.

## Que faire ensuite

«Ajout d'un hôte géré», à la page 76

### Concepts associés

«Hôtes gérés», à la page 74

Pour plus de flexibilité sur la collecte de données et le traitement des événements et des flux, générer un déploiement IBM QRadar réparti en ajoutant des hôtes gérés sans console, tels que des collecteurs, des processeurs et des nœuds de données.

### Tâches associées

Ajout d'un hôte géré

## Configuration d'un hôte géré

Configurez un hôte géré pour spécifier le rôle que l'hôte géré remplit dans votre déploiement. Par exemple, vous pouvez configurer l'hôte géré en tant que collecteur, processeur ou nœud de données. Vous pouvez également modifier les paramètres de chiffrement et affecter l'hôte à un groupe de conversion d'adresses réseau (NAT).



Pour effectuer des modifications de configuration réseau, telles qu'une modification d'adresse IP sur vos systèmes hôte QRadar Console et gérés après l'installation de votre déploiement QRadar, utilisez l'utilitaire `qchange_netsetup`. Si vous utilisez `qchange_netsetup`, vérifiez que le stockage externe qui n'est pas `/store/ariel` ou `/store` n'est pas monté. Pour plus d'informations sur les paramètres réseau, voir le *Guide d'installation* de votre produit.

## Avant de commencer

Vérifiez que l'hôte géré possède la même version IBM QRadar et le même niveau de groupe de correctifs que le QRadar Console utilisé pour la gérer. Vous ne pouvez pas éditer ou supprimer un hôte géré qui utilise une version différente de QRadar.

Si vous souhaitez activer la conversion d'adresses réseau statique (NAT) pour un hôte géré, le réseau doit utiliser une conversion NAT statique. Pour plus d'informations, voir «Réseaux NAT activés», à la page 68.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez l'hôte dans la table d'hôtes et dans le menu **Actions de déploiement**, cliquez sur **Editer l'hôte**.
  - a) Pour créer un tunnel de chiffrement SSH sur le port 22 pour l'hôte géré, sélectionnez la case à cocher **Chiffrer les connexions hôte** .
  - b) Pour configurer l'hôte géré pour qu'il utilise un réseau NAT activé, cochez la case **Traduction d'adresse réseau** , puis configurez **Groupe NAT** et **Adresse IP publique**.
  - c) Pour configurer les composants sur l'hôte géré, cliquez sur l'icône des paramètres **Gestion des composants** () et configurez les options.
  - d) Cliquez sur **Sauvegarder**.
5. Sous l'onglet **Admin**, sélectionnez **Avancé > Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.


## Retrait d'un hôte géré

Vous pouvez supprimer des hôtes non gérés de la console de votre déploiement. Vous ne pouvez pas supprimer un hôte géré qui héberge la console IBM QRadar.

### Avant de commencer

Vérifiez que l'hôte géré possède la même version IBM QRadar et le même niveau de groupe de correctifs que le QRadar Console utilisé pour la gérer. Vous ne pouvez pas supprimer un hôte qui exécute une version différente de QRadar.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Dans le menu **Actions de déploiement**, cliquez sur **Supprimer l'hôte** et sur **OK**.

Vous ne pouvez pas supprimer un hôte QRadar Console.


5. Sous l'onglet **Admin**, sélectionnez **Avancé > Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Configuration de votre pare-feu local

Utilisez le pare-feu local pour gérer l'accès à l'hôte géré IBM QRadar à partir d'unités spécifiques situées à l'extérieur du réseau. Lorsque la liste de pare-feu est vide, l'accès à l'hôte géré est désactivé, sauf par le biais des ports ouverts par défaut.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez l'hôte pour lequel vous souhaitez configurer les paramètres d'accès au pare-feu.
5. Dans le menu **Actions**, cliquez sur **Afficher et gérer le système**.
6. Cliquez sur l'onglet **Pare-feu** et entrez les informations relatives à l'unité qui doit se connecter à l'hôte.
  - a) Configurez l'accès pour les appareils qui se trouvent à l'extérieur de votre déploiement et qui doivent se connecter à cet hôte.
  - b) Ajoutez cette règle d'accès.
7. Cliquez sur **Sauvegarder**.

Si vous modifiez le paramètre **External Flow Source Monitoring Port** dans la configuration QFlow, vous devez également mettre à jour votre configuration d'accès au pare-feu.

## Ajout d'un serveur de messagerie

IBM QRadar utilise un serveur de messagerie pour distribuer des alertes, des rapports, des notifications et des messages d'événement.

### Pourquoi et quand exécuter cette tâche

Vous pouvez configurer un serveur de messagerie pour l'ensemble de votre déploiement QRadar ou plusieurs serveurs de messagerie.

**Important :** QRadar prend uniquement en charge le chiffrement pour le serveur de messagerie à l'aide de STARTTLS.

**Important :** Si vous configurez le paramètre de serveur de messagerie pour un hôte en tant que Hôte\_local, les messages ne quittent pas cet hôte.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Gestion des serveurs de messagerie**.
2. Cliquez sur **Ajouter** et configurez les paramètres de votre serveur de messagerie.
3. Cliquez sur **Sauvegarder**.

**Conseil :** Laissez l'option **TLS** définie sur **Activé** pour envoyer des courriers électroniques chiffrés. Cela nécessitera un certificat TLS externe.

4. Pour éditer un serveur de messagerie, cliquez sur l'icône **Autres paramètres** ( ? ) du serveur, faites vos modifications, puis cliquez sur **Sauvegarder**.
5. Pour supprimer un serveur de messagerie, cliquez sur l'icône **Autres paramètres** du serveur, puis sur **Supprimer**.
6. Après avoir configuré un serveur de messagerie, vous pouvez l'affecter à un ou plusieurs hôtes.
  - a) Sur la page **Gestion du système et de la licence**, sélectionnez un hôte.
  - b) Modifiez la liste **Afficher** pour afficher **Systemes**.
  - c) Cliquez sur **Actions > Afficher et gérer le système**.
  - d) Dans l'onglet **Serveur de messagerie**, sélectionnez un serveur de messagerie et cliquez sur **Sauvegarder**.
  - e) Testez la connexion au serveur de messagerie en cliquant sur le bouton **Tester la connexion**.
  - f) Cliquez sur **Sauvegarder**.

## Modifications de configuration dans votre environnement QRadar

Lorsque vous faites des modifications de configuration dans IBM QRadar, les modifications sont sauvegardées dans une zone de transfert et la bannière de déploiement de l'onglet **Admin** est mise à jour, ce qui indique que des modifications doivent être déployées. Le déploiement des modifications peut nécessiter le redémarrage des services QRadar.

QRadar dispose de deux méthodes de déploiement des modifications : la configuration standard et la configuration complète. Le type de déploiement requis dépend du type de modifications effectuées.

### Déploiement standard

Cette méthode de déploiement ne redémarre que les services directement affectés par les modifications apportées. Vous commencez un déploiement standard en cliquant sur **Déployer les modifications** sur la bannière de l'onglet **Admin**.

La liste suivante présente des exemples de modifications nécessitant un déploiement standard :

- Ajout ou modification d'un nouvel utilisateur ou d'un nouveau rôle d'utilisateur.
- Définition d'un mot de passe pour un autre utilisateur.

- Modification du rôle ou du profil de sécurité d'un utilisateur.

## Déploiement de configuration complète

Les modifications qui affectent l'ensemble du déploiement QRadar doivent être déployées à l'aide de la méthode de déploiement de configuration complète. Vous commencez un déploiement de configuration complète en cliquant sur **Déployer la configuration entière** dans le menu **Avancé** de l'onglet **Admin**.

Cette méthode reconstruit tous les fichiers de configuration sur chacun des hôtes gérés. Pour garantir que la nouvelle configuration est correctement chargée, tous les services sur les hôtes gérés sont automatiquement redémarrés, à l'exception du service de collecte d'événements. Pendant le redémarrage des autres services, QRadar continue de collecter des événements et les stocke dans une mémoire tampon jusqu'à ce que les hôtes gérés soient reconnectés.

La liste suivante présente des exemples de modifications nécessitant un déploiement de configuration complète :

- Ajout d'un hôte géré.
- Modification de la configuration pour un hôte géré
- Configuration des hôtes hors site pour l'envoi ou la réception de données à partir de QRadar Console.
- Restauration d'une sauvegarde de configuration

## Modifications qui ont une incidence sur la collecte d'événements

Les événements entrent dans QRadar via le service de collecte d'événements `ecs-ec-ingress`. À partir de QRadar V7.3.1, le service est géré séparément des autres services QRadar. Pour minimiser les interruptions dans la collecte des données d'événement, le service ne redémarre pas automatiquement lorsque le service `hostcontext` redémarre.

Les situations suivantes peuvent provoquer une interruption de la collecte d'événements :


- Réamorçage d'un dispositif qui collecte des événements.
- Ajout d'un hôte géré à haute disponibilité.
- Pendant le basculement à haute disponibilité.
- Restauration d'une sauvegarde de configuration
- Ajout ou suppression d'une connexion source externe
- Chaque fois que l'utilisation du disque d'une partition dépasse le seuil maximal.

Lorsque vous déployez des modifications après la restauration d'une sauvegarde de configuration, vous pouvez redémarrer le service de collecte d'événements maintenant ou ultérieurement. Lorsque vous choisissez de redémarrer le service ultérieurement, QRadar déploie toutes les modifications qui ne dépendent pas du service de collecte d'événements et continue de collecter des événements pendant le redémarrage des autres services. La bannière de déploiement continue d'afficher les modifications non déployées et le message `Le service de collecte d'événements doit être redémarré` s'affiche lorsque vous affichez les détails.

## Configuration de Collecteur d'événements

Ajoutez un QRadar Collecteur d'événements lorsque vous souhaitez développer votre déploiement, soit pour collecter d'autres événements en local, soit pour collecter des événements à partir d'un emplacement distant.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Cliquez sur **Configuration du système > Gestion des systèmes et des licences**.
3. Sélectionnez l'hôte géré à configurer.



4. Cliquez sur **Actions de déploiement > Éditer l'hôte.**
5. Cliquez sur **Gestion des composants.**
6. Entrez des valeurs pour les paramètres suivants :


Paramètre	Description
<b>Port d'écoute du transfert d'événement</b>	Port d'acheminement des événements Collecteur d'événements.
<b>Port d'écoute de transfert de flux</b>	Port d'acheminement du flux Collecteur d'événements.
<b>Détection automatique activée</b>	<p><b>Vrai</b> permet à Collecteur d'événements d'analyser et d'accepter automatiquement le trafic à partir de sources de journal précédemment inconnues. Les ports de pare-feu appropriés sont ouverts pour permettre à Autodétection de recevoir des événements. Cette option est la valeur par défaut.</p> <p><b>Faux</b> empêche le Collecteur d'événements d'analyser et d'accepter automatiquement le trafic à partir de sources de journal précédemment inconnues.</p> <p>Pour plus d'informations, voir <i>Managing Log Sources Guide</i>.</p>
<b>Détection automatique-Utiliser les paramètres globaux</b>	<p><b>Vrai</b> indique que Collecteur d'événements utilise les paramètres globaux pour la détection automatique des sources de journal.</p> <p><b>Faux</b> indique que Collecteur d'événements utilise des paramètres locaux individuels (fichier de configuration XML) pour la détection automatique des sources de journal.</p>
<b>Déduplication de flux activée</b>	
<b>Temps du filtre de dédoublement de flux</b>	Durée en secondes pendant laquelle les flux sont mis en mémoire tampon avant leur transmission.
<b>Temps de filtre de flux asymétrique</b>	Durée en secondes pendant laquelle le flux asymétrique est mis en mémoire tampon avant d'être transmis.
<b>Événements de réacheminement déjà en cours</b>	<p><b>Vrai</b> permet à Collecteur d'événements de transmettre des événements détectés sur le système.</p> <p><b>Faux</b> empêche le Collecteur d'événements de réacheminer les événements détectés sur le système. Cette option empêche le bouclage des événements de votre système.</p>
<b>Compression du trafic du processeur d'événements</b>	

7. Cliquez sur **Sauvegarder.**
8. Répétez l'opération pour tous les QRadar Event Collectors de votre déploiement que vous souhaitez configurer.

## Déploiement des modifications

Les modifications apportées au déploiement IBM QRadar doivent être envoyées de la zone de transfert vers la zone de production.

### Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Consultez la bannière de déploiement pour déterminer si des modifications doivent être déployées.
3. Cliquez sur **Afficher les détails** pour afficher des informations sur les modifications de configuration non déployées.
4. Choisissez la méthode de déploiement :
  - a) Pour déployer les modifications et redémarrer uniquement les services affectés, cliquez sur **Déployer les modifications** dans la bannière de déploiement.
  - b) Pour régénérer les fichiers de configuration et redémarrer tous les services sur chaque hôte géré, cliquez sur **Avancé > Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Redémarrage du service de collecte d'événements

Il peut y avoir des situations lorsque vous souhaitez redémarrer uniquement le service de collecte d'événements sur tous les hôtes gérés de votre environnement IBM QRadar. Par exemple, lorsqu'une nouvelle version du service **ecs-ec-ingress** est disponible pour la mise à niveau ou lorsque vous avez différé le redémarrage du service lors d'un déploiement antérieur.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans le menu **Avancé**, cliquez sur **Redémarrer les services de collecte d'événements**. La collecte d'événements est brièvement interrompue pendant le redémarrage du service.


**Remarque :** Vous pouvez également redémarrer le service de collecte d'événements sur la ligne de commande en entrant la commande suivante :

```
systemctl restart ecs-ec-ingress
```

## Arrêt d'un système

Lorsque vous arrêtez un système, le dispositif est hors tension. L'interface IBM QRadar n'est pas disponible et la collecte de données s'arrête lorsque le système est arrêté.


### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez le système que vous souhaitez arrêter.
5. Dans le menu **Actions**, sélectionnez **Arrêter le système**.

## Redémarrage d'un système

Lorsque vous redémarrez un système, l'interface IBM QRadar n'est pas disponible et la collecte de données s'arrête lorsque le système redémarre.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez le système que vous souhaitez redémarrer.
5. Dans le menu **Actions**, sélectionnez **Redémarrer le système**.

## Collecte des fichiers journaux

---

Les fichiers journaux IBM QRadar contiennent des informations détaillées sur votre déploiement, telles que les noms d'hôte, les adresses IP et les adresses électroniques. Si vous avez besoin d'aide pour l'identification et la résolution des incidents, vous pouvez collecter les fichiers journaux et les envoyer au support IBM.


### Pourquoi et quand exécuter cette tâche

Vous pouvez collecter les fichiers journaux pour un ou plusieurs systèmes hôtes simultanément. Selon la taille de votre déploiement et le nombre d'hôtes gérés, la collecte des fichiers journaux peut prendre un certain temps. Les fichiers journaux de la console QRadar sont automatiquement inclus dans chaque collection de fichiers journaux.

Vous pouvez continuer à utiliser la console QRadar pendant l'exécution de la collecte de fichiers journaux. Si le système collecte activement des fichiers journaux, vous ne pouvez pas lancer une nouvelle demande de collecte. Annuler le processus de collecte actif et démarrer une autre collection.

Lorsque le processus de collecte des fichiers journaux est terminé, une notification du système apparaît sur le tableau de bord **Surveillance du système**.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Dans la liste **Afficher**, sélectionnez **Systèmes**.
4. Sélectionnez les hôtes dans la table hôte.
5. Cliquez sur **Actions > Collecter les fichiers journaux**.
6. Cliquez sur **Options avancées** et choisissez les options pour la collecte des fichiers journaux.

**Important :** Fonctions modifiées dans la version 7.4.2 Si vous choisissez l'option **Chiffrer le fichier compressé**, vous devez entrer un mot de passe pour le fichier journal. Si vous envoyez des fichiers journaux chiffrés à IBM Support, vous devez également fournir le mot de passe afin que les fichiers journaux puissent être déchiffrés.

Dans les éditions précédentes, vous ne pouvez pas spécifier un mot de passe et les fichiers journaux chiffrés ne peuvent être déchiffrés que par le support IBM.

7. Cliquez sur **Collecter les fichiers journaux**.  
Vérifiez l'état du processus de collecte dans la section Messages des activités de support système.
8. Pour télécharger la collection de fichiers journaux, attendez la notification La collecte du fichier journal a abouti, puis cliquez sur le lien **Cliquez ici pour télécharger le fichier**.

## Modification du mot de passe racine de votre QRadar Console

En tant que bonne pratique de sécurité, modifiez le mot de passe root sur votre QRadar Console à intervalles réguliers.

### Procédure

1. Connectez-vous à QRadar Console en tant qu'utilisateur racine.
2. Utilisez la commande **passwd** pour changer votre mot de passe.


## Réinitialisation du module SIM

Une fois que vous avez effectué votre déploiement, évitez de recevoir d'autres informations positives supplémentaires en réinitialisant SIM pour supprimer toutes les violations, ainsi que les adresses IP source et de destination à partir de la base de données et du disque.

### Pourquoi et quand exécuter cette tâche

Le processus de réinitialisation SIM peut prendre plusieurs minutes, en fonction de la quantité de données dans votre système. Si vous tentez de vous déplacer vers d'autres zones de l'interface utilisateur IBM QRadar pendant le processus de réinitialisation SIM, un message d'erreur s'affiche.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans le menu **Avancé**, sélectionnez **Nettoyer le modèle SIM**.
3. Lisez les informations de la fenêtre **Réinitialiser le modèle de données SIM**.
4. Sélectionnez l'une des options suivantes.

Option	Description
<b>Nettoyage léger</b>	Ferme toutes les infractions dans la base de données. Si vous sélectionnez l'option <b>Nettoyage léger</b> , vous pouvez également cocher la case <b>Désactiver toutes les infractions</b> .
<b>Nettoyage physique</b>	Purge toutes les données SIM actuelles et historiques de la base de données, y compris les violations protégées, les adresses IP source et les adresses IP de destination.

5. Si vous souhaitez continuer, sélectionnez le **Souhaitez-vous vraiment réinitialiser le modèle de données ?** case à cocher.
6. Cliquez sur **Continuer**.
7. Lorsque le processus de réinitialisation SIM est terminé, cliquez sur **Fermer**.
8. Actualisez votre navigateur Web.

# Chapitre 6. QRadar des tâches de configuration

Utilisez les paramètres de l'onglet Admin pour configurer votre déploiement IBM QRadar, y compris votre hiérarchie de réseau, les mises à jour automatiques, les paramètres système, les compartiments de conservation d'événements, les notifications système, les paramètres de console et la gestion d'index.

## Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Hiérarchie du réseau

IBM QRadar utilise les objets et les groupes de hiérarchie de réseau pour afficher l'activité réseau et surveiller les groupes ou les services de votre réseau.

Lorsque vous développez votre hiérarchie de réseau, adoptez la méthode la plus appropriée pour afficher l'activité réseau. La hiérarchie du réseau n'a pas besoin de ressembler au déploiement physique de votre réseau. QRadar prend en charge n'importe quelle hiérarchie de réseau et peut être défini par une plage d'adresses IP. Vous pouvez baser votre réseau sur plusieurs variables différentes, y compris des unités géographiques ou d'activité.

## Concepts associés

[Mises à jour de la hiérarchie de réseau dans un déploiement multilocataires](#)

## Instructions pour la définition de votre hiérarchie de réseau

La création d'une hiérarchie de réseau dans IBM QRadar est une première étape essentielle de la configuration de votre déploiement. Sans une hiérarchie de réseau bien configurée, QRadar ne peut pas déterminer les directions de flux, créer une base de données d'actifs fiable ou bénéficier de blocs de construction utiles dans des règles.

Tenez compte des instructions suivantes lorsque vous définissez votre hiérarchie de réseau :

- Organisez vos systèmes et réseaux par rôle ou par des modèles de trafic similaires.

Par exemple, vous pouvez organiser votre réseau pour inclure des groupes pour les serveurs de messagerie, les utilisateurs ministériels, les laboratoires ou les équipes de développement. À l'aide de cette organisation, vous pouvez différencier le comportement du réseau et appliquer des règles de sécurité de gestion de réseau basées sur le comportement. Toutefois, ne groupez pas un serveur ayant un comportement unique avec d'autres serveurs sur votre réseau. Le fait de placer seul un serveur unique fournit au serveur une plus grande visibilité dans QRadar, et facilite la création de règles de sécurité spécifiques pour le serveur.

- Placez les serveurs avec des volumes de trafic élevés, tels que les serveurs de messagerie, en haut du groupe. Cette hiérarchie vous fournit une représentation visuelle lorsqu'une différence se produit.
- Ne configurez pas un groupe de réseau avec plus de 15 objets.

Les grands groupes de réseau peuvent entraîner des difficultés lorsque vous affichez des informations détaillées pour chaque objet. Si votre déploiement traite plus de 600 000 flux, envisagez de créer plusieurs groupes de niveau supérieur.

- Conservez l'espace disque en combinant plusieurs routages inter-domaines (CIDR) ou sous-réseaux en un seul groupe de réseau.

Par exemple, ajoutez des serveurs clés en tant qu'objets individuels et groupez d'autres serveurs principaux mais associés dans des objets multi-CIDR.

Groupe	Description	Adresses IP
1	Marketing	10.10.5.0/24

Groupe	Description	Adresses IP
2	Ventes	10.10.8.0/21
3	Cluster de base de données	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

- Définissez un groupe global de sorte que lorsque vous définissez de nouveaux réseaux, les règles appropriées et les moniteurs de comportement sont appliqués.

Dans l'exemple suivant, si vous ajoutez un réseau de service HR, tel que 10.10.50.0/24, au groupe de Cleveland, le trafic s'affiche comme basé sur Cleveland et toutes les règles que vous appliquez au groupe Cleveland sont appliquées par défaut.

Groupe	Sous-groupe	Adresse IP
Cleveland	Cleveland divers	10.10.0.0/16
Cleveland	Ventes Cleveland	10.10.8.0/21
Cleveland	Marketing Cleveland	10.10.1.0/24

- Dans un environnement activé par domaine, vérifiez que chaque adresse IP est affectée au domaine approprié.

#### Information associée

[QRadar Support Geodata FAQ](#)

## Valeurs CIDR acceptables

IBM QRadar accepte les valeurs CIDR spécifiques.

Le tableau suivant fournit une liste des valeurs CIDR acceptées par QRadar :

Longueur CIDR	Masque	Nombre de réseaux	Hôtes
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544

Longueur CIDR	Masque	Nombre de réseaux	Hôtes
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 sous-réseaux	124
/26	255.255.255.192	4 sous-réseaux	62
/27	255.255.255.224	8 sous-réseaux	30
/28	255.255.255.240	16 sous-réseaux	14
/29	255.255.255.248	32 sous-réseaux	6
/30	255.255.255.252	64 sous-réseaux	2
/31	255.255.255.254	Aucun	Aucun
/32	255.255.255.255	1/256 C	1

Par exemple, un réseau est appelé superréseau lorsque la limite de préfixe contient moins de bits que le masque naturel (ou classique) du réseau. Un réseau est appelé sous-réseau lorsque la limite de préfixe contient plus de bits que le masque naturel du réseau:

- 209.60.128.0 est une adresse réseau de classe C avec un masque de /24.
- 209.60.128.0 /22 est un supernet qui génère :
  - 209.60.128.0 /24
  - 209.60.129.0 /24
  - 209.60.130.0 /24
  - 209.60.131.0 /24
- 192.0.0.0 /25
  - Plage d'hôtes de sous-réseau
  - 0 192.0.0.1-192.0.0.126
  - 1 192.0.0.129-192.0.0.254
- 192.0.0.0 /26
  - Plage d'hôtes de sous-réseau
  - 0 192.0.0.1 - 192.0.0.62

- 1 192.0.0.65 - 192.0.0.126
- 2 192.0.0.129 - 192.0.0.190
- 3 192.0.0.193 - 192.0.0.254
- 192.0.0.0 /27
  - Plage d'hôtes de sous-réseau
  - 0 192.0.0.1 - 192.0.0.30
  - 1 192.0.0.33 - 192.0.0.62
  - 2 192.0.0.65 - 192.0.0.94
  - 3 192.0.0.97 - 192.0.0.126
  - 4 192.0.0.129 - 192.0.0.158
  - 5 192.0.0.161 - 192.0.0.190
  - 6 192.0.0.193 - 192.0.0.222
  - 7 192.0.0.225 - 192.0.0.254

### Tâches associées

#### Définition de votre hiérarchie réseau

Un hiérarchie de réseau par défaut, contenant des groupes de réseau prédéfinis, est incluse dans IBM QRadar. Vous pouvez éditer ses objets ou créer de nouveaux groupes ou objets de réseau.

## Définition de votre hiérarchie réseau


Un hiérarchie de réseau par défaut, contenant des groupes de réseau prédéfinis, est incluse dans IBM QRadar. Vous pouvez éditer ses objets ou créer de nouveaux groupes ou objets de réseau.

### Pourquoi et quand exécuter cette tâche

Les objets du réseau sont des conteneurs d'adresses CIDR (Classless Inter-Domain Routing). Toute adresse IP définie dans une plage CIDR dans la hiérarchie du réseau est considérée comme une adresse locale. Inversement, toute adresse IP non définie dans une plage CIDR dans la hiérarchie du réseau est considérée comme une adresse distante. Une plage CIDR ne peut appartenir qu'à un seul objet du réseau, mais des sous-ensembles de cette plage peuvent appartenir à un autre objet du réseau. Le trafic réseau correspond au CIDR le plus exact. Plusieurs plages CIDR peuvent être affectées à un objet réseau.

Dans QRadar, certains des blocs de construction et règles par défaut utilisent les objets de la hiérarchie de réseau par défaut. Avant de changer l'un de ces objets, faites une recherche sur les règles et les blocs de construction afin de bien comprendre comment cet objet est utilisé et quels sont les blocs et les règles qui pourraient nécessiter des ajustements consécutivement à la modification de l'objet. Pour éviter les fausses infractions, il est important que la hiérarchie du réseau, les règles et les blocs de construction soient maintenus à jour.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Hiérarchie du réseau**.
3. Dans le menu arborescent de la fenêtre **Vues de réseau**, sélectionnez la partie du réseau sur laquelle vous voulez travailler.
4. Pour ajouter des objets de réseau, cliquez sur **Ajouter** et remplissez les champs suivants :

Option	Description
<b>Nom</b>	Nom unique de l'objet du réseau.



Option	Description
	<b>Conseil :</b> Pour définir la position de l'objet dans la hiérarchie du réseau, vous pouvez utiliser un système de noms à points. Par exemple, si vous entrez D . E . F comme nom d'objet, cela revient à créer une hiérarchie à trois niveaux avec E comme sous-noeud de D et F comme sous-noeud de E.
<b>Groupe</b>	Le groupe de réseau dans lequel ajouter l'objet du réseau. Sélectionnez-le dans la liste <b>Groupe</b> ou cliquez sur <b>Ajouter un nouveau groupe</b> .  <b>Conseil :</b> Lorsque vous ajoutez un groupe de réseau, pour définir sa position dans la hiérarchie des groupes de réseau, vous pouvez utiliser un système de noms à points. Par exemple, si vous entrez A . B . C comme nom de groupe, cela revient à créer une hiérarchie à trois niveaux avec B comme sous-noeud de A et C comme sous-noeud de B.
<b>IP/CIDR</b>	Tapez une adresse IP ou une plage d'adresses CIDR pour l'objet du réseau, puis cliquez sur <b>Ajouter</b> . Vous pouvez ajouter plusieurs adresses IP individuelles et plages d'adresses CIDR.
<b>Description</b>	Description de l'objet du réseau. Cette zone est facultative.
<b>Pays/Région</b>	Pays ou région où se situe l'objet du réseau. Cette zone est facultative.
<b>Longitude et latitude</b>	Position géographique (longitude et latitude) de l'objet du réseau. Ces zones sont codépendantes et optionnelles.

5. Cliquez sur **Créer**.

6. Répétez ces étapes pour ajouter d'autres objets de réseau ou cliquez sur **Editer** ou **Supprimer** pour travailler sur les objets existants.

#### Concepts associés

Valeurs CIDR acceptables

IBM QRadar accepte les valeurs CIDR spécifiques.

## Mises à jour automatiques

Vous pouvez mettre à jour automatiquement ou manuellement vos fichiers de configuration pour vous assurer que vos fichiers de configuration contiennent les informations de sécurité réseau les plus récentes.

Les fichiers de configuration mis à jour aident à éliminer les faux positifs et à protéger votre système des derniers sites malveillants, des botnets et d'autres activités Internet suspectes.

### Exigences de mise à jour automatique

La console IBM QRadar doit être connectée à Internet pour recevoir les mises à jour. Si votre console n'est pas connectée à Internet, vous devez configurer un serveur de mise à jour interne pour votre console afin de télécharger les fichiers à partir de.

Les fichiers de mise à jour sont disponibles pour le téléchargement manuel à partir de [IBM Fix Central](http://www.ibm.com/support/fixcentral) (<http://www.ibm.com/support/fixcentral>).

Pour préserver l'intégrité de votre configuration et de vos informations actuelles, remplacez les fichiers de configuration existants ou intégrez les fichiers mis à jour avec vos fichiers existants.

Après avoir installé les mises à jour sur votre console et déployé vos modifications, la console met à jour ses hôtes gérés.

### Description des mises à jour

Les fichiers de mise à jour peuvent inclure les mises à jour suivantes :

- Mises à jour de configuration basées sur le contenu, y compris les modifications apportées aux fichiers de configuration, les vulnérabilités, les mappes QID, les scripts de support et les mises à jour des informations sur les menaces de sécurité.
- DSM, scanner et mises à jour de protocole qui incluent des corrections à l'analyse syntaxique des problèmes, des modifications du scanner et des mises à jour de protocole.
- Les principales mises à jour, telles que les fichiers JAR mis à jour ou les correctifs volumineux, nécessitent le redémarrage du service d'interface utilisateur.
- Mises à jour mineures, telles que les journaux de mise à jour automatique quotidienne ou les scripts de mappe QID, qui ne redémarque pas le service d'interface utilisateur.

## Mises à jour automatiques pour les déploiements à haute disponibilité

Lorsque vous mettez à jour vos fichiers de configuration sur un hôte principal et déployez vos modifications, les mises à jour sont automatiquement effectuées sur l'hôte secondaire. Si vous ne déployez pas vos modifications, les mises à jour sont effectuées sur l'hôte secondaire via un processus automatisé qui s'exécute toutes les heures.

## Fréquence des mises à jour automatiques pour les nouvelles installations et les mises à niveau

La fréquence par défaut de la mise à jour automatique est déterminée par le type d'installation et la version QRadar.

- Si vous effectuez une mise à niveau à partir de versions QRadar antérieures à V7.2, la valeur à laquelle la fréquence de mise à jour est définie reste la même après la mise à niveau. Par défaut, la mise à jour est hebdomadaire, mais vous pouvez modifier la fréquence manuellement.
- Si vous installez une nouvelle installation de QRadar V7.2 ou une version ultérieure, la fréquence par défaut de la mise à jour est quotidienne. Vous pouvez modifier manuellement la fréquence.

### Concepts associés

#### Mises à jour manuelles

Si votre déploiement inclut une console IBM QRadar qui n'est pas en mesure d'accéder à Internet ou que vous souhaitez gérer manuellement les mises à jour de votre système, vous pouvez gérer manuellement le processus de mise à jour en configurant un serveur de mise à jour IBM QRadar.

## Affichage des mises à jour en attente

Votre système est préconfiguré pour des mises à jour automatiques hebdomadaires. Vous pouvez voir les mises à jour en attente dans la fenêtre **Updates**.

### Pourquoi et quand exécuter cette tâche


Votre système doit rester en fonctionnement suffisamment longtemps pour récupérer les mises à jour hebdomadaires. Si aucune mise à jour n'est visible dans la fenêtre **Updates**, cela signifie que votre système n'est pas lancé depuis suffisamment longtemps pour avoir eu le temps de récupérer les mises à jour hebdomadaires ou qu'aucune mise à jour n'a été publiée. Dans ce cas, vous pouvez [rechercher manuellement les nouvelles mises à jour](#).

La barre d'outils **Check for Updates** offre les fonctions suivantes :

Tableau 18. Fonctions de la barre d'outils **Check for Updates**

Fonction	Description
<b>Masquer</b>	Sélectionnez une ou plusieurs mises à jour, puis cliquez sur <b>Hide</b> pour les retirer de la page Check for Updates. Vous pouvez afficher et restaurer les mises à jour masquées sur la page <b>Restaurer les mises à jour masquées</b> . Pour plus d'informations, voir « <a href="#">Restauration de mises à jour masquées</a> », à la page 97.
<b>Installation</b>	Vous pouvez installer vous-même les mises à jour. On parle alors d'installation manuelle. Lorsque vous lancez une installation manuelle des mises à jour, le processus d'installation démarre dans la minute. Pour plus d'informations, voir « <a href="#">Installation manuelle des mises à jour automatiques</a> », à la page 96.
<b>schedule</b>	Vous pouvez configurer une date et une heure spécifiques pour l'installation manuelle des mises à jour sélectionnées sur votre console. Cette programmation est utile si vous voulez que l'installation des mises à jour s'effectue en dehors des heures de pointe. Pour plus d'informations, voir « <a href="#">Planification d'une mise à jour</a> », à la page 95.
<b>Unschedule</b>	Vous pouvez déprogrammer l'installation manuelle des mises à jour sur votre console. Pour plus d'informations, voir « <a href="#">Planification d'une mise à jour</a> », à la page 95.
<b>Search By Name</b>	Vous pouvez rechercher une mise à jour spécifique par son nom.
<b>Next Refresh</b>	Ce compteur affiche le temps restant avant la prochaine actualisation automatique. La liste des mises à jour affichée dans la page <b>Check for Updates</b> s'actualise automatiquement toutes les 60 secondes. Le compteur est automatiquement mis en pause lorsque vous sélectionnez une ou plusieurs mises à jour.
<b>Mettre en pause</b>	Met en pause le processus d'actualisation automatique. Pour reprendre l'actualisation automatique, cliquez sur <b>Play</b> .
<b>Actualiser</b>	Actualise la liste de mises à jour.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Pour afficher les détails d'une mise à jour, sélectionnez-la.

## Configuration des paramètres de mise à jour automatique

Vous pouvez personnaliser les paramètres de mise à jour automatique pour changer la fréquence des mises à jour, leur type, la configuration du serveur et les modalités de sauvegarde.


### Pourquoi et quand exécuter cette tâche

Vous pouvez sélectionner **Déploiement automatique** pour obtenir que les mises à jour soient déployées automatiquement. Si cette option n'est pas sélectionnée, après l'installation des mises à jour, vous devrez déployer vous-même les changements à partir de l'onglet **Tableau de bord**.

**Restriction :** Dans un environnement haute disponibilité (HA), les mises à jour ne sont pas installées automatiquement lorsqu'un hôte secondaire est actif. Elles ne sont installées qu'une fois que l'hôte primaire redevient le noeud actif.

Vous pouvez sélectionner **Redémarrage automatique du service** pour autoriser l'installation automatique des mises à jour nécessitant un redémarrage de l'interface utilisateur. Le fonctionnement de celle-ci est interrompu lorsque le service redémarre. Vous pouvez, sinon, installer vous-même les mises à jour au moment qui vous convient à partir de la fenêtre **Vérifier les mises à jour**.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Cliquez sur **Modifier les paramètres**.
4. Sous l'onglet **Base**, sélectionnez le planning des mises à jour.
  - a) Dans la section **Mises à jour de la configuration**, choisissez la méthode que vous souhaitez utiliser pour mettre à jour vos fichiers de configuration.
    - Pour fusionner vos fichiers de configuration existants avec les mises à jour du serveur sans que cela affecte vos signatures personnalisées, entrées personnalisées et configurations de réseau distantes, sélectionnez **Intégration automatique**.
    - Pour que les réglages du serveur annulent et remplacent vos personnalisations, sélectionnez **Mise à jour automatique**.
  - b) Dans la section **Mises à jour de gestionnaire de service de données, scanner et protocole**, choisissez une option pour l'installation des mises à jour.
  - c) Dans la section **Mises à jour majeures**, sélectionnez une option pour recevoir les mises à jour majeures correspondant à de nouvelles éditions.
  - d) Dans la section **Mises à jour mineures**, sélectionnez une option pour recevoir les correctifs des problèmes système mineurs.
  - e) Si vous voulez que les changements soient déployés automatiquement après l'installation des mises à jour, cochez la case **Déploiement automatique**.
  - f) Si vous voulez que le service de l'interface utilisateur redémarre automatiquement après l'installation des mises à jour, cochez la case **Redémarrage automatique du service**.
5. Cliquez sur l'onglet **Avancé** pour configurer le serveur de mises à jour et les paramètres de sauvegarde.
  - a) Dans la zone **Serveur Web**, entrez l'URL du serveur web d'où vous souhaitez obtenir les mises à jour.

Le serveur Web par défaut est `https://auto-update.qradar.ibmcloud.com/`.
  - b) Dans la zone **Répertoire**, indiquez le répertoire dans lequel le serveur web stocke les mises à jour.

Le répertoire par défaut est `autoupdates/`.
  - c) Facultatif : Configurez les paramètres pour le serveur proxy.

Si le serveur d'application utilise un serveur proxy pour se connecter à l'internet, vous devez le configurer. Si vous utilisez un proxy authentifié, vous devez fournir son nom d'utilisateur et son mot de passe.

- d) Dans la liste **Durée de conservation de la sauvegarde**, tapez ou sélectionnez le nombre de jours pendant lesquels vous souhaitez que soient conservés les fichiers que le processus de mise à jour remplace.

Les fichiers sont stockés à l'endroit spécifié dans **Emplacement de la sauvegarde**. Le minimum est de un jour et le maximum, de 65535 ans.

- e) Dans la zone **Emplacement de la sauvegarde**, indiquez l'emplacement où vous souhaitez que soient stockés les fichiers de sauvegarde.
- f) Dans la zone **Chemin de téléchargement**, indiquez le chemin du répertoire dans lequel doivent être stockées les mises à jour DSM, mineures et majeures.

Le chemin de répertoire par défaut est `/store/configservices/staging/updates`.

6. Cliquez sur **Sauvegarder**.

#### Information associée

[QRadar: Important auto update server changes for administrators](#)

## Configuration des mises à jour derrière un serveur proxy qui utilise l'interception SSL ou TLS

Pour configurer les mises à jour IBM QRadar derrière un serveur proxy, ajoutez le certificat de l'autorité de certification de votre serveur proxy au fichier `ca-bundle.crt`.

### Procédure

1. Créez une copie de sauvegarde du fichier `ca-bundle.crt` dans QRadar.  
Par exemple, utilisez la commande `copy` pour créer un fichier `.bak` : `cp /etc/ssl/certs/ca-bundle.crt{,bak}`.
2. Récupère le certificat de l'autorité de certification racine à partir de votre serveur proxy. Pour plus d'informations, consultez la documentation Docker.

**Remarque :** Vous devez utiliser uniquement le certificat de l'autorité de certification racine à partir de votre serveur proxy.

3. Ajoutez le certificat de l'autorité de certification au fichier `ca-bundle.crt` en entrant la commande suivante :

```
cp proxycert.pem /etc/pki/ca-trust/source/anchors
```

4. Extrayez le certificat en entrant la commande suivante :

```
update-ca-trust extract
```

5. Entrez la commande suivante pour exécuter la mise à jour automatique :


```
/opt/qradar/bin/UpdateConfs.pl -ds runnow 1
```

6. Vérifiez que les mises à jour automatiques fonctionnent en adaptant le journal dans `/var/log/autoupdates/`.

## Planification d'une mise à jour

Les mises à jour automatiques se produisent sur une planification récurrente en fonction des paramètres de la page **Configuration des mises à jour**. Pour réduire les impacts de performances sur votre système, vous pouvez planifier une mise à jour importante ou un ensemble de mises à jour pour qu'elle s'exécute pendant les heures hors pointe.

## Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Facultatif : Si vous souhaitez planifier des mises à jour spécifiques, sélectionnez les mises à jour que vous souhaitez planifier.
4. Dans la liste **Planification**, sélectionnez le type de mise à jour à planifier.
5. À l'aide de l'agenda, sélectionnez la date et l'heure de début du moment auquel vous souhaitez démarrer les mises à jour planifiées.

## Suppression des mises à jour planifiées

Les mises à jour planifiées affichent le statut **Planifié** dans la zone **Statut**. Vous pouvez annuler toute mise à jour planifiée.

Une fois le planning supprimé, le statut de la mise à jour s'affiche sous la forme **Nouveau**.


## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Cliquez sur **Rechercher les mises à jour**.
4. Facultatif : Si vous souhaitez effacer des mises à jour planifiées spécifiques, sélectionnez les mises à jour que vous souhaitez effacer.
5. Dans la liste **Déplanifier**, sélectionnez le type de mise à jour planifiée que vous souhaitez effacer.

## Recherche de nouvelles mises à jour

IBM fournit des mises à jour sur une base régulière. Par défaut, la fonction de mise à jour automatique est planifiée pour télécharger et installer automatiquement les mises à jour. Si vous avez besoin d'une mise à jour à une heure autre que la planification préconfigurée, vous pouvez télécharger de nouvelles mises à jour.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Cliquez sur **Rechercher les mises à jour**.
4. Cliquez sur **Obtenir de nouvelles mises à jour**.


## Installation manuelle des mises à jour automatiques

IBM fournit des mises à jour régulièrement. Par défaut, les mises à jour sont automatiquement téléchargées et installées sur votre système. Toutefois, vous pouvez installer une mise à jour à une heure autre que la planification préconfigurée.

## Pourquoi et quand exécuter cette tâche

Le système extrait les nouvelles mises à jour à partir de IBM Fix Central ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)). Cela peut prendre une période prolongée. Une fois terminée, les nouvelles mises à jour sont répertoriées dans la fenêtre **Mises à jour**.

## Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.

2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Cliquez sur **Rechercher les mises à jour**.
4. Facultatif : Si vous souhaitez installer des mises à jour spécifiques, sélectionnez les mises à jour que vous souhaitez planifier.
5. Dans la liste **Installation**, sélectionnez le type de mise à jour que vous souhaitez installer.

## Affichage de l'historique des mises à jour

Après l'aboutissement ou l'échec de l'installation d'une mise à jour, celle-ci est affichée sur la page **Afficher l'historique des mises à jour**.

### Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Cliquez sur **Afficher historique des mises à jour**.
4. Facultatif : En utilisant la zone **Rechercher par nom**, vous pouvez entrer un mot clé, puis appuyer sur Entrée pour rechercher une mise à jour spécifique par nom.
5. Pour examiner une mise à jour spécifique, sélectionnez cette mise à jour.

Une description de la mise à jour et des messages d'erreur éventuels sont affichés dans le panneau de droite de la page **Afficher l'historique des mises à jour**.

## Restauration de mises à jour masquées

Vous pouvez supprimer des mises à jour depuis la page **Vérifier les mises à jour**. Vous pouvez afficher et restaurer les mises à jour masquées sur la page **Restaurer les mises à jour masquées**.


### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Cliquez sur **Restaurer les mises à jour masquées**.
4. Facultatif : Pour localiser une mise à jour par nom, entrez un mot clé dans la zone **Rechercher par nom** et appuyez sur Entrée.
5. Sélectionnez la mise à jour masquée que vous souhaitez restaurer.
6. Cliquez sur **Restaurer**.

## Affichage du journal des mises à jour automatiques

Le journal des mises à jour automatiques contient la mise à jour automatique la plus récente effectuée sur votre système.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
3. Dans le menu de navigation, cliquez sur **Afficher le journal**.

## Mises à jour manuelles

---

Si votre déploiement inclut une console IBM QRadar qui n'est pas en mesure d'accéder à Internet ou que vous souhaitez gérer manuellement les mises à jour de votre système, vous pouvez gérer manuellement le processus de mise à jour en configurant un serveur de mise à jour IBM QRadar.

Le package autoupdate inclut tous les fichiers nécessaires pour configurer manuellement un serveur de mises à jour en plus des fichiers de configuration système nécessaires pour chaque mise à jour. Après la configuration initiale, vous devez uniquement télécharger et décompresser le package autoupdate le plus actuel pour mettre à jour manuellement votre configuration.

Vous pouvez vous abonner aux notifications dans [IBM Fix Central](http://www.ibm.com/support/fixcentral/) ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)) pour recevoir la notification des nouvelles mises à jour.

### Concepts associés

#### Mises à jour automatiques

Vous pouvez mettre à jour automatiquement ou manuellement vos fichiers de configuration pour vous assurer que vos fichiers de configuration contiennent les informations de sécurité réseau les plus récentes.

## Configuration d'un serveur de mises à jour

Configurez un serveur Apache en tant que serveur de mise à jour pour votre déploiement IBM QRadar.


### Avant de commencer

Téléchargez le package de mise à jour automatique depuis [Fix Central](http://www.ibm.com/support/fixcentral/) ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)). Vous pouvez trouver des produits QRadar dans le **Groupe de produits** des systèmes de sécurité.

### Procédure

1. Accédez à votre serveur Apache et créez un répertoire de mise à jour nommé autoupdates/.  
Par défaut, le répertoire de mise à jour se trouve dans le répertoire racine web du serveur Apache. Vous pouvez placer le répertoire dans un autre emplacement si vous configurez IBM QRadar en conséquence.
2. Facultatif : Créez un compte utilisateur Apache et un mot de passe à utiliser par le processus de mise à jour.
3. Enregistrez le fichier de package de mise à jour automatique sur votre serveur Apache dans le répertoire autoupdates/ que vous avez créé.
4. Sur le serveur Apache, entrez la commande suivante pour décompresser le package de mise à jour automatique.

```
tar -zxf updatepackage-[timestamp].tgz
```

5. Dans le menu de navigation () , cliquez sur **Admin**.
6. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
7. Cliquez sur **Modifier les paramètres**, puis sur l'onglet **Avancé**.
8. Dans la sous-fenêtre **Configuration du serveur**, configurez les paramètres du serveur Apache.
  - a) Dans la zone **Serveur Web**, entrez l'adresse ou le chemin de répertoire de votre serveur Apache.  
Si le serveur Apache s'exécute sur des ports non standard, ajoutez le numéro de port à la fin de l'adresse. Par exemple, entrez `http://my-auto-update-server.com:8080/`.
  - b) Dans la zone **Répertoire**, entrez l'emplacement du répertoire dans lequel le serveur Web stocke les mises à jour.  
Le répertoire par défaut est autoupdates/.
  - c) Facultatif : Si le serveur d'applications utilise un serveur proxy pour se connecter à Internet, entrez l'URL dans la zone **Serveur proxy**.
  - d) Facultatif : Si vous utilisez un proxy authentifié, entrez les données d'identification dans les zones **Nom d'utilisateur du proxy** et **Mot de passe proxy**.
9. Cliquez sur **Sauvegarder**.



10. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.
11. À l'aide de SSH, connectez-vous à QRadar en tant que superutilisateur.
12. Entrez la commande suivante pour configurer le nom d'utilisateur que vous avez défini pour votre serveur Apache :

```
/opt/qradar/bin/UpdateConfs.pl -change_username <username>
```

13. Entrez la commande suivante pour configurer le mot de passe que vous avez défini pour votre serveur Apache :

```
/opt/qradar/bin/UpdateConfs.pl -change_password <password>
```

14. Pour tester le serveur de mises à jour, entrez la commande suivante sous la forme d'une seule ligne de texte dans l'interface de ligne de commande.

```
wget -q -O- --no-check-certificate  
https://<your update server>/<directory path to updates>/manifest_list
```

15. Entrez votre nom d'utilisateur et votre mot de passe.

### Information associée

[QRadar: Important auto update server changes for administrators](#)

## Configuration de la console QRadar en tant que serveur de mise à jour

Pour rationaliser votre processus de maintenance, vous pouvez configurer votre QRadar Console pour qu'il soit votre serveur de mise à jour de sorte que les mises à jour QRadar soient automatiquement téléchargées sur la console.

### Procédure

1. Téléchargez le module de mise à jour automatique à partir de [Fix Central](http://www.ibm.com/support/fixcentral/) (www.ibm.com/support/fixcentral/).  
Vous pouvez trouver des produits QRadar dans la liste Systèmes de sécurité **Groupe de produits** sur Fix Central.
2. Enregistrez le fichier du module de mise à jour automatique dans le répertoire /tmp/ de votre QRadar Console.

**Remarque :** La taille du fichier de mise à jour automatique est d'environ 2-5 Go.

3. Connectez-vous à QRadar en tant que superutilisateur.
4. Vérifiez si le dossier /opt/qradar/www/autoupdates existe. Si ce dossier existe, supprimez-le avant de terminer l'étape 5.
5. Créez un lien symbolique vers /opt/qradar/www/autoupdates en entrant la commande suivante :

```
mkdir -p /store/downloads/autoupdates; ln -s /store/downloads/autoupdates /opt/qradar/www
```

6. Pour vérifier que le lien symbolique a été correctement créé, entrez la commande suivante :


```
touch /store/downloads/autoupdates/testfile
```

7. Confirmez que la valeur du fichier de test est créée dans le répertoire /opt/qradar/www/autoupdates en entrant la commande suivante :

```
ls /opt/qradar/www/autoupdates
```

8. Copiez le fichier autoupdates-<version>.tgz du répertoire /tmp/ vers le répertoire QRadar Console, puis placez-le dans le répertoire /opt/qradar/www/autoupdates/ ou le répertoire de liens symboliques que vous avez créé à l'étape 6.
9. Sur QRadar Console, entrez les commandes suivantes pour extraire le module de mise à jour automatique :

```
cd /opt/qradar/www/autoupdates/  
tar -zxf /tmp/<name_of_autoupdate_file>
```

10. Connectez-vous à QRadar.
11. Dans le menu de navigation () , cliquez sur **Admin**.
12. Dans la section **Configuration système**, cliquez sur **Mise à jour automatique**.
13. Cliquez sur **Modifier les paramètres**, puis sélectionnez **Onglet Avancé**.
14. Dans la zone **Répertoire**, entrez `autoupdates/`.
15. Dans la zone **Serveur Web**, entrez `https://<console_IP_address_or_hostname>`.
16. Cliquez sur **Sauvegarder**.

## Téléchargement des mises à jour du serveur de mises à jour

Vous pouvez télécharger les mises à jour depuis Fix Central vers votre serveur de mises à jour.

### Avant de commencer

Vous devez configurer votre serveur de mises à jour et configurer IBM QRadar pour recevoir les mises à jour à partir du serveur de mises à jour.

### Procédure

1. Téléchargez le package autoupdate à partir de [IBM Fix Central](http://www.ibm.com/support/fixcentral/) (<http://www.ibm.com/support/fixcentral/>).

Vous pouvez trouver des produits QRadar dans la liste Systèmes de sécurité **Groupe de produits** sur Fix Central.

2. Enregistrez le fichier de package de mise à jour automatique sur votre serveur de mises à jour dans le répertoire `autoupdates/` que vous avez créé.
3. Entrez la commande suivante pour décompresser le package de mise à jour automatique :

```
tar -zxf autoupdate-[timestamp].tgz
```

4. Connectez-vous à QRadar en tant que superutilisateur.
5. Entrez la commande suivante pour tester votre serveur de mises à jour :


```
wget https://<your_update_server>/<directory_path_to_updates>/manifest_list
```

6. Entrez le nom d'utilisateur et le mot de passe de votre serveur de mises à jour.

## Configuration des paramètres système

Les paramètres système indiquent comment les composants du système IBM QRadar sont configurés pour une opération normale.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Paramètres de système**.
3. Configurez les paramètres système. Cliquez sur le bouton **Aide** pour consulter la description des paramètres.
4. Cliquez sur **Sauvegarder**.
5. Dans l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas

automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Personnalisation du menu contextuel

Pour fournir un accès rapide aux fonctions liées aux adresses IP, personnalisez les options de plug-in dans le menu contextuel de l'adresse IP. Par exemple, vous pouvez ajouter d'autres éléments de menu, par exemple une option permettant de rechercher l'adresse IP dans une base de données de sécurité.

### Pourquoi et quand exécuter cette tâche

Le fichier `ip_context_menu.xml` contrôle les options disponibles dans le menu contextuel et accepte les éléments XML `menuEntry`. Pour ajouter plus d'options, ajoutez un élément `menuEntry` pour chaque option de clic droit que vous souhaitez ajouter. La syntaxe de l'élément `menuEntry` est la suivante :

```
<menuEntry name="{Name}" description="{Description}" url="{URL}"
requiredCapabilities="{Required Capabilities}"/>
<menuEntry name="{Name}" description="{Description}"
exec="{Command}" requiredCapabilities="{Required Capabilities}"/>
```

La liste suivante décrit les attributs de l'élément `menuEntry` :

#### Nom

Texte affiché dans le menu contextuel.

#### Description

Description de l'entrée. Le texte de la description s'affiche dans l'infobulle de l'option de menu. Cette description est facultative.

#### URL

Indique l'adresse Web qui s'ouvre dans une nouvelle fenêtre.

Vous pouvez utiliser la marque de réservation `%IP%` pour représenter l'adresse IP. Le caractère perluète (`&`), le signe inférieur (`<`) et le signe supérieur (`>`) doivent être échappés en utilisant les chaînes `&amp;`, `&lt;` et `&gt;`, respectivement.

Par exemple, pour transmettre une URL avec de multiples paramètres incluant une marque de réservation pour l'adresse IP, vous pouvez utiliser cette syntaxe : `url="/lookup?&amp;ip=%IP%;force=true"`

#### Commande

Une commande que vous souhaitez exécuter sur IBM QRadar Console. Le résultat de la commande s'affiche dans une nouvelle fenêtre. Utilisez la marque de réservation, `%IP%`, pour représenter l'adresse IP qui est sélectionnée.

#### Capacités requises

Toutes les fonctions, par exemple « ADMIN », que l'utilisateur doit avoir avant de sélectionner cette option, délimitée par des virgules. Si l'utilisateur ne dispose pas de toutes les fonctions répertoriées, les entrées ne sont pas affichées. Les fonctions requises sont un champ facultatif. Pour plus d'informations sur les fonctions requises, voir le *IBM QRadar Application Framework Developer Quick Start Guide*.

Le fichier édité ressemble à l'exemple suivant :

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This is a configuration file to add custom actions into
the IP address right-click menu. Entries must be of one of the
following formats: -->
<contextMenu>
<menuEntry name="Traceroute" exec="/usr/sbin/traceroute %IP%" />
<menuEntry name="External ARIN Lookup"
url="http://ws.arin.net/whois/?queryinput=%IP%" />
</contextMenu>
```

**Important :** L'appel de scripts ou de programmes de shell à partir du menu contextuel ou de toute autre interface Web peut introduire des vulnérabilités de sécurité, telles que des attaques par injection de

commande de système d'exploitation ou des attaques de traversée de chemins. Envisagez des méthodes plus sécurisées, telles que l'implémentation d'une extension d'application QRadar.

## Procédure

1. À l'aide de SSH, connectez-vous à QRadar Console en tant qu'utilisateur racine.
2. Sous QRadar Console, si le fichier `ip_context_menu.xml` n'existe pas sous le répertoire `/opt/qradar/conf`, copiez le fichier `ip_context_menu.xml` du répertoire `/opt/qradar/conf/templates` vers le répertoire `/opt/qradar/conf`.
3. Ouvrez le fichier `/opt/qradar/conf/ip_context_menu.xml` pour l'éditer.
4. Éditez le fichier pour ajouter, modifier ou supprimer des éléments XML `menuEntry`.
5. Sauvegardez le fichier et fermez-le.
6. Pour appliquer ces modifications, redémarrez l'interface graphique QRadar en entrant la commande suivante :

```
systemctl restart tomcat
```

## Amélioration du menu contextuel pour les colonnes d'événements et de flux

Vous pouvez ajouter d'autres actions aux options de clic droit disponibles sur les colonnes du tableau **Activité de journal** ou du tableau **Activité réseau**. Par exemple, vous pouvez ajouter une option pour afficher plus d'informations sur l'adresse IP source ou la adresse IP de destination.

**Restriction :** La fonction de clic droit n'est pas disponible dans les zones de la fenêtre **Informations sur les événements**.

Vous pouvez transmettre toutes les données de l'événement ou du flux à l'URL ou au script.

## Procédure

1. À l'aide de SSH, connectez-vous au dispositif QRadar Console en tant qu'utilisateur racine
2. Accédez au répertoire `/opt/qradar/conf` et créez un fichier nommé `arielRightClick.properties`.
3. Éditez le fichier `/opt/qradar/conf/arielRightClick.properties`. Utilisez le tableau suivant pour spécifier les paramètres qui déterminent les options du menu contextuel.


*Tableau 19. Description des `arielRightClick.properties` paramètres de fichier*

Paramètre	Configuration requise	Description	Exemple
<b>pluginActions</b>	Obligatoire	Indique une URL ou une action de script.	
<b>arielProperty</b>	Obligatoire	Indique la colonne ou le nom de zone Ariel pour lequel le menu contextuel est activé.	<b>SourceIp</b> <b>SourcePort</b> <b>DestinationIp</b> <b>qid</b>
<b>text</b>	Obligatoire	Indique le texte affiché dans le menu contextuel.	Recherche Google
<b>useFormattedValue</b>	Facultatif	Indique si les valeurs formatées sont transmises au script.  Définissez sur <code>true</code> pour vous assurer que la valeur formatée pour les attributs, tels que <code>username</code> et <code>payload</code> , est transmise. Les valeurs formatées sont plus faciles à lire pour les administrateurs que les valeurs non formatées.	Si le paramètre est défini sur <code>true</code> pour la propriété Nom d'événement (QID), le nom d'événement de QID est transmis au script.  Si le paramètre est défini sur <code>false</code> , la valeur QID brute non formatée est transmise au script.

Tableau 19. Description des `arielRightClick`. propriétés paramètres de fichier (suite)

Paramètre	Configuration requise	Description	Exemple
<code>url</code>	Requis pour accéder à une URL	Indique l'URL, qui s'ouvre dans une nouvelle fenêtre, et les paramètres à transmettre à l'URL. Utilisez un format : <code>\$Ariel_Field Name\$</code>	<code>sourceIPwebUrlAction.url=http://www.mywebsite.com?q=\$sourceIP\$</code>
<code>command</code>	Obligatoire si l'action est une commande	Indique le chemin absolu de la commande ou du fichier script.	<code>destinationPortScriptAction.command=/bin/echo</code>
<code>arguments</code>	Obligatoire si l'action est une commande	Indique les données à transmettre au script. Utilisez le format suivant : <code>\$Ariel_Field Name\$</code>	<code>destinationPortScriptAction.arguments=\$qid\$</code>

Pour chacun des noms de clé spécifiés dans la liste `pluginActions`, définissez l'action à l'aide d'une clé avec le format `key name, property`.

4. Sauvegardez le fichier et fermez-le.
5. Connectez-vous à l'interface utilisateur QRadar.
6. Dans le menu de navigation () , cliquez sur **Admin**.
7. Cliquez sur **Avancé** > **Redémarrer le serveur Web**.

### Exemple

L'exemple suivant montre comment ajouter `URL de test` en tant qu'option de clic droit pour les adresses IP source.

```
pluginActions=sourceIPwebUrlAction
sourceIPwebUrlAction.arielProperty=sourceIP
sourceIPwebUrlAction.text=Test URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$
```

L'exemple suivant montre comment activer l'action de script pour les ports de destination.

```
pluginActions=destinationPortScriptAction
destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Test Unformatted Command
destinationPortScriptAction.useFormattedValue=false
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=$qid$
```

L'exemple suivant montre l'ajout de plusieurs paramètres à une URL ou à une action de scriptage.

```
pluginActions=qidwebUrlAction,sourcePortScriptAction
qidwebUrlAction.arielProperty=qid,device,eventCount
qidwebUrlAction.text=Search on Google
qidwebUrlAction.url=http://www.google.com?q=$qid$-$device$-$eventCount$
sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Port Unformatted Command
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=$qid$-$sourcePort$-$device$-$CONTEXT$
```

## Présentation des valeurs de conservation des actifs

Informations supplémentaires pour la période, en jours, que vous souhaitez stocker les informations de profil d'actif.

- Les actifs sont testés par rapport aux seuils de rétention à intervalles réguliers. Par défaut, l'intervalle de nettoyage est de 12 heures.
- Toutes les périodes de conservation spécifiées sont relatives à la dernière date d'observation de l'information, que l'information ait été vue pour la dernière fois par un scanner ou qu'elle ait été observée passivement par le système.
- Les informations sur les actifs sont supprimées au fur et à mesure de leur expiration, ce qui signifie qu'après un intervalle de nettoyage, toutes les informations sur les actifs restent à l'intérieur de leur seuil de conservation.
- Par défaut, les actifs associés à des vulnérabilités non corrigées (telles que détectées par IBM QRadar Vulnerability Manager ou un autre scanner) sont conservés.
- Les actifs peuvent toujours être supprimés manuellement via l'interface utilisateur.

*Tableau 20. Composants de l'actif*

<b>Composant d'actif</b>	<b>Conservation par défaut (en jours)</b>	<b>Remarques</b>
Adresse IP	120 jours	Par défaut, les adresses IP fournies par l'utilisateur sont conservées jusqu'à ce qu'elles soient supprimées manuellement.
Adresses MAC (Interfaces)	120 jours	Par défaut, les interfaces fournies par l'utilisateur sont conservées jusqu'à ce qu'elles soient supprimées manuellement.
Noms d'hôte DNS et NetBIOS	120 jours	Par défaut, les noms d'hôte fournis par l'utilisateur sont conservés jusqu'à ce qu'ils soient supprimés manuellement.

Tableau 20. Composants de l'actif (suite)

Composant d'actif	Conservation par défaut (en jours)	Remarques
Propriétés d'alerte	120 jours	<p>Par défaut, les adresses IP fournies par l'utilisateur sont conservées jusqu'à ce qu'elles soient supprimées manuellement.</p> <p>Les propriétés de l'actif que cette valeur peut affecter sont <b>Prénom, Nom unifié, Poids, Description, Propriétaire métier, Contact commercial, Propriétaire technique, Contact technique, Emplacement, Confiance en détection, PA sans fil, SSID sans fil, ID commutateur, ID du port de commutation, Exigence de confidentialité CVSS, Exigence d'intégrité CVSS, Exigence de disponibilité CVSS, Potentiel de dommages collatéraux CVSS, Utilisateur technique, Système d'exploitation fourni par l'utilisateur, Type de remplacement du système d'exploitation, ID de substitution du système d'exploitation, Etendu, Risque Cvss d'archivage (Pre-7.2), VLAN et Type d'actif.</b></p>
Produits d'actif	120 jours	<p>Par défaut, les produits fournis par l'utilisateur sont conservés jusqu'à ce qu'ils soient supprimés manuellement.</p> <p>Les produits d'actif comprennent Asset OS, Asset Installed Applications et des produits associés à des ports d'actifs ouverts.</p>
Ports « ouverts » de l'actif	120 jours	
Groupes NetBIOS d'actifs	120 jours	<p>Les groupes NetBIOS sont rarement utilisés et plus de clients peuvent ne pas être au courant de leur existence. Dans le cas où ils sont utilisés, ils sont supprimés après 120 jours.</p>
Application Client d'actif	120 jours	<p>Les applications client ne sont pas encore exploitées dans l'interface utilisateur. Cette erreur peut être ignorée.</p>


Tableau 20. Composants de l'actif (suite)

Composant d'actif	Conservation par défaut (en jours)	Remarques
Utilisateurs d'actifs	30 jours	

## Ajout ou édition d'un message de connexion QRadar

Créez un nouveau message de connexion ou éditez un message de connexion existant sur votre console IBM QRadar.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des utilisateurs**.
3. Cliquez sur **Authentification**, puis sur **Paramètres d'authentification généraux**.
4. Pour modifier le message de connexion, cliquez sur **Page de connexion**, puis définissez **Message de connexion** sur **On**.
  - a) Entrez votre message dans la fenêtre **Editer l'invite de connexion**.
  - b) Pour forcer les utilisateurs à consentir au message de connexion avant de pouvoir se connecter, définissez **Exiger un consentement explicite de ce message pour la connexion** sur **On**.
  - c) Cliquez sur **Save Settings**.

Le message de connexion est enregistré dans le fichier `opt/qradar/conf/loginMessage.txt`.

**Remarque :** Vous pouvez également télécharger le fichier `loginMessage.txt` dans le répertoire `opt/qradar/conf/`.

5. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.
6. Pour afficher vos modifications, déconnectez-vous de QRadar.

## Activation et configuration de la visualisation des performances des règles

Utilisez la fonction **Paramètres de règle personnalisés** pour activer et configurer des mesures pour l'analyse des performances des règles. La visualisation des performances des règles étend la journalisation actuelle sur la dégradation des performances et les règles personnalisées consommatrices dans le pipeline QRadar. Avec la visualisation des performances des règles, vous pouvez déterminer l'efficacité des règles dans le pipeline QRadar directement à partir de la page **Règles**.

### Pourquoi et quand exécuter cette tâche

Une fois que vous avez effectué la visualisation des performances des règles, les mesures restent vides à moins qu'un problème de performances d'événement ou de flux ne se produise.

### Procédure



1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Paramètres de système**.
3. Sur la page **Paramètres système**, cliquez sur **Avancé**.
4. Configurez **Paramètres de règle personnalisés**.



Tableau 21. Paramètres de règles personnalisées	
Paramètre	Description
<b>Activer l'analyse des performances</b>	Permet d'analyser les performances et le coût des règles personnalisées La valeur par défaut est False.
<b>Réinitialiser les métriques lors du changement de règle</b>	Active la remise à zéro des métriques d'analyse des performances des règles lorsqu'une règle est modifiée. La valeur par défaut est True.  <b>Conseil :</b> Pour réinitialiser les mesures d'une règle, modifiez la règle, puis enregistrez-la. Les mesures de la règle que vous avez modifiée sont supprimées.
<b>Limite haute pour l'analyse des performances</b>	La limite haute (en EPS ou FPS) utilisée pour déterminer la valeur de la barre de performance pour une règle.  <ul style="list-style-type: none"> <li>• Si le débit d'une règle est en dessous de cette limite tout en restant au-dessus de la <b>Limite basse pour l'analyse des performances</b>, la performance est figurée par deux barres oranges.</li> <li>• Si le débit d'une règle est au-dessus de cette limite, la performance est affichée sous la forme de trois barres vertes.</li> </ul> La valeur par défaut est 50 000.
<b>Limite basse pour l'analyse des performances</b>	La limite basse (en EPS ou FPS) utilisée pour déterminer la valeur de la barre de performance pour une règle. Si le débit d'une règle tombe en-deçà de cette limite, la performance est affichée sous la forme d'une unique barre rouge.  La valeur par défaut est 12 500.

5. Cliquez sur **Sauvegarder**.
6. Dans le menu de navigation () , cliquez sur **Admin**.
7. Cliquez sur **Déployer les changements**.

## Résultats

Lorsque la visualisation des performances des règles est activée, la colonne **Performances** est ajoutée à la page **Règles**. La colonne **Performances** de la page **Règles** est vide jusqu'à ce qu'un problème de performances se produise dans le moteur de règles personnalisé.

Pour plus d'informations sur la visualisation des performances des règles, voir le *IBM QRadar - Guide d'utilisation*.

## Identification et résolution des incidents de la visualisation des performances de règles

Cette référence fournit des informations d'identification et de résolution des incidents pour la visualisation des performances des règles.

## Pourquoi ne pas voir des indicateurs pour une règle ?

Problème	Solution
L'analyse des performances n'est pas activée.	Appliquez les modifications.
Les indicateurs ne s'affichent pas pour les règles qui ne sont pas activées.	Fonctionne comme prévu. L'affichage des métriques s'affiche uniquement pour les règles activées.
Les mesures ne s'affichent pas pour les règles de violation.	Fonctionne comme prévu. Les indicateurs sont recueillis uniquement pour tous les événements, les règles communes et les règles de flux.
Les indicateurs ne s'affichent pas pour une règle.	La règle peut être modifiée récemment, ce qui réinitialise les indicateurs. Les mesures de la règle que vous avez modifiée sont supprimées. Si vous ne souhaitez pas que la mesure soit réinitialisée lorsqu'une règle est redéfinie, désactivez <b>Réinitialiser les indicateurs lors du changement de règle</b> .

## Pourquoi vouloir modifier les seuils supérieurs et inférieurs ?

Si vous souhaitez modifier les limites de seuil supérieur et inférieur, cela dépend de ce que vous considérez comme un événement acceptable par seconde (EPS) ou un débit par seconde (FPS) pour vos règles. Vous pouvez commencer par le débit de votre système général EPS ou FPS. Augmentez votre limite supérieure de seuil de quelques milliers et diminuez votre limite inférieure de quelques milliers. Lorsque vous modifiez ces paramètres, gardez à l'esprit vos limitations de débit de licence et de matériel. Votre limite supérieure n'a pas besoin d'être supérieure à la capacité de votre licence ou de votre matériel. En règle générale, lorsque vous utilisez cette fonction pour ajuster vos règles, vous pouvez mettre à jour la limite inférieure avec une valeur légèrement plus élevée, de sorte de pouvoir vous concentrer sur les règles de sous-exécution.

Exemple :

- Charge générale EPS pour le système : 5 000 EPS
- Limite supérieure : 8 000 EPS
- Limite inférieure : 2 000 EPS

Les règles pouvant traiter 8 001 EPS ou plus affichent trois barres vertes. Les règles qui ne peuvent traiter que 1 999 EPS ou moins affichent 1 barre rouge. Toutes les règles entre ces gammes sont marquées de deux barres orange. Une fois que vous avez optimisé toutes vos règles qui affichent des barres rouges et que seules les barres orange et verte s'affichent, vous pouvez augmenter la limite inférieure à 3 000 EPS.

## Pourquoi une règle désactivée est-elle aussi chère ?

Lorsque les performances de la règle sont activées, les valeurs précédentes peuvent s'afficher pour les règles désactivées, ce qui peut entraîner le coût supérieur de la règle.

Si vous avez sélectionné **Réinitialiser les indicateurs sur le changement de règle** lorsque vous avez activé les performances des règles, réinitialisez les mesures de la règle en modifiant la règle, puis en l'enregistrant. Les mesures de la règle que vous avez modifiée sont supprimées.

Vous pouvez afficher les métriques d'une règle sur la page **Règles** lorsque vous déplacez le pointeur de la souris sur les barres colorées dans la colonne **Performances** ainsi que dans la zone de texte **Analyse des performances** qui se trouve dans le coin inférieur droit de la page **Règles**. Vous pouvez également afficher les métriques d'une règle dans l'**Assistant Règle** lorsque vous éditez une règle. L'horodatage de

la zone de texte **Analyse des performances** indique le moment où les métriques de la règle ont été mises à jour.



Figure 7. Horodatage dans la zone de texte Analyse des performances

Pour plus d'informations sur la modification des règles, voir le document *IBM QRadar - Guide d'utilisation*.

## Certificats de serveur IF-MAP

La réponse de règle Interface For Metadata Access Points (IF-MAP) permet à la console IBM QRadar de publier des données d'alerte et de d'infraction dérivées d'événements, de flux et d'infractions sur un serveur IF-MAP.

Avant de pouvoir configurer l'authentification IF-MAP dans la fenêtre **Paramètres système**, vous devez configurer votre certificat de serveur IF-MAP.

### Configuration du certificat de serveur IF-MAP pour l'authentification de base

Dans cette tâche, vous apprendrez à configurer votre certificat IF-MAP pour l'authentification de base.

#### Avant de commencer

Contactez votre administrateur de serveur IF-MAP pour obtenir une copie du certificat public du serveur IF-MAP. Le certificat doit avoir l'extension de fichier `.cert`.

#### Procédure

1. À l'aide de SSH, connectez-vous à IBM QRadar en tant que superutilisateur.
2. Copiez le certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`.

### Configuration du certificat de serveur IF-MAP pour l'authentification mutuelle

L'authentification mutuelle requiert une configuration de certificat sur votre console IBM QRadar et sur votre serveur IF-MAP.

Cette tâche permet de configurer le certificat sur votre console QRadar. Pour obtenir de l'aide sur la configuration du certificat sur votre serveur IF-MAP, contactez votre administrateur de serveur IF-MAP.

#### Avant de commencer

Contactez votre administrateur de serveur IF-MAP pour obtenir une copie du certificat public du serveur IF-MAP. Le certificat doit avoir l'extension de fichier `.cert`.

#### Procédure

1. À l'aide de SSH, connectez-vous à IBM QRadar en tant que superutilisateur.
2. Accéder au certificat dans le répertoire `/opt/qradar/conf/trusted_certificates`
3. Copiez le certificat intermédiaire SSL et le certificat racine SSL Verisign sur votre serveur IF-MAP en tant que certificats de l'autorité de certification. Pour obtenir de l'aide, contactez votre administrateur de serveur IF-MAP.

4. Entrez la commande suivante pour créer le fichier Public-Key Cryptography Standards avec l'extension de fichier .pkcs12 :

```
openssl pkcs12 -export -inkey <private_key> -in <certificate> -out  
<pkcs12_filename.pkcs12> -name "IFMAP Client"
```

5. Entrez la commande suivante pour copier le fichier pkcs12 dans le répertoire /opt/qradar/conf/key\_certificates :

```
cp <pkcs12_filename.pkcs12> /opt/qradar/conf/key_certificates
```

6. Créez un client sur le serveur IF-MAP avec l'authentification de certificat et téléchargez le certificat SSL. Pour obtenir de l'aide, contactez votre administrateur de serveur IF-MAP.
7. Entrez la commande suivante pour modifier les droits d'accès du répertoire :

```
chmod 755 /opt/qradar/conf/trusted_certificates  
chmod 644 /opt/qradar/conf/trusted_certificates/*.cert
```

8. Tapez la commande suivante pour redémarrer le service Tomcat :

```
systemctl restart tomcat
```

## Certificats SSL

---

Secure Sockets Layer (SSL) est un protocole de sécurité de l'industrie qui est utilisé par les sites Web pour protéger les transactions en ligne. Il fournit la confidentialité des communications afin que les applications client / serveur puissent communiquer d'une manière qui est conçue pour empêcher l'écoute, l'altération et la falsification de messages. Pour générer un lien SSL, un serveur Web requiert un certificat SSL. Les certificats SSL sont émis par des autorités de certification de tiers internes ou de confiance.

Les navigateurs et les systèmes d'exploitation incluent une liste préinstallée de certificats sécurisés, qui sont installés dans le magasin des autorités de certification racine de confiance.

### Certificat autosigné

Un certificat auto-signé fournit la sécurité de base, permettant le chiffrement des données entre l'utilisateur et l'application. Étant donné que les certificats d'auto-signature ne peuvent être authentifiés par aucune autorité de certification racine existante, les utilisateurs sont avertis de ce certificat inconnu et doivent l'accepter pour continuer.

### Certificats signés de l'autorité de certification interne

Les organisations ayant leur propre autorité de certification racine interne (CA) peuvent créer un certificat à l'aide de cette autorité de certification interne. Ce certificat est pris en charge par QRadar, et l'autorité de certification racine interne est également importée dans l'environnement QRadar.

### AC publique / AC intermédiaire signée

Les certificats signés par les autorités de certification publiques connues et les certificats intermédiaires sont pris en charge par QRadar.

Les certificats signés publics peuvent être utilisés directement dans QRadar, et les certificats signés avec l'autorité de certification intermédiaire sont installés à l'aide du certificat signé et du certificat intermédiaire pour fournir des fonctions de certificat valides.

**Remarque :** Un certificat intermédiaire est couramment utilisé par les organisations qui créent plusieurs clés SSL dans leur environnement et souhaitent les faire signer par un fournisseur de certificats commerciaux connu. Lorsqu'ils utilisent la clé intermédiaire, ils peuvent ensuite créer des sous-clés à partir de cette clé intermédiaire. Lorsque cette configuration est utilisée, QRadar doit être configuré avec le certificat intermédiaire et le certificat SSL de l'hôte de sorte que les connexions à l'hôte puissent vérifier le chemin complet du certificat.

## Connexions SSL entre les composants QRadar

Pour établir toutes les connexions SSL internes entre les composants, QRadar utilise le certificat du serveur Web préinstallé sur la console QRadar.

Tous les certificats sécurisés pour QRadar doivent répondre aux exigences suivantes :

- Le certificat doit être un certificat X.509 et avoir un codage PEM base64.
- Le certificat doit avoir une extension de fichier `.cert`, `.crt`, `.pem`, ou `.der`.
- Les fichiers de clés contenant des certificats doivent avoir l'extension de fichier `.truststore`.
- Le fichier de certificat doit être stocké dans le répertoire `/opt/qradar/conf/trusted_certificates`.

### Important :

Le remplacement d'un certificat SSL n'est pas pris en charge par QRadar Packet Capture et QRadar Network Packet Capture.

## Création d'une demande de signature de certificat SSL avec clés RSA 2048 bits

### Procédure

1. Utilisez SSH pour vous connecter à la console QRadar.
2. Générez un fichier de clés privées à l'aide de la commande suivante :

```
openssl genrsa -out qradar.key 2048
```

**Remarque :** N'utilisez pas les options de chiffrement privées, car elles peuvent entraîner des problèmes de compatibilité.

Le fichier `qradar.key` est créé dans le répertoire en cours. Conservez ce fichier à utiliser lorsque vous installez le certificat.

3. Générez le fichier de demande de signature de certificat (CSR).

Le fichier `qradar.csr` est utilisé pour créer le certificat SSL, avec une autorité de certification interne ou une autorité de certification commerciale. Exécutez la commande suivante et fournissez les informations nécessaires comme demandé :

```
openssl req -new -key qradar.key -out qradar.csr
```

Exemple de sortie :

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:MyState
Locality Name (eg, city) [Default City]:MyCity
Organization Name (eg, company) [Default Company Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyCompanyOrg
Common Name (eg, your name or your server's hostname) []:qradar.mycompany.com
Email Address []:username@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

4. Si vous souhaitez vérifier les informations du CSR avant de les envoyer, entrez la commande suivante :

```
openssl req -noout -text -in qradar.csr
```

Si des informations incorrectes ont été entrées, exécutez à nouveau la commande OpenSSL pour recréer le fichier CSR.

5. Utilisez le protocole Secure File Transfer ou un autre programme pour copier en toute sécurité le fichier CSR sur votre ordinateur.
6. Soumettez le CSR à votre autorité de certification interne ou commerciale pour la signature conformément à ses instructions.

**Remarque :** Le CSR est identifié comme un certificat au format Apache.

## Création d'une demande de signature de certificat SSL multidomaine (SAN)

### Procédure

1. Utilisez SSH pour vous connecter à la console QRadar.
2. Créez et enregistrez un fichier de configuration `sancert.conf` contenant les informations suivantes :

```
[ req ]
default_bits           = 2048 # RSA key size
encrypt_key           = no # Protect private key
default_md             = sha256 # MD to use
utf8                  = yes # Input is UTF-8
string_mask           = utf8only # Emit UTF-8 strings
prompt               = no # Prompt for DN
distinguished_name    = server_dn # DN template
req_extensions        = server_reqext # Desired extensions

[ server_dn ]
countryName           = <country_or_region_code> # ISO 3166
stateOrProvinceName  = <state_or_province>
localityName         = <city_or_locality>
organizationName     = <organization_name>
organizationalUnitName = <organizational_unit_name>
commonName           = <common_name> # Should match a SAN under alt_names

[ server_reqext ]
basicConstraints      = CA:FALSE
keyUsage              = critical,digitalSignature,keyEncipherment
extendedKeyUsage     = serverAuth
subjectKeyIdentifier = hash
subjectAltName       = @alt_names

[alt_names]
DNS.1                = qradar.example.com #Example
DNS.2                = console.example.com #Example
IP.3                 = 192.0.2.0 #Example
```

3. Générez une paire de clés privées et de demande de signature de certificat public (CSR) à l'aide de la commande suivante :

```
openssl req -new -nodes -sha256 -out <csr_filename>.csr -config sancert.conf
-keyout <privatekey_filename>.key
```

Le fichier CSR est utilisé pour créer le certificat SSL, avec une autorité de certification interne ou une autorité de certification commerciale. Le fichier de clés est créé dans le répertoire en cours. Conservez ce fichier à utiliser lorsque vous installez le certificat.

4. Si vous souhaitez vérifier les informations du CSR avant de les envoyer, entrez la commande suivante :

```
openssl req -noout -text -in <csr_filename>.csr
```

Si des informations incorrectes ont été entrées, mettez à jour le fichier de configuration `sancert.conf` et répétez l'étape précédente.

5. Utilisez le protocole Secure File Transfer ou un autre programme pour copier en toute sécurité le fichier CSR sur votre ordinateur.

6. Soumettez le REA à votre autorité de certification interne ou commerciale pour signature, conformément à leurs instructions.

**Remarque :** Le CSR est identifié comme un certificat au format Apache.

## Utilisation de certificats signés par une autorité de certification interne

Si le certificat est émis par une autorité de certification interne et non par un fournisseur de certificat commercial, IBM QRadar doit être mis à jour pour inclure le certificat racine interne dans le magasin de certificats local pour la validation appropriée du certificat. Les certificats de vérification racine sont automatiquement inclus avec le système d'exploitation.

### Pourquoi et quand exécuter cette tâche

Procédez comme suit pour mettre à jour le magasin de certificats racine des ancrages de confiance dans RHEL sur la console QRadar et tous les hôtes QRadar.

### Procédure

1. Copiez le certificat racine de l'autorité de certification sur `/etc/pki/ca-trust/source/anchors/` sur la console QRadar.
2. Exécutez les commandes suivantes sur la ligne de commande SSH sur la console :

```
/opt/qradar/support/all_servers.sh -p /etc/pki/ca-trust/source/anchors/<root_certificate>  
-r /etc/pki/ca-trust/source/anchors
```

```
/opt/qradar/support/all_servers.sh -C update-ca-trust
```

## Installation d'un nouveau certificat SSL

Par défaut, IBM QRadar est configuré avec un certificat SSL (Security Sockets Layer) signé par une autorité de certification interne. Lorsque vous vous connectez à la console pour la première fois, un message d'avertissement vous invite à indiquer que votre connexion n'est pas sécurisée ou n'est pas privée. Vous pouvez remplacer le certificat SSL par votre propre certificat auto-signé, un certificat signé par une autorité de certification privée (CA) ou un certificat signé par une autorité de certification publique.

### Avant de commencer

Vous devez disposer des informations suivantes :

- Le fichier `SSLCertificateFile` qui vient d'être signé à partir de votre autorité de certification interne ou d'un fichier public.
- Clé privée `qradar.key` pour générer le fichier CSR (Certificate Signing Request).

**Restriction :** Une clé privée avec une phrase passe n'est pas prise en charge.

Pour supprimer la phrase passe de la clé de certificat, entrez la commande suivante :

```
openssl rsa -in key-with-passphrase.key -out key-without-passphrase.key
```

- Un certificat intermédiaire, s'il est utilisé par votre fournisseur de certificats.

**Conseil :** Si un certificat intermédiaire est utilisé, exécutez la commande `install-ssl-cert.sh` avec l'indicateur `-i` pour installer à la fois le nouveau certificat et le certificat intermédiaire. Lorsqu'elle est utilisée, elle demande trois chemins de fichier :

- `SSLCertificateFile`
- `SSLIntermediateCertificateFile`
- `SSLCertificateKeyFile`

Si vous utilisez un certificat de format DER, vous devez le convertir en certificat au format PEM en tapant la ligne de commande suivante :

```
openssl x509 -in <cert>.der -inform der -outform pem -out <cert>.pem
```

## Procédure

1. Utilisez SSH pour vous connecter à la console QRadar en tant qu'utilisateur racine. Installez le certificat en entrant la commande suivante :

```
/opt/qradar/bin/install-ssl-cert.sh
```

- a) À l'invite Chemin d'accès au fichier de clés publiques (SSLCertificateFile), entrez le chemin d'accès au fichier de clés publiques. Par exemple :

```
/root/new.certs/cert.cert
```

- b) À l'invite Chemin d'accès au fichier de clés privées (SSLCertificateKeyFile), entrez le chemin d'accès au fichier de clés privées. Par exemple :

```
/root/new.certs/qradar.key
```

Exemple de sortie :

```
You have specified the following:
    SSLCertificateFile of /root/new.certs/cert.cert
    SSLCertificateKeyFile of /root/new.certs/qradar.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? y
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
- Restarting httpd service ... (OK)
Restarting running services:
- Stopping hostcontext ... (OK)
- Restarting Tomcat ... (OK)
- Starting hostcontext ... (OK)
Updating deployment:
- Copying certificate to managed hosts
  * 192.0.2.0 ..... (OK)
- Restarting hostcontext on managed hosts
  * 192.0.2.0 ..... (OK)
The event collection service must be restarted if WinCollect is used in your environment.
Restart the event collection service now (y/[n])? y
- Restarting ecs-ec-ingress on managed hosts
  * 192.0.2.0 ..... (OK)
- Restarting ecs-ec-ingress on console ... (OK)
Fri Jan 17 10:33:42 EST 2020 [install-ssl-cert.sh] OK: Install SSL Cert Completed
```

**Remarque :** La collecte de données pour les événements et les flux s'arrête lorsque les services sont redémarrés.

2. Si vous installez un certificat qui n'a pas été généré par QRadar ou que vous réinstallez un certificat remplacé qui n'a pas été généré par QRadar, désactivez la structure de l'autorité de certification et remplacez automatiquement le certificat. Éditez le fichier `/opt/qradar/ca/conf.d/httpd.json` et définissez la propriété **CertSkip** sur `true` et la propriété **CertMonitorThreshold** sur `0`. Par exemple :

```
{
  "ServiceName": "httpd",
  "CertDir": "/etc/httpd/conf/certs",
  "CertName": "cert",
  "ServiceCommand": "/opt/qradar/bin/install-ssl-cert.sh --deploy",
  "CASkip": "true",
  "CertSkip": "true",
  "CertMonitorThreshold": 0
}
```



3. Si le certificat a été émis par une autorité de certification interne et non par un fournisseur de certificat commercial, copiez le certificat racine de l'autorité de certification dans `/etc/pki/ca-trust/source/anchors/`, puis exécutez la commande suivante :

```
update-ca-trust
```

Répétez cette étape sur tous les hôtes gérés.

4. Pour recharger le certificat SSL, redémarrez le conteneur docker sur l'hôte qui exécute vos applications en exécutant la commande suivante :

```
systemctl restart docker
```

## Résultats

Si le script `install-ssl-cert.sh` s'est terminé avec le message `OK: Install SSL Cert Completed`, le certificat a été installé avec succès. Si vous avez répondu `y` (oui) à l'invite pour reconfigurer Apache, vous n'avez pas besoin de faire autre chose. Sinon, vous devez déployer la configuration complète. Dans le menu de navigation (☰), cliquez sur **Admin**, puis sur **Avancé > Déployer la configuration complète**.

## Rétablissement de certificats générés par l'autorité de certification locale QRadar

Si vous avez des problèmes avec votre certificat, par exemple un nom incorrect ou une adresse IP, la date d'expiration transmise ou l'adresse IP ou le nom d'hôte sur votre console modifiée, procédez comme suit pour générer des certificats signés par l'autorité de certification locale QRadar.

### Procédure

1. Sauvegardez les certificats installés précédemment qui ne fonctionnent pas.

Les certificats existants sont détectés et signalés lors de l'exécution de la génération de certificats, ce qui peut entraîner l'arrêt du processus de génération.

```
mkdir /root/backup.certs/  
cp /etc/httpd/conf/certs/cert.* /root/backup.certs/
```

2. Mettez à jour les éléments suivants dans le fichier `/opt/qradar/ca/conf.d/httpd.json` :

- Redéfinissez **CertMonitorThreshold** sur sa valeur d'origine. Si la valeur d'origine n'est pas connue, supprimez le fichier de sorte que les valeurs par défaut soient utilisées.
- Définissez **CertSkip** sur `faux`.

3. Exécutez la commande `/opt/qradar/ca/bin/install_qradar_ssl_cert.sh` pour générer de nouveaux certificats.

## Adressage IPv6 dans les déploiements QRadar

Le traitement d'IPv4 et d'IPv6 est pris en charge pour la connectivité réseau et la gestion du logiciel et des équipements IBM QRadar. Quand vous installez QRadar, vous êtes invité à spécifier si votre protocole Internet relève d'IPv4 ou d'IPv6.

### Composants QRadar qui prennent en charge le traitement d'IPv6

Les composants QRadar suivants prennent en charge le traitement IPv6.

## Onglet Activité réseau

Etant donné que **Adresse source IPv6** et **Adresse de destination IPv6** ne sont pas des colonnes par défaut, elles ne sont pas automatiquement affichées. Pour afficher ces colonnes, vous devez les sélectionner lorsque vous configurez vos paramètres de recherche (définition de colonne).

Pour économiser de l'espace et de l'indexation dans un environnement source IPv4 ou IPv6, les zones d'adresses IP supplémentaires ne sont pas stockées ou affichées. Dans un environnement mixte IPv4 et IPv6, un enregistrement de flux contient à la fois des adresses IPv4 et IPv6.

Les adresses IPv6 sont prises en charge pour les deux types de données de paquets, notamment les données sFlow et les données NetFlow V9. Cependant, les anciennes versions de NetFlow peuvent ne pas prendre en charge IPv6.

## Onglet Activité du journal

Etant donné que **Adresse source IPv6** et **Adresse de destination IPv6** ne sont pas des colonnes par défaut, elles ne sont pas automatiquement affichées. Pour afficher ces colonnes, vous devez les sélectionner lorsque vous configurez vos paramètres de recherche (définition de colonne).

Les DSM peuvent analyser les adresses IPv6 à partir de la charge d'événement. Si un DSM ne peut pas analyser les adresses IPv6, une extension de source de journal peut analyser les adresses. Pour plus d'informations sur les extensions de source de journal, voir le *DSM Configuration Guide*.

## Recherche, regroupement et création de rapports sur les zones IPv6

Vous pouvez rechercher des événements et des flux en utilisant les paramètres IPv6 dans les critères de recherche.

Vous pouvez également grouper et trier les enregistrements d'événements et de flux basés sur les paramètres IPv6.

Vous pouvez créer des rapports basés sur des données issues de recherches basées sur IPv6.

## Règles personnalisées

Dans les règles personnalisées et les blocs de construction, les paramètres IP prennent en charge les adresses IPv4 et IPv6 sauf si le libellé d'un paramètre contient l'une ou l'autre adresse (par exemple, **SRC IPv6** ne prend en charge que les adresses IPv6).

## Modules de support de périphérique (DSM)

Les DSM peuvent analyser l'adresse source et de destination IPv6 à partir des charges d'événement.

## Déploiement de QRadar dans des environnements IPv6 ou mixtes

Pour vous connecter à QRadar dans un environnement IPv6 ou mixte, encapsuler l'adresse IP entre crochets. Par exemple, `https://[<IP Address>]`

Les environnements IPv4 et IPv6 peuvent utiliser un fichier hosts pour la conversion d'adresse. Dans un environnement IPv6 ou mixte, le client convertit l'adresse de la console en son nom d'hôte. Vous devez ajouter l'adresse IP de la console IPv6 au fichier `/etc/hosts` sur le client.

Les sources de flux, telles que NetFlow et sFlow, sont acceptées à partir des adresses IPv4 et IPv6. Les sources d'événements, telles que syslog et SNMP, sont acceptées à partir des adresses IPv4 et IPv6. Vous pouvez désactiver les superflux et le regroupement de flux dans un environnement IPv6.

**Restriction :** Par défaut, vous ne pouvez pas ajouter un hôte géré IPv4 uniquement à une console en mode mixte IPv6 et IPv4. Vous devez exécuter un script pour activer un hôte géré IPv4 uniquement.

## Limitations de traitement IPv6

Lorsque QRadar est déployé dans un environnement IPv6, les limitations suivantes sont connues :

- Certaines parties du déploiement QRadar ne tirent pas parti de la hiérarchie du réseau activé par IPv6, y compris la surveillance, la recherche et l'analyse.

- Aucun test de profil d'hôte dans les règles personnalisées pour les adresses IPv6.
- Pas d'indexation ou d'optimisation spécialisée des adresses IPv6.

### Tâches associées

Ajout d'un hôte géré IPv4-only dans un environnement à deux piles

Pour ajouter un hôte géré IPv4-only à une console à deux piles, vous devez exécuter des scripts pour préparer l'hôte géré et la console avant de pouvoir ajouter l'hôte géré à la console.

## Exemples de règles iptables avancées

Vous pouvez configurer vos règles iptables pour mieux contrôler l'accès à QRadar, restreindre les sources de données entrantes et rediriger le trafic. Les exemples suivants peuvent vous aider à mieux comprendre votre réseau en ajustant manuellement vos iptables.

### Blocage de l'accès à SSH avec iptables

Les consoles et les hôtes non gérés autorisent SSH à partir de n'importe quelle demande entrante. Lorsqu'un hôte est ajouté au déploiement, les hôtes gérés autorisent l'accès SSH à partir de QRadar Console, et la console conserve le port 22 ouvert pour les connexions entrantes. Vous pouvez limiter les connexions entrantes sur le port 22 en modifiant les règles iptables d'un hôte.

Vous pouvez bloquer l'accès SSH à partir d'autres hôtes gérés sur votre console, qui peuvent interrompre les connexions chiffrées.

```
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.41 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.59 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -j DROP
```

### Activation de l'ICMP sur les systèmes QRadar

Vous pouvez activer les réponses ping à partir de votre système QRadar en ajoutant la règle suivante au fichier `/opt/qradar/conf/iptables.pre`.

```
-A INPUT -p icmp -j ACCEPT
```

Exécutez le script suivant pour créer une entrée dans le fichier `/etc/sysconfig/iptables`.

**Important :** Vous pouvez limiter cette règle à un hôte spécifique en ajoutant le champ `-s source.ip.address`.

### Bloquer les sources de données indésirables

Vous pouvez bloquer une source de données telle qu'une source de journal ou une source de données Netflow, pendant une courte durée, au lieu de désactiver l'unité d'origine. Pour bloquer un hôte particulier, vous pouvez ajouter une entrée similaire à la suivante à `/opt/qradar/conf/iptables.pre`.

Bloquer un flux réseau à partir du routeur :

```
-A INPUT -p udp -s <IP Address> --dport 2055 -j REJECT
```

Bloquer un syslog depuis une autre source :

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

Bloquer un syslog à partir d'un sous-réseau spécifique :

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
```

```
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

## Réacheminement des tables iptables vers les ports syslog

Vous pouvez rediriger le trafic syslog sur des ports non standard vers le port 514 sur un QRadar Collecteur d'événements. Vous pouvez utiliser les étapes suivantes pour activer une règle iptables pour rediriger le port alternatif vers 514 sur le Collecteur d'événements.

1. Activez l'option NAT dans le noyau Linux en ajoutant ou en mettant à jour la ligne suivante dans le fichier `/etc/sysctl.conf`.

```
net.ipv4.ip_forward = 1
```

**Remarque :** Pour que les modifications prennent effet à la règle NAT, vous devrez peut-être redémarrer votre service.

2. Activez ipforwarding dans le noyau actif en cours.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

3. Ajoutez les lignes suivantes au `/opt/qradar/conf/iptables-nat.post`. Entrez le numéro de port que vous souhaitez rediriger en tant que `<portnumber>`.

```
-A PREROUTING -p udp --dport <portnumber> -j REDIRECT --to-ports 514  
-A PREROUTING -p tcp --dport <portnumber> -j REDIRECT --to-ports 514
```

4. Entrez la commande suivante pour régénérer vos iptables.

```
/opt/qradar/bin/iptables_update.pl
```

5. Créez le répertoire en entrant la commande suivante :

```
iptables -nvL -t nat
```

Le code suivant est un exemple de ce à quoi la sortie peut ressembler.

```
Chain PREROUTING (policy ACCEPT 140 packets, 8794 bytes) pkts bytes target  
prot opt in out source destination 0 0 REDIRECT udp -- * * 0.0.0.0/0  
0.0.0.0/0 udp dpt:10529 redir ports 514 0 0 REDIRECT tcp -- * * 0.0.0.0/0  
0.0.0.0/0 tcp dpt:10529 redir ports 514 Chain POSTROUTING (policy ACCEPT 207  
packets, 25772 bytes) pkts bytes target prot opt in out source destination  
Chain OUTPUT (policy ACCEPT 207 packets, 25772 bytes) pkts bytes target prot  
opt in out source destination
```

## Réacheminement du trafic syslog entrant

Vous pouvez utiliser votre QRadar Console comme passerelle de messages syslog pour rediriger des événements entrants, en configurant les règles dans iptables.

1. Activez la règle de transfert pour une source de journal sur votre Collecteur d'événements.
2. Définissez la destination de transfert du syslog TCP comme adresse IP de la console sur le port 7780.
3. À partir de la ligne de commande de la console, ajoutez la règle iptables suivante pour rediriger vers un autre hôte.

```
iptables -I OUTPUT --src 0/0 --dst 153.2.200.80 -p  
tcp --dport 7780 -j REDIRECT --to-ports 514
```

## Configuration des règles iptables

L'accès aux services réseau QRadar est d'abord contrôlé sur les hôtes avec iptables. Les règles iptables sont ajustées et configurées en fonction des exigences du déploiement. Les ports pour la recherche

d'Ariel, le streaming et les heures lorsque vous utilisez le chiffrement (tunneling) peuvent mettre à jour diverses règles iptables.

## Pourquoi et quand exécuter cette tâche

Vous pouvez configurer et vérifier les règles iptables pour IPv4 et IPv6. La procédure suivante indique comment vous pouvez régler vos iptables manuellement.

### Procédure

1. Connectez-vous à QRadar en tant que superutilisateur à l'aide de SSH.

Identifiant de connexion : <root>

Mot de passe : <password>

2. Entrez la commande suivante pour éditer le fichier prérègles iptables :

IPv4:

```
vi /opt/qradar/conf/iptables.pre
```

IPv6:

```
vi /opt/qradar/conf/ip6tables.pre
```

Le fichier iptables.pre de configuration s'affiche.

3. Entrez la commande suivante pour éditer le fichier iptables de post-règles :

IPv4:

```
vi /opt/qradar/conf/iptables.post
```

IPv6:

```
vi /opt/qradar/conf/ip6tables.post
```

Le fichier de configuration iptables.post s'affiche.

4. Ajoutez la règle suivante pour QRadar pour accéder à un numéro de port spécifique, où *Numéro\_port* est le numéro de port :

Pour accepter le trafic UDP pour une entrée de port spécifique :

```
-A INPUT -m udp -p udp --dport <portnumber> -j ACCEPT
```

Pour accepter le trafic TCP pour une entrée de port spécifique :

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport <portnumber> -j ACCEPT
```

5. Sauvegardez votre configuration iptables.

6. Exécutez le script suivant pour propager les modifications :

```
/opt/qradar/bin/iptables_update.pl
```

7. Entrez les commandes suivantes pour rechercher les tables iptables existantes :

IPv4:

```
iptables -L -n -v
```

IPv6:

```
ip6tables -L -n -v
```

## Conservation des données

Les segments de conservation définissent la durée de conservation des données d'événement et de flux dans IBM QRadar.

Lorsque QRadar reçoit des événements et des flux, chacun est comparé aux critères de filtrage du compartiment de conservation. Lorsqu'un événement ou un flux correspond à un filtre de compartiment

de conservation, il est stocké dans ce compartiment de conservation jusqu'à l'expiration de la période de la règle de suppression. La durée de conservation par défaut est de 30 jours. Une fois ce délai écoulé, les données sont immédiatement supprimées.

Les compartiments de conservation sont classés par ordre de priorité, de la rangée supérieure à la rangée inférieure. Un enregistrement est stocké dans le compartiment qui correspond aux critères de filtrage ayant la priorité la plus élevée. Si l'enregistrement ne correspond à aucun de vos compartiments de conservation configurés, l'enregistrement est stocké dans le compartiment de conservation par défaut, qui est toujours situé sous la liste des compartiments de conservation configurables.

## Données de titulaire

Vous pouvez configurer jusqu'à 10 compartiments de conservation pour des données partagées et jusqu'à 10 compartiments de conservation pour chaque titulaire.

Lorsque les données parviennent au système, elles sont évaluées afin de déterminer s'il s'agit de données partagées ou si les données appartiennent à un titulaire. Les données spécifiques à un titulaire sont comparées aux filtres de compartiment de conservation qui sont définis pour ce titulaire. Lorsque les données correspondent à l'un des filtres des baquets de conservation, les données y sont stockées jusqu'à l'expiration de la période de conservation.

Si vous ne configurez pas des compartiments de conservation pour le titulaire, les données sont automatiquement placées dans le compartiment de conservation par défaut de ce titulaire. La durée de conservation par défaut est de 30 jours sauf si vous configurez un compartiment de conservation spécifique au titulaire.

Pour plus d'informations sur la conservation des données des locataires, voir [«Règles de conservation des locataires»](#), à la page 274.

## Configuration des compartiments de conservation

Configurez les règles de conservation pour définir la durée nécessaire à IBM QRadar pour conserver les données d'événement et de flux, et ce qu'il faut faire lorsque ces données atteignent un certain âge.


### Pourquoi et quand exécuter cette tâche

Les modifications apportées aux filtres de compartiment de conservation sont appliquées immédiatement aux données entrantes. Par exemple, si vous avez configuré un compartiment de conservation pour conserver toutes les données de l'adresse IP source 10.0.0.0/8 pendant 1 jour et que vous éditez ultérieurement le filtre pour conserver les données de la source IP 192.168.0.1, la modification n'est pas rétroactive. Immédiatement après la modification du filtre, le compartiment de conservation dispose de 24 heures de données de 10.0.0.0/8, et toutes les données collectées après le changement de filtre sont 192.168.0.1.

La règle de conservation sur le compartiment est appliquée à toutes les données du compartiment, quels que soient les critères des filtres. A l'aide de l'exemple précédent, si vous avez modifié la règle de conservation de 1 jour à 7 jours, les données 10.0.0.0/8 et 192.168.0.1 dans le compartiment sont conservées pendant 7 jours.

Le **Distribution** d'un compartiment de conservation indique l'utilisation de l'intervalle de conservation en tant que pourcentage de la conservation totale des données dans tous vos compartiments de conservation. La distribution est calculée sur une base par locataire.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Conservation des événements** ou sur **Conservation du flux**.
3. Si vous avez configuré les locataires, dans la liste **Locataire**, sélectionnez le titulaire auquel vous souhaitez que le compartiment de conservation s'applique.

**Remarque :** Pour gérer les règles de conservation des données partagées dans une configuration multi-locataires, choisissez **N/A** dans la liste **Locataire**.

4. Pour configurer un nouveau compartiment de conservation, procédez comme suit :
  - a) Cliquez deux fois sur la première ligne vide de la table pour ouvrir la fenêtre **Propriétés de conservation**.
  - b) Configurez les paramètres du compartiment de conservation.

**En savoir plus sur les paramètres du compartiment de conservation :**

Propriétés	Description
<b>Nom</b>	Entrez un nom unique pour le compartiment de conservation.
<b>Conserver les données placées dans ce compartiment pour</b>	Période de conservation indiquant la durée de conservation des données. Lorsque la durée de conservation est atteinte, les données sont supprimées en fonction du paramètre <b>Delete data in this bucket</b> . QRadar ne supprime pas les données dans la durée de conservation.
<b>Supprimer les données de ce compartiment</b>	<p>Sélectionnez <b>Immédiatement après l'expiration de la durée de conservation</b> pour supprimer immédiatement les données correspondant au paramètre <b>Keep data placed in this bucket for</b>. Les données sont supprimées lors du processus de maintenance du disque planifié suivant, quelles que soient les exigences de stockage sur disque.</p> <p>Sélectionnez <b>Lorsque l'espace de stockage est requis</b> pour conserver les données qui correspondent au paramètre <b>Keep data placed in this bucket for</b> dans l'espace de stockage, jusqu'à ce que le système de surveillance du disque détecte que le stockage est requis.</p> <p>Les suppressions basées sur l'espace de stockage commencent lorsque l'espace disque libre tombe à 15 % ou moins, et les suppressions se poursuivent jusqu'à ce que l'espace disque disponible soit de 18 % ou que le cadre temporel défini dans la zone <b>Conserver les données placées dans ce compartiment pour</b> s'exécute. Par exemple, si l'espace disque utilisé atteint 85 % pour les enregistrements, les données sont supprimées jusqu'à ce que le pourcentage d'utilisation tombe à 82 %. Lorsque le stockage est requis, seules les données correspondant à la zone <b>Conserver les données placées dans ce compartiment pour</b> sont supprimées.</p> <p>Si le compartiment est défini sur <b>Supprimer les données de cet intervalle: immédiatement après l'expiration de la période de conservation</b>, aucune vérification d'espace disque n'est effectuée et la tâche de suppression supprime immédiatement toutes les données antérieures à la conservation.</p>
<b>Description</b>	Entrez une description pour le compartiment de conservation.
<b>Filtres en cours</b>	Configurez les critères de filtrage sur lequel chaque élément de données doit être comparé.

- c) Cliquez sur **Ajouter un filtre** après avoir spécifié chaque ensemble de critères de filtre.
  - d) Cliquez sur **Sauvegarder**.
5. Pour éditer un compartiment de conservation existant, sélectionnez la ligne dans la table et cliquez sur **Éditer**.
6. Pour supprimer un compartiment de conservation, sélectionnez la ligne dans la table et cliquez sur **Supprimer**.
7. Cliquez sur **Sauvegarder**.

Les données entrantes qui correspondent aux propriétés de la règle de conservation sont immédiatement stockées dans le compartiment de conservation.

## Gestion de la séquence de compartiment de conservation


Vous pouvez modifier l'ordre des compartiments de conservation pour vous assurer que les données sont comparées aux compartiments de conservation dans l'ordre correspondant à vos besoins.

### Pourquoi et quand exécuter cette tâche

Les segments de conservation sont séquencés dans l'ordre de priorité de la ligne supérieure à la ligne inférieure des fenêtres **Conservation des événements** et **Conservation du flux**. Un enregistrement est stocké dans le premier compartiment de conservation qui correspond aux paramètres d'enregistrement.

Vous ne pouvez pas déplacer le compartiment de conservation par défaut. Il se trouve toujours au bas de la liste.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Conservation des événements** ou sur **Conservation du flux**.
3. Si vous avez configuré les locataires, dans la liste **Locataire**, sélectionnez le titulaire pour les compartiments de conservation que vous souhaitez réorganiser.

**Remarque :** Pour gérer les règles de conservation des données partagées dans une configuration multi-locataires, choisissez **N/A** dans la liste **Locataire**.

4. Sélectionnez la ligne qui correspond au compartiment de conservation que vous souhaitez déplacer, puis cliquez sur **Haut** ou **Bas** pour le déplacer vers l'emplacement correct.
5. Cliquez sur **Sauvegarder**.


## Activation et désactivation d'un compartiment de conservation

Lorsque vous configurez et enregistrez un compartiment de conservation, il est activé par défaut. Vous pouvez désactiver un compartiment pour régler votre événement ou la conservation du flux.

### Pourquoi et quand exécuter cette tâche

Lorsque vous désactivez un compartiment, les nouveaux événements ou flux qui correspondent aux exigences du compartiment désactivé sont stockés dans le compartiment suivant qui correspond à l'événement ou aux propriétés de flux.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Conservation des événements** ou sur **Conservation du flux**.
3. Si vous avez configuré les locataires, dans la liste **Tenant**, sélectionnez le titulaire du compartiment de conservation que vous souhaitez modifier.

**Remarque :** Pour gérer les règles de conservation des données partagées dans une configuration multi-locataires, choisissez **N/A** dans la liste **Locataire**.


4. Sélectionnez le compartiment de conservation à désactiver, puis cliquez sur **Activer / Désactiver**.

## Suppression d'un compartiment de conservation

Lorsque vous supprimez un compartiment de conservation, seuls les critères qui définissent le compartiment sont supprimés. Les événements ou les flux stockés dans le compartiment sont collectés par le compartiment de conservation par défaut. La durée de conservation par défaut est de 30 jours. Une fois ce délai écoulé, les données sont immédiatement supprimées.



## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Conservation des événements** ou sur **Conservation du flux**.
3. Si vous avez configuré les locataires, dans la liste **Tenant**, sélectionnez le titulaire du compartiment de conservation que vous souhaitez supprimer.

**Remarque :** Pour gérer les règles de conservation des données partagées dans une configuration multi-locataires, choisissez **N/A** dans la liste **Locataire**.



