IBM Security Access Manager for Web
Version 8.0

Guide d'installation



GC11-6786-02

IBM Security Access Manager for Web
Version 8.0

Guide d'installation



GC11-6786-02

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 441.

Quatrième édition - Avril 2013

Réf. US : GC23-6502-03

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

© Copyright IBM France 2013. Tous droits réservés.

© Copyright IBM Corporation 2001, 2013.

Table des matières

Figures ix

Tableaux xi

Avis aux lecteurs canadiens xiii

A propos de cette publication xv
Public concerné xv
Accès aux publications et à la terminologie xv
Publications connexes xviii
Accessibilité xx
Formation technique xx
Informations relatives au service de support . . . xx

Partie 1. Planification de l'installation 1

Chapitre 1. Présentation de l'installation 3
Planification du déploiement 3
Présentation du domaine sécurisé 4
Composants d'installation de Security Access Manager 4
Security Access Manager - composants de base . . 5
Security Access Manager - Composants de sécurité Web 7
Composants de gestion de sessions distribués Security Access Manager 8
Produits prérequis 9
Registres pris en charge 11
Composants et prérequis pour les système Security Access Manager 13
Security Access Manager - systèmes de base . . 13
Systèmes de sécurité Web Security Access Manager 14
Systèmes de gestion de sessions distribués Security Access Manager 16
Activation de la conformité SSL et TLS 17

Chapitre 2. Méthodes d'installation . . 19

Chapitre 3. Organigramme d'installation 21

Partie 2. Installation de logiciels prérequis 25

Chapitre 4. Plan des installations et configurations prérequises 27
Préparation du système d'exploitation 28
Préparation d'un système AIX 29
Préparation d'un système Linux 30
Préparation d'un système Windows 31
Préparation d'un système Solaris 31
Installation d'IBM Java Runtime 32
AIX : Installation d'IBM Java Runtime 32
Linux : Installation d'IBM Java Runtime 33
Solaris : Installation d'IBM Java Runtime . . . 33
Windows : Installation d'IBM Java Runtime . . 34
Installation d'IBM Global Security Kit (GSKit) . . . 35
AIX : Installation d'IBM Global Security Kit (GSKit) 35
Linux : Installation d'IBM Global Security Kit (GSKit) 36
Solaris : Installation d'IBM Global Security Kit (GSKit) 37
Windows : Installation d'IBM Global Security Kit (GSKit) 37
Installation de la licence IBM Security Access Manager 38
AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager 38
Windows : Installation de la licence IBM Security Access Manager 40
Installation d'IBM Security Utilities 40
AIX : Installation d'IBM Security Utilities . . . 40
Linux : Installation d'IBM Security Utilities . . . 41
Solaris : Installation d'IBM Security Utilities . . 42
Windows : Installation d'IBM Security Utilities 42
Installation du client IBM Tivoli Directory Server . . 43
AIX : Installation du client IBM Tivoli Directory Server 44
Linux : Installation du client IBM Tivoli Directory Server 45
Solaris : Installation du client IBM Tivoli Directory Server 46
Windows : Installation du client IBM Tivoli Directory Server 47
Installation de WebSphere Application Server . . . 47

Chapitre 5. Installation et configuration du serveur de registres d'utilisateurs . 51
Différences entre les registres d'utilisateurs 51
Considérations générales 52
Remarques relatives à LDAP 52
Considérations relatives à URAF 54
Longueur des noms 57
Installation et configuration de Tivoli Directory Server 59
Installation d'IBM Tivoli Directory Server avec l'assistant d'installation Tivoli Directory Server . 60
Configuration de Tivoli Directory Server à l'aide des fichiers scripts 62
Installation de Tivoli Directory Server avec le tableau de bord (Windows uniquement) 69
Configuration d'IBM Tivoli Directory Server pour l'accès SSL 71
Installation et configuration d'IBM Tivoli Directory Server for z/OS 77

© Copyright IBM Corp. 2001, 2013

Mise à jour du fichier schéma 78
Création de suffixe 78
Définitions de suffixe pour Security Access Manager 79
Administration utilisateur de l'authentification native 79
Configuration d'IBM Tivoli Directory Server pour l'accès à z/OS for SSL 81
Installation et configuration de Microsoft Active Directory 83
Installation et configuration de Microsoft Active Directory Lightweight Directory Service (AD LDS) . 85
Installation et configuration d'Active Directory Lightweight Directory Service (ADLDS) pour Security Access Manager 85
Configuration du schéma Security Access Manager pour Active Directory Lightweight Directory Service (AD LDS) 86
Emplacement des données du domaine de gestion pour Active Directory Lightweight Directory Service (AD LDS) 88
Configuration d'une partition de répertoires Security Access Manager 89
Ajout d'un administrateur à la partition des répertoires de métadonnées Security Access Manager 91
Autorisation de liaison anonyme 93
Configuration d'Active Directory Lightweight Directory Service (AD LDS) en vue d'utiliser SSL . 94
Installation et configuration de Novell eDirectory. . 95
Configuration de Novell eDirectory pour Security Access Manager 95
Utilisateurs et groupes dans Novell eDirectory . 98
Emplacement du domaine de gestion. 99
Accès SSL sur le serveur Novell eDirectory . . 100
Installation et configuration de Sun Java System Directory Server 103

Partie 3. Installation du composant système de base 107

Chapitre 6. Configuration d'un serveur de règles 109
Sélection de format de données LDAP 109
Domaines de gestion Security Access Manager . . 110
Exemple d'emplacement d'un domaine de gestion 111
Emplacement d'un domaine de gestion pour un registre Active Directory Lightweight Directory Service (AD LDS) 112
Installation du serveur de règles via la ligne de commande 112
AIX : Installation du serveur de règles 113
Linux : Installation du serveur de règles . . . 115
Solaris : Installation du serveur de règles . . . 117
Windows: Installation du serveur de règles . . 119
Installation d'un serveur de règles à l'aide du tableau de bord (Windows). 121
Installation du serveur de règles à l'aide de fichiers scripts. 123
Automatisation de l'installation d'un serveur de règles (AIX, Linux ou Solaris) 124
Automatisation de l'installation d'un serveur de règles (Windows) 124
Automatisation de la configuration d'un serveur de règles 126

Chapitre 7. Configuration du serveur d'autorisation 129
Installation du serveur d'autorisation à l'aide de la ligne de commande 129
AIX : Installation d'un serveur d'autorisations 130
Linux : Installation d'un serveur d'autorisations 132
Solaris : Installation d'un serveur d'autorisations 133
Windows : Installation d'un serveur d'autorisations 135
Installation d'un serveur d'autorisations à l'aide du tableau de bord (Windows). 136
Installation du serveur d'autorisation à l'aide des fichiers scripts 138
Automatisation de l'installation d'un serveur d'autorisations (AIX, Linux ou Solaris) 138
Automatisation de l'installation d'un serveur d'autorisations (Windows) 139
Automatisation de la configuration d'un serveur d'autorisations 140

Chapitre 8. Configuration d'un système de développement 143
Configuration d'un système de développement via une ligne de commande. 143
AIX : Installation d'un système de développement (ADK) 144
Linux : Installation d'un système de développement (ADK) 145
Solaris : Installation d'un système de développement (ADK) 146
Windows : Installation d'un système de développement (ADK) 147
Configuration d'un système de développement à l'aide du tableau de bord (Windows) 149
Configuration d'un système de développement à l'aide de fichiers scripts 150
Automatisation de l'installation d'un système de développement (AIX, Linux ou Solaris). . . . 150
Automatisation de l'installation d'un système de développement (Windows) 151

Chapitre 9. Configuration d'un système IBM Security Access Manager Runtime for Java. 155
Configuration d'un système Security Access Manager Runtime for Java via une ligne de commande 155
AIX : Installation d'IBM Security Access Manager Runtime for Java 156
Linux : Installation d'IBM Security Access Manager Runtime for Java 157

Solaris : Installation d'IBM Security Access Manager Runtime for Java 159
Windows : Installation d'IBM Security Access Manager Runtime for Java 160
Configuration d'un composant d'exécution pour système Java à l'aide du tableau de bord (Windows) 161
Configuration d'un serveur d'exécution pour serveur Java à l'aide de fichiers scripts 162
Automatisation de l'installation d'un système Runtime for Java (AIX, Linux ou Solaris) . . . 163
Automatisation de l'installation d'un système Runtime for Java (Windows) 164
Automatisation de la configuration d'un système d'exécution pour un système Java . . 165

Chapitre 10. Configuration d'un système de serveur proxy de règles . 167
Configuration d'un serveur proxy de règles via une ligne de commande 167
AIX : Installation d'un serveur proxy de règles 168
Linux : Installation d'un serveur proxy de règles 170
Solaris : Installation d'un serveur proxy de règles 171
Windows : Installation d'un serveur proxy de règles 173
Configuration d'un serveur proxy de règles à l'aide du tableau de bord (Windows) 174
Configuration d'un système de serveur proxy de règles à l'aide de fichiers scripts 176
Automatisation de l'installation d'un système de serveur proxy de règles (AIX, Linux ou Solaris) . 176
Automatisation de l'installation d'un serveur proxy de règles (Windows) 177
Automatisation de la configuration d'un serveur proxy de règles 178

Chapitre 11. Configuration d'un système d'exécution 181
Configuration d'un serveur d'exécution via une ligne de commande 181
AIX : Installation de Security Access Manager Runtime 182
Linux : Installation de Security Access Manager Runtime 183
Solaris : Installation de Security Access Manager Runtime 185
Windows : Installation de Security Access Manager Runtime 187
Configuration d'un serveur d'exécution à l'aide du tableau de bord (Windows) 188
Configuration d'un serveur d'exécution à l'aide de fichiers scripts 190
Automatisation de l'installation d'un système d'exécution (AIX, Linux ou Solaris) 190
Automatisation de l'installation d'un système d'exécution (Windows) 191
Automatisation de la configuration d'un système d'exécution 191

Chapitre 12. Configuration d'un système Web Portal Manager 195
Configuration d'un système Web Portal Manager via une ligne de commande 195
AIX : Installation d'un système Web Portal Manager 196
Linux : Installation d'un système Web Portal Manager 198
Solaris : Installation d'un système Web Portal Manager 201
Windows : Installation d'un système Web Portal Manager 204
Configuration d'un système Web Portal Manager à l'aide du tableau de bord (Windows) 206
Configuration de Web Portal Manager à l'aide de fichiers scripts 210
Configuration de WebSphere Application Server à l'aide de fichiers scripts 210
Automatisation de l'installation d'un système Web Portal Manager (AIX, Linux ou Solaris) . . 215
Automatisation de l'installation d'un composant Web Portal Manager (Windows) 216
Automatisation de la configuration de Web Portal Manager 217
Configuration de la sécurité de WebSphere Application Server 219

Partie 4. Installation du composant système de sécurité Web 221

Chapitre 13. Configuration de Security Access Manager Attribute Retrieval Service 223
Configuration d'Attribute Retrieval Service via une ligne de commande 223
AIX : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande 224
Linux : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande 225
Solaris : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande 226
Windows : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande 227

Chapitre 14. Configuration du composant Plug-in for Web Servers . 229
Exigences de préinstallation 229
Installation du plug-in pour Apache Web Server via une ligne de commande 230
AIX : composant Plug-in for Apache Web Server 230
Linux on x86-64 : composant Plug-in for Apache Web Server 232
Linux on System z : composant Plug-in for Apache Web Server 234

Solaris : composant Plug-in for Apache Web Server 235
Installation du plug-in pour IBM HTTP Server via une ligne de commande 237
AIX : plug-in for IBM HTTP Server 237
Linux : plug-in for IBM HTTP Server 239
Solaris : Plug-in for IBM HTTP Server 241
Installation du plug-in pour Internet Information Services via une ligne de commande 243
Configuration d'un plug-in pour Internet Information Services à l'aide du tableau de bord (Windows) 245
Configuration du module plug-in de serveur Web à l'aide de fichiers scripts 247
Automatisation de l'installation du plug-in de serveur Apache ou IBM HTTP Server 247
Automatisation de la configuration du plug-in de serveur Apache ou IBM HTTP Server . . . 248
Automatisation de l'installation du plug-in Internet Information Services 249
Automatisation de la configuration du plug-in Internet Information Service 249

Chapitre 15. Configuration d'un système de développement de sécurité Web 253
Configuration d'un système de développement de sécurité Web via une ligne de commande 253
AIX : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande 254
Linux : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande 255
Solaris : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande 257
Windows : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande 258
Configuration d'un système de développement de sécurité Web à l'aide du tableau de bord (Windows) 260
Configuration d'un système de développement de sécurité Web à l'aide de fichiers scripts 262
Automatisation de l'installation d'un système de développement de sécurité Web (AIX, Linux ou Solaris) 262
Automatisation de l'installation d'un système de développement de sécurité Web (Windows) . . 263

Chapitre 16. Configuration de WebSEAL 265
Configuration d'un système WebSEAL via une ligne de commande 265
AIX : Installation de WebSEAL via une ligne de commande 266
Linux : Installation de WebSEAL via une ligne de commande 267
Solaris : Installation de WebSEAL via une ligne de commande 269
Windows : Installation de WebSEAL via une ligne de commande 271
Configuration d'un système WebSEAL à l'aide du tableau de bord (Windows). 272
Configuration du système WebSEAL à l'aide de fichiers scripts 274
Automatisation de l'installation d'un système WebSEAL (AIX, Linux ou Solaris) 274
Automatisation de l'installation d'un système WebSEAL (Windows). 275
Automatisation de la configuration d'un système WebSEAL. 276

Partie 5. Installation du composant système de gestion des sessions . 279

Chapitre 17. Configuration d'un serveur de gestion de sessions . . . 281
Exigences de préinstallation 282
Configuration du serveur de gestion de sessions via une ligne de commande 284
AIX : Installation d'un système de serveur de gestion de sessions 284
Linux : Installation d'un système Session Management Server 285
Solaris : Installation d'un système Session Management Server 286
Windows : Installation d'un système Session Management Server 287
Création de la base de données d'historique de connexion 288
Déploiement de l'extension de console 291
Connexion et déconnexion de la console Session Management Server 291
Déploiement de l'application Session Management Server 292
Configuration du serveur de gestion de sessions 293
Configuration d'un serveur de gestion de session avec le tableau de bord (Windows) 295
Configuration d'un serveur de gestion de session à l'aide de fichiers scripts 300
Configuration de WebSphere Application Server à l'aide de fichiers scripts 300
Automatisation de l'installation d'un serveur de gestion de sessions (AIX, Linux ou Solaris) . . 305
Automatisation de l'installation d'un serveur de gestion de sessions (Windows) 306
Automatisation de la configuration d'un serveur de gestion de sessions 307

Chapitre 18. Configuration de la ligne de commande de gestion de session . 311
Exigences de préinstallation 311
Configuration du serveur de gestion de sessions via les utilitaires de ligne de commande 312
AIX : Installation de la ligne de commande de gestion des sessions 312

Linux : Installation de la ligne de commande de gestion des sessions 313
Solaris : Installation de session management command line 315
Windows : Installation de la ligne de commande de gestion des sessions 317
Configuration d'une ligne de commande de gestion de sessions avec le tableau de bord (Windows) . . 318
Configuration d'une ligne de commande de gestion de sessions à l'aide de fichiers scripts 320
Automatisation de l'installation d'une ligne de commande de gestion de sessions (AIX, Linux ou Solaris) 320
Automatisation de l'installation d'une ligne de commande de gestion de sessions (Windows) . 321
Automatisation de la configuration d'une ligne de commande de gestion de sessions 322

Partie 6. Annexes 325

Annexe A. Configuration de la sécurité SSL (Secure Sockets Layer) . 327
Configuration de SSL sur les serveurs Security Access Manager 327
Création d'une base de données et ajout du certificat de signataire 327
Configuration des communications SSL . . . 328
Test de l'accès SSL 329
Configuration du client Tivoli Directory Server pour l'authentification de client 330
Test de l'accès SSL lors de l'utilisation de l'authentification de serveur et de client 331

Annexe B. Identités des groupes et administrateurs sur les systèmes AIX, Linux et Solaris 333

Annexe C. Numéros de port par défaut 337

Annexe D. Options pdconfig 339
Security Access Manager Runtime : LDAP . . . 339
Security Access Manager Runtime : Active Directory 343
Security Access Manager Attribute Retrieval Service 348
Security Access Manager Authorization Server . . 349
IBM Security Access Manager Runtime for Java 350
Security Access Manager Plug-in for Web Servers sur AIX, Linux ou Solaris 351
Security Access Manager Plug-in for Web Servers sous Windows 353
Security Access Manager Policy Server 354
Security Access Manager Policy Proxy Server. . . 355
Security Access Manager Web Portal Manager . . 356
Security Access Manager WebSEAL 360

Annexe E. Installation du support de langue 363
Présentation du support de langue 363
Installation des modules de support de langue dans Security Access Manager 364
Installation des programmes de support de langue nationale pour IBM Tivoli Directory Server . . . 367
Variables d'environnement local 368
Variable LANG sur les systèmes AIX, Linux ou Solaris 369
Variable LANG sur les systèmes Windows . . 369
Utilisation de variantes d'environnement local 370
Catalogues de messages 370
Support de codage de texte (jeu de codes) 371
Emplacement des fichiers de jeu de codes . . . 372
Désinstallation des programmes de support de langue nationale Security Access Manager 372

Annexe F. Gestion des mots de passe 375
Masquage des mots de passe sous AIX, Linux ou Solaris 376
Masquage des mots de passe sous Windows . . . 377
Suppression d'un mot de passe stocké sous AIX, Linux et Solaris 379
Suppression d'un mot de passe enregistré sous Windows 380

Annexe G. Configuration du serveur de règles de secours (AIX) 381
Scénario d'environnement IBM PowerHA 382
Installation et configuration d'IBM PowerHA pour AIX 382
Création d'un environnement de serveur de règles de secours 383
Script : paramétrage des ID utilisateur pour les systèmes primaires et de secours 387
Script : création de liens entre fichiers et répertoires sur le système principal 389
Exemple : vérification des répertoires de serveur primaire, des liens lointains et des autorisations 390
Script : création d'un lien allant des fichiers système AIX vers le répertoire partagé sur le système de secours 392
Exemple : vérification des répertoires de serveur de secours, des liens lointains et des autorisations 393
Gestion de la haute disponibilité 394
Vérification de la configuration du serveur de règles pour la haute disponibilité 394
Consultation des fichiers journaux 395

Annexe H. Configuration d'un serveur de règles de secours avec IBM Tivoli System Automation for Multiplatforms 397
Composants du scénario. 397
Exigences de préinstallation 399
Exigences relatives à LDAP et à l'équilibreur de charge 399

Configuration requise pour le serveur principal 399
Exigences applicables au serveur de secours . . 399
Exigences applicables au serveur d'exécution 400
Installation du protocole LDAP et de l'équilibreur de charge. 400
Installation du serveur principal 400
Installation du serveur de secours 402
Vérification des serveurs Security Access Manager 403
Configuration de l'équilibreur de charge 408
Installation et configuration du serveur d'exécution 408
Installation et configuration de Tivoli System Automation for Multiplatforms 409
Activation de l'automatisation de la reprise en ligne 411
Script Polup pour le serveur principal 413
Script Polup pour le serveur de secours . . . 414
Script Poldown pour le serveur principal . . . 416
Script Poldown pour le serveur de secours . . 418
Script Polmon pour le serveur principal . . . 419
Script Polmon pour le serveur de secours . . . 420

Annexe I. Configuration de l'environnement de proxy Tivoli Directory Server 421
Ajout du suffixe Security Access Manager au proxy 422
Configuration de Security Access Manager pour utiliser le proxy 423
Redirection du serveur de règles vers le proxy 423
Configuration des contrôles d'accès pour le proxy 424
Annulation de la configuration de Security Access Manager à partir du proxy 425

Annexe J. Adaptateur de registre Security Access Manager pour les référentiels fédérés WebSphere . . . 427

Annexe K. Désinstallation 429
Annulation de la configuration des composant Security Access Manager 429
Annulation de la configuration d'IBM Tivoli Directory Server 430
Annulation de la configuration de la base de données 430
Suppression d'une instance de serveur d'annuaire 431
Suppression de packages 433
Désinstallation d'IBM Tivoli Directory Server 433
AIX : suppression de packages 434
Linux : suppression des packages 436
Solaris : suppression de packages 438
Windows : suppression de packages 439

Remarques 441

Index 445

Figures

1. Serveur de règles primaire après la configuration initiale 384
2. Serveur de règles principal après l'intégration de l'utilisation du système de fichiers partagé. 385
3. Environnement de serveur de règles principal ou de secours exécuté. 387

© Copyright IBM Corp. 2001, 2013

Tableaux

1. Composants requis sur les systèmes de base de Security Access Manager 13
2. Composants requis pour les systèmes de sécurité Web Security Access Manager . . . 15
3. Composants requis pour les systèmes de gestion de sessions Security Access Manager . 17
4. Méthodes d'installation pour AIX, Linux ou Solaris 19
5. Méthodes d'installation pour Windows 19
6. Tâches de planification. 21
7. Tâches prérequises 21
8. Tâches du serveur de règles 21
9. Tâches liées aux composants système de base 22
10. Tâches liées aux composants de sécurité Web 22
11. Tâche de gestion de sessions. 22
12. Tâches relatives à l'installation et à la configuration des logiciels prérequis 27
13. Packages de client pour AIX 44
14. Packages client pour systèmes d'exploitation Linux 45
15. Packages client pour Solaris 46
16. Longueurs maximales des noms par registre d'utilisateurs et longueur optimale dans les registres d'utilisateurs 57
17. Valeurs de conformité pour le fichier de clés 72
18. Valeurs des attributs de conformité 75
19. Valeurs de configuration SSL 329
20. Utilisateurs et groupes requis par Security Access Manager. 333
21. Numéros de port par défaut utilisés durant l'installation de Security Access Manager . . 337
22. Options de configuration de Security Access Manager Runtime – LDAP 339
23. Options de configuration de Security Access Manager Runtime – Active Directory . . . 343
24. Security Access Manager Attribute Retrieval Service. 348
25. Options de configuration de Security Access Manager Authorization Server 349
26. options de configuration IBM Security Access Manager Runtime for Java 350
27. Plug-in for Web Servers sur AIX, Linux ou Solaris 351
28. Plug-in for Web Servers sous Windows 353
29. Options de configuration de Security Access Manager Policy Server 354
30. Options de configuration de Security Access Manager Policy Proxy Server 356
31. Options de configuration de Security Access Manager Web Portal Manager 356
32. Options de configuration de Security Access Manager WebSEAL 360
33. Tâches liées aux mots de passe de configuration automatisée 375
34. Fichiers modèles d'options de composant par défaut sous AIX, Linux, ou Solaris 377
35. Composants du scénario utilisant IBM Tivoli System Automation for Multiplatforms . . . 398
36. Méthodes de désinstallation de Tivoli Directory Server 433

© Copyright IBM Corp. 2001, 2013

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

© Copyright IBM Corp. 2001, 2013

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de cette publication

IBM Security Access Manager for Web, précédemment appelé IBM Tivoli Access Manager for e-business, est une solution d'authentification utilisateur, d'autorisation et de connexion unique Web permettant d'appliquer des règles de sécurité sur une large gamme de ressources Web et d'applications.

Le manuel *IBM Security Access Manager for Web : Guide d'installation* explique comment installer et configurer Security Access Manager, notamment les systèmes Security Access Manager, les systèmes de gestion de session et les systèmes de sécurité Web.

Public concerné

Ce guide est destiné aux administrateurs système responsables de l'installation et du déploiement de Security Access Manager.

Les lecteurs de ce guide doivent être familiarisés avec les sujets suivants :

- Systèmes d'exploitation pris en charge
- Architecture et concepts de bases de données
- Gestion de la sécurité
- Protocoles Internet, notamment HTTP, TCP/IP, File Transfer Protocol (FTP) et Telnet
- Protocole LDAP (Lightweight Directory Access Protocol) et services d'annuaire
- Authentification et autorisation

Si vous activez la communication SSL (Secure Sockets Layer), vous devez également maîtriser le protocole SSL, l'échange de clés (publiques et privées), les signatures numériques, les algorithmes de cryptographie et les autorités de certification.

Accès aux publications et à la terminologie

Cette section contient :

- Une liste des publications présentes dans la «Bibliothèque IBM Security Access Manager for Web».
- Des liens vers les «Publications en ligne», à la page xviii.
- Un lien vers le «Site Web de terminologie IBM», à la page xviii.

Bibliothèque IBM Security Access Manager for Web

Les documents suivants se trouvent dans la bibliothèque IBM Security Access Manager for Web :

- *IBM Security Access Manager for Web : Guide de démarrage rapide*, GI11-9333-01

  Fournit des procédures qui récapitulent les tâches d'installation et de configuration majeures.

© Copyright IBM Corp. 2001, 2013

- *IBM Security Web Gateway Appliance - Hardware Offering : Guide de démarrage rapide*

  Guide les utilisateurs dans le processus de connexion et de configuration initiale de WebSEAL Hardware Appliance
- *IBM Security Web Gateway Appliance – Virtual Offering : Guide de démarrage rapide*

  Guide les utilisateurs dans le processus de connexion et de configuration initiale de WebSEAL Virtual Appliance.
- *IBM Security Access Manager for Web : Guide d'installation*, GC11-6786-02

  Explique comment installer et configurer Security Access Manager.
- *IBM Security Access Manager for Web Upgrade Guide*, SC23-6503-02

  Fournit aux utilisateurs des informations sur la mise à niveau de la version 6.0 ou 6.1.x vers la version 7.0.
- *IBM Security Access Manager for Web : Guide d'administration*, SC11-6383-03

  Describes the concepts and procedures for using Security Access Manager. Fournit des instructions sur l'exécution de tâches à partir de l'interface de Web Portal Manager et à l'aide de l'utilitaire **pdadmin**.
- *IBM Security Access Manager for Web WebSEAL Administration Guide*, SC23-6505-03

  Fournit des documents d'arrière-plan, des procédures administratives et des informations de référence pour gérer les ressources de votre domaine Web sécurisé avec WebSEAL.
- *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*, SC23-6507-02

  Fournit les procédures et les informations de référence pour la sécurisation de votre domaine Web à l'aide d'un plug-in de serveur Web.
- *IBM Security Access Manager for Web Shared Session Management Administration Guide*, SC23-6509-02

  Fournit les informations relatives à l'administration et les instructions de fonctionnement pour le serveur de gestion de session.
- *IBM Security Access Manager for Web Shared Session Management Deployment Guide*, SC22-5431-00

  Fournit les informations relatives au déploiement pour le serveur de gestion de session.
- *IBM Security Web Gateway Appliance Administration Guide*, SC22-5432-01

  Fournit les informations relatives aux procédures d'administration et aux références techniques pour WebSEAL Appliance.
- *IBM Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*, SC22-5433-01

  Fournit les informations relatives aux procédures de configuration et aux références techniques pour WebSEAL Appliance.
- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*, SC27-4442-01

  Fournit des informations de référence complètes sur les strophes pour le proxy inverse Web IBM® Security Web Gateway Appliance.
- *IBM Security Access Manager for Web WebSEAL Configuration Stanza Reference*, SC27-4443-01

  Fournit un référence de strophe complète pour WebSEAL.

- *IBM Global Security Kit: CapiCmd Users Guide*, SC22-5459-00

  Fournit des instructions sur la création de bases de données de clés, de paires de clés publiques-privées et de demandes de certificat.
- *IBM Security Access Manager for Web Auditing Guide*, SC23-6511-03

  Fournit des informations sur la configuration et la gestion d'événements d'audit via l'approche Security Access Manager native et Service commun de contrôle et de rapport. Vous pouvez également trouver des informations sur l'installation et la configuration dans Service commun de contrôle et de rapport. Utilisez ce service pour générer et afficher des rapports opérationnels.
- *IBM Security Access Manager for Web Command Reference*, SC23-6512-03

  Fournit les informations de référence relatives aux commandes, aux utilitaires et aux scripts qui accompagnent Security Access Manager.
- *IBM Security Access Manager for Web Administration C API Developer Reference*, SC23-6513-02

  Fournit des informations de référence sur la mise en oeuvre du langage C de l'API d'administration permettant à une application d'exécuter les tâches d'administration de Security Access Manager.
- *IBM Security Access Manager for Web Administration Java Classes Developer Reference*, SC23-6514-02

  Fournit des informations de référence sur la mise en oeuvre du langage Java™ de l'API d'administration permettant à une application d'exécuter les tâches d'administration de Security Access Manager.
- *IBM Security Access Manager for Web Authorization C API Developer Reference*, SC23-6515-02

  Fournit des informations de référence sur la mise en oeuvre du langage C de l'API d'autorisation permettant à une application d'utiliser la sécurité Security Access Manager.
- *IBM Security Access Manager for Web Authorization Java Classes Developer Reference*, SC23-6516-02

  Fournit des informations de référence sur la mise en oeuvre du langage Java de l'API d'autorisation permettant à une application d'utiliser la sécurité Security Access Manager.
- *IBM Security Access Manager for Web Web Security Developer Reference*, SC23-6517-02

  Fournit des informations de programmation et de référence pour le développement des modules d'authentification.
- *IBM Security Access Manager for Web Error Message Reference*, GI11-8157-02

  Fournit des explications et des actions correctives pour les messages et les codes de retour.
- *IBM Security Access Manager for Web Troubleshooting Guide*, GC27-2717-01

  Fournit des informations sur l'identification des problèmes.
- *IBM Security Access Manager for Web Performance Tuning Guide*, SC23-6518-02

  Fournit des informations sur l'optimisation des performances pour un environnement constitué de Security Access Manager avec IBM Tivoli Directory Server comme registre d'utilisateurs.

Publications en ligne

Lorsqu'un produit est mis sur le marché IBM publie les publications associées et leurs mises à jour aux emplacements suivants :

Centre de documentation IBM Security Access Manager for Web
Le site http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isam.doc_70/welcome.html affiche la page d'accueil du centre de documentation pour ce produit.

Pages IBM Security Systems Documentation Central et Welcome
La page IBM Security Systems Documentation Central fournit une liste alphabétique de toutes les documentations produit d'IBM Security Systems et offre un lien vers le centre de documentation produit des versions spécifiques de chaque produit.

La page Welcome to IBM Security Systems Information Centers offre une introduction, des liens ainsi que des informations générales sur les centres de documentation IBM Security Systems.

IBM Publications Center
Le site The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss fournit des fonctions pour vous aider à rechercher les publications IBM dont vous avez besoin.

Site Web de terminologie IBM

Le site Web de terminologie IBM rassemble la terminologie des bibliothèques de produits dans un seul emplacement. Vous pouvez accéder au site Web de terminologie à l'adresse http://www.ibm.com/software/globalization/terminology.

Publications connexes

Cette section affiche la liste des produits IBM associés inclus dans la solution Security Access Manager.

Remarque : Les produits middleware suivants ne sont pas packagés avec IBM Security Web Gateway Appliance.

IBM Global Security Kit

Security Access Manager permet le chiffrement des données à l'aide de Global Security Kit (GSKit) version 8.0.x. GSKit est inclus dans l'image ou le DVD du produit *IBM Security Access Manager for Web Version 7.0* correspondant à la plateforme considérée.

GSKit version 8 inclut l'outil de ligne de commande pour la gestion des clés, GSKCapiCmd (**gsk8capicmd_64**).

GSKit version 8 n'inclut plus l'utilitaire de gestion de clés, iKeyman (**gskikm.jar**). iKeyman est conditionné avec IBM Java version 6 ou ultérieure et est maintenant une application Java à part entière sans dépendance sur l'environnement d'exécution GSKit natif. La bibliothèque *java*/jre/lib/gskikm.jar ne doit être ni déplacée ni supprimée.

Le document *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7, iKeyman User's Guide for version 8.0* est disponible dans le centre de documentation Security Access Manager. Ce document est également directement accessible à l'adresse suivante :

http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf

Remarque :

GSKit version 8 inclut les modifications importantes apportées à l'implémentation du protocole TLS (Transport Layer Security) requises pour remédier aux problèmes de sécurité.

Les modifications de GSKit version 8 sont conformes aux exigences RCF (Request for Comments) du groupe de travail IETF (Internet Engineering Task Force). Toutefois, elles ne sont pas compatibles avec les versions antérieures de GSKit. Tout composant communiquant avec Security Access Manager et qui utilise GSKit doit être mis à niveau pour utiliser GSKit version 7.0.4.42, ou 8.0.14.26 ou version ultérieure. Sinon, des problèmes de communication peuvent se produire.

IBM Tivoli Directory Server

IBM Tivoli Directory Server version 6.3 FP17 (6.3.0.17-ISS-ITDS-FP0017) est inclus dans l'image ou le DVD du produit *IBM Security Access Manager for Web Version 7.0* correspondant à la plateforme concernée.

Vous trouverez des informations supplémentaires relatives à Tivoli Directory Server à l'adresse :

http://www.ibm.com/software/tivoli/products/directory-server/

IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator version 7.1.1 est inclus dans l'image ou le DVD du produit *IBM Tivoli Directory Integrator Identity Edition V 7.1.1 for Multiplatform* correspondant à la plateforme concernée.

Vous trouverez des informations supplémentaires relatives à IBM Tivoli Directory Integrator à l'adresse :

http://www.ibm.com/software/tivoli/products/directory-integrator/

IBM DB2 Universal Database

IBM DB2 Universal Database Enterprise Server Edition version 9.7 FP4 est fourni dans l'image ou le DVD du produit *IBM Security Access Manager for Web Version 7.0* correspondant à la plateforme concernée. Vous pouvez installer DB2 avec le logiciel Tivoli Directory Server ou en tant que produit autonome. DB2 est requis lorsque vous utilisez Tivoli Directory Server ou des serveurs LDAP z/OS comme registre d'utilisateurs pour Security Access Manager. Pour les serveurs LDAP z/OS, vous devez vous procurer DB2 séparément.

Vous trouverez des informations supplémentaires relatives à DB2 à l'adresse :

http://www.ibm.com/software/data/db2

Produits IBM WebSphere

Les modules d'installation destinés à WebSphere Application Server Network Deployment, version 8.0 et WebSphere eXtreme Scale version 8.5.0.1 sont inclus dans Security Access Manager version 7.0. WebSphere eXtreme Scale est requis uniquement lorsque le composant Session Management Server (SMS) est utilisé.

WebSphere Application Server permet la prise en charge des applications suivantes :

- l'interface de Web Portal Manager, qui gère Security Access Manager.
- Web Administration Tool, qui permet de gérer Tivoli Directory Server.
- Service commun de contrôle et de rapport, qui traite et génère des rapports sur les événements d'audit.
- Session Management Server, qui gère une session partagée dans un environnement de serveur de sécurité Web.
- Attribute Retrieval Service.

Vous trouverez des informations supplémentaires sur WebSphere Application Server à l'adresse :

http://www.ibm.com/software/webservers/appserv/was/library/

Accessibilité

Les fonctions d'accessibilité permettent aux utilisateurs porteurs d'un handicap physique, tel qu'une mobilité réduite ou une vision restreinte, d'utiliser avec succès des progiciels. Avec ce produit, vous pouvez utiliser des technologies d'assistance pour entendre les commandes et naviguer dans l'interface. Vous pouvez également recourir au clavier au lieu de la souris pour utiliser toutes les fonctions de l'interface graphique.

Pour plus d'informations sur les engagements d'accessibilité d'IBM, accédez au centre d'accessibilité IBM

Formation technique

Pour plus d'informations sur la formation technique, accédez au site Web IBM Education à l'adresse http://www.ibm.com/software/tivoli/education.

Informations relatives au service de support

Le service de support IBM vous aide à résoudre les problèmes liés aux codes ainsi que ceux liés aux routines, aux installations de courte durée ou à l'utilisation. Vous pouvez accéder directement au site IBM Software Support à l'adresse http://www.ibm.com/software/support/probsub.html.

Le document *IBM Security Access Manager for Web Troubleshooting Guide* fournit :

- Les informations à collecter avant de contacter le service de support IBM.
- Les différents moyens de contacter le service de support IBM.
- Le mode d'utilisation d'IBM Support Assistant.
- Les instructions et les ressources d'identification des problèmes qui vous permettront d'isoler et de résoudre le problème vous-même.

Remarque : L'onglet **Community and Support** du centre de documentation du produit permet d'accéder à d'autres ressources de support.

Partie 1. Planification de l'installation

© Copyright IBM Corp. 2001, 2013

Chapitre 1. Présentation de l'installation

Il est important de créer un plan de déploiement avant d'installer le logiciel Security Access Manager sur les systèmes de votre environnement distribué.

Si le logiciel Security Access Manager est déjà installé, consultez le plan de déploiement précédent afin de déterminer la meilleure méthode pour le mettre à niveau avec la version la plus récente. Suivez les instructions fournies dans le manuel*IBM Security Access Manager for Web Upgrade Guide*.

Remarque : Pour obtenir des informations sur la dernière version, notamment sur la configuration système, les exigences en matière d'espace disque et d'espace mémoire, ainsi que les défauts et limitations connus, consultez la section Notes sur l'édition du centre de documentation IBM Security Access Manager for Web, ou les notes techniques disponibles dans la base de connaissances du support.

Planification du déploiement

Avant de mettre en oeuvre une solution Security Access Manager spécifique, vous devez déterminer les fonctions de sécurité et de gestion spécifiques requises sur votre réseau.

La première étape de planification de déploiement d'un environnement de sécurité Security Access Manager consiste à définir les exigences de sécurité de votre environnement informatique. Cela implique de définir les processus métier à appliquer aux utilisateurs, aux programmes et aux données. Cette définition inclut :

- les objets à sécuriser
- les actions autorisées sur chacun des objets
- les utilisateurs autorisés à effectuer les actions

Pour appliquer une règle de sécurité, il est nécessaire de comprendre le flux des demandes d'accès au sein de votre topologie de réseau. Votre plan doit identifier les rôles et emplacements des pare-feux, des routeurs et des sous-réseaux. Le déploiement d'un environnement de sécurité Security Access Manager requiert également l'identification les points optimaux du réseau afin d'installer le logiciel qui évalue les demandes d'accès des utilisateurs, les accepte ou les refuse.

Pour mettre en oeuvre une stratégie de sécurité, il est nécessaire de connaître le nombre d'utilisateurs, la quantité de données et la capacité de traitement que votre réseau doit atteindre. Vous devez évaluer les caractéristiques de performance, l'évolutivité et les besoins relatifs aux fonctions de reprise en ligne. En outre, il est nécessaire de prendre en compte l'intégration des versions précédentes des logiciels, des bases de données et des applications dans le logiciel Security Access Manager.

Après avoir défini les fonctionnalités que vous souhaitez déployer, vous pouvez décider de quels systèmes Security Access Manager vous avez besoin pour votre environnement.

Pour obtenir de la documentation sur la planification, notamment des scénarios d'entreprise réels, consultez les sites Web ci-après.

© Copyright IBM Corp. 2001, 2013

http://www.ibm.com/redbooks/

http://www.ibm.com/software/sysmgmt/products/support/Field_Guides.html

Présentation du domaine sécurisé

L'environnement informatique dans lequel Security Access Manager applique les règles de sécurité pour l'authentification, l'autorisation et le contrôle d'accès est appelé un *domaine sécurisé*.

Le domaine sécurisé initial, appelé *domaine de gestion*, est créé lors de l'installation et la configuration des systèmes suivants :

Serveur de règles
Gère la base de données d'autorisation maître du domaine de gestion. En outre, il met à jour les répliques de la base d'autorisation et gère les informations d'emplacement relatives aux autres serveurs Security Access Manager.

Registre
Fournit une base de données des identités de l'utilisateur connues de Security Access Manager. Il fournit également une représentation des groupes dans les rôles de Security Access Manager associés aux utilisateurs.

Ces systèmes centraux doivent exister pour que Security Access Manager effectue des opérations fondamentales, comme l'autorisation ou le refus de l'accès à des objets protégés (ressources). Tous les autres services et composants Security Access Manager sont générés sur cette base.

Vous pouvez déployer Security Access Manager sur plusieurs systèmes ou installer tous les logiciels nécessaires pour configurer et utiliser le domaine de gestion sur un système autonome. Une configuration à système unique est utile lorsque vous générez un prototype de déploiement ou développez et testez une application.

Après avoir configuré le serveur de règles et le serveur de registre, vous pouvez configurer des systèmes supplémentaires dans le domaine de gestion. Par exemple, vous pouvez configurer un serveur d'autorisation ou un système de développement d'applications. Vous pouvez également créer des domaines sécurisés supplémentaires (si vous utilisez un registre LDAP) pour partitionner de façon sécurisée les données en groupes distincts et logiques. Pour plus d'informations sur la création de plusieurs domaines, voir *IBM Security Access Manager for Web : Guide d'administration*.

Composants d'installation de Security Access Manager

Security Access Manager inclut les composants de base et prérequis généralement communs à toutes les installations Security Access Manager.

Utilisez ces composants pour configurer les systèmes Security Access Manager répertoriés dans «Composants et prérequis pour les système Security Access Manager», à la page 13.

Remarque : Lors de l'installation de Security Access Manager sur un système d'exploitation Windows, vous pouvez indiquer un chemin d'installation différent de celui par défaut. Vérifiez que le chemin d'installation indiqué n'inclut aucun caractère de globalisation.

Security Access Manager - composants de base

Le système de base de Security Access Manager inclut les composants d'installation spécifiques suivants.

Ces composants se trouvent sur le support du produit pour les plateformes prises en charge. Utilisez-les pour configurer les systèmes de base répertoriés dans «Composants et prérequis pour les système Security Access Manager», à la page 13.

Security Access Manager Application Development Kit

Security Access Manager Application Development Kit constitue un environnement de développement qui vous permet de coder des applications tierces pour analyser le serveur d'autorisation et prendre des décisions d'autorisation.

Ce kit permet de prendre en charge les deux API C et les classes Java aux fins d'administration et d'autorisation. Pour exécuter le programme Java ou pour compiler et exécuter vos propres programmes Java, vous devez installer et configurer un système Security Access Manager Runtime for Java.

Security Access Manager Authorization Server

Security Access Manager Authorization Server permet d'accéder au service d'autorisation destiné aux applications tierces utilisant l'API d'autorisation de Security Access Manager en mode cache distant.

Le serveur d'autorisation sert également de serveur de collecte d'informations de consignation et d'audit permettant de stocker les enregistrements relatifs à l'activité du serveur.

Security Access Manager Policy Proxy Server

Le serveur proxy de règles Security Access Manager agit comme intermédiaire entre un réseau moins sécurisé et un réseau plus sécurisé.

Ce serveur garantit le niveau de sécurité et assure le contrôle administratif et les services de mise en cache. Il est associé à ou fait partie de :

- Un serveur de passerelle séparant le réseau d'entreprise du réseau extérieur.
- Un serveur pare-feu protégeant le réseau d'entreprise des accès non autorisés.

Dans un environnement Security Access Manager, le serveur proxy s'exécute en tant que serveur de règles pour un nombre spécifié d'applications d'autorisation et de fonctions d'administration, comme les commandes **pdadmin**.

Security Access Manager Policy Server

Le serveur de règles Security Access Manager gère la base de données d'autorisation maître du domaine de gestion. Il gère également les bases de données associées à d'autres domaines sécurisés que vous êtes susceptible de créer.

Ce serveur est essentiel dans le traitement des contrôles d'accès, des authentification et des requêtes d'autorisation. Il met également à jour les répliques de base d'autorisation et gère les informations d'emplacement relatives à d'autres serveurs Security Access Manager.

Security Access Manager prend en charge l'utilisation d'un serveur de règles *de secours* sur une plateforme prise en charge.

Dans les environnements équipés d'un serveur de règles de secours, si le serveur de règles primaire cesse de fonctionner, le serveur de règles de secours prend la relève. Il agit comme serveur de règles primaire jusqu'à ce que le serveur de règle primaire remplisse à nouveau son rôle d'origine. A son tour, le serveur de règles de secours remplit à nouveau un rôle de secours. A un moment donné, il n'y a *qu'un seul* serveur de règles actif et *qu'une seule* copie partagée des bases de données de règles.

Si vous souhaitez configurer un serveur de règles de secours, procédez de l'une des manières suivantes :

- Annexe G, «Configuration du serveur de règles de secours (AIX)», à la page 381
- Annexe H, «Configuration d'un serveur de règles de secours avec IBM Tivoli System Automation for Multiplatforms», à la page 397

Security Access Manager Runtime

Security Access Manager Runtime contient des bibliothèques d'exécution et des fichiers de prise en charge utilisés par les applications pour accéder aux serveurs Security Access Manager.

Vous devez installer et configurer le composant Security Access Manager Runtime sur chaque système exécutant Security Access Manager, à l'exception des systèmes :

- IBM Security Access Manager Runtime for Java
- Security Access Manager Attribute Retrieval Service
- et des systèmes de gestion de sessions distribués

IBM Security Utilities

Les utilitaires de sécurité IBM sont des utilitaires communs requis par Security Access Manager Runtime.

Ce composant est fourni séparément pour chaque plateforme prise en charge.

IBM Security Access Manager Runtime for Java

IBM Security Access Manager Runtime for Java offre un environnement fiable pour le développement et de déploiement des applications Java dans un domaine sécurisé Security Access Manager. Utilisez-le pour ajouter les services de sécurité et d'autorisation de Security Access Manager aux applications Java nouvelles ou existantes.

Vous pouvez utiliser la commande **pdjrtecfg** pour configurer un environnement d'exécution Java (JRE) et utiliser la sécurité Security Access Manager Java.

Si vous prévoyez d'installer l'interface Web Portal Manager, ce composant est requis. Il est également requis avec le composant Security Access Manager Application Development Kit si vous utilisez des classes IBM Security Access Manager Runtime for Java. Pour plus d'informations, voir *IBM Security Access Manager for Web : Administration Java Classes Developer Reference* et *IBM Security Access Manager for Web : Authorization Java Classes Developer Reference*.

Security Access Manager Web Portal Manager

Security Access Manager Web Portal Manager est une interface graphique utilisateur (GUI) Web utilisée pour l'administration de Security Access Manager.

L'équivalent GUI de l'interface de ligne de commande **pdadmin**, Web Portal Manager permet de gérer les utilisateurs, les groupes, les rôles, les droits d'accès, les règles et d'autres tâches Security Access Manager. L'utilisation de Web Portal Manager présente un avantage essentiel : la possibilité d'exécuter les tâches à distance, sans configuration réseau spécifique.

L'interface de Web Portal Manager inclut également un ensemble de services de gestion délégués qui permet à l'enteprise de déléguer l'administration des utilisateurs, des groupes ou des rôles, l'administration de sécurité et l'attribution des accès aux applications aux différents participants (sous-domaines) du système de la société. Ces sous-domaines permettent à leur tour de déléguer les tâches de gestion et d'administration à des sous-domaines sécurisés sous leur contrôle.

Consultez les notes sur l'édition dans le centre de documentation de Security Access Manager pour obtenir la liste des navigateurs utilisables avec Web Portal Manager.

Licence Security Access Manager

Ce composant contient les informations de licence de Security Access Manager. Ce composant est fourni séparément pour chaque plateforme prise en charge.

Security Access Manager - Composants de sécurité Web

Security Access Manager Web Security inclut les composants d'installation suivants.

Ces composants se trouvent sur le support du produit pour chaque plateforme prise en charge. Utilisez-les pour configurer les systèmes de sécurité Web répertoriés dans «Systèmes de sécurité Web Security Access Manager», à la page 14.

Security Access Manager Attribute Retrieval Service

Le service d'extraction d'attribut de Security Access Manager est utilisé avec la fonction d'informations de décision d'autorisation (ADI) de WebSEAL.

Ce service offre des services de communication et de traduction de format entre la bibliothèque de service d'autorisation WebSEAL et le fournisseur externe d'informations de décision d'autorisation. Pour plus d'informations, voir le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Security Access Manager Plug-in for Web Servers

Security Access Manager Plug-in for Web Servers gère la sécurité des ressources Web en faisant office de passerelle entre vos clients et l'espace Web sécurisé.

Le plug-in met en oeuvre les stratégies de sécurité qui protègent votre espace d'objet Web. Ce plug-in offre des solutions de connexion unique, prend en charge des serveurs Web s'exécutant comme des hôtes virtuels et intègre des ressources de serveur d'applications Web dans la stratégie de sécurité. Pour plus d'informations,

consultez le manuel *IBM Security Access Manager for Web: Plug-in for Web Servers Administration Guide*.

Security Access Manager Web Security Runtime

Security Access Manager Web Security Runtime contient des fichiers de bibliothèque d'authentification partagée utilisés par les systèmes Web security.

Ces fichiers partagés incluent Security Access Manager WebSEAL et le module d'extension Security Access Manager for Web Servers.

Security Access Manager Web Security Application Development Kit

Le composant Security Access Manager Web Security ADK contient l'API de développement pour les composants de sécurité Web.

Les API comprennent le service d'authentification interdomaine Security Access Manager (CDAS), l'infrastrucutre de mappage interdomaine Security Access Manager (CDMF), ainsi que le module de contrôle de mot de passe Security Access Manager.

Security Access ManagerWebSEAL

Security Access Manager WebSEAL est un gestionnaire de sécurité destiné aux ressources Web. WebSEAL est un serveur Web haute performance multiprocessus qui applique une stratégie de sécurité à granularité fine sur l'espace d'objet Web protégé.

WebSEAL offre des solutions de connexion unique et intègre des ressources de serveur d'applications back-end dans sa stratégie de sécurité.

Composants de gestion de sessions distribués Security Access Manager

Les systèmes de gestion de sessions distribués de Security Access Manager incluent les composants d'installation suivants.

Ces composants se trouvent sur le support du produit pour chacune des plateformes prises en charge. Utilisez ces composants d'installation pour configurer les systèmes de gestion de sessions distribuées répertoriés dans «Composants et prérequis pour les système Security Access Manager», à la page 13.

Security Access Manager Session Management Server

Security Access Manager Session Management Server (SMS) est un composant Security Access Manager facultatif qui s'exécute en tant que service d'IBM WebSphere Application Server.

Il gère des sessions d'utilisateur sur des clusters complexes de serveurs de sécurité Security Access Manager, et s'assure que la stratégie de sessions est identique sur tous les serveurs participants. Grâce au serveur de gestion de sessions, Security Access Manager WebSEAL et Security Access Manager Plug-in for Web Servers peuvent partager une vue unifiée de toutes les sessions en cours et les utilisateurs autorisés peuvent contrôler et gérer les sessions d'utilisateurs. Le serveur de gestion de sessions :

- Permet de partager les informations de sessions.
- Met à disposition les statistiques de sessions.
- Fournit des fonctions de connexion unique et de basculement haute performance et sécurisées sur les environnements cluster.

Administrez et gérez les sessions d'utilisateurs avec la Security Access Manager Session Management Command Line ou la console Session Management Server.

Security Access Manager Session Management Command Line

Vous pouvez administrer le serveur de gestion de session via le composant Security Access Manager Session Management Command Line.

Exécutez au choix l'utilitaire de ligne de commande **pdadmin** sur le serveur d'autorisations Security Access Manager spécifié, ou l'utilitaire **pdsmsadmin**.

Remarque : Si vous souhaitez utiliser **pdadmin** pour administrer le serveur de gestion de session, vous devez installer et configurer le serveur d'autorisation avant d'installer l'interface de ligne de commande.

Produits prérequis

Security Access Manager inclut plusieurs produits requis lors de la configuration de systèmes Security Access Manager spécifiques.

Pour obtenir la liste des composants obligatoires requis pour configurer un système Security Access Manager, voir tableau 1, à la page 13.

IBM Global Security Kit (GSKit)

IBM Global Security Kit (GSKit) fournit la fonction de chiffrement de données SSL (Secure Sockets Layer) entre les systèmes Security Access Manager et les serveurs de registre pris en charge.

Le package GSKit installe également l'outil GSKCapiCmd, qui vous permet de créer des bases de données de clés, des paires de clés publique-privée et des demandes de certificat.

Vous devez installer GSKit avant d'installer la plupart des autres composants Security Access Manager. GSKit est un composant prérequis de Security Access Manager Runtime, nécessaire sur tous les systèmes Security Access Manager excepté pour Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, Security Access Manager Session Management Server ou Security Access Manager Web Portal Manager.

Remarque : Les versions précédentes de GSKit contiennent un utilitaire appelé **ikeyman**. Cet utilitaire fait partie d'IBM Java. Pour plus d'informations, consultez le manuel *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7 iKeyman User's Guide for version 8.0* http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf.

IBM Java Runtime

Le composant IBM Java Runtime fourni avec Security Access Manager est requis lorsque vous installez et utilisez les modules de prise en charge linguistique.

Le composant IBM Security Access Manager Runtime for Java prend en charge IBM Java Runtime uniquement.

Client IBM Tivoli Directory Server

Vous devez installer le client IBM Tivoli Directory Server sur la plupart des systèmes Security Access Manager.

L'application client est fournie sur le support du produit pour les plateformes prises en charge.

Vous devez installer le client IBM Tivoli Directory Server sur chaque système exécutant Security Access Manager, avec les exceptions suivantes :

- Le système Security Access Manager se trouve sur un système Windows pris en charge qui est soit le domaine Active Directory, soit associé au domaine Active Directory où le serveur de règles Security Access Manager doit être configuré.
- Vous configurez le composant Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, ou Security Access Manager Web Portal Manager.

IBM Tivoli Directory Server

IBM Tivoli Directory Server est l'une des options de registre d'utilisateurs que vous avez définies pour votre environnement Security Access Manager. IBM Tivoli Directory Server permet de gérer facilement les informations de répertoire dans un emplacement central, afin de les stocker, les mettre à jour, les extraire et les échanger.

IBM Tivoli Directory Server est fourni sur le support du produit pour les plateformes prises en charge. Vous pouvez utiliser ce serveur comme serveur de registre Security Access Manager ou utiliser l'un des serveurs de registre répertoriés dans «Registres pris en charge», à la page 11. Ce répertoire (LDAP) Lightweight Directory Access Protocol s'exécute en tant que démon autonome. Il est basé sur un modèle de client/serveur qui permet au client d'accéder au serveur LDAP.

IBM Tivoli Directory Server Web Administration Tool

IBM Tivoli Directory Server fournit l'outil Web Administration Tool pour son administration.

Cet outil est une interface graphique utilisateur optionnelle qui s'exécute sur un serveur d'applications, tel qu'IBM WebSphere Application Server. Utilisez l'outil Web Administration Tool pour gérer les instances IBM Tivoli Directory Server en local ou à distance. Vous pouvez installer une console unique d'administration Web pour gérer plusieurs versions d'IBM Tivoli Directory Server.

L'outil Web Administration Tool est fourni avec les fichiers du produit IBM Tivoli Directory Server.

IBM WebSphere Application Server

IBM WebSphere Application Server est requis par plusieurs composants de Security Access Manager.

Ces composants sont les suivants :

- Security Access Manager - Web Portal Manager
- Le serveur de gestion de sessions Security Access Manager
- Security Access Manager Attribute Retrieval Service

IBM WebSphere Application Server est fourni sur son propre support pour les plateformes prises en charge.

Remarque : IBM Tivoli Directory Server, sur les systèmes Windows uniquement, inclut la version intégrée d'IBM WebSphere Application Server à utiliser avec l'outil Web Administration Tool.

Le même client WebSphere Application Server peut être utilisé pour Web Portal Manager et l'outil Web Administration Tool d'IBM Tivoli Directory Server.

Registres pris en charge

Security Access Manager prend en charge plusieurs registres d'utilisateurs, ainsi que les systèmes d'exploitation et logiciels prérequis par ces derniers.

Consultez le centre de documentation de IBM Security Access Manager for Web ou les notes techniques de la base de données de connaissances du support pour vous assurer que vous avez consulté les informations relatives aux versions les plus récentes, notamment la configuration système requise, les exigences d'espace disque et les incidents et limites connus. Vérifiez que tous les correctifs requis pour le système d'exploitation sont installés.

IBM Tivoli Directory Server

Security Access Manager prend en charge l'utilisation de IBM Tivoli Directory Server en tant que registre.

Notez les informations suivantes :

- IBM Tivoli Directory Server est inclus dans Security Access Manager.
- Le client IBM Tivoli Directory Server est requis si un registre d'utilisateurs LDAP est sélectionné lors de l'installation.
- Vous pouvez installer le client IBM Tivoli Directory Server sur le même système que la version précédente (6.2, 6.1 ou 6.0) du client IBM Tivoli Directory Server.

Avertissement : Si vous avez un client IBM Tivoli Directory Server que vous souhaitez utiliser pour Security Access Manager, assurez-vous de mettre à niveau le serveur sur un niveau pris en charge. Pour obtenir des instructions sur la mise à niveau, consultez le manuel *IBM Security Access Manager for Web Upgrade Guide*.

IBM Tivoli Directory Server for z/OS

Security Access Manager prend en charge l'utilisation de IBM Tivoli Directory Server for z/OS.

Pour obtenir des informations sur le produit, consultez le site Web de la bibliothèque Internet z/OS à l'adresse :

http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

Les clients peuvent également se procurer des publications au format électronique sur le DVD *z/OS : Collection*, SK3T-4269.

Microsoft Active Directory

Security Access Manager prend en charge l'utilisation de Microsoft Active Directory comme registre d'utilisateurs.

Les utilisateurs d'Active Directory peuvent exécuter Security Access Manager sur toutes les plateformes actuellement prises en charge sur le produit Security Access Manager 7.0.

Les plateformes AIX, Linux et Solaris utilisent le client IBM Tivoli Directory Server pour communiquer avec Active Directory. Ce client LDAP est également utilisé sur les plateformes Windows où le domaine Active Directory de l'hôte local est différent du domaine Active Directory où le serveur de règles doit être configuré.

