IBM QRadar
7.4.3

Guide du stockage externe

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 37.

Table des matières

Introduction aux unités de stockage externe pour les produits QRadar

Ce guide fournit des informations sur la façon de déplacer les systèmes de fichiers `/store`, `/store/backup`ou `/store/ariel` vers une unité de stockage externe pour les produits IBM® QRadar.

Utilisateurs concernés

Les administrateurs système responsables de la configuration des périphériques de stockage externe doivent avoir un accès administrateur aux systèmes QRadar et aux périphériques réseau et aux pare-feu. L'administrateur système doit connaître le réseau d'entreprise et les technologies de mise en 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).

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 (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir la note technique Support and Download (en anglais) (http://www.ibm.com/support/docview.wss?uid=swg21616144).

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'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE 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. Présentation du stockage externe

Pour augmenter la quantité d'espace de stockage disponible pour votre appliance, vous pouvez déplacer une partie de vos données vers un dispositif de stockage externe. Vous pouvez déplacer vos systèmes de fichiers `/store`, `/store/ariel` ou `/store/backup`.

Plusieurs méthodes sont disponibles pour l'ajout de mémoire externe, y compris iSCSI, canal optique et serveur de fichiers réseau (système NFS). Vous devez utiliser iSCSI ou le canal optique pour stocker des données accessibles et interrogeables, telles que le répertoire `/store/ariel`.

Avertissement :

Si vous utilisez un serveur de fichiers réseau ou un partage Windows pour le stockage externe, votre système peut verrouiller et provoquer une indisponibilité. Cette pratique n'est pas prise en charge par IBM QRadar.

Si vous choisissez d'utiliser NFS de toute façon, NFS ne peut être utilisé que pour les données de sauvegarde quotidiennes, telles que le répertoire `/store/backup`. Vous ne pouvez pas utiliser NFS pour stocker des données actives, qui incluent les bases de données PostgreSQL et ariel. Si vous utilisez NFS, cela peut entraîner des problèmes de corruption ou de performances de la base de documents.

Vous pouvez utiliser des solutions de stockage hors carte sur n'importe quel hôte géré ou console, y compris les systèmes haute disponibilité (HA). Lorsque vous utilisez iSCSI ou le canal optique avec la haute disponibilité, le périphérique de stockage externe est monté par le noeud haute disponibilité actif, ce qui garantit la cohérence des données pour un incident à haute disponibilité. Lorsque vous utilisez un stockage externe avec haute disponibilité, vous devez configurer ces unités sur les hôtes primaire et secondaire à haute disponibilité.

Avant de mettre en oeuvre une solution de stockage externe, examinez vos options de stockage locales, votre infrastructure matérielle existante et vos exigences de conservation et de tolérance aux pannes.

Stockage local

Les données stockées localement sur une appliance QRadar sont accessibles avec un temps d'attente inférieur à celui du stockage externe. Dans la mesure du possible, utilisez le stockage local et les dispositifs de nœud de données comme alternative à un périphérique de stockage externe.

Plusieurs dispositifs

Utilisez plusieurs dispositifs si une capacité de stockage plus grande est requise pour votre déploiement QRadar .

Lorsque plusieurs dispositifs ne sont pas réalisables ou lorsqu'un déploiement existant peut augmenter la capacité à l'aide de la mémoire externe disponible, le stockage externe peut être approprié pour votre déploiement.

Matériel et infrastructure

Votre infrastructure existante et votre expérience des réseaux de zone de stockage sont des facteurs importants pour décider s'il faut utiliser une solution de stockage externe.

Certains dispositifs externes nécessitent moins de configuration et peuvent être en mesure d'utiliser les infrastructures réseau existantes. Par exemple, iSCSI utilise le réseau Ethernet existant, tandis que le canal optique utilise du matériel spécialisé.

Conservation des données et tolérance aux pannes

Votre règle de conservation des données QRadar est importante pour la prise en compte d'une solution de stockage externe. Si vos paramètres de conservation de données dépassent la capacité de stockage existante ou si vous envisagez d'étendre la conservation des dispositifs déployés existants, vous pouvez avoir besoin d'une solution de stockage externe.

Une solution de stockage externe peut être utilisée pour améliorer vos capacités de tolérance aux pannes et de reprise après incident.

Configuration de stockage requise pour les dispositifs (installations virtuelles et logicielles)

Pour installer QRadar à l'aide d'options de configuration virtuelle ou logicielle, vous devez disposer de la quantité de stockage minimale requise.

Le tableau suivant indique la configuration minimale requise pour l'installation de QRadar à l'aide de l'option virtuelle ou logicielle.

Remarque : La quantité de stockage minimale peut varier en fonction d'un certain nombre de facteurs, comme la taille des événements, le nombre d'événements par seconde (EPS) et les règles de conservation.

Tableau 1. Quantité de stockage minimale requise pour les dispositifs qui utilisent l'option d'installation virtuelle ou logicielle.

Classification système	Informations sur le dispositif	IOPS	Vitesse de transfert des données (Mo/s)
Performances minimales	Prise en charge de l'octroi de licence XX05	800	500
Performances moyennes	Prend en charge les licences XX28 et XX29	1 200	1 000
Hautes performances	Prise en charge de l'octroi de licence XX48	10 000	2000
Small All-in-One ou 1600	Moins de 500 EPS	300	300
Collecteurs d'événements/ flux	Evénements et flux	300	300

Options du système de fichiers pour le stockage externe

Utilisez une solution de stockage externe pour déplacer le système de fichiers `/store` ou des sous-répertoires spécifiques, tels que le répertoire `/store/ariel`.

Vous pouvez déplacer le système de fichiers `/store` pour augmenter les niveaux de tolérance aux pannes dans votre déploiement IBM QRadar. Chaque option a une incidence sur les performances de QRadar.

Le répertoire `/store/ariel` est le système de fichiers le plus commun qui est déplacé vers une solution de stockage externe. En déplaçant le système de fichiers `/store/ariel`, vous pouvez déplacer les données de journal et d'activité réseau collectées vers la mémoire externe. Le disque local reste utilisé pour la base de données PostgreSQL et pour les résultats de la recherche temporaire.

Les administrateurs peuvent déplacer les types de données QRadar suivants vers les unités de stockage externe :

- Informations de configuration et de métadonnées PostgreSQL
- Activité de journal, charges utiles (données brutes), données normalisées et index

- Activité réseau, charges utiles, données normalisées et index
- Graphiques de séries temporelles (vues globales et agrégats)

Remarque : Ne déplacez pas `/transient` ou `/storetmp` sur une unité de stockage externe. Le déplacement de ces répertoires entraîne l'arrêt du bon fonctionnement de votre système.

Impact sur les performances des solutions de stockage externe

Le déplacement du système de fichiers `/store` vers une unité externe peut affecter les performances de QRadar .

Après la migration, toutes les E-S de données du système de fichiers `/store` ne sont plus exécutées sur le disque local. Avant de déplacer vos données QRadar vers une unité de stockage externe, vous devez prendre en compte les informations suivantes :

- Maintenez vos recherches d'activité de journal et de réseau sur votre disque local en installtant le système de fichiers `/store/transient` sur la partition de fichier `/store` inutilisée.
- Les recherches marquées comme sauvegardées se trouvent également dans le répertoire `/store/transient`. Si le disque local est défaillant, ces recherches ne sont pas sauvegardées.

Extension de stockage

Extension de stockage

En créant plusieurs volumes et en installant `/store/ariel/events` et `/store/ariel/flows`, vous pouvez développer vos capacités de stockage au-delà du système de fichiers unique configuré par défaut avec IBM QRadar. Un système de fichiers unique prend en charge jusqu'à 500 To.

Partition de magasin

Tout sous-répertoire du système de fichiers `/store` peut être utilisé comme point de montage pour votre périphérique de stockage externe. Toutefois, seuls les systèmes de fichiers `/store` et `/store/ariel` sont pris en charge pour ce qui est externe avec un déploiement à haute disponibilité.

Si vous souhaitez déplacer des données d'événement ou de flux dédiés, vous pouvez configurer des points de montage plus spécifiques. Par exemple, vous pouvez configurer `/store/ariel/events/records` et `/store/ariel/events/payloads` en tant que points de montage.

Autres options d'extension de stockage

Vous pouvez ajouter davantage de stockage de données à l'hôte QRadar ou optimiser votre stockage actuel en utilisant un ou plusieurs fichiers Ces options (https: //www.ibm.com/support/pages/qradar-data-storage-limits) :

- Installez un nœud de données. Les noeuds de données permettent aux déploiements de QRadar nouveaux et existants d'ajouter de la capacité de stockage et de traitement à la demande en fonction des besoins. Pour plus d'informations, voir *IBM QRadar - Guide d'architecture et de déploiement*.
- Configuration de l'archivage du serveur de fichiers réseau (Network File System). Vous pouvez configurer le serveur de fichiers réseau pour une console QRadar autonome, de nouveaux déploiements QRadar à haute disponibilité ou des déploiements QRadar à haute disponibilité existants.
- Configurez vos politiques de rétention pour définir la durée nécessaire à QRadar pour conserver les données d'événement et de flux, et ce que vous devez faire lorsque ces données atteignent un certain âge. Pour plus d'informations, voir *IBM QRadar Administration Guide*.
- Activez Coalescence d'événement (https: //www.ibm.com/support/pages/qradar-how-does-coalescing-work-qradar) pour améliorer les performances et réduire les impacts de stockage, lors de la réception d'un grand nombre d'événements correspondant à des critères spécifiques.

Options de stockage externe

Vous pouvez utiliser iSCSI, le canal optique ou le serveur de fichiers réseau (Network File System ou NFS) pour fournir une solution de stockage externe.

Les disques embarqués fournissent une solution de stockage à faible temps d'attente et à débit élevé, qui est testée et validée avec différentes charges de travail. Lorsque plusieurs dispositifs sont déployés, les performances et l'échelle de capacité sont au même taux.

Fibre Channel

LE canal optique fournit les performances externes les plus rapides en utilisant des vitesses de réseau de stockage (SAN) de 200 MBps à 3200 MBps, en fonction de la configuration de votre réseau.