4. Sélectionnez le compartiment de conservation à supprimer, puis cliquez sur **Supprimer**.

## Notifications système

---

IBM QRadar surveille en permanence tous les dispositifs et fournit des informations, des avertissements et des notifications d'erreur à QRadar Console, ce qui vous permet de surveiller plus facilement le statut et la santé de votre déploiement.

Les notifications système globales sont spécifiques à l'hôte et le seuil de chaque notification est défini automatiquement par QRadar.

Pour afficher les notifications système sur votre écran, vous devez configurer votre navigateur pour autoriser les fenêtres en incrustation et vous assurer que la case à cocher **Activer les notifications en incrustation** est cochée dans vos préférences utilisateur (). Si vous désactivez les notifications de bureau pour QRadar, vous pouvez toujours afficher les notifications système sous le menu notifications (.

Au cours de l'installation, QRadar détermine et configure automatiquement les seuils pour toutes les notifications système.

Pour plus d'informations sur les notifications système, voir le *IBM QRadar Troubleshooting and System Notifications Guide*.

**Remarque :** Les notifications par navigateur sont prises en charge pour Mozilla Firefox, Google Chrome et Microsoft Edge 10. Microsoft Internet Explorer ne prend pas en charge les notifications basées sur un navigateur. Les notifications dans Internet Explorer apparaissent dans une boîte de notification QRadar. La façon dont les notifications apparaissent et la durée pendant laquelle les messages restent à l'écran peuvent varier d'un navigateur à l'autre.

## Configuration des notifications par courrier électronique d'événements et de flux

Lorsque vous configurez des règles dans IBM QRadar, indiquez que chaque fois que la règle génère une réponse, une notification par courrier électronique est envoyée aux destinataires. La notification par e-mail fournit des informations utiles, comme les propriétés d'un événement ou d'un flux.

### Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser le contenu qui est inclus dans la notification par courrier électronique pour la réponse de règle en éditant le fichier `alert-config.xml`.

**Remarque :** Les références aux flux ne s'appliquent pas à IBM QRadar Log Manager.

Vous devez créer un répertoire temporaire dans lequel vous pouvez éditer en toute sécurité une copie de vos fichiers, sans risquer d'écraser les fichiers par défaut. Après avoir modifié et sauvegardé le fichier `alert-config.xml`, vous devez exécuter un script qui valide vos modifications. Le script de validation applique automatiquement vos modifications à une zone de transfert. Vous devez déployer la configuration complète pour régénérer les fichiers de configuration de tous les dispositifs.

## Procédure

1. Utilisez SSH pour vous connecter à QRadar Console en tant que superutilisateur.
2. Créez un nouveau répertoire temporaire à utiliser pour l'édition en toute sécurité des copies des fichiers par défaut.
3. Pour copier les fichiers stockés dans le répertoire `custom_alerts` dans le répertoire temporaire, entrez la commande suivante :

```
cp /store/configservices/staging/globalconfig/templates/custom_alerts/*. * <directory_name>
```

Le `<directory_name>` est le nom du répertoire temporaire que vous avez créé.

4. Confirmez que les fichiers ont bien été copiés :
  - a) Pour lister les fichiers du répertoire, entrez `ls -lah`.
  - b) Testez que le fichier `alert-config.xml` est répertorié.
5. Ouvrez le fichier `alert-config.xml` pour l'éditer.
6. Éditez le contenu de l'élément `<template>` .
  - a) Obligatoire : Indiquez le type de modèle à utiliser. Les options valides sont événement ou Flux.

```
<templatetype>event</templatetype>
```

```
<templatetype>flow</templatetype>
```

- b) Entrez un nom pour le modèle de rapport.

```
<templatename>Default flow template</templatename>
```

Si vous disposez de plusieurs modèles, assurez-vous que le nom du modèle est unique.

- c) Définissez l'élément `<active>` sur `true` :

```
<active>true</active>
```
- d) Éditez les paramètres dans les éléments `<body>` ou `<subject>` pour inclure les informations que vous souhaitez voir.

**Important :** La propriété `<active></active>` doit être définie sur `True` pour chaque type de modèle d'événement et de flux que vous souhaitez faire apparaître en tant qu'option dans QRadar. Il doit y avoir au moins un modèle actif pour chaque type.

Vous devez également vous assurer que la propriété `<filename></filename>` soit laissée vide.

### Paramètres de notification que vous pouvez utiliser dans le modèle :

Tableau 23. Paramètres de notification acceptés		
Paramètres de la commande	Paramètres d'événement	Paramètres de flux
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
Description de la règle	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList
Catégorie	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Hôte

Tableau 23. Paramètres de notification acceptés (suite)

Paramètres de la commande	Paramètres d'événement	Paramètres de flux
Contenu utile	SrcMACAddress	Port
Crédibilité	SrcPostNATIPAddress	SourceBytes
Pertinence	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPor	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
Protocole		DestinationASN
StartTime		InputIFIndex
Durée		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
Nom d'utilisateur		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Gravité		DestinationQOS
CustomProperty		SourcePayload
CustomPropertiesList		
CalculatedProperty		
CalculatedPropertiesList		
AQLCustomProperty		
AqlCustomPropertiesList		
LogSourceId		
LogSourceName		

**Remarque :** Si vous ne souhaitez pas extraire la liste entière lorsque vous utilisez le paramètre CustomProperties, CalculatedProperties ou AqlCustomProperties, vous pouvez sélectionner une propriété spécifique à l'aide des balises suivantes :

- Propriété personnalisée : `$$body.CustomProperty("<custom_property_name>")`
- Propriété calculée : `$$body.CalculatedProperty("<calculated_property_name>")`

- Propriété personnalisée AQL : \$  
`{body.AqlCustomProperty("<AQL_custom_property_name>")}`
7. Pour créer plusieurs modèles de courrier électronique, copiez et collez l'exemple de modèle de courrier électronique suivant dans l'élément `<template>` du fichier `alert-config.xml`. Répétez l'étape 6 pour chaque modèle que vous ajoutez.

### Exemple de modèle de courrier électronique :

```
<template>
<templatename>Default Flow</templatename>
<templatetype>flow</templatetype>
<active>true</active>
<filename></filename>
<subject>${RuleName} Fired </subject>
<body>
  The ${AppName} event custom rule engine sent an automated response:

  ${StartTime}

  Rule Name:                ${RuleName}
  Rule Description:         ${RuleDescription}

  Source IP:                ${SourceIP}
  Source Port:              ${SourcePort}
  Source Username (from event): ${UserName}
  Source Network:           ${SourceNetwork}

  Destination IP:          ${DestinationIP}
  Destination Port:        ${DestinationPort}
  Destination Username (from Asset Identity): ${DestinationUserName}
  Destination Network:     ${DestinationNetwork}

  Protocol:                 ${Protocol}
  QID:                      ${Qid}

  Event Name:               ${EventName}
  Event Description:        ${EventDescription}
  Category:                 ${Category}

  Log Source ID:           ${LogSourceId}
  Log Source Name:         ${LogSourceName}

  Payload:                  ${Payload}

  CustomPropertiesList:     ${CustomPropertiesList}

  AQL Custom Property, CEP_aql_1:  ${body.AqlCustomProperty("CEP_aql_1")}
  Calculated Property, CEP_calc_2:  ${body.CalculatedProperty("CEP_calc_2")}
  Regex Property, CEP_reg_3:       ${body.CustomProperty("CEP_reg_3")}

</body>
<from></from>
<to></to>
<cc></cc>
<bcc></bcc>
</template>
```

**Remarque :** Actuellement, dans les cas de partage de service (domaine multilocation) ou d'adresses IP chevauchantes, l'**ID de domaine** n'est pas disponible dans les modèles d'e-mail personnalisés.


8. Sauvegardez et fermez le fichier `alert-config.xml`.
9. Validez les modifications en entrant la commande suivante.

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

Le paramètre `<directory_name>` est le nom du répertoire temporaire que vous avez créé.

Si le script valide les modifications, le message suivant s'affiche :`File alert-config.xml was deployed successfully to staging!`

10. Déployez les modifications dans QRadar.
  - a) Connectez-vous à QRadar.

- b) Dans le menu de navigation () , cliquez sur **Admin**.
- c) Cliquez sur **Avancé > Déployer la configuration complète**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Configuration des notifications par courrier électronique de violation personnalisée

Vous pouvez créer des modèles pour les notifications par courrier électronique qui sont déclenchées pour des infractions.

Vous pouvez personnaliser le contenu qui est inclus dans la notification par courrier électronique en éditant le fichier `alert-config.xml`.

Vous devez créer un répertoire temporaire dans lequel vous pouvez éditer en toute sécurité une copie de vos fichiers, sans risquer d'écraser les fichiers par défaut. Après avoir modifié et sauvegardé le fichier `alert-config.xml`, vous devez exécuter un script qui valide vos modifications. Le script de validation applique automatiquement vos modifications à une zone de transfert. Vous devez déployer la configuration complète pour régénérer les fichiers de configuration de tous les dispositifs.

### Procédure

1. Utilisez SSH pour vous connecter à QRadar Console en tant que superutilisateur.
2. Créez un nouveau répertoire temporaire à utiliser pour l'édition en toute sécurité des copies des fichiers par défaut.
3. Entrez la commande suivante pour copier les fichiers stockés dans le répertoire `custom_alerts` dans le répertoire temporaire :

```
cp /store/configservices/staging/globalconfig/templates/custom_alerts/*.* <directory_name>
```

<directory\_name> est le nom du répertoire temporaire que vous avez créé.

Si le fichier n'existe pas dans le répertoire `staging`, vous pouvez le trouver dans le répertoire `/opt/qradar/conf/templates/custom_alerts`.

4. Confirmez que les fichiers ont bien été copiés :
  - a) Pour faire une liste des fichiers du répertoire, entrez `ls -lah`.
  - b) Testez que le fichier `alert-config.xml` est répertorié.
5. Ouvrez le fichier `alert-config.xml` pour l'éditer.
6. Ajoutez un nouvel élément `<template>` pour le nouveau modèle d'infraction.
  - a) Obligatoire : Entrez `Infraction` pour la valeur du type de modèle.

```
<templatetype>offense</templatetype>
```

- b) Entrez un nom pour le modèle d'infraction.  
Par exemple, `<templatename>Default offense template</templatename>`  
Si vous disposez de plusieurs modèles, assurez-vous que le nom du modèle est unique.
- c) Définissez l'élément `<active>` sur `true`.

```
<active>true</active>
```

**Important :** La propriété `<active></active>` doit être définie sur `true` pour chaque type de modèle que vous souhaitez voir apparaître comme option dans QRadar. Il doit y avoir au moins un modèle actif pour chaque type.

- d) Éditez les paramètres dans les éléments <body> ou <subject> pour inclure les informations que vous souhaitez voir.

Les listes suivantes fournissent les valeurs que vous pouvez utiliser dans le modèle de violation. Les valeurs \$Label fournissent le libellé de l'article et les valeurs \$Value fournissent les données.

#### Paramètres d'infractions

\$Value.DefaultSubject  
\$Value.Intro  
\$Value.OffenseId  
\$Value.OffenseStartTime  
\$Value.OffenseUrl  
\$Value.OffenseMRSC  
\$Value.OffenseDescription  
\$Value.EventCounts  
&NonBreakingSpace;  
\$Label.OffenseSourceSummary  
\$Value.OffenseSourceSummary  
&NonBreakingSpace;  
\$Label.TopSourceIPs  
\$Value.TopSourceIPs  
&NonBreakingSpace;  
\$Label.TopDestinationIPs  
\$Value.TopDestinationIPs  
&NonBreakingSpace;  
\$Label.TopLogSources  
\$Value.TopLogSources  
&NonBreakingSpace;  
\$Label.TopUsers  
\$Value.TopUsers  
&NonBreakingSpace;  
\$Label.TopCategories  
\$Value.TopCategories  
&NonBreakingSpace;  
\$Label.TopAnnotations  
\$Value.TopAnnotations  
&NonBreakingSpace;  
\$Label.ContributingCreRules  
\$Value.ContributingCreRules

&NonBreakingSpace;

Vous pouvez également faire une boucle sur certaines valeurs à l'aide de la syntaxe suivante dans le modèle :

```
#foreach( $item in $Value.X )  
  $item  
#end
```

Où X se trouve l'une des valeurs suivantes :

- OffenseSourceSummaryList
- TopSourceIPsList
- TopDestinationIPsList
- TopLogSourcesList
- TopUsersList
- TopCategoriesList
- TopAnnotationsList
- ContributingCreRulesList

&NonBreakingSpace;

Vous pouvez inclure les propriétés suivantes à l'aide de  $\${X}$ , où X est l'une des valeurs suivantes :

- OffenseID
- OffenseRuleID
- OffenseRuleName
- Magnitude
- Pertinence
- Gravité
- Crédibilité
- Domaine (« N/A » si introuvable)
- Locataire (« N/A » si introuvable)
- Type d'infraction

Par exemple, si une infraction a une magnitude de 7 et que vous incluez  $\${Magnitude}$  dans le modèle, la valeur de  $\${Magnitude}$  apparaît comme 7 dans le courrier électronique.

7. Sauvegardez et fermez le fichier `alert-config.xml`.


8. Validez les modifications en entrant la commande suivante.

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

`<directory_name>` est le nom du répertoire temporaire que vous avez créé.

Si le script valide les modifications, le message suivant s'affiche :`File alert-config.xml was deployed successfully to staging!`

9. Déployez les modifications dans QRadar.

- Connectez-vous à QRadar.
- Dans le menu de navigation () , cliquez sur **Admin**.
- Cliquez sur **Avancé > Déployer la configuration complète**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Motif de fermeture d'infraction personnalisée

Vous pouvez gérer les options répertoriées dans la zone de liste **Raison de la fermeture** de l'onglet **Infractions**.

Lorsqu'un utilisateur ferme une violation dans l'onglet **Infractions**, la fenêtre Fermer l'infraction s'affiche. L'utilisateur est invité à sélectionner une cause dans la zone de liste **Raison de la fermeture**. Trois options par défaut sont répertoriées :


- Faux positif, réglé
- Faux problème
- Violation de la stratégie

Les administrateurs peuvent ajouter, modifier et supprimer des raisons de fermeture d'infraction personnalisées à partir de l'onglet **Admin**.

## Ajout d'un motif de fermeture d'infraction personnalisé

Lorsque vous ajoutez une raison de fermeture d'infraction personnalisée, la nouvelle raison apparaît dans la fenêtre **Raisons de fermeture personnalisées** et dans la zone de liste **Raison de la fermeture** de la fenêtre **Fermer l'infraction** de l'onglet **Infractions**.

### Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Motifs de fermeture de l'infraction personnalisée**.
3. Cliquez sur **Ajouter**.
4. Entrez un motif unique de fermeture d'infractions. La longueur des motifs doit être comprise entre 5 et 60 caractères.
5. Cliquez sur **OK**.

Votre nouvelle raison de fermeture de violation personnalisée est maintenant répertoriée dans la fenêtre **Motifs de fermeture personnalisés**. La zone de liste **Motif de la fermeture** de la fenêtre **Fermer l'infraction** de l'onglet **Infractions** affiche également la raison personnalisée que vous avez ajoutée.

## Édition de la raison de fermeture de l'infraction personnalisée

L'édition d'une raison de fermeture d'infraction personnalisée met à jour la raison dans la fenêtre **Raisons de fermeture personnalisées** et la zone de liste **Raison de la fermeture** dans la fenêtre **Fermer l'infraction** de l'onglet **Infraction**.


### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Motifs de fermeture de l'infraction personnalisée**.
3. Sélectionnez la cause de fermeture de l'infraction que vous souhaitez modifier.
4. Cliquez sur **Editer**.
5. Entrez une nouvelle raison unique pour la fermeture des infractions. La longueur des motifs doit être comprise entre 5 et 60 caractères.
6. Cliquez sur **OK**.

## Suppression d'une raison de fermeture d'infraction personnalisée

La suppression d'une raison de fermeture d'infraction personnalisée supprime la raison de la fenêtre **Raisons de fermeture personnalisées** et de la zone de liste **Raison de la fermeture** dans la fenêtre **Fermer l'infraction** de l'onglet **Infractions**.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.




2. Dans la section **Configuration du système**, cliquez sur **Motifs de fermeture de l'infraction personnalisée**.
3. Sélectionnez la cause de fermeture de l'infraction que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **OK**.

## Configuration d'une propriété d'actif personnalisée

---

Les propriétés d'actifs personnalisés fournissent des options de requête supplémentaires lorsque vous exécutez des requêtes sur les actifs que vous avez dans IBM QRadar.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Propriétés de l'actif personnalisé**.
3. Dans la zone **Nom**, entrez un descripteur pour la propriété d'actif personnalisée.

**Remarque :** Le nom doit contenir uniquement des caractères alphanumériques, des espaces ou des traits de soulignement. Aucun caractère spécial n'est autorisé.

4. Dans la liste **Type**, sélectionnez **Numérique** ou **Texte** pour définir le type d'informations pour la propriété d'actif personnalisé.
5. Cliquez sur **OK**.
6. Cliquez sur l'onglet **Actifs**.
7. Cliquez sur **Modifier un actif > Propriétés d'actif personnalisées**.
8. Entrez les informations requises dans la zone de valeur.
9. Cliquez sur **OK**.

## Gestion de l'index

---

Utilisez Index Management pour contrôler l'indexation de base de données sur les propriétés d'événement et de flux. Pour améliorer la vitesse des recherches dans IBM QRadar, limitez les données globales en ajoutant une zone indexée dans votre requête de recherche.

Un *Index* est un ensemble d'éléments qui indiquent des informations sur les données d'un fichier et son emplacement dans le système de fichiers. Les index de données sont générés en temps réel car les données sont transmises en continu ou sont construites sur demande une fois les données collectées. La recherche est plus efficace parce que les systèmes qui utilisent les index n'ont pas à lire à travers chaque donnée pour localiser les correspondances. L'index contient des références à des termes uniques dans les données et leurs emplacements. Étant donné que les index utilisent l'espace disque, l'espace de stockage peut être utilisé pour réduire le temps de recherche.

Utilisez d'abord les propriétés d'événement d'indexation et de flux pour optimiser vos recherches. Vous pouvez activer l'indexation sur toute propriété répertoriée dans la fenêtre Gestion d'index et vous pouvez activer l'indexation sur plusieurs propriétés. Lorsqu'une recherche démarre dans QRadar, le moteur de recherche filtre d'abord les données par propriétés indexées. Le filtre indexé élimine les parties de l'ensemble de données et réduit le volume global de données et le nombre de journaux d'événements ou de flux à rechercher. Sans aucun filtre, QRadar prend plus de temps pour renvoyer les résultats pour les fichiers volumineux.

Par exemple, vous pouvez rechercher tous les journaux au cours des six derniers mois qui correspondent au texte : `l'opération n'est pas autorisée`. Par défaut, QRadar stocke l'indexation de texte intégral au cours des 30 derniers jours. Par conséquent, pour effectuer une recherche au cours des 6 derniers mois, le système doit relire chaque valeur de charge de chaque événement ou flux dans cette période pour rechercher les correspondances. Vos résultats s'affichent plus rapidement lorsque vous effectuez une recherche avec un filtre de valeur indexé tel qu'un **Type de source de journal**, **Nom de l'événement** ou **IP source**.

La fonction de gestion d'index fournit également des statistiques, telles que :

- Pourcentage de recherches sauvegardées exécutées dans votre déploiement incluant la propriété indexée
- Volume des données écrites sur le disque par l'index pendant la période sélectionnée

Pour activer l'indexation de charge, vous devez activer l'indexation sur la propriété **Filtre rapide**.


## Activation des index

La fenêtre **Gestion de l'index** répertorie toutes les propriétés d'événement et de flux pouvant être indexées et fournit des statistiques pour les propriétés. Les options de la barre d'outils vous permettent d'activer et de désactiver l'indexation pour les propriétés d'événement et de flux sélectionnées.

### Pourquoi et quand exécuter cette tâche

La modification de l'indexation de base de données peut réduire les performances du système. Pensez à surveiller les statistiques une fois que vous avez activé l'indexation pour plusieurs propriétés.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion de l'index**.
3. Sélectionnez une ou plusieurs propriétés dans la liste **Gestion de l'index**.
4. Choisissez l'une des options suivantes :

Situation	Période	Action	Motif
L'index est désactivé et <b>% de recherches utilisant la propriété</b> est supérieur à 30 % et <b>% de recherches sur l'index manquant</b> est supérieur à 30 %.	24 heures, 7 jours ou 30 jours	Cliquez sur <b>Activer l'index</b> .	Cette propriété de recherche est utilisée souvent. L'activation d'un index peut améliorer les performances.
L'index est activé et <b>% de recherches utilisant la propriété</b> est égal à zéro.	30 jours	Cliquez sur <b>Désactiver l'index</b> .	L'index activé n'est pas utilisé dans les recherches. Désactivez la propriété indexée pour préserver l'espace disque.

5. Cliquez sur **Sauvegarder**.
6. Cliquez sur **OK**.

### Résultats

Dans les listes qui incluent des propriétés d'événement et de flux, le texte suivant est ajouté à la fin des noms des propriétés indexées : [Indexé]. De telles listes peuvent inclure les paramètres de recherche sur les pages des critères de recherche des onglets **Activité du journal** et **Activité réseau** ainsi que dans la fenêtre **Ajouter un filtre**.


## Activation de l'indexation de charge pour optimiser les temps de recherche

Utilisez la fonction **Filtre rapide** dans l'onglet **Activité de journal** et **Activité réseau** pour rechercher des événements et des charges utiles à l'aide d'une chaîne de texte. Pour optimiser les temps de recherche d'événements et de flux, activez l'indexation de la charge sur la propriété **Filtre rapide**.

**Restriction :** L'indexation de charge augmente les exigences de stockage sur disque et peut affecter les performances du système. Activez l'indexation de charge si votre déploiement remplit les conditions suivantes :

- Les processeurs d'événement et de flux sont à moins de 70 % d'utilisation du disque.
- Les processeurs d'événements et de flux sont inférieurs à 70% du nombre maximal d'événements par seconde (EPS) ou de flux par interface (FPI).

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion de l'index**.
3. Dans la zone **Recherche rapide**, entrez **Filtre rapide**.  
La propriété **Filtre rapide** s'affiche.
4. Sélectionnez la propriété **Filtre rapide** à indexer.  
Dans la table des résultats, utilisez la valeur de la colonne **Base de données** pour identifier les événements ou les flux de propriété **Filtre rapide**.
5. Dans la barre d'outils, cliquez sur **Activer l'index**. Un point vert indique que l'index de charge est activé.  
Si une liste inclut des propriétés d'événement ou de flux indexées, les noms de propriété sont ajoutés au texte suivant : [Indexed].
6. Cliquez sur **Sauvegarder**.

## Que faire ensuite

Pour gérer les index de charge, voir [«Configuration de la période de conservation des index de charge»](#), à la page 133.

## Configuration de la période de conservation des index de charge

Par défaut, IBM QRadar définit 30 jours pour la durée de conservation des données de l'index de contenu. Vous pouvez rechercher des valeurs spécifiques dans des index de filtre rapide au-delà de 30 jours en modifiant la conservation par défaut dans QRadar.

### Avant de commencer

Vos appareils physiques et virtuels nécessitent un minimum de 24 Go de RAM pour activer l'indexation complète de contenu. Cependant, 48 Go de RAM sont proposés.


Les valeurs RAM minimales et suggérées s'appliquent à tous les systèmes QRadar, tels que les dispositifs 16xx, 17xx ou 18xx, qui traitent des événements ou des flux.

### Pourquoi et quand exécuter cette tâche

Les valeurs de conservation reflètent l'intervalle de temps que vous recherchez généralement. La durée minimale de conservation est de 1 jour et le maximum est de 2 ans.

**Remarque :** Les recherches de filtre rapide qui utilisent un intervalle de temps en dehors du paramètre de conservation de l'index de contenu peuvent déclencher des réponses système lentes et exigeantes en ressources. Par exemple, si la conservation de l'index de charge est définie pour 1 jour, vous utilisez un intervalle de temps pour les 30 dernières heures de la recherche.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Paramètres de système**.

3. Dans la section **Paramètres base de données**, sélectionnez une période de conservation dans la liste **Conservation de l'index de contenu**.
4. Cliquez sur **Sauvegarder**.
5. Fermez la fenêtre **Paramètres système**.
6. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

### Que faire ensuite

Si vous conservez des index de contenu plus longs que la valeur par défaut, l'espace disque supplémentaire est utilisé. Une fois que vous avez sélectionné une valeur supérieure dans la zone **Conservation de l'index de contenu**, surveillez les notifications système pour vous assurer que vous ne remplissez pas l'espace disque.

## Restrictions visant à empêcher les recherches à forte intensité de ressources

---

Vous pouvez équilibrer l'utilisation de votre infrastructure QRadar en définissant des restrictions de ressources sur les recherches d'événements et de flux IBM QRadar.

Avant de définir des restrictions de ressource, examinez avec soin les procédures d'exploitation normales de votre environnement. Essayez de définir des restrictions qui garantissent que tous les utilisateurs ont bien accès aux données dont ils ont besoin, tout en évitant qu'ils n'exécutent des requêtes volumineuses qui auraient une incidence négative sur la disponibilité et les performances du système pour les autres utilisateurs.

### Types de restrictions de ressources

Vous pouvez définir des limitations sur les recherches en configurant des restrictions de temps ou de fichier en fonction de l'utilisateur, du rôle ou du titulaire.

Les restrictions de ressource sont appliquées dans l'ordre suivant : utilisateur, rôle utilisateur et titulaire. Par exemple, les restrictions qui sont définies pour un utilisateur sont prioritaires sur les restrictions définies pour le rôle utilisateur ou le titulaire auquel est affecté l'utilisateur.

Vous pouvez définir les types de restrictions suivants sur les recherches d'événements et de flux :

- Durée pendant laquelle une recherche est exécutée avant le retour des données.
- L'intervalle de temps des données à rechercher.
- Nombre d'enregistrements traités par le serveur de requêtes Ariel.

**Remarque :** La recherche Ariel s'arrête lorsque la limite d'enregistrement est atteinte, mais tous les résultats de recherche en cours sont renvoyés au gestionnaire de recherche et ne sont pas tronqués. Par conséquent, l'ensemble de résultats de la recherche est souvent supérieur à la limite d'enregistrement spécifiée.

### Restrictions basées sur l'utilisateur

Les restrictions basées sur l'utilisateur définissent des limites pour un utilisateur individuel, et elles ont priorité sur les restrictions de rôle et de locataire.

Par exemple, votre organisation embauche des étudiants universitaires pour travailler avec les analystes subalternes de votre SOC. Les étudiants ont le même rôle d'utilisateur que les autres analystes juniors, mais vous appliquez des restrictions basées sur l'utilisateur plus restrictives jusqu'à ce que les étudiants soient correctement formés à la génération de requêtes QRadar.

## Restrictions basées sur les rôles

Les restrictions basées sur les rôles vous permettent de définir des groupes d'utilisateurs qui requièrent différents niveaux d'accès à votre déploiement QRadar. En définissant des restrictions basées sur les rôles, vous pouvez équilibrer les besoins des différents types d'utilisateurs.

Par exemple, un analyste subalterne de la sécurité pourrait se concentrer sur les incidents de sécurité qui se sont produits récemment, alors qu'un analyste principal de la sécurité pourrait être plus impliqué dans les enquêtes judiciaires qui examinent les données sur une plus longue période. En définissant des restrictions basées sur les rôles, vous pouvez limiter un analyste junior à n'accéder qu'aux 7 derniers jours de données, tandis qu'un analyste principal a accès à une plage de données beaucoup plus longue.

## Restrictions basées sur le locataire

Dans un fournisseur de services de sécurité géré (MSSP) ou une organisation à plusieurs divisions, les restrictions basées sur les locataires peuvent vous aider à garantir la qualité du service en empêchant les conflits de ressources et la dégradation des services. Vous pouvez empêcher un locataire d'interroger des téraoctets de données qui peuvent avoir un impact négatif sur les performances du système pour tous les autres locataires.

En tant que MSSP, vous pouvez définir des restrictions de ressources standard en fonction d'un ensemble de critères auxquels chaque locataire est comparé. Par exemple, la configuration standard d'un locataire de taille moyenne peut inclure des restrictions de ressources qui limitent les recherches pour accéder uniquement aux 14 derniers jours de données et un maximum de 10 000 enregistrements renvoyés.

## Restrictions de ressources dans les environnements répartis

Dans un environnement réparti, le moment du transfert de données entre la console IBM QRadar et les hôtes gérés peut avoir une incidence sur les résultats de la recherche.

Lorsque vous exécutez une recherche dans IBM QRadar, la recherche s'exécute sur tous les nœuds en même temps. Chaque hôte géré exécute la recherche et envoie les résultats agrégés à la console QRadar lorsque la recherche est terminée ou lorsqu'elle atteint le nombre prédéfini de lignes.

Il est important de comprendre comment les restrictions de ressources que vous définissez peuvent avoir une incidence sur les résultats de la recherche renvoyés à un utilisateur :

### Recherches annulées

Chaque hôte géré vérifie périodiquement l'état de la limite de restriction de ressources. Si une limite est atteinte, la recherche est automatiquement annulée afin d'éviter que les résultats incomplets ne soient mis en cache et réutilisés.

Les résultats qui ont été collectés avant l'annulation de la recherche par le système peuvent être affichés en cliquant sur **Rechercher** > **Gérer les résultats de la recherche** dans l'onglet **Activité de journal** ou **Activité réseau**.

### Résultats de recherche vides

Lorsque vous définissez des restrictions de délai ou de limite d'enregistrement, l'agrégation à distance peut amener la console QRadar à atteindre la limite de restriction de ressources avant que l'hôte géré n'envoie l'agrégat partiel à la console. Dans ce cas, les résultats de la recherche peuvent sembler vides même si certaines données ont été collectées.

### Résultats de recherche incohérents

QRadar surveille la charge sur chaque hôte géré et gère la recherche pour garantir des performances optimisées tout au long du déploiement. En fonction de la charge du système, les recherches exécutées à plusieurs reprises peuvent afficher des résultats légèrement différents en raison des hôtes gérés qui renvoient les données dans un ordre différent.

Par exemple, dans un déploiement doté de six processeurs d'événements, EP1, EP3 et EP5 peuvent être les premiers processeurs à renvoyer des données lors de l'exécution initiale. Dans les exécutions suivantes, EP2, EP4 et EP6 peuvent renvoyer d'abord les données, ce qui explique les résultats de recherche incohérents.

## Résultats de recherche limités

Vous pouvez définir une restriction de limite sur les résultats de la recherche pour QRadar qui limite le nombre d'enregistrements lus à partir du disque dans une requête de recherche. Une limite permet de s'assurer que la requête s'arrête après que tout hôte géré participant à la recherche lit le nombre restreint d'entrées du disque. La requête n'extrait pas toutes les données et ne vous donne que le nombre restreint de lignes. La définition de cette restriction peut empêcher un plantage du système dans l'instance d'une grande quantité de données.

Par exemple, si vous définissez la restriction sur 10 000 lignes, la requête s'arrête après que l'hôte géré traite 10 000 enregistrements.

Selon la fréquence à laquelle les utilisateurs atteignent les restrictions de ressources, vous pouvez ajuster les limites afin d'éviter que les utilisateurs ne puissent effectuer des recherches raisonnables pour répondre à leurs exigences professionnelles. Les utilisateurs qui exécutent systématiquement des recherches qui déforment le système peuvent bénéficier d'une formation plus grande pour la génération de requêtes QRadar. Pour plus d'informations, voir *IBM QRadar Ariel Query Language Guide*.

## Configuration des restrictions de ressources

Définissez des restrictions de ressource pour appliquer des limitations de durée ou de données aux recherches d'événement et de flux.

### Pourquoi et quand exécuter cette tâche

Vous pouvez définir les types de restrictions de ressources suivants :


- Les restrictions **Heure d'exécution** indiquent la durée maximale d'exécution d'une requête avant le renvoi des données.
- Les restrictions **Intervalle de temps** indiquent la durée des données à rechercher.
- Les restrictions **Limite d'enregistrement** indiquent le nombre d'enregistrements de données renvoyés par une requête de recherche.

Les utilisateurs qui exécutent des recherches limitées par des restrictions de ressources voient l'icône de

restriction de ressources () en regard des critères de recherche.

**Remarque :** L'ensemble de résultats de la recherche est souvent supérieur à la limite d'enregistrement spécifiée. Lorsque la limite d'enregistrement est atteinte, le gestionnaire de recherche signale à tous les participants à la recherche de s'arrêter (il y a plusieurs participants à la recherche même sur un même système), mais les résultats continuent de s'accumuler jusqu'à ce que la recherche s'arrête complètement sur tous les participants. Tous les résultats de la recherche sont ajoutés à l'ensemble de résultats.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Restrictions des ressources**.
3. Si votre déploiement a des locataires configurés, cliquez sur **Rôle** ou **Tenant** pour spécifier le type de restrictions à définir.
4. Cliquez deux fois sur le rôle ou le titulaire pour lequel vous voulez définir des restrictions.
5. Pour définir des restrictions pour tous les utilisateurs auxquels est affecté le rôle utilisateur ou titulaire, procédez comme suit :
  - a) Cliquez sur la ligne récapitulative en haut pour ouvrir la boîte de dialogue **Éditer une restriction**.
  - b) Cliquez sur **Activé** pour le type de restriction que vous souhaitez définir et indiquez les valeurs de restriction.
  - c) Cliquez sur **Sauvegarder**.

6. Pour définir les restrictions d'un utilisateur spécifique, procédez comme suit :
  - a) Cliquez deux fois sur l'utilisateur pour lequel vous voulez définir des restrictions.  
Pour rechercher un utilisateur, entrez son nom dans la zone de filtre.
  - b) Cliquez sur **Activé** pour le type de restriction que vous souhaitez définir et indiquez les valeurs de restriction.
  - c) Cliquez sur **Sauvegarder**.

## Hôtes d'application

Un hôte d'application est un hôte géré dédié à l'exécution d'applications. Les hôtes d'applications fournissent des ressources d'unité centrale, de mémoire et stockage supplémentaires pour vos applications sans que cela n'ait de conséquence sur la capacité de traitement de votre console QRadar Console. Les applications, telles User Behavior Analytics with Machine Learning Analytics, exigent plus de ressources que celles actuellement disponibles sur la console.

L'hôte d'application remplace le noeud d'application. QRadar gère toutes les mises à jour apportées à l'hôte d'application alors que ce n'était pas le cas pour le noeud d'application. L'hôte d'application prend en charge la haute disponibilité et vous pouvez l'inclure dans vos déploiements à haute disponibilité.

### Remarques :

- L'ID de dispositif de l'hôte d'application est 4000.
- Vous ne pouvez disposer que d'un seul hôte d'application par déploiement.
- Le port 5000 doit être ouvert sur la console.
- Le port 443 doit être ouvert sur votre console.
- Si votre hôte d'application n'est pas chiffré, ouvrez les ports 9000 et 14433 pour la communication unidirectionnelle de votre console vers l'hôte d'application.
- Si votre hôte d'application est chiffré, ouvrez le port 26000 et 26001 pour la communication unidirectionnelle de votre console vers l'hôte d'application.

### Spécifications de l'hôte d'application

Le tableau suivant indique la configuration requise minimale et les spécifications suggérées pour un hôte d'application.

**Remarque :** \*Les spécifications suggérées pour les déploiements de taille moyenne et de grande taille n'ont pas été testées. Si vous utilisez certaines applications plus volumineuses, telles que Pulse Dashboard ou User Behavior Analytics with Machine Learning, la configuration requise minimale est probablement insuffisante. Pensez à mettre à niveau votre environnement de déploiement.

<i>Tableau 24. Spécifications de l'hôte d'application</i>				
	<b>Cœurs de CPU</b>	<b>RAM</b>	<b>Espace disque</b>	<b>Description</b>
Petit	4	12 Go	256 Go	Configuration requise minimale pour un hôte d'application. Vous pouvez exécuter la plupart des applications avec cette configuration minimale, mais pas d'applications plus volumineuses telles que QRadar DNS Analyzer et User Behavior Analytics with Machine Learning.
Moyen	12 ou plus	64 Go ou plus	500 Go ou plus	*Vous pouvez exécuter toutes les applications qui existent aujourd'hui, mais cette spécification ne vous laisse pas de place pour des applications futures.

Tableau 24. Spécifications de l'hôte d'application (suite)

	Cœurs de CPU	RAM	Espace disque	Description
Grand	24 ou plus	128 Go ou plus	1 To ou plus	*Vous pouvez exécuter toutes les applications qui existent aujourd'hui et vous avez probablement de la place pour des applications futures.

## Scénarios d'installation

Si vous installez un hôte d'application et que votre déploiement ne comporte pas de noeud d'application, voir [«Installation d'un hôte d'application»](#), à la page 138.

Si vous possédez un noeud d'application et que vous procédez à une mise à niveau vers 7.4.3, voir [«Migration depuis un noeud d'application vers un hôte d'application»](#), à la page 140.

### Concepts associés

[Applications de sauvegarde et de restauration](#)

IBM QRadar permet de sauvegarder et de restaurer des configurations d'application distinctes des données d'application.

## Installation d'un hôte d'application

Vous pouvez exécuter des applications sur un hôte géré au lieu de votre console pour réduire la charge de traitement sur la console. Installez un hôte d'application de la même manière que n'importe quel autre hôte géré pour QRadar. Vous pouvez installer un hôte d'application sur du matériel ou sur une machine virtuelle en procédant soit à une installation de dispositif, soit à une installation de logiciel.

### Avant de commencer

- Si vous disposez d'un noeud d'application et que vous procédez à une mise à niveau vers la version 7.3.2, voir [«Migration depuis un noeud d'application vers un hôte d'application»](#), à la page 140.
- Cette procédure suppose que vous procédez à une installation de dispositif. Pour plus d'informations sur les environnements de machine virtuelle pris en charge et les installations de logiciels, voir le manuel *IBM QRadar - Guide d'installation*.
- Assurez-vous que toutes les applications (appli QRadar) de votre système sont mises à jour.
- Remédiez à tout problème d'applications à l'état d'erreur ou ne s'affichant pas correctement.
- Planifiez une période de maintenance pour cette tâche et assurez-vous que les utilisateurs n'effectuent aucune des opérations suivantes lors de la migration.
  - Installer ou désinstaller des applications.
  - N'effectuez pas de déploiement complet.
  - Procéder à une restauration.
  - Supprimer l'hôte d'application.
  - Modifier l'IP de la console.

### Procédure

1. Entrez `root` à l'invite de connexion pour lancer l'assistant d'installation. Entrez `password` si vous êtes invité à entrer un mot de passe.
2. Acceptez le **Contrat de licence utilisateur final**.
3. Sélectionnez **App Host Appliance** pour le type de dispositif.
4. Pour le type de configuration, sélectionnez **Normal Setup (default)** et paramétrez l'heure.
5. Sélectionnez la version de protocole IP :



- Sélectionnez **ipv4** ou **ipv6**.
6. Si vous avez sélectionné **ipv6**, sélectionnez **manual** ou **auto** pour l'option **Configuration type**.
  7. Sélectionnez la configuration de l'interface liée, si nécessaire.
  8. Sélectionnez l'interface de gestion.
  9. Dans l'assistant, entrez un nom de domaine complet dans la zone **Hostname**.
  10. Dans la zone **IP address**, entrez une adresse IP statique ou utilisez l'adresse IP affectée.
  11. Si vous ne disposez pas d'un serveur de messagerie, entrez localhost dans la zone **Email server name**.
  12. Entrez un mot de passe `root` qui respecte les critères suivants :
    - Il doit contenir au moins 5 caractères.
    - Il ne doit pas contenir d'espaces.
    - Il peut comporter les caractères spéciaux suivants : @, #, ^ et \*.
  13. Cliquez sur **Terminer**.
  14. Pour effectuer l'installation, suivez les instructions de l'assistant d'installation.

La procédure d'installation peut prendre quelques minutes.
  15. Ajoutez cet hôte géré à votre déploiement et aux modifications de déploiement.

### Que faire ensuite

«Modification de l'emplacement d'exécution des applications», à la page 139

#### Tâches associées

«Ajout d'un hôte géré», à la page 76

## Modification de l'emplacement d'exécution des applications

Modifiez l'emplacement d'exécution des applications lorsque vous ajoutez un hôte d'application à votre déploiement.

### Pourquoi et quand exécuter cette tâche

Les applications sont désactivées lors du processus de transfert. Elles sont activées une fois le transfert terminé.

Si vous ne disposez pas de suffisamment d'espace disque ou de mémoire disponible sur la console, le déplacement de vos applications depuis l'hôte d'application vers la console déplace uniquement les applications mais pas leurs données. Toutes les données d'application restent sur votre hôte d'application, et les applications ne démarrent pas sur la console une fois le transfert terminé. Les applications redémarrent lorsqu'elles sont à nouveau transférées sur l'hôte d'application.

### Procédure

1. Connectez-vous à l'interface utilisateur QRadar.
2. Cliquez sur **Admin**.
3. Dans l'écran **Gestion du système et de la licence**, cliquez sur le lien **Cliquez pour modifier l'emplacement d'exécution des applications**.
4. Choisissez l'emplacement d'exécution des applications.
  - Cliquez sur **Hôte d'applications** pour transférer les applications sur l'hôte d'applications.
  - Cliquez sur **Console** pour transférer des applications à la console.

**Remarque :** Plus vous disposez d'applications et plus la quantité de données d'application est élevée, plus le transfert est long.

## Migration depuis un nœud d'application vers un hôte d'application

Depuis QRadar V7.3.2, les nœuds d'application ne sont plus pris en charge. Si vous effectuez une mise à niveau vers QRadar 7.4.3 et que vous disposez d'un nœud d'application dans votre déploiement, vous devez sauvegarder les données de votre nœud d'application avant de terminer la mise à niveau. Vous pouvez réutiliser le nœud d'application comme hôte d'application après avoir sauvegardé ses données et l'avoir retiré du déploiement. Vous pouvez utiliser un autre dispositif à la place de votre dispositif nœud d'application pour réduire le risque de perte de données.

### Avant de commencer

- Si vous installez un hôte d'application et que votre déploiement ne comporte pas de nœud d'application, voir «[Installation d'un hôte d'application](#)», à la page 138.
- Vous devez contacter Q1PD@us.ibm.com pour vérifier que les autorisations requises sont configurées pour la migration depuis le nœud d'application vers l'hôte d'application. La ligne d'objet de votre e-mail doit s'intituler App Node to App Host migration (Migration du nœud d'application vers l'hôte d'application).
- Assurez-vous que toutes les applications (appli QRadar) de votre système sont mises à jour.
- Remédiez à tout problème d'applications à l'état d'erreur ou ne s'affichant pas correctement.
- Planifiez une période de maintenance pour cette tâche et assurez-vous que les utilisateurs n'effectuent aucune des opérations suivantes lors de la migration.
  - Installer ou désinstaller des applications.
  - N'effectuez pas de déploiement complet.
  - Procéder à une restauration.
  - Supprimer l'hôte d'application.
  - Modifier l'IP de la console.

### Pourquoi et quand exécuter cette tâche

Pour migrer d'un nœud d'application vers un hôte d'application, procédez comme suit.

**Remarque :** IBM ne prend pas en charge la migration des applications d'une console à deux piles vers un hôte d'application.

### Procédure

1. Utilisez **ssh** pour vous connecter à la console en tant qu'utilisateur **root**.
2. Montez le fichier SFS QRadar 7.4.3 sur la console dans `/media/updates`.
3. Créez une archive de sauvegarde des données de votre nœud d'application et retirez le nœud d'application du déploiement en saisissant la commande suivante sur la console :

```
/media/updates/supplementary_scripts/app_node_data_backup.py
```

Le script génère une archive de sauvegarde sur le nœud d'application appelé `/store/app-docker-volumes-<date_and_time_stamp>.tgz` et un total de contrôle MD5.



**Avertissement :** Il n'existe pas de mode test pour ce script. Le script retire le nœud d'application de votre déploiement.

4. Pour vérifier la validité de l'archive de sauvegarde, entrez la commande suivante :

```
tar -tzf app-docker-volumes-<date_and_time_stamp>.tgz
```

La sortie devrait être semblable à cet exemple :

```
qapp-1002/  
qapp-1002/log/  
qapp-1002/log/startup.log
```

```
qapp-1002/log/supervisord.log
qapp-1002/log/app.log
qapp-1003/
qapp-1003/log/
qapp-1003/log/startup.log
qapp-1003/log/poll.log
qapp-1003/log/supervisord.log
qapp-1003/log/app.log
qapp-1003/config.db
```

5. Créez une copie de l'archive de sauvegarde et notez la somme de contrôle MD5.

**Remarque :** Une somme de contrôle MD5 d41d8cd98f00b204e9800998ecf8427e équivaut à un fichier à zéro octet. Cela peut signifier qu'il n'y a pas suffisamment d'espace pour le fichier de sauvegarde. Pour obtenir des informations relatives au traitement des incidents, voir [«Traitement des incidents liés à la migration d'un nœud d'application vers une application hôte»](#), à la page 142.

Pour créer une copie de l'archive de sauvegarde sur votre console, entrez les commandes suivantes sur celle-ci :

- a) Entrez la commande suivante pour créer un répertoire de sauvegarde du nœud d'application sous /store.

```
mkdir /store/app_node_backup
```

- b) Entrez la commande suivante pour copier l'archive de sauvegarde du nœud d'application dans le répertoire de sauvegarde de la console.

```
scp root@<appnode_IP_address>:/store/app-docker-volumes-<date_and_time_stamp>.tgz /store/app_node_backup/
```

- c) Vérifiez la somme de contrôle MD5 de la copie de l'archive de sauvegarde sur votre console en entrant la commande suivante et en comparant le résultat à la somme de contrôle de l'archive sur votre nœud d'application.

```
md5sum /store/app_node_backup/app-docker-volumes-<date_and_time_stamp>.tgz
```

6. Mettez à niveau QRadar Console vers 7.4.3.
7. Installez votre hôte d'application et ajoutez-le au déploiement. Voir [«Installation d'un hôte d'application»](#), à la page 138.
8. Copiez l'archive de sauvegarde sur l'hôte d'application.
9. Restaurez les données du nœud d'application sur l'hôte d'application en saisissant la commande suivante sur la console.

```
/opt/qradar/bin/app_node_data_restore.py -a <apphost_IP_address> -f <path_to_archive_on_apphost>
```

Exemple :

```
/opt/qradar/bin/app_node_data_restore.py -a 192.0.2.4 -f /store/app-docker-volumes-2019XXXXXXXXXX.tgz
```

Le script contrôle l'intégrité de l'archive en confirmant la somme de contrôle MD5, puis extrait l'archive dans le répertoire /store/docker/volumes.

10. Connectez-vous à l'interface utilisateur QRadar.
11. Cliquez sur **Admin**.
12. Sur l'écran **Gestion du système et de la licence**, cliquez sur **Migrer**.
13. Cliquez sur **Continuer** pour terminer la migration du nœud d'application vers l'hôte d'application.

**Remarque :** Plus vous disposez d'applications et plus la quantité de données d'application est élevée, plus le transfert est long.

## Résultats

Vos applications s'exécutent maintenant sur l'hôte d'application.

## Traitement des incidents liés à la migration d'un nœud d'application vers une application hôte

Vous pouvez identifier et résoudre les problèmes suivants si vous les avez en rapport avec la migration de votre nœud d'application vers l'hôte d'application.

### La somme de contrôle de sauvegarde du nœud d'application MD5 est **d41d8cd98f00b204e9800998ecf8427e**

Une somme de contrôle MD5 de D41d8cd98f00b204e9800998ecf8427e indique que le fichier de sauvegarde du nœud d'application est un fichier de zéro octet. L'espace disque disponible pour le fichier de sauvegarde est insuffisant. Si vous recevez cette valeur pour le total de contrôle :

1. Utilisez **ssh** pour vous connecter à votre nœud d'application en tant que superutilisateur.
2. Entrez la commande suivante et notez l'espace disponible dans `/store`.

```
df -h /store
```

3. Entrez la commande suivante et notez l'espace utilisé dans `/store/backup/marathon`.

```
du -hs /store/backup/marathon/
```

4. Entrez la commande suivante et notez l'espace utilisé dans `/store/docker/volumes`.

```
du -hs /store/docker/volumes/
```

5. Comparez l'espace total utilisé par `/store/docker/volumes` à l'espace total disponible dans `/store`. Vous avez besoin d'au moins 1 à 1,5 fois plus d'espace disponible dans `/store` que l'espace utilisé par `/store/docker/volumes`. Si vous ne disposez pas de suffisamment d'espace disponible dans `/store`, vérifiez si vous disposez de suffisamment d'espace utilisé dans `/store/backup/marathon` pour faire la différence.

Par exemple, si l'espace utilisé par `/store/docker/volumes` est de 100 Go et que l'espace disponible dans `/store` est de 90 Go, vous ne disposez pas de suffisamment d'espace disponible pour le fichier de sauvegarde. Si `/store/backup/marathon` utilise 10 Go ou plus d'espace, vous pouvez libérer de l'espace dans `/store/backup/marathon`.

6. Sauvegardez et supprimez des fichiers de `/store/backup/marathon` pour libérer de l'espace en procédant comme suit :
  - a. Sur la console, créez un répertoire de sauvegarde de nœud d'application sous `/store` en entrant la commande suivante.

```
mkdir /store/app_node_backup
```

- b. Copiez les fichiers de sauvegarde du marathon à partir du nœud d'application vers la console en entrant la commande suivante.

```
scp root@<appnode_IP_address>:/store/backup/marathon/backup.marathon-volumes.qapp.*.tgz /store/app_node_backup/
```

- c. Vérifiez la somme de contrôle MD5 des fichiers de sauvegarde du marathon sur la console en tapant la commande suivante.

```
ls /store/app_node_backup/backup.marathon-volumes.qapp.*.tgz | xargs md5sum
```

- d. Sur le nœud d'application, vérifiez la somme de contrôle MD5 des fichiers de sauvegarde du marathon en tapant la commande suivante.

```
ls /store/backup/marathon/backup.marathon-volumes.qapp.*.tgz | xargs md5sum
```

- e. Vérifiez que les deux valeurs de total de contrôle sont identiques. Si tel est le cas, supprimez les fichiers de sauvegarde marathon du nœud d'application en tapant la commande suivante sur le nœud d'application.



**Avertissement :** La commande **rm -rf** supprime un répertoire et tous les fichiers qui y sont fichiers. Vérifiez que vous entrez la commande exactement comme indiqué ici.

```
rm -rf /store/backup/marathon/*
```

7. Exécutez le script de sauvegarde des données du nœud d'application en suivant l'étape 3 dans «[Migration depuis un nœud d'application vers un hôte d'application](#)», à la page 140, et effectuez cette procédure.

## Suppression d'un hôte d'application

Vous ne pouvez pas supprimer un hôte d'application si vous avez des applications qui s'exécutent dessus.

### Procédure

1. Remplacez vos applications dans la console. Voir «[Modification de l'emplacement d'exécution des applications](#)», à la page 139.

**Remarque :** Si vous n'avez pas assez d'espace disque ou de mémoire disponible sur la console, le déplacement de vos applications vers la console ne déplace que les applications elles-mêmes, mais pas les données d'application. Toutes les données d'application restent sur votre hôte d'application.

2. Cliquez sur **Admin**.
3. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
4. Dans la liste **Afficher**, sélectionnez **Systèmes**.
5. Sélectionnez votre hôte d'application.
6. Dans le menu **Actions de déploiement**, cliquez sur **Supprimer un hôte**.

## Vérification de l'intégrité des journaux des événements et des flux

Lorsque le hachage de journal est activé, tout système qui écrit des données d'événement et de flux crée des fichiers de hachage. Utilisez ces fichiers de hachage pour vérifier que les journaux d'événements et de flux n'ont pas été modifiés depuis qu'ils ont été écrits sur le disque.

Les fichiers de hachage sont générés en mémoire avant que les fichiers ne soient écrits sur le disque, de sorte que les journaux d'événements et de flux ne peuvent pas être altérés avant que les fichiers de hachage ne soient générés.

### Avant de commencer

Vérifiez que le hachage des journaux est activé pour votre système IBM QRadar. Pour plus d'informations sur l'activation du hachage des journaux, voir «[Activation du réadressage calculé de journal](#)», à la page 144.

### Pourquoi et quand exécuter cette tâche

Vous devez vous connecter au système qui dispose de la mémoire de données pour les événements et les flux, et exécuter un utilitaire pour vérifier les journaux. Vous ne pouvez pas vérifier l'intégrité du journal dans l'interface de l'afficheur d'événements et de flux.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Pour exécuter l'utilitaire, entrez la commande suivante :

```
/opt/qradar/bin/check_ariel_integrity.sh -d <duration> -n <database name>
[-t <endtime>] [-a <hash algorithm>] [-r <hash root directory>] [-k <hmac key>]
```

Ce tableau décrit les paramètres utilisés avec l'utilitaire **check\_ariel\_integrity.sh**.

Paramètre	Description
<b>-d</b>	Durée, en minutes, des données du fichier journal à analyser. La période précède immédiatement l'heure de fin qui est spécifiée en utilisant le paramètre <b>-t</b> . Par exemple, si <b>-d 5</b> est entré, toutes les données de journal qui ont été collectées cinq minutes avant l'heure de fin <b>-t</b> sont analysées.
<b>-n</b>	Base de données QRadar à analyser. Les options valides sont événements et flux.
<b>-t</b>	Heure de fin de l'analyse. Le format de l'heure de fin est "Aaaa/mm/jj hh:mm", où hh est indiqué au format 24 heures. Si aucune heure de fin n'est entrée, l'heure actuelle est utilisée.
<b>-a</b>	Algorithme de hachage à utiliser. Cet algorithme doit être le même que celui utilisé pour créer les clés de hachage. Si aucun algorithme n'est entré, SHA-1 est utilisé.
<b>-r</b>	Emplacement du hachage du journal. Cet argument est requis uniquement lorsque le hachage de journal n'est pas à l'emplacement spécifié dans le fichier de configuration, /opt/qradar/conf/arielConfig.xml.
<b>-k</b>	Clé utilisée pour le chiffrement HMAC (Message Authentication Code) à base de hachage. Si vous ne spécifiez pas de clé HMAC et que votre système est activé pour le chiffrement HMAC, le script <b>check_ariel_integrity.sh</b> prend par défaut la clé spécifiée dans les paramètres système.
<b>-h</b>	Affiche le message d'aide de l'utilitaire <b>check_ariel_integrity.sh</b> .

Par exemple, pour valider les 10 dernières minutes des données d'événement, entrez la commande suivante :

```
/opt/qradar/bin/check_ariel_integrity.sh -n events -d 10
```

## Résultats

Si un message ERROR ou FAILED est renvoyé, la clé de hachage qui est générée à partir des données en cours sur le disque ne correspond pas à la clé de hachage qui a été créée lors de l'écriture des données sur le disque. La clé ou les données ont été modifiées.

## Activation du réadressage calculé de journal

Activez le réadressage calculé de journal pour que tout système qui écrit des données d'événement et de flux crée des fichiers de réadressage calculé. Utilisez ces fichiers de hachage pour vérifier que les journaux d'événements et de flux n'ont pas été modifiés depuis qu'ils ont été écrits sur le disque. Les fichiers de hachage sont générés en mémoire avant que les fichiers ne soient écrits sur le disque, de sorte que les journaux d'événements et de flux ne peuvent pas être altérée avant que les fichiers de hachage ne soient générés.

### Pourquoi et quand exécuter cette tâche

Le système utilise les types d'algorithme de hachage suivants :

#### Algorithme de hachage de Message-Digest

Transforme les signatures numériques en valeurs plus courtes appelées Message-Digests (MD).

#### Algorithme de hachage SHA (Secure Hash Algorithm)

Algorithme standard qui crée un plus grand (60 bits) MD.

## Procédure

1. Sous l'onglet **Admin**, cliquez sur **Paramètres système**.
2. Dans la section Paramètres de base de données Ariel, sélectionnez **Oui** dans la zone **Hachage du journal de flux** et dans la zone **Hachage du journal des événements**.
3. Sélectionnez un algorithme de hachage pour l'intégrité de la base de données.
  - Si le paramètre **Chiffrement HMAC** est désactivé, les options d'algorithme de hachage suivantes sont disponibles :
    - MD2**  
Algorithme défini par la RFC 1319.
    - MD5**  
Algorithme défini par la RFC 1321.
    - SHA-1**  
Algorithme défini par la norme SHS (Secure Hash Standard), NIST FIPS 180-1. Il s'agit de la sélection par défaut.
    - SHA-256**  
Algorithme défini par l'ébauche de la norme fédérale de traitement de l'information 180-2, SHS. SHA-256 est un algorithme de hachage 255 bits destiné à une sécurité 128 bits contre les attaques de la sécurité.
    - SHA-384**  
Algorithme défini par l'ébauche de la norme fédérale de traitement de l'information 180-2, SHS. SHA-384 est un algorithme de hachage de bit, créé en tronquant la sortie SHA-512.
    - SHA-512**  
Algorithme défini par l'ébauche de la norme fédérale de traitement de l'information 180-2, SHS. SHA-512 est un algorithme de hachage de bit destiné à assurer une sécurité 256 bits.
  - Si le paramètre **Chiffrement HMAC** est activé, les options d'algorithme de hachage suivantes sont disponibles :
    - HMAC-MD5**  
Méthode de chiffrement basée sur l'algorithme de hachage MD5.
    - HMAC-SHA-1**  
Méthode de chiffrement basée sur l'algorithme de hachage SHA-1.
    - HMAC-SHA-256**  
Méthode de chiffrement basée sur l'algorithme de hachage SHA-256.
    - HMAC-SHA-384**  
Méthode de chiffrement basée sur l'algorithme de hachage SHA-384.
    - HMAC-SHA-512**  
Méthode de chiffrement basée sur l'algorithme de hachage SHA-512.
4. Cliquez sur **Sauvegarder**.

## Ajout d'actions personnalisées

---

Associez des scripts à des règles personnalisées pour effectuer des actions spécifiques en réponse à des événements réseau. Utilisez la fenêtre **Actions personnalisées** pour gérer les scripts d'action personnalisée.


Utilisez des actions personnalisées pour sélectionner ou définir la valeur transmise au script et l'action qui en résulte.

Par exemple, vous pouvez écrire un script pour créer une règle de pare-feu qui bloque une adresse IP source de votre réseau en réponse à une règle qui est déclenchée par un nombre défini d'échecs de tentative de connexion.

Les exemples suivants sont des actions personnalisées qui sont le résultat de la transmission de valeurs à un script :

- Blocage d'utilisateurs et de domaines.
- Initiation de flux de travaux et mises à jour sur des systèmes externes.
- Mise à jour de serveurs TAXI avec une représentation STIX d'une menace.

Les actions personnalisées fonctionnent mieux avec des événements de règle personnalisés à faible volume et avec des règles personnalisées dont la valeur du limiteur de réponse est faible.

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Actions personnalisées**, cliquez sur **Définir des actions**.
3. Pour télécharger vos scripts, cliquez sur **Ajouter**. Les versions de langage de programmation prises en charge par le produit sont répertoriées dans la liste **Interprète**.

Pour la sécurité de votre déploiement, QRadar ne prend pas en charge la gamme complète des fonctionnalités de scripting fournies par les langages Python, Perl ou Bash.

4. Indiquez les paramètres que vous souhaitez transmettre au script que vous avez téléchargé.

Paramètre	Description
<b>Fixed property</b>	Valeurs transmises au script d'action personnalisée.  Elles ne sont pas basées sur les événements ou les flux eux-mêmes, mais elles couvrent les autres valeurs définies que vous pouvez utiliser pour une action du script. Par exemple, transmettre les propriétés fixes <b>username</b> et <b>password</b> pour un système tiers à un script pour envoyer une alerte SMS.  Chiffrez les propriétés fixes en cochant la case <b>Chiffrer la valeur</b> .
<b>Network event property</b>	Propriétés Ariel dynamiques générées par des événements. Faites une sélection dans la liste <b>Propriété</b> .  Par exemple, la propriété d'événement de réseau <b>sourceip</b> fournit un paramètre qui correspond à l'adresse IP source de l'événement déclenché.  Pour plus d'informations sur les caractéristiques Ariel, voir <i>IBM QRadar Ariel Query Language Guide</i> .

Les paramètres sont transmis dans votre script dans l'ordre dans lequel vous les avez ajoutés dans la fenêtre **Actions personnalisées**.

Lorsque des scripts d'action personnalisés sont exécutés, un `chroot jail` est configuré dans le répertoire `/opt/qradar/bin/ca_jail/`. Tout contenu du répertoire `/opt/qradar/bin/ca_jail/` peut être modifié et écrit par des scripts. Le répertoire de base de l'utilisateur d'action personnalisée (`/home/customactionuser`) peut également être modifié.

Un script ne peut s'exécuter qu'à l'intérieur de l'environnement de prison de sorte qu'il n'interfère pas avec l'environnement d'exécution QRadar. Tous les accès aux fichiers lors de l'exécution de l'action personnalisée sont relatifs au répertoire `/opt/qradar/bin/ca_jail/`.

Le compte utilisateur d'action personnalisée n'est peut-être pas autorisé à exécuter des commandes de suivi, telles que la connexion à un pare-feu et le blocage d'une adresse IP. Testez si votre script s'exécute avec succès avant de l'associer à une règle.

**Remarque :** Le type d'action personnalisée que vous implémentez dépend de votre infrastructure réseau et de ses composants. Par exemple, vous pouvez configurer des API REST sur des périphériques Cisco pour bloquer les adresses IP suspectes. Il se peut que d'autres fournisseurs tiers ne fournissent pas



d'interface REST, vous pouvez donc avoir besoin de développer votre propre solution de services Web pour exécuter des actions personnalisées.

Vous devez exécuter l'utilitaire dos2unix sur des scripts provenant d'un système Windows ou DOS. Les systèmes Windows ou DOS ajoutent généralement des caractères de contrôle. Pour tester avec succès des scripts d'action personnalisés à l'aide de la fonction script **Exécution de test** dans QRadar, vous devez supprimer les caractères de contrôle.

#### Information associée

[Présentation des scripts d'action personnalisée](#)

## Test de votre action personnalisée

Testez si votre script s'exécute correctement et si le résultat prévu est avant de l'associer à une règle.


### Pourquoi et quand exécuter cette tâche

Les scripts d'action personnalisée s'exécutent dans un environnement de test isolé de votre environnement de production. Les scripts d'action personnalisés s'exécutent généralement sur l'hôte géré qui exécute le processeur d'événements. Toutefois, si vous disposez d'un dispositif All-In-One, les actions personnalisées s'exécutent sur QRadar Console.

**L'exécution de test** est prise en charge uniquement sur QRadar Console et n'est pas prise en charge sur les hôtes gérés.

Si vous devez écrire sur le disque à partir d'un script d'action personnalisé, vous devez utiliser le répertoire suivant : `/home/customactionuser`.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Actions personnalisées**, cliquez sur **Définir des actions**.
3. Sélectionnez une action personnalisée dans la liste et cliquez sur **Exécution de test** > **Exécuter** pour tester votre script. Le résultat du test et de toute sortie produite par le script est renvoyé.
4. Une fois que vous avez configuré et testé votre action personnalisée, utilisez l'**Assistant Règle** pour créer une nouvelle règle d'événement et lui associer l'action personnalisée.

Pour plus d'informations sur les règles d'événements, voir *IBM QRadar - Guide d'utilisation*.

#### Information associée

[Comment configurer des actions de règle dans ? \(cours Security Learning Academy\)](#)

## Transmission de paramètres à un script d'action personnalisé

Des exemples de scripts dans Bash, Python et Perl montrent comment transmettre des paramètres à des scripts d'action personnalisés.

Les exemples de scripts simples suivants montrent comment interroger l'API de modèle d'actif pour un actif avec l'adresse IP source de l'infraction fournie. Dans l'intérêt de cet exemple, les scripts extraient le JSON renvoyé par le nœud final.

Les scripts nécessitent trois paramètres :

- Adresse IP de la console
- API token
- Adresse IP source d'infraction

Ces paramètres sont configurés dans la zone **Paramètres de script** de la fenêtre Définir une action personnalisée :

**Define Custom Action**

Script File:

File will upload on save.

**Script Parameters**

Parameter Name:

Fixed Property

Network Event Property

Property:

Name	Type	Value
console_ip	Fixed Property	
api_token	Fixed Property	4e176ca6-a46a-3471-8211-45f3d7f2693e
offense_source_ip	Network Event Property	sourceip

Figure 8. Paramètres de script d'action personnalisée

Chaque paramètre est transmis au script dans l'ordre dans lequel il a été ajouté dans la fenêtre Définir une action personnalisée. Dans ce cas :

1. console\_ip
2. api\_token
3. offense\_source\_ip

**Important :** Cet exemple contient une propriété d'événement réseau. Pour que l'exemple de script soit exécuté avec succès sur la page de test, vous devez affecter une adresse IP source (xx.xx.xx.xx) en tant que valeur de propriété fixe à **Infraction\_source\_ip**.

Les variables définies au début de chaque exemple de script utilisent les exemples de noms de paramètre qui ont été ajoutés dans la fenêtre Définir une action personnalisée.

```
#!/bin/bash
console_ip=$1
api_token=$2
offense_source_ip=$3

auth_header="SEC:$api_token"

output=$(curl -k -H $auth_header https://$console_ip/console/restapi/api/
asset_model/assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29)

# Basic print out of the output of the command
echo $output
```

Figure 9. call\_asset\_model.sh

```
#!/usr/bin/python
import sys
import requests
console_ip = sys.argv[1]
api_token = sys.argv[2]
offense_source_ip = sys.argv[3]

auth_header = {'SEC' : api_token }

endpoint = "https://{0}/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22%21%22%29%29"
.format(console_ip, offense_source_ip)

response = requests.get(endpoint, headers=auth_header, verify=False)

# Basic print out of the output of the command
print(response.json())
```

Figure 10. *call\_asset\_model.py*

```
#!/usr/bin/perl
use strict;
use warnings;
use LWP::UserAgent;

my $console_ip = $ARGV[0];
my $api_token = $ARGV[1];
my $offense_source_ip = $ARGV[2];

my $endpoint = "https://$console_ip/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22%21%22%29%29";

my $client = LWP::UserAgent -> new(ssl_opts => { verify_hostname => 0 });

my $response = $client -> get($endpoint, "SEC" => $api_token);

# Basic print out of the output of the command
print $response -> decoded_content;
```

Figure 11. *call\_asset\_model.pl*

## Gestion des vues de données agrégées

Un volume important d'agrégation de données peut réduire les performances de votre système. La fonction Ariel utilise une base de données distincte pour les données agrégées afin d'améliorer les performances du système et de rendre les données plus facilement disponibles. Vous pouvez désactiver, activer ou supprimer des vues de données agrégées. Les graphiques de série temporelle, graphiques de rapport et règles d'anomalie utilisent des vues de données agrégées.

### Pourquoi et quand exécuter cette tâche


Les éléments qui apparaissent dans la liste **Afficher** trient les données.

La vue Données agrégées est requise pour générer des données pour les règles ADE, les graphiques de série temporelle et les rapports.

Désactivez ou supprimez les vues si le nombre maximum de vues est atteint.

Les vues en double peuvent apparaître dans la colonne **ID données agrégées** car une vue de données agrégées peut inclure plusieurs recherches.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des données agrégées**.
3. Pour filtrer la liste des vues de données agrégées, effectuez l'une des options suivantes :


- Sélectionnez une option dans la liste **Afficher, Base de données, Afficher** ou **Afficher**.
  - Entrez dans la zone de recherche un ID de données agrégées, un nom de rapport, un nom de graphique ou un nom de recherche sauvegardée.
4. Pour gérer une vue de données agrégée, sélectionnez la vue, puis cliquez sur l'action appropriée dans la barre d'outils :
- Si vous sélectionnez **Désactiver la vue** ou **Supprimer la vue**, les dépendances de contenu s'affichent pour la vue de données agrégée. Une fois que vous avez désactivé ou supprimé la vue, les composants dépendants n'utilisent plus les données agrégées.
  - Activez une vue de données agrégées précédemment désactivée pour restaurer la vue.

<i>Tableau 27. Descriptions des colonnes de la vue Gestion de données agrégées</i>	
<b>Colonne</b>	<b>Description</b>
ID données agrégées	Identificateur des données agrégées
Nom de la recherche sauvegardée	Nom défini pour la recherche sauvegardée
Nom de la colonne	Identificateur de colonne
Recherches de temps	Nombre de recherches
Données écrites	Taille des données écrites
Database Name	Base de données dans laquelle le fichier a été écrit
Heure de la dernière modification	Horodatage de la dernière modification de données
Comptage unique activé	Vrai ou Faux : Recherchez les résultats pour afficher l'événement unique et les comptes de flux au lieu des comptes moyens dans le temps.

## Accès à une base de données GLOBALVIEW

Utilisez l'interface de documentation de l'API REST QRadar pour obtenir les résultats de la base de données GLOBALVIEW pour un nom de recherche sauvegardée et une plage de temps donnés. Le type de données contenues dans les résultats de la base de données correspond au type de recherche enregistrée interrogée.

### Procédure

1. Rechercher une recherche sauvegardée.
  - a) Dans le menu de navigation () , cliquez sur **Admin**.
  - b) Dans la section **Configuration du système**, cliquez sur **Gestion des données agrégées**.
  - c) Dans la colonne **Nom de recherche sauvegardée**, enregistrez un nom de recherche enregistré dans la liste.
2. Interrogation de l'API REST QRadar pour rechercher un ID de recherche.
  - a) Connectez-vous à l'API QRadar, [https://<Console IP>/api\\_doc](https://<Console IP>/api_doc), en tant qu'administrateur.
  - b) Cliquez sur la version la plus récente de l'API QRadar.
  - c) Cliquez sur le nœud final `/ariel/searches`.
  - d) Cliquez sur **Publier**.
  - e) Dans la zone de paramètre **query\_expression**, entrez la commande suivante : `select * from GLOBALVIEW('savedsearch', 'timerange')`

Utilisez l'une des valeurs suivantes pour la variable *Timerange* :

```
NORMAL  
HOURLY  
DAILY
```

L'exemple suivant montre une requête pour les principales sources de journal avec une plage de temps des deux derniers jours :

```
select * from GLOBALVIEW('Top Log Sources', 'DAILY') last 2 days
```

- f) Cliquez sur **Essayer**
  - g) Copiez l'ID de recherche dans le corps de la réponse.
3. Obtenez les résultats de la recherche.
- a) À partir du nœud final `/ariel/searches/search{id}/results`, cliquez sur **UTILISER**.
  - b) Dans la zone de paramètre **search\_id**, entrez l'ID de recherche.
  - c) Cliquez sur **Essayer**.
  - d) Vérifiez que la recherche est terminée.
  - e) Récupérez les résultats de la base de données à partir du corps de la réponse.



---

# Chapitre 7. Traitement des données d'événement dans QRadar

Dans IBM QRadar, utilisez l'éditeur DSM pour résoudre les problèmes d'analyse syntaxique et ajouter l'analyse personnalisée.

L'éditeur DSM fournit des commentaires en temps réel afin que vous sachiez si votre personnalisation fonctionne comme vous le souhaitez.

## Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Présentation de DSM Editor

Plutôt que de créer manuellement une extension de source de journal pour corriger des problèmes d'analyse syntaxique ou étendre le support à de nouveaux types de source de journal, utilisez l'éditeur DSM. Celui-ci propose différentes vues de vos données. L'éditeur DSM permet d'extraire des zones, de définir des propriétés personnalisées, de catégoriser des événements et de définir une nouvelle définition QID.

L'éditeur DSM fournit les vues suivantes :

### Espace de travail

L'**Espace de travail** affiche les données d'événement brutes. Utilisez des exemples de charges utiles pour tester le comportement du type de source de journal, puis la zone **Espace de travail** vous montre les données que vous capturez en temps réel.

Tous les exemples d'événement sont envoyés depuis l'espace de travail au simulateur DSM, où les propriétés sont analysées syntaxiquement et les mappes QID sont recherchées. Les résultats s'affichent dans la section **Aperçu de l'activité de journal**. Cliquez sur l'icône d'édition pour passer en mode édition.

En mode édition, vous collez jusqu'à 100 000 caractères de données d'événement dans l'espace de travail ou éditez les données directement. Lorsque vous éditez des propriétés dans l'onglet **Propriétés**, les correspondances dans la charge sont mises en évidence dans l'espace de travail. Les propriétés personnalisées et les propriétés système remplacées sont également mises en évidence dans **Espace de travail**.

**Nouveautés de la version 7.4.1** Vous pouvez indiquer un délimiteur personnalisé qui facilite l'ingestion d'événements multilignes par QRadar . Pour vous assurer que votre événement est conservé sous la forme d'un événement multiligne, sélectionnez la case à cocher **Outrepasser le délimiteur d'événements** pour séparer les événements individuels via l'utilisation d'un autre caractère ou d'une suite de caractères. Par exemple, si votre configuration intègre des événements multilignes, vous pouvez ajouter un caractère spécial à la fin de chaque événement distinct dans l'**Espace de travail** puis identifier ce caractère spécial comme délimiteur d'événement.

**Nouveautés de la version 7.4.2** QRadar peut suggérer des expressions régulières (regex) lorsque vous entrez des données d'événement dans l'**Espace de travail**. Si vous n'êtes pas habitué à créer des expressions régulières, utilisez cette fonction pour cela. Mettez en évidence le texte que vous souhaitez capturer puis dans l'onglet **Propriétés**, cliquez sur **Suggérer une expression régulière**. L'expression suggérée s'affiche dans la zone **Expression**. Vous pouvez également cliquer sur le bouton **Expression régulière** dans l'**Espace de travail** puis sélectionner la propriété pour laquelle créer une expression. Si QRadar ne parvient pas à générer un regex approprié pour votre échantillon de données, un message système s'affiche.

**Conseil :** Le générateur d'expression régulière est particulièrement adapté pour les zones des contenus d'événement bien structurés. Si le contenu se compose de données complexes (langage naturel ou

événements non structurés), le générateur d'expression régulière peut ne pas pouvoir l'analyser et ne renvoie alors pas de résultat.

## Aperçu de l'activité des journaux

Nouveautés de la version 7.4.1 La colonne **État d'Analyse Syntaxique** a été ajoutée à l'aperçu de l'Activité de Journal.

L'**Aperçu de l'activité de journal** simule le mode d'affichage des charges dans l'espace de travail dans l'afficheur **Activité de journal**. La colonne de statut d'analyse indique si l'analyse de vos propriétés d'événement s'effectue correctement et si ces dernières sont correctement mappées à un enregistrement QID. Toutes les propriétés standard prises en charge sont affichées. Les champs marqués d'un astérisque (\*), par exemple, **Event name, Severity, Low-level category** et **QID**, sont remplis à partir de la mappe QID. Les zones qui sont renseignées à partir de la mappe QID ne peuvent pas être analysées textuellement à partir des données d'événements brutes de l'espace de travail, de sorte qu'elles ne peuvent pas être définies ou éditées. Vous pouvez ajuster leurs valeurs en sélectionnant l'ID d'événement et la combinaison de catégories correspondants dans l'onglet **Mappages d'événements**. Cliquez ensuite sur **Éditer** pour mapper à nouveau un événement à un autre enregistrement QID existant dans le système ou à un QID nouvellement créé.

**Important :** Vous devez définir un **Event ID** pour que toutes les propriétés du système soient analysées correctement.

Cliquez sur l'icône de configuration pour sélectionner les colonnes à afficher ou à masquer dans la fenêtre **Aperçu de l'activité de journal** et réorganiser les colonnes.

## Propriétés

L'onglet **Propriétés** contient l'ensemble de propriétés système et personnalisées qui constituent une configuration DSM. La configuration d'une propriété système diffère de la configuration d'une propriété personnalisée. Vous pouvez remplacer une propriété en cochant la case **Remplacer le comportement du système** et en définissant l'expression.

**Remarque :** Si vous remplacez la propriété **Catégorie d'événement**, vous devez également remplacer la propriété **ID événement**.

Les correspondances dans le contenu sont mises en évidence dans les données d'événement dans l'espace de travail. Il existe deux couleurs de mise en évidence, selon l'élément que vous capturez. Par exemple, la valeur du groupe de capture est mise en évidence en orange alors que le reste de l'expression régulière que vous avez spécifiée est mis en évidence en jaune. Le commentaire en retour dans l'espace de travail indique si l'expression régulière est correcte. Si une expression est sélectionnée, la mise en évidence dans l'espace de travail reflète uniquement les correspondances que vous pouvez obtenir avec cette expression. Si la propriété générale est sélectionnée, la mise en évidence est en vert et indique les correspondances pouvant être obtenues avec l'ensemble agrégé d'expressions, en prenant en compte l'ordre de priorité.

Dans la zone **Chaîne de format**, les groupes de capture sont représentés à l'aide de la notation  $\$<number>$ . Ainsi, \$1 représente le premier groupe de capture de l'expression régulière, \$2 le deuxième, et ainsi de suite.

Vous pouvez ajouter plusieurs expressions à une même propriété et affecter une priorité en faisant glisser les expressions et en les déposant en haut de la liste.

Une icône d'avertissement en regard d'une propriété indique qu'aucune expression n'a été ajoutée.

## Onglet Mappages d'événements

Nouveautés de la version 7.4.1 La prise en charge de la copie des champs d'ID d'Événement et de Catégorie d'Événement a été ajoutée à l'onglet **Mappage d'Événement**.

L'onglet **Mappages d'événements** affiche tous les ID d'événement et les combinaisons de catégories existant dans le système pour un type de source de journal sélectionné. Si un nouveau mappage



d'événements est créé, il est ajouté à la liste des combinaisons d'ID d'événement et de catégories qui s'affiche dans l'onglet **Mappages d'événements**. En général, l'onglet **Mappages d'événements** affiche tous les ID d'événement et les combinaisons de catégories ainsi que les enregistrements QID auxquels ils sont mappés.

## Onglet Configuration

Vous pouvez configurer la reconnaissance de propriété automatique pour les données structurées au format JSON. Par défaut, les types de source de journal disposent d'une reconnaissance de propriété automatique désactivée.

Lorsque vous activez **Reconnaissance de propriété automatique** dans l'onglet **Configuration**, le moteur de reconnaissance de propriétés génère automatiquement de nouvelles propriétés pour capturer toutes les zones présentes dans les événements reçus par un type de source de journal. Vous pouvez configurer le nombre d'événements consécutifs à inspecter pour les nouvelles propriétés dans la zone **Seuil d'achèvement de la reconnaissance**. Les propriétés nouvellement reconnues apparaissent dans l'onglet **Propriétés** et sont mises à disposition pour être utilisées dans les règles et les index de recherche. Toutefois, si aucune nouvelle propriété n'est reconnue avant le seuil, le processus de reconnaissance est considéré comme terminé et **Reconnaissance de propriété automatique** pour ce type de source de journal est désactivé. Vous pouvez activer manuellement la reconnaissance de propriété automatique dans l'onglet Configuration à tout moment.

**Remarque :** Pour inspecter en permanence les événements pour un type de source de journal, vous devez vous assurer que vous avez défini la valeur **Seuil d'achèvement de la reconnaissance** sur 0.

### Concepts associés

Propriétés dans l'éditeur DSM

Dans l'éditeur DSM, les propriétés système normalisées sont combinées avec des propriétés personnalisées et sont triées par ordre alphabétique.

## Propriétés dans l'éditeur DSM

---

Dans l'éditeur DSM, les propriétés système normalisées sont combinées avec des propriétés personnalisées et sont triées par ordre alphabétique.

Un DSM ne peut pas avoir plusieurs propriétés portant le même nom.

La configuration d'une propriété système diffère d'une propriété personnalisée.

### Propriétés système

Les propriétés système ne peuvent pas être supprimées, mais vous pouvez ignorer le comportement par défaut. Il existe deux types de propriétés système :

#### Propriété système prédéfinie

Affiche le comportement QRadar par défaut utilisé pour le DSM.

#### Ignorer la propriété système

Les propriétés du système avec substitution configurée (extension de source de journal) affichent **Override** dans la ligne d'état. Lorsqu'une propriété système est ignorée, une extension de source de journal pour cette DSM utilise les expressions régulières que vous avez entrées pour la configuration.

### Propriétés personnalisées

Les propriétés personnalisées affichent **Custom** dans la ligne d'état.

Les propriétés personnalisées diffèrent des propriétés système de ces manières :

- Les propriétés personnalisées affichent **Custom** au-dessous de leur nom.
- Les propriétés personnalisées ne comportent pas de case à cocher **Ignorer le comportement du système**.

- Pour rendre une propriété personnalisée disponible pour les règles et l'indexation de recherche, cochez la case **Activer cette propriété à utiliser dans les règles et l'indexation de la recherche** lorsque vous créez une propriété personnalisée.

**Remarque :** Lorsque vous sélectionnez cette option, QRadar tente d'extraire la propriété des événements dès qu'elle entre dans le pipeline. Les informations de propriété extraites et le reste de l'enregistrement d'événement sont conservés. La propriété n'a pas besoin d'être à nouveau extraite lorsqu'elle est utilisée dans une recherche ou un rapport. Le processus améliore les performances lorsque la propriété est extraite, mais le processus peut avoir un impact négatif sur les performances lors de la collecte et du stockage des événements.

- Les propriétés personnalisées doivent avoir une ou plusieurs expressions valides.

### Concepts associés

#### Présentation de DSM Editor

Plutôt que de créer manuellement une extension de source de journal pour corriger des problèmes d'analyse syntaxique ou étendre le support à de nouveaux types de source de journal, utilisez l'éditeur DSM. Celui-ci propose différentes vues de vos données. L'éditeur DSM permet d'extraire des zones, de définir des propriétés personnalisées, de catégoriser des événements et de définir une nouvelle définition QID.

#### Définitions de propriétés personnalisées dans l'éditeur DSM

Vous pouvez définir une propriété personnalisée et réutiliser la même propriété dans un DSM distinct. Utilisez ces propriétés dans les recherches, les règles et pour autoriser un comportement spécifique défini par l'utilisateur pour l'analyse des valeurs dans ces zones.

## Configuration des propriétés dans l'éditeur DSM

---

Configurez les propriétés dans l'éditeur DSM pour modifier le comportement d'une propriété système substituée ou de la propriété personnalisée d'un DSM.

Lorsque vous remplacez le comportement d'une propriété système, vous devez indiquer une expression valide dans l'onglet **Propriétés**. Le champ **Format String** est une combinaison de groupes de capture regex et de caractères littéraux. La chaîne est utilisée pour renseigner les propriétés du système en fonction d'une ou de plusieurs valeurs capturées à partir d'événements et avec plusieurs caractères de mise en forme ou informations injectées. Par exemple, vous pouvez analyser une adresse IP et un port pour les combiner dans une chaîne. Si votre expression régulière (regex) comporte deux groupes de capture, vous pouvez les combiner en utilisant la chaîne de format : \$1 : \$2.



**Avertissement :** L'éditeur DSM autorise les références de groupe de capture de 1 à 9 dans toute correspondance spécifique. Si vous référencez un groupe de capture au-delà de 9, l'extension de source de journal peut ne pas fonctionner correctement.

Vous devez configurer chaque propriété personnalisée que vous créez. Vous devez indiquer une expression valide et un groupe de capture pour une propriété personnalisée dans l'onglet **Propriétés**. Vous pouvez également définir la sélectivité et activer ou désactiver votre expression.

### Concepts associés

«Définitions de propriétés personnalisées dans l'éditeur DSM», à la page 169

Vous pouvez définir une propriété personnalisée et réutiliser la même propriété dans un DSM distinct. Utilisez ces propriétés dans les recherches, les règles et pour autoriser un comportement spécifique défini par l'utilisateur pour l'analyse des valeurs dans ces zones.

## Référencement des chaînes de capture à l'aide des zones de chaîne de format

Utilisez le champ **Format String** de l'onglet **Configuration des Propriétés** pour faire référence aux groupes de capture que vous avez définis dans regex. Les groupes de capture sont référencés dans leur ordre de priorité.

## Pourquoi et quand exécuter cette tâche

Un groupe de capture est un regex joint entre parenthèses. Un groupe de capture est référencé avec une notation \$n, où n est un numéro de groupe contenant une expression régulière (regex). Vous pouvez définir plusieurs groupes de capture.

Par exemple, vous disposez d'une charge avec des variables de nom d'entreprise et d'hôte.

```
"company": "ibm", "hostname": "localhost.com"
"company": "ibm", "hostname": "johndoe.com"
```

Vous pouvez personnaliser le nom d'hôte à partir de la charge pour afficher *ibm.hostname.com* à l'aide de groupes de capture.

## Procédure

1. Dans le champ **regex**, entrez l'expression régulière suivante :  
"company": "(.\*?)" .\* "hostname": "(.\*?)"
2. Dans le champ **Format String**, entrez le groupe de capture \$1. \$2 où \$1 est la valeur de la variable de société (dans ce cas *ibm*) et \$2 est la valeur du nom d'hôte dans la charge utile. Le résultat suivant est donné :  
*ibm.localhost.com ibm.johndoe.com*

## Regex pour les journaux bien structurés

Les journaux bien structurés sont un style de formatage d'événement composé d'un ensemble de propriétés et sont présentés de la manière suivante :

```
<name_of_property_1><assignment_character>
<value_of_property_1><delimiter_character>
<name_of_property_2><assignment_character>
<value_of_property_2><delimiter_character>
<name_of_property_3><assignment_character>
<value_of_property_3><delimiter_character>...
```

Utilisez les instructions générales suivantes :

- *<assignment\_character>* : « = » ou « : » ou une séquence à plusieurs caractères, telle que « -> ».
- *<delimiter\_character>* soit un espace blanc (espace ou tabulation), soit un délimiteur de liste, par exemple une virgule ou un point-virgule.
- Les *<value\_of\_property>* et parfois *<name\_of\_property>* sont encapsulés entre guillemets ou d'autres caractères d'emballage.

Par exemple, considérons un événement de connexion simple généré par un périphérique ou une application. L'unité peut faire rapport sur le compte d'un utilisateur connecté, le moment où la connexion s'est produite et l'adresse IP de l'ordinateur à partir duquel l'utilisateur s'est connecté. Un événement de type paire nom / valeur peut ressembler à ce fragment :

```
<13>Sep 09 22:40:40 192.0.2.12 action=login accountname=JohnDoe clientIP=192.0.2.24
timestamp=01/09/2016 22:40:39 UTC
```

**Remarque :** La chaîne « <13>Sep 09 22:40:40 192.0.2.12 » est un en-tête syslog. La chaîne ne fait pas partie du corps de l'événement.

Le tableau suivant montre comment les propriétés de l'exemple de journal bien structuré ci-dessus peuvent être capturées :

Tableau 28. Regex pour la capture des propriétés d'un journal bien structuré	
Propriété	Expression régulière
action	action=(.*?)\t

Tableau 28. Regex pour la capture des propriétés d'un journal bien structuré (suite)

Propriété	Expression régulière
accountname	accountname=(.*?)\t
clientIP	clientIP=(.*?)\t
horodatage	timestamp=(.*?)\t

Les modèles qui sont placés entre crochets indiquent le groupe de capture. Chaque régex de la table capture tout après le signe égal (=) et avant le caractère de tabulation suivant.

## Regex pour les journaux de langue naturelle

Les journaux de langue naturelle sont présentés sous forme de phrases et chaque type d'événement peut être différent.

Par exemple, un simple événement de connexion peut être présenté sous la forme suivante :

```
<13>Sep 09 22:40:40 192.0.2.12 Account JohnDoe initiated a login action  
from 192.0.2.24 at 01/09/2016 22:40:39 UTC
```

Le tableau suivant montre comment les propriétés du journal de langue naturelle dans l'exemple ci-dessus peuvent être capturées :

Tableau 29. Regex pour la capture des propriétés d'un journal de langue naturelle

Propriété	Expression régulière
action	a initié une action (.*?)
accountname	Compte (.*?) lancé
clientIP	depuis (.*?) à
horodatage	à (.*?)

**Remarque :** L'écriture de regex pour les journaux de langue naturelle nécessite que vous examiniez les informations statiques qui entourent la valeur que vous souhaitez capturer avant de créer le groupe de capture.

## Expressions au format JSON pour les données structurées

Les données structurées au format JSON contiennent une ou plusieurs propriétés, qui sont représentées en tant que paire valeur-clé.

### Pourquoi et quand exécuter cette tâche

Vous pouvez extraire des propriétés des données d'événement présentées au format JSON en écrivant une expression JSON qui correspond à la propriété. L'expression JSON doit être un chemin au format de `/"<name of top-level field>".`

Par exemple, vous disposez de données d'événement formatées au format JSON :

```
{ "action": "login", "user": "John Doe" }
```

Ou un événement dont le format JSON est imbriqué, par exemple :

```
{ "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }
```

## Procédure

Pour extraire des propriétés des données d'événement, choisissez l'une des méthodes suivantes :

- Pour extraire la propriété de "l'utilisateur" pour les données d'événement qui sont formatées au format JSON, entrez l'expression `/"user"` dans le champ **Expression** .
- Pour extraire le "nom" de l'utilisateur pour un événement dont le format JSON est imbriqué, entrez l'expression `/"user"/"last_name"` dans le champ **Expression** .

## Expressions de chemin de clé JSON

Pour identifier de manière unique les zones que vous souhaitez extraire d'un objet JSON, votre expression JSON doit suivre des conventions de chemin de clé JSON spécifiques.

Utilisez les instructions suivantes pour vos expressions de chemin de clé JSON :

- Une barre oblique (/) doit être au début de tous les chemins de clés JSON. Tous les chemins doivent commencer au début de l'objet JSON racine. Les barres obliques suivantes dans le fichier de clés indiquent l'accès aux zones imbriquées dans l'objet JSON.
- Les noms de zone doivent être placés entre guillemets.

Un chemin valide peut ressembler à l'exemple suivant :

```
/"object"/"nestedObject"/"furtherNestedObject"/"desiredPropertyName"
```

- Les crochets indiquent le traitement des tableaux JSON.

Si vous ne fournissez pas un index entre crochets, le corps entier du tableau est extrait. Si vous fournissez un index dans le crochet carré, cet index du tableau est extrait ou imbriqué. Les tableaux commencent à un index zéro, où 0 est le premier index du tableau, 1 est le deuxième index du tableau, et ainsi de l'index.

Dans l'exemple de fichier de clés suivant, l'analyseur syntaxique JSON examine le deuxième index de la matrice JSON « object », puis dans cet index de tableau, recherche une zone appelée « desiredPropertyName ».

```
/"object"[1]/"desiredPropertyName"
```

- Dans les extensions de source de journal, vous pouvez fournir et combiner plusieurs chemins de clés JSON pour donner un seul résultat ; cette convention exclut les propriétés personnalisées. Vous pouvez également choisir d'inclure un texte littéral. Chacun des chemins de clés JSON doit être entouré d'accolades.

Prenons l'exemple suivant :

```
{/"object"/"nestedObject"/"desiredPropertyName1"} {/"object"/"nestedObject"/"desiredPropertyName2"}
```

Vous obtenez une valeur analysée à partir du premier chemin de clé JSON, un espace de texte littéral, puis une valeur analysée à partir du second chemin de clé JSON.

**Exemple :** Les deux exemples suivants montrent comment extraire des données à partir d'un objet JSON :

- Le cas simple d'un objet JSON :

```
[{"name": "object1", "field1": "value1"}, {"name": "object2", "field2": "value2"}, {"name": "object3", "field3": "value3"}]
```

Le tableau suivant présente les valeurs extractibles à partir des chemins de clés de cet exemple d'objet :

Chemins d'accès	Description	Valeur
/[]	Extrait la totalité du tableau JSON à partir de la racine de l'objet JSON.	[{"name": "object1", "field1": "value1"}, {"name": "object2", "field2": "value2"}, {"name": "object3", "field3": "value3"}]
/[1]/"name"	Extrait la valeur de l'attribut « name » de l'objet JSON à l'index 1 dans le tableau JSON racine.	object2

- Le cas complexe d'un objet JSON :

```
<13>May 22 10:15:41 log.test.com {"module": "CPHalo", "version": "1.0", "user_name": "user123", "event_type": "File integrity scan request created", "event_category": "File Integrity Scanning Management", "srcName": "domain-lab-123", "timestamp": "2018-12-02T15:36:17.486", "user": {"email": "user123@example.com", "first_name": "fname", "last_name": "lname", "alias": ["alias name", "alias1", "name"]}, "client_ip": "12.12.12.12", "server_id": "12317412471421274", "server_reported_fqdn": "None", "actor_country": "USA", "server_group_name": "Example Server", "server_platform": "Linux", "message": "A file integrity monitoring scan was requested for Linux server domain-lab-123 (13.13.13.13) by Halo user user123@example.com from IP address 12.12.12.12 (USA).", "type": "fim_scan_request_created", "id": "c2e8bf72-b74f-11e2-9055-870a490fcfb6"}
```

Le tableau suivant présente les valeurs extractibles à partir des chemins de clés de cet exemple d'objet :

Chemins d'accès	Description	Valeur
/"user_name"	Extrait la valeur de l'attribut « user_name » à partir de la racine de l'objet JSON.	user123
/"user"/"alias"[]	Extrait l'ensemble du tableau JSON appelé « alias » qui est imbriqué sous l'objet JSON « utilisateur ».	["alias name", "alias1", "name"]
/"user"/"alias"[0]	Extrait la valeur à l'index 0 dans le tableau JSON « alias » qui est imbriqué sous l'objet JSON « user ».	nom d'alias
/"user"/"first_name"	Extrait la valeur de la propriété appelée « first_name » imbriquée sous l'objet JSON « user ».	fname
{/"user"/"first_name"}. {/user"/"last_name"}	Extrait la valeur de la propriété appelée "prénom" qui est imbriquée sous l'objet "utilisateur" JSON, puis insère un littéral '.' caractère, puis extrait la valeur de la propriété nommée "deuxième_nom" qui est imbriquée sous l'objet "utilisateur" JSON.  Conserve uniquement les extensions de source de journal et les propriétés non personnalisées dans l'éditeur DSM. Cette opération n'est pas possible dans les propriétés personnalisées.	fname.lname

Chemins d'accès	Description	Valeur
{/"user"/"alias"[1]}@{/"client_ip"}	Extrait la valeur à l'index 1 du tableau JSON « alias » qui est imbriqué sous l'objet JSON « utilisateur », insère un caractère littéral « @ », puis extrait la valeur de la propriété appelée « client_ip » sous l'objet JSON racine.  Conserve uniquement les extensions de source de journal et les propriétés non personnalisées dans l'éditeur DSM. Cette opération n'est pas possible dans les propriétés personnalisées.	alias1@12.12.12.12

## Expressions au format LEEF pour les données structurées

Les données structurées au format LEEF contiennent une ou plusieurs propriétés, qui sont représentées par des paires clé/valeur.

### Pourquoi et quand exécuter cette tâche

Vous pouvez extraire des propriétés d'un événement présenté au format LEEF en créant une expression LEEF correspondant à la propriété. Les expressions LEEF valides sont représentées par une référence de clé unique ou une référence de zone d'en-tête LEEF spéciale.

Par exemple, vous avez un événement au format LEEF version 1.0, tel que :

```
LEEF:1.0|ABC Company|SystemDefender|1.13|console_login|devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
devTime=2017-10-18T11:26:03.060+0200  usrName=flastname  name=Firstname Lastname
authType=interactivePassword  src=192.168.0.1
```

ou un événement au format LEEF version 2.0 avec le caractère de séparation (^), tel que :

```
LEEF:2.0|ABC Company|SystemDefender|1.13|console_login|^|devTimeFormat=yyyy-MMdd'T'HH:mm:ss.SSSZ^
devTime=2017-10-18T11:26:03.060+0200^usrName=flastname^name=Firstname Lastname
^authType=interactivePassword^src=192.168.0.1
```

Vous pouvez extraire une propriété ou une propriété de clé d'en-tête de l'événement en choisissant l'une des méthodes suivantes :

### Procédure

1. Pour extraire la propriété 'Nomd'utilisateur', entrez `usrName` dans le champ **Clé LEEF** .

Les clés possibles qui peuvent être extraites sont les suivantes :

- devTimeFormat
- devTime
- usrName
- nom
- authType
- src

2. Pour extraire une propriété de clé d'en-tête, entrez la clé au format suivant dans la zone **Clé LEEF** :

```
$eventid$
```

Les valeurs d'en-tête LEEF peuvent être extraites en utilisant les expressions suivantes :

- \$leefversion\$
- \$vendor\$
- \$product\$
- \$version\$
- \$eventid\$

## Expressions au format CEF pour les données structurées

Les données structurées au format CEF contiennent une ou plusieurs propriétés, qui sont représentées par des paires clé/valeur.

### Pourquoi et quand exécuter cette tâche

Vous pouvez extraire des propriétés d'un événement présenté au format CEF en créant une expression CEF correspondant à la propriété. Les expressions CEF valides sont représentées par une référence de clé unique ou une référence de zone d'en-tête CEF spéciale.

Par exemple, vous avez un événement au format CEF :

```
CEF:0|ABC Company|SystemDefender|1.13|console_login|Console Login|1|start=Oct 18 2017 11:26:03  
duser=jsmith cs1=John Smith cs1Label=Person Name cs2=interactivePassword cs2Label=authType  
src=1.1.1.1
```

Vous pouvez extraire une propriété ou une propriété de clé d'en-tête de l'événement en choisissant l'une des méthodes suivantes :

### Procédure

1. Pour extraire la propriété 'cs1', entrez cs1 dans le champ **Clé CEF** .

Les clés possibles qui peuvent être extraites sont les suivantes :

- démarrer
- duser
- cs1
- cs1Label
- cs2
- cs2Label
- src

2. Pour extraire une propriété de clé d'en-tête, entrez la clé au format suivant dans la zone **Clé CEF** :

```
$id$
```

Les valeurs d'en-tête CEF peuvent être extraites en utilisant les expressions suivantes :

- \$cefversion\$
- \$vendor\$
- \$product\$
- \$version\$
- \$id\$
- \$nom\$
- \$gravité\$



## Expressions dans le format Paire de valeur de nom pour les données structurées

Les données structurées au format Paire de valeur de nom contiennent une ou plusieurs propriétés, qui sont représentées en tant que paires clé-valeur.

### Pourquoi et quand exécuter cette tâche

Vous pouvez extraire des propriétés d'un événement au format Paire de valeur de nom en écrivant une expression qui correspond à la propriété. Les expressions Paire nom-valeur valides sont représentées par une référence de clé unique.

L'exemple suivant montre un événement au format Paire nom-valeur :

```
Company=ABC  
Company;Product=SystemDefender;Version=1.13;EventID=console_login;Username=jsmith;Name=John  
Smith;authType=interactivePassword;
```

### Procédure

1. Pour extraire la propriété `Username`, entrez `Nom d'utilisateur` dans la zone **Expression**.
2. Dans la zone **Délimiteur de valeur**, entrez le délimiteur de valeur de clé spécifique à votre contenu. Dans cet exemple, le délimiteur de valeur de clé est un signe égal (=).
3. Dans la zone **Délimiteur**, entrez le délimiteur de paires de valeur de clé spécifique à votre contenu. Dans cet exemple, le délimiteur entre les paires de valeur de clé est un point-virgule (;).

### Résultats

Les correspondances trouvées dans le contenu utile sont mises en évidence dans les données d'événement dans l'**Espace de travail** de l'éditeur DSM.

## Expressions dans le format de liste générique pour les données structurées

Les données structurées dans le format de liste générique contiennent une ou plusieurs propriétés, qui sont représentées sous forme d'éléments de liste.

### Pourquoi et quand exécuter cette tâche

Vous pouvez extraire des propriétés d'un événement au format de liste générique en écrivant une expression qui correspond à la propriété. Les expressions de liste générique valides sont sous la forme d'une notation `$<number>`. Par exemple, `$0` représente la première propriété de la liste, `$1` la deuxième, etc.

L'exemple suivant montre un événement au format Liste générique :

```
ABC Company;1.13;console_login;jsmith;John Smith;interactivePassword;
```

### Procédure

1. Pour extraire la première propriété de la liste, entrez `$0` dans la zone **Expression**.
2. Dans la zone **Délimiteur**, entrez le délimiteur d'éléments de liste spécifique à votre contenu. Dans cet exemple, le délimiteur entre les éléments de liste est un point-virgule (;).

### Résultats

Les correspondances trouvées dans le contenu utile sont mises en évidence dans les données d'événement dans l'**Espace de travail** de l'éditeur DSM.

## Expressions au format XML pour les données structurées

Les données structurées au format XML contiennent une ou plusieurs propriétés, qui sont représentées en tant que paires clé-valeur.

Vous pouvez extraire des propriétés d'un événement au format XML en écrivant une expression qui correspond à la propriété. Les expressions XML valides sont de la forme d'une référence de clé unique.

Entrez le chemin vers la zone XML à utiliser pour charger la valeur de la propriété. Un chemin de clé XML doit commencer par une barre oblique (/) pour indiquer la racine de l'objet XML suivie d'un ou de plusieurs noms de zone XML placés entre guillemets.

L'exemple suivant montre un événement au format XML :

```
<EPOEvent><MachineInfo><MachineName>NEPTUNE</MachineName><MachineName>VALUE23</MachineName><AgentGUID>9B-B5-A6-A8-37-B3</AgentGUID><IPAddress someattrib="someattribvalue">192.0.2.0</IPAddress><OSName>Windows 7</OSName><UserName>I am a test user</UserName></MachineInfo></EPOEvent>
```

Pour capturer la valeur imbriquée dans l'objet OSName de niveau supérieur, entrez / "EPOEvent" / "MachineInfo" / "OSName" dans le champ **Expression** .

Pour capturer la valeur d'attribut, utilisez un point (.) après le chemin de la clé. Par exemple, pour capturer someattribvalue, entrez / "EPOEvent" / "MachineInfo" / "IPAddress".someattrib dans le champ **Expression** .

Pour combiner plusieurs zones avec plusieurs chemins, utilisez des crochets. Par exemple, {/"EPOEvent"/"MachineInfo"/"OSName"} {/"EPOEvent"/"MachineInfo"/"MachineName" [1]}


Pour capturer la valeur imbriquée dans plusieurs balises du même nom, utilisez [0], [1], et ainsi de suite après le chemin de la clé. Par exemple, pour capturer VALUE23, entrez / "EPOEvent" / "MachineInfo" / "MachineName" [1] dans le champ **Expression** .

Les correspondances trouvées dans le contenu utile sont mises en évidence dans les données d'événement dans l'**Espace de travail** de l'éditeur DSM.

## Ouverture de l'éditeur DSM

Vous pouvez ouvrir l'éditeur DSM à partir de l'onglet **Activité de journal**, ou si vous êtes un administrateur, vous pouvez l'ouvrir à partir de l'onglet **Admin**. Par exemple, si les événements envoyés au système ne sont pas gérés correctement, vous pouvez sélectionner les données d'événement dans l'onglet **Activité de journal** et l'envoyer à l'éditeur DSM. Pour les événements qui ne sont pas encore envoyés au système, vous devez être un administrateur et accéder à l'éditeur DSM à partir de l'onglet **Admin**.

### Procédure

1. Pour ouvrir l'éditeur DSM à partir de l'onglet **Admin**, procédez comme suit :
  - a) Dans le menu de navigation () , cliquez sur **Admin**.
  - b) Dans la section **Sources de données**, cliquez sur **Éditeur DSM**.
2. Pour ouvrir l'éditeur DSM à partir de l'onglet **Activité de journal**, procédez comme suit :
  - a) Cliquez sur l'onglet **Activité du journal**.
  - b) Interrompre les résultats entrants puis mettre en évidence un ou plusieurs événements.

**Important :** Si plusieurs événements provenant de deux sources de journal ou plus sont sélectionnés, vous êtes invité à sélectionner le type de source de journal sur lequel vous souhaitez opérer. Vous ne pouvez sélectionner qu'un seul type de source de journal, et seuls les événements de l'activité de journal qui correspondent au type de source de journal sélectionné sont automatiquement ajoutés à l'espace de travail.


- c) Dans le menu de navigation, sélectionnez **Actions > Éditeur DSM**

## Configuration d'un type de source de journal

---

Avec l'éditeur DSM, vous pouvez configurer un nouveau type de source de journal ou en utiliser un existant dans IBM QRadar.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Éditeur DSM**.
3. Créez un type de source de journal ou sélectionnez un type de source de journal existant :
  - Pour créer un type de source de journal, cliquez sur **Créer nouveau** et suivez les invites.
  - Pour localiser un type de source de journal existant, utilisez la zone **Filtrer**, puis cliquez sur **Sélectionner**.

## Configuration de la détection automatique des propriétés pour les types de source de journal

---

Lorsque vous activez **Détection automatique des propriétés**, les nouvelles propriétés sont générées automatiquement pour capturer toutes les zones qui se trouvent dans les événements reçus par le type de source de journal sélectionné. Configurez la détection automatique des propriétés des nouvelles propriétés pour un type de source de journal, de sorte que vous n'avez pas besoin de créer manuellement une propriété personnalisée pour chaque instance.

### Pourquoi et quand exécuter cette tâche

Par défaut, **Détection automatique des propriétés** pour un type de source de journal est désactivé.

### Procédure

1. Dans l'éditeur DSM, sélectionnez un type de source de journal ou en créez un à partir de la page **Sélectionner le type de source de journal**.
2. Cliquez sur l'onglet **Configuration**.
3. **Restriction** : La détection automatique des propriétés ne fonctionne que pour les données structurées qui sont au format JSON, CEF, LEEF, XML ou Paire de Valeurs de Nom.  
Cliquez sur **Activer la détection automatique des propriétés**.
4. Sélectionnez le format de données structuré pour le type de source de journal dans la liste **Format de détection de propriété**.  
Si vous choisissez **Paire de valeur de nom**, dans la section **Délimiteur dans les paires de valeurs de nom**, entrez le délimiteur utilisé pour séparer chaque nom et valeur, et le délimiteur utilisé pour séparer chaque nom de valeur de nom. Les délimiteurs de chaque paire sont automatiquement créés.
5. Pour activer les nouvelles propriétés à utiliser dans les règles et les recherches, cliquez sur **Activer les propriétés à utiliser dans les règles et l'indexation de la recherche**.
6. Dans la zone **Seuil d'achèvement de la détection automatique**, définissez le nombre d'événements consécutifs à inspecter pour les nouvelles propriétés.  
Si aucune nouvelle propriété n'est reconnue lorsque le nombre d'événements consécutifs est inspecté, le processus de reconnaissance est considéré comme terminé et **Détection automatique des propriétés** est désactivé. Vous pouvez réactiver manuellement **Détection automatique des propriétés** à tout moment. Une valeur de seuil 0 signifie que le processus de reconnaissance inspecte perpétuellement les événements pour le type de source de journal sélectionné.
7. Cliquez sur **Sauvegarder**.

## Résultats

Les propriétés nouvellement reconnues s'affichent dans l'onglet **Propriétés** de l'éditeur DSM.

# Configuration de la détection automatique des sources de journal pour les types de source de journal

---

Configurez la détection automatique des sources de journal pour un type de source de journal, de sorte que vous n'avez pas besoin de créer manuellement une source de journal pour chaque instance. La configuration de la détection automatique des sources de journaux permet également d'améliorer la précision des dispositifs de détection qui partagent un format commun et peut améliorer les performances du pipeline en évitant la création d'unités incorrectement détectées.

## Avant de commencer

Dans QRadar V7.3.2, les mises à niveau des versions précédentes permettent d'activer les paramètres de configuration globaux, qui sont stockés dans la base de données QRadar. Les paramètres globaux sont initialement définis en fonction du contenu du fichier `TrafficAnalysisConfig.xml` dans le répertoire `/opt/qradar/conf/` du répertoire QRadar Console. Si ce fichier a été personnalisé avant la mise à niveau vers V7.3.2, les personnalisations sont conservées. Si des personnalisations différentes existent sur d'autres hôtes gérés dans le déploiement, ces personnalisations ne sont pas reportées sur les paramètres globaux. Vous pouvez toujours activer les paramètres de détection automatique de processeur par événement en utilisant la méthode de fichier de configuration. Désactivez les paramètres globaux de détection automatique dans **Admin > Gestion des licences système > Éditer l'hôte géré > Gestion des composants**.