Microsoft Active Directory Lightweight Directory Service (ADLDS)

Security Access Manager prend en charge l'utilisation de Microsoft Active Directory Lightweight Directory Service comme registre d'utilisateurs.

Les utilisateurs de ADLDS peuvent exécuter Security Access Manager avec les versions prises en charge de Windows Server. Consultez les notes sur l'édition de Security Access Manager dans le centre de documentation pour obtenir la liste des navigateurs utilisables avec Web Portal Manager.

Sun Java System Directory Server

Security Access Manager prend en charge l'utilisation de Sun Java System Directory Server en tant que registre d'utilisateurs.

Pour obtenir des informations sur l'installation, consultez la documentation livrée avec le serveur. La documentation sur le produit Sun Java System Directory Server est disponible à l'adresse :

http://docs.sun.com/app/docs/prod/entsys

Novell eDirectory

Security Access Manager prend en charge l'utilisation de Novell eDirectory en tant que registre d'utilisateurs.

Pour obtenir des informations sur l'installation, consultez la documentation livrée avec le serveur Novell eDirectory. Cette dernière est disponible à l'adresse suivante :

http://www.novell.com/documentation/a-z.html

Les derniers modules de correction de ces produits sont disponibles à l'adresse suivante :

http://support.novell.com/patches.html

Avertissement : Si vous souhaitez utiliser une version pré-existante de Novell eDirectory avec Security Access Manager, veillez à migrer le serveur à un niveau pris en charge.

Composants et prérequis pour les système Security Access Manager

Tous les déploiements Security Access Manager incluent plusieurs types de systèmes Security Access Manager configurés dans un domaine sécurisé.

Les composants d'installation requis pour chaque type de système sont fournis avec Security Access Manager. Pour conserver la flexibilité et assurer l'efficacité de l'équilibrage de charge, il est recommandé de configurer le serveur de règles sur un système distinct de votre serveur de registre. Cependant, les autres types de systèmes ne sont pas nécessairement autonomes. Par exemple, vous pouvez installer l'interface Web Portal Manager et le serveur de règles sur le même système.

Security Access Manager - systèmes de base

Chaque système Security Access Manager de base implique des exigences spécifiques en termes de composants.

Le tableau 1 répertorie les types de systèmes de base de Security Access Manager que vous pouvez configurer dans un domaine sécurisé.

Remarque : Vous devez installer le client IBM Tivoli Directory Server sur chaque système exécutant Security Access Manager, avec les exceptions suivantes :

- Le système Security Access Manager se trouve sur un système Windows pris en charge qui est soit le domaine Active Directory, soit associé au domaine Active Directory où le serveur de règles Security Access Manager doit être configuré.
- Vous configurez le composant Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, ou Security Access Manager Web Portal Manager.

Tableau 1. Composants requis sur les systèmes de base de Security Access Manager

Type de système	Composants d'installation
Serveur d'autorisations	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Authorization Server
Development (ADK)	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Application Development Kit

Tableau 1. Composants requis sur les systèmes de base de Security Access Manager (suite)

Type de système	Composants d'installation
IBM Tivoli Directory Server	Si vous souhaitez installer IBM Tivoli Directory Server en tant que registre de Security Access Manager, les composants suivants sont requis : • IBM Global Security Kit (GSKit) • DB2 Enterprise Server Edition • Client IBM Tivoli Directory Server • Serveur IBM Tivoli Directory Server
Runtime for Java	• Licence Security Access Manager • IBM Java • IBM Security Access Manager Runtime for Java
Serveur proxy de règles	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Policy Proxy Server
Serveur de règles	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Policy Server
Runtime	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime
Web Portal Manager	• IBM WebSphere Application Server (sur un DVD et une image Passport Advantage séparés) • Licence Security Access Manager • IBM Java • IBM Security Access Manager Runtime for Java • Security Access Manager Web Portal Manager

Systèmes de sécurité Web Security Access Manager

Chaque système de sécurité Web Security Access Manager implique des exigences spécifiques en termes de composants.

Le tableau 2 répertorie les types de système de sécurité Web que vous pouvez configurer dans votre domaine sécurisé. Les composants d'installation de ces systèmes figurent sur le support du produit correspondant à votre système d'exploitation.

Remarque : Vous devez installer le client IBM Tivoli Directory Server sur chaque système exécutant Security Access Manager, avec les exceptions suivantes :

- Le système Security Access Manager se trouve sur un système Windows pris en charge qui est soit le domaine Active Directory, soit associé au domaine Active Directory où le serveur de règles Security Access Manager doit être configuré.
- Vous configurez le composant Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, ou Security Access Manager Web Portal Manager.

Tableau 2. Composants requis pour les systèmes de sécurité Web Security Access Manager

Type de système	Composants d'installation
Attribute Retrieval Service	• IBM WebSphere Application Server (sur un DVD et une image Passport Advantage séparés) • Security Access Manager Attribute Retrieval Service
WebSEAL	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access ManagerWebSEAL
Système Web Security Application Development Kit (ADK)	• IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Application Development Kit • Security Access Manager Web Security Runtime • Security Access Manager Web Security Application Development Kit
Plug-in for Apache Web Server	• Apache Web Server (non fourni avec le produit Security Access Manager) • IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager Plug-in for Web Servers • Security Access Manager Plug-in for Apache Web Server

Tableau 2. Composants requis pour les systèmes de sécurité Web Security Access Manager (suite)

Type de système	Composants d'installation
Plug-in for IBM HTTP Server	• IBM HTTP Server (non fourni avec le produit Security Access Manager) • IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager Plug-in for Web Servers • Security Access Manager Plug-in for IBM HTTP Server
Plug-in for Internet Information Services	• Internet Information Services (non fourni avec le produit Security Access Manager) • IBM Global Security Kit (GSKit) • Client IBM Tivoli Directory Server (en fonction du registre utilisé) • Licence Security Access Manager • IBM Security Utilities • Security Access Manager Runtime • Security Access Manager Web Security Runtime • Security Access Manager Plug-in for Web Servers • Security Access Manager Plug-in for Internet Information Services

Systèmes de gestion de sessions distribués Security Access Manager

Chaque système de gestion de sessions Security Access Manager implique des exigences spécifiques en termes de composants.

Le tableau 3, à la page 17 répertorie les types de systèmes de gestion de sessions que vous pouvez configurer dans votre domaine sécurisé. Les composants d'installation de ces systèmes figurent sur le support du produit correspondant à votre plateforme.

Remarque : Vous devez installer le client IBM Tivoli Directory Server sur chaque système exécutant Security Access Manager, avec les exceptions suivantes :

- Le système Security Access Manager se trouve sur un système Windows pris en charge qui est soit le domaine Active Directory, soit associé au domaine Active Directory où le serveur de règles Security Access Manager doit être configuré.
- Vous configurez le composant Security Access Manager Attribute Retrieval Service, IBM Security Access Manager Runtime for Java, ou Security Access Manager Web Portal Manager.

Tableau 3. Composants requis pour les systèmes de gestion de sessions Security Access Manager

Type de système	Composants d'installation
Session Management Server	• IBM WebSphere Application Server (sur un DVD et une image Passport Advantage séparés) • Licence Security Access Manager • Security Access Manager Session Management Server
ligne de commande de gestion des sessions	• IBM Global Security Kit (GSKit) • Security Access Manager Session Management Command Line • Licence Security Access Manager • IBM Security Utilities Si vous souhaitez utiliser l'utilitaire Security Access Manager **pdadmin** pour gérer des sessions, les composants suivants sont également requis : • Licence Security Access Manager • Security Access Manager Runtime • Security Access Manager Authorization Server • Security Access Manager Session Management Command Line • Client IBM Tivoli Directory Server (en fonction du registre utilisé)

Activation de la conformité SSL et TLS

Vous pouvez configurer Security Access Manager pour assurer sa conformité à diverses normes de sécurité. Ces normes sont généralement utilisées pour répondre aux exigences de sécurité, telles que celles requises par le gouvernement américain.

Security Access Manager utilise la cryptographie dans les tâches suivantes :

- Pour créer et remplacer des certificats internes auto-signés. Ces certificats sont utilisés par Security Access Manager Runtime et par le serveur Security Access Manager afin de s'authentifier mutuellement.
- Communication sécurisée entre le programme d'exécution et les serveurs.
- Communication sécurisée avec LDAP.
- Communication sécurisée avec les serveurs Syslog.

Les normes de sécurité suivantes sont exigées par le gouvernement américain :

FIPS 140-2
Normes FIPS (Federal Information Processing Standards) qui spécifient les exigences applicables aux modules cryptographiques. Pour plus d'informations, visitez le site Web du National Institute of Standards and Technology : http://csrc.nist.gov/publications/PubsFIPS.html.

SP800-131
Exigence du National Institute of Standards and Technology (NIST) qui requiert des clés plus longues et une cryptographie plus forte. La

spécification fournit également une configuration de transition permettant aux utilisateurs de passer à une application stricte de la norme SP800-131. La norme SP800-131 peut être exécutée dans deux modes : `transition` et `strict`.

L'application stricte des exigences SP800-131 implique les points suivants :

- L'utilisation de protocole tlsv1.2.
- Les certificats doivent avoir une longueur minimale de 2048. Les certificats EC (Elliptical Curve) exigent des courbes d'une taille minimale de 244 bits.
- Les certificats doivent être signés à l'aide d'un algorithme de signature SHA256, SHA384 ou SHA512. Les algorithmes de signature valides comprennent :
  - SHA256withRSA
  - SHA384withRSA
  - SHA512withRSA
  - SHA256withECDSA
  - SHA384withECDSA
  - SHA512withECDSA
  - Algorithmes de chiffrement approuvés par la norme SP800-131

  Pour plus d'informations sur cette norme, visitez le site Web du National Institute of Standards and Technology : http://csrc.nist.gov/publications/PubsSPs.html.

Suite B

Exigence de l'agence nationale de sécurité (NSA) américaine de spécifier une stratégie d'interopérabilité cryptographique. Cette norme est similaire à SP800-131 avec quelques limitations plus strictes. L'algorithme Suite B peut fonctionner dans deux modes : 128 bits ou 192 bits. Si vous utilisez le mode 192 bits avec les applications Java de Security Access Manager, vous devez appliquer le fichier de règles non restreint au kit JDK afin de pouvoir exploiter l'algorithme de chiffrement le plus fort que ce mode requiert.

Les exigences relatives à Suite B sont les suivantes :

- L'utilisation de protocole tlsv1.2.
- Algorithmes de chiffrement approuvés par la Suite B
- Certificats :
  - Les certificats en mode 128 bits doivent être signés avec SHA256withECDSA
  - Les certificats en mode 192 bits doivent être signés avec SHA384withECDSA
- Chiffrements :
  - SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Chapitre 2. Méthodes d'installation

Vous disposez de plusieurs options pour installer les composants Security Access Manager ainsi que leurs prérequis.

Les tableaux suivants décrivent les méthodes pour chaque système d'exploitation.

Tableau 4. Méthodes d'installation pour AIX, Linux ou Solaris

Méthode	Description
Ligne de commande	Fournit les utilitaires spécifiques aux plateformes pour installer les composants Security Access Manager. Si vous appliquez cette méthode, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.
Script	Fournit les exemples de scripts pour une installation sans assistance (mode silencieux). Lorsque vous exécutez le script pour chaque composant, tous les prérequis de ce composant sont également installés. Si les composants prérequis sont déjà installés, le script d'installation ignore cette installation et poursuit jusqu'à ce que tous les prérequis soient installés. **Remarque :** Vous ne pouvez pas installer le service d'extraction d'attribut avec le script. Utilisez la méthode de la ligne de commande.

Tableau 5. Méthodes d'installation pour Windows

Méthode	Description
Tableau de bord	Fournit une interface utilisateur graphique pour l'installation étape par étape et la configuration initiale. Vous pouvez accomplir les tâches d'installation suivantes à l'aide du tableau de bord : • Installer les logiciels prérequis, tels qu'IBM Java Runtime ou GSKit. • Installer Tivoli Directory Server (si vous souhaitez utiliser celui-ci en tant que registre d'utilisateurs). • Installer les composants de Security Access Manager. • Démarrer l'outil de configuration interactif (pdconfig). **Remarque :** Vous ne pouvez pas installer le service d'extraction d'attribut avec le tableau de bord. Utilisez la méthode de la ligne de commande.

© Copyright IBM Corp. 2001, 2013

Tableau 5. Méthodes d'installation pour Windows (suite)

Méthode	Description
Ligne de commande	Fournit une commande Windows qui ouvre un programme graphique permettant d'installer les composants Security Access Manager. Si vous appliquez cette méthode, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.
Script	Fournit les exemples de scripts pour une installation sans assistance (mode silencieux). Lorsque vous exécutez le script pour chaque composant, tous les prérequis de ce composant sont également installés. **Remarque :** Vous ne pouvez pas installer le service d'extraction d'attribut avec le script. Utilisez la méthode de la ligne de commande.

Chapitre 3. Organigramme d'installation

Utilisez cette planification pas à pas pour configurer votre environnement Security Access Manager.

Procédure

1. Planifiez votre installation.

Tableau 6. Tâches de planification

Tâche	Pour plus d'informations
Planifiez le déploiement de Security Access Manager. Assurez-vous d'avoir bien compris les exigences de sécurité d'entreprise nécessitant le déploiement de Security Access Manager.	«Planification du déploiement», à la page 3
Déterminez quelle combinaison de systèmes Security Access Manager doit être installée. Un registre pris en charge et le système de serveur de règles sont nécessaires pour configurer le domaine de gestion initial.	«Présentation du domaine sécurisé», à la page 4
Décidez quel type de registre d'utilisateurs vous prévoyez d'utiliser.	«Registres pris en charge», à la page 11
Prenez note des composants que vous devez installer pour votre déploiement.	«Composants et prérequis pour les système Security Access Manager», à la page 13
Choisissez une méthode d'installation.	Chapitre 2, «Méthodes d'installation», à la page 19

2. Préparez vos systèmes en vue de l'installation et installez les logiciels prérequis.

Tableau 7. Tâches prérequises

Tâche	Pour plus d'informations
Préparez le système d'exploitation en vue de l'installation.	«Préparation du système d'exploitation», à la page 28
Déterminer les tâches prérequises pour votre environnement, ainsi que la méthode d'installation, et effectuer ces tâches.	Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

3. Installez et configurez les composants du système de base.
   a. Installez le composant du serveur de règles pour établir votre domaine de gestion.

Tableau 8. Tâches du serveur de règles

Tâche	Pour plus d'informations
Installez le serveur de règles.	Chapitre 6, «Configuration d'un serveur de règles», à la page 109

© Copyright IBM Corp. 2001, 2013

Tableau 8. Tâches du serveur de règles (suite)

Tâche	Pour plus d'informations
Si vous envisagez d'utiliser un serveur de règles de secours, installez-le et configurez-le.	• Annexe G, «Configuration du serveur de règles de secours (AIX)», à la page 381. • Annexe H, «Configuration d'un serveur de règles de secours avec IBM Tivoli System Automation for Multiplatforms», à la page 397

b. Installez et configurez les autres systèmes Security Access Manager de base nécessaires à votre déploiement.

Tableau 9. Tâches liées aux composants système de base

Tâche	Pour plus d'informations
Installez et configurez Security Access Manager Authorization Server.	Chapitre 7, «Configuration du serveur d'autorisation», à la page 129
Installez et configurez Security Access Manager Application Development Kit (ADK).	Chapitre 8, «Configuration d'un système de développement», à la page 143
Installez et configurez IBM Security Access Manager Runtime for Java.	Chapitre 9, «Configuration d'un système IBM Security Access Manager Runtime for Java», à la page 155
Installez et configurez Security Access Manager Policy Proxy Server.	Chapitre 10, «Configuration d'un système de serveur proxy de règles», à la page 167
Installez et configurez Security Access Manager Runtime.	Chapitre 11, «Configuration d'un système d'exécution», à la page 181
Installez et configurez Security Access Manager Web Portal Manager.	Chapitre 12, «Configuration d'un système Web Portal Manager», à la page 195

4. Installez les systèmes de sécurité Web Security Access Manager nécessaires à votre déploiement.

Tableau 10. Tâches liées aux composants de sécurité Web

Tâche	Pour plus d'informations
Installez et configurez Security Access Manager Attribute Retrieval Service.	Chapitre 13, «Configuration de Security Access Manager Attribute Retrieval Service», à la page 223
Installez et configurez Security Access Manager Plug–in for Web Servers.	Chapitre 14, «Configuration du composant Plug-in for Web Servers», à la page 229
Installez et configurez Security Access Manager Web Security Application Development Kit (ADK).	Chapitre 15, «Configuration d'un système de développement de sécurité Web», à la page 253
Installez et configurez Security Access Manager WebSEAL.	Chapitre 16, «Configuration de WebSEAL», à la page 265

5. Installez les systèmes distribués de gestion de sessions Security Access Manager nécessaires à votre déploiement.

Tableau 11. Tâche de gestion de sessions

Tâche	Pour plus d'informations
Installez Security Access Manager Session Management Server.	Chapitre 17, «Configuration d'un serveur de gestion de sessions», à la page 281

Tableau 11. Tâche de gestion de sessions (suite)

Tâche	Pour plus d'informations
Installez Security Access Manager Session Management Command Line.	«Configuration du serveur de gestion de sessions via les utilitaires de ligne de commande», à la page 312

6. Utilisez un certificat émis par une autorité de certification pour activer la communication SSL entre votre serveur de registre pris en charge et les clients IBM Tivoli Directory Server. Voir Annexe A, «Configuration de la sécurité SSL (Secure Sockets Layer)», à la page 327.
7. Facultatif : Installez IBM Tivoli Directory Integrator si vous avez besoin de ses fonctions dans votre environnement.

   Tivoli Directory Integrator permet de renforcer la sécurité, la fidélité et l'intégrité des données génériques et relatives à l'identité des utilisateurs. Ce logiciel facilite la migration des données, la transformation en d'autres formats de fichiers, ainsi que la synchronisation entre deux systèmes ou plus. Ce composant inclut en outre le connecteur 7.1.1 d'IBM Tivoli Directory Integrator pour Security Access Manager.

   Le connecteur permet la mise à disposition et la gestion des sources de données de Security Access Manager sur les applications externes. Les sources de données sont les suivantes :

   - Comptes utilisateur
   - Groupes
   - Règles
   - Domaines
   - Ressources SSO
   - Groupes de ressources SSO
   - Données d'identification utilisateur SSO

   Le connecteur utilise l'API Java de Security Access Manager. Pour plus d'informations sur ce connecteur et sur l'installation de Tivoli Directory Integrator (y compris la configuration système requise), voir le chapitre relatif à l'installation dans le manuel *IBM Tivoli Directory Integrator Installation and Administrator Guide*. Celui-ci est disponible sur le centre de documentation http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDI.doc_7.1/toc.xml.

Partie 2. Installation de logiciels prérequis

© Copyright IBM Corp. 2001, 2013

Chapitre 4. Plan des installations et configurations prérequises

Avant l'installation des composants Security Access Manager, les systèmes présents dans votre environnement doivent répondre aux conditions requises.

1. Effectuez la procédure décrite à la section «Préparation du système d'exploitation», à la page 28.
2. Les prochaines étapes dépendent des variables d'environnement suivantes :
   - Le système d'exploitation sur lequel vous installez les composants.
   - La méthode d'installation que vous prévoyez d'utiliser.
   - Le registre d'utilisateurs que vous prévoyez d'utiliser.

   Consultez le tableau pour déterminer les étapes ultérieures.

Tableau 12. Tâches relatives à l'installation et à la configuration des logiciels prérequis

Système d'exploitation et méthode d'installation du composant	**Tâches prérequises**
Windows à l'aide du tableau de bord	1. Configurez votre registre d'utilisateurs. Voir Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51. 2. Installez les composants : • Partie 3, «Installation du composant système de base», à la page 107 • Partie 4, «Installation du composant système de sécurité Web», à la page 221 • Partie 5, «Installation du composant système de gestion des sessions», à la page 279
Windows, AIX, Linux ou Solaris à l'aide des fichiers scripts	1. Configurez votre registre d'utilisateurs. Voir Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51. 2. Installez les composants : • Partie 3, «Installation du composant système de base», à la page 107 • Partie 4, «Installation du composant système de sécurité Web», à la page 221 • Partie 5, «Installation du composant système de gestion des sessions», à la page 279

© Copyright IBM Corp. 2001, 2013

Tableau 12. Tâches relatives à l'installation et à la configuration des logiciels prérequis (suite)

Système d'exploitation et méthode d'installation du composant	Tâches prérequises
Windows, AIX, Linux ou Solaris via une ligne de commande	1. Configurez tous les logiciels requis pour votre environnement. a. Voir «Composants et prérequis pour les système Security Access Manager» , à la page 13. Notez les logiciels que vous devez installer. b. Installez les logiciels requis : • «Installation d'IBM Java Runtime», à la page 32 • «Installation d'IBM Global Security Kit (GSKit)», à la page 35 • «Installation de la licence IBM Security Access Manager», à la page 38 • «Installation d'IBM Security Utilities», à la page 40 • «Installation du client IBM Tivoli Directory Server», à la page 43 • «Installation de WebSphere Application Server», à la page 47 2. Configurez le registre d'utilisateurs. Voir Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51. 3. Installez les composants : • Partie 3, «Installation du composant système de base», à la page 107 • Partie 4, «Installation du composant système de sécurité Web», à la page 221 • Partie 5, «Installation du composant système de gestion des sessions», à la page 279

Préparation du système d'exploitation

Avant de commencer l'installation des logiciels prérequis, assurez-vous que votre système d'exploitation est bien préparé.

Vérifiez que vous avez consulté les informations de version les plus récentes, notamment les exigences concernant les correctifs des systèmes d'exploitation, la configuration système requise, les exigences d'espace disque, les incidents connus et les limitations. Consultez les notes sur l'édition dans le centre de documentation et les notes techniques dans la base de connaissances du support.

- «Préparation d'un système AIX», à la page 29
- «Préparation d'un système Linux», à la page 30
- «Préparation d'un système Windows», à la page 31
- «Préparation d'un système Solaris», à la page 31

Préparation d'un système AIX

Avant d'installer les logiciels prérequis sur un système AIX, effectuez les étapes de cette tâche pour garantir que le système est correctement configuré.

Procédure

1. Consultez les informations de version les plus récentes, notamment les exigences concernant les correctifs des systèmes d'exploitation, les exigences d'espace disque, les incidents connus et les limitations. Consultez les notes sur l'édition dans le centre de documentation et les notes techniques dans la base de connaissances du support.
2. Vérifiez que votre système utilise du matériel 64 bits. A l'invite de commande, entrez :

   ```
   bootinfo –y
   ```

   Si le résultat affiche 64, votre matériel est de type 64 bits. De plus, si vous entrez la commande **lsattr -El proc0**, sa sortie renvoie le type de processeur de votre serveur. Les types de processeurs suivants sont de 64 bits : RS64 I, II, III, IV, POWER3, POWER3 II, POWER4 ou POWER5
3. Vérifiez que votre système utilise un noyau 64 bits. A l'invite de commande, entrez :

   ```
   bootinfo –K
   ```

   Si le résultat affiche 64, le noyau est de type 64 bits. En revanche, si le résultat est 32, vous devez passer du noyau 32 bits à un noyau 64 bits. Pour ce faire, procédez comme suit.

   a. Assurez-vous d'avoir les packages 64 bits suivants :

      ```
      bos.64bit
      bos.mp64
      ```

   b. Pour passer au noyau 64 bits, entrez les commandes suivantes :

      ```
      ln -sf /usr/lib/boot/unix_64 /unix
      ln -sf /usr/lib/boot/unix_64 /usr/lib/boot/unix
      lslv -m hd5
      ```

      La sortie de la commande **lslv** est similaire à la sortie suivante :

      ```
      #lslv -m hd5
      hd5:N/A
      LP PP1 PV1PP2 PV2PP3 PV3
      0001 0001 hdisk0
      ```

   c. Entrez :

      ```
      bosboot -ad /dev/unité_ipl
      ```

      où *ipldevice* est l'unité de disque dur qui est affichée lors de l'exécution de la commande **lslv**. La sortie de la commande **bosboot** est similaire à la sortie suivante :

      ```
      #bosboot -ad/dev/hdisk0
      bosboot: Boot image is 13025 512 byte blocks
      ```

   d. Entrez :

      ```
      shutdown -Fr
      ```
4. Assurez-vous que les E-S asynchrones sont activées. Pour ce faire, entrez les commandes suivantes :

   ```
   /usr/sbin/mkdev -l aio0
   /usr/sbin/chdev -l aio0 -P
   /usr/sbin/chdev -l aio0 -P -a autoconfig=available
   ```

5. Facultatif : Si vous prévoyez d'installer Tivoli Directory Server sur AIX 6.1, vous devez effectuer la mise à niveau vers AIX 6.1 TL 2 ou une version supérieure requise par DB2 9.7. Reportez-vous à la documentation de DB2 pour connaître la configuration système requise pour IBM DB2 9.7 : http://www.ibm.com/software/data/db2/udb/sysreqs.html

Préparation d'un système Linux

Avant d'installer les logiciels prérequis sur un système Linux, effectuez les étapes de cette tâche pour garantir que le système est correctement configuré.

Procédure

1. **Sur les systèmes Linux uniquement (tous systèmes d'exploitation)**, effectuez les tâches ci-après.
   a. Consultez les informations de version les plus récentes, notamment les exigences concernant les correctifs des systèmes d'exploitation, les exigences d'espace disque, les incidents connus et les limitations. Consultez les notes sur l'édition dans le centre de documentation et les notes techniques dans la base de connaissances du support.
   b. Sur certaines versions de Linux, le programme d'installation de Linux ne permet pas d'installer le shell Korn (`/bin/ksh`). Installez le fichier `ksh rpm` qui correspond au matériel sur lequel vous allez installer Security Access Manager. Le fichier `rpm` correspondant se trouve sur le support d'installation Linux ou peut être téléchargé depuis les sites Web d'assistance de Linux (SUSE, Red Hat, etc.). Si le fichier `ksh rpm` n'est pas installé, il se peut que l'exécution des scripts échoue durant la configuration de Security Access Manager. Une erreur s'affiche pour indiquer que le répertoire `/bin/ksh` est introuvable.
   c. Si vous avez installé le système d'exploitation Red Hat Enterprise Linux avec `SELINUX` activé (valeur par défaut), la création de l'instance échoue. Si le paramètre `SELINUX` est activé, utilisez la commande `setenforce 0` le désactiver. Puis, dans le fichier `/etc/selinux/config`, modifiez `SELINUX=enforcing` en `SELINUX=disabled`.
   d. Si vous installez Tivoli Directory Server, il peut être nécessaire de spécifier manuellement certains paramètres de DB2 avant l'installation de Tivoli Directory Server. Les paramètres incluent le noyau préliminaire, le système d'exploitation et les paramètres de l'interpréteur de commandes. Consultez la documentation de DB2 pour obtenir des instructions sur la configuration de ces paramètres : http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/index.jsp
   e. Installez les composants du système d'exploitation éventuellement requis pour la version de DB2 que vous utilisez. Pour les exigences concernant DB2, visitez le site http://www.ibm.com/software/data/db2/udb/sysreqs.html.
   f. Pour installer IBM Java Runtime avec succès sur un système Red Hat Enterprise Linux 5, assurez-vous que les bibliothèques de compatibilité suivantes sont installées :

      ```
      compat-libstdc-++-33-3.2.3
      ```

2. **Sur les systèmes Linux 64 bits uniquement**, installez les bibliothèques 32 bits suivantes à partir des packages *i686.rpm :

   ```
   ld-linux.so.2
   libstdc++.so.6
   ```

3. **Sur les systèmes Linux on System z uniquement**, effectuez les tâches ci-après.

a. Obtenez l'accès aux fichiers `rpm` Linux du support du produit pour Linux sur System z. Les fichiers `rpm` se trouvent dans le répertoire */package_path*/`linux_s390`.

b. Assurez-vous que vous utilisez les noyaux 64 bits suivants : Entrez la commande suivante :

```
uname -m
```

Si le résultat affiche `s390x`, vous exécutez un noyau 64 bits.

Si le résultat affiche `s390`, vous n'exécutez pas de noyau 64 bits.

c. IBM requiert le nom d'hôte du noeud réseau de la machine. Pour vous assurer que votre système est correctement configuré, entrez la commande suivante :

```
uname -n
```

Si le résultat affiche le nom d'hôte d'un noeud, vous pouvez poursuivre l'installation et la configuration de Security Access Manager. Si tel n'est pas le cas, consultez la documentation de votre système d'exploitation pour obtenir des instructions sur la configuration du nom d'hôte du noeud réseau de la machine.

Préparation d'un système Windows

Avant de commencer à installer les logiciels prérequis sur un système Windows, effectuez les étapes de cette tâche afin de garantir que le système est configuré correctement.

Procédure

1. Consultez les informations de version les plus récentes, notamment les exigences concernant les correctifs des systèmes d'exploitation, les exigences d'espace disque, les incidents connus et les limitations. Consultez les notes sur l'édition dans le centre de documentation et les notes techniques dans la base de connaissances du support.
2. Toutes les méthodes d'installation de Security Access Manager sur un système Windows nécessitent IBM Java. Avant de commencer une installation, assurez-vous qu'IBM Java est disponible dans l'environnement. Effectuez l'une des actions suivantes :
   - Autorisez la méthode d'installation (ligne de commande, tableau de bord ou script) à installer IBM Java pour vous. Passez à l'étape Chapitre 6, «Configuration d'un serveur de règles», à la page 109 avec la méthode d'installation de votre choix.
   - Installez IBM Java avant de démarrer une procédure d'installation. Voir «Windows : Installation d'IBM Java Runtime», à la page 34.
   - Assurez-vous que le chemin d'accès à une installation de Java est spécifié dans la variable `PATH` de votre environnement. Par exemple, à une invite de commande, tapez :

     ```
     set Path=c:\Program Files\IBM\Java60\jre\bin;%Path%
     ```

Préparation d'un système Solaris

Avant d'installer les logiciels prérequis sur un système Solaris, effectuez les étapes de cette tâche pour garantir que le système est correctement configuré.

Procédure

1. Consultez les informations de version les plus récentes, notamment les exigences concernant les correctifs des systèmes d'exploitation, les exigences

d'espace disque, les incidents connus et les limitations. Reportez-vous au manuel *IBM Security Access Manager for Web : Notes sur l'édition* et aux notes techniques dans la base de connaissances du support.

2. Installez les composants du système d'exploitation éventuellement requis pour la version de DB2 que vous utilisez. Pour les exigences concernant DB2, visitez le site http://www.ibm.com/software/data/db2/udb/sysreqs.html.

Installation d'IBM Java Runtime

Installez IBM Java Runtime avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

IBM Java Runtime est fourni avec Security Access Manager.

IBM Security Access Manager Runtime for Java prend uniquement en charge la version d'IBM Java Runtime fournie avec Security Access Manager ou l'environnement JRE fourni avec IBM WebSphere Application Server.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

AIX : Installation d'IBM Java Runtime

Installez IBM Java Runtime sur AIX avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Installez les modules suivants :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où *chemin_package* désigne le répertoire sur lequel le DVD est monté et *packages*, les packages suivants :

   Java6_64.samples
   Indique le package d'exemples de fichiers IBM Java Runtime.

   Java6_64.sdk
   Indique le package d'extensions SDK IBM Java Runtime.

   Java6_64.source
   Indique le package de fichiers source IBM Java Runtime.
4. Une fois l'installation terminée, effectuez l'une des tâches suivantes :
   - Définissez la variable d'environnement PATH. Par exemple :

     ```
     export PATH=/usr/java6_64/bin:$PATH
     ```

     Remarque : Pour afficher si IBM Java Runtime est déjà dans le chemin, utilisez la commande **java –version**.

- Définissez la variable d'environnement JAVA_HOME sur le chemin où vous avez installé IBM Java Runtime. Par exemple, utilisez **ksh** et entrez la commande suivante pour définir JAVA_HOME :

  ```
  export JAVA_HOME=/usr/java6_64/
  ```

Résultats

Une fois l'installation d'IBM Java Runtime effectuée, aucune configuration n'est nécessaire.

Linux : Installation d'IBM Java Runtime

Installez IBM Java Runtime sur Linux avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Remarque à l'attention des utilisateurs Linux sur System z : vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux. Les fichiers `rpm` se trouvent dans le répertoire */package_path*`/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire *chemin_package*`/`*distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
4. Installez le package IBM Java Runtime :

   ```
   rpm -ihv package
   ```

   où *package* désigne les éléments suivants :

Linux sur x86-64	ibm-java-x86_64-sdk-6.0-10.0.x86_64.rpm (64 bits)
Linux on System z	ibm-java-s390x-sdk-6.0-10.0.s390x.rpm

5. Définissez la variable d'environnement PATH :

   ```
   export PATH=chemin_jre:$PATH
   ```

   Par exemple, pour s'assurer qu'IBM Java Runtime est accessible via la variable d'environnement PATH, entrez la commande suivante :

   ```
   export PATH=/opt/ibm/java-x86_64-60/jre/bin:$PATH
   ```

Résultats

Une fois l'installation d'IBM Java Runtime effectuée, aucune configuration n'est nécessaire.

Solaris : Installation d'IBM Java Runtime

Installez IBM Java Runtime sur Solaris avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Installez le package IBM Java Runtime :
   a. Entrez : `mkdir -p /opt/ibm/solaris`
   b. Procédez à l'extraction du fichier :
      chemin_package_IBM_Java`/sol6460sr10hybrid-20111110_01-sdk.tar.Z`

      vers le répertoire `/opt/ibm/solaris`.
4. Une fois l'installation terminée, effectuez l'une des tâches suivantes.
   - Définissez la variable d'environnement PATH.
     `export PATH=`*chemin_java*`:$PATH` Par exemple :
     `export PATH=/opt/ibm/solaris/jre/bin:$PATH`

     Remarque :
     – Le programme d'installation suppose que le JRE est installé dans l'emplacement par défaut utilisé dans l'exemple.
     – Pour indiquer si IBM JavaRuntime se trouve déjà dans le chemin, utilisez la commande **`java –version`**.
   - Si vous prévoyez d'utiliser un chemin d'installation différent de celui par défaut, définissez la variable d'environnement JAVA_HOME sur le chemin où vous prévoyez d'installer IBM Java Runtime. Par exemple, entrez la commande suivante pour définir JAVA_HOME :
     `export JAVA_HOME=/opt/ibm/solaris`

Résultats

Une fois l'installation d'IBM Java Runtime effectuée, aucune configuration n'est nécessaire.

Windows : Installation d'IBM Java Runtime

Installez IBM Java Runtime sur Windows avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web. Vous pouvez également installer IBM Java avant d'utiliser les scripts d'installation ou le tableau de bord.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

3. Entrez la commande suivante :

   ```
   chemin_package\windows\JDK\
   run ibm-java-sdk-60-win-x86_64.exe
   ```

4. Procédez à l'installation en suivant les invites. Lorsque le message `Installer cet environnement Java Runtime Environment en tant que JVM système ?`, cliquez sur **Oui**.
5. Une fois l'installation terminée, cliquez sur **Terminer**.
6. Si vous prévoyez d'utiliser l'utilitaire iKeyman, procédez comme suit.
   a. Définissez la variable d'environnement JAVA_HOME sur le chemin d'accès complet à votre installation de Java. Par exemple :

      ```
      set JAVA_HOME=c:\Program Files\IBM\Java60\jre
      ```

   b. Ajoutez les répertoires GSKit `bin` et `lib` à la variable PATH. Par exemple :

      ```
      set PATH="C:\Program Files\ibm\gsk8\bin";%PATH%
      set PATH="C:\Program Files\ibm\gsk8\lib";%PATH%
      ```

Résultats

Une fois l'installation d'IBM Java Runtime effectuée, aucune configuration n'est nécessaire.

Installation d'IBM Global Security Kit (GSKit)

Installez IBM Global Security Kit (GSKit) avant d'utiliser la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

IBM Global Security Kit (GSKit) fournit la fonction de chiffrement de données SSL (Secure Sockets Layer) entre les systèmes Security Access Manager et les serveurs de registre pris en charge.

Le package GSKit installe également l'outil GSKCapiCmd, qui vous permet de créer des bases de données de clés, des paires de clés publique-privée et des demandes de certificat.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Reportez-vous aux informations de la section «Composants et prérequis pour les système Security Access Manager», à la page 13 pour obtenir une liste de composants qui requièrent le client GSKit Tivoli Directory Server en tant que prérequis.

Remarque : Les versions précédentes de GSKit contiennent un utilitaire appelé **`ikeyman`**. Cet utilitaire fait maintenant partie d'IBM Java. Si vous souhaitez utilisez ikeyman avec les fichiers de la base de données de clés Security Access Manager version 7.0, vous devez modifier le fichier `java.security`, puis ajouter le fournisseur de sécurité Java CMS. Pour plus d'informations, consultez le manuel *IBM Developer Kit and Runtime Environment, Java Technology Edition, Version 6 and 7 iKeyman User's Guide for version 8.0* http://download.boulder.ibm.com/ibmdl/pub/software/dw/jdk/security/60/iKeyman.8.User.Guide.pdf.

AIX : Installation d'IBM Global Security Kit (GSKit)

Installez GSKit sur AIX avant d'utiliser la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Entrez les commandes suivantes pour installer le module d'exécution :

   ```
   installp -acgXd . GSKit8.gskcrypt64.ppc.rte
   installp -acgXd . GSKit8.gskssl64.ppc.rte
   ```

   où :

   - `-a` signifie "apply"
   - `-c` signifie "commit"
   - `-g` installe ou valide automatiquement les logiciels prérequis
   - `-X` développe le système de fichiers, si nécessaire
   - `-d` signifie "device". Cette option indique où trouver le support d'installation.

Résultats

Une fois l'installation de GSKit effectuée, aucune configuration supplémentaire n'est nécessaire.

Linux : Installation d'IBM Global Security Kit (GSKit)

Installez GSKit sur Linux avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux du support produit pour Linux sur System z. Les fichiers `rpm` se trouvent dans le répertoire */package_path*`/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire *chemin_package*`/`*distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
4. Installez les packages IBM Global Security Kit (GSKit) spécifiques à votre système d'exploitation.
   - Linux pour x86-64

     ```
     rpm -ihv gskcrypt64-8.0.14.26.linux.x86_64.rpm
     rpm -ihv gskssl64-8.0.14.26.linux.x86_64.rpm
     ```

- Linux on System z, 64 bits

  ```
  rpm -ihv gskcrypt64-8.0.14.26.linux.s390x.rpm
  rpm -ihv gskssl64-8.0.14.26.linux.s390x.rpm
  ```

Solaris : Installation d'IBM Global Security Kit (GSKit)

Installez GSKit sur Solaris avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Pourquoi et quand exécuter cette tâche

La procédure suivante utilise **pkgadd** pour installer le progiciel.

Avertissement : Dans le cas d'une installation sur Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Installez IBM Global Security Kit (GSKit). Spécifiez les packages suivants :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault -G
   gsk8cry64
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault -G
   gsk8ssl64
   ```

   où *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers. L'option `-G` ajoute le package uniquement dans la zone en cours.

Windows : Installation d'IBM Global Security Kit (GSKit)

Installez GSKit sur Windows avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire `\windows\GSKit`.
4. Démarrez l'installation à l'aide de la commande suivante :

   ```
   gsk8ssl64
   ```

5. Cliquez sur **Suivant**. La fenêtre Choose Destination Location s'affiche.

6. Acceptez le répertoire de destination par défaut ou cliquez sur **Parcourir** pour sélectionner un chemin d'accès à un autre répertoire sur le système local. Si le répertoire n'existe pas, vous devez confirmer que vous souhaitez le créer ou indiquer un répertoire existant.
7. Cliquez sur **Suivant** pour installer GSKit. La fenêtre Setup Complete s'affiche.
8. Cliquez sur **Terminer** pour quitter le programme d'installation.

Résultats

Une fois l'installation de GSKit effectuée, aucune configuration supplémentaire n'est nécessaire.

Installation de la licence IBM Security Access Manager

Installez la licence IBM Security Access Manager avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Reportez-vous aux informations de la section «Composants et prérequis pour les système Security Access Manager», à la page 13 pour obtenir une liste de composants qui requièrent la licence IBM Security Access Manager en tant que prérequis.

AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager

Installez la licence avant d'utiliser les méthodes de ligne de commande pour installer les composants IBM Security Access Manager for Web sur les systèmes d'exploitation AIX, Linux ou Solaris.

Pourquoi et quand exécuter cette tâche

Le script `isamLicense` exécute un outil interactif qui affiche le texte de la licence. Sur chaque page de la licence, vous êtes invité à appuyez sur Entrée pour afficher le reste du contrat de licence, puis sur 1 pour accepter le contrat ou 2 pour le refuser, ou encore sur 99 pour revenir à la page précédente. Le script installe la licence dans le répertoire `/opt/PolicyDirector/license`. Après avoir exécuté le script et accepté la licence, vous devez installer celle-ci.

Remarque : L'acceptation de la licence signifie la reconnaissance de ses conditions.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Ouvrez une fenêtre de commande.
4. Placez-vous dans le répertoire `/scripts` de l'image d'installation.
5. Exécutez le script `isamLicense`.

   ```
   isamLicense
   ```

   Le script `isamLicense` comporte les options suivantes :

   -q Quiet : exécute le script sans afficher la licence. Cette option est utile dans les installations automatisées.

Avertissement : Lorsque vous utilisez cette option, vous acceptez automatiquement la licence sans l'afficher.

-f Force : force l'affichage de la licence et vous invite à l'accepter, même si la licence est déjà installée.

-t Test : vérification silencieuse pour déterminer si la licence en cours est déjà installée. Dans l'affirmative, la valeur `exit status 0 (SUCCESS)` est renvoyée.

-? Help : affiche la syntaxe du fichier script.

6. Prenez connaissance de la licence.
7. Acceptez la licence en appuyant sur 1.
8. Installez la licence :

AIX :

```
installp -acgYXd chemin_package/usr/sys/inst.images PD.lic
```

où : *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers.

Linux :

```
rpm -ihv package
```

où *package* désigne les éléments suivants :

- **Linux on x86 :** `PDlic-PD-7.0.0-0.x86_64.rpm`
- **Linux on System z :** `PDlic-PD-7.0.0-0.s390.rpm`

Solaris :

```
pkgadd -d /chemin_package/solaris
  -a /chemin_package/solaris/pddefault PDlic
```

où :

/chemin_package/solaris
Indique l'emplacement du package.

/chemin_package/solaris/pddefault
Indique l'emplacement du script d'administration de l'installation.

Remarque : Lorsque vous installez le package PDlic, le message suivant s'affiche :

```
The following files are already installed on the system and
are being used by another package:
* /opt/PolicyDirector/attribute_change_only
* /-conflict with a file that does not belong to any package.
Do you want to install these conflicting files [y, n, ?, q]
```

Répondez y à cette question.

Que faire ensuite

L'installation de la licence est terminée. Poursuivez l'installation d'un autre produit ou système prérequis pour Security Access Manager. Suivez les étapes indiquées à la rubrique Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation de la licence IBM Security Access Manager

Installez la licence avant d'appliquer la méthode de la ligne de commande pour installer les composants IBM Security Access Manager for Web sur les systèmes d'exploitation Windows.

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Exécutez le programme **setup.exe** dans ce répertoire :

   `\windows\PolicyDirector\Disk Images\Disk1\PDLIC\Disk Images\Disk1`

   Suivez les instructions en ligne et sélectionnez l'installation de Security Access Manager License.

Que faire ensuite

L'installation de la licence est terminée. Poursuivez l'installation d'un autre produit ou système prérequis pour Security Access Manager. Suivez les étapes indiquées à la rubrique Chapitre 3, «Organigramme d'installation», à la page 21.

Installation d'IBM Security Utilities

Installez IBM Security Utilities avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

IBM Tivoli Security Utilities fournit des utilitaires communs requis par Security Access Manager Runtime.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Reportez-vous aux informations de la section «Composants et prérequis pour les système Security Access Manager», à la page 13 pour obtenir une liste de composants qui requièrent IBM Security Utilities en tant que prérequis.

AIX : Installation d'IBM Security Utilities

Installez IBM Security Utilities avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Entrez la commande suivante pour installer le package :

   `installp -acgYXd` *`chemin_package`*`/usr/sys/inst.images TivSec.Utl`

où *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers.

Avertissement : Vous devez installer le package IBM Security Utilities avant d'installer le package Security Access Manager Runtime.

4. Démontez, le cas échéant, le DVD.

Résultats

Une fois l'installation d'IBM Security Utilities effectuée, aucune configuration n'est nécessaire.

Cette étape termine la configuration d'IBM Security Utilities. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation d'IBM Security Utilities

Installez IBM Security Utilities avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire *chemin_package/distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
4. Installez le module :

   ```
   rpm -ih package
   ```

   où *package* désigne les éléments suivants :

   - Linux on x86-64 : `TivSecUtl-TivSec-7.0.0-0.x86_64.rpm`
   - Linux on System z : `TivSecUtl-TivSec-7.0.0-0.s390x.rpm`

   Avertissement : Vous devez installer le package IBM Security Utilities avant d'installer le package Security Access Manager Runtime.
5. Démontez, le cas échéant, le DVD.

Résultats

Une fois l'installation d'IBM Security Utilities effectuée, aucune configuration n'est nécessaire.

Cette étape termine la configuration d'IBM Security Utilities. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation d'IBM Security Utilities

Installez IBM Security Utilities avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Pourquoi et quand exécuter cette tâche

La procédure suivante utilise **pkgadd** pour installer le progiciel.

Avertissement : Dans le cas d'une installation sur Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Cette étape termine la configuration d'IBM Security Utilities. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Pour installer le package IBM Security Utilities, entrez la commande suivante :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault
   -G TivSecUtl
   ```

   où */chemin_package*/solaris indique l'emplacement du package et */chemin_package*/solaris/pddefault indique celui du script d'administration de l'installation.

   Avertissement : Vous devez installer le package IBM Security Utilities avant d'installer le package Security Access Manager Runtime.

Résultats

Une fois l'installation d'IBM Security Utilities effectuée, aucune configuration n'est nécessaire.

Windows : Installation d'IBM Security Utilities

Installez IBM Security Utilities avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire suivant :

   ```
   \windows\TivSecUtl\Disk Images\Disk1
   ```

4. Exécutez le programme **setup.exe** à partir de ce répertoire.
5. Sélectionnez la langue d'installation.
6. Cliquez sur **Suivant**.
7. Cliquez sur **Accepter** pour accepter le contrat de licence. La fenêtre Choose Destination Location s'affiche.
8. Acceptez le répertoire de destination par défaut ou cliquez sur **Parcourir** pour sélectionner un chemin d'accès à un autre répertoire sur le système local. Si le répertoire n'existe pas, vous devez confirmer que vous souhaitez le créer ou indiquer un répertoire existant.
9. Cliquez sur **Suivant** pour installer IBM Security Utilities. La fenêtre Setup Complete s'affiche.

Résultats

Une fois l'installation d'IBM Security Utilities effectuée, aucune configuration n'est nécessaire.

Cette étape termine la configuration d'IBM Security Utilities. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Installation du client IBM Tivoli Directory Server

Installez le client IBM Tivoli Directory Server avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web.

Remarque : Si vous envisagez d'exécuter l'installation du serveur pour IBM Tivoli Directory Server, vous n'avez pas besoin d'installer le client séparément. Voir Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51 pour plus d'informations sur les procédures d'installation de Tivoli Directory Server qui permettent d'installer à la fois le client et le serveur.

Le client IBM Tivoli Directory Server est inclus avec IBM Tivoli Directory Server sur les DVD Security Access Manager ou dans les fichiers Passport Advantage des systèmes d'exploitation pris en charge.

Vous devez explicitement installer le client Tivoli Directory Server sur chaque système qui exécute Security Access Manager, avec les exceptions suivantes :

- Le système Security Access Manager est un système Windows pris en charge qui est rattaché à un domaine Active Directory.
- Vous configurez IBM Security Access Manager Runtime for Java, Security Access Manager Web Portal Manager, Security Access Manager Attribute Retrieval Service, ou le serveur de gestion de sessions de Security Access Manager.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Reportez-vous aux informations de la section «Composants et prérequis pour les système Security Access Manager», à la page 13 pour obtenir une liste de composants qui requièrent le client IBM Tivoli Directory Server en tant que prérequis.

Remarque : Vous pouvez avoir plusieurs versions du client IBM Tivoli Directory Server installées sur le même système. Assurez-vous que le correctif correspondant à la version la plus récente disponible du client IBM Tivoli Directory Server que vous exécutez est installé.

AIX : Installation du client IBM Tivoli Directory Server

Installez le client IBM Tivoli Directory Server avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Installez les fichiers de licence Tivoli Directory Server en exécutant le script `idsLicense` dans le répertoire *chemin_image*`/usr/sys/inst.images/tdsLicense/license`, où *chemin_image* est le chemin d'accès à l'image du DVD, ou celui sous lequel lequel vous avez téléchargé le fichier d'archive à partir dePassport Advantage.
4. Installez les packages du client IBM Tivoli Directory Server. A l'invite de commande, entrez :

   ```
   installp -acgXd chemin_package/usr/sys/inst.images packages
   ```

   Le tableau 13 répertorie les packages requis pour chaque type de client. Installez les packages correspondant à votre client dans l'ordre indiqué.

   Pour installer plusieurs packages, séparez leurs noms par un espace.

Tableau 13. Packages de client pour AIX

Client	Packages	Descriptions des packages
Client 64 bits (sans SSL)	1. `idsldap.license63` 2. `idsldap.cltbase63` 3. `idsldap.clt64bit63`	1. Licence 2. Exécution du client de base et kit de développement de logiciel du client de base 3. Client 64 bits (sans SSL)
Client 64 bits (SSL)	1. `idsldap.license63` 2. `idsldap.cltbase63` 3. `idsldap.clt64bit63` 4. `idsldap.clt_max_crypto64bit63`	1. Licence 2. Exécution du client de base et kit de développement de logiciel du client de base 3. Client 64 bits (sans SSL) 4. Client 64 bits (SSL)
Client Java	`idsldap.cltjava63`	Le client Java est requis pour la prise en charge X11

   Remarque : Les versions serveur complètes requièrent un environnement X11. Pour un client sans exigence relative à X11, installez le client 64 bits comme si un environnement X11 était requis.
5. Le cas échéant, démontez le DVD comme suit :

   ```
   umount /dvd
   ```

où */dvd* désigne le point de montage.

Résultats

Une fois le client IBM Tivoli Directory Server installé, aucune configuration supplémentaire n'est nécessaire.

Linux : Installation du client IBM Tivoli Directory Server

Installez le client IBM Tivoli Directory Server avant d'appliquer la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Remarque à l'attention des utilisateurs Linux sur System z : vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux. Les fichiers `rpm` se trouvent dans le répertoire */package_path*`/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire *chemin_package*`/`*distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
4. Installez les fichiers de licence pour Tivoli Directory Server en exécutant le script `idsLicense` dans le répertoire *chemin_package*`/`*distribution*`/tdsLicense/license`.
5. Installez les packages du client IBM Tivoli Directory Server correspondant à votre déploiement.

   ```
   rpm -ihv packages
   ```

   Le tableau 14 répertorie les packages requis pour chaque type de client. Installez les packages correspondant à votre client dans l'ordre indiqué.

Tableau 14. Packages client pour systèmes d'exploitation Linux

Type de client	Packages	Descriptions des packages
Client Linux on x86-64, 64 bits	1. `idsldap-license63-6.3.0-17.x86_64.rpm` 2. `idsldap-cltbase63-6.3.0-17.x86_64.rpm` 3. `idsldap-clt64bit63-6.3.0-17.x86_64.rpm` 4. `idsldap-cltjava63-6.3.0-17.x86_64.rpm`	1. Licence 2. Client de base 3. Client 64 bits 4. Client Java
Linux on System z, 64 bits	1. `idsldap-license63-6.3.0-17.s390.rpm` 2. `idsldap-cltbase63-6.3.0-17.s390.rpm` 3. `idsldap-clt64bit63-6.3.0-17.s390x.rpm` 4. `idsldap-cltjava63-6.3.0-17.s390.rpm`	1. Licence 2. Client de base 3. Client 64 bits 4. Client Java

6. Démontez, le cas échéant, le DVD.

Résultats

Une fois le client IBM Tivoli Directory Server installé, aucune configuration supplémentaire n'est nécessaire.

Solaris : Installation du client IBM Tivoli Directory Server

Installez le client IBM Tivoli Directory Server avant d'utiliser la méthode de la ligne de commande pour installer IBM Security Access Manager for Web sous Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Pourquoi et quand exécuter cette tâche

La procédure suivante utilise **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Installez les fichiers de licence Tivoli Directory Server en exécutant le script `idsLicense` dans le répertoire *chemin_image*`/solaris/tdsLicense/license`, où *chemin_image* est le chemin d'accès à l'image du DVD, ou celui sous lequel lequel vous avez téléchargé le fichier d'archive à partir dePassport Advantage.
4. Installez les packages client de IBM Tivoli Directory Server correspondant à votre système d'exploitation :

   ```
   pkgadd -d /chemin_package/solaris/packages -a /chemin_package/solaris/pddefault
   ```

   Le tableau 15 répertorie les packages requis pour chaque type de client. Installez les packages correspondant à votre client dans l'ordre indiqué.

Tableau 15. Packages client pour Solaris

Type de client	Packages	Descriptions des packages
Client 64 bits	1. `idsldap.license63.pkg` 2. `idsldap.cltbase63.pkg` 3. `idsldap.clt64bit63.pkg` 4. `idsldap.cltjava63.pkg`	1. Licence 2. Client de base 3. Client 64 bits 4. Client Java

Remarque :

- Lors de l'installation, le système vous demande si vous souhaitez utiliser `/opt` en tant que répertoire de base. Si l'espace le permet, acceptez `/opt` comme répertoire de base. Pour accepter `/opt` en tant que répertoire de base, appuyez sur Entrée.
- Lorsque vous installez les packages client ou serveur, vous pouvez recevoir une invite du système avec la demande suivante : `This package contains scripts which will be executed with super-user permission during the process of installing the package. Continue with installation?`

Entrez `y` pour poursuivre. Ces scripts créent l'ID utilisateur Tivoli Directory Server.

Résultats

Une fois le client IBM Tivoli Directory Server installé, aucune configuration supplémentaire n'est nécessaire.

Windows : Installation du client IBM Tivoli Directory Server

Installez le client IBM Tivoli Directory Server avant d'utiliser les méthodes de la ligne de commande pour installer IBM Security Access Manager for Web sur Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Accédez au répertoire `\windows\tds_client64`.
4. Pour installer le client IBM Tivoli Directory Server, exécutez le fichier **`install_tds.bat`**.

   La fenêtre Choose Setup Language s'affiche.
5. Sélectionnez la langue à utiliser pour l'installation, puis cliquez sur **OK**.
6. La fenêtre Bienvenue s'affiche. Cliquez sur **Suivant** pour continuer.
7. Lisez le contrat de licence. Acceptez les termes du contrat, puis cliquez sur **Suivant**. Une fenêtre s'affiche et vous informe des packages qui sont déjà installés et si une action est requise. Si nécessaire, remplissez les exigences, puis cliquez sur **Suivant**.
8. Choisissez d'installer la fonction **C Client** , puis cliquez sur **Suivant**.
9. Vérifiez les options de configuration que vous avez sélectionnées. Si vous souhaitez modifier l'une de vos sélections, cliquez sur **Précédent**. Cliquez sur **Suivant** pour commencer l'installation.

Résultats

Une fois le client IBM Tivoli Directory Server installé, aucune configuration supplémentaire n'est nécessaire.

Installation de WebSphere Application Server

Installez WebSphere Application Server sur les systèmes sur lesquels vous envisagez de configurer Web Portal Manager, Attribute Retrieval Service, ou Session Management Server.

Avant de commencer

- Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.

- Lors de l'installation de WebSphere Application Server, vous êtes invité à sélectionner les fonctions à installer. Pour plus d'informations sur ces fonctions, consultez le manuel centre de documentation WebSphere Application Server, Network Deployment (Distributed platforms and Windows) version 8.0.
- Si vous prévoyez de déployer Session Management Server dans un environnement WebSphere version 8.0, vous devez installer WebSphere Application Server version 8.0 FP5 (ou une version ultérieure).
- Si vous utilisez des caractères de globalisation et n'avez pas installé WebSphere Application Server version 8.0 FP5 ou une version ultérieure, sélectionnez l'une des actions suivantes pour éviter les restrictions au niveau des caractères :
  - Lors de la création du profil, sélectionnez "Création de profil avancée" au lieu de l'option Typique.
  - Installez WebSphere Application Server 8.0 FP5 à l'étape 8, à la page 50 avant de créer le profil de serveur d'applications à l'étape 7, à la page 49.

Remarque : Comme alternative, vous pouvez automatiser l'installation de WebSphere Application Server à l'aide de fichiers scripts. Voir :

- «Automatisation de l'installation de WebSphere Application Server (AIX, Linux ou Solaris)», à la page 211
- «Automatisation de l'installation de WebSphere Application Server (Windows)», à la page 213

Pourquoi et quand exécuter cette tâche

Les étapes de cette tâche sont génériques et s'appliquent à WebSphere Application Server version 8.0. Pour des informations détaillées sur ces fonctions, consultez le centre de documentation correspondant : WebSphere Application Server, Network Deployment (Distributed platforms and Windows) version 8.0.