Les performances de canal optique peuvent être affectées par des facteurs de l'implémentation SAN, tels que les facteurs suivants :

- Nombre de disques ou de broches par volume
- Nombre de sessions simultanées
- Capacité du cache dans les contrôleurs SAN

iSCSI

ISCSI utilise un canal de stockage dédié sur une infrastructure Ethernet standard, plutôt qu'un réseau SAN dédié. Pour cette raison, iSCSI peut être le plus facile à implémenter, le plus rentable et le plus facilement disponible.

Si vous implémentez une solution iSCSI, la capacité réseau est partagée entre l'accès au stockage externe et les E/S de l'interface de gestion. Dans ce cas, vous pouvez configurer une interface réseau secondaire sur un réseau de stockage distinct.

QRadar prend en charge la connectivité 1 Gbit et 10 Gbit de la box sur de nombreux dispositifs.

NFS

Avertissement :

Si vous utilisez un serveur de fichiers réseau ou un partage Windows pour le stockage externe, votre système peut verrouiller et provoquer une indisponibilité. Cette pratique n'est pas prise en charge par IBM QRadar.

Si vous choisissez d'utiliser NFS de toute façon, NFS ne peut être utilisé que pour les données de sauvegarde quotidiennes, telles que le répertoire `/store/backup`. Vous ne pouvez pas utiliser NFS pour stocker des données actives, qui incluent les bases de données PostgreSQL et ariel. Si vous utilisez NFS, cela peut entraîner des problèmes de corruption ou de performances de la base de documents.

Utilisez NFS pour les tâches pendant les heures creuses, les tâches qui impliquent des écritures de fichier de traitement par lots et les tâches qui impliquent un volume limité d'E-S de fichier. Par exemple, utilisez NFS pour la configuration quotidienne et les sauvegardes de données.

Le stockage NFS fonctionne sur les réseaux Ethernet de gestion existants et est limité par les performances de réseau. Il est possible d'utiliser une interface réseau dédiée pour améliorer les performances réseau par rapport au partage d'une interface de gestion. Le protocole du serveur de fichier réseau (NFS) peut affecter les performances des droits d'accès aux fichiers, de verrouillage et de réseau.

Si le serveur de fichiers réseau n'est utilisé que pour les sauvegardes, le même partage NFS peut être utilisé pour chaque hôte. Les fichiers de sauvegarde contiennent le nom d'hôte système, qui permet d'identifier chaque fichier de sauvegarde. Si vous stockez une longue période de données sur vos partages NFS, envisagez une part ou une exportation distincte pour chaque appliance dans votre déploiement.

Limitations de la mémoire externe

Plusieurs systèmes ne peuvent pas accéder à la même unité par bloc dans un déploiement IBM QRadar.

Si vous configurez iSCSI dans un environnement à haute disponibilité, ne montez pas les volumes iSCSI ou de canal optique sur l'hôte secondaire alors que l'hôte primaire accède aux volumes.

Un dispositif de stockage externe doit pouvoir fournir une capacité de lecture et d'écriture cohérente de 100 MBps à 200 MBps. Lorsqu'une capacité de lecture et d'écriture cohérente n'est pas disponible, les problèmes suivants peuvent se produire :

- Les performances d'écriture des données sont affectées.
- Les performances de recherche sont affectées.

Si les performances continuent à se dégrader, le pipeline de traitement peut être bloqué et QRadar peut afficher des messages d'avertissement et supprimer des événements et des flux.

Stockage externe dans les environnements à haute disponibilité

Si vous choisissez de déplacer le système de fichiers `/store` dans un environnement à haute disponibilité (HA), le système de fichiers `/store` n'est pas répliqué à l'aide de l'unité par bloc de réplication de disque.

Si vous déplacez le système de fichiers `/store/ariel` vers un périphérique de stockage externe et que vous maintenez le système de fichiers `/store` sur le disque local, le système de fichiers `/store` est synchronisé avec l'hôte secondaire à haute disponibilité. Par défaut, lorsque votre environnement est configuré pour la haute disponibilité, l'unité par bloc de réplication de disque est activée.

Si vous utilisez la haute disponibilité et que vous déplacez un système de fichiers autre que `/store` ou `/store/ariel` vers une solution de stockage externe multi-accès, vous devez arrêter **`multipathd`** avant de mettre à niveau QRadar.

Chapitre 2. Périphérique de stockage externe iSCSI

Vous pouvez configurer un périphérique de stockage iSCSI dans un déploiement IBM QRadar standard ou haute disponibilité (HA).

Lorsque vous configurez un périphérique de stockage externe iSCSI, vous devez faire migrer les données QRadar qui sont gérées sur votre système de fichiers `/store` ou `/store/ariel`, puis monter le système de fichiers `/store` ou `/store/ariel` sur une partition sur le volume de dispositif iSCSI.

Selon la configuration de votre unité, vous devrez peut-être créer une partition sur le volume de votre disque iSCSI.

Si vous configurez iSCSI dans un déploiement à haute disponibilité et que votre hôte HA primaire échoue, votre périphérique iSCSI peut être utilisé pour maintenir la cohérence des données avec votre hôte HA secondaire.

Dans les environnements HA, consultez le fichier `/var/log/messages` pour des erreurs dans votre configuration de stockage iSCSI.

Configuration iSCSI dans les déploiements QRadar standard

Pour déplacer des données d'une console QRadar ou d'un hôte géré vers un périphérique de stockage iSCSI :

- Suivez les instructions de Configuration des volumes iSCSI.
- Faites migrer le système de fichiers vers un périphérique de stockage iSCSI.
  - Déplacez le système de fichiers /store/ariel vers une solution de stockage iSCSI.
  - Déplacez le système de fichiers /store vers une solution de stockage iSCSI.
- Suivez les instructions dans Monter automatiquement le volume iSCSI.
- Suivez les instructions dans Vérifier les connexions iSCSI.

Configuration iSCSI dans les déploiements à haute disponibilité

Pour déplacer des données dans un déploiement à haute disponibilité vers un périphérique de stockage iSCSI:

- Suivez les instructions de Configuration des volumes iSCSI sur votre dispositif principal.
- Faites migrer le système de fichiers de votre dispositif principal vers un périphérique de stockage iSCSI.
  - Déplacez le système de fichiers /store/ariel vers une solution de stockage iSCSI.
  - Déplacez le système de fichiers /store vers une solution de stockage iSCSI.
- Suivez les instructions de Monter automatiquement le volume iSCSI sur votre dispositif principal.
- Suivez les instructions de «Configuration d'iSCSI dans un déploiement à haute disponibilité», à la page 13 sur votre dispositif secondaire.
- Suivez les instructions dans Vérifier les connexions iSCSI.

Configuration des volumes iSCSI

Vous pouvez configurer iSCSI pour un QRadar Console autonome ou un QRadar Console qui est l'hôte primaire à haute disponibilité (HA) dans un déploiement à haute disponibilité.

Pourquoi et quand exécuter cette tâche

Vous pouvez éventuellement créer une partition sur le volume de l'unité du périphérique de stockage iSCSI externe.

IBM QRadar V7.2.1 et version ultérieure utilisent le système de fichiers XFS. Vous pouvez créer la partition sur votre dispositif iSCSI avec un système de fichiers ext4 ou XFS.

Les partitions de disque sont créées à l'aide d'une table de partitions GUID (GPT). Vous pouvez utiliser une nouvelle partition de dispositif comme point de montage pour le système de fichiers, tel que `/store` ou `/store/ariel` que vous faites migrer.

Important : Si vous avez créé une partition de dispositif iSCSI ou canal optique sur votre périphérique externe et que les données QRadar sont stockées, vous ne pouvez pas créer de partition ou reformater la partition sur le volume.

Procédure

1. À l'aide de SSH, connectez-vous à QRadar Console en tant qu'utilisateur racine.
2. Editez le fichier `/etc/iscsi/initiatorname.iscsi` pour inclure le nom qualifié iSCSI de votre hôte.

   ```
   InitiatorName=<iqn.yyyy-mm>.<reversed_domain_name>:<hostname>
   ```

   Exemple : `InitiatorName=iqn.2014-11.com.qradar:pl13`
3. Ouvrez une session sur le serveur iSCSI en entrant la commande suivante :

   ```
   systemctl restart iscsi
   ```
4. Pour détecter des volumes sur le serveur iSCSI, entrez la commande suivante :

   ```
   iscsiadm -m discovery --type sendtargets --<portal_IP_address>:[<port>]
   ```

   L'option *Adresse IP* est l'adresse IP du serveur iSCSI. Le *port* est facultatif. Enregistrez le nom du demandeur.
5. Pour vous connecter au serveur iSCSI, entrez la commande suivante :

   ```
   iscsiadm -m node --targetname <initiator_name_from_step_4> --portal <IP_address>:[<port>]>
   --login
   ```
6. Pour rechercher le nom de volume de dispositif iSCSI, entrez la commande suivante :

   ```
   dmesg | grep "Attached SCSI disk"
   ```
7. Pour créer une partition, utilisez la commande GNU parted :

   ```
   parted /dev/<volume>
   ```
8. Configurez le libellé de partition pour utiliser GPT en entrant la commande suivante :

   ```
   mklabel gpt
   ```
9. Si le message suivant s'affiche, entrez `Oui`.

   ```
   Avertissement : le label de disque existant sur /dev/<volume> sera
   détruit et toutes les données sur ce disque seront perdues. Voulez-vous
   continuer ?
   ```
10. Créez une partition sur le volume de disque iSCSI.
    a) Pour créer la partition, entrez la commande suivante :

       ```
       mkpart primary 0% 100%
       ```

    b) Définissez les unités par défaut sur téraoctet en entrant la commande suivante :

       ```
       unit TB
       ```

    c) Vérifiez que la partition est créée en entrant la commande suivante :

       ```
       print
       ```

d) Quittez GNU parted en entrant la commande suivante :

```
quit
```

e) Mettez à jour le noyau avec les nouvelles données de partition en entrant la commande suivante :

```
partprobe /dev/<volume>
```

Après avoir mis à jour le noyau, vous pouvez être invité à redémarrer l'appliance. Si vous êtes invité à le faire, redémarrez l'appliance.

f) Pour vérifier que la partition est créée, entrez la commande suivante :

```
cat /proc/partitions
```

11. Reformater la partition et créer un système de fichiers.

- Pour créer un système de fichiers XFS, entrez la commande suivante :

```
mkfs.xfs -f /dev/<partition>
```

- Pour un système de fichiers ext4 , entrez la commande suivante :

```
mkfs.ext4 /dev/<partition>
```

Que faire ensuite

Voir «Déplacement du système de fichiers /store/ariel vers une solution de stockage iSCSI», à la page 11 ou «Déplacement du système de fichiers /store vers une solution de stockage iSCSI», à la page 9.