## Pourquoi et quand exécuter cette tâche

Lorsque la fonction de détection automatique de source de journal est activée, si vous créez un type de source de journal personnalisé qui comporte de nombreuses instances dans votre réseau, vous n'avez pas besoin de créer manuellement une source de journal pour chaque instance.


Vous pouvez également utiliser l'API REST QRadar ou un script de ligne de commande pour activer et désactiver les types de source de journal qui sont détectés automatiquement. Si vous utilisez un plus petit nombre de types de source de journal, vous pouvez configurer les sources de journal qui sont automatiquement détectées pour améliorer la vitesse de détection.

Si vous choisissez de revenir aux paramètres basés sur des fichiers (non globaux), vous pouvez uniquement configurer la détection automatique à l'aide du fichier de configuration. L'éditeur DSM et l'API REST fonctionnent uniquement avec les paramètres globaux. Déplacez toutes les configurations de détection automatique personnalisées vers les paramètres globaux et vers l'éditeur DSM.

Réglage du moteur de détection automatique de sorte que les sources de journal ne soient pas correctement identifiées comme étant du type incorrect. Une détection incorrecte se produit lorsqu'un DSM reconnaît incorrectement les événements comme étant ses propres, même s'ils ne proviennent pas du type de système auquel correspond le DSM. Par exemple, si les événements sont formatés de la même manière que les événements que le DSM prend en charge, ou ils contiennent les mêmes mots clés que le DSM recherche. Cela peut également se produire même si un DSM existe pour le système qui génère les événements, si les événements sont si similaires que le DSM incorrect a réussi à analyser les événements comme le DSM correct. Le DSM reconnaît incorrectement les événements comme ses propres événements, et le moteur de détection automatique crée une source de journal qui n'est pas du type correct.

Par exemple, si vous disposez de systèmes Linux® et AIX dans votre déploiement QRadar et que la plupart d'entre eux sont Linux. Vous pouvez réduire le paramètre **Nombre minimal d'événements réussis pour la détection automatique** ou **Nombre minimal d'événements réussis pour la détection automatique** pour Linux. Vous pouvez également augmenter le paramètre **Nombre minimal d'événements réussis pour la détection automatique** ou le paramètre **Nombre minimal d'événements réussis pour la détection automatique** pour AIX.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Éditeur DSM**.
3. Sélectionnez un type de source de journal ou créez un type de source dans la fenêtre **Sélectionner le type de source de journal**.
4. Cliquez sur l'onglet **Configuration**, puis sur **Activer la détection automatique des sources de journal**.
5. Configurez les paramètres suivants :

Paramètre	Description
<b>Modèle de nom des sources de journaux</b>	Entrez le modèle pour définir le nom des sources de journal autodétectées.  Deux variables peuvent être utilisées : <ul style="list-style-type: none"><li>• <b>\$\$DEVICE_TYPE\$\$</b> correspond au nom du type de source de journal.</li><li>• <b>\$\$SOURCE_ADDRESS\$\$</b> correspond à l'adresse source dont proviennent les événements.</li></ul>
<b>Modèle de description des sources de journaux</b>	Entrez le modèle pour définir la description des sources de journal détectées automatiquement.  Deux variables peuvent être utilisées : <ul style="list-style-type: none"><li>• <b>\$\$DEVICE_TYPE\$\$</b> correspond au nom du type de source de journal.</li><li>• <b>\$\$SOURCE_ADDRESS\$\$</b> correspond à l'adresse source dont proviennent les événements.</li></ul>
<b>Nombre minimum d'événements réussis pour l'autodétection</b>	Nombre minimal d'événements d'une source inconnue qui doivent être analysés avec succès pour que la détection automatique se produise.
<b>Taux de réussite minimum pour l'autodétection</b>	Pourcentage minimal de réussite de l'analyse syntaxique des événements provenant d'une source inconnue pour la détection automatique.
<b>Limite d'interprétation tentée</b>	Nombre maximal d'événements d'une source inconnue à essayer avant l'abandon de la détection automatique.
<b>Limite d'échecs consécutifs de l'interprétation</b>	Nombre d'événements consécutifs provenant d'une source inconnue pour abandonner la détection automatique.

6. Cliquez sur **Sauvegarder**.


## Configuration des paramètres DSM pour les types de source de journal

Utilisez l'éditeur DSM pour configurer les paramètres DSM pour votre type de source de journal.

### Pourquoi et quand exécuter cette tâche

Si votre type de source de journal comporte des paramètres DSM, vous pouvez utiliser l'éditeur DSM pour modifier les paramètres.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Éditeur DSM**.
3. Sélectionnez un type de source de journal ou créez un type de source dans la fenêtre **Sélectionner le type de source de journal**.
4. Cliquez sur l'onglet **Configuration**, puis sur **Affichage de la configuration des paramètres DSM**.
5. Configurez les paramètres ci-après.

Les paramètres par défaut s'appliquent à toutes les instances de ce DSM dans votre déploiement qui n'ont pas de substitution spécifique au collecteur d'événements. Pour définir des valeurs de paramètre différentes pour ce DSM pour un collecteur d'événements spécifique, sélectionnez-le dans la liste **Collecteur d'événements** pour remplacer les paramètres par défaut.

6. Cliquez sur **Sauvegarder**.

## Types de source de journal personnalisés

---

Utilisez l'éditeur DSM pour créer et configurer un type de source de journal personnalisé pour analyser vos événements. Si vous créez un type de source de journal pour vos applications et systèmes personnalisés qui n'ont pas de DSM pris en charge, QRadar analyse les données de la même manière que pour les DSM pris en charge.

Vous pouvez sélectionner des événements dans l'onglet **Activité de journal** et les envoyer directement à l'éditeur DSM à analyser. Vous pouvez également ouvrir l'éditeur DSM à partir de l'onglet **Admin** pour créer et configurer un nouveau type de source de journal.

Terminez les zones de l'éditeur DSM avec les données structurées correctes pour analyser les informations pertinentes à partir des événements. QRadar utilise les champs **Catégorie d'événement** et **ID d'événement** pour mapper une signification à l'événement. L'ID événement est une zone obligatoire qui définit l'événement et la catégorie interrompt davantage l'événement. Vous pouvez définir **Catégorie d'événement** sur le nom de type d'unité, ou vous pouvez le laisser comme inconnu. Si vous laissez l'élément **Catégorie d'événement** inconnu, vous devez le définir à l'état inconnu pour les mappages d'événements que vous créez pour ce type de source de journal.

Utilisez l'éditeur DSM pour mapper vos combinaisons ID/Catégorie d'événement que vous analyseront à partir de vos événements. Entrez la combinaison ID événement / Catégorie d'événement dans la nouvelle entrée de l'onglet **Mappage d'événements**. Vous pouvez choisir une catégorisation de l'entrée de mappage QID précédemment créée qui est pertinente pour votre événement ou cliquez sur **Choisissez QID** pour créer une nouvelle entrée de mappage.

## Création d'un type de source de journal personnalisé pour analyser les événements

Si vous avez des événements importés dans QRadar, vous pouvez sélectionner les événements sur lesquels vous souhaitez baser votre type de source de journal personnalisé et les envoyer directement à l'éditeur DSM.

### Procédure

1. Cliquez sur l'onglet **Activité du journal**.
2. Interrompre les résultats entrants puis mettre en évidence un ou plusieurs événements.

**Important :** Vous ne pouvez sélectionner qu'un seul type de source de journal, et seuls les événements de l'activité de journal qui correspondent au type de source de journal sélectionné sont automatiquement ajoutés à l'espace de travail.

3. Dans le menu de navigation, sélectionnez **Actions** > **Éditeur DSM** et choisissez l'une des options suivantes :

- Si vous analysez-vous des événements connus, sélectionnez votre type de source de journal dans la liste.
  - Si vous analysez des événements stockés, cliquez sur **Créer nouveau**. Entrez un nom pour votre type de source de journal dans la zone **Nom du type de source de journal** et cliquez sur **Sauvegarder**.
4. Dans l'onglet **Propriétés**, cochez la case **Remplacer les propriétés système** pour les propriétés que vous souhaitez modifier.

## Que faire ensuite

[«Configuration des propriétés dans l'éditeur DSM», à la page 156](#)

### Tâches associées

[«Création d'une mappe d'événements et d'une catégorisation», à la page 175](#)

Un mappage d'événement est un ID d'événement et une combinaison de catégories que vous utilisez pour mapper un événement à un QID. Avec l'éditeur DSM, vous pouvez créer un mappage d'événements pour mapper tous les événements inconnus à une entrée de la mappe QID. De plus, vous pouvez remapper les existants à une nouvelle catégorisation d'événements (QID) ou à une catégorisation existante dans le système.

[«Configuration de la détection automatique des propriétés pour les types de source de journal», à la page 165](#)

Lorsque vous activez **Détection automatique des propriétés**, les nouvelles propriétés sont générées automatiquement pour capturer toutes les zones qui se trouvent dans les événements reçus par le type de source de journal sélectionné. Configurez la détection automatique des propriétés des nouvelles propriétés pour un type de source de journal, de sorte que vous n'avez pas besoin de créer manuellement une propriété personnalisée pour chaque instance.

[«Configuration de la détection automatique des sources de journal pour les types de source de journal», à la page 166](#)

Configurez la détection automatique des sources de journal pour un type de source de journal, de sorte que vous n'avez pas besoin de créer manuellement une source de journal pour chaque instance. La configuration de la détection automatique des sources de journaux permet également d'améliorer la précision des dispositifs de détection qui partagent un format commun et peut améliorer les performances du pipeline en évitant la création d'unités incorrectement détectées.

[«Création d'une propriété personnalisée», à la page 170](#)

Dans l'éditeur DSM, vous pouvez définir une propriété personnalisée pour un ou plusieurs types de source de journal dont les événements ne correspondent pas au modèle d'événement normalisé IBM QRadar. Par exemple, l'ensemble des propriétés système peut ne pas capturer toutes les données pertinentes provenant de certaines applications, de systèmes d'exploitation, de bases de données et d'autres systèmes.

## Définitions de propriétés personnalisées dans l'éditeur DSM

Vous pouvez définir une propriété personnalisée et réutiliser la même propriété dans un DSM distinct. Utilisez ces propriétés dans les recherches, les règles et pour autoriser un comportement spécifique défini par l'utilisateur pour l'analyse des valeurs dans ces zones.

Le cas échéant, chaque propriété personnalisée possède un ensemble d'options de configuration qui inclut la sélectivité et l'analyse syntaxique des données. Chaque définition de propriété personnalisée dans une configuration DSM est un groupe ordonné d'expressions qui se compose d'un type d'expression, d'une expression, d'un groupe de capture, d'une configuration de sélection facultative et d'un bouton à bascule activé ou désactivé. Vous ne pouvez pas modifier les zones **Name**, **Field type**, **Description**, **optimize** ou les options avancées d'une propriété personnalisée dans l'onglet **Propriétés** de l'Éditeur DSM.

Une propriété personnalisée est partagée par tous les DSM, tandis que les implémentations spécifiques pour la lecture des valeurs des charges sont au niveau DSM.

La sélection est spécifiée lorsque vous configurez une expression à exécuter uniquement lorsque certaines conditions sont remplies.

**Remarque :** La zone **Capture Group** d'une propriété personnalisée ne peut pas être affectée à une valeur supérieure au nombre de groupes de capture dans le regex.

### Concepts associés

Propriétés dans l'éditeur DSM

Dans l'éditeur DSM, les propriétés système normalisées sont combinées avec des propriétés personnalisées et sont triées par ordre alphabétique.

## Création d'une propriété personnalisée

Dans l'éditeur DSM, vous pouvez définir une propriété personnalisée pour un ou plusieurs types de source de journal dont les événements ne correspondent pas au modèle d'événement normalisé IBM QRadar. Par exemple, l'ensemble des propriétés système peut ne pas capturer toutes les données pertinentes provenant de certaines applications, de systèmes d'exploitation, de bases de données et d'autres systèmes.

### Pourquoi et quand exécuter cette tâche

Vous pouvez créer une propriété personnalisée pour les données qui ne correspondent pas aux propriétés système QRadar. Utilisez les propriétés personnalisées dans les recherches et testez-les dans les règles.

### Procédure

1. Dans l'onglet **Propriétés** de l'éditeur DSM, cliquez sur **Ajouter (+)**.
2. Pour créer une définition de propriété personnalisée, procédez comme suit :
  - a) Sur la page **Choisissez une définition de propriété personnalisée pour Express**, sélectionnez **Créer nouveau**.
  - b) Sur la page **Créer une définition de propriété personnalisée**, configurez les paramètres dans le tableau suivant.

Paramètre	Description
<b>Nom</b>	Nom descriptif de la propriété personnalisée que vous créez.
<b>Field Type</b>	La valeur par défaut est <b>Texte</b> . <b>Conseil :</b> Lorsque vous sélectionnez <b>Numéro</b> ou <b>Date</b> dans la liste <b>Type de zone</b> , des zones supplémentaires s'affichent.



Tableau 32. Paramètres de propriété personnalisée (suite)

Paramètre	Description
<p><b>Activer cette propriété à utiliser dans les règles et l'indexation de la recherche</b></p>	<p>Lorsque cette option est activée, lors de l'étape d'analyse du pipeline d'événements, QRadar tente d'extraire la propriété des événements immédiatement lors de son entrée dans le système. D'autres composants en aval dans le pipeline, tels que les règles, les profils de transfert et l'indexation, peuvent utiliser les valeurs extraites. Les informations de propriété sont conservées avec le reste de l'enregistrement d'événement et n'ont pas besoin d'être extraites à nouveau lorsqu'elles sont extraites dans le cadre d'une recherche ou d'un rapport. Cette option améliore les performances lorsque la propriété est extraite, mais peut avoir un impact négatif sur les performances lors du processus d'analyse syntaxique des événements et affecter le stockage.</p> <p>Lorsque cette option n'est pas activée, QRadar extrait la propriété des événements uniquement lorsqu'ils sont extraits ou visualisés.</p> <p><b>Important :</b> Pour utiliser les propriétés personnalisées dans les tests de règles, les profils de transfert ou pour l'indexation de recherche, assurez-vous que cette case est cochée. L'évaluation des règles, la transmission des événements et l'indexation se produisent avant que les événements ne soient écrits sur le disque, de sorte que les valeurs doivent être extraites au stade de l'analyse.</p>
<p><b>Utiliser le format numérique à partir d'un environnement local</b></p>	<p>Cette zone s'affiche lorsque vous sélectionnez <b>Numéro</b> dans la liste <b>Type de zone</b>. Si vous cochez la case <b>Utiliser le format numérique à partir d'un environnement local</b>, vous devez sélectionner un <b>Format de nombre extrait</b> dans la liste.</p>
<p><b>Format de date / heure extrait</b></p>	<p>Cette zone s'affiche lorsque vous sélectionnez <b>Date</b> dans la liste <b>Type de zone</b>. Vous devez fournir un modèle de date et heure qui correspond à la façon dont la date et heure apparaît dans l'événement d'origine.</p> <p>Par exemple, « MMM jj AAAA HH:mm:ss » est un modèle de date et heure valide pour un horodatage comme « Apr 17 2017 11:29:00 ».</p>

Tableau 32. Paramètres de propriété personnalisée (suite)	
Paramètre	Description
<b>Environnement local</b>	<p>Cette zone s'affiche lorsque vous sélectionnez <b>Date</b> dans la liste <b>Type de zone</b>. Vous devez sélectionner l'environnement local de l'événement.</p> <p>Par exemple, si l'environnement local est <b>Anglais</b>, il reconnaît « Apr » comme une forme abrégée du mois « April ». Mais si l'événement est présenté en français et que le jeton du mois est « Avr » (pour « April »), définissez l'environnement local sur un environnement <b>français</b>, ou le code ne le reconnaît pas comme une date valide.</p>

- c) Si vous souhaitez extraire la propriété des événements lors de son entrée dans le système, cochez la case **Activer cette propriété pour l'utilisation dans les règles et l'indexation de recherche**.
- d) Cliquez sur **Sauvegarder**.
3. Pour utiliser une propriété personnalisée existante, procédez comme suit :
- Sur la page **Choisir une Définition de Propriété Personnalisée à exprimer**, recherchez une Propriété Personnalisée existante depuis le champ **Filter Definitions**.
  - Cliquez sur **Sélectionner** pour ajouter la propriété personnalisée.

## Que faire ensuite

[Configuration d'une expression de propriété personnalisée](#)

**Information associée**

[Conseils sur la définition d'un modèle de date et d'heure](#)

## Expressions

Vous pouvez définir des expressions pour des propriétés personnalisées dans l'éditeur DSM. Les expressions sont le mécanisme qui définit le comportement d'une propriété. Le composant principal d'une expression est une expression régulière ou JSON valide. Les données qui constituent une expression dépendent du type de propriété.

Pour une propriété personnalisée, vous ne pouvez choisir qu'un seul groupe de capture à partir du regex.

## Configuration d'une expression de propriété personnalisée

Vous pouvez utiliser différentes expressions pour capturer des propriétés personnalisées pour le même événement. Vous pouvez également utiliser une combinaison de types d'expression pour capturer la même propriété personnalisée si cette dernière peut également être capturée depuis plusieurs formats d'événement.

## Pourquoi et quand exécuter cette tâche

IBM QRadar prend en charge les types d'expression de propriété personnalisée :

- Expression régulière
- JSON
- LEEF
- CEF
- Paire nom/valeur
- Liste générique

- XML

## Procédure

1. Dans l'onglet **Propriétés**, recherchez et sélectionnez la propriété personnalisée. Les propriétés personnalisées affichent le mot **Custom** à côté d'elles pour les distinguer des propriétés du système.
2. Sélectionnez un type d'expression dans la liste **Type d'expression** et définissez une expression valide pour celle-ci.

### Conseils :

- Pour Regex, l'expression doit être une expression régulière compatible Java valide. La correspondance insensible à la casse n'est prise en charge qu'à l'aide du jeton (?i) au début de l'expression. Le jeton (?i) est enregistré dans le fichier .xml de l'extension source du journal. Pour utiliser d'autres expressions, telles que (?s), éditez manuellement le fichier .xml de l'extension source du journal.
  - Pour JSON, l'expression doit être un chemin dans le format de /"<name of top-level field>" avec des sous-objets /"<name of sub-field>" supplémentaires pour capturer des sous-zones, le cas échéant.
  - Pour capturer la valeur d'une paire valeur-clé pour LEEF et CEF, définissez l'expression sur la clé.
  - Pour capturer la valeur d'une zone d'en-tête, définissez l'expression sur le mot réservé correspondant pour cette zone d'en-tête.
3. Si le type d'expression est Regex, sélectionnez un groupe de capture.
  4. Pour limiter une expression à exécuter sur une catégorie spécifique, cliquez sur **Éditer** pour ajouter la sélectivité à la propriété personnalisée, puis sélectionnez un **Catégorie de haut niveau** et un **Catégorie de bas niveau**.
  5. Pour limiter une expression à exécuter sur un événement ou un QID spécifique, cliquez sur **Choisir un événement** pour rechercher un QID spécifique.
  6. Dans la fenêtre **Expression**, cliquez sur **Ok**.
  7. Pour ajouter plusieurs expressions et les réorganiser, procédez comme suit :
    - a) Cliquez sur Ajouter (+) dans la liste des expressions.
    - b) Faites glisser les expressions dans l'ordre que vous souhaitez qu'elles s'exécutent.

### Tâches associées


«Suppression d'une expression de propriété personnalisée», à la page 173

Vous pouvez supprimer une expression de propriété personnalisée dans l'éditeur DSM. Si vous supprimez une expression de propriété personnalisée, seule l'expression est supprimée. La propriété personnalisée n'est pas supprimée.

## Suppression d'une expression de propriété personnalisée

Vous pouvez supprimer une expression de propriété personnalisée dans l'éditeur DSM. Si vous supprimez une expression de propriété personnalisée, seule l'expression est supprimée. La propriété personnalisée n'est pas supprimée.

## Procédure

1. Dans l'onglet Admin, cliquez sur **Éditeur DSM**.
2. Dans la fenêtre **Sélectionner le type de source de journal**, choisissez un type de source de journal et cliquez sur **Sélectionner**.
3. Dans la sous-fenêtre Type de source de journal, sélectionnez la propriété personnalisée avec l'expression à supprimer.
4. Dans la section Configuration des propriétés, sélectionnez l'expression à supprimer et cliquez sur l'icône de suppression ()
5. Cliquez sur **Supprimer**.

## Sélection

Dans l'éditeur DSM, vous pouvez limiter l'exécution d'une propriété personnalisée à certains critères d'amélioration des performances.

Voici les types de restrictions :

### Par catégorie de haut niveau et catégorie de bas niveau

Une propriété est évaluée uniquement lorsque les catégories de haut niveau et de bas niveau correspondent à une combinaison spécifique. Par exemple, une propriété n'est évaluée que lorsque l'événement est connu pour avoir une catégorie de niveau supérieur de **Authentication** et une catégorie de niveau inférieur de **Admin Logout**.

### Par QID spécifique

Une propriété est évaluée uniquement lorsque l'événement qui est vu mappe vers un QID spécifique. Par exemple, lorsque l'événement mappe vers un QID de **Login Failed**, la propriété est évaluée.

## Mappage d'événement

---

Dans l'éditeur DSM, le mappage d'événements affiche tous les ID d'événement et les combinaisons de catégories qui se trouvent dans le système.

Un mappage d'événements représente une association entre un ID événement et une combinaison de catégories et un enregistrement QID (appelé catégorisation des événements). Les ID d'événement et les valeurs de catégorie sont extraits par les DSM des événements et sont ensuite utilisés pour rechercher la catégorisation des événements mappés ou QID. Les catégorisations d'événements stockait des métadonnées supplémentaires pour l'événement qui n'existe peut-être pas dans les données d'événement brut, telles qu'un nom et une description lisibles par l'utilisateur, une valeur de gravité ou une affectation de catégorie de bas niveau. La catégorisation et la gravité de bas niveau sont utiles pour les définitions de recherche et de règle.



**Avertissement :** Pour les environnements multi-locataires, les informations de mappage ou de catégorisation d'événements définies par l'utilisateur qui sont définies dans l'éditeur de DSM deviennent visibles dans tous les locataires. Vous devez vous assurer qu'aucune donnée spécifique au locataire n'est présentée dans les noms ou les descriptions de catégorisation des événements.

## Propriétés d'identité pour les mappages d'événements

Les données d'identité sont un ensemble spécial de propriétés du système qui inclut **Identity Username, Identity IP, Identity NetBIOS Name, Identity Extended Field, Identity Host Name, Identity MAC, Identity Group Name**.

Lorsque les propriétés d'identité sont remplies par un DSM, les données d'identité sont transmises au service de profileur d'actifs qui s'exécute sur la console IBM QRadar. Le profileur d'actifs est utilisé pour mettre à jour le modèle d'actif, soit en ajoutant de nouveaux actifs, soit en mettant à jour les informations sur les actifs existants, y compris les zones d'actifs **Last User** et **User Last Seen** lorsqu'un **Identity Username** est fourni.

Les DSM IBM QRadar peuvent remplir les données d'identité pour certains événements, tels que ceux qui établissent une association ou une désassociation entre les propriétés d'identité. Cette association ou cette désassociation est relative aux performances et à certains événements qui fournissent des informations nouvelles ou utiles qui sont nécessaires pour les mises à jour d'actifs. Par exemple, un événement de connexion établit une nouvelle association entre un nom d'utilisateur et un actif (une adresse IP, une adresse MAC ou un nom d'hôte ou une combinaison d'entre eux). Le DSM génère des données d'identité pour tous les événements de connexion qu'il analyse, mais les événements suivants de différents types impliquant le même utilisateur ne fournissent pas de nouvelles informations d'association. Par conséquent, le DSM ne génère pas d'identité pour d'autres types d'événements.

De plus, les DSM des services DHCP peuvent générer des données d'identité pour les événements attribués à DHCP, car ces événements établissent une association entre une adresse IP et une adresse MAC. Les DSM pour les services DNS génèrent des informations d'identité pour les événements qui

représentent des recherches DNS car ces événements établissent une association entre une adresse IP et un nom d'hôte ou un nom DNS.

Vous pouvez configurer l'éditeur DSM pour remplacer le comportement des propriétés d'identité. Toutefois, contrairement à d'autres propriétés système, la propriété d'identité remplacée n'a aucun effet, sauf si elle est liée à des combinaisons d'ID événement ou de catégorie d'événement spécifiques (mappages d'événements). Lorsque des substitutions de propriété d'identité sont configurées, vous pouvez accéder à l'onglet **Mappages d'événements** et sélectionner un mappage d'événements pour configurer des propriétés d'identité spécifiques pour cet événement. Seules les propriétés d'identité disponibles et capturées par la propriété configurée regex ou json sont remplies pour un événement.

**Remarque :** La propriété **Identity Username** est unique et ne peut pas être configurée de manière indépendante. Si des propriétés d'identité sont activées pour un mappage d'événements particulier, la propriété **Identity Username** est automatiquement remplie pour l'événement à partir de la valeur de propriété **Username** disponible.

## Création d'une mappe d'événements et d'une catégorisation

Un mappage d'événement est un ID d'événement et une combinaison de catégories que vous utilisez pour mapper un événement à un QID. Avec l'éditeur DSM, vous pouvez créer un mappage d'événements pour mapper tous les événements inconnus à une entrée de la mappe QID. De plus, vous pouvez remapper les existants à une nouvelle catégorisation d'événements (QID) ou à une catégorisation existante dans le système.

### Procédure

1. Pour ajouter un mappage d'événements, cliquez sur l'icône Ajouter (+) dans l'onglet **Mappage d'événements** de l'éditeur DSM.
2. Vérifiez que les valeurs sont entrées pour les zones **Event ID** et **Event Category**.
3. Pour créer une catégorisation d'événements, procédez comme suit :
  - a) Dans la fenêtre **Créer un nouveau mappage d'événement**, cliquez sur **Choisir QID**.
  - b) Dans la fenêtre **Enregistrements QID**, cliquez sur **Créer un enregistrement QID**.
  - c) Entrez des valeurs pour les zones **Name**, **Description** et sélectionnez un **Log Source Type**, un **High Level Category**, un **Low Level Category** et un **Severity**.
  - d) Cliquez sur **Sauvegarder** pour créer la catégorisation des événements.
4. Pour utiliser une catégorisation d'événements existante, procédez comme suit :
  - a) Dans la fenêtre **Créer un nouveau mappage d'événement**, cliquez sur **Choisir un événement**.
  - b) Recherchez une catégorisation d'événements existante dans la fenêtre **Catégorisations d'événements**.
  - c) Sélectionnez un **High Level category**, **Low Level category**, **Log Source Type** ou **QID**. Les résultats sont affichés dans la sous-fenêtre **Résultats de la recherche**.
  - d) Cliquez sur **Ok** pour ajouter la catégorie d'événement.

## Exportation de contenus à partir de l'éditeur DSM

Vous pouvez utiliser un script d'outil de gestion de contenu pour exporter le contenu personnalisé créé dans l'éditeur DSM. Le contenu peut être exporté à partir d'un déploiement IBM QRadar et importé dans un autre déploiement QRadar. Vous pouvez également exporter le contenu personnalisé sur un support externe.

L'éditeur DSM produit les types de contenu suivants :

Type de contenu personnalisé	Chaîne	ID
Propriétés personnalisées	customproperty	6

Tableau 33. Types de contenu de l'éditeur DSM (suite)

Type de contenu personnalisé	Chaîne	ID
Type de source de journal	sensordevicetype	24
Extensions de source de journal	deviceextension	16
Entrées QidMap personnalisées	qidmap	27

Le script contentManagement.pl se trouve dans le répertoire /opt/qradar/bin

## Exportation du contenu en tant que package

Vous pouvez utiliser le script de l'outil de gestion de contenu pour rechercher un contenu spécifique créé dans l'éditeur DSM. Ces contenus sont exportés sous forme de package.

### Procédure

1. Utilisez SSH pour vous connecter à QRadar comme utilisateur root.
2. Pour rechercher des éléments de contenu spécifiques à exporter, entrez la commande suivante :

```
./contentManagement.pl -a search -c [content_type] -r [regex]
```

Par exemple, pour rechercher les éléments de contenu d'un type de source de journal, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl -a search -c 24 -r  
"<search_name>"
```

3. Créez un fichier texte qui répertorie le contenu que vous souhaitez exporter.

Chaque ligne doit inclure le type de contenu personnalisé suivi d'une liste d'ID uniques séparés par des virgules pour ce type.

Par exemple, pour exporter trois types de source de journal avec l'ID 24, l'ID 26 et l'ID 95, toutes les propriétés personnalisées, créez un fichier texte avec les entrées suivantes :

```
sensordevicetype, 24,26,95
```

4. Exportez les éléments de contenu en tant que package à l'aide de la commande suivante :

```
/opt/qradar/bin/contentManagement.pl -a export -c package -f <source_file>
```

## Exportation de contenu pour une propriété personnalisée unique

Vous pouvez utiliser le script de l'outil de gestion de contenu pour exporter le contenu de chaque propriété personnalisée créée à partir de l'onglet **Propriétés** de l'éditeur DSM.

### Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez l'éditeur DSM pour créer des propriétés personnalisées, une entité **customproperty** est produite pour chaque propriété personnalisée créée.

### Procédure

1. Utilisez SSH pour vous connecter à QRadar comme utilisateur root.
2. Pour rechercher un contenu spécifique à exporter, entrez la commande suivante :

```
./contentManagement.pl -a search -c [content_type] -r [regex]
```

Par exemple, pour rechercher le contenu d'une propriété personnalisée, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl -a search -c 6 -r  
"<name_of_custom_property>"
```

3. Pour exporter un contenu de propriété personnalisé, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl -a export -c [content_type]  
-i [content_identifiant]
```





---

## Chapitre 8. Utilisation des données de référence dans QRadar

Utilisez les collectes de données de référence pour stocker et gérer les données métier que vous souhaitez corrélater avec les événements et les flux dans votre environnement IBM QRadar. Vous pouvez ajouter des données métier ou des données de sources externes dans une collection de données de référence, puis utiliser les données dans des recherches QRadar, des filtres, des conditions de test de règle et des réponses de règle.

Les collections de données de référence sont stockées sur la console QRadar, mais les collections sont régulièrement copiées sur chaque hôte géré. Pour de meilleures performances sur les recherches de données, l'hôte géré met en cache les valeurs de données les plus fréquemment référencées.

### Données sur les menaces externes

Vous pouvez utiliser des collectes de données de référence pour intégrer des données sur les indicateurs de compromission (IOC) provenant de fournisseurs tiers dans QRadar. QRadar utilise les données IOC pour détecter plus rapidement les comportements suspects, ce qui permet aux analystes de sécurité d'examiner les menaces et de répondre plus rapidement aux incidents.

Par exemple, vous pouvez importer des données IOC, telles que des adresses IP, des noms DNS, des URL et MD5s, à partir de fournisseurs de données de menace à base d'abonnement ou de source ouverte, et les corrélater avec des événements et des incidents sur votre réseau.

### Données métier

Les collections de données de référence peuvent contenir des données métier spécifiques à votre organisation, telles qu'une liste d'utilisateurs disposant d'un accès système privilégié. Utilisez les données métier pour créer des listes noires et des listes blanches.

Par exemple, utilisez un ensemble de références contenant les ID utilisateur des anciens employés pour les empêcher de se connecter au réseau. Ou bien, vous pouvez utiliser des données métier pour générer une liste blanche qui n'autorise qu'un ensemble limité d'adresses IP à effectuer des fonctions spécifiques.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Types d'ensembles de données de référence

IBM QRadar possède différents types d'ensembles de données de référence qui peuvent gérer différents niveaux de complexité des données. Les types les plus courants sont les ensembles de référence et les cartes de référence.

Si vous souhaitez utiliser les mêmes données de référence dans QRadar SIEM et QRadar Risk Manager, utilisez un ensemble de références. Vous ne pouvez pas utiliser d'autres types d'ensembles de données de référence avec QRadar Risk Manager.

Tableau 34. Types d'ensembles de données de référence

Type d'ensemble	Description	Procédures d'utilisation	Exemples
Ensemble de références	Un ensemble de valeurs uniques.	Utilisez un ensemble de références pour comparer une valeur de propriété à une liste, telle que des adresses IP ou des noms d'utilisateur.	Pour vérifier si une ID de connexion utilisée pour se connecter à QRadar est affectée à un utilisateur, créez un ensemble de références avec le paramètre <b>LoginID</b> .
Mappage de références	Ensemble de données qui mappe une clé unique à une valeur.	Utilisez une mappe de référence pour vérifier une combinaison unique de deux valeurs de propriété.	Pour corrélérer l'activité d'utilisateur sur votre réseau, créez une mappe de référence qui utilise le paramètre <b>LoginID</b> comme clé et <b>Username</b> comme valeur.
Mappage de références d'ensembles	Ensemble de données qui mappe une clé à plusieurs valeurs. Chaque clé est unique et se mappe à un ensemble de références.	Utilisez une mappe de référence d'ensembles pour vérifier une combinaison de deux valeurs de propriété sur une liste.	Pour tester l'accès autorisé à un brevet, créez une mappe d'ensembles qui utilise une propriété d'événement personnalisée pour <b>Patent ID</b> comme clé et le paramètre <b>Username</b> comme valeur. Utilisez la mappe des ensembles pour remplir une liste d'utilisateurs autorisés.
Mappage de références de mappes	Ensemble de données qui mappe une clé à une autre clé, qui est alors mappée à une valeur unique. Chaque clé est unique et elle est mappée à une carte de référence.	Utilisez une mappe de référence de mappes pour vérifier une combinaison de trois valeurs de propriété.	Pour tester les violations de bande passante du réseau, créez une mappe des mappes qui utilise le paramètre <b>Source IP</b> comme première clé, le paramètre <b>Application</b> comme seconde clé et le paramètre <b>Total Bytes</b> comme valeur.
Table de référence	Ensemble de données qui mappe une clé à une autre clé, qui est alors mappée à une valeur unique. La deuxième clé est affectée à un type de données.	Utilisez une table de référence pour vérifier une combinaison de trois valeurs de propriété lorsque l'une des propriétés est un type de données spécifique.	Créez une table de référence qui stocke <b>Username</b> comme première clé, <b>Source IP</b> comme seconde clé avec un type de données <b>cidr</b> affecté, et <b>Source Port</b> comme valeur.

#### Tâches associées

«Création de collections de données de référence à l'aide de la ligne de commande», à la page 186

Utilisez la ligne de commande pour gérer les collections de données de référence qui ne peuvent pas être gérées dans IBM QRadar, telles que les mappes de référence, la mappe des ensembles, la carte des mappes et les tables. Bien qu'il soit plus facile de gérer des ensembles de références à l'aide de QRadar, utilisez la ligne de commande lorsque vous souhaitez planifier des tâches de gestion.

«Création de collections de données de référence avec les API», à la page 190

Vous pouvez utiliser l'interface de programme d'application (API) pour gérer les collections de données de référence IBM QRadar.

## Présentation des jeux de références

---

Utilisez des ensembles de références dans IBM QRadar pour stocker des données dans un format de liste simple.

Vous pouvez remplir l'ensemble de référence avec des données externes, telles que des indicateurs de compromis (IOC), ou vous pouvez l'utiliser pour stocker des données métier, telles que des adresses IP et des noms d'utilisateur, collectées à partir d'événements et de flux qui se produisent sur votre réseau.

Un ensemble de références contient des valeurs uniques que vous pouvez utiliser dans les recherches, les filtres, les conditions de test de règles et les réponses aux règles. Les règles d'utilisation permettent de vérifier si un ensemble de référence contient un élément de données ou de configurer la réponse de règle pour ajouter des données à un ensemble de références. Par exemple, vous pouvez créer une règle qui détecte lorsqu'un employé accède à un site Web interdit et configurer la réponse de règle pour ajouter l'adresse IP ou le nom d'utilisateur de l'employé à un ensemble de référence.

Pour plus d'informations sur la configuration des réponses de règle pour ajouter des données à un ensemble de références, voir *IBM QRadar - Guide d'utilisation*.

Les ensembles de référence sont le seul type de collecte de données de référence que vous pouvez gérer dans QRadar. Vous pouvez également utiliser les fichiers [command-line](#) et [Interface de la documentation de l'API de résilience](#) pour gérer les ensembles de références.

### Tâches associées

[Création de collections de données de référence à l'aide de la ligne de commande](#)

Utilisez la ligne de commande pour gérer les collections de données de référence qui ne peuvent pas être gérées dans IBM QRadar, telles que les mappes de référence, la mappe des ensembles, la carte des mappes et les tables. Bien qu'il soit plus facile de gérer des ensembles de références à l'aide de QRadar, utilisez la ligne de commande lorsque vous souhaitez planifier des tâches de gestion.

[Création de collections de données de référence avec les API](#)

Vous pouvez utiliser l'interface de programme d'application (API) pour gérer les collections de données de référence IBM QRadar.

## Ajout, édition et suppression d'ensembles de références

Utilisez un ensemble de références pour comparer une valeur de propriété, telle qu'une adresse IP ou un nom d'utilisateur, à une liste. Vous pouvez utiliser des ensembles de référence avec des règles pour conserver des listes de surveillance. Par exemple, vous pouvez créer une règle pour détecter quand un employé accède à un site Web interdit, puis ajouter l'adresse IP de cet employé à un ensemble de références.

### Pourquoi et quand exécuter cette tâche


Une fois que vous avez ajouté des données au jeu de références, les paramètres **Nombre d'éléments** et **Règles associées** sont automatiquement mis à jour.

Lorsque vous éditez un ensemble de références, vous pouvez modifier les valeurs de données, mais vous ne pouvez pas modifier le type de données que contient le jeu de références.

Avant de supprimer un jeu de référence, QRadar exécute une vérification de dépendance pour voir si l'ensemble de référence comporte des règles qui lui sont associées.

**Remarque :** Si vous utilisez des techniques pour brouiller les données des propriétés d'événement que vous souhaitez comparer aux données de l'ensemble de référence, utilisez un ensemble de références alphanumériques et ajoutez les valeurs de données brouillées.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des ensembles de référence**.
3. Pour ajouter un ensemble de références, procédez comme suit :
  - a) Cliquez sur **Ajouter** et configurez les paramètres.

### En savoir plus sur les paramètres de l'ensemble de références :

Le tableau suivant décrit chacun des paramètres utilisés pour configurer un ensemble de référence.

Paramètre	Description
<b>Nom</b>	Le nom d'ensemble de référence ne peut pas comporter plus de 255 caractères.
<b>Type</b>	<p>Sélectionnez les types de données pour les éléments de référence. Vous ne pouvez pas éditer le paramètre <b>Type</b> après avoir créé un ensemble de référence.</p> <p>Le type <b>IP</b> permet de stocker des adresses IPv4. Le type <b>Alphanumérique (Ignorer la casse)</b> convertit automatiquement toute valeur alphanumérique en minuscules.</p> <p>Pour comparer des propriétés de flux et d'événement brouillées aux données de référence, vous devez utiliser un ensemble de référence alphanumérique.</p>
<b>Durée de vie des éléments</b>	<p>Indique à quel moment les éléments de référence arrivent à expiration. Si vous sélectionnez le paramètre par défaut <b>Lives Forever</b>, les éléments de référence n'expirent pas.</p> <p>Si vous spécifiez une durée, indiquez si l'intervalle de temps à vivre est basé sur la date à laquelle les données ont été vues pour la première fois ou pour la dernière fois.</p> <p>QRadar supprime périodiquement les éléments périmés de l'ensemble de référence (par défaut, toutes les 5 minutes).</p>

Paramètre	Description
<b>Lorsque des éléments arrivent à expiration</b>	<p>Indique comment les éléments de référence périmés sont consignés dans le fichier qradar.log lorsqu'ils sont supprimés de l'ensemble de référence.</p> <p>L'option <b>Consigner chaque élément dans une entrée de journal distincte</b> déclenche un événement de journal <b>élément de donnée de référence expirée</b> pour chaque élément de référence supprimé. Celui-ci contient le nom de l'ensemble de référence et la valeur d'élément.</p> <p>L'option <b>Éléments de journal dans une entrée de journal</b> déclenche un événement de journal <b>élément de donnée de référence expirée</b> pour tous les éléments de référence qui sont supprimés en même temps. L'événement contient le nom de l'ensemble de référence et les valeurs d'élément.</p> <p>L'option <b>Ne pas consigner les éléments</b> ne déclenche pas d'événement de journal pour les éléments de référence supprimés.</p>

b) Cliquez sur **Créer**.

4. Cliquez sur **Éditer** ou sur **Supprimer** pour utiliser les ensembles de référence existants.

**Conseil :** Pour supprimer plusieurs jeux de références, utilisez la zone de texte **Recherche rapide** pour rechercher les ensembles de références que vous souhaitez supprimer, puis cliquez sur **Supprimer la liste**.

#### Tâches associées

[Affichage des contenus d'un ensemble de référence](#)


[Suivi des comptes utilisateur arrivés à expiration](#)

Utilisez les collectes de données de référence pour identifier les données périmées, telles que les comptes utilisateur arrivés à expiration, dans votre environnement IBM QRadar.

## Affichage des contenus d'un ensemble de référence

Affichez les informations relatives aux éléments de données dans l'ensemble de référence, telles que l'affectation de domaine, l'expiration des données et la date à laquelle l'élément a été vu pour la dernière fois dans votre réseau.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des ensembles de référence**.
3. Sélectionnez un ensemble de références et cliquez sur **Afficher le contenu**.
4. Cliquez sur l'onglet **Contenu** pour afficher des informations sur chaque élément de données.

**Conseil :** Utilisez la zone de recherche pour filtrer tous les éléments qui correspondent à un mot clé. Vous ne pouvez pas rechercher des données dans la colonne **Durée de vie**.

#### En savoir plus sur les éléments de données :

Le tableau suivant décrit les informations affichées pour chaque élément de données de l'ensemble de référence.

<i>Tableau 36. Informations sur les éléments de données de l'ensemble de référence</i>	
<b>Paramètre</b>	<b>Description</b>
<b>Domain</b>	Les données de référence propres à un domaine peuvent être consultées par les utilisateurs titulaires qui ont accès au domaine, les administrateurs MSSP et les utilisateurs qui ne possèdent pas d'affectation de titulaire. Les utilisateurs dans tous les titulaires peuvent afficher les données de référence partagées.
<b>Valeur</b>	Élément de données qui est stocké dans l'ensemble de référence. Par exemple, la valeur peut correspondre aux noms d'utilisateur ou aux adresses IP.
<b>Origine</b>	Affiche le nom d'utilisateur lorsque l'élément de données est ajouté manuellement et le nom de fichier lorsque les données ont été importées depuis un fichier externe. Affiche le nom de règle lorsque l'élément de données est ajouté en réponse à une règle.
<b>Durée de vie</b>	Temps restant avant le retrait de cet élément de l'ensemble de référence.
<b>Date de la dernière consultation</b>	Date et heure de la dernière détection de cet élément sur votre réseau.

5. Cliquez sur l'onglet **Références** pour afficher les règles qui utilisent l'ensemble de référence dans un test de règle ou dans une réponse à la règle.

<i>Tableau 37. Paramètres de l'onglet Contenu</i>	
<b>Paramètre</b>	<b>Description</b>
<b>Nom de la règle</b>	Nom de la règle qui est configurée pour utiliser l'ensemble de référence.
<b>Grouper</b>	Groupe auquel appartient la règle.
<b>Catégorie</b>	Indique si la règle est une règle personnalisée ou une règle de détection des anomalies.
<b>Type</b>	Affiche <b>événement</b> , <b>flux</b> , <b>commun</b> ou <b>infraction</b> pour indiquer le type de données sur lesquelles la règle est testée.
<b>Activé</b>	Une règle doit être activée pour que le moteur de règle personnalisée puisse l'évaluer.
<b>response</b>	Réponses qui sont configurées pour cette règle.
<b>Origine</b>	<b>Système</b> indique une règle par défaut. <b>Modifiée</b> indique qu'une règle par défaut a été personnalisée. <b>Utilisateur</b> indique une règle créée par l'utilisateur.

6. Pour afficher ou modifier une règle associée, cliquez deux fois sur la règle dans la liste **Références** et exécutez l'assistant de règle.

## Ajout d'éléments à un ensemble de référence

Ajoutez des éléments à un ensemble de références lorsque vous souhaitez que IBM QRadar compare une propriété à la valeur de l'élément. Utilisez QRadar pour ajouter manuellement des éléments à un ensemble de référence ou pour importer des éléments à partir d'un fichier .csv.


## Avant de commencer

Pour importer des éléments, assurez-vous que le fichier .csv est stocké localement.

## Pourquoi et quand exécuter cette tâche

Vous pouvez affecter des données de référence à un domaine spécifique. Les données de référence propres à un domaine peuvent être consultées par les utilisateurs titulaires qui ont accès au domaine, les administrateurs MSSP et les utilisateurs qui ne possèdent pas d'affectation de titulaire. Les utilisateurs dans tous les titulaires peuvent afficher les données de référence partagées. Par exemple, les utilisateurs MSSP qui ne sont pas des administrateurs peuvent afficher les données de référence qui sont affectées à un domaine.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des ensembles de référence**.
3. Sélectionnez le jeu de référence auquel vous souhaitez ajouter les éléments, puis cliquez sur **Afficher le contenu**.
4. Cliquez sur l'onglet **Contenu**.
5. Pour ajouter des éléments de données manuellement, procédez comme suit :

- a) Cliquez sur **Ajouter** et configurez les paramètres.

Les valeurs de port valides sont comprises entre 0 et 65535. Les adresses IP valides sont comprises entre 0 et 255.255.255.255.

**Remarque :** Si vous utilisez des techniques de brouillage de données pour les propriétés d'événement que vous voulez comparer aux données de l'ensemble de référence, vous devez utiliser un ensemble de référence alphanumérique contenant les valeurs de données brouillées.

- b) Cliquez sur **Ajouter**.
6. Pour ajouter des éléments à partir d'un fichier .csv, procédez comme suit :
  - a) Cliquez sur **Importer**.
  - b) Cliquez sur **Sélectionner un fichier** et parcourez pour sélectionner le fichier .csv à importer.


Le fichier .csv doit être formaté avec tous les éléments séparés par des virgules sur une seule ligne, ou avec chaque élément sur une ligne distincte. Il n'est pas nécessaire d'utiliser un délimiteur lorsque chaque élément se trouve sur une ligne distincte.
  - c) Sélectionnez le **Domaine** auquel vous souhaitez ajouter les données de l'ensemble de références.
  - d) Cliquez sur **Importer**.

L'importation ajoute le contenu du fichier texte à l'ensemble de référence.

## Exportation d'éléments depuis un ensemble de référence

Exportez les éléments d'ensemble de référence dans un fichier .csv lorsque vous souhaitez inclure les informations dans les rapports ou partager les informations avec des personnes qui n'utilisent pas IBM QRadar.

## Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des ensembles de référence**.
3. Sélectionnez l'ensemble de référence à exporter et cliquez sur **Afficher le contenu**.
4. Cliquez sur l'onglet **Contenu**, puis cliquez sur **Exporter**.

- Indiquez si vous souhaitez ouvrir le fichier immédiatement, ou enregistrez le fichier, puis cliquez sur **OK**.

## Suppression d'éléments dans un ensemble de référence

Il se peut que vous devez supprimer des éléments d'un ensemble de références lorsqu'un élément est ajouté à l'ensemble de références erroné ou lorsque vous n'avez plus besoin de comparer l'élément avec d'autres propriétés IBM QRadar. Par exemple, il se peut que vous devez supprimer un actif qui a été ajouté par erreur à une liste noire d'exclusion d'actifs.

### Procédure

- Dans le menu de navigation () , cliquez sur **Admin**.
- Dans la section **Configuration du système**, cliquez sur **Gestion des ensembles de référence**.
- Sélectionnez l'ensemble de référence contenant les éléments à supprimer, puis cliquez sur **Afficher le contenu**.
- Cliquez sur l'onglet **Contenu** et choisissez l'une des options suivantes :
  - Pour supprimer un seul élément, sélectionnez-le dans la liste, puis cliquez sur **Supprimer**.
  - Pour supprimer plusieurs éléments, utilisez la zone de recherche afin de filtrer la liste et de n'afficher que les éléments à supprimer, puis cliquez sur **Supprimer les éléments répertoriés**.

## Création de collections de données de référence à l'aide de la ligne de commande

Utilisez la ligne de commande pour gérer les collections de données de référence qui ne peuvent pas être gérées dans IBM QRadar, telles que les mappes de référence, la mappe des ensembles, la carte des mappes et les tables. Bien qu'il soit plus facile de gérer des ensembles de références à l'aide de QRadar, utilisez la ligne de commande lorsque vous souhaitez planifier des tâches de gestion.

### Pourquoi et quand exécuter cette tâche

Utilisez le script `ReferenceDataUtil.sh` pour gérer des ensembles de référence et d'autres types de collectes de données de référence.

Lorsque vous utilisez un fichier externe pour remplir la collecte de données de référence, la première ligne de non-commentaire dans le fichier identifie les noms de colonne dans la collecte de données de référence. Chaque ligne après cette ligne est un enregistrement de données qui est ajouté à la collection. Alors que le type de données pour les valeurs de collection de référence est spécifié lors de la création de la collection, chaque clé est une chaîne alphanumérique.

Le tableau suivant présente des exemples de formatage de données dans un fichier externe à utiliser pour renseigner les mappes de référence.

Type de collection de référence	Exemples de formatage de données
Mappage de références	key1,data key1,value1 key2,value2



Tableau 38. Formatage des données dans un fichier externe à utiliser pour le remplissage des collections de données de référence (suite)

Type de collection de référence	Exemples de formatage de données
Mappage de références d'ensembles	key1,data key1,value1 key1,value2
Mappage de références de mappes	key1,key2,data map1,key1,value1 map1,key2,value2

Vous pouvez également créer des collections de données de référence à l'aide du nœud final /reference\_data dans l'API QRadar RESTful.

## Procédure

1. À l'aide de SSH, connectez-vous à IBM QRadar en tant que superutilisateur.
2. Accédez au répertoire /opt/qradar/bin.
3. Pour créer la collecte de données de référence, entrez la commande suivante :

```
./ReferenceDataUtil.sh create name
[SET | MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
[ALN | NUM | IP | PORT | ALNIC | DATE]
[-timeoutType=[FIRST_SEEN | LAST_SEEN]] [-timeToLive=]
```

4. Pour remplir la mappe avec les données d'un fichier externe, entrez la commande suivante :

```
./ReferenceDataUtil.sh load name filename
[-encoding=...] [-sdf=" ... "]
```

## Exemple

Voici quelques exemples d'utilisation de la ligne de commande pour créer différents types de collections de données de référence :

- Créez une mappe alphanumérique :

```
./ReferenceDataUtil.sh create testALN MAP ALN
```

- Créez une mappe d'ensembles contenant des valeurs de port qui vieilliront 3 heures après avoir été vues pour la dernière fois :

```
./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT
-timeoutType=LAST_SEEN -timeToLive='3 hours'
```

- Créez une mappe de mappes contenant des valeurs numériques qui vieilliront 3 heures 15 minutes après qu'elles ont été vues pour la première fois :

```
./ReferenceDataUtil.sh create testNUM MAPOFMAPS
NUM -timeoutType=FIRST_SEEN -timeToLive='3 hours 15 minutes'
```

- Créez une table de référence où le format par défaut est alphanumérique :

```
./ReferenceDataUtil.sh create testTable REFTABLE
ALN -keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

## Que faire ensuite

Connectez-vous à QRadar pour créer des règles qui ajoutent des données à vos collections de données de référence. Vous pouvez également créer des tests de règle qui détectent l'activité à partir d'éléments de votre collection de données de référence.

### Concepts associés

[Présentation des jeux de références](#)

## Référence de commande pour les utilitaires de données de référence

Vous pouvez gérer vos collections de données de référence à l'aide de l'utilitaire `ReferenceDataUtil.sh` sur la ligne de commande. Les commandes suivantes sont disponibles pour être utilisées avec le script.

### Créer

Crée une collecte de données de référence.

#### *name*

Nom de la collecte de données de référence.

#### **[SET | MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]**

Type de collecte de données de référence.

#### **[ALN | ALNIC | NUM | IP | PORT | DATE]**

Type de données dans l'ensemble de référence.

- **ALN** indique les valeurs alphanumériques. Ce type de données prend en charge les adresses IPv4 et IPv6.
- **ALNIC** indique les valeurs alphanumériques, mais les tests de règles ignorent le cas. Ce type de données prend en charge les adresses IPv4 et IPv6.
- **NUM** indique les valeurs numériques.
- **IP** indique les adresses IP. Ce type de données prend en charge uniquement l'adresse IPv4.
- **PORT** indique les adresses de port.
- **DATE** indique les valeurs de date.

#### **[-timeoutType=[FIRST\_SEEN | LAST\_SEEN]]**

Indique si la durée d'exécution des éléments de données dans la collecte de données de référence est à partir du moment où l'élément a été vu ou vu pour la dernière fois.

#### **[-TimeToLive=""]**

Durée pendant que les éléments de données restent dans la collecte de données de référence.

#### **[-keyType=name:elementType,name:elementType,...]**

Un paramètre **REFTABLE** obligatoire composé de paires de nom de clé **ELEMENTTYPE**.

#### **[-key1Label=""]**

Libellé facultatif pour key1 ou la clé primaire. Une clé est un type d'information, telle qu'une adresse IP.

#### **[-valueLabel=""]**

Libellé facultatif pour les valeurs de la collection.

### Mettre à jour

Met à jour une collecte de données de référence.

#### *name*

Nom de la collecte de données de référence.

#### **[-timeoutType=[FIRST\_SEEN | LAST\_SEEN]]**

Indique si la durée d'exécution des éléments de données dans la collecte de données de référence est à partir du moment où l'élément a été vu ou vu pour la dernière fois.

**[-timeToLive=""]**

Durée pendant que les éléments de données restent dans la collecte de données de référence.

**[-keyType=name:elementType,name:elementType,...]**

Un paramètre **REFTABLE** obligatoire composé de paires de nom de clé **elementType** .

**[-key1Label=""]**

Libellé facultatif pour key1.

**[-valueLabel=""]**

Libellé facultatif pour les valeurs de la collection.

## Ajouter

Ajoute un élément de données à une collecte de données de référence

**name**

Nom de la collecte de données de référence.

**<value> <key1> [key2]**

La paire de valeurs de clé que vous souhaitez ajouter. Les clés sont des chaînes alphanumériques.

- Les MAP et MAPOFSETS requièrent la clé 1.
- MAPOFMAPS et REFTABLE nécessitent la clé 1 et la clé 2 de deuxième niveau.

**[-sdf=" ... "]**

Chaîne de format de date simple utilisée pour analyser les données de date.

## Supprimer

Supprime un élément d'une collecte de données de référence.

**name**

Nom de la collecte de données de référence.

**<value> <key1> [key2]**

La paire de valeurs de clé que vous souhaitez supprimer. Les clés sont des chaînes alphanumériques.

- Les MAP et MAPOFSETS requièrent la clé 1.
- MAPOFMAPS et REFTABLE nécessitent la clé 1 et la clé 2 de deuxième niveau.

**[-sdf=" ... "]**

Chaîne de format de date simple utilisée pour analyser les données de date.

## Retirer

Supprime une collecte de données de référence.

**name**

Nom de la collecte de données de référence.

## Purge

Purge tous les éléments d'une collecte de données de référence.

**name**

Nom de la collecte de données de référence.

## Liste

Répertorie les éléments d'une collection de données de référence.

**name**

Nom de la collecte de données de référence.

**[displayContents]**

Répertorie tous les éléments de la collecte de données de référence spécifiée.

## Listall

Répertorie tous les éléments de toutes les collections de données de référence.

### [displayContents]

Répertorie tous les éléments de toutes les collections de données de référence.

## Charger

Remplit une collecte de données de référence avec des données issues d'un fichier .csv externe.

### *name*

Nom de la collecte de données de référence.

### *filename*

Nom de fichier complet à charger. Chaque ligne du fichier représente un enregistrement à ajouter à la collecte de données de référence.

### [-encoding=...]

Codage utilisé pour lire le fichier.

### [-sdf=" ... "]

Chaîne de format de date simple utilisée pour analyser les données de date.

## Création de collections de données de référence avec les API

Vous pouvez utiliser l'interface de programme d'application (API) pour gérer les collections de données de référence IBM QRadar.

### Procédure

1. Utilisez un navigateur Web pour accéder à `https://<Console IP>/api_doc` et connectez-vous en tant qu'administrateur.
2. Sélectionnez la dernière itération de l'API IBM QRadar.
3. Sélectionnez le répertoire `/reference_data`.
4. Pour créer un ensemble de référence, procédez comme suit :
  - a) Sélectionnez `/sets`.
  - b) Cliquez sur **PUBLIER** et entrez les informations pertinentes dans les zones **Valeur**.

#### En savoir plus sur les paramètres pour créer un ensemble de référence :

Le tableau suivant fournit des informations sur les paramètres requis pour créer un ensemble de références :

Paramètre	Type	Valeur	Type de données	Type MIME	Exemple
element_type	requête	(obligatoire)	Chaîne	texte/brut	Chaîne <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
nom	requête	(obligatoire)	Chaîne	texte/brut	Chaîne
champs	requête	(facultatif)	Chaîne	texte/brut	field_one (field_two, field_three), field_four
time_to_live	requête	(facultatif)	Chaîne	texte/brut	Chaîne

Tableau 39. Paramètres - Ensemble de référence (suite)					
Paramètre	Type	Valeur	Type de données	Type MIME	Exemple
timeout_type	requête	(facultatif)	Chaîne	texte/brut	Chaîne <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>

- c) Cliquez sur **Essayer** pour terminer la création de la collecte de données de référence et pour afficher les résultats.
5. Pour créer une nouvelle mappe de référence, procédez comme suit :
- Cliquez sur /maps.
  - Cliquez sur **PUBLIER** et entrez les informations pertinentes dans les zones **Valeur**.

**En savoir plus sur les paramètres pour créer une mappe de référence :**

Le tableau suivant fournit des informations sur les paramètres requis pour créer une mappe de référence :

Tableau 40. Paramètres - Mappe de référence					
Paramètre	Type	Valeur	Type de données	Type MIME	Exemple
element_type	requête	(obligatoire)	Chaîne	texte/brut	Chaîne <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
nom	requête	(obligatoire)	Chaîne	texte/brut	Chaîne
champs	requête	(facultatif)	Chaîne	texte/brut	field_one (field_two, field_three), field_four
key_label	requête	(facultatif)	Chaîne	texte/brut	Chaîne
time_to_live	requête	(facultatif)	Chaîne	texte/brut	Chaîne
timeout_type	requête	(facultatif)	Chaîne	texte/brut	Chaîne <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>
value_label	requête	(facultatif)	Chaîne	texte/brut	Chaîne

- c) Cliquez sur **Essayer** pour terminer la création de la collecte de données de référence et pour afficher les résultats.
6. Pour créer une nouvelle mappe de référence d'ensembles, procédez comme suit :
- Sélectionnez /map\_of\_sets.
  - Cliquez sur **PUBLIER** et entrez les informations pertinentes dans les zones **Valeur**.

**En savoir plus sur les paramètres pour créer une mappe de référence d'ensembles :**

Le tableau suivant fournit des informations sur les paramètres requis pour créer une mappe de référence d'ensembles :

Tableau 41. Paramètres - Mappe de référence des ensembles					
Paramètre	Type	Valeur	Type de données	Type MIME	Exemple
element_type	requête	(obligatoire)	Chaîne	texte/brut	Chaîne <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
nom	requête	(obligatoire)	Chaîne	texte/brut	Chaîne
champs	requête	(facultatif)	Chaîne	texte/brut	field_one (field_two, field_three), field_four
key_label	requête	(facultatif)	Chaîne	texte/brut	Chaîne
time_to_live	requête	(facultatif)	Chaîne	texte/brut	Chaîne
timeout_type	requête	(facultatif)	Chaîne	texte/brut	Chaîne <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>
value_label	requête	(facultatif)	Chaîne	texte/brut	Chaîne

c) Cliquez sur **Essayer** pour terminer la création de la collecte de données de référence et pour afficher les résultats.

7. Pour créer une table de référence ou une mappe de mappes, procédez comme suit :

a) Cliquez sur /tables.

b) Cliquez sur **PUBLIER** et entrez les informations pertinentes dans les zones **Valeur**.

#### En savoir plus sur les paramètres pour créer une table de référence ou une mappe de mappes :

Le tableau suivant fournit des informations sur les paramètres requis pour créer une table de référence ou une mappe de mappes :

Tableau 42. Paramètres - Table de référence					
Paramètre	Type	Valeur	Type de données	Type MIME	Exemple
element_type	requête	(obligatoire)	Chaîne	texte/brut	Chaîne <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
nom	requête	(obligatoire)	Chaîne	texte/brut	Chaîne
champs	requête	(facultatif)	Chaîne	texte/brut	field_one (field_two, field_three), field_four
key_name_types	requête	(facultatif)	Array	application/json	[ { "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>", "key_name": "String" } ]

Tableau 42. Paramètres - Table de référence (suite)					
Paramètre	Type	Valeur	Type de données	Type MIME	Exemple
outer_key_label	requête	(facultatif)	Chaîne	texte/brut	Chaîne
time_to_live	requête	(facultatif)	Chaîne	texte/brut	Chaîne
timeout_type	requête	(facultatif)	Chaîne	texte/brut	Chaîne <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>

- c) Cliquez sur **Essayer** pour terminer la création de la collecte de données de référence et pour afficher les résultats.

### Concepts associés

[Présentation des jeux de références](#)

## Exemples d'utilisation des ensembles de données de référence

Ces exemples montrent comment utiliser des collectes de données de référence pour suivre et stocker les données que vous souhaitez utiliser dans les recherches QRadar, les filtres, les conditions de test de règles et les réponses aux règles.

### Suivi des comptes utilisateur arrivés à expiration

Utilisez les collectes de données de référence pour identifier les données périmées, telles que les comptes utilisateur arrivés à expiration, dans votre environnement IBM QRadar.

#### Pourquoi et quand exécuter cette tâche

Par défaut, les données de référence restent dans QRadar jusqu'à ce qu'elles soient supprimées. Toutefois, lorsque vous créez une collecte de données de référence, vous pouvez configurer QRadar pour supprimer les données après une période donnée.

Lorsque l'élément de données expire, QRadar supprime automatiquement la valeur de la collecte de données de référence et déclenche un événement pour suivre l'expiration.

#### Procédure

1. Créez un ensemble de références pour conserver le suivi de l'heure depuis la dernière connexion d'un utilisateur.
  - a) Définissez **Temps de vie des éléments** pour représenter la période de temps après laquelle un compte utilisateur inutilisé a expiré.
  - b) Cliquez sur le bouton **Depuis la dernière vue**.
2. Créez une règle d'événement personnalisé pour ajouter des données de connexion, telles que **username**, au jeu de références.

**Remarque :** QRadar effectue le suivi de **Date de la dernière vue** pour chaque élément de données. Si aucune donnée n'est ajoutée pour un utilisateur particulier dans la période de temps à vivre, l'élément de jeu de référence expire et un événement **Expiration des données de référence** est déclenché. L'événement contient le nom de l'ensemble de référence et le nom d'utilisateur qui est arrivé à expiration.

3. Utilisez l'onglet **Activité de journal** pour suivre les événements **Expiration des données de référence**.

### **Que faire ensuite**

Utilisez les données de l'ensemble de référence dans les recherches, les filtres, les conditions de test de règle et les réponses des règles.

### **Tâches associées**

Ajout, édition et suppression d'ensembles de références

## **Intégration de données dynamiques à partir de sources externes**

Les grandes organisations d'entreprise peuvent utiliser des collectes de données de référence pour partager des informations sur leurs actifs informatiques avec les équipes de sécurité qui gèrent le déploiement IBM QRadar.

Par exemple, l'équipe Technologie de l'information (IT) gère une base de données de gestion d'actifs qui contient des informations sur tous les actifs du réseau. Certaines informations, telles que les adresses IP des serveurs Web, changent fréquemment.

Une fois par semaine, l'équipe informatique exporte la liste des adresses IP pour tous les serveurs Web déployés sur le réseau et fournit la liste à l'équipe de sécurité. L'équipe de sécurité importe la liste dans un ensemble de référence, qui peut ensuite être utilisé dans les règles, les recherches et les rapports pour fournir plus de contexte aux événements et aux flux traités par QRadar.



---

## Chapitre 9. Configuration de la source d'informations utilisateur

Configurez votre système IBM QRadar pour collecter des informations sur les utilisateurs et les groupes à partir des nœuds finaux Identity and Access Management.

QRadar utilise les informations collectées à partir des nœuds finaux pour enrichir les informations utilisateur associées au trafic et aux événements qui se produisent sur votre réseau.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Présentation de la source d'informations utilisateur

Vous pouvez configurer une source d'informations utilisateur pour activer la collecte des informations utilisateur à partir d'un point de terminaison de gestion des accès et des identités.

Un nœud final de gestion des identités et des accès est un produit qui collecte et gère les identités électroniques des utilisateurs, les appartenances de groupe et les droits d'accès. Ces nœuds finaux sont appelés sources d'informations utilisateur.

Utilisez les utilitaires suivants pour configurer et gérer les sources d'informations utilisateur :

- **Tivoli Directory Integrator**- Vous devez installer et configurer Tivoli Directory Integrator sur un hôte non-IBM QRadar.
- **UISConfigUtil.sh** - Utilisez cet utilitaire pour créer, extraire, mettre à jour ou supprimer des sources d'informations utilisateur. Vous pouvez utiliser les sources d'informations utilisateur pour intégrer IBM QRadar SIEM à l'aide d'un serveur Tivoli Directory Integrator.
- **GetUserInfo.sh** - Utilisez cet utilitaire pour collecter des informations utilisateur à partir d'une source d'informations utilisateur et stocker les informations dans une collecte de données de référence. Vous pouvez utiliser cet utilitaire pour collecter des informations utilisateur sur demande ou sur un planning.

## source d'informations utilisateur

Une source d'informations utilisateur est un composant configurable qui permet la communication avec un nœud final pour extraire des informations d'utilisateur et de groupe.

Les systèmes IBM QRadar prennent en charge les sources d'informations utilisateur suivantes :

Tableau 43. Sources d'informations prises en charge

Source d'informations	Informations collectées
<p>Microsoft Windows Active Directory (AD), version 2008- Microsoft Windows AD est un service d'annuaire qui authentifie et autorise tous les utilisateurs et ordinateurs qui utilisent votre réseau Windows.</p>	<ul style="list-style-type: none"> <li>• full_name</li> <li>• user_name</li> <li>• user_principal_name</li> <li>• family_name</li> <li>• given_name</li> <li>• account_is_disabled</li> <li>• account_is_locked</li> <li>• password_is_expired</li> <li>• password_can_not_be_changed</li> <li>• no_password_expired</li> <li>• password_does_not_expire</li> </ul>
<p>IBM Security Access Manager (ISAM), version 7.0-ISAM est une solution d'authentification et d'autorisation pour les applications Web, client/serveur et existantes. Pour plus d'informations, consultez la documentation d'IBM Security Access Manager (ISAM).</p>	<ul style="list-style-type: none"> <li>• name_in_rgy</li> <li>• prénom</li> <li>• nom</li> <li>• account_valid</li> <li>• password_valid</li> </ul>
<p>IBM Security Identity Manager (ISIM), version 6.0-ISIM fournit le logiciel et les services permettant de déployer des solutions d'application des accès basées sur des règles. Ce produit automatise le processus d'application des accès des employés, des entrepreneurs et des partenaires commerciaux IBM ayant des droits d'accès aux applications dont ils ont besoin, que ce soit dans un environnement d'entreprise fermé ou dans une entreprise virtuelle ou étendue. Pour plus d'informations, consultez la documentation d'IBM Security Integration Manager (ISIM).</p>	<ul style="list-style-type: none"> <li>• Nom complet</li> <li>• Nom distinctif</li> </ul>

## Collections de données de référence pour les informations utilisateur

Cette rubrique fournit des informations sur la manière dont les ensembles de données de référence stockent les données collectées à partir des sources d'informations utilisateur.

Lorsque IBM QRadar SIEM recueille des informations à partir d'une source d'informations utilisateur, il crée automatiquement un ensemble de données de référence pour stocker les informations. Le nom de l'ensemble de données de référence est dérivé du nom du groupe de sources d'informations utilisateur. Par exemple, un ensemble de données de référence qui est recueilli à partir de Microsoft Windows AD peut être nommé Admins du domaine.

Le type d'ensemble de données de référence est une mappe de mappes. Dans une mappe de référence des mappes, les données sont stockées dans des enregistrements qui mappent une clé vers une autre clé, qui est ensuite mappée à une valeur unique.

Par exemple :

- #
- # Domain Admins

- # key1, key2, data
- smith\_j, Full Name, John Smith
- smith\_j, account\_is\_disabled, 0
- smith\_j, account\_is\_locked, 0
- smith\_j, account\_is\_locked, 1
- smith\_j, password\_does\_not\_expire, 1

Pour plus d'informations sur les ensembles de données de référence, voir la *Note technique sur les ensembles de données de référence*.

## Exemple de flux d'intégration

Une fois que les informations d'utilisateur et de groupe sont collectées et stockées dans une collecte de données de référence, vous pouvez utiliser les données dans IBM QRadar SIEM de plusieurs manières.

Vous pouvez créer des rapports et des alertes significatifs qui caractérisent l'adhésion des utilisateurs aux règles de sécurité de votre entreprise.

Prenons l'exemple suivant :

Pour vous assurer que les activités exécutées par des utilisateurs ISIM privilégiés sont conformes à vos règles de sécurité, vous pouvez effectuer les tâches suivantes :

Créez une source de journal pour collecter et analyser les données d'audit pour chaque serveur ISIM à partir duquel les journaux sont collectés. Pour plus d'informations sur la création d'une source de journal, voir *Managing Log Sources Guide*.

1. Créez une source d'informations utilisateur pour le serveur ISIM et collectant des informations sur les groupes d'utilisateurs ISIM. Cette étape crée une collecte de données de référence appelée Administrateurs ISIM.

Voir «Création d'une source d'informations utilisateur», à la page 200.

2. Configurez un bloc de construction pour tester les événements dans lesquels l'adresse IP source est le serveur ISIM et le nom d'utilisateur est répertorié dans la collecte de données de référence de l'administrateur ISIM. Pour plus d'informations sur les blocs de construction, voir *Guide de l'utilisateur* pour votre produit.
3. Créez une recherche d'événements qui utilise le bloc de génération personnalisé comme filtre. Pour plus d'informations sur les recherches d'événements, voir *IBM QRadar - Guide d'utilisation* pour votre produit.
4. Créez un rapport personnalisé qui utilise la recherche d'événements personnalisés pour générer des rapports quotidiens sur l'activité d'audit des utilisateurs ISIM privilégiés. Ces rapports générés indiquent si une activité d'administrateur ISIM viole votre règle de sécurité. Pour plus d'informations sur les rapports, voir *IBM QRadar - Guide d'utilisation* pour votre produit.

**Remarque :** Si vous souhaitez collecter des journaux de sécurité d'application, vous devez créer un module de support de périphérique (DSM). Pour plus d'informations, voir *IBM QRadar DSM Configuration Guide*.

## Présentation de la configuration de la source d'informations utilisateur et de la tâche de gestion

Pour intégrer initialement des sources d'informations utilisateur, vous devez effectuer les tâches suivantes :

1. Configurez un serveur Tivoli Directory Integrator. Voir «[Configuration du serveur Tivoli Directory Integrator](#)», à la page 198.
2. Créer et gérer des sources d'informations utilisateur. Voir «[Création et gestion de la source d'informations utilisateur](#)», à la page 200.
3. Collectez les informations utilisateur. Voir «[Collecte d'informations utilisateur](#)», à la page 202.

## Configuration du serveur Tivoli Directory Integrator

Pour que IBM QRadar s'intègre à des sources d'informations utilisateur, vous devez installer et configurer Tivoli Directory Integrator sur un hôte non-QRadar.

### Pourquoi et quand exécuter cette tâche

Aucune configuration n'est requise sur votre système QRadar ; cependant, vous devez accéder à la console pour obtenir le fichier QRadarIAM\_TDI.zip. Ensuite, installez et configurez un serveur Tivoli Directory Integrator sur un hôte distinct. Créez et importez un certificat autosigné.

Lorsque vous extrayez le fichier QRadarIAM\_TDI.zip sur le serveur Tivoli Directory Integrator, le répertoire TDI est automatiquement créé. Le répertoire TDI inclut les fichiers suivants :

- QRadarIAM.sh, qui est le script de démarrage TDI pour Linux
- QRadarIAM.bat, qui est le script de démarrage TDI pour Microsoft Windows
- QRadarIAM.xml, qui est le script XML TDI et doit être stocké au même emplacement que le fichier QRadarIAM.properties
- QRadarIAM.properties, qui est le fichier de propriétés du script xml TDI

Lorsque vous installez Tivoli Directory Integrator, vous devez configurer un nom pour le répertoire Solutions. Cette tâche vous demande d'accéder au répertoire Solutions. Par conséquent, dans la procédure de tâche, <solution\_directory> fait référence au nom que vous avez attribué au répertoire.

Les paramètres suivants sont utilisés pour créer et importer des certificats :

Paramètre	Description
<server_ip_address>	Définit le nom d'hôte du serveur Tivoli Directory Integrator.
<days_valid>	Définit le nombre de jours de validité du certificat.
<keystore_file>	Définit le nom du fichier de clés.
-storepass <password>	Définit le mot de passe du fichier de clés.
- keypass <password>	Définit le mot de passe de la paire de clés privées / publiques.
<alias>	Définit l'alias d'un certificat exporté.
<certificate_file>	Définit le nom de fichier du certificat.

### Procédure

1. Installez Tivoli Directory Integrator sur un hôte non QRadar. Pour plus d'informations sur l'installation et la configuration de Tivoli Directory Integrator, reportez-vous à la documentation Tivoli Directory Integrator (TDI).
2. À l'aide de SSH, connectez-vous à votre console IBM QRadar en tant que superutilisateur.
  - a) Nom d'utilisateur : racine
  - b) Mot de passe: <password>
3. Copiez le fichier QRadarIAM\_TDI.zip sur le serveur Tivoli Directory Integrator.
4. Sur le serveur Tivoli Directory Integrator, extrayez le fichier QRadarIAM\_TDI.zip dans le répertoire Solutions.
5. Configurez votre serveur Tivoli Directory Integrator pour qu'il s'intègre à QRadar.
  - a) Ouvrez le fichier <solution\_directory>/solution.properties de Tivoli Directory Integrator.

- b) Supprimez la mise en commentaire de la propriété `com.ibm.di.server.autoload`. Si cette propriété est déjà non commentée, notez la valeur de la propriété.
- c) Choisissez l'une des options suivantes :
- Accédez au répertoire `autoload.tdi`, qui contient la propriété `com.ibm.di.server.autoload` par défaut.
  - Créez un répertoire `autoload.tdi` dans `<solution_directory>` pour stocker la propriété `com.ibm.di.server.autoload`.
- d) Déplacez les fichiers `TDI/QRadarIAM.xml` et `TDI/QRadarIAM.property` du répertoire Tivoli Directory Integrator vers le répertoire `<solution_directory>/autoload.tdi` ou le répertoire que vous avez créé à l'étape précédente.
- e) Déplacez les scripts `QradarIAM.bat` et `QradarIAM.sh` du répertoire Tivoli Directory Integrator vers l'emplacement à partir duquel vous souhaitez démarrer Tivoli Directory Integrator.
6. Créez et importez le certificat auto-signé dans le fichier de clés certifiées Tivoli Directory Integrator.
- a) Pour générer un fichier de clés et une paire de clés privée / publique, entrez la commande suivante :
- `keytool -genkey -dname cn=<server_ip_address> -validity <days_valid> -keystore <keystore_file> -storepass <password> -keypass <password>`
  - Par exemple, `keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret`
- b) Pour exporter le certificat à partir du fichier de clés, entrez la commande suivante :
- `keytool -export -alias <alias> -file <certificate_file> -keystore <keystore_file> -storepass <password>`
  - Par exemple, `keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret`
- c) Pour importer le certificat principal dans le fichier de clés en tant que certificat d'autorité de certification auto-signé, entrez la commande suivante :
- `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>`
  - Par exemple, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
- d) Copiez le fichier de certificat dans le fichier `/opt/qradar/conf/trusted_certificates` sur QRadar Console.
7. Importez le certificat de l'autorité de certification dans le fichier de clés certifiées de Tivoli Directory Integrator.
- a) Pour importer le certificat de l'autorité de certification dans le fichier de clés en tant que certificat d'autorité de certification auto-signé, entrez la commande suivante :
- `keytool -import -trustcacerts -file <certificate_file> -keystore <keystore_file> -storepass <password> -alias <alias>`
  - Par exemple, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`
- b) Copiez le fichier de certificat de l'autorité de certification dans le fichier `/opt/qradar/conf/trusted_certificates` sur QRadar Console.
8. Éditez le fichier `<solution_directory>/solution.properties` pour annuler la mise en commentaire et configurer les propriétés suivantes:
- `javax.net.ssl.trustStore=<keystore_file>`
  - `{protect}-javax.net.ssl.trustStorePassword=<password>`
  - `javax.net.ssl.keyStore=<keystore_file>`
  - `{protect}-javax.net.ssl.keyStorePassword=<password>`

**Remarque :** Le mot de passe non modifié par défaut peut être affiché au format suivant : {encr}EyHbak. Entrez le mot de passe sous forme de texte en clair. Le mot de passe chiffre la première fois que vous démarrez Tivoli Directory Integrator.

9. Démarrez Tivoli Directory Integrator.

## Création et gestion de la source d'informations utilisateur

Utilisez l'utilitaire UISConfigUtil pour créer, extraire, mettre à jour ou supprimer des sources d'informations utilisateur.

### Création d'une source d'informations utilisateur

Utilisez l'utilitaire UISConfigUtil pour créer une source d'informations utilisateur.

#### Avant de commencer

Avant de créer une source d'informations utilisateur, vous devez installer et configurer votre serveur Tivoli Directory Integrator. Pour plus d'informations, voir [«Configuration du serveur Tivoli Directory Integrator»](#), à la page 198.

#### Pourquoi et quand exécuter cette tâche

Lorsque vous créez une source d'informations utilisateur, vous devez identifier les valeurs de propriété requises pour configurer la source d'informations utilisateur. Le tableau suivant décrit les valeurs de propriété prises en charge :

Propriété	Description
tdiserver	Définit le nom d'hôte du serveur Tivoli Directory Integrator.
tdiport	Définit le port d'écoute du connecteur HTTP sur le serveur Tivoli Directory Integrator.
Nom d'hôte	Définit le nom d'hôte de l'hôte source d'informations utilisateur.
port	Définit le port d'écoute du registre de gestion de l'identité et des accès sur l'hôte d'informations utilisateur.
username	Définit le nom d'utilisateur utilisé par IBM QRadar SIEM et pour s'authentifier auprès du registre de gestion de l'identité et des accès.
password	Définit le mot de passe requis pour l'authentification auprès du registre de gestion de l'identité et des accès.
base de recherche	Définit le nom distinctif de base. <b>Remarque :</b> Tous les utilisateurs référencés dans tous les groupes doivent être trouvés dans une recherche à partir de la base de recherche.
search filter	Définit le filtre de recherche requis pour filtrer les groupes extraits du registre de gestion de l'identité et des accès.

## Procédure

1. À l'aide de SSH, connectez-vous à votre console IBM QRadar en tant que superutilisateur.
  - a) Nom d'utilisateur : racine
  - b) Mot de passe : <password>
2. Pour ajouter une source d'informations utilisateur, entrez la commande suivante :  
UISConfigUtil.sh add <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=valeur1,prop2=valeur2... ,propn=valeurn]

Où :

- <name> Indique le nom de la source d'informations utilisateur à ajouter.
- <AD|ISAM|ISIM|ISFIM> indique le type de source d'informations utilisateur.
- [-d description ] est une description de la source d'informations utilisateur. Ce paramètre est facultatif.
- [-p prop1=value1,prop2=value2, . . . ,propn=valuen] identifie les valeurs de propriété requises pour la source d'informations utilisateur. Pour plus d'informations sur les paramètres pris en charge, voir «Création d'une source d'informations utilisateur», à la page 200.

Par exemple :

- ```
/UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p "tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080,hostname=vmibm7094.ottawa.ibm.com,port=389,username=cn=root,password=password,\"searchbase=ou=org,DC=COM\", \"searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem)(objectClass=erSystemUser))\"
```

## Extraction des sources d'informations utilisateur

Utilisez l'utilitaire UISConfigUtil pour extraire les sources d'informations utilisateur.

### Procédure

1. À l'aide de SSH, connectez-vous à votre console IBM QRadar en tant que superutilisateur.
  - a) Nom d'utilisateur : racine
  - b) Mot de passe : <password>
2. Choisissez l'une des options suivantes :
  - a) Entrez la commande suivante pour extraire toutes les sources d'informations utilisateur :  
UISConfigUtil.sh get <name>
  - b) Entrez la commande suivante pour extraire une source d'informations utilisateur spécifique :  
UISConfigUtil.sh get <name>

Où <name> est le nom de la source d'informations utilisateur que vous souhaitez extraire.

Par exemple :

```
[root@vmibm7089 bin]# .UISConfigUtil.sh get "UIS_AD"
```

## Édition d'une source d'informations utilisateur

Utilisez l'utilitaire UISConfigUtil pour éditer une source d'informations utilisateur.

### Procédure

1. À l'aide de SSH, connectez-vous à votre console IBM QRadar en tant que superutilisateur.
  - a) Nom d'utilisateur : racine
  - b) Mot de passe : <password>

2. Entrez la commande suivante pour éditer une source d'informations utilisateur :  
`UISConfigUtil.sh update <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2,...,propn=valuen]`

Où :

- <name> est le nom de la source d'informations utilisateur que vous souhaitez modifier.
- <AD|ISAM|ISIM|ISFIM> indique le type de source d'informations utilisateur. Pour mettre à jour ce paramètre, entrez une nouvelle valeur.
- [-d description ] est une description de la source d'informations utilisateur. Ce paramètre est facultatif. Pour mettre à jour ce paramètre, entrez une nouvelle description.
- [-p prop1=value1,prop2=value2,...,propn=valuen] identifie les valeurs de propriété requises pour la source d'informations utilisateur. Pour mettre à jour ce paramètre, entrez `Nouvelles propriétés`. Pour plus d'informations sur les paramètres pris en charge, voir [«Création d'une source d'informations utilisateur»](#), à la page 200.

Par exemple :

```
./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p "searchbase=DC=local"
```

## Suppression d'une source d'informations utilisateur

Utilisez l'utilitaire UISConfigUtil pour supprimer une source d'informations utilisateur.

### Procédure

1. À l'aide de SSH, connectez-vous à votre console IBM QRadar en tant que superutilisateur.
  - a) Nom d'utilisateur : `racine`
  - b) Mot de passe : `<password>`
2. Entrez la commande suivante pour supprimer une source d'informations utilisateur :

```
UISConfigUtil.sh delete <name>
```

Où <name> est le nom de la source d'informations utilisateur que vous souhaitez supprimer.

### Que faire ensuite

Les informations utilisateur recueillies sont stockées dans un ensemble de données de référence dans la base de données IBM QRadar. Si aucun ensemble de données de référence n'existe, un nouvel ensemble de données de référence est créé. Si une collecte de données de référence a été créée pour cette source d'informations utilisateur, la mappe de référence est purgée des données précédentes et les nouvelles informations utilisateur sont stockées. Pour plus d'informations sur les ensembles de données de référence, voir [Ensembles de données de référence](#).

## Collecte d'informations utilisateur

---

L'utilitaire GetUserInfo permet de collecter des informations utilisateur à partir des sources d'informations utilisateur et de stocker les données dans une collecte de données de référence.

### Pourquoi et quand exécuter cette tâche

Cette tâche permet de collecter des informations utilisateur sur demande. Si vous souhaitez créer une collecte automatique d'informations utilisateur sur un planning, créez une entrée de travail cron. Pour plus d'informations sur les travaux cron, reportez-vous à la documentation Linux.

### Procédure

1. À l'aide de SSH, connectez-vous à votre console IBM QRadar en tant que superutilisateur.



- a) Nom d'utilisateur : racine
  - b) <password>
2. Entrez la commande suivante pour collecter les informations utilisateur sur demande :
- ```
GetUserInfo.sh <UISName>
```

Où <UISName> est le nom de la source d'informations utilisateur à partir de qui vous voulez collecter des informations.

### **Que faire ensuite**

Les informations utilisateur collectées sont stockées dans une collection de données de référence sur la base de données. Si aucune collection de données de référence n'existe, une nouvelle collecte de données de référence est créée. Si une collecte de données de référence a été créée pour cette source d'informations utilisateur, la mappe de référence est purgée des données précédentes et les nouvelles informations utilisateur sont stockées. Pour plus d'informations sur les collections de données de référence, voir [«Collections de données de référence pour les informations utilisateur»](#), à la page 196.



---

## Chapitre 10. Intégration d'IBM X-Force

Les experts de sécurité IBM X-Force utilisent une série de centre de données internationaux pour collecter de dizaines de milliers d'échantillons de logiciel malveillant, analyser des pages Web et des URL, et exécuter des analyses pour classer des adresses IP et des URL potentiellement malveillantes. IBM X-Force Exchange est la plateforme de partage de ces données, qui peut être utilisée dans IBM QRadar.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Flux X-Force Threat Intelligence

Vous pouvez intégrer des données IBM X-Force Exchange dans IBM QRadar afin d'aider votre organisation à rester en avance sur les menaces émergentes en identifiant et en remédiant à une activité indésirable dans votre environnement avant qu'elle ne menace la stabilité de votre réseau.

Vous pouvez, par exemple, identifier et hiérarchiser ces types d'incident :

- Une série de tentatives de connexions pour une plage dynamique d'adresses IP
- Une connexion proxy anonyme à un portail de partenaire commercial
- Une connexion entre un point de terminaison interne et une commande de réseau de zombies connue
- Une communication entre un point de terminaison et un site de distribution de logiciels malveillants connu

**Remarque :** L'intégration IBM X-Force vous permet d'utiliser les données X-Force Threat Intelligence dans les règles de corrélation QRadar et les requêtes AQL. L'accès à l'API REST IBM X-Force Exchange n'est pas inclus.


## Activation du flux X-Force Threat Intelligence

Vous devez activer le flux X-Force Threat Intelligence pour pouvoir utiliser le contenu amélioré installé avec l'application IBM QRadar Security Threat Monitoring Content Extension.

### Pourquoi et quand exécuter cette tâche

QRadar télécharge environ 30 Mo de données de réputation IP par jour lorsque vous activez le flux X-Force Threat Intelligence.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Paramètres de système**.
3. Sélectionnez **Oui** dans la zone **Activer le flux X-Force Threat Intelligence**.

### Que faire ensuite

Déployez les modifications du paramètre système pour recevoir les données des serveurs X-Force. Pour plus d'informations, voir [Déploiement des modifications](#).

## Mise à jour des données X-Force dans un serveur proxy

IBM QRadar utilise une recherche par proxy inverse via un serveur Apache pour collecter des données directement à partir des serveurs IBM Security X-Force Threat Intelligence sur Internet.

## Pourquoi et quand exécuter cette tâche

Tous les dispositifs QRadar d'un déploiement contactant le serveur Apache pour envoyer des requêtes mises en cache. Une fois les données reçues par la console IBM QRadar, le résultat est mis en cache et rejoué pour tous les autres hôtes gérés qui font une demande de nouvelles données de réputation IP.

Si un proxy est configuré dans votre réseau, vous devez mettre à jour la configuration pour recevoir les données X-Force.

**Restriction :** L'authentification NTLM n'est pas prise en charge.

## Procédure

1. Utilisez SSH pour vous connecter à QRadar Console.
2. Ouvrez le fichier `/etc/httpd/conf.d/ssl.conf` dans un éditeur de texte.
3. Ajoutez les lignes suivantes avant `</VirtualHost>`:

```
ProxyRemote https://license.xforce-security.com/ http://PROXY_IP:PROXY_PORT
ProxyRemote https://update.xforce-security.com/ http://PROXY_IP:PROXY_PORT
```

4. Mettez à jour l'adresse IP et le port du serveur proxy d'entreprise pour permettre une connexion anonyme aux serveurs de sécurité X-Force.
5. Enregistrez les modifications dans le fichier `ssl.conf`.
6. Redémarrez le serveur Apache en entrant la commande suivante :

```
apachectl restart
```

Le redémarrage du serveur Apache sur le serveur QRadar Console consigne tous les utilisateurs et les hôtes gérés peuvent générer des messages d'erreur. Redémarrez le serveur Apache pendant les fenêtres de maintenance planifiées.

## Empêcher les données X-Force de télécharger des données localement

QRadar télécharge environ 30 Mo de données de réputation IP par jour. Pour empêcher QRadar de télécharger les données X-Force sur votre système local, désactivez le flux X-Force Threat Intelligence.


### Avant de commencer

Avant de désactiver le flux X-Force, vérifiez que les règles X-Force sont désactivées et que vous n'utilisez pas les fonctions X-Force dans les recherches sauvegardées.

## Pourquoi et quand exécuter cette tâche

Une fois que le flux X-Force Threat Intelligence est désactivé, le contenu X-Force est toujours visible dans QRadar, mais vous ne pouvez pas utiliser les règles X-Force ou ajouter des fonctions X-Force aux recherches d'AQL.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Paramètres de système**.
3. Sélectionnez **Non** dans la zone **Activer le flux X-Force Threat Intelligence**.

## Que faire ensuite

Déployez les modifications du paramètre système pour recevoir les données des serveurs X-Force. Pour plus d'informations, voir [Déploiement des modifications](#).

## Extension de contenu IBM QRadar Security Threat Monitoring

Le fichier Extension de contenu IBM QRadar Security Threat Monitoring sur IBM Security App Exchange (<https://exchange.xforce.ibmcloud.com/hub>) contient des règles, des blocs de construction et des propriétés personnalisées qui sont destinés à être utilisés avec les données de flux X-Force.

Les données X-Force incluent une liste des URL et des adresses IP potentiellement malveillantes avec un score de menace correspondant. Utilisez les règles X-Force pour marquer automatiquement les données d'activité réseau ou d'événement de sécurité qui impliquent les adresses et pour hiérarchiser les incidents avant de commencer à les examiner.

La liste suivante présente des exemples d'incident que vous pouvez identifier en utilisant les règles X-Force :

- **when the [source IP|destinationIP|anyIP] is part of any of the following [remote network locations]**
- **Lorsque [cette propriété hôte] est catégorisé par X-Force en tant que [Anonymization Servers|Botnet C&C|DynamicIPs|Malware|ScanningIPs|Spam] avec la valeur de confiance [égal à] [ce montant]**
- **when [this URL property] is categorized by X-Force as [Gambling|Auctions|Job Search|Alcohol|Social Networking|Dating]**

QRadar télécharge environ 30 Mo de données de réputation IP par jour lorsque vous activez le flux X-Force Threat Intelligence à utiliser avec Extension de contenu IBM QRadar Security Threat Monitoring.

## Installation de l'application IBM QRadar Security Threat Monitoring Content Extension

L'application IBM QRadar Security Threat Monitoring Content Extension contient du contenu IBM QRadar, tel que des règles, des blocs de construction et des propriétés personnalisées, conçus spécifiquement pour être utilisés avec les données X-Force. Le contenu amélioré peut vous aider à identifier et à corriger des activités indésirables dans votre environnement avant qu'il ne menace la stabilité de votre réseau.

### Avant de commencer

Téléchargez l'application IBM QRadar Security Threat Monitoring Content Extension à partir de [IBM Security App Exchange](https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:IBMContentPackageInternalThreat) (<https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:IBMContentPackageInternalThreat>).


### Pourquoi et quand exécuter cette tâche

Pour utiliser les données X-Force dans les règles, les infractions et les événements QRadar, vous devez configurer IBM QRadar pour charger automatiquement les données des serveurs X-Force vers votre dispositif QRadar.

Pour charger localement les données X-Force, activez le flux X-Force Threat Intelligence dans les paramètres système. Si de nouvelles informations sont disponibles lorsque X-Force démarre, la réputation d'adresse IP ou la base de données URL est mise à jour. Ces mises à jour sont fusionnées dans leurs propres bases de données et le contenu est répliqué de QRadar Console à tous les hôtes gérés du déploiement.

Les règles X-Force sont visibles dans le produit même si l'application est désinstallée ultérieurement.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des extensions**.
3. Téléchargez l'application sur la console QRadar en procédant comme suit :
  - a) Cliquez sur **Ajouter**.
  - b) Cliquez sur **Parcourir** pour rechercher l'extension.

- c) Cliquez sur **Installer immédiatement** pour installer l'extension sans afficher le contenu.
  - d) Cliquez sur **Ajouter**.
4. Pour afficher le contenu de l'extension, sélectionnez-le dans la liste des extensions et cliquez sur **Détails supplémentaires**.
5. Pour installer l'extension, procédez comme suit :
- a) Sélectionnez l'extension dans la liste et cliquez sur **Installation**.
  - b) Si l'extension n'inclut pas de signature numérique, ou si elle est signée mais que la signature n'est pas associée à l'autorité de certification IBM (CA), vous devez confirmer que vous souhaitez toujours l'installer. Cliquez sur **Installation** pour poursuivre l'installation.
  - c) Vérifiez les modifications apportées par l'installation au système.
  - d) Sélectionnez **Remplacer** ou **Conserver les données existantes** pour indiquer comment traiter les éléments de contenu existants.
  - e) Cliquez sur **Installer**.
  - f) Consultez le récapitulatif de l'installation et cliquez sur **OK**.
- Les règles apparaissent sous le groupe **Menaces** dans la fenêtre **Liste des règles**. Elles doivent être activées avant d'être utilisées.

## Que faire ensuite

Activez le flux X-Force Threat Intelligence pour pouvoir utiliser les règles X-Force ou ajouter des fonctions X-Force aux recherches d'AQL. Pour plus d'informations, voir [«Activation du flux X-Force Threat Intelligence»](#), à la page 205.

## IBM X-Force Exchange plug-in pour QRadar

---

IBM X-Force Exchange est une plateforme de partage du renseignement de menace utilisée par les analystes de sécurité, les spécialistes de la sécurité du réseau et les équipes du centre des opérations de sécurité.

Le plug-in (XFE) IBM X-Force Exchange fournit l'option de recherche des informations sur le site Web IBM X-Force Exchange pour les adresses IP, les URL, les CVE et les applications Web qui se trouvent dans QRadar.

Par exemple, vous pouvez cliquer avec le bouton droit de la souris sur une URL à partir d'un événement QRadar pour voir quelles données le X-Force Exchange contient à propos de l'URL.

Vous pouvez également utiliser l'option de recherche avec le bouton droit de la souris pour soumettre des adresses IP ou des données URL à partir de recherches QRadar, d'infractions et de règles à une collection publique ou privée. La collection stocke les informations en un seul endroit lorsque vous utilisez les données pour plus de recherche.

Les collections contiennent également une section qui sert de bloc-notes de style wiki, où vous pouvez ajouter des commentaires ou tout texte libre qui est pertinent. Vous pouvez utiliser la collection pour sauvegarder des rapports X-Force, des commentaires texte ou tout autre contenu. Un rapport X-Force contient à la fois une version du rapport à partir du moment où il a été enregistré et un lien vers la version en cours du rapport.

## Installation du plug-in IBM X-Force Exchange

Installez le plug-in IBM X-Force Exchange sur votre QRadar Console de sorte de disposer de la fonctionnalité de clic droit pour accéder aux données dans IBM X-Force Exchange.


### Avant de commencer

Cette procédure nécessite un redémarrage du serveur Web à partir de l'onglet **Admin** pour charger le plug-in une fois le fichier RPM installé. Le redémarrage du serveur Web consigne tous les utilisateurs QRadar. Il est donc conseillé d'installer ce plug-in lors de la maintenance planifiée.

## Pourquoi et quand exécuter cette tâche

Si votre système QRadar est la version 7.2.3 ou ultérieure, le plug-in est déjà installé. Les administrateurs peuvent vérifier que le plug-in est installé en cliquant avec le bouton droit de la souris sur n'importe quelle adresse IP dans QRadar et en sélectionnant **Autres options > Options du plug-in**. Si la recherche IBM X-Force Exchange s'affiche, le plug-in est installé.

## Procédure

1. Téléchargez le plug-in X-Force Exchange à l'aide du bouton droit de la souris à partir de [IBM Fix Central](https://ibm.biz/BdX4BW) (<https://ibm.biz/BdX4BW>).
  - a) Copiez le fichier RPM dans le fichier QRadar Console.
  - b) Entrez la commande suivante pour installer le plug-in : `Rpm -Uvh RightClick-XFE-7.2.<version>.x86_64.rpm`
2. Connectez-vous à QRadar Console en tant qu'administrateur.
3. Dans le menu de navigation ()<sup>1</sup>, cliquez sur **Admin**.
4. Sélectionnez **Avancé > Redémarrer le serveur Web**.

Une fois le serveur Web redémarré, le plug-in de clic droit X-Force est activé pour les adresses IP dans QRadar pour les zones URL de l'onglet **Activité de journal**.
5. Connectez-vous à la fenêtre en incrustation du site Web X-Force Exchange en utilisant votre IBMidou en tant qu'invité.

Les utilisateurs invités ne sont pas en mesure d'utiliser toutes les fonctions du site Web X-Force Exchange.
6. Fermez la fenêtre du navigateur après la connexion initiale au site Web IBM X-Force Exchange.





# Chapitre 11. Gestion des services autorisés

Vous pouvez configurer des services autorisés dans l'onglet **Admin** pour authentifier un appel d'API pour votre déploiement IBM QRadar.

L'API RESTful QRadar utilise des services autorisés pour authentifier les appels d'API vers QRadar Console. Vous pouvez ajouter ou révoquer un service autorisé à tout moment. Pour plus d'informations sur l'API RESTful, voir le *IBM QRadar API Guide*.

La fenêtre **Gérer les services autorisés** fournit les informations suivantes :

Tableau 46. Paramètres des services autorisés	
Paramètre	Description
Nom du service	Nom du service autorisé.
Autorisé par	Nom de l'utilisateur ou de l'administrateur qui a autorisé l'ajout du service.
Jeton d'authentification	Fonctions supprimées dans la version 7.4.3 Jeton associé à ce service autorisé.
Rôle utilisateur	Rôle utilisateur associé à ce service autorisé.
Profil de sécurité	Profil de sécurité associé à ce service autorisé.
Créé	Date à laquelle ce service autorisé a été créé.
Expiration	Date et heure d'expiration du service autorisé. Par défaut, le service autorisé est valide pendant 30 jours.


## Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Affichage des services autorisés

Fonctions supprimées dans la version 7.4.3 La fenêtre **des Services Autorisés** affiche la liste des services autorisés, à partir de laquelle vous pouvez copier le jeton du service.

### Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Services autorisés**.
3. Dans la fenêtre **Gérer les services autorisés**, sélectionnez le service autorisé approprié.

Le jeton s'affiche dans la zone **Jeton sélectionné** dans la barre supérieure. Vous pouvez copier le jeton dans votre logiciel fournisseur pour vous authentifier auprès de IBM QRadar.

## Ajout d'un service autorisé

Utilisez la fenêtre **Ajouter un service autorisé** pour ajouter un nouveau service autorisé.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Services autorisés**.

3. Cliquez sur **Add Authorized Service**.
4. Dans la zone **Nom du service**, indiquez un nom pour ce service autorisé. Ce nom peut contenir jusqu'à 225 caractères.
5. Dans la liste **Rôle utilisateur**, sélectionnez le rôle utilisateur à affecter à ce service autorisé. Les rôles utilisateur affectés à un service autorisé déterminent les fonctions accessibles à ce service sur l'interface utilisateur IBM QRadar.
6. Dans la liste **Profil de sécurité**, sélectionnez le profil de sécurité à affecter à ce service autorisé. Le profil de sécurité détermine les réseaux et les sources de journal auxquels peut accéder ce service dans l'interface utilisateur de QRadar.
7. Dans la liste **Date d'expiration**, entrez ou sélectionnez la date à laquelle ce service doit expirer. Si une date d'expiration n'est pas requise, sélectionnez **Pas d'expiration**.
8. Cliquez sur **Créer un service**.

Le message de confirmation contient une zone de jeton que vous devez copier dans votre logiciel fournisseur pour vous authentifier auprès de QRadar.


**Nouveautés de la version 7.4.3** Le jeton de service autorisé ne peut pas être rendu visible après la fermeture de la boîte de dialogue **Service autorisé créé avec succès**. Copiez le jeton dans un emplacement sécurisé avant de fermer la boîte de dialogue.

## Révocation des services autorisés

---

Utilisez la fenêtre **Ajouter un service autorisé** pour révoquer un service autorisé.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Services autorisés**.
3. Dans la fenêtre **Gérer les services autorisés**, sélectionnez le service que vous souhaitez révoquer.
4. Cliquez sur **Révocation de l'autorisation**.

---

## Chapitre 12. Sauvegarde et récupération

Vous pouvez sauvegarder et récupérer les informations de configuration et les données d'IBM QRadar.

Vous pouvez utiliser la fonction de sauvegarde et de reprise pour sauvegarder vos données d'événement et de flux. Vous devez toutefois les restaurer manuellement. Pour plus d'informations, voir [«Restauration des données de»](#), à la page 227.

Chaque hôte géré de votre déploiement, y compris QRadar Console, crée et stocke tous les fichiers de sauvegarde dans le répertoire `/store/backup/`. Votre système peut inclure un montage `/store/backup/` à partir d'un service SAN ou NAS externe. Les services externes fournissent une rétention des données hors ligne à long terme, ce qui est généralement requis pour les réglementations de conformité, telles que PCI.

Par défaut, QRadar crée une archive de sauvegarde de vos informations de configuration. Cette archive comporte des informations et/ou des données de configuration du jour précédent. La taille de votre sauvegarde dépend de la quantité de données d'événement de ce dernier.

Vous pouvez utiliser deux types de sauvegardes : les sauvegardes de configuration et les sauvegardes de données.

Les sauvegardes de configuration incluent les composants suivants :

- Configuration d'application
- Actifs
- Logos personnalisés
- Règles personnalisées
- Modules de support de périphérique (DSM)
- Catégories d'événement
- Sources de flux
- Recherches d'événement et de flux
- Groupes
- Informations de gestion d'index
- Informations clés sur la licence
- Sources de journal
- Infractions
- Éléments d'ensemble de références
- Plannings de stockage et de réacheminement
- Informations sur l'utilisateur et les rôles d'utilisateur
- Données de vulnérabilité (si IBM QRadar Vulnerability Manager est installé)

Les sauvegardes de données incluent les informations suivantes :

- Informations sur le journal d'audit
- Données d'événement
- Données de flux
- Données de rapport
- Index

La sauvegarde des données ne comprend pas les données d'application. Pour configurer et gérer les sauvegardes des données d'application, voir [«Sauvegarde et restauration de données d'application»](#), à la page 231.

## Concepts associés

Fonctions de votre produit IBM QRadar

## Tâches associées

Restauration des données de

# Sauvegarde des configurations et des données QRadar

Par défaut, IBM QRadar crée une archive de sauvegarde de vos informations de configuration tous les jours à minuit. Cette archive contient vos informations de configuration et/ou vos données du jour précédent. Vous pouvez personnaliser cette sauvegarde nocturne et créer une sauvegarde de configuration à la demande, le cas échéant.

## Planification de la sauvegarde nocturne

Utilisez la fenêtre **Configuration de la récupération de la sauvegarde** pour configurer un processus de sauvegarde planifié nocturne.

### Pourquoi et quand exécuter cette tâche

Par défaut, le processus de sauvegarde nocturne inclut uniquement vos fichiers de configuration. Vous pouvez personnaliser votre processus de sauvegarde nocturne pour inclure des données de votre console IBM QRadar et des hôtes gérés sélectionnés. Vous pouvez également personnaliser votre période de conservation de sauvegarde, l'emplacement de l'archive de sauvegarde, le délai d'une sauvegarde à traiter avant expiration et la priorité de sauvegarde par rapport à d'autres processus QRadar.

**Remarque :** La sauvegarde nocturne démarre à minuit dans le fuseau horaire où QRadar Console est installé. Si les mises à jour automatiques QRadar sont planifiées pour s'exécuter en même temps, les performances de QRadar peuvent être affectées.

La fenêtre Sauvegarde de la configuration de reprise fournit les paramètres suivants :

<i>Tableau 47. Paramètres de configuration de reprise de sauvegarde</i>	
<b>Paramètre</b>	<b>Description</b>
Configuration de la sauvegarde générale	

Tableau 47. Paramètres de configuration de reprise de sauvegarde (suite)

Paramètre	Description
Chemin de référentiel de sauvegarde	<p>Entrez l'emplacement où vous souhaitez stocker le fichier de sauvegarde. L'emplacement par défaut est /store/backup. Ce chemin doit exister avant le lancement du processus de sauvegarde. Si ce chemin n'existe pas, le processus de sauvegarde est abandonné.</p> <p>Si vous modifiez ce chemin, vérifiez que le nouveau chemin d'accès est valide sur chaque système de votre déploiement.</p> <p><b>Fonctions modifiées dans la version 7.4.3</b> Le répertoire doit correspondre à l'un des formats suivants :</p> <ul style="list-style-type: none"> <li>• /stocker/sauvegarder/*</li> <li>• /monter/ *</li> <li>• /mnt/*</li> <li>• /home/*</li> </ul> <p>Les données actives sont stockées dans le répertoire /store. Si vous disposez à la fois de données actives et d'archives de sauvegarde stockées dans le même répertoire, la capacité de stockage des données peut être facilement atteinte et vos sauvegardes planifiées risquent d'échouer. Nous vous recommandons de spécifier un emplacement de stockage sur un autre système ou de copier vos archives de sauvegarde vers un autre système une fois le processus de sauvegarde terminé. Vous pouvez utiliser une solution de stockage NFS (Network File System) dans votre déploiement QRadar. Pour plus d'informations sur l'utilisation de NFS, voir le <i>Offboard Storage Guide</i>.</p>
Durée de conservation de la sauvegarde (en jours)	<p>Entrez ou sélectionnez la durée, en jours, que vous souhaitez stocker les fichiers de sauvegarde. La valeur par défaut est de 7 jours.</p> <p>Cette période affecte uniquement les fichiers de sauvegarde générés à la suite d'un processus planifié. Les sauvegardes à la demande ou les fichiers de sauvegarde importés ne sont pas affectés par cette valeur.</p>
Planification de sauvegarde nocturne	Sélectionnez une option de sauvegarde.

Tableau 47. Paramètres de configuration de reprise de sauvegarde (suite)

Paramètre	Description
Sélectionner les hôtes gérés sur lesquels vous souhaitez exécuter des sauvegardes de données :	<p>Cette option s'affiche uniquement si vous sélectionnez l'option <b>Configuration et sauvegardes de données</b>.</p> <p>Tous les hôtes dans votre déploiement sont répertoriés. Le premier hôte de la liste est votre console ; il est activé pour la sauvegarde des données par défaut. Par conséquent, aucune case à cocher n'est affichée. Si vous avez géré des hôtes dans votre déploiement, les hôtes gérés sont répertoriés sous la console et chaque hôte géré inclut une case à cocher.</p> <p>Cochez la case des hôtes gérés sur qui vous souhaitez exécuter des sauvegardes de données.</p> <p>Pour chaque hôte (Console ou hôtes gérés), vous pouvez éventuellement effacer les éléments de données à exclure de l'archive de sauvegarde.</p>
Sauvegarde de configuration uniquement	
Limite de temps de la sauvegarde (en minutes)	Entrez ou sélectionnez la durée, en minutes, que vous souhaitez autoriser à exécuter la sauvegarde. La valeur par défaut est de 30 minutes. Si le processus de sauvegarde dépasse la limite de temps configurée, le processus de sauvegarde est automatiquement annulé.
Priorité de la sauvegarde	<p>Dans cette zone de liste, sélectionnez le niveau d'importance que vous souhaitez que le système place sur le processus de sauvegarde de configuration par rapport à d'autres processus.</p> <p>Une priorité moyenne ou élevée a un impact plus important sur la performance du système.</p>
Sauvegarde des données	
Limite de temps de la sauvegarde (en minutes)	Entrez ou sélectionnez la durée, en minutes, que vous souhaitez autoriser à exécuter la sauvegarde. La valeur par défaut est de 30 minutes. Si le processus de sauvegarde dépasse la limite de temps configurée, la sauvegarde est annulée automatiquement.
Priorité de la sauvegarde	<p>Dans la liste, sélectionnez le niveau d'importance que vous souhaitez que le système place sur le processus de sauvegarde des données par rapport à d'autres processus.</p> <p>Une priorité moyenne ou élevée a un impact plus important sur la performance du système.</p>

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.