Si vous installez WebSphere Application Server version 7.0, consultez le centre de documentation correspondant : WebSphere Application Server, Network Deployment (Plateformes réparties et Windows) version 7.0.

Procédure

1. Obtenez les fichiers d'installation de WebSphere Application Server et du référentiel de produit. Ces fichiers se trouvent aux emplacements suivants :
   - Les DVD de WebSphere Application Server fournis avec les DVD d'IBM Security Access Manager.
   - Le site Passport Advantage.
2. Copiez les fichiers de WebSphere Application Server sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
3. Extrayez dans un répertoire tous les fichiers de WebSphere Application Server à partir de leurs fichiers compressés.
4. Obtenez Installation Manager à partir de l'un des emplacements suivants :
   - Le site Passport Advantage.
   - Site Web de téléchargement d'IBM Installation Manager : http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager

   a. Téléchargez les fichiers.
   b. Extrayez les fichiers dans un même répertoire. Envisagez d'utiliser le même répertoire que celui dans lequel se trouvent les fichiers de WebSphere Application Server.

c. Installez le composant Installation Manager sur votre système. Utilisez les instructions d'installation fournies avec Installation Manager.

5. Ajoutez le référentiel de produit aux préférences d'Installation Manager.
   a. Démarrez Installation Manager.
   b. Dans le menu du haut, cliquez sur **Fichier** > **Préférences**.
   c. Sélectionnez **Référentiels**.
   d. Cliquez sur **Ajouter le référentiel**.
   e. Entrez le chemin d'accès au fichier `repository.config` sous l'emplacement qui contient le fichier référentiel. Par exemple :
      `/var/repositories/nom_produit/local-repositories`
   f. Cliquez sur **OK**.
   g. Dans la fenêtre Repositories, désélectionnez tous les emplacements que vous n'utilisez pas.
   h. Cliquez sur **Appliquer**.
   i. Cliquez sur **OK**.
   j. Cliquez sur **Fichier** > **Quitter** pour fermer Installation Manager.
6. Installez WebSphere Application Server :
   a. Démarrez Installation Manager.
   b. Cliquez sur **Installer**.
   c. Sélectionnez **IBM WebSphere Application Server Network Deployment**, ainsi que la version appropriée.
   d. Cliquez sur **Suivant**.
   e. Acceptez les termes du contrat de licence. Cliquez sur **Suivant**.
   f. Indiquez le répertoire d'installation racine des fichiers du produit, qui sont référencés en tant que fichiers du produit central ou fichiers système.
   g. Cliquez sur **Suivant**.
   h. Choisissez les langues à installer.
   i. Cliquez sur **Suivant**.
   j. Sélectionnez les fonctions que vous souhaitez installer.
   k. Cliquez sur **Suivant**.
   l. Cliquez sur **Installer**.
   m. Sélectionnez **Outil de gestion de profil pour créer un profil**.
   n. Cliquez sur **Terminer**.
   o. Cliquez sur **Fichier** > **Quitter** pour fermer Installation Manager. L'outil de gestion des profils apparaît.
7. Créez un profil de serveur d'applications à l'aide de l'outil de gestion de profils.
   a. Dans l'outil de gestion de profils, cliquez sur **Créer**.
   b. Sélectionnez **Serveur d'applications**.
   c. Cliquez sur **Suivant**.
   d. Sélectionnez **Création de profil typique**.
   e. Cliquez sur **Suivant**.
   f. Cochez la case **Sécurité administrative** et renseignez les zones du panneau pour activer l'administration sécurisée.
   g. Cliquez sur **Suivant**.
   h. Passez les informations en revue, puis cliquez sur **Créer**.
   i. Désélectionnez la case **Lancer la console Premiers Pas**.

j. Cliquez sur **Terminer**.

8. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis. Localisez le groupe de correctifs dans le référentiel Web de WebSphere Application Server ou téléchargez le module et installez-le à partir d'un référentiel local.
   - Pour effectuer l'installation à partir du référentiel Web :
     a. Cliquez sur **Mettre à jour** dans la fenêtre IBM Installation Manager.
     b. Sélectionnez **IBM WebSphere Application Server Network Deployment V8.0**.
     c. Cliquez sur **Suivant**. Poursuivez l'installation.
   - Pour effectuer l'installation à partir d'un référentiel local :
     a. Localisez le groupe de correctifs sur la page de support de WebSphere Application Server : http://www.ibm.com/support/docview.wss?uid=swg27004980
     b. Téléchargez le groupe de correctifs dans un référentiel local.
     c. cliquez sur **Mettre à jour**.
     d. Sélectionnez **IBM WebSphere Application Server Network Deployment V8.0**.
     e. Cliquez sur **Suivant**. Poursuivez l'installation. Utilisez le fichier Readme fourni sur la page WebSphere Application Server Support pour obtenir de l'aide.
9. Démarrez le serveur d'applications. Par exemple, tapez :

   AIX, Linux ou Solaris
   ```
   /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/
     bin/startServer.sh server1
   ```

   Windows
   ```
   C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\
     bin\startServer.bat server1
   ```
10. Facultatif : Installez IBM HTTP Server et les plug-ins de serveur Web correspondants si vous souhaitez les configurer dans votre environnement. Appliquez les instructions fournies dans le centre de documentation d'IBM WebSphere Application Server : WebSphere Application Server, Network Deployment (Distributed platforms and Windows) version 8.0

    Si vous installez WebSphere Application Server version 7.0, consultez le centre de documentation correspondant : WebSphere Application Server, Network Deployment (Plateformes réparties et Windows) version 7.0.

Chapitre 5. Installation et configuration du serveur de registres d'utilisateurs

La première étape de la création d'un domaine de gestion est la configuration d'un serveur de registres à utiliser avec Security Access Manager.

Lisez la rubrique «Différences entre les registres d'utilisateurs».

Puis, pour installer et configurer un registre, effectuez l'une des procédures suivantes :

- Pour installer et configurer IBM Tivoli Directory Server (inclus avec Security Access Manager), suivez les instructions contenues dans l'une des rubriques suivantes :
  - «Installation d'IBM Tivoli Directory Server avec l'assistant d'installation Tivoli Directory Server», à la page 60
  - «Installation de Tivoli Directory Server avec le tableau de bord (Windows uniquement)», à la page 69
  - «Configuration de Tivoli Directory Server à l'aide des fichiers scripts», à la page 62

  Vous pouvez également consulter la documentation IBM Tivoli Directory Server disponible sur le Web à l'adresse :

  http://www.ibm.com/software/tivoli/products/directory-server
- Pour installer un registre pris en charge différent d'IBM Tivoli Directory Server, consultez la documentation du produit de registre. Pour obtenir une liste des registres pris en charge, consultez les notes sur l'édition dans le centre de documentation IBM Security Access Manager for Web. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés.

  Remarque : Le client IBM Tivoli Directory Server doit être utilisé comme client de registre pour les registres d'utilisateurs basés sur LDAP.
- Pour utiliser un serveur de registres existant avec Security Access Manager, assurez-vous d'avoir mis à niveau le serveur vers une version prise en charge par cette édition de Security Access Manager. Pour obtenir les instructions de mise à niveau pour IBM Tivoli Directory Server, consultez le manuel *IBM Security Access Manager for Web Upgrade Guide*. Pour les autres registres pris en charge, consultez la documentation du produit de registre. Suivez ensuite les instructions de ce chapitre pour configurer votre registre en vue de l'utilisation avec Security Access Manager.

Différences entre les registres d'utilisateurs

Chaque registre d'utilisateurs, lorsqu'il est intégré à Security Access Manager, fait l'objet de considérations uniques.

Security Access Manager prend en charge les registres d'utilisateurs LDAP et URAF.

© Copyright IBM Corp. 2001, 2013

Utilisez un registre d'utilisateurs LDAP si vous exécutez Security Access Manager sur un système AIX, Linux, Solaris ou Microsoft Windows. Security Access Manager prend en charge les registres d'utilisateurs LDAP suivants :

- Tivoli Directory Server
- IBM z/OS Security Server LDAP Server
- Novell eDirectory Server
- Sun Java System Directory Server
- Microsoft Active Directory Lightweight Directory Services (ADLDS)

Utilisez un registre d'utilisateurs URAF si vous exécutez Security Access Manager sous Windows. Les registres d'utilisateurs URAF ne peuvent pas être utilisés lorsque Security Access Manager est exécuté sur un système d'exploitation autre que Windows. Security Access Manager prend en charge les registres d'utilisateurs URAF suivants :

- Microsoft Active Directory Server

Considérations générales

Quelques considérations générales s'appliquent à tous les registres pris en charge.

Consultez ces informations avant de configurer un registre d'utilisateurs pour votre environnement.

- Evitez d'utiliser la barre oblique (/) lorsque vous définissez les noms des utilisateurs et des groupes et que ces noms sont définis à l'aide des chaînes de noms distinctifs. Chaque registre d'utilisateurs traite ce caractère différemment.
- Evitez d'utiliser des interlignages et des blancs de fin dans les noms d'utilisateurs et de groupes. Chaque registre d'utilisateurs traite les blancs différemment.

Remarques relatives à LDAP

Plusieurs considérations spécifiques s'appliquent à tous les registres LDAP pris en charge.

Consultez ces informations avant de configurer un registre d'utilisateurs pour votre environnement.

- Aucune étape de configuration n'est nécessaire dans Security Access Manager pour prendre en charge les règles sur les mots de passe spécifiques à LDAP. Security Access Manager ne tient pas compte de l'existence ou pas de règles sur les mots de passe LDAP.

  Security Access Manager applique tout d'abord ses propres règles sur les mots de passe. Security Access Manager tente de mettre à jour le mot de passe dans LDAP uniquement lorsque le mot de passe fourni passe le contrôle des propres règles sur les mots de passe de Security Access Manager.

  Security Access Manager tente ensuite de mettre en oeuvre les règles sur les mots de passe LDAP à l'aide du code retour reçu de LDAP lors d'une mise à jour du mot de passe.

  Si Security Access Manager peut mapper ce code retour au code d'erreur Security Access Manager correspondant, il le fait et renvoie un message d'erreur.
- Pour tirer parti du support multi-domaine de Security Access Manager, vous devez utiliser un registre d'utilisateurs LDAP. Lorsque vous utilisez un registre d'utilisateurs URAF, un seul domaine Security Access Manager est pris en charge.

- Lors de l'utilisation d'un registre d'utilisateurs LDAP, la capacité à posséder des droits d'authentification unique doit être explicitement accordée à un utilisateur. Une fois cette capacité accordée, elle peut être supprimée. Inversement, les utilisateurs créés dans un registre d'utilisateurs URAF disposent automatiquement de cette capacité. Elle ne peut pas être supprimée.
- Les espaces de début et de fin dans les noms d'utilisateur et les noms de groupe sont ignorés lors de l'utilisation d'un registre d'utilisateurs LDAP dans un domaine Security Access Manager sécurisé. Pour que le processus soit cohérent quel que soit le registre d'utilisateurs, définissez les noms d'utilisateur et de groupe sans espaces.
- Le fait d'ajouter un utilisateur en double unique à un groupe ne génère pas d'erreur lors de l'utilisation d'un registre d'utilisateurs LDAP.
- L'API d'autorisation Security Access Manager fournit un service d'habilitation d'attribut de droits d'accès. Ce service permet d'extraire des attributs utilisateur d'un registre d'utilisateurs. Lorsque ce service est utilisé avec un registre d'utilisateurs LDAP, les attributs extraits peuvent correspondre à des données de type chaîne ou binaire. Cependant, lorsque ce service est utilisé avec un registre d'utilisateurs URAF, les attributs extraits peuvent être des données de type chaîne, binaire ou entier.

Considérations relatives à Sun Java System Directory Server

En plus des généralités spécifiques à LDAP, les points suivants sont spécifiques à Sun Java System Directory Server. Consultez ces informations avant de configurer une instance Sun Java System Directory Server pour votre environnement.

- Si le registre d'utilisateurs contient plus d'entrées que la limite d'exploration définie, le serveur de répertoires peut renvoyer l'état suivant que Security Access Manager traite comme une erreur :

  `LDAP_ADMINLIMIT_EXCEEDED`

  Lorsque le serveur de répertoires est installé, la valeur par défaut est 5000. Pour modifier cette valeur, procédez comme suit à partir de la console Sun Java System Directory Server :

  1. Sélectionnez l'onglet **Configuration**.
  2. Développez l'entrée **Data**.
  3. Sélectionnez **Database Settings**.
  4. Sélectionnez l'onglet **LDBM Plug-in Settings**.
  5. Dans la zone **Look-through Limit**, entrez le nombre maximal d'entrées que vous voulez que le serveur contrôle en réponse à la recherche ou entrez `-1` pour définir aucune limite maximale.

  Si vous liez le répertoire comme Directory Manager, la limite d'exploration est illimitée et écrase tout paramètre spécifié dans cette zone.

Considérations relatives à Microsoft Active Directory Lightweight Directory Services (AD LDS)

En plus des généralités spécifiques à LDAP, les points suivants sont spécifiques à Microsoft AD LDS. Consultez ces informations avant de configurer un registre d'utilisateurs Microsoft AD LDS pour votre environnement.

- La configuration du serveur de règles permet de sélectionner un modèle de données standard ou minimal pour le registre d'utilisateurs. Comme AD LDS ne permet l'utilisation que d'un seul attribut d'appellation lors de la création d'objets AD LDS, il nécessite le modèle de données minimal. Quel que soit le modèle de données choisi lors de la configuration du serveur de règles, Security Access Manager utilise toujours le modèle de données minimal lorsqu'AD LDS est sélectionné comme registre d'utilisateurs.

- L'attribut de nom usuel (cn) est un attribut à valeur unique et ne peut stocker qu'une seule valeur. Le registre AD LDS requiert que la valeur cn soit la même que l'attribut d'appellation cn dans l'attribut de nom distinctif (dn). Lors de la création d'un utilisateur ou d'un groupe dans Security Access Manager, indiquez la même valeur pour cn que pour l'attribut d'appellation cn dans le dn. Security Access Manager ignore la valeur de l'attribut cn si elle est différente de celle de l'attribut d'appellation cn dans le dn. Par exemple, vous ne pouvez pas utiliser la commande suivante pour créer un utilisateur car la valeur de l'attribut cn, *fred*, est différente de celle de l'attribut d'appellation cn dans le dn, *user1* :

  ```
  pdadmin user create user1 cn=user1,o=ibm,c=us fred smith password1
  ```

Considérations relatives à URAF

Plusieurs considérations spécifiques s'appliquent à tous les registres URAF pris en charge.

Consultez ces informations avant de configurer un registre URAF pour votre environnement.

- Pour utiliser un registre d'utilisateurs URAF, vous devez exécuter Security Access Manager sur un système d'exploitation Microsoft Windows. Voir les *Notes sur l'édition de IBM Security Access Manager for Web* pour une liste des systèmes d'exploitation pris en charge.
- Lorsque vous utilisez un registre d'utilisateurs URAF, un seul domaine Security Access Manager est pris en charge. Pour tirer parti du support multidomaine Security Access Manager, utilisez un registre d'utilisateurs LDAP.
- Les utilisateurs créés dans un registre d'utilisateurs URAF ont automatiquement la capacité de disposer de droits d'authentification unique. Cette capacité ne peut pas être supprimée. Lors de l'utilisation d'un registre d'utilisateurs LDAP, cette capacité doit être explicitement accordée. Une fois cette capacité accordée, elle peut être supprimée.
- L'API d'autorisation Security Access Manager fournit un service d'habilitation d'attribut de droits d'accès. Ce service permet d'extraire des attributs utilisateur d'un registre d'utilisateurs. Lorsque ce service est utilisé avec un registre d'utilisateurs URAF, les attributs extraits peuvent être des données de type chaîne, binaire ou entier. Cependant, lorsqu'il est utilisé avec un registre d'utilisateurs LDAP, les attributs extraits peuvent uniquement correspondre à des données de type chaîne ou binaire.

Remarques concernant Microsoft Active Directory Server

En plus des généralités spécifiques à URAF, les points suivants sont spécifiques à Microsoft Active Directory Server. Consultez ces informations avant de configurer une instance Active Directory Server pour votre environnement.

- Les utilisateurs créés dans Active Directory peuvent avoir un groupe primaire associé. Le groupe primaire Active Directory par défaut est Utilisateurs de domaine.

  Mais Active Directory n'ajoute pas les informations de groupe primaire à l'attribut memberOf de l'utilisateur ou à l'attribut member du groupe. Cela signifie que lorsque Security Access Manager demande une liste des membres d'un groupe, le résultat n'inclut pas les membres du groupe primaire. De plus, lorsque Security Access Manager demande la liste de tous les groupes auxquels un utilisateur appartient, le résultat de la requête n'affiche pas le groupe primaire de l'utilisateur.

  Pour cette raison, évitez d'utiliser un groupe Security Access Manager comme groupe primaire Active Directory pour les utilisateurs de Security Access Manager.

- Security Access Manager peut être configuré dans un environnement Active Directory à domaine unique ou multi-domaines. Pour plus d'informations sur les environnements à domaine unique ou multi-domaines, consultez la documentation produit d'Active Directory.
- Lorsque Security Access Manager est configuré pour utiliser le registre d'utilisateurs Active Directory avec plusieurs domaines Active Directory, le serveur de règles doit être installé et configuré uniquement à partir du domaine Active Directory racine ou d'un client de ce domaine racine.
- Si Security Access Manager doit être installé sur un système non contrôleur de domaine, ce système doit être associé au domaine Active Directory dans lequel Security Access Manager doit être configuré.
- Pour obtenir les informations liées au groupe dynamique, consultez la documentation produit d'Active Directory.
- Microsoft prend en charge deux types de stockage d'autorisation différents, Active Directory et XML, qui stockent des groupes d'applications comme groupes dynamiques. Toutefois, Security Access Manager restreint la prise en charge des groupes dynamiques aux magasins d'autorisation Active Directory des groupes dynamiques. Security Access Manager ne prend pas en charge les groupes dynamiques qui sont créées dans XML Authorization Storage.
- Security Access Manager prend uniquement en charge le groupe global de sécurité.
- Pour importer un utilisateur Active Directory comme utilisateur Security Access Manager, utilisez le nom de connexion de l'utilisateur Active Directory comme ID de l'utilisateur Security Access Manager.
- Si vous avez installé et configuré Security Access Manager sur un client d'Active Directory (Security Access Manager et Active Directory se trouvent sur des systèmes différents, par exemple), le système client doit rejoindre le domaine. Vous devez vous connecter au domaine à l'aide de l'administrateur Active Directory créé pour effectuer la configuration Security Access Manager sur le système client.
- Lorsque vous utilisez SSL pour communiquer avec le serveur Active Directory, Active Directory limite le port SSL au numéro de port SSL par défaut **636**.
- Si l'environnement Active Directory se trouve derrière un pare-feu, assurez-vous que le port Microsoft-DS 445 est ouvert. Pour plus d'informations sur le protocole SMB (Server Message Block) sur IP, reportez-vous au site de support de Microsoft.
- Le serveur de nom de domaine du paramètre TCP/IP réseau sur le système client doit être identique au paramètre TCP/IP réseau du contrôleur de domaine. Vous pouvez utiliser le contrôleur de domaine racine comme serveur DNS ou un serveur de noms de domaine différent.
- Lorsque Security Access Manager est configuré pour utiliser Active Directory comme registre d'utilisateurs, le serveur catalogue global doit être en cours d'exécution et accessible pour les serveurs Security Access Manager. Active Directory utilise également le serveur catalogue global pour l'authentification utilisateur. Ce serveur utilise le port 3268 pour l'authentification non SSL et le port 3269 pour l'authentification SSL.

  Pour plus d'informations sur les ports de Global Catalog et les exigences applicables à l'utilisateur et à la connexion sur l'ordinateur, consultez le site de support de Microsoft.
- Security Access Manager ne prend pas en charge l'appartenance à un groupe interdomaine ou les groupes universels. Security Access Manager ne prend pas en charge l'importation de ces types de groupes.

- Lorsque Security Access Manager importe un groupe dynamique, les groupes `ivacld-servers` et `remote-acl-users` appliquent des droits de lecture sur chaque magasin d'autorisation auquel le groupe dynamique appartient. Ce droit de lecture active les serveurs lame Security Access Manager, comme WebSEAL, pour disposer de droit de lecture sur le magasin d'autorisation de registre ; fournissant ainsi au serveur lame la possibilité de lire les données du groupe dynamique, comme l'appartenance au groupe pour la génération de droits Security Access Manager. La suppression manuelle de ce droit de lecture alors que Security Access Manager est configuré sur le registre Active Directory entraîne un comportement inverse, tel qu'une appartenance inappropriée au groupe.
- Si l'option permettant de modifier un mot de passe utilisateur à l'aide de l'API LDAP est activée dans un environnement caractérisé par les deux conditions suivantes :
  - Security Access Manager est configuré pour utiliser le registre d'utilisateurs Active Directory
  - les serveurs lames Security Access Manager utilisent les API LDAP pour communiquer avec le serveur Active Directory

  puis, Security Access Manager doit être configuré avec Secure Socket Layer (SSL) pour permettre les connexions entre le client LDAP et le serveur Active Directory. L'environnement Active Directory doit également être activé pour accepter les connexions LDAP sur Secure Socket Layer (SSL).
- Lors de l'utilisation d'un registre d'utilisateurs Active Directory dans une configuration Security Access Manager avec des serveurs lame qui utilisent des API LDAP pour communiquer avec le serveur Active Directory, Security Access Manager prend en charge les demandes de modification du mot de passe utilisateur utilisant le serveur de règles ou des API LDAP. Les demandes de modification du mot de passe utilisateur utilisant les API LDAP ne nécessitent que le serveur de règles soit en cours de fonctionnement.

  L'utilisation d'API LDAP pour communiquer avec Active Directory Server pour des serveurs lames est un support multiplateformes qui permet aux serveurs d'être installés sur des machines qui ne sont pas clientes du même domaine que le serveur de règles. Dans cette configuration, le serveur de règles doit être installé et configuré sur un système d'exploitation Windows.
- Lors de l'utilisation d'un registre d'utilisateurs Active Directory, chaque nom d'utilisateur et chaque nom de groupe d'un domaine doivent être uniques. Les valeurs courtes de nom d'utilisateur et de groupe sont stockées dans l'attribut sAMAccountName des objets d'utilisateur et des objets de groupe Active Directory. Les objets d'utilisateur et les objets de groupe Active Directory ont tous les deux l'attribut sAMAccountName. Microsoft exige que les attributs sAMAccountName soient uniques au sein d'un domaine Active Directory.
- Avec un registre utilisateur Active Directory multi-domaine, de multiples utilisateurs et groupes peuvent être définis avec le même nom abrégé tant qu'ils se trouvent dans différents domaines. Cependant, le nom complet de l'utilisateur ou du groupe, y compris le suffixe de domaine, doivent toujours être indiqués dans Security Access Manager.
- Les espaces de début et de fin dans les noms d'utilisateur et les noms de groupe sont ignorés lors de l'utilisation d'un registre d'utilisateurs Microsoft Active Directory Server dans un domaine Security Access Manager sécurisé. Pour que le processus soit cohérent quel que soit le registre d'utilisateurs, définissez les noms d'utilisateur et de groupe sans espaces.
- Security Access Manager prend en charge l'utilisation d'une adresse électronique ou d'un format alternatif de l'attribut userPrincipalName de l'objet de

l'utilisateur de registre Active Directory comme une identité de l'utilisateur Security Access Manager. Cette amélioration est facultative. Lorsqu'elle est activée, l'adresse électronique et l'adresse par défaut ou le format alternatif de l'attribut userPrincipalName peuvent coexister dans l'environnement Security Access Manager.

Le format par défaut de l'attribut de registre userPrincipalName est `id_utilisateur@`*`suffixe_domaine`*, où *suffixe_domaine* désigne le domaine Active Directory dans lequel l'identité utilisateur est créée.

Par exemple, `johndoe@tivoli.com` est la valeur de l'attribut userPrincipalName; **`tivoli.com`** est le domaine Active Directory dans lequel l'identité utilisateur est créée. Dans cet exemple, l'identité utilisateur Security Access Manager correspondant à l'utilisateur de registre est soit **`johndoe@tivoli.com`**, soit **`johndoe`**, selon que Security Access Manager est configuré pour utiliser Active Directory avec plusieurs domaines ou un seul domaine.

Le format alternatif de l'attribut userPrincipalName est `id_utilisateur@suffixe`, où `suffixe` désigne n'importe quel domaine (Active Directory ou pas) autre que le domaine Active Directory dans lequel l'identité utilisateur est créée. Par exemple, si l'utilisateur de registre `johndoe@other_domain.com` est créé dans Active Directory `tivoli.com`, et si l'utilisateur de registre `johndoe@tivoli.com` est créé dans le domaine Active Directory `child_domain.tivoli.com`. Ces deux utilisateurs peuvent être des utilisateurs Security Access Manager, et leurs identités sont respectivement`johndoe@other_domain.com` et `johndoe@tivoli.com`.

La prise en charge de nom principal d'utilisateur alternatif (UPN) doit être activée dans tous les environnements d'exécution Security Access Manager pour que les identités utilisateur Security Access Manager fonctionnent correctement avec les UPN alternatifs.

Une fois l'utilisation du format UPN alternatif comme identité d'utilisateur Security Access Manager activée, il est impossible de revenir à l'état antérieur sans rompre les fonctionnalités Security Access Manager.

- Bien que les utilisateurs et les groupes puissent être créés avec des noms utilisant une chaîne de nom distinctif qui contient une barre oblique (/), les opérations ultérieures sur l'objet peuvent échouer. Certaines fonctions Active Directory interprètent la barre oblique comme un séparateur entre le nom d'objet et le nom d'hôte. Pour éviter le problème, n'utilisez pas de barre oblique pour définir l'utilisateur.

Longueur des noms

Les longueurs maximales des différents noms associés à un utilisateur Security Access Manager varient selon le registre d'utilisateurs utilisé dans l'environnement.

Voir tableau 16 pour obtenir une comparaison des longueurs autorisées et de la longueur maximale recommandée pour assurer la compatibilité avec tous les registres utilisateur pris en charge par Security Access Manager

Tableau 16. Longueurs maximales des noms par registre d'utilisateurs et longueur optimale dans les registres d'utilisateurs

Nom	IBM Tivoli Directory Server	IBM z/OS Security Server	Novell eDirectory Server	Sun Java System Directory Server	Microsoft Active Directory Server	Active Directory Lightweight Directory Service (ADLDS)	Longueur optimale
Prénom (LDAP CN)	256	256	64	256	64	64	64

Tableau 16. Longueurs maximales des noms par registre d'utilisateurs et longueur optimale dans les registres d'utilisateurs (suite)

Nom	IBM Tivoli Directory Server	IBM z/OS Security Server	Novell eDirectory Server	Sun Java System Directory Server	Microsoft Active Directory Server	Active Directory Lightweight Directory Service (ADLDS)	Longueur optimale
Nom intermédiaire	128	128	128	128	64	64	64
Nom	128	128	128	128	64	64	64
UID registre (LDAP DN)	1024	1024	1024	1024	2048	1024	255
identité utilisateur Security Access Manager	256	256	256	256	64	64	64
Mot de passe utilisateur	illimitée	illimitée	illimitée	illimitée	256	128	256
Description utilisateur	1024	1024	1024	1024	1024	1024	1024
Nom du groupe	256	256	256	256	64	64	64
Description du groupe	1024	1024	1024	1024	1024	1024	1024
Nom de ressource à connexion unique	240	240	240	240	60	240	60
Description de ressource à connexion unique	1024	1024	1024	1024	1024	1024	1024
ID utilisateur à connexion unique	240	240	240	240	60	240	60
Mot de passe à connexion unique	illimitée	illimitée	illimitée	illimitée	256	illimitée	256
Nom de groupe à connexion unique	240	240	240	240	60	240	60
Description de groupe à connexion unique	1024	1024	1024	1024	1024	1024	1024
Nom d'action	1	1	1	1	1	1	1
Description d'action, type d'action	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée

Tableau 16. Longueurs maximales des noms par registre d'utilisateurs et longueur optimale dans les registres d'utilisateurs (suite)

Nom	IBM Tivoli Directory Server	IBM z/OS Security Server	Novell eDirectory Server	Sun Java System Directory Server	Microsoft Active Directory Server	Active Directory Lightweight Directory Service (ADLDS)	Longueur optimale
Nom et description d'objet	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée
Nom d'espace objets et description d'espace objets	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée
Nom et description d'ACL	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée
Nom et description de règles POP	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée	illimitée

Bien que la longueur maximale d'un nom distinctif Active Directory (numéro utilisateur de registre) soit de 2048, la longueur maximale de chaque nom distinctif associé (RDN) est de 64.

Si vous configurez Security Access Manager pour utiliser plusieurs domaines Active Directory, la longueur maximale de l'identité utilisateur et du nom de groupe ne comprend pas le suffixe du domaine. Lorsque vous utilisez plusieurs domaines, le format de l'identité utilisateur est *ID_util@suffixe_domaine*. La longueur maximale de 64 s'applique uniquement à la portion *ID_util*. Si vous utilisez une adresse électronique ou un autre format pour l'identité utilisateur de Security Access Manager dans Active Directory, la longueur de nom maximale reste la même, mais inclut le suffixe.

Même si la longueur de certains noms peut être illimitée, une longueur excessive risque d'entraîner des difficultés de gestion des règles et de diminuer les performances du système. Il est donc recommandé de choisir des valeurs maximales logiques pour votre environnement.

Installation et configuration de Tivoli Directory Server

Tivoli Directory Server est fourni avec le produit Security Access Manager. Vous pouvez utiliser une installation de Tivoli Directory Server nouvelle ou existante dans votre environnement.

Lisez la rubrique «Différences entre les registres d'utilisateurs», à la page 51. Puis, sélectionnez une méthode d'installation ou, pour utiliser un serveur de registre existant avec Security Access Manager, assurez-vous que vous avez effectué la mise à niveau du serveur vers une version prise en charge par la présente édition de Security Access Manager. Pour obtenir les instructions de mise à niveau pour IBMTivoli Directory Server, consultez le manuel *IBM Security Access Manager for Web Upgrade Guide*. Pour les autres registres pris en charge, consultez la

documentation du produit de registre. Suivez ensuite les instructions de ce chapitre pour configurer votre registre en vue de l'utilisation avec Security Access Manager.

Installation d'IBM Tivoli Directory Server avec l'assistant d'installation Tivoli Directory Server

Installez IBM Tivoli Directory Server à l'aide de l'assistant d'installation dans le "chemin d'installation typique". Cette configuration utilise les valeurs par défaut et installe automatiquement tous les composants Tivoli Directory Server pour Security Access Manager.

Avant de commencer

Remarque : Si des packages de Tivoli Directory Server, tels que les modules client, sont déjà installés à un niveau supérieur à 6.3.0.0, supprimez-les avant d'exécuter l'assistant d'installation.

Effectuez les tâches suivantes avant de configurer IBM Tivoli Directory Server :

- Effectuez les tâches de préinstallation correspondant à votre environnement et décrites à la section «Préparation du système d'exploitation», à la page 28.
- Passez en revue les considérations générales concernant les registres d'utilisateurs à la rubrique «Considérations générales», à la page 52
- Passez en revue les considérations relatives au registre utilisateur LDAP à la rubrique «Remarques relatives à LDAP», à la page 52.
- Consultez les instructions applicables à la méthode utilisant le "Chemin d'installation typique" décrites dans le centre de documentation de IBM Tivoli Directory Server version 6.3.
  1. Visitez le site http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm
  2. Recherchez "Chemin d'installation typique".

Pourquoi et quand exécuter cette tâche

Cette tâche exécute les installations des composants suivants :

- Tous les composants requis par Tivoli Directory Server.
- Tous les produits corequis par Tivoli Directory Server, s'ils ne sont pas déjà installés. Ces produits sont les suivants :
  - GSKit
  - DB2
- La version imbriquée de WebSphere Application Server. Ce logiciel est requis par l'outil d'administration Web, lequel est installé automatiquement via la méthode utilisant le "chemin d'installation typique".

Cette tâche exécute également la configuration suivante :

- Déploie l'outil d'administration Web.
- Crée le répertoire par défaut d'une instance de serveur **dsrdbm01**.
- Crée l'ID utilisateur du système d'exploitation nommé **dsrdbm01** et propriétaire de l'instance.
- Crée un nom distinctif d'administrateur appelé **cn=root**.
- Crée un suffixe par défaut nommé **o=example**.

Procédure

1. Ouvrez une session sur le système.

   AIX, Linux ou Solaris
   Connectez-vous en tant qu'utilisateur `root`.

   Windows
   Connectez-vous en tant qu'administrateur.

2. Exécutez les étapes suivantes pour préparer et démarrer le programme d'installation :
   a. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
   b. **Pour les systèmes AIX, Linux ou Solaris :** Installez les fichiers de licence Tivoli Directory Server en exécutant le script `idsLicense` dans le répertoire *chemin_image*`/tdsV6.3FP/license`, où *chemin_image* est le chemin d'accès à l'image du DVD, ou celui sous lequel lequel vous avez téléchargé le fichier d'archive à partir Passport Advantage.
   c. Placez-vous dans le répertoire *plateforme*`/tdsV6.3/tds`.

3. Exécutez le programme d'installation.

   AIX, Linux ou Solaris
   Exécutez `install_tds.bin`.

   Windows
   Cliquez deux fois sur l'icône **install_tds.exe**.

4. Effectuez l'installation d'après les instructions utilisant le "Chemin d'installation typique", décrites dans le centre de documentation d'IBM Tivoli Directory Server. Pour consulter le centre de documentation d'IBM Tivoli Directory Server 6.3, voir http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm.

   Remarque : Enregistrez les mots de passe que vous avez éventuellement définis lors de l'installation afin de pouvoir les utiliser au cours des étapes d'installation ultérieures.

5. Lorsque l'outil d'administration d'instance Tivoli Directory Server s'affiche :
   a. Vérifiez que l'instance par défaut est indiquée dans la configuration.

      Remarque : Si vous utilisez Red Hat Enterprise Linux 6, l'instance par défaut n'est pas affichée dans l'outil. Pour vérifier que l'entrée est référencée dans la configuration, utilisez la commande **idsilist**. Voir le centre de documentation d'IBM Tivoli Directory Server version 6.3 pour plus de détails sur la commande. Par défaut, cette commande se trouve dans `opt/PolicyDirector/sbin/pdconf`.
   b. Ne démarrez pas l'instance.
   c. Quittez l'outil.

6. Démarrez le processus de configuration à l'aide d'une ligne de commande. Pour créer le suffixe sous lequel Security Access Manager maintient ses métadonnées, utilisez la commande **idscfgsuf**. La commande se trouve par défaut aux emplacements suivants :

   AIX, Linux ou Solaris
   `/opt/ibm/ldap/V6.3/sbin/idscfgsuf`

   Windows
   `c:\Program Files\IBM\LDAP\V6.3\sbin\idscfgsuf`

Par exemple, exécutez :

```
idscfgsuf -s "secAuthority=nom_domaine"
```

où *nom_domaine* est le nom du domaine de gestion.

Le suffixe par défaut est Default ; par exemple :

```
idscfgsuf -s "secAuthority=Default"
```

Si vous spécifiez un emplacement pour les métadonnées qui ne correspond pas à un suffixe autonome, assurez-vous que cet emplacement existe sur le serveur LDAP.

Ce suffixe est ajouté au fichier `ibmslapd.conf` de l'instance par défaut. Si vous avez plusieurs instances, spécifiez le nom de l'instance à l'aide de l'option *-I*.

7. Facultatif : Vous pouvez créer des suffixes supplémentaires pour maintenir les définitions des utilisateurs et des groupes. Par exemple :

   ```
   idscfgsuf -s "c=US"
   ```

8. Démarrez le serveur LDAP.

   AIX, Linux ou Solaris

   ```
   ibmslapd&
   ```

   Windows

   Dans la fenêtre **Services**, démarrez les services suivants :

   ```
   IBM Tivoli Directory Server Instance V6.3 - nom_instance
   ```

9. **Pour les systèmes AIX, Linux ou Solaris uniquement :** mettez à jour l'installation d'après le niveau de correctifs approprié.

   Remarque : Pour les installations Windows, l'image d'installation inclut le niveau du groupe de correctifs approprié.

   a. Arrêtez tous les services Tivoli Directory Server.
   b. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
   c. Placez-vous dans le répertoire approprié pour votre système d'exploitation.

      ```
      platform/tdsV6.3FP
      ```

   d. Consultez le fichier Readme inclus avec le groupe de correctifs pour plus d'informations et pour obtenir les instructions d'installation.
   e. Exécutez le programme d'installation.

      ```
      ./idsinstall –u -f
      ```

10. Une fois l'installation terminée, vérifiez la version installée.
    a. Ouvrez une invite de commande.
    b. Entrez :

       ```
       idsversion
       ```

Que faire ensuite

- Si vous configurez la communication SSL, reportez-vous à la section «Configuration d'IBM Tivoli Directory Server pour l'accès SSL», à la page 71.
- Sinon, passez à la section Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Configuration de Tivoli Directory Server à l'aide des fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

AIX, Linux ou Solaris : automatisation de la configuration de Tivoli Directory Server

Utilisez le fichier script pour automatiser l'installation de Tivoli Directory Server.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*). Cette tâche utilise la commande **idsNative Install**.

Procédure

1. Connectez-vous au système avec les privilèges de superutilisateur.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Extrayez le fichier archive Tivoli Directory Server dans un répertoire comportant un espace disque suffisant. Par exemple, `/tdsV6.3/`. Si vous utilisez un DVD pour installer Tivoli Directory Server, les fichiers se trouvent dans le répertoire `tdsV6.3`.
4. Localisez les fichiers scripts suivants et modifiez les autorisations afin de rendre les fichiers accessibles en écriture :

   ```
   chmod +w chemin_image/tdsV6.3/responsefile.txt
   chmod +w chemin_image/scripts/ISAMConfigTDS.sh
   chmod +w chemin_image/scripts/ISAMGenSSLCert.sh
   chmod +w chemin_image/platform/tdsV6.3/idsConfigServerSSL.sh
   ```

5. Installez les fichiers de licence Tivoli Directory Server en procédant comme suit :
   a. Accédez au répertoire *chemin_image*`/tdsV6.3FP/license`.
   b. Exécutez le script suivant :

      ```
      idsLicense -q
      ```

      où l'option `-q` installe les fichiers de licence afficher la licence. Si vous utilisez l'option `-q`, vous acceptez automatiquement la licence sans l'afficher.
6. Dans le répertoire `tdsV6.3`, localisez le fichier du programme d'installation et le fichier de réponses :
   - `idsNativeInstall.sh`
   - `responseFile.txt`

   Ces fichiers doivent se trouver dans le même répertoire.
7. Mettez à jour les entrées suivantes dans le fichier `responseFile.txt`. Par défaut, les valeurs de la variable sont définies sur `false` et les variables de chemin correspondantes ne sont pas définies.
   - Pour installer DB2, définissez la variable *db2FeatureInstall* sur `true`. Mettez à jour la variable *db2InstallimagePath* avec le chemin d'accès absolu sous lequel les fichiers d'installation de DB2 sont situés.

     Par exemple :

     ```
     db2FeatureInstall=true
     db2InstallimagePath=/chemin_image/plateforme/tdsV6.3/db2
     ```

   - Pour installer GSKit, définissez la variable *gskitFeatureInstall* sur `true`. Mettez à jour la variable *gskitInstallimagePath* avec le chemin d'accès absolu sous lequel les fichiers d'installation de GSKit sont situés. Par exemple :

     ```
     gskitFeatureInstall=true
     gskitInstallimagePath=/chemin_image/plateforme/tdsV6.3/gskit
     ```

- Pour installer la version intégrée de WebSphere Application Server (eWAS), définissez la variable *eWasFeatureInstall* sur `true`. Mettez à jour la variable *eWasInstallimagePath* avec le chemin d'accès absolu sous lequel les fichiers d'installation de la version intégrée de WebSphere Application Server sont situés. Par exemple :

  ```
  eWasFeatureInstall=true
  eWasInstallimagePath=/chemin_image/plateforme/tdsV6.3/appsrv
  ```

- Pour installer Tivoli Directory Server, mettez à jour la variable *tdsInstallimagePath* avec le chemin d'accès absolu sous lequel les fichiers d'installation de Tivoli Directory Server sont situés. Mettez à jour la variable *tdsFixPackInstallimagePath* avec le chemin d'accès absolu sous lequel les fichiers d'installation de groupe de correctifs Tivoli Directory Server sont situés. Par exemple :

  ```
  tdsInstallimagePath=/chemin_image/plateforme/tdsV6.3/
  tdsFixPackInstallimagePath=/chemin_image/plateforme/tdsV6.3FP
  ```

  Remarque : Si vous souhaitez installer la version complète de Tivoli Directory Server, mais que certains packages Tivoli Directory Server sont déjà installés, comme les packages clients, supprimez les images avant d'exécuter ce script.

8. Enregistrez le fichier `responseFile.txt`.
9. **Pour les systèmes Solaris uniquement :**
   a. Vérifiez que le répertoire `/export/home` existe. Si le répertoire n'existe pas, créez-le.
   b. Assurez-vous que les paramètres de noyau suivants sont correctement définis dans le fichier `/etc/system` en fonction de votre système. Les valeurs suivantes sont suggérées en tant que valeurs de début :

      ```
      set msgsys:msginfo_msgmax = 65535
      set msgsys:msginfo_msgmnb = 65535
      set shmsys:shminfo_shmmax = 2134020096
      ```

   Pour plus d'informations, voir la documentation relative à l'optimisation de Solaris.
10. Ouvrez une invite de commande et lancez l'installation à l'aide de la commande **`idsNativeInstall.sh`** :
11. Vérifiez l'installation en consultant le journal d'installation : `/var/idsldap/V6.3/idsNativeInstall_horodatage.log`
12. **Pour les systèmes AIX, Linux ou Solaris uniquement :** mettez à jour l'installation d'après le niveau de correctifs approprié.

    Remarque : Pour les installations Windows, l'image d'installation inclut le niveau du groupe de correctifs approprié.
    a. Arrêtez tous les services Tivoli Directory Server.
    b. Accédez au DVD ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
    c. Placez-vous dans le répertoire approprié pour votre système d'exploitation.

       `plateforme/tdsV6.3FP`
    d. Consultez le fichier Readme inclus avec le groupe de correctifs pour plus d'informations et pour obtenir les instructions d'installation.
    e. Exécutez le programme d'installation.

       ```
       ./idsinstall –u -f
       ```

13. Facultatif : Si vous souhaitez utiliser Tivoli Directory Server Web Administration Tool, déployez Tivoli Directory Server sur la version intégrée de WebSphere Application Server :
    a. Ouvrez une invite de commande.
    b. Exécutez la commande *racine_ldap*/idstools/deploy_IDSWebApp. Remplacez *racine_ldap* par le chemin d'installation.
14. Créez l'instance et le suffixe par défaut :
    a. Ouvrez une invite de commande.
    b. Placez-vous dans le répertoire suivant : *chemin_image*/*platform*/tdsV6.3/
    c. Exécutez la commande suivante :

       ```
       idsdefinst -p motdepasse_nd -w motdepasse_util
       -e valeur_départ_chiffrement
       ```

       où :

       motdepasse_nd
       Mot de passe associé au nom distinctif d'administration. Par exemple, le mot de passe cn=root.

       motdepasse_util
       Mot de passe du propriétaire de base de données. Par exemple le mot de passe associé à l'ID administrateur dsrdbm01.

       valeur_départ_chiffrement
       Valeur de départ du chiffrement. Cette valeur permet de générer un ensemble de valeurs de clés confidentielles AES (Advanced Encryption Standard). La longueur doit être comprise entre 12 et 1 016 caractères.
15. Configurez Tivoli Directory Server pour Security Access Manager:
    a. Localisez le fichier *chemin_image*/scripts/ISAMConfigTDS.sh.
    b. Ouvrez le fichier dans un éditeur de texte.
    c. Définissez adminPW sur le mot de passe cn=root. Ce mot de passe a été créé lors de l'exécution de l'outil **idsdefinst**.
    d. Passez en revue les autres paramètres du fichier. Si vous avez utilisé les valeurs par défaut lors de l'installation de Tivoli Directory Server, aucune autre modification n'est nécessaire.
    e. Enregistrez, puis refermez le fichier ISAMConfigTDS.sh.
    f. Ouvrez une invite de commande.
    g. Exécutez *chemin_image*/scripts/ISAMConfigTDS.sh. Remplacez *chemin_image* par le chemin d'accès aux fichiers scripts.
    h. Consultez les messages de sortie et vérifiez que le script s'est exécuté avec succès.

       Remarque : Si vous avez utilisé un nom de base de données incorrect, il se peut que l'exécution du script soit abandonnée et renvoie un code retour nul. Consultez tous les messages de sortie pour vous assurer que le script s'est exécuté avec succès. Le nom de base de données par défaut est dsrdbm01. Il n'est pas nécessaire de changer le nom par défaut si vous avez utilisé les valeurs par défaut avec la commande **idsdefinst**.
16. Facultatif : Si vous configurez la mise en conformité Suite B et NIST entre le registre d'utilisateurs et les composants Security Access Manager, reportez-vous à la section «Configuration d'IBM Tivoli Directory Server pour

l'accès SSL», à la page 71. Si vous souhaitez effectuer une configuration SSL de base, poursuivez avec les étapes suivantes :

a. Pour créer un certificat autosigné :
   1) Ouvrez le fichier *chemin_image*/scripts/ISAMGenSSLCert.sh dans un éditeur de texte.
   2) Définissez le mot de passe pour la base de données de clés avec la variable KEYFILEPWD.
   3) Sauvegardez le fichier et fermez-le.
   4) Exécutez *chemin_image*/scripts/ISAMGenSSLCert.sh. Remplacez *chemin_image* par le chemin d'accès aux fichiers scripts.

      Remarque : Le certificat autosigné est extrait vers am_key.der.

b. Pour activer SSL avec Tivoli Directory Server :
   1) Ouvrez le fichier *chemin_image*/*plateforme*/tdsV6.3/idsConfigServerSSL.sh dans un éditeur de texte.
   2) Définissez les valeurs des variables suivantes. Les valeurs en gras sont les valeurs par défaut typiques. Utilisez des valeurs spécifiques et appropriées pour votre environnement.

      ```
      tdsinstancename=dsrdbm01
      port=389
      ssl_port=636
      serverpwd=
      serverlabel=AMLDAP
      serverkeywithpath=/am_key.kdb
      user_dn=cn=root
      password_dn=
      ```

      Remarque : Les zones des mots de passe doivent être définies conformément à vos mots de passe.
   3) Sauvegardez le fichier et fermez-le.
   4) Exécutez *chemin_image*/*plateforme*/tdsV6.3/idsConfigServerSSL.sh. Remplacez *chemin_image*/*plateforme* par le chemin d'accès aux fichiers d'installation de Tivoli Directory Server.

Que faire ensuite

Passez à l'étape Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Windows : automatisation de la configuration de Tivoli Directory Server

Utilisez le fichier script pour automatiser l'installation de Tivoli Directory Server.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*). Cette tâche utilise la commande **install_tdsSilent**.

Procédure

1. Connectez-vous au système avec les privilèges d'administrateur.
2. Extrayez le fichier archive de Tivoli Directory Server dans un répertoire comportant un espace disque suffisant, par exemple /tdsV6.3/. Si vous utilisez un DVD pour installer Tivoli Directory Server, les fichiers se trouvent dans le répertoire tdsV6.3.

3. Localisez les fichiers scripts suivants et modifiez les autorisations afin de rendre les fichiers accessibles en écriture :

   chemin_image\tds\optionsFile\InstallServer.txt
   chemin_image\scripts\ISAMConfigTDS.bat
   chemin_image\scripts\ISAMGenSSLCert.bat
   chemin_image\Windows\tdsV6.3\idsConfigServerSSL.bat

   Par exemple :

   a. Pour chaque fichier répertorié ci-dessus, cliquez avec le bouton droit sur le fichier, puis cliquez sur **Properties**.
   b. Cliquez sur l'onglet **Sécurité**.
   c. Dans la zone de liste **Nom**, sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier.
   d. Dans la zone **Autorisations**, sélectionnez **Ecriture**.
   e. Cliquez sur **OK**.
4. Dans le répertoire, localisez le fichier du programme d'installation et le fichier de réponses :
   - *chemin_image*\windows*tdsV6.3*\tds\install_tdsSilent.exe
   - *chemin_image*\windows*tdsV6.3*\tds\optionsFile\InstallServer.txt
5. Mettez à jour les entrées dans le fichier InstallServer.txt avec les valeurs appropriées pour votre installation. Utilisez les instructions du fichier texte. Pour plus de détails, reportez-vous aux rubriques concernant les fichiers d'options pour l'installation en mode silencieux dans le centre de documentation de Tivoli Directory Server :

   http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm
6. Enregistrez le fichier InstallServer.txt.
7. Ouvrez une invite de commande et placez-vous dans le répertoire suivant :

   chemin_image\windows\tdsV6.3\tds
8. Démarrez l'installation en exécutant la commande suivante :

   install_tdsSilent -is:silent
   -options *chemin_image*\optionsFiles\InstallServer.txt

   où *chemin_image* est le chemin d'accès complet au répertoire optionsFiles.
9. Vérifiez l'installation en consultant le journal d'installation :

   C:\Program Files\IBM\LDAP\V6.3\var\ldapinst.log
10. Créez l'instance et le suffixe par défaut :
    a. Ouvrez une invite de commande.
    b. Accédez au répertoire suivant : *racine_ldap*\idstools
    c. Exécutez la commande suivante :

       idsdefinst -p *motdepasse_nd* -w *motdepasse_util*
       -e *valeur_départ_chiffrement*

       où :

       motdepasse_nd
       Mot de passe associé au nom distinctif d'administration. Par exemple, le mot de passe cn=root.

       motdepasse_util
       Mot de passe du propriétaire de base de données. Par exemple le mot de passe associé à l'ID administrateur dsrdbm01.

valeur_départ_chiffrement
Valeur de départ du chiffrement. Cette valeur permet de générer un ensemble de valeurs de clés confidentielles AES (Advanced Encryption Standard). La longueur doit être comprise entre 12 et 1 016 caractères.

11. Configurez Tivoli Directory Server pour Security Access Manager :
    a. Localisez le fichier *chemin_image*\scripts\ISAMConfigTDS.bat.
    b. Ouvrez le fichier dans un éditeur de texte.
    c. Définissez adminPW sur le mot de passe cn=root.
    d. Passez en revue les autres paramètres du fichier. Si vous avez utilisé les valeurs par défaut lors de l'installation de Tivoli Directory Server, aucune autre modification n'est nécessaire.
    e. Enregistrez, puis refermez le fichier ISAMConfigTDS.bat.
    f. Ouvrez une invite de commande.
    g. Exécutez *chemin_image*\scripts\ISAMConfigTDS.bat. Remplacez *chemin_image* par le chemin d'accès aux fichiers scripts.
    h. Vérifiez la configuration en consultant le journal d'installation :
    C:\Users\Administrator\ConfigTDSforISAM.log
12. Facultatif : Si vous configurez la mise en conformité Suite B et NIST entre le registre d'utilisateurs et les composants Security Access Manager, reportez-vous à la section «Configuration d'IBM Tivoli Directory Server pour l'accès SSL», à la page 71. Si vous souhaitez effectuer une configuration SSL de base, poursuivez avec les étapes suivantes :
    a. Pour créer un certificat autosigné :
        1) Ouvrez le fichier *chemin_image*\scripts\ISAMGenSSLCert.bat dans un éditeur de texte.
        2) Définissez le mot de passe pour la base de données de clés avec la variable KEYFILEPWD.
        3) Sauvegardez le fichier et fermez-le.
        4) Exécutez *chemin_image*\scripts\ISAMGenSSLCert.bat. Remplacez *chemin_image* par le chemin d'accès aux fichiers scripts.

        Remarque : Le certificat autosigné est extrait vers am_key.der.
    b. Pour activer SSL avec Tivoli Directory Server :
        1) Ouvrez le fichier *chemin_image*\Windows\tdsV6.3\idsConfigServerSSL.bat dans un éditeur de texte.
        2) Définissez les valeurs des variables suivantes. Les valeurs en gras sont les valeurs par défaut typiques. Utilisez des valeurs spécifiques et appropriées pour votre environnement.

        ```
        tdsinstancename=dsrdbm01
        port=389
        ssl_port=636
        serverpwd=
        serverlabel=AMLDAP
        serverkeywithpath=C:\am_key.kdb
        user_dn=cn=root
        password_dn=
        ```

        Remarque : Les zones des mots de passe doivent être définies conformément à vos mots de passe.
        3) Sauvegardez le fichier et fermez-le.

4) Exécutez *chemin_image*\Windows\tdsV6.3\idsConfigServerSSL.bat. Remplacez *chemin_image* par le chemin d'accès aux fichiers d'installation de Tivoli Directory Server.

Que faire ensuite

Passez à l'étape Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Installation de Tivoli Directory Server avec le tableau de bord (Windows uniquement)

Utilisez la méthode d'installation du tableau de bord pour installer les composants d'un système Tivoli Directory Server sur un ordinateur exécutant le système d'exploitation Windows.

Avant de commencer

Effectuez les tâches suivantes avant de configurer IBM Tivoli Directory Server :

- Effectuez les tâches de préinstallation correspondant à votre environnement et décrites à la section «Préparation du système d'exploitation», à la page 28.
- Passez en revue les considérations générales concernant les registres d'utilisateurs à la rubrique «Considérations générales», à la page 52.
- Passez en revue les considérations relatives au registre utilisateur LDAP à la rubrique «Remarques relatives à LDAP», à la page 52.
- Consultez les instructions applicables à la méthode utilisant le "Chemin d'installation typique" décrites dans le centre de documentation d'IBM Tivoli Directory Server version 6.3.
  1. Rendez-vous sur le site http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm.
  2. Recherchez "Chemin d'installation typique".

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale. Le tableau de bord installe tous les logiciels prérequis, s'ils n'ont déjà été installés.

Puis, le tableau de bord démarre l'installation via l'interface utilisateur graphique du composant Tivoli Directory Server.

Cette tâche installe les composants suivants :

- Tous les composants requis par Tivoli Directory Server.
- Tous les produits corequis par Tivoli Directory Server, s'ils ne sont pas déjà installés. Ces produits sont les suivants :
  - GSKit
  - DB2
- La version imbriquée de WebSphere Application Server. Ce logiciel est requis par l'outil d'administration Web, lequel est installé automatiquement via la méthode utilisant le "chemin d'installation typique".

Cette tâche exécute également la configuration suivante :

- Déploie l'outil d'administration Web.
- Crée le répertoire par défaut d'une instance de serveur dsrdbm01.

- Crée l'ID utilisateur du système d'exploitation nommé `dsrdbm01` et propriétaire de l'instance.
- Crée un nom distinctif d'administrateur appelé `cn=root`.
- Crée un suffixe par défaut nommé `o=example`.

Procédure

1. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.

      Remarque : Si vous utilisez des fichiers archives, assurez-vous qu'ils sont tous extraits dans le même répertoire. Assurez-vous, par exemple, que les fichiers archives du package IBM Security Access Manager et des packages Tivoli Directory Server sont bien extraits dans le même répertoire.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
2. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
3. Cliquez sur **Suivant**.
4. Sélectionnez le composant **IBM Tivoli Directory Server**.
5. Cliquez sur **Suivant**. La liste affichée sur la partie gauche indique le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis par ce composant qui ne sont pas encore installés.
6. Cliquez sur **Suivant**. Le panneau d'installation du premier composant répertorié s'affiche. Une flèche à gauche du nom d'un composant indique que celui-ci est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
7. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 8.
8. Cliquez sur **Suivant**.
9. Répondez aux invites qui s'affichent au cours de l'installation.
10. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord. L'assistant d'installation de Tivoli Directory Server s'affiche.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Lorsque vous y êtes invité pour le type d'installation, sélectionnez **Typique**.
13. Effectuez l'installation d'après les instructions utilisant le "Chemin d'installation typique", décrites dans le centre de documentation d'IBM Tivoli Directory Server. Pour consulter le centre de documentation d'IBM Tivoli Directory Server version 6.3, voir http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm.

    Remarque : Enregistrez les mots de passe que vous avez éventuellement définis lors de l'installation afin de pouvoir les utiliser au cours des étapes d'installation ultérieures.
14. Lorsque l'assistant d'installation de Tivoli Directory Server s'affiche :
    a. Vérifiez que l'instance par défaut est indiquée dans la configuration.
    b. Ne démarrez pas l'instance.
    c. Quittez l'outil.
15. Une fois Tivoli Directory Server installé, vous êtes invité à indiquer le mot de passe `cn=root` fourni lors de l'installation.
16. Cliquez sur le bouton **Configurer IBM Tivoli Directory Server**.

17. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué. Effectuez l'une des actions suivantes :
    - Si l'installation a abouti, cliquez sur **Suivant**.
    - Si l'installation a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\ConfigTDSforISAM.log`. Apportez les corrections nécessaires ou réinstallez Tivoli Directory Server comme indiqué par le fichier journal.
18. Cliquez sur **Terminer** pour fermer le tableau de bord.

Que faire ensuite

- Si vous configurez les communications SSL, reportez-vous à la section «Configuration d'IBM Tivoli Directory Server pour l'accès SSL».
- Sinon, passez à la section Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Configuration d'IBM Tivoli Directory Server pour l'accès SSL

Activez SSL pour sécuriser les communications entre les composants Tivoli Directory Server et Security Access Manager.

Avant de commencer

Effectuez les opérations suivantes :

- Installez et configurez Tivoli Directory Server.
- Installez GSKit.