Tâches associées

Identification et résolution des problèmes liés à iSCSI

Déplacement du système de fichiers /store vers une solution de stockage iSCSI

Vous pouvez faire migrer les données IBM QRadar qui sont gérées dans le système de fichiers `/store` et monter le système de fichiers `/store` sur une partition de dispositif iSCSI.

La migration du système de fichiers `/store` vers votre dispositif de stockage externe peut prendre un certain temps.

Avant de commencer

Configuration des volumes iSCSI.

Procédure

1. Arrêtez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

Remarque : Exécutez la commande `systemctl stop solr` uniquement si vous disposez de l'analyse légale d'incident QRadar dans votre déploiement.

```
systemctl stop hostcontext
systemctl stop ecs-ec-ingress
systemctl stop tomcat
systemctl stop hostservices
systemctl stop systemStabMon
systemctl stop crond
systemctl stop soir
```

Remarque : Exécutez la commande `systemctl stop tomcat` sur la console.

2. Démontez les systèmes de fichiers en tapant les commandes suivantes :

```
umount /store
```

3. Créez le répertoire /store_old en entrant la commande suivante :

```
mkdir /store_old
```

4. Calculer l'identificateur unique universel (UUID) de la partition de dispositif iSCSI en entrant la commande suivante :

   blkid /dev/<*partition*>

5. Editez le fichier /etc/fstab pour mettre à jour le point de montage du système de fichiers /store existant sur /store_old.
6. Créez un nouveau point de montage pour le système de fichiers /store en ajoutant le texte suivant au fichier /etc/fstab :
   - Si le système de fichiers est XFS, ajoutez le texte suivant :

     ```
     UUID=<uuid> /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
     ```

   - Si le système de fichiers est ext4, ajoutez le texte suivant :

     ```
     UUID=<uuid> /store ext4 noatime,noauto,nobarrier 0 0
     ```

   Sauvegardez le fichier et fermez-le.
7. Montez le système de fichiers /store sur la partition du dispositif iSCSI en entrant la commande suivante :

   mount /store

8. Montez le système de fichiers /store_old sur le disque local en entrant la commande suivante :

   mount /store_old

9. Déplacez les données du disque local vers le périphérique de stockage iSCSI en entrant la commande suivante :

   cp -af /store_old/* /store

10. Démontez /store_old en entrant la commande suivante :

    umount /store_old

11. Supprimez le répertoire /store_old en entrant la commande suivante :

    rmdir /store_old

12. Editez le fichier /etc/fstab pour supprimer l'entrée /store_old.
13. Démarrez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

    Remarque : Exécutez la commande systemctl start solruniquement si vous disposez de l'analyse légale des accidents QRadar dans votre déploiement.

```
systemctl start crond
systemctl start systemStabMon
systemctl start hostservices
systemctl start tomcat
systemctl start ecs-ec-ingress
systemctl start hostcontext
systemctl start solr
```

14. Supprimez la copie locale de /store du gestionnaire de volume logique (LVM) en entrant les commandes suivantes :

```
lvchange -an /dev/storerhel/store 2>/dev/null
lvrename /dev/storerhel/store /dev/storerhel/storeold 2>/dev/null
```

Que faire ensuite

Voir «Montage automatique du volume iSCSI», à la page 12.

Tâches associées

Déplacement du système de fichiers /store/ariel vers une solution de stockage iSCSI
Vous pouvez migrer les données IBM QRadar qui sont gérées dans le système de fichiers `/store/ariel` et monter le système de fichiers `/store/ariel` sur une partition de dispositif iSCSI.

Déplacement du système de fichiers /store/ariel vers une solution de stockage iSCSI

Vous pouvez migrer les données IBM QRadar qui sont gérées dans le système de fichiers `/store/ariel` et monter le système de fichiers `/store/ariel` sur une partition de dispositif iSCSI.

Avant de commencer

Configurez les volumes iSCSI.

Procédure

1. Arrêtez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl stop hostcontext
systemctl stop ecs-ec-ingress
systemctl stop tomcat
systemctl stop hostservices
systemctl stop systemStabMon
systemctl stop crond
```

2. Déplacez le point de montage existant en entrant les commandes suivantes :

```
cd /store
mv ariel ariel_old
```

3. Vérifiez l'identificateur unique universel (UUID) de la partition d'unité iSCSI en entrant la commande suivante :

   `blkid /dev/`*`partition`*

4. Ajoutez le point de montage du système de fichiers `/store/ariel` en ajoutant le texte suivant au fichier `/etc/fstab` :

   - Si le système de fichiers est XFS, copiez le texte suivant dans un éditeur de texte, supprimez le retour à la ligne et collez en une seule ligne :

     ```
     UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,
     noauto,nobarrier 0 0
     ```

   - Si le système de fichiers est ext4, ajoutez le texte suivant

     ```
     UUID=uuid /store/ariel ext4 noatime,noauto,nobarrier 0 0
     ```

5. Créez le répertoire ariel pour le point de montage en entrant la commande suivante :

   `mkdir /store/ariel`

6. Montez `/store/ariel` sur la partition d'un dispositif iSCSI en entrant la commande suivante :

   `mount /store/ariel`

7. Vérifiez que /store/ariel est correctement monté en entrant la commande suivante :

   `df -h`

8. Déplacez les données du disque local vers le périphérique de stockage iSCSI en entrant la commande suivante :

```
cp -af /store/ariel_old/* /store/ariel
```

9. Supprimez le répertoire `/store/ariel_old` en entrant la commande suivante :

```
rmdir /store/ariel_old
```

10. Démarrez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl start crond
systemctl start systemStabMon
systemctl start hostservices
systemctl start tomcat
systemctl start ecs-ec-ingress
systemctl start hostcontext
```

Que faire ensuite

Voir «Montage automatique du volume iSCSI», à la page 12.

Tâches associées

Déplacement du système de fichiers /store vers une solution de stockage iSCSI

Montage automatique du volume iSCSI

Vous devez configurer IBM QRadar pour monter automatiquement le volume iSCSI.

Avant de commencer

Assurez-vous que vous avez déplacé les systèmes de fichiers `/store/ariel` ou `/store` vers une solution de stockage iSCSI.

Procédure

1. Ajoutez le script iSCSI aux informations de démarrage en entrant les commandes suivantes :

```
systemctl enable iscsi
```

2. Activez le service iscsi-mount en entrant la commande suivante :

```
systemctl enable iscsi-mount
```

3. Vérifiez que le dispositif iSCSI est correctement monté en entrant la commande suivante :

```
df -h
```

Que faire ensuite

Si vous configurez iSCSI dans un déploiement QRadar standard, voir «Vérification des connexions iSCSI», à la page 14.

Si vous configurez un environnement à haute disponibilité (HA), vous devez configurer votre hôte secondaire à haute disponibilité en utilisant les mêmes connexions iSCSI que celles utilisées pour votre hôte primaire à haute disponibilité. Pour plus d'informations, voir «Configuration d'iSCSI dans un déploiement à haute disponibilité», à la page 13.

Tâches associées

Configuration d'iSCSI dans un déploiement à haute disponibilité
Pour utiliser un dispositif iSCSI dans un environnement à haute disponibilité, vous devez configurer les hôtes primaire et secondaire à haute disponibilité pour qu'ils utilisent le même périphérique de stockage externe iSCSI. Seul le chemin d'accès unique iSCSI est pris en charge pour le déploiement à haute disponibilité.

Configuration d'iSCSI dans un déploiement à haute disponibilité

Pour utiliser un dispositif iSCSI dans un environnement à haute disponibilité, vous devez configurer les hôtes primaire et secondaire à haute disponibilité pour qu'ils utilisent le même périphérique de stockage externe iSCSI. Seul le chemin d'accès unique iSCSI est pris en charge pour le déploiement à haute disponibilité.

Pourquoi et quand exécuter cette tâche

Veillez à utiliser un **initiatorname** différent sur les hôtes principal et secondaire à haute disponibilité. Votre dispositif iSCSI doit être configuré pour permettre à chaque **initiatorname** d'accéder au même volume sur le dispositif iSCSI.

Important : Configurez iSCSI pour votre hôte secondaire à hauite disponibilité avant de créer votre cluster à haute disponibilité.

Procédure

1. Utilisez Secure Shell pour vous connecter à l'hôte secondaire à haute disponibilité en tant que superutilisateur.
2. Pour configurer votre hôte secondaire à haute disponibilité afin d'identifier le volume du dispositif iSCSI, ajoutez le nom qualifié iSCSI de votre hôte au fichier `/etc/iscsi/initiatorname.iscsi`.

   ```
   Initiatorname=iqn.<yyyy-mm>.{reversed domain name}:<hostname>
   ```

   Important : Le **initiatorname** de votre hôte secondaire à haute disponibilité doit être différent du **initiatorname** de votre hôte principal à haute disponibilité.