2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Dans la barre d'outils, cliquez sur **Configurer**.
4. Dans la fenêtre **Configuration de la récupération de sauvegarde**, personnalisez votre sauvegarde nocturne.
5. Cliquez sur **Sauvegarder**.
6. Fermez la fenêtre **Archives de sauvegarde**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.


## Création d'une archive de sauvegarde de configuration à la demande

Si vous devez créer une sauvegarde de vos fichiers de configuration à un autre moment que la sauvegarde nocturne planifiée, vous pouvez créer une archive de sauvegarde à la demande. Les archives de sauvegarde à la demande contiennent uniquement des informations de configuration.

### Pourquoi et quand exécuter cette tâche

Vous lancez une archive de sauvegarde à la demande pendant une période où IBM QRadar a une charge de traitement faible, par exemple après les heures normales de bureau. Pendant le processus de sauvegarde, les performances du système sont affectées.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Dans la barre d'outils, cliquez sur **Sauvegarde à la demande**.
4. Entrez des valeurs pour les paramètres suivants :

Option	Description
<b>Nom</b>	Entrez un nom unique que vous souhaitez affecter à cette archive de sauvegarde. Le nom peut contenir jusqu'à 100 caractères alphanumériques. Le nom peut contenir les caractères suivants : trait de soulignement (_), tiret (-) ou point (.).
<b>Description</b>	Entrez une description pour cette archive de sauvegarde de configuration. La description peut contenir jusqu'à 255 caractères.

5. Cliquez sur **Exécuter la sauvegarde**.

Vous ne pouvez démarrer un nouveau processus de sauvegarde ou de restauration qu'une fois la sauvegarde à la demande terminée. Vous pouvez surveiller le processus d'archivage de sauvegarde dans la fenêtre **Archives de sauvegarde**.

## Création d'une notification par courrier électronique pour une sauvegarde ayant échoué

Pour recevoir une notification par courrier électronique concernant un incident de sauvegarde sur la console IBM QRadar ou sur un processeur d'événements QRadar, créez une règle basée sur le message de notification système.

### Avant de commencer

Vous devez configurer un serveur de messagerie pour distribuer les notifications système dans QRadar. Pour plus d'informations, voir [«Configuration de votre pare-feu local»](#), à la page 80.

## Pourquoi et quand exécuter cette tâche

Si une sauvegarde échoue, vous voyez l'une des notifications du système d'échec de sauvegarde suivantes :

- Sauvegarde : nécessite plus d'espace disque
- Sauvegarde : la dernière sauvegarde a dépassé le seuil d'exécution
- Sauvegarde : impossible d'exécuter la requête

## Procédure

1. Cliquez sur l'onglet **Infractions**.
2. Dans la sous-fenêtre **Infractions**, cliquez sur **Règles**.
3. Cliquez sur **Actions** > **Nouvelle règle d'événement**.
4. Dans **Assistant de règle**, cochez la case **Ignorer cette page lors de l'exécution de cet assistant de règles** et cliquez sur **Suivant**.
5. Dans la zone de filtre, entrez la requête de recherche suivante :

Lorsque l'événement QID est l'un des QID suivants

**En savoir plus. :**



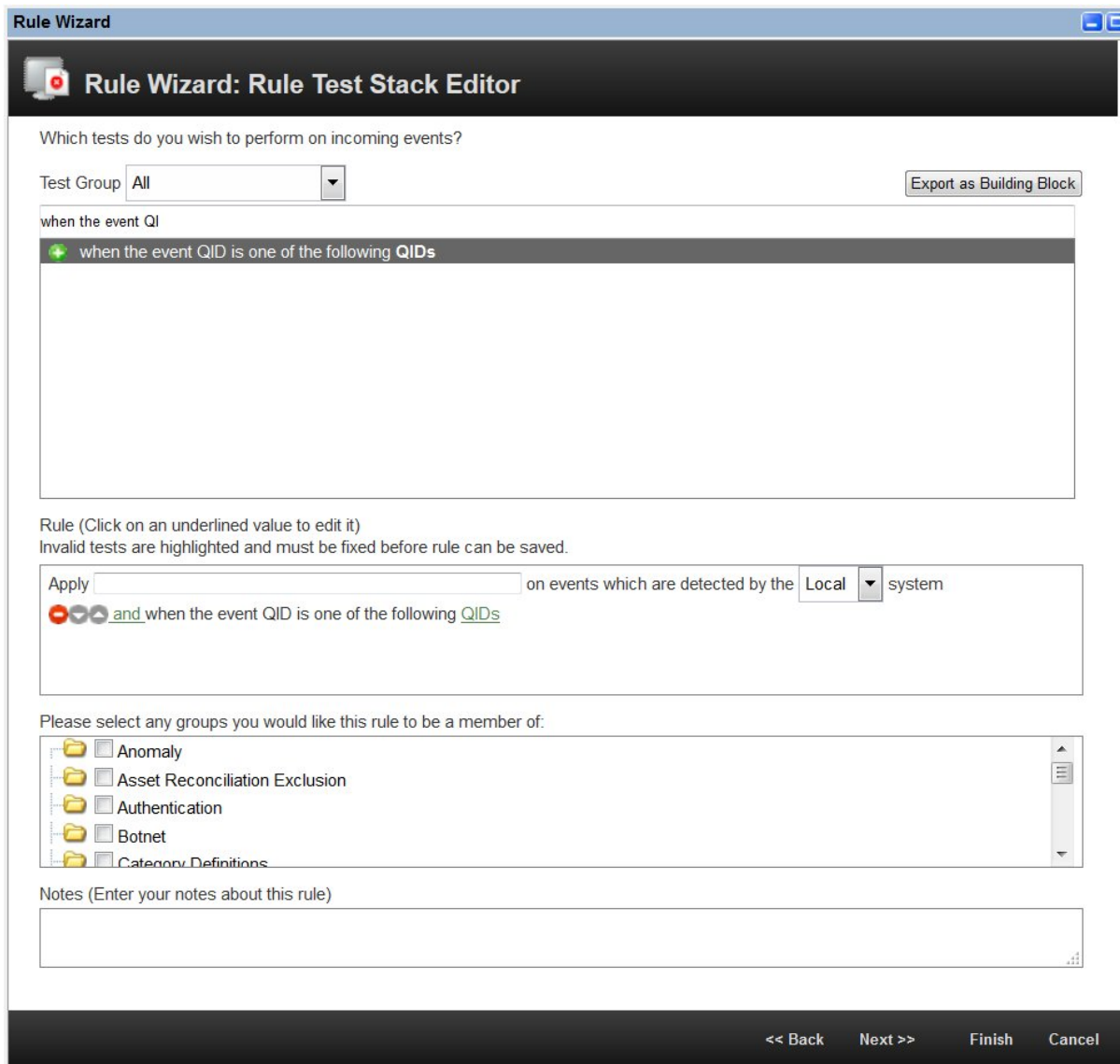


Figure 12. Test d'événement de l'assistant de règle

6. Cliquez sur l'icône Ajouter (+).
7. Dans la sous-fenêtre **Règle**, cliquez sur le lien **QID**.
8. Dans la zone **QID/Nom**, entrez Sauvegarde :
9. Sélectionnez les QID suivants et cliquez sur **Ajouter +** :
  - **La sauvegarde nécessite plus d'espace disque**
  - **Sauvegarde : la dernière sauvegarde a dépassé le seuil d'exécution**
  - **Sauvegarde impossible à exécuter sur demande**

**En savoir plus sur les QID :**

Browse or Search for QIDs below. Select the desired QIDs and click 'Add'

High-Level Category: Any

Low-Level Category: Any

Log Source Type: Any

QID/Name: Backup

Search

Matching QIDs

QID	Name ▲	Description	Sever
38750033	Backup requires more disk space	Backup: Not enou...	7
38750032	Backup unable to clean up bad backup	Backup: Unable to ...	6
38750031	Backup unable to clean up db	Backup: Unable to ...	6
38750035	Backup unable to execute request	Backup: Unable to ...	6
38750030	Backup unable to init recovery engine	Backup: Unable to ...	6
38750034	Backup unable to release running lock	Backup: Unable To...	3
38750059	Backup: last backup exceeded executio...	Backup: The last s...	6
38750036	File Location Incorrect	Backup: File Locat...	5

Add +

Selected Items

(38750033) Backup requires more disk space  
(38750035) Backup unable to execute request  
(38750059) Backup: last backup exceeded execution threshold

Remove -

Submit Cancel

Figure 13. QID de l'assistant de règles

10. Cliquez sur **Soumettre**.
11. Dans la sous-fenêtre **Règle**, entrez le nom suivant pour votre test de règle et cliquez sur **Suivant** :  
Échec de la sauvegarde
12. Dans la section **Réponse de règle**, cochez la case **Courrier électronique** et entrez les adresses électroniques à notifier.

## Gérer les archives de sauvegarde existantes

Utilisez l'icône **Sauvegarde et reprise** dans l'onglet **Admin** pour afficher et gérer toutes les archives de sauvegarde réussies.


### Importation d'une archive de sauvegarde

L'importation d'une archive de sauvegarde est utile si vous souhaitez restaurer une archive de sauvegarde qui a été créée sur un autre hôte IBM QRadar.

#### Pourquoi et quand exécuter cette tâche

Si vous placez un fichier d'archive de sauvegarde QRadar dans le répertoire /store/backupHost/inbound sur le serveur de la console, le fichier d'archive de sauvegarde est automatiquement importé.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Dans la zone **Télécharger l'archive**, cliquez sur **Parcourir**.
4. Localisez et sélectionnez le fichier archive que vous souhaitez télécharger. Le fichier archive doit inclure une extension `.tgz`.
5. Cliquez sur **Ouvrir**.
6. Cliquez sur **Télécharger**.


## Suppression d'une archive de sauvegarde

Pour supprimer un fichier d'archive de sauvegarde, le fichier d'archive de sauvegarde et le composant Contexte d'hôte doivent être situés sur le même système. Le système doit également être en communication avec la console IBM QRadar et aucune autre sauvegarde ne peut être en cours.

### Pourquoi et quand exécuter cette tâche

Si un fichier de sauvegarde est supprimé, il est supprimé du disque et de la base de données. De plus, l'entrée est supprimée de cette liste et un événement d'audit est généré pour indiquer le retrait.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Dans la section **Sauvegardes existantes**, sélectionnez l'archive que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.

## Restauration des données et des configurations QRadar

---

La restauration d'une archive de sauvegarde est utile si vous souhaitez restaurer des fichiers de configuration précédemment archivés, des données de violation et des données d'actif sur votre système IBM QRadar.

Avant de restaurer une archive de sauvegarde, notez les considérations suivantes :

- Vous ne pouvez restaurer qu'une archive de sauvegarde créée dans le cadre de la même édition de logiciels et de son niveau de mise à jour logicielle. Par exemple, si vous exécutez QRadar 7.4.3 p1, vérifiez que l'archive de sauvegarde est créée sur la Console QRadar 7.4.3 p1.
- Le processus de restauration restaure uniquement les informations de configuration, données d'infraction, et les données d'actif. Pour plus d'informations, voir [«Restauration des données de»](#), à la page 227.
- Si l'archive de sauvegarde provient d'un système de console NATed, vous ne pouvez restaurer que cette archive de sauvegarde sur un système NATed.
- Vous ne pouvez pas terminer une restauration de configuration sur une console dans laquelle l'adresse IP correspond à l'adresse IP d'un hôte géré dans la sauvegarde.

**Restriction :** Votre restauration peut échouer si vous prenez une configuration à partir d'un autre déploiement et exécutez l'utilitaire `qchange_netsetup` pour modifier l'adresse IP privée de la console. L'utilitaire `qchange_netsetup` modifie la configuration déployée, mais pas celle de la sauvegarde. Lorsque vous effectuez une restauration, la configuration de sauvegarde est lue et la restauration peut convertir des composants avec une adresse IP incorrecte.

Si possible, avant de restaurer une sauvegarde de configuration, exécutez une sauvegarde à la demande pour préserver l'environnement en cours. La description suivante est une vue de haut niveau du processus de restauration de configuration :

- Tomcat est arrêté
- Tous les processus système sont arrêtés.
- Tous les fichiers sont extraits de l'archive de sauvegarde et restaurés sur le disque.
- Les tableaux de base de données sont restaurés.
- Tous les processus système sont restaurés.
- Tomcat est redémarré.

#### Important :

- Si vous restaurez des données WinCollect, vous devez installer WinCollect SFS qui correspond à la version de WinCollect dans votre sauvegarde avant de restaurer la configuration. Pour plus d'informations, voir [«Les fichiers WinCollect ne sont pas restaurés lors d'une restauration de configuration.»](#), à la page 229
- Lorsque vous effectuez une restauration de déploiement croisée ou lorsque vous effectuez une restauration après une réinstallation d'usine, l'hôte géré qui est connecté à la console d'origine est automatiquement dirigé vers le nouveau déploiement restauré. Toutefois, toute modification avant la restauration concernant le déploiement (ajout ou suppression d'hôtes gérés) entraîne l'échec du processus de restauration.

Pour plus d'informations sur la sauvegarde ou la restauration d'une archive, voir les rubriques suivantes.

#### Tâches associées

[Restauration des données de](#)

## Restauration d'une archive de sauvegarde

Vous pouvez restaurer une archive de sauvegarde. La restauration d'une archive de sauvegarde est utile si vous avez un incident matériel système ou si vous souhaitez restaurer une archive de sauvegarde sur un dispositif de remplacement.

### Pourquoi et quand exécuter cette tâche

Vous ne pouvez redémarrer la console qu'une fois le processus de restauration terminé.

Le processus de restauration peut prendre plusieurs heures ; le temps de traitement dépend de la taille de l'archive de sauvegarde qui doit être restaurée. Une fois terminé, un message de confirmation s'affiche.

Une fenêtre fournit le statut du processus de restauration. Cette fenêtre fournit toutes les erreurs pour chaque hôte et les instructions de résolution des erreurs.


Les paramètres suivants sont disponibles dans la fenêtre **Restauration d'une sauvegarde** :

<i>Tableau 48. Paramètres <b>Restauration d'une sauvegarde</b></i>	
Paramètre	Description
<b>Nom</b>	Nom de l'archive de sauvegarde.
<b>Description</b>	Description, le cas échéant, de l'archive de sauvegarde.
<b>Type</b>	Type de sauvegarde. Seules les sauvegardes de configuration peuvent être restaurées. Par conséquent, ce paramètre affiche <b>config</b> .
<b>Sélectionner tous les éléments de configuration</b>	Lorsque cette option est sélectionnée, cette option indique que tous les éléments de configuration sont inclus dans la restauration de l'archive de sauvegarde.

Tableau 48. Paramètres **Restauration d'une sauvegarde** (suite)

Paramètre	Description
<b>Restaurer la configuration</b>	Répertorie les éléments de configuration à inclure dans la restauration de l'archive de sauvegarde. Pour supprimer des éléments, vous pouvez décocher les cases de chaque élément que vous souhaitez supprimer ou désélectionner la case à cocher <b>Sélectionner tous les éléments de configuration</b> .
<b>Sélectionner tous les éléments de données</b>	Lorsque cette option est sélectionnée, cette option indique que tous les éléments de données sont inclus dans la restauration de l'archive de sauvegarde.
<b>Restaurer les données</b>	Répertorie les éléments de configuration à inclure dans la restauration de l'archive de sauvegarde. Tous les éléments sont effacés par défaut. Pour restaurer des éléments de données, vous pouvez cocher les cases correspondant à chaque élément à restaurer.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Sélectionnez l'archive à restaurer.
4. Cliquez sur **Restaurer**.
5. Dans la fenêtre **Restaurer une sauvegarde**, configurez les paramètres.

Cochez la case **Configuration des règles personnalisées** pour restaurer les règles et les données de référence utilisées par les applications. Cochez la case **Configuration des utilisateurs** pour restaurer les jetons autorisés utilisés par les applications.

Le tableau suivant répertorie les configurations de restauration et les éléments inclus dans chacun d'entre eux :

**Remarque :** Le contenu inclus dans chaque configuration n'est pas limité au contenu répertorié.

Restaurer les paramètres de la configuration	Contenu inclus
<b>Configuration des règles personnalisées</b>	<ul style="list-style-type: none"> <li>• Règles</li> <li>• Ensembles de référence</li> <li>• Données de référence</li> <li>• Recherches sauvegardées</li> <li>• Destinations de réacheminement</li> <li>• Règles de routage</li> <li>• Propriétés personnalisées</li> <li>• Recherches d'historique</li> <li>• Règles d'historique</li> <li>• Configuration du compartiment de conservation</li> </ul>

Restaurer les paramètres de la configuration	Contenu inclus
<b>Configuration de déploiement</b>	<p>Tout le contenu.</p> <p>Si vous sélectionnez cette option, il est recommandé de sélectionner toutes les autres options de configuration.</p>
<b>Configuration des utilisateurs</b>	<ul style="list-style-type: none"> <li>• Utilisateurs</li> <li>• Rôles utilisateur</li> <li>• Profils de sécurité</li> <li>• Services autorisés</li> <li>• Tableaux de bord</li> <li>• Paramètres utilisateur</li> <li>• Recherches rapides de l'utilisateur</li> </ul>
<b>Licence</b>	<ul style="list-style-type: none"> <li>• Clés de licence</li> <li>• Allocations de pool de licences</li> <li>• Historique des licences</li> </ul>
<b>Modèles de rapport</b>	<p>Modèles de rapport</p> <p>Cela n'inclut pas le contenu du rapport généré.</p>
<b>Paramètres système</b>	<ul style="list-style-type: none"> <li>• Paramètres système</li> <li>• Configuration du profileur d'actif</li> </ul>
<b>Profils et résultats de l'analyse QVM</b>	<p>Profils d'analyse QVM et résultats</p>
<b>Configuration des applications installées</b>	<p>Configurations d'application</p> <p>Ceci n'inclut pas les données de l'application.</p> <p>Les applications en fonction des services autorisés peuvent ne pas fonctionner comme prévu si <b>Configuration des utilisateurs</b> n'est pas sélectionné.</p> <p>Lorsque <b>Configuration des applications installées</b> est sélectionné, <b>Groupe de configuration de déploiement</b> est sélectionné automatiquement.</p>
<b>Actifs</b>	<p>Modèle d'actif</p> <p>Lorsque <b>Actifs</b> est sélectionné, <b>Groupe de configuration de déploiement</b> est sélectionné automatiquement.</p>
<b>Infractions</b>	<ul style="list-style-type: none"> <li>• Données en infraction</li> <li>• Associations d'infraction (par exemple, liens QID, liens de règles ou liens d'actifs)</li> <li>• Recherches d'infractions</li> </ul> <p><b>Important :</b> Lorsque Infractions est sélectionné, le groupe Configuration</p>

Restaurer les paramètres de la configuration	Contenu inclus
	de déploiement est sélectionné automatiquement.

6. Cliquez sur **Restaurer**.
7. Cliquez sur **OK**.
8. Cliquez sur **OK**.
9. Choisissez l'une des options suivantes :
  - Si l'interface utilisateur a été fermée pendant le processus de restauration, ouvrez un navigateur Web et connectez-vous à IBM QRadar.
  - Si l'interface utilisateur n'a pas été fermée, la fenêtre de connexion s'affiche. Connectez-vous à QRadar.
10. Suivez les instructions de la fenêtre d'état.

## Que faire ensuite

Une fois que vous avez vérifié que vos données sont restaurées sur votre système, assurez-vous que les DSM, les scanners d'évaluation de la vulnérabilité (VA) et les protocoles de source de journal sont également restaurés.

Si l'archive de sauvegarde provient d'un cluster HA, vous devez cliquer sur **Déployer les modifications** pour restaurer la configuration de cluster à haute disponibilité une fois la restauration terminée. Si la réplication de disque est activée, l'hôte secondaire synchronise immédiatement les données une fois le système restauré. Si l'hôte secondaire a été supprimé du déploiement après une sauvegarde, l'hôte secondaire affiche un statut ayant échoué dans la fenêtre **Gestion des systèmes et des licences**.

## Restauration d'une archive de sauvegarde créée sur un autre système QRadar


Chaque archive de sauvegarde inclut les informations d'adresse IP du système où elle a été créée. Lorsque vous restorez une archive de sauvegarde à partir d'un système IBM QRadar différent, l'adresse IP de l'archive de sauvegarde et le système que vous restaurez ne correspondent pas. Vous pouvez corriger les adresses IP non concordantes.

### Pourquoi et quand exécuter cette tâche

Vous ne pouvez redémarrer la console qu'une fois le processus de restauration terminé. Le processus de restauration peut prendre plusieurs heures ; le temps de traitement dépend de la taille de l'archive de sauvegarde qui doit être restaurée. Une fois terminé, un message de confirmation s'affiche.

Une fenêtre fournit le statut du processus de restauration et fournit toutes les erreurs pour chaque hôte et les instructions de résolution des erreurs.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Sélectionnez l'ensemble des artefacts modifiés que vous souhaitez restaurer, puis cliquez sur **Restaurer**.
4. Dans la fenêtre **Restauration d'une sauvegarde**, configurez les paramètres suivants, puis cliquez sur **Restaurer**.

<i>Tableau 49. Paramètres <b>Restauration d'une sauvegarde</b></i>	
<b>Paramètre</b>	<b>Description</b>
<b>Sélectionner tous les éléments de configuration</b>	Indique que tous les éléments de configuration sont inclus dans la restauration de l'archive de sauvegarde. Cette case est cochée par défaut.
<b>Restaurer la configuration</b>	Répertorie les éléments de configuration à inclure dans la restauration de l'archive de sauvegarde. Toutes les colonnes sont sélectionnées par défaut.
<b>Sélectionner tous les éléments de données</b>	Indique que tous les éléments de données sont inclus dans la restauration de l'archive de sauvegarde. Cette case est cochée par défaut.
<b>Restaurer les données</b>	Répertorie les éléments de configuration à inclure dans la restauration de l'archive de sauvegarde. Tous les éléments sont effacés par défaut.

5. Arrêtez le service de table IP sur chaque hôte géré de votre déploiement. Les tables IP sont un pare-feu basé sur Linux.
  - a) Avec SSH, connectez-vous à l'hôte secondaire à haute disponibilité en tant que superutilisateur.
  - b) Pour l'hôte d'application, entrez les commandes suivantes :
 

```
systemctl stop docker_iptables_monitor.timer
```

```
systemctl stop iptables
```
  - c) Pour tous les autres hôtes gérés, entrez la commande suivante :
 

```
service iptables stop
```
  - d) Répétez l'opération pour tous les hôtes gérés dans votre déploiement.
6. Dans la fenêtre **Restauration d'une sauvegarde**, cliquez sur **Accès aux hôtes de test**.
7. Une fois les tests terminés pour tous les hôtes gérés, vérifiez que le statut de la colonne **Statut d'accès** indique un statut **OK**.
8. Si la colonne **Statut d'accès** indique le statut de **Aucun accès** pour un hôte, arrêtez à nouveau iptables, puis cliquez à nouveau sur **Test de l'accès aux hôtes** pour tenter une connexion.
9. Dans la fenêtre **Restaurer une sauvegarde**, configurez les paramètres.
 

**Important :** En sélectionnant la case à cocher **Configuration des applications installées**, vous restaurez uniquement les configurations de l'application d'installation. Les configurations d'extension ne sont pas restaurées. Cochez la case **Configuration de déploiement** si vous souhaitez restaurer les configurations d'extension.
10. Cliquez sur **Restaurer**.
11. Cliquez sur **OK**.
12. Cliquez sur **OK** pour vous connecter.
13. Choisissez l'une des options suivantes :
  - Si l'interface utilisateur a été fermée pendant le processus de restauration de l'utilisateur, ouvrez un navigateur Web et connectez-vous à QRadar.
  - Si l'interface n'a pas été fermée, la fenêtre de connexion s'affiche. Connectez-vous à QRadar.
14. Affichez les résultats du processus de restauration et suivez les instructions pour résoudre les éventuelles erreurs.
15. Actualisez la fenêtre de votre navigateur Web.
16. Sous l'onglet **Admin**, sélectionnez **Avancé > Déployer la configuration entière**.



QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

17. Pour activer les tables IP d'un hôte d'application, entrez la commande suivante :

```
systemctl start docker_iptables_monitor.timer
```

## Que faire ensuite

Une fois que vous avez vérifié que vos données sont restaurées sur votre système, vous devez réappliquer les RPM pour tous les DSM, les scanners d'évaluation de vulnérabilité (VA) ou les protocoles de source de journal.

Si l'archive de sauvegarde provient d'un cluster HA, vous devez cliquer sur **Déployer les modifications** pour restaurer la configuration de cluster à haute disponibilité une fois la restauration terminée. Si la réplication de disque est activée, l'hôte secondaire synchronise immédiatement les données une fois le système restauré. Si l'hôte secondaire a été supprimé du déploiement après une sauvegarde, l'hôte secondaire affiche un statut ayant échoué dans la fenêtre **Gestion des systèmes et des licences**.

## Restauration des données de

Vous pouvez restaurer les données sur votre console IBM QRadar et les hôtes gérés à partir des fichiers de sauvegarde. La partie de données des fichiers de sauvegarde inclut des informations telles que les informations d'adresse IP source et de destination, les données d'actif, les informations sur les catégories d'événements, les données de vulnérabilité, données de flux, et les données d'événement.

Chaque hôte géré de votre déploiement, y compris QRadar Console, crée tous les fichiers de sauvegarde dans le répertoire `/store/backup/`. Votre système peut inclure un montage `/store/backup` à partir d'un service SAN ou NAS externe. Les services externes fournissent une rétention des données hors ligne à long terme, ce qui est généralement requis pour les réglementations de conformité, telles que PCI.

## Avant de commencer

**Restriction :** Si vous restez des données sur un nouveau QRadar Console, la sauvegarde de configuration doit être restaurée avant de restaurer la sauvegarde de données.

Assurez-vous que les conditions suivantes sont remplies :

- Vous connaissez l'emplacement de l'hôte géré sur lequel les données sont sauvegardées.
- Si votre déploiement inclut un point de montage distinct pour ce volume, le répertoire `/store` ou `/store/ariel` dispose d'un espace suffisant pour les données que vous souhaitez récupérer.
- Vous connaissez la date et l'heure des données que vous souhaitez récupérer.
- Si votre configuration a été modifiée, avant de restaurer la sauvegarde de données, vous devez restaurer la sauvegarde de configuration.

## Procédure

1. Utilisez SSH pour la connexion à IBM QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire `/store/backup`.
3. Pour répertorier les fichiers de sauvegarde, entrez la commande suivante :

```
ls -l
```

4. Si des fichiers de sauvegarde sont répertoriés, accédez au répertoire racine en entrant la commande suivante :

```
cd /
```

**Important :** Les fichiers restaurés doivent se trouver dans le répertoire `/store`. Si vous entrez `cd` au lieu de `cd /`, les fichiers sont restaurés dans le répertoire `/root/store`.

5. Pour extraire les fichiers de sauvegarde dans leur répertoire d'origine, entrez la commande suivante :

```
tar -zxpvPf /store/backup/backup.name.hostname_hostID .target date.backup
type.timestamp.tgz
```

Variable de nom de fichier	Description
<i>name</i>	Nom de la sauvegarde.
<i>hostname_hostID</i>	Nom du système QRadar qui héberge le fichier de sauvegarde suivi de l'identificateur du système QRadar.
<i>date cible</i>	Date à laquelle le fichier de sauvegarde a été créé. Le format de la date cible est <i>jour_mois_année</i> .
<i>type de sauvegarde</i>	Les options sont données ou config.
<i>Horodatage</i>	Heure de création du fichier de sauvegarde.

## Résultats

La sauvegarde quotidienne des données capture toutes les données sur chaque hôte. Si vous souhaitez restaurer des données sur un hôte géré qui ne contient que des données d'événement ou de flux, seules les données sont restaurées sur cet hôte. Si vous souhaitez conserver les données restaurées, augmentez les paramètres de conservation des données afin d'éviter que les routines de maintenance du disque de nuit ne suppriment vos données restaurées.

### Concepts associés

Sauvegarde et récupération

Vous pouvez sauvegarder et récupérer les informations de configuration et les données d'IBM QRadar.

Restauration des données et des configurations QRadar

La restauration d'une archive de sauvegarde est utile si vous souhaitez restaurer des fichiers de configuration précédemment archivés, des données de violation et des données d'actif sur votre système IBM QRadar.

## Vérification des données restaurées

Vérifiez que vos données sont restaurées correctement dans IBM QRadar.

### Procédure

1. Pour vérifier que les fichiers sont restaurés, consultez le contenu de l'un des répertoires restaurés en entrant la commande suivante :

```
cd /store/ariel/flows/payloads/<yyyy/mm/dd>
```

```
cd /store/ariel/events/payloads/<yyyy/mm/dd>
```

Vous pouvez afficher les répertoires restaurés créés pour chaque heure de la journée. Si des répertoires sont manquants, les données risquent de ne pas être capturées pour cette période.

2. Vérifiez que les données restaurées sont disponibles.

a) Connectez-vous à l'interface QRadar.

b) Cliquez sur l'onglet **Activité de journal** Ou **Activité réseau**.

c) Sélectionnez **Éditer la recherche** dans la liste **Rechercher** de la barre d'outils.

d) Dans la sous-fenêtre **Intervalle de temps** de la fenêtre **Rechercher**, sélectionnez **Intervalle spécifique**.

e) Sélectionnez la plage horaire des données que vous avez restaurées, puis cliquez sur **Filtrer**.

f) Affichez les résultats pour vérifier les données restaurées.

- g) Si les données restaurées ne sont pas disponibles dans l'interface QRadar, vérifiez que les données sont restaurées dans le bon emplacement et que les droits d'accès aux fichiers sont correctement configurés.

Les fichiers restaurés doivent se trouver dans le fichier `/store` directory. Si vous avez entré `cd` au lieu de `cd /` lorsque vous avez extrait les fichiers restaurés, vérifiez le répertoire `/root/store` pour les fichiers restaurés. Si vous n'avez pas modifié les répertoires avant d'extraire les fichiers restaurés, vérifiez le répertoire `/store/backup/store` des fichiers restaurés.

En général, les fichiers sont restaurés avec les droits d'origine. Toutefois, si les fichiers ne sont pas détenus par le compte superutilisateur, des problèmes peuvent se produire. La propriété correcte des répertoires et des fichiers dans `/store/ariel/events/payloads` et `/store/ariel/flows/payloads` est `root:root`. Si les fichiers et les dossiers n'ont pas la propriété correcte, modifiez la propriété à l'aide de la commande **chown**.

Les droits d'accès corrects des répertoires et des fichiers dans `/store/ariel/events/payloads` et `/store/ariel/flows/payloads` sont 755 pour les dossiers et 644 pour les fichiers. Si les fichiers et les dossiers ne disposent pas des droits appropriés, modifiez les droits d'accès à l'aide de la commande **chmod**.

## Que faire ensuite

Une fois que vous avez vérifié que vos données sont restaurées, vous devez effectuer une mise à jour automatique dans QRadar. La mise à jour automatique garantit que les DSM, les scanners d'évaluation de la vulnérabilité (VA) et les protocoles de source de journal sont à la dernière version. Pour plus d'informations, voir [c\\_tuning\\_guide\\_deploy\\_dsmupdates.dita](#).

## Extraction des fichiers de sauvegarde manquants sur le disque

Lorsque les fichiers de sauvegarde sont manquants sur le disque, l'entrée de la table de sauvegarde correspondante sur la page **sauvegarde et reprise** est marquée par une icône d'exclamation pour indiquer que le fichier n'est pas récupérable. Les fichiers manquants ne peuvent pas être téléchargés ou restaurés. Ce problème peut se produire lorsque vous utilisez un stockage externe qui n'est plus disponible ou est hors ligne.

### Procédure

1. Dans l'onglet **Admin**, cliquez sur **Sauvegarde et reprise**.
2. Si le stockage externe est hors ligne ou n'est plus disponible, supprimez l'entrée de table en utilisant l'option **Supprimer** en haut de la page **Sauvegarde et reprise**.  
**Remarque** : Si vous ne vous attendez pas à ce comportement et que vous utilisez le stockage externe pour votre emplacement d'archivage de sauvegarde, examinez si le système de stockage est toujours accessible. S'il est hors ligne et que vous pouvez restaurer le répertoire, les icônes de l'indicateur sont automatiquement mises à jour et supprimées lorsque le système détecte les fichiers restaurables.
3. Sur la page **Sauvegarde et reprise**, cliquez sur **Configurer** et prenez note de **Chemin du référentiel de sauvegarde**.
4. Déconnectez-vous de QRadar et reconnectez-vous pour vous assurer que les fichiers sont à nouveau accessibles en réparant le montage externe ou en restaurant les fichiers manquants vers l'emplacement de sauvegarde approprié.
5. Actualisez la page **Sauvegarde et reprise** pour synchroniser les sauvegardes.

## Les fichiers WinCollect ne sont pas restaurés lors d'une restauration de configuration.

Lorsque vous effectuez une restauration de configuration et que certains fichiers WinCollect ne sont pas restaurés, cela peut être dû au fait que l'ISO d'installation contient une version précédente de WinCollect.

L'ISO QRadar contient une version intégrée de WinCollect. Lorsque vous restai à l'aide de cette ISO, elle déploie les fichiers WinCollect qui sont stockés dans cette ISO, plutôt que les fichiers de votre sauvegarde.

Pour remédier à cette situation, vous devez installer WinCollect SFS qui correspond à la version de WinCollect dans votre sauvegarde avant de restaurer la configuration. Effectuez les tâches suivantes dans l'ordre suivant :

1. Effectuez une sauvegarde QRadar.
2. Apportez un nouveau matériel en ligne et déployez l'ISO.
3. Installez WinCollect SFS qui correspond à la version de WinCollect dans votre sauvegarde sur la console.
4. Restaurez la sauvegarde de la configuration.

Les fichiers WinCollect appropriés sont déployés avec la restauration de configuration.

## Applications de sauvegarde et de restauration

---

IBM QRadar permet de sauvegarder et de restaurer des configurations d'application distinctes des données d'application.

Les configurations d'application sont sauvegardées dans le cadre de la sauvegarde de la configuration nocturne. La sauvegarde de configuration inclut des applications installées sur QRadar Console et sur un hôte d'application. Vous pouvez restaurer la configuration des applications en sélectionnant l'option **Configuration des applications installées** lorsque vous restaurez une sauvegarde.

Les données d'application sont sauvegardées séparément de la configuration d'application à l'aide d'un script facile à utiliser qui s'exécute tous les soirs. Vous pouvez également utiliser le script pour restaurer les données de l'application et configurer les temps de sauvegarde et les périodes de conservation des données pour les données d'application.

### Concepts associés

#### Hôtes d'application

Un hôte d'application est un hôte géré dédié à l'exécution d'applications. Les hôtes d'applications fournissent des ressources d'unité centrale, de mémoire et stockage supplémentaires pour vos applications sans que cela n'ait de conséquence sur la capacité de traitement de votre console QRadar Console. Les applications, telles User Behavior Analytics with Machine Learning Analytics, exigent plus de ressources que celles actuellement disponibles sur la console.

## Sauvegarde et restauration d'applications

Utilisez la fenêtre **Sauvegarde et reprise** de l'onglet IBM QRadar **Admin** pour sauvegarder et restaurer des applications.

### Pourquoi et quand exécuter cette tâche


Vous pouvez sauvegarder vos applications en créant une sauvegarde de configuration. Pour plus d'informations sur la sauvegarde de vos applications, voir «Sauvegarde des configurations et des données QRadar», à la page 214. Une sauvegarde de configuration ne sauvegarde pas les données de votre application. Pour plus d'informations sur la sauvegarde des données de votre application, voir «Sauvegarde et restauration de données d'application», à la page 231.

Si un hôte d'application est connecté à votre QRadar Console, la configuration de l'hôte d'application est sauvegardée dans le cadre de la configuration de déploiement de la console. Vous ne pouvez pas restaurer un hôte d'application sur un QRadar Console avec une adresse IP différente de celle initialement configurée avec l'hôte d'application.

Par défaut, les applications sont restaurées sur la console, sauf si un hôte d'application est présent. Si QRadar ne peut pas restaurer des applications sur votre hôte d'application, il tente de les restaurer dans le fichier QRadar Console. Le nombre d'applications d'hôtes d'applications qui peuvent être restaurés sur

la console est limité par la quantité de mémoire disponible sur QRadar Console. Les applications définies comme **node\_only** dans leur fichier manifeste d'application ne peuvent pas être restaurées dans QRadar Console.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système** , cliquez sur **Sauvegarde et reprise**.
3. Sélectionnez une sauvegarde existante dans la fenêtre **Sauvegarde et reprise** et cliquez sur **Restaurer**.
4. Vérifiez que la case **Configuration des applications installées** est cochée et cliquez sur **Restaurer**.

**Remarque :** Sélectionnez la case à cocher **Configuration des applications installées** pour restaurer uniquement les configurations des applications installées. Les configurations d'extension ne sont pas restaurées. Sélectionnez la case à cocher **Configuration du déploiement** pour restaurer les configurations d'extension.

## Sauvegarde et restauration de données d'application

Utilisez le script `app-volume-backup.py` pour sauvegarder et récupérer les données d'application.

### Pourquoi et quand exécuter cette tâche

Une sauvegarde de configuration que vous effectuez dans la fenêtre **Sauvegarde et reprise** ne sauvegarde pas les données de vos applications. Le script `/opt/qradar/bin/app-volume-backup.py` s'exécute la nuit à 2h30 et sauvegarde le volume monté `/store` de chaque application installée. Par défaut, les données sont conservées pendant 7 jours.

Utilisez le script pour effectuer les tâches suivantes :

- Sauvegardez les données manuellement pour les applications installées.
- Répertoriez toutes les sauvegardes de données d'application installées sur le système.
- Restaurez les données des applications installées.
- Exécutez le processus de conservation et définissez la durée de conservation des sauvegardes.

Ce script se trouve à la fois sur l'hôte QRadar Console et sur l'hôte d'application si celui-ci est installé. Le script sauvegarde les données d'application uniquement si les applications se trouvent sur l'hôte en cours.

## Procédure

1. Utilisez SSH pour vous connecter à votre console ou à votre hôte d'application en tant qu'utilisateur `root`.
2. Accédez au répertoire `/opt/qradar/bin/`.
  - Utilisez la commande suivante pour sauvegarder les données d'application :

```
./app-volume-backup.py backup
```

Le script `app-volume-backup.py` exécute la nuit à 2h30 heure locale pour sauvegarder toutes les applications installées. Les archives de sauvegarde sont stockées dans le dossier `/store/apps/backup`. Vous pouvez modifier l'emplacement des archives de sauvegarde en modifiant la variable `APP_VOLUME_BACKUP_DIR` dans `/store/configservices/staging/globalconfig/nva.conf`. Vous devez déployer les modifications après avoir modifié cette variable.

- Pour afficher toutes les sauvegardes de données pour les applications installées, entrez la commande suivante :
- ```
./app-volume-backup.py ls
```

Cette commande génère toutes les archives de sauvegarde stockées dans le dossier des archives de sauvegarde.

- Pour restaurer une archive de sauvegarde, entrez la commande suivante :

```
./app-volume-backup.py restore -i <backup_name>
```

Utilisez la commande **ls** pour rechercher le nom d'une archive de sauvegarde.

- Par défaut, toutes les archives de sauvegarde sont conservées pendant une semaine. Le processus de conservation s'exécute la nuit à 2h30 heure locale avec la sauvegarde.

– Pour effectuer la conservation manuellement et utiliser la période de conservation par défaut, entrez la commande suivante :

```
./app-volume-backup.py retention
```

- Vous pouvez également définir manuellement la durée de conservation en ajoutant **-t** (durée par défaut à 1) et **-p** (durée par défaut à 0).

Le commutateur **-p** accepte trois valeurs : 0 pour une semaine, 1 pour un jour et 2 pour une heure.

Par exemple, pour définir la durée de conservation d'un retour à 3 semaines, entrez la commande suivante :

```
./app-volume-backup.py retention -t 3 -p 0
```

- Si vous souhaitez modifier la durée de conservation utilisée par le temporisateur nocturne, ajoutez des indicateurs à la commande de conservation trouvée dans le fichier de service systemd suivant.

```
/usr/lib/systemd/system/app-data-backup.service
```

Par exemple, pour modifier la période de conservation utilisée par le processus de conservation nocturne à 5 jours, recherchez la ligne suivante :

```
ExecStart=/opt/qradar/bin/app-volume-backup.py retention
```

Remplacez-la par :

```
ExecStart=/opt/qradar/bin/app-volume-backup.py retention -t 5 -p 1
```

Enregistrez vos modifications et exécutez la commande `systemctl daemon-reload` pour que le système applique les modifications.

3. Utilisez la commande suivante pour redémarrer chaque conteneur d'applications :

```
docker restart <container_id>
```

Si vous ne connaissez pas l'ID du conteneur, utilisez les commandes suivantes pour le rechercher :

```
psql -U qradar -c 'select id, name from installed_application'
```

La commande renvoie l'ID application. Insérez l'ID d'application dans la commande suivante pour rechercher l'ID conteneur :

```
docker ps -a --format "{{.ID}},{{.Image}}" | grep 'qapp/<app_id>:' | cut -d , -f1
```

## Redondance des données et reprise dans les déploiements QRadar

Pour éviter la perte de données, configurez vos déploiements de manière à inclure la redondance des données et la fonctionnalité de reprise. La synchronisation des données est possible lorsque vous avez deux systèmes QRadar identiques dans des environnements géographiques distincts qui sont un miroir l'un de l'autre, et que les données sont synchronisées sur les deux sites. Les données de transfert utilisent le *réacheminement hors site*, qui est configuré sur les déploiements principal et secondaire. Vous pouvez configurer la synchronisation des données avec des déploiements se trouvant dans des emplacements géographiques différents.

### **Application de synchronisation de données**

Implémentez l'application Data Synchronization pour sauvegarder vos données et configurations IBM QRadar en mettant en miroir vos données vers un autre système QRadar identique. La récupération à partir d'une perte de données est possible lorsque vous avez deux systèmes QRadar identiques dans des environnements géographiques distincts qui sont un miroir l'un de l'autre, et que des données sont collectées sur les deux sites. Pour en savoir plus sur l'application Data Synchronization, voir [Redondance et reprise pour les déploiements QRadar](#).

Si vous ne respectez pas les exigences de l'application Data Synchronization, vous pouvez trouver d'autres solutions. La récupération à partir de la perte de données est possible lorsque vous réachemiez des données en direct, par exemple, des flux et des événements à partir d'un système QRadar principal, vers un système parallèle sur un autre site.

### **QRadar Console principal et console de sauvegarde**

Une solution de panne matérielle, où la console de sauvegarde est une copie du serveur principal, avec la même configuration mais reste hors tension. Une seule console est opérationnelle à la fois. Si la console principale échoue, vous mettez manuellement l'alimentation sur la console de sauvegarde, appliquez la sauvegarde de configuration principale et utilisez l'adresse IP de la console principale. Une fois que vous avez restauré le serveur principal et avant de l'activer, vous désactivez manuellement le serveur de sauvegarde. Si le système est arrêté pendant une longue période, appliquez la sauvegarde de configuration de la console de sauvegarde au serveur principal.

### **Événement et transfert de flux**

Les événements et les flux sont transmis d'un site principal à un site secondaire. Des architectures identiques sont requises dans deux centres de données distincts.

### **Distribution des mêmes événements et flux vers les sites principaux et secondaires**

Distribuez les mêmes données d'événement et de flux à deux sites en direct à l'aide d'un équilibreur de charge ou d'une autre méthode pour livrer les mêmes données aux dispositifs en miroir. Chaque site possède un enregistrement des données de journal envoyées.

## **QRadar Console Principal et sauvegarde QRadar Console**

Lorsque le QRadar Console principal échoue et que vous souhaitez que la sauvegarde QRadar Console prenne en compte le rôle principal, vous devez activer manuellement la console de sauvegarde, appliquer la sauvegarde de configuration et l'adresse IP à partir de la console principale. Utilisez une méthode de commutation similaire pour d'autres dispositifs tels qu'un QRadar QFlow Collector ou un Collecteur d'événements, où chaque dispositif est doté d'une sauvegarde ou d'une sauvegarde à froid qui est un dispositif identique.

La console de sauvegarde prend en compte le rôle principal QRadar Console à partir du moment de l'activation et ne stocke pas les événements, le flux ou les violations passés à partir du fichier QRadar Consoleprincipal d'origine. Utilisez ce type de déploiement pour vos dispositifs, pour minimiser les temps d'arrêt, en cas d'incident matériel.

- Une console de sauvegarde nécessite sa propre clé de licence dédiée (correspondant aux valeurs EPS et FPM de la console principale).
- La console de sauvegarde utilise une clé d'activation de dispositif standard.
- La configuration de licence de la console de sauvegarde doit correspondre aux valeurs du fichier QRadar Consoleprincipal ; cela inclut les valeurs EPS et FPS du fichier QRadar Consoleprincipal.

**Exemple :** Si le processeur d'événements QRadar principal a été concédé sous licence pour 15K EPS, la console de sauvegarde redondante doit également être sous licence pour 15K EPS.

- Il existe des composants spéciaux de mise à niveau de reprise en ligne qui doivent être achetés pour la console de sauvegarde.
- D'un point de vue technique, la licence des consoles principale et de sauvegarde est identique, mais pour des raisons de conformité, la console de sauvegarde (et la licence associée) ne peut pas traiter les données en direct à moins qu'un incident n'ait eu lieu avec le QRadar Consoleprincipal.
- Les données collectées par la console de sauvegarde devront être copiées sur la console principale lorsque la console principale sera à nouveau fonctionnelle.

En cas d'échec de la commande principale, procédez comme suit pour configurer la console de sauvegarde en tant que QRadar Console principal :

1. Mettez la console de secours sous tension.
2. Ajoutez l'adresse IP de la console principale.
3. Restaurez les données de sauvegarde de configuration de la console principale vers la console de sauvegarde.

La console de sauvegarde fonctionne comme console principale jusqu'à ce que la console principale soit ramenée en ligne. Vérifiez que les deux serveurs ne sont pas en ligne en même temps.

## Configuration de l'adresse IP sur la console de sauvegarde

Lorsque le QRadar Console principal échoue, vous configurez la console secondaire de sauvegarde pour qu'elle prenne en compte le rôle de la console principale. Ajoutez l'adresse IP du QRadar Console ayant échoué à la console de sauvegarde de sorte que votre système QRadar continue de fonctionner.

### Avant de commencer

Mettez la console de secours sous tension.

### Procédure

1. Utilisez SSH pour vous connecter en tant qu'utilisateur root.
2. Pour configurer l'adresse IP sur la console de sauvegarde, procédez comme suit :

- a) Entrez la commande suivante :

```
qchange_netsetup
```

**Remarque :** Vérifiez que le stockage externe qui n'est pas /store/ariel ou /store n'est pas monté.

- b) Suivez les instructions de l'assistant pour entrer les paramètres de configuration.

Une fois les modifications demandées traitées, le système QRadar s'arrête et redémarre automatiquement.

## Sauvegarde et récupération

Sauvegardez vos données et vos informations de configuration IBM QRadar pour vous permettre de récupérer d'une panne système ou d'une perte de données.

Utilisez la sauvegarde et la récupération intégrées à QRadar pour sauvegarder vos données. Cependant, vous devez restaurer les données manuellement. Par défaut, QRadar crée une archive de sauvegarde quotidienne de vos informations de configuration à minuit. L'archive de sauvegarde inclut des informations de configuration, des données générées ou les deux à partir de la veille.

Vous pouvez créer les types de sauvegarde suivants :

- Les sauvegardes de configuration, qui incluent des données de configuration système, par exemple, des ressources et des sources de journal dans votre déploiement QRadar .
- Les sauvegardes de données, qui incluent des informations générées par un déploiement QRadar de travail tel que des informations de journal ou des dates d'événements.

Pour plus d'informations sur la sauvegarde et la récupération de vos données, voir le *IBM QRadar Administration Guide*.

## Événement et transfert de flux d'un centre de données principal vers un autre centre de données

Pour vous assurer qu'il existe un magasin de données redondant pour les événements, les flux, les violations et qu'il existe une architecture identique dans deux centres de données distincts, les données d'événement et de flux vers l'avant du site 1 vers le site 2.



Les renseignements suivants ne sont fournis qu'à titre d'orientation générale et ne sont pas conçus ni prévus pour servir de guide.

Ce scénario dépend du site 1 restant actif. Si le site 1 échoue, les données ne sont pas transmises au site 2, mais les données sont à jour jusqu'au moment de l'échec. En cas d'échec sur le site 1, vous implémentez la récupération de vos données, en modifiant manuellement les adresses IP et en utilisant une sauvegarde et une restauration pour basculer du site 1 vers le site 2, et passer au site 2 pour tous les hôtes QRadar.

La liste suivante décrit la configuration de l'acheminement des événements et des flux du site principal vers le site secondaire :

- Il existe une architecture répartie identique dans deux centres de données distincts, qui comprend un centre de données principal et un centre de données secondaire.
- Le QRadar Console principal est actif et collecte tous les événements et flux à partir de sources de journal et génère des infractions corrélées.
- Vous configurez des cibles hors site sur le QRadar Console principal pour permettre la transmission des données d'événement et de flux depuis le centre de données principal vers les processeurs d'événements et de flux dans un autre centre de données.

**Raccourci :** Utilisez des règles de routage plutôt que des cibles hors site car la configuration est plus facile.

- De temps à autre, utilisez l'outil de gestion de contenu pour mettre à jour le contenu du fichier QRadar Console principal vers le QRadar Console secondaire.

Pour plus d'informations sur les destinations de transfert et les règles de routage, voir le *IBM QRadar Administration Guide*.

Dans le cas d'un incident sur le site 1, vous pouvez utiliser un déploiement à haute disponibilité (HA) pour déclencher une reprise en ligne automatique sur le site 2. L'hôte secondaire à haute disponibilité sur le site 2 prend en compte le rôle de l'hôte primaire de haute disponibilité sur le site 1. Le site 2 continue de collecter, stocker et traiter des données d'événements et de flux. Les hôtes HA secondaires qui sont à l'état de secours n'ont pas de services en cours d'exécution, mais les données sont synchronisées si la réplication de disque est activée. Pour plus d'informations sur la planification des déploiements à haute disponibilité, voir [Planification du déploiement à haute disponibilité](#).

**Remarque :** Vous pouvez utiliser un équilibreur de charge pour diviser les événements et séparer les flux tels que NetFlow, J-Flow et sFlow, mais vous ne pouvez pas utiliser un équilibreur de charge pour diviser les flux QFlows. Utilisez des technologies externes telles qu'un robinet régénératif pour diviser QFlow et envoyer au site de sauvegarde.

Le diagramme suivant montre comment le site 2 est utilisé comme magasin de données redondant pour le site 1. Les données sur les événements et les débits sont transmises du site 1 au site 2.

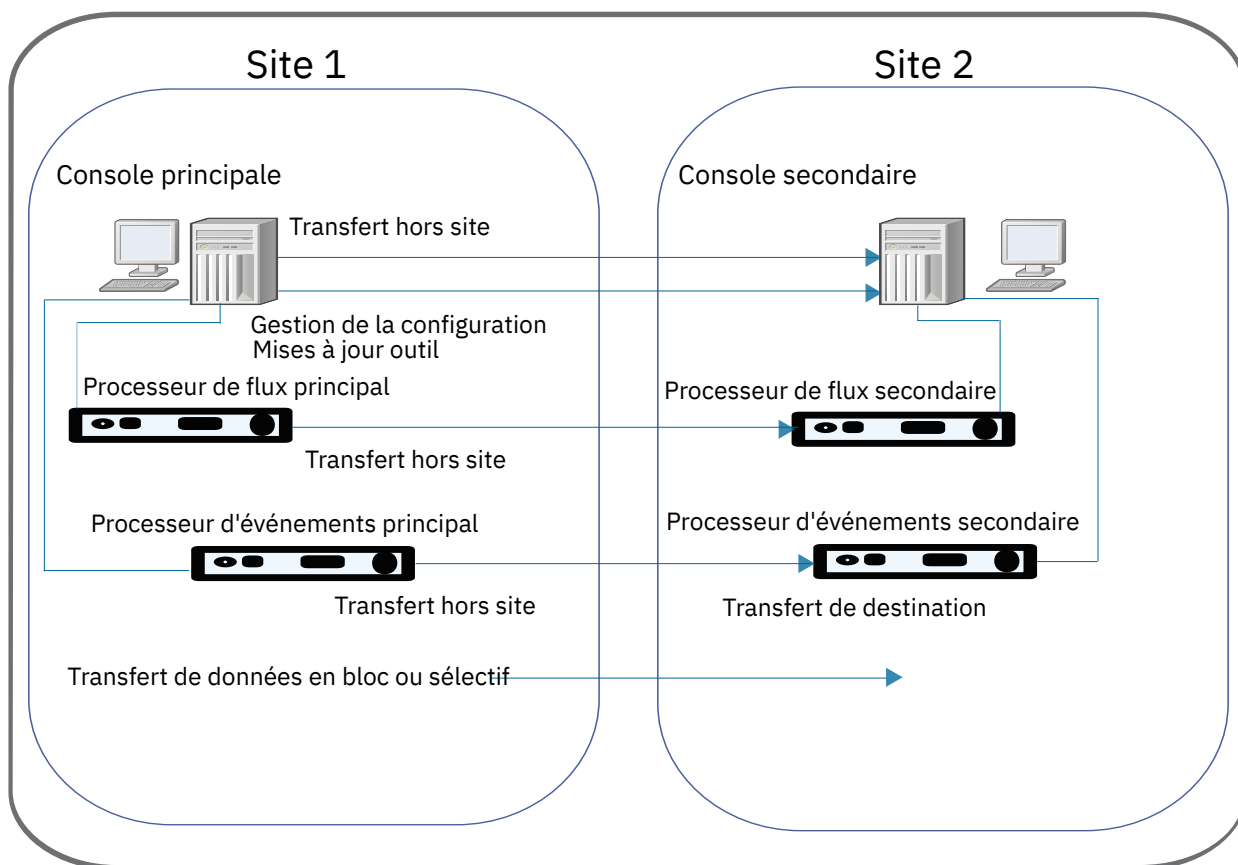


Figure 14. Événement et acheminement du flux du site 1 vers le site 2 pour la reprise après incident

## Configuration de l'acheminement des événements et des flux

Pour la redondance des données, configurez les systèmes IBM QRadar pour transférer des données d'un site vers un site de sauvegarde.

Le système cible qui reçoit les données de QRadar est appelé *destination de réacheminement*. Les systèmes QRadar assurent que toutes les données transmises ne sont pas modifiées. Les versions plus récentes des systèmes QRadar peuvent recevoir des données des versions antérieures des systèmes QRadar. Cependant, les versions antérieures ne peuvent pas recevoir de données des versions ultérieures. Pour éviter les problèmes de compatibilité, mettez à niveau tous les récepteurs avant de mettre à niveau les systèmes QRadar qui envoient des données. Pour configurer la transmission, procédez comme suit :

1. Configurez une ou plusieurs destinations de transfert.

Une destination de transfert est le système cible qui reçoit les données d'événement et de flux à partir de la console principale IBM QRadar. Vous devez ajouter des destinations de transfert avant de pouvoir configurer le transfert de données en bloc ou sélectif. Pour plus d'informations sur les destinations de transfert, voir le *IBM QRadar Administration Guide*.

2. Configurez les règles de routage, les règles personnalisées ou les deux.

Une fois que vous avez ajouté une ou plusieurs destinations de transfert pour vos données d'événement et de flux, vous pouvez créer des règles de routage basées sur des filtres pour transmettre de grandes quantités de données. Pour plus d'informations sur les règles de routage, voir le *IBM QRadar Administration Guide*.

3. Configurez les exportations de données, les importations et les mises à jour.

Utilisez l'outil de gestion de contenu pour déplacer des données de votre QRadar Console principal vers la console secondaire QRadar. Exportez la sécurité et le contenu de configuration de IBM QRadar

en un format externe et portable. Pour plus d'informations sur l'utilisation de l'outil de gestion de contenu pour transférer des données, voir le *IBM QRadar Administration Guide*.

## Équilibrage de charge des événements et des flux entre deux sites

Lorsque vous exécutez deux déploiements IBM QRadar en direct sur un site principal et secondaire, vous envoyez des données d'événement et de flux aux deux sites. Chaque site possède un enregistrement des données de journal envoyées. Utilisez l'outil de gestion de contenu pour synchroniser les données entre les déploiements

Le diagramme suivant montre deux sites en direct, où les données de chaque site sont répliquées sur l'autre site.

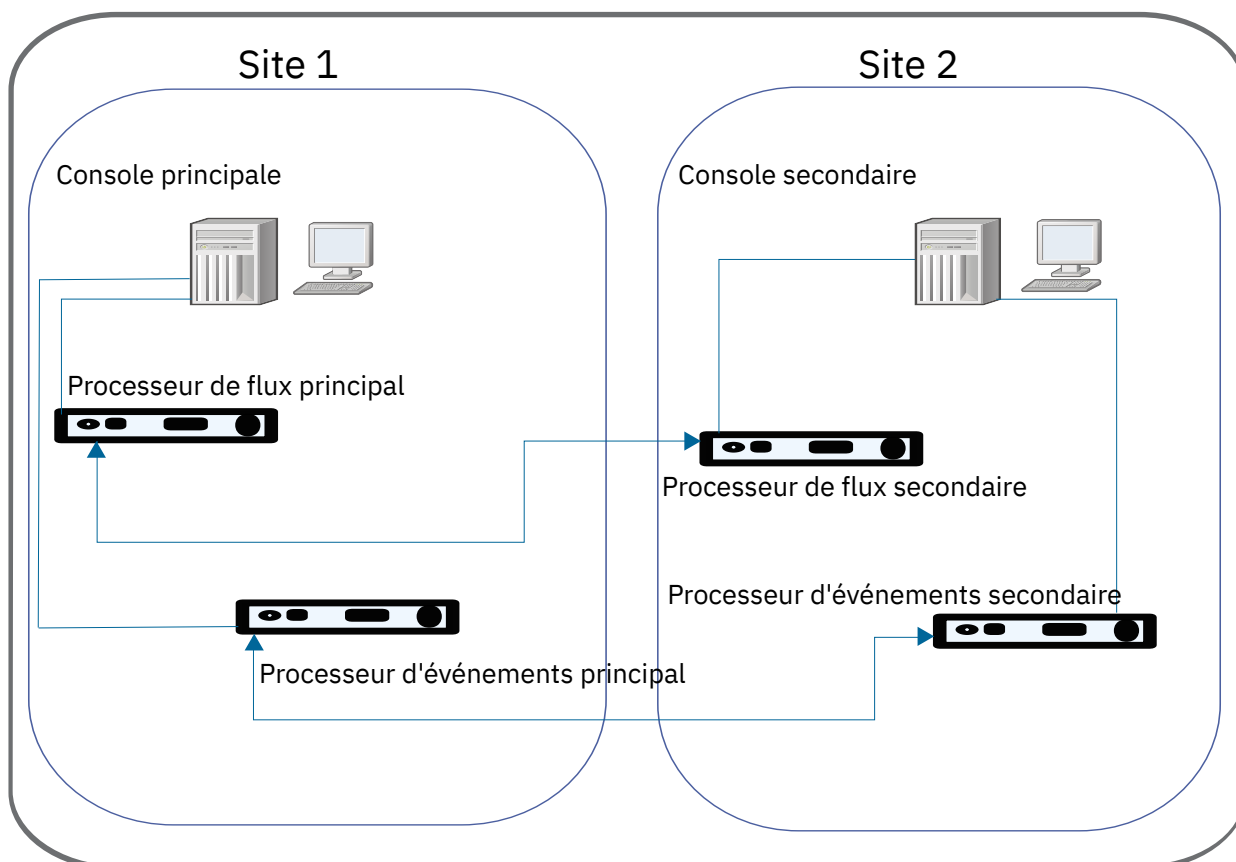


Figure 15. Équilibrage de charge des événements et des flux entre deux sites

### Concepts associés

«Redondance des données d'événement et de flux», à la page 238

Envoyez les mêmes événements et flux dans des centres de données ou des sites séparés géographiquement et activez la redondance des données à l'aide d'un équilibreur de charge ou d'une autre méthode pour transmettre les mêmes données aux dispositifs en miroir.


## Restauration des données de configuration depuis le serveur principal vers le système QRadar Console secondaire

Une fois que vous avez configuré le QRadar Console secondaire comme destination des journaux, vous ajoutez ou importez une archive de sauvegarde à partir du fichier QRadar Console principale. Vous pouvez restaurer une archive de sauvegarde créée sur un autre hôte QRadar. Connectez-vous au QRadar Console secondaire et effectuez une restauration complète de l'archive de sauvegarde de la console principale sur le QRadar Console secondaire.

## Avant de commencer

Vous devez disposer d'une sauvegarde de données à partir de votre console principale pour effectuer cette tâche.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans le menu de navigation, cliquez sur **Configuration système**.
3. Cliquez sur l'icône **Sauvegarde et reprise**.
4. Dans la zone **Télécharger l'archive**, cliquez sur **Parcourir**.
5. Localisez et sélectionnez le fichier archive que vous souhaitez télécharger.

**Conseil :** Si le fichier d'archive de sauvegarde QRadar se trouve dans le répertoire `/store/backupHost/inbound` sur le serveur de console, le fichier d'archive de sauvegarde est automatiquement importé.

Le fichier archive doit avoir une extension `.tgz`.

6. Cliquez sur **Ouvrir**.
7. Cliquez sur **Télécharger**.
8. Sélectionnez l'archive que vous avez téléchargée et cliquez sur **Restaurer**.

Lorsque la restauration est terminée, le QRadar Console secondaire devient la console principale.

## Redondance des données d'événement et de flux

Envoyez les mêmes événements et flux dans des centres de données ou des sites séparés géographiquement et activez la redondance des données à l'aide d'un équilibreur de charge ou d'une autre méthode pour transmettre les mêmes données aux dispositifs en miroir.

Configurez la distribution des sources de journal et de flux pour la redondance des données :

- Envoyez les données de la source de journal à processeur d'événements sur le second site.
- Envoyer des données de source de flux à processeur de flux sur le second site.

Pour plus d'informations sur la configuration des sources de journal, voir le *IBM QRadar Log Sources - Guide de configuration*.

Pour plus d'informations sur les sources de flux, voir *IBM QRadar Administration Guide*.

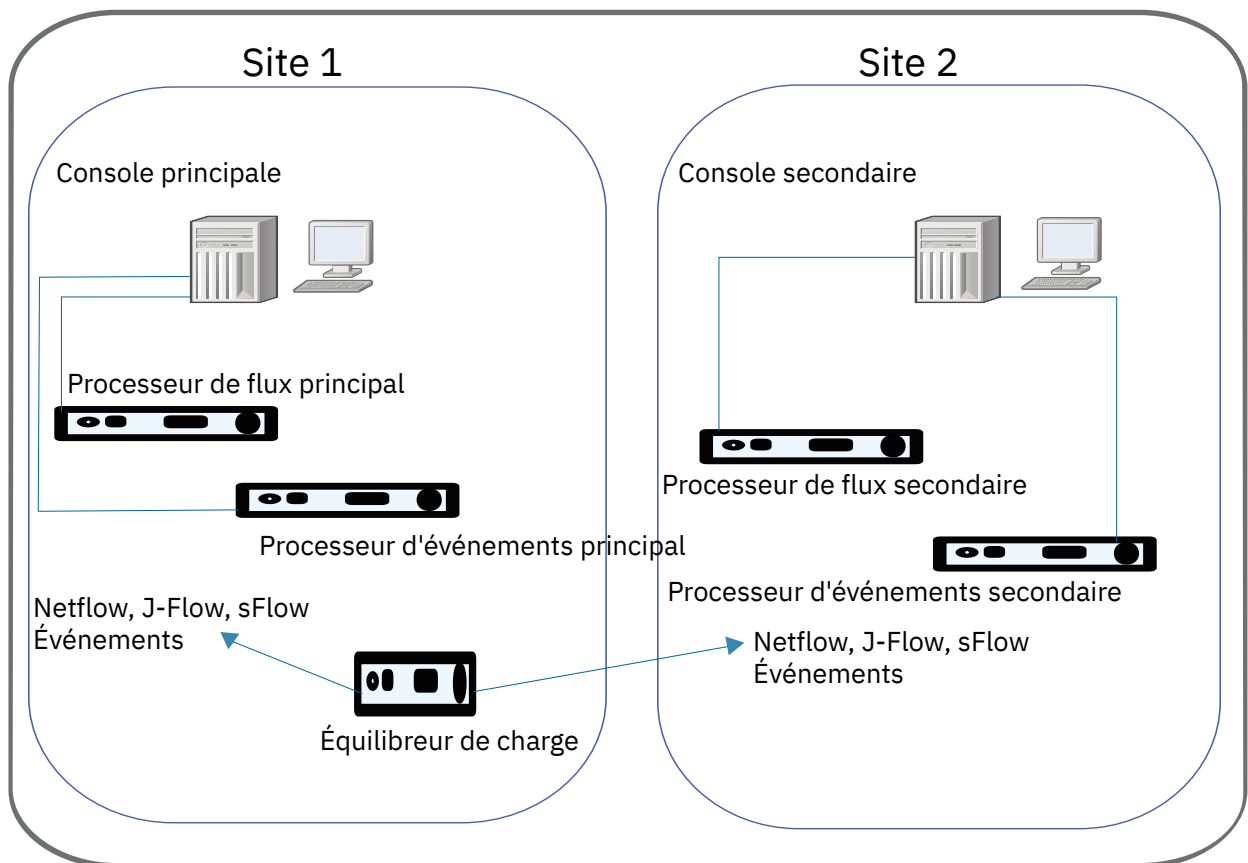


Figure 16. Envoi d'événements et de flux à deux sites

### Configuration de QRadar pour la réception d'événements

QRadar reconnaît automatiquement de nombreuses sources de journal qui envoient des messages syslog dans votre déploiement. Les sources de journal qui sont automatiquement reconnues par QRadar apparaissent dans la fenêtre **Sources de journal**.

Vous configurez la reconnaissance automatique des sources de journal pour chaque Collecteur d'événements à l'aide du paramètre **Autodetection Enabled** dans la configuration Collecteur d'événements. Si vous souhaitez conserver la synchronisation des ID d'événement source du journal avec le Collecteur d'événements primaire, vous désactivez le paramètre **Autodetection**. Dans ce cas, utilisez l'outil de gestion de contenu pour synchroniser la configuration de la source de journal ou restaurer une sauvegarde de configuration sur le site.

Pour plus d'informations sur les sources de journal reconnues automatiquement et les configurations spécifiques à votre unité ou dispositif, voir *IBM QRadar DSM Configuration Guide* et *IBM QRadar Log Sources - Guide de configuration*.

### Configuration de QRadar pour la réception des flux

Pour activer la redondance des données pour les flux, vous devez envoyer NetFlow, J-Flow et sFlow aux deux sites pour la collection QFlow.

Vous pouvez collecter des flux à partir d'un SPAN ou d'un robinet, puis envoyer des paquets à votre emplacement de sauvegarde, ou vous rétroviser du SPAN ou du robinet à l'emplacement de sauvegarde à l'aide de technologies externes. Un équilibreur de charge divise les flux tels que NetFlow, J-Flow et sFlow, mais il ne peut pas séparer QFlow.

Pour plus d'informations sur les sources de flux, voir *IBM QRadar Administration Guide*.

### Utilisation de l'outil de gestion de contenu (CMT)

Si vous souhaitez vous assurer que le QRadar Console principal du site 1 et le QRadar Console secondaire du site 2 ont des configurations identiques, utilisez l'outil de gestion de contenu pour mettre à jour le site 2 avec les configurations du site 1.

Pour plus d'informations sur l'utilisation de l'outil de gestion de contenu, voir le *IBM QRadar Administration Guide*.

## Sauvegarde et restauration de QRadar Analyst Workflow

---

Si vous devez restaurer QRadar Analyst Workflow sur une autre console QRadar, vous devez réinstaller QRadar Analyst Workflow après la restauration QRadar.

QRadar Analyst Workflow se trouve dans <https://exchange.xforce.ibmcloud.com/hub>, qui est lié à Fix Central, où vous pouvez télécharger le fichier `QRadarAnalystWorkflow<x.x.x>.zip`.

La fonction de sauvegarde et de reprise QRadar sauvegarde et restaure toutes les données pour QRadar Analyst Workflow, et peut être restaurée sur un hôte différent. Toutefois, si vous restaurez sur un hôte différent, les images de docker QRadar Analyst Workflow ne sont pas incluses dans la reprise.

Une fois que vous avez restauré QRadar, vous devez copier le fichier `QRadarAnalystWorkflow<x.x.x>.zip` sur le nouvel hôte, décompressez le fichier et installez sur le nouvel hôte.

Pour obtenir des instructions sur l'installation du fichier `QRadarAnalystWorkflow<x.x.x>.zip`, voir [Installation de QRadar Analyst Workflow \(https://www.ibm.com/support/knowledgecenter/SS42VS\\_latest/com.ibm.qradar.doc/t\\_installing\\_launching\\_new\\_ui.html\)](https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/t_installing_launching_new_ui.html).

---

## Chapitre 13. Sources de flux

Pour les dispositifs IBM QRadar, QRadar ajoute automatiquement les sources de flux par défaut pour les ports physiques sur le dispositif et inclut une source de flux NetFlow par défaut.

Si QRadar est installé sur votre propre matériel, QRadar tente de détecter et d'ajouter automatiquement des sources de flux par défaut pour toutes les unités physiques, telles qu'une carte d'interface réseau (NIC). Lorsque vous affectez un IBM QRadar QFlow Collector, QRadar inclut une source de flux NetFlow par défaut.

---

### Types de sources de flux

IBM QRadar QFlow Collector peut traiter les flux provenant de plusieurs sources, qui sont catégorisés comme sources internes ou externes.

#### Sources de flux internes

Les sources qui incluent des données de paquets en se connectant à un port SPAN ou à un TAP réseau sont considérées comme des sources internes. Ces sources fournissent des données de paquets brutes à un port de surveillance sur collecteur de flux, qui convertit les détails du paquet en enregistrements de flux.

QRadar ne conserve pas l'intégralité du contenu de paquet. Au lieu de cela, il capture un instantané du flux, appelé *Charge* ou *Capture de contenu*, qui inclut des paquets depuis le début de la communication.

La collecte de flux à partir de sources internes requiert normalement un collecteur de flux dédié.

#### Sources de flux externes

QRadar prend en charge les sources de flux externes suivantes :

- [NetFlow](#)
- [IPFIX](#)
- [sFlow](#)
- [J-Flow](#)
- [Packeteer](#)
- [Interface Napatech](#)
- [Interface réseau](#)

Pour plus d'informations sur les zones prises en charge pour chaque type de source de flux, voir le *IBM QRadar - Guide d'utilisation*.

Les sources externes ne nécessitent pas autant d'utilisation de l'unité centrale à traiter pour que vous puissiez envoyer les flux directement à un processeur de flux. Dans cette configuration, vous pouvez disposer d'un collecteur de flux dédié et d'un processeur de flux, qui reçoivent et créent des données de flux.

Si votre collecteur de flux collecte des flux à partir de plusieurs sources, vous pouvez affecter à chaque source de flux un nom distinct. Un nom distinct permet de distinguer les données de flux externes d'autres sources.

QRadar SIEM peut acheminer des données de source de flux externes à l'aide de la méthode d'usurpation ou de non-usurpation :

#### Usurpation

Rend les données entrantes reçues d'une source de flux vers une destination secondaire.

Pour configurer la méthode de spoofing, configurez la source de flux de sorte que **Interface de surveillance** soit défini sur le port de gestion sur lequel les données sont reçues.

Lorsque vous utilisez une interface spécifique, le collecteur de flux utilise une capture de mode promiscuité pour collecter les données de flux, plutôt que le port d'écoute UDP par défaut sur le port 2055. De cette façon, le collecteur de flux peut capturer et transmettre les données.

### Non-usurpation

Pour la méthode de non-usurpation, configurez le paramètre **Interface de surveillance** dans la configuration de la source de flux en tant que Tout.

Le collecteur de flux ouvre le port d'écoute, qui est le port configuré en tant que **Port de surveillance**, pour accepter les données de flux. Les données sont traitées et transmises à une autre destination de source de flux.


Lorsque les données sont transmises, l'adresse IP source du flux devient l'adresse IP du système QRadar SIEM, et non le routeur d'origine qui a envoyé les données.

## Ajout ou édition d'une source de flux

---

Utilisez la fenêtre **Source de flux** de l'onglet **Admin** pour ajouter ou éditer une source de flux.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Sources de flux** sous **Flux**.
3. Effectuez l'une des actions suivantes :
  - Pour ajouter une source de flux, cliquez sur **Ajouter**.
  - Pour modifier une source de flux, sélectionnez celle-ci et cliquez sur **Editer**.
4. Pour créer cette source de flux à partir d'une source de flux existante, cochez la case **Créer depuis une source de flux existante** et sélectionnez une source de flux dans la liste **Utiliser comme modèle**.
5. Renseignez la zone **Nom de la source de flux**.

**Conseil :** Si la source de flux externe est elle-même une unité physique, utilisez le nom de cette unité comme nom de la source de flux. Si la source de flux n'est pas une unité physique, utilisez un nom représentatif.

Par exemple, si vous souhaitez utiliser le trafic IPFIX, entrez **ipf1**. Si vous souhaitez utiliser le trafic NetFlow, entrez **nf1**.

6. Sélectionnez une source de flux dans la liste **Type de la source de flux** et configurez les propriétés.
  - Si vous sélectionnez l'option **Fichier Flowlog**, assurez-vous de configurer l'emplacement du fichier Flowlog pour le paramètre **Chemin du fichier source**.
  - Si vous sélectionnez **JFlow**, **Netflow**, **Packeteer FDR** ou **sFlow** pour le paramètre **Type de la source de flux**, vérifiez que vous configurez un port disponible pour le paramètre **Port de surveillance**.

Le port par défaut de la première source de données NetFlow configurée dans votre réseau est 2055. Pour chaque source de flux NetFlow supplémentaire, le numéro de port par défaut s'incrémente de 1. Par exemple, la source de flux NetFlow par défaut pour la seconde source de flux NetFlow est 2056.

- Si vous sélectionnez l'option **Interface Napatech** , entrez l'**Interface de flux** que vous souhaitez affecter à la source de flux.

**Restriction :** L'option **Interface Napatech** s'affiche uniquement si vous avez installé Napatech Network Adapter sur votre système.

- Si vous sélectionnez l'option **Interface réseau**, configurez pour l'**Interface de flux** une seule source de journal pour chaque interface Ethernet.



**Restriction :** Vous ne pouvez pas envoyer des types de flux différents au même port.

- Si le trafic sur votre réseau est configuré pour prendre d'autres chemins pour le trafic entrant et sortant, cochez la case **Activer les flux asymétriques** .
- Cliquez sur **Sauvegarder**.
- Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Transmission de paquets à QRadar Packet Capture

Vous pouvez surveiller le trafic réseau en envoyant des paquets de données brutes à un dispositif IBM QRadar QFlow Collector 1310. QRadar QFlow Collector utilise une carte de contrôle Napatech dédiée pour copier des paquets entrants d'un port de la carte sur un deuxième port qui se connecte à un dispositif IBM QRadar Packet Capture.

Si vous disposez déjà d'un dispositif QRadar QFlow Collector 1310 avec une carte réseau Napatech 10G, vous pouvez reproduire le trafic sur QRadar Packet Capture.

Comme présenté dans le diagramme suivant, si vous disposez déjà d'un dispositif QRadar QFlow Collector 1310 avec une carte réseau Napatech 10G, vous pouvez reproduire le trafic sur QRadar Packet Capture.

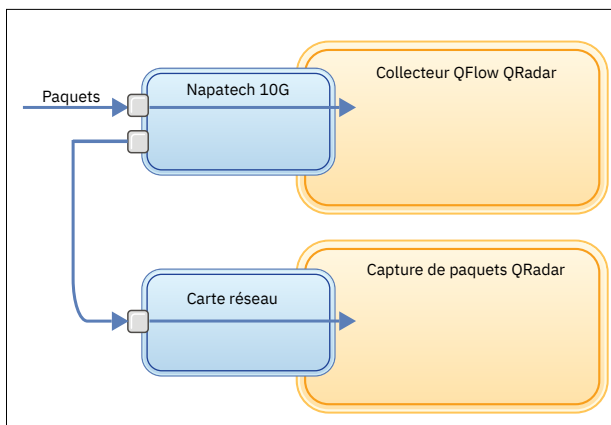


Figure 17. Transmission de données de paquet à partir d'un dispositif QRadar QFlow Collector vers QRadar Packet Capture en utilisant la carte Napatech

### Avant de commencer

Vérifiez que le matériel suivant est configuré dans votre environnement :

- Vous avez relié le câble au port 1 de la carte Napatech sur le dispositif QRadar QFlow Collector 1310.
- Vous avez relié le câble qui est connecté au port 2 de la carte Napatech (port de transmission) au dispositif QRadar Packet Capture.
- Vérifiez la connectivité de couche 2 à l'aide des voyants de liaison sur les deux dispositifs.

### Procédure

- En utilisant SSH à partir de votre console IBM QRadar Console, connectez-vous à QRadar QFlow Collector en tant qu'utilisateur root. Sur le dispositif QRadar QFlow Collector, éditez le fichier suivant.

```
/opt/qradar/init/apply_tunings
```

- Recherchez la ligne suivante aux alentours de la ligne 137.

```
apply_multithread_qflow_changes()
{
    APPLIANCEID=`$NVABIN/myver -a`
    if [ "$APPLIANCEID" == "1310" ]; then
        MODELNUM=$( /opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut
-d'-' -f2)
        if [ "$MODELNUM" == "9220" ]; then..
```

- b) Dans les lignes `AppendToConf` qui suivent le code de l'étape précédente, ajoutez les lignes suivantes :

```
AppendToConf SV_NAPATECH_FORWARD YES
AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDEST "0:1"
```

Ces instructions permettent la transmission de paquet et font transiter les paquets du port 0 au port 1.


- c) Assurez-vous que le *traitement multitâche* est activé en vérifiant que la ligne suivante figure dans le fichier `/opt/qradar/conf/nva.conf`.
- ```
.
MULTI_THREAD_ON=YES
```
2. Exécutez le script `apply_tunings` pour mettre à jour les fichiers de configuration sur QRadar QFlow Collector en tapant la commande suivante :
- ```
./apply_tunings restart
```
3. Redémarrez les services IBM QRadar en entrant la commande suivante :
- ```
systemctl restart hostcontext
```
4. Facultatif : Vérifiez que la carte Napatech reçoit et transmet des données.
- a) Pour vérifier que la carte Napatech reçoit des données, entrez la commande suivante :
- ```
/opt/napatech/bin/Statistics -dec -interactive
```
- Le paquet "RX" et les statistiques s'incrémentent si la carte reçoit des données.
- b) Pour vérifier que la carte Napatech transmet des données, entrez la commande suivante :
- ```
/opt/napatech/bin/Statistics -dec -interactive
```
- Les statistiques "TX" s'incrémentent si la carte transmet des données.
5. Facultatif : Vérifiez que QRadar Packet Capture reçoit des paquets de votre dispositif QRadar QFlow Collector.
- a) En utilisant SSH depuis votre console QRadar Console, connectez-vous à votre dispositif QRadar Packet Capture en tant qu'utilisateur root sur le port 4477.
- b) Vérifiez que le dispositif QRadar Packet Capture reçoit des paquets en entrant la commande suivante :
- ```
watch -d cat /var/www/html/statisdata/int0.txt
```
- Le fichier `int0.txt` est mis à jour à mesure que les données circulent dans votre dispositif QRadar Packet Capture.
- Pour plus d'informations sur la capture de paquet, voir le document *IBM QRadar Packet Capture - Aide-mémoire*.

## Activation et désactivation d'une source de flux

---

À l'aide de la fenêtre **Source de flux**, vous pouvez activer ou désactiver une source de flux.

### Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Sources de flux** sous **Flux**.
3. Sélectionnez la source de flux que vous souhaitez activer ou désactiver puis cliquez sur **Activer/Désactiver**.
4. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Suppression d'une source de flux

---

Utilisez la fenêtre **Source de flux** pour supprimer une source de flux.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Sources de flux** sous **Flux**.
3. Sélectionnez la source de flux à supprimer, puis cliquez sur **Supprimer**.
4. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Alias de source de flux

---

Un alias de source de flux utilise un nom virtuel pour identifier les flux externes envoyés au même port sur un collecteur de flux. Par exemple, IBM QRadar QFlow Collector peut disposer d'une seule source de flux NetFlow qui écoute sur le port 2055 et peut avoir plusieurs sources NetFlow envoyées au même QRadar QFlow Collector. En utilisant des alias de source de flux, vous pouvez identifier les différentes sources NetFlow en fonction de leurs adresses IP.

Lorsque QRadar QFlow Collector reçoit le trafic d'une unité ayant une adresse IP mais ne possède pas d'alias en cours, QRadar QFlow Collector tente une recherche DNS inverse. La recherche est utilisée pour déterminer le nom d'hôte de l'unité.


Vous pouvez configurer QRadar QFlow Collector pour créer automatiquement des alias de source de flux. Lorsque le QRadar QFlow Collector reçoit le trafic d'une unité ayant une adresse IP mais qu'il n'a pas d'alias en cours, il effectue une recherche DNS inverse pour déterminer le nom d'hôte de l'unité.

Si la recherche aboutit, QRadar QFlow Collector ajoute ces informations à la base de données et les signale à tous les composants QRadar QFlow Collector de votre déploiement. Si la recherche échoue, QRadar crée un alias par défaut pour la source de flux en fonction du nom de la source de flux et de l'adresse IP source. Par exemple, l'alias par défaut peut apparaître sous la forme **default\_NetFlow\_172.16.10.139**.

## Ajout d'un alias de source de flux

Utilisez la fenêtre **Alias de source de flux** pour ajouter un alias de source de flux.

### Procédure


1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, sous **Flux**, cliquez sur **Alias de source de flux**.
3. Effectuez l'une des actions suivantes :
  - Pour ajouter un alias de source de flux, cliquez sur **Ajouter** et renseignez les valeurs des paramètres.
  - Pour modifier un alias de source de flux existant, sélectionnez cet alias, cliquez sur **Editer** et mettez à jour ses paramètres.
4. Cliquez sur **Sauvegarder**.
5. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

**Remarque :** Si vous renommez un alias de source de flux, vous devez utiliser le nom d'origine pour effectuer une recherche historique.

## Suppression d'un alias de source de flux

Utilisez la fenêtre **Alias de source de flux** pour supprimer un alias de source de flux.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, sous **Flux**, cliquez sur **Alias de source de flux**.
3. Sélectionnez l'alias de source de flux à supprimer, puis cliquez sur **Supprimer**.
4. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Correction des horodatages de flux

---

Vous pouvez spécifier la façon dont vous souhaitez que les horodatages de flux soient traités lorsque Netflow V9 commence à envoyer des enregistrements avec des valeurs de temps d'uptime de système dépassées.

### Pourquoi et quand exécuter cette tâche

Deux nouveaux paramètres de configuration permettent de contrôler davantage la façon dont les horodatages de flux sont traités lorsque Netflow V9 commence à envoyer des enregistrements avec des valeurs de temps d'uptime de système dépassées. Les nouveaux paramètres éliminent le besoin de réinitialisation lors de la première et de la dernière période de commutation.

Les nouvelles options de configuration et valeurs par défaut sont présentées ici :

- `NORMALISE_OVERFLOWED_UPTIMES=OUI`
- `UPTIME_OVERFLOW_THRESHOLD_MSEC=86400000`

Les horodatages sont corrigés lorsque la valeur d'heure de mise à jour du système est inférieure à la première et à la dernière heure de paquet commutée par rapport à la valeur spécifiée dans la configuration `UPTIME_OVERFLOW_THRESHOLD_MSEC`. Les horodatages sont corrigés en fonction de l'hypothèse que le temps de fonctionnement du système s'est terminé autour de la valeur maximale de 32 bits.

### Procédure

1. Pour modifier ces paramètres, ajoutez les paramètres au fichier `/store/configservices/staging/globalconfig/nva.conf`.
2. Pour affiner les paramètres, indiquez un intervalle de temps différent pour le paramètre `UPTIME_OVERFLOW_THRESHOLD_MSEC`.
3. Pour désactiver cette fonction, définissez le `NORMALISE_OVERFLOWED_UPTIMES` sur `NON`.

Lorsque cette fonction est désactivée, QRadar ne modifie pas les horodatages NetFlow v9 qui répondent à cette condition.

4. Après avoir modifié les paramètres de configuration, vous devez déployer le système.

# Chapitre 14. Configuration des réseaux et services distants

Les groupes de réseaux et de services distants permettent de représenter l'activité du trafic sur votre réseau pour un profil spécifique. Les groupes de réseaux distants affichent le trafic utilisateur qui provient de réseaux distants nommés.

Tous les groupes de réseaux et de services distants incluent des niveaux Groupe et des niveaux Objet feuille. Vous pouvez modifier des groupes de réseaux et de services distants en ajoutant des objets à des groupes existants ou en modifiant des propriétés préexistantes en fonction de votre environnement.

Si vous déplacez un objet existant vers un autre groupe, son nom passe du groupe existant au groupe nouvellement sélectionné. Toutefois, lorsque les changements de configuration sont déployés, les données de l'objet stockées dans la base de données sont perdues et l'objet ne fonctionne plus. Pour résoudre le problème, créez une vue et recréez l'objet qui existe avec un autre groupe.

Vous pouvez regrouper des réseaux et des services distants à utiliser dans le moteur de règles personnalisé, le flux et les recherches d'événements. Vous pouvez également regrouper des réseaux et des services dans IBM QRadar Risk Manager, s'il est disponible.

## Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Groupes de réseaux distants par défaut

IBM QRadar inclut les groupes de réseaux distants par défaut.

Le tableau suivant décrit les groupes de réseaux distants par défaut.

| Groupe       | Description                                                                                                                                                                                                                                                                                                                                                          |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BOT          | Indique le trafic provenant des applications BOT.<br>Pour plus d'informations, voir <a href="#">Règles de suppression de la commande et du contrôle de Botnet sur le site Web Nouvelles menaces</a> ( <a href="http://rules.emergingthreats.net/blockrules/emerging-botcc.rules">http://rules.emergingthreats.net/blockrules/emerging-botcc.rules</a> )              |
| Bogon        | Indique le trafic provenant d'adresses IP non affectées.<br>Pour plus d'informations, voir <a href="#">Référence de bogon sur le site Web de l'équipe CYMRU</a> ( <a href="http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt">http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt</a> ).                                                       |
| Nets_hotiles | Indique le trafic provenant de réseaux hostiles connus.<br>HostileNets dispose d'un ensemble de plages CIDR configurables de 20 (rang 1-20 inclus).<br>Pour plus d'informations, voir <a href="#">Référence HostileNets sur le site Web de DShield</a> ( <a href="http://www.dshield.org/ipsascii.html?limit=20">http://www.dshield.org/ipsascii.html?limit=20</a> ) |

Tableau 51. Groupes de réseaux distants par défaut (suite)

| Groupe                 | Description                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Voisinage              | Indique le trafic provenant des réseaux voisins avec lequel votre organisation a des accords de trafic réseau.<br><br>Ce groupe est vide par défaut. Vous devez configurer ce groupe pour classer le trafic provenant des réseaux voisins.                                                     |
| Smurfs                 | Indique le trafic provenant d'attaques smurf.<br><br>Une attaque smurf est un type d'attaque par déni de service qui inonde un système de destination avec des messages de ping-diffusés spoofed.                                                                                              |
| Super-flux             | Ce groupe n'est pas configurable.<br><br>Un flux superflux est un flux qui est un agrégat d'un certain nombre de flux ayant un ensemble prédéterminé similaire d'éléments.                                                                                                                     |
| Réseaux_accrédités     | Indique le trafic à partir de réseaux sécurisés, y compris les partenaires commerciaux qui ont un accès distant à vos applications et services critiques.<br><br>Ce groupe est vide par défaut.<br><br>Vous devez configurer ce groupe pour classer le trafic provenant des réseaux sécurisés. |
| Listes de surveillance | Classe le trafic provenant des réseaux que vous souhaitez surveiller.<br><br>Ce groupe est vide par défaut.                                                                                                                                                                                    |

Les groupes et les objets qui incluent des superflux sont uniquement à des fins d'information et ne peuvent pas être modifiés. Les groupes et les objets qui incluent des bogons sont configurés par la fonction de mise à jour automatique.

**Remarque :** Vous pouvez utiliser des ensembles de référence au lieu de réseaux distants pour fournir une partie de cette fonctionnalité. Bien que vous puissiez attribuer un niveau de confiance à une valeur IP dans une table de référence, les ensembles de référence sont utilisés uniquement avec des adresses IP uniques et ne peuvent pas être utilisés avec les plages CIDR. Vous pouvez utiliser une valeur CIDR après une mise à jour du réseau distant, mais pas avec des niveaux de poids ou de confiance.

#### Concepts associés

«Types d'ensembles de données de référence», à la page 179

IBM QRadar possède différents types d'ensembles de données de référence qui peuvent gérer différents niveaux de complexité des données. Les types les plus courants sont les ensembles de référence et les cartes de référence.

## Groupes de services distants par défaut

IBM QRadar inclut les groupes de services distants par défaut.

Le tableau suivant décrit les groupes de services distants par défaut.

Tableau 52. Groupes de réseaux distants par défaut

| Paramètre                    | Description                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Serveurs_IRC                 | Indique le trafic provenant d'adresses communément appelées serveurs de discussion.                                     |
| Services_en_ligne            | Indique le trafic provenant d'adresses de services en ligne généralement connus pouvant impliquer une perte de données. |
| Pornographie                 | Indique le trafic provenant d'adresses communément connues pour contenir du matériel pornographique explicite.          |
| Proxies                      | Indique le trafic provenant des serveurs proxy ouverts connus.                                                          |
| Reserved_IP_Ranges           | Indique le trafic provenant des plages d'adresses IP réservées.                                                         |
| Courrier_indésirable         | Indique le trafic provenant d'adresses communément appelées à produire du SPAM ou des courriels non désirés.            |
| Publiciels/logiciels_espions | Indique le trafic provenant d'adresses communément appelées spyware ou adware.                                          |
| Super-flux                   | Indique le trafic provenant d'adresses communément appelées à produire des superflux.                                   |
| Warez                        | Indique le trafic provenant d'adresses communément connues pour contenir des logiciels piratés.                         |

## Instructions pour les ressources réseau

Compte tenu des complexités et des ressources réseau requises pour IBM QRadar SIEM dans les grands réseaux structurés, suivez les instructions suggérées.

La liste suivante décrit certaines des pratiques suggérées que vous pouvez suivre :

- Regroupement d'objets et utilisation des onglets **Activité réseau** et **Activité de journal** pour analyser vos données réseau.

Moins d'objets créent moins d'entrées et de sorties sur votre disque.

- De manière générale, pour les exigences système standard, ne dépassez pas plus de 200 objets par groupe.

D'autres objets peuvent avoir un impact sur votre puissance de traitement lorsque vous examinez votre trafic.

## Gestion des objets de réseaux distants

Une fois que vous avez créé des groupes de réseaux distants, vous pouvez agréger des résultats de recherche de flux et d'événements sur des groupes de réseaux distants. Vous pouvez également créer des règles qui testent l'activité sur des groupes de réseaux distants.

La fenêtre **Réseaux distants** vous permet d'ajouter ou de modifier un objet de réseaux distants.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.

2. Dans la section **Configuration des réseaux et services distants**, cliquez sur **Réseaux et services distants**.
3. Pour ajouter un objet réseaux distants, cliquez sur **Ajouter** et entrez des valeurs pour les paramètres.
4. Pour éditer un objet de réseaux distants, procédez comme suit :
  - a) Cliquez deux fois sur le nom du groupe.
  - b) Sélectionnez le profil et cliquez sur l'icône d'édition (✎) pour éditer le profil distant.
5. Cliquez sur **Sauvegarder**.
6. Cliquez sur l'icône précédente (◀) pour revenir à la fenêtre **Réseaux et services distants**.
7. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications**.

## Gestion des objets de services distants

---

Les groupes de services distants organisent le trafic provenant des plages réseau définies par l'utilisateur ou du serveur de mise à jour automatique IBM. Une fois que vous avez créé des groupes de services distants, vous pouvez agréger des résultats de recherche de flux et d'événements et créer des règles qui teste l'activité sur les groupes de services distants.

Utilisez la fenêtre **Services distants** pour ajouter ou éditer un objet de services distants.

### Procédure

1. Dans le menu de navigation (☰), cliquez sur **Admin**.
2. Dans la section **Configuration des réseaux et services distants**, cliquez sur **Réseaux et services distants**.
3. Pour ajouter un objet de services distants, cliquez sur **Ajouter** et entrez les valeurs des paramètres.
4. Pour éditer un objet de services distants, cliquez sur le groupe que vous souhaitez afficher, cliquez sur l'icône **Éditer** et modifiez les valeurs.
5. Cliquez sur **Sauvegarder**.
6. Cliquez sur **Return**.
7. Fermez la fenêtre **Services distants**.
8. Dans le menu de l'onglet **Admin**, cliquez sur **Déployer les modifications**.



## Chapitre 15. Reconnaissance des serveurs

La fonction **Reconnaissance des serveurs** utilise la base de données de profils d'actif pour reconnaître les différents types de serveur basés sur les définitions de port. Vous pouvez ensuite sélectionner les serveurs à ajouter à un bloc de construction de type de serveur pour des règles.

La fonction **Reconnaissance des serveurs** est basée sur des blocs de construction de type serveur. Les ports sont utilisés pour définir le type de serveur. Ainsi, le bloc de construction de type serveur fonctionne comme un filtre basé sur un port lorsque vous effectuez une recherche dans la base de données de profils d'actif.

Pour plus d'informations sur les blocs de construction, voir *IBM QRadar - Guide d'utilisation*.

Utilisez la fonction **Reconnaissance des serveurs** avec IBM QRadar Vulnerability Manager pour créer des règles d'exception pour les vulnérabilités bénignes. Réduisez le nombre de vulnérabilités que vous voyez pour les **types de serveur** suivants :

| Type de serveur        | Vulnérabilité                    |
|------------------------|----------------------------------|
| Serveurs FTP           | Serveur FTP présent              |
| Serveurs DNS           | Serveur DNS en cours d'exécution |
| Serveurs de messagerie | Serveur SMTP détecté             |
| Serveurs Web           | Service Web en cours d'exécution |

Pour plus d'informations sur les vulnérabilités à faux positif, voir *IBM QRadar Vulnerability Manager - Guide d'utilisation*.


### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Reconnaissance des serveurs

Utilisez l'onglet **Actifs** pour reconnaître les serveurs de votre réseau.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Actifs** pour ouvrir l'onglet **Actifs**.
2. Dans le menu de navigation **Actifs**, cliquez sur **Reconnaissance de serveur**.
3. Dans la liste **Type de serveur**, sélectionnez le type de serveur que vous souhaitez reconnaître.
4. Sélectionnez l'une des options suivantes pour déterminer les serveurs à reconnaître :
  - Pour utiliser le **Type de serveur** actuellement sélectionné pour effectuer une recherche parmi tous les serveurs dans votre déploiement, sélectionnez **Tous**.
  - Pour rechercher des serveurs dans votre déploiement qui sont affectés au **Type de serveur** actuellement sélectionné, sélectionnez **Affectés**.
  - Pour rechercher des serveurs dans votre déploiement qui ne sont pas affectés, sélectionnez **Non affectés**.
5. Pour modifier la liste des ports du serveur standard, cliquez sur **Éditer les ports**.
6. Dans la liste **Réseau**, sélectionnez le réseau sur lequel effectuer la recherche.
7. Cliquez sur **Reconnaître les serveurs**.
8. Dans le tableau **Serveurs correspondants**, cochez la case de tous les serveurs que vous souhaitez affecter au rôle serveur.

9. Cliquez sur **Approuver les serveurs sélectionnés**.

## Chapitre 16. Segmentation de domaine

La segmentation de votre réseau en différents domaines contribue à garantir que les informations pertinentes sont disponibles aux seuls utilisateurs qui le nécessitent.

Vous pouvez créer des profils de sécurité pour limiter les informations qui sont disponibles pour un groupe d'utilisateurs dans ce domaine. Les profils de sécurité permettent aux utilisateurs autorisés d'accéder aux seuls renseignements qui sont nécessaires pour accomplir leurs tâches quotidiennes. Vous modifiez uniquement le profil de sécurité des utilisateurs concernés, et non chaque utilisateur individuellement.

Vous pouvez également utiliser des domaines pour gérer les plages d'adresses IP qui se chevauchent. Cette méthode est utile lorsque vous utilisez une infrastructure IBM QRadar pour recueillir des données provenant de plusieurs réseaux. En créant des domaines qui représentent un espace d'adresse particulier sur le réseau, plusieurs périphériques qui sont dans des domaines distincts peuvent avoir la même adresse IP et peuvent toujours être traités comme des périphériques séparés.

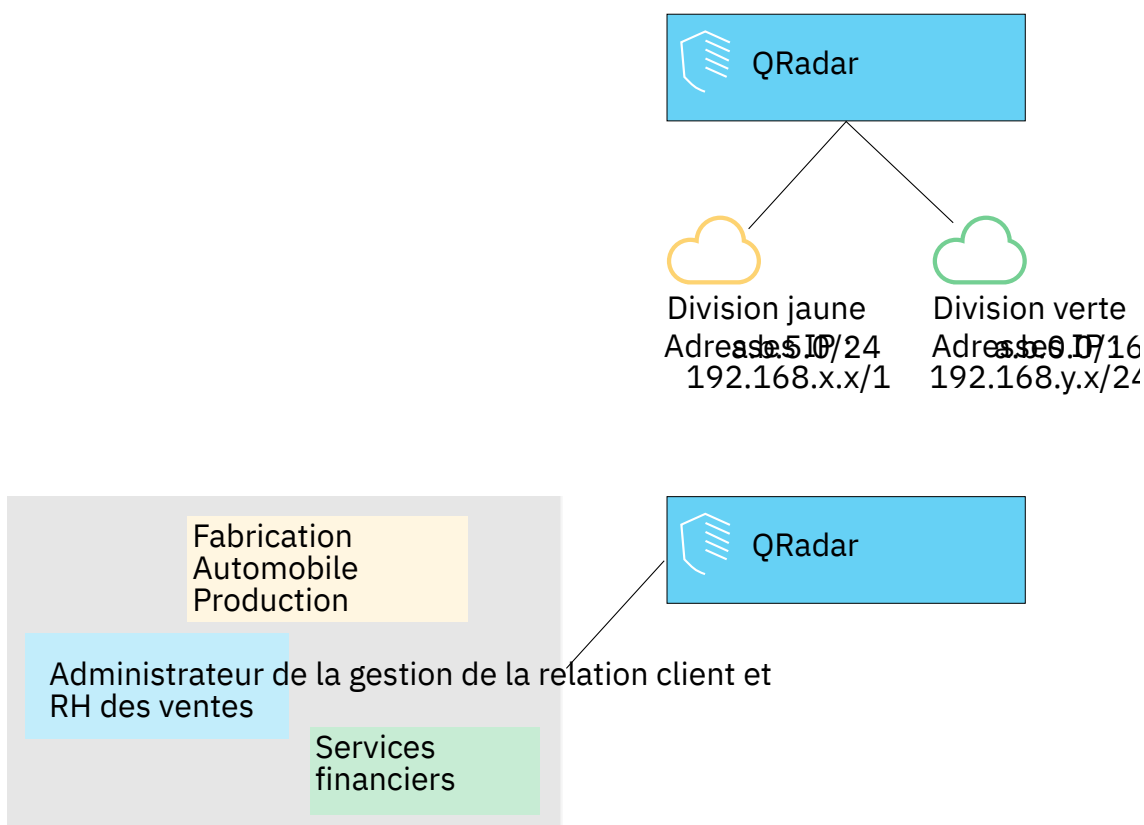


Figure 18. Segmentation de domaine

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Adresses IP de chevauchement

Une adresse IP qui se chevauchent est une adresse IP affectée à plusieurs unités ou unités logiques, telles qu'un type de source d'événement, sur un réseau. Le chevauchement des plages d'adresses IP peut entraîner des problèmes importants pour les sociétés qui fusionnent les réseaux après des acquisitions d'entreprise ou pour les fournisseurs de services de sécurité gérés (MSSP) qui apportent de nouveaux clients.

IBM QRadar doit être en mesure de différencier les événements Et flux provenant de différents périphériques et ayant la même adresse IP. Si la même adresse IP est attribuée à plusieurs sources d'événement, vous pouvez créer des domaines afin de les distinguer.

Par exemple, examinons une situation où la société A acquiert la société B et souhaite utiliser une instance partagée de QRadar pour surveiller les actifs de la nouvelle société. L'acquisition a une structure de réseau similaire qui entraîne l'utilisation de la même adresse IP pour différentes sources de journal dans chaque société. Les sources de journal ayant la même adresse IP causent des problèmes de corrélation, de génération de rapports, de recherche et de profilage d'actifs.

Pour distinguer l'origine des événements Et flux qui entrent dans QRadar à partir de la source de journal, vous pouvez créer deux domaines et affecter chaque source de journal à un domaine différent. Si nécessaire, vous pouvez également affecter chaque collecteur d'événements Et collecteur de flux au même domaine que la source de journal qui leur envoie des événements.

Pour afficher les événements entrants par domaine, créez une recherche et incluez les informations de domaine dans les résultats de la recherche.

## Balisage et définition de domaine

Les domaines sont définis en fonction des sources d'entrée IBM QRadar. Lorsque les événements et les flux entrent dans QRadar, les définitions de domaine sont évaluées et les événements et flux sont marqués avec les informations de domaine.

### Spécification de domaines pour des événements

Le diagramme suivant montre l'ordre de priorité pour l'évaluation des critères de domaine pour les événements.

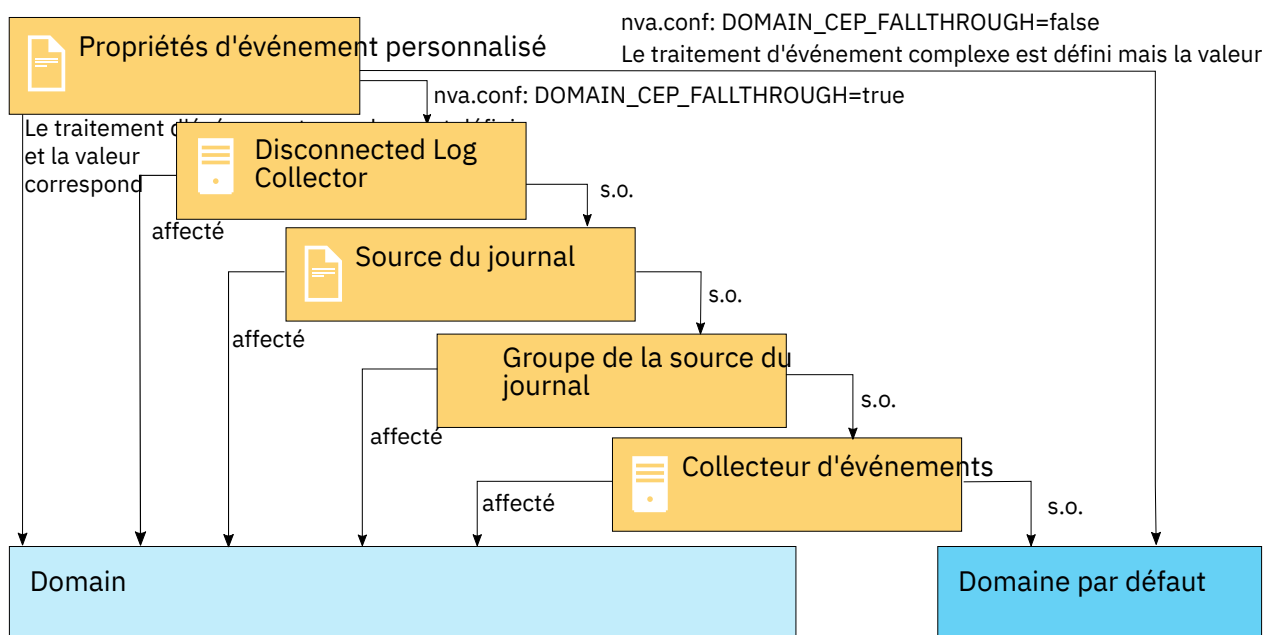


Figure 19. Ordre de priorité des événements

Les différentes méthodes permettant de spécifier des domaines pour des événements sont présentées ci-dessous :

#### Propriétés personnalisées

Vous pouvez appliquer des propriétés personnalisées aux messages journaux provenant d'une source de journal.

Pour déterminer le domaine auquel ces messages de journal spécifiques appartiennent, la valeur d'une propriété personnalisée est recherchée dans un mappage défini dans l'éditeur de gestion des domaines.

Cette option est utilisée pour les sources de journal à service partagé ou à plusieurs plages d'adresses, comme les serveurs de fichiers et les référentiels de documents.

### **Collecteur de journaux déconnectés**

Vous pouvez utiliser un collecteur de journal déconnecté (DLC) pour le mappage de domaine. Les DLC ajoutent leurs identificateurs uniques universels (UUID) à la valeur de l'identificateur de source de journal des événements qu'ils collectent. L'apposition de l'identificateur unique universel à la valeur de l'identificateur de source de journal garantit que l'identificateur de source de journal est unique.

### **Sources de journal**

Vous pouvez configurer des sources de journal spécifiques de telle sorte qu'elles appartiennent à un domaine.

Cette méthode de marquage des domaines est une option pour les déploiements dans lesquels un Collecteur d'événements peut recevoir des événements de plusieurs domaines.

### **Groupes de source de journal**

Vous pouvez affecter des groupes de source de journal à un domaine spécifique. Cette option permet de contrôler de manière plus étendue la configuration de source de journal.

Toute nouvelle source de journal ajoutée au groupe de sources de journal obtient automatiquement le balisage de domaine associé à ce groupe.

### **Collecteurs d'événements**

Si un collecteur d'événements est dédié à un segment de réseau spécifique, à une plage d'adresses IP, à un locataire, à un emplacement géographique ou à une unité commerciale, vous pouvez marquer l'ensemble du collecteur d'événements comme faisant partie de ce domaine.

Tous les événements qui arrivent à ce collecteur d'événements appartiennent au domaine auquel le collecteur d'événements est affecté, sauf si la source de journal de l'événement appartient à un autre domaine en fonction d'autres méthodes de balisage plus élevées, telles qu'une propriété personnalisée.

#### **Important :**

Si une source de journal est redirigée d'un collecteur d'événements à un autre dans un autre domaine, vous devez ajouter un mappage de domaine à la source de journal pour vous assurer que les événements de cette source de journal sont toujours affectés au domaine droit.

À moins que la source de journal ne soit mappée vers le domaine droit, les utilisateurs non administrateurs possédant des restrictions de domaine peuvent ne pas voir les infractions associées à la source de journal.

### **Spécification de domaines pour les flux**

Le diagramme suivant montre l'ordre de priorité pour l'évaluation des critères de domaine pour les flux.