Pourquoi et quand exécuter cette tâche

Les étapes générales suivantes sont requises pour activer la prise en charge SSL pour Tivoli Directory Server à des fins d'authentification de serveur. Consultez les informations relatives à la sécurisation des communications dans le manuel *IBM Tivoli Directory Server Administration Guide* afin de connaître les détails de chaque étape. Pour procéder, vous devez déjà avoir installé et configuré Tivoli Directory Server.

Procédure

1. Créer la base de données de clés, associée au fichier de mot de passe secret, ainsi que le mot de passe, sur le système Tivoli Directory Server. Par exemple, utilisez gsk8capicmd_64 pour créer la base de données, le fichier de dissimulation et le mot de passe.

   ```
   gsk8capicmd_64 -keydb -create -db /key/myldap.kdb -pw passw0rd
     -type cms -stash -empty
   ```

2. Si vous ne disposez pas déjà d'un certificat personnel ou d'un certificat autosigné, effectuez *l'une* des procédures suivantes :

   Pour un certificat personnel :

   a. Demandez un certificat personnel à une autorité de certification (AC)
   b. Entrez ce certificat personnel dans le fichier de la base de données de clés.
   c. Ajoutez un certificat de signataire pour l'autorité de certification dans le fichier de clés.

Pour un certificat autosigné :

a. Créez un certificat autosigné. Par exemple :

```
gsk8capicmd_64 -cert -create -db /key/myldap.kdb
-pw motdepasse_serveur \
-sigalg ID_algorithme -label libellé_serveur
-dn "cn=LDAP_Server,o=sample" -size taille_de_clé
```

où :

db Spécifie le fichier `.kdb` qui correspond à la base de données de clés.

pw Spécifie le mot de passe d'accès à la base de données de clés.

sigalg Spécifie l'algorithme de signature utilisé pour signer le message. Les valeurs acceptables qui correspondent à un mode de conformité sont répertoriées dans le tableau suivant.

Remarque : Ce paramètre nécessite une version de Tivoli Directory Server au moins égale à 6.3.0.17. Ignorez ce paramètre si vous utilisez une version antérieure de Tivoli Directory Server ou que votre environnement ne nécessite pas de configuration pour la mise en conformité.

Tableau 17. Valeurs de conformité pour le fichier de clés

Mode de conformité planifié pour Security Access Manager 7.0	**Valeur** *ID_algorithme*	**Valeur** *taille de clé*
`aucun(e)`	`SHA1WithRSA`	`2048`
`fips`	`SHA1WithRSA`	`2048`
`sp800-131-transition`	`SHA256WithRSA`	`2048`
`sp800-131-strict`	`SHA256WithRSA`	`2048`
`suite-b-128`	`SHA256WithECDSA`	`256`
`suite-b-192`	`SHA384WithECDSA`	`384`

label Indique le libellé rattaché au certificat client SSL. Le nom du libellé est configuré dans Tivoli Directory Server. Soit le nom de libellé doit correspondre à la valeur configurée dans Tivoli Directory Server, soit vous devez mettre à jour la valeur du nom dans Tivoli Directory Server afin qu'il corresponde à l'étiquette définie ici.

dn Indique un nom distinctif X.500. Exemple de format : `CN=common_name, O=organization, C=country`.

size Taille de la nouvelle paire de clés à créer. Les valeurs de taille dépendent du type de clé. **Remarque :** vous pouvez, pour certains algorithmes, spécifier une valeur nulle (0) en tant que taille de clé par défaut. Cette valeur correspond généralement à la taille minimale considérée comme sûre. Les valeurs correctes sont :

Pour les algorithmes RSA :

`512 à 4 096` ; il convient de sélectionner les tailles de clé comprises dans cette plage de valeurs

conformément à la norme NIST SP800-131. La valeur 8 192 est prise en charge pour la validation uniquement. **Remarque :** les tailles de clé disponibles sont susceptibles de varier en fonction de la configuration de la sécurité. Il n'est pas possible, par exemple, de générer des clés RAS de 512 bits en mode FIPS. La valeur par défaut est `1024`.

Pour les algorithmes EC :

`224` à `512` **Remarque :** la génération de clés GSKit EC prend uniquement en charge les courbes P256, P384 et P521. Les clés de courbe P521 utilisent un hachage SHA2 sur 512 bits. Les valeurs par défaut sont les suivantes :

- `256` (SHA256)
- `384` (SHA384)
- `512` (SHA512)

b. Extrayez le certificat au format ASCII. Par exemple, tapez :

```
gsk8capicmd_64 -cert -extract -db /key/myldap.kdb
-pw motdepasse_serveur
-label myldap -format ascii -target myldap.cert
```

Au cours d'une tape de configuration ultérieure, vous importerez ce certificat dans la section signataire de la base de données de clés sur tous les systèmes clients qui communiquent de façon sécurisée avec le serveur. **Remarque :** un système client est :

- N'importe quelque système serveur de Security Access Manager.
- Tout autre système qui utilise le client Tivoli Directory Server pour communiquer de façon sécurisée avec Tivoli Directory Server.
- Tout système qui utilise le composant Security Access Manager Runtime

Pour plus de détails, voir Annexe A, «Configuration de la sécurité SSL (Secure Sockets Layer)», à la page 327.

3. Configurez l'instance Tivoli Directory Server en vue d'utiliser le certificat dans le fichier de configuration.

Remarque : Créez un fichier `ldif` avec les valeurs de configuration appropriées pour effectuer cette étape. Pour plus d'informations sur les fichiers `ldif`, consultez le manuel *Tivoli Directory Server Administration Guide*. Si vous ne créez pas de fichier `ldif` pour cette étape, vous devez utiliser l'entrée standard pour saisir la configuration.

a. Créez un fichier `ldif` contenant les valeurs suivantes. Remplacez les valeurs en italique par vos propres paramètres.

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslAuth
ibm-slapdSslAuth: serverAuth
```

Remarque : Utilisez la valeur `serverAuth` ou la valeur appropriée pour votre environnement. L'autre valeur correcte est `serverClientAuth`.

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: SSL
```

Remarque : Utilisez la valeur SSL ou la valeur appropriée pour votre environnement. Les valeurs admises sont none, SSL, SSlOnly, TLS et SSLTLS.

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /key/myldap.kdb
```

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace:ibm-slapdSslCertificate
ibm-slapdSslCertificate: libellé_serveur

dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSslKeyDatabasepw
ibm-slapdSslKeyDatabasepw: motdepasse_serveur
```

b. Sauvegardez le fichier et nommez-le. Vous pouvez par exemple l'appeler serverauth.ldif.

c. Exécutez la commande **ldapmodify**.

```
idsldapmodify -h server.in.ibm.com -p 389 -D cn=root -w root \
-i /home/dsrdbm01/serverauth.ldif
```

où :

h *nom_hôte*
Spécifie l'hôte sur lequel est exécuté le serveur LDAP.

p *numéro_port*
Spécifie un port d'écoute TCP alternatif pour le serveur LDAP. Le numéro de port LDAP par défaut est le 389. Si l'option -p n'est pas spécifiée, la valeur par défaut du port SSL LDAP 636 est utilisée.

D *binddn*
Utilisez *binddn* pour établir la liaison avec l'annuaire LDAP. *binddn* est un nom distinctif représenté par une chaîne. Utilisé avec l'option-m DIGEST-MD5, ce paramètre spécifie l'identificateur d'autorisation. Il peut s'agir d'un nom distinctif ou d'une chaîne de type "authzId" commençant par "u:" ou "dn:". **Remarque : -D** binddn **-w** passwd n'appelle pas de fonctions d'association sur les noms distinctifs des superutilisateurs.

i *nom_fichier*
Spécifie les informations relatives à la modification d'entrées en provenance d'un fichier LDIF au lieu de l'entrée standard. Si aucun fichier LDIF n'est indiqué, vous devez utiliser l'entrée standard pour spécifier les enregistrements de mise à jour au format LDIF.

4. Mettez à jour le type de conformité (telle que FIPS), si cela est nécessaire pour votre environnement.

Remarque : Cette étape nécessite une version de Tivoli Directory Server au moins égale à 6.3.0.17. Ignorez cette étape si vous utilisez une version antérieure de Tivoli Directory Server ou que votre environnement ne nécessite pas de configuration pour la mise en conformité.
Créez un fichier ldif avec les valeurs de configuration appropriées pour effectuer cette étape. Pour plus d'informations sur les fichiers ldif, consultez le

manuel *Tivoli Directory Server Administration Guide*. Si vous ne créez pas de fichier `ldif` pour cette étape, vous devez utiliser l'entrée standard pour saisir la configuration.

a. Sélectionnez le mode de conformité souhaité pour votre environnement.
   - `aucun(e)`
   - `fips`
   - `sp800-131-transition`
   - `sp800-131-strict`
   - `suite-b-128`
   - `suite-b-192`

   Pour un descriptif des modes de conformité, reportez-vous à la documentation fournie avec le groupe de correctifs Tivoli Directory Server.

b. Créez un fichier `ldif` contenant les valeurs appropriées en fonction du mode de conformité que vous souhaitez utiliser.

Tableau 18. Valeurs des attributs de conformité

Mode de conformité	Valeurs pour cn=Front End, cn=Configuration	Attributs pour cn=SSL, cn=Configuration
aucun(e)	ibm-slapdSetenv : IBMSLAPD_SECURITY_PROTOCOL= SSLV3,TLS10,TLS11,TLS12	ibm-slapdSecurity : SSLTLS ibm-slapdSslFIPSModeEnabled : false ibm-slapdSslFIPSProcessingMode : false ibm-slapdSslCipherSpec : AES ibm-slapdSslCipherSpec : AES-128 ibm-slapdSslCipherSpec : RC4-128-MD5 ibm-slapdSslCipherSpec : RC4-128-SHA ibm-slapdSslCipherSpec : TripleDES-168 ibm-slapdSslCipherSpec : DES-56 ibm-slapdSslCipherSpec : RC2-40-MD5 ibm-slapdSslCipherSpec : RC4-40-MD5 ibm-slapdSslCipherSpec : TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_RSA_WITH_RC4_128_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_RC4_128_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_RC4_128_SHA

Tableau 18. Valeurs des attributs de conformité (suite)

Mode de conformité	Valeurs pour **cn=Front End, cn=Configuration**	**Attributs pour** cn=SSL, cn=Configuration
fips	ibm-slapdSetenv : IBMSLAPD_SECURITY_PROTOCOL= TLS10,TLS11,TLS12	ibm-slapdSecurity : SSLTLS ibm-slapdSslFIPsProcessingMode : true ibm-slapdSslCipherSpec : AES ibm-slapdSslCipherSpec : AES-128 ibm-slapdSslCipherSpec : TripleDES-168 ibm-slapdSslCipherSpec : TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
sp800-131-transition	ibm-slapdSetenv : IBMSLAPD_SECURITY_PROTOCOL= TLS10,TLS11,TLS12	ibm-slapdSecurity : SSLTLS ibm-slapdSslFIPsProcessingMode : true ibm-slapdSslCipherSpec : AES ibm-slapdSslCipherSpec : AES-128 ibm-slapdSslCipherSpec : TripleDES-168 ibm-slapdSslCipherSpec : TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
sp800-131-strict	ibm-slapdSetenv : IBMSLAPD_SECURITY_PROTOCOL=TLS12 ibm-slapdSetenv : IBMSLAPD_SSL_EXTN_SIGALG= GSK_TLS_SIGALG_RSA_WITH_SHA224, GSK_TLS_SIGALG_RSA_WITH_SHA256, GSK_TLS_SIGALG_RSA_WITH_SHA384, GSK_TLS_SIGALG_RSA_WITH_SHA512, GSK_TLS_SIGALG_ECDSA_WITH_SHA224, GSK_TLS_SIGALG_ECDSA_WITH_SHA256, GSK_TLS_SIGALG_ECDSA_WITH_SHA384, GSK_TLS_SIGALG_ECDSA_WITH_SHA512	ibm-slapdSecurity : SSLTLS ibm-slapdSslFIPsProcessingMode : true ibm-slapdSslCipherSpec : TLS_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_RSA_WITH_AES_256_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ibm-slapdSslCipherSpec : TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
suite-b-128	ibm-slapdSetenv : IBMSLAPD_SUITEB_MODE=128	ibm-slapdSecurity : SSLTLS

Tableau 18. Valeurs des attributs de conformité (suite)

Mode de conformité	Valeurs pour cn=Front End, cn=Configuration	Attributs pour cn=SSL, cn=Configuration
suite-b-192	ibm-slapdSetenv : IBMSLAPD_SUITEB_MODE=192	ibm-slapdSecurity : SSLTLS

c. Sauvegardez le fichier et nommez-le. Vous pouvez par exemple l'appeler `compmode.ldif`.

d. Exécutez la commande **ldapmodify**. Remplacez les valeurs en italique par vos propres valeurs.

```
idsldapmodify -h server.in.ibm.com -p 389 -D cn=root -w root \
-i /home/dsrdbm01/compmode.ldif
```

où :

h *nom_hôte*
Spécifie l'hôte sur lequel est exécuté le serveur LDAP.

p *numéro_port*
Spécifie un port d'écoute TCP alternatif pour le serveur LDAP. Le numéro de port LDAP par défaut est le 389. Si l'option -p n'est pas spécifiée, la valeur par défaut du port SSL LDAP 636 est utilisée.

D *binddn*
Utilisez *binddn* pour établir la liaison avec l'annuaire LDAP. *binddn* est un nom distinctif représenté par une chaîne. Utilisé avec l'option-m DIGEST-MD5, ce paramètre spécifie l'identificateur d'autorisation. Il peut s'agir d'un nom distinctif ou d'une chaîne de type "authzId" commençant par "u:" ou "dn:". **Remarque :** `-D binddn -w passwd` n'appelle pas de fonctions d'association sur les noms distinctifs des superutilisateurs.

i *nom_fichier*
Spécifie les informations relatives à la modification d'entrées en provenance d'un fichier LDIF au lieu de l'entrée standard. Si aucun fichier LDIF n'est indiqué, vous devez utiliser l'entrée standard pour spécifier les enregistrements de mise à jour au format LDIF.

5. Notez le numéro de port SSL sécurisé sur ce serveur. Le numéro de port par défaut est `636`.
6. Copiez le certificat de signataire et ayez-le à disposition pour le copier sur l'ordinateur sur lequel les composants Security Access Manager sont installés et avec lesquels vous souhaitez activer les communications SSL. Au cours d'une tâche ultérieure, vous ajouterez ce certificat à la base de données de clés sur cet ordinateur.

Que faire ensuite

Une fois que vous avez correctement activé les communications SSL sur Tivoli Directory Server, passez à l'étape Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Installation et configuration d'IBM Tivoli Directory Server for z/OS

Utilisez cette tâche pour préparer le serveur LDAP sur z/OS pour Security Access Manager.

Une attention particulière est portée à la configuration de Security Access Manager sur un serveur Tivoli Directory Server for z/OS configuré pour utiliser sa fonction d'authentification native. Cette fonction d'authentification native utilise un registre SAF (System Authorization Facility).

Ces instructions supposent qu'une nouvelle instance de serveur LDAP dédiée au registre Security Access Manager est utilisée. Pour plus d'informations, consultez le manuel *LDAP Server Administration and Use* correspondant à votre version de z/OS. Ce document est disponible via la bibliothèque z/OS à l'adresse :

http://www.ibm.com/systems/z/os/zos/bkserv/

Mise à jour du fichier schéma

Vous devez mettre à jour le schéma z/OS pour prendre en charge la version actuelle de Security Access Manager.

Cette procédure doit être effectuée suite à l'application des fichiers schema.user.ldif et schema.IBM.ldif fournis avec le serveur. Pour obtenir des instructions sur l'application de ces fichiers de schéma, voir la documentation *IBM Tivoli Directory Server for z/OS Administration and Use* à l'adresse :

http://www.ibm.com/systems/z/os/zos/bkserv/

Pour appliquer le schéma de Security Access Manager à Tivoli Directory Server, exécutez l'utilitaire **ivrgy_tool**. Pour obtenir des instructions, voir *IBM Security Access Manager for Web Command Reference*.

Création de suffixe

Security Access Manager requiert la création d'un suffixe qui gère les métadonnées Security Access Manager.

Vous ne devez ajouter ce suffixe qu'une seule fois lors de votre première configuration du serveur LDAP. Ce suffixe permet à Security Access Manager de localiser et de gérer facilement les données. Il sécurise également l'accès aux données en évitant les problèmes d'intégrité et de corruption.

Pour plus d'informations sur les domaines de gestion et la création d'un emplacement pour les métadonnées, voir «Domaines de gestion Security Access Manager», à la page 110 et «Exemple d'emplacement d'un domaine de gestion», à la page 111.

Pour ajouter des suffixes au fichier `slapd.conf`, consultez le manuel *Tivoli Server Administration and Use* à l'adresse :

http://www.ibm.com/systems/z/os/zos/bkserv/

Remarque : Redémarrez le serveur LDAP pour que les changements entrent en vigueur.

Si vous décidez d'ajouter des suffixes après la configuration du serveur de règles Security Access Manager, vous devez appliquer les listes de contrôle d'accès appropriées aux nouveaux suffixes. Vous pouvez utiliser l'outil **ivrgy-tool** pour ce faire. Pour plus d'informations sur **ivrgy-tool**, voir *IBM Security Access Manager for Web Command Reference*.

Pour obtenir des détails sur la mise à jour du fichier de configuration du serveur de sécurité, voir le manuel *Tivoli Directory Server for z/OS Administration and Use Guide*.

Définitions de suffixe pour Security Access Manager

Par défaut, Security Access Manager traite tous les suffixes LDAP définis.

Si des suffixes sont définis sur le serveur LDAP mais ne doivent pas être utilisés par Security Access Manager, ajoutez-les au fichier */rép_install_access_mgr*/etc/ldap.conf à l'aide du mot-clé ignore-suffix lors de la configuration de Security Access Manager pour LDAP sous z/OS.

Par exemple :

```
ignore-suffix = sysplex=UTCPLXJ8
ignore-suffix = "o=Your Company"
ignore-suffix = o=MQuser
```

Dans cet exemple, le suffixe sysplex=UTCPLXJ8 est utilisé pour accéder à la base de données z/OS SDBM (RACF). L'ID administrateur LDAP utilisé par Security Access Manager pendant la configuration n'est pas un ID utilisateur RACF sur le système z/OS et n'a donc pas le droit d'effectuer des recherches SDBM. Si ce suffixe n'a pas été ajouté à la liste ignore-suffix, Security Access Manager reçoit un code retour x'32' - LDAP_INSUFFICIENT_ACCESS pendant la configuration.

Les autres suffixes de la liste sont utilisés par d'autres applications sous z/OS et peuvent âtre ignorés par Security Access Manager.

Notez que Security Access Manager prend en charge la reprise en ligne et l'équilibrage des charges LDAP pour les opérations de lecture. Si vous avez configuré un serveur réplique, vous pouvez fournir le nom d'hôte de la réplique à Security Access Manager dans le fichier ldap.conf, installé avec Security Access Manager dans le sous-répertoire etc.

Administration utilisateur de l'authentification native

L'authentification native fournit la fonction supplémentaire de mappage plusieurs-à-un des utilisateurs Security Access Manager aux ID utilisateur SAF.

La majorité des tâches d'administration reste inchangée avec l'ajout de l'authentification native. Les opérations telles que **user create**, **user show**, l'ajout d'un utilisateur à une entrée ou à un groupe de liste de contrôle et toutes les commandes **user modify** (sauf password) fonctionnent de la même manière que Security Access Manager configuré avec tout autre registre LDAP. Les utilisateurs peuvent modifier leurs propres mots de passe SAF avec l'utilitaire **pkmspasswd** basé sur le Web.

Plusieurs utilisateurs peuvent avoir le même ID **ibm-nativeId** et se connecter avec le même mot de passe. C'est pourquoi, vous devez empêcher les utilisateur mappés plusieurs-à-un de modifier le mot de passe SAF (sinon, vous augmentez le risque qu'un utilisateur verrouille accidentellement ses pairs de leurs comptes).

```
pdadmin sec_master> group modify SAFusers add user1
pdadmin sec_master> acl create deny_pkms
pdadmin sec_master> acl modify deny_pkms set group SAFusers T
pdadmin sec_master> acl attach /Webseal/nom_serveur/pkmspasswd deny_pkms
```

En outre, il n'existe aucune commande d'administration prête à l'emploi permettant de définir l'entrée ibm-nativeId pour un utilisateur. Pour ce faire, les instructions suivantes permettent de gérer les utilisateurs Security Access Manager associés à un nativeId.

La commande **user create** ne change pas :

```
pdadmin sec_master> user create user1 cn=user1,o=tivoli,c=us user1 user1 ChangeMe1
pdadmin sec_master> user modify user1 account-valid yes
```

Le mot de passe (ChangeMe1 dans cet exemple) est défini sur l'entrée userpassword de l'utilisateur dans LDAP, qui n'a aucun effet avec l'authentification native activée. Dans les environnements de production, utilisez le programme utilitaire fourni avec Tivoli Directory Server for z/OS pour supprimer les valeurs userpassword de LDAP. Cela empêche l'accès du mot de passe si l'authentification native est accidentellement désactivée.

Pour définir l'entrée ibm-nativeId pour un utilisateur, créez un fichier ldif appelé *fichier schéma*, similaire au suivant :

```
dn: cn=user1,o=tivoli,c=us
changetype: modify
objectclass: ibm-nativeAuthentication
ibm-nativeId: SAF_username
```

Vous pouvez charger le fichier ldif à l'aide de la commande **ldapmodify** sous z/OS comme suit :

```
ldapmodify -h nom_hôte -p port -D DN_connexion
-w mdp_connexion -f fichier_schéma
```

Remarque : Pour exécuter **idsldapmodify** depuis un client Tivoli Directory Server sur un système distribué, le format du fichier ldif change légèrement :

```
dn: cn=user1,o=tivoli,c=us
objectclass: inetOrgPerson
objectclass: ibm-nativeAuthentication
ibm-nativeId: SAF_username
```

La commande SAF qui permet de réinitialiser le mot de passe d'un utilisateur est :

```
ALTUSER nom_util_SAF PASSWORD(nouveau_mot_de_passe)
```

Outre la redéfinition du mot de passe, la commande marque le mot de passe comme expiré, ce qui requiert sa modification à la prochaine connexion. Si vous le souhaitez, l'option NOEXPIRED peut être ajoutée à la commande pour empêcher ce comportement.

Remarque : Le nom_util_SAF doit être défini comme utilisateur des services système UNIX z/OS. C'est-à-dire que le nom_util_SAF doit être défini sous z/OS avec un segment OMVS. L'exemple suivant est une commande SAF qui permet de définir un nom_util_SAF comme utilisateur des services système UNIX :

```
altuser nom_util_SAF omvs(home(/u/nom_util_SAF) program(/bin/sh) uid(123456))
```

Notez que pour utiliser l'identification utilisateur native, vous devez désactiver l'entrée de strophe auth-using-compare. Pour ce faire, modifiez la strophe [ldap] des fichiers ivmgrd.conf et webseald.conf et modifiez la ligne comme suit :

```
auth-using-compare = no
```

Par défaut, les authentifications sur LDAP sont réalisées avec une opération de comparaison au lieu d'une liaison.

Pour obtenir des informations sur la configuration de l'authentification native, voir la documentation *IBM Tivoli Directory Server for z/OS Administration and Use* à l'adresse :

http://www.ibm.com/systems/z/os/zos/bkserv/

Après avoir configuré IBM Tivoli Directory Server for z/OS en vue de l'utilisation avec Security Access Manager, l'étape suivante consiste à configurer le serveur de règles. Pour obtenir des instructions, voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Configuration d'IBM Tivoli Directory Server pour l'accès à z/OS for SSL

Si Security Access Manager et les services LDAP ne sont pas sur le même réseau protégé, activez la communication SSL entre le serveur LDAP et les clients prenant en charge le logiciel Security Access Manager. Ce protocole permet d'établir des communications chiffrées sécurisées entre chaque serveur et chaque client. Security Access Manager utilise ces canaux de communication dans le processus de décision d'authentification et de décision.

Pourquoi et quand exécuter cette tâche

Pour configurer les communications SSL/TLS, consultez le manuel *IBM Tivoli Directory Server for z/OS for Administration and Use* correspondant à votre version de z/OS. Ce document se trouve à l'adresse :

http://www.ibm.com/systems/z/os/zos/bkserv/

Les étapes générales suivantes sont requises pour activer la prise en charge de SSL/TLS sur z/OS. Pour procéder à ces étapes, vous devez avoir installé et configuré le serveur d'annuaire LDAP, avoir installé z/OS Cryptographic Services System SSL, et avoir configuré `STEPLIB`, `LPALIB`, ou `LINKLIST`.

Procédure

1. Configurez le serveur LDAP pour être à l'écoute des demandes LDAP émises sur le port SSL pour l'authentification de serveur et, le cas échéant, l'authentification de clients. Voir «Options de sécurité du fichier ibmslapd.conf», à la page 82.
2. Générez la clé privée et le certificat du serveur LDAP. Définissez le certificat comme certificat par défaut dans la base de données de clés ou le fichier de clés, ou identifiez-le en indiquant son libellé dans l'option `sslCertificate` du fichier de configuration.

   L'instance z/OS LDAP Server peut utiliser des certificats dans un fichier de clés géré avec la commande RACF **`RACDCERT`**.

   L'utilitaire **`gskkyman`**, utilisé dans les versions précédentes, peut également être utilisé. Un exemple d'utilisation de cet utilitaire pour créer un fichier de base de données de clés se trouve dans «Création d'un fichier de base de données de clés», à la page 83.

   Vous trouvez plus d'informations sur la commande **`RACDCERT`** dans le manuel *IBM z/OS Security Server RACF Command Language Reference* correspondant à votre version de z/OS. Ce document se trouve à l'adresse :

   http://www.ibm.com/systems/z/os/zos/bkserv/
3. Redémarrez le serveur LDAP.

Options de sécurité du fichier ibmslapd.conf

Utilisez les options suivantes pour SSL dans le fichier `ibmslapd.conf`.

listen *URL_ldap*
: Indique l'adresse IP (ou le nom d'hôte), au format URL LDAP, et le numéro de port sur lequel le serveur LDAP est à l'écoute des demandes entrantes des clients. Ce paramètre peut être spécifié plusieurs fois dans le fichier de configuration.

sslAuth {serverAuth | serverClientAuth}
: Indique la méthode d'authentification SSL/TLS. La méthode **serverAuth** permet au client LDAP de valider le serveur LDAP lors du contact initial entre le client et le serveur. La méthode **serverAuth** est la valeur par défaut.

sslCertificate {*certificateLabel* | **none**}
: Indique le libellé du certificat utilisé pour l'authentification de serveur. Cette option est nécessaire si un certificat par défaut n'est pas défini dans le fichier de base de données de clés ou le fichier de clés, ou si un certificat autre que celui par défaut est requis. Si cette option est omise, le certificat par défaut est utilisé.

sslCipherSpecs {*string* | **ANY**}
: Indique les spécifications de chiffrement SSL/TLS des clients qui peuvent être acceptées. Pour obtenir une liste complète des chiffrements pris en charge par votre instance z/OS LDAP Server, consultez le manuel *IBM Tivoli Directory Server for z/OS Administration and Use* correspondant à votre version de z/OS. Ce document se trouve à l'adresse :

  http://www-03.ibm.com/systems/z/os/zos/bkserv/

sslKeyRingFile *nom_fichier* | *fichier_de_clés*
: Indique le chemin et le nom du fichier de la base de données ou fichier de clés SSL/TLS du serveur.

sslKeyRingFilePW *chaîne*
: Indique le mot de passe protégeant l'accès au fichier de la base de données de clés SSL/TLS.

  Lorsqu'un fichier de clés RACF est utilisé au lieu du fichier de la base de données de clés, n'indiquez pas cette option dans le fichier de configuration.

  Remarque : L'utilisation de l'option de configuration **sslKeyRingFilePW** est déconseillée. En revanche, vous pouvez utiliser la prise en charge de fichier de clés RACF ou l'option de configuration **sslKeyRingPWStashFile**. Vous éliminez ainsi le mot de passe du fichier de configuration.

sslKeyRingPWStashFile *nom_fichier*
: Indique un nom de fichier dans lequel le mot de passe du fichier de la base de données de clés du serveur est dissimulé. Si cette option est définie, le mot de passe de ce fichier de dissimulation supprime la valeur spécifiée pour l'option de configuration **sslKeyRingFilePW**. Utilisez l'utilitaire **gskkyman**avec l'option **–s** afin de créer un fichier de dissimulation de mot de passe de base de données de clés.

  Lorsqu'un fichier de clés RACF est utilisé au lieu du fichier de la base de données de clés, n'indiquez pas cette option dans le fichier de configuration.

Création d'un fichier de base de données de clés

L'exemple suivant vous explique comment utiliser l'utilitaire **gskkyman** afin de créer un nouveau fichier de base de données de clés.

Procédure

1. Lancez l'utilitaire **gskkyman** à partir d'une invite shell, comme suit :
   ```
   $ gskkyman
   ```
2. Entrez l'option 1 pour créer un nouveau fichier de base de données de clés.
3. Entrez un nom de base de données de clés ou acceptez le nom par défaut (**key.kdb**).
4. Appuyer sur Entrée.
5. Créez un mot de passe afin de protéger la base de données de clés.
6. Entrez à nouveau le mot de passe de base de données pour vérification.
7. Entrez un délai d'expiration de mot de passe en jours ou acceptez le paramètre par défaut (pas de date d'expiration).
8. Entrez une longueur d'enregistrement de base de données ou acceptez la longueur par défaut (**2500**).
   La base de données de clés est créée et un message s'affiche indiquant si l'opération a abouti ou a échoué
9. Dans le menu Key Management, sélectionnez l'option **6** pour créer un certificat de serveur autosigné et suivez les invites.
10. Une fois le certificat créé, vous devez l'extraire pour l'envoyer au système client LDAP et l'ajouter comme certificat délivré par une autorité digne de confiance. Pour ce faire, procédez comme suit.
    a. Sélectionnez l'option 1 pour gérer des clés et des certificats.
    b. Dans la liste Key and Certificate List, entrez le numéro du libellé du certificat à exporter.
    c. Dans le menu Key and Certificate, entrez l'option 6 pour exporter le certificat vers un fichier.
    d. Dans la boîte de dialogue Export File Format, sélectionnez le format d'exportation. Par exemple, sélectionnez l'option **1** pour exporter au format `Binary ASN.1 DER`.
    e. Entrez le nom du fichier d'exportation.

Résultats

Le certificat est exporté. Vous pouvez maintenant transférer le fichier exporté vers le système client LDAP, et l'ajouter comme certificat délivré par une autorité digne de confiance. Du fait que le format de fichier `binary DER` a été spécifié pour l'exportation, le même type de fichier doit être spécifié pour l'utilitaire **gsk7ikm** sur le système client LDAP, lors de l'opération **Ajouter**.

Que faire ensuite

Passez à l'étape Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Installation et configuration de Microsoft Active Directory

Installez et configurez Microsoft Active Directory à l'aide de la documentation fournie avec le produit. Cette tâche récapitule les étapes et met en évidence les informations spécifiques à la configuration d'Active Directory dans un environnement Security Access Manager.

Avant de commencer

Avant de créer et de configurer un domaine Active Directory, configurez un serveur DNS destiné à héberger le domaine Active Directory. Modifiez le paramètre TCP/IP de sorte que le serveur DNS pointe vers l'ordinateur sur lequel Active Directory est configuré.

Passez en revue les considérations présentées dans les rubriques suivantes :

- «Considérations relatives à URAF», à la page 54
- «Remarques concernant Microsoft Active Directory Server», à la page 54

Pourquoi et quand exécuter cette tâche

Utilisez la documentation de Microsoft Active Directory pour effectuer les étapes décrites dans cette tâche.

Procédure

1. Utilisez la commande **dcpromo** pour installer Active Directory Domain Services.
2. Une fois le domaine créé et le redémarrage de l'ordinateur effectué, vérifiez que les enregistrements d'emplacement du service DNS ont été créés :
   a. Démarrez la console de l'administrateur DNS. Cliquez sur **Démarrer** > **Outils d'administration** > **DNS**.
   b. Développez le nom du serveur, l'option **Forward Lookup Zones**, ainsi que le domaine.
   c. Vérifiez que les dossiers suivants sont présents :
      - **_msdcs**
      - **_sites**
      - **_tcp**
      - **_udp**

      Ces dossiers, ainsi que les enregistrements d'emplacement de service qu'ils contiennent, sont indispensables au fonctionnement d'Active Directory et de Windows Server.
3. Associez l'ordinateur à un domaine Active Directory.
4. Créez un utilisateur dans le domaine.
5. Ajoutez l'utilisateur au groupe d'administrateurs Active Directory.
6. Elevez le domaine à un niveau fonctionnel.
7. Créez un magasin d'autorisations.
8. Créez un groupe dynamique dans le magasin d'autorisations.
9. Ajoutez les privilèges d'administrateur au rôle d'administrateur du magasin Directory Server.

   Par défaut, le magasin d'autorisations peut uniquement être géré par l'administrateur du domaine dans lequel le magasin d'autorisations est créé.

   Pour utiliser la prise en charge du groupe dynamique dans l'environnement de domaine multiple Security Access Manager, ajoutez le groupe Administrateur Enterprise au le rôle d'administrateur. Dès lors, les groupes dynamiques issus de domaines Active Directory situés hors du domaine racine peuvent être utilisés avec Security Access Manager.

10. Modifiez les paramètres de réplication d'Active Directory en définissant les intervalles suivant lesquels vous souhaitez que des notifications soient envoyées entre le contrôleur de domaine et ses partenaires de réplication.
    - **Notification de pause du réplicateur après modification (secondes)**
    - **Notification de pause du réplicateur entre DSA (secondes)**
11. Si vous souhaitez activer SSL pour sécuriser les communications entre Active Directory et les composants Security Access Manager, continuez avec les étapes restantes. SSL permet de chiffrer les données transmises entre les services Security Access Manager et Active Directory afin d'assurer la confidentialité et l'intégrité des données. Envisagez d'activer SSL pour protéger les informations telles que les mots de passe utilisateur et les données privées. SSL n'est pas obligatoire pour que Security Access Manager fonctionne.
    a. Créez un certificat contenant la clé publique et la clé privée de l'ordinateur sur lequel Active Directory est installé. Voir la documentation Microsoft relative à Windows et Active Directory.
    b. Vérifiez que le protocole SSL est configuré et que le port 636 est en cours d'utilisation.
    c. Exportez le certificat *sans* sa clé privée. Conservez un exemplaire de ce certificat. Une fois tous vos systèmes Security Access Manager installés, vous importerez ce certificat sur chacun d'eux.

Que faire ensuite

Après avoir configuré un domaine Active Directory pour l'utilisation avec Security Access Manager, l'étape suivante consiste à configurer le serveur de règles sur un système Windows. Pour obtenir des instructions, voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Installation et configuration de Microsoft Active Directory Lightweight Directory Service (AD LDS)

Utilisez cette tâche pour préparer le serveur AD LDS en vue de l'utilisation avec Security Access Manager.

Avant d'installer Microsoft Active Directory Lightweight Directory Service, lisez «Installation et configuration d'Active Directory Lightweight Directory Service (ADLDS) pour Security Access Manager», qui résume les considérations et exigences importantes sur Security Access Manager lors de l'installation et de la configuration d'AD LDS.

Pour des instructions complètes sur le téléchargement, l'installation et la configuration, reportez-vous à la documentation sur AD LDS fournie par Microsoft Corporation.

Installation et configuration d'Active Directory Lightweight Directory Service (ADLDS) pour Security Access Manager

La présentation suivante fournit des instructions d'installation et de configuration d'Active Directory Lightweight Directory Service (ADLDS) pour l'utilisation comme registre d'utilisateurs avec Security Access Manager.

Procédure

1. Lors de l'installation d'ADLDS, connectez-vous au système à l'aide d'un compte appartenant au groupe Administrateurs local. Utilisez l'assistant d'installation d'Active Directory Lightweight Directory Service pour configurer votre instance ADLDS.
2. Lorsque vous créez une instance d'ADLDS, vous devez spécifier un nom d'instance ADLDS, qui sera utilisé pour identifier de manière unique l'instance et le nom du service ADLDS.
3. Spécifiez les ports utilisés à la fois pour les types de connexion SSL et non-SSL au sein de l'instance ADLDS. Notez les numéros de port que vous indiquez, car ils doivent être entrés lors de la configuration de Security Access Manager.
4. Dans le panneau Partition de l'annuaire d'application de l'assistant d'installation d'Active Directory Lightweight Directory Service, créez une partition d'annuaire d'application qui contient les définitions d'utilisateur et de groupe que vous utilisez.

   Sous la partition d'annuaire, vous pouvez créer d'autres entrées Directory Information Tree (DIT), le cas échéant.
5. Dans le panneau Importation des fichiers LDIF de l'assistant d'installation d'Active Directory Lightweight Directory Service, importez les fichiers LDIF suivants pour mettre à jour le schéma utilisé par cette instance d'ADLDS :
   - MS-InetOrgPerson.LDF
   - MS-User.LDF
   - MS-UserProxy.LDF
6. Lorsque l'installation d'ADLDS est terminée, assurez-vous qu'elle a abouti et qu'elle ne comporte pas d'erreurs. Les fichiers `adamsetup.log` et `adamsetup_loader.log` contiennent des informations qui vous permettent d'identifier et de résoudre les défaillances d'installation d'ADLDS.

Configuration du schéma Security Access Manager pour Active Directory Lightweight Directory Service (AD LDS)

Security Access Manager définit son propre ensemble de types d'entrées et d'attributs LDAP qu'il utilise pour suivre les informations d'utilisateur, de groupe et de règles.

Avant de commencer

Avant d'ajouter des extensions de schéma Security Access Manager, assurez-vous d'avoir défini les définitions de inetOrgPerson et du schéma utilisateur inclus avec AD LDS. Si les extensions inetOrgPerson et schéma utilisateur n'ont pas encore été ajoutées, elles peuvent l'être à l'aide de l'outil de ligne de commande **`ldifde.exe`** et cette opération doit être effectuée avant l'ajout du schéma Security Access Manager.

Pourquoi et quand exécuter cette tâche

Ces extensions du schéma de serveur LDAP de base doivent être ajoutées à Active Directory Lightweight Directory Service (AD LDS) avant de configurer Access Manager.

Une fois AD LDS installé et l'instance AD LDS configurée à l'aide de l'assistant d'installation Active Directory Lightweight Directory, les extensions de schéma Security Access Manager peuvent être ajoutées à AD LDS à l'aide de l'outil de ligne de commande **`ldifde.exe`** inclus avec AD LDS.

Pour ajouter des extensions inetOrgPerson et schéma utilisateur, utilisez la procédure suivante. Une fois ces commandes commandées, le schéma AD LDS inclut les définitions d'attributs et de classes d'objet AD LDS, inetOrgPerson et utilisateur. Si ces extensions de schéma ont déjà été ajoutées, vous pouvez ignorer cette procédure :

Procédure

1. Appliquez le fichier schéma `tam-adamschema.ldf` sur le serveur AD LDS. Le fichier se trouve dans les répertoires suivants :
   - AIX : `/opt/PolicyDirector/etc`
   - Solaris : `/opt/PolicyDirector/etc`
   - Linux : `/opt/PolicyDirector/etc`
   - Windows : *`install base`*`\etc`

     Où *`install-base`* correspond au répertoire d'installation. Le répertoire par défaut est `C:\Program Files\Tivoli\Policy Director`.

   Remarque : Bien que `tam-adamschema.ldf` soit installé comme partie du composant d'exécution de Security Access Manager sur toutes les plateformes, vous devez appliquer le schéma sur le serveur AD LDS opérant uniquement sur Windows. Si vous utilisez Security Access Manager sur un système d'exploitation autre que Windows en même temps qu'AD LDS, vous devez copier le fichier de définition de schéma du programme d'installation Security Access Manager sur le système Windows exécutant AD LDS.
2. Cliquez sur **Démarrer** > **Programmes** > **Accessoires**.
3. Cliquez avec le bouton droit de la souris sur **Invite de commandes**.
4. Cliquez sur **Exécuter en tant qu'administrateur**.
5. Dans l'invite de commande, entrez la commande suivante et appuyez sur ENTREE :

   ```
   ldifde –i –f ms-inetorgperson.ldf –s nom_serveur:numéro_port –k –j . –c
    "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
   ```

   où *nom_serveur* représente le nom du poste de travail et *numéro_port* est le port de connexion LDAP de votre instance AD LDS. Si AD LDS est exécuté sur votre poste de travail local, vous pouvez également utiliser `localhost` comme nom de poste de travail.
6. Entrez la commande suivante et appuyez sur ENTREE :

   ```
   ldifde –i –f ms-user.ldf –s nom_serveur:numéro_port –k –j . –c
    "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext
   ```

   où *nom_serveur* représente le nom du poste de travail et *numéro_port* est le port de connexion LDAP de votre instance AD LDS. Si AD LDS est exécuté sur votre poste de travail local, vous pouvez également utiliser `localhost` comme nom de poste de travail.
7. Après vous être assuré que le schéma AD LDS inclut les définitions d'inetOrgPerson et utilisateur, ajoutez les extensions de schéma Security Access Manager :
   a. Cliquez sur **Démarrer** > **Programmes** > **Accessoires**.
   b. Cliquez avec le bouton droit de la souris sur **Invite de commandes**.
   c. Cliquez sur **Exécuter en tant qu'administrateur**.

d. Dans l'invite de commande, entrez la commande suivante et appuyez sur ENTREE :

```
ldifde –i –e –f tam-adamschema.ldf –s nom_serveur:numéro_port –k –j . –c
 "CN=Schema,CN=Configuration" #schemaNamingContext
```

où *nom_serveur* représente le nom du poste de travail et *numéro_port* est le port de connexion LDAP de votre instance AD LDS. Si AD LDS est exécuté sur votre poste de travail local, vous pouvez également utiliser `localhost` comme nom de poste de travail. Le fichier `tam-adamschema.ldf` est inclus avec la fonction Security Access Manager AD LDS.

Emplacement des données du domaine de gestion pour Active Directory Lightweight Directory Service (AD LDS)

Le registre utilisateur crée et stocke des métadonnées qui permettent le suivi des informations relatives au domaine de gestion Security Access Manager. Vous devez spécifier l'emplacement du stockage de métadonnées.

Ce domaine est créé lors de la configuration du serveur de règles Security Access Manager. Ce domaine est le domaine de sécurité initial.

Durant la configuration du serveur de règles, l'administrateur spécifie le nom du domaine de gestion ou utilise le nom par défaut `Default`.

L'administrateur spécifie également l'emplacement du registre dans lequel ces métadonnées sont stockées en spécifiant le nom distinctif de l'emplacement du domaine de gestion. L'emplacement spécifié doit exister dans le registre d'utilisateurs. Si l'administrateur choisit d'utiliser l'emplacement du domaine de gestion par défaut, les informations sont gérées dans la partition Active Directory Lightweight Directory Service (AD LDS) spécifique, qui doit être appelée

`secAuthority=`*`nom_domaine_gestion`*

où *nom_domaine_gestion* est le nom du domaine de gestion spécifié. Par exemple, si le nom de domaine de gestion par défaut est utilisé, la partition serait appelée `secAuthority=Default`. Si l'administrateur n'utilise pas l'emplacement par défaut et spécifie le nom distinctif de l'emplacement du domaine de gestion, tout emplacement existant dans le registre AD LDS peut être utilisé tant qu'il s'agit d'un objet conteneur.

Remarque : Vous devez sélectionner un nom distinctif d'emplacement dans la même partition d'annuaire que celle dans laquelle les informations d'utilisateur et de groupe sont stockées. AD LDS nécessite que le serveur de règle soit situé dans la même partition de répertoire que les informations sur les utilisateurs et les groupes.

Le serveur de règles ne peut pas gérer les informations d'utilisateur et de groupe hors de la partition d'annuaire AD LDS dans laquelle il est défini.

C'est pourquoi il est recommandé que l'emplacement de gestion par défaut ne soit pas choisi lors de la configuration du serveur de règles si AD LDS est utilisé en tant que registre Security Access Manager. Choisissez l'emplacement du domaine de gestion dans la partition AD LDS dans laquelle vous souhaitez gérer l'utilisateur et les groupes de manière à refléter la structure organisationnelle de l'entreprise.

Avertissement : Si vous sélectionnez l'emplacement de gestion par défaut pendant la configuration du serveur de règles, l'option de suppression permanente des informations de domaine du registre supprime toutes les données dans la partition AD LDS de l'emplacement de gestion de domaine par défaut, y compris les données spécifiques au registre, lorsque vous annulez la configuration de Security Access Manager. Pour conserver les données spécifiques au registre, sélectionnez l'emplacement de domaine de gestion dans la partition AD LDS dans laquelle vous souhaitez gérer des utilisateurs et des groupes. L'emplacement de gestion par défaut est l'emplacement des métadonnées de Security Access Manager.

Configuration d'une partition de répertoires Security Access Manager

Par défaut, Security Access Manager gère ses informations de métadonnées dans une partition de répertoires Active Directory Lightweight Directory Service (AD LDS) spécifique (également appelée contexte d'affectation de nom ou suffixe). La partition de répertoires des métadonnées Security Access Manager par défaut est `secAuthority=Default`.

Pourquoi et quand exécuter cette tâche

Vous devez créer la partition après l'ajout des extensions de schéma Security Access Manager à AD LDS et avant la configuration du serveur de règles Security Access Manager. Pour plus d'informations sur l'ajout d'extensions de schéma, voir «Configuration du schéma Security Access Manager pour Active Directory Lightweight Directory Service (AD LDS)», à la page 86.

Pour créer la partition de répertoires de métadonnées Security Access Manager par défaut, utilisez l'outil d'administration AD LDS **ldp.exe**. Et outil est installé en tant que partie de l'ensemble d'outils d'administration AD LDS. Pour utiliser l'outil **ldp.exe**, vous devez vous connecter et vous lier à l'instance AD LDS en utilisant la procédure suivante.

Vous pouvez également choisir un nom de domaine de gestion et un nom distinctif d'emplacement autres que ceux définis par défaut. Le nom du domaine de gestion doit être unique dans le serveur LDAP et le nom distinctif d'emplacement doit déjà exister. Ces informations vous sont demandées durant l'installation du serveur de règles. Pour obtenir des instructions sur la configuration de ces paramètres pour Security Access Manager Policy Server, voir Annexe D, «Options pdconfig», à la page 339.

Remarque : Vous devez sélectionner un nom distinctif d'emplacement dans la même partition d'annuaire que celle dans laquelle vous allez stocker les informations d'utilisateur et de groupe. Cela est obligatoire car AD LDS requiert l'existence préalable du serveur de règles dans la même partition d'annuaire que celle dans laquelle les informations d'utilisateur et de groupe sont gérées. Le serveur de règles ne peut pas gérer des informations d'utilisateurs et de groupes en dehors de la partition de répertoire où il est lui-même défini.

Procédure

1. Connectez-vous à l'instance AD LDS :
   a. A l'invite de commande, entrez `ldp` et appuyez sur **ENTREE**. La fenêtre **ldp** s'affiche.
   b. Dans le menu **Connection**, cliquez sur **Connexion...**.

c. Dans la zone **Server**, entrez le nom d'hôte ou de serveur de noms de domaine du système sur lequel AD LDS est exécuté. Lorsque l'instance AD LDS est exécutée en local, vous pouvez également entrer `localhost` pour cette valeur de zone.

d. Dans la zone **Port**, entrez le numéro de port LDAP ou SSL de l'instance AD LDS à laquelle vous souhaitez vous connecter. Cliquez ensuite sur **OK**. L'outil ldp se connecte à l'instance AD LDS et affiche les informations de progression obtenues depuis le DSE racine dans le panneau à droite de la fenêtre.

2. Etablissez la liaison avec l'instance AD LDS :

   a. Dans le menu **Connection**, sélectionnez **Bind...**

   b. Pour établir la liaison en utilisant les données d'identification avec lesquelles vous êtes connecté, cliquez sur **Bind as currently logged on user**.

   c. Lorsque vous avez terminé de spécifier les options de liaison, cliquez sur **OK**. L'outil ldp effectue la liaison avec l'instance AD LDS suivant la méthode et les données d'identification spécifiées.

3. Ajoutez des enfants :

   a. Dans le menu **Parcourir**, sélectionnez **Add child**.

   b. Dans la zone **Nom distinctif**, entrez `secAuthority=Default` comme nom distinctif pour la nouvelle partition d'annuaire.

   c. Dans la zone **Edit Entry**, entrez les informations suivantes et cliquez sur **ENTREE**.

      - Dans la zone **Attribute**, entrez `ObjectClass`.
      - Dans la zone **Values**, entrez `secAuthorityInfo`.

   d. Dans la zone **Edit Entry**, entrez les informations suivantes et cliquez sur **ENTREE**.

      - Dans la zone **Attribute**, entrez `secAuthority`.
      - Dans la zone **Values**, entrez `Default`.

   e. Dans la zone **Edit Entry**, entrez les informations suivantes et cliquez sur **ENTREE**.

      - Dans la zone **Attribute**, entrez `version`.
      - Dans la zone **Values**, entrez `7.0`.

   f. Dans la zone **Edit Entry**, entrez les informations suivantes et cliquez sur **ENTREE**.

      - Dans la zone **Attribute**, entrez `cn`.
      - Dans la zone **Values**, entrez `secAuthority`.

   g. Dans la zone **Edit Entry**, entrez les informations suivantes et cliquez sur **ENTREE**.

      - Dans la zone **Attribute**, entrez `instanceType`.
      - Dans la zone **Values**, entrez `5`.

      L'ensemble d'attributs et de valeurs apparaît dans le panneau Entry List.

   h. Assurez-vous que l'option **Synchronous** est sélectionnée et cliquez sur **Run**. La partition de répertoire de métadonnées Security Access Manager requise est ainsi ajoutée à l'instance AD LDS. Pour vérifier que la partition a bien été ajoutée, vous pouvez utiliser l'outil AD LDS ADSI Edit afin de vous connecter à la partition et l'afficher.

Ajout d'un administrateur à la partition des répertoires de métadonnées Security Access Manager

Après avoir ajouté un schéma Security Access Manager à l'instance Active Directory Lightweight Directory Service (AD LDS) et spécifié l'emplacement du répertoire des métadonnées Security Access Manager, ajoutez un administrateur AD LDS pour la partition du répertoire des métadonnées Security Access Manager. L'utilisateur AD LDS est titulaire des droits d'administration pour la partition des répertoires de métadonnées Security Access Manager et est spécifié comme l'administrateur LDAP lors de la configuration de Security Access Manager.

Pourquoi et quand exécuter cette tâche

L'exemple suivant suppose que vous avez accepté le domaine de gestion et l'emplacement par défaut. Si vous avez spécifié un nom de domaine ou un emplacement différent, ajoutez l'administrateur AD LDS à la partition AD LDS que vous avez indiquée.

Procédure

1. Créez l'administrateur LDAP AD LDS :
   a. Démarrez l'éditeur ADSI (`Adsiedit.msc`).
   b. Dans le menu **Action**, cliquez sur **Connect To...** . La boîte de dialogue "Connection Settings" s'affiche.
   c. Dans la zone **Connection name**, entrez le libellé sous lequel cette connexion apparaît dans l'arborescence de console de AD LDS ADSI Edit. Pour cette connexion, entrez `secAuthority`.
   d. Dans la zone **Server name**, entrez le nom d'hôte ou de serveur de noms de domaine du système sur lequel l'instance AD LDS est exécutée. Si l'instance AD LDS se trouve sur le système local, vous pouvez utiliser `localhost` comme nom de serveur.
   e. Dans la zone **Port**, entrez le port de communication LDAP ou SSL utilisé par cette instance AD LDS.

      Remarque : Pour afficher la liste des numéros de port qui sont utilisés par les instances AD LDS, à l'invite de commande, entrez :

      ```
      dsdbutil "list instances" quit
      ```

      sur le système sur lequel l'instance AD LDS est exécutée.
   f. Sous **Connect to the following node**, sélectionnez **Distinguished name (DN) or naming context** et entrez `"secAuthority=Default"` pour le nom distinctif par défaut. Si vous utilisez une partition de répertoires différente, sélectionnez-la. Cet exemple suppose l'utilisation de la partition par défaut.
   g. Sous **Connect using these credentials**, cliquez sur **The account of the currently logged on user**.
   h. Cliquez sur **OK**. Le terme "secAuthority" doit désormais apparaître dans l'arborescence de la console.
2. Sélectionnez les attributs utilisateur :
   a. Développez l'arborescence de secAuthority en cliquant deux fois sur **secAuthority**, puis sur **SECAUTHORITY=DEFAULT**.
   b. Mettez en surbrillance et cliquez avec le bouton droit sur le conteneur **SECAUTHORITY=DEFAULT**, pointez sur **New**, puis cliquez sur **Object...**
   c. Sous **Select a classe**, cliquez sur **user**.

d. Cliquez sur **Suivant**.
e. Pour la valeur de l'attribut `cn`, entrez le nom commun de l'administrateur que vous voulez créer. Par exemple, entrez `tam`.
f. Cliquez sur **Suivant**.
g. Cliquez sur **More Attributes**.
h. Sélectionnez et définissez les propriétés suivantes :

msDS-UserDontExpirePassword
Paramétrez cette propriété sur **True**. Ce paramètre empêche l'application de la règle de délai d'expiration du mot de passe par défaut à cet administrateur. Si vous préférez que cette règle de mot de passe s'applique à cet administrateur, vous pouvez laisser cette propriété non définie.

msDS-UserAccountDisabled
Paramétrez cette propriété sur **False**. Ce paramètre active l'instance que vous avez créée.

i. Cliquez sur **OK**.
j. Aucun attribut supplémentaire n'est requis, mais si vous souhaitez en définir un, cliquez sur **More Attributes**, sélectionnez les attributs à définir et entrez leurs valeurs. Lorsque vous avez terminé, cliquez sur **Terminer**. L'utilisateur est créé avec le nom distinctif `cn=tam,secAuthority=Default`.
k. Pour définir le mot de passe de l'administrateur, mettez en évidence l'utilisateur que vous venez de créer et cliquez dessus avec le bouton droit de la souris. Sélectionnez **Reset password...**
l. Dans le panneau "Reset Password", entrez et confirmez le mot de passe que vous souhaitez utiliser. Lorsque vous avez terminé, cliquez sur **OK**. Mémorisez le nom distinctif de l'utilisateur et le mot de passe que vous avez créés, car ils seront spécifiés comme nom distinctif et mot de passe de l'administrateur LDAP lors de la configuration de Security Access Manager.

3. Ajoutez l'utilisateur au groupe Administrateurs de cette partition :
   a. Dans la partition d'annuaire SECAUTHORITY=DEFAULT, il existe trois conteneurs appelés CN=LostAndFound, CN=NTDSQuotas et CN=Roles.
      1) Mettez en évidence le conteneur **CN=Roles** en cliquant une fois dessus. Dans le panneau de détails à droite de l'outil AD LDS ADSI Edit, les groupes du conteneur Roles sont affichés.
      2) Mettez en évidence le groupe **CN=Administrators** en cliquant une fois dessus.
      3) Cliquez avec le bouton droit de la souris sur le groupe **CN=Administrators** et sélectionnez **Properties**. La page **CN=Administrators Properties** s'affiche.
   b. Sous **Attributes**, faites défiler l'écran pour localiser un membre, puis cliquez dessus.
   c. Cliquez sur **Edit**.
   d. Cliquez sur **Add ADLDS Account...**. Entrez le nom distinctif de l'administrateur que vous avez créé dans la zone **DN**.
   e. Cliquez sur **OK**. L'administrateur est ajouté au groupe Administrateurs et affiché comme membre.
   f. Cliquez sur **OK** pour terminer la mise à jour d'appartenance. Cliquez sur **OK** pour fermer la page "CN=Administrators Properties".

Autorisation de liaison anonyme

Afin de configurer Security Access Manager avec Active Directory Service Mode Active Directory Lightweight Directory Service (AD LDS), AD LDS doit être configuré pour autoriser la liaison anonyme.

Pourquoi et quand exécuter cette tâche

Par défaut, AD LDS n'autorise pas ces liaisons. La configuration de Security Access Manager utilise cependant la liaison anonyme pour vérifier la validité du nom d'hôte, du port et des paramètres SSL configurés pour LDAP.

Si vous souhaitez désactiver la liaison anonyme pendant le fonctionnement normal, l'option peut être réinitialisée sur le serveur AD LDS une fois la configuration terminée.

Procédure

1. Cliquez sur**Démarrer** > **Tous les programmes** > **ADLDS** > **ADLDS ADSI Edit**.
2. Dans l'arborescence de la console, cliquez sur **ADLDS ADSI Edit**.
3. Dans le menu **Action**, cliquez sur **Connect To...** . La boîte de dialogue "Connection Settings" s'affiche.
4. Dans la zone **Connection name**, entrez `Configuration`.
5. Dans la zone **Server name**, entrez le nom d'hôte ou de serveur de noms de domaine du système sur lequel l'instance AD LDS est exécutée. Si l'instance AD LDS se trouve sur le système local, vous pouvez utiliser `localhost` comme nom de serveur.
6. Dans la zone **Port**, entrez le port de communication LDAP ou SSL utilisé par cette instance AD LDS.