   Exemple : `InitiatorName=iqn.2008-11.com.qradar:pl14`
3. Redémarrez le service iSCSI pour ouvrir une session sur le serveur en entrant la commande suivante :

   ```
   systemctl restart iscsi
   ```
4. Pour détecter le volume sur le serveur iSCSI, entrez la commande suivante :

   ```
   iscsiadm -m discovery --type sendtargets --portal <IP_address>:[<port>]
   ```

   Remarque : Le *port* est facultatif.
5. Vérifiez la connexion à votre serveur iSCSI en entrant la commande suivante :

   ```
   iscsiadm -m node --targetname <initiator_name_from_the_previous_step> --portal <IP_address>:
   [<port>] --login
   ```
6. Pour rechercher le nom de volume de dispositif iSCSI, entrez la commande suivante :

   ```
   dmesg | grep "Attached SCSI disk"
   ```
7. Configurez le point de montage de l'hôte secondaire à haute disponibilité.
   a) Si vous déplacez le système de fichiers `/store`, démontez les systèmes de fichiers en tapant les commandes suivantes :

      ```
      umount /store
      ```
   b) Identifiez l'UUID de la partition de dispositif iSCSI en entrant la commande suivante :

      ```
      blkid /dev/<partition>
      ```
   c) Pour déplacer le système de fichiers `/store`, modifiez les paramètres de fichier dans le fichier `/etc/fstab` pour qu'ils soient identiques aux points de montage qui peuvent être répertoriés dans le fichier `/etc/fstab file` sur l'hôte primaire à haute disponibilité :

- `/store`
- Pour la partition `/store` , utilisez la même valeur `UUID` que celle utilisée pour la partition `/store` sur la partition primaire.

d) Si vous déplacez le système de fichiers `/store/ariel`, modifiez les paramètres dans le fichier `/etc/fstab` pour qu'ils soient identiques au point de montage répertorié dans le fichier `/etc/fstab file` sur l'hôte primaire à haute disponibilité pour `/store/ariel`.

8. Configurez l'hôte secondaire à haute disponibilité pour monter automatiquement le volume iSCSI.

a) Ajoutez le script iSCSI aux informations de démarrage en entrant les commandes suivantes :

```
systemctl enable iscsi
```

b) Activez le service iscsi-mount en entrant la commande suivante :

```
systemctl enable iscsi-mount
```

c) Si vous déplacez le système de fichiers `/store`, supprimez la copie locale de `/store` en entrant les commandes suivantes :

```
lvchange -an /dev/storerhel/store 2>/dev/null
lvrename /dev/storerhel/store /dev/storerhel/storeold 2>/dev/null
```

Que faire ensuite

Créez un cluster à haute disponibilité. Pour plus d'informations, voir *IBM QRadar High Availability Guide*.

Voir «Vérification des connexions iSCSI», à la page 14.

Vérification des connexions iSCSI

Vérifiez que les connexions entre un hôte primaire à haute disponibilité ou un hôte secondaire à haute disponibilité et un périphérique iSCSI sont opérationnelles

Procédure

1. A l'aide de Secure Shell, connectez-vous à l'hôte primaire ou secondaire à haute disponibilité en tant que superutilisateur.
2. Pour tester la connexion à votre périphérique de stockage iSCSI, entrez la commande suivante :

   `ping` *`iSCSI_Storage_IP_Address`*
3. Vérifiez que le service iSCSI est en cours d'exécution et que le port iSCSI est disponible en entrant la commande suivante :

   `telnet` *`iSCSI_Storage_IP_Address`* `3260`

   Remarque : Le port par défaut est 3260.
4. Vérifiez que la connexion au dispositif iSCSI est opérationnelle en entrant la commande suivante :

   `iscsiadm -m node`

   Pour vérifier que le dispositif iSCSI est correctement configuré, vous devez vous assurer que la sortie affichée pour l'hôte primaire à haute disponibilité correspond à la sortie affichée pour l'hôte secondaire à haute disponibilité.

   Si la connexion à votre volume iSCSI n'est pas opérationnelle, le message suivant s'affiche :

   `iscsiadm: Aucun enregistrement trouvé`
5. Si la connexion à votre volume iSCSI n'est pas opérationnelle, consultez les options d'identification et résolution des problèmes suivantes :

   - Vérifiez que le périphérique de stockage iSCSI externe est opérationnel.

- Accédez au fichier /var/log/messages et examinez les erreurs spécifiques à votre configuration de stockage iSCSI.
- Vérifiez que les valeurs **initiatornames** iSCSI sont correctement configurées à l'aide du fichier `/etc/iscsi/inititatorname.iscsi`.
- Si vous ne trouvez pas d'erreurs dans le journal des erreurs et que vos connexions iSCSI restent désactivées, contactez votre administrateur de réseau pour confirmer que votre serveur iSCSI est fonctionnel ou pour identifier les modifications de configuration réseau.
- Si votre configuration réseau a été modifiée, vous devez reconfigurer vos connexions iSCSI.

Que faire ensuite

Etablir un cluster à haute disponibilité. Vous devez connecter votre hôte primaire à haute disponibilité principal à votre hôte secondaire à haute disponibilité à l'aide de l'interface utilisateur QRadar. Pour plus d'informations sur la création d'un cluster à haute disponibilité, voir le *IBM QRadar High Availability Guide*.

Identification et résolution des problèmes liés à iSCSI

Pour éviter les problèmes de communication et de disque iSCSI, vous devez connecter QRadar, le serveur iSCSI et vos commutateurs réseau à une alimentation de secours (UPS). La panne d'alimentation dans un commutateur réseau peut générer des erreurs de disque de rapport de volume iSCSI ou rester en lecture seule.

Pourquoi et quand exécuter cette tâche

Dans un environnement à haute disponibilité (HA), si votre hôte principal échoue, vous devez restaurer votre configuration iSCSI sur l'hôte principal. Dans ce cas, les données `/store or /store/ariel` sont déjà migrées vers le périphérique de stockage externe partagé iSCSI. Par conséquent, pour restaurer la configuration iSCSI de l'hôte principal, assurez-vous de configurer un hôte HA secondaire. Pour plus d'informations, voir «Configuration d'iSCSI dans un déploiement à haute disponibilité», à la page 13

Procédure

1. Déterminez si une erreur de disque existe.
   a) A l'aide de Secure Shell, connectez-vous à la console QRadar en tant que superutilisateur.
   b) Créez un fichier vide `filename.txt` sur votre volume iSCSI en entrant l'une des commandes suivantes :
      - `touch /store/ariel/filename.txt`
      - `touch /store/filename.txt`

   Si votre volume iSCSI est monté correctement et que vous disposez de droits d'accès en écriture sur le volume, la commande appuyer crée un fichier vide nommé filename.txt sur votre volume iSCSI.

   Si un message d'erreur s'affiche, démontez et remontez le volume iSCSI.
2. Arrêtez les services QRadar.
   - Si vous avez migré le système de fichiers /store, entrez les commandes suivantes dans l'ordre indiqué :

     ```
     systemctl stop hostcontext
     systemctl stop ecs-ec-ingress
     systemctl stop tomcat
     systemctl stop hostservices
     systemctl stop systemStabMon
     systemctl stop crond
     ```

   - Si vous avez migré le système de fichiers `/store/ariel`, entrez la commande suivante :

     ```
     systemctl stop hostcontext
     ```
3. Démontez le volume iSCSI.

- Si vous avez migré le système de fichiers `/store`, entrez les commandes suivantes :

```
umount /store
```

- Si vous avez migré le système de fichiers `/store/ariel`, entrez la commande suivante :

```
umount /store/ariel
```

4. Montez le volume iSCSI.
   - Si vous avez migré le système de fichiers `/store`, entrez les commandes suivantes :

```
mount /store
```

   - Si vous avez migré le système de fichiers `/store/ariel`, entrez la commande suivante :

```
mount /store/ariel
```

5. Testez les points de montage.
   - Si vous avez migré le système de fichiers `/store`, entrez la commande suivante :

```
touch /store/filename.txt
```

   - Si vous avez migré le système de fichiers `/store/ariel`, entrez la commande suivante :

```
mount /store/ariel/filename.txt
```

   Si vous continuez à recevoir un message d'erreur en lecture seule après avoir renvoyé le disque, reconfigurez votre volume iSCSI.

   Vous pouvez également démonter le système de fichiers et exécuter une vérification manuelle du système de fichiers à l'aide de la commande suivante : `fsck /dev/`*`partition`*.
6. Démarrez les services QRadar .

Tâches associées

Configuration des volumes iSCSI

Vous pouvez configurer iSCSI pour un QRadar Console autonome ou un QRadar Console qui est l'hôte primaire à haute disponibilité (HA) dans un déploiement à haute disponibilité.

Interfaces réseau secondaires

Vous pouvez configurer une interface réseau secondaire avec une adresse IP privée pour vous connecter à un réseau de stockage iSCSI (SAN).

Vous utilisez une interface réseau secondaire pour améliorer les performances. Si vous configurez une interface réseau secondaire, vous devez fournir des informations d'adresse à partir de votre gestionnaire de réseau SAN. Pour plus d'informations sur la configuration d'une interface réseau, voir "Gestion de l'interface réseau" dans *IBM QRadar Administration Guide*.

Systèmes à haute disponibilité dans les déploiements iSCSI

Pour un accès dédié au réseau de stockage iSCSI, utilisez l'ordre suivant pour configurer la haute disponibilité (HA), iSCSI et une interface réseau :

__ 1. Configurez les dispositifs primaires et secondaires.

__ 2. Configurez le stockage iSCSI externe sur les deux hôtes.

__ 3. Configurez la haute disponibilité sur les hôtes primaires et secondaires.

__ 4. Configurez le contrôle des interfaces secondaires pour vos appareils à haute disponibilité.

Le processus de haute disponibilité pour IBM QRadar contrôle toutes les interfaces réseau. Lorsqu'un dispositif de haute disponibilité est en mode actif, le processus à haute disponibilité active les interfaces. Lorsque la haute disponibilité est en mode veille, le processus de haute disponibilité désactive les

interfaces. Si l'interface réseau dédiée à la mémoire est désactivée et que le système à haute disponibilité passe en ligne de secours, l'hôte de secours tente de passer en mode actif. Si le système à haute disponibilité est en mode veille, vous ne pouvez pas accéder au système de stockage iSCSI. Les problèmes d'accès sont causés lors de la transition du nœud à haute disponibilité de veille à actif. Le processus de haute disponibilité met en ligne l'interface secondaire, mais lorsque le système iSCSI est monté, le réseau n'est pas disponible et le processus de bascule échoue. L'hôte à haute disponibilité en veille ne peut pas passer en mode actif.

Pour résoudre ce problème, vous devez supprimer le contrôle de l'interface réseau iSCSI du système à haute disponibilité pour vous assurer que l'interface réseau est toujours active. Supprimez toutes les dépendances que l'interface réseau a sur le statut du nœud haute disponibilité. Les hôtes primaires et secondaires à haute disponibilité doivent posséder des adresses IP uniques sur ces interfaces réseau secondaires.