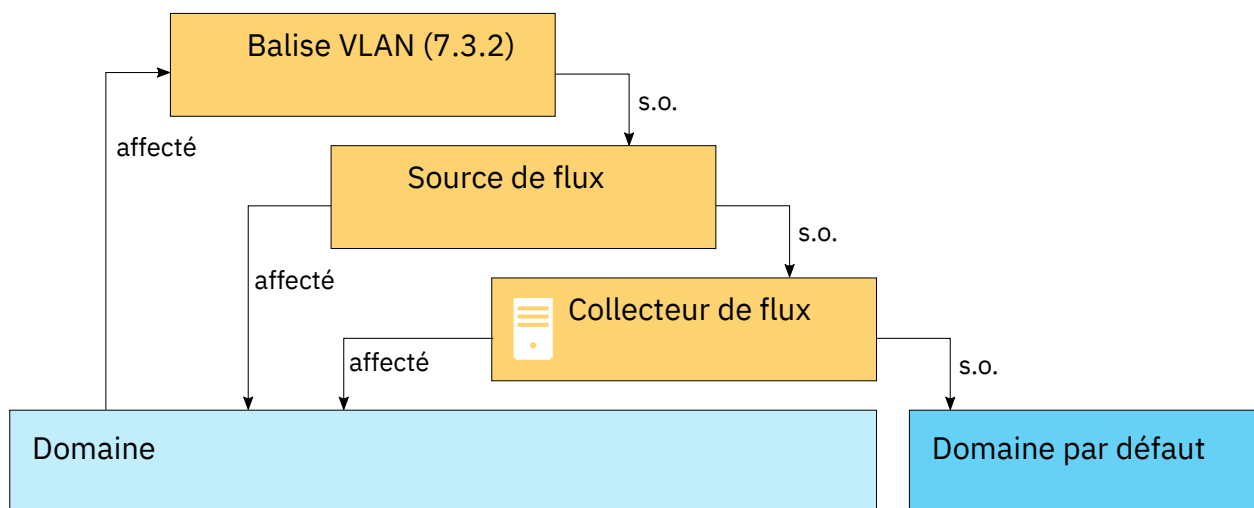


Figure 20. Ordre de priorité des flux

Les méthodes permettant de spécifier des domaines pour les flux sont présentées ci-dessous :

### Collecteurs de flux

Vous pouvez affecter des collecteurs QFlow spécifiques à un domaine.

Toutes les sources de flux arrivant sur ce collecteur de flux appartiennent au domaine. C'est pourquoi, toute nouvelle source de flux automatiquement détectée est ajoutée au domaine.

### Sources de flux

Vous pouvez désigner des sources de flux spécifiques dans un domaine.

Cette option est utile lorsqu'un collecteur QFlow collecte des flux dans plusieurs segments de réseau ou routeurs qui contiennent des plages d'adresses IP se chevauchant.

### ID de VLAN de flux

Vous pouvez désigner des réseaux VLAN spécifiques dans un domaine.

Cette option est utile lorsque vous collectez le trafic à partir de plusieurs segments réseau, souvent avec des plages IP se chevauchant. Cette définition de réseau VLAN est effectuée en fonction des ID de réseau VLAN du client et d'entreprise.

Les éléments d'information suivants sont envoyés à partir de QFlow lors de l'analyse des flux contenant des informations de réseau VLAN. Ces deux zones peuvent être affectées dans une définition de domaine :

- PEN 2 (IBM), ID élément 82 : ID de réseau VLAN d'entreprise
- PEN 2 (IBM), ID élément 83 : ID de réseau VLAN du client

## Spécification de domaines pour les résultats d'analyse

Vous pouvez également affecter des scanners de vulnérabilité à un domaine spécifique afin que ces résultats d'analyse puissent être correctement marqués comme appartenant à ce domaine. Une définition de domaine peut être constituée de toutes les sources d'entrée QRadar.

Pour plus d'informations sur l'affectation de votre réseau à des domaines préconfigurés, voir «[Hiérarchie du réseau](#)», à la page 87.

## Ordre de priorité pour l'évaluation des critères de domaine

Lorsque les événements et les flux entrent dans le système QRadar, les critères de domaine sont évalués en fonction de la granularité de la définition de domaine.

Si la définition de domaine dépend d'un événement, des propriétés personnalisées mappées à la définition de domaine sont recherchées dans l'événement entrant. Si le résultat d'une expression

régulière définie dans une propriété personnalisée ne correspond à aucun mappage de domaine, l'événement est automatiquement affecté au domaine par défaut.

Si l'événement ne correspond pas à la définition de domaine pour les propriétés personnalisées, l'ordre de priorité suivant est appliqué :

1. contrôle de liaison de données
2. Source du journal
3. Groupe de la source de journal
4. Collecteur d'événements

Si le domaine est défini en fonction d'un flux, l'ordre de priorité suivant est appliqué :

1. Source de flux
2. Collecteur de flux

Si un scanner a un domaine associé, tous les actifs qu'il détecte sont automatiquement affectés au même domaine que le scanner.

## Transfert de données vers un autre système QRadar

Les informations de domaine sont supprimées lorsque les données sont transmises à un autre système QRadar. Les événements et les flux qui contiennent des informations de domaine sont automatiquement affectés au domaine par défaut sur le système QRadar de réception. Pour identifier quels événements et flux sont affectés au domaine par défaut, vous pouvez créer une recherche personnalisée sur le système de réception. Vous pouvez réaffecter ces événements et flux à un domaine défini par l'utilisateur.

## Création de domaines

---

Utilisez la fenêtre **Gestion de domaine** pour créer des domaines basés sur des sources d'entrée IBM QRadar.


### Pourquoi et quand exécuter cette tâche

Utilisez les instructions suivantes lorsque vous créez des domaines :

- Tout ce qui n'est pas attribué à un domaine défini par l'utilisateur est automatiquement affecté au domaine par défaut. Les utilisateurs disposant d'un accès de domaine limité ne doivent pas avoir de privilèges d'administrateur car ce privilège accorde un accès illimité à tous les domaines.
- Vous pouvez associer la même propriété personnalisée à deux domaines différents, toutefois le résultat de capture doit être différent pour chacun.
- Vous ne pouvez pas affecter une source de journal, un groupe de sources de journal, ou un collecteur d'événements à deux différents domaines. Quand un groupe de source de journal est affecté à un domaine, chacun des attributs mappés est visible dans la fenêtre **Gestion de domaine**.

Les profils de sécurité doivent être mis à jour avec un domaine associé. Les restrictions de niveau domaine ne sont appliquées que lorsque les profils de sécurité sont mis à jour et que les modifications sont déployées.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion des domaines**.
3. Pour ajouter un domaine, cliquez sur **Ajouter** et tapez un nom unique et une description pour le domaine.

**Conseil :** Vous pouvez rechercher les noms uniques en tapant le nom dans la boîte de recherche **Nom de domaine d'entrée**.

4. En fonction des critères de domaine à définir, cliquez sur l'onglet approprié.
  - Pour définir le domaine en fonction d'une propriété personnalisée, d'un groupe de sources de journal, d'une source de journal ou d'un collecteur d'événements, cliquez sur l'onglet **Événements**.
  - Pour définir le domaine en fonction d'une source de flux, d'un collecteur de flux ou d'un gateway de données, cliquez sur l'onglet **Flux**.
  - Pour définir le domaine en fonction d'un scanner, y compris les scanners IBM QRadar Vulnerability Manager, cliquez sur l'onglet **Scanneurs**.
5. Pour affecter une propriété personnalisée à un domaine, dans la zone **Résultat de la capture**, entrez le texte correspondant au résultat du filtre d'expression régulière (regex).

**Important :** Vous devez cocher la case **Optimisation de l'analyse pour les règles, les rapports et les recherches** dans la fenêtre **Propriétés de l'événement personnalisé** pour analyser et stocker la propriété d'événement personnalisé. La segmentation de domaine ne se produira pas si cette option n'est pas cochée.
6. Dans la liste, sélectionnez les critères de domaine et cliquez sur **Ajouter**.
7. Après avoir ajouté les éléments source au domaine, cliquez sur **Créer**.

### Que faire ensuite

Création de profils de sécurité pour définir les utilisateurs qui ont accès aux domaines. Après avoir créé le premier domaine dans votre environnement, vous devez mettre à jour les profils de sécurité pour tous les utilisateurs non administrateurs afin de spécifier l'affectation de domaine. Dans les environnements au niveau du domaine, les utilisateurs non administratifs dont le profil de sécurité ne spécifie pas d'affectation de domaine ne verront aucune activité de journal ou activité réseau.

Vérifiez la configuration de la hiérarchie pour votre réseau et affectez les adresses IP existantes aux domaines appropriés. Pour plus d'informations, voir «Hiérarchie du réseau», à la page 87.


## Création de domaines pour les flux de réseau local virtuel

Utilisez la fenêtre **Gestion de domaine** pour créer des domaines basés sur des sources de flux VLAN IBM QRadar.

### Pourquoi et quand exécuter cette tâche

Dans QRadar, vous pouvez affecter des domaines à des flux entrants en fonction des informations VLAN se trouvant dans le flux. Les flux entrants sont mappés à des domaines qui contiennent la même définition de VLAN.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Gestion des domaines**.
3. Cliquez sur **Ajouter** et entrez un nom unique et une description du domaine.

**Conseil :** Vous pouvez rechercher les noms uniques en tapant le nom dans la boîte de recherche **Nom de domaine d'entrée**.



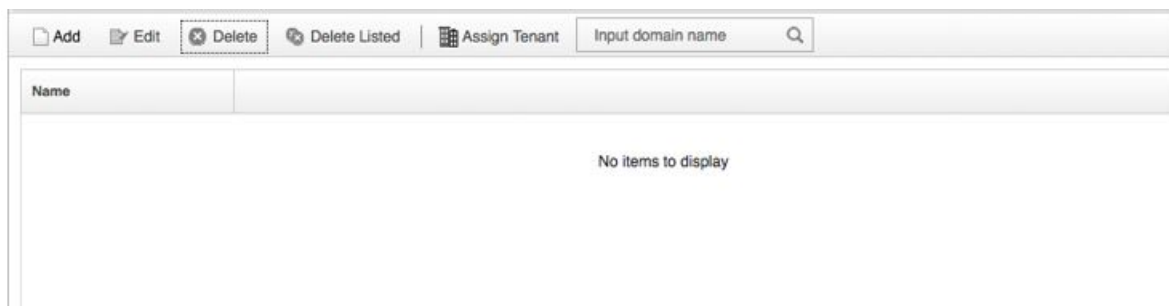


Figure 21. Entrer un nom de domaine

4. Cliquez sur l'onglet **Flux** puis sélectionnez **ID de VLAN de flux**.
5. Sélectionnez les valeurs d'ID de VLAN d'entreprise et d'ID de VLAN du client qui correspondent à celles des flux entrants, puis cliquez sur **Ajouter**.

**Remarques :**

- L'ID de VLAN d'entreprise (Enterprise VLAN ID) est spécifié par le numéro PEN (Private Enterprise Number) 2 et l'élément IE (Information Element) 82 sur les flux entrants.
- L'ID de VLAN du client (Customer VLAN ID) est spécifié par le numéro PEN 2 et l'élément IE 83 sur les flux entrants.

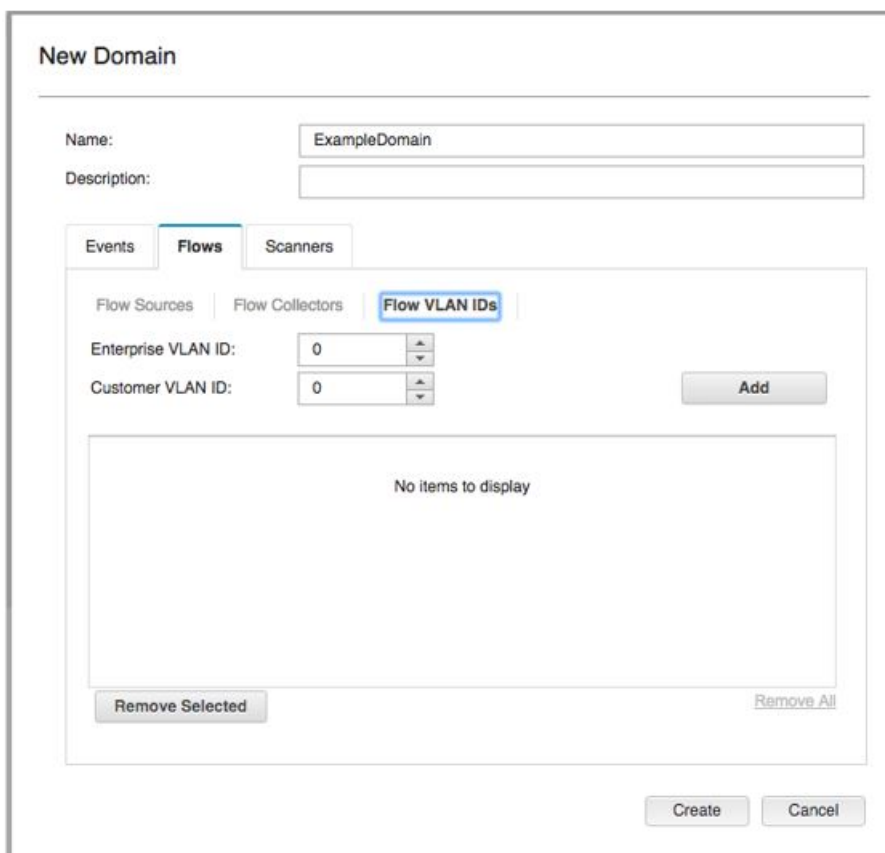


Figure 22. Créer domaine

6. Dans la zone **Nom**, entrez un nom unique pour le domaine, puis cliquez sur **Créer**.

**Résultats**

La définition du domaine est créée et les flux entrants sont mappés. L'affectation des titulaires à un domaine se déroule normalement.

| Name          | Flow VLAN IDs                   |
|---------------|---------------------------------|
| ExampleDomain | Enterprise: 500 ; Customer: 100 |

Figure 23. Définition de domaine créée

## Privilèges de domaine dérivés des profils de sécurité

Vous pouvez utiliser des profils de sécurité pour accorder des privilèges de domaine et veiller à ce que les restrictions de domaine soient respectées dans l'ensemble du système IBM QRadar. Les profils de sécurité permettent également de gérer plus facilement les privilèges d'un grand groupe d'utilisateurs lorsque vos besoins métier changent soudainement.

Les utilisateurs ne peuvent voir que les données dans les limites de domaine qui sont définies pour les profils de sécurité qui leur sont affectés. Les profils de sécurité incluent les domaines comme l'un des premiers critères évalués pour restreindre l'accès au système. Lorsqu'un domaine est affecté à un profil de sécurité, il prend la priorité sur les autres autorisations de sécurité. Une fois les restrictions de domaine évaluées, les profils de sécurité individuels sont évalués pour déterminer les autorisations de réseau et de journal pour ce profil particulier.

Par exemple, un utilisateur dispose de privilèges sur Domain\_2 et d'un accès au réseau 10.0.0.0/8. Cet utilisateur ne peut voir que les événements, les violations, les actifs et les flux provenant de Domain\_2 et qui contiennent une adresse du réseau 10.0.0.0/8.

En tant qu'administrateur QRadar, vous pouvez voir tous les domaines et vous pouvez affecter des domaines à des utilisateurs non administratifs. N'attribuez pas des privilèges d'administration aux utilisateurs que vous souhaitez limiter à un domaine particulier.

Les profils de sécurité doivent être mis à jour avec un domaine associé. Les restrictions de niveau domaine ne sont pas appliquées tant que la sécurité n'a pas été mise à jour et que les modifications n'ont pas été déployées.

Lorsque vous affectez des domaines à un profil de sécurité, vous pouvez accorder l'accès aux types de domaines suivants :

### Domaines définis par l'utilisateur

Vous pouvez créer des domaines basés sur des sources d'entrée à l'aide de l'outil de gestion de domaine. Pour plus d'informations, voir [Création de règles](#).

### Domaine par défaut

Tout ce qui n'est pas attribué à un domaine défini par l'utilisateur est automatiquement affecté au domaine par défaut. Le domaine par défaut contient des événements système.

**Remarque :** Les utilisateurs qui ont accès au domaine par défaut peuvent voir des événements à l'échelle du système sans restriction. Vérifiez que cet accès est acceptable avant d'affecter l'accès par domaine par défaut aux utilisateurs. Tous les administrateurs ont accès au domaine par défaut.

Toute source de journal qui est reconnue automatiquement sur un collecteur d'événements partagé (un collecteur qui n'est pas explicitement affecté à un domaine) est automatiquement reconnue dans le domaine par défaut. Ces sources de journal nécessitent une intervention manuelle. Pour identifier ces sources de journal, vous devez exécuter périodiquement une recherche dans le domaine par défaut qui est regroupé par source de journal.

### Tous les domaines

Les utilisateurs affectés à un profil de sécurité qui a accès à **Tous les domaines** peuvent voir tous les domaines actifs dans le système, le domaine par défaut et tous les domaines précédemment supprimés dans l'ensemble du système. Ils peuvent également voir tous les domaines qui sont créés à l'avenir.

**Important :** Si vous devez affecter un utilisateur à un profil de sécurité qui a un profil de domaine différent, supprimez le compte utilisateur et recréez-le.

Si vous supprimez un domaine, il ne peut pas être affecté à un profil de sécurité. Si l'utilisateur dispose de l'affectation **Tous les domaines** ou si le domaine a été affecté à l'utilisateur avant sa suppression, le domaine supprimé est renvoyé dans les résultats de la recherche d'historique pour les événements, flux, actifs et infractions. Vous ne pouvez pas filtrer par domaine supprimé lorsque vous exécutez une recherche.

Les administrateurs peuvent voir quels domaines sont affectés aux profils de sécurité dans l'onglet **Résumé** de la fenêtre **Gestion de domaine**.

## Modification des règles dans des environnements au niveau du domaine

Les règles peuvent être affichées, modifiées ou désactivées par tout utilisateur disposant des droits **Gestion des règles personnalisées** et **Afficher les règles personnalisées**, quel que soit le domaine auquel appartient l'utilisateur.

**Important :** Lorsque vous ajoutez la fonction **Activité de journal** à un rôle utilisateur, les droits **Gestion des règles personnalisées** et **Afficher les règles personnalisées** sont automatiquement accordés. Les utilisateurs disposant de ces droits ont accès à toutes les données de journal pour tous les domaines et peuvent éditer des règles dans tous les domaines, même si leurs paramètres de profil de sécurité ont des restrictions de niveau domaine. Pour empêcher les utilisateurs de domaine d'accéder aux données de journal et de modifier des règles dans d'autres domaines, modifiez le rôle utilisateur et supprimez les droits **Gestion des règles personnalisées** et **Afficher les règles personnalisées**.

## Recherches au niveau du domaine

Vous pouvez utiliser des domaines comme critères de recherche dans les recherches personnalisées. Votre profil de sécurité contrôle les domaines sur lesquels vous pouvez effectuer une recherche.

Les événements et événements à l'échelle du système qui ne sont pas affectés à un domaine défini par l'utilisateur sont automatiquement affectés au domaine par défaut. Les administrateurs ou les utilisateurs ayant un profil de sécurité donnant accès au domaine par défaut peuvent créer une recherche personnalisée pour afficher tous les événements qui ne sont pas affectés à un domaine défini par l'utilisateur.

L'administrateur de domaine par défaut peut partager une recherche enregistrée avec d'autres utilisateurs de domaine. Lorsque l'utilisateur de domaine exécute la recherche enregistrée, les résultats sont limités à leur domaine.

## Règles et infractions spécifiques au domaine

---

Une règle peut fonctionner dans le contexte d'un domaine unique ou dans le contexte de tous les domaines. Les règles de connaissance du domaine offrent l'option d'inclure le test **Et le domaine est**.

Le diagramme suivant illustre un exemple utilisant plusieurs domaines.

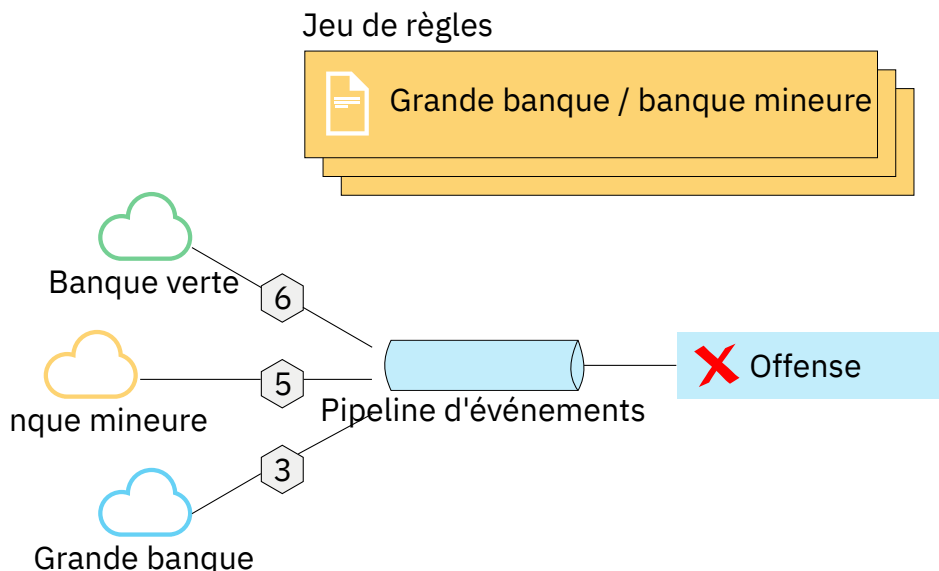


Figure 24. Règles de connaissance du domaine

Vous pouvez restreindre une règle de sorte qu'elle soit appliquée uniquement aux événements qui se produisent dans un domaine spécifié. Un événement qui comporte une balise de domaine différente du domaine qui est défini dans la règle ne déclenche pas une réponse d'événement.

Dans un système IBM QRadar qui n'a pas de domaines définis par l'utilisateur, une règle crée une violation et y contribue chaque fois que la règle se déclenche. Dans un environnement de connaissance de domaine, une règle crée une nouvelle infraction chaque fois que la règle est déclenchée dans le contexte d'un domaine différent.

Les règles qui fonctionnent dans le contexte de tous les domaines sont appelées règles à l'échelle du système. Pour créer une règle à l'échelle du système qui testant les conditions sur l'ensemble du système, sélectionnez **Tout domaine** dans la liste de domaines pour le test **Et le domaine est**. Une règle **Tout domaine** crée une infraction **Tout domaine**.

#### Règle de domaine unique

Si la règle est une règle avec état, les états sont conservés séparément pour chaque domaine. La règle est déclenchée séparément pour chaque domaine. Lorsque la règle est déclenchée, les infractions sont créées séparément pour chaque domaine impliqué et les infractions sont marquées avec ces domaines.

#### Infraction à domaine unique

L'infraction est marquée avec le nom de domaine correspondant. Il ne peut contenir que des événements marqués avec ce domaine.

#### Règle à l'échelle du système

Si la règle est une règle avec état, un état unique est maintenu pour l'ensemble du système et les balises de domaine sont ignorées. Lorsque la règle s'exécute, elle crée ou contribue à une infraction à l'échelle du système.

#### Infraction à l'échelle du système

L'infraction est balisée avec **Tout domaine**. Il contient uniquement les événements qui sont marqués avec tous les domaines.

Le tableau suivant fournit des exemples de règles de connaissance de domaine. Les exemples utilisent un système qui comporte trois domaines définis : Domain\_A, Domain\_B et Domain\_C.

Les exemples de règles du tableau suivant peuvent ne pas être applicables dans votre environnement QRadar. Par exemple, les règles qui utilisent des flux et des violations ne sont pas applicables dans IBM QRadar Log Manager.

Tableau 54. Règles de connaissance du domaine

| Texte du domaine                                                                                                                                                       | Explication                                                                                                                                                                                                                                                                                                                | Réponse à la règle                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>domaine est l'un des domaines suivants : Domain_A</b>                                                                                                               | Regarde uniquement les événements qui sont marqués avec Domain_A et ignore les règles qui sont marquées avec d'autres domaines.                                                                                                                                                                                            | Crée ou contribue à une infraction marquée avec Domain_A.                                                                                                                                                                                                                                                  |
| <b>domaine est l'un des domaines suivants : Domain_A et un test avec état qui est défini en tant que lorsque le flux HTTP est détecté 10 fois en 1 minute</b>          | Regarde uniquement les événements qui sont marqués avec Domain_A et ignore les règles qui sont marquées avec d'autres domaines.                                                                                                                                                                                            | Crée ou contribue à une infraction marquée avec Domain_A. Un seul état, un compteur de flux HTTP, est conservé pour Domain_A.                                                                                                                                                                              |
| <b>Domaine est l'un des domaines suivants : Domain_A, Domain_B</b>                                                                                                     | Regarde uniquement les événements qui sont marqués avec Domain_A et Domain_B et ignore les événements qui sont marqués avec Domain_C.<br><br>Cette règle se comporte comme deux instances indépendantes d'une règle de domaine unique et crée des infractions distinctes pour différents domaines.                         | Pour les données qui sont marquées avec Domain_A, elles créent ou contribuent à une infraction de domaine unique balisée avec Domain_A.<br><br>Pour les données qui sont marquées avec Domain_B, elles créent ou contribuent à une infraction de domaine unique balisée avec Domain_B.                     |
| <b>Domaine est l'un des domaines suivants: Domain_A, Domain_B et un test avec état qui est défini en tant que Lorsque le flux HTTP est détecté 10 fois en 1 minute</b> | Regarde uniquement les événements qui sont marqués avec Domain_A et Domain_B et ignore les événements qui sont marqués avec Domain_C.<br><br>Cette règle se comporte comme deux instances indépendantes d'une règle de domaine unique et gère deux états distincts (compteurs de flux HTTP) pour deux domaines différents. | Lorsque la règle détecte 10 flux HTTP marqués avec Domain_A en moins d'une minute, elle crée ou contribue à une infraction marquée avec Domain_A.<br><br>Lorsque la règle détecte 10 flux HTTP marqués avec Domain_B en moins d'une minute, elle crée ou contribue à une infraction marquée avec Domain_B. |
| Aucun test de domaine défini                                                                                                                                           | Recherche les événements qui sont marqués avec tous les domaines et qui créent ou contribuent à des infractions par domaine.                                                                                                                                                                                               | Chaque domaine indépendant comporte des infractions qui lui sont générées, mais les infractions ne contiennent pas de contributions provenant d'autres domaines.                                                                                                                                           |
| Une règle a un test avec état qui est défini comme <b>Lorsque le flux HTTP est détecté 10 fois en 1 minute</b> et aucun test de domaine n'est défini                   | Regarde les événements qui sont marqués avec Domain_A, Domain_B ou Domain_C.                                                                                                                                                                                                                                               | Maintient des états distincts et crée des infractions distinctes pour chaque domaine.                                                                                                                                                                                                                      |
| <b>Domaine est l'un des domaines suivants : Tout domaine</b>                                                                                                           | Il s'agit de tous les événements, quel que soit le domaine avec lequel il est étiqueté.                                                                                                                                                                                                                                    | Crée ou contribue à une infraction unique à l'échelle du système unique qui est marquée avec Any Domain.                                                                                                                                                                                                   |

Tableau 54. Règles de connaissance du domaine (suite)

| Texte du domaine                                                                                                                                                         | Explication                                                                                                                                   | Réponse à la règle                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domaine est l'un des domaines suivants : Tout domaine</b> et un test avec état qui est défini en tant que <b>Lorsque le flux HTTP est détecté 10 fois en 1 minute</b> | Il s'agit de tous les événements, quel que soit le domaine avec lequel il est étiqueté, et il conserve un état unique pour tous les domaines. | Crée ou contribue à une infraction unique à l'échelle du système unique qui est marquée avec Any Domain.<br><br>Par exemple, s'il détecte 3 événements qui sont marqués avec Domain_A, 3 événements qui sont marqués avec Domain_Bet 4 événements qui sont marqués avec Domain_C en moins d'une minute, il crée une infraction car il a détecté 10 événements au total. |
| <b>Domain est l'un des domaines suivants : Tout domaine, Domain_A</b>                                                                                                    | Fonctionnait de la même manière qu'une règle ayant <b>Domaine est l'un des domaines suivants : Tout domaine</b> .                             | Lorsque le test de domaine inclut Any Domain, tous les domaines uniques qui sont répertoriés sont ignorés.                                                                                                                                                                                                                                                              |

Lorsque vous affichez la table de violation, vous pouvez trier les infractions en cliquant sur la colonne **Domaine**. Le **Domaine par défaut** n'est pas inclus dans la fonction de tri, de sorte qu'il n'apparaît pas dans l'ordre alphabétique. Toutefois, il apparaît en haut ou en bas de la liste **Domaine**, selon que la colonne est triée par ordre croissant ou décroissant. **Tout domaine** n'apparaît pas dans la liste des infractions?

## Exemple : affectations de privilèges de domaine basées sur des propriétés personnalisées

Si vos fichiers journaux contiennent des informations que vous souhaitez utiliser dans une définition de domaine, vous pouvez exposer les informations en tant que propriété d'événement personnalisé.

Vous affectez une propriété personnalisée à un domaine en fonction des résultats de la capture. Vous pouvez affecter la même propriété personnalisée à plusieurs domaines, mais les résultats de capture doivent être différents.

Par exemple, une propriété d'événement personnalisée, telle que userID, peut être évaluée à un utilisateur unique ou à une liste d'utilisateurs. Chaque utilisateur ne peut appartenir qu'à un seul domaine.

Dans le diagramme suivant, les sources de journal contiennent des informations d'identification de l'utilisateur qui sont exposées comme une propriété personnalisée, userID. Le collecteur d'événements renvoie deux fichiers utilisateur et chaque utilisateur est affecté à un seul domaine. Dans ce cas, un utilisateur est affecté au domaine : 9 et l'autre utilisateur est affecté au domaine : 12.

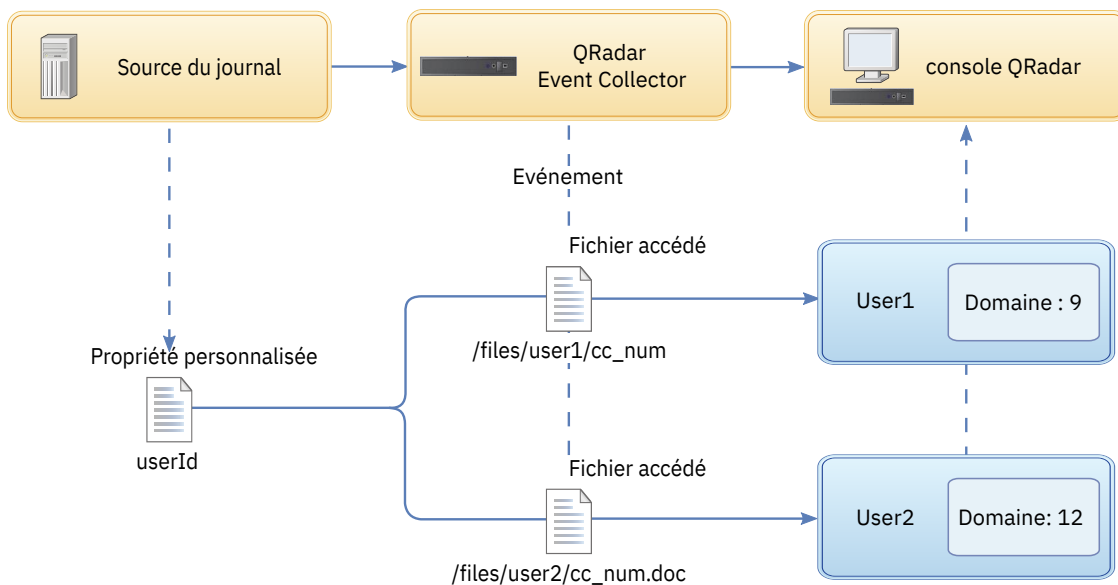


Figure 25. Affectation de domaines à l'aide d'une propriété d'événement personnalisée

Si les résultats de capture renvoient un utilisateur qui n'est pas affecté à un domaine défini par l'utilisateur spécifique, cet utilisateur est automatiquement affecté au domaine par défaut. Les affectations de domaine par défaut nécessitent une intervention manuelle. Effectuez des recherches périodiques pour vous assurer que toutes les entités du domaine par défaut sont correctement affectées.

**Important :** Avant d'utiliser une propriété personnalisée dans une définition de domaine, vérifiez que **Optimisation de l'analyse pour les règles, les rapports et les recherches** est coché dans la fenêtre **Propriétés de l'événement personnalisé**. Cette option garantit que la propriété d'événement personnalisé est analysée et stockée lorsque IBM QRadar reçoit l'événement pour la première fois. La segmentation de domaine ne se produit pas si cette option n'est pas sélectionnée.





## Chapitre 17. Gestion à service partagé

Les environnements à service partagé permettent aux fournisseurs MSSP (Managed Security Service Providers) et aux organisations multi-division de fournir des services de sécurité à plusieurs organisations clientes à partir d'un déploiement IBM QRadar unique et partagé. Vous n'avez pas à déployer une instance QRadar unique pour chaque client.

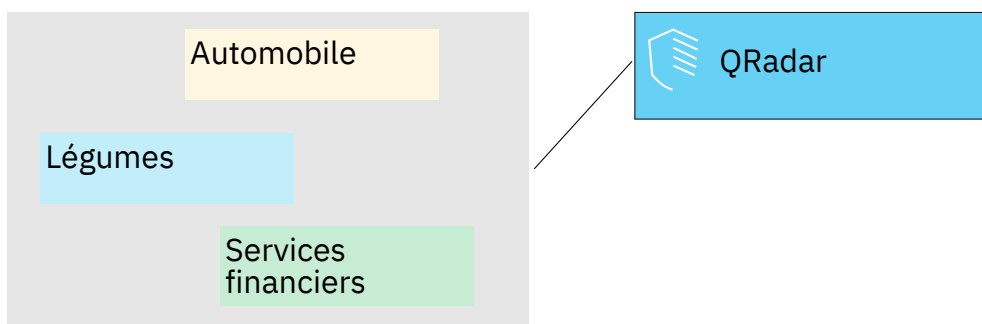
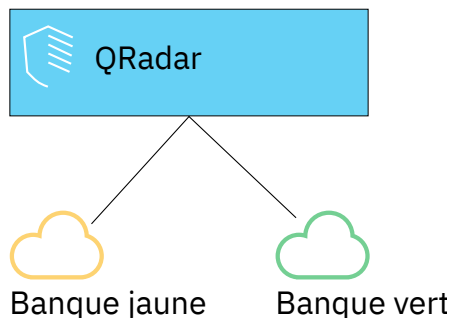


Figure 26. environnement multilocataire

Dans un environnement à service partagé, vous garantissez que les clients voient uniquement leurs données en créant des domaines qui sont basés sur les sources d'entrée QRadar. Utilisez ensuite des profils de sécurité et des rôles utilisateur pour gérer les privilèges de grands groupes d'utilisateurs au sein du domaine. Les profils de sécurité et les rôles utilisateur garantissent que les utilisateurs ont accès uniquement aux informations qu'ils sont autorisés à consulter.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Rôles utilisateur dans un environnement multilocataires

Les environnements multilocataires comprennent un fournisseur de services et plusieurs locataires. Chaque rôle a des responsabilités distinctes et des activités associées.

### Fournisseur de services

Le fournisseur de services est propriétaire du système et gère son utilisation par plusieurs locataires. Le fournisseur de services peut consulter les données de tous les locataires. L'administrateur du fournisseur de services de sécurité géré (MSSP) est généralement responsable des activités suivantes :

- Administrer et surveiller la santé système du déploiement IBM QRadar.
- Approvisionner les nouveaux locataires.
- Créer des rôles et des profils de sécurité pour les administrateurs et les utilisateurs locataires.

- Garantir le système contre un accès non autorisé.
- Créer des domaines pour isoler les données des locataires.
- Déployer les modifications effectuées par l'administrateur locataire dans l'environnement locataire.
- Surveiller les licences QRadar.
- Collaborer avec l'administrateur locataire.

## Titulaires

Chaque location comprend un administrateur locataire et des utilisateurs locataires. L'administrateur locataire peut être un employé de l'organisation locataire, ou le fournisseur de services peut administrer le locataire pour le compte du client.

L'administrateur locataire est responsable des activités suivantes :

- Configurer les définitions de la [hiérarchie de réseau](#) dans sa propre location.
- Configurer et gérer les données des locataires.
- Afficher les sources du journal.
- Collaborer avec l'administrateur MSSP.

L'administrateur locataire peut configurer des déploiements spécifiques aux locataires, mais ils ne peuvent pas y accéder ou modifier la configuration d'un autre locataire. Ils doivent contacter l'administrateur MSSP pour déployer les modifications dans l'environnement QRadar, y compris les changements de hiérarchie de réseau au sein de leur propre locataire.

Les utilisateurs locataires n'ont pas de privilèges d'administration et ne peuvent voir que les données auxquelles ils ont accès. Par exemple, un utilisateur peut disposer de privilèges pour afficher des données à partir d'une seule source de journal dans un domaine disposant de plusieurs sources de journal.

## Domaines et sources de journal dans des environnements multilocataires

---

Utilisez des domaines pour séparer les adresses IP qui se chevauchent et pour affecter des sources de données, telles que des événements et des flux, à des ensembles de données spécifiques aux locataires.

Lorsque des événements ou des flux entrent dans IBM QRadar, QRadar évalue les définitions de domaine qui sont configurées, et les événements et les flux sont affectés à un domaine. Un locataire peut avoir plusieurs domaines. Si aucun domaine n'est configuré, les événements et les flux sont affectés au domaine par défaut.

### Segmentation de domaine

Les domaines sont des compartiments virtuels permettant de séparer les données en fonction de la source de données. Ce sont les blocs de construction des environnements multilocataires. Vous configurez des domaines à partir des sources d'entrée suivantes :

- Collecteurs d'événements et de flux
- Sources de flux
- Sources de journal et groupes de sources de journal
- Propriétés personnalisées
- Scanners

Un déploiement multilocataires peut consister en une configuration matérielle de base comprenant une console QRadar, un processeur d'événements centralisé, puis un collecteur d'événements pour chaque client. Dans cette configuration, vous définissez des domaines au niveau du collecteur, qui affecte ensuite automatiquement les données reçues par QRadar dans un domaine.

Pour consolider encore la configuration matérielle, vous pouvez utiliser un collecteur pour plusieurs clients. Si les sources de journal ou de flux sont agrégées par le même collecteur mais appartiennent à des locataires différents, vous pouvez affecter les sources à différents domaines. Lorsque vous utilisez des définitions de domaine au niveau de la source de journal, chaque nom de source de journal doit être unique pour l'ensemble du déploiement QRadar.

Si vous devez séparer les données d'une source de journal unique et les affecter à différents domaines, vous pouvez configurer des domaines à partir de propriétés personnalisées. QRadar recherche la propriété personnalisée dans le contenu et l'affecte au domaine approprié. Par exemple, si vous avez configuré QRadar pour l'intégrer à une unité Provider-1 Check Point, vous pouvez utiliser des propriétés personnalisées pour affecter les données de cette source de journal à différents domaines.

## Détection automatique des sources de journal

Lorsque des domaines sont définis au niveau du collecteur et que le collecteur d'événements dédié est affecté à un domaine unique, les nouvelles sources de journal qui sont automatiquement détectées sont affectées à ce domaine. Par exemple, toutes les sources de journal détectées sur `Event_Collector_1` sont affectées à `Domain_A`. Toutes les sources de journal qui sont automatiquement collectées sur `Event_Collector_2` sont affectées à `Domain_B`.

Lorsque des domaines sont définis au niveau de la source de journal ou de la propriété personnalisée, les sources de journal qui sont automatiquement détectées et qui ne sont pas déjà affectées à un domaine sont automatiquement affectées au domaine par défaut. L'administrateur MSSP doit examiner les sources de journal dans le domaine par défaut et les allouer aux domaines client corrects. Dans un environnement multilocataires, l'affectation de sources de journal à un domaine spécifique empêche les fuites de données et impose la séparation des données entre les domaines.

## Mettre en place un nouveau titulaire

---

En tant qu'administrateur MSSP (Managed Security Services Provider), vous utilisez une seule instance de IBM QRadar pour fournir à plusieurs clients une architecture unifiée pour la détection des menaces et la hiérarchisation des priorités.

Dans ce scénario, vous intégrez un nouveau client. Vous mettez à disposition un nouveau locataire et créez un compte administrateur locataire qui effectue des tâches administratives limitées au sein de son propre locataire. Vous limitez l'accès de l'administrateur locataire afin qu'il ne puisse pas voir ou modifier des informations dans d'autres locataires.

Avant de fournir un nouveau titulaire, vous devez créer les sources de données, telles que les sources de journal ou les collecteurs de flux, pour le client et les affecter à un domaine.

Effectuez les tâches suivantes à l'aide des outils de l'onglet **Admin** pour fournir le nouveau titulaire dans QRadar :

1. Pour créer le titulaire, cliquez sur **Gestion des locataires**.

Pour plus d'informations sur la définition des événements par seconde (EPS) et les limites de flux par minute (FPM) pour chaque titulaire, voir [«Surveillance de l'utilisation de la licence dans les déploiements à service partagé»](#), à la page 270.

2. Pour affecter des domaines au locataire, cliquez sur **Gestion de domaine**.
3. Pour créer le rôle d'administrateur locataire et accorder les droits **Administration déléguée**, cliquez sur **Rôles utilisateur**.

Dans un environnement multilocataires, les utilisateurs locataires disposant de droits **Administration déléguée** ne peuvent voir que les données de leur propre environnement locataire. Si vous affectez d'autres droits d'administration qui ne font pas partie de **Administration déléguée**, l'accès n'est plus limité à ce domaine.

4. Pour créer les profils de sécurité des locataires et restreindre l'accès aux données en spécifiant les domaines locataires, cliquez sur **Profils de sécurité**.

5. Pour créer les utilisateurs du titulaire et affecter le rôle utilisateur, le profil de sécurité et le titulaire, cliquez sur **Utilisateurs**.

## Surveillance de l'utilisation de la licence dans les déploiements à service partagé

---


En tant qu'administrateur MSSP (Managed Security Service Provider), vous surveillez les débits d'événements et de flux sur l'ensemble du déploiement IBM QRadar.

Lorsque vous créez un titulaire, vous pouvez définir des limites tant pour le nombre d'événements par seconde (EPS) que pour les flux par minute (FPM). En spécifiant des limites EPS et FPM pour chaque titulaire, vous pouvez mieux gérer les capacités de licence entre les divers clients. Si votre processeur collecte des événements ou des flux pour un seul client, vous n'avez pas besoin d'affecter des limites EPS et FPM au titulaire. Si vous avez un seul processeur collectant des événements ou des flux pour plusieurs clients, vous pouvez définir des limites EPS et FPM pour chaque titulaire.

Si vous attribuez aux limites EPS et FPM des valeurs excédant les capacités de vos licences logicielles ou du matériel du dispositif, le système ajuste automatiquement les événements et les flux pour ce titulaire de sorte à respecter ces capacités. Si vous ne définissez pas de limites EPS et FPM pour les titulaires, chaque titulaire reçoit des événements et des flux jusqu'à ce que les limites de la licence ou du dispositif soient atteintes. Les limites de licence sont appliquées à l'hôte géré. Si vous dépassez régulièrement les limites de licence, vous pouvez acquérir une licence différente mieux adaptée à votre déploiement.

### Consultation des limites de licence cumulées dans votre déploiement

Les plafonds EPS et FPM que vous affectez à chaque titulaire ne sont pas validés automatiquement vis à vis des licences qui vous ont été octroyées. Pour examiner les limites cumulées pour les licences logicielles qui sont appliquées au système par rapport aux limites du matériel du dispositif, procédez comme suit :

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet admin.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Développez **Détails du déploiement** et placez le pointeur de la souris sur **Limite d'événement** ou **Limite de flux**.

### Affichage des taux EPS par source de journal

Utilisez la zone **Recherche avancée** pour entrer une requête AQL (Ariel Query Language) pour afficher les taux EPS pour les sources de journal.

1. Dans l'onglet **Activité de journal**, sélectionnez **Recherche avancée** dans la liste de la barre d'outils **Rechercher**.
2. Pour afficher l'EPS par source de journal, entrez la requête AQL suivante dans la zone **Recherche avancée** :

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by logsourceid
order by EPS desc
last 24 hours
```

### Affichage des taux EPS par domaine

Utilisez la zone **Recherche avancée** pour entrer une requête AQL (Ariel Query Language) pour afficher les taux EPS pour les domaines.

1. Dans l'onglet **Activité du journal**, sélectionnez **Recherche avancée** dans la liste déroulante sur la barre d'outils **Rechercher**.


2. Pour afficher le serveur EPS par domaine, entrez la requête AQL suivante dans la zone **Recherche avancée** :

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by domainid
order by EPS desc
last 24 hours
```

Si vous souhaitez afficher les taux d'EPS moyens pour les sources de journal uniquement, cliquez sur **Sources de journal** dans la sous-fenêtre **Sources de données** de l'onglet **Admin**. Vous pouvez utiliser cette méthode pour identifier rapidement des problèmes de configuration de sources de données ne générant pas de rapports.

## Affichage des limites de licence individuelles dans votre déploiement

Les plafonds EPS et FPM que vous affectez à chaque titulaire ne sont pas validés automatiquement vis à vis des licences qui vous ont été octroyées. Pour afficher les limites individuelles des licences logicielles appliquées au système par rapport aux limites matérielles du dispositif, procédez comme suit :

1. Dans le menu de navigation () , cliquez sur **Admin** pour ouvrir l'onglet admin.
2. Dans la section **Configuration système**, cliquez sur **Gestion du système et de la licence**.
3. Développez **Détails du déploiement** et survolez avec le curseur **Limite d'événements** ou **Limite de flux**.

## Affichage du taux EPS pour une source de journal individuelle

Utilisez la zone **Recherche avancée** pour entrer une requête AQL (Ariel Query Language) pour afficher le taux EPS d'une source de journal individuelle.

1. Dans l'onglet **Activité de journal**, sélectionnez **Recherche avancée** dans la liste de la barre d'outils **Rechercher**.
2. Pour obtenir un ID de source de journal, entrez la requête AQL suivante dans la zone **Recherche avancée** :

```
select domainid,logsourceid,LOGSOURCENAME(logsourceid) from events GROUP BY
domainid,logsourceid order by domainid ASC last 1 HOURS
```

3. Pour afficher le taux EPS de votre source de journal sélectionnée, entrez la requête AQL suivante dans la zone **Recherche avancée** :

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) / 24*60*60 as EPS from
events
where logsourceid=logsourceid
group by logsourceid
order by EPS desc
last 24 hours
```

## Affichage du taux EPS pour un domaine individuel

La zone **Recherche avancée** permet d'entrer une requête AQL (Ariel Query Language) pour afficher le taux EPS d'un domaine individuel.

1. Dans l'onglet **Activité de journal**, sélectionnez **Recherche avancée** dans la liste de la barre d'outils **Rechercher**.
2. Pour obtenir un ID de domaine, entrez la requête AQL suivante dans la zone **Recherche avancée** :

```
select domainid, DOMAINNAME(domainid) from events GROUP BY domainid last 1 HOURS
```

3. Pour afficher le taux EPS de votre domaine sélectionné, entrez la requête AQL suivante dans la zone **Recherche avancée** :

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
where domainid=domainid
group by domainid
order by EPS desc
last 24 hours
```

## Détection d'événements et de flux supprimés

Les événements et les flux sont supprimés lorsque le pipeline de traitement IBM QRadar ne peut pas gérer le volume des événements et flux entrants, ou lorsque le nombre d'événements et de flux dépasse les limites de licence de votre déploiement. Vous pouvez consulter les messages du fichier journal QRadar lorsque ces situations se produisent.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Affichez le fichier journal `/var/log/qradar.error` et recherchez ces messages :

Ces messages indiquent que les événements ou les flux ont été supprimés :

```
[Titulaire:[IDdutilitaire]:[Nomdutilitaire]
Événement a été supprimé lors de la tentative d'ajout à la file d'attente Régulateur
d'Événement de Titulaire.
La file d'attente de régulation des événements du locataire est pleine.
```

```
[Titulaire:[IDdutilitaire]:[Nomdutilitaire]
Le flux a été supprimé lors de la tentative d'ajout à la file d'attente Régulateur de Flux de
Titulaire.
La file d'attente de régulation de flux du locataire est pleine.
```

Ces messages indiquent que le pipeline de traitement était près de la capacité :

```
Le processeur de régulation ne peut pas suivre les événements.
TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC est probablement trop court.
```

```
Le processeur de régulation ne peut pas suivre les flux.
TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC est probablement trop court.
```

Si cet avertissement persiste, QRadar peut supprimer des événements ou des flux.

### Que faire ensuite

Si votre système supprime des événements et des flux, vous pouvez développer votre licence pour gérer plus de données ou vous pouvez définir des limites EPS et FPM plus restrictives pour chaque titulaire.

## Gestion des règles dans les déploiements multilocataires

Dans un environnement multilocataires, vous devez personnaliser les règles pour les rendre conscients des locataires. Les règles conscientes utilisent le test de règle **lorsque le domaine est l'un des tests de règles suivants**, mais le modificateur de domaine détermine la portée de la règle.

Le tableau suivant montre comment utiliser le modificateur de domaine pour modifier la portée des règles dans un déploiement multilocataires.

| Portée de la règle       | Description                                              | Exemple de test de règle                                                |
|--------------------------|----------------------------------------------------------|-------------------------------------------------------------------------|
| Règles de domaine unique | Ces règles ne comprennent que 1 modificateur de domaine. | <b>et lorsque le domaine est l'un des suivants</b> : <i>fabrication</i> |

Tableau 55. Portée des règles dans un environnement multilocataires (suite)

| Portée de la règle         | Description                                                                                                                                                                                        | Exemple de test de règle                                                                     |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Règles de locataire unique | Ces règles incluent tous les domaines qui sont affectés au locataire. Utilisez des règles de locataire unique pour corrélérer des événements entre plusieurs domaines au sein d'un seul locataire. | <b>et lorsque le domaine est l'un des suivants :</b> <i>fabrication, finances, juridique</i> |
| Règles globales            | Ces règles utilisent le modificateur <b>Tout domaine</b> et s'exécutent sur tous les locataires.                                                                                                   | <b>et lorsque le domaine est l'un des suivants :</b> <i>tout domaine</i>                     |

En étant conscient du domaine, le moteur de règles personnalisées (CRE) isole automatiquement les corrélations d'événements de différents locataires en utilisant leurs domaines respectifs. Pour plus d'informations sur l'utilisation des règles dans un réseau segmenté par domaine, voir [Chapitre 16](#), «Segmentation de domaine», à la page 253.

## Restriction des fonctions d'activité de journal pour les utilisateurs locataires


Pour vous assurer que l'administrateur locataire et les utilisateurs peuvent afficher les données du journal uniquement pour leur titulaire, vous devez restreindre les droits d'accès pour la fonction **Activité de journal**.

### Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez la fonction **Activité de journal** à un rôle utilisateur, les droits **Gestion des règles personnalisées** et **Afficher les règles personnalisées** sont automatiquement accordés. Les utilisateurs disposant de ces droits ont accès à toutes les données de journal pour tous les domaines. Ils peuvent éditer des règles dans tous les domaines, même si leurs paramètres de profil de sécurité ont des restrictions de niveau domaine.

Pour empêcher les utilisateurs d'accéder aux données du journal et de modifier des règles dans d'autres domaines ou locataires, modifiez le rôle utilisateur et supprimez les droits **Gestion des règles personnalisées** et **Afficher les règles personnalisées**. Sans ces droits, l'administrateur du locataire et les utilisateurs ne peuvent pas modifier les règles, y compris les règles dans leur domaine.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Rôles utilisateur** et sélectionnez le rôle utilisateur que vous souhaitez modifier.
3. Sous **Activité de journal**, désélectionnez les cases à cocher **Gestion des règles personnalisées** et **Afficher les règles personnalisées**.
4. Cliquez sur **Sauvegarder**.

## Mises à jour de la hiérarchie de réseau dans un déploiement multilocataires

IBM QRadar utilise la hiérarchie réseau pour comprendre et analyser le trafic réseau dans votre environnement. Les administrateurs de locataires qui ont le droit **Définir une hiérarchie de réseau** peuvent modifier la hiérarchie du réseau au sein de leur propre locataire.

Les modifications de la hiérarchie de réseau nécessitent un déploiement de configuration complet pour appliquer les mises à jour dans l'environnement QRadar. Les déploiements de configuration

complets redémarrent tous les services QRadar, et les recueils de données pour les événements et les flux s'arrêtent jusqu'à la fin du déploiement. Les administrateurs du locataire doivent contacter l'administrateur du fournisseur de services de sécurité géré (MSSP) pour déployer les modifications. Les administrateurs MSSP peuvent planifier le déploiement lors d'une interruption planifiée et informer à l'avance tous les administrateurs de locataires.

Dans un environnement multilocataires, le nom d'objet réseau doit être unique pour l'ensemble du déploiement. Vous ne pouvez pas utiliser des objets réseau portant le même nom, même s'ils sont affectés à des domaines différents.

### **Concepts associés**

#### Hiérarchie du réseau

IBM QRadar utilise les objets et les groupes de hiérarchie de réseau pour afficher l'activité réseau et surveiller les groupes ou les services de votre réseau.

## **Règles de conservation des locataires**

---

Vous pouvez configurer jusqu'à 10 compartiments de conservation pour des données partagées et jusqu'à 10 compartiments de conservation pour chaque titulaire. La période de conservation par défaut est de 30 jours, puis les données du locataire sont automatiquement supprimées. Pour conserver les données du locataire pendant plus de 30 jours, vous devez configurer un compartiment de conservation. Jusqu'à ce que vous configuriez un compartiment de conservation, tous les événements ou flux sont stockés dans le compartiment de conservation par défaut de chaque titulaire.

Si votre déploiement QRadar compte plus de 10 locataires, vous pouvez configurer une règle de conservation des données partagées et utiliser le filtre de domaine pour créer une règle de conservation basée sur le domaine pour chacun des domaines du titulaire. L'ajout des domaines indique que la règle s'applique uniquement aux données de ce titulaire.

### **Concepts associés**

#### Conservation des données



---

## Chapitre 18. Gestion des actifs

Les actifs et les profils d'actifs créés pour les serveurs et les hôtes de votre réseau fournissent des informations importantes pour vous aider à résoudre les problèmes de sécurité. À l'aide des données d'actif, vous pouvez connecter des infractions qui sont déclenchées dans votre système à des actifs physiques ou virtuels pour fournir un point de départ dans une enquête de sécurité.

L'onglet **Actifs** de IBM QRadar fournit une vue unifiée des informations connues sur les actifs de votre réseau. Lorsque QRadar détecte plus d'informations, le système met à jour le profil d'actif et génère une image complète de l'actif.

Les profils d'actif sont générés dynamiquement à partir des informations d'identité qui sont absorbées passivement à partir des données d'événement ou de flux, ou à partir de données que QRadar recherche activement lors d'une analyse de vulnérabilité. Vous pouvez également importer les données d'actif ou éditer le profil d'actif manuellement. Pour plus d'informations, voir les rubriques *Importation de profils d'actif* et *Ajout ou édition d'un profil d'actif* dans *IBM QRadar - Guide d'utilisation*.

**Restriction :** IBM QRadar Log Manager suit uniquement les données d'actif si IBM QRadar Vulnerability Manager est installé. Pour plus d'informations sur les différences entre QRadar SIEM et QRadar Log Manager, voir [«Fonctions de votre produit IBM QRadar»](#), à la page 7.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Sources des données d'actif

Les données d'actif sont reçues de plusieurs sources différentes dans votre déploiement IBM QRadar.

Les données d'actif sont écrites dans la base de données d'actifs de manière incrémentielle, généralement par incréments de 2 ou 3 données à la fois. À l'exception des mises à jour à partir de scanners de vulnérabilité du réseau, chaque mise à jour d'actifs contient des informations sur un seul actif à la fois.

Les données d'actifs proviennent généralement de l'une des sources de données d'actifs suivantes :

### Événements

Les contenus d'événements, tels que ceux créés par les serveurs DHCP ou d'authentification, contiennent souvent des connexions d'utilisateurs, des adresses IP, des noms d'hôte, des adresses MAC et d'autres informations d'actifs. Ces données sont immédiatement transmises à la base de données d'actifs pour aider à déterminer à quel actif la mise à jour d'actif s'applique.

Les événements sont la principale cause des écarts de croissance d'actifs.

### Flux

Les contenus de flux contiennent des informations de communication telles que l'adresse IP, le port et le protocole qui sont collectées au cours d'intervalles configurables, réguliers. À la fin de chaque intervalle, les données sont fournies à la base de données d'actifs, une adresse IP à la fois.

Étant donné que les données d'actifs provenant des flux sont jumelées avec un actif sur la base d'un identifiant unique, l'adresse IP, les données de flux ne sont jamais la cause d'écarts de croissance d'actifs.

**Important :** La génération d'actifs à partir de flux IPv6 n'est pas prise en charge.

### Programmes d'analyse des vulnérabilités

QRadar s'intègre aux scanners de vulnérabilité IBM et d'autres marques pouvant fournir des données d'actifs telles que le système d'exploitation, les logiciels installés et les informations sur les correctifs. Le type de données varie d'un scanner à l'autre et peut également varier d'une analyse à l'autre. Au fur et à mesure que de nouveaux actifs, informations de port, et vulnérabilités sont découverts, les données sont introduites dans le profil de l'actif sur la base des plages CIDR qui sont définies dans l'analyse.

Certains scanners peuvent intégrer des écarts de croissance d'actifs mais cela est rare.

### **Interface utilisateur**

Les utilisateurs qui disposent du rôle Actifs peuvent importer ou fournir des informations sur les actifs directement vers la base de données d'actifs. Les mises à jour d'actifs fournis directement par un utilisateur concernent un actif spécifique. Par conséquent, la phase de rapprochement des actifs est ignorée.

Les mises à jour d'actifs qui sont fournies par les utilisateurs n'introduisent pas d'écarts de croissance d'actifs.

### **Données d'actifs de domaine**

Quand une source de données d'actifs est configurée avec les informations de domaine, toutes les données d'actifs qui proviennent de cette source de données sont automatiquement marquées avec le même domaine. Etant donné que les données dans le modèle d'actif sont compatibles avec le domaine, les informations de domaine sont appliquées à tous les composants QRadar y compris les identités, les infractions, les profils d'actifs, et la découverte de serveur.

Lorsque vous affichez le profil d'actifs, certaines zones peuvent être vides. Des zones vides existent lorsque le système n'a pas reçu ces informations dans une mise à jour d'actifs, ou lorsque les informations ont dépassé la période de rétention des actifs. La période de rétention par défaut est de 120 jours. Une adresse IP qui apparaît comme 0.0.0.0 indique que l'actif ne contient pas d'information de l'adresse IP.

## **Flux des données d'actifs entrantes**

---

IBM QRadar utilise les informations d'identité d'un contenu d'événement afin de déterminer si un nouvel actif doit être créé ou si un actif existant doit être mis à jour.

**Important :** La génération d'actifs à partir de flux IPv6 n'est pas prise en charge.

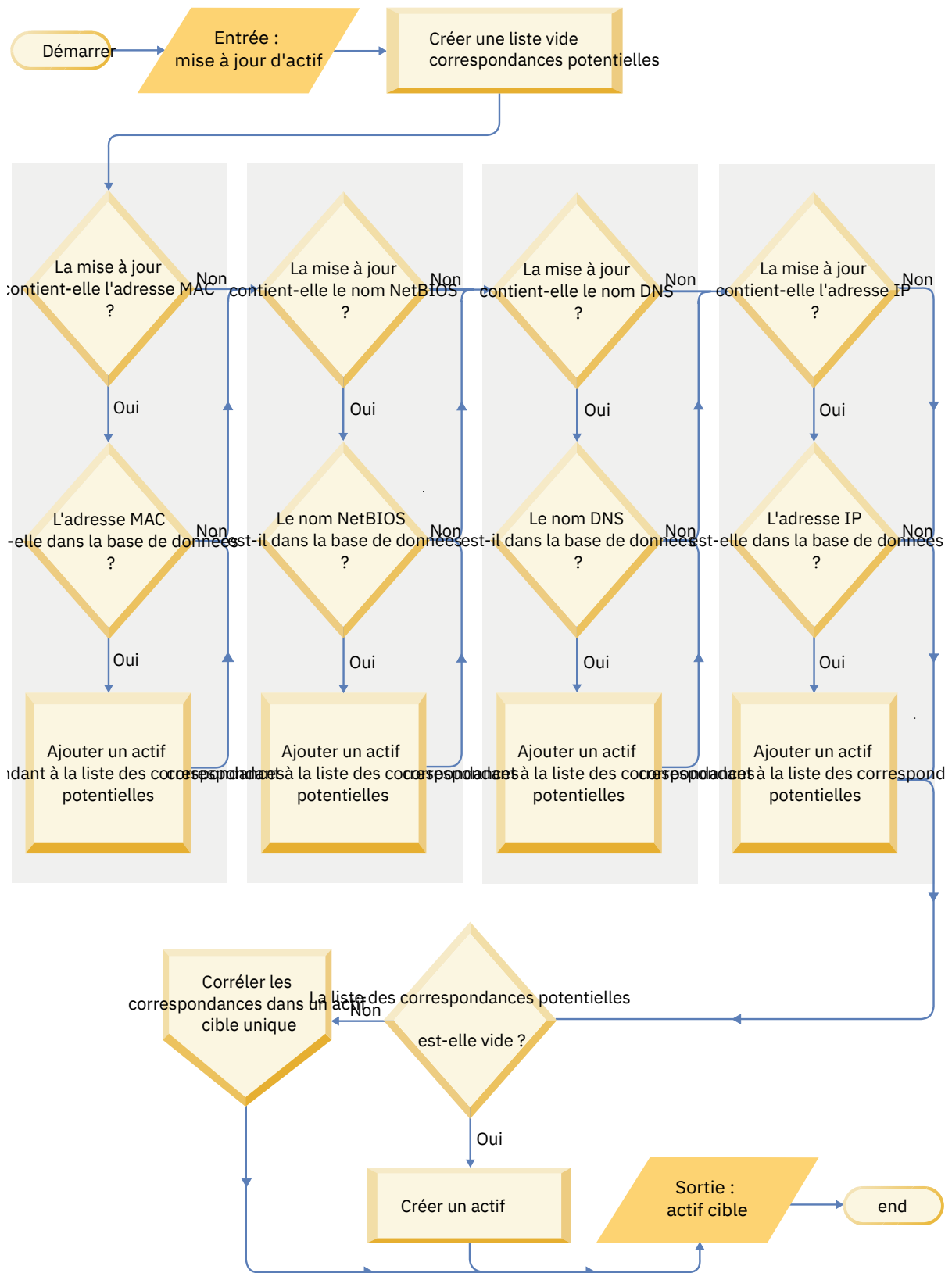


Figure 27. Graphique des flux de données d'actifs

1. QRadar reçoit l'événement. Le profileur d'actifs examine le contenu d'événement pour obtenir des informations d'identité.

2. Si les informations d'identité incluent une adresse MAC, un nom d'hôte NetBIOS ou un nom d'hôte DNS déjà associé à un actif dans la base de données des actifs, cet actif est mis à jour pour inclure les nouvelles informations.
3. Si les seules informations d'identité disponibles sont une adresse IP, le système rapproche la mise à jour de l'actif existant qui a la même adresse IP.
4. Si une mise à jour d'actif contient une adresse IP qui correspond à un actif existant mais les informations d'identité ne correspondent pas, le système utilise d'autres informations pour exclure une correspondance de faux positif avant de mettre à jour l'actif existant.
5. Si les informations d'identité ne correspondent pas à un actif existant dans la base de données, un nouvel actif est créé conformément aux informations du contenu d'événement.

## Mises à jour des données d'actifs

---

IBM QRadar utilise les informations d'identité d'un contenu d'événement afin de déterminer si un nouvel actif doit être créé ou si un actif existant doit être mis à jour.

Chaque mise à jour d'actifs doit contenir des informations fiables au sujet d'un actif unique. Lorsque QRadar reçoit une mise à jour d'actif, le système détermine l'actif auquel s'applique la mise à jour.

Le *rapprochement d'actifs* est le processus de détermination de la relation entre les mises à jour d'actifs et l'actif connexe dans la base d'actifs. Le rapprochement d'actifs survient après que QRadar reçoit la mise à jour, mais avant que les informations sont écrites dans la base de données d'actifs

### Informations d'identité

Chaque actif doit contenir au moins une donnée d'identité. Les mises à jour ultérieures qui contiennent une ou plusieurs de ces mêmes données d'identité sont rapprochées avec l'actif qui possède ces données. Les mises à jour qui sont basées sur les adresses IP sont manipulées avec précaution pour éviter les correspondances d'actifs faux positifs. Les correspondances d'actifs constituant des faux positifs se produisent lorsqu'un actif physique devient propriétaire d'une adresse IP qui appartenait auparavant à un autre actif du système.

Lorsque plusieurs données d'identités sont fournies, le profileur d'actif classe les informations par ordre de priorité, de la plus déterminante à la moins déterminante, dans l'ordre suivant :

- Adresse MAC
- Nom d'hôte NetBIOS
- Nom d'hôte DNS
- Adresse IP

Les adresses MAC, les noms d'hôte NetBIOS et les noms d'hôte DNS sont uniques et sont par conséquent considérés comme des données d'identité définitives. Les mises à jour entrantes qui correspondent à un actif existant seulement par l'adresse IP sont gérées différemment des mises à jour qui correspondent à des données d'identité plus définitives.

## Règles d'exclusion de rapprochement d'actifs

Avec chaque mise à jour d'actifs qui entre dans IBM QRadar, les règles d'exclusion de rapprochement d'actifs effectuent des tests sur l'adresse MAC, le nom d'hôte NetBIOS, le nom d'hôte DNS et l'adresse IP dans la mise à jour d'actifs.

Par défaut, chaque donnée d'actif est suivie sur une période de deux heures. Si une donnée d'identité dans la mise à jour d'actifs présente un comportement suspect deux fois ou plus dans les 2 heures, cette donnée est ajoutée aux listes noires d'actifs. Chaque type de données d'actif d'identité testé génère une nouvelle liste noire.

**Conseil :** QRadar exclut les événements en fonction des données reçues dans l'événement, et non en fonction des données ultérieurement déduites de l'événement ou liées à ce dernier.

Dans les environnements de domaine, les règles d'exclusion de rapprochement d'actifs suivent le comportement des données d'actifs séparément pour chaque domaine.

Les règles d'exclusion de rapprochement des actifs testent les scénarios suivants :

| <i>Tableau 56. Tests de règle et réponses</i>                                                           |                                                                                             |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Scénario</b>                                                                                         | <b>Réponse à la règle</b>                                                                   |
| Quand une adresse MAC est associée à trois adresses IP différentes ou plus en 2 heures ou moins         | Ajoutez l'adresse MAC à la liste noire MAC du domaine de rapprochement d'actifs             |
| Quand un nom d'hôte DNS est associé à trois adresses IP différentes ou plus en 2 heures ou moins        | Ajoutez le nom d'hôte DNS à la liste noire DNS du domaine de rapprochement d'actifs         |
| Quand un nom d'hôte NetBIOS est associé à trois adresses IP différentes ou plus en 2 heures ou moins    | Ajoutez le nom d'hôte NetBIOS à la liste noire NetBIOS du domaine de rapprochement d'actifs |
| Quand une adresse IPv4 est associée à trois adresses MAC différentes ou plus en 2 heures ou moins       | Ajoutez l'adresse IP à la liste noire IPv4 du domaine de rapprochement d'actifs             |
| Quand un nom d'hôte NetBIOS est associé à trois adresses MAC différentes ou plus en 2 heures ou moins   | Ajoutez le nom d'hôte NetBIOS à la liste noire NetBIOS du domaine de rapprochement d'actifs |
| Quand un nom d'hôte DNS est associé à trois adresses MAC différentes ou plus en 2 heures ou moins       | Ajoutez le nom d'hôte DNS à la liste noire DNS du domaine de rapprochement d'actifs         |
| Quand une adresse IPv4 est associée à trois noms d'hôte DNS différents ou plus en 2 heures ou moins     | Ajoutez l'adresse IP à la liste noire IPv4 du domaine de rapprochement d'actifs             |
| Quand un nom d'hôte NetBIOS est associé à trois noms d'hôte DNS différents ou plus en 2 heures ou moins | Ajoutez le nom d'hôte NetBIOS à la liste noire NetBIOS du domaine de rapprochement d'actifs |
| Quand une adresse MAC est associée à trois noms d'hôte DNS différents ou plus en 2 heures ou moins      | Ajoutez l'adresse MAC à la liste noire MAC du domaine de rapprochement d'actifs             |
| Quand une adresse IPv4 est associée à trois noms d'hôte NetBIOS différents ou plus en 2 heures ou moins | Ajoutez l'adresse IP à la liste noire IPv4 du domaine de rapprochement d'actifs             |
| Quand un nom d'hôte DNS est associé à trois noms d'hôte NetBIOS différents ou plus en 2 heures ou moins | Ajoutez le nom d'hôte DNS à la liste noire DNS du domaine de rapprochement d'actifs         |
| Quand une adresse MAC est associée à trois noms d'hôte NetBIOS différents ou plus en 2 heures ou moins  | Ajoutez l'adresse MAC à la liste noire MAC du domaine de rapprochement d'actifs             |

Vous pouvez consulter ces règles sur l'onglet **Infractions** en cliquant sur **Règles** puis en sélectionnant le groupe d'**exclusion de rapprochement d'actifs** dans la liste déroulante.

## Fusion d'actifs

La *fusion d'actifs* est le processus par lequel les informations d'un actif sont combinées aux informations d'un autre actif en vertu du principe qu'ils sont en fait le même actif physique.

La fusion d'actifs se produit quand une mise à jour d'actifs contient des données d'identité qui correspondent à deux profils d'actifs différents. Par exemple, une seule mise à jour contenant un nom d'hôte NetBIOS qui correspond à un profil d'actifs et une adresse MAC qui correspond à un profil d'actifs différent pourrait déclencher une fusion d'actifs.

Certains systèmes peuvent causer des volumes élevés de fusion d'actifs, car ils ont des sources de données d'actifs qui combinent par inadvertance des informations d'identité de deux actifs physiques différents dans une seule mise à jour d'actifs. Certains exemples de ces systèmes comprennent les environnements suivants :

- Serveurs syslog centraux qui agissent en tant que proxy de l'événement
- Machines virtuelles
- Environnements d'installation automatisée
- Noms d'hôtes non uniques, communs avec des actifs tels que les iPads et les iPhones..
- Réseaux privés virtuels qui présentent des adresses MAC partagées
- Extensions de source de journal dont le champ d'identité est `OverrideAndAlwaysSend=true`

Les actifs qui ont de nombreuses adresses IP, adresses MAC, ou noms d'hôte présentent des écarts de croissance d'actifs et peuvent déclencher des notifications système.

## Identification des écarts de croissance d'actifs

---

Parfois, les sources de données d'actifs produisent des mises à jour que IBM QRadar ne peut pas correctement traiter sans une résolution manuelle. Selon la cause de la croissance d'actifs anormale, vous pouvez corriger la source de données d'actif à l'origine du problème ou vous pouvez bloquer les mises à jour d'actif qui proviennent de cette source de données.

Des *écarts de croissance d'actifs* se produisent lorsque le nombre de mises à jour d'actifs pour une seule unité s'accroît au-delà de la limite définie par le seuil de rétention pour un type spécifique d'informations d'identité. Un traitement approprié des écarts de croissance d'actifs est essentiel pour maintenir un modèle d'actif précis.

A la base de chaque écart de croissance d'actifs se trouve une source de données d'actifs dont les données sont peu fiables pour la mise à jour du modèle d'actif. Lorsqu'un écart de croissance d'actifs potentiel est identifié, vous devez examiner la source des informations afin de déterminer s'il y a une explication plausible à l'accumulation par l'actif d'importants volumes de données d'identité. La cause d'un écart de croissance d'actifs est spécifique à chaque environnement.

### Exemple de serveur DHCP de croissance d'actifs non naturelle dans un profil d'actifs

Considérons un serveur de réseau privé virtuel (VPN) dans un réseau Dynamic Host Configuration Protocol (DHCP). Le serveur VPN est configuré pour attribuer des adresses IP aux clients VPN entrants par mandatement des requêtes DHCP pour le compte du client vers le serveur DHCP du réseau.

Du point de vue du serveur DHCP, la même adresse MAC demande à plusieurs reprises de nombreuses affectations d'adresses IP. Dans le cadre de l'exploitation du réseau, le serveur VPN délègue les adresses IP aux clients, mais le serveur DHCP ne peut pas distinguer quand une demande est faite par un actif pour le compte d'un autre.

Le journal du serveur DHCP, qui est configuré en tant que source de journal QRadar génère un événement d'accusé de réception DHCP (DHCP ACK) qui associe l'adresse MAC du serveur VPN à l'adresse IP qui est attribuée au client VPN. Lorsque le rapprochement des actifs se produit, le système rapproche cet événement par adresse MAC, qui se traduit par un actif existant unique qui augmente d'une adresse IP pour chaque événement DHCP ACK qui est analysé.

Finalement, un profil d'actifs contient toutes les adresses IP qui ont été allouées au serveur VPN. Cet écart de croissance d'actifs est causé par des mises à jour d'actifs qui contiennent des informations sur plusieurs actifs.

## Paramètres de seuil

Lorsqu'un actif dans la base de données atteint un nombre spécifique de propriétés, telles que des adresses IP ou des adresses MAC multiples QRadar empêche cet actif de recevoir plus de mises à jour.

Les paramètres de seuil Profileur d'actif précisent les conditions dans lesquelles un actif est verrouillé pour empêcher les mises à jour. L'actif est mis à jour normalement jusqu'à la valeur de seuil. Lorsque le système recueille suffisamment de données pour dépasser le seuil, l'actif montre un écart de croissance d'actifs. Les futures mises à jour de l'actif sont bloquées jusqu'à ce que l'écart de croissance soit redressé.

## Notifications système indiquant des écarts de croissance d'actifs

IBM QRadar génère des notifications système pour vous aider à identifier et à gérer les écarts de croissance d'actifs dans votre environnement.

Les messages système suivants indiquent que QRadar a identifié des écarts potentiels de croissance d'actifs :

- The system detected asset profiles that exceed the normal size threshold
- The asset blacklist rules have added new asset data to the asset blacklists

Les messages de notification du système incluent des liens vers des rapports pour vous aider à identifier les actifs présentant des écarts de croissance.

## Données d'actif qui changent fréquemment

La croissance d'actifs peut être causée par de gros volumes de données d'actifs qui changent de manière légitime, comme dans les situations suivantes :

- Un appareil mobile qui change souvent de bureau et auquel une adresse IP est affectée à chaque connexion.
- Un appareil qui se connecte à un réseau wifi public avec des baux d'adresses IP courts, par exemple sur un campus d'université, peut collecter de gros volumes de données d'actif sur un semestre.

## Exemple : comment les erreurs de configuration pour extensions de source de journal peuvent causer des écarts de croissance d'actifs

Les extensions personnalisées de source de journal qui sont mal configurées peuvent causer des écarts de croissance d'actifs.

Vous configurez une extension de source de journal personnalisée pour fournir des mises à jour d'actifs à IBM QRadar en analysant les noms d'utilisateur depuis le contenu d'événement situé sur un serveur central. Vous configurez l'extension de source de journal pour remplacer la propriété de nom d'hôte d'événement de sorte que les mises à jour d'actifs qui sont générées par la source de journal personnalisée précisent toujours le nom d'hôte DNS du serveur central.

Plutôt que QRadar reçoive une mise à jour qui comporte le nom d'hôte de l'actif auquel l'utilisateur s'est connecté, la source de journal génère de nombreuses mises à jour d'actifs qui ont toutes le même nom d'hôte.

Dans ce cas, l'écart de croissance d'actifs est causé par un profil d'actifs qui contient un grand nombre d'adresses IP et de noms d'utilisateur.

## Traitement des problèmes des profils d'actifs qui dépassent le seuil de taille normale

IBM QRadar génère une notification système lorsque l'accumulation de données sous un seul actif dépasse les seuils limites configurés pour les données d'identité.

```
The system detected asset profiles that exceed the normal size threshold
```

## Explication

Le contenu de la notification montre une liste des cinq actifs présentant le plus souvent un écart et pourquoi le système a marqué chaque actif en tant qu'écart de croissance. Comme le montre l'exemple suivant, le contenu indique également le nombre de fois que l'actif a tenté de croître au-delà du seuil de taille des actifs.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q11labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][192.0.2.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Lorsque les données d'actifs dépassent le seuil configuré, QRadar empêche les futures mises à jour sur l'actif. Cette intervention empêche le système de recevoir davantage de données corrompues et atténue les impacts de performance qui pourraient survenir si le système tente de rapprocher les mises à jour entrantes avec un profil d'actifs anormalement grand.

## Action utilisateur requise

Utilisez les informations du contenu de notification pour identifier les actifs qui contribuent à l'écart de croissance d'actifs et déterminer la cause de la croissance anormale. La notification fournit un lien vers un rapport de tous les actifs qui ont connu un écart de croissance d'actifs au cours des dernières 24 heures.

Après avoir résolu l'écart de croissance d'actifs dans votre environnement, vous pouvez exécuter de nouveau le rapport.

1. Cliquez sur l'onglet **Activité du journal** et cliquez sur **Rechercher > Nouvelle recherche**.
2. Sélectionnez la recherche sauvegardée **Croissance d'actifs présentant un écart : rapports d'actifs**.
3. Utilisez le rapport pour identifier et réparer les données d'actifs inexactes qui ont été créées pendant l'écart.

## Concepts associés

### Données d'actif périmées

Les données d'actif périmées peuvent être problématiques lorsque le taux auquel les nouveaux enregistrements d'actifs sont créés dépasse le taux auquel les données d'actif périmées sont supprimées. Le contrôle et la gestion des seuils de conservation des actifs est la clé pour traiter les écarts de croissance des actifs qui sont causés par des données d'actif périmées.

## De nouvelles données d'actifs sont ajoutées aux listes noires d'actifs

IBM QRadar génère une notification système quand une donnée d'actif présente un comportement qui est compatible avec une croissance déviante d'actif.

```
The asset blacklist rules have added new asset data to the asset blacklists
```

## Explication

Les règles d'exclusion d'actifs surveillent les données d'actifs par souci de cohérence et d'intégrité. Les règles suivent des données spécifiques d'actifs au fil du temps afin d'assurer qu'elles sont constamment observées avec le même sous-ensemble de données dans un délai raisonnable.

Par exemple, si une mise à jour d'actif comprend à la fois une adresse MAC et un nom d'hôte DNS, l'adresse MAC est associée à ce nom d'hôte DNS pour une période prolongée. Les mises à jour ultérieures d'actifs qui contiennent cette adresse MAC contiennent également ce même nom d'hôte DNS quand un nom d'hôte est inclus dans la mise à jour d'actif. Si l'adresse MAC est soudainement associée à un nom d'hôte DNS différent pendant une brève période, la modification est surveillée. Si l'adresse MAC change à nouveau dans un court délai, l'adresse MAC est signalée comme contribuant à une instance de croissance d'actifs déviante et anormale.



## Action utilisateur requise

Utilisez les informations du contenu de notification pour identifier les règles utilisées pour contrôler les données d'actifs. Cliquez sur le lien **Écarts d'actifs par source de journal** dans la notification pour voir les écarts d'actifs qui se sont produits dans les dernières 24 heures.

Si les données d'actifs sont valables, les administrateurs QRadar peuvent configurer QRadar pour résoudre le problème.

- Si vos listes noires se remplissent trop rapidement, vous pouvez affiner les règles d'exclusion de rapprochement d'actifs qui les remplissent.
- Si vous voulez ajouter les données à la base de données d'actifs, vous pouvez supprimer les données d'actifs de la liste noire et les ajouter à la liste blanche d'actifs correspondante. L'ajout de données d'actifs à la liste blanche les empêche de réapparaître par inadvertance sur la liste noire.

### Concepts associés

Optimisation avancée des règles d'exclusion de rapprochement des actifs

Vous pouvez ajuster les règles d'exclusion de rapprochement des actifs pour affiner la définition de la croissance d'actifs déviants dans une ou plusieurs règles.

## Prévention des écarts de croissance d'actifs

---

Après avoir confirmé que la croissance d'actifs est légitime, vous pouvez empêcher de différentes manières que IBM QRadar déclenche l'affichage de messages d'écart pour cet actif.

Utilisez la liste ci-après afin de déterminer comment empêcher les écarts de croissance d'actifs :

- Déterminez comment QRadar traite les données d'actif périmées.
- Optimisez les paramètres de conservation de profileur d'actif pour limiter la durée de conservation des données d'actif.
- Réglez le nombre d'adresses IP autorisées pour un seul actif.
- Créez de recherches d'exclusion d'identité pour exclure certains événements des fournitures de mises à jour d'actif.
- Optimisez les règles Exclusion de rapprochement d'actifs pour affiner la définition d'un écart de croissance d'actifs.
- Créez des listes blanches d'actifs pour éviter que des données réapparaissent dans les liste noire d'actifs.
- Modifiez les entrées dans les listes noires d'actifs et les listes blanches d'actifs.
- Assurez-vous que vos gestionnaires de service de données sont à jour. QRadar assure une mise à jour hebdomadaire automatique qui peut contenir des mises à jour et des corrections des gestionnaires de service de donnée pour des problèmes d'analyse syntaxique.

## Données d'actif périmées

Les données d'actif périmées peuvent être problématiques lorsque le taux auquel les nouveaux enregistrements d'actifs sont créés dépasse le taux auquel les données d'actif périmées sont supprimées. Le contrôle et la gestion des seuils de conservation des actifs est la clé pour traiter les écarts de croissance des actifs qui sont causés par des données d'actif périmées.

Les *données d'actif périmées* sont des données d'actif historiques qui ne sont pas activement ou passivement observées dans un délai spécifique. Les données d'actif périmé sont supprimées lorsqu'elles dépassent la période de conservation configurée.

Les enregistrements historiques sont à nouveau actifs s'ils sont observés par IBM QRadar passivement, via les événements et les flux, ou activement, via les scanners de port et de vulnérabilité.

La prévention des écarts de croissance d'actifs nécessite de trouver le bon équilibre entre le nombre d'adresses IP autorisées pour un actif unique et la durée pendant laquelle QRadar conserve les données d'actif. Vous devez prendre en compte les performances et les compromis de géralité avant de

configurer QRadar pour qu'il puisse contenir des niveaux élevés de conservation des données d'actif. Bien que des périodes de conservation plus longues et des seuils par actif plus élevés puissent sembler souhaitables tout le temps, une meilleure approche consiste à déterminer une configuration de base acceptable pour votre environnement et à tester cette configuration. Ensuite, vous pouvez augmenter les seuils de rétention en petites incréments jusqu'à ce que le bon équilibre soit atteint.

### Tâches associées

[Optimisation des paramètres de conservation du profileur d'actifs](#)

[Optimisation du nombre d'adresses IP autorisées pour un seul actif](#)

## Listes noires et listes blanches d'actifs

IBM QRadar utilise un groupe de règles de rapprochement des actifs pour déterminer si les données d'actifs sont dignes de confiance. Lorsque les données d'actif sont interrogeables, QRadar utilise des listes noires et des listes blanches d'actifs pour déterminer s'il est nécessaire de mettre à jour les profils d'actif avec les données d'actif.

Une *liste noire d'actifs* est une collecte de données qu'QRadar considère peu fiables. Les données dans la liste noire d'actifs sont susceptibles de contribuer à des écarts de croissance d'actifs et QRadar empêche l'ajout de données à la base de données d'actifs.

Une *liste blanche d'actifs* est une collecte de données d'actifs qui remplace la logique de moteur de rapprochement d'actifs concernant les données qui sont ajoutées à une liste noire d'actifs. Lorsque le système identifie une correspondance de liste noire, il consulte la liste blanche pour voir si la valeur existe. Si la mise à jour d'actif correspond aux données qui figurent dans la liste blanche, la modification est synchronisée et l'actif est mis à jour. Les données d'actifs sur la liste blanche sont appliquées globalement pour tous les domaines.

Les listes noires d'actifs et les listes blanches d'actifs sont des ensembles de référence. Vous pouvez afficher et modifier les données de la liste noire et de la liste blanche des actifs en utilisant l'outil de **Gestion des Ensembles de Référence** dans QRadar Console. Pour plus d'informations sur l'utilisation des ensembles de références, voir [«Présentation des jeux de références»](#), à la page 181.

Alternativement, vous pouvez utiliser l'interface de ligne de commande (CLI) ou le nœud final de l'API RestFUL pour mettre à jour le contenu des listes noires et des listes blanches ds actifs.

## Listes de refus d'actifs

Une *liste de refus d'actifs* est un ensemble de données que IBM QRadar considère comme non fiables sur la base des règles d'exclusion de rapprochement des actifs. Les données de la liste de refus des actifs sont susceptibles de contribuer aux écarts de croissance des actifs et QRadar empêche l'ajout des données à la base de données d'actifs.

Chaque mise à jour d'actif dans QRadar est comparée aux listes de refus d'actifs. Les données de les actifs refusés sont appliquées globalement pour tous les domaines. Si la mise à jour de l'actif contient des informations d'identité (adresse MAC, nom d'hôte NetBIOS, nom d'hôte DNS ou adresse IP) qui se trouve sur une liste de refus, la mise à jour entrante est supprimée et la base de données d'actifs n'est pas mise à jour.

| Type de données d'identité | Nom de collection de référence                | Type de collection de référence                   |
|----------------------------|-----------------------------------------------|---------------------------------------------------|
| Adresses IP (v4)           | Liste noire IPv4 de rapprochement d'actifs    | Ensemble de références [type d'ensemble : IP]     |
| Noms d'hôte DNS            | Liste noire DNS de rapprochement d'actifs     | Ensemble de références [type d'ensemble : ALNIC*] |
| Noms d'hôte NetBIOS        | Liste noire NetBIOS de rapprochement d'actifs | Ensemble de références [type d'ensemble : ALNIC*] |

Tableau 57. Noms d'ensembles de référence pour les données de listes de refus d'actifs (suite)

| Type de données d'identité                                                                                   | Nom de collection de référence            | Type de collection de référence                   |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------|
| Adresses Mac                                                                                                 | Liste noire MAC de rapprochement d'actifs | Ensemble de références [type d'ensemble : ALNIC*] |
| * ALNIC est un type alphanumérique qui peut accueillir à la fois le nom d'hôte et les valeurs d'adresse MAC. |                                           |                                                   |

Vous pouvez utiliser l'outil **Gestion des ensembles de référence** pour éditer les entrées de la liste de refus. Pour plus d'informations sur l'utilisation des ensembles de référence, voir [Gestion des ensembles de référence](#).

### Concepts associés

[Liste blanches d'actifs](#)

## Liste blanches d'actifs

Vous pouvez utiliser des listes blanches d'actifs pour éviter que les données d'actif d'IBM QRadar ne réapparaissent par erreur dans les listes noires d'actifs.

Une *liste blanche d'actifs* est une collecte de données d'actifs qui remplace la logique de moteur de rapprochement d'actifs concernant les données qui sont ajoutées à une liste noire d'actifs. Lorsque le système identifie une correspondance de liste noire, il consulte la liste blanche pour voir si la valeur existe. Si la mise à jour d'actif correspond aux données qui figurent dans la liste blanche, la modification est synchronisée et l'actif est mis à jour. Les données d'actifs sur la liste blanche sont appliquées globalement pour tous les domaines.

Vous pouvez utiliser l'outil **Gestion de l'ensemble de référence** pour éditer les entrées de liste blanche. Pour plus d'informations sur l'utilisation des ensembles de référence, voir [Gestion des ensembles de référence](#).

### Exemple d'un cas d'utilisation de liste blanche

La liste blanche est utile si vous avez des données d'actif qui continuent de s'afficher dans les listes noires lorsqu'il s'agit d'une mise à jour d'actif valide. Par exemple, si vous avez un équilibrage de charge DNS de rondes qui est configuré pour l'utilisation par rotation d'un ensemble de cinq adresses IP. Les règles Exclusion de rapprochement d'actifs peuvent déterminer que les différentes adresses IP associées au même nom d'hôte DNS sont indicatives d'un écart de croissance d'actifs, et le système peut ajouter l'équilibrage de charge DNS à la liste noire. Pour résoudre ce problème, vous pouvez ajouter le nom d'hôte DNS à la Liste blanche DNS de rapprochement d'actifs.

### Entrées de masse dans la liste blanche d'actifs

Une base de données exacte d'actifs facilite l'association des infractions qui sont déclenchées dans votre système à des actifs physiques ou virtuels dans votre réseau. Si les écarts d'actifs sont ignorés par l'ajout d'entrées de masse dans la liste blanche d'actifs, cela ne contribue pas à générer une base de données d'actifs exacte. Au lieu d'ajouter des entrées de liste blanche en masse, passez en revue la liste noire d'actifs afin de déterminer ce qui contribue à l'écart de croissance d'actif, puis déterminez comment résoudre ce problème.

### Types de listes blanches d'actifs

Chaque type de données d'identité est conservé dans une liste blanche distincte. Le tableau suivant indique le nom et le type de la collection de référence pour chaque type de données d'actifs d'identité.

Tableau 58. Nom de collection de référence pour les données de la liste blanche d'actifs

| Type de données     | Nom de collection de référence                  | Type de collection de référence                   |
|---------------------|-------------------------------------------------|---------------------------------------------------|
| Adresses IP         | Liste blanche IPv4 de rapprochement d'actifs    | Ensemble de références [type d'ensemble : IP]     |
| Noms d'hôte DNS     | Liste blanche DNS de rapprochement d'actifs     | Ensemble de références [type d'ensemble : ALNIC*] |
| Noms d'hôte NetBIOS | Liste blanche NetBIOS de rapprochement d'actifs | Ensemble de références [type d'ensemble : ALNIC*] |
| Adresses MAC        | Liste blanche MAC de rapprochement d'actifs     | Ensemble de références [type d'ensemble : ALNIC*] |

\* ALNIC est un type alphanumérique qui peut accueillir à la fois le nom d'hôte et les valeurs d'adresse MAC.

### Concepts associés

#### Listes de refus d'actifs

Une *liste de refus d'actifs* est un ensemble de données que IBM QRadar considère comme non fiables sur la base des règles d'exclusion de rapprochement des actifs. Les données de la liste de refus des actifs sont susceptibles de contribuer aux écarts de croissance des actifs et QRadar empêche l'ajout des données à la base de données d'actifs.

### Mise à jour des listes noires et des listes blanches d'actifs à l'aide de la fonctionnalité jeu de références

Vous pouvez utiliser la fonctionnalité jeu de références IBM QRadar pour ajouter ou modifier les entrées figurant sur les listes noires ou blanches d'actifs.

Pour gérer vos ensembles de références, exécutez la fonctionnalité `ReferenceDataUtil.sh` à partir de `/opt/qradar/bin` sur QRadar Console.

Les commandes permettant d'ajouter de nouvelles valeurs à chaque liste sont décrites dans le tableau suivant. Les valeurs de paramètre doivent correspondre exactement aux valeurs de mise à jour de l'actif fournies par la source de données d'actif d'origine.

Tableau 59. Syntaxe de commande permettant de modifier les données de la liste noire et de liste blanche des actifs

| Nom                                        | Syntaxe de commande                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Liste noire IPv4 de rapprochement d'actifs | <pre>ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Blacklist" IP</pre> <p>Par exemple, cette commande ajoute l'adresse IP 192.168.3.56 à la liste noire :</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56</pre>                                           |
| Liste noire DNS de rapprochement d'actifs  | <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Blacklist" DNS</pre> <p>Par exemple, cette commande ajoute le nom de domaine 'misbehaving.asset.company.com' à la liste noire :</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"</pre> |

Tableau 59. Syntaxe de commande permettant de modifier les données de la liste noire et de liste blanche des actifs (suite)

| Nom                                             | Syntaxe de commande                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Liste noire NetBIOS de rapprochement d'actifs   | <pre>ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Blacklist" NETBIOS</pre> <p>Par exemple, cette commande supprime le nom d'hôte NetBIOS 'deviantGrowthAsset-156384' de la liste noire :</p> <pre>ReferenceDataUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"</pre> |
| Liste noire MAC de rapprochement d'actifs       | <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Blacklist" MACADDR</pre> <p>Par exemple, cette commande ajoute l'adresse MAC '00:a0:1a:2b:3c:4d' à la liste noire :</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:1a:2b:3c:4d"</pre>                                       |
| Liste blanche IPv4 de rapprochement d'actifs    | <pre>ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP</pre> <p>Par exemple, cette commande supprime l'adresse IP 10.1.95.142 de la liste blanche :</p> <pre>ReferenceDataUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142</pre>                                                   |
| Liste blanche DNS de rapprochement d'actifs     | <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Whitelist" DNS</pre> <p>Par exemple, cette commande ajoute le nom de domaine 'loadbalancer.company.com' à la liste blanche :</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"</pre>                       |
| Liste blanche NetBIOS de rapprochement d'actifs | <pre>ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Whitelist" NETBIOS</pre> <p>Par exemple, cette commande ajoute le nom NetBIOS 'assetName-156384' à la liste blanche :</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"</pre>                              |
| Liste blanche MAC de rapprochement d'actifs     | <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Whitelist" MACADDR</pre> <p>Par exemple, cette commande ajoute l'adresse MAC '00:a0:1a:2b:3c:4d' à la liste blanche :</p> <pre>ReferenceDataUtil.sh add "Asset Reconciliation MAC Whitelist" "00:a0:1a:2b:3c:4d"</pre>                                     |

#### Tâches associées

Mise à jour des listes noires et des listes blanches en utilisant l'API RESTful

### Mise à jour des listes noires et des listes blanches en utilisant l'API RESTful

Vous pouvez utiliser l'API IBM QRadar RESTful pour personnaliser le contenu des listes noires et des listes blanches des actifs.

## Pourquoi et quand exécuter cette tâche

Vous devez indiquer le nom exact du jeu de références que vous souhaitez afficher ou mettre à jour.

- Liste noire IPv4 de rapprochement d'actifs
- Liste noire DNS de rapprochement d'actifs
- Liste noire NetBIOS de rapprochement d'actifs
- Liste noire MAC de rapprochement d'actifs
- Liste blanche IPv4 de rapprochement d'actifs
- Liste blanche DNS de rapprochement d'actifs
- Liste blanche NetBIOS de rapprochement d'actifs
- Liste blanche MAC de rapprochement d'actifs

## Procédure

1. Entrez l'URL suivante dans votre navigateur Web pour accéder à l'interface de l'API RESTful :

```
https://ConsoleIPaddress/api_doc
```

2. Dans le panneau de navigation de gauche, recherchez `4.0>/reference_data >/sets > /{name}`.
3. Pour afficher le contenu d'une liste noire ou d'une liste blanche d'actifs, procédez comme suit :
  - a) Cliquez sur l'onglet **OBTENIR** et faites défiler vers le bas jusqu'à la section **Paramètres**.
  - b) Dans la zone **Valeur** du paramètre **Nom** , entrez le nom de la liste noire ou de la liste blanche des actifs que vous souhaitez afficher.
  - c) Cliquez sur **Essayer** et affichez les résultats en bas de l'écran.
4. Pour ajouter une valeur à une liste noire ou à une liste blanche d'actifs, procédez comme suit :
  - a) Cliquez sur l'onglet **PUBLIER** et faites défiler vers le bas jusqu'à la section **Paramètres**.
  - b) Entrez les valeurs des paramètres suivants :

| <i>Tableau 60. Paramètres requis pour l'ajout de nouvelles données d'actif</i> |                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nom du paramètre :</b>                                                      | <b>Description</b>                                                                                                                                                                                                                    |
| nom                                                                            | Représente le nom de la collection de référence que vous souhaitez mettre à jour.                                                                                                                                                     |
| valeur                                                                         | Représente l'élément de données que vous souhaitez ajouter à la liste noire ou à la liste blanche des actifs. Doit correspondre exactement aux valeurs de mise à jour de l'actif fournies par la source de données d'actif d'origine. |

- c) Cliquez sur **Essayer** pour ajouter la nouvelle valeur à la liste blanche ou liste noire des actifs.

## Que faire ensuite

Pour plus d'informations sur l'utilisation de l'API RESTful pour modifier les ensembles de références, voir *IBM QRadar API Guide*.

### Concepts associés

Mise à jour des listes noires et des listes blanches d'actifs à l'aide de la fonctionnalité jeu de références  
Vous pouvez utiliser la fonctionnalité jeu de références IBM QRadar pour ajouter ou modifier les entrées figurant sur les listes noires ou blanches d'actifs.

## Optimisation des paramètres de conservation du profileur d'actifs

IBM QRadar utilise les paramètres de conservation des actifs pour gérer la taille des profils d'actif.

La période de conservation par défaut de la plupart des données d'actif est de 120 jours après la dernière fois qu'elle a été observée passivement ou activement dans QRadar. Les noms d'utilisateurs sont conservés pendant 30 jours.

Les données d'actifs ajoutées manuellement par les utilisateurs QRadar ne contribuent généralement pas aux écarts de croissance des actifs. Par défaut, ces données sont conservées perpétuellement. Pour tous les autres types de données d'actifs, l'indicateur **Conserver perpétuellement** n'est suggéré que pour les environnements statiques.

## Pourquoi et quand exécuter cette tâche


Vous pouvez ajuster le temps de conservation en fonction du type de données d'identité d'actif qui se trouve dans l'événement. Par exemple, si plusieurs adresses IP fusionnent sous un même actif, vous pouvez modifier la durée de conservation IP des actifs de 120 jours à une valeur inférieure.

Lorsque vous modifiez la période de conservation des actifs pour un type spécifique de données d'actif, la nouvelle période de conservation est appliquée à toutes les données d'actif dans QRadar. Les données d'actifs existantes qui dépassent déjà le nouveau seuil sont supprimées lorsque le déploiement est terminé. Pour vous assurer que vous pouvez toujours identifier des hôtes nommés même lorsque les données d'actifs dépassent la période de conservation, le processus de nettoyage de la conservation des actifs ne supprime pas la dernière valeur de nom d'hôte connu pour un actif.

Avant de déterminer le nombre de jours pendant lequel vous souhaitez conserver les données d'actifs, comprenez les caractéristiques suivantes concernant les périodes de conservation plus longues :

- Fournit une meilleure vue historique de vos actifs.
- Crée des volumes de données plus importants par actif dans la base de données d'actifs.
- Augmente la probabilité que les données périmées contribuent aux messages d'écart de croissance des actifs.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Configuration du profileur d'actifs**.
3. Cliquez sur **Configuration de conservation du profileur d'actifs**.
4. Ajustez les valeurs de conservation et cliquez sur **Sauvegarder**.
5. Déployez les modifications dans votre environnement pour que les mises à jour prennent effet.

### Tâches associées

[Optimisation du nombre d'adresses IP autorisées pour un seul actif](#)

## Optimisation du nombre d'adresses IP autorisées pour un seul actif

IBM QRadar surveille le nombre d'adresses IP qu'un seul actif s'accumule dans le temps.

Par défaut, QRadar génère un message système lorsqu'un seul actif accumule plus de 75 adresses IP. Si vous prévoyez d'accumuler plus de 75 adresses IP, vous pouvez ajuster la valeur **Nombre d'adresses IP autorisées pour un seul actif** pour éviter les messages système futurs.

## Pourquoi et quand exécuter cette tâche

La définition de la limite du nombre d'adresses IP trop élevées empêche QRadar de détecter les écarts de croissance des actifs avant qu'ils n'aient un impact négatif sur le reste du déploiement. Le fait de fixer la limite trop faible augmente le nombre d'écarts de croissance des actifs signalés.


Vous pouvez utiliser la directive suivante lorsque vous optimisez le paramètre **Nombre d'adresses IP autorisées pour un seul actif** pour la première fois.

Nombre d'adresses IP autorisées pour un seul actif = (<retention time (days)> x <estimated IP addresses per day>) + <buffer number of IP addresses>

Où

- *<estimated IP addresses per day>* est le nombre d'adresses IP qu'un seul actif peut s'accumuler en une journée dans des conditions normales
- *<retention time (days)>* est le temps privilégié pour conserver les adresses IP de l'actif

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Actifs**, cliquez sur **Configuration du profileur d'actifs**.
3. Cliquez sur **Configuration du profileur d'actifs**.
4. Réglez les valeurs de configuration et cliquez sur **Sauvegarder**.
5. Déployez les modifications dans votre environnement pour que les mises à jour prennent effet.

## Tâches associées

[Optimisation des paramètres de conservation du profileur d'actifs](#)

## Optimisation du nombre d'adresses MAC autorisées pour un seul actif

Nouveautés de la version 7.4.2 IBM QRadar surveille le nombre d'adresses MAC qu'un seul actif accumule dans le temps.

Par défaut, QRadar génère un message système lorsqu'un seul actif accumule plus de dix adresses MAC. Si vous prévoyez d'accumuler plus de dix adresses MAC, vous pouvez ajuster la valeur **Nombre d'adresses MAC autorisées pour un actif unique** pour éviter les messages système futurs.

## Pourquoi et quand exécuter cette tâche

La définition de la limite du nombre d'adresses MAC trop élevée empêche QRadar de détecter les écarts de croissance des actifs avant qu'ils n'aient un impact négatif sur le reste du déploiement. Le fait de fixer la limite trop faible augmente le nombre d'écarts de croissance des actifs signalés.


Vous pouvez utiliser la directive suivante lorsque vous optimisez le paramètre **Nombre d'adresses MAC autorisées pour un actif unique** pour la première fois.

Nombre d'adresses MAC autorisées pour un seul actif = (*<retention time (days)>* x *<estimated MAC addresses per day>*) + *<buffer number of MAC addresses>*

Où

- *<estimated MAC addresses per day>* est le nombre d'adresses MAC qu'un seul actif peut s'accumuler en une journée dans des conditions normales
- *<retention time (days)>* est le temps privilégié pour conserver les adresses MAC de l'actif

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Actifs**, cliquez sur **Configuration du profileur d'actifs**.
3. Cliquez sur **Configuration du profileur d'actifs**.
4. Ajustez la valeur **Nombre d'adresses MAC autorisées pour un actif unique** et cliquez sur **Sauvegarder**.
5. Déployez les modifications dans votre environnement pour que les mises à jour prennent effet.

## Recherches d'exclusion d'identité

Des recherches d'exclusion d'identité peuvent être utilisées pour gérer des actifs uniques qui cumulent de gros volumes d'informations d'identité similaires pour des raisons connues valides.



Par exemple, les sources de journal peuvent fournir de gros volumes d'informations d'identité d'actif à la base de données d'actifs. Elles fournissent à IBM QRadar des modifications en temps quasi réel de l'information sur les actifs et ils peuvent conserver le courant de votre base de données d'actifs. Mais les sources de journal sont le plus souvent la source des écarts de croissance des actifs et d'autres anomalies liées aux actifs.

Lorsqu'une source de journal envoie des données d'actif incorrectes à QRadar, essayez de corriger la source de journal de sorte que les données qu'elle envoie soient utilisables par la base de données d'actifs. Si la source de journal ne peut pas être corrigée, vous pouvez générer une recherche d'exclusion d'identité qui bloque les informations d'actif à partir de la saisie de la base de données d'actifs.

Vous pouvez également utiliser une recherche d'exclusion d'identité où `Identity_Username+Is Any Of + Anonymous Logon` pour vous assurer que vous ne mettez pas à jour des actifs qui sont liés aux comptes de service ou aux services automatisés.

## Différences entre les recherches d'exclusion d'identité et les listes noires

Bien que les recherches d'exclusion d'identité semblent avoir des fonctionnalités similaires à des listes noires d'actifs, il existe des différences significatives.

Les listes noires ne peuvent spécifier que les données d'actif brutes, telles que les adresses MAC et les noms d'hôte, qui doivent être exclues. Les recherches d'exclusion d'identité filtrent les données d'actif en fonction des zones de recherche telles que la source de journal, la catégorie et le nom de l'événement.

Les listes noires ne tiennent pas compte du type de source de données qui fournit les données, alors que les recherches d'exclusion d'identité ne peuvent être appliquées qu'aux événements. Les recherches d'exclusion d'identité peuvent bloquer les mises à jour d'actifs en fonction des zones de recherche d'événements communs, telles que le type d'événement, le nom d'événement, la catégorie et la source de journal.

## Création de recherches d'exclusion d'identité

Pour exclure certains événements de la fourniture de données d'actif à la base de données d'actifs, vous pouvez créer une recherche d'exclusion d'identité IBM QRadar.

### Pourquoi et quand exécuter cette tâche


Les filtres que vous créez pour la recherche doivent correspondre aux événements que vous souhaitez exclure, et non aux événements que vous souhaitez conserver.

Il peut être utile d'exécuter la recherche sur les événements qui se trouvent déjà dans le système. Toutefois, lorsque vous enregistrez la recherche, vous devez sélectionner **Temps réel (streaming)** dans les options **Durée de vie**. Si vous ne choisissez pas ce paramètre, la recherche ne correspond à aucun résultat lorsqu'elle s'exécute sur le flux en direct des événements qui entrent dans QRadar.

Lorsque vous mettez à jour la recherche d'exclusion d'identité enregistrée sans modifier le nom, la liste d'exclusion d'identité utilisée par Asset Profiler est mise à jour. Par exemple, vous pouvez éditer la recherche pour ajouter davantage de filtrage des données d'actif que vous souhaitez exclure. Les nouvelles valeurs sont incluses et l'exclusion d'actif démarre immédiatement après la sauvegarde de la recherche.

## Procédure

1. Créez une recherche pour identifier les événements qui ne fournissent pas de données d'actif à la base de données d'actifs.
  - a) Dans l'onglet **Activité de journal**, cliquez sur **Rechercher > Nouvelle recherche**.
  - b) Créez la recherche en ajoutant des critères de recherche et des filtres pour qu'ils correspondent aux événements que vous souhaitez exclure des mises à jour d'actif.
  - c) Dans la zone **Intervalle de temps**, sélectionnez **Temps réel (streaming)**, puis cliquez sur **Filtrer** pour exécuter la recherche.

- d) Dans l'écran des résultats de la recherche, cliquez sur **Sauvegarder les critères** et fournissez les informations pour la recherche sauvegardée.
- Remarque :** Vous pouvez affecter la recherche sauvegardée à un groupe de recherche. Un groupe de recherche d'exclusion d'identité existe dans le dossier **Authentification, identité et activité des utilisateurs**.
- e) Cliquez sur **OK** pour enregistrer la recherche.
2. Identifiez la recherche que vous avez créée en tant que recherche d'exclusion d'identité.
- a) Dans le menu de navigation () , cliquez sur **Admin**.
- b) Dans la section **Configuration du système**, cliquez sur **Configuration du profileur d'actifs**.
- c) Cliquez sur **Gérer l'exclusion d'identité** au bas de l'écran.
- d) Sélectionnez la recherche d'exclusion d'identité que vous avez créée dans la liste de recherches à gauche, puis cliquez sur l'icône Ajouter (>).
- Conseil :** Si vous ne trouvez pas la recherche, tapez les premières lettres dans le filtre en haut de la liste.
- e) Cliquez sur **Sauvegarder**.
3. Dans l'onglet **Admin**, cliquez sur **Déployer les modifications** pour que les mises à jour prennent effet.

## Optimisation avancée des règles d'exclusion de rapprochement des actifs

Vous pouvez ajuster les règles d'exclusion de rapprochement des actifs pour affiner la définition de la croissance d'actifs déviants dans une ou plusieurs règles.

Par exemple, considérons ce modèle normalisé à partir d'une règle d'exclusion de rapprochement des actifs.