   Remarque : Pour répertorier les numéros de port utilisés par les instances AD LDS, cliquez sur **Démarrer** > **Tous les programmes** > **ADLDS** > **ADLDS Tools Command Prompt**. Sur la ligne de commande, entrez : `dsdbutil "list instances" quit` sur le système sur lequel l'instance AD LDS est en cours d'exécution.
7. Sous **Connect to the following node**, sélectionnez **Well-known naming context:** et choisissez **Configuration** dans la liste déroulante.
8. Sous **Connect using these credentials**, cliquez sur **The account of the currently logged on user**.
9. Cliquez sur **OK**. La configuration doit maintenant apparaître sous l'arborescence de la console.
10. Développez le dossier **Configuration** en cliquant deux fois dessus.
11. Cliquez deux fois sur **CN=Configuration,CN=**{*GUID*}, où *GUID* a été généré lors de la configuration de l'instance AD LDS.
12. Cliquez deux fois sur le dossier **CN=Services** pour le développer puis cliquez deux fois sur **CN=Windows NT**.
13. Mettez en évidence **CN=Directory Service** et cliquez dessus avec le bouton droit de la souris puis cliquez sur **Properties**.
14. Cliquez sur **dsHeuristics**.
15. Cliquez sur **Edit**.

16. Modifiez la valeur. Modifiez le septième caractère (en partant de la gauche) sur 2. La valeur doit être similaire à `0000002001001` dans String Attribute Editor.
17. Cliquez sur **OK**.
18. Cliquez sur **OK**. La liaison anonyme est désormais autorisée.

Que faire ensuite

- Si vous configurez les communications SSL, reportez-vous à la section «Configuration d'Active Directory Lightweight Directory Service (AD LDS) en vue d'utiliser SSL».
- Sinon, passez à la section Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Configuration d'Active Directory Lightweight Directory Service (AD LDS) en vue d'utiliser SSL

Activez SSL pour sécuriser les communications entre Active Directory Lightweight Directory Service et les composants Security Access Manager.

Avant de commencer

Installez et configurez Active Directory Lightweight Directory Service, y compris Internet Information Service et le service de gestion Web.

Pourquoi et quand exécuter cette tâche

SSL chiffre les données transmises entre les services Security Access Manager et Active Directory Lightweight Directory Service. Envisagez d'activer SSL pour protéger les informations telles que les mots de passe utilisateur et les données privées. SSL n'est pas obligatoire pour que Security Access Manager fonctionne.

La tâche suivante récapitule les étapes requises pour l'activation des communications SSL.

Remarque : Pour plus d'informations sur l'activation de SSL sur Active Directory Lightweight Directory Service, voir la documentation de Microsoft relative à Windows 2008 et Active Directory Lightweight Directory Service.

Procédure

1. Créez un certificat contenant la clé publique et la clé privée de l'ordinateur sur lequel Active Directory Lightweight Directory Service est installé.
2. Exportez le certificat avec sa clé privée.
3. Localisez le fichier de clés exporté, cliquez deux fois dessus et installez le certificat dans tous les dossiers Personal et Trusted Authorities.
4. À l'aide de la console MMC, importer ce certificat dans les dossiers Personal et Trusted Authorities sous l'instance Active Directory Lightweight Directory Service.
5. Modifiez les droits d'accès aux fichiers de clés privées dans le certificat. Consultez la documentation de Microsoft pour plus de détails.
6. Redémarrez l'instance Active Directory Lightweight Directory Service.
7. À l'aide de la console MMC, exportez le certificat (*sans exporter la clé privée)* depuis le dossier *AD_LDS_instance*`\Personal` et enregistrez le certificat au format de fichier `.cer`.

8. Copier ce fichier `.cer` sur l'ordinateur sur lequel le composant Security Access Manager est installé. Utiliser ce certificat pour configurer Security Access Manager avec le SSL activé.

Que faire ensuite

Une fois que vous avez activé avec succès les communications SSL sur Active Directory Lightweight Directory Service, poursuivez avec Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Installation et configuration de Novell eDirectory

Utilisez cette tâche pour configurer Novell eDirectory en tant que registre d'utilisateurs dans votre environnement Security Access Manager.

Avant de commencer, assurez-vous d'avoir terminé l'installation et la configuration du serveur de base pour Novell eDirectory et l'outil ConsoleOne, comme décrit dans la documentation produit de Novell.

Remarque : Si vous configurez les communications SSL entre le registre d'utilisateurs et les composants Security Access Manager, reportez-vous à la section Annexe A, «Configuration de la sécurité SSL (Secure Sockets Layer)», à la page 327.

Configuration de Novell eDirectory pour Security Access Manager

Si vous installez un nouveau domaine sécurisé Security Access Manager, le schéma Security Access Manager est automatiquement installé sur Novell eDirectory Server (NSD) lorsque le serveur de règles Security Access Manager est configuré. Toutefois, avant de configurer le serveur de règles, vous devez apporter plusieurs modifications au serveur Novell eDirectory.

Pourquoi et quand exécuter cette tâche

Remarque : Dans le schéma Novell eDirectory par défaut, on part du principe que l'annuaire n'utilise pas les classes d'objets X.500 `inetOrgPerson` ou `groupOfNames`. Par défaut, ces classes sont mappées respectivement vers les classes eDirectory User et Group. Dans la mesure où Security Access Manager utilise les classes d'objets `inetOrgPerson` et `groupOfNames` pour créer ses propres utilisateurs et groupes, il est nécessaire d'apporter des modifications au schéma eDirectory par défaut.

Vous pouvez configurer Novell eDirectory pour Security Access Manager en utilisant l'un des outils suivants :

- Utilitaire de gestion de répertoires Novell eDirectory ConsoleOne
- Console d'administration Web de Novell iManager

Pour configurer Novell eDirectory pour Security Access Manager à l'aide de l'utilitaire de gestion d'annuaire Novell eDirectory ConsoleOne, procédez comme suit.

Procédure

1. Démarrez l'utilitaire de gestion d'annuaires Novell ConsoleOne.
2. Sélectionnez l'objet organisation dans l'arborescence Novell eDirectory. Une liste d'objets s'affiche dans la partie droite de la fenêtre ConsoleOne.

3. Cliquez à l'aide du bouton droit de la souris sur l'objet **groupe LDAP** (et non l'objet serveur LDAP), puis cliquez sur **Properties** dans le menu.
4. Cliquez sur l'onglet **Class Map** dans la table des noms de classes LDAP. Les noms de classes Novell eDirectory s'affichent.
5. Supprimez les entrées dotées des classes LDAP `inetOrgPerson` et `groupOfNames`.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **Fermer**.
8. Cliquez sur l'onglet **Attribute Map** dans la table des noms d'attributs LDAP. Les noms d'attributs Novell eDirectory s'affichent.
9. Faites défiler la table et recherchez l'attribut `member` de Novell eDirectory. Vérifiez la valeur de l'attribut LDAP correspondant. Si la valeur de l'attribut LDAP est `member`, aucune modification n'est requise. Si l'attribut affiche la valeur par défaut de `uniqueMember`, il doit être modifié comme suit.
   - Cliquez sur **Modify**. La fenêtre Attribute Mapping s'affiche.
   - Modifiez la zone **Primary LDAP Attribute** et remplacez `uniqueMember` par `member`.
   - Modifiez la zone **Secondary LDAP attribute** et remplacez `member` par `uniqueMember`.
   - Dans la fenêtre Attribute, cliquez sur **OK** pour accepter les modifications.
10. Si vous utilisez Solaris, passez à l'étape suivante. Si vous utilisez Windows NT, vous pouvez ajouter un autre mappage pour l'attribut LDAP `ndsHomeDirectory` comme suit :
    - Dans la partie droite de la fenêtre Attribute Mappings, cliquez sur **Add**. La fenêtre Attribute Mapping est retracée et s'affiche à nouveau.
    - Dans la zone **NSD Attribute** de Novell eDirectory, cliquez sur **Home Directory**.
    - Dans la zone **Primary LDAP Attribute**, cliquez sur `ndsHomeDirectory`.
    - Dans la fenêtre Attribute Mapping, cliquez sur **OK** pour accepter les modifications.
11. Dans la fenêtre Propriétés, cliquez sur **OK**.

Pour configurer Novell eDirectory pour Security Access Manager à l'aide de la console d'administration Web Novell iManager, procédez comme suit.

Procédure

1. Lancez la page Web iManager et connectez-vous en tant qu'administrateur pour que l'arborescence Novell eDirectory soit mise à jour.
2. Cliquez sur l'icône **Roles and Tasks** dans la partie supérieure de la fenêtre iManager pour ouvrir la vue Roles and Tasks.
3. Dans le cadre de navigation Roles and Tasks, développez la catégorie **LDAP**.
4. Dans la liste détaillée, cliquez sur la tâche **Options LDAP**.
5. Dans la page Options LDAP, cliquez sur le groupe LDAP répertorié.

   Remarque : Si l'objet groupe LDAP est manquant, assurez-vous que les plug-ins pour eDirectory ont été installés lors de l'installation de eDirectory. Vous pouvez télécharger le fichier eDir_88_iMan27_Plugins.npm à partir du site de téléchargement de Novell à l'adresse http://download.novell.com.
6. Cliquez sur **Class Map** pour afficher la classe Novell eDirectory dans les mappages de classes LDAP.

7. Supprimez les mappages de `inetOrgPerson` et `groupOfNames`.
   - Faites dérouler la liste et rechercher les mappages de classes eDirectory dans la classe LDAP `inetOrgPerson`.
   - Si un mappage existe, sélectionnez la ligne et cliquez sur l'icône **Remove Mapping** pour le supprimer.
   - Cliquez sur **OK** dans la fenêtre en incrustation pour confirmer la suppression du mappage.
   - Cliquez sur **Appliquer** pour appliquer les modifications.
   - Répétez cette étape pour supprimer un mappage de la classe LDAP `groupOfNames`.
8. Cliquez sur **OK** pour accepter les modifications effectuées.
9. Dans le cadre de navigation Roles and Tasks, développez la catégorie **LDAP**.
10. Dans la liste détaillée, cliquez sur la tâche **Options LDAP**.
11. Dans la page Options LDAP, cliquez sur le groupe LDAP répertorié.
12. Cliquez sur **Attribute Map** pour accéder à l'attribut Novell eDirectory des mappages d'attribut LDAP.
13. Faites défiler la table et recherchez l'attribut membre de Novell eDirectory. Vérifiez la valeur de l'attribut LDAP correspondant. Si l'attribut LDAP est un `membre`, aucune modification n'est requise. Si l'attribut affiche la valeur par défaut de `uniqueMember`, il doit être modifié comme suit :
    - Sélectionnez la ligne et cliquez sur l'icône **View/Edit Mapping**.
    - Modifiez la zone **Primary LDAP Attribute** et remplacez `uniqueMember` par `member`.
    - Modifiez la zone **Secondary LDAP attribute** et remplacez `member` par `uniqueMember`.
    - Cliquez sur **OK** dans la fenêtre en incrustation pour confirmer la modification.
    - Cliquez sur **Appliquer** pour appliquer les modifications.
14. Activez les mots de passe LDAP avec texte en clair.

    Suivez les étapes 1 à 10 de la procédure **Activation des mots de passe LDAP en clair** dans la documentation de Novell Access Manager 3.1, à la section *6.4.4 Configuration d'une règle d'injection d'identité pour l'authentifcation de base* de : http://www.novell.com/documentation//novellaccessmanager31/basicconfig/data/b6z0c3k.html#bbk7tko.
15. Si vous utilisez Solaris, passez à l'étape suivante. Sous Windows, il peut être nécessaire d'ajouter un autre mappage pour l'attribut LDAP `ndsHomeDirectory`. Pour ajouter un autre mappage pour l'attribut LDAP `ndsHomeDirectory` :
    - Cliquez sur l'icône **Add Mapping** dans la partie droite de la fenêtre. Une fenêtre en incrustation permettant de définir le mappage s'affiche.
    - Dans la zone **eDirectory Attribute**, sélectionnez **Home Directory**.
    - Dans la zone Primary LDAP Attribute, entrez `ndsHomeDirectory`.
    - Cliquez sur **OK** pour confirmer le mappage et fermer la fenêtre en incrustation.
16. Cliquez sur **OK** dans la fenêtre Attribute Map pour accepter les modifications.

Après avoir configuré Novell eDirectory pour l'utilisation avec Security Access Manager, l'étape suivante consiste à configurer le serveur de règles. Pour obtenir des instructions, voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Utilisateurs et groupes dans Novell eDirectory

Novell eDirectory définit les classes d'objets `User` et `Group` dans le cadre de son schéma de base. Des instances de ces classes d'objets sont créées par un administrateur eDirectory lors de la définition d'un utilisateur ou d'un groupe, respectivement.

Ces deux classes d'objets sont définies par eDirectory sous forme de *noeuds terminaux*. eDirectory ajoute à chacune de ces définitions de classes d'objets un attribut `X-NDS_NOT_CONTAINER '1'` indiquant qu'elles ne correspondent pas à des objets conteneurs. Les objets qui ne sont pas spécifiés comme objets conteneur ne peuvent pas être définis sous des instances de ces classes d'objet.

Security Access Manager requiert la capacité d'ajout de ses propres objets sous des utilisateurs et groupes eDirectory déjà existants, de sorte qu'ils soient importés et qu'ils puissent être utilisés par Security Access Manager. Lorsque Security Access Manager ajoute ses propres définitions de classes d'objets au schéma eDirectory, il redéfinit également les classes d'objets eDirectory `User` et `Group` pour que des instances de ces classes puissent correspondre à des objets conteneurs. Novell eDirectory autorise que cette modification soit apportée à sa définition de schéma.

Les actions ci-dessous de l'administrateur Novell eDirectory entraînent l'annulation de la modification de Security Access Manager apportée à la classe d'objets `User`. La classe d'objet `Group` n'est pas concernée.

- Exécution de l'outil de réparation de base de données eDirectory, **ndsrepair**, à l'aide de l'option **rebuild schema**.
- Exécution de la réparation de base à partir de la console iManager et exécution de la **réparation de base de données locale** à l'aide de l'option **rebuild operational schema**.
- Application d'une mise à jour corrective à Novell eDirectory.
- Mise à niveau de Novell eDirectory vers une version plus récente.

S'il est nécessaire d'effectuer une de ces opérations après la configuration de Security Access Manager dans le serveur eDirectory, exécutez immédiatement l'utilitaire Security Access Manager ci-dessous pour vous assurer que la définition de la classe d'objets `User` est restaurée.

```
ivrgy_tool -h hôte -p port -D nom_distinctif -w mot_de_passe schema
```

où :

hôte Spécifie le nom d'hôte du serveur LDAP (Novell eDirectory), qui est obligatoire.

port Spécifie le numéro de port du serveur LDAP (Novell eDirectory).

dn Spécifie le nom distinctif de la connexion au serveur LDAP (Novell eDirectory).

mot de passe
Spécifie le mot de passe de connexion du serveur LDAP (Novell eDirectory).

schéma Spécifie le nom du fichier de schéma de Novell eDirectory.

Le fichier **ivrgy_tool.exe** se trouve dans le sous-répertoire `sbin`. Par exemple :

- Sur les systèmes Windows : `d:\Program Files\Tivoli\Policy Director\sbin`
- Sur les systèmes AIX, Linux ou Solaris : `/opt/PolicyDirector/sbin`

Vous devez exécuter cet utilitaire depuis de répertoire sbin car Security Access Manager n'ajoute pas le répertoire sbin au système PATH. Pour plus d'informations sur cet utilitaire, voir *IBM Security Access Manager for Web Command Reference*.

Emplacement du domaine de gestion

Security Access Manager vous permet de spécifier un emplacement de domaine de gestion qui gère les métadonnées Security Access Manager, sauf si vous utilisez l'emplacement de domaine de gestion par défaut.

Créez cet emplacement sur le serveur Novell eDirectory avant de configurer le serveur de règles Security Access Manager.

Security Access Manager étend le schéma Novell eDirectory pour ajouter des attributs et des classes d'objet de métadonnées Security Access Manager. La classe d'objet secAuthorityInfo, définie par Security Access Manager est explicitement définie pour être contenue dans les classes d'objet suivantes :

- treeRoot
- container
- organization
- organizationalUnit
- domain
- country

Novell eDirectory applique strictement la règle de confinement. Si vous spécifiez un emplacement de domaine de gestion ayant une classe d'objet différente de celle répertoriée ici, vous devez modifier manuellement le fichier de schéma novschema.def pour qu'il inclue cette classe d'objet.

Remarque : Vous devez modifier le fichier de schéma avant de configurer Security Access Manager.

Le chemin d'accès complet du fichier schéma de Security Access Manager Novell eDirectory se trouve sous *[répertoire d'installation de Security Access Manager]*/etc/novschema.def. L'exemple suivant indique comment modifier le fichier de schéma.

1. Ouvrez le fichier de schéma.
2. Remplacez la partie suivante :

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' )
 )
-
add: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
```

```
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' 'container' 'organization'
 'organizationalUnit' 'domain' 'country')
 )
```

par

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' )
 )
-
add: objectclasses
objectClasses: (
1.3.6.1.4.1.4228.1.8
NAME 'secAuthorityInfo'
DESC 'Security Authority Information'
SUP 'eApplicationSystem'
STRUCTURAL
MUST ( secAuthority $ version )
X-NDS_NAMING 'secAuthority'
X-NDS_CONTAINMENT ( 'treeRoot' 'container' 'organization'
'organizationalUnit' 'domain' 'country'
 'votre_classe_objet')
 )
```

Pour plus d'informations sur les domaines de gestion et la création d'un emplacement pour les métadonnées, voir «Domaines de gestion Security Access Manager», à la page 110 et «Exemple d'emplacement d'un domaine de gestion», à la page 111.

Accès SSL sur le serveur Novell eDirectory

Secure Socket Layer (SSL) permet de chiffrer les données transmises entre les services Security Access Manager et le serveur Novell eDirectory, afin de garantir leur confidentialité et leur intégrité.

Les administrateurs doivent envisager l'utilisation de SSL pour protéger les informations, comme les mots de passe utilisateur et les données privées. Toutefois, SSL n'est pas requis pour Security Access Manager. Si SSL n'est pas requis dans votre environnement Security Access Manager, ignorez cette section.

Security Access Manager prend en charge l'authentification côté serveur avec Novell eDirectory uniquement. Pour configurer le serveur Novell eDirectory pour SSL, vérifiez que l'outil ConsoleOne est installé et complétez les sections suivantes.

- «Création d'un objet d'autorité de certification organisationnelle», à la page 101
- «Création d'un certificat autosigné», à la page 102
- «Création d'un certificat pour le serveur LDAP», à la page 102
- «Activation du protocole SSL», à la page 103

Remarque : Pour plus d'informations, consultez la documentation du produit Novell sur les sites Web suivants :

Pour Novell eDirectory version 8.6.*x*, voir :

http://www.novell.com

Pour Novell eDirectory version 8.7, voir :

http://www.novell.com

Création d'un objet d'autorité de certification organisationnelle

Lors de l'installation d'eDirectory, un objet **NDSPKI:Certificate Authority** est créé par défaut (s'il n'existe pas sur le réseau).

Pourquoi et quand exécuter cette tâche

Important : le nom de sujet (pas le nom d'objet) doit être un signataire valide. Le nom de sujet doit avoir une zone **organisation** et une zone de pays pour être reconnu comme valide par Security Access Manager. Le nom de sujet par défaut est le suivant :

`0=`*`nom_entrée_organisationnelle`*`.OU=Organizational DVD`

Ce n'est pas un signataire valide. Pour le modifier, vous devez recréer l'objet Autorité de certification avec un nom de sujet valide. Pour ce faire, procédez comme suit.

Procédure

1. Démarrez ConsoleOne.
2. Sélectionnez l'objet conteneur **Security**. Les objets s'affichent dans le panneau de droite de la fenêtre.
3. Sélectionnez l'objet Organization AC et supprimez-le.
4. Cliquez à nouveau avec le bouton droit sur l'objet conteneur **Security** et cliquez sur **New → Object**.
5. Dans la zone de liste de la boîte de dialogue New Object, cliquez deux fois sur **NDSPKI: certificate authority**. La boîte de dialogue Create an Organizational Certificate Authority Object s'affiche. Suivez les instructions en ligne.
6. Sélectionnez le serveur cible et entrez un nom d'objet eDirectory. Par exemple :
   Zone Host Server = `C22Knt_NDS.AM`
   Zone Object Name = `C22KNT-CA`
7. Sous Creation Method, sélectionnez **Custom**.
8. Cliquez sur **Suivant**. En fonction de la version installée de Novell eDirectory, deux écrans supplémentaires peuvent s'afficher.
9. Cliquez deux fois sur **Suivant** pour continuer.
10. Acceptez le nom de sujet par défaut ou entrez un nom distinctif valide de l'autorité de certification en cours de configuration. Tous les certificats générés par l'autorité de certification sont placés à cet endroit.
11. L'autorité de certification organisationnelle s'affiche dans ConsoleOne sous le nom `C22KNT-CA`.

Création d'un certificat autosigné

Pour activer SSL, vous avez besoin d'un certificat. Vous pouvez créer un certificat autosigné pour répondre à cette exigence.

Procédure

1. Accédez aux propriétés de l'autorité de certificat organisationnelle (`C22KNT-CA`). La fenêtre Propriétés s'affiche.
2. Sélectionnez l'onglet **Certificate** puis choisissez **Self Signed Certificate** dans le menu.
3. Validez le certificat.
4. Exportez le certificat. La fenêtre Export a Certificate s'ouvre.
5. Acceptez les valeurs par défaut et notez l'emplacement de sauvegarde du certificat autosigné. Par exemple :

   ```
   c:\c22knt\CA-SelfSignedCert.der
   ```
6. Transférez le fichier (via FTP) vers le répertoire hôte de Security Access Manager. Par exemple :

   ```
   c:\Program Files\Tivoli\Policy Directory\keytab
   ```

   Remarque : il s'agit d'un fichier binaire.

Création d'un certificat pour le serveur LDAP

Un certificat serveur est requis pour activer SSL.

Procédure

1. Pour créer un certificat pour le serveur LDAP, cliquez avec le bouton droit sur l'entrée Organization.
2. Cliquez sur **New → Object**. La fenêtre New Object s'affiche.
3. Sélectionnez **NDSPKI: Key Material**.
4. Cliquez sur **OK**. La fenêtre Create Server Certificate (Key Material) s'affiche.
5. Entrez le nom du certificat. Par exemple, `AM`
6. Sélectionnez la méthode de création **Custom**.
7. Cliquez sur **Suivant**.
8. Utilisez les valeurs par défaut pour l'option **Specify the certificate authority option**, ce qui signe le certificat.
9. Cliquez sur **Suivant**.
10. Indiquez la taille de la clé et acceptez les valeurs par défaut de toutes les autres options.
11. Cliquez sur **Suivant**.

    Remarque : La taille de clé par défaut de Novell eDirectory Version 8.6.2 est **1024** bits, et **2048** bits pour la version 8.7.
12. Dans la fenêtre Specify the Certificate Parameters, cliquez sur le bouton **Edit** en regard de la zone **Subject Name**. La fenêtre Edit Subject s'ouvre.
13. Entrez le nom du sujet.
14. Cliquez sur **OK**. La fenêtre Create Server Certificate (Key Material) s'affiche avec le champ **Subject Name** mis à jour.
15. Cliquez sur **Suivant** pour continuer.
16. Pour accepter les valeurs par défaut dans les fenêtres suivantes, cliquez sur **Suivant** à deux reprises.

17. Cliquez sur **Terminer** pour créer un élément de clé. La fenêtre Creating Certificate s'affiche temporairement. Lorsqu'elle s'efface, le panneau droit de ConsoleOne est mis à jour avec l'entrée de matériel clé appelée `AM`. Cette entrée est le certificat de serveur.

Activation du protocole SSL

Appliquez la procédure suivante pour activer SSL.

Procédure

1. Dans le panneau de droite de ConsoleOne, recherchez une entrée appelée **LDAP Server –** *nom_hôte* et cliquez avec le bouton droit dessus.
2. Dans le menu, sélectionnez **Propriétés**. Dans le bloc-notes de propriétés, sélectionnez l'onglet SSL Configuration.
3. Cliquez sur l'icône **Tree Search** en regard de la zone **SSL Certificate**. La fenêtre Select SSL Certificate s'affiche. Le panneau SSL Certificate List affiche les certificats connus de l'organisation.
4. Sélectionnez le certificat `AM`.
5. Cliquez sur **OK**. La fenêtre Properties of LDAP Server – *nom_hôte* s'affiche à nouveau avec la zone **SSL Certificate** mise à jour.
6. Copiez le certificat de signataire et tenez-le à disposition afin de le copier sur les serveurs Security Access Manager avec lesquels vous souhaitez configurer les communications SSL.

Que faire ensuite

Passez à l'étape Chapitre 6, «Configuration d'un serveur de règles», à la page 109.

Installation et configuration de Sun Java System Directory Server

Vous pouvez utiliser une version prise en charge de Sun Java System Directory Server en tant que registre d'utilisateurs pour Security Access Manager.

Avant de commencer

Passez en revue les considérations des rubriques suivantes avant de configurer Sun Java System Directory Server dans votre environnement :

- «Remarques relatives à LDAP», à la page 52
- «Considérations relatives à Sun Java System Directory Server», à la page 53

Pourquoi et quand exécuter cette tâche

Effectuez l'installation et la configuration de base du serveur comme décrit dans la documentation du produit Sun Java System Directory Server. Par exemple, pour Sun Java System Directory Server version 7.0, voir :

- Guide d'installation : http://download.oracle.com/docs/cd/E19424-01/820-4807/820-4807.pdf
- Guide d'administration : http://download.oracle.com/docs/cd/E19424-01/820-4809/820-4809.pdf

Puis, reportez-vous à la même documentation pour créer un suffixe pour Security Access Manager.

Procédure

1. Créez l'emplacement du domaine de gestion destiné à contenir les données de Security Access Manager.

   Utilisez le nom distinctif du suffixe de l'emplacement ; par exemple : `secAuthority=Default`.

   Le nom doit être au format de nom distinctif (DN) relatif et comprendre une paire attribut-valeur. Si vous indiquez plusieurs paires attribut-valeur, séparez-les par des virgules. L'emplacement par défaut est `secAuthority=Default`.

   Pour plus d'informations sur les domaines de gestion et la création d'un emplacement pour les métadonnées, voir :

   - «Domaines de gestion Security Access Manager», à la page 110
   - «Exemple d'emplacement d'un domaine de gestion», à la page 111
2. Modifiez le nom de la base de données lorsque vous créez un nouveau suffixe.

   Avertissement : N'acceptez pas la valeur par défaut pour le nom de la base de données lors de la création d'un suffixe. Par défaut, l'emplacement des fichiers de base de données pour ce suffixe est sélectionné automatiquement par le serveur. De même, par défaut, le suffixe gère uniquement les index système, aucune attribut n'est chiffré et la réplication n'est pas configurée. Si vous acceptez la valeur par défaut, Sun Java Directory Server stocke le suffixe sous le nom de base de données **Default**. Vos données sont supprimées lors du redémarrage de Sun Java Directory Server.
3. Assurez-vous que le suffixe a été créé. Si vous décidez de créer un suffixe pour gérer les données d'utilisateur et de groupe, effectuez à nouveau cette procédure pour créer un autre suffixe dans la base de données par défaut ou dans une nouvelle base de données. Vous pouvez par exemple créer un suffixe `o=ibm,c=us` dans la même base de données.
4. Effectuez l'action appropriée :
   - Si vous n'avez pas ajouté de suffixe différent de l'emplacement du domaine de gestion, la configuration est terminée. Une entrée d'annuaire est automatiquement ajoutée pour l'emplacement du domaine de gestion lors de la configuration du serveur de règles.
   - Si vous avez ajouté des suffixes différents de l'emplacement du domaine de gestion, créez des entrées d'annuaire pour chaque nouveau suffixe.
5. Si vous souhaitez activer les communications SSL entre Directory Server et Security Access Manager, continuez avec les étapes restantes :
   a. Démarrez l'instance Sun Java System Directory Server.
   b. Obtenez un certificat pour l'instance et enregistrez-la dans la base de données de clés. Le certificat peut être émis par une autorité de certification (CA) ou autosigné. Le certificat inclut un certificat serveur et une clé privée. Appliquez les méthodes décrites dans la documentation de Sun Java System Directory Server.
   c. Notez le numéro de port SSL sécurisé sur ce serveur. Le numéro de port par défaut est `636`.
   d. Obtenez le certificat de signataire.

      Remarque : Si le certificat est émis par une autorité de certification, le certificat serveur contient un certificat de signataire. Si le certificat est autosigné, le certificat serveur fait office de certificat de signataire.

e. Copiez le certificat de signataire sur l'ordinateur sur lequel les composants Security Access Manager sont installés et avec lesquels vous souhaitez activer les communications SSL.

Que faire ensuite

Après avoir configuré Directory Server en vue de l'utilisation avec Security Access Manager, vous pouvez configurer le serveur de règles. Voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109. Utilisez les valeurs suivantes dans votre configuration :

- La valeur de l'ID administrateur LDAP pour Sun Directory Server est `cn=Directory Manager`. La valeur par défaut de cet attribut est `cn=root`, mais elle n'est pas appropriée pour Sun Directory Server.
- La valeur du nom distinctif pour l'emplacement du domaine de gestion LDAP sous Sun Directory Server est un suffixe (par exemple, `dc=ibm,dc=isam`) créé dans le répertoire d'instance. La valeur par défaut de cet attribut est vide et n'est pas appropriée pour Sun Directory Server.

Partie 3. Installation du composant système de base

© Copyright IBM Corp. 2001, 2013

Chapitre 6. Configuration d'un serveur de règles

Le serveur de règles Security Access Manager gère la base de données d'autorisation maître du domaine de gestion ainsi que les bases de données de règles associées à d'autres domaines sécurisés que vous êtes susceptible de créer.

Ce serveur est essentiel dans le traitement des contrôles d'accès, des authentification et des requêtes d'autorisation. Il met également à jour les répliques de base d'autorisation et gère les informations d'emplacement relatives à d'autres serveurs Security Access Manager.

Vous devez installer et configurer un seul serveur de règles pour chaque domaine sécurisé.

Pour conserver la flexibilité et assurer l'efficacité de l'équilibrage de charge, il est recommandé de configurer le serveur de règles sur un système distinct de votre serveur de registre.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Facultatif : vous pouvez également configurer un serveur de règles de secours afin de prévenir tout incident système. Cette fonction requiert des logiciels et du matériel supplémentaires. Pour plus d'informations, voir :

- Annexe G, «Configuration du serveur de règles de secours (AIX)», à la page 381
- Annexe H, «Configuration d'un serveur de règles de secours avec IBM Tivoli System Automation for Multiplatforms», à la page 397

Le serveur de règles nécessite l'installation des produits et des composants Security Access Manager prérequis suivants :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server (en fonction du registre utilisé)
- Security Access Manager License
- IBM Security Utilities
- Security Access Manager Runtime
- Security Access Manager Policy Server

Remarque : Security Access Manager ne prend pas en compte les règles de mot de passe natif de registre lors de la création des comptes de serveur lors de la configuration. Les règles natives sur les mots de passe de registre peuvent entraîner l'échec de la configuration du serveur. Avant de procéder à la configuration, désactivez les règles natives de mot de passe de registre, comme le registre par défaut et les règles de mot de passe global. Après la configuration, définissez des exceptions sur le registre pour que les nouveaux comptes de serveurs de soient pas affectés par les règles natives de mot de passe de registre. Vous pouvez maintenant activer les règles de mot de passe natives du registre.

Sélection de format de données LDAP

Lors de la configuration du serveur de règles, sélectionnez le format de données LDAP à utiliser pour les informations de suivi d'utilisateurs et de groupes.

© Copyright IBM Corp. 2001, 2013

Les deux formats de données LDAP disponibles pour les informations d'utilisateurs et de groupes sont :

Minimal
Le format **Minimal** utilise moins d'objets LDAP pour conserver les informations de suivi d'utilisateur et de groupe. L'utilisation de ce format permet de réduire la taille de votre registre d'utilisateurs en stockant des informations minimales de suivi d'utilisateur et de groupe.

Standard
Le format **Standard** utilise davantage d'objets LDAP pour conserver les informations de suivi d'utilisateur et de groupe. Ce format a également été utilisé dans les versions d'IBM Tivoli Access Manager for E-Business antérieures à la version 6.0.

Si les informations d'utilisateur et de groupe du registre LDAP sont utilisées par d'autres produits Security Access Manager tels que IBM Tivoli Access Manager for Operating Systems ou IBM Tivoli Federated Identity Manager, le même format de données LDAP doit être utilisé pour tous les produits.

Domaines de gestion Security Access Manager

Si vous utilisez LDAP comme registre d'utilisateurs, Security Access Manager propose un ou plusieurs domaines d'administration. Un domaine est composé de l'ensemble des utilisateurs, groupes et ressources devant être protégés par la règle de sécurité utilisée pour protéger les ressources.

En fonction des gestionnaires de ressources installés, les ressources peuvent être toute entité physique ou logique, notamment des objets tels que des fichiers, des répertoires, des pages Web, des services réseau et d'impression et des files d'attente de messages. Une règle de sécurité appliquée dans un domaine affecte uniquement les objets se trouvant dans ce domaine. Les utilisateurs qui sont autorisés à exécuter des tâches dans un domaine n'ont nécessairement pas le droit d'exécuter ces tâches dans d'autres domaines.

Le domaine initial dans un registre LDAP est appelé le *domaine de gestion*. Il est créé lors de la configuration du serveur de règles. Lors de la configuration du serveur de règles, vous êtes invité à indiquer le nom de domaine de gestion et le nom distinctif d'emplacement de domaine de gestion dans l'arborescence DIT (Directory Information Tree) sur le serveur LDAP où sont conservées les informations sur le domaine. Voir Annexe D, «Options pdconfig», à la page 339 pour obtenir des instructions la configuration de ces paramètres pour le serveur de règles Security Access Manager.

Si l'emplacement du domaine de gestion n'est pas spécifié, cette information est stockée dans son propre suffixe par défaut sur le serveur LDAP. Que vous utilisiez l'emplacement par défaut ou spécifiiez un emplacement spécifique dans la DIT LDAP, l'emplacement spécifié pour le domaine de gestion doit déjà exister, sauf si le registre d'utilisateurs est Novell eDirectory. Pour Novell eDirectory, si vous n'avez pas spécifié l'emplacement du domaine de gestion, Security Access Manager utilise l'emplacement racine. L'emplacement racine est un emplacement de domaine qui n'a pas de suffixe. Si vous entrez un emplacement spécifique pour le domaine de gestion, vérifiez que l'emplacement spécifié existe déjà.

Lorsqu'un domaine Security Access Manager est créé, notamment le domaine de gestion initial, une entrée est créée dans le serveur LDAP et est appelée objet secAuthorityInfo. Cet objet représente le domaine Security Access Manager et il est

nommé à l'aide de l'attribut secAuthority avec le nom de domaine comme valeur ; par exemple : `secAuthority=<nom_domaine>`.

Si vous n'indiquez pas de nom, le nom par défaut du domaine sera `Default`, et le nom de l'objet secAuthorityInfo sera `secAuthority=Default`.

Exemple d'emplacement d'un domaine de gestion

Si vous souhaitez spécifier un emplacement autre que celui par défaut pour le domaine de gestion, vous pouvez utiliser tout emplacement dans la DIT LDAP.

A titre d'exemple, si le serveur LDAP est configuré avec un suffixe `c=us` et que l'administrateur indique un nom distinctif d'emplacement de domaine de gestion `ou=austin,o=ibm,c=us`, cet objet peut être créé à l'aide d'un fichier contenant le LDIF suivant :

```
dn: c=us
objectClass: top
objectClass: country
c: US

dn: o=ibm,c=us
objectClass: top
objectClass: organization
o: IBM

dn: ou=austin,o=ibm,c=us
objectClass: top
objectClass: organizationalunit
ou: Austin
```

L'objet peut alors être créé à l'aide de l'utilitaire de ligne de commande **idsldapadd** comme suit :

```
idsldapadd –h <nom_hôte_ldap> -p <port_ldap> -D <ND_admin_ldap>
-w <motdepasse_admin_ldap> -v –f DIT_exemple
```

où :

- *nomhôte_ldap* est le nom d'hôte du serveur LDAP.
- *port_ldap* est le port de serveur LDAP.
- *ND_admin_ldap* est le nom distinctif de l'administrateur de serveur LDAP.
- *motdepasse_admin_ldap* est le mot de passe de l'administrateur de serveur LDAP.
- *DIT_exemple* est le nom du fichier contenant le LDIF.

Modifiez cet exemple pour le nom d'espace LDAP spécifique correspondant à votre organisation.

Une fois l'objet LDAP créé, vous pouvez l'utiliser comme nom distinctif d'emplacement de domaine de gestion lors de la configuration de serveur de règles. Pour obtenir des instructions la configuration de ces paramètres pour le serveur de règles Access Manager, voir Annexe D, «Options pdconfig», à la page 339.

Remarque :

Si les conditions suivantes sont vérifiées, une instance WebSEAL ne peut pas modifier les mots de passe des utilisateurs en raison de l'absence de paramètres ACL requis pour rechercher des emplacements de domaines.

- Vous avez configuré le serveur de règles dans un emplacement autre que celui par défaut (`secAuthority=Default`).
- Vous avez créé des sous-domaines Security Access Manager au nouvel emplacement.
- Vous avez configuré une instance WebSEAL dans l'un des nouveaux sous-domaines.

Si vous configurez le serveur de règles dans un emplacement autre que celui par défaut et que ces autres conditions existent, voir le manuel *IBM Security Access Manager for Web Troubleshooting Guide* pour plus d'informations sur la définition correcte de la liste de contrôle d'accès.

Emplacement d'un domaine de gestion pour un registre Active Directory Lightweight Directory Service (AD LDS)

Si Active Directory Lightweight Directory Service (AD LDS) est utilisé comme registre LDAP, vous devez choisir un nom distinctif d'emplacement dans la même partition de répertoire pour stocker les informations de groupes et d'utilisateurs.

Cela est dû à une restriction d'AD LDS qui stipule que le serveur de règles doit exister dans la même partition de répertoire que celle où sont gérées les informations de groupes et d'utilisateurs. Le serveur de règles ne peut pas gérer d'informations d'utilisateurs et de groupes en dehors de la partition de répertoire dans laquelle il est lui-même défini.

Installation du serveur de règles via la ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer le serveur de règles. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **`pkgadd`**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows

setup.exe

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **pdconfig** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **pdjrtecfg**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **amwpmcfg** pour configurer le composant Security Access Manager Web Portal Manager.

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation du serveur de règles

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Assurez-vous que votre serveur de registre est en cours d'exécution en mode normal avant d'installer le serveur de règles.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
5. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
8. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers.

- *packages* représente les packages suivants :

  PD.RTE Spécifie le package Security Access Manager.

  PD.Mgr Spécifie le package du serveur de règles Security Access Manager.

Avertissement : *Ne configurez pas* Security Access Manager Runtime avant que le serveur de règles ne soit installé.

9. Démontez, le cas échéant, le DVD.
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration : `pdconfig`
    Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez le composant Security Access Manager Runtime, puis le package du serveur de règles Security Access Manager.
    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.
    Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** (Quitter) deux fois pour fermer l'utilitaire de configuration.

Remarque : Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Résultats

Cette étape termine la configuration du système de serveur de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : la configuration du serveur de règles Security Access Manager crée un fichier d'autorité de certification SSL par défaut appelé `pdcacert.b64`. Le fichier de clés SSL et le certificat sont créés au moyen d'algorithmes appropriés selon le type de configuration.

Lorsque la configuration du composant Security Access Manager Policy Server Policy Server aboutit, un message similaire au suivant s'affiche.

```
La configuration de Security Access Manager Policy Server a abouti.
Le certificat d'AC du gestionnaire est codé en base 64 et sauvegardé dans le fichier
/var/PolicyDirector/keytab/pdcacert.b64
Vous devez distribuer ce fichier à toutes
les machines de votre domaine sécurisé.
Cette opération est indispensable à la réussite de la configuration.
```

Pour qu'un système d'exécution Security Access Manager s'authentifie sur les serveurs Security Access Manager, chaque système d'exécution requiert une copie de fichier. Pour créer ce fichier, procédez comme suit.

- Lors de la configuration du package Security Access Manager Runtime (à l'aide de l'utilitaire **pdconfig**), sélectionnez le téléchargement automatique du fichier `pdcacert.b64`.
- Copiez manuellement le fichier `pdcacert.b64` sur le système Security Access Manager avant de configurer le composant Security Access Manager Runtime.

Linux : Installation du serveur de règles

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire */chemin_package*`/linux_s390`.

Remarque à l'attention de tous les utilisateurs de Linux : si vous effectuez une installation sur un système Linux avec SELinux activé, vous devez exécuter les commandes suivantes pour activer serveur de règles et d'autorisations :

```
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/C/icc/osslib/libcryptoIBM080.so.0.9.8
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/N/icc/osslib/libcryptoIBM081.so.0.9.8
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamzcars.so
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/libgsk8krsw.so
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamcars.so
```

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Assurez-vous que votre serveur de registre est en cours d'exécution (en mode normal) avant d'installer le serveur de règles.
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Accédez au répertoire *chemin_package*`/`*distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.

6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
9. Installez les Security Access Managerpackages.

	Linux sur x86-64	**Linux on System z**
Package Security Access Manager Runtime	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Package **Security Access Manager** Policy Server	`PDMgr-PD-7.0.0-0.x86_64.rpm`	`PDMgr-PD-7.0.0-0.s390.rpm`

Avertissement : *Ne configurez pas* Security Access Manager Runtime avant que le serveur de règles ne soit installé.

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration : `pdconfig`
    Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez le composant Security Access Manager Runtime, puis le package du serveur de règles Security Access Manager.
    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.
    Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** (Quitter) deux fois pour fermer l'utilitaire de configuration.

Remarque : Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Résultats

Cette étape termine la configuration du système de serveur de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : la configuration du serveur de règles Security Access Manager crée un fichier d'autorité de certification SSL par défaut appelé `pdcacert.b64`. Le fichier de clés SSL et le certificat sont créés au moyen d'algorithmes appropriés selon le type de configuration.

Lorsque la configuration du composant Security Access Manager Policy Server aboutit, un message similaire au suivant s'affiche :

```
La configuration de Security Access Manager Policy Server a abouti.
Le certificat d'AC du gestionnaire est codé en base 64 et sauvegardé dans le fichier
/var/PolicyDirector/keytab/pdcacert.b64
Vous devez distribuer ce fichier à toutes
les machines de votre domaine sécurisé.
Cette opération est indispensable à la réussite de la configuration.
```

Pour qu'un système d'exécution Security Access Manager s'authentifie sur les serveurs Security Access Manager, chaque système d'exécution requiert une copie de fichier. Pour obtenir ce fichier, choisissez l'une des options suivantes :

- Lors de la configuration du package Security Access Manager Runtime (à l'aide de l'utilitaire **pdconfig**), sélectionnez le téléchargement automatique du fichier `pdcacert.b64`.
- Copiez manuellement le fichier `pdcacert.b64` sur le système Security Access Manager avant de configurer le composant Security Access Manager Runtime.

Solaris : Installation du serveur de règles

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Assurez-vous que votre serveur de registre est en cours d'exécution (en mode normal) avant d'installer le serveur de règles.
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
6. Installez la licence IBM Security Access Manager for Web, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages Security Access Manager suivants :

   ```
   pkgadd -d /chemin_package/solaris
     -a /chemin_package/solaris/pddefault -G packages
   ```

   où :

   /*chemin_package*/solaris
   Indique l'emplacement du package.

   /*chemin_package*/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et où les *packages* sont les suivants :

   PDRTE Spécifie le package Security Access Manager.

   PDMgr Spécifie le package du serveur de règles Security Access Manager.

   Avertissement : *Ne configurez pas* Security Access Manager Runtime avant que le serveur de règles ne soit installé.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Installation of package successful.
   ```
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration :

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez le composant Security Access Manager Runtime, puis le package Security Access Manager Policy Server.

       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Remarque : Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Résultats

Cette étape termine la configuration du système de serveur de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : la configuration du serveur de règles Security Access Manager crée un fichier d'autorité de certification SSL par défaut appelé `pdcacert.b64`. Le fichier de clés SSL et le certificat sont créés au moyen d'algorithmes appropriés selon le type de configuration.

Lorsque la configuration du composant Security Access Manager Policy Server Policy Server aboutit, un message similaire au suivant s'affiche :

```
La configuration de Security Access Manager Policy Server a abouti.
Le certificat d'AC du gestionnaire est codé en base 64 et sauvegardé dans le fichier
/var/PolicyDirector/keytab/pdcacert.b64
Vous devez distribuer ce fichier à toutes
les machines de votre domaine sécurisé.
Cette opération est indispensable à la réussite de la configuration.
```

Pour qu'un système d'exécution Security Access Manager s'authentifie sur les serveurs Security Access Manager, chaque système d'exécution requiert une copie de fichier. Pour obtenir ce fichier, choisissez l'une des options suivantes :

- Lors de la configuration du package Security Access Manager Runtime (à l'aide de l'utilitaire **pdconfig**), sélectionnez le téléchargement automatique du fichier `pdcacert.b64`.
- Copiez manuellement le fichier `pdcacert.b64` sur le système Security Access Manager avant de configurer le composant Security Access Manager Runtime.

Windows: Installation du serveur de règles

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.
2. Assurez-vous que votre serveur de registre est en cours d'exécution (en mode normal) avant d'installer le serveur de règles.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
3. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
4. Si vous utilisez un registre d'utilisateurs LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
5. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
6. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
7. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
8. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :
   - Security Access Manager Runtime
   - Security Access Manager Policy Server

   Avertissement : *Ne configurez pas* Security Access Manager Runtime avant que le serveur de règles ne soit installé.
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration :

       ```
       pdconfig
       ```

       La fenêtre Configuration de Security Access Manager s'affiche.
    b. Sélectionnez le package **Security Access Manager Runtime** et cliquez sur **Configurer**.
    c. Sélectionnez le package **Security Access Manager Policy Server** et cliquez sur **Configurer**.

    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

    Remarque : Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de

Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Résultats

Cette étape termine la configuration du système de serveur de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : la configuration du serveur de règles Security Access Manager crée un fichier d'autorité de certification SSL par défaut appelé `pdcacert.b64`. Le fichier de clés SSL et le certificat sont créés au moyen d'algorithmes appropriés selon le type de configuration.

Lorsque la configuration du composant Security Access Manager Policy Server Policy Server aboutit, un message similaire au suivant s'affiche :

```
La configuration de Security Access Manager Policy Server a abouti.
Le certificat d'AC du gestionnaire est codé en base 64 et sauvegardé dans le fichier
C:\PROGRA~1\Tivoli\POLICY~1\keytab\pdcacert.b64
Vous devez distribuer ce fichier à toutes
les machines de votre domaine sécurisé.
Cette opération est indispensable à la réussite de la configuration.
```

Pour qu'un système d'exécution Security Access Manager s'authentifie sur les serveurs Security Access Manager, chaque système d'exécution requiert une copie de fichier. Pour obtenir ce fichier, choisissez l'une des options suivantes :

- Lors de la configuration du package Security Access Manager Runtime (à l'aide de l'utilitaire **`pdconfig`**), sélectionnez le téléchargement automatique du fichier `pdcacert.b64`.
- Copiez manuellement le fichier `pdcacert.b64` sur le système Security Access Manager avant de configurer le composant Security Access Manager Runtime.

Installation d'un serveur de règles à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer un serveur de règles et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord fournit une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants.

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server
- IBM Security Utilities
- Licence Security Access Manager
- Security Access Manager Runtime
- Security Access Manager Policy Server

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
4. Cliquez sur **Suivant**.
5. Sélectionnez le composant **Policy Server**.
6. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
7. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que celui-ci est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
8. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 9.
9. Cliquez sur **Suivant**.
10. Répondez aux invites qui s'affichent au cours de l'installation.
11. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
12. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 13.
13. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs

signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.

14. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
15. Sélectionnez le composant
16. Cliquez sur **Configurer**.
17. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339.

    Remarque : Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html
    Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
18. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **`pdconfig`** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
19. Cliquez sur **Terminer** pour fermer le tableau de bord.

Installation du serveur de règles à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Les scripts installent les logiciels et composants Security Access Manager prérequis suivants, s'ils ne sont pas déjà installés :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server
- Security Access Manager License
- IBM Security Utilities
- Security Access Manager Runtime
- Security Access Manager Policy Server

Automatisation de l'installation d'un serveur de règles (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un serveur de règles.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i PolicyServer -d chemin_packages -a [accept|display]
   ```

   où :

   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux x86-64 :

   ```
   ./install_isam.sh -i PolicyServer -d /mnt/dvd/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l PolicyServer
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur de règles», à la page 126.

Automatisation de l'installation d'un serveur de règles (Windows)

Utilisez le fichier script pour automatiser l'installation d'un serveur de règles sous Windows.

Avant de commencer

Le script d'installation utilise les répertoires de destination par défaut suivants :

IBM Security Access Manager
`C:\Program Files\Tivoli\Policy Director`

Client Tivoli Directory Server
`C:\Program Files\IBM\ldap\V6.3`

IBM Security Utilities
`C:\Program Files\Tivoli\TivSecUtl`

Si vous souhaitez modifier les répertoires, vous devez le faire avant d'exécuter le script :

1. Copiez *tous* les fichiers `.iss` depuis le DVD ou extrayez les fichiers d'archive dans un répertoire temporaire sur votre ordinateur. Les fichiers que vous pouvez modifier sont les suivants :

   IBM Security Access Manager
   `ISAMLicense.iss`

   Client IBM Tivoli Directory Server
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Utilisez un éditeur de texte pour modifier le chemin de destination dans l'un des trois fichiers, ou dans les trois.
3. Enregistrez les fichiers.
4. Copiez le fichier de commandes de script, `install_isam.bat`, depuis le DVD ou le fichier extrait de l'archive et collez-le dans le même répertoire sur votre ordinateur.
5. Exécuter la commande de script comme décrit dans la tâche suivante.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i PolicyServer /d chemin_packages
   ```

   où :

chemin_packages correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit. Par exemple, pour installer le serveur de règles, entrez :

```
install_isam.bat /i PolicyServer /d c:\images_isam
```

où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option -l.

```
install_isam.bat /l PolicyServer
```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur de règles».

Automatisation de la configuration d'un serveur de règles

Utilisez le fichier script pour automatiser l'installation d'un serveur de règles.

Avant de commencer

- Effectuez l'installation du serveur de règles. Voir :
  - «Automatisation de l'installation d'un serveur de règles (AIX, Linux ou Solaris)», à la page 124
  - «Automatisation de l'installation d'un serveur de règles (Windows)», à la page 124
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche se trouvent par défaut aux emplacements suivants :

AIX, Linux et Solaris : `/opt/PolicyDirector/example/config`

Windows : `C:\Program Files\Tivoli\Policy Director\example\config`

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant.

AIX, Linux ou Solaris

```
configure_policysvr.options.template
```

Windows

```
configure_policysvr.options.template.cmd
```

b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

Remarque : Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html.

d. Sauvegardez le fichier.

2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Sous Windows, copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options.
   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.
   c. Revenez à ces instructions pour exécuter le script de configuration.
3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

AIX, Linux ou Solaris

```
./configure_isam.sh -f fichier_options
```

Windows

```
configure_isam.cmd -f fichier_options.cmd
```

où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

Par exemple :

AIX, Linux ou Solaris

```
./configure_isam.sh -f my_configure_policysvr.options
```

Windows

Sous Windows, entrez :

```
configure_isam.cmd -f my_configure_policysvr.options.cmd
```

Chapitre 7. Configuration du serveur d'autorisation

Security Access Manager Authorization Server permet d'accéder au service d'autorisation destiné aux applications tierces utilisant l'API d'autorisation de Security Access Manager en mode cache distant. Le serveur d'autorisation sert également de serveur de collecte d'informations de consignation et d'audit permettant de stocker les enregistrements relatifs à l'activité du serveur.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Remarque :

1. Security Access Manager ne prend pas en compte les règles de mot de passe natif de registre lors de la création des comptes de serveur lors de la configuration. Les règles natives sur les mots de passe de registre peuvent entraîner l'échec de la configuration du serveur. Avant de procéder à la configuration, désactivez les règles natives de mot de passe de registre, comme le registre par défaut et les règles de mot de passe global. Après la configuration, définissez des exceptions sur le registre pour que les nouveaux comptes de serveurs de soient pas affectés par les règles natives de mot de passe de registre. Vous pouvez maintenant activer les règles de mot de passe natives du registre.
2. Dans les deux conditions suivantes, vous devez définir `[ldap] auth-using-compare` sur `no` dans `ivacld.conf` après l'installation du serveur d'autorisations :
   - Vous installez un serveur d'autorisations sur une version mise à niveau de Security Access Manager.
   - Vous utilisez le registre Tivoli Directory Server pour installer le serveur d'autorisations.

   Le processus de mise à niveau ne met pas automatiquement à jour l'entrée ACLEntry de Security Access Manager dans Tivoli Directory Server pour permettre au serveur d'autorisations d'utiliser cette méthode d'authentification.

   Sinon, vous pouvez vérifier si l'entrée ACLEntry est mise à jour sur chaque suffixe LDAP dans lequel les comptes Security Access Manager sont stockés. L'entrée ACLEntry mise à jour est la suivante :

   ```
   ACLEntry=group:CN=IVACLD-SERVERS,CN=SECURITYGROUPS
   ,SECAUTHORITY=DEFAULT:normal:rsc
   :system:rsc:at.userPassword:wc:at.secAcctValid:rwsc:at.secPwdFailCountTime
   :rwsc:at.secPwdFailures:rwsc:at.secPwdLastChanged
   :rwsc:at.secPwdLastFailed:rwsc:at.secPwdLastUsed:rwsc:at
   .secPwdUnlockTime:rwsc:at.secPwdValid:rwsc
   ```

   Remarquez l'ajout d'`at.userPassword:wc:` à la liste d'accès.
3. Vous pouvez configurer plusieurs serveurs d'autorisation sur une seule machine.

Installation du serveur d'autorisation à l'aide de la ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer un système de serveur d'autorisations. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

© Copyright IBM Corp. 2001, 2013

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **`pkgadd`**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows
`setup.exe`

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **`pdconfig`** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **`pdjrtecfg`**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **`amwpmcfg`** pour configurer le composant Security Access Manager Web Portal Manager.

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'un serveur d'autorisations

Utilisez **`installp`** pour installer les progiciels et l'utilitaire **`pdconfig`** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
8. Installez les packages Security Access Manager.

   `installp -acgYXd` *`chemin_package`*`/usr/sys/inst.images` *`packages`*

   où *`chemin_package`* désigne le répertoire sur lequel le DVD est monté et *`packages`*, les packages suivants :

   `PD.RTE` Spécifie le package Security Access Manager Runtime.

   `PD.Acld`
   Indique le package Security Access Manager Authorization Server.
9. Démontez, le cas échéant, le DVD.
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez les packages Security Access Manager Runtime et Policy Server packages, puis le package Security Access Manager Authorization Server package de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit. `pdconfig`. Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration d'un système de serveur d'autorisations Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation d'un serveur d'autorisations

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire `/chemin_package/linux_s390`.

Remarque à l'attention de tous les autres utilisateurs de Linux :

- Si vous effectuez une installation sur un système Linux et que SELinux est activé, vous devez exécuter les commandes suivantes afin de démarrer les serveurs de règles et d'autorisations :

```
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/C/icc/osslib/libcryptoIBM080.so.0.9.8
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/N/icc/osslib/libcryptoIBM081.so.0.9.8
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamzcars.so
chcon -t textrel_shlib_t /usr/local/ibm/gsk8_64/lib64/libgsk8krsw.so
chcon -t textrel_shlib_t /opt/PolicyDirector/lib/libamcars.so
```

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Accédez au répertoire `chemin_package/distribution` où `chemin_package` désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
9. Installez les packages :

`rpm -ihv packages`

où *packages* désigne les packages suivants :

	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	PDRTE-PD-7.0.0-0.x86_64.rpm	PDRTE-PD-7.0.0-0.ppc.rpm
Package Security Access Manager Authorization Server	PDAcld-PD-7.0.0-0.x86_64.rpm	PDAcld-PD-7.0.0-0.ppc.rpm

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez les packages Security Access Manager Runtime et Policy Server packages, puis le package Security Access Manager Authorization Server package de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit. `pdconfig` Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration d'un système de serveur d'autorisations Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation d'un serveur d'autorisations

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
6. Installez la licence IBM Security Access Manager for Web, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages Security Access Manager, l'un après l'autre :

   ```
   pkgadd -d /chemin_package/solaris
      -a /package_path/solaris/pddefault -G packages
   ```

   où :

   /chemin_package/solaris
   Indique l'emplacement du package.

   /chemin_package/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et où les *packages* sont les suivants :

   PDRTE Spécifie le package Security Access Manager.