Tâches associées

Configuration du contrôle des interfaces secondaires dans les déploiements à haute disponibilité
Si vous utilisez iSCSI et une interface réseau dédiée dans un déploiement à haute disponibilité (HA), vous devez vous assurer que l'interface secondaire n'est pas gérée par le processus HA. Configurez la gestion de l'interface secondaire pour vous assurer que si une reprise en ligne sur l'hôte secondaire à haute disponibilité se produit, l'interface reste toujours active.

Configuration du contrôle des interfaces secondaires dans les déploiements à haute disponibilité

Si vous utilisez iSCSI et une interface réseau dédiée dans un déploiement à haute disponibilité (HA), vous devez vous assurer que l'interface secondaire n'est pas gérée par le processus HA. Configurez la gestion de l'interface secondaire pour vous assurer que si une reprise en ligne sur l'hôte secondaire à haute disponibilité se produit, l'interface reste toujours active.

Avant de commencer

Assurez-vous que les conditions suivantes sont remplies :

- Séparez les adresses IP de l'interface réseau iSCSI dédiée sur chacun des serveurs HA. Les adresses IP doivent être sur des réseaux différents.

  Des adresses IP distinctes empêchent les conflits d'adresses IP lorsque les interfaces réseau sont actives sur les deux hôtes HA en même temps. Le logiciel et les pilotes iSCSI peuvent accéder au stockage externe au démarrage et pendant la reprise en ligne à haute disponibilité. De plus, le volume externe peut être monté avec succès lorsque le nœud HA passe de veille à actif.

  Pour plus d'informations sur la configuration des interfaces réseau, voir "Configuration des interfaces réseau" dans *IBM QRadar Administration Guide*.
- Les dispositifs primaires et secondaires sont configurés.

  Pour plus d'informations, voir *IBM QRadar High Availability Guide*.
- La mémoire iSCSI est configurée.
- NetworkManager est désactivé en tapant la commande suivante.

```
systemctl status NetworkManager
```

Procédure

1. Sur l'hôte principal, utilisez Secure Shell pour vous connecter à QRadar Console en tant que superutilisateur.
2. Désactivez le contrôle de service QRadar HA de l'interface réseau.
   a) Accédez au répertoire `/opt/qradar/ha/interfaces/`

Le répertoire contient une liste de fichiers dont le nom commence par `ifcfg-`. Un fichier existe pour chaque interface contrôlée par les processus QRadar HA.

b) Supprimez le fichier utilisé pour accéder à votre réseau de stockage iSCSI.

La suppression du fichier supprime le contrôle de l'interface des processus HA.

3. Réactivez le contrôle au niveau du système d'exploitation des interfaces réseau.
   a) Accédez au répertoire `/etc/sysconfig/network-scripts`.
   b) Ouvrez le fichier `ifcfg-` de l'interface qui se connecte à votre réseau iSCSI.
   c) Pour vous assurer que l'interface réseau est toujours active, remplacez la valeur du paramètre ONBOOT par `ONBOOT=yes`.
4. Pour redémarrer les services iSCSI, entrez la commande suivante :

```
systemctl restart iscsi
```

5. Répétez ces étapes pour le dispositif secondaire à haute disponibilité.
6. Pour tester l'accès à votre stockage iSCSI à partir de votre dispositif secondaire, utilisez la commande ping :

```
ping <iscsi_server_ip_address>
```

Concepts associés

Interfaces réseau secondaires

Vous pouvez configurer une interface réseau secondaire avec une adresse IP privée pour vous connecter à un réseau de stockage iSCSI (SAN).

Chapitre 3. Stockage sur le canal optique

Vous pouvez configurer le canal optique (FC) dans un déploiement QRadar standard ou dans un environnement à haute disponibilité (HA). Vous pouvez également configurer le multi-accès FC pour fournir une redondance si votre commutateur FC échoue.

Lorsque vous configurez un dispositif FC, vous pouvez déplacer les données IBM QRadar dans votre système de fichiers `/store` ou `/store/ariel`. Ensuite, montez le système de fichiers `/store` ou `/store/ariel` sur une partition sur le dispositif FC.

Les données fréquemment recherchées doivent être déplacées vers un disque plus rapide. Par exemple, déplacer les données récentes ou les données utilisées pour les enquêtes sur les incidents de sécurité. Toutefois, le déploiement d'un stockage externe sur disque à haute performance peut être coûteux. Dans la mesure du possible, utilisez des performances inférieures et un stockage externe moins coûteux pour les activités telles que le déplacement de données plus anciennes, l'archivage ou à des fins de production de rapports.

Si vous utilisez FC uniquement à des fins d'archivage, utilisez le même point de montage pour chaque appliance et configurez ces points de montage pour qu'ils correspondent à chaque volume FC unique.

Dans les déploiements utilisant plusieurs appliances, vérifiez que chaque appliance est configurée pour utiliser un volume FC distinct. Si vous n'utilisez pas de volumes distincts, deux unités peuvent monter la même unité par bloc, ce qui peut endommager le système de fichiers de l'unité par bloc.

Selon la configuration de votre unité, vous devrez peut-être créer une partition sur le volume de votre disque FC.

La configuration du canal optique (FC) est différente pour un hôte primaire à haute disponibilité (HA) que pour l'hôte secondaire à haute disponibilité. Pour configurer FC, vous devez vous assurer que l'hôte primaire à haute disponibilité et l'hôte secondaire à haute disponibilité ne sont pas connectés dans un cluster à haute disponibilité.

Configuration du canal optique dans les déploiements QRadar standard

Pour déplacer des données d'une console QRadar ou d'un hôte géré vers un périphérique de stockage FC :

- Suivez les instructions dans «Vérification de l'installation de l'adaptateur Emulex», à la page 20.
- Suivez les instructions dans «Vérification des connexions de canal optique», à la page 21.
- Faites migrer le système de fichiers vers un dispositif FC :
  - «Déplacement du système de fichiers /magasin vers une solution de canal optique», à la page 22.
  - «Déplacement du système de fichiers /store/ariel vers une solution de canal optique», à la page 24.

Configuration du canal optique multi-accès dans les déploiements QRadar standard

Pour déplacer des données à partir d'une console QRadar ou d'un hôte géré vers plusieurs unités d'archivage FC :

- Suivez les instructions dans «Vérification de l'installation de l'adaptateur Emulex», à la page 20.
- Suivez les instructions dans «Vérification des connexions de canal optique», à la page 21.
- Suivez les instructions dans «Déplacement du système de fichiers /store vers une solution de canal optique multi-accès», à la page 25.

Configuration du canal optique dans les déploiements à haute disponibilité

Pour déplacer des données dans un déploiement à haute disponibilité vers un périphérique de stockage FC:

- Suivez les instructions dans «Vérification de l'installation de l'adaptateur Emulex», à la page 20.

- Suivez les instructions dans «Vérification des connexions de canal optique», à la page 21.
- Faites migrer le système de fichiers vers un dispositif FC :
  - «Déplacement du système de fichiers /magasin vers une solution de canal optique», à la page 22.
  - «Déplacement du système de fichiers /store/ariel vers une solution de canal optique», à la page 24
- Suivez les instructions de «Configuration du point de montage pour l'hôte secondaire à haute disponibilité», à la page 27 sur le dispositif secondaire.

Si vous configurez FC dans un déploiement à haute disponibilité et que votre hôte primaire à haute disponibilité échoue, votre dispositif FC peut être utilisé pour maintenir la cohérence de données avec votre hôte secondaire à haute disponibilité. Pour plus d'informations sur la cohérence de données et le stockage partagé dans un environnement à haute disponibilité, voir *IBM QRadar High Availability Guide*.

Configuration du canal optique multi-accès dans les déploiements à haute disponibilité

Pour déplacer des données dans un déploiement à haute disponibilité vers de multiples dispositifs de stockage FC :

- Suivez les instructions dans «Vérification de l'installation de l'adaptateur Emulex», à la page 20.
- Suivez les instructions dans «Vérification des connexions de canal optique», à la page 21.
- Suivez les instructions dans «Déplacement du système de fichiers /store vers une solution de canal optique multi-accès dans un déploiement à haute disponibilité», à la page 27.

Vérification de l'installation de l'adaptateur Emulex

Vous devez vérifier qu'un adaptateur de bus hôte Emulex LPe12002 ou LPe16002B est connecté et installé avec les versions de microprogramme et de pilote correctes.

Avant de commencer

Pour utiliser le protocole de canal optique, vous devez installer un adaptateur de bus hôte Emulex LPe12002 ou LPe16002B sur votre appliance IBM QRadar. Dans un déploiement à haute disponibilité (HA), vous devez installer une carte Emulex LPe12002 ou LPe16002B sur l'hôte primaire et secondaire à haute disponibilité.

L'adaptateur de bus hôte Emulex LPe doit utiliser les versions de pilote et de microprogramme suivantes, ou plus récentes :

- Version de pilote : 8.3.5.68.5p
- Version de microprogramme : 1.10A5(U3D1.10A5), sli-3

Procédure

1. A l'aide de Secure Shell, connectez-vous à votre hôte QRadar en tant que superutilisateur :
2. Vérifiez qu'une carte Emulex LPe12002 ou LPe16002B est associée en entrant la commande suivante :

   ```
   hbacmd listhbas
   ```

   Si aucun résultat n'est affiché, contactez votre administrateur système.
3. Vérifiez que la carte Emulex utilise les versions de microprogramme et de pilote correctes en entrant la commande suivante :

   ```
   hbacmd HBAAttrib <device_id>
   ```

   device_id est le port WWN qui s'affiche à l'étape précédente.

Que faire ensuite

«Vérification des connexions de canal optique», à la page 21

Vérification des connexions de canal optique

Vous devez identifier le volume de disque sur le dispositif de canal optique externe. Si nécessaire, vous devez également créer une partition sur le volume.

Avant de commencer

Vérifiez l'installation de l'adaptateur Emulex.