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
by the Local system and NOT when any of
Identity Host Name are contained in any of
Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
and when at least N1 events are seen with the same
Identity Host Name and different Identity IP in N2
```

Ce tableau répertorie les variables du modèle de règle qui peuvent être optimisées et le résultat du changement. Évitez de modifier d'autres variables dans le modèle.

| Variable | Valeur par défaut | Résultat de l'optimisation                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N1       | 3                 | L'optimisation de cette variable par rapport à une valeur plus faible entraîne l'ajout de plus de données à la liste noire car moins d'événements avec des données en conflit sont nécessaires pour que la règle s'applique.<br><br>L'optimisation de cette variable par rapport à une valeur plus élevée entraîne l'ajout de moins de données à la liste noire car il faut plus d'événements avec des données contradictoires pour que la règle s'applique. |

Tableau 61. Options d'optimisation des règles de rapprochement des actifs (suite)

| Variable | Valeur par défaut | Résultat de l'optimisation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N2       | 2 heures          | <p>L'optimisation de cette variable par une valeur inférieure réduit la fenêtre de temps dans laquelle les événements N1 doivent être vus pour que la règle s'applique. Le temps requis pour observer les données correspondantes est diminué, ce qui entraîne l'ajout de moins de données à la liste noire.</p> <p>L'optimisation de cette variable par une valeur plus élevée augmente le temps dans lequel les événements N1 doivent être considérés pour la règle s'applique. Le temps d'observation des données correspondantes est augmenté, ce qui entraîne l'ajout de plus de données à la liste noire.</p> <p>L'augmentation de la période peut avoir une incidence sur les ressources de mémoire système, car les données sont suivies sur des périodes plus longues.</p> |

Les règles d'exclusion de rapprochement des actifs sont des règles à l'échelle du système. Les modifications apportées aux règles affectent la façon dont la règle se comporte dans l'ensemble du système.

## Application d'un réglage différent pour les règles

Il peut être nécessaire d'appliquer différents réglages pour les règles dans différentes parties du système. Pour appliquer des règles d'optimisation différentes, vous devez dupliquer les règles d'exclusion de rapprochement des actifs que vous souhaitez optimiser et ajouter un ou plusieurs tests pour contraindre les règles de sorte que vous ne testez que certaines parties du système. Par exemple, vous pouvez créer des règles qui testent uniquement les réseaux, les sources de journal ou les types d'événement.

## Pourquoi et quand exécuter cette tâche

Soyez toujours prudent lorsque vous ajoutez de nouvelles règles au système car certaines tâches et règles CRE peuvent avoir un impact sur les performances du système. Il peut être avantageux d'ajouter les nouvelles règles au début de chaque pile de test pour permettre au système de contourner le reste de la logique de test chaque fois qu'une mise à jour d'un actif correspond aux critères de la nouvelle règle.

## Procédure

1. Dupliquer la règle.

- a) Dans l'onglet **Infractions**, cliquez sur **Règles** et sélectionnez la règle à copier.
- b) Cliquez sur **Actions > Dupliquer**.

Il peut être utile que le nom de la nouvelle règle indique la raison de la duplication.

2. Ajoutez un test à la règle.

Déterminez un filtre que vous souhaitez utiliser pour appliquer la règle uniquement à un sous-ensemble de données système. Par exemple, vous pouvez ajouter un test qui ne correspond que à des événements provenant d'une source de journal spécifique.

3. Ajustez les variables de la règle pour obtenir le comportement souhaité.

4. Mettez à jour la règle d'origine.

- a) Ajoutez le même test que vous avez ajouté à la règle en double à la règle d'origine, mais cette fois, inversez les règles ET et ET PAS les opérateurs.

L'annulation des opérateurs empêche les événements d'être déclenchés dans les deux règles.

## Exemple : règles d'exclusion d'actifs ajustées pour exclure des adresses IP de la liste noire

Vous pouvez exclure des adresses IP de la mise sur liste noire en ajustant les règles d'exclusion d'actifs.

En tant qu'administrateur de sécurité réseau, vous gérez un réseau d'entreprise qui comprend un segment de réseau wifi public où les baux d'adresses IP sont généralement courts et fréquents. Les actifs sur ce segment du réseau ont tendance à être transitoires, principalement des ordinateurs portables et des appareils portables qui se connectent et se déconnectent du réseau WiFi public fréquemment. Généralement, une seule adresse IP est utilisée plusieurs fois par différentes unités sur une courte période.

Dans le reste de votre déploiement, vous disposez d'un réseau géré personnalisé constitué uniquement de périphériques de l'entreprise inventoriés. Les baux d'adresses IP sont beaucoup plus longs dans cette partie du réseau, et les adresses IP sont accessibles par l'authentification uniquement. Sur ce segment de réseau, vous voulez savoir immédiatement quand il existe des écarts de croissance d'actifs et vous souhaitez conserver les paramètres par défaut pour les règles d'exclusion de rapprochement d'actifs.

### Mise d'adresses IP sur liste noire

Dans cet environnement, les règles d'exclusion de rapprochement d'actifs par défaut mettent en liste noire par inadvertance l'ensemble du réseau dans un court laps de temps.

Votre équipe de sécurité estime que les notifications relatives aux actifs qui sont générées par le segment de wifi constituent une nuisance. Vous souhaitez empêcher le wifi de déclencher davantage de notifications d'écart de croissance d'actifs.

### Ajustement de règles de rapprochement d'actifs pour ignorer certaines mises à jour d'actifs

Vous passez en revue le rapport **Ecart d'actifs par source de journal** dans la dernière notification du système. Vous déterminez que les données sur la liste noire proviennent du serveur DHCP sur votre réseau wifi.

Les valeurs de la colonne **Nombre d'événements**, **Nombre de flux** et de la colonne **Infractions** pour la ligne correspondant à la règle **AssetExclusion: Exclude IP By MAC Address** indiquent que votre serveur DHCP wifi déclenche cette règle.

Vous ajoutez un test aux règles d'exclusion de rapprochement d'actifs existantes pour faire en sorte que les règles cessent d'ajouter des données Wi-Fi à la liste noire.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

La règle mise à jour teste uniquement les événements des sources de journaux qui ne sont pas sur votre serveur DHCP wifi. Pour éviter que les événements DHCP wifi soient soumis à des tests d'analyse de comportement et à des ensembles de référence plus onéreux, vous avez également déplacé ce test en haut de la pile de tests.

## Nettoyer les données d'actif après les écarts de croissance

IBM QRadar utilise le modèle d'actif pour connecter les violations de votre déploiement à des actifs physiques ou virtuels dans votre réseau. La capacité de recueillir et d'afficher des données pertinentes sur la façon dont les biens sont utilisés est une étape importante dans le règlement des questions de sécurité. Il est important de maintenir la base de données sur les biens afin de s'assurer que les données sont à jour et exactes.

Que vous fixiez la source du problème ou que vous bloquiez les mises à jour de l'actif, vous devez nettoyer la base de données d'actifs en supprimant les données d'actif non valides et en supprimant les entrées de la liste noire d'actifs.

## Suppression d'actifs non valides

Après avoir fixé les actifs qui ont contribué à l'écart de croissance de l'actif, nettoyez vos artefacts d'actif à l'aide du nettoyage sélectif ou de la régénération de la base de données d'actifs.

### Pourquoi et quand exécuter cette tâche

#### Nettoyage sélectif

Cette méthode est pour les écarts de croissance d'actifs d'une portée limitée. La suppression sélective des actifs affectés est la méthode la moins invasive pour nettoyer les artefacts d'actifs, mais si de nombreux actifs ont été affectés, elle peut également être la plus fastidieuse.

#### Reconstruire la base de données d'actifs

La reconstruction de la base de données d'actifs à partir de zéro est la méthode la plus efficace et la plus précise pour supprimer les actifs lorsque les écarts de croissance d'actifs sont omniprésents.

Cette méthode régénère passivement les actifs de votre base de données en fonction de la nouvelle optimisation que vous avez configurée pour résoudre les problèmes de croissance des actifs. Avec cette approche, tous les résultats d'analyse et les données d'actifs résiduels sont perdus, mais les données peuvent être réaffirmées en réexécutant une analyse ou en réimportation des résultats d'analyse.

### Procédure

1. Pour supprimer de manière sélective des artefacts non valides dans la base de données d'actifs, procédez comme suit :
  - a) Dans l'onglet **Activité de journal**, exécutez la recherche d'événements **Deviating Asset Growth: Asset Report**.  
Cette recherche renvoie un rapport d'actifs qui sont affectés par la déviation de la croissance des actifs et doivent être supprimés.
  - b) Dans l'onglet **Actifs**, cliquez sur **Actions > Supprimer l'actif**  
Il peut y avoir un retard avant que l'actif n'apparaisse plus dans IBM QRadar.
2. Pour régénérer la base de données d'actifs à partir de zéro, procédez comme suit :
  - a) Utilisez SSH pour vous connecter à QRadar Console en tant qu'administrateur.
  - b) Exécutez le script `/opt/qradar/support/cleanAssetModel.sh` à partir de la ligne de commande de la console et sélectionnez **Variante 1** lorsque vous y êtes invité.

La reconstruction de la base de données d'actifs redémarre le moteur de rapprochement des actifs.


### Résultats

La purge d'une liste noire supprime toutes les entrées de la liste noire, y compris celles qui ont été ajoutées manuellement. Les entrées de liste noire ajoutées manuellement doivent être ajoutées à nouveau.

## Suppression d'entrées de liste noire

Une fois que vous avez corrigé la cause des entrées de la liste noire, vous devez nettoyer les entrées restantes. Vous pouvez supprimer les entrées de la liste noire, mais il est préférable de purger toutes les entrées de la liste noire et d'autoriser les valeurs de liste noire qui ne sont pas liées à l'écart de croissance de l'actif à régénérer.

## Procédure

1. Pour purger une liste noire à l'aide de la console IBM QRadar :
  - a) Dans le menu de navigation () , cliquez sur **Admin**.
  - b) Dans la section **Configuration du système**, cliquez sur **Gestion des ensembles de référence**.
  - c) Sélectionnez un ensemble de références, puis cliquez sur **Supprimer**.
  - d) Utilisez la zone de texte de recherche rapide pour rechercher les ensembles de références que vous souhaitez supprimer, puis cliquez sur **Supprimer la liste**.
2. Pour purger une liste noire à l'aide de l'interface de ligne de commande QRadar Console :
  - a) Accédez au répertoire `/opt/qradar/bin`.
  - b) Exécutez la commande suivante :

```
./ReferenceDataUtil.sh purge "Reference Collection Name"
```

Où *Nom de la collection de référence* est l'une des listes suivantes :

- Liste noire NetBIOS de rapprochement d'actifs
- Liste noire DNS de rapprochement d'actifs
- Liste noire IPv4 de rapprochement d'actifs
- Liste noire MAC de rapprochement d'actifs

## Résultats

La purge d'une liste noire supprime toutes les entrées de la liste noire, y compris celles qui ont été ajoutées manuellement. Les entrées de liste noire ajoutées manuellement doivent être ajoutées à nouveau.

---

# Chapitre 19. Configuration de QRadar pour réacheminer des données à d'autres systèmes

Configurez IBM QRadar pour transférer des données vers un ou plusieurs systèmes fournisseurs, tels que des systèmes de billetterie ou d'alerte.

Vous pouvez également envoyer des données normalisées à d'autres déploiements QRadar. Le système cible qui reçoit les données de QRadar est appelé *Destination de réacheminement*. QRadar garantit que toutes les données réacheminées restent inchangées.



**Avertissement :** Les données normalisées accordées doivent correspondre ou exister dans les deux déploiements QRadar. Sinon, l'événement peut avoir un QID associé incorrect ou rester non analysé. Ces données incluent des expressions QIDS, des types de source de journal personnalisés, des propriétés personnalisées, des ID d'événement et des expressions de catégorie d'événement. Pour éviter les problèmes de synchronisation, réachemchez les événements en utilisant le format brut.

Pour éviter les problèmes de compatibilité lors de l'envoi de données d'événement et flux, assurez-vous que le déploiement qui reçoit les données est de la même version ou d'une version supérieure à celle du déploiement qui envoie les données en utilisant le flux de travaux suivant.

1. Configurez une ou plusieurs destinations de transfert.
2. Pour déterminer les données que vous souhaitez transférer, configurez les règles de routage, les règles personnalisées ou les deux.
3. Configurez les options de routage à appliquer aux données.

Par exemple, vous pouvez configurer toutes les données d'un collecteur d'événements spécifique pour les transférer vers un système de billetterie spécifique. Vous pouvez également ignorer la corrélation en supprimant les données qui correspondent à une règle de routage.

## Concepts associés

[Fonctions de votre produit IBM QRadar](#)


---

## Ajout de destinations de réacheminement

Avant de pouvoir configurer des règles de routage ou des règles personnalisées pour transférer des données, vous devez ajouter une destination de transfert. Les événements normalisés que vous réacheminez ne peuvent être interprétés que par d'autres systèmes QRadar.

**Restriction :** Vous ne pouvez pas transférer des données vers des systèmes utilisant des adresses IP dynamiques. La connexion est établie lorsque le service démarre et que les modifications apportées à l'adresse IP ne sont pas détectées avant le redémarrage du service. La destination de transfert doit avoir une adresse IP statique.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Transfert de destinations**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Dans la fenêtre **Destinations de réacheminement**, entrez des valeurs pour les paramètres.

Le tableau suivant décrit certains des paramètres de **Transfert de destinations** .

| Tableau 62. Paramètres <b>Transfert de destinations</b>           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Adresse de destination</b>                                     | Adresse IP ou nom d'hôte du système du fournisseur auquel réacheminer des données.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Format d'événement</b>                                         | <ul style="list-style-type: none"> <li>• <b>Payload</b> représente les données dans le format envoyé par la source de journal ou la source de flux. Si vous sélectionnez cette option, assurez-vous que le port 514 est ouvert.</li> <li>• <b>Normalisé</b> représente des données brutes analysées et préparées en tant qu'informations lisibles pour l'interface utilisateur. Si vous sélectionnez cette option, assurez-vous que les ports 32000 et 32004 sont ouverts.</li> <li>• <b>JSON</b> (JavaScript Object Notation) : format d'échange de données. Si vous sélectionnez cette option, assurez-vous que le port 5141 est ouvert.</li> </ul>                                                                                                              |
| <b>protocole</b>                                                  | <p>Utilisez le protocole <b>TCP</b> pour envoyer des données normalisées à l'aide du protocole TCP. Vous devez créer une source hors site à l'adresse de destination sur le port 32004 pour les Événements, ou sur le port 32000 pour les Flux.</p> <p>Utilisez le protocole <b>TCP sur SSL</b> pour envoyer des données normalisées en toute sécurité en utilisant le protocole TCP avec un certificat SSL. Vous devez installer un certificat SSL pour établir la communication vers la destination.</p> <p><b>Restriction</b> : Vous ne pouvez pas transmettre de données normalisées et JSON à l'aide du protocole UDP. Si vous sélectionnez les options <b>Normalisé</b> ou <b>JSON</b>, l'option <b>UDP</b> de la liste <b>Protocole</b> est désactivée.</p> |
| <b>Préfixez un en-tête syslog s'il est manquant ou non valide</b> | <p>Applicable uniquement lorsque le format d'événement est <b>Payload</b>.</p> <p>Lorsque QRadar transmet les messages syslog, le message sortant est vérifié pour s'assurer qu'il possède un en-tête syslog valide.</p> <p>Si un en-tête syslog valide n'est pas détecté et que cette case est cochée, l'en-tête syslog préfixé inclut l'adresse IP d'origine du paquet que QRadar a reçu dans le champ <b>Nom d'hôte</b> de l'en-tête syslog. Si cette case n'est pas cochée, les données sont envoyées sans être modifiées.</p>                                                                                                                                                                                                                                 |

5. Facultatif : Si vous utilisez le protocole **TCP sur SSL** , procédez comme suit :

- A partir de la ligne de commande du collecteur d'événements ou du processeur qui utilise la règle de routage pour réacheminer les données, modifiez le répertoire sur `/tmp`.
- Exécutez la commande suivante :  

```
:/opt/qradar/bin/getcert.sh tlssyslog_server_ip tlssyslog_port
```

Une copie du certificat client est téléchargée à partir du système cible et est titrée avec l'IP et le port à partir desquels vous l'avez téléchargée.
- Déplacez le certificat vers `/opt/qradar/conf/trusted_certificates/`
- Si le certificat a été signé par une autorité de certification commerciale ou privée (CA), copiez l'autorité de certification racine et les certificats intermédiaires dans `/etc/pki/ca-trust/source/anchors`
- Exécutez la commande suivante :`update-ca-trust`

6. Cliquez sur **Sauvegarder**.

### Que faire ensuite

La configuration d'une destination de transfert n'envoie pas automatiquement de données à cette destination. Vous devez configurer une règle de routage ou une règle personnalisée pour transférer des



données vers la destination. Pour plus d'informations, voir [«Configuration des règles de routage pour réacheminer des données»](#), à la page 299.

### Concepts associés

«Utilisation du port QRadar», à la page 441

Examinez la liste des ports usuels utilisés par les services et les composants IBM QRadar pour communiquer au sein du réseau. Vous pouvez utiliser cette liste pour déterminer quels ports doivent être ouverts dans votre réseau. Vous pouvez, par exemple, déterminer quel port doit être ouvert pour que QRadar Console communique avec des processeurs d'événements distants.

## Configuration des profils de transfert

---

Si vous souhaitez indiquer les propriétés à transférer vers la destination de transfert, configurez un profil de transfert.

Vous devez recréer les profils de transfert JSON que vous avez créés dans IBM QRadar V7.2.3 ou version antérieure.

### Pourquoi et quand exécuter cette tâche


Vous ne pouvez utiliser les profils de transfert que lorsque les données d'événement sont envoyées au format JSON.

Vous pouvez sélectionner des propriétés d'événement ou de flux spécifiques, y compris des propriétés personnalisées, pour les transférer vers une destination externe. Vous pouvez améliorer la lisibilité des données d'événement en spécifiant un nom d'alias et une valeur par défaut pour l'attribut. Les noms d'alias et les valeurs par défaut sont spécifiques au profil dans. Si les attributs sont utilisés dans d'autres profils, les noms d'alias et les valeurs par défaut doivent être redéfinis.

Vous pouvez utiliser un seul profil comportant plusieurs destinations d'acheminement. Lorsque vous éditez un profil, assurez-vous que les modifications sont appropriées pour toutes les destinations de transfert associées au profil.

Lorsque vous supprimez un profil, toutes les destinations de réacheminement qui ont utilisé le profil reviennent automatiquement à l'aide du profil par défaut.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Transfert de destinations**.
3. Dans la barre d'outils, cliquez sur **Gestionnaire de profils**.
4. Pour créer un profil, cliquez sur **Nouveau**.
5. Entrez un nom pour le profil et cochez la case en regard des attributs que vous souhaitez inclure dans le fichier d'événements.
6. Pour modifier un profil existant, sélectionnez le profil et cliquez sur **Éditer** ou **Supprimer**.
7. Cliquez sur **Sauvegarder**.

## Configuration des règles de routage pour réacheminer des données

---

Réacheminer des données en configurant des règles de routage basées sur des filtres.

### Pourquoi et quand exécuter cette tâche


Vous pouvez configurer des règles de routage pour réacheminer des données en mode en ligne ou hors ligne :

- En mode **En ligne**, vos données restent à jour car le réacheminement est effectué en temps réel. Si la destination de transfert devient inaccessible, les données envoyées à cette destination ne sont pas

fournies, ce qui entraîne la disparition des données sur ce système distant. Pour garantir la réussite de la diffusion, utilisez le mode hors connexion.

- En mode **Hors ligne**, toutes les données sont d'abord stockées dans la base de données, puis envoyées à la destination de réacheminement. Ce mode garantit qu'aucune donnée n'est perdue. Cependant, des retards dans le réacheminement de données peuvent se produire.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Règles de routage**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Dans la fenêtre **Règle de routage**, entrez un nom et une description pour votre règle de routage.
5. Dans la zone **Mode**, sélectionnez l'une des options suivantes : **En ligne** ou **Hors ligne**.
6. Dans la liste **Collecteur d'événements de réacheminement** ou **Processeur d'événement de réacheminement**, sélectionnez le collecteur d'événements à partir duquel vous souhaitez réacheminer des données.

### En savoir plus sur le dispositif de réacheminement :

#### Collecteur d'événements de réacheminement

Indique le Collecteur d'événements depuis lequel vous souhaitez que cette règle de routage traite les données. Cette option s'affiche lorsque vous sélectionnez l'option **En ligne**.

**Remarque :** Le réacheminement en ligne/en temps réel n'est pas affecté par les configurations de Limitation de débit ou de Planification qui peuvent être configurées sur les collecteurs d'événements Stockage et réacheminement (15xx).

#### Processeur d'événement de réacheminement

Indique le processeur d'événements depuis lequel vous souhaitez que cette règle de routage traite les données. Cette option s'affiche lorsque vous sélectionnez l'option **Hors ligne**.

**Restriction :** Cette option n'est pas disponible si l'option **Supprimer** est sélectionnée dans le volet **Options de routage**.

7. Dans la zone **Source de données**, sélectionnez la source de données que vous souhaitez router : **Événements** ou **Flux**.

Les libellés de la section suivante changent en fonction de la source de données que vous sélectionnez.

8. Spécifiez les événements ou flux à transmettre en appliquant des filtres :
  - a) Pour transférer toutes les données entrantes, cochez la case **Correspondance avec tous les événements entrants** ou **Correspondance avec tous les flux entrants**.

**Restriction :** Si vous cochez cette case, vous ne pouvez pas ajouter de filtre.
  - b) Pour réacheminer uniquement certains événements ou flux, spécifiez les critères de filtrage, puis cliquez sur **Ajouter un filtre**.
9. Spécifiez les options de routage à appliquer aux données réacheminées :
  - a) Si vous souhaitez modifier, ajouter ou supprimer une destination de réacheminement, cliquez sur le lien **Gérer les destinations**.
  - b) Pour acheminer les données de journal correspondant aux filtres spécifiés, cochez la case **Transmettre**, puis cochez la case correspondant à chaque destination de transfert.

**Restriction :** Si vous cochez la case **Transmettre**, vous ne pouvez sélectionner qu'une de ces cases à cocher : **Supprimer**, **Ignorer la corrélation** ou **Consigner uniquement**.

Pour plus d'informations, voir [«Options de routage pour les règles»](#), à la page 301.

10. Cliquez sur **Sauvegarder**.

## Options de routage pour les règles

Vous pouvez choisir parmi quatre options de routage de règle : Forward, Drop, Bypass correlation et Log Only. Le tableau suivant décrit les différentes options et comment les utiliser.

| Type de routage                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Forward</b>                      | Les données sont transmises à la destination de réacheminement spécifiée. Les données sont également stockées dans la base de données et traitées par le moteur de règles (CRE).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Drop</b>                         | Les données sont supprimées. Les données ne sont pas stockées dans la base de données et ne sont pas traitées par le CRE. Cette option n'est pas disponible si vous sélectionnez l'option <b>Hors ligne</b> . Tous les événements supprimés sont recrédités à 100 % sur la licence.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Bypass Correlation</b>           | <p>Les données contournent la CRE, mais elles sont stockées dans la base de données. Cette option n'est pas disponible si vous sélectionnez l'option <b>Hors ligne</b>.</p> <p>L'option <b>Bypass correlation</b> ne requiert pas d'autorisation pour le magasin de données QRadar. La corrélation de contournement permet aux événements reçus par lots de contourner les règles en temps réel. Vous pouvez utiliser les événements dans les applications analytiques et pour les exécutions de corrélation d'historique. Pour les exécutions de corrélation d'historique, les événements peuvent être relus comme s'ils avaient été reçus en temps réel.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Log Only (Exclude Analytics)</b> | <p>Les événements sont stockés et marqués dans la base de données sous la forme <b>Consigner uniquement</b> et ignorent CRE. Ces événements ne sont pas disponibles pour la corrélation historique et sont recrédités à 100 % à la licence. Cette option n'est pas disponible pour les flux ou si vous sélectionnez l'option <b>Hors ligne</b>.</p> <p>L'option <b>Log Only</b> requiert une autorisation pour le magasin de données QRadar. Une fois que l'autorisation a été achetée et que l'option <b>Log Only</b> est sélectionnée, les événements qui correspondent à la règle de routage sont stockés sur le disque et sont disponibles pour la vue et pour les recherches. Les événements ignorent le moteur de règle personnalisée et aucune corrélation ou analyse en temps réel n'a lieu. Les événements ne peuvent pas contribuer aux infractions et sont ignorés lorsque la corrélation historique s'exécute. Certaines applications ignorent également les événements <b>Consigner uniquement</b> (<a href="https://www.ibm.com/support/docview.wss?uid=swg22009471">https://www.ibm.com/support/docview.wss?uid=swg22009471</a>).</p> |

Le tableau suivant décrit différentes combinaisons d'options de routage que vous pouvez utiliser. Ces options ne sont pas disponibles en mode hors ligne.

Tableau 64. Options de combinaison de routage de règle

| Combinaison de routage                                         | Description                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Forward et Drop</b>                                         | Les données sont transmises à la destination de réacheminement spécifiée. Les données ne sont pas stockées dans la base de données et ne sont pas traitées par le CRE. Tous les événements supprimés sont recredités à 100 % sur la licence.                                                                              |
| <b>Réacheminer et Ignorer la corrélation</b>                   | Les données sont transmises à la destination de réacheminement spécifiée. Les données sont stockées dans la base de données, mais elles ne sont pas traitées par le CRE.                                                                                                                                                  |
| <b>Réacheminer et Consigner uniquement (exclure l'analyse)</b> | Les événements sont transmis à la destination de transfert indiquée. Les événements sont stockés et marqués dans la base de données en tant que Consigner uniquement et ignorent le traitement par le CRE. Ces événements ne sont pas disponibles pour la corrélation historique et sont recredités à 100 % à la licence. |

Si les données correspondent à plusieurs règles, l'option de routage la plus sûre est appliquée. Par exemple, si les données correspondent à une règle configurée pour supprimer des données et à une autre configurée pour ignorer le traitement par le moteur de données personnalisées, les données ne sont pas supprimées. A la place, les données ignorent le moteur de règles personnalisées et sont stockées dans la base de données.

## Configuration des règles de routage pour utiliser le magasin de données QRadar

Une nouvelle offre, IBM QRadar Data Store, normalise et stocke les données de sécurité et de journal opérationnel pour les analyses et les examens ultérieurs. L'offre prend en charge le stockage d'un nombre illimité de journaux sans compter sur les événements de votre organisation par seconde QRadar SIEM, et permet à votre organisation de générer des applications et des rapports personnalisés basés sur ces données stockées afin d'obtenir des informations plus approfondies sur vos environnements.

### Pourquoi et quand exécuter cette tâche


L'utilisation de l'option **Log Only (Exclude Analytics)** requiert l'autorisation pour QRadar Data Store, mais n'est pas appliquée actuellement. Lorsqu'elle sera appliquée, l'accès aux données d'événement collectées sera restreint aux systèmes pour lesquels vous disposez d'une licence. Lorsque la licence est appliquée et que l'option **Log Only (Exclude Analytics)** est sélectionnée, les événements qui correspondent à la règle de routage seront stockés sur le disque et seront disponibles pour la vue et pour les recherches. Les événements ignorent le moteur de règle personnalisée et aucune corrélation ou analyse en temps réel n'a lieu. Les événements ne peuvent pas contribuer aux infractions et sont ignorés lorsque la corrélation historique s'exécute.

Les applications suivantes ignorent également les événements de journal uniquement :

- QRadar User Behavior Analytics
- QRadar Advisor with Watson

**Restriction :** Les utilisateurs QRadar on Cloud doivent ouvrir un ticket de support pour transmettre des données à d'autres systèmes. Pour plus d'informations, voir [Éléments de travail QRadar on Cloud nécessitant un ticket de support](#).

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Règles de routage**.
3. Dans la barre d'outils, cliquez sur **Ajouter**.
4. Dans la fenêtre **Règle de routage**, entrez un nom et une description pour votre règle de routage.
5. Dans le champ **Mode**, sélectionnez **En ligne**.
6. Dans la liste **Transfert du collecteur d'événements**, sélectionnez le collecteur d'événements sur lequel vous souhaitez appliquer l'option **Log Only (Exclude Analytics)**.
7. Dans la zone **Source de données**, sélectionnez **Événements**.
8. Indiquez les événements à appliquer à l'option **Log Only (Exclude Analytics)** en appliquant des filtres :
  - a) Pour appliquer l'option **Log Only (Exclude Analytics)** à toutes les données entrantes, cochez la case **Correspondance avec tous les événements entrants**.

**Restriction :** Si vous cochez cette case, vous ne pouvez pas ajouter de filtre.

b) Pour appliquer l'option **Log Only (Exclude Analytics)** à certains événements uniquement, indiquez les critères de filtrage, puis cliquez sur **Ajouter un filtre**.

9. Pour appliquer l'option **Log Only (Exclude Analytics)** aux données de journal correspondant aux filtres spécifiés, sélectionnez **Log Only (Exclude Analytics)**.

**Remarque :** L'option **Consigner uniquement (exclure l'analyse)** spécifie que les événements sont stockés et marqués dans la base de données en tant que Consigner uniquement et ignorent le traitement par le CRE. Ces événements ne sont pas disponibles pour la corrélation historique et sont recredités à 100 % à la licence. Cette option n'est pas disponible pour les flux.

Vous pouvez combiner les options **Suivant** et **Log Only (Exclude Analytics)**. Les événements sont transmis à la destination de réacheminement spécifiée en mode en ligne. Les événements sont stockés et marqués dans la base de données en tant que Consigner uniquement et ignorent le traitement par le CRE. Ces événements ne sont pas disponibles pour la corrélation historique et sont recredités à 100 % à la licence. Cette option n'est pas disponible en mode hors ligne.

Si les données correspondent à plusieurs règles, l'option de routage la plus sûre est appliquée. Par exemple, si les données correspondent à une règle configurée pour supprimer des données et à une autre configurée pour ignorer le traitement par le moteur de données personnalisées, les données ne sont pas supprimées. A la place, les données ignorent le moteur de règles personnalisées et sont stockées dans la base de données.

10. Cliquez sur **Sauvegarder**.

## Utilisation de règles personnalisées et de réponses de règle pour transmettre des données

Utilisez l'assistant **Règle personnalisée** pour configurer la transmission des données d'événement qui correspondent aux règles de votre système. Configurez la réponse de règle pour transférer les données d'événement vers une ou plusieurs destinations de transfert.

### Pourquoi et quand exécuter cette tâche

Les critères qui déterminent les données d'événement envoyées à une destination de transfert sont basés sur les tests et les blocs de construction inclus dans la règle.

Lorsque la règle est configurée et activée, toutes les données d'événement qui correspondent aux tests de règle sont automatiquement envoyées aux destinations de transfert indiquées. Pour plus d'informations sur l'édition ou l'ajout d'une règle, voir *IBM QRadar - Guide d'utilisation* pour votre produit.

## Procédure

1. Cliquez sur l'onglet **Infractions** ou **Activité de journal**.
2. Dans le menu **Règles**, sélectionnez **Règles**.
3. Dans la fenêtre **Liste des règles**, sélectionnez la règle à éditer ou cliquez sur **Actions** pour créer une nouvelle règle.
4. Sur la page **Réponse de règle** de l'assistant **Règle**, veillez à sélectionner l'option **Envoi aux destinations de transfert**.


## Affichage des destinations de transfert

La fenêtre **Transfert de destinations** fournit des informations précieuses sur vos destinations de transfert. Les statistiques des données envoyées à chaque destination de transfert s'affichent.

Par exemple, vous pouvez voir les informations suivantes :

- Nombre total d'événements et de flux qui ont été vus pour cette destination d'acheminement.
- Nombre d'événements ou de flux envoyés à cette destination d'acheminement.
- Nombre d'événements ou de flux qui ont été supprimés avant que la destination d'acheminement n'ait été atteinte.


## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Transfert de destinations**.
3. Affichez les statistiques de vos destinations de réacheminement.

## Affichage et gestion des destinations de transfert

Utilisez la fenêtre **Destination de transfert** pour afficher, éditer et supprimer des destinations de réacheminement.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Transfert de destinations**.

Les statistiques des données envoyées à chaque destination de transfert s'affichent. Par exemple, vous pouvez voir les informations suivantes :

- Nombre total d'événements et de flux qui ont été vus pour cette destination d'acheminement.
  - Nombre d'événements ou de flux envoyés à cette destination d'acheminement.
  - Nombre d'événements ou de flux qui ont été supprimés avant que la destination d'acheminement n'ait été atteinte.
3. Dans la barre d'outils, cliquez sur une action, comme décrit dans le tableau suivant.


| Action | Description                                                                 |
|--------|-----------------------------------------------------------------------------|
|        | Modifie le nom, le format, l'adresse IP, le port ou le protocole configurés |

## Affichage et gestion des règles de routage

---

Utilisez la fenêtre **Règles de routage des événements** pour activer ou désactiver les règles, ou pour modifier une règle pour modifier le nom configuré, Collecteur d'événements, les filtres ou les options de routage.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration système**, cliquez sur **Règles de routage**.
3. Sélectionnez la règle de routage que vous souhaitez gérer.
4. Pour modifier la règle de routage, dans la barre d'outils, cliquez sur **Éditer** et mettez à jour les paramètres.
5. Pour supprimer la règle de routage, dans la barre d'outils, cliquez sur **Supprimer**.
6. Pour activer ou désactiver la règle de routage, dans la barre d'outils, cliquez sur **Activer / Désactiver**.

Si vous activez une règle de routage configurée pour supprimer des événements, un message de confirmation s'affiche.





---

## Chapitre 20. Magasin d'événements et transmission

Utilisez la fonction de stockage et de transfert pour gérer les planifications de transfert des événements de vos dispositifs Collecteur d'événements dédiés aux composants processeur d'événements dans votre déploiement.

La fonction de stockage et de transfert est prise en charge sur Event Collector 1501 et le collecteur d'événements 1599. Pour plus d'informations sur ces fichiers, voir le *IBM QRadar Hardware Guide*.

Un Collecteur d'événements dédié ne traite pas les événements et n'inclut pas un processeur d'événements de bord. Par défaut, un Collecteur d'événements dédié envoie en continu des événements à un processeur d'événements connecté à QRadar.

Vous pouvez planifier une plage horaire pour le moment où vous souhaitez que le Collecteur d'événements achemine des événements vers processeur d'événements. En transmettant les événements pendant les heures non ouvrables, vous pouvez vous assurer que la transmission n'affecte pas la bande passante de votre réseau. Lorsque la transmission des événements est planifiée, les événements sont stockés en local sous Collecteur d'événements jusqu'à ce que la planification des réacheminement s'y trouve. Pendant cette période, vous ne pouvez pas afficher les événements dans la console IBM QRadar.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Affichage de la liste de planification de stockage et de réacheminement

Utilisez la fenêtre **Stocker et réacheminer** pour afficher la liste des planifications. Les plannings incluent des statistiques qui vous aident à évaluer le statut, les performances et l'avancement de vos plannings.

### Avant de commencer


Vous devez créer un planning. Par défaut, la première fois que vous accédez à la fenêtre **Stocker et réacheminer**, aucun planning n'est répertorié.

### Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser les options de la barre d'outils et la zone de liste **Afficher** pour modifier votre vue de la liste de planification. Changez votre vue de la liste pour vous concentrer sur les statistiques de différents points de vue. Par exemple, si vous souhaitez afficher les statistiques d'un collecteur d'événements particulier, vous pouvez sélectionner **Collecteurs d'événements** dans la liste **Afficher**. La liste répertorie ensuite les groupes par la colonne **Collecteur d'événements** et vous permet de localiser plus facilement le fichier Collecteur d'événements que vous souhaitez étudier.

Par défaut, la liste Stocker et réacheminer est configurée pour afficher la liste organisée par le planning (**Afficher > Planifications**).

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Stocker et réacheminer**.
3. Dans la fenêtre **Stocker et réacheminer**, affichez les paramètres de chaque planning.

Le tableau suivant décrit certains des paramètres de la planification.

| Tableau 66. Paramètres de la fenêtre <b>Stocker et réacheminer</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Afficher                                                           | <p>L'option <b>Planifications</b> affiche une hiérarchie de la relation parent-enfant entre les plannings, les processeurs d'événements et les collecteurs d'événements associés.</p> <p>L'option <b>Collecteurs d'événements</b> affiche le niveau le plus bas de la hiérarchie, qui est une liste de collecteurs d'événements.</p> <p>L'option <b>Processeurs d'événements</b> affiche une hiérarchie de la relation parent-enfant entre les processeurs d'événements et les collecteurs d'événements associés.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Nom                                                                | <p>Pour l'option <b>Planifications</b>, la colonne <b>Nom</b> est affichée au format suivant.</p> <ul style="list-style-type: none"> <li>• <b>Premier niveau</b> représente le nom de la planification.</li> <li>• <b>Deuxième niveau</b> représente le nom du processeur d'événements.</li> <li>• <b>Troisième niveau</b> représente le nom du collecteur d'événements.</li> </ul> <p>Pour l'option <b>Processeurs d'événements</b>, la colonne est affichée au format suivant</p> <ul style="list-style-type: none"> <li>• <b>Premier niveau</b> représente le nom du processeur d'événements.</li> <li>• <b>Deuxième niveau</b> représente le nom du collecteur d'événements.</li> </ul> <p><b>Conseil :</b> Vous pouvez utiliser le symbole plus (+) et le symbole moins (-) en regard du nom ou des options de la barre d'outils pour développer et réduire l'arborescence hiérarchique. Vous pouvez également développer et réduire l'arborescence hiérarchique à l'aide des options de la barre d'outils.</p> |
| Nom de la planification                                            | <p>Affiche le nom du planning pour les options <b>Collecteurs d'événements</b> ou <b>Processeurs d'événements</b>.</p> <p>Si un processeur d'événement est associé avec plus d'un planning, le <b>nom de planning</b> affiche plusieurs <math>n</math>, où <math>n</math> est le nombre de plannings.</p> <p><b>Conseil :</b> Cliquez sur le symbole plus (+) pour afficher les plannings associés.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Tableau 66. Paramètres de la fenêtre **Stocker et réacheminer** (suite)

| Paramètre                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dernier état             | <p>Affiche l'état du processus Stocker et réacheminer :</p> <ul style="list-style-type: none"> <li>• <b>Transfert</b> indique que la transmission d'événements est en cours.</li> <li>• <b>Réacheminement terminé</b> indique que la transmission des événements est terminée et que les événements sont stockés en local sur le collecteur d'événements. Les événements stockés sont transmis lorsque le planning indique que la transmission peut redémarrer.</li> <li>• <b>Avertir</b> indique que le pourcentage d'événements qui restent en mémoire dépasse le pourcentage de temps restant dans le calendrier Stockage et réacheminement.</li> <li>• <b>Erreur</b> indique que la transmission des événements a été arrêtée avant la transmission de tous les événements stockés.</li> <li>• <b>Inactif</b> indique qu'aucun collecteur d'événements n'est affecté à la planification ou que les collecteurs d'événements affectés ne reçoivent aucun événement.</li> </ul> <p><b>Conseil :</b> Déplacez le pointeur de la souris sur la colonne <b>Dernier statut</b> pour afficher un récapitulatif du statut.</p> |
| Evénements réacheminés   | <p>Affiche le nombre d'événements (en K, M ou G) transmis dans la session en cours.</p> <p><b>Conseil :</b> Déplacez le pointeur de la souris sur la valeur de la colonne <b>Événements transférés</b> pour afficher le nombre d'événements.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Evénements restants      | <p>Affiche le nombre d'événements (en K, M ou G) restant à transmettre dans la session en cours.</p> <p><b>Conseil :</b> Déplacez le pointeur de la souris sur la valeur de la colonne <b>Autres événements</b> pour afficher le nombre d'événements.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Débit d'événements moyen | <p>Affiche le débit moyen auquel les événements sont transmis du collecteur d'événements au processeur d'événements.</p> <p><b>Conseil :</b> Déplacez le pointeur de la souris sur la valeur de la colonne <b>Débit moyen d'événements</b> pour afficher les événements moyens par seconde (EPS).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Tableau 66. Paramètres de la fenêtre <b>Stocker et réacheminer</b> (suite) |                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                  | Description                                                                                                                                                                                                                                                                                 |
| Taux d'événements actuel                                                   | Affiche le débit auquel les événements sont transmis du collecteur d'événements au processeur d'événements.<br><br><b>Conseil :</b> Déplacez le pointeur de la souris sur la valeur de la colonne <b>Taux d'événements en cours</b> pour afficher les événements en cours par seconde (EPS) |
| Limite de taux de transfert                                                | La limite de taux de transfert est configurable.<br><br>La limite de taux de transfert peut être configurée pour être affichée en kilooctets par seconde (Ko), en mégaoctets par seconde (Mo) ou en gigaoctets par seconde (Go).                                                            |

## Création d'un planning de stockage et de réacheminement


Utilisez l'assistant de planification de magasin et de réacheminement pour créer un planning qui contrôle le moment où votre collecteur d'événements démarre et arrête de transférer des données vers un processeur d'événements.

Vous pouvez créer et gérer plusieurs planifications pour contrôler la transmission d'événements à partir de plusieurs collecteurs d'événements IBM QRadar dans un déploiement réparti géographiquement.

### Avant de commencer

Vérifiez que votre collecteur d'événements dédié est ajouté à votre déploiement et connecté à un processeur d'événements. Utilisez la fenêtre **Gestion des systèmes et des licences** pour configurer la connexion entre un collecteur d'événements et un processeur d'événements.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Stocker et réacheminer**.
3. Cliquez sur **Actions > Créer**.
  - a) Cliquez sur **Suivant** pour passer à la page **Sélectionner des collecteurs**.
  - b) Sur la page **Sélectionner des collecteurs**, configurez les paramètres.  
Si le collecteur d'événements que vous souhaitez configurer n'est pas répertorié, vous devez l'ajouter avant de poursuivre. Pour plus d'informations sur l'ajout d'un collecteur d'événements, voir «Ajout d'un hôte géré», à la page 76.
  - c) Sur la page **Options de planification**, configurez les paramètres.  
**Remarque :** Le taux de transfert minimal est 0. Le taux de transfert maximal est de 9 999 999. La valeur 0 signifie que le taux de transfert est illimité.
  - d) Terminez la configuration.


Vous pouvez maintenant afficher le planning dans la fenêtre **Stocker et réacheminer**. Une fois que vous avez créé un planning, il peut prendre jusqu'à 10 minutes pour que les statistiques commencent à s'afficher dans la fenêtre **Stocker et réacheminer**.

## Édition d'une planification de magasin et de réacheminement

---

Vous pouvez éditer une planification **Stocker et réacheminer** pour ajouter ou supprimer des collecteurs d'événements IBM QRadar et modifier les paramètres de planification. Après avoir modifié un planning **Stocker et réacheminer**, les statistiques affichées dans la liste **Stocker et réacheminer** sont réinitialisée.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Stocker et réacheminer**.
3. Sélectionnez le planning que vous souhaitez modifier.
4. Cliquez sur **Actions > Editer**.

Vous pouvez également cliquer deux fois sur un planning pour l'éditer.

5. Cliquez sur **Suivant** pour passer à la page **Sélectionner des collecteurs**.
6. Dans **Page Sélectionner des collecteurs**, modifiez les paramètres.
7. Cliquez sur **Suivant** pour passer à la page **Options de planification**.
8. Sur la page **Options de planification**, modifiez les paramètres de planification.
9. Cliquez sur **Suivant** pour passer à la page **Résumé**.
10. Sur la page **Résumé**, confirmez les options que vous avez éditées pour cette planification.

Une fois que vous avez modifié un planning, il peut prendre jusqu'à 10 minutes pour que les statistiques se mettent à jour dans la fenêtre **Stocker et réacheminer**.

## Suppression d'un planning de stockage et retransmission

---

Vous pouvez supprimer un planning de **stockage et retransmission**.

### Procédure

1. Dans le menu de navigation, cliquez sur **Configuration du système**.
2. Cliquez sur l'icône **Stockage et retransmission**.
3. Sélectionnez le planning à supprimer.
4. Cliquez sur **Actions > Supprimer**.

Une fois la planification supprimée, les collecteurs d'événements IBM QRadar associés reprennent le transfert continu des événements vers leur processeur d'événements affecté.



---

# Chapitre 21. Contenu de sécurité

Vous utilisez les outils de gestion de contenu dans IBM QRadar pour importer du contenu de sécurité comme des règles, des rapports, des tableaux de bord et des applications dans QRadar. Le contenu de sécurité peut provenir d'autres systèmes QRadar, ou il peut être développé indépendamment pour étendre les fonctions existantes de QRadar.

## Concepts associés

Fonctions de votre produit IBM QRadar

---

## Types de contenu de sécurité

Le contenu IBM QRadar est regroupé en deux types : les packs de contenu et les extensions.

### Packs de contenu

Les *packs de contenu* de sécurité contiennent les améliorations apportées à des types de contenu de sécurité spécifiques. Souvent, ils contiennent du contenu pour les intégrations de tiers ou les systèmes d'exploitation. Par exemple, un pack de contenu de sécurité pour une intégration tiers peut contenir de nouvelles propriétés d'événement personnalisé qui rendent les informations dans la charge d'événement interrogeables pour la source de journal et disponibles pour la génération de rapports.

Les packs de contenu de sécurité sont disponibles à partir de IBM Fix Central (<http://www.ibm.com/support/fixcentral>). Les packs de contenu ne sont pas disponibles dans le cadre d'une mise à jour automatique.

### Extensions

IBM et d'autres fournisseurs écrivent des *extensions* de sécurité qui améliorent ou étendent les fonctionnalités de QRadar. Une extension peut contenir des applications, des éléments de contenu, tels que des règles personnalisées, des modèles de rapport, des recherches sauvegardées ou des mises à jour des éléments de contenu existants. Par exemple, une extension peut inclure une application pour ajouter un onglet dans QRadar qui fournit des visualisations pour une infraction.

Sous IBM Security App Exchange, les extensions sont appelées applications. Vous pouvez télécharger des applications QRadar à partir de IBM Security App Exchange et utiliser l'outil **Gestion des extensions** pour les installer. Les applications ne sont pas disponibles dans le cadre d'une mise à jour automatique.

## Sources de contenu de sécurité

Le contenu QRadar est disponible à partir des sources suivantes :

### IBM Security App Exchange

IBM Security App Exchange (<https://apps.xforce.ibmcloud.com>) est un magasin d'applications et un portail où vous pouvez parcourir et télécharger des extensions QRadar. Il s'agit d'un nouveau mode de partage de code, de visualisations, de rapports, de règles et d'applications.

### IBM Fix Central

IBM Fix Central ([www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)) fournit des correctifs et des mises à jour sur votre logiciel système, votre matériel et votre système d'exploitation. Vous pouvez télécharger des packs de contenu de sécurité depuis IBM Fix Central.

### Déploiements de QRadar

Vous exportez du contenu personnalisé depuis un déploiement QRadar en tant qu'extension et l'importez dans un autre système lorsque vous voulez le réutiliser. Par exemple, vous pouvez exporter du contenu depuis votre environnement de développement vers votre environnement de production. Vous pouvez utiliser le script de gestion de contenu pour exporter tout le contenu, ou vous pouvez choisir de n'exporter que certains contenus personnalisés.

## Méthodes d'importation et d'exportation de contenu

Vous pouvez utiliser les outils suivants pour importer et exporter du contenu dans votre déploiement IBM QRadar.

### Outil de gestion des extensions

L'outil **Extensions Management** permet d'ajouter des extensions à votre déploiement QRadar. Lorsque vous importez du contenu à l'aide de l'outil **Extensions Management**, vous pouvez afficher le contenu avant de l'installer. Si les éléments de contenu existent dans votre système, vous pouvez indiquer s'il faut les remplacer ou ignorer la mise à jour.

Vous ne pouvez pas utiliser l'outil **Extensions Management** pour exporter du contenu.

### Script de gestion du contenu

Utilisez le script de gestion du contenu pour exporter le contenu personnalisé depuis votre déploiement QRadar dans un format externe transférable. Vous pouvez ensuite utiliser le script pour importer le contenu personnalisé dans un autre déploiement QRadar. Ce script est utile lorsque vous souhaitez automatiser le déplacement du contenu entre vos déploiements QRadar.

Le script `contentManagement.pl` se trouve dans le répertoire `/opt/qradar/bin`.

Vous devez utiliser le script de gestion du contenu pour exporter du contenu à partir du déploiement source QRadar. Vous pouvez utiliser le script de gestion du contenu ou l'outil **Gestion des extensions** pour importer le contenu dans le déploiement cible.

### Editeur DSM

Dans QRadar versions V7.3.3 et ultérieures, vous pouvez exporter le contenu personnalisé que vous créez dans l'éditeur DSM. Cliquez sur le bouton **Exporter** dans l'éditeur DSM pour exporter votre contenu d'un déploiement QRadar vers un autre ou vers le support externe.

**Remarque :** Vous pouvez exporter le contenu à partir d'une version antérieure de QRadar et l'importer dans une version ultérieure. Cependant, vous ne pouvez pas importer du contenu d'une version ultérieure vers une version antérieure.

**Remarque :** Si vous déplacez des règles remplacées d'un déploiement QRadar vers un autre, utilisez l'option **Replace Existing Content Items** pour vous assurer que les règles sont correctement importées.

## Exportation de tous les contenus personnalisés

Vous utilisez le script `contentManagement.pl` pour exporter tous les contenus personnalisés dans votre déploiement IBM QRadar.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Allez au répertoire `/opt/qradar/bin` et entrez la commande permettant d'exporter l'ensemble du contenu personnalisé :

```
./contentManagement.pl -a export -c all
```

### Exemples :

- Pour inclure les données cumulées dans l'exportation, entrez la commande suivante :

```
./contentManagement.pl --action export --content-type all -g
```

- Pour spécifier le répertoire du fichier exporté et modifier le format de compression, entrez la commande suivante :



```
./contentManagement.pl -a export -c all -o [filepath] -t [compression_type]
```

## Résultats

Le contenu est exporté dans un fichier compressé, par exemple, all-ContentExport-20151022101803.zip. Vous pouvez modifier manuellement le nom de fichier en un nom plus descriptif. Le fichier exporté peut contenir plus d'éléments de contenu que prévu car toutes les dépendances sont exportées avec les éléments de contenu spécifiés. Par exemple, si vous exportez un rapport, la recherche sauvegardée utilisée par le rapport est également exportée.

## Exportation de tous les contenus personnalisés d'un type spécifique

Vous pouvez exporter tous les contenus personnalisés d'un type spécifique dans une action.

### Pourquoi et quand exécuter cette tâche

Le script de gestion de contenu utilise des identificateurs de texte ou des identificateurs numériques pour spécifier le type de contenu que vous souhaitez exporter.

| Type de contenu personnalisé        | Identificateur de texte      | Identificateur numérique |
|-------------------------------------|------------------------------|--------------------------|
| Tableaux de bord                    | <b>dashboard</b>             | 4                        |
| Rapports                            | <b>report</b>                | 10                       |
| Recherches sauvegardées             | <b>search</b>                | 1                        |
| FGroups <sup>1</sup>                | <b>fgroup</b>                | 12                       |
| Types de FGroup                     | <b>fgrouptype</b>            | 13                       |
| Règles personnalisées               | <b>customrule</b>            | 3                        |
| Propriétés personnalisées           | <b>customproperty</b>        | 6                        |
| Sources de journal                  | <b>sensordevice</b>          | 17                       |
| Types de source de journal          | <b>sensordevicetype</b>      | 24                       |
| Catégories de source de journal     | <b>sensordevicecategory</b>  | 18                       |
| Extensions de source de journal     | <b>deviceextension</b>       | 16                       |
| Collecte de données de référence    | <b>referencedata</b>         | 28                       |
| Entrées de mappe QID personnalisée  | <b>qidmap</b>                | 27                       |
| Profils de corrélation d'historique | <b>historicalsearch</b>      | 25                       |
| Fonctions personnalisées            | <b>custom_function</b>       | 77                       |
| Actions personnalisées              | <b>custom_action</b>         | 78                       |
| Applications                        | <b>installed_application</b> | 100                      |
| Mappage d'événements DSM            | <b>dsmevent</b>              | 41                       |

<sup>1</sup>Un FGroup représente un groupe de contenu, tel qu'un groupe de sources de journal, un groupe de rapports ou un groupe de recherche.

## Procédure

1. Utilisez SSH pour la connexion à IBM QRadar en tant qu'utilisateur racine.
2. Allez dans le répertoire /opt/qradar/bin et entrez la commande pour exporter tout le contenu du type spécifié :

```
./contentManagement.pl -a export --content-type [content_type] --id all
```

### Paramètres :


| Tableau 68. Paramètres de script <code>contentManagement.pl</code> pour l'exportation de contenu personnalisé d'un type spécifique |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>-c [contenu_type]</code><br>ou<br><code>--content-type [contenu_type]</code>                                                 | Indique le type de contenu.<br><br>Vous pouvez entrer le texte ou l'identificateur numérique correspondant pour spécifier le type de contenu.<br><br> <b>Avertissement :</b> Si vous choisissez d'exporter des données d'un type de contenu spécifique, des données supplémentaires provenant d'un contenu connexe d'un type de contenu peuvent être exportées. |
| <code>-e</code><br>ou<br><code>--include-reference-data-elements</code>                                                            | Définissez cet indicateur pour inclure des clés de données de référence et des éléments dans l'exportation.<br><br>Les clés de données de référence et les éléments de données de référence sont applicables au type de contenu <code>referencedata</code> . Ce paramètre est applicable uniquement lorsque vous exportez des données de référence ou des éléments de contenu qui dépendent des données de référence.                            |
| <code>-g</code><br>ou<br><code>--global-view</code>                                                                                | Inclut les données cumulées dans l'exportation.                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>-i [contenu_identificateur]</code><br>ou<br><code>--id [contenu_identificateur]</code>                                       | Indique <u>Identificateur</u> d'une instance spécifique de contenu personnalisé, par exemple un seul rapport ou un seul ensemble de références.<br><br>Vous pouvez indiquer <i>Tous</i> pour <u>Exporter tout le contenu du type spécifié</u> .                                                                                                                                                                                                  |
| <code>-o [chemin_fichier]</code><br>ou<br><code>--output-directory [chemin_fichier]</code>                                         | Indique le chemin d'accès complet au répertoire dans lequel le fichier d'exportation est écrit.<br><br>Si aucun répertoire de sortie n'est spécifié, le contenu est exporté dans le répertoire en cours. Si le répertoire de sortie indiqué n'existe pas, il est créé.                                                                                                                                                                           |

Tableau 68. Paramètres de script `contentManagement.pl` pour l'exportation de contenu personnalisé d'un type spécifique (suite)

| Paramètre                                                                                        | Description                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-t</b> <i>[type_compression]</i><br>ou<br><b>--compression-type</b> <i>[type_compression]</i> | Indique le type de compression du fichier d'exportation.<br><br>Les options valides sont ZIP et TARGZ (sensible à la casse). Si vous n'indiquez pas de type de compression, le type de compression par défaut est ZIP. |

#### Exemples :

- Pour exporter toutes les recherches personnalisées, entrez la commande suivante :

```
./contentManagement.pl --action export --content-type search --id all
```

- Pour exporter tous les rapports et inclure les données cumulées, entrez la commande suivante :

```
./contentManagement.pl -a export -c 10 --id all --global-view
```

## Résultats

Le contenu est exporté dans un fichier compressé, par exemple, `reports-ContentExport-20151022101803.zip`. Vous pouvez modifier manuellement le nom de fichier en un nom plus descriptif. Le fichier exporté peut contenir plus d'éléments de contenu que prévu car toutes les dépendances sont exportées avec les éléments de contenu spécifiés. Par exemple, si vous exportez un rapport, la recherche sauvegardée utilisée par le rapport est également exportée.

## Recherche d'éléments de contenu spécifiques à exporter

Vous utilisez le script de gestion de contenu pour rechercher un contenu spécifique dans votre déploiement IBM QRadar . Après avoir trouvé le contenu, vous pouvez utiliser l'identificateur unique pour exporter l'objet de contenu.

### Pourquoi et quand exécuter cette tâche

Le tableau suivant répertorie les identificateurs à utiliser lorsque vous souhaitez rechercher des types de contenu spécifiques.

| Type de contenu personnalisé    | Identificateur de texte     | Identificateur numérique |
|---------------------------------|-----------------------------|--------------------------|
| Tableaux de bord                | <b>dashboard</b>            | 4                        |
| Rapports                        | <b>report</b>               | 10                       |
| Recherches sauvegardées         | <b>search</b>               | 1                        |
| FGroups <sup>1</sup>            | <b>fgroup</b>               | 12                       |
| Types de FGroup                 | <b>fgrouptype</b>           | 13                       |
| Règles personnalisées           | <b>customrule</b>           | 3                        |
| Propriétés personnalisées       | <b>customproperty</b>       | 6                        |
| Sources de journal              | <b>sensordevice</b>         | 17                       |
| Types de source de journal      | <b>sensordevicetype</b>     | 24                       |
| Catégories de source de journal | <b>sensordevicecategory</b> | 18                       |

Tableau 69. Identificateurs de type de contenu pour la recherche de contenu personnalisé (suite)

| Type de contenu personnalisé        | Identificateur de texte      | Identificateur numérique |
|-------------------------------------|------------------------------|--------------------------|
| Extensions de source de journal     | <b>deviceextension</b>       | 16                       |
| Collecte de données de référence    | <b>referencedata</b>         | 28                       |
| Entrées de mappe QID personnalisée  | <b>qidmap</b>                | 27                       |
| Profils de corrélation d'historique | <b>historicalsearch</b>      | 25                       |
| Fonctions personnalisées            | <b>custom_function</b>       | 77                       |
| Actions personnalisées              | <b>custom_action</b>         | 78                       |
| Applications                        | <b>installed_application</b> | 100                      |

<sup>1</sup>Un FGroup représente un groupe de contenu, tel qu'un groupe de sources de journal, un groupe de rapports ou un groupe de recherche.

## Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire `/opt/qradar/bin` et entrez la commande suivante pour rechercher un contenu personnalisé qui correspond à une expression régulière :

```
./contentManagement.pl -a search -c [content_type] -r [regex]
```

### Paramètres :

Tableau 70. Paramètres de script `contentManagement.pl` pour la recherche d'éléments de contenu

| Paramètre                                                              | Description                                                                                                                                                                                                                          |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-c [contenu_type]</b><br>ou<br><b>--content-type [contenu_type]</b> | Indique le type de contenu à rechercher.<br><br>Vous devez spécifier le fichier <u>Type de contenu à rechercher</u> . Vous ne pouvez pas utiliser <code>-c package</code> ou <code>-c all</code> avec l'action <code>search</code> . |
| <b>-r [regex]</b><br>ou<br><b>--regex [regex]</b>                      | Indique le contenu à rechercher.<br><br>Tout le contenu correspondant à l'expression s'affiche.                                                                                                                                      |

### Exemples :

- Pour rechercher tous les rapports qui incluent `Aperçu` dans la description, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl --action search  
--content-type report --regex "Overview"
```

- Pour répertorier toutes les sources de journal, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl -a search -c 17 -r "\w"
```

Les détails de la liste des résultats de la recherche, y compris l'ID unique, pour les éléments de contenu trouvés.

```
[INFO] Search results:  
[INFO] - [ID] - [Name] - [Description]  
[INFO] - [67] - [Asset Profiler-2 :: hostname] - [Asset Profiler]
```

```
[INFO] - [62] - [SIM Generic Log DSM-7 :: hostname] - [SIM Generic Log DSM]
[INFO] - [63] - [Custom Rule Engine-8 :: hostname] - [Custom Rule Engine]
[INFO] - [71] - [Pix @ apophis] - [Pix device]
[INFO] - [70] - [Snort @ wolverine] - [Snort device]
[INFO] - [64] - [SIM Audit-2 :: hostname] - [SIM Audit]
[INFO] - [69] - [Health Metrics-2 :: hostname] - [Health Metrics]
```

## Que faire ensuite

Utilisez l'identificateur unique pour exporter des éléments de contenu spécifiques à partir de QRadar. Pour plus d'informations, voir «Exportation d'éléments de contenu personnalisés de types différents», à la page 320 et «Exportation d'un élément de contenu personnalisé unique», à la page 319.

## Exportation d'un élément de contenu personnalisé unique

Exportez un élément de contenu personnalisé unique, tel qu'une règle personnalisée ou une recherche enregistrée, à partir de IBM QRadar.

### Avant de commencer

Vous devez connaître l'identificateur unique de l'élément de contenu personnalisé que vous souhaitez exporter. Pour plus d'informations sur la recherche des identificateurs uniques pour les éléments de contenu, voir «Recherche d'éléments de contenu spécifiques à exporter», à la page 317.

### Procédure

1. Utilisez SSH pour vous connecter à QRadar en tant que superutilisateur.
2. Allez dans le répertoire `/opt/qradar/bin` et entrez la commande permettant d'exporter le contenu :

```
./contentManagement.pl -a export -c [content_type] -i [content_identifieur]
```

#### Paramètres :

| <i>Tableau 71. Paramètres de script contentManagement.pl pour l'exportation d'un élément de contenu unique</i> |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
| -c [type_de_contenu]<br>ou<br>--content-type [type_de_contenu]                                                 | Indique le type de contenu à exporter.<br><br>Entrez l'identificateur de texte correspondant ou l'identificateur numérique pour des types de contenu spécifiques.                                                                                                                                                                                                                                                     |
| -e<br>ou<br>--include-reference-data-elements                                                                  | Définissez cet indicateur pour inclure des clés de données de référence et des éléments dans l'exportation.<br><br>Les clés de données de référence et les éléments de données de référence sont applicables au type de contenu <code>referencedata</code> . Ce paramètre est applicable uniquement lorsque vous exportez des données de référence ou des éléments de contenu qui dépendent des données de référence. |
| -g<br>ou<br>--global-view                                                                                      | Inclut les données cumulées dans l'exportation.                                                                                                                                                                                                                                                                                                                                                                       |

| Tableau 71. Paramètres de script <code>contentManagement.pl</code> pour l'exportation d'un élément de contenu unique (suite) |                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                                                                    | Description                                                                                                                                                                                                                                                            |
| <b>-i</b> [identificateur_de_contenu]<br>ou<br><b>--id</b> [identificateur_de_contenu]                                       | Indique l'Identificateur d'une instance spécifique de contenu personnalisé, par exemple un seul rapport ou un seul ensemble de références.                                                                                                                             |
| <b>-o</b> [chemin_du_fichier]<br>ou<br><b>--output-directory</b> [chemin_du_fichier]                                         | Indique le chemin d'accès complet au répertoire dans lequel le fichier d'exportation est écrit.<br><br>Si aucun répertoire de sortie n'est spécifié, le contenu est exporté dans le répertoire en cours. Si le répertoire de sortie indiqué n'existe pas, il est créé. |
| <b>-t</b> [type_de_compression]<br>ou<br><b>--compression-type</b> [type_de_compression]                                     | Utilisé avec l'action <code>export</code> .<br><br>Indique le type de compression du fichier d'exportation. Les options valides sont ZIP et TARGZ (sensible à la casse). Si vous n'indiquez pas de type de compression, le type de compression par défaut est ZIP.     |

#### Exemples :

- Pour exporter le tableau de bord ayant l'ID 7 dans le répertoire en cours, entrez la commande suivante :

```
./contentManagement.pl -a export -c dashboard -i 7
```

- Pour exporter la source de journal dont l'ID est 70, y compris les données cumulées, dans le répertoire `/store/cmt/exports`, entrez la commande suivante :

```
./contentManagement.pl -a export -c sensordevice -i 70 -o /store/cmt/exports -g
```

## Résultats

Le contenu est exporté dans un fichier compressé `.zip`. Le fichier exporté peut contenir plus d'éléments de contenu que prévu car toutes les dépendances sont exportées avec les éléments de contenu spécifiés. Par exemple, si vous exportez un rapport, la recherche sauvegardée utilisée par le rapport est également exportée. Vous pouvez modifier manuellement le nom de fichier en un nom plus descriptif.

## Exportation d'éléments de contenu personnalisés de types différents

Exportez plusieurs éléments de contenu personnalisés à partir de IBM QRadar, tels que des règles personnalisées ou des tableaux de bord et des rapports, à l'aide du script de gestion de contenu.

### Avant de commencer

Vous devez connaître les identificateurs uniques pour chaque élément de contenu personnalisé que vous souhaitez exporter. Pour plus d'informations sur la recherche des identificateurs uniques pour les éléments de contenu, voir [«Recherche d'éléments de contenu spécifiques à exporter»](#), à la page 317.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Créez un fichier texte qui répertorie le contenu que vous souhaitez exporter.

Chaque ligne doit inclure le type de contenu personnalisé suivi d'une liste d'ID uniques séparés par des virgules pour ce type.

**Exemple :** Pour exporter deux tableaux de bord ayant l'ID 5 et l'ID 7, toutes les règles personnalisées et un groupe, créez un fichier texte contenant les entrées suivantes :

```
dashboard, 5,7
customrule, all
fgroup, 77
```

3. Allez à /opt/qradar/bin et entrez la commande pour exporter le contenu :

```
./contentManagement.pl -a export -c package -f [source_file]
```

#### Paramètres :

| <i>Tableau 72. Paramètres de script contentManagement.pl pour l'exportation de différents types d'objet de contenu</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>-c</b> [contenu_type]<br>ou<br><b>--content-type</b> [contenu_type]                                                 | Indique le type de contenu.<br><br>Vous pouvez spécifier -c package ou entrer <u>Identificateur de texte ou numérique correspondant pour des types de contenu spécifiques</u> . Lorsque vous utilisez -c package, vous devez spécifier les paramètres de --file ou --name .                                                                                                                                                         |
| <b>-e</b><br>ou<br><b>--include-reference-data-elements</b>                                                            | Définissez cet indicateur pour inclure des clés de données de référence et des éléments dans l'exportation.<br><br>Les clés de données de référence et les éléments de données de référence sont applicables au type de contenu referencedata . Ce paramètre est applicable uniquement lorsque vous exportez des données de référence ou des éléments de contenu qui dépendent des données de référence.                            |
| <b>-f</b> [fichier_source]<br>ou<br><b>--file</b> [fichier_source]                                                     | Indique le chemin d'accès et le nom du fichier texte qui contient la liste des éléments de contenu personnalisés que vous souhaitez exporter.<br><br>La première fois que vous utilisez le paramètre --file , un fichier modèle de package est écrit dans le répertoire /store/cmt/packages afin que vous puissiez le réutiliser.<br><br>Le nom de fichier et le chemin sont sensibles à la casse.                                  |
| <b>-g</b><br>ou<br><b>--global-view</b>                                                                                | Inclut les données cumulées dans l'exportation.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>-n</b> [nom]<br>ou<br><b>--name</b> [nom]                                                                           | Indique le nom du fichier modèle de package qui contient la liste des contenus personnalisés à exporter.<br><br>Le fichier modèle de package est créé la première fois que vous utilisez le paramètre --file . Par défaut, le paramètre --name suppose que le fichier texte se trouve dans le répertoire /store/cmt/packages .<br><br>Vous devez indiquer le paramètre --file ou --name lorsque --content-type package est utilisé. |

| Tableau 72. Paramètres de script <code>contentManagement.pl</code> pour l'exportation de différents types d'objet de contenu (suite) |                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                                                                            | Description                                                                                                                                                                                                                                                        |
| <b>-o</b> <i>[chemin_fichier]</i><br>ou<br><b>--output-directory</b> <i>[chemin_fichier]</i>                                         | Indique le chemin d'accès complet au répertoire dans lequel le fichier d'exportation est écrit.<br>Si aucun répertoire de sortie n'est spécifié, le contenu est exporté dans le répertoire en cours. Si le répertoire de sortie indiqué n'existe pas, il est créé. |
| <b>-t</b> <i>[type_compression]</i><br>ou<br><b>--compression-type</b> <i>[type_compression]</i>                                     | Indique le type de compression du fichier d'exportation.<br>Les types de compression valides sont ZIP et TARGZ (sensible à la casse). Si vous n'indiquez pas de type de compression, le type de compression par défaut est ZIP.                                    |

### Exemples :

- Pour exporter tous les éléments du fichier `exportlist.txt` dans le répertoire `qradar` et enregistrer le fichier exporté dans le répertoire en cours, entrez la commande suivante :

```
./contentManagement.pl -a export -c package -f /qradar/exportlist.txt
```

- Pour exporter tous les éléments du fichier `exportlist.txt` dans le répertoire `qradar`, y compris les données cumulées, et enregistrer la sortie dans le répertoire `/store/cmt/exports`, entrez la commande suivante :

```
./contentManagement.pl -a export -c package
```

```
--file /qradar/exportlist.txt -o /store/cmt/exports -g
```

Lorsque vous utilisez le paramètre **--file**, un fichier modèle de package est automatiquement généré dans `/store/cmt/packages`. Pour utiliser le fichier modèle de package, indiquez le nom de fichier comme valeur du paramètre **--name**.

## Résultats

Le contenu est exporté dans un fichier compressé `.zip`. Le fichier exporté peut contenir plus d'éléments de contenu que prévu car toutes les dépendances sont exportées avec les éléments de contenu spécifiés. Par exemple, si vous exportez un rapport, la recherche sauvegardée utilisée par le rapport est également exportée. Vous pouvez modifier manuellement le nom de fichier en un nom plus descriptif.

## Installation des extensions à l'aide d'extensions Management

Utilisez l'outil **Gestion des extensions** pour ajouter des extensions de sécurité à IBM QRadar. L'outil **Gestion des extensions** vous permet d'afficher les éléments de contenu dans l'extension et de spécifier la méthode de traitement des mises à jour de contenu avant d'installer l'extension.

### Avant de commencer

Les extensions doivent être sur votre ordinateur local avant de les installer dans QRadar.


Vous pouvez télécharger des extensions QRadar à partir de IBM Security App Exchange (<https://apps.xforce.ibmcloud.com/>) et de IBM Fix Central ([www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)).



## Pourquoi et quand exécuter cette tâche

Une extension est un ensemble de fonctions QRadar. Une extension peut inclure des contenus tels que des règles, des rapports, des recherches, des ensembles de références et des tableaux de bord. Il peut également inclure des applications qui améliorent les fonctions QRadar.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des extensions**.
3. Pour télécharger une nouvelle extension vers la console QRadar, procédez comme suit :
  - a) Cliquez sur **Ajouter**.
  - b) Cliquez sur **Parcourir** et naviguez pour trouver l'extension.
  - c) Cliquez sur **Installer immédiatement** pour installer l'extension sans afficher le contenu. Accédez à «5.b», à la page 323.
  - d) Cliquez sur **Ajouter**.
4. Pour afficher le contenu de l'extension, sélectionnez-le dans la liste des extensions et cliquez sur **Détails supplémentaires**.
5. Pour installer l'extension, procédez comme suit :
  - a) Sélectionnez l'extension dans la liste et cliquez sur **Installation**.
  - b) Pour affecter un utilisateur à l'application, sélectionnez le menu **Sélection de l'utilisateur** et sélectionnez un utilisateur.  
Par exemple, vous pouvez associer l'application à un utilisateur spécifié qui est répertorié dans le menu **Sélection de l'utilisateur** qui dispose des droits définis.

#### Remarque :

Cet écran n'apparaît que si l'une des applications de l'extension que vous installez est configurée pour demander l'authentification pour les processus d'arrière-plan.

- c) Si l'extension n'inclut pas de signature numérique, ou si elle est signée mais que la signature n'est pas associée à l'autorité de certification de sécurité IBM, vous devez confirmer que vous souhaitez toujours l'installer. Cliquez sur **Installation** pour poursuivre l'installation.
- d) Vérifiez les modifications apportées par l'installation au système.
- e) Sélectionnez **Conserver les articles existants** ou **Remplacer les éléments existants** pour indiquer comment traiter les éléments de contenu existants.

**Remarque :** Si l'extension contient des règles système remplacées, sélectionnez **Remplacer les éléments existants** pour vous assurer que les règles sont correctement importées.

- f) Cliquez sur **Installer**.
- g) Consultez le récapitulatif de l'installation et cliquez sur **OK**.

## Désinstallation d'une extension de contenu

Supprimez une extension de contenu qui n'est plus utile ou qui a un impact négatif sur le système. Vous pouvez supprimer des règles, des propriétés personnalisées, des données de référence et des recherches sauvegardées. Il se peut que vous ne soyez pas en mesure de supprimer un contenu si un autre objet de contenu en dépend.

## Pourquoi et quand exécuter cette tâche


Lorsque vous désinstallez une extension de contenu, toutes les règles, les propriétés personnalisées et les données de référence qui ont été installées par l'extension de contenu sont supprimées ou répercutées sur leur état précédent. Les recherches sauvegardées ne peuvent pas être rétablies. Elles peuvent uniquement être supprimées.

Par exemple, si vous avez édité des règles personnalisées dans une application que vous souhaitez maintenant désinstaller, vous pouvez conserver les modifications que vous avez apportées pour chaque règle personnalisée. Si la règle personnalisée existait précédemment sur le système, vous pouvez rétablir la règle dans son état précédent. Si la règle personnalisée n'existait pas précédemment, vous pouvez la supprimer.

**Remarque :**

Si vous avez introduit une dépendance externe sur une extension de contenu installée par l'application, QRadar ne supprime pas ce contenu lorsque vous désinstallez l'application. Par exemple, si vous créez une règle personnalisée qui utilise l'une des propriétés personnalisées de l'application, cette propriété personnalisée n'est pas supprimée lorsque vous désinstallez l'application.

## Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Configuration du système**, cliquez sur **Gestion des extensions**.
3. Sélectionnez l'extension à désinstaller et cliquez sur **Désinstaller**.  
QRadar recherche les applications, les règles, les propriétés personnalisées, les données de référence et les recherches sauvegardées qui sont installées par l'extension de contenu qui peut être supprimée.
4. Si vous avez modifié manuellement les règles, les propriétés personnalisées ou les données de référence après avoir installé l'application, choisissez **Conserver** ou **Retirer / reverser** cette extension de contenu.
5. Cliquez sur **Désinstaller**, puis sur **OK**.

## Importation de contenu à l'aide du script de gestion de contenu

Vous pouvez importer du contenu personnalisé que vous avez exporté à partir d'un autre système IBM QRadar .

### Avant de commencer

Si vous souhaitez importer du contenu à partir d'un autre système QRadar, vous devez d'abord exporter le contenu et le copier sur le système cible. Pour plus d'informations sur l'exportation de contenu, voir [«Identificateurs de type de contenu pour l'exportation de contenu personnalisé»](#), à la page 326.

Lorsque vous importez du contenu qui possède des sources de journal, vérifiez que DSM et les RPM de protocole sont installés et en cours sur le système cible.

**Remarque :** Si le contenu contient des règles système écartées, utilisez l'action `update` au lieu de l'action `import` pour vous assurer que les règles sont correctement importées.

Vous pouvez exporter le contenu à partir d'une version antérieure de QRadar et l'importer dans une version ultérieure. Cependant, vous ne pouvez pas importer du contenu d'une version ultérieure vers une version antérieure.

Vous n'avez pas à exporter du contenu dans un ordre spécifique. Toutefois, ne démarrez pas plusieurs importations sur le même système en même temps. Les importations échouent en raison de conflits avec des ressources partagées.

## Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire dans lequel se trouve le fichier de contenu d'exportation.
3. Entrez cette commande pour importer le contenu :

```
/opt/qradar/bin/contentManagement.pl -a import -f [source_file] -u [user]
```

**Paramètres :**

Tableau 73. Paramètres de script `contentManagement.pl` pour l'importation de contenu personnalisé

| Paramètre                                                                            | Description                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-f</b> [ <i>fichier_source</i> ]<br>ou<br><b>--file</b> [ <i>fichier_source</i> ] | Indique le fichier contenant les éléments de contenu à importer.<br>Les types de fichier valides sont zip, targz, et xml.<br>Le nom et le chemin du fichier sont sensibles à la casse.                |
| <b>-u</b> [ <i>utilisateur</i> ]<br>ou<br><b>--user</b> [ <i>utilisateur</i> ]       | Indique l'utilisateur qui remplace le propriétaire actuel lorsque vous importez des données spécifiques à l'utilisateur. L'utilisateur doit exister sur le système cible avant d'importer le contenu. |

#### Exemples :

- Pour importer du contenu à partir du fichier `fgroup-ContentExport-20120418163707.tar.gz` dans le répertoire en cours, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl --action import
-f fgroup-ContentExport-20120418163707.tar.gz
```

- Pour importer du contenu à partir du fichier `fgroup-ContentExport-20120418163707.tar.gz` dans le répertoire en cours et faire de l'utilisateur `admin` le propriétaire de toutes les données sensibles de l'importation, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl --action import
--file fgroup-ContentExport-20120418163707.tar.gz --user admin
```

Le script d'importation affiche le message suivant lorsque les données de référence sont collectées activement lors de l'exportation : *Violation de contrainte de clé externe*. Pour éviter ce problème, exécutez le processus d'exportation lorsqu'aucune donnée de référence n'est en cours de collecte.

#### Tâches associées

«Mise à jour du contenu à l'aide du script de gestion de contenu», à la page 325

Utilisez l'action de mise à jour pour mettre à jour le contenu IBM QRadar existant ou ajouter un nouveau contenu au système.

## Mise à jour du contenu à l'aide du script de gestion de contenu

Utilisez l'action de mise à jour pour mettre à jour le contenu IBM QRadar existant ou ajouter un nouveau contenu au système.

#### Avant de commencer

Si vous souhaitez mettre à jour le contenu avec du contenu exporté à partir d'un autre système QRadar, vérifiez que le fichier exporté se trouve sur le système cible. Pour plus d'informations sur l'exportation de contenu, voir «Identificateurs de type de contenu pour l'exportation de contenu personnalisé», à la page 326.

Lorsque vous importez du contenu qui possède des sources de journal, vérifiez que DSM et les RPM de protocole sont installés et en cours sur le système cible.

Vous pouvez exporter le contenu à partir d'une version antérieure de QRadar et l'importer dans une version ultérieure. Cependant, vous ne pouvez pas importer du contenu d'une version ultérieure vers une version antérieure.

Vous n'avez pas à exporter du contenu dans un ordre spécifique. Toutefois, ne démarrez pas plusieurs importations sur le même système en même temps. Les importations échoueront en raison de conflits avec des ressources partagées.

## Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Pour mettre à jour le contenu, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl -a update -f [source_file]
```

### Paramètres :

| <i>Tableau 74. Paramètres de script contentManagement.pl pour la mise à jour du contenu personnalisé</i> |                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Paramètre                                                                                                | Description                                                                                                                                                                                                  |
| <b>-f</b> [fichier_source]<br>ou<br><b>--file</b> [fichier_source]                                       | Indique le fichier contenant les éléments de contenu à mettre à jour.<br><br>Les types de fichier valides sont zip, targz, et xml.<br><br>Le nom de fichier et le chemin sont sensibles à la casse.          |
| <b>-u</b> [utilisateur]<br>ou<br><b>--user</b> [utilisateur]                                             | Indique l'utilisateur qui remplace le propriétaire actuel lorsque vous importez des données spécifiques à l'utilisateur.<br><br>L'utilisateur doit exister sur le système cible avant d'importer le contenu. |

### Exemple :

- Pour mettre à jour en fonction du contenu du fichier fgroup-ContentExport-20120418163707.zip, entrez la commande suivante :

```
/opt/qradar/bin/contentManagement.pl --action update  
-f fgroup-ContentExport-20120418163707.zip
```

## Identificateurs de type de contenu pour l'exportation de contenu personnalisé

Lorsque vous exportez un type spécifique de contenu personnalisé à partir de IBM QRadar, vous devez spécifier le type de contenu. Vous devez utiliser l'identificateur de texte ou l'identificateur numérique du type de contenu.

Lorsque vous exportez du contenu à partir d'un dispositif QRadar, le script de gestion de contenu vérifie les dépendances de contenu, puis inclut le contenu associé dans l'exportation.

Par exemple, lorsque le script de gestion de contenu détecte qu'une recherche sauvegardée est associée à un rapport que vous souhaitez exporter, la recherche sauvegardée est également exportée. Vous ne pouvez pas exporter d'infraction, d'actif ou de recherche de vulnérabilité.

Vous utilisez l'identificateur de type de contenu lorsque vous souhaitez exporter tous les contenus personnalisés d'un type spécifique. Si vous souhaitez exporter un élément de contenu spécifique à partir de votre déploiement QRadar, vous devez connaître l'identificateur unique de cet élément de contenu spécifique.

Pour plus d'informations, voir «Recherche d'éléments de contenu spécifiques à exporter», à la page 317.

Le tableau suivant décrit les identificateurs de type de contenu qui sont transmis au script `contentManagement.pl` pour le paramètre `-c`.

*Tableau 75. Identificateurs de type de contenu pour l'exportation de contenu personnalisé*

| Type de contenu personnalisé        | Identificateur de texte      | Identificateur numérique |
|-------------------------------------|------------------------------|--------------------------|
| Tous les contenus personnalisés     | <b>all</b>                   | Non applicable           |
| Liste personnalisée de contenu      | <b>package</b>               | Non applicable           |
| Tableaux de bord                    | <b>dashboard</b>             | 4                        |
| Rapports                            | <b>report</b>                | 10                       |
| Recherches sauvegardées             | <b>search</b>                | 1                        |
| FGroups <sup>1</sup>                | <b>fgroup</b>                | 12                       |
| Types de FGroup                     | <b>fgrouptype</b>            | 13                       |
| Règles personnalisées               | <b>customrule</b>            | 3                        |
| Propriétés personnalisées           | <b>customproperty</b>        | 6                        |
| Sources de journal                  | <b>sensordevice</b>          | 17                       |
| Types de source de journal          | <b>sensordevicetype</b>      | 24                       |
| Catégories de source de journal     | <b>sensordevicecategory</b>  | 18                       |
| Extensions de source de journal     | <b>deviceextension</b>       | 16                       |
| Collecte de données de référence    | <b>referencedata</b>         | 28                       |
| Entrées de mappe QID personnalisée  | <b>qidmap</b>                | 27                       |
| Profils de corrélation d'historique | <b>historicalsearch</b>      | 25                       |
| Fonctions personnalisées            | <b>custom_function</b>       | 77                       |
| Actions personnalisées              | <b>custom_action</b>         | 78                       |
| Applications                        | <b>installed_application</b> | 100                      |

<sup>1</sup>Un FGroup est un groupe de contenu tel qu'un groupe de sources de journal, un groupe de rapports ou un groupe de recherche.

## Paramètres de script de gestion de contenu

Utilisez le script `contentManagement.pl` pour exporter du contenu à partir d'un déploiement IBM QRadar et l'importer dans un autre déploiement.

Le tableau suivant décrit les paramètres du script `contentManagement.pl` et les actions auxquelles chaque paramètre s'applique.

```
/opt/qradar/bin/contentManagement.pl --action [action_type] [script_parameters]
```

Tableau 76. Paramètres de script `contentManagement.pl`

| Paramètre                                                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>-a</b> <i>[type_d'action]</i></p> <p>ou</p> <p><b>--action</b> <i>[type_d'action]</i></p>           | <p>Obligatoire. Indique l'action.</p> <p>Les types d'actions valides sont export, search, importet update.</p> <p>L'action import ajoute uniquement du contenu qui n'existe pas dans le déploiement.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>-c</b> <i>[type_de_contenu]</i></p> <p>ou</p> <p><b>--content-type</b> <i>[type_de_contenu]</i></p> | <p>Utilisé avec les actions export et search . Indique le type de contenu.</p> <p>Lorsqu'il est utilisé avec l'action export , vous pouvez indiquer -c all ou -c package, ou bien vous pouvez entrer <u>le texte ou l'identificateur numérique correspondant pour des types de contenu spécifiques</u>. Lorsque vous utilisez -c package, vous devez indiquer les paramètres --file ou --name .</p> <p>Lorsqu'il est utilisé avec l'action search , vous devez indiquer le <u>type de contenu à rechercher</u>. Vous ne pouvez pas utiliser -c package ou -c all avec l'action search .</p>                                                                                                                       |
| <p><b>-d</b></p> <p>ou</p> <p><b>--debug</b></p>                                                          | <p>Utilisé avec toutes les actions.</p> <p>Utilisez la journalisation de niveau de débogage lorsque vous exécutez le script <code>contentManagement.pl</code> pour afficher des informations plus détaillées, telles que des journaux pour le support technique.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p><b>-e</b></p> <p>ou</p> <p><b>--include-reference-data-elements</b></p>                                | <p>Utilisé avec l'action export .</p> <p>Définissez cet indicateur pour inclure des clés de données de référence et des éléments dans l'exportation.</p> <p>Les clés de données de référence et les éléments de données de référence sont applicables au type de contenu <code>referencedata</code> . Ce paramètre est applicable uniquement lorsque vous exportez des données de référence ou des éléments de contenu qui dépendent des données de référence.</p>                                                                                                                                                                                                                                                |
| <p><b>-f</b> <i>[chemin_de_fichier]</i></p> <p>ou</p> <p><b>--file</b> <i>[chemin_de_fichier]</i></p>     | <p>Utilisé avec les actions export, importet update .</p> <p>Lorsqu'il est utilisé avec l'action export , indique le chemin et le nom de fichier du fichier texte qui contient la liste des éléments de contenu personnalisé que vous souhaitez exporter. La première fois que vous utilisez le paramètre --file , un fichier modèle de package est écrit dans le répertoire <code>/store/cmt/packages</code> afin que vous puissiez le réutiliser.</p> <p>Lorsqu'il est utilisé avec l'action import ou update , spécifie le fichier qui contient les éléments de contenu à importer. Les types de fichier valides sont zip, targz, et xml.</p> <p>Le nom de fichier et le chemin sont sensibles à la casse.</p> |

Tableau 76. Paramètres de script `contentManagement.pl` (suite)

| Paramètre                                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>-g</b></p> <p>ou</p> <p><b>--global-view</b></p>                                                                | <p>Utilisé avec l'action <code>export</code> .</p> <p>Inclut les données cumulées dans l'exportation.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p><b>-h</b> <i>[type_d'action]</i></p> <p>ou</p> <p><b>--help</b> <i>[type_d'action]</i></p>                         | <p>Utilisé avec toutes les actions.</p> <p>Affiche l'aide spécifique à <code>action_type</code>. Lorsqu'aucun <code>action_type</code> n'est spécifié, affiche un message d'aide générale.</p>                                                                                                                                                                                                                                                                                                                                                                               |
| <p><b>-i</b> <i>[identificateur_de_contenu]</i></p> <p>ou</p> <p><b>--id</b> <i>[identificateur_de_contenu]</i></p>   | <p>Utilisé avec l'action <code>export</code> .</p> <p>Indique l'Identificateur d'une instance spécifique de contenu personnalisé, par exemple un seul rapport ou un seul ensemble de références. Vous pouvez indiquer <i>Tous</i> pour <a href="#">Exporter tout le contenu du type spécifié</a>.</p>                                                                                                                                                                                                                                                                        |
| <p><b>-n</b> <i>[nom]</i></p> <p>ou</p> <p><b>--name</b> <i>[nom]</i></p>                                             | <p>Utilisé avec l'action <code>export</code> .</p> <p>Indique le nom du fichier modèle de package qui contient la liste des contenus personnalisés à exporter.</p> <p>Le fichier modèle de package est créé la première fois que vous utilisez le paramètre <code>--file</code> . Le paramètre <code>--name</code> suppose que le fichier modèle de package se trouve dans le répertoire <code>/store/cmt/packages</code> .</p> <p>Vous devez spécifier le paramètre <code>--file</code> ou <code>--name</code> lorsque <code>--content-type package</code> est utilisé.</p> |
| <p><b>-o</b> <i>[chemin_du_fichier]</i></p> <p>ou</p> <p><b>--output-directory</b> <i>[chemin_du_fichier]</i></p>     | <p>Utilisé avec l'action <code>export</code> .</p> <p>Indique le chemin d'accès complet au répertoire dans lequel le fichier d'exportation est écrit.</p> <p>Si aucun répertoire de sortie n'est spécifié, le contenu est exporté dans le répertoire en cours. Si le répertoire de sortie indiqué n'existe pas, il est créé.</p>                                                                                                                                                                                                                                             |
| <p><b>-q</b></p> <p>ou</p> <p><b>--quiet</b></p>                                                                      | <p>Utilisé avec toutes les actions. Aucun résultat n'apparaît à l'écran.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>-r</b> <i>[regex]</i></p> <p>ou</p> <p><b>--regex</b> <i>[regex]</i></p>                                        | <p>Utilisé avec l'action <code>search</code> .</p> <p>Lors de la recherche, vous devez utiliser le paramètre <code>--regex</code> pour indiquer le contenu à rechercher. Tout le contenu correspondant à l'expression s'affiche.</p>                                                                                                                                                                                                                                                                                                                                         |
| <p><b>-t</b> <i>[type_de_compression]</i></p> <p>ou</p> <p><b>--compression-type</b> <i>[type_de_compression]</i></p> | <p>Utilisé avec l'action <code>export</code> .</p> <p>Indique le type de compression du fichier d'exportation. Les types de compression valides sont ZIP et TARGZ (sensible à la casse). Si vous n'indiquez pas de type de compression, le type de compression par défaut est ZIP.</p>                                                                                                                                                                                                                                                                                       |

Tableau 76. Paramètres de script `contentManagement.pl` (suite)

| Paramètre                                                             | Description                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>-u</b> [utilisateur]<br/>ou<br/><b>--user</b> [utilisateur]</p> | <p>Utilisé avec l'action <code>import</code> .<br/><br/>Indique l'utilisateur qui remplace le propriétaire actuel lorsque vous importez des données spécifiques à l'utilisateur. L'utilisateur doit exister sur le système cible avant d'importer le contenu.</p> |
| <p><b>-v</b><br/>ou<br/><b>--verbose</b></p>                          | <p>Utilisé avec toutes les actions.<br/><br/>Utilisez lorsque vous vous connectez pour afficher les informations de niveau par défaut pour l'outil de gestion de contenu.</p>                                                                                     |



---

## Chapitre 22. Configuration des alertes SNMP

IBM QRadar utilise l'agent Net-SNMP, qui prend en charge diverses MIB de surveillance des ressources système. Ils peuvent être interrogés par les solutions de gestion de réseau pour la surveillance et l'alerte des ressources système. Pour plus d'informations sur Net-SNMP, voir la documentation Net-SNMP.

Dans IBM QRadar, vous pouvez configurer une règle pour générer une réponse à la règle qui envoie une alerte SNMP lorsque les conditions configurées sont remplies. QRadar agit en tant qu'agent pour envoyer les alertes SNMP à un autre système.

Une alerte SNMP (Simple Network Management Protocol) est une notification d'événement ou d'infraction envoyée par QRadar à un hôte SNMP configuré pour un traitement supplémentaire.

Personnalisez les paramètres de configuration SNMP dans l'assistant de règles personnalisées et modifiez les alertes SNMP que le moteur de règles personnalisé envoie à d'autres logiciels pour la gestion. QRadar fournit deux alertes par défaut. Toutefois, vous pouvez ajouter des alertes personnalisées ou modifier les pièges existants pour utiliser de nouveaux paramètres.

Pour plus d'informations sur SNMP, accédez au site Web [Le Groupe de travail sur l'ingénierie de l'Internet](http://www.ietf.org/) (<http://www.ietf.org/>) et entrez RFC 1157 dans la zone de recherche.

**Important :** Les réponses des règles SNMPv3 sont envoyées sous forme d'informations SNMP et non de pièges.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Personnalisation des informations d'alerte SNMP envoyées à un autre système

Dans IBM QRadar, vous pouvez éditer les paramètres d'alerte SNMP pour personnaliser les informations envoyées à un autre système de gestion SNMP lorsqu'une condition de règle est remplie.

**Restriction :** Les paramètres d'alerte SNMP sont affichés dans l'assistant de règles personnalisées uniquement si SNMP est activé dans les paramètres du système QRadar.

**Important :** Les réponses des règles SNMPv3 sont envoyées sous forme d'informations SNMP et non de pièges.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire `/opt/qradar/conf` et faites des copies de sauvegarde des fichiers suivants :
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
3. Ouvrez le fichier de configuration pour l'éditer.
  - Pour éditer les paramètres SNMP pour les règles d'événement, ouvrez le fichier `eventCRE.snmp.xml`.
  - Pour éditer les paramètres SNMP pour les règles de d'infraction, ouvrez le fichier `offenseCRE.snmp.xml`.
4. À l'intérieur de l'élément `<snmp>` et avant l'élément `<creSNMPTrap>`, insérez la section suivante, mettant à jour les libellés selon les besoins :

```
<creSNMPResponse name="snmp_response_1">
  <custom name="MyColor">
    <string label="What is your favorite color?"/>
  </custom>
```

```
<custom name="MyCategory">
  <list label="Select a category">
    <option label="Label1" value="Category1"/>
    <option label="Label2" value="Category2"/>
  </list>
</custom>
</creSNMPResponse>
```

5. Sauvegardez le fichier et fermez-le.
6. Copiez le fichier du répertoire /opt/qradar/conf vers le répertoire /store/configservices/staging/globalconfig.
7. Connectez-vous à l'interface QRadar.
8. Dans l'onglet **Admin**, sélectionnez **Avancé** > **Déployer la configuration entière**.

**Important** : QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Que faire ensuite

Personnalisez la sortie de l'alerte SNMP.

## Personnalisation de la sortie d'alerte SNMP

IBM QRadar utilise SNMP pour envoyer des alertes qui fournissent des informations lorsque les conditions de règle sont remplies.

Par défaut, QRadar utilise la base d'informations de gestion QRadar (MIB) pour gérer les unités du réseau de communications. Toutefois, vous pouvez personnaliser la sortie des alertes SNMP pour adhérer à une autre base d'informations de gestion.

**Important** : Les réponses des règles SNMPv3 sont envoyées sous forme d'informations SNMP et non de pièges.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire /opt/qradar/conf et faites des copies de sauvegarde des fichiers suivants :
  - eventCRE.snmp.xml
  - offenseCRE.snmp.xml
3. Ouvrez le fichier de configuration pour l'éditer.
  - Pour éditer les paramètres SNMP pour les règles d'événement, ouvrez le fichier eventCRE.snmp.xml.
  - Pour éditer les paramètres SNMP pour les règles de d'infraction, ouvrez le fichier offenseCRE.snmp.xml.
4. Pour modifier l'interruption utilisée pour la notification d'alerte SNMP, mettez à jour le texte suivant avec l'identificateur d'objet d'alerte (OID) approprié :

```
-<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
name="eventCRENotification">
```


5. Utilisez le tableau suivant pour vous aider à mettre à jour les informations de liaison de variable :  
Chaque liaison de variable associe une instance d'objet MIB particulière à sa valeur actuelle.

Type de valeur	Description	Exemple
chaîne	Caractères alphanumériques Vous pouvez configurer plusieurs valeurs.	
integer32	Une valeur numérique	<code>name="ATTACKER_PORT" type="integer32"&gt;%ATTACKER_PORT%</code>
oid	Chaque alerte SNMP porte un identificateur affecté à un objet dans la base d'informations de gestion	<code>OID="1.3.6.1.4.1.20212.2.46"</code>
gauge32	Plage de valeurs numériques	
counter64	Valeur numérique qui s'incrémente dans une plage minimale et maximale définie	

6. Pour chacun des types de valeur, incluez l'une des zones suivantes :

Zone	Description	Exemple
Natif	Pour plus d'informations sur ces fichiers, voir le <code>/opt/qradar/conf/snmp.help</code> .	<b>Exemple :</b> <sup>1</sup> Si le type de valeur est <code>ipAddress</code> , vous devez utiliser une variable qui est une adresse IP. Le type de valeur de chaîne accepte n'importe quel format.
Personnalisation	Informations sur les alertes SNMP personnalisées que vous avez configurées pour l'assistant de règles personnalisées	<b>Exemple :</b> <sup>1</sup> Si vous avez utilisé les informations de fichier par défaut et vous souhaitez inclure ces informations dans l'alerte SNMP, y compris le code suivant : <pre>&lt;variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string"&gt; My favorite color is %MyColor%&lt;/variableBinding&gt;</pre>

<sup>1</sup>Entourez le nom de zone avec des signes pourcentage (%). Dans le pourcentage de signes, les zones doivent correspondre au type de valeur.

7. Sauvegardez le fichier et fermez-le.
8. Copiez le fichier du répertoire `/opt/qradar/conf` vers le répertoire `/store/configservices/staging/globalconfig`.
9. Connectez-vous à la console QRadar tant qu'administrateur.
10. Dans le menu de navigation () , cliquez sur **Admin**.

11. Sélectionnez **Avancé** > **Déployer la configuration complète**.

**Important** : QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

**Information associée**

[Ajout d'une alerte SNMP personnalisée à QRadar](#)

## Ajout d'une alerte SNMP personnalisée à QRadar

Dans les produits IBM QRadar, vous pouvez créer une nouvelle option pour la sélection des alertes SNMP dans l'assistant de règles personnalisées. Les noms d'alerte spécifiés dans la zone de liste sont configurés dans le fichier de configuration `snmp-master.xml`.

**Important** : Les réponses des règles SNMPv3 sont envoyées sous forme d'informations SNMP et non de pièges.

### Procédure

1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire `/opt/qradar/conf`.
3. Créez un fichier de paramètres SNMP pour le nouveau piège.

**Conseil** : Copiez, renommez et modifiez l'un des fichiers de paramètres SNMP existants.

4. Faites une copie de sauvegarde du fichier `snmp-master.xml`.
5. Ouvrez le fichier `snmp-master.xml` pour l'éditer.
6. Ajoutez un nouvel élément `<include>`


L'élément `<include>` possède les attributs suivants :

Tableau 79. Attributs de l'élément <code>&lt;include&gt;</code>	
Attribut	Description
<code>name</code>	Affiché dans la zone de liste
<code>uri</code>	Nom du fichier de paramètres SNMP personnalisé

Par exemple :

```
<include name="Custom_Event_Name" uri="customSNMPdef01.xml"/>
```

Les interruptions sont affichées dans le menu dans le même ordre dans lequel elles sont répertoriées dans le fichier `snmp-master.xml`.

7. Sauvegardez le fichier et fermez-le.
8. Copiez le fichier `snmp-master.xml` et le fichier `customSNMPdef01.xml` du répertoire `/opt/qradar/conf` vers le répertoire `/store/configservices/staging/globalconfig`.
9. Connectez-vous à l'interface QRadar.
10. Connectez-vous à la console QRadar en tant qu'administrateur.
11. Dans le menu de navigation () , cliquez sur **Admin**.
12. Sélectionnez **Avancé** > **Déployer la configuration complète**.

**Important** : QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

## Information associée

Personnalisation de la sortie d'alerte SNMP

# Envoi d'alertes SNMP à un hôte spécifique

Par défaut, dans les produits IBM QRadar, les alertes SNMP sont envoyées à l'hôte identifié dans votre fichier `host.conf`. Vous pouvez personnaliser le fichier `snmp.xml` pour envoyer des alertes SNMP à un autre hôte.

**Important :** Les réponses des règles SNMPv3 sont envoyées sous forme d'informations SNMP et non de pièges.

## Procédure


1. Utilisez SSH pour la connexion à QRadar en tant qu'utilisateur racine.
2. Accédez au répertoire `/opt/qradar/conf` et faites des copies de sauvegarde des fichiers suivants :
  - `eventCRE.snmp.xml`
  - `offenseCRE.snmp.xml`
3. Ouvrez le fichier de configuration pour l'éditer.
  - Pour éditer les paramètres SNMP pour les règles d'événement, ouvrez le fichier `eventCRE.snmp.xml`.
  - Pour éditer les paramètres SNMP pour les règles de d'infraction, ouvrez le fichier `offenseCRE.snmp.xml`.
4. Ajoutez au moins un élément `<trapConfig>` dans l'élément `<snmp>` à l'intérieur de l'élément `<creSNMPTrap>` et avant tout autre élément enfant.

```
<trapConfig>
  <!-- All attribute values are default -->
  <snmpHost snmpVersion="3" port="162" retries="2" timeout="500">HOST
  </snmpHost>
  <!-- Community String for Version 2 -->
  <communityString>COMMUNITY_STRING</communityString>
  <!-- authenticationProtocol (MD5 or SHA)securityLevel (AUTH_PRIV, AUTH_NOPRIV
  or NOAUTH_PRIV) -->
  <authentication authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
    AUTH_PASSWORD
  </authentication>
  <!-- decryptionProtocol (DES, AES128, AES192 or AES256) -->
  <decryption decryptionProtocol="AES256">
    DECRYPTIONPASSWORD
  </decryption>
  <!-- SNMP USER-->
  <user> SNMP_USER </user>
</trapConfig>
```

5. Utilisez le tableau suivant pour vous aider à mettre à jour les attributs.

Élément	Description
<code>&lt;/snmpHost&gt;</code>	Le nouvel hôte auquel vous souhaitez envoyer des alertes SNMP. La valeur de l'attribut <code>snmpVersion</code> pour l'élément <code>&lt;snmpHost&gt;</code> doit être 2 ou 3.
<code>&lt;communityString&gt;</code>	Chaîne de communauté de l'hôte. N'utilisez pas de caractères spéciaux.
<code>&lt;authentication&gt;</code>	Protocole d'authentification, niveau de sécurité et mot de passe de l'hôte.

Tableau 80. Valeurs d'attribut à mettre à jour dans l'élément <trapConfig> (suite)	
Élément	Description
<decryption>	Protocole de déchiffrement et mot de passe de l'hôte.
<user>	Utilisateur SNMP

6. Sauvegardez le fichier et fermez-le.
7. Copiez le fichier du répertoire /opt/qradar/conf vers le répertoire /store/configservices/staging/globalconfig.
8. Connectez-vous à la console QRadar en tant qu'administrateur.
9. Dans le menu de navigation () , cliquez sur **Admin**.
10. Sélectionnez **Avancé > Déployer la configuration complète**.

**Important :** QRadar continue de collecter des événements lorsque vous déployez la configuration complète. Lorsque le service de collecte d'événements doit redémarrer, QRadar ne le redémarre pas automatiquement. Un message qui vous permet d'annuler le déploiement et de redémarrer le service à un moment plus approprié s'affiche.

---

## Chapitre 23. Protection des données sensibles

Configurez un profil de brouillage de données pour empêcher l'accès non autorisé à des informations sensibles ou personnelles dans IBM QRadar.

*Le brouillage des données* est le processus de masquage stratégique des données des utilisateurs QRadar. Vous pouvez masquer des propriétés personnalisées, normaliser des propriétés telles que des noms d'utilisateur ou masquer le contenu d'une charge, par exemple des numéros de carte de crédit ou de sécurité sociale.

Les expressions dans le profil de brouillage de données sont évaluées par rapport au contenu et aux propriétés normalisées. Si les données correspondent à l'expression de brouillage, les données sont masquées dans QRadar. Les données peuvent être masquées pour tous les utilisateurs, ou uniquement pour les utilisateurs appartenant à des domaines ou des locataires particuliers. Les utilisateurs affectés qui tentent d'interroger directement la base de données ne peuvent pas voir les données sensibles. Les données doivent être répercutées sur le formulaire d'origine en téléchargeant la clé privée qui a été générée lors de la création du profil de brouillage des données.

Pour garantir que QRadar puisse toujours corréler les valeurs de données masquées, le processus d'obscurcissement est déterministe. Il affiche le même ensemble de données chaque fois que la valeur de données est détectée.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Comment fonctionne le brouillage des données ?

Avant de configurer le brouillage des données dans votre déploiement IBM QRadar, vous devez comprendre comment il fonctionne pour les violations, les actifs, les règles et les extensions de source de journal nouvelles et existantes.

### Données d'événement existantes

Lorsqu'un profil de brouillage de données est activé, le système masque les données pour chaque événement tel qu'il est reçu par QRadar. Les événements reçus par le dispositif avant la configuration de brouillage des données restent dans l'état initial non masqué. Les données d'événement plus anciennes ne sont pas masquées et les utilisateurs peuvent voir les informations.

### Actifs

Lorsque le brouillage des données est configuré, le modèle d'actif accumule des données masquées alors que les données du modèle d'actif préexistant restent masquées.

Pour éviter que quelqu'un d'utiliser des données en clair pour tracer les informations obscurcies, purgez les données du modèle d'actif pour supprimer les données en clair. QRadar réinsérera la base de données d'actifs avec des valeurs brouillées.

### Infractions

Pour vous assurer que les violations n'affichent pas de données précédemment masquées, fermez toutes les violations existantes en réinitialisant le modèle SIM. Pour plus d'informations, voir [«Réinitialisation du module SIM»](#), à la page 86.

### Règles

Vous devez mettre à jour les règles qui dépendent des données précédemment masquées. Par exemple, les règles basées sur un nom d'utilisateur spécifique ne sont pas incendiées lorsque le nom d'utilisateur est masqué.

## Extensions de source de journal

Les extensions de source de journal qui modifient le format de la charge d'événement peuvent provoquer des problèmes avec le brouillage des données.

## Profils de brouillage de données

Le profil du brouillage des données contient des informations sur les données à masquer. Il suit également le fichier de clés requis pour déchiffrer les données.

### Profils activés

Activez un profil uniquement lorsque vous êtes certain que les expressions ciblent correctement les données que vous souhaitez masquer. Si vous souhaitez tester l'expression régulière avant d'activer le profil du brouillage des données, vous pouvez créer une propriété personnalisée basée sur le regex.

Un profil activé commence immédiatement à masquer les données telles que définies par les expressions activées dans le profil. Le profil activé est automatiquement verrouillé. Seul l'utilisateur qui dispose de la clé privée peut désactiver ou modifier le profil une fois celui-ci activé.

Pour vous assurer que les données obfusquées peuvent être retracées dans un profil d'obfuscation, vous ne pouvez pas supprimer un profil qui a été activé, même après la désactivation.

### Profils verrouillés

Un profil est automatiquement verrouillé lorsque vous l'activez, ou vous pouvez le verrouiller manuellement.

Un profil verrouillé comporte les restrictions suivantes :

- Vous ne pouvez pas l'éditer.
- Vous ne pouvez pas l'activer ou le désactiver. Vous devez fournir le fichier de clés et déverrouiller le profil avant de pouvoir le modifier.
- Vous ne pouvez pas le supprimer, même après avoir été déverrouillé.
- Si un fichier de clés est utilisé avec un profil verrouillé, tous les autres profils qui utilisent ce fichier de clés sont automatiquement verrouillés.

Le tableau suivant présente des exemples de profils verrouillés ou déverrouillés :

<i>Tableau 81. Exemples de profils verrouillés</i>	
<b>Scénario</b>	<b>Résultat</b>
Le profil A est verrouillé. Il a été créé à l'aide du magasin de clés A. Le profil B est également créé à l'aide du magasin de clés A.	Le profil B est automatiquement verrouillé.
Le profil A est créé et activé.	Le profil A est automatiquement verrouillé.
Le profil A, le profil B et le profil C sont actuellement verrouillés. Tous ont été créés à l'aide du magasin de clés A. Le profil B est sélectionné et le client clique sur <b>Verrouiller / Déverrouiller</b> .	Le profil A, le profil B et le profil C sont tous déverrouillés.

## Expressions de brouillage de données

Les expressions de brouillage des données identifient les données à masquer. Vous pouvez créer des expressions de brouillage de données basées sur des propriétés de zone ou utiliser des expressions régulières.



## Propriétés basées sur le champ

Utilisez une propriété de zone pour masquer les noms d'utilisateur, les noms de groupe, les noms d'hôte et les noms NetBIOS. Les expressions qui utilisent des propriétés basées sur le champ masquent toutes les instances de la chaîne de données. Les données sont masquées quelle que soit leur source de journal, leur type de source de journal, leur nom d'événement ou leur catégorie d'événements.

Si la même valeur de données existe dans plusieurs zones, les données sont masquées dans toutes les zones contenant les données, même si vous avez configuré le profil pour masquer une seule des quatre zones. Par exemple, si vous avez un nom d'hôte appelé IBMHost et un nom de groupe appelé IBMHost, la valeur IBMHost est brouillée dans la zone du nom d'hôte et dans la zone Nom de groupe, même si le profil de brouillage de données est configuré pour brouiller uniquement les noms d'hôte.

## Expressions régulières

Utilisez une expression régulière pour masquer une chaîne de données dans la charge. Les données sont masquées uniquement si elles correspondent à la source de journal, au type de source de journal, au nom de l'événement ou à la catégorie définie dans l'expression.

Vous pouvez utiliser des catégories de haut niveau et de bas niveau pour créer une expression régulière qui est plus spécifique qu'une propriété de zone. Par exemple, vous pouvez utiliser les modèles de regex suivants pour analyser les noms d'utilisateur :

Exemple de modèles de regex	Correspond
<code>userName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*(@[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])\.)+[a-zA-Z]{2,20})\$</code>	john_smith@EXAMPLE.com, jon@example.com, jon@us.example.com
<code>userName=(^[[\\w]+[^\w])((^[\w]\.?)([\\w]+[^\w]\$))</code>	john.smith, John.Smith, john, jon_smith
<code>userName=^[a-zA-Z][a-zA-Z_-]*[\w_-]*[\S]\$ ^[a-zA-Z][0-9_-]*[\S]\$ ^[a-zA-Z]*[\S]\$</code>	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith
<code>userName=(/S+)</code>	Correspond à n'importe quel espace non blanc après le signe égal, =. Cette expression régulière est non spécifique et peut entraîner des problèmes de performances système.
<code>msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*\b([01]?[0-9]?[0-9] 2[0-4][0-9] 25[0-5])\.)\}{3}([01]?[0-9]?[0-9] 2[0-4][0-9] 25[0-5])\b</code>	Correspond aux utilisateurs ayant une adresse IP. Par exemple, john.smith@192.0.2.0
<code>src=\b([01]?[0-9]?[0-9] 2[0-4][0-9] 25[0-5])\.)\}{3}([01]?[0-9]?[0-9] 2[0-4][0-9] 25[0-5])\b</code>	Correspond aux formats d'adresse IP.
<code>host=^(([a-zA-Z0-9] [a-zA-Z0-9][a-zA-Z0-9\-.]*[a-zA-Z0-9])\.)*([A-Za-z0-9] [A-Za-z0-9][A-Za-z0-9\-.]*[A-Za-z0-9])\$</code>	hostname.example.com, hostname.co.uk

## Scénario : brouiller les noms d'utilisateur

Vous êtes un administrateur IBM QRadar. Votre organisation a convenu avec le syndicat des travailleurs que toutes les informations personnelles identifiables doivent être cachées aux utilisateurs de QRadar. Vous souhaitez configurer QRadar pour masquer tous les noms d'utilisateur.