   PDAcld Désigne le package Security Access Manager Authorization Server.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Tnstallation of package successful.
   ```
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les composants Security Access Manager Runtime et Policy Server, puis le package Security Access Manager Authorization Server comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

```
pdconfig
```

Le menu d'installation de Security Access Manager s'affiche.

b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.

c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.

En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système de serveur de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation d'un serveur d'autorisations

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
6. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.

7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :
   - Security Access Manager Runtime
   - Security Access Manager Authorization Server
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les packages Security Access Manager Runtime et Policy Server packages, puis le package Security Access Manager Authorization Server package de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       La fenêtre Configuration de Security Access Manager s'affiche.
    b. Sélectionnez le package **Security Access Manager Runtime** et cliquez sur **Configurer**.
    c. Sélectionnez le package **Security Access Manager Authorization Server**, puis cliquez sur **Configurer**.

    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Cette étape termine la configuration d'un système de serveur d'autorisations Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Installation d'un serveur d'autorisations à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer un serveur d'autorisations et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Authorization Server

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
4. Cliquez sur **Suivant**.
5. Sélectionnez le composant **Serveur d'autorisations**.
6. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
7. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
8. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 9.
9. Cliquez sur **Suivant**.
10. Répondez aux invites qui s'affichent au cours de l'installation.
11. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
12. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 13.
13. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs

signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.

14. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
15. Sélectionnez le composant
16. Cliquez sur **Configurer**.
17. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
18. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant à l'aide de l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
19. Cliquez sur **Terminer** pour fermer le tableau de bord.

Installation du serveur d'autorisation à l'aide des fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un serveur d'autorisations (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un serveur d'autorisations.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i AuthServer -d chemin_packages -a [accept|display]
   ```

   où :
   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

Linux x86-64
/mnt/dvd/linux_x86

Linux on System z
/linux_s390

Solaris
/dvd/*dvd0*/solaris

- `-a [accept|display]`

  L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

Par exemple, si vous procédez à l'installation sur Linux x86-64 :

```
./install_isam.sh -i AuthServer -d /mnt/dvd/linux_x86 -a accept
```

Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

```
./install_isam.sh -l AuthServer
```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur d'autorisations», à la page 140.

Automatisation de l'installation d'un serveur d'autorisations (Windows)

Utilisez le fichier script pour automatiser l'installation d'un serveur d'autorisations sous Windows.

Avant de commencer

Le script d'installation utilise les répertoires de destination par défaut suivants :

IBM Security Access Manager
C:\Program Files\Tivoli\Policy Director

Client Tivoli Directory Server
C:\Program Files\IBM\ldap\V6.3

IBM Security Utilities
C:\Program Files\Tivoli\TivSecUtl

Si vous souhaitez modifier les répertoires, vous devez le faire avant d'exécuter le script :

1. Copiez *tous* les fichiers `.iss` depuis le DVD ou extrayez les fichiers d'archive dans un répertoire temporaire sur votre ordinateur. Les fichiers que vous pouvez modifier sont les suivants :

   IBM Security Access Manager
   ISAMLicense.iss

   Client IBM Tivoli Directory Server
   LDAPClient.iss

IBM Security Utilities
IBMSecurityUtils.iss

2. Utilisez un éditeur de texte pour modifier le chemin de destination dans l'un des trois fichiers, ou dans les trois.
3. Enregistrez les fichiers.
4. Copiez le fichier de commandes de script, `install_isam.bat`, depuis le DVD ou le fichier extrait de l'archive et collez-le dans le même répertoire sur votre ordinateur.
5. Exécuter la commande de script comme décrit dans la tâche suivante.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :
   ```
   install_isam.bat /i AuthServer /d chemin_packages
   ```
   où *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit. Par exemple, pour installer le serveur d'autorisations, entrez :
   ```
   install_isam.bat /i AuthServer /d c:\images_isam
   ```
   où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option /l.
   ```
   install_isam.bat /l AuthServer
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur d'autorisations».

Automatisation de la configuration d'un serveur d'autorisations

Utilisez le fichier script pour automatiser l'installation d'un serveur d'autorisations.

Avant de commencer

- Effectuez l'installation du serveur d'autorisations. Voir :
  - «Automatisation de l'installation d'un serveur d'autorisations (AIX, Linux ou Solaris)», à la page 138
  - «Automatisation de l'installation d'un serveur d'autorisations (Windows)», à la page 139
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche se trouvent par défaut aux emplacements suivants :

AIX, Linux et Solaris : `/opt/PolicyDirector/example/config`

Windows : `C:\Program Files\Tivoli\Policy Director\example\config`

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. Pour le serveur d'autorisations :

      AIX, Linux ou Solaris

      ```
      configure_authzsvr.options.template
      ```

      Windows

      ```
      configure_authzsvr.options.template.cmd
      ```

   b. Copiez le fichier dans un répertoire temporaire.
   c. Sauvegardez le fichier en lui attribuant un nom unique dans votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.
   d. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.
   e. Sauvegardez le fichier.
2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Sous Windows, copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options.

b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir *IBM Security Access Manager for Web: Command Reference*.

c. Revenez à ces instructions pour exécuter le script de configuration.

3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

   Par exemple :

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f my_configure_authzsvr.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_authzsvr.options.cmd
   ```

Chapitre 8. Configuration d'un système de développement

Security Access Manager Application Development Kit fournit un environnement de développement qui vous permet de coder des applications tierces pour interroger le serveur d'autorisations et prendre des décisions d'autorisation.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Configuration d'un système de développement via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer un système de développement. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **`pkgadd`**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows
`setup.exe`

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **`pdconfig`** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **`pdjrtecfg`**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **`amwpmcfg`** pour configurer le composant Security Access Manager Web Portal Manager.

© Copyright IBM Corp. 2001, 2013

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'un système de développement (ADK)

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
5. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
8. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* désigne les composants suivants :

     PD.RTE Spécifie le package Security Access Manager Runtime.

     PD.AuthADK
     Spécifie le package Security Access Manager Application Development Kit.
9. Démontez, le cas échéant, le DVD.
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Résultats

Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation d'un système de développement (ADK)

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire `/chemin_package/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Accédez au répertoire `chemin_package`*`distribution`*, où `chemin_package` désigne le point de montage de votre DVD ou l'emplacement des fichiers et *`distribution`* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
6. Si vous utilisez un registre d'utilisateur basé sur LDAP, installez le client IBM Tivoli Directory Server, le cas échéant. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
9. Installez les packages :

   ```
   rpm -ihv packages
   ```

où *packages* représente les packages suivants ci-après.

	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	PDRTE-PD-7.0.0-0.x86_64.rpm	PDRTE-PD-7.0.0-0.s390.rpm
Package Security Access Manager Application Development Kit	PDAuthADK-PD-7.0.0-0.x86_64.rpm	PDAuthADK-PD-7.0.0-0.s390.rpm

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Résultats

Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation d'un système de développement (ADK)

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
8. Installez les Security Access Manager packages (l'un après l'autre) :

   ```
   pkgadd -d /chemin_package/solaris
     -a /package_path/solaris/pddefault -G packages
   ```

   où :

   /chemin_package/solaris
   Indique l'emplacement du package.

   /chemin_package/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et *packages* désigne les fichiers suivants :

   PDRTE Spécifie le package Security Access Manager Runtime.

   PDAuthADK
   Spécifie le package Security Access Manager Application Development Kit.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Tnstallation of package successful.
   ```
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager» , à la page 364.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation d'un système de développement (ADK)

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
6. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :
   - Security Access Manager Runtime
   - Security Access Manager Application Development Kit
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager» , à la page 364.

Résultats

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Configuration d'un système de développement à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer un système de développement et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Application Development Kit

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
4. Cliquez sur **Suivant**.
5. Sélectionnez le composant **Application Development Kit**.
6. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
7. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
8. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 9.
9. Cliquez sur **Suivant**.
10. Répondez aux invites qui s'affichent au cours de l'installation.

11. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
12. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 13.
13. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
14. Cliquez sur le bouton **Configurer Application Development Kit**.
15. Sélectionnez le composant
16. Cliquez sur **Configurer**.
17. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
18. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
19. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration d'un système de développement à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un système de développement (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un système de développement.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i ADK -d chemin_packages -a [accept|display]
   ```

   où :

   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux x86-64 :

   ```
   ./install_isam.sh -i ADK -d chemin_package/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l ADK
   ```

Que faire ensuite

Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la valeur par défaut, installez votre programme de support de langue nationale. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Automatisation de l'installation d'un système de développement (Windows)

Utilisez le fichier script pour automatiser l'installation d'un système de développement sous Windows.

Avant de commencer

Le script d'installation utilise les répertoires de destination par défaut suivants :

IBM Security Access Manager
C:\Program Files\Tivoli\Policy Director

Client Tivoli Directory Server
C:\Program Files\IBM\ldap\V6.3

IBM Security Utilities
C:\Program Files\Tivoli\TivSecUtl

Si vous souhaitez modifier les répertoires, vous devez le faire avant d'exécuter le script :

1. Copiez *tous* les fichiers `.iss` depuis le DVD ou extrayez les fichiers d'archive dans un répertoire temporaire sur votre ordinateur. Les fichiers que vous pouvez modifier sont les suivants :

   IBM Security Access Manager
   `ISAMLicense.iss`

   Client IBM Tivoli Directory Server
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Utilisez un éditeur de texte pour modifier le chemin de destination dans l'un des trois fichiers, ou dans les trois.
3. Enregistrez les fichiers.
4. Copiez le fichier de commandes de script, `install_isam.bat`, depuis le DVD ou les fichiers extraits de l'archive et collez-le dans le même répertoire sur votre ordinateur.
5. Exécuter la commande de script comme décrit dans la tâche suivante.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   `install_isam.bat /i ADK /d` *`chemin_packages`*

   où :

- *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.
- Par exemple, pour installer le composant ADK, entrez :

  ```
  install_isam.bat /i ADK /d c:\images_isam
  ```

  où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option /l.

   ```
   install_isam.bat /l ADK
   ```

Que faire ensuite

Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la valeur par défaut, installez votre programme de support de langue nationale. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Chapitre 9. Configuration d'un système IBM Security Access Manager Runtime for Java

IBM Security Access Manager Runtime for Java offre un environnement fiable pour le développement et de déploiement des applications Java dans un domaine sécurisé Security Access Manager. Utilisez-le pour ajouter les services de sécurité et d'autorisation de Security Access Manager aux applications Java nouvelles ou existantes.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

IBM Security Access Manager Runtime for Java configure des fonctions de sécurité complémentaires dans l'environnement JRE spécifié.

Remarque :

1. IBM Security Access Manager Runtime for Java prend uniquement en charge les environnements JRE (Java Runtime Environment) suivants :
   - IBM Java Runtime fourni avec Security Access Manager
   - L'environnement JRE fourni avec WebSphere Application Server.
2. Si vous réinstallez et reconfigurez le serveur de règles Security Access Manager ou installez un module de correction IBM WebSphere Application Server, vous devez annuler la configuration de IBM Security Access Manager Runtime for Java puis le reconfigurer.
3. Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut "`none`", vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Configuration d'un système Security Access Manager Runtime for Java via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer le système Runtime for Java. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

© Copyright IBM Corp. 2001, 2013

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **installp**

Linux **rpm**

Solaris
pkgadd

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows
setup.exe

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **pdconfig** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **pdjrtecfg**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **amwpmcfg** pour configurer le composant Security Access Manager Web Portal Manager.

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'IBM Security Access Manager Runtime for Java

Utilisez **installp** pour installer IBM Security Access Manager Runtime for Java et l'utilitaire **pdjrtecfg** pour le configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez les packages :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images PDJ.rte
   ```

où *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers.

5. Assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server est installé. Pour obtenir des instructions sur l'installation d'IBM Java Runtime, voir la page «AIX : Installation d'IBM Java Runtime», à la page 32.
   IBM Security Access Manager Runtime for Java configure les fonctionnalités de sécurité supplémentaires dans l'environnement JRE indiqué. Seuls ces deux environnements JRE sont pris en charge.
6. Démontez, le cas échéant, le DVD.
7. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
8. Pour configurer un système IBM Security Access Manager Runtime for Java avec un type de configuration **Full**, vérifiez que le serveur de règles et le serveur de registre sont en cours d'exécution. Si le type de configuration est **standalone**, cette étape n'est pas requise.
9. Avant de configurer le composant IBM Security Access Manager Runtime for Java, assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server peut être localisé à l'aide de la variable d'environnement PATH.
10. Pour configurer le composant IBM Security Access Manager Runtime for Java, accédez au répertoire `/opt/PolicyDirector/sbin` et entrez la commande suivante :

    ```
    ./pdjrtecfg -action config -interactive
    ```

Résultats

Cette étape termine la configuration du composant Security Access Manager IBM Security Access Manager Runtime for Java. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation d'IBM Security Access Manager Runtime for Java

Utilisez le programme **rpm** pour installer le système IBM Security Access Manager Runtime for Java et l'utilitaire **pdjrtecfg** pour le configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire `/chemin_package/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
4. Accédez au répertoire *chemin_package*/*distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
5. Installez le module :

   `rpm -ihv package`

   où *package* désigne l'une des options suivantes :

	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime for Java	`PDJrte-PD-7.0.0-0.x86_64.rpm`	`PDJrte-PD-7.0.0-0.s390.rpm`

6. Assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server est installé. Pour obtenir des instructions sur l'installation d'IBM Java Runtime, voir la page «Linux : Installation d'IBM Java Runtime», à la page 33.
   IBM Security Access Manager Runtime for Java configure les fonctionnalités de sécurité supplémentaires dans l'environnement JRE indiqué. Seuls ces deux environnements JRE sont pris en charge.
7. Démontez, le cas échéant, le DVD.
8. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
9. Pour configurer IBM Security Access Manager Runtime for Java sous le type de configuration **Full**, vérifiez que le serveur de règles et le serveur de registre sont en cours d'exécution. Si le type de configuration est **standalone**, cette étape n'est pas requise.
10. Avant de configurer le composant IBM Security Access Manager Runtime for Java, assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server peut être localisé à l'aide de la variable d'environnement PATH.
11. Pour configurer le composant IBM Security Access Manager Runtime for Java, accédez au répertoire `/opt/PolicyDirector/sbin` et entrez la commande suivante : `./pdjrtecfg -action config -interactive`

Résultats

Cette étape termine la configuration du composant Security Access Manager IBM Security Access Manager Runtime for Java. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation d'IBM Security Access Manager Runtime for Java

Utilisez le programme **pkgadd.exe** pour installer le package IBM Security Access Manager Runtime for Java et l'utilitaire **pdjrtecfg** pour le configurer sous Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
3. Installez la licence IBM Security Access Manager for Web, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez les packages Security Access Manager :

   ```
   pkgadd -d /chemin_package/solaris
     -a /chemin_package/solaris/pddefault -G PDJrte
   ```

   où :

   /chemin_package/solaris
   Indique l'emplacement du package.

   /chemin_package/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.
5. Assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server est installé. Pour obtenir des instructions sur l'installation d'IBM Java Runtime, voir la page «Solaris : Installation d'IBM Java Runtime», à la page 33.

   IBM Security Access Manager Runtime for Java configure les fonctionnalités de sécurité supplémentaires dans l'environnement JRE indiqué. Seuls ces deux environnements JRE sont pris en charge.
6. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager» , à la page 364.
7. Pour configurer IBM Security Access Manager Runtime for Java sous le type de configuration **Full**, vérifiez que le serveur de règles et le serveur de registre sont en cours d'exécution. Si le type de configuration est **standalone**, cette étape n'est pas requise.

8. Avant de configurer le composant IBM Security Access Manager Runtime for Java, assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server peut être localisé à l'aide de la variable d'environnement PATH.
9. Pour configurer le composant IBM Security Access Manager Runtime for Java, accédez au répertoire `/opt/PolicyDirector/sbin` et entrez la commande suivante :

   ```
   ./pdjrtecfg -action config -interactive
   ```

Résultats

Cette étape termine la configuration du composant Security Access Manager IBM Security Access Manager Runtime for Java. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation d'IBM Security Access Manager Runtime for Java

Utilisez le programme **setup.exe** pour installer le package IBM Security Access Manager Runtime for Java et l'utilitaire **pdjrtecfg** pour le configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
3. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
4. Installez le package Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** à partir du répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et sélectionnez **IBM Security Access Manager Runtime for Java**.
5. Assurez-vous que le composant IBM Java Runtime fourni avec Security Access Manager ou l'environnement JRE fourni avec WebSphere Application Server est installé. Pour obtenir des instructions sur l'installation d'IBM Java Runtime, voir la page «Windows : Installation d'IBM Java Runtime», à la page 34.

   IBM Security Access Manager Runtime for Java configure les fonctionnalités de sécurité supplémentaires dans l'environnement JRE indiqué. Seuls ces deux environnements JRE sont pris en charge.

6. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager» , à la page 364.
7. Pour configurer IBM Security Access Manager Runtime for Java sous le type de configuration **Full**, vérifiez que le serveur de règles et le serveur de registre sont en cours d'exécution. Si le type de configuration est **standalone**, cette étape n'est pas requise.
8. Pour configurer le composant IBM Security Access Manager Runtime for Java, accédez au répertoire `c:\Program Files\Tivoli\Policy Director\sbin` et entrez la commande suivante :

   ```
   pdjrtecfg -action config -interactive
   ```

Que faire ensuite

Cette étape termine la configuration du composant Security Access Manager IBM Security Access Manager Runtime for Java. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Configuration d'un composant d'exécution pour système Java à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer le serveur de règles et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- Security Access Manager License
- Security Access Manager Runtime for Java
- IBM Java SDK

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.

b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.

3. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
4. Cliquez sur **Suivant**.
5. Sélectionnez le composant **Java Runtime**.
6. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
7. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
8. Cliquez sur **Suivant**. L'installation du premier composant débute.
9. Répondez aux invites qui s'affichent au cours de l'installation.
10. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
11. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 12.
12. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
13. Cliquez sur le bouton **Configurer Java Runtime**.
14. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
15. Effectuez l'une des actions suivantes :
    - Si l'installation a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
16. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration d'un serveur d'exécution pour serveur Java à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un système Runtime for Java (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un système Runtime for Java.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i RuntimeJava -d chemin_packages -a [accept|display]
   ```

   où :

   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux x86-64 :

   ```
   ./install_isam.sh -i RuntimeJava -d /mnt/dvd/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option -l.

   ```
   ./install_isam.sh -l RuntimeJava
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un système d'exécution pour un système Java», à la page 165.

Automatisation de l'installation d'un système Runtime for Java (Windows)

Utilisez le fichier script pour automatiser l'installation d'un composant Runtime for Java sous Windows.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i RuntimeJava /d chemin_packages
   ```

   où :

   - *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.
   - Par exemple, pour installer le composant Runtime for Java, entrez :

     ```
     install_isam.bat /i RuntimeJava /d c:\images_isam
     ```

     où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits.

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option /l.

   ```
   install_isam.bat /l RuntimeJava
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un système d'exécution pour un système Java», à la page 165.

Automatisation de la configuration d'un système d'exécution pour un système Java

Utilisez le fichier script pour automatiser l'installation d'un système d'exécution pour un système Java.

Avant de commencer

- Effectuez l'installation de Runtime for Java. Voir :
  - «Automatisation de l'installation d'un système Runtime for Java (AIX, Linux ou Solaris)», à la page 163
  - «Automatisation de l'installation d'un système Runtime for Java (Windows)», à la page 164
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche se trouvent par défaut aux emplacements suivants :

AIX, Linux et Solaris : `/opt/PolicyDirector/example/config`

Windows : `C:\Program Files\Tivoli\Policy Director\example\config`

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. Pour l'environnement d'exécution du composant Java, utilisez le modèle suivant :

      AIX, Linux ou Solaris
      `configure_javarte.options.template`

      Windows
      `configure_javarte.options.template.cmd`

   b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèle Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

   c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

   d. Sauvegardez le fichier.

2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Sous Windows, copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options.
   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir *IBM Security Access Manager for Web: Command Reference*.
   c. Revenez à ces instructions pour exécuter le script de configuration.
3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

   Par exemple :

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f my_configure_javarte.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_javarte.options.cmd
   ```

Chapitre 10. Configuration d'un système de serveur proxy de règles

Le serveur proxy de règles Security Access Manager configure un serveur proxy. Un serveur proxy agit comme un intermédiaire entre un réseau moins sécurisé et et un réseau plus fiable. Ce serveur garantit le niveau de sécurité et assure le contrôle administratif et les services de mise en cache. Il est associé et intégré à un serveur de passerelle qui sépare le réseau d'entreprise du réseau extérieur et à un serveur de pare-feu qui protège le réseau d'entreprise des accès non-autorisés. Dans un environnement Security Access Manager, le serveur proxy s'exécute en tant que serveur de règles pour un nombre spécifié d'applications d'autorisation et de fonctions d'administration, comme les commandes **pdadmin**.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Remarque : Security Access Manager ne prend pas en compte les règles de mot de passe natif de registre lors de la création des comptes de serveur lors de la configuration. Les règles natives sur les mots de passe de registre peuvent entraîner l'échec de la configuration du serveur. Lors de la configuration, désactivez les règles natives de registre, comme les règles LDAP par défaut ou les règles globales, qui peuvent affecter les nouveaux comptes de serveur.

Après avoir créé les comptes, définissez les règles de façon à ne pas affecter les comptes lorsque vous réactivez les règles.

Pour les registres LDAP, n'activez pas `pwdMustChange` lors de la configuration. Il n'est pas nécessaire d'activer `pwdMustChange` après la configuration car Security Access Manager ne met pas à jour les comptes de serveur.

Vérifiez que LDAP `pwdMaxAge` n'entraîne pas l'expiration des comptes de serveur Security Access Manager après la configuration.

Security Access Manager génère des mots de passe sûrs qui contiennent entre 8 et 20 caractères, dont au moins une lettre en minuscule, une lettre en majuscule et un chiffre. Toutefois, si les règles de mot de passe de registre sont trop restrictives, la configuration de Security Access Manager peut échouer lorsque vous définissez le mot de passe généré. Désactivez les règles de mot de passe de registre lors de la configuration.

Configuration d'un serveur proxy de règles via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer le serveur proxy de règles. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

© Copyright IBM Corp. 2001, 2013

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **installp**

Linux **rpm**

Solaris
pkgadd

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows
setup.exe

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **pdconfig** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **pdjrtecfg**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **amwpmcfg** pour configurer le composant Security Access Manager Web Portal Manager.

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'un serveur proxy de règles

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
8. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où *chemin_package* désigne le répertoire sur lequel le DVD est monté ou dans lequel se trouvent les fichiers, et où les *packages* sont :

   PD.RTE Spécifie le package Security Access Manager.

   PD.MgrProxy
   Désigne le package Security Access Manager Proxy Policy Server.
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les composants Security Access Manager Runtime et Policy Server, puis le package Security Access Manager Policy Proxy Server comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système de serveur proxy de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation d'un serveur proxy de règles

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers rpm Linux qui se trouvent dans le répertoire */chemin_package*/linux_s390.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Accédez au répertoire chemin_package/*distribution* où chemin_package désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie linux_x86 pour x86-64 ou linux_s390 pour System z.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
9. Installez les Security Access Managerpackages. rpm -ihv *packages*

   où *packages* représente les packages suivants :

	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	PDRTE-PD-7.0.0-0.x86_64.rpm	PDRTE-PD-7.0.0-0.s390.rpm
Package Security Access Manager Policy Proxy Server	PDMgrPrxy-PD-7.0.0-0.x86_64.rpm	PDMgrPrxy-PD-7.0.0-0.s390.rpm

10. Démontez, le cas échéant, le DVD.

    pdconfig

Le menu d'installation de Security Access Manager s'affiche.

11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez les composants Security Access Manager Runtime et Policy Server, puis le package Security Access Manager Policy Proxy Server comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système de serveur proxy de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation d'un serveur proxy de règles

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateur basé sur LDAP, installez le client IBM Tivoli Directory Server, le cas échéant. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages Security Access Manager, l'un après l'autre :

   ```
   pkgadd -d /chemin_package/solaris
     -a /chemin_package/solaris/pddefault -G packages
   ```

   où :

   /*chemin_package*/solaris
   Indique l'emplacement du package.

   /*chemin_package*/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et où les *packages* sont les suivants :

   PDRTE Spécifie le package Security Access Manager.

   PDMgrPrxy
   Désigne le package Security Access Manager Policy Proxy Server.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Tnstallation of package successful.
   ```

9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les composants Security Access Manager Runtime et Policy Server, puis le package Security Access Manager Policy Proxy Server comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.

       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système de serveur proxy de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation d'un serveur proxy de règles

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
6. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   `\windows\PolicyDirector\Disk Images\Disk1`

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :
   - Security Access Manager Runtime
   - Security Access Manager Policy Proxy Server
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez les composants Security Access Manager Runtime et Policy Server, puis le package Security Access Manager Policy Proxy Server comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

`pdconfig`

La fenêtre Configuration de Security Access Manager s'affiche.

b. Sélectionnez le package **Security Access Manager Runtime** et cliquez sur **Configurer**.

c. Sélectionnez le package **Security Access Manager Policy Proxy Server** et cliquez sur **Configurer**.

En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Cette étape termine la configuration du système de serveur proxy de règles Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Configuration d'un serveur proxy de règles à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer un serveur proxy de règles et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server (en fonction du registre utilisé)
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Policy Proxy Server

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.

2. Lancez le tableau de bord.

   a. Recherchez le fichier `launchpad64.exe`.

b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.

3. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
4. Cliquez sur **Suivant**.
5. Sélectionnez le composant **Policy Proxy Server**.
6. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
7. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
8. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 9.
9. Cliquez sur **Suivant**.
10. Répondez aux invites qui s'affichent au cours de l'installation.
11. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
12. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 13.
13. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
14. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
15. Sélectionnez le composant
16. Cliquez sur **Configurer**.
17. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
18. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
19. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration d'un système de serveur proxy de règles à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un système de serveur proxy de règles (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un système de serveur proxy de règles.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i ProxyServer -d chemin_packages -a [accept|display]
   ```

   où :

   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux x86-64 :

   ```
   ./install_isam.sh -i ProxyServer -d /mnt/dvd/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l ProxyServer
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur proxy de règles», à la page 178.

Automatisation de l'installation d'un serveur proxy de règles (Windows)

Utilisez le fichier script pour automatiser l'installation d'un système proxy de règles sous Windows.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i ProxyServer /d chemin_packages
   ```

   où :

   - *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.
   - Par exemple, pour installer le composant du serveur proxy de règles, entrez :

     ```
     install_isam.bat /i ProxyServer /d c:\images_isam
     ```

     où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers extraits.

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `/l`.

   ```
   install_isam.bat /l ProxyServer
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur proxy de règles», à la page 178.

Automatisation de la configuration d'un serveur proxy de règles

Utilisez le fichier script pour automatiser l'installation d'un serveur proxy de règles.

Avant de commencer

- Effectuez l'installation du serveur proxy de règles. Voir :
  - «Automatisation de l'installation d'un système de serveur proxy de règles (AIX, Linux ou Solaris)», à la page 176
  - «Automatisation de l'installation d'un serveur proxy de règles (Windows)», à la page 177
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche se trouvent par défaut aux emplacements suivants :

AIX, Linux et Solaris : `/opt/PolicyDirector/example/config`

Windows : `C:\Program Files\Tivoli\Policy Director\example\config`

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant.

      AIX, Linux ou Solaris

      ```
      configure_policysvrproxy.options.template
      ```

      Windows

      ```
      configure_policysvrproxy.options.template.cmd
      ```

   b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

   c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

   d. Sauvegardez le fichier.

2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Sous Windows, copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options.
   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.
   c. Revenez à ces instructions pour exécuter le script de configuration.
3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

   Par exemple :

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f my_configure_policysvrproxy.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_policysvrproxy.options.cmd
   ```

Chapitre 11. Configuration d'un système d'exécution

Security Access Manager Runtime contient des bibliothèques d'exécution et des fichiers de prise en charge utilisés par les applications pour accéder aux serveurs Security Access Manager. Vous devez installer et configurer le composant Access Manager Runtime sur chaque système exécutant Security Access Manager, à l'exception des systèmes Java, du composant Security Access Manager Attribute Retrieval Service, ainsi que systèmes de gestion des sessions distribuées.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Configuration d'un serveur d'exécution via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer le serveur d'exécution. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **`pkgadd`**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows
`setup.exe`

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **`pdconfig`** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **`pdjrtecfg`**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **`amwpmcfg`** pour configurer le composant Security Access Manager Web Portal Manager.

© Copyright IBM Corp. 2001, 2013

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation de Security Access Manager Runtime

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
5. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
8. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images PD.RTE
   ```

   où *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers.
9. Démontez, le cas échéant, le DVD.
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez le package Security Access Manager Runtime comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.

c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.
Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Résultats

Cette étape termine la configuration du système d'exécution Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation de Security Access Manager Runtime

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire */chemin_package*/`linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Accédez au répertoire *chemin_package*/*distribution*, où :
   - *chemin_package* est le point de montage de votre lecteur de DVD ou l'emplacement des packages
   - *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.

8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
9. Installez les packages Security Access Manager :

   ```
   rpm -ihv package
   ```

   où *package* désigne les éléments suivants :

	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	PDRTE-PD-7.0.0-0.x86_64.rpm	PDRTE-PD-7.0.0-0.s390.rpm

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez le package Security Access Manager Runtime comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.

Résultats

Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système d'exécution Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Démarrage des composants Security Access Manager sur SUSE Linux Enterprise Server 10

Après l'installation de Security Access Manager sur un système SUSE Linux Enterprise Server 10, les composants ne démarrent pas automatiquement lors du redémarrage du système. Vous devez procéder comme suit pour démarrer les composants.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Recherchez et supprimez les fichiers suivants :
   - `/etc/init.d/rc0.d/K005pd`
   - `/etc/init.d/rc3.d/S590pd`

- /etc/init.d/rc5.d/S590pd

2. Activez l'édition du fichier /opt/PolicyDirector/bin/pd_start en exécutant la commande suivante :

   ```
   chmod +w /opt/PolicyDirector/bin/pd_start
   ```

3. Ajoutez les lignes suivantes après la première ligne du fichier /opt/PolicyDirector/bin/pd_start :

   ```
   ### BEGIN INIT INFO
   # Provides:       pd
   # Required-Start: $network
   # Required-Stop:
   # Default-Start:  3 5
   # Default-Stop:
   # Description:Script to start and stop Security Access Manager.
   ### END INIT INFO
   ```

4. Exécutez la commande suivante pour activer le démarrage des serveurs Security Access Manager lors du démarrage du système :

   ```
   chkconfig pd on
   ```

   Cette commande crée les liens de script de démarrage et d'arrêt suivants :

   ```
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc3.d/K16pd -> ../pd
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc3.d/S06pd -> ../pd
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc5.d/K16pd -> ../pd
   lrwxrwxrwx 1 root root 5 Mar 15 16:11 /etc/init.d/rc5.d/S06pd -> ../pd
   ```

Résultats

Remarque :

1. Exécutez la commande suivante avant de désinstaller Security Access Manager Runtime de votre ordinateur :

   ```
   chkconfig pd off
   ```

2. Si Tivoli Directory Server est installé sur le même ordinateur que Security Access Manager, ajoutez Tivoli Directory Server à la ligne # Required-Start: du fichier /opt/PolicyDirector/bin/pd_start.

   Exécutez les commandes suivantes dans cet ordre :

   a. `chkconfig pd off`

   b. `chkconfig pd on`

   L'exécution de ces commandes garantit que les fichiers journaux de Security Access Manager ne contiennent pas de messages indiquant que le serveur LDAP a échoué puis repris.

Solaris : Installation de Security Access Manager Runtime

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
4. Installez IBM Global Security Kit (GSKit) s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
6. Installez IBM Security Access Manager License, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
8. Installez les packages Security Access Manager :

   ```
   pkgadd -d /chemin_package/solaris
          -a/chemin_package/solaris/pddefault -G PDRTE
   ```

   où :

   /chemin_package/**solaris**
   Indique l'emplacement du package.

   /chemin_package/**solaris/pddefault**
   Indique l'emplacement du script d'administration de l'installation.

   Lorsque le processus d'installation est terminée pour chaque package, le message suivant s'affiche : `Installation of package successful.`
9. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
10. Configurez le package Security Access Manager Runtime comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.

c. Sélectionnez le numéro de menu du package à configurer. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.
Cette étape termine la configuration du système d'exécution Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation de Security Access Manager Runtime

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Connectez-vous en tant qu'utilisateur disposant de droits d'administrateur.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
7. Installez la licence Security Access Manager, si elle ne l'est pas déjà. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
9. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et sélectionnez l'installation de **Security Access Manager Runtime**.

10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez le package Security Access Manager Runtime comme suit :
    a. Ouvrez une nouvelle fenêtre de ligne de commande.
    b. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       La fenêtre Configuration de Security Access Manager s'affiche.
    c. Sélectionnez le package **Security Access Manager Runtime** et cliquez sur **Configurer**.

    Vous êtes invité à entrer les options de configuration. Pour obtenir une assistance avec ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Cette étape termine la configuration du système d'exécution Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Configuration d'un serveur d'exécution à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer les composants d'un système d'exécution sur un ordinateur exécutant Windows.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.

2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser lors de l'installation, puis cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
4. Cliquez sur **Suivant**.
5. Sélectionnez le composant **Runtime**.
6. Cliquez sur **Suivant**. La liste sur la gauche affiche le composant que vous avez sélectionné. Cette liste affiche également les logiciels prérequis par ce composant qui n'ont pas encore été installés.
7. Cliquez sur **Suivant**. Le panneau d'installation du premier composant répertorié s'affiche. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
8. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 9.
9. Cliquez sur **Suivant**.
10. Répondez aux invites qui s'affichent au cours de l'installation.
11. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
12. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 13.
13. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
14. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
15. Sélectionnez un ou plusieurs composants.
16. Cliquez sur **Configurer**.
17. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
18. Effectuez l'une des actions suivantes :
    - Si l'installation a abouti, cliquez sur **Suivant**.
    - Si l'installation a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`). Apportez les corrections nécessaires ou réinstallez le serveur de règles comme indiqué par le fichier journal.

19. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration d'un serveur d'exécution à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un système d'exécution (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un système d'exécution.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   install_isam.sh -i Runtime -d chemin_packages -a [accept|display]
   ```

   où :

   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux x86-64 :

   ```
   install_isam.sh -i Runtime -d /mnt/dvd/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   install_isam.sh -l Runtime
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un système d'exécution».

Automatisation de l'installation d'un système d'exécution (Windows)

Utilisez le fichier script pour automatiser l'installation d'un système d'exécution sous Windows.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i Runtime /d chemin_packages
   ```

   où :

   - *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.
   - Par exemple, pour installer le composant d'exécution, entrez :

     ```
     install_isam.bat /i Runtime /d c:\images_isam
     ```

   où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `/l`.

   ```
   install_isam.bat /l composant
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un système d'exécution».

Automatisation de la configuration d'un système d'exécution

Utilisez le fichier script pour automatiser l'installation d'un système d'exécution.

Avant de commencer

- Effectuez l'installation du serveur d'exécution. Voir :
  - «Automatisation de l'installation d'un système d'exécution (AIX, Linux ou Solaris)», à la page 190
  - «Automatisation de l'installation d'un système d'exécution (Windows)», à la page 191
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche se trouvent par défaut aux emplacements suivants :

AIX, Linux et Solaris : `/opt/PolicyDirector/example/config`

Windows : `C:\Program Files\Tivoli\Policy Director\example\config`

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. Pour l'environnement d'exécution du composant Java, utilisez le modèle suivant :

      AIX, Linux ou Solaris
      `configure_runtime.options.template`

      Windows
      `configure_runtime.options.template.cmd`

   b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

   c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

   d. Sauvegardez le fichier.
2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Sous Windows, copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options.

b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.

c. Revenez à ces instructions pour exécuter le script de configuration.

3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   AIX, Linux ou Solaris

   ```
   configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

   Par exemple :

   AIX, Linux ou Solaris

   ```
   configure_isam.sh -f my_configure_runtime.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_runtime.options.cmd
   ```

Chapitre 12. Configuration d'un système Web Portal Manager

Security Access Manager Web Portal Manager est une interface graphique utilisateur (GUI) Web utilisée pour l'administration de Security Access Manager. L'équivalent GUI de l'interface de ligne de commande **pdadmin**, Web Portal Manager permet de gérer les utilisateurs, les groupes, les rôles, les droits d'accès, les règles et d'autres tâches Security Access Manager. L'utilisation de Web Portal Manager présente un avantage essentiel : la possibilité d'exécuter les tâches à distance, sans configuration réseau spécifique.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Avant de commencer, lisez les informations suivantes :

- Si des correctifs ou groupes de correctifs IBM WebSphere Application Server appliqués modifient le fichier `PD.jar`, vous devez également annuler, puis redéfinir la configuration de IBM Security Access Manager Runtime for Java en vue d'utiliser le fichier `PD.jar` fourni avec Security Access Manager 7.0.
- Si vous réinstallez ou reconfigurez le serveur de règles Security Access Manager, vous devez également annuler la configuration et reconfigurer le composant IBM Security Access Manager Runtime for Java, qui est un composant prérequis sur un système Web Portal Manager.
- Si vous configurez la norme de sécurité Security Access Manager sous l'option `ssl-compliance` sur Suite B, NIST SP800-131 ou FIPS, et non sur la valeur par défaut `"none"`, vous devez également, durant la configuration de Web Portal Manager, configurer WebSphere Application Server en vue d'activer la même norme de sécurité. Si les paramètres des normes de sécurité ne correspondent pas, la configuration de Web Portal Manager échoue. Pour activer le même paramètre de sécurité dans WebSphere Application Server, voir http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=%2Fcom.ibm.websphere.nd.multiplatform.doc%2Finfo%2Fae%2Fae%2Fcsec_security_standards.html

Configuration d'un système Web Portal Manager via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer Web Portal Manager. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **`installp`**

© Copyright IBM Corp. 2001, 2013

Linux **rpm**

Solaris

pkgadd

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows

setup.exe

Une fois l'installation terminée, utilisez les commandes de configuration appropriées. Par exemple, si le composant Security Access Manager Runtime est installé sur votre système, vous pouvez exécuter l'utilitaire **pdconfig** pour configurer les composants Security Access Manager. Si le composant Security Access Manager Runtime *n'est pas* installé, vous pouvez exécuter les utilitaires spécifiques aux composants, tels que **pdjrtecfg**, pour configurer IBM Security Access Manager Runtime for Java, ou bien **amwpmcfg** pour configurer le composant Security Access Manager Web Portal Manager.

Remarque : Pour plus d'informations sur ces utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'un système Web Portal Manager

Utilisez **installp** pour installer les progiciels et les utilitaires **pdjrtecfg** et **amwpmcfg** pour les configurer sous AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Assurez-vous d'avoir installé un navigateur Web pris en charge sur un système de votre domaine sécurisé. Voir les *Notes sur l'édition de IBM Security Access Manager for Web* pour obtenir une liste des systèmes d'exploitation pris en charge.
4. Assurez-vous que le module IBM Java Runtime fourni avec Security Access Manager est installé. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Java Runtime», à la page 32.
5. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.

6. Installez IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
7. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
8. Installez les packages Security Access Manager :

   `installp -acgYXd chemin_package/usr/sys/inst.images packages`

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* représente les packages suivants :

     PDJ.rte
     Spécifie le package IBM Security Access Manager Runtime for Java.

     PD.WPM Spécifie le package Security Access Manager Web Portal Manager.

   Remarque : ces packages doivent être installés sur le même système qu'IBM WebSphere Application Server.
9. Démontez, le cas échéant, le DVD.
10. Facultatif : Vous pouvez utiliser le script IBM WebSphere Application Server **setupCmdLine** pour réinitialiser les variables d'environnement, y compris l'emplacement d'IBM Java Runtime, puis configurer IBM Security Access Manager Runtime for Java et Web Portal Manager.
    a. Exécutez la commande **which java** sur la ligne de commande pour afficher les paramètres PATH par défaut utilisés. Par exemple, la commande indique que Java est actuellement exécuté depuis le répertoire `/usr/bin/java`.
    b. Pour mettre à jour la variable d'environnement *PATH* et réinitialiser la variable *JAVA_HOME*, éditez le fichier `setupCmdLine.sh` et modifiez la variable d'environnement selon vos besoins.
    c. Entrez : `/opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh`
    d. Définissez la variable *JAVA_HOME* sur la version de Java Runtime Environment qui est configurée pour IBM Security Access Manager Runtime for Java. La variable *JAVA_HOME* doit être définie sur le répertoire principal. `/opt/IBM/WebSphere/AppServer/java`
11. Pour afficher le statut et les messages du composant IBM Security Access Manager Runtime for Java dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez le composant IBM Security Access Manager Runtime for Java pour l'utilisation dans l'environnement d'exécution Java Runtime Environment qui est installé avec WebSphere. Pour ce faire, procédez comme suit.
    a. Arrêtez WebSphere Application Server et IBM HTTP Server.
    b. Accédez au répertoire `/opt/PolicyDirector/sbin` et entrez la commande suivante : `./pdjrtecfg -action config -interactive`
    c. Sélectionnez le type de configuration **Complète**.
    d. Spécifiez l'instance Java Runtime Environment qui est installée avec IBM WebSphere Application Server. Par exemple : `/usr/IBM/WebSphere/AppServer/java/jre`

e. Spécifiez le nom d'hôte, le port et le domaine du serveur de règles. Pour plus d'informations sur cet utilitaire, voir : *IBM Security Access Manager for Web Command Reference*.

13. Redémarrez WebSphere Application Server et IBM HTTP Server.
Pour redémarrer WebSphere Application Server, exécutez le script **startServer.sh**, situé dans le répertoire `/opt/IBM/WebSphere/AppServer/bin` comme suit :

```
./startServer.sh server1
```

Pour redémarrer IBM HTTP Server, entrez la commande suivante :`/opt/IBM/HTTPServer/bin/apachectl restart` **Remarque :** Si vous avez installé un serveur de registre qui n'utilise pas IBM HTTP Server *et* si vous installez Web Portal Manager sur le même système, assurez-vous que les ports du serveur Web sont différents. Pour modifier le port par défaut d'IBM HTTP Server :

a. Editez le fichier `/usr/HTTPServer/conf/httpd.conf`.

b. Changez le port par défaut `80` pour un port inutilisé, par exemple `8080`.

c. Redémarrez IBM HTTP Server.`# Port : port d'écoute du serveur autonome. Port 8080`

14. Configurez le package Security Access Manager Web Portal Manager en exécutant la commande **amwpmcfg**, située dans le répertoire `/opt/PolicyDirector/sbin/` comme suit : `./amwpmcfg -action config -interactive`.

Spécifiez les paramètres de configuration nécessaires, tels que le chemin d'installation d'IBM WebSphere Application Server, le nom d'hôte et le numéro de port du serveur de règles et l'ID et le mot de passe de l'administrateur Security Access Manager. Pour plus d'informations sur cet utilitaire et tous ses paramètres, consultez le manuel *IBM Security Access Manager for Web Command Reference*.

15. Pour accéder à l'interface Web Portal Manager, entrez l'adresse suivante dans votre navigateur Web : `http://`*`nom_hôte`*`:`*`port`*`/ibm/console`
où *nom_hôte* est le nom d'hôte du système et le port sur lequel IBM WebSphere Application Server est exécuté et *port* est le numéro de port utilisé, par exemple `9060`. Par exemple : `http://wpm14.example.com:9060/ibm/console`

Que faire ensuite

Cette étape termine la configuration d'un système Security Access Manager Web Portal Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21. Pour plus d'informations sur les tâches d'administration Web Portal Manager, voir le manuel *IBM Security Access Manager for Web : Guide d'administration*.

Notez que Security Access Manager ne fournit pas de certificat par défaut pour permettre à Web Portal Manager d'avoir une connexion sécurisée entre le navigateur et le serveur HTTP utilisé par WebSphere Application Server. Achetez un certificat d'autorité de certification et configurez-le dans l'environnement Web Portal Manager.

Linux : Installation d'un système Web Portal Manager

Utilisez **rpm** pour installer les progiciels et les utilitaires **pdjrtecfg** et **amwpmcfg** pour les configurer sous Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Assurez-vous d'avoir installé un navigateur Web pris en charge sur un système de votre domaine sécurisé. Voir les *Notes sur l'édition de IBM Security Access Manager for Web* pour obtenir une liste des systèmes d'exploitation pris en charge.
4. Assurez-vous que le module IBM Java Runtime fourni avec Security Access Manager est installé. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Java Runtime», à la page 33.

   Remarque : Si vous configurez Web Portal Manager pour des versions de Java Runtime Environment autres que l'instance Java Runtime Environment pris en charge par Security Access Manager, il se peut que la configuration échoue.
5. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
6. Installez IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
7. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
8. Accédez au répertoire *chemin_package*`/`*distribution*,

   où :

   - *chemin_package* est le point de montage de votre lecteur de DVD ou l'emplacement des fichiers.
   - *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
9. Installez les packages Security Access Manager :

   ```
   rpm -ihv package
   ```

   où *package* désigne les éléments suivants :

	Linux sur x86-64	Linux on System z
Package IBM Security Access Manager Runtime for Java	`PDJrte-PD-7.0.0-0.x86_64.rpm`	`PDJrte-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Web Portal Manager	`PDWPM-PD-7.0.0-0.x86_64.rpm`	`PDWPM-PD-7.0.0-0.s390.rpm`

   Remarque : ces packages doivent être installés sur le même système qu'IBM WebSphere Application Server.
10. Démontez, le cas échéant, le DVD.
11. Facultatif : Vous pouvez utiliser le script IBM WebSphere **`setupCmdLine`** pour réinitialiser les variables d'environnement, y compris l'emplacement de Java

Runtime Environment, avant de configurer IBM Security Access Manager Runtime for Java et Web Portal Manager.

a. Exécutez la commande **which java** sur la ligne de commande pour afficher les paramètres PATH par défaut utilisés. Par exemple, la commande indique que Java est actuellement exécuté depuis le répertoire `/usr/bin/java`.

b. Pour mettre à jour la variable d'environnement *PATH* et réinitialiser la variable *JAVA_HOME*, éditez le fichier `setupCmdLine.sh` et modifiez la variable d'environnement selon vos besoins.

c. Entrez : `. /opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh` Définissez la variable *JAVA_HOME* sur la version de Java Runtime Environment qui est configurée pour IBM Security Access Manager Runtime for Java. La variable *JAVA_HOME* doit être définie sur le répertoire principal. `/opt/WebSphere/AppServer/java`

12. Pour afficher le statut et les messages du composant IBM Security Access Manager Runtime for Java dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

13. Configurez le composant IBM Security Access Manager Runtime for Java pour l'utilisation dans l'environnement d'exécution Java Runtime Environment qui est installé avec WebSphere. Pour ce faire, procédez comme suit.

a. Arrêtez WebSphere Application Server et IBM HTTP Server.

b. Accédez au répertoire `/opt/PolicyDirector/sbin` et entrez la commande suivante :

```
./pdjrtecfg -action config -interactive
```

c. Sélectionnez le type de configuration **Complète**.

d. Spécifiez l'instance Java Runtime Environment qui est installée avec IBM WebSphere Application Server. Par exemple :

```
/opt/WebSphere/AppServer/java/jre
```

e. Spécifiez le nom d'hôte, le port et le domaine du serveur de règles. Pour plus d'informations sur cet utilitaire, voir : *IBM Security Access Manager for Web Command Reference*.

14. Redémarrez WebSphere Application Server et IBM HTTP Server.
Pour redémarrer IBM WebSphere Application Server, exécutez le script **startServer.sh**, situé dans le répertoire `/opt/IBM/WebSphere/AppServer/bin` comme suit :

```
./stopServer.sh server1 ./startServer.sh server1
```

Pour redémarrer IBM HTTP Server, entrez la commande suivante :`/opt/IBM/HTTPServer/bin/apachectl restart`

Remarque : Si vous avez installé un serveur de registre qui n'utilise pas IBM HTTP Server *et* si vous installez Web Portal Manager sur le même système, assurez-vous que les ports du serveur Web sont différents. Pour modifier le port par défaut d'IBM HTTP Server, éditez le fichier `/opt/IBMHTTPServer/conf/httpd.conf`, modifiez le port par défaut `80` sur `8080` comme indiqué, puis redémarrez IBM HTTP Server.`# Port : Port d'écoute autonome. Port 8080`

15. Configurez le package Security Access Manager Web Portal Manager en exécutant la commande **amwpmcfg**, située dans le répertoire `/opt/PolicyDirector/sbin/` comme suit :

```
./amwpmcfg -action config -interactive
```

Spécifiez les paramètres de configuration nécessaires, tels que le chemin d'installation d'IBM WebSphere Application Server, le nom d'hôte et le numéro de port du serveur de règles, ainsi que l'ID et le mot de passe de l'administrateur Security Access Manager.
Pour plus d'informations sur cet utilitaire et tous ses paramètres, consultez le manuel *IBM Security Access Manager for Web Command Reference*.

16. Pour accéder à l'interface Web Portal Manager, entrez l'adresse suivante dans votre navigateur Web : `http://nom_hôte:port/ibm/console`
où *nom_hôte* est le nom d'hôte du système et le port sur lequel IBM WebSphere Application Server est exécuté et *port* est le numéro de port utilisé, par exemple `9060`. Par exemple :
`http://wpm14.example.com:9060/ibm/console`

Que faire ensuite

Cette étape termine la configuration d'un système Security Access Manager Web Portal Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21. Pour plus d'informations sur les tâches d'administration Web Portal Manager, voir le manuel *IBM Security Access Manager for Web : Guide d'administration*.

Notez que Security Access Manager ne fournit pas de certificat par défaut pour permettre à Web Portal Manager d'avoir une connexion sécurisée entre le navigateur et le serveur HTTP utilisé par WebSphere Application Server. Achetez un certificat d'autorité de certification et configurez-le dans l'environnement Web Portal Manager.

Solaris : Installation d'un système Web Portal Manager

Utilisez **pkgadd** pour installer les progiciels et les utilitaires **pdjrtecfg** et **amwpmcfg** pour les configurer sous Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Assurez-vous d'avoir installé un navigateur Web pris en charge sur un système de votre domaine sécurisé. Voir les *Notes sur l'édition de IBM Security Access Manager for Web* pour obtenir une liste des systèmes d'exploitation pris en charge.

4. Assurez-vous que le module IBM Java Runtime fourni avec Security Access Manager est installé. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Java Runtime», à la page 33.
5. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
6. Installez IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
7. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
8. Installez les packages Security Access Manager, l'un après l'autre :

   ```
   pkgadd -d /chemin_package/solaris
     -a /chemin_package/solaris/pddefault -G packages
   ```

   où :

   /chemin_package/**solaris**
   Indique l'emplacement du package.

   /chemin_package/**solaris/pddefault**
   Indique l'emplacement du script d'administration de l'installation.

   et où les *packages* sont les suivants :

   PDJrte Spécifie le package IBM Security Access Manager Runtime for Java.

   PDWPM Spécifie le package Security Access Manager Web Portal Manager.

   Remarque : Ces packages doivent être installés sur le même système qu'IBM WebSphere Application Server.
9. Facultatif : Vous pouvez utiliser le script IBM WebSphere **setupCmdLine** pour réinitialiser les variables d'environnement, y compris l'emplacement de Java Runtime Environment, avant de configurer IBM Security Access Manager Runtime for Java et Web Portal Manager.
   a. Exécutez la commande **which java** sur la ligne de commande pour afficher les paramètres PATH par défaut utilisés. Par exemple, la commande indique que Java est actuellement exécuté depuis le répertoire `/usr/bin/java`.
   b. Pour mettre à jour la variable d'environnement *PATH* et réinitialiser la variable *JAVA_HOME*, éditez le fichier `setupCmdLine.sh` et modifiez la variable d'environnement selon vos besoins.
   c. Entrez :

      ```
      ./opt/IBM/WebSphere/AppServer/bin/setupCmdLine.sh
      ```

      Définissez la variable *JAVA_HOME* sur la version de Java Runtime Environment qui est configurée pour IBM Security Access Manager Runtime for Java. La variable *JAVA_HOME* doit être définie sur le répertoire principal.

      ```
      /opt/WebSphere/AppServer/java
      ```
10. Pour afficher le statut et les messages du composant IBM Security Access Manager Runtime for Java dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

11. Configurez le composant IBM Security Access Manager Runtime for Java pour l'utilisation dans l'environnement d'exécution Java Runtime Environment qui est installé avec WebSphere. Pour ce faire, procédez comme suit.
    a. Arrêtez WebSphere Application Server et IBM HTTP Server.
    b. Accédez au répertoire `/opt/PolicyDirector/sbin` et entrez la commande suivante :
       ```
       ./pdjrtecfg -action config -interactive
       ```
    c. Sélectionnez le type de configuration **Complète**.
    d. Spécifiez l'instance Java Runtime Environment qui est installée avec IBM WebSphere Application Server. Par exemple :
       ```
       /opt/WebSphere/AppServer/java/jre
       ```
    e. Spécifiez le nom d'hôte, le port et le domaine du serveur de règles.
       Pour plus d'informations sur cet utilitaire, voir : *IBM Security Access Manager for Web Command Reference*.
12. Redémarrez WebSphere Application Server et IBM HTTP Server. Pour redémarrer WebSphere Application Server, exécutez le script **`startServer.sh`**, situé dans le répertoire `/opt/WebSphere/AppServer/bin` comme suit :
    ```
    ./stopServer.sh server1
    ./startServer.sh server1
    ```
    Pour redémarrer IBM HTTP Server, entrez la commande suivante :
    ```
    /opt/IBMHTTPServer/bin/apachectl restart
    ```

    Remarque : Si vous avez installé un serveur de registre qui n'utilise pas IBM HTTP Server *et* si vous installez Web Portal Manager sur le même système, assurez-vous que les ports du serveur Web sont différents. Pour modifier le port par défaut d'IBM HTTP Server, éditez le fichier `/opt/IBMHTTPServer/conf/httpd.conf`, modifiez le port par défaut `80` sur `8080` comme indiqué, et redémarrez IBM HTTP Server.
    ```
    # Port : port d'écoute du serveur autonome.
    Port 8080
    ```
13. Configurez le package Security Access Manager Web Portal Manager :
    ```
    ./amwpmcfg -action config -interactive
    ```

    Spécifiez les paramètres de configuration nécessaires, tels que le chemin d'installation d'IBM WebSphere Application Server, le nom d'hôte et le numéro de port du serveur de règles, ainsi que l'ID et le mot de passe de l'administrateur Security Access Manager.

    Pour plus d'informations sur cet utilitaire et tous ses paramètres, consultez le manuel *IBM Security Access Manager for Web Command Reference*.
14. Pour accéder à l'interface Web Portal Manager, entrez l'adresse suivante dans votre navigateur Web :
    `http://`*`nom_hôte`*`:`*`port`*`/ibm/console`

    où *nom_hôte* est le nom d'hôte du système et le port sur lequel IBM WebSphere Application Server est exécuté et *port* est le numéro de port utilisé, par exemple `9060`. Par exemple :
    ```
    http://wpm14.example.com:9060/ibm/console
    ```

Que faire ensuite

Cette étape termine la configuration d'un système Security Access Manager Web Portal Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21

21. Pour plus d'informations sur les tâches d'administration Web Portal Manager, voir le manuel *IBM Security Access Manager for Web : Guide d'administration*.

Notez que Security Access Manager ne fournit pas de certificat par défaut pour permettre à Web Portal Manager d'avoir une connexion sécurisée entre le navigateur et le serveur HTTP utilisé par WebSphere Application Server. Achetez un certificat d'autorité de certification et configurez-le dans l'environnement Web Portal Manager.

Windows : Installation d'un système Web Portal Manager

Utilisez **setup.exe** pour installer les progiciels et les utilitaires **pdjrtecfg** et **amwpmcfg** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
3. Assurez-vous d'avoir installé un navigateur Web pris en charge sur un système de votre domaine sécurisé. Voir les *Notes sur l'édition de IBM Security Access Manager for Web* pour obtenir une liste des systèmes d'exploitation pris en charge.
4. Assurez-vous que le module IBM Java Runtime fourni avec Security Access Manager est installé. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Java Runtime», à la page 34.
5. Installez IBM WebSphere Application Server. Voir «Installation de WebSphere Application Server», à la page 47.
6. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
7. Installez la licence Security Access Manager, si elle ne l'est pas déjà. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
8. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :

   - IBM Security Access Manager Runtime for Java
   - Security Access Manager Web Portal Manager

   Remarque : ces packages doivent être installés sur le même système qu'IBM WebSphere Application Server.
9. Facultatif : Vous pouvez utiliser le script IBM WebSphere **setupCmdLine** pour réinitialiser les variables d'environnement, y compris l'emplacement de Java

Runtime Environment, avant de configurer IBM Security Access Manager Runtime for Java et Web Portal Manager.

a. Exécutez la commande **which java** sur la ligne de commande pour afficher les paramètres PATH par défaut utilisés. Par exemple, la commande indique que Java est exécuté depuis le répertoire `C:\Program Files\IBM\WebSphere\AppServer\java`.

b. Pour mettre à jour la variable d'environnement *PATH* et réinitialiser la variable *JAVA_HOME*, éditez le fichier `setupCmdLine.bat` et modifiez la variable d'environnement selon vos besoins.

c. Entrez :

```
C:\Program Files\IBM\WebSphere\AppServer\bin\setupCmdLine.bat
```

Définissez la variable *JAVA_HOME* sur la version de Java Runtime Environment qui est configurée pour IBM Security Access Manager Runtime for Java. La variable *JAVA_HOME* doit être définie sur le répertoire principal.