Procédure

1. Reliez les deux câbles de canal optique à l'adaptateur de bus hôte Emulex LPe12002 ou LPe16002B sur votre appliance QRadar Console.
2. À l'aide de SSH, connectez-vous à votre QRadar Console en tant que superutilisateur.
3. Identifiez le volume de canal optique en entrant la commande suivante :

   ```
   ls -l /dev/disk/by-path/*-fc-*
   ```

   Si plusieurs dispositifs de canal optique sont connectés et que vous ne pouvez pas identifier le volume de canal optique correct, contactez votre administrateur système.
4. S'il n'y a pas de partition sur le volume de canal optique, créez une partition sur le volume du dispositif de canal optique.

   Remarque : QRadar ne prend pas en charge la création d'une partition sur une unité de gestionnaire de volume logique (LVM). Le système de fichiers ne parvient pas à monter au cours d'un amorçage du système lorsqu'une partition est créée sur une unité LVM.

   a) Pour créer une partition, utilisez la commande GNU parted :

   ```
   parted /dev/<volume>
   ```

   b) Configurez le libellé de partition pour utiliser GPT en entrant la commande suivante :

   ```
   mklabel gpt
   ```

   c) Si le message suivant s'affiche, entrez `Oui`.

   ```
   Avertissement : le label de disque existant sur /dev/<volume> sera
   détruit et toutes les données sur ce disque seront perdues. Voulez-vous
   continuer ?
   ```

   d) Pour créer la partition, entrez la commande suivante :

   ```
   mkpart primary 0% 100%
   ```

   e) Définissez les unités par défaut sur téraoctet en entrant la commande suivante :

   ```
   unit TB
   ```

   f) Vérifiez que la partition est créée en entrant la commande suivante :

   ```
   print
   ```

   g) Quittez GNU parted en entrant la commande suivante :

   ```
   quit
   ```

   h) Mettez à jour le noyau avec les nouvelles données de partition en entrant la commande suivante :

   ```
   partprobe /dev/<volume>
   ```

Vous pouvez être invité à redémarrer l'appliance.

i) Pour vérifier que la partition est créée, entrez la commande suivante :

```
cat /proc/partitions
```

5. Reformater la partition et créer un système de fichiers.
   - Pour créer un système de fichiers XFS, entrez la commande suivante :

     ```
     mkfs.xfs -f /dev/<partition>
     ```

   - Pour créer un système de fichiers ext4, entrez la commande suivante :

     ```
     mkfs.ext4 -f /dev/<partition>
     ```

   - Pour créer un système de fichiers XFS pour le canal optique multi-accès, entrez la commande suivante :

     ```
     mkfs.xfs -f -L multiPath /dev/<partition>
     ```

   - Pour créer un système de fichiers ext4 pour le canal optique multi-accès, entrez la commande suivante :

     ```
     mkfs.ext4 -f -L multiPath /dev/<partition>
     ```

Que faire ensuite

Si vous déplacez le système de fichiers `/store` vers une solution de canal optique accédez à «Déplacement du système de fichiers /magasin vers une solution de canal optique», à la page 22.

Si vous déplacez le système de fichiers `/store/ariel` vers une solution de canal optique accédez à «Déplacement du système de fichiers /store/ariel vers une solution de canal optique», à la page 24.

Si vous déplacez le système de fichiers `/store` vers une solution de canal optique multi-accès, accédez à «Déplacement du système de fichiers /store vers une solution de canal optique multi-accès», à la page 25.

Si vous déplacez le système de fichiers `/store` vers une solution de canal optique multi-accès dans un déploiement à haute disponibilité, accédez à «Déplacement du système de fichiers /store vers une solution de canal optique multi-accès dans un déploiement à haute disponibilité», à la page 27.

Déplacement du système de fichiers /magasin vers une solution de canal optique

Vous pouvez déplacer les données IBM QRadar qui sont gérées dans le système de fichiers `/store` et monter le système de fichiers `/store` sur une partition de dispositif de canal optique (FC).

Avant de commencer

«Vérification des connexions de canal optique», à la page 21

Procédure

1. Après l'installation de QRadar, connectez QRadar à un canal optique et redémarrez.
2. Arrêtez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl stop hostcontext
systemctl stop ecs-ec-ingress
systemctl stop tomcat
systemctl stop hostservices
systemctl stop systemStabMon
systemctl stop crond
```

3. Démontez les systèmes de fichiers en tapant les commandes suivantes :

```
umount /store
```

   Le système de fichiers `/transient` est monté uniquement lorsque `/store file system` est XFS.
4. Créez le répertoire `/store_old` en entrant la commande suivante :

```
mkdir /store_old
```

5. Calculer l'identificateur unique universel (UUID) de la partition de dispositif en entrant la commande suivante :

```
blkid /dev/partition
```

6. Editez le fichier `/etc/fstab` pour mettre à jour le point de montage du système de fichiers `/store` existant sur `/store_old`.
7. Ajoutez un point de montage pour le système de fichiers `/store` en ajoutant le texte suivant au fichier `/etc/fstab` :
   - Si le système de fichiers est XFS et que vous n'utilisez pas la haute disponibilité, ajoutez le texte suivant :

     ```
     UUID=uuid /store xfs inode64,logbsize=256k,noatime,nobarrier 0 0
     ```

   - Si le système de fichiers est XFS et que vous utilisez la haute disponibilité, ajoutez le texte suivant :

     ```
     UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
     ```

   - Si le système de fichiers est ext4 et que vous n'utilisez pas la haute disponibilité, ajoutez le texte suivant :

     ```
     UUID=uuid /store ext4 noatime,nobarrier 0 0
     ```

   - Si le système de fichiers est ext4 et que vous utilisez la haute disponibilité, ajoutez le texte suivant :

     ```
     UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
     ```

   Sauvegardez le fichier et fermez-le.
8. Montez le système de fichiers `/store` sur la partition de dispositif FC en entrant la commande suivante :

```
mount /store
```

9. Montez le système de fichiers `/store_old` sur le disque local en entrant la commande suivante :

```
mount /store_old
```

10. Copiez les données dans la partition de canal optique en entrant la commande suivante :

```
cp -af /store_old/* /store
```

11. Démontez `/store_old` en entrant la commande suivante :

```
umount /store_old
```

12. Supprimez le répertoire `/store_old` en entrant la commande suivante :

```
rmdir /store_old
```

13. Éditez le fichier `/etc/fstab` pour supprimer l'entrée du point de montage `/store_old`.
14. Démarrez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl start crond
systemctl start systemStabMon
systemctl start hostservices
systemctl start tomcat
systemctl start ecs-ec-ingress
systemctl start hostcontext
```

15. Supprimez la copie locale de /store du gestionnaire de volume logique (LVM) en entrant la commande suivante :

```
lvchange -an /dev/storerhel/store 2>/dev/null
lvrename /dev/storerhel/store /dev/storerhel/storeold 2>/dev/null
```

16. Vérifiez le point de montage du canal optique en entrant la commande suivante :

```
df -h
```

Déplacement du système de fichiers `/store/ariel` vers une solution de canal optique

Vous pouvez déplacer les données IBM QRadar qui sont gérées dans le système de fichiers `/store/ariel` et monter le système de fichiers `/store/ariel` sur une partition de dispositif de canal optique (FC).

Avant de commencer

Voir «Vérification des connexions de canal optique», à la page 21.

Procédure

1. Connectez QRadar au canal optique et redémarrez.
2. Arrêtez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl stop systemStabMon
systemctl stop hostcontext
systemctl stop ecs-ec-ingress
systemctl stop tomcat
systemctl stop hostservices
systemctl stop crond
```

3. Créez un répertoire temporaire en entrant la commande suivante :

   `mkdir /tmp/fcdata`

4. Montez la partition de stockage de canal optique dans le répertoire temporaire en entrant la commande suivante, où *<partition>* est le nom de la partition du dispositif :

```
mount /dev/<partition> /tmp/fcdata
```

5. Copiez les données dans le dispositif Canal optique en entrant la commande suivante :

```
cp -af /store/ariel/* /tmp/fcdata
```

6. Démontez la partition Canal optique en entrant la commande suivante :

```
umount /tmp/fcdata
```

7. Vérifiez l'identificateur unique universel (UUID) de la partition de dispositif de canal optique en tapant la commande suivante, où *<partition>* est le nom de la partition du dispositif :

```
blkid /dev/<partition>
```

8. Editez le fichier `fstab` en entrant la commande suivante :

```
vi /etc/fstab
```

9. Ajoutez le point de montage du système de fichiers `/store/ariel` en ajoutant le texte suivant, où *<uuid>* est l'UUID de la partition de dispositif de canal optique, dans le fichier `/etc/fstab`.

   Si le système de fichiers est XFS :

   ```
   UUID=<uuid> /store/ariel xfs inode64,logbsize=256k,noatime,nobarrier 0 0
   ```

   Si le système de fichiers est ext4 :

   ```
   UUID=<uuid> /store/ariel ext4 defaults,noatime,nobarrier 0 0
   ```

10. Sauvegardez le fichier et fermez-le.
11. Montez le système de fichiers `/store/ariel` sur la partition de dispositif FC en entrant la commande suivante :

    ```
    mount /store/ariel
    ```

12. Démarrez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

    ```
    systemctl start crond
    systemctl start hostservices
    systemctl start tomcat
    systemctl start ecs-ec-ingress
    systemctl start hostcontext
    systemctl start systemStabMon
    ```

13. Vérifiez le point de montage du canal optique en entrant la commande suivante :

    ```
    df -h
    ```

Déplacement du système de fichiers /store vers une solution de canal optique multi-accès

Dans IBM QRadar, vous pouvez implémenter le canal optique multi-accès. Si vous avez un problème de réseau de stockage SAN ou de commutateur de réseau de stockage, le multi-accès fournit une redondance supplémentaire pour éviter toute perturbation des données de flux et d'événements.

Avant de commencer

Vérifiez que vous avez effectué les tâches suivantes :

- Vérification de l'installation de l'adaptateur Emulex.
- Vérification des connexions de canal optique.

Procédure

1. Connectez-vous à QRadar Console en tant que superutilisateur à l'aide de Secure Shell.
2. Identifiez une partition SAN (réseau de stockage SAN) en entrant la commande suivante :

   ```
   blkid -o list
   ```

3. Arrêtez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

   ```
   systemctl stop systemStabMon
   systemctl stop hostcontext
   systemctl stop ecs-ec-ingress
   systemctl stop tomcat
   systemctl stop imq
   systemctl stop hostservices
   systemctl stop crond
   ```

4. Démontez les systèmes de fichiers en tapant les commandes suivantes :

   ```
   umount /store
   ```

5. Créez un répertoire /store_old en entrant la commande suivante :