Utilisez la fonction **Gestion du brouillage des données** dans l'onglet **Admin** pour configurer QRadar afin de masquer les données :

1. Créez un profil de brouillage de données et téléchargez la clé privée générée par le système.  
Enregistrez la clé dans un emplacement sécurisé.
2. Créez les expressions de brouillage de données pour cibler les données que vous souhaitez masquer.
3. Activez le profil pour que le système commence à masquer les données.
4. Pour lire les données dans QRadar, téléchargez la clé privée pour démasquer les données.

## Création d'un profil de débrouillage des données


IBM QRadar utilise des profils de débrouillage des données pour déterminer les données à masquer et pour s'assurer que le fichier de clés correct est utilisé pour démasquer les données.

### Pourquoi et quand exécuter cette tâche

Vous pouvez créer un profil qui crée un fichier de clés ou vous pouvez utiliser un fichier de clés existant. Si vous créez un fichier de clés, il doit être téléchargé et stocké dans un emplacement sécurisé. Supprimez le fichier de clés du système local et stockez-le dans un emplacement accessible uniquement par les utilisateurs autorisés à afficher les données non masquées.

La configuration de profils qui utilisent des fichiers de clés différents est utile lorsque vous souhaitez limiter l'accès aux données à différents groupes d'utilisateurs. Par exemple, créez deux profils qui utilisent des magasins de clés différents lorsque vous souhaitez qu'un groupe d'utilisateurs voit les noms d'utilisateur et un autre groupe d'utilisateurs pour afficher les noms d'hôte.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Gestion du brouillage des données**.
3. Pour créer un profil, cliquez sur **Ajouter** et entrez un nom et une description uniques pour le profil.
4. Pour créer un fichier de clés pour le profil, procédez comme suit :
  - a) Cliquez sur **Système généré par le système**.
  - b) Dans la zone de liste **Fournisseur**, sélectionnez **IBMJCE**.
  - c) Dans la zone de liste **Algorithme**, sélectionnez **JCE** et choisissez de générer des clés de chiffrement 512 bits ou 1024 bits.  
Dans la zone **Certificat de Keystore CN**, le nom de domaine complet du serveur QRadar est généré automatiquement.
  - d) Dans la zone **Mot de passe du fichier de clés**, entrez le mot de passe du fichier de clés.  
Le mot de passe du fichier de clés est requis pour protéger l'intégrité du fichier de clés. Votre mot de passe doit comporter au moins 8 caractères.
  - e) Dans **Vérification du mot de passe de**, entrez de nouveau le mot de passe.
5. Pour utiliser un fichier de clés existant avec le profil, procédez comme suit :
  - a) Cliquez sur **Télécharger le magasin de clés**.
  - b) Cliquez sur **Parcourir** et sélectionnez le fichier de clés.
  - c) Dans la zone **Mot de passe du fichier de clés**, entrez le mot de passe du fichier de clés.
6. Cliquez sur **Soumettre**.
7. Téléchargez le fichier de clés.  
Retirez le fichier de clés de votre système et rangez-le dans un emplacement sécurisé.

### Que faire ensuite

[Création des expressions de brouillage de données qui cible les données que vous souhaitez masquer.](#)

## Création d'expressions de brouillage de données

Le profil de brouillage des données utilise des expressions pour spécifier les données à masquer pour les utilisateurs IBM QRadar. Les expressions peuvent utiliser des propriétés basées sur le champ ou des expressions régulières.


### Pourquoi et quand exécuter cette tâche

Une fois l'expression créée, vous ne pouvez pas modifier le type. Par exemple, vous ne pouvez pas créer d'expression basée sur des propriétés, puis la remplacer ultérieurement par une expression régulière.

Vous ne pouvez pas masquer une zone numérique normalisée, telle que le numéro de port ou une adresse IP.

Plusieurs expressions qui masquent les mêmes données provoquent la masquage des données deux fois. Pour déchiffrer les données qui sont masquées plusieurs fois, chaque fichier de clés utilisé dans le processus de brouillage doit être appliqué dans l'ordre où le brouillage s'est produit.

### Procédure

1. Dans le menu de navigation () , cliquez sur **Admin**.
2. Dans la section **Sources de données**, cliquez sur **Gestion du brouillage des données**.
3. Cliquez sur le profil que vous souhaitez configurer, puis sur **Afficher le contenu**.  
Vous ne pouvez pas configurer les profils verrouillés.
4. Pour créer une expression de brouillage de données, cliquez sur **Ajouter** et entrez un nom et une description uniques pour le profil.
5. Cochez la case **Activé** pour activer le profil.
6. Facultatif : Pour appliquer l'expression de brouillage à des domaines ou à des locataires spécifiques, sélectionnez-les dans la zone **Domaine**. Ou sélectionnez **Tous les domaines** pour appliquer l'expression de brouillage à tous les domaines et locataires.
7. Pour créer une expression basée sur une zone, cliquez sur **Basé sur une zone** et sélectionnez le type de zone à brouiller.
8. Pour créer une expression régulière, cliquez sur **RegEx** et configurez les propriétés regex.
9. Cliquez sur **Sauvegarder**.

## Débrouillage des données pour qu'elles puissent être affichées dans la console

Lorsque l'obfuscation des données est configurée sur un système IBM QRadar, la version masquée des données est affichée dans l'ensemble de l'application. Vous devez disposer du fichier de clés correspondant et du mot de passe pour débrouiller les données afin qu'elles puissent être visualisés.

### Avant de commencer

Vous devez être un administrateur et disposer de la clé privée et du mot de passe de la clé avant de pouvoir démasquer les données. La clé privée doit être sur votre ordinateur local.

### Pourquoi et quand exécuter cette tâche

Avant de voir les données brouillées, vous devez télécharger la clé privée. Une fois la clé téléchargée, elle reste disponible sur le système pour la durée de la session en cours. La session se termine lorsque vous vous déconnectez de QRadar, lorsque le cache est désélectionné sur QRadar Console, ou lorsque la période d'inactivité est prolongée. Lorsque la session se termine, les clés privées qui ont été téléchargées lors de la session précédente ne sont plus visibles.

QRadar peut utiliser les clés disponibles dans la session en cours pour déobfuser automatiquement les données. Avec la fonction de débrouillage automatique activée, il n'est pas nécessaire de sélectionner

à plusieurs reprises la clé privée dans la fenêtre **Clé de session de brouillage** chaque fois que vous souhaitez afficher les données. L'auto-débrouillage est automatiquement désactivé lorsque la session en cours se termine.

## Procédure

1. Sur la page **Détails de l'événement**, recherchez les données que vous souhaitez débrouiller.
2. Pour débrouiller les données basées sur l'identité :
  - a) Cliquez sur l'icône de verrouillage en regard des données que vous souhaitez débrouiller.
  - b) Dans la section **Clé de téléchargement**, cliquez sur **Sélectionner un fichier** et sélectionnez le fichier de clés à télécharger.
  - c) Dans la zone **Mot de passe**, entrez le mot de passe correspondant au fichier de clés.
  - d) Cliquez sur **Télécharger**.

La fenêtre **Débrouillage** affiche la charge d'événement, les noms de profil associés au fichier de clés, le texte débrouillé et le texte débrouillé.
  - e) Facultatif : Cliquez sur **Basculer le débrouillage automatique** pour activer le débrouillage automatique.

Une fois que vous avez désactivé le paramètre de débrouillage automatique, vous devez régénérer la fenêtre du navigateur et recharger la page des détails de l'événement pour que les modifications apparaissent.
3. Pour débrouiller les données de charge qui ne sont pas basées sur l'identité :
  - a) Dans la barre d'outils de la page **Détails de l'événement**, cliquez sur **Brouillage > Clés de débrouillage**.
  - b) Dans la section **Clé de téléchargement**, cliquez sur **Sélectionner un fichier** et sélectionnez la clé privée à télécharger.
  - c) Dans la zone **Mot de passe**, entrez le mot de passe correspondant à la clé privée et cliquez sur **Télécharger**.
  - d) Dans la zone **Informations de charge**, sélectionnez et copiez le texte masqué dans le presse-papiers.
  - e) Dans la barre d'outils de la page **Détails de l'événement**, cliquez sur **Brouillage > Débrouillage**.
  - f) Collez le texte masqué dans la boîte de dialogue.
  - g) Sélectionnez le profil d'obfuscation dans la liste déroulante et cliquez sur **Débrouillage**.

## Éditer ou désactiver des expressions de brouillage créées dans les versions précédentes

Lorsque vous effectuez une mise à niveau vers IBM QRadar V7.2.6, les expressions de brouillage des données qui ont été créées dans les versions précédentes sont automatiquement reportées et continuent à masquer les données. Ces expressions apparaissent dans un profil de brouillage de données unique, nommé **AutoGeneratedProperty**.

Bien que vous puissiez voir les expressions, vous ne pouvez pas modifier ou désactiver les expressions de brouillage des données qui ont été créées dans les versions antérieures. Vous devez les désactiver manuellement et créer un profil de brouillage de données contenant les expressions révisées.

### Pourquoi et quand exécuter cette tâche

Pour désactiver une expression ancienne, vous devez éditer le fichier de configuration xml qui définit les attributs de l'expression. Vous pouvez ensuite exécuter le script `obfuscation_updater.sh` pour le désactiver.

Assurez-vous de désactiver les anciennes expressions avant de créer de nouvelles expressions qui masquent les mêmes données. Les expressions multiples qui masquent les mêmes données font que

les données doivent être masquées deux fois. Pour déchiffrer les données qui sont masquées plusieurs fois, chaque fichier de clés utilisé dans le processus de brouillage doit être appliqué dans l'ordre où le brouillage s'est produit.

## Procédure

1. Utilisez SSH pour vous connecter à votre console QRadar en tant que superutilisateur.
2. Éditez le fichier de configuration `.xml` des expressions d'obfuscation que vous avez créé lorsque vous avez configuré les expressions.
3. Pour chaque expression que vous souhaitez désactiver, remplacez l'attribut **Enabled** par `faux`.
4. Pour désactiver les expressions, exécutez le script `obfuscation_updater.sh` en entrant la commande suivante :

```
obfuscation_updater.sh [-p <path_to_private_key>] [-e  
<path_to_obfuscation_xml_config_file>]
```

Le script `obfuscation_updater.sh` se trouve dans le répertoire `/opt/qradar/bin`, mais vous pouvez exécuter le script à partir de n'importe quel répertoire de votre console QRadar.

## Que faire ensuite

Créer un [profil de brouillage des données](#) pour masquer les données et gérer les expressions de brouillage directement dans QRadar.



---

## Chapitre 24. Fichiers journaux

Les opérations effectuées dans IBM QRadar sont enregistrées dans des fichiers journaux à des fins de suivi. Les fichiers journaux peuvent vous aider à identifier et résoudre les incidents en enregistrant les activités qui ont lieu lorsque vous travaillez avec un produit.

Les fichiers journaux suivants peuvent vous aider à identifier et à résoudre les incidents lorsqu'ils se produisent :

- /var/log/qradar.log
- /var/log/qradar.error
- /var/log/qradar-sql.log
- /opt/tomcat/logs/catalina.log
- /var/log/qflow.debug

Si vous souhaitez collecter les fichiers journaux QRadar et les consulter ultérieurement, voir [«Collecte des fichiers journaux»](#), à la page 85.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Journaux d'audit

Les modifications effectuées par les utilisateurs IBM QRadar sont enregistrées dans les journaux d'audit.

Tous les journaux d'audit sont stockés en texte normal et sont archivés et compressés lorsque le fichier journal d'audit atteint 50 Mo. Le fichier journal en cours est nommé `audit.log`. Lorsque le fichier atteint 50 Mo, le fichier est compressé et renommé `audit.1.gz`. Le numéro de fichier s'incrémente chaque fois qu'un fichier journal est archivé. QRadar stocke jusqu'à 25 fichiers journaux archivés.

Les données du journal d'audit sont également stockées dans la source de journal `SIM Audit-2`, qui peut être utilisée pour le filtrage et la génération de rapports pour suivre la façon dont les utilisateurs interagissent avec QRadar. La conservation des données est déterminée par votre configuration de conservation des événements.

## Affichage du fichier journal d'audit

Utilisez Secure Shell (SSH) pour vous connecter à votre système IBM QRadar et surveiller les modifications apportées à votre système.

### Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'onglet **Activité de journal** pour afficher les événements de journal d'audit normalisés.

La taille maximale de tout message d'audit, à l'exception de la date, de l'heure et du nom d'hôte, est de 1024 caractères.

Chaque entrée du fichier journal s'affiche en utilisant le format suivant :

```
<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>
```

Le tableau suivant décrit les options de format de fichier journal.

Partie de format de fichier	Description
<i>date_time</i>	Date et heure de l'activité au format : Mois Date HH:MM:SS
<i>nom d'hôte</i>	Le nom d'hôte de la console dans laquelle cette activité a été consignée.
<i>user</i>	Nom de l'utilisateur qui a modifié les paramètres.
<i>Adresse IP</i>	Adresse IP de l'utilisateur qui a modifié les paramètres.
<i>ID unité d'exécution)</i>	Identificateur de l'unité d'exécution Java qui a consigné cette activité.
<i>Catégorie</i>	La catégorie de haut niveau de cette activité.
<i>sous-catégorie</i>	La catégorie de bas niveau de cette activité.
<i>Action</i>	L'activité qui s'est déroulée.
<i>payload</i>	L'enregistrement complet, qui peut inclure l'enregistrement utilisateur ou la règle d'événement, qui a été modifié.

## Procédure

1. À l'aide de SSH, connectez-vous à QRadar en tant que superutilisateur :
2. **Nom d'utilisateur** : racine
3. **Mot de passe** : *mot de passe*
4. Accédez au répertoire suivant :  

```
/var/log/audit
```
5. Ouvrez et affichez le fichier journal d'audit.

## Création de rapports à partir de recherches de journaux d'audit dans QRadar


Pour vous aider à déterminer comment les utilisateurs interagissent avec IBM QRadar, créez des rapports basés sur vos résultats de recherche.

## Procédure

1. Cliquez sur **Activité de journal** > **Ajouter un filtre**.
2. Dans la fenêtre **Ajouter un filtre**, configurez les paramètres suivants :

Paramètres à configurer	Valeur
<b>paramètre</b>	Source du journal [Indexée]
<b>Opérateur</b>	Est égal à cette valeur
<b>Source du journal</b>	SIM Audit-2



3. Cliquez sur **Ajouter un filtre**.
4. Si les événements sont en flux dans l'onglet **Activité de journal**, cliquez sur **Pause** (  ).
5. Dans la liste **Afficher**, sélectionnez un intervalle de temps.
6. Pour enregistrer la recherche, cliquez sur **Sauvegarder les critères**, fournissez un nom pour la recherche, puis cliquez sur **OK**.
7. Pour générer un rapport à partir de votre résultat de recherche, procédez comme suit :
  - a) Dans l'onglet **Rapports**, cliquez sur **Actions > Créer**.
  - b) Suivez l'assistant de rapport.
  - c) Dans la zone **Recherches enregistrées**, entrez le nom de la recherche que vous avez créée pour la source du journal d'audit SIM.
  - d) Cliquez sur **Sauvegarder les détails du conteneur**.
  - e) Terminez les pages de l'assistant de rapport.

## Actions consignées

Les journaux d'audit IBM QRadar se trouvent dans le répertoire `/var/log/audit`.

La liste suivante décrit les catégories d'actions qui se trouvent dans le fichier journal d'audit :

### Authentification de l'administrateur

- Connectez-vous à la console d'administration.
- Déconnectez-vous de la console d'administration.

### Actifs

- Supprimer un actif.
- Supprimer tous les actifs.

### Accès au journal d'audit

Recherche incluant des événements ayant une catégorie d'événement de haut niveau d'audit.

### Sauvegarde et reprise

- Modifier la configuration.
- Lancer la sauvegarde.
- Effectuer la sauvegarde.
- Échec de la sauvegarde.
- Supprimer la sauvegarde.
- Synchroniser la sauvegarde.
- Annuler la sauvegarde.
- Télécharger une sauvegarde
- Télécharger une sauvegarde non valide.
- Lancer la restauration.
- Purger la sauvegarde.

### Configuration de graphique

Sauvegarder la configuration du flux ou du graphique d'événements.

### Gestion de contenu

- Exportation de contenu lancée.
- Exportation du contenu terminée.
- Importation de contenu lancée.
- Importation du contenu terminée.

- Mise à jour du contenu lancée.
- Mise à jour du contenu terminée.
- Recherche de contenu lancée.
- Applications ajoutées.
- Applications modifiées.
- Actions personnalisées ajoutées.
- Actions personnalisées modifiées.
- La propriété Ariel a été ajoutée.
- Propriété Ariel modifiée.
- Expression de la propriété Ariel ajoutée.
- Expression de propriété Ariel modifiée.
- Règle CRE ajoutée.
- Règle CRE modifiée.
- Tableau de bord ajouté.
- Tableau de bord modifié.
- Extension d'unité ajoutée.
- Extension d'unité modifiée.
- Association d'extension de périphérique modifiée.
- Groupement ajouté.
- Regroupement modifié.
- Profil de corrélation d'historique ajouté.
- Profil de corrélation d'historique modifié.
- Entrée de mappe QID ajoutée.
- Entrée de mappe QID modifiée.
- Données de référence créées.
- Données de référence mises à jour.
- Profil de sécurité ajouté.
- Profil de sécurité modifié.
- Unité de détection ajoutée.
- L'unité de détection a été modifiée.

### **Propriétés personnalisées**

- Ajouter une propriété d'événement personnalisé.
- Éditer une propriété d'événement personnalisé.
- Supprimer une propriété d'événement personnalisé.
- Éditer une propriété de flux personnalisé.
- Supprimer une propriété de flux personnalisé.

### **Expressions de propriété personnalisées**

- Ajouter une expression de propriété d'événement personnalisé.
- Éditer une expression de propriété d'événement personnalisé.
- Supprimer une expression de propriété d'événement personnalisé.
- Ajouter une expression de propriété de flux personnalisé.
- Éditer une expression de propriété de flux personnalisé.
- Supprimer une expression de propriété de flux personnalisé.

### **Sources de flux**

- Ajouter une source de flux.
- Modifier une source de flux.
- Supprimer une source de flux.

### **Groupes**

- Ajouter un groupe
- Supprimez un groupe.
- Éditer un groupe.

### **Corrélation d'historique**

- Ajouter un profil de corrélation d'historique.
- Supprimer un profil de corrélation d'historique
- Modifier un profil de corrélation d'historique.
- Activer un profil de corrélation d'historique.
- Désactiver un profil de corrélation d'historique.
- Le profil de corrélation d'historique est en cours d'exécution.
- Le profil de corrélation d'historique est annulé.

### **Licence**

- Ajouter une clé de licence.
- Supprimer une clé de licence.
- Supprimer l'allocation du pool de licences.
- Mettre à jour l'allocation du pool de licences.

### **Extension de la source de journal**

- Ajouter une extension de source de journal.
- Éditer l'extension de source de journal.
- Supprimer une extension de source de journal.
- Télécharger une extension de source de journal.
- Télécharger une extension de source de journal avec succès.
- Télécharger une extension de source de journal non valide.
- Télécharger une extension de source de journal.
- Signaler une extension de source de journal.
- Modifier une association de sources de journal à un type d'unité ou d'unité.

### **Infractions**

- Créer une infraction.
- Masquer une infraction.
- Fermer une infraction.
- Fermer toutes les infractions.
- Ajouter une note de destination.
- Ajouter une note source.
- Ajouter une note réseau.
- Ajouter une note d'infraction.
- Ajouter un motif de fermeture des infractions.
- Éditer un motif de fermeture des infractions.

## **Configuration de protocole**

- Ajouter une configuration de protocole.
- Supprimer une configuration de protocole.
- Modifier une configuration de protocole.

## **QIDmap**

- Ajouter une entrée de mappe QID.
- Éditer une entrée de mappe QID.

## **IBM QRadar Vulnerability Manager**

- Créer un planning de scanner.
- Mettre à jour un planning de scanner.
- Supprimer un planning de scanner.
- Démarrer un planning de scanner.
- Mettre en pause un planning de scanner.
- Reprendre un planning de scanner.

## **Ensembles de référence**

- Créer un ensemble de références.
- Éditer un ensemble de références.
- Purger les éléments dans un ensemble de référence.
- Supprimer un ensemble de références.
- Ajouter des éléments d'ensemble de référence.
- Supprimer des éléments d'ensemble de référence.
- Supprimer tous les éléments d'ensemble de référence.
- Importer des éléments d'ensemble de référence.
- Exporter les éléments d'ensemble de référence.

## **Rapports**

- Ajouter un modèle
- Supprimer un modèle
- Éditer un modèle.
- Générer un rapport.
- Supprimer un rapport
- Supprimer le contenu généré.
- Afficher un rapport généré.
- Envoyer un rapport généré par courrier électronique.

## **Compartiments de conservation**

- Ajouter un compartiment.
- Supprimer un compartiment.
- Modifier un compartiment.
- Activer ou désactiver un compartiment.

## **Connexion superutilisateur**

- Connectez-vous à QRadar en tant que superutilisateur.
- Déconnectez-vous de QRadar en tant que superutilisateur.

## **Règles**

- Ajouter une règle.
- Supprimer une règle.
- Éditer une règle.

## **Scanner**

- Ajouter un scanner.
- Supprimer un scanner.
- Éditer un scanner.

## **Planification du scanner**

- Ajouter un planning.
- Éditer un planning.
- Supprimer un planning.

## **Authentification de session**

- Créer une session d'administration.
- Mettre fin à une session d'administration.
- Refuser une session d'authentification non valide.
- Expiration d'une authentification de session.
- Créer une session d'authentification.
- Mettre fin à une session d'authentification.

## **SIM**

Nettoyer un modèle SIM.

## **Stockage et réacheminement**

- Ajouter un planning Stockage et retransmission.
- Éditer un planning Stockage et retransmission.
- Supprimer un planning Stockage et retransmission.

## **Transmission Syslog**

- Ajouter une transmission syslog.
- Supprimer une transmission syslog.
- Modifier une transmission syslog.

## **Gestion des systèmes**

- Arrêter le système.
- Redémarrer le système.

## **Comptes utilisateur**

- Ajouter un compte
- Modifier un compte.
- Supprimer un compte.

## **Authentification de l'utilisateur**

- Connectez-vous à l'interface utilisateur.
- Déconnectez-vous de l'interface Web. utilisateur.

## **Authentification de l'utilisateurAriel**

- Refuser une tentative de connexion.

- Ajouter une propriété Ariel.
- Supprimer une propriété Ariel.
- Éditer une propriété Ariel.
- Ajouter une extension de propriété Ariel.
- Supprimer une extension de propriété Ariel.
- Éditer une extension de propriété Ariel.

#### **Rôles utilisateur**

- Ajouter un rôle.
- Éditer un rôle.
- Supprimer un rôle.

#### **VIS**

- Découvrir un nouvel hôte.
- Découvrir un nouveau système d'exploitation.
- Découvrir un nouveau port.
- Découvrir une nouvelle vulnérabilité.

## Chapitre 25. Catégories d'événement

Les catégories d'événement sont utilisées pour regrouper les événements entrants pour le traitement par IBM QRadar. Les catégories d'événements sont consultables et vous aident à surveiller votre réseau.

Les événements survenant sur votre réseau sont regroupés en catégories de niveau supérieur et en catégories de niveau inférieur. Chaque catégorie de niveau supérieur contient des catégories de niveau inférieur ainsi qu'un niveau de gravité et un numéro d'ID.

Vous pouvez revoir les niveaux de gravité affectés aux événements et les ajuster en fonction des besoins de votre stratégie d'entreprise.

Vous pouvez exécuter une requête AQL à l'aide d'ID de catégorie d'événement de haut niveau et de niveau inférieur. Les ID catégorie des noms de catégorie associés peuvent être extraits des tableaux de catégories d'événements.

Par exemple, si vous développez des applications sous QRadar, vous pouvez exécuter une recherche AQL similaire à la requête suivante à partir de la ligne de commande pour collecter des données à partir de Ariel :

```
select qidname(qid) as 'Event', username as 'Username', devicetime as 'Time'  
from events where '<high-level category ID>' and '<Low-level category ID>' and  
LOGSOURCENAME(logsourceid) like "%Low-level category name%" last 3 days
```

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

## Catégories d'événements de haut niveau

Les événements des sources de journal IBM QRadar sont regroupés en catégories de haut niveau. Chaque événement est affecté à une catégorie de haut niveau spécifique.

Une telle catégorisation des événements facilite ensuite la recherche de données.

Le tableau suivant décrit les catégories d'événements de haut niveau.

Catégorie	ID de catégorie	Description
<a href="#">«Recon», à la page 355</a>	1 000	Événements liés à l'analyse et à d'autres techniques utilisées pour identifier les ressources réseau, par exemple, les analyses de réseau ou de ports d'hôte.
<a href="#">«DoS», à la page 356</a>	2000	Les événements associés aux attaques DDoS (dénier de service ou déni de service distribué) contre des services ou des hôtes, par exemple, les attaques par le réseau de force brute DoS.
<a href="#">«Authentification», à la page 360</a>	3000	Les événements associés aux contrôles d'authentification, au groupe ou aux modifications de privilèges, par exemple, se connectant ou se déconnectant.
<a href="#">«Accès», à la page 369</a>	4000	Événements résultant d'une tentative d'accès aux ressources réseau, par exemple, un pare-feu accepte ou refuse.

Tableau 85. Catégories d'événements de haut niveau (suite)

Catégorie	ID de catégorie	Description
<a href="#">«Exploitation», à la page 372</a>	5 000	Événements liés aux tentatives d'exploitation et aux tentatives de débordement de mémoire tampon, par exemple, dépassement de mémoire tampon ou exploitation d'applications Web.
<a href="#">«Logiciel malveillant», à la page 374</a>	6000	Les événements qui sont liés à des virus, des chevaux de Troie, des attaques à la porte arrière ou d'autres formes de logiciels hostiles. Les événements malveillants peuvent inclure un virus, un cheval de Troie, un logiciel malveillant ou un logiciel espion.
<a href="#">«Activité suspecte», à la page 376</a>	7000	La nature de la menace est inconnue, mais le comportement est suspect. La menace peut inclure des anomalies de protocole qui pourraient indiquer des techniques évasives, par exemple, la fragmentation de paquets ou les techniques de détection d'intrusion (IDS) connues.
<a href="#">«Système», à la page 381</a>	8000	Événements liés aux changements système, à l'installation de logiciel ou aux messages d'état.
<a href="#">«Politique», à la page 386</a>	9000	Événements concernant les violations de la politique d'entreprise ou l'utilisation abusive.
<a href="#">«Inconnu», à la page 388</a>	10000	Événements liés à une activité inconnue sur votre système.
<a href="#">«CRE», à la page 388</a>	12000	Événements générés à partir d'une règle d'événement ou d'infraction.
<a href="#">«Utilisation potentielle», à la page 389</a>	13000	Les événements se rapportent à des tentatives d'applications potentielles et à des tentatives de débordement de mémoire tampon.
Flux	14000	Événements liés aux actions de flux.
<a href="#">«Défini par l'utilisateur», à la page 392</a>	15000	Événements liés aux objets définis par l'utilisateur
<a href="#">«Audit SIM», à la page 396</a>	16000	Événements liés à l'interaction de l'utilisateur avec la console et les fonctions d'administration.
<a href="#">«Découverte d'hôte VIS», à la page 397</a>	17000	Événements liés à l'hôte, aux ports ou aux vulnérabilités que le composant VIS reconnaît.
<a href="#">«Application», à la page 397</a>	18000	Événements liés à l'activité de l'application.
<a href="#">«Audit», à la page 424</a>	19000	Événements liés à l'activité d'audit.
<a href="#">«Risque», à la page 428</a>	20000	Événements liés à l'activité de risque dans IBM QRadar Risk Manager.
<a href="#">«Audit Risk Manager», à la page 430</a>	21000	Événements associés à l'activité d'audit dans QRadar Risk Manager.
<a href="#">«Contrôle», à la page 430</a>	22000	Événements liés à votre système physique.
<a href="#">«Profileur d'actif», à la page 433</a>	23000	Événements liés aux profils d'actif.



Tableau 85. Catégories d'événements de haut niveau (suite)

Catégorie	ID de catégorie	Description
Sens	24000	Événements liés à l'UBA.

## Recon

La catégorie Recon contient des événements associés à l'analyse et à d'autres techniques utilisées pour identifier les ressources réseau.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie Recon.

Tableau 86. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements Recon

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Forme inconnue de reconnaissance	1001	Une forme inconnue de reconnaissance.	2
Requête d'application	1002	Reconnaissance des applications sur votre système.	3
Requête de l'hôte	1003	Reconnaissance à un hôte de votre réseau.	3
Balayage réseau	1004	Reconnaissance sur votre réseau.	4
Reconnaissance messagerie	1005	Reconnaissance sur votre système de messagerie.	3
Reconnaissance Windows	1006	Reconnaissance pour le système d'exploitation Windows.	3
Portmap / RPC r\Request	1007	Reconnaissance sur votre requête portmap ou RPC.	3
Analyse des ports de l'hôte	1008	Indique qu'une analyse s'est produite sur les ports hôtes.	4
Vidage RPC	1009	Indique que les informations RPC (Remote Procedure Call) sont supprimées.	3
Reconnaissance DNS	1010	Reconnaissance sur le serveur DNS.	3
Événement de reconnaissance divers	1011	Événement de reconnaissance divers.	2
Reconnaissance Web	1012	Reconnaissance Web sur votre réseau.	3

Tableau 86. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements Recon (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Reconnaissance de base de données	1013	Reconnaissance de base de données sur votre réseau.	3
Reconnaissance ICMP	1014	Reconnaissance du trafic ICMP.	3
Reconnaissance UDP	1015	Reconnaissance sur le trafic UDP.	3
Reconnaissance SNMP	1016	Reconnaissance sur le trafic SNMP.	3
Requête d'hôte ICMP	1017	Indique une requête d'hôte ICMP.	3
Requête d'hôte UDP	1018	Indique une requête hôte UDP.	3
Reconnaissance NMAP	1019	Indique une reconnaissance NMAP.	3
Reconnaissance TCP	1020	Indique la reconnaissance TCP sur votre réseau.	3
Reconnaissance UNIX	1021	Reconnaissance sur votre réseau UNIX.	3
Reconnaissance FTP	1022	Indique la reconnaissance FTP.	3

## DoS

La catégorie DoS contient des événements associés à des attaques de déni de service (DoS) contre des services ou des hôtes.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie DoS.

Tableau 87. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements DoS

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Attaque par saturation inconnue	2001	Indique une attaque DoS inconnue.	8
Attaque par saturation ICMP	2002	Indique une attaque ICMP DoS.	9
Attaque par saturation TCP	2003	Indique une attaque TCP DoS.	9
Attaque par saturation UDP	2004	Indique une attaque UDP DoS.	9
Attaque par saturation du service DNS	2005	Indique une attaque DoS de service DNS.	8

Tableau 87. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements DoS (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Attaque par saturation du service Web	2006	Indique une attaque DoS de service Web.	8
Attaque par saturation du service mail	2007	Indique une attaque DoS du serveur de messagerie.	8
Attaque par saturation distribuée	2008	Indique une attaque DoS distribuée.	9
Attaque par saturation autre	2009	Indique une attaque DoS diverse.	8
UNIX DoS	2010	Indique une attaque UNIX DoS.	8
Windows DoS	2011	Indique une attaque Windows DoS.	8
Attaque par saturation de base de données	2012	Indique une attaque DoS de base de données.	8
Attaque par saturation FTP	2013	Indique une attaque FTP DoS.	8
Attaque par saturation de l'infrastructure	2014	Indique une attaque DoS sur l'infrastructure.	8
Attaque par saturation Telnet	2015	Indique une attaque Telnet DoS.	8
Connexion par force brute	2016	Indique l'accès à votre système via des méthodes non autorisées.	8
Attaque par saturation TCP haut débit	2017	Indique une attaque TCP DoS à taux élevé.	8
Attaque par saturation UDP haut débit	2018	Indique une attaque UDP DoS à taux élevé.	8
Attaque par saturation ICMP haut débit	2019	Indique une attaque ICMP DoS à taux élevé.	8
Attaque par saturation haut débit	2020	Indique une attaque par DoS à taux élevé.	8
Attaque par saturation TCP moyen débit	2021	Indique une attaque TCP à taux moyen.	8
Attaque par saturation UDP moyen débit	2022	Indique une attaque UDP à taux moyen.	8
Attaque par saturation ICMP moyen débit	2023	Indique une attaque ICMP de taux moyen.	8
Attaque par saturation moyen débit	2024	Indique une attaque DoS à taux moyen.	8

Tableau 87. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements DoS (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Attaque par saturation TCP bas débit	2025	Indique une attaque TCP DoS à taux faible.	8
Attaque par saturation UDP bas débit	2026	Indique une attaque UDP DoS à faible taux.	8
Attaque par saturation ICMP bas débit	2027	Indique une attaque ICMP DoS à faible taux.	8
Attaque par saturation bas débit	2028	Indique une attaque par DoS à faible taux.	8
Attaque par saturation TCP haut débit distribuée	2029	Indique une attaque TCP DoS distribuée à taux élevé.	8
Attaque par saturation UDP haut débit distribuée	2030	Indique une attaque UDP DoS distribuée à taux élevé.	8
Attaque par saturation ICMP haut débit distribuée	2031	Indique une attaque ICMP DoS distribuée à taux élevé.	8
Attaque par saturation haut débit distribuée	2032	Indique une attaque de DoS à taux élevé distribué.	8
Attaque par saturation TCP moyen débit distribuée	2033	Indique une attaque TCP DoS à taux moyen distribué.	8
Attaque par saturation UDP moyen débit distribuée	2034	Indique une attaque UDP DoS à taux moyen distribué.	8
Attaque par saturation ICMP moyen débit distribuée	2035	Indique une attaque ICMP DoS à taux moyen distribué.	8
Attaque par saturation moyen débit distribuée	2036	Indique une attaque DoS à taux moyen distribué.	8
Attaque par saturation TCP bas débit distribuée	2037	Indique une attaque TCP DoS à taux réduit distribué.	8
Attaque par saturation UDP bas débit distribuée	2038	Indique une attaque UDP DoS à taux réduit distribué.	8
Attaque par saturation ICMP bas débit distribuée	2039	Indique une attaque ICMP DoS distribuée à taux réduit.	8
Attaque par saturation bas débit distribuée	2040	Indique une attaque DoS à taux réduit distribué.	8

Tableau 87. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements DoS (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Analyse TCP haut débit	2041	Indique une analyse TCP à taux élevé.	8
Analyse UDP haut débit	2042	Indique une analyse UDP à taux élevé.	8
Analyse ICMP haut débit	2043	Indique une analyse ICMP à taux élevé.	8
Analyse haut débit	2044	Indique une analyse de taux élevée.	8
Analyse TCP moyen débit	2045	Indique une analyse TCP à taux moyen.	8
Analyse UDP moyen débit	2046	Indique une analyse UDP à taux moyen.	8
Analyse ICMP moyen débit	2047	Indique une analyse ICMP de taux moyen.	8
Analyse moyen débit	2048	Indique une analyse de taux moyen.	8
Analyse TCP bas débit	2049	Indique une analyse TCP à faible débit.	8
Analyse UDP bas débit	2050	Indique une analyse UDP à faible taux.	8
Analyse ICMP bas débit	2051	Indique une analyse ICMP à faible taux.	8
Analyse bas débit	2052	Indique une analyse de débit faible.	8
Attaque par saturation VoIP	2053	Indique une attaque VoIP DoS.	8
Inondation	2054	Indique une attaque flood.	8
Inondation TCP	2055	Indique une attaque flood TCP.	8
Inondation UDP	2056	Indique une attaque flood UDP.	8
Inondation ICMP	2057	Indique une attaque flood ICMP.	8
Inondation SYN	2058	Indique une attaque flood SYN.	8
Inondation URG	2059	Indique une attaque flood avec drapeau d'urgence (URG).	8
Inondation URG SYN	2060	Indique une attaque flood SYN avec drapeau d'urgence (URG).	8

Tableau 87. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements DoS (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Inondation FIN SYN	2061	Indique une attaque flood SYN FIN.	8
Inondation ACK SYN	2062	Indique une attaque flood SYN ACK.	8

## Authentification

La catégorie d'authentification contient des événements liés à l'authentification, aux sessions et aux contrôles d'accès qui surveillent les utilisateurs sur le réseau.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'authentification.

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Authentification inconnue	3001	Indique une authentification inconnue.	1
Réussite de la connexion à l'hôte	3002	Indique une connexion hôte réussie.	1
Echec de la connexion à l'hôte	3003	Indique que la connexion de l'hôte a échoué.	3
Réussite de la connexion autre	3004	Indique que la séquence de connexion a abouti.	1
Echec de la connexion autre	3005	Indique que la séquence de connexion a échoué.	3
Echec de l'escalade de privilèges	3006	Indique que l'escalade privilégiée a échoué.	3
Réussite de l'escalade de privilèges	3007	Indique que l'escalade des privilèges a abouti.	1
Réussite de la connexion au service de messagerie	3008	Indique que la connexion au service de messagerie a abouti.	1
Echec de la connexion au service de messagerie	3009	Indique que la connexion au service de messagerie a échoué.	3
Echec de la connexion au serveur d'authentification	3010	Indique que la connexion au serveur d'authentification a échoué.	3

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Réussite de la connexion au serveur d'authentification	3011	Indique que la connexion au serveur d'authentification a abouti.	1
Réussite de la connexion au service Web	3012	Indique que la connexion au service Web a abouti.	1
Echec de la connexion au service Web	3013	Indique que la connexion au service Web a échoué.	3
Réussite de la connexion d'administrateur	3014	Indique qu'une connexion d'administration a abouti.	1
Echec de la connexion de l'administrateur	3015	Indique que la connexion d'administration a échoué.	3
Nom d'utilisateur suspect	3016	Indique qu'un utilisateur a tenté d'accéder au réseau en utilisant un nom d'utilisateur incorrect.	4
La connexion avec nom d'utilisateur/mot de passe a abouti	3017	Indique qu'un utilisateur a accédé au réseau en utilisant le nom d'utilisateur et le mot de passe par défaut.	4
Échec de la connexion avec nom d'utilisateur/mot de passe	3018	Indique qu'un utilisateur n'a pas réussi à accéder au réseau en utilisant le nom d'utilisateur et le mot de passe par défaut.	4
Réussite de la connexion FTP	3019	Indique que la connexion FTP a abouti.	1
Echec de la connexion FTP	3020	Indique que la connexion FTP a échoué.	3
Réussite de la connexion SSH	3021	Indique que la connexion SSH a abouti.	1
Echec de la connexion SSH	3022	Indique que la connexion SSH a échoué.	2

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Droit d'utilisateur affecté	3023	Indique que l'accès utilisateur aux ressources réseau a été accordé avec succès.	1
Droit d'utilisateur supprimé	3024	Indique que l'accès utilisateur aux ressources réseau a été supprimé.	1
Domaine de confiance ajouté	3025	Indique qu'un domaine sécurisé a été ajouté à votre déploiement.	1
Domaine de confiance supprimé	3026	Indique qu'un domaine sécurisé a été supprimé de votre déploiement.	1
Accès à la sécurité du système accordé	3027	Indique que l'accès à la sécurité du système a été accordé avec succès.	1
Accès à la sécurité du système supprimé	3028	Indique que l'accès à la sécurité du système a été supprimé.	1
Politique ajoutée	3029	Indique qu'une règle a été ajoutée avec succès.	1
Modification de politique	3030	Indique qu'une règle a été modifiée avec succès.	1
Compte d'utilisateur ajouté	3031	Indique qu'un compte utilisateur a été ajouté.	1
Compte d'utilisateur changé	3032	Indique une modification d'un compte utilisateur existant.	1
Echec du changement de mot de passe	3033	Indique qu'une tentative de modification d'un mot de passe existant a échoué.	3
Réussite du changement de mot de passe	3034	Indique qu'un changement de mot de passe a abouti.	1
Compte d'utilisateur supprimé	3035	Indique qu'un compte utilisateur a été supprimé.	1
Membre de groupe ajouté	3036	Indique qu'un membre de groupe a été ajouté.	1



Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Membre de groupe supprimé	3037	Indique qu'un membre de groupe a été supprimé.	1
Groupe ajouté	3038	Indique qu'un groupe a été ajouté.	1
Groupe modifié	3039	Indique un changement à un groupe existant.	1
Groupe supprimé	3040	Indique qu'un groupe a été supprimé.	1
Compte d'ordinateur ajouté	3041	Indique qu'un compte d'ordinateur a été ajouté.	1
Compte d'ordinateur modifié	3042	Indique une modification d'un compte d'ordinateur existant.	1
Compte d'ordinateur supprimé	3043	Indique qu'un compte d'ordinateur a été supprimé.	1
Réussite de la connexion par accès distant	3044	Indique que l'accès au réseau à l'aide d'une connexion distante a abouti.	1
Echec de la connexion par accès distant	3045	Indique qu'une tentative d'accès au réseau à l'aide d'une connexion distante a échoué.	3
Réussite de l'authentification générale	3046	Indique que les processus d'authentification ont abouti.	1
Echec de l'authentification générale	3047	Indique que le processus d'authentification a échoué.	3
Réussite de la connexion Telnet	3048	Indique que la connexion telnet a abouti.	1
Echec de la connexion Telnet	3049	Indique que la connexion telnet a échoué.	3

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Mot de passe suspect	3050	Indique qu'un utilisateur a tenté de se connecter en utilisant un mot de passe suspect.	4
Connexion Samba réussie	3051	Indique qu'un utilisateur s'est connecté avec succès à l'aide de Samba.	1
Echec de la connexion Samba	3052	Indique qu'un utilisateur n'a pas pu se connecter à l'aide de Samba.	3
Ouverture de la session sur le serveur d'authentification	3053	Indique qu'une session de communication avec le serveur d'authentification a été démarrée.	1
Fermeture de la session sur le serveur d'authentification	3054	Indique qu'une session de communication avec le serveur d'authentification a été fermée.	1
Fermeture de la session sur le pare-feu	3055	Indique qu'une session de pare-feu a été fermée.	1
Déconnexion de l'hôte	3056	Indique qu'un hôte a réussi à se déconnecter.	1
Déconnexion autre	3057	Indique qu'un utilisateur a réussi à se déconnecter.	1
Déconnexion du serveur d'authentification	3058	Indique que le processus de connexion du serveur d'authentification a abouti.	1
Déconnexion du service Web	3059	Indique que le processus de connexion du service Web a abouti.	1
Déconnexion de l'administrateur	3060	Indique que l'utilisateur administrateur a réussi à se déconnecter.	1
Déconnexion FTP	3061	Indique que le processus de déconnexion du service FTP a abouti.	1

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Déconnexion SSH	3062	Indique que le processus de déconnexion à la session SSH a abouti.	1
Déconnexion de l'accès distant	3063	Indique que le processus de déconnexion à l'aide de l'accès à distance a abouti.	1
Déconnexion Telnet	3064	Indique que le processus de déconnexion à la session Telnet a abouti.	1
Déconnexion Samba	3065	Indique que le processus de déconnexion de Samba a abouti.	1
Session SSH démarrée	3066	Indique que la session de connexion SSH a été lancée sur un hôte.	1
Session SSH terminée	3067	Indique la fin d'une session de connexion SSH sur un hôte.	1
Session Admin démarrée	3068	Indique qu'une session de connexion a été lancée sur un hôte par un utilisateur d'administration ou un utilisateur privilégié.	1
Session Admin terminée	3069	Indique la fin d'une session de connexion d'un administrateur ou d'un utilisateur privilégié sur un hôte.	1
Réussite de la connexion VoIP	3070	Indique une connexion de service VoIP réussie	1
Echec de la connexion VoIP	3071	Indique une tentative infructueuse d'accès au service VoIP.	1
Déconnexion VoIP	3072	Indique une déconnexion de l'utilisateur,	1
Session VoIP démarrée	3073	Indique le début d'une session VoIP.	1

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session VoIP terminée	3074	Indique la fin d'une session VoIP.	1
Réussite de la connexion à la base de données	3075	Indique une connexion de base de données réussie.	1
Échec de connexion à la base de données	3076	Indique qu'une tentative de connexion à la base de données a échoué.	3
Echec de l'authentification IKE	3077	Indique qu'une authentification IKE (Internet Key Exchange) a échoué a été détectée.	3
Réussite de l'authentification IKE	3078	Indique qu'une authentification IKE réussie a été détectée.	1
Session IKE démarrée	3079	Indique qu'une session IKE a démarré.	1
Session IKE terminée	3080	Indique qu'une session IKE s'est terminée.	1
Erreur IKE	3081	Indique un message d'erreur IKE.	1
Etat IKE	3082	Indique le message d'état IKE.	1
Session RADIUS démarrée	3083	Indique qu'une session RADIUS a démarré.	1
Session RADIUS terminée	3084	Indique une session RADIUS terminée.	1
Session RADIUS refusée	3085	Indique qu'une session RADIUS a été refusée.	1
Etat de la session RADIUS	3086	Indique un message d'état de session RADIUS.	1
Echec de l'authentification RADIUS	3087	Indique un incident d'authentification RADIUS.	3
L'authentification RADIUS a abouti	3088	Indique qu'une authentification RADIUS a abouti.	1
Session TACACS démarrée	3089	Indique qu'une session TACACS a démarré.	1
Session TACACS terminée	3090	Indique qu'une session TACACS s'est terminée.	1

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session TACACS refusée	3091	Indique qu'une session TACACS a été refusée.	1
Etat de la session TACACS	3092	Indique un message d'état de session TACACS.	1
TACACS-Authentification réussie	3093	Indique qu'une authentification TACACS a abouti.	1
Echec de l'authentification TACACS	3094	Indique un échec d'authentification TACACS.	1
Réussite d'annulation de l'authentification de l'hôte	3095	Indique que la désactivation de l'hôte a abouti.	1
Échec d'annulation de l'authentification de l'hôte	3096	Indique que la désactivation de l'hôte a échoué.	3
Réussite de l'authentification du poste	3097	Indique que l'authentification de la station a abouti.	1
Échec de l'authentification du poste	3098	Indique que l'authentification de station d'un hôte a échoué.	3
Réussite de l'association du poste	3099	Indique que l'association de la station a abouti.	1
Échec de l'association du poste	3100	Indique que l'association de la station a échoué.	3
Réussite de la réassociation du poste	3101	Indique que la réassociation de la station a abouti.	1
Échec de la réassociation du poste	3102	Indique que l'association de la station a échoué.	3
Réussite de la dissociation de l'hôte	3103	Indique que la dissociation d'un hôte a abouti.	1
Échec de la dissociation de l'hôte	3104	Indique que la dissociation d'un hôte a échoué.	3

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Erreur SA	3105	Indique un message d'erreur de l'association de sécurité (SA).	5
Echec de création SA	3106	Indique un échec de création de l'association de sécurité (SA).	3
SA établi	3107	Indique qu'une connexion d'association de sécurité (SA) a été établie.	1
SA rejeté	3108	Indique qu'une connexion d'association de sécurité (SA) a été rejetée.	3
Suppression de SA	3109	Indique la suppression d'une association de sécurité (SA).	1
Création de SA	3110	Indique la création d'une association de sécurité (SA).	1
Non-concordance de certificats	3111	Indique une non-concordance de certificat.	3
Non-concordance des données d'identification	3112	Indique une non-concordance des données d'identification.	3
Tentative de connexion administrative	3113	Indique une tentative de connexion d'administrateur.	2
Tentative de connexion utilisateur	3114	Indique une tentative de connexion utilisateur.	2
Connexion utilisateur réussie	3115	Indique une connexion utilisateur réussie.	1
Echec de la connexion utilisateur	3116	Indique une connexion utilisateur ayant échoué.	3
Réussite de la connexion SFTP	3117	Indique une connexion SFTP (SSH File Transfer Protocol) réussie.	1
Echec de la connexion SFTP	3118	Indique une connexion SFTP (SSH File Transfer Protocol) ayant échoué.	3

Tableau 88. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'authentification (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Déconnexion SFTP	3119	Indique une déconnexion du protocole de transfert de fichiers SSH (SFTP).	1
Identité accordée	3120	Indique qu'une identité a été accordée.	1
Identité retirée	3121	Indique qu'une identité a été supprimée.	1
Identité révoquée	3122	Indique qu'une identité a été révoquée.	1
Politique retirée	3123	Indique qu'une règle a été supprimée.	1
Rôle du compte d'utilisateur	3124	Indique qu'un compte utilisateur a été verrouillé.	1
Déverrouiller le compte utilisateur	3125	Indique qu'un compte utilisateur a été déverrouillé	1
Compte d'utilisateur arrivé à expiration	3126	Indique qu'un compte utilisateur est arrivé à expiration	1

## Accès

La catégorie d'accès contient des contrôles d'authentification et d'accès utilisés pour la surveillance des événements réseau.

Le tableau suivant décrit les catégories d'événement de bas niveau et les niveaux de gravité associés pour la catégorie d'accès.

Tableau 89. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'accès

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Événement de communication réseau inconnu	4001	Indique un événement de communication réseau inconnu.	3
Autorisation pare-feu	4002	Indique que l'accès au pare-feu a été autorisé.	0
Refus pare-feu	4003	Indique que l'accès au pare-feu a été refusé.	4
Réponse du contexte de flux (QRadar SIEM uniquement)	4004	Indique les événements du moteur de classification en réponse à une demande SIM.	5

Tableau 89. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'accès (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Événement de communication réseau autre	4005	Indique un événement de communication divers.	3
Refus IPS	4006	Indique que les systèmes de prévention des intrusions (IPS) ont refusé le trafic.	4
Ouverture de la session sur le pare-feu	4007	Indique que la session de pare-feu a été ouverte.	0
Fermeture de la session sur le pare-feu	4008	Indique que la session de pare-feu a été fermée.	0
Réussite de la traduction dynamique d'adresse	4009	Indique que la conversion d'adresse dynamique a abouti.	0
Aucun groupe de traduction trouvé	4010	Indique qu'aucun groupe de conversion n'a été trouvé.	2
Autorisation autre	4011	Indique que l'accès a été accordé à un serveur d'authentification divers.	2
Autorisation liste de contrôle d'accès	4012	Indique qu'une liste de contrôle d'accès (ACL) a autorisé l'accès.	0
Refus liste de contrôle d'accès	4013	Indique qu'une liste de contrôle d'accès (ACL) a refusé l'accès.	4
Accès autorisé	4014	Indique que l'accès a été autorisé.	0
Accès refusé	4015	Indique que l'accès a été refusé.	4
Session ouverte	4016	Indique qu'une session a été ouverte.	1
Session fermée	4017	Indique qu'une session a été fermée.	1
Session réinitialisée	4018	Indique qu'une session a été réinitialisée.	3
Session terminée	4019	Indique qu'une session a été autorisée.	4
Session refusée	4020	Indique qu'une session a été refusée.	5



Tableau 89. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'accès (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
révision en cours	4021	Indique qu'une session est en cours.	1
Session différée	4022	Indique qu'une session a été retardée.	3
Session en file d'attente	4023	Indique qu'une session a été mise en file d'attente.	1
Session entrante	4024	Indique qu'une session est entrante.	1
Session sortante	4025	Indique qu'une session est sortante.	1
Tentative d'accès non autorisé	4026	Indique qu'une tentative d'accès non autorisée a été détectée.	6
Action sur autre application autorisée	4027	Indique qu'une action d'application a été autorisée.	1
Action sur autre application refusée	4028	Indique qu'une action d'application a été refusée.	3
Action sur base de données autorisée	4029	Indique qu'une action de base de données a été autorisée.	1
Action sur base de données refusée	4030	Indique qu'une action de base de données a été refusée.	3
Action FTP autorisée	4031	Indique qu'une action FTP a été autorisée.	1
Action FTP refusée	4032	Indique qu'une action FTP a été refusée.	3
Objet mis en cache	4033	Indique qu'un objet a été mis en cache.	1
Objet non mis en cache	4034	Indique qu'un objet n'a pas été mis en cache.	1
Limitation de débit	4035	Indique que le trafic limite le débit du réseau.	4
Pas de limitation de débit	4036	Indique que le réseau ne limite pas le trafic.	0
Accès P11 autorisé	4037	Indique que l'accès P11 est autorisé.	8
Accès P11 refusé	4038	Indique que l'accès P11 a été tenté et refusé.	8

Tableau 89. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'accès (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Autorisation IPS	4039	Indique un permis IPS.	0

## Exploitation

La catégorie d'exploitation contient des événements où une communication ou une exploitation d'accès s'est produite.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'exploitation.

Tableau 90. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'exploitation

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Attaque par exploitation inconnue	5001	Indique une attaque d'exploitation inconnue.	9
Débordement de tampon	5002	Indique un dépassement de mémoire tampon.	9
Utilisation DNS	5003	Indique une exploitation DNS.	9
Utilisation Telnet	5004	Indique une exploitation Telnet.	9
Linux Exploit	5005	Indique une exploitation Linux.	9
UNIX Exploit	5006	Indique une exploitation UNIX.	9
Windows Exploit	5007	Indique une exploitation Microsoft Windows.	9
Utilisation messagerie	5008	Indique un serveur de messagerie exploité.	9
Utilisation d'infrastructure	5009	Indique une exploitation d'infrastructure.	9
Utilisation autre	5010	Indique une exploitation diverse.	9
Utilisation Web	5011	Indique une exploitation Web.	9
Détournement de session	5012	Indique qu'une session de votre réseau a été intercédée.	9
Ver actif	5013	Indique un ver actif.	10

Tableau 90. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'exploitation (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Découverte/récupération du mot de passe	5014	Indique qu'un utilisateur a demandé l'accès à ses informations de mot de passe à partir de la base de données.	9
Utilisation FTP	5015	Indique une exploitation FTP.	9
Utilisation RPC	5016	Indique une exploitation RPC.	9
Utilisation SNMP	5017	Indique une exploitation SNMP.	9
Utilisation NOOP	5018	Indique une exploitation NOOP.	9
Utilisation Samba	5019	Indique une exploitation Samba.	9
Utilisation SSH	5020	Indique une exploitation SSH.	9
Utilisation de base de données	5021	Indique une exploitation de base de données.	9
Utilisation ICMP	5022	Indique une exploitation ICMP.	9
Utilisation UDP	5023	Indique une exploitation UDP.	9
Utilisation du navigateur	5024	Indique une exploitation sur votre navigateur.	9
Utilisation DHCP	5025	Indique une exploitation DHCP	9
Utilisation d'accès distant	5026	Indique une exploitation d'accès à distance	9
Utilisation ActiveX	5027	Indique une exploitation via une application ActiveX.	9
Injection SQL	5028	Indique qu'une injection SQL s'est produite.	9
Transfert de script entre sites	5029	Indique une vulnérabilité de script intersite.	9
Vulnérabilité de format de chaîne	5030	Indique une vulnérabilité de chaîne de format.	9

Tableau 90. Catégories de bas niveau et niveaux de gravité pour la catégorie des événements d'exploitation (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Utilisation de validation d'entrée	5031	Indique qu'une tentative d'exploitation de validation d'entrée a été détectée.	9
Exécution de code à distance	5032	Indique qu'une tentative d'exécution de code à distance a été détectée.	9
Corruption de mémoire	5033	Indique qu'une exploitation de corruption de mémoire a été détectée.	9
Exécution de commande	5034	Indique qu'une tentative d'exécution de commande à distance a été détectée.	9
Injection de code	5035	Indique qu'une injection de code a été détectée.	9
Attaque par réinsertion	5036	Indique qu'une attaque de réexécution a été détectée.	9

## Logiciel malveillant

La catégorie des logiciels malveillants (logiciels malveillants) contient des événements liés aux tentatives d'exploitation et aux tentatives de débordement de mémoire tampon.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de logiciels malveillables.

Tableau 91. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements de logiciels malveillants

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Logiciel malveillant inconnu	6001	Indique un virus inconnu.	4
Porte dérobée détectée	6002	Indique qu'une porte arrière du système a été détectée.	9
Pièce jointe hostile	6003	Indique une pièce jointe de courrier hostile.	6
Logiciel malveillant	6004	Indique un virus.	6
Téléchargement d'un logiciel hostile	6005	Indique un téléchargement de logiciel hostile sur votre réseau.	6

Tableau 91. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements de logiciels malveillants (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Virus détecté	6006	Indique qu'un virus a été détecté.	8
Logiciel malveillant autre	6007	Indique un logiciel malveillant divers	4
Cheval de Troie détecté	6008	Indique qu'un cheval de Troie a été détecté.	7
Logiciel espion détecté	6009	Indique qu'un logiciel espion a été détecté sur votre système.	6
Analyse de contenu	6010	Indique qu'une tentative d'analyse de votre contenu a été détectée.	3
Echec de l'analyse de contenu	6011	Indique qu'une analyse de votre contenu a échoué.	8
Réussite de l'analyse de contenu	6012	Indique qu'une analyse de votre contenu a abouti.	3
Analyse de contenu en cours	6013	Indique qu'une analyse de votre contenu est en cours.	3
Journal de clés	6014	Indique qu'un consignateur de clés a été détecté.	7
Logiciel publicitaire détecté	6015	Indique que Ad-Ware a été détecté.	4
Réussite de la mise en quarantaine	6016	Indique qu'une action de quarantaine a abouti.	3
Echec de la mise en quarantaine	6017	Indique qu'une action de quarantaine a échoué.	8
Infection par logiciel malveillant	6018	Indique qu'une infection par un logiciel malveillant a été détectée.	10
Retrait réussi	6019	Indique que la suppression a abouti.	3
Echec du retrait	6020	Indique que la suppression a échoué.	8

## Activité suspecte

La catégorie suspecte contient des événements liés à des virus, des chevaux de Troie, des attaques à la porte arrière et d'autres formes de logiciels hostiles.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'activité suspecte.

*Tableau 92. Catégories et niveaux de gravité de faible niveau pour la catégorie d'événements d'activité suspects*

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Événement suspect inconnu	7001	Indique un événement suspect inconnu.	3
Modèle suspect détecté	7002	Indique qu'un modèle suspect a été détecté.	3
Contenu modifié par le pare-feu	7003	Indique que le contenu a été modifié par le pare-feu.	3
Commande ou données non valides	7004	Indique une commande ou des données non valides.	3
Paquet suspect	7005	Indique un paquet suspect.	3
Activité suspecte	7006	Indique une activité suspecte.	3
Nom de fichier suspect	7007	Indique un nom de fichier suspect.	3
Activité de port suspecte	7008	Indique une activité de port suspecte.	3
Routage suspect	7009	Indique un routage suspect.	3
Vulnérabilité Web potentielle	7010	Indique une vulnérabilité Web potentielle.	3
Événement d'évitement inconnu	7011	Indique un événement de fraude inconnu.	5
Usurpation d'adresse IP	7012	Indique un usurpateur IP.	5
Fragmentation IP	7013	Indique une fragmentation IP.	3
Chevauchement de fragments IP	7014	Indique des fragments IP qui se chevauchent.	5
Évitement système de détection d'intrusion	7015	Indique une fraude IDS.	5
Anomalie du protocole DNS	7016	Indique une anomalie de protocole DNS.	3

Tableau 92. Catégories et niveaux de gravité de faible niveau pour la catégorie d'événements d'activité suspects (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Anomalie du protocole FTP	7017	Indique une anomalie de protocole FTP.	3
Anomalie du protocole de messagerie	7018	Indique une anomalie de protocole de messagerie.	3
Anomalie du protocole de routage	7019	Indique une anomalie du protocole de routage.	3
Anomalie du protocole Web	7020	Indique une anomalie de protocole Web.	3
Anomalie du protocole SQL	7021	Indique une anomalie de protocole SQL.	3
Code exécutable détecté	7022	Indique qu'un code exécutable a été détecté.	5
Événement suspect autre	7023	Indique un événement suspect divers.	3
Fuite d'informations	7024	Indique une fuite d'informations.	1
Vulnérabilité de messagerie potentielle	7025	Indique une vulnérabilité potentielle dans le serveur de messagerie.	4
Vulnérabilité de version potentielle	7026	Indique une vulnérabilité potentielle dans la version IBM QRadar.	4
Vulnérabilité FTP potentielle	7027	Indique une vulnérabilité FTP potentielle.	4
Vulnérabilité SSH potentielle	7028	Indique une vulnérabilité SSH potentielle.	4
Vulnérabilité DNS potentielle	7029	Indique une vulnérabilité potentielle dans le serveur DNS.	4
Vulnérabilité SMB potentielle	7030	Indique une vulnérabilité de SMB (Samba) potentielle.	4
Vulnérabilité de base de données potentielle	7031	Indique une vulnérabilité potentielle dans la base de données.	4

Tableau 92. Catégories et niveaux de gravité de faible niveau pour la catégorie d'événements d'activité suspects (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Anomalie de protocole IP	7032	Indique une anomalie potentielle du protocole IP	3
Adresse IP suspecte	7033	Indique qu'une adresse IP suspecte a été détectée.	2
Utilisation du protocole IP non valide	7034	Indique un protocole IP non valide.	2
Protocole non valide	7035	Indique un protocole non valide.	4
Événements de fenêtre suspects	7036	Indique un événement suspect avec un écran sur votre bureau.	2
Activité ICMP suspecte	7037	Indique une activité ICMP suspecte.	2
Vulnérabilité NFS potentielle	7038	Indique une vulnérabilité potentielle du système de fichiers réseau (NFS).	4
Vulnérabilité NNTP potentielle	7039	Indique une vulnérabilité NNTP (Network News Transfer Protocol) potentielle.	4
Vulnérabilité RPC potentielle	7040	Indique une vulnérabilité RPC potentielle.	4
Vulnérabilité Telnet potentielle	7041	Indique une vulnérabilité Telnet potentielle sur votre système.	4
Vulnérabilité SNMP potentielle	7042	Indique une vulnérabilité SNMP potentielle.	4
Combinaison d'indicateurs TCP interdite	7043	Indique qu'une combinaison d'indicateur TCP non valide a été détectée.	5
Combinaison d'indicateurs TCP suspecte	7044	Indique qu'une combinaison d'indicateur TCP potentiellement non valide a été détectée.	4



Tableau 92. Catégories et niveaux de gravité de faible niveau pour la catégorie d'événements d'activité suspects (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Utilisation du protocole ICMP interdite	7045	Indique qu'une utilisation non valide du protocole ICMP a été détectée.	5
Utilisation du protocole ICMP suspecte	7046	Indique qu'une utilisation potentiellement non valide du protocole ICMP a été détectée.	4
Type ICMP interdit	7047	Indique qu'un type ICMP non valide a été détecté.	5
Code ICMP interdit	7048	Indique qu'un code ICMP non valide a été détecté.	5
Type ICMP suspect	7049	Indique qu'un type ICMP potentiellement non valide a été détecté.	4
Code ICMP suspect	7050	Indique qu'un code ICMP potentiellement non valide a été détecté.	4
Port TCP 0	7051	Indique qu'un paquet TCP utilise un port réservé (0) pour la source ou la destination.	4
Port UDP 0	7052	Indique qu'un paquet UDP utilise un port réservé (0) pour la source ou la destination.	4
Adresse IP hostile	7053	Indique l'utilisation d'une adresse IP hostile connue.	4
Adresse IP de la liste de surveillance	7054	Indique l'utilisation d'une adresse IP à partir d'une liste de surveillance d'adresses IP.	4
Adresse IP d'un attaquant connu	7055	Indique l'utilisation d'une adresse IP d'un contrevenant connu.	4
Adresse IP RFC 1918 (privée)	7056	Indique l'utilisation d'une adresse IP à partir d'une plage d'adresses IP privées.	4

Tableau 92. Catégories et niveaux de gravité de faible niveau pour la catégorie d'événements d'activité suspects (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Vulnérabilité VoIP potentielle	7057	Indique une vulnérabilité VoIP potentielle.	4
Adresse de liste noire	7058	Indique qu'une adresse IP figure sur la liste noire.	8
Adresse de liste de surveillance	7059	Indique que l'adresse IP figure sur la liste des adresses IP surveillées.	7
Adresse Darknet	7060	Indique que l'adresse IP fait partie d'un darknet.	5
Adresse Botnet	7061	Indique que l'adresse fait partie d'un botnet.	7
Adresse suspecte	7062	Indique que l'adresse IP doit être surveillée.	5
Contenu incorrect	7063	Indique que le contenu incorrect a été détecté.	7
Certificat non valide	7064	Indique qu'un certificat non valide a été détecté.	7
Activité utilisateur	7065	Indique qu'une activité utilisateur a été détectée.	7
Utilisation de protocole suspecte	7066	Indique qu'une utilisation suspecte du protocole a été détectée.	5
Activité BGP suspecte	7067	Indique qu'une utilisation du protocole BGP (Border Gateway Protocol) a été détectée.	5
Empoisonnement de chemin	7068	Indique qu'une corruption de routage a été détectée.	5
Empoisonnement ARP	7069	Indique qu'un empoisonnement par ARP-cache a été détecté.	5
Périphérique voyou détecté	7070	Indique qu'un périphérique voyou a été détecté.	5
Adresse de l'organisme gouvernemental	7071	Indique qu'une adresse d'agence gouvernementale a été détectée.	3

## Système

La catégorie système contient les événements associés aux modifications du système, à l'installation des logiciels ou aux messages d'état.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie système.

*Tableau 93. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements système*

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Événement système inconnu	8001	Indique un événement système inconnu.	1
Initialisation du système	8002	Indique un redémarrage du système.	1
Configuration système	8003	Indique une modification de la configuration du système.	1
Arrêt système	8004	Indique que le système a été arrêté.	1
Echec du système	8005	Indique une défaillance du système.	6
Statut du système	8006	Indique un événement d'information.	1
Erreur système	8007	Indique une erreur système.	3
Événement système autre	8008	Indique un événement système divers.	1
Démarrage du service	8009	Indique que les services système ont démarré.	1
Arrêt du service	8010	Indique que les services système ont été arrêtés.	1
Echec du service	8011	Indique une défaillance du système.	6
Réussite de la modification du registre	8012	Indique qu'une modification du registre a abouti.	1
Réussite de la modification de la politique de l'hôte	8013	Indique qu'une modification de la règle d'hôte a abouti.	1
Réussite de la modification du fichier	8014	Indique qu'une modification d'un fichier a abouti.	1
Réussite de la modification de la pile	8015	Indique qu'une modification de la pile a abouti.	1

Tableau 93. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements système (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Réussite de la modification de l'application	8016	Indique qu'une modification de l'application a abouti.	1
Réussite de la modification de la configuration	8017	Indique qu'une modification de la configuration a abouti.	1
Réussite de la modification du service	8018	Indique qu'une modification d'un service a abouti.	1
Echec de la modification du registre	8019	Indique qu'une modification du registre a échoué.	1
Echec de la modification de la politique de l'hôte	8020	Indique qu'une modification de la règle d'hôte a échoué.	1
Echec de la modification du fichier	8021	Indique qu'une modification d'un fichier a échoué.	1
Echec de la modification de la pile	8022	Indique qu'une modification de la pile a échoué.	1
Echec de la modification de l'application	8023	Indique qu'une modification d'une application a échoué.	1
Echec de la modification de la configuration	8024	Indique qu'une modification de la configuration a échoué.	1
Echec de la modification du service	8025	Indique qu'une modification du service a échoué.	1
Ajout au registre	8026	Indique qu'un nouvel élément a été ajouté au registre.	1
Création des politiques de l'hôte	8027	Indique qu'une nouvelle entrée a été ajoutée au registre.	1
Création du fichier	8028	Indique qu'une nouvelle a été créée dans le système.	1
Application installée	8029	Indique qu'une nouvelle application a été installée sur le système.	1

Tableau 93. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements système (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Service installé	8030	Indique qu'un nouveau service a été installé sur le système.	1
Suppression du registre	8031	Indique qu'une entrée de registre a été supprimée.	1
Politique de l'hôte supprimée	8032	Indique qu'une entrée de règle hôte a été supprimée.	1
Fichier supprimé	8033	Indique qu'un fichier a été supprimé.	1
Application désinstallée	8034	Indique qu'une application a été désinstallée.	1
Service désinstallé	8035	Indique qu'un service a été désinstallé.	1
Informations sur le service	8036	Indique des informations système.	3
Autorisation action système	8037	Indique qu'une tentative d'action sur le système a été autorisée.	3
Refus action système	8038	Indique qu'une tentative d'action sur le système a été refusée.	4
Tâche périodique	8039	Indique un message crontab.	1
Etat tâche périodique	8040	Indique un message d'état crontab.	1
Echec tâche périodique	8041	Indique un message d'échec crontab.	4
Réussite tâche périodique	8042	Indique un message de réussite crontab.	1
Démon	8043	Indique un message daemon.	1
Etat démon	8044	Indique un message d'état daemon.	1
Echec démon	8045	Indique un message d'échec daemon.	4
Réussite démon	8046	Indique un message de réussite daemon.	1
Noyau	8047	Indique un message de noyau.	1

Tableau 93. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements système (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Etat noyau	8048	Indique un message d'état du noyau.	1
Echec noyau	8049	Indique un message d'échec du noyau.	
Réussite noyau	8050	Indique un message de réussite du noyau.	1
Authentification	8051	Indique un message d'authentification.	1
Informations	8052	Indique un message d'information.	2
Remarque	8053	Indique un message de notification.	3
Avertissement	8054	Indique un message d'avertissement.	5
Erreur	8055	Indique un message d'erreur.	7
Critique	8056	Indique un message critique.	9
Débogage	8057	Indique un message de débogage.	1
Messages	8058	Indique un message générique.	1
Accès par privilège	8059	Indique que l'accès au privilège a été tenté.	3
Alerte	8060	Indique un message d'alerte.	9
Urgence	8061	Indique un message d'urgence.	9
Etat SNMP	8062	Indique un message d'état SNMP.	1
Etat FTP	8063	Indique un message d'état FTP.	1
Etat NTP	8064	Indique un message d'état NTP.	1
Défaillance radio point d'accès	8065	Indique un incident radio point d'accès.	3
Non-concordance de configuration de protocole de chiffrement	8066	Indique une non concordance de configuration de protocole de chiffrement.	3

Tableau 93. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements système (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Unité client ou serveur d'authentification mal configuré(e)	8067	Indique qu'un périphérique client ou un serveur d'authentification n'a pas été configuré correctement.	5
Échec d'activation du secours automatique	8068	Indique un incident d'activation de secours automatique.	5
Échec de désactivation du secours automatique	8069	Indique un incident de désactivation de secours automatique.	5
Secours automatique activé	8070	Indique que la fonction de secours automatique a été activée.	1
Association du secours automatique perdue	8071	Indique qu'une association de secours automatique a été perdue.	5
Échec lancement MainMode	8072	Indique l'échec de l'initialisation de MainMode.	5
MainMode lancé	8073	Indique que l'initialisation de MainMode a abouti.	1
État de MainMode	8074	Indique qu'un message d'état MainMode a été signalé.	1
Échec lancement de QuickMode	8075	Indique que l'initialisation de QuickMode a échoué.	5
Mode rapide lancé	8076	Indique que l'initialisation de QuickMode a abouti.	1
Etat mode rapide	8077	Indique qu'un message d'état du mode QuickMode a été signalé.	1
Licence non valide	8078	Indique une licence non valide.	3
Licence arrivée à expiration	8079	Indique une licence expirée.	3
Nouvelle licence appliquée	8080	Indique une nouvelle licence appliquée.	1

Tableau 93. Catégories de bas niveau et niveaux de gravité pour la catégorie d'événements système (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Erreur de licence	8081	Indique une erreur de licence.	5
Statut de la licence	8082	Indique un message d'état de la licence.	1
Erreur de configuration	8083	Indique qu'une erreur de configuration a été détectée.	5
Interruption de service	8084	Indique qu'une interruption de service a été détectée.	5
Allocation EPS ou FPM dépassée	8085	Indique que les allocations du pool de licences pour EPS ou FPM ont été dépassées.	3
Etats des performances	8086	Indique que l'état des performances a été signalé.	1
Dégradation des performances	8087	Indique que les performances sont en cours de dégradation.	4
Problème de configuration	8088	Indique qu'une configuration incorrecte a été détectée.	5

## Politique

La catégorie de règles contient des événements associés à l'administration de la stratégie de réseau et des ressources réseau de surveillance pour les violations de règles.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de règles.

Tableau 94. Catégories de bas niveau et niveaux de gravité pour la catégorie de règles

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Violation de politique inconnue	9001	Indique une violation de règle inconnue.	2
Violation de la politique Web	9002	Indique une violation de règle Web.	2
Violation de la politique d'accès distant	9003	Indique une violation de règle d'accès à distance.	2
Violation de la politique IRC/IM	9004	Indique une violation de règle de messagerie instantanée.	2



Tableau 94. Catégories de bas niveau et niveaux de gravité pour la catégorie de règles (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Violation de la politique P2P	9005	Indique une violation de règle d'égal à égal (P2P).	2
Violation de la politique d'accès IP	9006	Indique une violation de règle d'accès IP.	2
Violation de la politique d'application	9007	Indique une violation de règle d'application.	2
Violation de la politique de base de données	9008	Indique une violation de règle de base de données.	2
Violation de la politique de seuil réseau	9009	Indique une violation de règle de seuil réseau.	2
Violation de la politique relative au contenu pornographique	9010	Indique une violation de règle de porno.	2
Violation de la politique relative aux jeux	9011	Indique une violation de règle de jeu.	2
Violation de la politique Autre	9012	Indique une violation de règles diverses.	2
Violation de la politique de conformité	9013	Indique une violation de règle de conformité.	2
Violation de la politique de messagerie	9014	Indique une violation de règle de messagerie.	2
Violation de la politique IRC	9015	Indique une violation de règle IRC	2
Violation de la politique de message instantané	9016	Indique une violation de règle liée aux activités de message instantané (IM).	2
Violation de la politique VoIP	9017	Indique une violation de règle VoIP	2
Réussite	9018	Indique un message de réussite de règle.	1
Echec	9019	Indique un message d'échec de règle.	4
Violation de la politique de prévention de perte de données	9020	Indique une violation de règle de prévention des pertes de données.	2
Objet de liste de surveillance	9021	Indique un objet de liste de surveillance.	2
Autorisation de la politique Web	9022	Indique une nouvelle allocation de politique Web.	1

## Inconnu

La catégorie Inconnu contient des événements qui ne sont pas analysés et ne peuvent donc pas être catégorisés.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie Inconnu.

*Tableau 95. Catégories de bas niveau et niveaux de gravité pour la catégorie Inconnu*

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Inconnu	10001	Indique un événement inconnu.	3
Événement Snort inconnu	10002	Indique un événement Snort inconnu.	3
Événement Dragon inconnu	10003	Indique un événement Dragon inconnu.	3
Événement de pare-feu Pix inconnu	10004	Indique un événement Pare-feu Cisco Private Internet Exchange (PIX) inconnu.	3
Événement de point de basculement inconnu	10005	Indique un événement HP TippingPoint inconnu.	3
Événement Windows Auth Server inconnu	10006	Indique un événement Windows Auth Server inconnu.	3
Événement Nortel inconnu	10007	Indique un événement Nortel inconnu.	3
Stocké	10009	Indique un événement stocké inconnu.	3
Comportement	11001	Indique un événement comportemental inconnu.	3
Seuil	11002	Indique un événement de seuil inconnu.	3
Anomalie	11003	Indique un événement d'anomalie inconnu.	3

## CRE

La catégorie d'événement de règle personnalisée (CRE) contient des événements générés à partir de la règle une infraction, un flux ou même personnalisé.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie CRE.

Tableau 96. Catégories de bas niveau et niveaux de gravité pour la catégorie CRE

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Événement CRE inconnu	12001	Indique un événement de moteur de règles personnalisé inconnu.	5
Correspondance de règle d'événement unique	12002	Indique une correspondance de règle d'événement unique.	5
Correspondance de règle de séquence d'événements	12003	Indique une correspondance de règle de séquence d'événements.	5
Correspondance de règle de séquence d'événements d'infractions croisées	12004	Indique une correspondance de règle de séquence d'événements d'infraction croisée.	5
Correspondance de règle d'infraction	12005	Indique une correspondance de règle d'infraction.	5

## Utilisation potentielle

La catégorie d'exploitation potentielle contient des événements liés à des tentatives d'exploitation potentielles et à des tentatives de débordement de mémoire tampon.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'exploitation potentielle.

Tableau 97. Catégories et niveaux de gravité de faible niveau pour la catégorie d'exploitation potentielle

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Attaque par exploitation potentielle inconnue	13001	Indique qu'une attaque d'exploitation potentielle a été détectée.	7
Débordement de tampon potentiel	13002	Indique qu'un dépassement de tampon potentiel a été détecté.	7
Utilisation DNS potentielle	13003	Indique qu'une attaque potentiellement abusive via le serveur DNS a été détectée.	7
Utilisation Telnet potentielle	13004	Indique qu'une attaque potentiellement abusive via Telnet a été détectée.	7

Tableau 97. Catégories et niveaux de gravité de faible niveau pour la catégorie d'exploitation potentielle (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Exploitation Linux potentielle	13005	Indique qu'une attaque potentiellement abusive via Linux a été détectée.	7
Exploitation UNIX potentielle	13006	Indique qu'une attaque potentiellement abusive via UNIX a été détectée.	7
Exploitation Windows potentielle	13007	Indique qu'une attaque potentiellement abusive via Windows a été détectée.	7
Utilisation de messagerie potentielle	13008	Indique qu'une attaque potentiellement abusive via le courrier a été détectée.	7
Utilisation d'infrastructure potentielle	13009	Indique qu'une attaque d'exploitation potentielle sur l'infrastructure système a été détectée.	7
Utilisation de type autre potentielle	13010	Indique qu'une attaque potentiellement abusive a été détectée.	7
Utilisation Web potentielle	13011	Indique qu'une attaque potentiellement abusive via le Web a été détectée.	7
Connexion Botnet potentielle	13012	Indique qu'une attaque potentiellement abusive utilisant le botnet a été détectée.	6
Activité de ver potentielle	13013	Indique qu'une attaque potentielle utilisant une activité de ver a été détectée.	6

## Flux

La catégorie de flux inclut les événements associés aux actions de flux.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de flux.

Tableau 98. Catégories de bas niveau et niveaux de gravité pour la catégorie de flux

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Flux unidirectionnel	14001	Indique un flux unidirectionnel d'événements.	5
Nombre bas de flux unidirectionnels	14002	Indique un nombre faible de flux unidirectionnels d'événements.	5
Nombre moyen de flux unidirectionnels	14003	Indique un nombre moyen de flux unidirectionnels d'événements.	5
Nombre élevé de flux unidirectionnels	14004	Indique un nombre élevé de flux unidirectionnels d'événements.	5
Flux TCP unidirectionnels	14005	Indique un flux TCP unidirectionnel.	5
Nombre bas de flux TCP unidirectionnels	14006	Indique un nombre faible de flux TCP unidirectionnels.	5
Nombre moyen de flux TCP unidirectionnels	14007	Indique un nombre moyen de flux TCP unidirectionnels.	5
Nombre élevé de flux TCP unidirectionnels	14008	Indique un nombre élevé de flux TCP unidirectionnels.	5
Flux ICMP unidirectionnel	14009	Indique un flux ICMP unidirectionnel.	5
Nombre bas de flux ICMP unidirectionnels	14010	Indique un nombre faible de flux ICMP unidirectionnels.	5
Nombre moyen de flux ICMP unidirectionnels	14011	Indique un nombre moyen de flux ICMP unidirectionnels.	5
Nombre élevé de flux ICMP unidirectionnels	14012	Indique un nombre élevé de flux ICMP unidirectionnels.	5
Flux ICMP suspect	14013	Indique un flux ICMP suspect.	5
Flux UDP suspect	14014	Indique un flux UDP suspect.	5
Flux TCP suspect	14015	Indique un flux TCP suspect.	5
Flux suspect	14016	Indique un flux suspect.	5
Flux de paquets vides	14017	Indique les flux de paquets vides.	5
Nombre bas de flux de paquets vides	14018	Indique un nombre faible de flux de paquets vides.	5
Nombre moyen de flux de paquets vides	14019	Indique un nombre moyen de flux de paquets vides.	5
Nombre élevé de flux de paquets vides	14020	Indique un nombre élevé de flux de paquets vides.	5
Flux à gros contenu utile	14021	Indique une charge importante de flux.	5

Tableau 98. Catégories de bas niveau et niveaux de gravité pour la catégorie de flux (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Nombre bas de flux à gros contenu utile	14022	Indique un faible nombre de flux de charge de grande taille.	5
Nombre moyen de flux à gros contenu utile	14023	Indique un nombre moyen de flux de charge importants.	5
Nombre élevé de flux à gros contenu utile	14024	Indique un nombre élevé de flux de charge importants.	5
Un pirate sur plusieurs flux cibles	14025	Indique qu'un pirate cible de nombreux flux.	5
Plusieurs pirates sur un flux cible	14026	Indique que de nombreux pirates ciblent un flux.	5
Flux inconnu	14027	Indique un flux inconnu.	5
Enregistrement Netflow	14028	Indique un enregistrement Netflow.	5
Enregistrement QFlow	14029	Indique un enregistrement QFlow.	5
Enregistrement SFlow	14030	Indique un enregistrement SFlow.	5
Enregistrement Packeteer	14031	Indique un enregistrement de paquet.	5
Flux autre	14032	Indique un flux autre.	5
Gros transfert de données	14033	Indique un transfert important de données.	5
Transfert de données important sortant	14034	Indique un transfert important de données sortantes.	5
Flux VoIP	14035	Indique les flux VoIP.	5

## Défini par l'utilisateur

La catégorie Défini par l'utilisateur contient des événements associés à des objets définis par l'utilisateur

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie Défini par l'utilisateur.

Tableau 99. Catégories de bas niveau et niveaux de gravité pour la catégorie Défini par l'utilisateur

Catégorie d'événements de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Sentinelle personnalisée basse	15001	Indique un événement d'anomalie personnalisé de gravité faible.	3
Sentinelle personnalisée intermédiaire	15002	Indique un événement d'anomalie personnalisé de gravité moyenne.	5

Tableau 99. Catégories de bas niveau et niveaux de gravité pour la catégorie Défini par l'utilisateur (suite)

Catégorie d'événements de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Sentinelle personnalisée élevée	15003	Indique un événement d'anomalie personnalisé de gravité élevée.	7
Sentinelle personnalisée 1	15004	Indique un événement d'anomalie personnalisé avec un niveau de gravité 1.	1
Sentinelle personnalisée 2	15005	Indique un événement d'anomalie personnalisé avec un niveau de gravité 2.	2
Sentinelle personnalisée 3	15006	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 3.	3
Sentinelle personnalisée 4	15007	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 4.	4
Sentinelle personnalisée 5	15008	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 5.	5
Sentinelle personnalisée 6	15009	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 6.	6
Sentinelle personnalisée 7	15010	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 7.	7
Sentinelle personnalisée 8	15011	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 8.	8
Sentinelle personnalisée 9	15012	Indique un événement d'anomalie personnalisé avec un niveau de gravité de 9.	9
Politique personnalisée basse	15013	Indique un événement de règle personnalisé avec un niveau de gravité faible.	3

Tableau 99. Catégories de bas niveau et niveaux de gravité pour la catégorie Défini par l'utilisateur (suite)

Catégorie d'événements de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Politique personnalisée intermédiaire	15014	Indique un événement de règle personnalisé avec un niveau de gravité moyen.	5
Politique personnalisée élevée	15015	Indique un événement de règle personnalisé avec un niveau de gravité élevé.	7
Politique personnalisée 1	15016	Indique un événement de règle personnalisé avec un niveau de gravité 1.	1
Politique personnalisée 2	15017	Indique un événement de règle personnalisé avec un niveau de gravité 2.	2
Politique personnalisée 3	15018	Indique un événement de règle personnalisé avec un niveau de gravité de 3.	3
Politique personnalisée 4	15019	Indique un événement de règle personnalisé avec un niveau de gravité de 4.	4
Politique personnalisée 5	15020	Indique un événement de règle personnalisé avec un niveau de gravité 5.	5
Politique personnalisée 6	15021	Indique un événement de règle personnalisé avec un niveau de gravité 6.	6
Politique personnalisée 7	15022	Indique un événement de règle personnalisé avec un niveau de gravité 7.	7
Politique personnalisée 8	15023	Indique un événement de règle personnalisé avec un niveau de gravité de 8.	8
Politique personnalisée 9	15024	Indique un événement de règle personnalisé avec un niveau de gravité 9.	9



Tableau 99. Catégories de bas niveau et niveaux de gravité pour la catégorie Défini par l'utilisateur (suite)

<b>Catégorie d'événements de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Utilisateur personnalisé bas	15025	Indique un événement utilisateur personnalisé avec un niveau de gravité faible.	3
Utilisateur personnalisé moyen	15026	Indique un événement utilisateur personnalisé avec un niveau de gravité moyen.	5
Utilisateur personnalisé élevé	15027	Indique un événement utilisateur personnalisé avec un niveau de gravité élevé.	7
Utilisateur personnalisé 1	15028	Indique un événement utilisateur personnalisé avec un niveau de gravité 1.	1
Utilisateur personnalisé 2	15029	Indique un événement utilisateur personnalisé avec un niveau de gravité 2.	2
Utilisateur personnalisé 3	15030	Indique un événement utilisateur personnalisé avec un niveau de gravité de 3.	3
Utilisateur personnalisé 4	15031	Indique un événement utilisateur personnalisé avec un niveau de gravité de 4.	4
Utilisateur personnalisé 5	15032	Indique un événement utilisateur personnalisé avec un niveau de gravité 5.	5
Utilisateur personnalisé 6	15033	Indique un événement utilisateur personnalisé avec un niveau de gravité 6.	6
Utilisateur personnalisé 7	15034	Indique un événement utilisateur personnalisé avec un niveau de gravité 7.	7
Utilisateur personnalisé 8	15035	Indique un événement utilisateur personnalisé avec un niveau de gravité de 8.	8

Tableau 99. Catégories de bas niveau et niveaux de gravité pour la catégorie Défini par l'utilisateur (suite)

Catégorie d'événements de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Utilisateur personnalisé 9	15036	Indique un événement utilisateur personnalisé avec un niveau de gravité de 9.	9

## Audit SIM

La catégorie Audit SIM contient les événements associés à l'interaction utilisateur avec la console IBM QRadar et les fonctions d'administration.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie Audit SIM.

Tableau 100. Catégories de bas niveau et niveaux de gravité de la catégorie d'audit SIM

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Authentification d'utilisateur SIM	16001	Indique une connexion utilisateur ou déconnexion sur la console.	5
Modification de configuration SIM	16002	Indique qu'un utilisateur a modifié la configuration ou le déploiement SIM.	3
Action utilisateur SIM	16003	Indique qu'un utilisateur a lancé un processus, tel que le démarrage d'une sauvegarde ou la génération d'un rapport, dans le module SIM.	3
Session créée	16004	Indique qu'une session utilisateur a été créée.	3
Session détruite	16005	Indique qu'une session utilisateur a été détruite.	3
Session Admin créée	16006	Indique qu'une session d'administration a été créée.	
Session Admin détruite	16007	Indique qu'une session d'administration a été détruite.	3
Authentification de session non valide	16008	Indique une authentification de session non valide.	5
Authentification de session arrivée à expiration	16009	Indique qu'une authentification de session a expiré.	3

Tableau 100. Catégories de bas niveau et niveaux de gravité de la catégorie d'audit SIM (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Configuration de Risk Manager	16010	Indique qu'un utilisateur a modifié la configuration IBM QRadar Risk Manager.	3

## Découverte d'hôte VIS

Lorsque le composant VIS reconnaît et stocke de nouveaux hôtes, ports ou vulnérabilités détectés sur le réseau, le composant VIS génère des événements. Ces événements sont envoyés à Collecteur d'événements pour être en corrélation avec d'autres événements de sécurité.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de reconnaissance d'hôte VIS.

Tableau 101. Catégories de niveau inférieur et niveaux de gravité pour la catégorie de reconnaissance d'hôte VIS

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Nouvel hôte découvert	17001	Indique que le composant VIS a détecté un nouvel hôte.	3
Nouveau port découvert	17002	Indique que le composant VIS a détecté un nouveau port ouvert.	3
Nouvelle vulnérabilité découverte	17003	Indique que le composant VIS a détecté une nouvelle vulnérabilité.	3
Nouveau système d'exploitation découvert	17004	Indique que le composant VIS a détecté un nouveau système d'exploitation sur un hôte.	3
Hôte en bloc découvert	17005	Indique que le composant VIS a détecté de nombreux nouveaux hôtes dans une courte période.	3

## Application

La catégorie d'application contient des événements associés à l'activité de l'application, tels que le courrier électronique ou l'activité FTP.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'application.

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Mail ouvert	18001	Indique qu'une connexion par courrier électronique a été établie.	1
Mail fermé	18002	Indique qu'une connexion par courrier électronique a été fermée.	1
Mail réinitialisé	18003	Indique qu'une connexion par courrier électronique a été réinitialisée.	3
Mail terminé	18004	Indique qu'une connexion par courrier électronique a été arrêtée.	4
Mail refusé	18005	Indique qu'une connexion par courrier électronique a été refusée.	4
Courrier en cours	18006	Indique qu'une connexion par courrier électronique est en cours de tentative.	1
Mail différé	18007	Indique qu'une connexion par courrier électronique a été retardée.	4
Mail en file d'attente	18008	Indique qu'une connexion par courrier électronique a été mise en file d'attente.	3
Mail redirigé	18009	Indique qu'une connexion par courrier électronique a été redirigée.	1
FTP ouvert	18010	Indique qu'une connexion FTP a été ouverte.	1
FTP fermé	18011	Indique qu'une connexion FTP a été fermée.	1
FTP réinitialisé	18012	Indique qu'une connexion FTP a été réinitialisée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
FTP terminé	18013	Indique qu'une connexion FTP a été arrêtée.	4
FTP refusé	18014	Indique qu'une connexion FTP a été refusée.	4
FTP en cours	18015	Indique qu'une connexion FTP est en cours.	1
FTP redirigé	18016	Indique qu'une connexion FTP a été redirigée.	3
HTTP ouvert	18017	Indique qu'une connexion HTTP a été établie.	1
HTTP fermé	18018	Indique qu'une connexion HTTP a été fermée.	1
HTTP réinitialisé	18019	Indique qu'une connexion HTTP a été réinitialisée.	3
HTTP terminé	18020	Indique qu'une connexion HTTP a été arrêtée.	4
HTTP refusé	18021	Indique qu'une connexion HTTP a été refusée.	4
HTTP en cours	18022	Indique qu'une connexion HTTP est en cours.	1
HTTP différé	18023	Indique qu'une connexion HTTP a été retardée.	3
HTTP en file d'attente	18024	Indique qu'une connexion HTTP a été mise en file d'attente.	1
HTTP redirigé	18025	Indique qu'une connexion HTTP a été redirigée.	1
Proxy HTTP	18026	Indique qu'une connexion HTTP est en cours de proxy.	1
HTTPS ouvert	18027	Indique qu'une connexion HTTPS a été établie.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
HTTPS fermé	18028	Indique qu'une connexion HTTPS a été fermée.	1
HTTPS réinitialisé	18029	Indique qu'une connexion HTTPS a été réinitialisée.	3
HTTPS terminé	18030	Indique qu'une connexion HTTPS a été arrêtée.	4
HTTPS refusé	18031	Indique qu'une connexion HTTPS a été refusée.	4
HTTPS en cours	18032	Indique qu'une connexion HTTPS est en cours.	1
HTTPS différé	18033	Indique qu'une connexion HTTPS a été retardée.	3
HTTPS en file d'attente	18034	Indique qu'une connexion HTTPS a été mise en file d'attente.	3
HTTPS redirigé	18035	Indique qu'une connexion HTTPS a été redirigée.	3
Proxy HTTPS	18036	Indique qu'une connexion HTTPS est établie par proxy.	1
SSH ouvert	18037	Indique qu'une connexion SSH a été établie.	1
SSH fermé	18038	Indique qu'une connexion SSH a été fermée.	1
SSH réinitialisé	18039	Indique qu'une connexion SSH a été réinitialisée.	3
SSH terminé	18040	Indique qu'une connexion SSH a été arrêtée.	4
SSH refusé	18041	Indique qu'une session SSH a été refusée.	4
SSH en cours	18042	Indique qu'une session SSH est en cours.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
RemoteAccess ouvert	18043	Indique qu'une connexion d'accès à distance a été établie.	1
RemoteAccess fermé	18044	Indique qu'une connexion d'accès à distance a été fermée.	1
RemoteAccess réinitialisé	18045	Indique qu'une connexion d'accès à distance a été réinitialisée.	3
RemoteAccess terminé	18046	Indique qu'une connexion d'accès à distance a été arrêtée.	4
RemoteAccess refusé	18047	Indique qu'une connexion d'accès à distance a été refusée.	4
RemoteAccess en cours	18048	Indique qu'une connexion d'accès à distance est en cours.	1
RemoteAccess différé	18049	Indique qu'une connexion d'accès à distance a été retardée.	3
RemoteAccess redirigé	18050	Indique qu'une connexion d'accès à distance a été redirigée.	3
VPN ouvert	18051	Indique qu'une connexion VPN a été ouverte.	1
VPN fermé	18052	Indique qu'une connexion VPN a été fermée.	1
VPN réinitialisé	18053	Indique qu'une connexion VPN a été réinitialisée.	3
VPN terminé	18054	Indique qu'une connexion VPN a été arrêtée.	4
VPN refusé	18055	Indique qu'une connexion VPN a été refusée.	4
VPN en cours	18056	Indique qu'une connexion VPN est en cours.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
VPN différé	18057	Indique qu'une connexion VPN a été retardée	3
VPN en file d'attente	18058	Indique qu'une connexion VPN a été mise en file d'attente.	3
VPN redirigé	18059	Indique qu'une connexion VPN a été redirigée.	3
RDP ouvert	18060	Indique qu'une connexion RDP a été établie.	1
RDP fermé	18061	Indique qu'une connexion RDP a été fermée.	1
RDP réinitialisé	18062	Indique qu'une connexion RDP a été réinitialisée.	3
RDP terminé	18063	Indique qu'une connexion RDP a été arrêtée.	4
RDP refusé	18064	Indique qu'une connexion RDP a été refusée.	4
RDP en cours	18065	Indique qu'une connexion RDP est en cours.	1
RDP redirigé	18066	Indique qu'une connexion RDP a été redirigée.	3
FileTransfer ouvert	18067	Indique qu'une connexion de transfert de fichier a été établie.	1
FileTransfer fermé	18068	Indique qu'une connexion de transfert de fichier a été fermée.	1
FileTransfer réinitialisé	18069	Indique qu'une connexion de transfert de fichier a été réinitialisée.	3
FileTransfer terminé	18070	Indique qu'une connexion de transfert de fichier a été arrêtée.	4



Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
FileTransfer refusé	18071	Indique qu'une connexion de transfert de fichier a été refusée.	4
FileTransfer en cours	18072	Indique qu'une connexion de transfert de fichier est en cours.	1
FileTransfer différé	18073	Indique qu'une connexion de transfert de fichier a été retardée.	3
FileTransfer en file d'attente	18074	Indique qu'une connexion de transfert de fichier a été mise en file d'attente.	3
FileTransfer redirigé	18075	Indique qu'une connexion de transfert de fichier a été redirigée.	3
DNS ouvert	18076	Indique qu'une connexion DNS a été établie.	1
DNS fermé	18077	Indique qu'une connexion DNS a été fermée.	1
DNS réinitialisé	18078	Indique qu'une connexion DNS a été réinitialisée.	5
DNS terminé	18079	Indique qu'une connexion DNS a été arrêtée.	5
DNS refusé	18080	Indique qu'une connexion DNS a été refusée.	5
DNS en cours	18081	Indique qu'une connexion DNS est en cours.	1
DNS différé	18082	Indique qu'une connexion DNS a été retardée.	5
DNS redirigé	18083	Indique qu'une connexion DNS a été redirigée.	4
Discussion ouverte	18084	Indique qu'une connexion de discussion a été ouverte.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Discussion fermée	18085	Indique qu'une connexion de discussion a été fermée.	1
Discussion réinitialisée	18086	Indique qu'une connexion de discussion a été réinitialisée.	3
Discussion terminée	18087	Indique qu'une connexion de discussion a été interrompue.	3
Discussion refusée	18088	Indique qu'une connexion de discussion a été refusée.	3
Discussion en cours	18089	Indique qu'une connexion de discussion est en cours.	1
Discussion redirigée	18090	Indique qu'une connexion de discussion a été redirigée.	1
Base de données ouverte	18091	Indique qu'une connexion de base de données a été établie.	1
Base de données fermée	18092	Indique qu'une connexion de base de données a été fermée.	1
Base de données réinitialisée	18093	Indique qu'une connexion de base de données a été réinitialisée.	5
Base de données terminée	18094	Indique qu'une connexion de base de données a été arrêtée.	5
Base de données refusée	18095	Indique qu'une connexion à la base de données a été refusée.	5
Base de données en cours	18096	Indique qu'une connexion de base de données est en cours.	1
Base de données redirigée	18097	Indique qu'une connexion de base de données a été redirigée.	3
SMTP ouvert	18098	Indique qu'une connexion SMTP a été établie.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
SMTP fermé	18099	Indique qu'une connexion SMTP a été fermée.	1
SMTP réinitialisé	18100	Indique qu'une connexion SMTP a été réinitialisée.	3
SMTP terminé	18101	Indique qu'une connexion SMTP a été arrêtée.	5
SMTP refusé	18102	Indique qu'une connexion SMTP a été refusée.	5
SMTP en cours	18103	Indique qu'une connexion SMTP est en cours.	1
SMTP différé	18104	Indique qu'une connexion SMTP a été retardée.	3
SMTP en file d'attente	18105	Indique qu'une connexion SMTP a été mise en file d'attente.	3
SMTP redirigé	18106	Indique qu'une connexion SMTP a été redirigée.	3
Authentification ouverte	18107	Indique qu'une connexion au serveur d'autorisation a été établie.	1
Authentification fermée	18108	Indique qu'une connexion au serveur d'autorisation a été fermée.	1
Authentification réinitialisée	18109	Indique qu'une connexion au serveur d'autorisation a été réinitialisée.	3
Authentification terminée	18110	Indique qu'une connexion au serveur d'autorisation a été interrompue.	4
Authentification refusée	18111	Indique qu'une connexion au serveur d'autorisation a été refusée.	4

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Authentification en cours	18112	Indique qu'une connexion au serveur d'autorisation est en cours.	1
Authentification différée	18113	Indique qu'une connexion au serveur d'autorisation a été retardée.	3
Authentification en file d'attente	18114	Indique qu'une connexion au serveur d'autorisation a été mise en file d'attente.	3
Authentification redirigée	18115	Indique qu'une connexion au serveur d'autorisation a été redirigée.	2
P2P ouvert	18116	Indique qu'une connexion entre homologues (P2P) a été établie.	1
P2P fermé	18117	Indique qu'une connexion P2P a été fermée.	1
P2P réinitialisé	18118	Indique qu'une connexion P2P a été réinitialisée.	4
P2P terminé	18119	Indique qu'une connexion P2P a été arrêtée.	4
P2P refusé	18120	Indique qu'une connexion P2P a été refusée.	3
P2P en cours	18121	Indique qu'une connexion P2P est en cours.	1
Web ouvert	18122	Indique qu'une connexion Web a été établie.	1
Web fermé	18123	Indique qu'une connexion Web a été fermée.	1
Web réinitialisé	18124	Indique qu'une connexion Web a été réinitialisée.	4

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Web terminé	18125	Indique qu'une connexion Web a été arrêtée.	4
Web refusé	18126	Indique qu'une connexion Web a été refusée.	4
Web en cours	18127	Indique qu'une connexion Web est en cours.	1
Web différé	18128	Indique qu'une connexion Web a été retardée.	3
Web en file d'attente	18129	Indique qu'une connexion Web a été mise en file d'attente.	1
Web redirigé	18130	Indique qu'une connexion Web a été redirigée.	1
Proxy Web	18131	Indique qu'une connexion Web a été établie par proxy.	1
VoIP ouvert	18132	Indique qu'une connexion VoIP (Voice Over IP) a été établie.	1
VoIP fermé	18133	Indique qu'une connexion VoIP a été fermée.	1
VoIP réinitialisé	18134	Indique qu'une connexion VoIP a été réinitialisée.	3
VoIP terminé	18135	Indique qu'une connexion VoIP a été arrêtée.	3
VoIP refusé	18136	Indique qu'une connexion VoIP a été refusée.	3
VoIP en cours	18137	Indique qu'une connexion VoIP est en cours.	1
VoIP différé	18138	Indique qu'une connexion VoIP a été retardée.	3
VoIP redirigé	18139	Indique qu'une connexion VoIP a été redirigée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session LDAP démarrée	18140	Indique qu'une session LDAP a démarré.	1
Session LDAP terminée	18141	Indique qu'une session LDAP s'est terminée.	1
Session LDAP refusée	18142	Indique qu'une session LDAP a été refusée.	3
Etat de la session LDAP	18143	Indique qu'un message d'état de session LDAP a été signalé.	1
Echec de l'authentification LDAP	18144	Indique qu'une authentification LDAP a échoué.	4
Réussite de l'authentification LDAP	18145	Indique qu'une authentification LDAP a abouti.	1
Session AAA démarrée	18146	Indique qu'une session d'authentification, d'autorisation et de comptabilité (AAA) a démarré.	1
Session AAA terminée	18147	Indique qu'une session AAA s'est terminée.	1
Session AAA refusée	18148	Indique qu'une session AAA a été refusée.	3
Etat de la session AAA	18149	Indique qu'un message d'état de session AAA a été signalé.	1
Echec de l'authentification AAA	18150	Indique qu'une authentification AAA a échoué.	4
Réussite de l'authentification AAA	18151	Indique qu'une authentification AAA a abouti.	1
Echec de l'authentification IPSec	18152	Indique qu'une authentification IPSEC ( Internet Protocol Security) a échoué.	4
Réussite de l'authentification IPSec	18153	Indique qu'une authentification IPSEC a abouti.	1
Session IPSec démarrée	18154	Indique qu'une session IPSEC a démarré.	1
Session IPSec terminée	18155	Indique qu'une session IPSEC s'est terminée.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Erreur IPSec	18156	Indique qu'un message d'erreur IPSEC a été signalé.	5
État IPSec	18157	Indique qu'un message d'état de session IPSEC a été signalé.	1
Session IM ouverte	18158	Indique qu'une session Instant Messenger (IM) a été établie.	1
Session IM fermée	18159	Indique qu'une session IM a été fermée.	1
Session IM réinitialisée	18160	Indique qu'une session IM a été réinitialisée.	3
Session IM terminée	18161	Indique qu'une session IM a été arrêtée.	3
Session IM refusée	18162	Indique qu'une session IM a été refusée.	3
Session IM en cours	18163	Indique qu'une session de messagerie instantanée est en cours.	1
Session IM différée	18164	Indique qu'une session IM a été retardée	3
Session IM redirigée	18165	Indique qu'une session IM a été redirigée.	3
Session Whois ouverte	18166	Indique qu'une session WHOIS a été établie.	1
Session Whois fermée	18167	Indique qu'une session WHOIS a été fermée.	1
Session Whois réinitialisée	18168	Indique qu'une session WHOIS a été réinitialisée.	3
Session Whois terminée	18169	Indique qu'une session WHOIS a été arrêtée.	3
Session Whois refusée	18170	Indique qu'une session WHOIS a été refusée.	3
Session Whois en cours	18171	Indique qu'une session WHOIS est en cours.	1
Session Whois redirigée	18172	Indique qu'une session WHOIS a été redirigée.	3
Session Traceroute ouverte	18173	Indique qu'une session Traceroute a été établie.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session Traceroute fermée	18174	Indique qu'une session Traceroute a été fermée.	1
Session Traceroute refusée	18175	Indique qu'une session Traceroute a été refusée.	3
Session Traceroute en cours	18176	Indique qu'une session Traceroute est en cours.	1
Session TN3270 ouverte	18177	TN3270 est un programme d'émulation de terminal qui est utilisé pour se connecter à un terminal IBM 3270. Cette catégorie indique qu'une session TN3270 a été établie.	1
Session TN3270 fermée	18178	Indique qu'une session TN3270 a été fermée.	1
Session TN3270 réinitialisée	18179	Indique qu'une session TN3270 a été réinitialisée.	3
Session TN3270 terminée	18180	Indique qu'une session TN3270 a été arrêtée.	3
Session TN3270 refusée	18181	Indique qu'une session TN3270 a été refusée.	3
Session TN3270 en cours	18182	Indique qu'une session TN3270 est en cours.	1
Session TFTP ouverte	18183	Indique qu'une session TFTP a été établie.	1
Session TFTP fermée	18184	Indique qu'une session TFTP a été fermée.	1
Session TFTP réinitialisée	18185	Indique qu'une session TFTP a été réinitialisée.	3
Session TFTP terminée	18186	Indique qu'une session TFTP a été arrêtée.	3
Session TFTP refusée	18187	Indique qu'une session TFTP a été refusée.	3
Session TFTP en cours	18188	Indique qu'une session TFTP est en cours.	1
Session Telnet ouverte	18189	Indique qu'une session Telnet a été établie.	1
Session Telnet fermée	18190	Indique qu'une session Telnet a été fermée.	1



Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session Telnet réinitialisée	18191	Indique qu'une session Telnet a été réinitialisée.	3
Session Telnet terminée	18192	Indique qu'une session Telnet a été arrêtée.	3
Session Telnet refusée	18193	Indique qu'une session Telnet a été refusée.	3
Session Telnet en cours	18194	Indique qu'une session Telnet est en cours.	1
Session Syslog ouverte	18201	Indique qu'une session syslog a été établie.	1
Session Syslog fermée	18202	Indique qu'une session syslog a été fermée.	1
Session Syslog refusée	18203	Indique qu'une session syslog a été refusée.	3
Session Syslog en cours	18204	Indique qu'une session syslog est en cours.	1
Session SSL ouverte	18205	Indique qu'une session SSL (Secure Socket Layer) a été établie.	1
Session SSL fermée	18206	Indique qu'une session SSL a été fermée.	1
Session SSL réinitialisée	18207	Indique qu'une session SSL a été réinitialisée.	3
Session SSL terminée	18208	Indique qu'une session SSL a été arrêtée.	3
Session SSL refusée	18209	Indique qu'une session SSL a été refusée.	3
Session SSL en cours	18210	Indique qu'une session SSL est en cours.	1
Session SNMP ouverte	18211	Indique qu'une session SNMP (Simple Network Management Protocol) a été établie.	1
Session SNMP fermée	18212	Indique qu'une session SNMP a été fermée.	1
Session SNMP refusée	18213	Indique qu'une session SNMP a été refusée.	3
Session SNMP en cours	18214	Indique qu'une session SNMP est en cours.	1
Session SMB ouverte	18215	Indique qu'une session SMB (Server Message Block) a été établie.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session SMB fermée	18216	Indique qu'une session SMB a été fermée.	1
Session SMB réinitialisée	18217	Indique qu'une session SMB a été réinitialisée.	3
Session SMB terminée	18218	Indique qu'une session SMB a été arrêtée.	3
Session SMB refusée	18219	Indique qu'une session SMB a été refusée.	3
Session SMB en cours	18220	Indique qu'une session SMB est en cours.	1
Session de contenu multimédia en temps réel ouverte	18221	Indique qu'une session Streaming Media a été établie.	1
Session de contenu multimédia fermée	18222	Indique qu'une session Streaming Media a été fermée.	1
Session de contenu multimédia réinitialisée	18223	Indique qu'une session Streaming Media a été réinitialisée.	3
Session de contenu multimédia terminée	18224	Indique qu'une session Streaming Media a été arrêtée.	3
Session de contenu multimédia refusée	18225	Indique qu'une session Streaming Media a été refusée.	3
Session de contenu multimédia en cours	18226	Indique qu'une session Streaming Media est en cours.	1
Session RUSERS ouverte	18227	Indique qu'une session (Remote Users) RUSERS a été établie.	1
Session RUSERS fermée	18228	Indique qu'une session RUSERS a été fermée.	1
Session RUSERS refusée	18229	Indique qu'une session RUSERS a été refusée.	3
Session RUSERS en cours	18230	Indique qu'une session RUSERS est en cours.	1
Session RSH ouverte	18231	Indique qu'une session de shell distant (rsh) a été établie.	1
Session RSH fermée	18232	Indique qu'une session rsh a été fermée.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session RSH réinitialisée	18233	Indique qu'une session rsh a été réinitialisée.	3
Session RSH terminée	18234	Indique qu'une session rsh a été arrêtée.	3
Session RSH refusée	18235	Indique qu'une session rsh a été refusée.	3
Session RSH en cours	18236	Indique qu'une session rsh est en cours.	1
Session RLOGIN ouverte	18237	Indique qu'une session de connexion à distance (RLOGIN) a été établie.	1
Session RLOGIN fermée	18238	Indique qu'une session RLOGIN a été fermée.	1
Session RLOGIN réinitialisée	18239	Indique qu'une session RLOGIN a été réinitialisée.	3
Session RLOGIN terminée	18240	Indique qu'une session RLOGIN a été arrêtée.	3
Session RLOGIN refusée	18241	Indique qu'une session RLOGIN a été refusée.	3
Session RLOGIN en cours	18242	Indique qu'une session RLOGIN est en cours.	1
Session REXEC ouverte	18243	Indique qu'une session REXEC (Remote Execution) a été établie.	1
Session REXEC fermée	18244	Indique qu'une session REXEC a été fermée.	1
Session REXEC réinitialisée	18245	Indique qu'une session REXEC a été réinitialisée.	3
Session REXEC terminée	18246	Indique qu'une session REXEC a été arrêtée.	3
Session REXEC refusée	18247	Indique qu'une session REXEC a été refusée.	3
Session REXEC en cours	18248	Indique qu'une session REXEC est en cours.	1
Session RPC ouverte	18249	Indique qu'une session d'appel de procédure éloignée (RPC) a été établie.	1
Session RPC fermée	18250	Indique qu'une session RPC a été fermée.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session RPC réinitialisée	18251	Indique qu'une session RPC a été réinitialisée.	3
Session RPC terminée	18252	Indique qu'une session RPC a été arrêtée.	3
Session RPC refusée	18253	Indique qu'une session RPC a été refusée.	3
Session RPC en cours	18254	Indique qu'une session RPC est en cours.	1
Session NTP ouverte	18255	Indique qu'une session NTP (Network Time Protocol) a été établie.	1
Session NTP fermée	18256	Indique qu'une session NTP a été fermée.	1
Session NTP réinitialisée	18257	Indique qu'une session NTP a été réinitialisée.	3
Session NTP terminée	18258	Indique qu'une session NTP a été arrêtée.	3
Session NTP refusée	18259	Indique qu'une session NTP a été refusée.	3
Session NTP en cours	18260	Indique qu'une session NTP est en cours.	1
Session NNTP ouverte	18261	Indique qu'une session Network News Transfer Protocol (NNTP) a été établie.	1
Session NNTP fermée	18262	Indique qu'une session NNTP a été fermée.	1
Session NNTP réinitialisée	18263	Indique qu'une session NNTP a été réinitialisée.	3
Session NNTP terminée	18264	Indique qu'une session NNTP a été arrêtée.	3
Session NNTP refusée	18265	Indique qu'une session NNTP a été refusée.	3
Session NNTP en cours	18266	Indique qu'une session NNTP est en cours.	1
Session NFS ouverte	18267	Indique qu'une session NFS (Network File System) a été établie.	1
Session NFS fermée	18268	Indique qu'une session NFS a été fermée.	1
Session NFS réinitialisée	18269	Indique qu'une session NFS a été réinitialisée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session NFS terminée	18270	Indique qu'une session NFS a été arrêtée.	3
Session NFS refusée	18271	Indique qu'une session NFS a été refusée.	3
Session NFS en cours	18272	Indique qu'une session NFS est en cours.	1
Session NCP ouverte	18273	Indique qu'une session de programme de contrôle de réseau (NCP) a été établie.	1
Session NCP fermée	18274	Indique qu'une session NCP a été fermée.	1
Session NCP réinitialisée	18275	Indique qu'une session NCP a été réinitialisée.	3
Session NCP terminée	18276	Indique qu'une session NCP a été arrêtée.	3
Session NCP refusée	18277	Indique qu'une session NCP a été refusée.	3
Session NCP en cours	18278	Indique qu'une session NCP est en cours.	1
Session NetBIOS ouverte	18279	Indique qu'une session NetBIOS a été établie.	1
Session NetBIOS fermée	18280	Indique qu'une session NetBIOS a été fermée.	1
Session NetBIOS réinitialisée	18281	Indique qu'une session NetBIOS a été réinitialisée.	3
Session NetBIOS terminée	18282	Indique qu'une session NetBIOS a été arrêtée.	3
Session NetBIOS refusée	18283	Indique qu'une session NetBIOS a été refusée.	3
Session NetBIOS en cours	18284	Indique qu'une session NetBIOS est en cours.	1
Session MODBUS ouverte	18285	Indique qu'une session MODBUS a été établie.	1
Session MODBUS fermée	18286	Indique qu'une session MODBUS a été fermée.	1
Session MODBUS réinitialisée	18287	Indique qu'une session MODBUS a été réinitialisée.	3
Session MODBUS terminée	18288	Indique qu'une session MODBUS a été arrêtée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session MODBUS refusée	18289	Indique qu'une session MODBUS a été refusée.	3
Session MODBUS en cours	18290	Indique qu'une session MODBUS est en cours.	1
Session LPD ouverte	18291	Indique qu'une session LPD (Line Printer Daemon) a été établie.	1
Session LPD fermée	18292	Indique qu'une session LPD a été fermée.	1
Session LPD réinitialisée	18293	Indique qu'une session LPD a été réinitialisée.	3
Session LPD terminée	18294	Indique qu'une session LPD a été arrêtée.	3
Session LPD refusée	18295	Indique qu'une session LPD a été refusée.	3
Session LPD en cours	18296	Indique qu'une session LPD est en cours.	1
Session Lotus Notes ouverte	18297	Indique qu'une session Lotus Notes a été établie.	1
Session Lotus Notes fermée	18298	Indique qu'une session Lotus Notes a été fermée.	1
Session Lotus Notes réinitialisée	18299	Indique qu'une session Lotus Notes a été réinitialisée.	3
Session Lotus Notes terminée	18300	Indique qu'une session Lotus Notes a été arrêtée.	3
Session Lotus Notes refusée	18301	Indique qu'une session Lotus Notes a été refusée.	3
Session Lotus Notes en cours	18302	Indique qu'une session Lotus Notes est en cours.	1
Session Kerberos ouverte	18303	Indique qu'une session Kerberos a été établie.	1
Session Kerberos fermée	18304	Indique qu'une session Kerberos a été fermée.	1
Session Kerberos réinitialisée	18305	Indique qu'une session Kerberos a été réinitialisée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session Kerberos terminée	18306	Indique qu'une session Kerberos a été arrêtée.	3
Session Kerberos refusée	18307	Indique qu'une session Kerberos a été refusée.	3
Session Kerberos en cours	18308	Indique qu'une session Kerberos est en cours.	1
Session IRC ouverte	18309	Indique qu'une session Internet Relay Chat (IRC) a été établie.	1
Session IRC fermée	18310	Indique qu'une session IRC a été fermée.	1
Session IRC réinitialisée	18311	Indique qu'une session IRC a été réinitialisée.	3
Session IRC terminée	18312	Indique qu'une session IRC a été arrêtée.	3
Session IRC refusée	18313	Indique qu'une session IRC a été refusée.	3
Session IRC en cours	18314	Indique qu'une session IRC est en cours.	1
Session IEC 104 ouverte	18315	Indique qu'une session IEC 104 a été établie.	1
Session IEC 104 fermée	18316	Indique qu'une session IEC 104 a été fermée.	1
Session IEC 104 réinitialisée	18317	Indique qu'une session IEC 104 a été réinitialisée.	3
Session IEC 104 terminée	18318	Indique qu'une session IEC 104 a été arrêtée.	3
Session IEC 104 refusée	18319	Indique qu'une session IEC 104 a été refusée.	3
Session IEC 104 en cours	18320	Indique qu'une session IEC 104 est en cours.	1
Session Ident ouverte	18321	Indique qu'une session TCP Client Identity Protocol (Ident) a été établie.	1
Session Ident fermée	18322	Indique qu'une session Ident a été fermée.	1
Session Ident réinitialisée	18323	Indique qu'une session Ident a été réinitialisée.	3
Session Ident terminée	18324	Indique qu'une session Ident a été arrêtée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session Ident refusée	18325	Indique qu'une session Ident a été refusée.	3
Session Ident en cours	18326	Indique qu'une session Ident est en cours.	1
Session ICCP ouverte	18327	Indique qu'une session ICCP (Inter-Control Center Communications Protocol) a été établie.	1
Session ICCP fermée	18328	Indique qu'une session ICCP a été fermée.	1
Session ICCP réinitialisée	18329	Indique qu'une session ICCP a été réinitialisée.	3
Session ICCP terminée	18330	Indique qu'une session ICCP a été arrêtée.	3
Session ICCP refusée	18331	Indique qu'une session ICCP a été refusée.	3
Session ICCP en cours	18332	Indique qu'une session ICCP est en cours.	1
Session GroupWise ouverte	18333	Indique qu'une session GroupWise a été établie.	1
Session GroupWise fermée	18334	Indique qu'une session GroupWise a été fermée.	1
Session GroupWise réinitialisée	18335	Indique qu'une session GroupWise a été réinitialisée.	3
Session GroupWise terminée	18336	Indique qu'une session GroupWise a été arrêtée.	3
Session GroupWise refusée	18337	Indique qu'une session GroupWise a été refusée.	3
Session GroupWise en cours	18338	Indique qu'une session GroupWise est en cours.	1
Session Gopher ouverte	183398	Indique qu'une session Gopher a été établie.	1
Session Gopher fermée	18340	Indique qu'une session Gopher a été fermée.	1
Session Gopher réinitialisée	18341	Indique qu'une session Gopher a été réinitialisée.	3
Session Gopher terminée	18342	Indique qu'une session Gopher a été arrêtée.	3



Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session Gopher refusée	18343	Indique qu'une session Gopher a été refusée.	3
Session Gopher en cours	18344	Indique qu'une session Gopher est en cours.	1
Session GIOP ouverte	18345	Indique qu'une session GIOP (General Inter-ORB Protocol) a été établie.	1
Session GIOP fermée	18346	Indique qu'une session GIOP a été fermée.	1
Session GIOP réinitialisée	18347	Indique qu'une session GIOP a été réinitialisée.	3
Session GIOP terminée	18348	Indique qu'une session GIOP a été arrêtée.	3
Session GIOP refusée	18349	Indique qu'une session GIOP a été refusée.	3
Session GIOP en cours	18350	Indique qu'une session GIOP est en cours.	1
Session Finger ouverte	18351	Indique qu'une session Finger a été établie.	1
Session Finger fermée	18352	Indique qu'une session Finger a été fermée.	1
Session Finger réinitialisée	18353	Indique qu'une session Finger a été réinitialisée.	3
Session Finger terminée	18354	Indique qu'une session Finger a été arrêtée.	3
Session Finger refusée	18355	Indique qu'une session Finger a été refusée.	3
Session Finger en cours	18356	Indique qu'une session Finger est en cours.	1
Session Echo ouverte	18357	Indique qu'une session Echo a été établie.	1
Session Echo fermée	18358	Indique qu'une session Echo a été fermée.	1
Session Echo refusée	18359	Indique qu'une session Echo a été refusée.	3
Session Echo en cours	18360	Indique qu'une session Echo est en cours.	1
Session .NET distante ouverte	18361	Indique qu'une session .NET distante a été établie.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session .NET distante fermée	18362	Indique qu'une session .NET distante a été fermée.	1
Session .NET distante réinitialisée	18363	Indique qu'une session .NET distante a été réinitialisée.	3
Session .NET distante terminée	18364	Indique qu'une session .NET distante a été arrêtée.	3
Session .NET distante refusée	18365	Indique qu'une session .NET distante a été refusée.	3
Session .NET distante en cours	18366	Indique qu'une session .NET distante est en cours.	1
Session DNP3 ouverte	18367	Indique qu'une sessionDNP3(Distribute d Network Proctologic) a été établie.	1
Session DNP3 fermée	18368	Indique qu'une session DNP3 a été fermée.	1
Session DNP3 réinitialisée	18369	Indique qu'une session DNP3 a été réinitialisée.	3
Session DNP3 terminée	18370	Indique qu'une session DNP3 a été arrêtée.	3
Session DNP3 refusée	18371	Indique qu'une session DNP3 a été refusée.	3
Session DNP3 en cours	18372	Indique qu'une session DNP3 est en cours.	1
Session Discard ouverte	18373	Indique qu'une session Discard a été établie.	1
Session Discard fermée	18374	Indique qu'une session Discard a été fermée.	1
Session Discard réinitialisée	18375	Indique qu'une session Discard a été réinitialisée.	3
Session Discard terminée	18376	Indique qu'une session Discard a été arrêtée.	3
Session Discard refusée	18377	Indique qu'une session Discard a été refusée.	3
Session Discard en cours	18378	Indique qu'une session Discard est en cours.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session DHCP ouverte	18379	Indique qu'une session DHCP (Dynamic Host Configuration Protocol) a été établie.	1
Session DHCP fermée	18380	Indique qu'une session DHCP a été fermée.	1
Session DHCP refusée	18381	Indique qu'une session DHCP a été refusée.	3
Session DHCP en cours	18382	Indique qu'une session DHCP est en cours.	1
Réussite DHCP	18383	Indique qu'un bail DHCP a été obtenu	1
Echec DHCP	18384	Indique qu'un bail DHCP ne peut pas être obtenu.	3
Session CVS ouverte	18385	Indique qu'une session CVS (Concurrent Versions System) a été établie.	1
Session CVS fermée	18386	Indique qu'une session CVS a été fermée.	1
Session CVS réinitialisée	18387	Indique qu'une session CVS a été réinitialisée.	3
Session CVS terminée	18388	Indique qu'une session CVS a été arrêtée.	3
Session CVS refusée	18389	Indique qu'une session CVS a été refusée.	3
Session CVS en cours	18390	Indique qu'une session CVS est en cours.	1
Session CUPS ouverte	18391	Indique qu'une session Common UNIX Printing System (CUPS) a été établie.	1
Session CUPS fermée	18392	Indique qu'une session CUPS a été fermée.	1
Session CUPS réinitialisée	18393	Indique qu'une session CUPS a été réinitialisée.	3
Session CUPS terminée	18394	Indique qu'une session CUPS a été arrêtée.	3
Session CUPS refusée	18395	Indique qu'une session CUPS a été refusée.	3
Session CUPS en cours	18396	Indique qu'une session CUPS est en cours.	1

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Session Chargen démarrée	18397	Indique qu'une session Générateur de caractères (Chargen) a été démarrée.	1
Session Chargen fermée	18398	Indique qu'une session Chargen a été fermée.	1
Session Chargen réinitialisée	18399	Indique qu'une session Chargen a été réinitialisée.	3
Session Chargen terminée	18400	Indique qu'une session Chargen a été arrêtée.	3
Session Chargen refusée	18401	Indique qu'une session Chargen a été refusée.	3
Session Chargen en cours	18402	Indique qu'une session Chargen est en cours.	1
Divers VPN	18403	Indique qu'une session VPN diverses a été détectée	1
Session DAP démarrée	18404	Indique qu'une session DAP a été établie.	1
Session DAP terminée	18405	Indique qu'une session DAP s'est terminée.	1
Session DAP refusée	18406	Indique qu'une session DAP a été refusée.	3
Etat de la session DAP	18407	Indique qu'une demande de statut de session DAP a été effectuée.	1
Session DAP en cours	18408	Indique qu'une session DAP est en cours.	1
Echec de l'authentification DAP	18409	Indique qu'une authentification DAP a échoué.	4
Réussite de l'authentification DAP	18410	Indique que l'authentification DAP a abouti.	1
Session TOR démarrée	18411	Indique qu'une session TOR a été établie.	1
Session TOR fermée	18412	Indique qu'une session TOR a été fermée.	1
Session TOR réinitialisée	18413	Indique qu'une session TOR a été réinitialisée.	3

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Session TOR terminée	18414	Indique qu'une session TOR a été arrêtée.	3
Session TOR refusée	18415	Indique qu'une session TOR a été refusée.	3
Session TOR en cours	18416	Indique qu'une session TOR est en cours.	1
Session de jeu démarrée	18417	Indique qu'une session de jeu a été démarrée.	1
Session de jeu fermée	18418	Indique qu'une session de jeu a été fermée.	1
Session de jeu réinitialisée	18419	Indique qu'une session de jeu a été réinitialisée.	3
Session de jeu terminée	18420	Indique qu'une session de jeu a été arrêtée.	3
Session de jeu fermée	18421	Indique qu'une session de jeu a été refusée.	3
Session de jeu en cours	18422	Indique qu'une session de jeu est en cours.	1
Tentative de connexion administrative	18423	Indique qu'une tentative de connexion en tant qu'utilisateur d'administration a été détectée.	2
Tentative de connexion utilisateur	18424	Indique qu'une tentative de connexion en tant qu'utilisateur non administrateur a été détectée.	2
Serveur client	18425	Indique une activité client/serveur.	1
Diffusion de contenu	18426	Indique l'activité de distribution de contenu.	1
Transfert de données	18427	Indique un transfert de données.	3
Entreposage de données	18428	Indique une activité d'entreposage de données.	3
Services d'annuaire	18429	Indique une activité de service d'annuaire.	2
Impression de fichier	18430	Indique une activité d'impression de fichier.	1
Transfert de fichier	18431	Indique le transfert de fichier.	2

Tableau 102. Catégories de bas niveau et niveaux de gravité pour la catégorie d'application (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Jeux	18432	Indique une activité de jeu.	4
Santé	18433	Indique une activité de soins de santé.	1
Système interne	18434	Indique l'activité du système interne.	1
Internet Protocol	18435	Indique l'activité Internet Protocol.	1
Existant	18436	Indique une activité existante.	1
Mail	18437	Indique une activité de messagerie.	1
Divers	18438	Indique une activité diverse.	2
Multimédia	18439	Indique une activité multimédia.	2
Gestion de réseau	18440	Indique une activité de gestion de réseau.	
P2P	18441	Indique une activité entre homologues (P2P).	4
Accès distant	18442	Indique l'activité d'accès distant.	3
Protocoles de routage	18443	Indique l'activité du protocole de routage.	1
Protocoles de sécurité	18444	Indique l'activité du protocole de sécurité.	2
Diffusion en flux	18445	Indique l'activité de diffusion en continu.	2
Protocole non commun	18446	Indique une activité de protocole peu commune.	3
VoIP	18447	Indique une activité VoIP.	1
Web	18448	Indique une activité Web.	1
ICMP	18449	Indique l'activité ICMP	1

## Audit

La catégorie d'audit contient des événements liés à l'activité d'audit, tels que le courrier électronique ou l'activité FTP.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'audit.

<i>Tableau 103. Catégories de bas niveau et niveaux de gravité pour la catégorie d'audit</i>			
<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Evénement d'audit général	19001	Indique qu'un événement d'audit général a été démarré.	1
Exécution intégrée	19002	Indique qu'une tâche d'audit intégrée a été exécutée.	1
Copie en bloc	19003	Indique qu'une copie en bloc des données a été détectée.	1
Cliché de données	19004	Indique qu'un vidage de données a été détecté.	1
Importation de données	19005	Indique qu'une importation de données a été détectée.	1
Sélection de données	19006	Indique qu'un processus de sélection de données a été détecté.	1
Troncature de données	19007	Indique que le processus de troncature des données a été détecté.	1
Mise à jour de données	19008	Indique que le processus de mise à jour des données a été détecté.	1
Exécution de procédure/déclencheur	19009	Indique que la procédure de base de données ou l'exécution du déclencheur a été détectée.	1
Modification de schéma	19010	Indique que le schéma d'une procédure ou d'une exécution de déclencheur a été modifié.	1
Tentative de création	19011	Indique que la création d'activité a été tentée.	1
La création a abouti	19012	Indique que la création de l'activité a abouti.	1
La création a échoué	19013	Indique que la création de l'activité a échoué.	3
Tentative de lecture	19014	Indique qu'une activité de lecture a été tentée.	1

Tableau 103. Catégories de bas niveau et niveaux de gravité pour la catégorie d'audit (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
La lecture a abouti	19015	Indique qu'une activité de lecture a abouti.	1
La lecture a échoué	19016	Indique que l'activité de lecture a échoué.	3
Tentative de mise à jour	19017	Indique que l'activité de mise à jour a été tentée.	1
La mise à jour a abouti	19018	Indique que l'activité de mise à jour a abouti.	1
La mise à jour a échoué	19019	Indique que l'activité de mise à jour a échoué.	3
Tentative de suppression	19020	Indique que la suppression de l'activité a été tentée.	1
La suppression a abouti	19021	Indique que la suppression de l'activité a abouti.	1
La suppression a échoué	19022	Indique que la suppression de l'activité a échoué.	3
Tentative de sauvegarde	19023	Indique que l'activité de sauvegarde a été tentée.	1
La sauvegarde a abouti	19024	Indique que l'activité de sauvegarde a abouti.	1
La sauvegarde a échoué	19025	Indique que l'activité de sauvegarde a échoué.	3
Tentative de capture	19026	Indique que l'activité de capture a été tentée.	1
La capture a abouti	19027	Indique que l'activité de capture a abouti.	1
La capture a échoué	19028	Indique que l'activité de capture a échoué.	3
Tentative de configuration	19029	Indique que l'activité de configuration a été tentée.	1
La configuration a abouti	19030	Indique que l'activité de configuration a abouti.	1
La configuration a échoué	19031	Indique que l'activité de configuration a échoué.	3
Tentative de déploiement	19032	Indique que l'activité de déploiement a été tentée.	1



Tableau 103. Catégories de bas niveau et niveaux de gravité pour la catégorie d'audit (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Le déploiement a abouti	19033	Indique que l'activité de déploiement a abouti.	1
Le déploiement a échoué	19034	Indique que l'activité de déploiement a échoué.	3
Tentative de désactivation	19035	Indique que l'activité de désactivation a été tentée.	1
La désactivation a abouti	19036	Indique que l'activité de désactivation a abouti.	1
La désactivation a échoué	19037	Indique que l'activité de désactivation a échoué.	3
Tentative d'activation	19038	Indique que l'activité d'activation a été tentée.	1
L'activation a abouti	19039	Indique que l'activité d'activation a abouti.	1
L'activation a échoué	19040	Indique que l'activation de l'activité d'activation a échoué.	3
Tentative de surveillance	19041	Indique que l'activité de surveillance a été tentée.	1
La surveillance a abouti	19042	Indique que l'activité de surveillance a abouti.	1
La surveillance a échoué	19043	Indique que l'activité de surveillance a échoué.	3
Tentative de restauration	19044	Indique que l'activité de restauration a été tentée.	1
La restauration a abouti	19045	Indique que l'activité de restauration a abouti.	1
La restauration a échoué	19046	Indique que l'activité de restauration a échoué.	3
Tentative de démarrage	19047	Indique que l'activité de démarrage a été tentée.	1
Le démarrage a abouti	19048	Indique que l'activité de démarrage a abouti.	1
Le démarrage a échoué	19049	Indique que l'activité de démarrage a échoué.	3
Tentative d'arrêt	19050	Indique que l'activité d'arrêt a été tentée.	1
L'arrêt a abouti	19051	Indique que l'activité d'arrêt a abouti	1

Tableau 103. Catégories de bas niveau et niveaux de gravité pour la catégorie d'audit (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
L'arrêt a échoué	19052	Indique que l'activité d'arrêt a échoué.	3
Tentative de non déploiement	19053	Indique que l'activité d'annulation de déploiement a été tentée.	1
Le non déploiement a abouti	19054	Indique que l'activité d'annulation de déploiement a abouti.	1
Le non déploiement a échoué	19055	Indique que l'activité d'annulation de déploiement a échoué.	3
Tentative de réception	19056	Indique que l'activité de réception a été tentée.	1
La réception a abouti	19057	Indique que l'activité de réception a abouti.	1
La réception a échoué	19058	Indique que l'activité de réception a échoué	3
Tentative d'envoi	19059	Indique que l'activité d'envoi a été tentée.	1
L'envoi a abouti	19060	Indique que l'activité d'envoi a abouti.	1
L'envoi a échoué	19061	Indique que l'activité d'envoi a échoué.	3

## Risque

La catégorie de risque contient des événements associés à IBM QRadar Risk Manager.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de risque.

Tableau 104. Catégories de bas niveau et niveaux de gravité pour la catégorie de risque

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Exposition de politique	20001	Indique qu'une exposition de règle a été détectée.	5
Violation de conformité	20002	Indique qu'une violation de conformité a été détectée.	5
Vulnérabilité exposée	20003	Indique que le réseau ou l'unité a une vulnérabilité exposée.	9

Tableau 104. Catégories de bas niveau et niveaux de gravité pour la catégorie de risque (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Vulnérabilité d'accès distant	20004	Indique que le réseau ou l'unité a une vulnérabilité d'accès à distance.	9
Vulnérabilité d'accès local	20005	Indique que le réseau ou l'unité a une vulnérabilité d'accès local.	7
Accès sans fil ouvert	20006	Indique que le réseau ou l'unité a un accès sans fil ouvert.	5
Chiffrement faible	20007	Indique que le chiffrement de l'hôte ou de l'unité est faible.	5
Transfert de données non chiffré	20008	Indique qu'un hôte ou un périphérique transmet des données non chiffrées.	3
Magasin de données non chiffré	20009	Indique que le magasin de données n'est pas chiffré.	3
Règle mal configurée	20010	Indique qu'une règle n'est pas configurée correctement.	3
Unité mal configurée	20011	Indique qu'une unité sur le réseau n'est pas configurée correctement.	3
Hôte mal configuré	20012	Indique qu'un hôte réseau n'est pas configuré correctement.	3
Perte de données possible	20013	Indique que la possibilité de perte de données a été détectée.	5
Authentification faible	20014	Indique qu'un hôte ou un périphérique est susceptible de fraude.	5
Aucun mot de passe	20015	Indique qu'aucun mot de passe n'existe.	7
Fraude	20016	Indique qu'un hôte ou un périphérique est susceptible de fraude.	7
Cible d'attaque par saturation possible	20017	Indique qu'un hôte ou un périphérique est une cible DoS possible.	3

Tableau 104. Catégories de bas niveau et niveaux de gravité pour la catégorie de risque (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Faiblesse aux attaques par saturation possible	20018	Indique qu'un hôte ou un périphérique a une faiblesse DoS possible.	3
Perte de confidentialité	20019	Indique qu'une perte de confidentialité a été détectée.	5
Cumul de score de risque du moniteur de politique d'administration	20020	Indique qu'une accumulation de score de risque du moniteur de règles a été détectée.	1

## Audit Risk Manager

La catégorie de risque contient des événements associés aux événements d'audit IBM QRadar Risk Manager.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie d'audit du gestionnaire de risques.

Tableau 105. Catégories et niveaux de gravité de niveau inférieur pour la catégorie d'audit du gestionnaire de risques

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Moniteur de politique d'administration	21001	Indique qu'un moniteur de règles a été modifié.	3
Topologie	21002	Indique qu'une topologie a été modifiée.	3
Simulations	21003	Indique qu'une simulation a été modifiée.	3
Administration	21004	Indique que des modifications administratives ont été apportées.	3

## Contrôle

La catégorie de contrôle contient des événements associés à votre système matériel.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de contrôle.

Tableau 106. Catégories de bas niveau et niveaux de gravité pour la catégorie de contrôle

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Lecture d'unité	22001	Indique qu'un périphérique a été lu.	1

Tableau 106. Catégories de bas niveau et niveaux de gravité pour la catégorie de contrôle (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Communication d'unité	22002	Indique la communication avec un périphérique.	1
Audit d'unité	22003	Indique qu'une vérification d'unité s'est produite.	1
Événement d'unité	22004	Indique qu'un événement d'unité s'est produit.	1
Ping d'unité	22005	Indique qu'une action ping a été effectuée sur un périphérique.	1
Configuration d'unité	22006	Indique qu'un périphérique a été configuré.	1
Enregistrement d'unité	22007	Indique qu'un périphérique a été enregistré.	1
Acheminement d'unité	22008	Indique qu'une action de route d'unité s'est produite.	1
Importation d'unité	22009	Indique qu'une importation de dispositif s'est produite.	1
Informations sur l'unité	22010	Indique qu'une action d'information d'unité s'est produite.	1
Avertissement sur unité	22011	Indique qu'un avertissement a été généré sur un périphérique.	1
Erreur sur unité	22012	Indique qu'une erreur a été générée sur un périphérique.	1
Événement de relais	22013	Indique un événement relais.	1
Événement NIC	22014	Indique un événement NIC (Network Interface Card).	1
Événement UIQ	22015	Indique un événement sur un périphérique mobile.	1
Événement IMU	22016	Indique un événement sur une unité de gestion intégrée (IMU).	1

Tableau 106. Catégories de bas niveau et niveaux de gravité pour la catégorie de contrôle (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Evénement de facturation	22017	Indique un événement de facturation.	1
Evénement SGBD	22018	Indique un événement sur le système de gestion de base de données (SGBD).	1
Evénement d'importation	22019	Indique qu'une importation s'est produite.	1
Importation d'emplacement	22020	Indique qu'une importation d'emplacement s'est produite.	1
Importation de route	22021	Indique qu'une importation de route s'est produite.	1
Evénement d'exportation	22022	Indique qu'une exportation s'est produite.	1
Signalisation à distance	22023	Indique la notification à distance.	1
Etat de la passerelle	22024	Indique le statut de la passerelle.	1
Evénement de travail	22025	Indique qu'un travail s'est produit.	1
Evénement de sécurité	22026	Indique qu'un événement de sécurité s'est produit.	1
Détection de violation d'unité	22027	Indique que le système a détecté une action de modification.	1
Événement temporel	22028	Indique qu'un événement de temps s'est produit.	1
Comportement suspect	22029	Indique qu'un comportement suspect s'est produit.	1
Coupure d'alimentation	22030	Indique qu'une coupure d'alimentation s'est produite.	1
Restauration de l'alimentation	22031	Indique que le courant a été restauré.	1

Tableau 106. Catégories de bas niveau et niveaux de gravité pour la catégorie de contrôle (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Signal de présence	22032	Indique qu'une commande ping a été effectuée.	1
Événement de connexion à distance	22033	Indique une connexion distante au système.	1

## Profilleur d'actif

La catégorie du profilleur d'actifs contient des événements associés à des profils d'actifs.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de profilleur d'actifs.

Tableau 107. Catégories de bas niveau et niveaux de gravité pour la catégorie de profilleur d'actifs

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Actif créé	23001	Indique qu'un actif a été créé.	1
Actif mis à jour	23002	Indique qu'un actif a été mis à jour.	1
Actif observé	23003	Indique qu'un actif a été observé.	1
Actif déplacé	23004	Indique qu'un actif a été déplacé.	1
Actif supprimé	23005	Indique qu'un actif a été supprimé.	1
Nom d'hôte d'actif nettoyé	23006	Indique qu'un nom d'hôte a été nettoyé.	1
Nom d'hôte d'actif créé	23007	Indique qu'un nom d'hôte a été créé.	1
Nom d'hôte d'actif mis à jour	23008	Indique qu'un nom d'hôte a été mis à jour.	1
Nom d'hôte d'actif observé	23009	Indique qu'un nom d'hôte a été observé.	1
Nom d'hôte d'actif déplacé	23010	Indique qu'un nom d'hôte a été déplacé.	1
Nom d'hôte d'actif supprimé	23011	Indique qu'un nom d'hôte a été supprimé.	1
Port d'actif nettoyé	23012	Indique qu'un port a été nettoyé.	1
Port d'actif créé	23013	Indique qu'un port a été créé.	1
Port d'actif mis à jour	23014	Indique qu'un port a été mis à jour.	1

Tableau 107. Catégories de bas niveau et niveaux de gravité pour la catégorie de profileur d'actifs (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Port d'actif observé	23015	Indique qu'un port a été observé.	1
Port d'actif déplacé	23016	Indique qu'un port a été déplacé.	1
Port d'actif supprimé	23017	Indique qu'un port a été supprimé.	1
Instance Vuln d'actif nettoyée	23018	Indique qu'une instance de vulnérabilité a été nettoyée.	1
Instance Vuln d'actif créée	23019	Indique qu'une instance de vulnérabilité a été créée.	1
Instance Vuln d'actif mise à jour	23020	Indique qu'une instance de vulnérabilité a été mise à jour.	1
Instance Vuln d'actif observée	23021	Indique qu'une instance de vulnérabilité a été observée.	1
Instance Vuln d'actif déplacée	23022	Indique qu'une instance de vulnérabilité a été déplacée.	1
Instance Vuln d'actif supprimée	23023	Indique qu'une instance de vulnérabilité a été supprimée.	1
Système d'exploitation d'actif nettoyé	23024	Indique qu'un système d'exploitation a été nettoyé.	1
Système d'exploitation d'actif créé	23025	Indique qu'un système d'exploitation a été créé.	1
Système d'exploitation d'actif mis à jour	23026	Indique qu'un système d'exploitation a été mis à jour.	1
Système d'exploitation d'actif observé	23027	Indique qu'un système d'exploitation a été observé.	1
Système d'exploitation d'actif déplacé	23028	Indique qu'un système d'exploitation a été déplacé.	1
Système d'exploitation d'actif supprimé	23029	Indique qu'un système d'exploitation a été supprimé.	1
Propriété d'actif nettoyée	23030	Indique qu'une propriété a été nettoyée.	1



Tableau 107. Catégories de bas niveau et niveaux de gravité pour la catégorie de profileur d'actifs (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Propriété d'actif créée	23031	Indique qu'une propriété a été créée.	1
Propriété d'actif mise à jour	23032	Indique qu'une propriété a été mise à jour.	1
Propriété d'actif observée	23033	Indique qu'une propriété a été observée.	1
Propriété d'actif déplacée	23034	Indique qu'une propriété a été déplacée.	1
Propriété d'actif supprimée	23035	Indique qu'une propriété a été déplacée.	1
Adresse IP d'actif nettoyée	23036	Indique qu'une adresse IP a été nettoyée.	1
Adresse IP d'actif créée	23037	Indique qu'une adresse IP a été créée.	1
Adresse IP d'actif mise à jour	23038	Indique qu'une adresse IP a été mise à jour.	1
Adresse IP d'actif observée	23039	Indique qu'une adresse IP a été observée.	1
Adresse IP d'actif déplacée	23040	Indique qu'une adresse IP a été déplacée.	1
Adresse IP d'actif supprimée	23041	Indique qu'une adresse IP a été supprimée.	1
Interface d'actif nettoyée	23042	Indique qu'une interface a été nettoyée.	1
Interface d'actif créée	23043	Indique qu'une interface a été créée.	1
Interface d'actif mise à jour	23044	Indique qu'une interface a été mise à jour.	1
Interface d'actif observée	23045	Indique qu'une interface a été observée.	1
Interface d'actif déplacée	23046	Indique qu'une interface a été déplacée.	1
Interface d'actif fusionnée	23047	Indique qu'une interface a été fusionnée.	1
Interface d'actif supprimée	23048	Indique qu'une interface a été supprimée.	1
Utilisateur d'actif nettoyé	23049	Indique qu'un utilisateur a été nettoyé.	1

Tableau 107. Catégories de bas niveau et niveaux de gravité pour la catégorie de profileur d'actifs (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Utilisateur d'actif observé	23050	Indique qu'un utilisateur a été observé.	1
Utilisateur d'actif déplacé	23051	Indique qu'un utilisateur a été déplacé.	1
Utilisateur d'actif supprimé	23052	Indique qu'un utilisateur a été supprimé.	1
Politique analysée d'actif nettoyée	23053	Indique qu'une règle scannée a été nettoyée.	1
Politique analysée d'actif observée	23054	Indique qu'une règle scannée a été observée.	1
Politique analysée d'actif déplacée	23055	Indique qu'une règle scannée a été déplacée.	1
Politique analysée d'actif supprimée	23056	Indique qu'une règle scannée a été supprimée.	1
Application Windows d'actif nettoyée	23057	Indique qu'une application Windows a été nettoyée.	1
Application d'actifs Windows observée	23058	Indique qu'une application Windows a été observée.	1
Application Windows d'actif déplacée	23059	Indique qu'une application Windows a été déplacée.	1
Application Windows d'actif supprimée	23060	Indique qu'une application Windows a été supprimée.	1
Service analysé d'actif nettoyé	23061	Indique qu'un service analysé a été nettoyé.	1
Service analysé d'actif observé	23062	Indique qu'un service analysé a été observé.	1
Service analysé d'actif déplacé	23063	Indique qu'un service analysé a été déplacé.	1
Service analysé d'actif supprimé	23064	Indique qu'un service analysé a été supprimé.	1
Correctif Windows de l'actif nettoyé	23065	Indique qu'un correctif Windows a été nettoyé.	1
Correctif Windows d'actif observé	23066	Indique qu'un correctif Windows a été observé.	1
Correctif Windows de l'actif déplacé	23067	Indique qu'un correctif Windows a été déplacé.	1

Tableau 107. Catégories de bas niveau et niveaux de gravité pour la catégorie de profileur d'actifs (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Correctif Windows de l'actif supprimé	23068	Indique qu'un correctif Windows a été supprimé.	1
Correctif UNIX de l'actif nettoyé	23069	Indique qu'un correctif UNIX a été nettoyé.	1
Correctif UNIX d'actif observé	23070	Indique qu'un correctif UNIX a été observé.	1
Correctif UNIX de l'actif déplacé	23071	Indique qu'un correctif UNIX a été déplacé.	1
Correctif UNIX de l'actif supprimé	23072	Indique qu'un correctif UNIX a été supprimé.	1
Analyse de correctif d'actif nettoyée	23073	Indique qu'une analyse de correctif a été nettoyée.	1
Analyse de correctif d'actif créée	23074	Indique qu'un scannage de correctifs a été créé.	1
Analyse de correctif d'actif déplacée	23075	Indique qu'un scannage de correctifs a été déplacé.	1
Analyse de correctif d'actif supprimée	23076	Indique qu'un scannage de correctifs a été supprimé.	1
Analyse de port d'actif nettoyée	23077	Indique qu'une analyse de port a été nettoyée.	1
Analyse de port d'actif créée	23078	Indique qu'une analyse de port a été nettoyée.	1
Analyse de port d'actif déplacée	23079	Indique qu'un scannage de correctifs a été déplacé.	1
Analyse de port d'actif supprimée	23080	Indique qu'un scannage de correctifs a été supprimé.	1
Application client d'actif nettoyée	23081	Indique qu'une application client a été nettoyée.	1
Application client d'actif observée	23082	Indique qu'une application client a été observée.	1
Application client d'actif déplacée	23083	Indique qu'une application client a été déplacée.	1

Tableau 107. Catégories de bas niveau et niveaux de gravité pour la catégorie de profileur d'actifs (suite)

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Application client d'actif supprimée	23084	Indique qu'une application client a été supprimée.	1
Analyse de correctif d'actif observée	23085	Indique qu'une analyse de correctif a été observée.	1
Analyse de port d'actif observée	23086	Indique qu'une analyse de port a été observée.	1
Groupe NetBIOS créé	23087	Indique qu'un groupe NetBIOS a été créé.	1
Groupe NetBIOS mis à jour	23088	Indique qu'un groupe NetBIOS a été mis à jour.	1
Groupe NetBIOS observé	23089	Indique qu'un groupe NetBIOS a été observé.	1
Groupe NetBIOS supprimé	23090	Indique qu'un groupe NetBIOS a été supprimé.	1
Groupe NetBIOS nettoyé	23091	Indique qu'un groupe NetBIOS a été nettoyé.	1
Groupe NetBIOS transféré	23092	Indique qu'un groupe NetBIOS a été déplacé.	1

## Sense

La catégorie d'analyse contient des événements associés à l'analyse de comportement de l'utilisateur logique.

Le tableau suivant décrit les catégories d'événements de bas niveau et les niveaux de gravité associés pour la catégorie de détection.

Tableau 108.

Catégorie d'événement de bas niveau	ID de catégorie	Description	Niveau de gravité (0 à 10)
Comportement utilisateur	24001	Indique le comportement de l'utilisateur.	5
Zone géographique de l'utilisateur	24002	Indique la géographie de l'utilisateur.	5
Temps utilisateur	24003	Indique l'heure de l'utilisateur.	5
Accès utilisateur	24004	Indique l'accès de l'utilisateur.	5
Privilège utilisateur	24005	Indique le privilège de l'utilisateur.	5

Tableau 108. (suite)

<b>Catégorie d'événement de bas niveau</b>	<b>ID de catégorie</b>	<b>Description</b>	<b>Niveau de gravité (0 à 10)</b>
Risque utilisateur	24006	Indique le risque de l'utilisateur.	5
Infraction Sense	24007	Indique qu'une violation de sens s'est produite.	5
Risque sur la ressource	24008	Indique les ressources en péril.	5



---

# Chapitre 26. Ports et serveurs courants utilisés par QRadar

IBM QRadar requiert que certains ports soient prêts à recevoir des informations des composants QRadar et de l'infrastructure externe. Pour garantir que QRadar utilise les informations de sécurité les plus récentes, il requiert également un accès aux serveurs publics et aux flux RSS.

## Communication SSH sur le port 22

Tous les ports utilisés par la console QRadar pour communiquer avec les hôtes gérés peuvent être tunnelisés, par chiffrement, via le port 22 sur SSH.

Pour communiquer de manière sécurisée, la console se connecte aux hôtes gérés en utilisant une session SSH chiffrée. Les sessions SSH sont démarrées depuis la console afin de fournir les données à l'hôte géré. Par exemple, QRadar Console peut démarrer plusieurs sessions SSH sur les dispositifs du processeur d'événements pour une communication sécurisée. Cette communication peut inclure les ports tunnelisés sur SSH, comme des données HTTPS pour le port 443 et des données de requête Ariel pour le port 32006. IBM QRadar QFlow Collector utilisant un chiffrement peut initier des sessions SSH sur les dispositifs Flow Processor qui ont besoin de données.

## Ports ouverts non requis par QRadar

Vous pouvez trouver des ports ouverts supplémentaires dans les situations suivantes :

- Lorsque vous installez QRadar sur votre propre matériel, vous pouvez rencontrer des ports ouverts qui sont utilisés par des services, des démons, et des programmes inclus dans Red Hat Enterprise Linux.
- Lorsque vous montez ou exportez un partage de fichiers réseau, vous pouvez voir des ports affectés dynamiquement pour les services RPC, tels que `rpc.mountd` et `rpc.rquotad`.

### Concepts associés

[Fonctions de votre produit IBM QRadar](#)

---

## Utilisation du port QRadar

Examinez la liste des ports usuels utilisés par les services et les composants IBM QRadar pour communiquer au sein du réseau. Vous pouvez utiliser cette liste pour déterminer quels ports doivent être ouverts dans votre réseau. Vous pouvez, par exemple, déterminer quel port doit être ouvert pour que QRadar Console communique avec des processeurs d'événements distants.

## Interrogation WinCollect à distance

Les agents WinCollect qui interrogent à distances d'autres systèmes d'exploitation Microsoft Windows peuvent nécessiter des affectations de ports supplémentaires.

Pour plus d'informations, reportez-vous au manuel IBM QRadar WinCollect - *Guide d'utilisation*.

## Ports d'écoute QRadar

Le tableau suivant présente les ports QRadar qui sont ouverts dans un état LISTEN . Les ports LISTEN ne sont valides que lorsque iptables est activé sur votre système. Sauf mention contraire, les informations sur le numéro de port affecté s'appliquent à tous les produits QRadar.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar

Port	Description	Protocole	Direction	Configuration requise
22	SSH	TCP	Trafic bidirectionnel entre QRadar Console et tous les autres composants.	Accès de gestion à distance. Ajout d'un système distant en tant qu'hôte géré. Protocoles de source de journal pour extraction de fichiers depuis des périphériques externes, par exemple le protocole de fichier journal. Utilisateurs recourant à l'interface de ligne de commande pour communiquer avec la console depuis leur ordinateur de bureau. Haute disponibilité (HA).
25	SMTP	TCP	De tous les hôtes gérés à la passerelle SMTP.	Courriers électronique depuis QRadar vers une passerelle SMTP. Remise de messages d'erreur et d'avertissement à une adresse de contact électronique d'administration.
111 et port généré au hasard	Associateur de port	TCP/UDP	Hôtes gérés communiquant avec la console QRadar Console. Utilisateurs se connectant à QRadar Console.	Appels de procédure distante aux services requis, tels que NFS (Network File System).
123	Network Time Protocol (NTP)	UDP	Élément sortant provenant de la console QRadar Console et destiné au serveur NTP Élément sortant de l'hôte géré et destiné à la console QRadar Console	Synchronisation de l'heure via Chrony entre : <ul style="list-style-type: none"> <li>La console QRadar et le serveur NTP</li> <li>Les hôtes gérés QRadar et la console QRadar</li> </ul>
Port 135 et ports alloués dynamiquement au-delà du port 1024 pour les appels RPC	DCOM	TCP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements. Trafic bidirectionnel entre les composants QRadar Console ou les collecteurs d'événement IBM QRadar utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter. <b>Remarque :</b> DCOM alloue généralement une plage de ports aléatoire pour la communication. Vous pouvez configurer les produits Microsoft Windows afin d'utiliser un port spécifique. Pour plus d'informations, reportez-vous à la documentation Microsoft Windows.



Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
137	Service de noms Windows NetBIOS	UDP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.  Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
138	Service de datagramme Windows NetBIOS	UDP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.  Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
139	Service de session Windows NetBIOS	TCP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.  Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant soit Microsoft Security Event Log Protocol, soit des agents Adaptive Log Exporter, et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
162	NetSNMP	UDP	Hôtes gérés QRadar se connectant à QRadar Console.  Sources de journal externes vers QRadar Event Collectors.	Port UDP pour le démon NetSNMP à l'écoute de communications (v1, v2c et v3) depuis des sources de journal externes. Le port n'est ouvert que si l'agent SNMP est activé.
199	NetSNMP	TCP	Hôtes gérés QRadar se connectant à QRadar Console.  Sources de journal externes vers QRadar Event Collectors.	Port TCP pour le démon NetSNMP à l'écoute de communications (v1, v2c et v3) depuis des sources de journal externes. Le port n'est ouvert que si l'agent SNMP est activé.
427	Service Location Protocol (SLP)	UDP/TCP		Le module Integrated Management Module utilise le port pour rechercher des services sur un réseau local.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
443	Apache/HTTPS	TCP	Trafic bidirectionnel pour les communications sécurisées depuis tous les produits vers QRadar Console.  Trafic unidirectionnel entre l'hôte d'applications et la console QRadar Console.	Téléchargement des configurations sur les hôtes gérés depuis QRadar Console.  Hôtes gérés QRadar se connectant à QRadar Console.  Utilisateurs devant pouvoir se connecter à QRadar.  QRadar Console qui gère et fournit des mises à jour de la configuration aux agents WinCollect.  Applications pour lesquelles l'accès à l'API QRadar est requis.
445	Microsoft Directory Service	TCP	Trafic bidirectionnel entre les agents WinCollect et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.  Trafic bidirectionnel entre les composants QRadar Console ou QRadar Event Collectors utilisant Microsoft Security Event Log Protocol et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.  Trafic bidirectionnel entre les agents Adaptive Log Exporter et les systèmes d'exploitation Windows interrogés à distance quant à l'existence d'événements.	Ce trafic est généré par WinCollect, Microsoft Security Event Log Protocol ou Adaptive Log Exporter.
514	Syslog	UDP/TCP	Dispositifs réseau externes fournissant des événements syslog TCP et utilisant le trafic bidirectionnel  Dispositifs réseau externes fournissant des événements syslog UDP et utilisant le trafic unidirectionnel  Trafic syslog interne depuis les hôtes QRadar vers QRadar Console.	Sources de journal externes envoyant des données d'événement aux composants QRadar.  Le trafic Syslog inclut les agents WinCollect, les collecteurs d'événements et les agents Adaptive Log Exporter capables d'envoyer des événements UDP ou TCP à QRadar.
762	Démon de montage (mountd) Network File System (NFS)	TCP/UDP	Connexions entre QRadar Console et le serveur NFS.	Démon de montage NFS (Network File System) traitant les demandes de montage d'un système de fichiers à un emplacement spécifié.
1514	Syslog-ng	TCP/UDP	Connexion entre le composant local Collecteur d'événements et le composant local processeur d'événements au démon syslog-ng pour journalisation.	Port de journalisation interne pour syslog-ng.
2049	NFS	TCP	Connexions entre QRadar Console et le serveur NFS.	Protocole NFS (Network File System) pour partage de fichiers ou de données entre les composants.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
2055	NetFlowdonnées	UDP	De l'interface de gestion sur la source du flux (en général, un routeur) au IBM QRadar QFlow Collector.	Datagramme NetFlow à partir de composants, comme des routeurs.
2376	Port de commande Docker	TCP	Communications internes. Ce port n'est pas disponible depuis l'extérieur.	Utilisé pour gérer les ressources d'infrastructure d'application QRadar.
3389	Remote Desktop Protocol (RDP) et Ethernet sur USB sont activés	TCP/UDP		Si le système d'exploitation Microsoft Windows est configuré pour prise en charge de RDP et d'Ethernet over USB, un utilisateur peut ouvrir une session sur le serveur via le réseau de gestion. Cela signifie que le port par défaut pour RDP, le port 3389, doit être ouvert.
3900	Port de présence distante de Integrated Management Module	TCP/UDP		Utilisez ce port pour interagir avec la console QRadar par le biais de Integrated Management Module.
4333	Port de redirection	TCP		Ce port est affecté comme port de redirection pour les demandes du protocole de résolution d'adresse (ARP) dans la résolution des infractions QRadar.
5 000	Utilisé pour la communication avec le registre docker fonctionnant sur la Console. Permet à tous les hôtes gérés de tirer des images de la Console qui seront utilisées pour créer des conteneurs locaux.	TCP	Unidirectionnel de l'hôte géré QRadar vers la console QRadar Console. Port uniquement ouvert sur la Console. Les hôtes gérés doivent obligatoirement tirer de la Console.	Requis pour les applications fonctionnant sur un hôte d'applications.
5432	Postgres	TCP	Communication pour l'hôte géré utilisé pour accéder à l'instance de base de données locale.	Requis pour mettre à disposition des hôtes gérés depuis l'onglet <b>Admin</b> .
6514	Syslog	TCP	Les dispositifs réseau externes qui fournissent des événements syslog TCP chiffrés utilisent un trafic bidirectionnel.	Sources de journal externes envoyant des données d'événement chiffrées aux composants QRadar.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
7676, 7677 et quatre ports associés de façon aléatoire au-delà du port 32000.	Connexions de messagerie (IMQ)	TCP	Communications de file d'attente de message entre les composants sur un hôte géré	<p>Courtier de file d'attente de messages pour les communications entre les composants sur un hôte géré.</p> <p><b>Remarque :</b> Vous devez autoriser l'accès à ces ports depuis la console QRadar pour les hôtes non chiffrés.</p> <p>Les ports 7676 et 7677 sont des ports TCP statiques et quatre connexions supplémentaires sont créées sur des ports aléatoires.</p> <p>Pour plus d'informations sur l'identification de ports liés de manière aléatoire, voir «Affichage des associations de ports IMQ», à la page 450.</p>
5791, 7700, 7777, 7778, 7779, 7780, 7781, 7782, 7783, 7787, 7788, 7790, 7791, 7792, 7793, 7794, 7795, 7799, 8989 et 8990.	Ports du serveur JMX	TCP	Communications internes. Ces ports ne sont pas disponibles depuis l'extérieur.	<p>Serveur JMX (Java Management Beans) suivant tous les processus QRadar internes pour exposer les métriques de prise en charge.</p> <p>Ces ports sont utilisés par la prise en charge de QRadar.</p>
7789	Dispositif de bloc répliqué distribué HA	TCP/UDP	Trafic bidirectionnel entre l'hôte secondaire et l'hôte principal dans un cluster HA.	Architecture de dispositif de bloc répliqué distribué (Distributed Replicated Block Device) utilisée pour maintenir la synchronisation entre hôte primaire et hôte secondaire dans les configurations HA.
7800	Apache Tomcat	TCP	Depuis le processeur d'événements vers QRadar Console.	Diffusion en temps réel (diffusion en flux) des événements.
7801	Apache Tomcat	TCP	Depuis le processeur d'événements vers QRadar Console.	Diffusion en temps réel (diffusion en flux) des flux.
7803	Moteur de détection d'anomalies	TCP	Depuis le processeur d'événements vers QRadar Console.	Port du moteur de détection d'anomalies.
7804	Générateur QRM Arc	TCP	Communications de contrôle interne entre les processus QRadar et le générateur ARC.	Ce port est utilisé uniquement pour QRadar Risk Manager. Il n'est pas disponible en externe.
7805	Communication de tunnel syslog	TCP	Trafic bidirectionnel entre la console QRadar Console et les hôtes gérés	Élément utilisé pour les communications chiffrées entre la console et les hôtes gérés.
8000	Service de collecte d'événements (ECS)	TCP	Depuis le Collecteur d'événements vers QRadar Console.	Port d'écoute pour service de collecte d'événements (ECS) spécifique.
8001	Port du démon SNMP	TCP	Systèmes SNMP externes demandant des informations d'interception SNMP auprès de QRadar Console.	Port d'écoute pour les demandes de données SNMP externes.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
8005	Apache Tomcat	TCP	Communications internes. Non disponible en externe.	Ouvert pour contrôle de Tomcat. Ce port est lié et n'accepte des connexions que depuis l'hôte local.
8009	Apache Tomcat	TCP	Depuis le processus du démon HTTP (HTTPd) vers Tomcat.	Connecteur Tomcat lorsque la demande est utilisée et substituée par proxy au service Web
8080	Apache Tomcat	TCP	Depuis le processus du démon HTTP (HTTPd) vers Tomcat.	Connecteur Tomcat lorsque la demande est utilisée et substituée par proxy au service Web
8082	Tunnel sécurisé pour QRadar Risk Manager	TCP	Trafic bidirectionnel entre QRadar Console et QRadar Risk Manager	Requis pour lorsque le chiffrement est utilisé entre QRadar Risk Manager et QRadar Console.
8413	Agents WinCollect	TCP	Trafic bidirectionnel entre l'agent WinCollect et QRadar Console.	Ce trafic est généré par l'agent WinCollect et la communication est chiffrée. Requis pour fournir des mises à jour de la configuration à l'agent WinCollect et pour utiliser WinCollect en mode connecté.
8844	Apache Tomcat	TCP	Unidirectionnel de QRadar Console vers le dispositif qui exécute le processeur QRadar Vulnerability Manager.	Utilisé par Apache Tomcat pour lire les informations de l'hôte qui exécute le processeur QRadar Vulnerability Manager.
9000	Conman	TCP	Unidirectionnel de la console QRadar vers un hôte d'applications QRadar.	Utilisé avec un hôte d'applications. Il permet à la console de déployer des applications sur un hôte d'applications et de gérer ces dernières.
9090	Base de données et serveur XForce IP Reputation	TCP	Communications internes. Non disponible en externe.	Communications entre les processus QRadar et la base de données XForce Reputation IP.
9381	Téléchargement de fichiers de certificat	TCP	Unidirectionnel de l'hôte géré QRadar ou du réseau externe vers la console QRadar Console	Téléchargement de fichiers CRL (liste de révocation de certificat) et de certificat de l'autorité de certification QRadar pouvant être utilisés pour la validation des certificats générés QRadar.
9381	localca-server	TCP	Trafic bidirectionnel entre les composants QRadar.	Utilisé pour stocker les certificats racine et intermédiaires locaux de QRadar ainsi que les listes de révocation de certificat associées.
9393, 9394	vault-qrd	TCP	Communications internes. Non disponible en externe.	Utilisé pour stocker des secrets et permettre d'y accéder de façon sécurisée pour les services.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
9913, plus un port affecté dynamiquement	Conteneur d'application Web	TCP	Communication RMI (Remote Method Invocation) Java bidirectionnelle entre machines virtuelles Java	Lorsque l'application Web est enregistrée, un port supplémentaire est affecté dynamiquement.
9995	NetFlowdonnées	UDP	De l'interface de gestion sur la source du flux (en général, un routeur) au QRadar QFlow Collector.	Datagramme NetFlow à partir de composants, comme des routeurs.
9999	Processeur IBM QRadar Vulnerability Manager	TCP	Unidirectionnel depuis le scanner vers le dispositif exécutant le processeur QRadar Vulnerability Manager	Utilisé pour les informations de la commande QRadar Vulnerability Manager (QVM). QRadar Console se connecte à ce port sur l'hôte qui exécute le processeur QRadar Vulnerability Manager. Ce port n'est utilisé que si QVM est activé.
10000	Interface d'administration du système QRadar basée sur le Web	TCP/UDP	Systèmes des ordinateurs de bureau des utilisateurs vers tous les hôtes QRadar.	Dans QRadar version 7.2.5 et antérieure, ce port est utilisé pour les modifications sur le serveur, comme le mot de passe racine des hôtes et l'accès au pare-feu.  Le port 10000 est désactivé dans V7.2.6.
10101, 10102	Commande de signal de présence	TCP	Trafic bidirectionnel entre le noeud à haute disponibilité principal et le noeud à haute disponibilité secondaire.	Requis pour s'assurer que les noeuds HA sont toujours actifs.
12500	Elément binaire socat	TCP	Elément sortant entre l'hôte géré et la console QRadar Console	Port utilisé pour la tunnellation des demandes udp chrony via tcp lorsque la console QRadar Console ou l'hôte géré est chiffré
14433	traefik	TCP	Trafic bidirectionnel entre les composants QRadar.	Requis pour la reconnaissance des services d'application.
15432				Doit être ouvert pour les communications internes entre QRM et QRadar.
15433	Postgres	TCP	Communication pour l'hôte géré utilisé pour accéder à l'instance de base de données locale.	Utilisé pour la configuration et le stockage QRadar Vulnerability Manager (QVM). Ce port n'est utilisé que si QVM est activé.
15434				Doit être ouvert pour les communications internes entre Forensics et QRadar.
20000-23000	Tunnel SSH	TCP	Trafic bidirectionnel entre la console QRadar et tous les hôtes gérés chiffrés.	Point d'écoute local pour les tunnels SSH utilisés pour la communication JMS (Java Message Service) avec les hôtes gérés chiffrés. Utilisé pour exécuter des tâches asynchrones de longue durée, telles que la mise à jour de configuration réseau via le système et la gestion des licences.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
23111	Serveur Web SOAP	TCP		Port SOAP du serveur Web pour le service de collecte d'événements (ECS).
23333	Emulex Fibre Channel	TCP	Systèmes des ordinateurs de bureau des utilisateurs se connectant aux dispositifs QRadar via une carte Fibre Channel.	Service elxmgmt (Emulex Fibre Channel HBAAnywhere Remote Management).
26000	traefik	TCP	Trafic bidirectionnel entre les composants QRadar.	Utilisé avec un hôte d'application chiffré. Requis pour la reconnaissance des services d'application.
26001	Conman	TCP	Unidirectionnel de la console QRadar Console vers un hôte d'applications QRadar.	Utilisé avec un hôte d'application chiffré. Il permet à la console de déployer des applications sur un hôte d'applications et de gérer ces dernières.
32000	Transfert du flux normalisé	TCP	Trafic bidirectionnel entre les composants QRadar.	Données de flux normalisé communiquées à partir d'une source hors site ou entre des QRadar QFlow Collector.
32004	Transfert d'événements normalisés	TCP	Trafic bidirectionnel entre les composants QRadar.	Données d'événement normalisées communiquées à partir d'une source hors site ou entre des QRadar Event Collectors
32005	Flux de données	TCP	Trafic bidirectionnel entre les composants QRadar.	Port de communication du flux de données entre QRadar Event Collectors sur des hôtes gérés distincts.
32006	Requêtes Ariel	TCP	Trafic bidirectionnel entre les composants QRadar.	Port de communication entre le serveur proxy Ariel et le serveur de requêtes Ariel.
32007	Données en infraction	TCP	Trafic bidirectionnel entre les composants QRadar.	Événements et flux impliqués dans une infraction ou dans une corrélation globale.
32009	Données d'identité	TCP	Trafic bidirectionnel entre les composants QRadar.	Données d'identité communiquées entre le service d'informations de vulnérabilité passif (VIS) et le service de collecte d'événements (ECS)
32010	Port source d'écoute du flux	TCP	Trafic bidirectionnel entre les composants QRadar.	Port d'écoute du flux pour collecte de données à partir des QRadar QFlow Collector
32011	Port d'écoute Ariel	TCP	Trafic bidirectionnel entre les composants QRadar.	Port d'écoute Ariel pour les recherches dans la base de données, les informations de progression et les autres commandes associées.
32000-33999	Flux de données (flux, événements, contexte du flux)	TCP	Trafic bidirectionnel entre les composants QRadar.	Flux de données, tels que les événements, les flux, le contexte du flux, les requêtes de recherche d'événement et le proxy Docker.

Tableau 109. Ports d'écoute utilisés par les services et composants QRadar (suite)

Port	Description	Protocole	Direction	Configuration requise
40799	Données PCAP	UDP	Depuis des dispositifs Juniper Networks SRX Series vers QRadar.	Collecte de données de capture de paquets entrants (PCAP) à partir de dispositif Juniper Networks SRX Series.  <b>Remarque :</b> La capture de paquets sur votre dispositif peut utiliser un autre port. Pour plus d'informations sur la configuration de la capture de paquets, consultez la documentation des dispositifs Juniper Networks SRX Series.
ICMP	ICMP		Trafic bidirectionnel entre l'hôte secondaire et l'hôte principal dans un cluster HA.	Test à l'aide du protocole ICMP (Internet Control Message Protocol) de la connexion réseau entre l'hôte secondaire et l'hôte principal dans un cluster HA.

## Affichage des associations de ports IMQ

Plusieurs ports utilisés par IBM QRadar allouent des numéros de port aléatoires supplémentaires. Par exemple, Message Queues (IMQ) ouvre des ports aléatoires pour la communication entre les composants sur un hôte géré. Vous pouvez afficher les affectations de port aléatoires d'IMQ en utilisant Telnet pour vous connecter à l'hôte local et en effectuant une recherche sur le numéro de port.

Les associations de port aléatoires ne sont pas des numéros de port statiques. Lorsqu'un service redémarre, les ports générés pour un service sont réalloués et un nouvel ensemble de numéros de port est affecté au service.

### Procédure

1. À l'aide de SSH, connectez-vous à QRadar Console en tant qu'utilisateur racine.
2. Pour afficher une liste des ports associés pour la connexion de messagerie IMQ, entrez la commande suivante :

```
telnet localhost 7676
```

Les résultats de la commande telnet peuvent être similaires à la sortie suivante :

```
[root@domain ~]# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
101 imqbroker 4.4 Update 1
portmapper tcp PORTMAPPER 7676
[imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=<session_id>]
cluster_discovery tcp CLUSTER_DISCOVERY 44913
jmxrmi rmi JMX 0 [url=service:jmx:rmi://domain.ibm.com/stub/<urlpath>]
admin tcp ADMIN 43691
jms tcp NORMAL 7677
cluster tcp CLUSTER 36615
```

La sortie telnet présente 3 des 4 ports TCP à valeur aléatoire élevée pour IMQ. Le quatrième port, qui n'est pas affiché, est un port RMI JMX (Remote Method Invocation) disponible via l'URL JMX présentée dans la sortie.

Si la connexion telnet est refusée, cela signifie qu'IMQ n'est pas actuellement en cours d'exécution. Il est possible que le système soit en cours de démarrage ou d'arrêt ou que les services aient été arrêtés manuellement.



## Recherche des ports utilisés par QRadar

Utilisez la commande **netstat** pour déterminer les ports utilisés sur la Console IBM QRadar ou l'hôte géré. Utilisez la commande **netstat** pour afficher tous les ports d'écoute et les ports définis sur le système.

### Procédure

1. Avec SSH, connectez-vous à QRadar Console en tant qu'utilisateur root.
2. Pour afficher toutes les connexions actives et tous les ports TCP et UDP écoutés par l'ordinateur, entrez la commande suivante :

```
netstat -nap
```

3. Pour rechercher des informations spécifiques dans la liste des ports netstat, entrez la commande suivante :

```
netstat -nap | grep port
```

### Exemples :

- Pour afficher tous les ports correspondant à 199, entrez la commande suivante :

```
netstat -nap | grep 199
```

- Pour afficher des informations sur tous les ports d'écoute, entrez la commande suivante :

```
netstat -nap | grep LISTEN
```

## Serveurs QRadar publics

Pour vous fournir les informations de sécurité les plus récentes, IBM QRadar requiert l'accès à un certain nombre de serveurs publics.

### Serveurs publics

*Tableau 110. Serveurs publics auxquels QRadar doit pouvoir accéder. Ce tableau répertorie les descriptions des adresses IP ou des noms d'hôte auxquels QRadar accède. <https://www.ibm.com/support/pages/node/6244622>*

Adresse IP ou nom d'hôte	Description
194.153.113.31	Scanner de zone démilitarisée IBM QRadar Vulnerability Manager
194.153.113.32	Scanner de zone démilitarisée QRadar Vulnerability Manager
auto-update.qradar.ibmcloud.com/	Serveurs de mise à jour automatique QRadar. Pour plus d'informations sur les serveurs de mise à jour automatique, voir QRadar: Important auto update server changes for administrators ( <a href="https://www.ibm.com/support/pages/node/6244622">https://www.ibm.com/support/pages/node/6244622</a> ).
update.xforce-security.com	Serveur de mise à jour du Flux de menaces X-Force
license.xforce-security.com	Serveur de licences du Flux de menaces X-Force

## Conteneurs de Docker et interfaces réseau

Un réseau Docker définit une zone de confiance de communication dans laquelle la communication est illimitée entre les conteneurs de ce réseau.

Chaque réseau est associé à une interface de pont sur l'hôte, et des règles de pare-feu sont définies pour filtrer le trafic entre ces interfaces. Généralement, les conteneurs d'une zone qui partagent le même réseau Docker et l'interface de pont hôte peuvent communiquer entre eux. Une exception à cette règle générale est que les applications s'exécutent sur le même réseau `dockerApps`, mais qu'elles sont isolées les unes des autres par le pare-feu.

### Interfaces Docker

Pour afficher la liste des interfaces Docker, entrez la commande suivante :

```
docker network ls
```

Voici un exemple de résultat :

```
[root@q1dk00 ~]# docker network ls
NETWORK ID   NAME      DRIVER SCOPE
943dd35a4747 appProxy  bridge local
9e2ba36111d1 dockerApps bridge local
514471d98b42 dockerInfra bridge local
```

L'interface `dockerApps` est utilisée pour appliquer des règles de communication entre les applications.

L'interface `appProxy` affiche le conteneur `nginx_framework_apps_proxy`.

L'interface `dockerInfra` est utilisée pour héberger `service_launcher` et `qoauth`. Les applications sont isolées de la plupart des composants d'infrastructure, mais elles doivent pouvoir se connecter à `service_launcher` et `qoauth` pour gérer les secrets et l'autorisation.

### Informations sur les interfaces Docker

Entrez la commande suivante pour obtenir des informations sur les interfaces Docker :

```
docker inspect <docker_container_ID> | grep NetworkMode
```

Voici un exemple de résultat :

```
"NetworkMode": "appProxy"
```

Cet exemple montre comment utiliser la commande **docker inspect <docker\_container\_ID>** et l'amener à **Moins** pour afficher plus de détails sur le réseau :

```
docker inspect d9b3e58649de | less
```

Voici un exemple de résultat :

```
"Networks": {
    "dockerApps": {
        "IPAMConfig": null,
        "Links": null,
        "Aliases": [
            "d9b3e58649de"
        ], "NetworkID":
"79bc4716da5139a89cfa5360a3b72824e67701523768822d11b53caeea5e349e",
        "EndpointID":
"9dba9d9a174b037f72333945b72cdf60c3719fdb9a3a10a14a8ee3cc0e92a856",
        "Gateway": "172.18.0.1",
        "IPAddress": "172.18.0.2",
        "IPPrefixLen": 16,
        "IPv6Gateway": "2003:db8:1::1",
        "GlobalIPv6Address": "2003:db8:1::2",
        "GlobalIPv6PrefixLen": 64,
        "MacAddress": "02:42:ac:12:00:02"
    }
}
```

La sortie de cet exemple montre la configuration du réseau utilisé par le conteneur spécifié (`d9b3e58649de`), et affiche le nom de l'interface réseau Docker (`dockerApps`) et l'adresse IP du réseau affecté au conteneur Docker.





## Chapitre 27. API RESTful

L'interface de programme d'application (API) REST (Representational State Transfer) permet d'intégrer IBM QRadar à d'autres solutions. Vous pouvez effectuer des actions sur QRadar Console en envoyant des demandes HTTPS à des noeuds finaux spécifiques (URL) de QRadar Console.

Chaque noeud final contient l'URL de la ressource à atteindre et l'action à y réaliser. L'action est indiquée par la méthode HTTP de la demande : GET, POST, PUT ou DELETE. Pour plus d'informations sur les paramètres et les réponses de chaque noeud final, voir le [Guide QRadar API](#).

### Forum d'API et exemples de code QRadar

Le forum d'API fournit des informations supplémentaires sur l'API REST, ainsi que des réponses aux questions fréquentes et des exemples de codes annotés que vous pouvez utiliser dans un environnement test. Pour plus d'informations, voir le [forum sur les API](https://ibm.biz/qradarforums) (https://ibm.biz/qradarforums).

## Accès à la page de documentation interactive de l'API

La page de documentation de l'API interactive permet d'accéder aux détails techniques des API RESTful et d'essayer de faire des demandes d'API à votre serveur.

### Pourquoi et quand exécuter cette tâche

L'interface utilisateur de la documentation de l'API fournit des descriptions et la possibilité d'utiliser les interfaces API REST suivantes :

Tableau 111. Interfaces d'API REST

API REST	Description
/api/analytics	Créer, mettre à jour et supprimer des actions personnalisées pour les règles.
/api/ariel	Afficher les propriétés d'événement et de flux, créer des recherches d'événements et de flux et gérer les recherches.
/api/asset_model	Renvoie une liste de tous les actifs du modèle. Vous pouvez également afficher une liste de toutes les recherches sauvegardées et de tous les types de propriétés d'actifs disponibles et mettre à jour un actif.
/api/auth	Déconnecte et invalide la session en cours.
/api/config	Afficher et gérer les locataires, les domaines et les extensions QRadar.
/api/data_classification	Affichez toutes les catégories de niveau élevé et faible, les enregistrements d'identificateur QRadar (QID) et les mappages d'événements. Vous pouvez également créer ou modifier des enregistrements et des mappages QID.
/api/forensics	Gérer les récupérations et les cas de capture.
/api/gui_app_framework	Installer et gérer les applications créées à l'aide de l'interface graphique Application Framework Software Development Kit.

Tableau 111. Interfaces d'API REST (suite)

API REST	Description
/api/help	Renvoie une liste des fonctions de l'API.
/api/qrm	Gérer les groupes de recherche sauvegardés, les groupes de questions, les groupes de simulation, les groupes de recherche de topologie enregistrés et les groupes de modèles.
/api/qvm	Extrait les actifs, les vulnérabilités, les réseaux, les services ouverts et les filtres. Vous pouvez également créer ou mettre à jour des tickets de rattrapage.
/api/reference_data	Affiche et gère les collectes de données de référence.
/api/scanner	Affiche, crée ou démarre une analyse distante associée à un profil d'analyse.
/api/services	Exécutez des tâches telles que les recherches WHOIS, les recherches d'analyse de port, les recherches DNS et les recherches DIG. Vous pouvez également extraire des données de géolocalisation pour une adresse IP ou un ensemble d'adresses IP.
/api/siem	Afficher, mettre à jour et fermer les infractions. Vous pouvez également ajouter des remarques et gérer des motifs de fermeture d'infraction.
/api/staged_config	Extraire la configuration mise en scène pour les utilisateurs, les hôtes, les notifications, les réseaux distants et les services distants. Vous pouvez également lancer ou afficher l'état d'une action de déploiement, et mettre à jour et supprimer les règles Yara.
/api/system	Gérez les hôtes serveur, les interfaces réseau et les règles de pare-feu.

## Procédure

1. Pour accéder à l'interface de documentation de l'API interactive, entrez l'URL suivante dans votre navigateur Web : [https://ConsoleIPaddress/api\\_doc/](https://ConsoleIPaddress/api_doc/).
2. Sélectionnez la version de l'API que vous souhaitez utiliser dans la liste.
3. Accédez au noeud final souhaité.
4. Consultez la documentation du noeud final et définissez les paramètres de la demande.
5. Cliquez sur **Essayer** pour envoyer la demande d'API à votre console et recevoir une réponse HTTPS correctement formatée.

**Remarque :** Lorsque vous cliquez sur **Essayer**, l'action est exécutée sur le système QRadar. Toutes les actions ne peuvent pas être inversées, par exemple, vous ne pouvez pas rouvrir une infraction après avoir fermé.

6. Consultez et collectez les informations que vous devez intégrer à QRadar.

## Remarques

---

:NONE.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Cependant, il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations  
IBM Canada Ltd.  
3600 Steeles Avenue East  
Markham, Ontario  
L3R 9Z7 Canada

Pour obtenir des informations sur les licences relatives aux produits utilisant des jeux de caractères codés sur deux octets (DBCS), contactez le service de la propriété intellectuelle IBM de votre pays ou envoyez vos demandes de renseignements, par écrit, à :

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFACON ET D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Toute référence à ces informations sur des sites Web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites Web. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
92066 Paris-La Défense Cedex 50  
USA

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du document IBM Customer Agreement, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM affichés sont des prix de détail suggérés par IBM. Ils sont à jour et peuvent être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

## Marques

---

IBM, le logo IBM et [ibm.com](http://ibm.com) sont des marques d'International Business Machines Corporation dans de nombreux pays. Les autres noms de produit et de service peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page web "Copyright and trademark information" à l'adresse [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans d'autres pays.

UNIX est une marque de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java et tous les logos et marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.



Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

VMware, le logo VMware, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server et VMware vSphere sont des marques de VMware, Inc. ou de ses filiales aux Etats-Unis et/ou dans certains autres pays.



## Dispositions pour la documentation du produit

---

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

### Domaine d'application

Ces dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site web IBM.

### Usage personnel

Vous pouvez reproduire ces informations pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

### Usage commercial

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

### Droits

Excepté les droits d'utilisation expressément accordés dans le présent document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si IBM estime, à sa discrétion, que l'utilisation des publications devient préjudiciable à ses intérêts ou qu'à son avis les instructions ci-dessus n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

## Déclaration de confidentialité en ligne d'IBM

---

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des sessions et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez la Déclaration de confidentialité d'IBM à l'adresse <http://www.ibm.com/privacy> et la section « Cookies, pixels espions et autres technologies » de la Déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy/details/>.

## Règlement général sur la protection des données (RGPD)

---

Il incombe au client de veiller à sa propre conformité aux différentes lois et réglementations, y compris au Règlement général sur la protection des données (RGPD) de l'Union européenne. Il relève de la seule responsabilité du client de consulter les services juridiques compétents aussi bien pour identifier et interpréter les lois et règlements susceptibles d'affecter son activité, que pour toute action à entreprendre pour se mettre en conformité avec ces lois et réglementations. Les produits, services et autres fonctionnalités décrits ici ne sont pas adaptés à toutes les situations des clients et peuvent présenter une disponibilité limitée. IBM ne donne aucun avis juridique, comptable ou d'audit et ne garantit pas que ses produits ou services assurent la conformité de ses clients par rapport aux lois applicables.

En savoir plus sur le niveau de préparation au RGPD IBM et sur nos offres et fonctionnalités RGPD ici : <https://ibm.com/gdpr>

# Glossaire

---

Ce glossaire contient les termes et définitions du logiciel et des produits IBM QRadar.

Les références croisées suivantes sont utilisées :

- *Voir* vous renvoie d'un terme moins utilisé au terme généralement utilisé ou d'une abréviation à la forme développée.
- *Voir aussi* renvoie à un terme connexe ou opposé.

Pour d'autres termes et définitions, voir le [site Web de terminologie IBM](#) (s'ouvre dans une nouvelle fenêtre).

## A

---

### **accumulateur**

Registre dans lequel une opérande d'une opération peut être stockée et remplacée ensuite par le résultat de cette opération.

### **système actif**

Dans un cluster haute disponibilité, système ayant tous ses services en cours d'exécution.

### **protocole de résolution d'adresse (ARP)**

Protocole qui établit une correspondance dynamique entre une adresse IP et une adresse d'adaptateur de réseau dans un réseau local.

### **partage administratif**

Ressource réseau qui est masquée aux utilisateurs ne disposant pas de privilèges d'administration. Les partages administratifs donne accès aux administrateurs à toutes les ressources sur un système réseau.

### **anomalie**

Ecart par rapport au comportement attendu du réseau.

### **signature d'application**

Ensemble unique de caractéristiques dérivées de l'examen de contenus de paquets puis utilisées pour identifier une application spécifique.

### **ARP**

Voir [protocole de résolution d'adresse](#).

### **redirection du protocole de résolution d'adresse**

Méthode du protocole ARP permettant de notifier l'hôte en cas de problème sur un réseau.

### **ASN**

Voir [numéro de système autonome](#).

### **actif**

Objet gérable déployé ou conçu pour être déployé dans un environnement opérationnel.

### **numéro de système autonome (ASN)**

Dans TCP/IP, numéro affecté à un système autonome par la même autorité centrale que celle qui affecte les adresses IP. Le numéro de système autonome permet aux algorithmes de routage automatique de distinguer les systèmes autonomes.

## B

---

### **comportement**

Effets observables d'une opération ou d'un événement, y compris de ses résultats.

### **interface liée**

Voir [agrégation de liaisons](#).

**rafale**

Augmentation soudaine et rapide du débit d'événements ou de flux entrants entraînant un dépassement de la limite du débit d'événements ou de flux sous licence.

**C**

---

**CIDR**

Voir [routage CIDR](#).

**routage CIDR**

Méthode d'ajout d'adresses IP (Internet Protocol) de classe C. Les adresses sont fournies aux fournisseurs de services Internet (ISP) pour une utilisation par leurs clients. Les adresses CIDR réduisent la taille des tables de routage et augmentent le nombre d'adresses IP disponibles au sein des organisations.

**client**

Programme logiciel ou ordinateur demandant des services à un serveur.

**adresse IP virtuelle du cluster**

Adresse IP partagée entre l'hôte principal ou secondaire et le cluster haute disponibilité.

**intervalle de coalescence**

Fréquence à laquelle les événements sont regroupés. Le regroupement d'événements se produit à des intervalles de 10 secondes et commence avec le premier événement qui ne correspond à aucun événement de coalescence en cours. A l'intérieur de l'intervalle de coalescence, les trois premiers événements correspondants sont regroupés et envoyés au processeur d'événement.

**système de notation de vulnérabilité commune (CVSS)**

Système d'évaluation permettant de mesurer la gravité d'une vulnérabilité.

**console**

Clavier-écran à partir duquel un opérateur peut contrôler et observer le fonctionnement du système.

**capture de contenu**

Processus permettant de capturer une quantité configurable de contenus et de stocker ensuite les données dans un journal de flux.

**donnée d'identification**

Ensemble d'informations accordant certains droits d'accès à un utilisateur ou à un processus.

**crédibilité**

Classement numérique compris entre 0 et 10, utilisé pour déterminer l'intégrité d'un événement ou la présence d'une infraction. La crédibilité augmente lorsque plusieurs sources signalent le même événement ou la même infraction.

**CVSS**

Voir [système de notation de vulnérabilité commune](#).

**D**

---

**objet Noeud terminal de la base de données**

Objet de terminal ou noeud dans une hiérarchie de base de données.

**point de données**

Valeur calculée d'une mesure à un moment donné.

**module de support de périphérique (DSM)**

Fichier de configuration analysant les événements reçus de plusieurs sources de journal et les convertissant à un format de taxonomie standard affichable comme sortie.

**DHCP**

Voir [Dynamic Host Configuration Protocol](#).

**DNS**

Voir [système de noms de domaine](#).

**système de noms de domaine (DNS)**

Système de base de données répartie qui mappe des noms de domaine à des adresses IP.

**gestionnaire de services de données**

Voir [module de support de périphérique](#).

**flux double**

Plusieurs instances de la même transmission de données provenant de sources de flux distinctes.

**Dynamic Host Configuration Protocol (DHCP)**

Protocole de communication utilisé pour gérer les informations de configuration de façon centralisée. Par exemple, DHCP affecte automatiquement des adresses IP aux ordinateurs d'un réseau.

**E**

---

**chiffrement**

Dans le cadre de la sécurité informatique, processus de conversion de données dans une forme inintelligible, de sorte que les données d'origine ne puissent pas être obtenues ou puisse l'être uniquement via un processus de déchiffrement.

**noeud final**

Adresse d'une interface de programme d'application ou d'un service dans un environnement. Une interface de programme d'application expose un noeud final et appelle en même temps les noeuds finaux pour d'autres services.

**dispositif d'analyse externe**

Machine qui est connectée au réseau pour la collecte de données de vulnérabilité concernant des actifs du réseau.

**F**

---

**faux positif**

Événement ou flux que l'utilisateur considère comme n'étant pas une infraction ou qu'il considère comme une infraction n'affectant pas la sécurité.

**flux**

Transmission de données unique passant par un lien lors d'une conversation.

**journal de flux**

Collection d'enregistrements de flux.

**sources de flux**

Origine du flux capturé. Une source de flux est classée comme interne lorsque le flux provient d'un matériel installé sur un hôte géré et comme externe lorsque le flux est envoyé à un collecteur de flux.

**destination d'acheminement**

Système d'un ou plusieurs fournisseurs recevant des données brutes et normalisées de sources de journal et de sources de flux.

**NDQC**

Voir [nom de domaine qualifié complet](#).

**NRQC**

Voir [nom de réseau qualifié complet](#).

**nom de domaine qualifié complet (NDQC)**

Dans les communications Internet, le nom d'un système hôte qui inclut tous les sous-noms du nom de domaine. rchland.vnet.ibm.com est un exemple de nom de domaine complet.

**nom de réseau qualifié complet (NDQC)**

Dans une hiérarchie de réseau, le nom d'un objet comprenant tous les services. CompanyA.Department.Marketing est un exemple de nom de réseau complet.

## G

---

### **passerelle**

Périphérique ou programme permettant de connecter des réseaux ou des systèmes à des architectures réseau différentes.

## H

---

### **HA**

Voir [haute disponibilité](#).

### **cluster à haute disponibilité**

Une configuration haute disponibilité se compose d'un serveur principal et d'un serveur secondaire.

### **code d'authentification de message basé sur le hachage (HMAC)**

Code cryptographique qui utilise une fonction de hachage chiffrée et une clé secrète.

### **haute disponibilité**

Se dit d'un système en cluster reconfiguré en cas de défaillance d'un noeud ou d'un démon, de telle sorte que la charge puisse être redistribuée entre les autres noeuds du cluster.

### **HMAC**

Voir [code d'authentification de message basé sur le hachage](#).

### **contexte d'hôte**

Service surveillant les composants pour s'assurer que chaque composant fonctionne comme prévu.

## I

---

### **ICMP**

Voir [protocole de message de gestion inter-réseau](#).

### **identité**

Collection d'attributs provenant d'une source de données et représentant une personne, une organisation, un lieu ou un élément.

### **IDS**

Voir [système de détection d'intrusion](#).

### **protocole de message de gestion inter-réseau (ICMP)**

Protocole Internet utilisé par une passerelle pour communiquer avec un hôte source, par exemple, pour signaler une erreur dans un datagramme.

### **protocole Internet (IP)**

Protocole acheminant les données via un réseau ou des réseaux interconnectés. Ce protocole joue le rôle d'intermédiaire entre les couches de protocole de niveau supérieur et le réseau physique. Voir également [protocole TCP](#).

### **fournisseur d'accès à Internet (FAI)**

Organisation fournissant un accès à Internet.

### **système de détection d'intrusion (IDS)**

Logiciel détectant les tentatives d'attaques ou attaques réussies sur les ressources surveillées d'un réseau ou d'un système hôte.

### **système de prévention contre les intrusions (IPS)**

Système essayant de refuser les activités potentiellement malveillantes. Les mécanismes de refus peuvent impliquer le filtrage, le suivi ou la définition de limites de débit.

### **IP**

Voir [protocole Internet](#).

### **multi-diffusion IP**

Transmission d'un datagramme IP (Internet Protocol) à une série de systèmes constituant un groupe de multi-diffusion unique.

**IPS**

Voir système de prévention contre les intrusions.

**ISP**

Voir fournisseur d'accès à Internet.

## K

---

**fichier de clés**

Dans le domaine de la sécurité informatique, fichier qui contient des clés publiques et privées, des clés d'authentification et des certificats.

## L

---

**L2L**

Voir local à local.

**L2R**

Voir local à distant.

**LAN**

Voir réseau local.

**LDAP**

Voir Lightweight Directory Access Protocol.

**feuille**

Dans une arborescence, entrée ou noeud ne possédant pas d'enfant.

**protocole LDAP (Lightweight Directory Access Protocol)**

Protocole ouvert utilisant TCP/IP pour fournir l'accès aux annuaires qui prennent en charge un modèle X.500 et pour lequel les ressources exigées par le protocole X.500 DAP (Directory Access Protocol) plus complexe ne sont pas requises. Par exemple, le protocole LDAP peut être utilisé pour localiser des personnes, des organisations et d'autres ressources dans un annuaire Internet ou Intranet.

**agrégation de liens**

Regroupement des cartes d'interface réseau physique, telles que les câbles ou les ports, en une seule interface réseau logique. L'agrégation de lien permet d'augmenter la bande passante et la disponibilité du réseau.

**analyse immédiate**

Analyse de vulnérabilité qui génère des données de rapport à partir de résultats d'analyse d'après le nom de session.

**réseau local**

Réseau reliant plusieurs périphériques dans une zone limitée (telle qu'un bâtiment ou un campus) et pouvant être connecté à un réseau plus grand.

**local à local (L2L)**

Concerne le trafic interne d'un réseau local à un autre réseau local.

**local à distant (L2R)**

Concerne le trafic interne d'un réseau local à un autre réseau distant.

**source de journal**

Équipement de sécurité ou équipement réseau duquel un journal d'événement provient.

**extension de source de journal**

Fichier XML qui inclut l'ensemble des schémas d'expression régulière requis pour identifier et catégoriser les événements de contenu d'événement.

## M

---

**magistrat**

Composant interne analysant le trafic réseau et les événements de sécurité à l'aide de règles personnalisées définies.

## **ampleur**

Mesure de l'importance relative d'une infraction. L'ampleur est une valeur pondérée calculée à partir des mesures de pertinence, de gravité et de crédibilité.

## **N**

---

### **NAT**

Voir [conversion d'adresses réseau](#).

### **NetFlow**

Protocole de réseau Cisco surveillant les données de flux du trafic réseau. Les données NetFlow contiennent des informations sur le client et le serveur, les ports utilisés et le nombre d'octets et de paquets circulant via les commutateurs et routeurs connectés à un réseau. Les données sont envoyées aux connecteurs NetFlow où l'analyse des données se produit.

### **conversion d'adresse réseau (NAT)**

Au niveau d'un pare-feu, conversion d'adresses IP (Internet Protocol) sécurisées en adresses enregistrées externes. Ceci permet la communication avec des réseaux externes mais masque les adresses IP utilisées à l'intérieur du pare-feu.

### **structure hiérarchique du réseau**

Type de conteneur représentant une collection hiérarchique d'objets réseau.

### **couche réseau**

Dans une architecture OSI, couche fournissant des services pour établir un chemin d'accès entre les systèmes ouverts avec une qualité de service prévisible.

### **objet réseau**

Composant d'une hiérarchie réseau.

## **O**

---

### **infraction**

Message envoyé ou événement généré en réponse à une condition contrôlée. Par exemple, une infraction indiquera si une règle a été violée ou si le réseau se trouve en état d'attaque.

### **source hors site**

Périphérique situé en dehors du site principal renvoyant les données normalisées à un collecteur d'événements.

### **cible hors site**

Périphérique situé en dehors du site principal recevant des flux d'événements ou de données d'un collecteur d'événements.

### **Open Source Vulnerability Database (OSVDB)**

Créée par et pour la communauté de sécurité réseau, cette base de données open source fournit des informations techniques sur les vulnérabilités de la sécurité réseau.

### **interconnexion de systèmes ouverts**

Interconnexion de systèmes ouverts conforme aux normes ISO (International Organization for Standardization) pour l'échange d'informations.

### **OSI**

Voir [interconnexion de systèmes ouverts](#).

### **OSVDB**

Voir [Open Source Vulnerability Database](#).

## **P**

---

### **ordre d'analyse syntaxique**

Définition de source de journal dans laquelle l'utilisateur peut définir l'ordre d'importance pour les sources de journal qui partagent une adresse IP ou un nom d'hôte communs.



**données utiles**

Données d'application contenues dans un flux IP, excluant l'en-tête et les informations administratives.

**hôte à haute disponibilité principal**

Ordinateur principal connecté au cluster haute disponibilité.

**protocol**

Ensemble de règles gérant les communications et le transfert de données entre plusieurs unités ou systèmes, dans un réseau de communication.

## Q

---

**mappe QID**

Taxonomie identifiant chaque événement unique et mappant les événements à des catégories de bas niveau et de haut niveau afin de déterminer la façon dont un événement doit être corrélé et organisé.

## R

---

**R2L**

Voir [local à local](#).

**R2R**

Voir [distant à distant](#).

**recon**

Voir [reconnaissance](#).

**reconnaissance (recon)**

Méthode par laquelle les informations appartenant à l'identité des ressources réseau sont collectées. L'analyse réseau et d'autres techniques sont utilisées pour compiler une liste d'événements de ressource réseau auxquels un niveau de sécurité est ensuite affecté.

**mappe de références**

enregistrement de données d'un mappage direct d'une clé à une valeur (un nom d'utilisateur vers un ID global, par exemple).

**mappe de références de mappes**

enregistrement de données de deux clés mappées à un grand nombre de valeurs (mappage, par exemple, du nombre d'octets total d'une application vers un IP source).

**mappe de références d'ensembles**

enregistrement de données d'une clé mappée à un grand nombre de valeurs (mappage, par exemple, d'une liste d'utilisateurs privilégiés à un hôte).

**ensemble de référence**

Liste d'éléments uniques dérivés d'événements ou de flux sur un réseau, (liste d'adresses IP ou liste de noms d'utilisateur, par exemple).

**table de référence**

tableau dans lequel l'enregistrement de données mappe les clés qui ont un type affecté à d'autres clés, qui sont ensuite mappées à une valeur unique.

**minuteur d'actualisation**

Périphérique interne déclenché manuellement ou automatiquement à des intervalles temporisés, mettant à jour les données d'activité réseau en cours.

**pertinence**

Mesure de l'impact relatif d'un événement, d'une catégorie ou d'une infraction sur le réseau.

**distant à local (R2L)**

Trafic externe entre un réseau distant et un réseau local.

**distant à distant (R2R)**

Trafic externe entre un réseau distant et un autre réseau distant.

**rapport**

Dans la gestion des requêtes, données dont la mise en forme résulte de l'exécution d'une requête et de l'application d'un formulaire particulier aux enregistrements renvoyés par cette requête.

**intervalle de rapport**

Intervalle de temps configurable au terme duquel le processeur d'événement doit envoyer la totalité des événements capturés et des données de flux à la console.

**règle de routage**

Condition qui, lorsque ses critères sont satisfaits par les données d'événement, entraîne une collection de conditions et le routage conséquent.

**règle**

Ensemble d'instructions conditionnelles permettant à des systèmes informatiques d'identifier des relations et d'exécuter les réponses automatisées correspondantes.

## S

---

**scanner**

Programme de sécurité automatisée qui recherche les vulnérabilités logicielles au sein d'applications Web.

**hôte à haute disponibilité secondaire**

Ordinateur de secours connecté au cluster haute disponibilité. L'hôte à haute disponibilité secondaire assume la responsabilité de l'hôte à haute disponibilité principal en cas de défaillance de ce dernier.

**gravité**

Mesure de la menace relative qu'une source représente pour une destination.

**Simple Network Management Protocol (SNMP)**

Ensemble de protocoles permettant de surveiller les systèmes et les périphériques dans des réseaux complexes. Les informations sur les périphériques gérés sont définies et stockées dans une base d'informations de gestion.

**SNMP**

Voir [Simple Network Management Protocol](#).

**SOAP**

Protocole simple reposant sur XML pour l'échange d'informations dans un environnement réparti décentralisé. Le protocole SOAP peut être utilisé pour rechercher et renvoyer des informations et pour appeler des services via Internet.

**système de secours**

Système s'activant automatiquement en cas de défaillance du système actif. Si la réplication de disque est activée, il réplique les données du système actif.

**subnet**

Voir [sous-réseau](#).

**masque de sous-réseau**

Pour la mise en sous-réseau Internet, masque de 32 bits permettant d'identifier les bits d'adresse de sous-réseau de la partie hôte d'une adresse IP.

**sous-réseau**

Réseau divisé en plusieurs sous-groupes indépendants de plus petite taille, connectés entre eux.

**sous-recherche**

Fonction permettant d'effectuer une requête de recherche sur un ensemble de résultats de recherche terminés.

**super-flux**

Flux unique composé de plusieurs flux aux propriétés similaires permettant d'améliorer la capacité de traitement en réduisant les contraintes de stockage.

**vue système**

Représentation visuelle de l'hôte principal et de l'hôte géré composant un système.

## T

---

### **TCP**

Voir [Transmission Control Protocol](#).

### **Transmission Control Protocol (TCP)**

Protocole de communication utilisé sur Internet et dans tout réseau respectant les normes IETF (Internet Engineering Task Force) relatives au protocole inter-réseau. TCP constitue un protocole hôte à hôte fiable dans les réseaux à commutation de paquets et dans les systèmes interconnectés de ces réseaux. Voir également [Protocole Internet](#).

### **magasin de clés certifiées**

Fichier de la base de données de clés contenant les clés publiques d'une entité de confiance.

## V

---

### **violation**

Acte visant à détourner ou contourner les règles de l'entreprise.

### **vulnérabilité**

Risque lié à la sécurité dans un système d'exploitation, un logiciel système ou un composant de logiciel d'application.

## W

---

### **serveur whois**

Serveur utilisé pour récupérer les informations sur des ressources Internet enregistrées, telles que les allocations de noms de domaine et adresses IP.



# Index

## A

- à propos [11](#)
- actions consignées
  - fichier suivi responsable [347](#)
- administrateur de réseau [xiii](#)
- adresses IP de chevauchement
  - segmentation de domaine [253](#)
- affichage de l'événement
  - building [59](#)
- affichage de la liste de planification [307](#)
- alertes SNMP
  - ajout [334](#)
  - configuration dans l'assistant de règles client [331](#)
  - configuration de la sortie d'interruption [332](#)
  - envoi à un hôte différent [335](#)
  - présentation de la configuration [331](#)
- arrêt [84](#)
- arrêt du système [84](#)
- assistant de règles personnalisées
  - ajout d>alertes SNMP [334](#)
  - configuration des alertes SNMP [331](#)
- authentification
  - LDAP [32](#)
  - SAML [41](#)
- Authentification
  - Active Directory [27](#)
  - fournisseurs d'authentification pris en charge [25](#)
  - LDAP [27](#)
  - présentation [25](#)
  - RADIUS [27](#)
  - système [27](#)
  - TACACS [27](#)
- authentication system
  - configuration [28](#)

## B

- Base de données Ariel
  - actions de clic droit [102](#)
- brouillage
  - données
    - déchiffrement [341](#)
- brouillage de données
  - création d'expressions [341](#)
  - création d'un profil [340](#)
  - présentation [337](#)

## C

- Catégorie CRE
  - description [388](#)
  - événement de règle personnalisée, *Voir* CRE
- catégorie d'accès
  - description [369](#)
- catégorie d'association
  - description [397](#)

- catégorie d'audit
  - description [424](#)
- Catégorie d'audit de Risk Manager
  - description [430](#)
- Catégorie d'audit SIM [396](#)
- catégorie d'authentification
  - description [360](#)
- catégorie d'exploitation potentielle
  - description [389](#)
- catégorie de malware
  - description [374](#)
- catégorie de politique
  - description [386](#)
- Catégorie de reconnaissance d'hôte VIS
  - description [397](#)
- catégorie de risque
  - description [428](#)
- Catégorie définie par l'utilisateur
  - description [392](#)
- Catégorie DoS
  - description [356](#)
- catégorie inconnue
  - description [388](#)
- catégorie recon
  - description [355](#)
- catégorie suspecte
  - description [376](#)
- catégorie système
  - description [381](#)
- catégories d'événements
  - description [353](#)
- catégories de niveau supérieur
  - description [353](#)
- certificat SSL
  - configuration [38](#)
- Certificat TLS
  - configuration [38](#)
- chiffrement [76](#)
- cible
  - chiffrement [72](#)
  - hors site [72](#)
- cible hors site [72](#)
- clé de licence [54](#), [58](#)
- clé publique
  - génération [71](#)
- collecte de données de référence [179](#), [196](#)
- collecte des fichiers journaux [85](#)
- Collecteur d'événements
  - à propos [59](#)
  - configuration [82](#)
- Commande create [17](#)
- commandes
  - description [188](#)
- compartiments de conservation [119](#)
- Complaint Management Tool, *Voir* outil de gestion de contenu
- comptesutilisateur [20](#)

- configuration
  - authentification system [28](#)
  - profils de réacheminement [299](#)
- configuration de flux [242](#)
- configuration de Microsoft Active Directory [31](#)
- configuration de serveur horaire [66](#)
- conservation des événements
  - activation et désactivation [122](#)
  - configuration [120](#)
  - gestion [122](#)
  - séquencement [122](#)
  - suppression [122](#)
- conservation du flux
  - activation et désactivation [122](#)
  - configuration [120](#)
  - gestion [122](#)
  - séquencement [122](#)
  - suppression [122](#)
- content
  - importation [322](#)
- Conversion d'adresse réseau. [68](#)
- corrélation de catégorie d'événement
  - catégorie d'accès [369](#)
  - catégorie d'association [397](#)
  - Catégorie d'audit de Risk Manager [430](#)
  - catégorie d'authentification [360](#)
  - Catégorie d'événements d'audit SIM [396](#)
  - Catégorie de reconnaissance d'hôte VIS [397](#)
  - catégorie de risque [428](#)
  - catégorie inconnue [388](#)
  - catégorie suspecte [376](#)
  - catégories de niveau supérieur [353](#)
- corrélation de catégorie d'événements
  - Catégorie CRE [388](#)
  - catégorie d'audit [424](#)
  - catégorie d'exploitation potentielle [389](#)
  - catégorie de malware [374](#)
  - catégorie de politique [386](#)
  - Catégorie définie par l'utilisateur [392](#)
  - Catégorie DoS [356](#)
  - catégorie recon [355](#)
  - catégorie système [381](#)
  - exploiter la catégorie
    - description [372](#)
- création [11](#), [200](#)
- création d'un nouveau magasin et d'un calendrier d'exécution [310](#)
- création de compte [21](#)
- créer une source d'informations utilisateur [200](#)

## D

- déclenchement d'une sauvegarde [217](#)
- déploiement des modifications [84](#)
- désactivation du compte [22-24](#)
- destinations de réacheminement
  - affichage [304](#)
  - dans des environnements de domaine [254](#)
  - gestion [304](#)
  - spécification de propriétés [299](#)
- détails de la licence
  - affichage [56](#)
- domaines
  - adresses IP de chevauchement [253](#)

- domaines (*suite*)
  - balisage d'événements et de flux [254](#)
  - création [257](#), [258](#)
  - domaine par défaut [260](#)
  - domaines définis par l'utilisateur [260](#)
  - recherches au niveau du domaine [260](#)
  - règles et infractions [261](#)
  - segmentation de votre réseau [253](#)
  - utilisation des profils de sécurité [260](#)
- données
  - brouillage
    - déchiffrement [341](#)
- données restaurées
  - vérification [228](#)
- Duplication d'un profil de sécurité [19](#)

## E

- e-mail, notifications personnalisées [123](#), [127](#)
- éditer [18](#)
- édition [15](#), [201](#)
- édition d'un magasin et d'un calendrier d'exécution [311](#)
- ensembles de référence
  - affichage [181](#)
  - affichage du contenu [183](#)
  - ajout [181](#)
  - ajout d'éléments [184](#)
  - exportation d'éléments [185](#)
  - suppression d'éléments [186](#)
- événements
  - balisage de domaine [254](#)
  - création de domaine [257](#), [258](#)
  - stockage et réacheminement [307](#)
  - stockage et réacheminement d'événements [307](#)
- exploiter la catégorie [372](#)
- exportation [58](#)
- extensions
  - importation [322](#)
- extraction [201](#)

## F

- fichier suivi responsable
  - actions consignées [347](#)

## G

- gestion [11](#), [20](#), [200](#)
- gestion des systèmes [59](#)
- gestion des utilisateurs
  - Authentification [25](#)
- gestion du système et des licences
  - collection de fichiers journaux [85](#)
- glossaire [461](#)
- groupes de réseaux distants
  - description [247](#)
- Groupes de services distants
  - description [248](#)

## H

- heure système [66](#)
- historique des connexions [21](#)

historique des mises à jour [97](#)

hôte

ajout [76](#)

hôte géré

ajout [76](#)

édition [79](#)

suppression [80](#)

hôtes gérés

Prise en charge d'IPv6 [115](#)

## I

importation de contenu [322](#)

importation des archives de sauvegarde [220](#)

indexation de contenu

activation [132](#)

informations système [64](#), [80](#)

informations utilisateur [196](#), [202](#)

infractions

connaissance du domaine [261](#)

interface utilisateur [7](#)

introduction [xiii](#)

IPv6

prise en charge et limitations [115](#)

## J

journal d'audit

affichage [345](#)

journal des mises à jour automatiques [97](#)

journaux d'audit

description [345](#)

## L

LDAP

Affichage des informations utilisateur [39](#)

authentification [32](#)

liaison [64](#)

liaison de variable

alertes SNMP [332](#)

licence

statut de licence [55](#)

## M

masquage des données, *Voir* brouillage de données

menus contextuels

ajout à l'aide du bouton droit de la souris [102](#)

mise à jour automatique

planification [96](#)

mises à jour

planification [95](#)

mises à jour masquées [97](#)

modifications

déploiement [84](#)

motif de fermeture d'infraction [129](#)

mots de passe

complexité [28](#)

expiration [28](#)

## N

NAT

activation [79](#)

utilisation avec QRadar [68](#)

noeud de données

archivage de données [64](#)

sauvegarde des données du processeur d'événements [63](#)

Noeud de données

Rééquilibrage de la progression, affichage [63](#)

nouveautés [1](#), [2](#), [4](#)

nouvelles fonctions

7.4.1 [4](#)

7.4.2 [2](#)

7.4.3 [1](#)

Version 7.4.0 [4](#)

## O

objet de réseaux distants

ajout [249](#)

objet de services distants

ajout [250](#)

objets de services distants

configuration [250](#)

Onglet Admin [7](#)

options de routage

configuration [305](#)

outil de gestion de contenu

contenu existant, mise à jour [325](#)

contenu personnalisé, exportation d'un type spécifique [315](#)

contenu personnalisé, importation [324](#)

éléments de contenu personnalisés, exportation de plusieurs [320](#)

exportation d'un élément de contenu personnalisé unique [319](#)

exportation de plusieurs éléments de contenu personnalisés [320](#)

exportation de tous les contenus personnalisés d'un type spécifique [315](#)

importation de contenu personnalisé [324](#)

mettre à jour [325](#)

objet de contenu personnalisé, exportation [319](#)

recherche de contenu personnalisé [165](#), [168](#), [170](#), [175](#), [317](#)

## P

paramètres

description [188](#)

paramètres système [100](#)

password [86](#)

planification de votre sauvegarde [214](#)

présentation [195](#)

présentation des tâches de gestion [197](#)

Processeur d'événement

à propos [59](#)

profil de sécurité [17–19](#)

profils de réacheminement

configuration [299](#)

profils de sécurité

profils de sécurité (*suite*)  
privilèges de domaine [260](#)

## R

recherche  
dans des environnements de domaine [260](#)  
Recherches de données utiles  
activation des index [132](#)  
redémarrage [85](#)  
redémarrage du système [85](#)  
règles  
connaissance du domaine [261](#)  
règles de routage  
édition [305](#)  
réinitialisation du module SIM [86](#)  
réseau  
domaines [253](#)  
Réseaux et services distants  
description [247](#)  
Ressources réseau  
lignes directrices suggérées [249](#)  
restauration des informations de configuration  
adresse IP différente [225](#)  
même adresse IP [222](#)  
restoring  
Dépannage des données restaurées [228](#)  
rôles [11](#), [15](#), [16](#)  
rôles utilisateur [11](#)

## S

SAML  
authentification [41](#)  
santé du système [59](#)  
sauvegarde de vos informations [214](#)  
sauvegarde et reprise  
à propos [234](#)  
importation des archives de sauvegarde [220](#)  
lancement d'une sauvegarde [217](#)  
planification des sauvegardes [214](#)  
suppression d'archives de sauvegarde [221](#)  
Serveur Tivoli Directory Integrator [195](#), [198](#)  
serveurs  
reconnaissance [251](#)  
services autorisés  
révocation [212](#)  
SIM  
réinitialisation [86](#)  
source  
hors site [72](#)  
source d'informations utilisateur [195](#), [197](#), [200–202](#)  
source de flux  
à propos [241](#)  
activation ou désactivation [244](#)  
ajout d'alias [245](#)  
ajout de source de flux [242](#)  
balisage de domaine [254](#)  
externe [241](#)  
gestion des alias [245](#)  
interne [241](#)  
modification des alias [245](#)  
nom virtuel [245](#)

source de flux (*suite*)  
suppression d'alias [245](#)  
suppression de la source de flux [245](#)  
source hors site [72](#)  
sources d'informations utilisateur [200](#)  
sources de données externes [241](#)  
sources de flux  
création de domaine [257](#), [258](#)  
sources de flux internes [241](#)  
stockage et retransmission  
affichage de la liste de planification [307](#)  
création d'un planning [310](#)  
édition d'un planning [311](#)  
suppression d'une planification [311](#)  
stocker les informations utilisateur [202](#)  
structure hiérarchique du réseau  
création [87](#)  
suppression [16](#), [202](#)  
suppression d'archives de sauvegarde [221](#)  
Suppression d'un planning de stockage et retransmission [311](#)  
suppression d'un profil de sécurité [19](#)  
syslog  
réacheminement [297](#)  
système [84](#), [85](#)

## T

téléchargement [54](#)  
traitement des incidents  
données restaurées [228](#)  
Transfert des événements / flux de Primaire à Secondaire [236](#)  
transmission d'événements  
configuration [299](#), [302](#)  
transmission d'événements et de flux normalisés [72](#)

## U

utilisateurs [11](#), [21–24](#)

## V

Valeurs de conservation des actifs, présentation [104](#)  
vue de données agrégées  
activation [149](#)  
désactivation [149](#)  
gestion [149](#)  
suppression [149](#)  
vue système  
ajout d'un hôte [76](#)