```
C:\Program Files\IBM\WebSphere\AppServer\java
```

10. Pour afficher le statut et les messages du composant IBM Security Access Manager Runtime for Java dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

11. Configurez le composant IBM Security Access Manager Runtime for Java pour l'utilisation dans l'environnement d'exécution Java Runtime Environment qui est installé avec WebSphere. Pour ce faire, procédez comme suit.

a. Arrêtez WebSphere Application Server et IBM HTTP Server.

b. Accédez au répertoire *rép_install*`\sbin` (par exemple, `C:\Program Files\Tivoli\Policy Director\sbin`) et entrez la commande suivante :

```
pdjrtecfg -action config -interactive
```

c. Sélectionnez le type de configuration **Complète**.

d. Cliquez sur **Suivant**. Pour obtenir des descriptions des options de configuration, cliquez sur **Aide**.

e. Spécifiez l'instance Java Runtime Environment qui est installée avec IBM WebSphere Application Server. Par exemple :

```
C:\Program Files\IBM\WebSphere\AppServer\java\jre
```

f. Cliquez sur **Suivant** pour continuer.

g. Spécifiez le nom d'hôte, le port et le domaine du serveur de règles.

h. Cliquez sur **OK** pour démarrer la configuration.

i. Lorsque la configuration a abouti, cliquez sur **OK** pour fermer l'utilitaire de configuration.
Pour plus d'informations sur cet utilitaire, voir : *IBM Security Access Manager for Web Command Reference*.

12. Redémarrez IBM WebSphere Application Server et IBM HTTP Server. Sélectionnez par exemple **Démarrer → Paramètres → Panneau de configuration → Outils d'administration** et cliquez deux fois sur l'icône **Services** pour redémarrer ces serveurs.

Remarque : Si vous avez installé un serveur de registre qui n'utilise pas IBM HTTP Server *et* si vous installez Web Portal Manager sur le même système, assurez-vous que les ports du serveur Web sont différents. Pour modifier le port par défaut d'IBM HTTP Server, éditez le fichier `C:\Program`

Files\IBMHTTPServer\conf\httpd.conf, modifiez le port par défaut 80 sur 8080 comme indiqué, et redémarrez IBM HTTP Server.

```
# Port : port d'écoute du serveur autonome. Port 8080
```

13. Configurez le package Security Access Manager Web Portal Manager. Pour ce faire, procédez comme suit.
    a. Accédez au répertoire *rép_install*\sbin (par exemple, C:\Program Files\Tivoli\Policy Director\sbin) et entrez la commande suivante :

       ```
       amwpmcfg -action config -interactive
       ```

       Spécifiez les paramètres de configuration nécessaires, tels que le chemin d'installation d'IBM WebSphere Application Server, le nom d'hôte et le numéro de port du serveur de règles et l'ID et le mot de passe de l'administrateur Security Access Manager.
       Pour plus d'informations sur cet utilitaire et tous ses paramètres, consultez le manuel *IBM Security Access Manager for Web Command Reference*.
    b. Lorsque la configuration a abouti, cliquez sur **OK** pour fermer l'utilitaire de configuration.
14. Pour accéder à l'interface Web Portal Manager, entrez l'adresse suivante dans votre navigateur Web : http://*nom_hôte*:*port*/ibm/console
    où *nom_hôte* est le nom d'hôte du système et le port sur lequel IBM WebSphere Application Server est exécuté et *port* est le numéro de port utilisé, par exemple 9060. Par exemple :

    ```
    http://wpm14.example.com:9060/ibm/console
    ```

Que faire ensuite

Cette étape termine la configuration d'un système Security Access Manager Web Portal Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21. Pour plus d'informations sur les tâches d'administration Web Portal Manager, voir le manuel *IBM Security Access Manager for Web : Guide d'administration*.

Notez que Security Access Manager ne fournit pas de certificat par défaut pour permettre à Web Portal Manager d'avoir une connexion sécurisée entre le navigateur et le serveur HTTP utilisé par WebSphere Application Server. Achetez un certificat d'autorité de certification et configurez-le dans l'environnement Web Portal Manager.

Configuration d'un système Web Portal Manager à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer le composant Web Portal Manager et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51
- Web Portal Manager requiert une version prise en charge d'IBM WebSphere Application Server. Utilisez la version fournie avec IBM Security Access Manager

ou consultez les informations de version sur le centre de documentation d'IBM Security Access Manager pour obtenir une liste des versions prises en charge.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM WebSphere Application Server, y compris IBM Installation Manager (si ce composant n'est pas déjà installé)
- Security Access Manager License
- Security Access Manager Runtime for Java
- Security Access Manager Web Portal Manager

Si une version prise en charge de WebSphere Application Server est déjà installée, vous pouvez ignorer son installation au cours de cette procédure et passer à l'installation des composants restants.

Avertissement : Si WebSphere Application Server est déjà installé, vérifiez que Java est spécifié dans la variable d'environnement PATH avant d'exécuter le tableau de bord. Par exemple, tapez :

```
set Path=c:\Program Files\IBM\Java60\jre\bin;%Path%
```

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage. Vous avez besoin des fichiers correspondant aux produits suivants :
   - WebSphere Application Server
   - Installation Manager
   - IBM Security Access Manager

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers images ne comporte aucun espace.
2. Lancez le tableau de bord sur les fichiers IBM Security Access Manager.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser durant l'installation.
4. Cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
5. Cliquez sur **Suivant**.
6. Sélectionnez le composant **Web Portal Manager**.
7. Cliquez sur **Suivant**. La liste affichée sur la partie gauche indique le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis par ce composant qui ne sont pas encore installés.
8. Installez WebSphere Application Server ou, si WebSphere Application Server est déjà installé, cliquez sur **Suivant**. Pour installer WebSphere Application Server :
   a. Cliquez sur **Installer les composants WebSphere Application Server** pour installer WebSphere Application Server.
   b. Sélectionnez le chemin d'accès à l'image d'IBM Installation Manager.

Remarque : Le chemin d'accès à l'image Installation Manager est limitée à une longueur de 172 caractères.

c. Cliquez sur **OK**.

Remarque : Une fois l'installation d'Installation Manager effectuée, un délai de 30 secondes s'écoule avant l'ouverture et le lancement de l'installation de WebSphere Application Server.

d. Dans la console d'Installation Manager, cliquez sur **Installer** pour débuter l'installation de WebSphere Application Server.

e. Cliquez sur **Fichier** > **Préférences**.

f. Sélectionnez **Référentiels**.

g. Cliquez sur **Ajouter le référentiel**.

h. Sélectionnez l'emplacement du fichier `repository.config` dans l'image de WebSphere Application Server.

i. Cliquez sur **OK**.

j. Cliquez sur **Installer**. Procédez à l'installation en suivant les invites. Les sélections par défaut fournies par le programme d'installation d'IBM WebSphere Application Server sont suffisantes pour IBM Security Access Manager. À la fin de l'installation, une liste des packages installés et une invite de démarrage du programme s'affiche.

   - Si l'installation réussit, une liste des packages installés et une invite de lancement de l'outil de gestion de profil s'affiche. Passez à l'étape 8k.
   - Si l'installation d'Installation Manager ou de WebSphere Application Server échoue, ou si une erreur s'affiche, consultez les fichiers journaux et les actions que ceux-ci indiquent. Les fichiers se trouvent par défaut sous `%USERPROFILE%`, par exemple `C:\Users\Administrator\`.

     Journaux d'Installation Manager

     `IMInstall.log`

     `IMInstallLog.xml`

     Journal d'installation de WebSphere Application Server

     `LaunchIMforWAS.log`

k. Sélectionnez le composant **Profile Management Tool** pour créer un profil.

l. Cliquez sur **Terminer**. La boîte à outils de personnalisation WebSphere Customization Toolbox s'ouvre dans l'outil de gestion de profils.

m. Dans l'outil de gestion de profils, cliquez sur **Créer**.

n. Démarrez l'outil Premiers pas et cliquez sur **Démarrer le serveur**. Le message `Ouvrir pour e-business` s'affiche.

o. Fermez les fenêtres suivantes :

   - Premiers pas
   - WebSphere Customization Toolbox

p. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis.

q. Localisez le groupe de correctifs dans le référentiel Web de WebSphere Application Server ou téléchargez le module et installez-le à partir d'un référentiel local.

   - Pour effectuer l'installation à partir du référentiel Web :
     1) Cliquez sur **Mettre à jour** dans la fenêtre IBM Installation Manager.

2) Sélectionnez **IBM WebSphere Application Server Network Deployment V8.0**.
3) Cliquez sur **Suivant**. Poursuivez l'installation.

- Pour effectuer l'installation à partir d'un référentiel local :
  1) Localisez le groupe de correctifs sur la page de support de WebSphere Application Server : http://www.ibm.com/support/docview.wss?uid=swg27004980
  2) Téléchargez le groupe de correctifs dans un référentiel local.
  3) cliquez sur **Mettre à jour**.
  4) Sélectionnez **IBM WebSphere Application Server Network Deployment V8.0**.
  5) Cliquez sur **Suivant**. Poursuivez l'installation. Utilisez le fichier Readme joint fourni sur la page de support de WebSphere Application Server pour obtenir une assistance.

r. Démarrez IBM WebSphere Application Server.
1) Cliquez sur **Démarrer** > **Administrative Tools (Outils d'administration)** > **Services**.
2) Sélectionnez l'instance IBM WebSphere Application Server qui a été ajoutée.
3) Cliquez avec le bouton droit sur le service, puis cliquez sur **Démarrer**.

s. Fermez la fenêtre d'IBM Installation Manager.

t. Revenez à la fenêtre du tableau de bord.

9. Cliquez sur **Suivant**. Le panneau d'installation du composant suivant s'affiche. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
10. Cliquez sur **Suivant**. L'installation du premier composant débute.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
13. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 14.
14. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
15. Cliquez sur **Configurer Java Runtime**.
16. Spécifiez l'emplacement de WebSphere Application Server Java. Par exemple, spécifiez :

    ```
    C:\Program Files (x86)\IBM\WebSphere\AppServer\java\jre
    ```
17. Cliquez sur **Suivant**.
18. Cliquez sur **Configurer Web Portal Manager**.

19. Terminez la configuration. Pour obtenir de l'aide, voir «Security Access Manager Web Portal Manager», à la page 356. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
20. Cliquez sur **OK**.
21. Effectuez l'une des actions suivantes :
    - Si l'installation et la configuration ont abouti, cliquez sur **Suivant**.
    - Si l'installation ou la configuration a échoué, ou si une erreur est affichée, consultez les journaux situés à l'emplacement par défaut `%USERPROFILE%` :

      Installation Manager
      `IMInstall.log`

      `IMInstallLog.xml`

      Installation de WebSphere Application Server
      `LaunchIMforWAS.log`

      Configuration de WebSphere Application Server
      `ConfigJRTEforWAS.log`

      Configuration de Web Portal Manager
      `ConfigAMWPM.log`

      Apportez les corrections nécessaires ou réinstallez le composant comme indiqué par le fichier journal. Voir le manuel *IBM Security Access Manager for Web Troubleshooting Guide* pour obtenir une assistance.
22. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration de Web Portal Manager à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Web Portal Manager nécessite WebSphere Application Server. Si WebSphere Application Server n'est pas déjà installé, installez-le et configurez-le d'après l'une des méthodes suivantes :

- «Installation de WebSphere Application Server», à la page 47 pour l'installation et la configuration manuelles.
- «Configuration de WebSphere Application Server à l'aide de fichiers scripts» pour automatiser l'installation et la configuration.

Configuration de WebSphere Application Server à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation de WebSphere Application Server (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation de WebSphere Application Server sous AIX, Linux ou Solaris.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*). WebSphere Application Server est un produit prérequis pour les composants suivants :

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager est requis pour l'installation de WebSphere Application Server.

Procédure

1. Obtenez les fichiers d'installation de WebSphere Application Server et du référentiel du produit à partir de l'un des emplacements suivants :
   - Les supports produit de WebSphere Application Server fournis avec les DVD de Security Access Manager.
   - Le site Passport Advantage.
2. Copiez les fichiers de WebSphere Application Server sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
3. Extrayez dans un répertoire tous les fichiers de WebSphere Application Server à partir de leurs fichiers compressés.
4. Obtenez Installation Manager à partir de l'un des emplacements suivants :
   - Le site Passport Advantage.
   - Le site Web de téléchargement d'IBM Installation Manager :

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copiez les fichiers d'Installation Manager sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
6. Extrayez les fichiers Installation Manager dans son propre répertoire.
7. Copiez le fichier `install_was.sh` depuis le répertoire `scripts` situé sur le support du produit Security Access Manager et collez-le dans un emplacement temporaire sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
8. Copiez le fichier `WASInstall_*.xml` correspondant à votre plateforme depuis le répertoire `scripts` du Support de produit Security Access Manager vers le même emplacement temporaire que celui dans lequel vous avez copié le fichier `install_was.sh`. Les fichiers de réponses sont les suivants :

   Linux x86-64
   `WASInstall_linux_x86.xml`

   Linux s390
   `WASInstall_linux_s390x.xml`

   AIX `WASInstall_aix_ppc.xml`

   Solaris
   `WASInstall_solaris_sparc.xml`

9. Ouvrez la copie du fichier `install_was.sh` dans un éditeur de texte.
10. Modifier le chemin d'Installation Manager dans le fichier `install_was.sh` de manière à spécifier l'emplacement où se trouvent les images d'Installation Manager. Par exemple, modifiez la ligne suivante :

    ```
    INSTALL_MGR_DIR=/images/InstallationManager
    ```

11. Modifiez la variable `WAS_RESPONSE_FILE` de manière à spécifier le nom du fichier de réponses à utiliser lors de l'exécution du script. Utilisez le nom du fichier de réponses approprié pour votre plateforme :

    Linux x86-64
    `WASInstall_linux_x86.xml`

    Linux s390
    `WASInstall_linux_s390x.xml`

    AIX `WASInstall_aix_ppc.xml`

    Solaris
    `WASInstall_solaris_sparc.xml`

    Par exemple, sous Linux for x86-64, spécifiez :

    ```
    WAS_RESPONSE_FILE=./WASInstall_linux_x86.xml
    ```

12. Sauvegardez le fichier et fermez-le.
13. Ouvrez la copie du fichier `WASInstall_*.xml` dans un éditeur de texte.
14. Modifiez le chemin d'accès à l'emplacement du référentiel dans le fichier `WASInstall_*.xml` où se trouvent les images de WebSphere Application Server. Par exemple, modifiez la ligne suivante :

    ```
    <repository location='/images/WebSphere'/>
    ```

15. Facultatif : Modifiez l'emplacement dans lequel WebSphere Application Server est installé par le script. Les emplacements d'installation par défaut sont les suivants :

    Linux ou Solaris
    `/opt/IBM/WebSphere/AppServer`

    AIX `/usr/IBM/WebSphere/AppServer`

    Pour changer l'emplacement, modifiez les lignes suivantes dans le fichier `WASInstall_*.xml` :

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
       installLocation='/opt/IBM/WebSphere/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
    ```

16. Enregistrez le fichier de réponses.
17. Exécutez le fichier script.

    ```
    install_was.sh
    ```

Avertissement : Si vous spécifiez le nom d'un fichier de référentiel incorrect à l'étape 14, à la page 212, une erreur s'affiche. Répéter les instructions de modification indiquées à l'étape 14, à la page 212 de manière à corriger le nom de fichier du référentiel. Puis, supprimez le référentiel incorrect dans Installation Manager avant d'exécuter le script :

a. Sur une ligne de commande, placez-vous dans le répertoire d'installation d'Installation Manager :

   ```
   /opt/IBM/InstallationManager/eclipse
   ```

b. Exécutez `IBMIM`.

c. Supprimez le référentiel incorrect.

d. Exécutez à nouveau le script.

18. Une fois l'installation de WebSphere Application Server terminée, créez un profil d'Application Server en exécutant la commande WebSphere Application Server **manageprofiles**.

    Par exemple, tapez :

    ```
    /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -create -templatePath
    /opt/IBM/WebSphere/AppServer/profileTemplates/default
    ```

    Pour plus de détails sur la commande **manageprofiles**, consultez le centre de documentation de WebSphere Application Server :

    http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

19. Démarrez le serveur d'applications.

    Par exemple, tapez :

    ```
    /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/startServer.sh server1
    ```

20. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis.

    a. Localisez le groupe de correctifs sur la page de support de WebSphere Application Server. http://www.ibm.com/support/docview.wss?uid=swg27004980

    b. Téléchargez le groupe de correctifs et utilisez les instructions contenues dans le fichier Readme joint pour l'installer.

Que faire ensuite

Passez à l'étape «Automatisation de l'installation d'un système Web Portal Manager (AIX, Linux ou Solaris)», à la page 215.

Automatisation de l'installation de WebSphere Application Server (Windows)

Utilisez le fichier script pour automatiser l'installation de WebSphere Application Server sous Windows.

Avant de commencer

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_was.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*). WebSphere Application Server est un produit prérequis pour les composants suivants:

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager est requis pour l'installation de WebSphere Application Server.

Procédure

1. Obtenez les fichiers d'installation de WebSphere Application Server et du référentiel du produit à partir de l'un des emplacements suivants :
   - Les supports produit de WebSphere Application Server fournis avec les DVD de Security Access Manager.
   - Le site Passport Advantage.
2. Copiez les fichiers de WebSphere Application Server sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
3. Extrayez dans un répertoire tous les fichiers de WebSphere Application Server à partir de leurs fichiers compressés.
4. Obtenez Installation Manager à partir de l'un des emplacements suivants :
   - Le site Passport Advantage.
   - Le site Web de téléchargement d'IBM Installation Manager :

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copiez les fichiers d'Installation Manager sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
6. Extrayez les fichiers Installation Manager dans son propre répertoire.
7. Copiez le fichier `install_was.bat` depuis le répertoire `scripts` situé sur le support du produit Security Access Manager et collez-le dans un emplacement temporaire sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
8. Copiez le fichier `WASInstall.xml` depuis le répertoire `scripts` du support de produit Security Access Manager vers le même emplacement temporaire que celui dans lequel vous avez copié le fichier `install_was.bat`.
9. Ouvrez la copie du fichier `install_was.bat` dans un éditeur de texte.
10. Modifier le chemin d'Installation Manager dans le fichier `install_was.bat` de manière à spécifier l'emplacement où se trouvent les images d'Installation Manager. Par exemple, modifiez la ligne suivante :

    ```
    set INSTALL_MGR_DIR=C:\images\Installation Manager
    ```
11. Sauvegardez le fichier et fermez-le.
12. Ouvrez la copie du fichier `WASInstall.xml` dans un éditeur de texte.
13. Modifiez le chemin d'accès à l'emplacement du référentiel dans le fichier `WASInstall.xml` où se trouvent les images de WebSphere Application Server. Par exemple, modifiez la ligne suivante :

    ```
    <repository location='C:\images\WebSphere'/>
    ```
14. Facultatif : Modifiez l'emplacement dans lequel WebSphere Application Server est installé par le script. Par exemple, modifiez les lignes suivantes.

```
<profile id='IBM WebSphere Application Server Network Deployment V8.0'
  installLocation='C:\Program Files\IBM\WebSphere\AppServer'/>
<data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
```

15. Exécutez le fichier script.

    ```
    install_was.bat
    ```

16. Une fois l'installation de WebSphere Application Server terminée, créez un profil d'Application Server en exécutant la commande WebSphere Application Server **manageprofiles**.

    Par exemple, tapez :

    ```
    C:\Program Files\IBM\WebSphere\AppServer\bin\manageprofiles.bat -create
      -templatePath "C:\Program Files\IBM\WebSphere\AppServer\
       profileTemplates\default"
    ```

    Pour plus de détails sur la commande **manageprofiles**, consultez le centre de documentation de WebSphere Application Server :

    http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

17. Démarrez le serveur d'applications.

    Par exemple, tapez :

    ```
    C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\
    startServer.bat server1
    ```

18. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis.
    a. Localisez le groupe de correctifs sur la page de support de WebSphere Application Server. http://www.ibm.com/support/docview.wss?uid=swg27004980
    b. Téléchargez le groupe de correctifs et utilisez les instructions contenues dans le fichier Readme joint pour l'installer.

Que faire ensuite

Passez à l'étape «Automatisation de l'installation d'un composant Web Portal Manager (Windows)», à la page 216.

Automatisation de l'installation d'un système Web Portal Manager (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un système Web Portal Manager.

Avant de commencer

Assurez-vous que WebSphere Application Server est installé et configuré.

- «Installation de WebSphere Application Server», à la page 47 pour l'installation et la configuration manuelles.
- «Configuration de WebSphere Application Server à l'aide de fichiers scripts», à la page 210 pour automatiser l'installation et la configuration.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i WPM -d chemin_packages -a [accept|display]
   ```

   où :

   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX
     point_montage_dvd`/usr/sys/inst.images`

     Linux x86-64
     `/mnt/dvd/linux_x86`

     Linux on System z
     `/linux_s390`

     Solaris
     `/dvd/`*dvd0*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux x86-64 :

   ```
   ./install_isam.sh -i WPM -d /mnt/dvd/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l WPM
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration de Web Portal Manager», à la page 217.

Automatisation de l'installation d'un composant Web Portal Manager (Windows)

Utilisez le fichier script pour automatiser l'installation d'un système Portal Manager sous Windows.

Avant de commencer

Web Portal Manager nécessite WebSphere Application Server. Avant de commencer cette tâche, installez et configurez WebSphere Application Server, si ce n'est déjà fait :

- «Installation de WebSphere Application Server», à la page 47 pour l'installation et la configuration manuelles.

- «Automatisation de l'installation de WebSphere Application Server (Windows)», à la page 213 pour automatiser l'installation et la configuration.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i WPM /d chemin_packages
   ```

   où :

   - `WPM` est le nom du composant Web Portal Manager.
   - *`chemin_packages`* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.

   Par exemple, pour installer le composant Web Portal Manager, entrez :

   ```
   install_isam.bat /i WPM /d c:\images_isam
   ```

   où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option /l.

   ```
   install_isam.bat /l WPM
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration de Web Portal Manager».

Automatisation de la configuration de Web Portal Manager

Utilisez le fichier script pour automatiser la configuration de Web Portal Manager.

Avant de commencer

- Effectuez l'installation de Web Portal Manager. Voir :
  - «Automatisation de l'installation d'un système Web Portal Manager (AIX, Linux ou Solaris)», à la page 215
  - «Automatisation de l'installation d'un composant Web Portal Manager (Windows)», à la page 216

- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche se trouvent par défaut aux emplacements suivants :

AIX, Linux et Solaris : `/opt/PolicyDirector/example/config`

Windows : `C:\Program Files\Tivoli\Policy Director\example\config`

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. Pour l'environnement d'exécution du composant Java, utilisez le modèle suivant :

      AIX, Linux ou Solaris
      `configure_wpm.options.template`

      Windows
      `configure_wpm.options.template.cmd`

   b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèle Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

   c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

   d. Sauvegardez le fichier.
2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Sous Windows, copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options.

   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.

   c. Revenez à ces instructions pour exécuter le script de configuration.
3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

AIX, Linux ou Solaris

```
./configure_isam.sh -f fichier_options
```

Windows

```
configure_isam.cmd -f fichier_options.cmd
```

où *fichier_options* et *fichier_options*.cmd sont les fichiers texte contenant les options de configuration.

Par exemple :

AIX, Linux ou Solaris

```
./configure_isam.sh -f my_configure_wpm.options
```

Windows

```
configure_isam.cmd -f my_configure_wpm.options.cmd
```

Configuration de la sécurité de WebSphere Application Server

Vous devez configurer les paramètres de sécurité de WebSphere Application Server pour que la connexion unique de Web Portal Manager fonctionne correctement.

Procédure

1. Pour démarrer IBM Integrated Solutions Console, sélectionnez **Démarrer** > **Tous les programmes** > **IBM WebSphere Application Server <version>** > **Profils** > **<nom profil>** > **Console d'administration**.
2. Cliquez sur **Sécurité** > **Sécuriser l'administration, les applications et l'infrastructure**.
3. Développez **Sécurité Web** à droite pour afficher :
   - **Paramètres généraux**
   - **Connexion unique (SSO)**
   - **Relation de confiance**
4. Cliquez sur **Paramètres généraux**.
5. Assurez-vous que la case**Authentifier uniquement quand l'URI est protégé** est cochée.
6. Cochez la case **Utiliser les données d'authentification disponibles quand un URI protégé est accédé**.
7. Cliquez sur **OK**.

Partie 4. Installation du composant système de sécurité Web

© Copyright IBM Corp. 2001, 2013

Chapitre 13. Configuration de Security Access Manager Attribute Retrieval Service

Le composant Security Access Manager Attribute Retrieval Service est utilisé en association avec la fonction d'informations de décision d'autorisation (ADI) de WebSEAL. Ce service offre des services de communication et de traduction de format entre la bibliothèque de service d'autorisation WebSEAL et le fournisseur externe d'informations de décision d'autorisation. Pour plus d'informations, voir *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Configurez ce système en suivant les instructions correspondant à votre système d'exploitation.

Configuration d'Attribute Retrieval Service via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer le composant Attribute Retrieval Service.

Remarque : Si vous souhaitez créer et déployer un service d'extraction d'attributs personnalisé, un fichier WSDL est inclus dans la configuration de Security Access Manager Application Development Kit pour vous permettre de démarrer. Le fichier est accessible via le chemin d'accès suivant :

AIX, Linux ou Solaris

```
/opt/PolicyDirector/example/amwebars/azn_ent_amwebars.wsdl
```

Windows

```
C:\Program Files\Tivoli\Policy Director\example\amwebars\
azn_ent_amwebars.wsdl
```

Voir le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide* pour plus d'informations sur l'utilisation du fichier WSDL.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX `installp`

Linux `rpm`

Solaris

`pkgadd`

Remarque : Si vous effectuez une installation sur Solaris version 10 ou supérieure, spécifiez l'option **-G**. L'option **-G** garantit que les modules sont ajoutés dans la zone actuelle uniquement. Lorsque l'option **-G** est utilisée dans la zone globale, le module est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non-globale, les modules sont ajoutés à la zone non-globale uniquement.

© Copyright IBM Corp. 2001, 2013

Windows

```
setup.exe
```

Une fois l'installation terminée, utilisez les commandes de configuration appropriées.

Remarque : Pour plus d'informations sur ces utilitaires, voir *IBM Security Access Manager for Web Command Reference*.

AIX : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande

Utilisez **Installp** pour installer les progiciels sous AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Assurez-vous que la version de IBM Java Runtime fournie avec Security Access Manager est installée. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Java Runtime», à la page 32.
3. Installez IBM Security Access Manager License, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
5. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
6. Installez le package suivant :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images PDWeb.ARS
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - PDWeb.ARS est le module Security Access Manager Attribute Retrieval

   Remarque : ce package doit être installé sur le même système qu'IBM WebSphere Application Server.
7. Démontez, le cas échéant, le DVD.
8. Pour déployer Security Access Manager Attribute Retrieval Service dans l'environnement IBM WebSphere Application Server, exécutez le fichier Deploy.sh et suivez les instructions du fichier Readme.deploy, situé dans le répertoire /opt/pdwebars/.
9. Pour configurer WebSEAL en vue d'utiliser Security Access Manager Attribute Retrieval Service, voir le manuel *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

Que faire ensuite

Cette étape termine la configuration du composant Security Access Manager Attribute Retrieval Service. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Pour plus d'informations sur Security Access Manager Attribute Retrieval Service, consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Linux : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande

Utilisez **rpm** pour installer les progiciels sous Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Assurez-vous que le module IBM Java Runtime fourni avec Security Access Manager est installé. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Java Runtime», à la page 33.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
5. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
6. Accédez au répertoire *chemin_package/distribution*,

   où :

   - `chemin_package` est le point de montage de votre lecteur de DVD ou l'emplacement des fichiers
   - *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
7. Installez le package suivant :`rpm -ihv package`
   où *package* désigne les éléments suivants :

	Security Access Manager Attribute Retrieval Service
Linux sur x86-64	`PDWebARS-PD-7.0.0-0.x86_64.rpm`
Linux on System z	`PDWebARS-PD-7.0.0-0.s390x.rpm`

   Remarque : ce package doit être installé sur le même système qu'IBMWebSphere Application Server.
8. Démontez, le cas échéant, le DVD.

9. Pour déployer Security Access Manager Attribute Retrieval Service dans l'environnement WebSphere Application Server, exécutez le fichier `Deploy.sh` et suivez les instructions du fichier `Readme.deploy`, situé dans le répertoire `/opt/pdwebars/`.
10. Pour configurer WebSEAL en vue d'utiliser Security Access Manager Attribute Retrieval Service, voir le manuel *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

Que faire ensuite

Cette étape termine la configuration de Security Manager Attribute Retrieval Service. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Pour plus d'informations sur Security Access Manager Attribute Retrieval Service, consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Solaris : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande

Utilisez **pkgadd** pour installer les progiciels sous Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Assurez-vous que la version de IBM Java Runtime fournie avec Security Access Manager est installée. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Java Runtime», à la page 33.

   Remarque : Si vous configurez le composant Security Access Manager Attribute Retrieval Service pour des versions de Java Runtime Environments autres que l'instance Java Runtime Environment prise en charge par Security Access Manager, il se peut que la configuration échoue.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
5. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

6. Installez les packages suivants, l'un après l'autre :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault
   -G PDWebARS
   ```

   où :

   -d /*chemin_package*/solaris
   Indique l'emplacement du package.

   -a /*chemin_package*/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et `PDWebARS` spécifie le package Security Access Manager Attribute Retrieval Service.

   Remarque : Ce package doit être installé sur le même système qu'IBM WebSphere Application Server.

7. Pour déployer Security Access Manager Attribute Retrieval Service dans l'environnement WebSphere Application Server, exécutez le fichier `Deploy.sh` et suivez les instructions du fichier `Readme.deploy`, situé dans le répertoire `/opt/pdwebars/`.
8. Pour configurer WebSEAL en vue d'utiliser Security Access Manager Attribute Retrieval Service, voir le manuel *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

Que faire ensuite

Cette étape termine la configuration du composant Security Access Manager Attribute Retrieval Service. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Pour plus d'informations sur Security Access Manager Attribute Retrieval Service, consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Windows : Installation de Security Access Manager Attribute Retrieval Service via une ligne de commande

Utilisez **setup.exe** pour installer les progiciels sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de droits d'administrateur.
2. Assurez-vous que la version de IBM Java Runtime fournie avec Security Access Manager est installée. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Java Runtime», à la page 34.

3. Installez IBM WebSphere Application Server. Voir «Installation de WebSphere Application Server», à la page 47.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez le package Security Access Manager Attribute Retrieval Service. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   `\windows\PolicyDirector\Disk Images\Disk1`

   Suivez les instructions en ligne pour exécuter l'installation.**Remarque :** ce package doit être installé sur le même système qu'IBM WebSphere Application Server.
6. Pour déployer Security Access Manager Attribute Retrieval Service dans l'environnement WebSphere Application Server, exécutez le fichier `Deploy.bat` et suivez les instructions du fichier `Readme.deploy`, situé dans le répertoire `C:\Program Files\Tivoi\PDWebARS\`.
7. Pour configurer WebSEAL en vue d'utiliser Security Access Manager Attribute Retrieval Service, voir le manuel *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

Que faire ensuite

Cette étape termine la configuration de Security Manager Attribute Retrieval Service. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Pour plus d'informations sur Security Access Manager Attribute Retrieval Service, consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Chapitre 14. Configuration du composant Plug-in for Web Servers

Le composant Security Access Manager Plug-in for Web Servers gère la sécurité des ressources Web en faisant office de passerelle entre vos clients et l'espace Web sécurisé.

Le plug-in met en oeuvre les stratégies de sécurité qui protègent votre espace d'objet Web. Ce plug-in offre des solutions de connexion unique, prend en charge des serveurs Web s'exécutant comme des hôtes virtuels et intègre des ressources de serveur d'applications Web dans la stratégie de sécurité. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web: Plug-in for Web Servers Administration Guide*.

Le composant IBM Security Access Manager Plug-in for Web Servers prend en charge les serveurs et plateformes suivants :

- Apache Web Server on AIX, Linux sur x86-64, Linux sur System z et Solaris
- IBM HTTP Server sur AIX, Linux sur x86-64, Linux sur System z et Solaris.
- Internet Information Services sous Windows

Voir les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de connaissances de support pour obtenir plus d'informations sur les versions des serveurs Web prises en charge. Pour plus d'informations sur les composants de sécurité Web, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

Exécutez les instructions qui s'appliquent à votre serveur Web.

Exigences de préinstallation

Avant d'installer et de configurer le composant Security Access Manager Plug-in for Web Servers, vérifiez que les exigences suivantes sont remplies. Ces exigences sont applicables, quelle que soit la méthode que vous prévoyez d'utiliser.

- Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.
- Effectuez les tâches préalables appropriées décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27
- Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Vérifiez que vous avez consulté les informations de version les plus récentes, notamment les exigences concernant les systèmes d'exploitation, les exigences d'espace disque, les incidents connus et les limitations. Voir *IBM Security Access Manager for Web - Notes sur l'édition* ou les notes techniques dans la base de connaissances du support.
- Vérifiez qu'un serveur de registre Security Access Manager et que le serveur de règles sont configurés dans votre domaine sécurisé. Pour obtenir des instructions sur la configuration de ces systèmes, voir Partie 3, «Installation du composant système de base», à la page 107.
- Vérifiez que le cache direct/proxy inverse est désactivé dans votre environnement de serveur Web.

© Copyright IBM Corp. 2001, 2013

- Vérifiez que votre serveur Web est installé et configuré sur ce système. En outre, votre serveur Web doit être configuré pour SSL et/ou les certificats client si vous souhaitez activer la communication SSL.
- Vérifiez que Security Access Manager prend en charge la plateforme sur laquelle vous exécutez votre serveur Web.
- Assurez-vous que IIS 6 Management Compatibility est installé sur les systèmes Windows avec Internet Information Services (IIS). Le composant Security Access Manager Plug-in for Internet Information Services requiert le composant IIS 6 Management Compatibility.
- Vérifiez que la prise en charge des objets partagés dynamiquement (DSO) est activée sur le serveur Web Apache car le composant Security Access Manager Plug-in for Apache Web Server requiert les DSO.
- Pour Solaris, vérifiez que les modules Apache ont été précédemment compilés à l'aide de GNU Compiler Collection (GCC) version 3.2 ou ultérieure pour éviter la survenue d'erreurs.
- Un ID groupe valide est obligatoire afin d'accéder au serveur Web Apache à l'aide du plug-in. La valeur de l'ID groupe par défaut de -1 dans le fichier de configuration d'Apache est non valide. Avant de configurer la composant Security Access Manager Plug-in for Web Servers, vous devez changer la valeur de l'ID groupe sur un groupe de systèmes connu dans l'entrée Group configuration du fichier de configuration d'Apache. Ce changement est uniquement obligatoire lors de l'exécution d'Apache sous Red Hat Enterprise Linux 5.

Installation du plug-in pour Apache Web Server via une ligne de commande

Utilisez ces instructions pour installer le plug-in pour Apache Web Server.

Pourquoi et quand exécuter cette tâche

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

AIX : composant Plug-in for Apache Web Server

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez également les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
9. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* représente les packages suivants :

     PD.RTE Spécifie le package Security Access Manager Runtime.

     PD.WebRTE
     Spécifie le package Security Access Manager Web Security Runtime.

     PD.WPI Spécifie le package Security Access Manager Plug-in for Web Servers.

     PD.WPIApache
     Spécifie le package Security Access Manager Plug-in for Apache Web Server.

   Remarque : Ces packages doivent être installés sur le même système que le serveur Web Apache.
10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Définissez la variable d'environnement AIX Extended Shared Memory Support (EXTSHM) sur **ON** avant de configurer le composant Access Manager Plug-in for Apache Web Server et avant de démarrer le plug-in pour le serveur proxy Apache Web Server ou le serveur Web Apache.
13. Configurez Security Access Manager Runtime, puis le package Security Access Manager Plug-in for Web Servers de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.

c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

   Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.

14. Redémarrez le serveur Web.
15. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante :

    ```
    pdwebpi_start start
    ```

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour Apache Server sous AIX. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux on x86-64 : composant Plug-in for Apache Web Server

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux x86-64.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Assurez-vous de consulter les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus, ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Placez-vous dans le répertoire *chemin_package*`/linux_x86`, où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement de votre fichier.
6. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
7. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
8. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.

9. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
10. Installez les packages Security Access Manager :

    ```
    rpm -ihv packages
    ```

    où *packages* représente les packages suivants :

Package	Linux sur x86-64
Package Security Access Manager Runtime	PDRTE-PD-7.0.0-0.x86_64.rpm
Package Security Access Manager Web Security Runtime	PDWebRTE-PD-7.0.0-0.x86_64.rpm
Package Security Access Manager Plug-in for Web Servers	PDWPI-PD-7.0.0-0.x86_64.rpm
Package Security Access Manager Plug-in for Apache Web Server	PDWPI-Apache-7.0.0-0.x86_64.rpm

    Remarque : ces packages doivent être installés sur le même système que le serveur Web Apache.
11. Démontez, le cas échéant, le DVD.
12. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
13. Configurez Security Access Manager Runtime, puis le package Security Access Manager Plug-in for Web Servers de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

       Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.
14. Redémarrez le serveur Web.
15. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante :

    ```
    démarrer pdwebpi_start
    ```

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour Apache Server sous Linux x86-64. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux on System z : composant Plug-in for Apache Web Server

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux on System z. Pour installer le plug-in du serveur Web pour Apache Web Server (version 31 bits uniquement) pour Linux on System z, procédez comme suit.

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire `/chemin_package/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
9. Installez les packages Security Access Manager :

   `rpm -ihv packages`

   où *packages* désigne les packages suivants :

Package	Linux on System z
Package Security Access Manager Runtime	`PDRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Web Security Runtime	`PDWebRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Plug-in for Web Servers	`PDWPI-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Plug-in for Apache Web Server	`PDWPI-Apache-7.0.0-0.s390.rpm`

Remarque : ces packages doivent être installés sur le même système que le serveur Web Apache.

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit. `pdconfig` Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez Security Access Manager Runtime, puis le module Security Access Manager Plug-in for Web Servers.
    d. En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339. Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.
13. Redémarrez le serveur Web.
14. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
15. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante : `pdwebpi_start start`.

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour Apache Web Server pour Linux on System z. Pour configurer un autre systèmes Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : composant Plug-in for Apache Web Server

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.

3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
7. Installez IBM Security Access Manager License, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
9. Installez les Security Access Manager packages (l'un après l'autre) :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault
   -G packages
   ```

   où :

   /*chemin_package*/solaris
   Indique l'emplacement du package.

   /*chemin_package*/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et *packages* désigne les fichiers suivants :

   PDRTE Spécifie le package Security Access Manager Runtime.

   PDWebRTE
   Spécifie le package Security Access Manager Web Security Runtime.

   PDWPI Spécifie le package Security Access Manager Plug-in for Web Servers.

   PDWPIapa
   Spécifie le package Security Access Manager Plug-in for Apache Web Server.

   Remarque : Ces packages doivent être installés sur le même système que le serveur Web Apache.
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Définissez les paramètres de noyau de mémoire partagée sur des valeurs supérieures aux valeurs par défaut. Ajoutez les lignes suivantes au fichier `/etc/system` pour augmenter les paramètres sur des valeurs admissibles :

    ```
    set shmsys:shminfo_shmmax=0x2000000
    set shmsys:shminfo_shmseg=256
    set shmsys:shminfo_shmmni=256
    ```

    Redémarrez votre système pour que ces changements prennent effet.

12. Configurez les packages Security Access Manager comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez Security Access Manager Runtime, puis le module Security Access Manager Plug-in for Web Servers.

       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

       Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.
13. Redémarrez le serveur Web.
14. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
15. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante :

    ```
    démarrer pdwebpi_start
    ```

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour Apache Web Server sous Solaris. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Installation du plug-in pour IBM HTTP Server via une ligne de commande

Utilisez ces instructions pour installer le plug-in pour IBM HTTP Server.

Pourquoi et quand exécuter cette tâche

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

AIX : plug-in for IBM HTTP Server

Utilisez **`installp`** pour installer les progiciels et l'utilitaire **`pdconfig`** pour les configurer sur AIX.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.

3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
9. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* représente les packages suivants :

     PD.RTE Spécifie le package Security Access Manager Runtime.

     PDWeb.RTE
     Spécifie le package Security Access Manager Web Security Runtime.

     PD.WPI Spécifie le package Security Access Manager Plug-in for Web Servers.

     PD.WPIIHS
     Indique le package Security Access Manager Plug-in for IBM HTTP Server.

   Remarque : Ces packages doivent être installés sur le même système qu'IBM HTTP Server.
10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Définissez la variable d'environnement EXTSHM sur **ON** avant de configurer le composant Security Access Manager Plug-in for IBM HTTP Server et avant de démarrer le plug-in pour le serveur proxy IBM HTTP Server ou pour IBM HTTP Server.
13. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.

b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez Security Access Manager Runtime, puis le module Security Access Manager Plug-in for Web Servers.

   En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

   Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.

14. Redémarrez le serveur Web.
15. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante :

    ```
    démarrer pdwebpi_start
    ```

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour IBM HTTP Server sous AIX. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : plug-in for IBM HTTP Server

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire */chemin_package*`/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Accédez au répertoire *chemin_package*`/distribution`,

   où :

- *chemin_package* est le point de montage de votre lecteur de DVD ou l'emplacement des fichiers
- *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z

6. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
7. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
8. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
9. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
10. Installez les packages Security Access Manager :

    ```
    rpm -ihv packages
    ```

    où *packages* représente les packages suivants :

Package	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Web Security Runtime	`PDWebRTE-PD-7.0.0-0.x86_64.rpm`	`PDWebRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Plug-in for Web Servers	`PDWPI-PD-7.0.0-0.x86_64.rpm`	`PDWPI-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Plug-in for IBM HTTP Web Server	`PDWPI-IHS-7.0.0-0.x86_64.rpm`	`PDWPI-IHS-7.0.0-0.s390.rpm`

    Remarque : ces packages doivent être installés sur le même système que l'instance IBM HTTP Server.
11. Démontez, le cas échéant, le DVD.
12. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
13. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez Security Access Manager Runtime, puis le module Security Access Manager Plug-in for Web Servers.
       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.

14. Redémarrez le serveur Web.
15. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
16. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante :

    ```
    pdwebpi_start start
    ```

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour IBM HTTP Server sous Linux. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Plug-in for IBM HTTP Server

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.

8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
9. Installez les Security Access Manager packages (l'un après l'autre) :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault
   -G packages
   ```

   où :

   /chemin_package/**solaris**
   Indique l'emplacement du package.

   /chemin_package/**solaris/pddefault**
   Indique l'emplacement du script d'administration de l'installation.

   et où les *packages* sont les suivants :

   PDRTE Spécifie le package Security Access Manager Runtime.

   PDWebRTE
   Spécifie le package Security Access Manager Web Security Runtime.

   PDWPI Spécifie le package Security Access Manager Plug-in for Web Servers.

   PDWPIihs
   Indique le package Security Access Manager Plug-in for IBM HTTP Server.

   Remarque : Ces packages doivent être installés sur le même système qu'IBM HTTP Server.
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Définissez les paramètres de noyau de mémoire partagée sur des valeurs supérieures aux valeurs par défaut. Ajoutez les lignes suivantes au fichier `/etc/system` pour augmenter les paramètres sur des valeurs admissibles :

    ```
    set shmsys:shminfo_shmmax=0x2000000
    set shmsys:shminfo_shmseg=256
    set shmsys:shminfo_shmmni=256
    ```

    Redémarrez votre système pour que ces changements prennent effet.
12. Configurez les packages Security Access Manager de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre. Configurez Security Access Manager Runtime, puis le module Security Access Manager Plug-in for Web Servers.

       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

       Lorsqu'un message s'affiche indiquant que le package a été configuré, sélectionnez deux fois de suite l'option **x** pour fermer l'utilitaire de configuration.

13. Redémarrez le serveur Web.
14. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.
15. Pour démarrer le processus du plug-in, accédez au répertoire `/opt/pdwebpi/bin` et saisissez la commande suivante :

    ```
    pdwebpi_start start
    ```

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour IBM HTTP Server sous Solaris. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Installation du plug-in pour Internet Information Services via une ligne de commande

Le plug-in de serveur Web pour Internet Information Services est disponible sur les plateformes Windows prises en charge uniquement. Utilisez le programme **`setup.exe`** pour installer les progiciels et l'utilitaire **`pdconfig`** pour les configurer.

Avant de commencer

Vérifiez que IIS 6 Management Compatibility est installé sur le système Windows. Le composant Security Access Manager Plug-in for Internet Information Services requiert le composant IIS 6 Management Compatibility.

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs qui dispose de droits d'administration.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que vous respectez les exigences indiquées à la section «Exigences de préinstallation», à la page 229.
4. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
5. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
6. Installez la licence Security Access Manager, si elle ne l'est pas déjà. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
7. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
8. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.

9. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** à partir du répertoire suivant :
   `\windows\PolicyDirector\Disk Images\Disk1`

   La boîte de dialogue Choose Setup Language s'affiche.
10. Sélectionnez la langue que vous souhaitez utiliser pour l'installation.
11. Cliquez sur **OK**. La fenêtre Bienvenue s'affiche.
12. Cliquez sur **Suivant** pour continuer.
13. Lisez le contrat de licence, puis cliquez sur **Oui** si vous acceptez les termes.
14. Sélectionnez les modules suivants :
    - Security Access Manager Runtime
    - Access Manager Web Security Runtime
    - Access Manager Plug-in for Web Servers
15. Cliquez sur **Suivant**.
16. Acceptez le répertoire de destination par défaut ou cliquez sur **Parcourir** pour sélectionner un chemin d'accès à un autre répertoire sur le système local. Si le répertoire n'existe pas, vous devez confirmer que vous souhaitez qu'il soit créé ou indiquer un répertoire qui existe.
17. Pour démarrer la copie des fichiers vers le répertoire de destination, cliquez sur **Suivant**.
18. Cliquez sur **Terminer** pour quitter le programme de configuration.
19. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
20. Vous devez configurer IIS de sorte à utiliser les identités par défaut lors de l'exécution de Security Access Manager Plug-in for Microsoft Internet Information Services (IIS) sur un contrôleur de domaine Windows. En raison d'une limitation du système d'exploitation Windows, l'utilisation d'une identité autre que les identités utilisateur par défaut génère une erreur `503 Service Unavailable`.
21. Configurez Security Access Manager Runtime, puis le package Security Access Manager Plug-in for Web Servers. Pour cela, cliquez sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.

    Pour obtenir une assistance avec les options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

    Remarque : Vous pouvez également configurer les composants Security Access Manager à l'aide de l'utilitaire **pdconfig** à partir d'une ligne de commande.
22. Redémarrez le serveur Web.
23. Personnalisez le fichier `pdwebpi.conf` pour votre serveur Web spécifique. Pour plus d'informations, consultez le manuel *IBM Security Access Manager for Web Plug-in for Web Servers Administration Guide*.

Résultats

Cette étape termine la configuration du plug-in de serveur Web Security Access Manager pour IIS Web Server sous Windows. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : Avant d'installer un autre composant, ouvrez une nouvelle fenêtre de ligne de commande.

Configuration d'un plug-in pour Internet Information Services à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer le plug-in Internet Information Services sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Vérifiez que IIS 6 Management Compatibility est installé sur le système Windows. Le composant Security Access Manager Plug-in for Internet Information Services requiert le composant IIS 6 Management Compatibility.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- Client d'IBM Tivoli Directory Server
- IBM Security Utilities
- Licence Security Access Manager
- Security Access Manager Runtime
- Security Access Manager Web Security Runtime
- Security Access Manager Plug-in for Web Servers

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser durant l'installation.

4. Cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
5. Cliquez sur **Suivant**.
6. Sélectionnez le composant **Plug-in for Web Servers**.
7. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
8. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
9. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 10.
10. Cliquez sur **Suivant**.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
13. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 14.
14. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
15. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
16. Sélectionnez le composant
17. Cliquez sur **Configurer**.
18. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque la configuration est terminée, un message de réussite ou d'échec s'affiche.
19. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
20. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration du module plug-in de serveur Web à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques automatisent les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation du plug-in de serveur Apache ou IBM HTTP Server

Utilisez le fichier script pour automatiser l'installation du plug-in de serveur Apache ou IBM HTTP Server.

Avant de commencer

Assurez-vous que votre système répond aux conditions préalables à l'installation, y compris l'installation du serveur Web. Voir «Exigences de préinstallation», à la page 229.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i composant -d chemin_packages -a [accept|display]
   ```

   où :

   - *composant* est le nom du composant que vous souhaitez installer. Les noms de composant des plug-ins sont les suivants :
     - `PluginApache`
     - `PluginIBMHTTP`
   - *chemin_packages* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *point_montage_dvd*`/usr/sys/inst.images`

     Linux `/`*point_montage_dvd*`/linux_x86`

     Solaris
     `/`*point_montage_dvd*`/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.
   - Par exemple, pour installer le plug-in pour Apache Server sur Linux :

     ```
     ./install_isam.sh -i PluginApache -d /mnt/dvd/linux_x86 -a accept
     ```

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option -l.

   ```
   ./install_isam.sh -l composant
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration du plug-in de serveur Apache ou IBM HTTP Server».

Automatisation de la configuration du plug-in de serveur Apache ou IBM HTTP Server

Utilisez le fichier script pour automatiser la configuration du plug-in de serveur Apache ou IBM HTTP Server.

Avant de commencer

Effectuez l'installation des composants de sécurité Web. Voir «Automatisation de l'installation du plug-in de serveur Apache ou IBM HTTP Server», à la page 247.

Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Les fichiers scripts et de modèle qui sont utilisés pour cette tâche sont installés dans le répertoire `/opt/PolicyDirector/example/config`.

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. L'emplacement du modèle Plug-in for Web Servers est le suivant :

      ```
      /opt/PolicyDirector/example/config/configure_webpi.options.template
      ```

   b. Copiez le fichier dans un répertoire temporaire.
   c. Sauvegardez le fichier en lui attribuant un nom unique dans votre environnement.
   d. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.
   e. Sauvegardez le fichier.
2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.

b. Revenez à ces instructions pour exécuter le script de configuration.

3. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   ```
   ./configure_isam.sh -f fichier_options
   ```

   où *fichier_options* est le fichier texte qui contient les options de configuration. Par exemple :

   ```
   ./configurep_isam.sh -f my_configure_webpi.options
   ```

Automatisation de l'installation du plug-in Internet Information Services

Utilisez le fichier script pour automatiser l'installation du plug-in Internet Information Services.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i PluginIIS /d chemin_packages
   ```

   où :

   - `PluginIIS` est le nom du composant.
   - *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.
   - Par exemple, tapez :

     ```
     install_isam.bat /i PluginIIS /d chemin_packages
     ```

   Le script installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option /l.

   ```
   install_isam.bat /l PluginIIS
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration du plug-in Internet Information Service».

Automatisation de la configuration du plug-in Internet Information Service

Utilisez le fichier script pour automatiser la configuration du plug-in Internet Information Service.

Avant de commencer

Effectuez l'installation du plug-in Internet Information Service. Voir «Automatisation de l'installation du plug-in Internet Information Services», à la page 249.

Vérifiez que IIS 6 Management Compatibility est installé sur le système Windows. Le composant Security Access Manager Plug-in for Internet Information Services requiert le composant IIS 6 Management Compatibility.

Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Ouvrez une nouvelle fenêtre. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Pour utiliser le script :

1. Créez un fichier d'options contenant les paramètres de configuration pour votre environnement spécifique.
2. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. L'emplacement du modèle Plug-in for Web Servers est le suivant :

      ```
      C:\Program Files\Tivoli\PDWebPI\etc\
      configure_webpi.options.template.cmd
      ```

   b. Copiez le fichier dans un répertoire temporaire.
   c. Sauvegardez le fichier en lui attribuant un nom unique dans votre environnement.
   d. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.
   e. Sauvegardez le fichier.
2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Copiez le fichier `configure_isam.conf` depuis le répertoire `C:\Program Files\Tivoli\Policy Director\example\config` vers le même répertoire que celui où vous avez copié les fichiers d'options.
   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.
   c. Revenez à ces instructions pour exécuter le script de configuration.

3. Copiez le fichier `configure_isam.cmd` depuis le répertoire `C:\Program Files\Tivoli\Policy Director\example\config` vers le même répertoire que celui où vous avez enregistré le fichier modèle.
4. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   ```
   configure_isam.cmd -f fichier_options
   ```

   où *fichier_options* est le fichier texte qui contient les options de configuration. Par exemple :

   ```
   configure_isam.cmd -f my_configure_webpi.options.cmd
   ```

Chapitre 15. Configuration d'un système de développement de sécurité Web

Le composant Security Access Manager Web Security ADK contient les API de développement pour les composants de sécurité Web. Les API comprennent le service d'authentification interdomaine Security Access Manager (CDAS), l'infrastructure de mappage interdomaine Security Access Manager (CDMF), ainsi que le module de contrôle de mot de passe Security Access Manager.

Pour plus d'informations sur ce système de sécurité Web, voir le manuel *IBM Security Access Manager for Web : WebSEAL Administration Guide*.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Configuration d'un système de développement de sécurité Web via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer un système de développement de sécurité Web. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX `installp`

Linux `rpm`

Solaris
`pkgadd`

Remarque : Si vous effectuez une installation sur Solaris version 10 ou supérieure, spécifiez l'option **-G**. L'option **-G** garantit que les modules sont ajoutés dans la zone actuelle uniquement. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non-globale, les modules sont ajoutés à la zone non-globale uniquement.

Windows
`setup.exe`

Après avoir terminé l'installation, utilisez les commandes de configuration appropriées.

© Copyright IBM Corp. 2001, 2013

Remarque : Pour plus d'informations sur ces utilitaires, voir *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
9. Installez les Security Access Managerpackages :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* représente les packages suivants :

     PD.RTE Spécifie le package Security Access Manager Runtime.

     PDWeb.RTE
     Spécifie le package Security Access Manager Web Security Runtime.

PD.AuthADK
Spécifie le package Security Access Manager Application Development Kit.

PDWeb.ADK
Spécifie le package Security Access Manager Web Services Application Development Kit.

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez le package Security Access Manager Runtime comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.
       ```
       pdconfig
       ```
       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Suivez les étapes de l'utilitaire `pdconfig` afin de terminer la configuration.

Résultats

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire `/`*`chemin_package`*`/linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).

4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
6. Accédez au répertoire *chemin_package/distribution* où *chemin_package* désigne le point de montage de votre DVD ou l'emplacement des fichiers et *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z.
7. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
8. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
9. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
10. Installez les packages Security Access Manager :

    `rpm -ihv` *packages*
    où *packages* désigne les packages suivants :

Package	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Web Security Runtime	`PDWebRTE-PD-7.0.0-0.x86_64.rpm`	`PDWebRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Application Development Kit	`PDAuthADK-PD-7.0.0-0.x86_64.rpm`	`PDAuthADK-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Web Services Application Development Kit	`PDWebADK-PD-7.0.0-0.x86_64.rpm`	`PDWebADK-PD-7.0.0-0.s390.rpm`

11. Démontez, le cas échéant, le DVD.
12. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
13. Configurez le package comme suit :
    a. Démarrez l'utilitaire de configuration comme suit. `pdconfig`
       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Suivez les étapes de l'utilitaire `pdconfig` afin de terminer la configuration.

Que faire ensuite

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access

Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
9. Installez les packages Security Access Manager :

   ```
   pkgadd -d /chemin_package/solaris
     -a /chemin_package/solaris/pddefault -G packages
   ```

   où :

   - `-d /chemin_package/solaris` spécifie l'emplacement du package
   - *packages* représente les packages suivants :

PDRTE Spécifie le package Security Access Manager Runtime.

PDWebRTE
Spécifie le package Security Access Manager Web Security Runtime.

PDADK Spécifie le package Security Access Manager Application Development Kit.

PDWebADK
Spécifie le package Security Access Manager Web Services Application Development Kit.

Lorsqu'un message vous demande `Do you want to install these as setuid/setgid?`, saisissez **Y** et appuyez sur Entrée. Lorsque vous êtes invité à continuer, saisissez **Y** et appuyez sur Entrée.

Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

`Installation of packages successful.`

10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez le package Security Access Manager Runtime comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       `pdconfig`

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Suivez les étapes de l'utilitaire `pdconfig` afin de terminer la configuration.

Résultats

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation d'un système de développement de sécurité Web (WebADK) via une ligne de commande

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de privilèges du groupe Administrateurs.

2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
7. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
9. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :
   - Security Access Manager Runtime
   - Access Manager Web Security Runtime
   - Security Access Manager Application Development Kit
   - Access Manager Web Security Application Development Kit
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez le package Security Access Manager Runtime comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       La fenêtre Configuration de Security Access Manager s'affiche.
    b. Sélectionnez le package **Security Access Manager Runtime** et cliquez sur **Configurer**.

    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Cette étape termine la configuration d'un système de développement (ADK) Security Access Manager. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : Avant d'installer un autre composant, ouvrez une nouvelle fenêtre de ligne de commande.

Configuration d'un système de développement de sécurité Web à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer le système de développement de sécurité Web et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Si vous envisagez d'utiliser un registre d'utilisateurs autre qu'IBM Tivoli Directory Server, passez à l'étape Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- Client IBM Tivoli Directory Server
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Web Security Runtime
- Security Access Manager Application Development Kit
- Security Access Manager Web Security Application Development Kit

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser durant l'installation.
4. Cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
5. Cliquez sur **Suivant**.