```
mkdir /store_old
```

6. Déterminez l'identificateur unique universel (UUID) de la partition de dispositif en entrant la commande suivante :

```
blkid /dev/<partition>
```

7. Éditez le fichier /etc/fstab.
   a) Remplacez le point de montage /store par /store_old.
   b) Ajoutez le nouveau point de montage /store .

   Si le système de fichiers est XFS et que vous n'utilisez pas la haute disponibilité, ajoutez le texte suivant :

   ```
   UUID=<uuid> /store xfs inode64,logbsize=256k,noatime,nobarrier 0 0
   ```

   Si le système de fichiers est XFS et que vous utilisez la haute disponibilité, ajoutez le texte suivant :

   ```
   UUID=<uuid> /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
   ```

   Si le système de fichiers est ext4 et que vous n'utilisez pas la haute disponibilité, ajoutez le texte suivant :

   ```
   UUID=<uuid> /store ext4 noatime,nobarrier 0 0
   ```

   Si le système de fichiers est ext4 et que vous utilisez la haute disponibilité, ajoutez le texte suivant :

   ```
   UUID=<uuid> /store ext4 noatime,noauto,nobarrier 0 0
   ```

8. Montez les systèmes de fichiers et copiez les données sur votre périphérique en tapant les commandes suivantes :

```
mount /store
mount /store_old
cp -af /store_old/* /store
umount /store_old
```

9. Démarrez les services QRadar en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl start crond
systemctl start hostservices
systemctl start imq
systemctl start tomcat
systemctl start ecs-ec-ingress
systemctl start hostcontext
systemctl start systemStabMon
```

10. Activez le multi-accès de canal optique en entrant la commande suivante :

```
mpathconf --enable
```

11. Supprimez la copie locale de /store en entrant la commande suivante :

```
lvchange -an /dev/storerhel/store 2>/dev/null
lvrename /dev/storerhel/store /dev/storerhel/storeold 2>/dev/null
```

12. Éditez le fichier /etc/fstab pour supprimer l'entrée du point de montage /store_old.

Déplacement du système de fichiers /store vers une solution de canal optique multi-accès dans un déploiement à haute disponibilité

Pour utiliser le stockage de canal optique multi-accès dans un environnement à haute disponibilité (HA), vous devez configurer l'hôte primaire et l'hôte secondaire à haute disponibilité pour utiliser la même partition de stockage.

Pourquoi et quand exécuter cette tâche

Important :

- Vous devez configurer le multi-accès sur les dispositifs primaire et secondaire à haute disponibilité avant de lancer la synchronisation des hautes disponibilités.
- Avant d'ajouter une haute disponibilité à une configuration de canal optique, vérifiez que `/store/backup` est local. Créez des liens vers `/store/backup` uniquement après l'ajout de la haute disponibilité.

Procédure

1. Vérifiez que le matériel de canal optique correct est installé sur votre appliance secondaire à haute disponibilité. Pour plus d'informations, voir «Vérification de l'installation de l'adaptateur Emulex», à la page 20
2. Vérifiez les connexions de canal optique à haute disponibilité. Pour plus d'informations, voir «Vérification des connexions de canal optique», à la page 21
3. Configurez le canal optique sur votre appliance primaire à haute disponibilité. Pour plus d'informations, «Déplacement du système de fichiers /store vers une solution de canal optique multi-accès», à la page 25
4. Configurez le point de montage du système de fichiers pour l'hôte secondaire à haute disponibilité. Pour plus d'informations, voir «Configuration du point de montage pour l'hôte secondaire à haute disponibilité», à la page 27.

Configuration du point de montage pour l'hôte secondaire à haute disponibilité

Vous devez configurer le point de montage sur l'hôte secondaire à haute disponibilité (HA) pour le système de fichiers qui est déplacé vers un périphérique de stockage de canal optique.

Procédure

1. A l'aide de Secure Shell, connectez-vous à l'hôte secondaire à haute disponibilité en tant que superutilisateur.
2. Calculer l'UUID en entrant la commande suivante :

   `blkid /dev/<partition>`
3. Mettez à jour le noyau avec les données de partition de canal optique en entrant la commande suivante :

   ```
   partprobe
   ```

   Traitement des incidents : Si un message d'erreur d'avertissement s'affiche que le noyau ne peut pas lire la table de partition, entrez la commande suivante : `ls -l /dev/disk/by-uuid/<UUID>`. Si aucune sortie n'est affichée, redémarrez l'hôte HA secondaire en entrant `reboot`.
4. Si vous déplacez le répertoire `/store`, démontez les systèmes de fichiers en entrant la commande suivante :

```
umount /store
```

Le système de fichiers /transient est monté uniquement lorsque le système de fichiers /store est XFS.

5. Si vous avez redirigé le système de fichiers /store vers un dispositif externe, choisissez l'une des options suivantes pour éditer le fichier /etc/fstab.
   - Si le système de fichiers /store est un système de fichiers XFS, mettez à jour les lignes suivantes. Pour chaque ligne, copiez le texte dans un éditeur de texte, supprimez les sauts de ligne et collez en une seule ligne.

     ```
     UUID=<uuid> /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
     ```

   - Si le système de fichiers /store est ext4, mettez à jour la ligne suivante :

     ```
     UUID=<uuid> /store ext4 defaults,noatime,noauto,nobarrier 0 0
     ```

6. Si vous déplacez le système de fichiers /store/ariel vers un dispositif externe, choisissez l'une des options suivantes pour éditer le fichier /etc/fstab.
   - Si le système de fichiers /store/ariel est un système de fichiers XFS, mettez à jour les lignes suivantes. Pour chaque ligne, copiez le texte dans un éditeur de texte, supprimez les sauts de ligne et collez en une seule ligne.

     ```
     UUID=<uuid> /store/ariel xfs inode64,logbsize=256k,noatime,
     noauto,nobarrier 0 0
     ```

   - Si le système de fichiers /store/ariel est ext4, mettez à jour la ligne suivante :

     ```
     UUID=<uuid> /store/ariel ext4 defaults,noatime,noauto,nobarrier 0 0
     ```

7. Si vous déplacez le système de fichiers /store, supprimez la copie locale de /store en entrant la commande suivante :

```
lvchange -an /dev/storerhel/store 2>/dev/null
lvrename /dev/storerhel/store /dev/storerhel/storeold 2>/dev/null
```

Que faire ensuite

Créez un cluster à haute disponibilité. Pour plus d'informations, voir *IBM QRadar High Availability Guide*.

Suppression de la haute disponibilité d'une solution de canal optique

Supprimez la valeur 'noauto' de l'entrée du point de montage /store dans /etc/fstab avant de supprimer la haute disponibilité.

Procédure

1. Editez le fichier /etc/fstab pour supprimer la valeur 'noauto' de l'entrée du point de montage /store .
   - Si le système de fichiers est XFS, l'entrée du point de montage doit avoir le texte suivant :

     ```
     UUID=uuid /store xfs inode64,logbsize=256k,noatime,nobarrier 0 0
     ```

   - Si le système de fichiers est ext4, l'entrée du point de montage doit avoir le texte suivant :

     ```
     UUID=uuid /store ext4 noatime,nobarrier 0 0
     ```

   Sauvegardez le fichier et fermez-le.
2. Connectez-vous à l'interface utilisateur QRadar.

3. Cliquez sur **Admin**.
4. Cliquez sur l'icône **Gestion du système et de la licence**.
5. Sélectionnez l'hôte à haute disponibilité vous souhaitez supprimer.
6. Dans la barre d'outils, sélectionnez **Haute disponibilité** > **Retrait de l'hôte à haute disponibilité**.
7. Cliquez sur **OK**.

   Remarque : Lorsque vous supprimez un hôte à haute disponibilité d'un cluster, l'hôte redémarre.

Chapitre 4. Dispositif de stockage externe de serveur de fichiers réseau

Vous pouvez sauvegarder les données IBM QRadar sur un système NFS (Network File System) externe.

Avertissement :

Si vous utilisez un serveur de fichiers réseau ou un partage Windows pour le stockage externe, votre système peut verrouiller et provoquer une indisponibilité. Cette pratique n'est pas prise en charge par IBM QRadar.

Si vous choisissez d'utiliser NFS de toute façon, NFS ne peut être utilisé que pour les données de sauvegarde quotidiennes, telles que le répertoire `/store/backup`. Vous ne pouvez pas utiliser NFS pour stocker des données actives, qui incluent les bases de données PostgreSQL et ariel. Si vous utilisez NFS, cela peut entraîner des problèmes de corruption ou de performances de la base de documents.

Stockage de serveur de fichiers réseau avec un QRadar Console autonome

Pour déplacer des fichiers de sauvegarde vers le serveur de fichiers réseau à partir d'un QRadar Consoleautonome, suivez les instructions fournies dans «Déplacement de sauvegardes vers un serveur de fichiers réseau», à la page 31.

Stockage dans un serveur de fichiers réseau avec un nouveau déploiement à haute disponibilité

Pour déplacer des fichiers de sauvegarde vers le serveur de fichiers réseau pour un nouveau déploiement à haute disponibilité :

- Suivez les instructions de «Déplacement de sauvegardes vers un serveur de fichiers réseau», à la page 31 pour votre appliance primaire à haute disponibilité.
- Suivez les instructions de «Configuration d'un point de montage pour un hôte secondaire à haute disponibilité», à la page 33 pour votre appliance secondaire à haute disponibilité.
- Créez un cluster à haute disponibilité. Pour plus d'informations, voir *IBM QRadar High Availability Guide*.

Stockage sur un serveur de fichiers réseau avec un déploiement à haute disponibilité existant

Pour déplacer des fichiers de sauvegarde à partir d'un déploiement à haute disponibilité existant, suivez les instructions fournies dans «Configuration de la sauvegarde NFS sur un cluster à haute disponibilité existant», à la page 34.

Déplacement de sauvegardes vers un serveur de fichiers réseau

Vous pouvez configurer le système NFS (Network File System ou Serveur de fichiers réseau) pour une appliance QRadar autonome, ou une appliance QRadar que vous utilisez comme hôte principal dans un déploiement à haute disponibilité.

Avant de commencer

Vous devez vous assurer que le dispositif QRadar peut accéder au serveur NFS.

Important :

Conservez une copie locale (backup.nfs) de votre sauvegarde sur votre système de sorte que, si le montage NFS échoue, les sauvegardes soient toujours disponibles. Surveillez le répertoire qui contient les

sauvegardes locales avec soin pour vous assurer que le répertoire que vous utilisez pour conserver vos sauvegardes ne cause pas de problèmes de stockage sur disque.

Pourquoi et quand exécuter cette tâche

Avertissement :

Si vous utilisez un serveur de fichiers réseau ou un partage Windows pour le stockage externe, votre système peut verrouiller et provoquer une indisponibilité. Cette pratique n'est pas prise en charge par IBM QRadar.

Même si le risque est faible avec un système d'exploitation Linux , le rançonlogiciel peut chiffrer toutes les unités distantes. Si vous utilisez un montage NFS, vous pouvez réduire votre risque en installant uniquement l'unité NFS pendant que vous copiez des données à partir d'une unité locale vers l'unité montée NFS. Retirez ensuite l'unité montée NFS pour les opérations quotidiennes.

Si vous choisissez d'utiliser NFS de toute façon, NFS ne peut être utilisé que pour les données de sauvegarde quotidiennes, telles que le répertoire `/store/backup`. Vous ne pouvez pas utiliser NFS pour stocker des données actives, qui incluent les bases de données PostgreSQL et ariel. Si vous utilisez NFS, cela peut entraîner des problèmes de corruption ou de performances de la base de documents.

Procédure

1. Exécutez des sauvegardes nocturnes sur l'unité locale, /store/backup.
2. Utilisez Secure Shell pour vous connecter à l'hôte QRadar en tant que superutilisateur.
3. Démarrez les services NFS en entrant les commandes suivantes :

```
systemctl enable rpcbind
systemctl start rpcbind
```

4. Ajoutez la ligne suivante au fichier `/etc/fstab`.

```
nfsserver:/nfs/export/path /store/backup nfs rw,soft,intr,noac 0 0
```

   Vous devrez peut-être ajuster les paramètres du point de montage NFS pour prendre en charge votre configuration.
5. Déplacez vos fichiers de sauvegarde du répertoire existant vers un emplacement temporaire en tapant les commandes suivantes :

```
cd /store/
mv backup backup.local
```

6. Créez un nouveau répertoire de sauvegarde en entrant la commande suivante :

```
mkdir /store/backup
```

7. Définissez les droits d'accès au volume NFS en entrant la commande suivante :

```
chown nobody:nobody /store/backup
```

8. Montez le volume NFS en entrant la commande suivante :

```
mount /store/backup
```

   L'utilisateur root doit disposer d'un accès en lecture et en écriture au volume NFS monté car le processus `hostcontext` s'exécute en tant qu'utilisateur root.

   Utilisez la copie locale de votre sauvegarde que vous avez créée. Voir Remarque importante.
9. Vérifiez que `/store/backup` est monté en entrant la commande suivante :

```
df -h
```

10. Copiez les fichiers de sauvegarde de l'emplacement temporaire vers le volume NFS en entrant la commande suivante :

```
cp -f /store/backup.local/* /store/backup
```

11. Vérifiez les fichiers en tapant la commande suivante :

```
sha256sum /store/backup.local/* > backuplocal.sha256.txt
sha256sum /store/backup.nfs/* > backupnfs.sha256.txt
diff backuplocal.sha256.txt backupnfs.sha256.txt
```

    Si vous voyez des différences entre les fichiers, arrêtez et déterminez la raison. Une raison peut être que votre copie a rempli la partition cible, ou une autre raison peut être qu'il y a eu une indisponibilité du réseau pendant la procédure de copie.

12. Une fois que vous avez vérifié que la procédure de copie a abouti, supprimez le répertoire `backup.local` en entrant les commandes suivantes :

```
cd /store
rm -r backup.local
```

    Lorsque vous supprimez le répertoire `backup.local`, vous empêchez le remplissage de la partition locale.

Que faire ensuite

Si vous configurez le serveur de fichiers réseau pour un nouveau déploiement à haute disponibilité, suivez les instructions de «Configuration d'un point de montage pour un hôte secondaire à haute disponibilité», à la page 33 pour votre appliance de haute disponibilité secondaire.

Configuration d'un point de montage pour un hôte secondaire à haute disponibilité

Sur votre hôte secondaire à haute disponibilité (HA) existant, vous devez configurer un point de montage NFS pour l'emplacement du fichier de sauvegarde IBM QRadar de remplacement.

Avant de commencer

Vérifiez que l'hôte secondaire HA peut se connecter au serveur NFS.

Pourquoi et quand exécuter cette tâche

Avertissement :

Si vous utilisez un serveur de fichiers réseau ou un partage Windows pour le stockage externe, votre système peut verrouiller et provoquer une indisponibilité. Cette pratique n'est pas prise en charge par IBM QRadar.

Si vous choisissez d'utiliser NFS de toute façon, NFS ne peut être utilisé que pour les données de sauvegarde quotidiennes, telles que le répertoire `/store/backup`. Vous ne pouvez pas utiliser NFS pour stocker des données actives, qui incluent les bases de données PostgreSQL et ariel. Si vous utilisez NFS, cela peut entraîner des problèmes de corruption ou de performances de la base de documents.

Procédure

1. A l'aide de Secure Shell, connectez-vous à l'hôte secondaire HA QRadar en tant que superutilisateur :
2. Créez un emplacement de fichier de sauvegarde qui correspond à l'emplacement du fichier de sauvegarde sur votre hôte primaire à haute disponibilité. L'emplacement par défaut des sauvegardes QRadar est `/store/backup`.

Pour plus d'informations, voir «Configuration de la sauvegarde NFS sur un cluster à haute disponibilité existant», à la page 34.

Restriction : Ne créez pas votre nouvel emplacement de sauvegarde sous le système de fichiers `/store`. Utilisez un autre répertoire, tel que `/backup` ou `/nfs`.

3. Démarrez les services NFS en entrant les commandes suivantes :

```
systemctl enable rpcbind
systemctl start rpcbind
```

4. Ajoutez la ligne suivante au fichier `/etc/fstab` :

```
<hostname>:<shared_directory> <backup_location> nfs
rw,soft,intr,clientaddr=<HA_IP_address> 0 0
```

5. Montez le nouvel emplacement du fichier de sauvegarde QRadar en entrant la commande suivante :

```
mount <backup_location>
```

Configuration de la sauvegarde NFS sur un cluster à haute disponibilité existant

Vous pouvez configurer le système NFS (Network File System) pour un cluster à haute disponibilité existant.

Pourquoi et quand exécuter cette tâche

Avertissement :

Si vous utilisez un serveur de fichiers réseau ou un partage Windows pour le stockage externe, votre système peut verrouiller et provoquer une indisponibilité. Cette pratique n'est pas prise en charge par IBM QRadar.

Si vous choisissez d'utiliser NFS de toute façon, NFS ne peut être utilisé que pour les données de sauvegarde quotidiennes, telles que le répertoire `/store/backup`. Vous ne pouvez pas utiliser NFS pour stocker des données actives, qui incluent les bases de données PostgreSQL et ariel. Si vous utilisez NFS, cela peut entraîner des problèmes de corruption ou de performances de la base de documents.

Procédure

1. Utilisez Secure Shell pour vous connecter à l'hôte primaire à haute disponibilité en tant que superutilisateur.
2. Démarrez les services NFS en entrant les commandes suivantes :

```
systemctl enable rpcbind
systemctl start rpcbind
```

3. Ajoutez la ligne suivante au fichier `/opt/qradar/ha/fstab.back`.

```
nfsserver:/nfs/export/path /store/backup nfs rw,soft,intr,noac 0 0
```

Vous devrez peut-être ajuster les paramètres du point de montage NFS pour prendre en charge votre configuration.

4. Ajoutez la même ligne au fichier `/etc/fstab`, précédé de `#HA`.

```
#HA nfsserver:/nfs/export/path /store/backup nfs rw,soft,intr,noac 0 0
```

Vous devrez peut-être ajuster les paramètres du point de montage NFS pour prendre en charge votre configuration.

5. Répétez les étapes 1 à 4 sur l'hôte secondaire à haute disponibilité.

6. Déplacez vos fichiers de sauvegarde du répertoire existant sur l'hôte primaire à haute disponibilité un emplacement temporaire en tapant les commandes suivantes :

```
cd /store/
mv backup backup.local
```

7. Créez un répertoire de sauvegarde sur l'hôte primaire à haute disponibilité en entrant la commande suivante :

```
mkdir /store/backup
```

8. Définissez les droits d'accès au volume NFS sur l'hôte primaire à haute disponibilité en entrant la commande suivante :

```
chown nobody:nobody /store/backup
```

9. Dans le menu de navigation (☰), cliquez sur **Admin**.
10. Cliquez sur **Avancé** > **Déployer la configuration complète**.

    Tous les services redémarrent.
11. Vérifiez que le point de montage `/store/backup` est répertorié dans la sortie de la commande suivante sur les hôtes primaire et secondaire à haute disponibilité :

```
grep MOUNTS /opt/qradar/ha/ha.conf
```

12. Vérifiez que `/store/backup` est monté sur l'hôte primaire à haute disponibilité en entrant la commande suivante :

```
df -h
```

13. Sur l'hôte primaire à haute disponibilité, déplacez les fichiers de sauvegarde de l'emplacement temporaire vers le volume NFS en entrant la commande suivante :

```
mv -f /store/backup.local/* /store/backup
```

14. Supprimez le répertoire `backup.local` en entrant les commandes suivantes :

```
cd /store
rm -rf backup.local
```

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 le fonctionnement d'un produit, d'un programme ou d'un service nonIBM .

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.</lines>
Pour le Canada, veuillez adresser votre courrier à :
<lines>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 sont des marques d'International Business Machines Corp., 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.

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 session 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