6. Sélectionnez le composant **Web Security Application Development Kit**.
7. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
8. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
9. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 10.
10. Cliquez sur **Suivant**.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
13. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 14.
14. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
15. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
16. Sélectionnez le composant
17. Cliquez sur **Configurer**.
18. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
19. Effectuez l'une des actions suivantes :
    - Si l'installation a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
20. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration d'un système de développement de sécurité Web à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques automatisent les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un système de développement de sécurité Web (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation du système de développement de sécurité Web.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i WebADK -d chemin_packages -a [accept|display]
   ```

   où :

   - `WebADK` est le nom du composant.
   - *`chemin_packages`* est l'emplacement des packages du composant d'installation.

     Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *`point_montage_dvd`*`/usr/sys/inst.images`

     Linux `/`*`point_montage_dvd`*`/linux_x86`

     Solaris
     `/point_montage_dvd``/solaris`
   - `-a [accept|display]`

     L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

   Par exemple, si vous procédez à l'installation sur Linux :

   ```
   ./install_isam.sh -i WebADK -d /mnt/dvd/linux_x86 -a accept
   ```

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l WebADK
   ```

Que faire ensuite

Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la valeur par défaut, installez votre programme de support de langue nationale. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Automatisation de l'installation d'un système de développement de sécurité Web (Windows)

Utilisez le fichier script pour automatiser l'installation d'un système de développement de sécurité Web sous Windows.

Avant de commencer

Le script d'installation utilise les répertoires de destination par défaut suivants :

IBM Security Access Manager
`C:\Program Files\Tivoli\Policy Director`

Client Tivoli Directory Server
`C:\Program Files\IBM\ldap\V6.3`

IBM Security Utilities
`C:\Program Files\Tivoli\TivSecUtl`

Si vous souhaitez modifier les répertoires, vous devez le faire avant d'exécuter le script :

1. Copiez *tous* les fichiers `.iss` depuis le DVD ou extrayez les fichiers d'archive dans un répertoire temporaire sur votre ordinateur. Les fichiers que vous pouvez modifier sont les suivants :

   IBM Security Access Manager
   `ISAMLicense.iss`

   Client IBM Tivoli Directory Server
   `LDAPClient.iss`

   IBM Security Utilities
   `IBMSecurityUtils.iss`
2. Utilisez un éditeur de texte pour modifier le chemin de destination dans l'un des trois fichiers, ou dans les trois.
3. Enregistrez les fichiers.
4. Copiez le fichier de commandes de script, `install_isam.bat`, depuis le DVD ou les fichiers extraits de l'archive et collez-le dans le même répertoire sur votre ordinateur.
5. Exécuter la commande de script comme décrit dans la tâche suivante.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i WebADK /d chemin_packages
   ```

   où :

   - `WebADK` est le nom du composant.
   - *`chemin_packages`* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.

   Par exemple, pour installer le composant Web security ADK, entrez :

   ```
   install_isam.bat /i WebADK /d c:\images_isam
   ```

   où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `/l`.

   ```
   install_isam.bat /l WebADK
   ```

Que faire ensuite

Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la valeur par défaut, installez votre programme de support de langue nationale. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Chapitre 16. Configuration de WebSEAL

Security Access Manager WebSEAL est un gestionnaire de sécurité destiné aux ressources Web. WebSEAL est un serveur Web haute performance multiprocessus qui applique une stratégie de sécurité à granularité fine sur l'espace d'objet Web protégé. Utilisez les instructions de cette section pour installer et configurer un système WebSEAL via une ligne de commande.

Pour plus d'informations sur ce système de sécurité Web, voir le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide*.

Remarque : Avant d'installer WebSEAL sur un système AIX, assurez-vous que les composants **xlC.rte** > **xlC.aix50.rte** sont au niveau 8.0.0.4.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Configuration d'un système WebSEAL via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer un système de développement de sécurité Web. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX `installp`

Linux `rpm`

Solaris
`pkgadd`

Remarque : Si vous effectuez une installation sur Solaris version 10 ou supérieure, spécifiez l'option **-G**. L'option **-G** garantit que les packages sont ajoutés dans la zone actuelle uniquement. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non-globale, les modules sont ajoutés à la zone non-globale uniquement.

Windows
`setup.exe`

Après avoir terminé l'installation, utilisez les commandes de configuration appropriées.

© Copyright IBM Corp. 2001, 2013

Remarque : Pour plus d'informations sur ces utilitaires, voir *IBM Security Access Manager for Web Command Reference*.

AIX : Installation de WebSEAL via une ligne de commande

Utilisez **installp** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur AIX.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Pourquoi et quand exécuter cette tâche

Avertissement : Avant d'installer WebSEAL sur un système AIX, assurez-vous que les composants **xlC.rte** et **xlC.aix50.rte** sont au niveau 8.0.0.4.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
6. Installez le client IBM Directory Server s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
7. Installez IBM Security Access Manager License, si ce n'est déjà fait. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
9. Installez les packages Security Access Manager :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* représente les packages suivants :

     PD.RTE Spécifie le package Security Access Manager Runtime.

PDWeb.RTE
Spécifie le package Security Access Manager Web Security Runtime.

PDWeb.Web
Spécifie le package Security Access Manager WebSEAL.

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une langue différente de l'anglais, qui est la valeur par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez le package Security Access Manager Runtime, puis le package Security Access Manager WebSEAL comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.
       ```
       pdconfig
       ```
       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.
       Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Résultats

Cette étape termine la configuration d'un système Security Access Manager WebSEAL. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : Le système Security Access Manager WebSEAL prend en charge plusieurs instances de WebSEAL sur chaque ordinateur hôte. Consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide* pour plus d'informations sur la configuration d'instances WebSEAL multiples.

Linux : Installation de WebSEAL via une ligne de commande

Utilisez **rpm** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Linux.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire */chemin_package*`/linux_s390x`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Accédez au répertoire *chemin_package*/*distribution*, où :
   - *chemin_package* est le point de montage de votre lecteur de DVD ou l'emplacement des fichiers
   - *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z
6. Installez IBM Global Security Kit (GSKit) s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
7. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
8. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
9. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
10. Installez les packages Security Access Manager :

    `rpm -ihv packages`

    où *packages* représente les packages suivants :

Package	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390x.rpm`
Package Security Access Manager Web Security Runtime	`PDWebRTE-PD-7.0.0-0.x86_64.rpm`	`PDWebRTE-PD-7.0.0-0.s390x.rpm`
Package Security Access Manager WebSEAL	`PDWeb-PD-7.0.0-0.x86_64.rpm`	`PDWeb-PD-7.0.0-0.s390x.rpm`

11. Démontez, le cas échéant, le DVD.
12. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

13. Configurez le package Security Access Manager Runtime, puis le package Security Access Manager WebSEAL comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.
       ```
       pdconfig
       ```
       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
       En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.
       Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Que faire ensuite

Cette étape termine la configuration d'un système Security Access Manager WebSEAL. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : Le système Security Access Manager WebSEAL prend en charge plusieurs instances de WebSEAL sur chaque ordinateur hôte. Consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide* pour plus d'informations sur la configuration d'instances WebSEAL multiples.

Solaris : Installation de WebSEAL via une ligne de commande

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sur Solaris.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).

4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
9. Installez les Security Access Manager packages (l'un après l'autre) :

   ```
   pkgadd -d chemin_package/solaris
     -a /chemin_package/solaris/pddefault -G packages
   ```

   où :

   /*chemin_package*/solaris
   Indique l'emplacement du package.

   /*chemin_package*/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et *packages* désigne les fichiers suivants :

   PDRTE Spécifie le package Security Access Manager Runtime.

   PDWebRTE
   Spécifie le package Security Access Manager Web Security Runtime.

   PDWeb Spécifie le package Security Access Manager WebSEAL.

   Lorsqu'un message demande `Do you want to install these as setuid/setgid`, saisissez **Y** et appuyez sur Entrée. Lorsque vous êtes invité à continuer, saisissez **Y** et appuyez sur Entrée.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Installation of packages successful.
   ```
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez le package Security Access Manager Runtime, puis le package Security Access Manager WebSEAL comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Saisissez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.

En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir de l'aide sur ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Résultats

Cette étape termine la configuration d'un système Security Access Manager WebSEAL. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : Le système Security Access Manager WebSEAL prend en charge plusieurs instances de WebSEAL sur chaque ordinateur hôte. Consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide* pour plus d'informations sur la configuration d'instances WebSEAL multiples.

Windows : Installation de WebSEAL via une ligne de commande

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdconfig** pour les configurer sous Windows.

Avant de commencer

Effectuez les tâches préalables à l'installation décrites dans les rubriques suivantes :

- «Préparation du système d'exploitation», à la page 28.
- Chapitre 4, «Plan des installations et configurations prérequises», à la page 27

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Vérifiez que tous les modules de correction nécessaires pour le système d'exploitation sont installés. Consultez les informations de version les plus récentes, notamment la configuration requise, les exigences relatives à l'espace disque, les incidents connus ainsi que les limitations dans les *Notes sur l'édition IBM Security Access Manager for Web* ou les notes techniques dans la base de données de connaissance de support.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
7. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.

8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
9. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** situé dans le répertoire suivant :

   ```
   \windows\PolicyDirector\Disk Images\Disk1
   ```

   Suivez les instructions en ligne et choisissez d'installer les packages suivants :
   - Security Access Manager Runtime
   - Access Manager Web Security Runtime
   - Security Access Manager WebSEAL
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez le package Security Access Manager Runtime, puis le package Security Access Manager WebSEAL comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       La fenêtre Configuration de Security Access Manager s'affiche.
    b. Sélectionnez le package **Security Access Manager Runtime** et cliquez sur **Configurer**.
    c. Sélectionnez le package **Security Access Manager WebSEAL** et cliquez sur **Configurer**.

    En fonction du package sélectionné, vous êtes invité à choisir des options de configuration. Pour obtenir une assistance avec ces options de configuration, voir Annexe D, «Options pdconfig», à la page 339.

Résultats

Cette étape termine la configuration d'un système Security Access Manager WebSEAL. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Remarque : Le système Security Access Manager WebSEAL prend en charge plusieurs instances de WebSEAL sur chaque ordinateur hôte. Consultez le manuel *IBM Security Access Manager for Web WebSEAL Administration Guide* pour plus d'informations sur la configuration d'instances WebSEAL multiples.

Configuration d'un système WebSEAL à l'aide du tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer WebSEAL et ses logiciels prérequis sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :
- «Préparation du système d'exploitation», à la page 28

- Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM Global Security Kit (GSKit)
- client IBM Tivoli Directory Server
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Web Security Runtime
- Security Access Manager WebSEAL

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser durant l'installation.
4. Cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
5. Cliquez sur **Suivant**.
6. Sélectionnez le composant **WebSEAL**.
7. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
8. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
9. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 10.
10. Cliquez sur **Suivant**.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
13. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 14.
14. Cliquez sur **Suivant** pour commencer la configuration.

Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.

15. Cliquez sur **Configurer Security Access Manager**. L'outil de configuration s'affiche.
16. Sélectionnez le composant
17. Cliquez sur **Configurer**.
18. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
19. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
20. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration du système WebSEAL à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques automatisent les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'un système WebSEAL (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation du système WebSEAL.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i WebSEAL -d chemin_packages -a [accept|display]
   ```

   où :

- `WebSEAL` est le nom du composant.
- *chemin_packages* est l'emplacement des packages du composant d'installation.

  Par exemple, si vous effectuez l'installation à partir d'un DVD :

  AIX *point_montage_dvd*`/usr/sys/inst.images`

  Linux x86-64
  /point_montage_dvd`/linux_x86`

  Linux on System z
  /point_montage_dvd`/linux_s390`

  Solaris
  /point_montage_dvd`/solaris`
- `-a [accept|display]`

  L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

Par exemple, si vous procédez à l'installation sur Linux x86-64 :

```
./install_isam.sh -i WebSEAL -d /mnt/dvd/linux_x86 -a accept
```

Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l WebSEAL
   ```

Automatisation de l'installation d'un système WebSEAL (Windows)

Utilisez le fichier script pour automatiser l'installation d'un système WebSEAL sous Windows.

Avant de commencer

Le script d'installation utilise les répertoires de destination par défaut suivants :

IBM Security Access Manager
`C:\Program Files\Tivoli\Policy Director`

Client Tivoli Directory Server
`C:\Program Files\IBM\ldap\V6.3`

IBM Security Utilities
`C:\Program Files\Tivoli\TivSecUtl`

Si vous souhaitez modifier les répertoires, vous devez le faire avant d'exécuter le script :

1. Copiez *tous* les fichiers `.iss` depuis le DVD ou extrayez les fichiers d'archive dans un répertoire temporaire sur votre ordinateur. Les fichiers que vous pouvez modifier sont les suivants :

   IBM Security Access Manager
   `ISAMLicense.iss`

   Client IBM Tivoli Directory Server
   `LDAPClient.iss`

IBM Security Utilities
IBMSecurityUtils.iss

2. Utilisez un éditeur de texte pour modifier le chemin de destination dans l'un des trois fichiers, ou dans les trois.
3. Enregistrez les fichiers.
4. Copiez le fichier de commandes de script, `install_isam.bat`, depuis le DVD ou les fichiers extraits de l'archive et collez-le dans le même répertoire sur votre ordinateur.
5. Exécuter la commande de script comme décrit dans la tâche suivante.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :
   ```
   install_isam.bat /i WebSEAL /d chemin_packages
   ```
   où :
   - `WebSEAL` est le nom du composant.
   - *`chemin_packages`* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.
   - Par exemple, pour installer le composant WebSEAL, entrez :
     ```
     install_isam.bat /i WebSEAL /d c:\images_isam
     ```
     où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits.

   Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `/l`.
   ```
   install_isam.bat /l WebSEAL
   ```

Automatisation de la configuration d'un système WebSEAL

Utilisez le fichier script pour automatiser l'installation d'un système WebSEAL.

Avant de commencer

- Effectuez l'installation de Web Portal Manager. Voir :

- «Automatisation de l'installation d'un système WebSEAL (AIX, Linux ou Solaris)», à la page 274
- «Automatisation de l'installation d'un système WebSEAL (Windows)», à la page 275

• Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant.

      AIX, Linux ou Solaris
      ```
      /opt/PolicyDirector/example/config/
      configure_webseal.options.template
      ```

      Windows
      ```
      C:\Program Files\Tivoli\PDWeb\etc\
      configure_webseal.options.template.cmd
      ```

   b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

   c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

   d. Sauvegardez le fichier.

2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options. Le fichier est situé dans les emplacements suivants :

      AIX, Linux ou Solaris
      ```
      /opt/PolicyDirector/example/config/
      ```

      Windows
      ```
      C:\Program Files\Tivoli\Policy Director\example\config\
      ```

   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour

masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.

c. Revenez à ces instructions pour exécuter le script de configuration.

3. Copiez le fichier script depuis son emplacement d'origine vers le même répertoire que celui où vous avez copié les fichiers d'options. Les fichiers script se trouvent dans les emplacements suivants :

   AIX, Linux ou Solaris

   Répertoire : `/opt/PolicyDirector/example/config/`

   Nom de fichier : `configure_isam.sh`

   Windows

   Répertoire : `C:\Program Files\Tivoli\Policy Director\example\config\`

   Nom de fichier : `configure_isam.cmd`

4. Exécutez le script de configuration et utilisez le fichier d'options comme entrée.

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* est le fichier texte qui contient les options de configuration.

   Par exemple :

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f my_configure_webseal.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_configure_webseal.options.cmd
   ```

Partie 5. Installation du composant système de gestion des sessions

© Copyright IBM Corp. 2001, 2013

Chapitre 17. Configuration d'un serveur de gestion de sessions

Le serveur Session Management Server est un composant facultatif de Security Access Manager. Il est exécuté en tant que service d'IBM WebSphere Application Server.

Avant de commencer, lisez les informations suivantes sur le serveur Session Management Server :

- Le serveur Session Management Server peut gérer et surveiller des sessions sur des serveurs Web dispersés, en cluster.
- Si vous souhaitez installer et configurer les membres du cluster pour qu'ils fassent partie d'un groupe de noeuds qui représente une zone WebSphere eXtreme Scale, effectuez cette tâche avant de déployer et de configurer SMS. Pour plus de détails, voir la discussion sur WebSphere eXtreme Scale dans le manuel *IBM Security Access Manager for Web Shared Session Management Administration Guide*.
- L'utilisation du serveur de gestion de sessions permet aux composants Security Access Manager WebSEAL et Security Access Manager Plug-in for Web Servers de partager une vue unifiée de toutes les sessions en cours. Le de gestion de sessions permet à tout utilisateur autorisé de surveiller et d'administrer des sessions utilisateur.
- Le serveur de gestion de session enregistre différentes informations de session, notamment : les informations sur l'inactivité de la session et le délai d'expiration du cycle de vie, l'activité de connexion et les informations de connexion actuelles. Le serveur de gestion de sessions enregistre également les informations de statistiques de session, telles que le nombre d'utilisateurs actuellement connectés.
- L'étendue d'une session dans le cluster est appelée *domaine de session*. Session Management Server peut fournir une expérience de connexion unique transparente dans l'ensemble du domaine de session. Effectuez la configuration en ajoutant et en supprimant des domaines de session.
- Session Management Server garantit que la règle de session reste cohérente dans tous les cluster des serveurs de sécurité Web. Les *ensembles de répliques* d'un domaine de session partagent le registre et la base de données de règles Security Access Manager.
- Pour configurer le système Session Management Server, utilisez l'utilitaire **smscfg**. Exécutez la commande depuis le système sur lequel Session Management Server est installé.
- Vous pouvez administrer Session Management Server en utilisant un (ou tous) des outils suivants :

  pdadmin
  : Est installé en tant que partie du package Security Access Manager Runtime. Cette interface vous permet de gérer les listes de contrôle d'accès, les serveurs, les utilisateurs, les objets et d'autres ressources de votre domaine sécurisé. Vous pouvez également automatiser certaines fonctions de gestion en écrivant des scripts s'appuyant sur les commandes **pdadmin**.

© Copyright IBM Corp. 2001, 2013

pdsmsadmin
Utilise le protocole SOAP pour communiquer directement avec un serveur Session Management Server installé sur WebSphere Application Server.

La console du serveur de gestion de sessions
Interface graphique de WebSphere Application Server installée en tant qu'extension de la console d'administration.

Pour plus d'informations sur la gestion de sessions distribuées, voir le manuel *IBM Security Access Manager for Web Shared Session Management Administration Guide*.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Exigences de préinstallation

Avant d'installer et de configurer un serveur de gestion de sessions Security Access Manager, vous devez effectuer plusieurs tâches de préinstallation.

Ces exigences sont applicables, quelle que soit la méthode que vous prévoyez d'utiliser.

- Effectuez les tâches préalables à l'installation décrites à la section «Préparation du système d'exploitation», à la page 28.
- Effectuez les tâches préalables appropriées décrites à la section Chapitre 4, «Plan des installations et configurations prérequises», à la page 27
- Lorsque vous déployez le serveur Session Management Server sur un cluster, le kit d'outil ObjectGrid est automatiquement déployé pour gérer la distribution et la gestion des données de session entre les différents noeuds du cluster. L'installation de ce kit d'outils nécessite environ 600 Mo d'espace disque sur les partitions qui contiennent l'installation WebSphere de chaque noeud. Si vous prévoyez de déployer le serveur Session Management Server sur un cluster, assurez-vous que vous disposez d'un espace disque suffisant pour installer le kit d'outils ObjectGrid.
- Si IBM WebSphere Application Server est installé, le serveur Session Management Server peut être exécuté en tant que service. IBM WebSphere Application Server peut également être installé comme serveur autonome et Session Management Server peut être déployé sur un serveur d'applications ou sur un cluster.
- Un environnement Security Access Manager doit exister avant l'installation du serveur de gestion de sessions.
- Une fois Session Management Server installé, vous devez reconfigurer Security Access Manager WebSEAL et/ou Security Access Manager Plug-in for Web Servers afin d'utiliser Session Management Server pour gérer les sessions.
- La structure de vos domaines de session et les ensembles de répliques associés doivent être planifiés et mappés.
- Déterminez si vous souhaitez répliquer les instances de Session Management Server qui fournissent une fonction de reprise en ligne et des performances améliorées.
- Si vous souhaitez administrer le système de gestion de sessions à l'aide de l'utilitaire **pdadmin**, installez et configurez une instance de Security Access Manager Authorization Server.
- Si WebSphere Application Server est exécuté en tant qu'utilisateur non superutilisateur sur un système AIX, Linux ou Solaris, les étapes suivantes doivent être effectuées.

- En tant que superutilisateur, octroyez à l'utilisateur WebSphere un droit d'écriture pour les répertoires suivants (et tous les sous-répertoires) dans le répertoire d'installation principal de WebSphere Application Server :

  ```
  deploytool
  java
  lib
  ```

  Ces droits peuvent être supprimés une fois la configuration de Session Management Server terminée.
- Si Tivoli Common Directory est activé pour la première fois sur le système, en tant que superutilisateur, créez les répertoires suivants et octroyez à l'utilisateur WebSphere user le droit d'y créer des sous-répertoires :

  ```
  /etc/ibm
  /var/ibm
  ```
- Si Tivoli Common Directory est activé, octroyez à l'utilisateur WebSphere un accès en écriture sur le répertoire de journalisation principal, comme`/var/ibm/tivoli/common`.

  Ce droit peut être supprimé une fois la configuration de Session Management Server terminée.
- Si Tivoli Common Directory est activé, octroyez à l'utilisateur WebSphere un accès en écriture au sous-répertoire de journalisation de Session Management Server, comme`CTGSM`.

- Décidez si vous souhaitez activer la sécurité globale WebSphere pour vous assurer que les actions d'administration sont sécurisées.

  Voir les informations dans les rubriques relatives à la configuration et à l'activation de la sécurité dans le centre de documentation de WebSphere Application Server :

  http://www.ibm.com/software/webservers/appserv/was/library/
- Si la sécurité globale de WebSphere est activée, créez trois groupes dans WebSphere Application Server, qui peuvent être utilisés pour gérer l'environnement Session Management Server :
  - Un groupe pour les administrateurs, par exemple : **administrateurs-sms**
  - Un groupe pour les délégués, par exemple : **délégués-sms**
  - Un groupe pour les clients, par exemple : **clients-sms**

  Les noms des groupes doivent suivre les conventions de dénomination du registre d'utilisateurs utilisé par WebSphere Application Server. Vous pouvez utiliser des groupes existants à cette fin.
- Déterminez si vous souhaitez activer SSL (Secure Sockets Layer) pour les communications de Session Management Server. Vous pouvez activer SSL entre les serveurs Security Access Manager du jeu de répliques et le serveur IBM WebSphere Application Server sur lequel Session Management Server est installé.
- Si vous prévoyez d'utiliser des certificats Security Access Manager pour l'authentification avec SMS ou si vous souhaitez spécifier l'utilisateur Security Access Manager sec_master (ou d'autres utilisateurs et groupes définis dans le suffixe `secAuthority=Default`) pour administrer SMS à l'aide de la ligne de commande de gestion des sessions ou de la console, vous devez annuler la configuration du nom distinctif de base dans le registre d'utilisateurs LDAP utilisé par WebSphere Application Server.

  Des informations sur la modification du nom distinctif de base pour le registre d'utilisateurs de WebSphere Application Server sont disponibles dans le centre

de documentation WebSphere Application Server dans la rubrique consacrée à la configuration de Lightweight Directory Access Protocol, à l'adresse :

http://www.ibm.com/software/webservers/appserv/was/library/

Configuration du serveur de gestion de sessions via une ligne de commande

Exécutez les utilitaires de ligne de commande spécifiques à la plateforme pour installer le serveur de gestion de sessions. Cette méthode est une des méthodes d'installation que vous pouvez utiliser.

Pour plus d'informations, reportez-vous au Chapitre 2, «Méthodes d'installation», à la page 19.

Lors de l'exécution des utilitaires de ligne de commande, vous devez installer manuellement chaque composant et son logiciel prérequis dans l'ordre adéquat.

Accomplissez d'abord les tâches préalables à l'installation. Voir Partie 2, «Installation de logiciels prérequis», à la page 25.

Les utilitaires d'installation spécifiques aux plateformes utilisés sont :

AIX **`installp`**

Linux **`rpm`**

Solaris
`pkgadd`

Remarque : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **`pkgadd`**. L'option **-G** ajoute le package uniquement dans la zone en cours. Lorsque l'option **-G** est utilisée dans la zone globale, le package est ajouté à la zone globale uniquement, et n'est pas propagé aux zones existantes ou futures non-globales. Lorsqu'elle est utilisée dans une zone non globale, les packages sont ajoutés à la zone non globale uniquement.

Windows
`setup.exe`

Après avoir terminé l'installation, utilisez les commandes de configuration appropriées.

Remarque : Pour plus d'informations sur ces utilitaires, voir *IBM Security Access Manager for Web Command Reference*.

AIX : Installation d'un système de serveur de gestion de sessions

L'installation d'un système de serveur de gestion de sessions sur AIX fait partie d'un processus en trois étapes qui comprend l'installation, le déploiement sur le serveur d'applications ou le cluster et la configuration.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.

2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 282.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Installez le serveur IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
5. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez les packages Security Access Manager suivants :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

   où :

   - *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
   - *packages* représente les packages suivants :

     PD.SMS Spécifie le package Security Access Manager Session Management Server.
8. Démontez, le cas échéant, le DVD.
9. Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données comme décrit dans «Création de la base de données d'historique de connexion» , à la page 288.

Que faire ensuite

Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données avant de déployer l'application Session Management Server. Voir «Création de la base de données d'historique de connexion», à la page 288. Sinon, passez aux sections «Déploiement de l'application Session Management Server», à la page 292 et «Configuration du serveur de gestion de sessions», à la page 293.

Linux : Installation d'un système Session Management Server

L'installation d'un système Session Management Server sur Linux fait partie d'un processus en trois étapes qui comprend l'installation, le déploiement sur le serveur d'applications ou le cluster et la configuration.

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire */chemin_package/linux_s390*.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).

3. Installez le serveur IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
6. Accédez au répertoire *chemin_package*/*distribution*,

   où :

   - *chemin_package* est le point de montage de votre lecteur de DVD ou l'emplacement des fichiers
   - *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z
7. Installez les packages Security Access Manager :

   `rpm -ihv packages`

   où *packages* représente les packages suivants :

Package	Linux sur x86-64	Linux on System z
Package Security Access Manager Session Management Server	`PDSMS-PD-7.0.0-0.x86_64.rpm`	`PDSMS-PD-7.0.0-0.s390.rpm`

8. Démontez, le cas échéant, le DVD.
9. Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données comme décrit dans «Création de la base de données d'historique de connexion» , à la page 288.

Que faire ensuite

Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données avant de déployer l'application Session Management Server. Voir «Création de la base de données d'historique de connexion», à la page 288. Sinon, passez aux sections «Déploiement de l'application Session Management Server», à la page 292 et «Configuration du serveur de gestion de sessions», à la page 293.

Solaris : Installation d'un système Session Management Server

L'installation d'un système Session Management Server sur Solaris fait partie d'un processus en trois étapes qui comprend l'installation, le déploiement sur le serveur d'applications ou le cluster et la configuration.

Pourquoi et quand exécuter cette tâche

La procédure suivante utilise **pkgadd** pour installer les progiciels.

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 282.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Installez le serveur IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
5. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
6. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
7. Installez les packages Security Access Manager :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault
   -G packages
   ```

   où :

   /chemin_package/**solaris**
   Indique l'emplacement du package.

   /chemin_package/**solaris/pddefault**
   Indique l'emplacement du script d'administration de l'installation.

   et *packages* représente les packages suivants :

   PDSMS Spécifie le package Security Access Manager Session Management Server.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Installation of package successful.
   ```
8. Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données comme décrit dans «Création de la base de données d'historique de connexion» , à la page 288.

Que faire ensuite

Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données avant de déployer l'application Session Management Server. Voir «Création de la base de données d'historique de connexion», à la page 288. Sinon, passez aux sections «Déploiement de l'application Session Management Server», à la page 292 et «Configuration du serveur de gestion de sessions», à la page 293.

Windows : Installation d'un système Session Management Server

L'installation d'un système Session Management Server fait partie d'un processus en trois étapes qui comprend l'installation, le déploiement sur le serveur d'applications ou le cluster et la configuration.

Procédure

1. Connectez-vous en tant que membre du groupe Administrateurs.
2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 282.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Installez le serveur IBM WebSphere Application Server. Pour obtenir des instructions, voir «Installation de WebSphere Application Server», à la page 47.
5. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
6. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
7. Installez le package Security Access Manager Session Management Server. Pour ce faire, exécutez le programme **setup.exe** à partir du répertoire suivant `:\windows\PolicyDirector\Disk Images\Disk1`
   Suivez les instructions en ligne et sélectionnez **Access Manager Session Management Server**.
8. Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données comme décrit dans «Création de la base de données d'historique de connexion».

Que faire ensuite

Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données avant de déployer l'application Session Management Server. Voir «Création de la base de données d'historique de connexion». Sinon, passez aux sections «Déploiement de l'application Session Management Server», à la page 292 et «Configuration du serveur de gestion de sessions», à la page 293.

Création de la base de données d'historique de connexion

Si vous avez l'intention d'utiliser une base de données DB2 pour stocker les informations d'historique de connexion, vous devez créer la base de données avant de déployer l'application Session Management Server.

Pourquoi et quand exécuter cette tâche

Si vous n'avez pas l'intention d'utiliser une base de données DB2, continuez avec «Déploiement de l'application Session Management Server», à la page 292.

Procédure

1. Un utilisateur du système du serveur de la base de données DB2 doit être propriétaire de la base de données DB2. Créez un utilisateur sur le système et attribuez-lui un mot de passe valide. Si cela est cohérent avec la stratégie de sécurité de votre organisation, vous pouvez choisir d'indiquer que le mot de passe n'expire jamais. Par exemple, vous pouvez appeler cet utilisateur `isamloginuser`.

2. Créez une base de données dans DB2. Par exemple, vous pouvez nommer la nouvelle base de données `isamLOGIN`. Configurez la base de données pour autoriser les connexions TCP/IP sur le port `50000`.
3. Ouvrez **DB2 Control Center** et recherchez votre base de données.
4. Cliquez sur **User and Group Objects** > **DB Users**, puis cliquez sur **Add New User**.
5. Ajoutez l'utilisateur et octroyez-lui les droits **Connect to database** > **Create tables**.
6. Cliquez sur **OK**.
7. Configurez WebSphere Application Server pour accéder à la base de données.

   Des informations sur cette tâche sont disponibles dans le centre de documentation WebSphere Application Server à l'adresse :

   http://www.ibm.com/software/webservers/appserv/was/library/

   Effectuez spécifiquement les opérations suivantes :

   - Création et configuration d'un fournisseur JDBC et d'une source de données
   - Paramètres minimum requis des sources de données classés par fournisseur
8. Rendez le pilote IBM DB2 JDBC disponible pour WebSphere Application Server en copiant les fichiers `db2jcc.jar` et `db2jcc_license_cu.jar` depuis l'arborescence de répertoire DB2 vers le répertoire `lib` de votre serveur d'applications.

   AIX, Linux et Solaris
   `/opt/IBM/WebSphere/AppServer/lib`
9. Vérifiez que le pilote IBM JDBC fonctionne dans WebSphere en accédant au sous-répertoire `lib` et en entrant la commande suivante :

   ```
   java -classpath db2jcc.jar com.ibm.db2.jcc.DB2Jcc -version
   ```
10. Ouvrez la console d'administration WebSphere Application Server et connectez-vous si nécessaire.
11. Cliquez sur **Environnement** > **Variables WebSphere**.
12. Définissez la variable `DB2UNIVERSAL_JDBC_DRIVER_PATH` sur le répertoire dans lequel de trouve le fichier `db2jcc.jar`. Sauvegardez vos changements.
13. Déconnectez-vous de la console d'administration WebSphere Application Server.
14. Redémarrez vos serveurs d'applications. Si vous utilisez WebSphere Application Server Network Deployment, vous devez également redémarrer le gestionnaire de déploiement et le gestionnaire de noeuds.
15. Ouvrez la console d'administration WebSphere Application Server et reconnectez-vous.
16. Cliquez sur **Ressources** > **Fournisseurs JDBC**.
17. Dans un environnement à un seul serveur, sélectionnez votre noeud de serveur d'applications ; dans WebSphere Application Server Network Deployment, sélectionnez votre cluster.
18. Cliquez sur **Nouveau** pour créer un fournisseur JDBC.
19. Dans la zone **Type de base de données**, sélectionnez DB2 et spécifiez les informations suivantes :

    Type de fournisseur
    Fournisseur de pilotes JDBC DB2 Universal

    Type de mise en oeuvre
    Source de données du pool de connexions
20. Cliquez sur **Suivant** pour continuer.

21. Sur la page JDBC Providers Summary, cliquez sur **Appliquer** pour accepter les paramètres par défaut.

    Ne redémarrez pas WebSphere Application Server maintenant.
22. Sur la page Fournisseurs JDBC, sélectionnez Fournisseur JDBC DB2 Universal.
23. Cliquez sur **Sources de données**.
24. Cliquez sur **Nouveau** pour créer une source de données et spécifiez les informations suivantes :

    Nom de la base de données
    isamLOGIN

    Type de pilote
    4

    Nom du serveur
    nom_hôte_système_DB2

    Numéro de port
    50000
25. Cliquez sur **Appliquer**. Vous revenez à la page précédente.
26. Sur la page JDBC Providers, sélectionnez DB2 Universal JDBC Driver DataSource.
27. Cliquez sur **Related items** puis sur **J2EE Connector Architecture (J2C) authentication data entries**.
28. Cliquez sur **Nouveau** pour créer une entrée de données d'authentification et spécifiez les informations suivantes :

    Alias logindbuser

    ID utilisateur
    isamloginuser

    Mot de passe
    password_for_isamloginuser

    Description
    Accès à la base de données d'historique de connexion
29. Cliquez sur **Appliquer**. Vous revenez à la page précédente.
30. Revenez aux propriétés de la source de données DB2 Universal JDBC Driver et, sous **Alias d'authentification de composant géré**, sélectionnez l'alias `logindb2user`.
31. Cliquez sur **Appliquer**.
32. Déconnectez-vous de la console d'administration WebSphere Application Server.
33. Redémarrez vos serveurs d'applications. Si vous utilisez WebSphere Application Server Network Deployment, vous devez également redémarrer le gestionnaire de déploiement et le gestionnaire de noeuds.
34. Ouvrez la console d'administration WebSphere Application Server et reconnectez-vous.
35. Cliquez sur **Ressources** > **Fournisseurs JDBC** > **Fournisseur de pilotes JDBC DB2 Universal** > **Sources de données**.
36. Sélectionnez votre source de données et cliquez sur **Test connection**. Si le test échoue, diagnostiquez et corrigez le problème. Sinon, passez à la section «Déploiement de l'application Session Management Server», à la page 292.

Déploiement de l'extension de console

L'extension de la console Session Management Server est une interface graphique utilisateur (GUI) qui permet de déployer, de configurer et d'administrer Session Management Server. Après avoir installé Session Management Server à l'aide des utilitaires natifs, vous pouvez déployer la console à l'aide de l'utilitaire **smscfg**.

Pourquoi et quand exécuter cette tâche

Remarque : Les instructions de cette section supposent que vous exécutez l'utilitaire **smscfg** en mode interactif.

Pour déployer l'extension ISC, vous pouvez exécuter l'utilitaire **smscfg**. Cet utilitaire se trouve par défaut aux emplacements suivants :

AIX, Linux ou Solaris :

```
/opt/pdsms/bin
```

Windows :

```
C:\Program Files\Tivoli\PDSMS\bin
```

Voir le manuel *IBM Security Access Manager for Web: Shared Session Management Administration Guide* pour des informations plus détaillées sur le déploiement.

Procédure

1. Avant d'exécuter **smscfg**, exécutez le script WebSphere `setupCmdLine.bat` (sous Windows) ou `setupCmdLine.sh` (sur AIX, Linux ou Solaris).
2. Déployez la console l'aide de l'utilitaire de configuration :

   ```
   smscfg -action deploy
   ```
3. Lorsque vous y êtes invité, spécifiez `ISC` en tant que nom d'instance.

Que faire ensuite

Passez à l'étape «Connexion et déconnexion de la console Session Management Server».

Connexion et déconnexion de la console Session Management Server

Accédez à la console IBM Security Access Manager Session Management Server en ouvrant un navigateur Web et en tapant l'adresse URL appropriée.

Avant de commencer

Pour composer correctement l'URL, vous devez connaître les paramètres de la console. L'adresse URL requise peut par exemple être : `https://isam.example.com:9043/ibm/console`

Cette URL est composée des éléments suivants :

- Nom du système hôte exécutant la console.
- Numéro de port de la console. Le port utilisé par la console du serveur de gestion de sessions est le même que celui qui est utilisé par la console hébergeant WebSphere Application Server.
- URL d'accès à la page de connexion de la console. La partie suivante de l'URL est toujours identique :

  ```
  /ibm/console
  ```

Lorsque vous établissez l'adresse URL correcte, vous devez connaître le nom d'utilisateur et le mot de passe de l'administrateur de la console. Le nom et le mot de passe ont été spécifiés lors de la configuration.

Procédure

1. Entrez l'URL de console dans la barre d'adresse de la fenêtre de votre navigateur. Par exemple, pour l'URL d'un système dont le nom d'hôte est `isam.example.com` et qui utilise le numéro de port par défaut, entrez :

   ```
   https://isam.example.com:9043/ibm/console
   ```

2. Entrez l'ID et le mot de passe de l'administrateur. Le panneau Bienvenue de la console s'affiche.
3. Utilisez les liens de navigation situés sur la gauche pour visualiser et utiliser les tâches de la console.

   Avertissement : N'utilisez pas le bouton **Précédent** de votre navigateur pour vous déplacer dans la console.
4. Pour vous déconnecter, cliquez sur **Déconnecter** dans le coin supérieur droit du panneau.

Déploiement de l'application Session Management Server

Après avoir installé Session Management Server à l'aide des utilitaires natifs, vous pouvez déployer le fichier `DSess.ear` à l'aide de l'utilitaire **`smscfg`** ou de Session Management Server Console.

Déploiement à l'aide de l'utilitaire smscfg

Vous pouvez déployer l'application à l'aide de l'utilitaire **`smscfg`**.

Pourquoi et quand exécuter cette tâche

Remarque : Les instructions de cette section supposent que vous exécutez l'utilitaire **`smscfg`** en mode interactif.

Procédure

1. Avant d'exécuter **`smscfg`**, exécutez le script WebSphere `setupCmdLine.bat` (sous Windows) ou `setupCmdLine.sh` (sur AIX, Linux ou Solaris).
2. Déployez l'application Session Management Server à l'aide de l'utilitaire de configuration : `smscfg -action deploy`
   Voir le manuel *IBM Security Access Manager for Web: Shared Session Management Administration Guide* pour des informations détaillées sur le déploiement.

Déploiement à l'aide de la console de Session Management Server

Vous pouvez déployer une instance de l'application Session Management Server à l'aide de la console SMS.

Pourquoi et quand exécuter cette tâche

Remarque : Pour utiliser la console afin de déployer l'instance Session Management Server, vous devez d'abord déployer l'extension de la console. Pour plus d'informations, voir «Déploiement de l'extension de console», à la page 291.

Voir le manuel *IBM Security Access Manager for Web: Shared Session Management Administration Guide* pour des informations détaillées sur le déploiement.

Procédure

1. Connectez-vous à la console du serveur de gestion de sessions en tant qu'administrateur Session Management Server. Voir «Connexion et déconnexion de la console Session Management Server», à la page 291 pour obtenir une assistance.
2. Sélectionnez **Session Management Server** > **Déploiement**.
3. Dans la zone **Nom d'application**, entrez le nom de l'application Session Management Server. Cette zone est obligatoire.
4. Entrez l'élément de cellule WebSphere Application Server sur lequel l'instance de Session Management Server doit être déployée dans la zone **Cible**.
5. Dans la zone **Hôte virtuel**, entrez les hôtes virtuels du serveur Web qui utiliseront l'instance de l'application Session Management Server.
6. Entrez la source de données à utiliser avec l'instance de l'application Session Management Server dans la zone **Source de données**.
7. Lorsque vous êtres prêt à effectuer le déploiement, cliquez sur **Déploiement**.

Configuration du serveur de gestion de sessions

Après avoir installé Session Management Server à l'aide des utilitaires natifs et après avoir déployé l'application DSess.ear, vous pouvez configurer le serveur Session Management Server à l'aide de l'utilitaire **smscfg** ou de Session Management Server console Solutions Console (ISC).

Configuration du serveur Session Management Server à l'aide de l'utilitaire `smscfg`

Vous pouvez configurer le serveur de gestion de sessions à l'aide de l'utilitaire **smscfg**.

Procédure

1. Exécutez le script IBM WebSphere Application Server **`setupCmdLine`** pour configurer l'environnement d'exécution correct pour l'outil de configuration du serveur Session Management Server. Le script **`setupCmdLine`** se trouve dans le répertoire IBM WebSphere Application Server `bin` du profil que vous utilisez. Par exemple :

   AIX, Linux ou Solaris

   ```
   /racine_serveur_app/serveur_applications/bin/setupCmdLine.sh
   ```

   Windows

   ```
   racine_serveur_app\bin\setupCmdLine.bat
   ```

   où *racine_serveur_app* est l'emplacement du profil de serveur d'applications WebSphere Application Server.
2. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
3. Configurez le package Security Access Manager Session Management Server à l'aide de l'utilitaire de configuration :

   ```
   smscfg -action config
   ```

   Voir le manuel *IBM Security Access Manager for Web Shared Session Management Administration Guide* pour des informations de configuration détaillées.

Résultats

Cette étape termine la configuration de Security Access Manager Session Management Server. Une fois Session Management Server configuré, vous devez configurer Security Access Manager WebSEAL et/ou Security Access Manager Plug-in for Web Servers afin d'utiliser Session Management Server pour gérer les sessions. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Configuration du serveur de gestion de sessions à l'aide de la console

Avant de pouvoir utiliser le serveur de gestion de sessions, vous devez le configurer. Pour effectuer cette configuration, vous pouvez utiliser la console de Session Management Server.

Procédure

1. Configurez des domaines de session :
   a. Connectez-vous à la console Session Management Server en tant qu'administrateur Session Management Server. Voir «Connexion et déconnexion de la console Session Management Server», à la page 291 pour obtenir une assistance.
   b. Sélectionnez **Session Management Server** > **Configuration**.
   c. Sélectionnez l'instance de Session Management Server à configurer.

      Remarque : Si vous venez de déployer ou de démarrer une instance et qu'elle n'apparaît pas dans la liste des instances Session Management Server, cliquez sur **Mise à jour de la liste d'instances SMS**.
   d. Cliquez sur **Configurer**.
   e. Sélectionnez **Domaines de session**.
   f. Sélectionnez si l'application de la règle du nombre maximal de sessions et de déplacement doit être activée.
   g. Dans la zone **Noms des domaines de session**, entrez le nom du domaine de session à configurer.
   h. Cochez la case **Nombre maximal de sessions pour ce domaine de session** afin de restreindre le nombre maximum de sessions simultanées stockées dans ce domaine de session. Entrez le nombre maximum de sessions simultanées à stocker dans la zone Nombre maximal de sessions.
   i. Lorsque vous entrez les informations du domaine de session, cliquez sur **Mise à jour des domaines de session**. La table des domaines de session est mise à jour avec les valeurs de configuration spécifiées.
   j. Pour créer un jeu de répliques, sélectionnez le nom du domaine de session dans le menu déroulant **Nom du domaine de session** .
   k. Spécifiez le nom de la réplique à configurer dans la zone **Nom du jeu de répliques**.
   l. Cliquez sur **Mise à jour des jeux de répliques** pour mettre à jour la table des jeux de répliques avec les valeurs spécifiées.
2. Cliquez sur **Stockage dans la base de données**. Si vous souhaitez que Session Management Server stocke les informations de session dans une base de données, cochez la case **Activer le stockage dans la base de données**.
3. Cliquez sur **Intégration IBM Security Access Manager**. Indiquez si l'intégration de Security Access Manager est activée. Pour activer l'intégration de Security Access Manager, cochez la case **Activer l'intégration Security Access Manager**.

4. Cliquez sur **Enregistrement de la dernière connexion**. Indiquez si l'enregistrement des informations de dernière connexion est activé. Pour activer l'enregistrement des dernières informations de connexion, cochez la case **Activer l'enregistrement des dernières informations de connexion**.
5. Cliquez sur **Consignation TCD**. Pour configurer la consignation Tivoli Common Directory (TCD), indiquez les informations suivantes :
   - Cochez la case **Activer la consignation Tivoli Common Directory** pour activer la consignation Tivoli Common Directory.
   - Définissez un répertoire à utiliser pour Tivoli Common Directory dans la zone **Répertoire de consignation**. Si une instance Tivoli Common Directory est déjà configurée sur cette machine, cette valeur n'est pas utilisée. L'instance Tivoli Common Directory est utilisée à sa place.
6. Cliquez sur **Contrôle**. Spécifiez si le contrôle est activé. Pour activer le contrôle, cochez la case**Activation du contrôle**.
7. Cliquez sur **Délais d'attente**. Indiquez le délai d'inactivité du client et la durée de vie de la clé :
   - Entrez la durée, en secondes, après laquelle un client est considéré comme inactif. Ceci s'applique uniquement si le client ne demande pas explicitement de mises à jour à Session Management Server.
   - Entrez le nombre de jours, à partir de la génération d'une clé de signature de session, après lequel Session Management Server génère automatiquement une nouvelle clé de signature.
8. Cliquez sur **Récapitulatif**. Vérifiez les options de configuration que vous avez sélectionnées.
9. Lorsque vous êtes prêt à effectuer la configuration, cliquez sur **Terminer**.

   Cette étape termine la configuration de Security Access Manager Session Management Server.

Que faire ensuite

Une fois Session Management Server configuré, vous devez configurer Security Access Manager WebSEAL et/ou Security Access Manager Plug-in for Web Servers afin d'utiliser Session Management Server pour gérer les sessions. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Voir le manuel *IBM Security Access Manager for Web Shared Session Management Administration Guide* pour des informations de configuration détaillées.

Configuration d'un serveur de gestion de session avec le tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer le logiciel du serveur de gestion sous Windows. Le tableau de bord est une interface graphique.

Avant de commencer

Effectuez les tâches de configuration prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28

- Si vous envisagez d'utiliser un registre d'utilisateurs autre qu'IBM Tivoli Directory Server, suivez les instructions indiquées à la section Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.
- Consultez l'introduction du manuel *IBM Security Access Manager for Web Shared Session Management Administration Guide*. Cette introduction décrit les fonctionnalités du serveur de gestion de sessions. Elle présente également plusieurs considérations relatives au déploiement et à la sécurité qui sont importantes à vérifier avant l'installation du serveur de gestion de sessions.

Pourquoi et quand exécuter cette tâche

Utilisez l'interface graphique utilisateur du tableau de bord pour effectuer l'installation étape par étape et la configuration initiale des composants suivants :

- IBM WebSphere Application Server
- Security Access Manager License
- Security Access Manager Session Management Server

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage. Vous avez besoin des fichiers correspondant aux produits suivants :
   - WebSphere Application Server
   - Installation Manager
   - IBM Security Access Manager

   Avertissement : Les fichiers image doivent se trouver sous un chemin de répertoire ne comportant aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser pour l'installation.
4. Cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
5. Cliquez sur **Suivant**.
6. Sélectionnez le composant **Session Management Server**.
7. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
8. Effectuez l'une des actions suivantes :
   - Si WebSphere Application Server est déjà installé, passez à l'étape 9, à la page 298.
   - Si WebSphere Application Server n'est pas installé :
     a. Cliquez sur **Installer les composants WebSphere Application Server**.
     b. Sélectionnez le chemin d'accès à l'image d'IBM Installation Manager.

        Remarque : Le chemin d'accès à l'image Installation Manager est limitée à une longueur de 172 caractères.
     c. Cliquez sur **OK**.

Remarque : Une fois l'installation d'Installation Manager effectuée, un délai de 30 secondes s'écoule avant l'ouverture et le lancement de l'installation de WebSphere Application Server.

d. Dans la console d'Installation Manager, cliquez sur **Installer** pour débuter l'installation de WebSphere Application Server.
e. Cliquez sur **Fichier** > **Préférences**.
f. Sélectionnez **Référentiels**.
g. Cliquez sur **Ajouter le référentiel**.
h. Sélectionnez l'emplacement du fichier `repository.config` dans l'image de WebSphere Application Server.
i. Cliquez sur **OK**.
j. Cliquez sur **Installer**. Procédez à l'installation en suivant les invites. Les sélections par défaut fournies par le programme d'installation d'IBM WebSphere Application Server sont suffisantes pour IBM Security Access Manager.
   - Si l'installation réussit, une liste des packages installés et une invite de lancement de l'outil de gestion de profil s'affiche. Continuez avec 8k.
   - Si l'installation d'Installation Manager ou de WebSphere Application Server échoue, ou si une erreur s'affiche, consultez les fichiers journaux et les actions que ceux-ci indiquent. Les fichiers se trouvent par défaut sous `%USERPROFILE%`, par exemple `C:\Users\Administrator\`.

     Journaux d'Installation Manager

     `IMInstall.log`

     `IMInstallLog.xml`

     Journal d'installation de WebSphere Application Server

     `LaunchIMforWAS.log`
k. Sélectionnez **Outil de gestion de profil pour créer un profil**.
l. Cliquez sur **Terminer**.
m. Cliquez sur **Créer**. Vous êtes invité à indiquer plusieurs paramètres de configuration pour le profil de WebSphere Application Server.

   Remarque : Parmi ces paramètres figure la sécurité administrative de WebSphere Application Server. Pour activer le protocole SSL sur l'instance WebSphere Application Server, cochez la case **Activer la sécurité administrative** et renseignez les zones **Nom d'utilisateur** et **Mot de passe**. Notez ces paramètres afin de les réutiliser à l'étape 14, à la page 298.
n. Démarrez l'outil Premiers pas et cliquez sur **Démarrer le serveur**. Le message `Ouvrir pour e-business` s'affiche.
o. Fermez les fenêtres suivantes :
   - Premiers pas
   - WebSphere Customization Toolbox
p. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis.
q. Localisez le groupe de correctifs dans le référentiel Web de WebSphere Application Server ou téléchargez le module et installez-le à partir d'un référentiel local.

- Pour effectuer l'installation à partir du référentiel Web :
  1) Cliquez sur **Mettre à jour** dans la fenêtre IBM Installation Manager.
  2) Sélectionnez **IBM WebSphere Application Server Network Deployment V8.0**.
  3) Cliquez sur **Suivant**. Poursuivez l'installation.
- Pour effectuer l'installation à partir d'un référentiel local :
  1) Localisez le groupe de correctifs sur la page de support de WebSphere Application Server : http://www.ibm.com/support/docview.wss?uid=swg27004980
  2) Téléchargez le groupe de correctifs dans un référentiel local.
  3) cliquez sur **Mettre à jour**.
  4) Sélectionnez **IBM WebSphere Application Server Network Deployment V8.0**.
  5) Cliquez sur **Suivant**. Poursuivez l'installation. Utilisez le fichier Readme joint fourni sur la page de support de WebSphere Application Server pour obtenir une assistance.

r. Démarrez IBM WebSphere Application Server.
  1) Cliquez sur **Démarrer** > **Administrative Tools (Outils d'administration)** > **Services**.
  2) Sélectionnez l'instance IBM WebSphere Application Server qui a été ajoutée.
  3) Cliquez avec le bouton droit sur le service, puis cliquez sur **Démarrer**.

s. Fermez la fenêtre d'IBM Installation Manager.

t. Revenez à la fenêtre du tableau de bord.

9. Cliquez sur **Suivant**. Le panneau d'installation du composant répertorié suivant s'affiche.
   - Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation.
   - Une coche en regard d'un nom de composant signifie que ce composant est installé.
10. Cliquez sur **Suivant**. L'installation du premier composant débute.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
13. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 14.
14. Spécifiez les paramètres de sécurité de WebSphere Application Server. Par défaut, la case **SSL est activé sur le serveur IBM WebSphere Application Server** est cochée.
    - Si SSL n'est pas activé sur WebSphere Application Server, ne cochez pas la case. Puis cliquez sur **Suivant**.
    - Si SSL n'est pas activé sur WebSphere Application Server, spécifiez les paramètres SSL. Cliquez enfin sur **Suivant**. Les paramètres que vous êtes invité à définir ont été configurés lors de la création du profil de WebSphere Application Server.

ID administrateur de WebSphere Application Server
Identificateur d'un compte administrateur existant d'IBM WebSphere Application Server.

Mot de passe administrateur de WebSphere Application Server
Mot de passe associé à l'ID administrateur IBM WebSphere Application Server indiqué.

Fichier de clés certifiées SSL
Nom du fichier de clés certifiées. Recherchez le fichier et sélectionnez-le. Par exemple :

```
C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\
  AppSrv01\etc\trust.p12
```

Mot de passe du fichier de clés certifiées SSL
Mot de passe du fichier de clés certifiées. Le mot de passe par défaut est `WebAS`.

Fichier de clés SSL
Le fichier de clés. Recherchez un fichier de clés existant et sélectionnez-le. Par exemple :

```
C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\
  AppSrv01\etc\key.p12
```

Mot de passe du fichier des clés SSL
Mot de passe du fichier de clés. Le mot de passe par défaut est `WebAS`.

15. Cliquez sur **Suivant**.
16. Cliquez sur **Déployer la console de Session Management Server**.
    - Si le déploiement a été effectué avec succès, cliquez sur **Suivant**.
    - Si le déploiement a échoué ou si une erreur s'affiche :
      a. Consultez le fichier journal situé à l'emplacement par défaut `%USERPROFILE%`, par exemple `C:\Users\Administrator\deploySMSconsole.log`.
      b. Apportez les corrections indiquées dans le fichier journal.
      c. Cliquez sur **Déployer la console de Session Management Server** ou exécutez la commande **smscfg.bat**.

      Ce fichier se trouve dans le répertoire *répertoire_installation*\bin\, où *répertoire_installation* est le répertoire dans lequel vous avez installé le composant, par exemple `C:\Program Files\Tivoli\PDSMS`. Voir le manuel *IBM Security Access Manager for Web Command Reference* pour plus d'informations sur la commande **smscfg.bat**.
17. Cliquez sur **Terminer** pour fermer le tableau de bord.
18. Connectez-vous à la console Session Management Server en tant qu'administrateur Session Management Server. Voir «Connexion et déconnexion de la console Session Management Server», à la page 291 pour obtenir une assistance.
19. Si la sécurité est activée sur WebSphere Application Server, vous devez ajouter le rôle `sms-administrator` aux utilisateurs ou aux groupes qui administrent le serveur de gestion de sessions.
    a. Dans la console, cliquez sur **Utilisateurs et groupes** > **Rôles des utilisateurs administratifs**.
    b. Cliquez sur **Ajouter**.
    c. Recherchez et sélectionnez un ou plusieurs utilisateurs.
    d. Sélectionnez **sms-administrator** et **Administrateur** dans la liste des rôles.

e. Cliquez sur **OK**.
f. Fermez la console.

20. Créez l'instance.
    a. Connectez-vous à la console Session Management Server en vous identifiant comme l'un des utilisateurs auxquels vous avez attribué les rôles **sms-administrator** et **Administrateur** à l'étape précédente. Voir «Connexion et déconnexion de la console Session Management Server», à la page 291 pour obtenir une assistance.
    b. Sélectionnez **Session Management Server** > **Déploiement**.
    c. Dans la zone **Nom d'application**, entrez le nom de l'application Session Management Server.
    d. Entrez l'élément de cellule WebSphere Application Server sur lequel l'instance de Session Management Server doit être déployée dans la zone **Cible**.
    e. Dans la zone **Hôte virtuel**, entrez les hôtes virtuels du serveur Web qui utiliseront l'instance de l'application Session Management Server.
    f. Entrez la source de données à utiliser avec l'instance de l'application Session Management Server dans la zone **Source de données**.
    g. Lorsque vous êtres prêt à effectuer le déploiement, cliquez sur **Déploiement**.

Que faire ensuite

Une fois l'instance déployée, vous devez la configurer. Consultez le manuel *IBM Security Access Manager for Web Shared Session Management Administration Guide* pour connaître les instructions de configuration.

Configuration d'un serveur de gestion de session à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques automatisent les installations et configurations sans assistance (en mode *silencieux*). Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Un serveur de gestion de sessions requiert WebSphere Application Server. Si WebSphere Application Server n'est pas déjà installé, installez-le et configurez-le d'après l'une des méthodes suivantes :

- «Installation de WebSphere Application Server», à la page 47 pour l'installation et la configuration manuelles.
- «Configuration de WebSphere Application Server à l'aide de fichiers scripts», à la page 210 pour automatiser l'installation et la configuration.

Configuration de WebSphere Application Server à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques peuvent automatiser les installations et configurations sans assistance (en mode *silencieux*).

Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation de WebSphere Application Server (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation de WebSphere Application Server sous AIX, Linux ou Solaris.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*). WebSphere Application Server est un produit prérequis pour les composants suivants :

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager est requis pour l'installation de WebSphere Application Server.

Procédure

1. Obtenez les fichiers d'installation de WebSphere Application Server et du référentiel du produit à partir de l'un des emplacements suivants :
   - Les supports produit de WebSphere Application Server fournis avec les DVD de Security Access Manager.
   - Le site Passport Advantage.
2. Copiez les fichiers de WebSphere Application Server sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
3. Extrayez dans un répertoire tous les fichiers de WebSphere Application Server à partir de leurs fichiers compressés.
4. Obtenez Installation Manager à partir de l'un des emplacements suivants :
   - Le site Passport Advantage.
   - Le site Web de téléchargement d'IBM Installation Manager :

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copiez les fichiers d'Installation Manager sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
6. Extrayez les fichiers Installation Manager dans son propre répertoire.
7. Copiez le fichier `install_was.sh` depuis le répertoire `scripts` situé sur le support du produit Security Access Manager et collez-le dans un emplacement temporaire sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
8. Copiez le fichier `WASInstall_*.xml` correspondant à votre plateforme depuis le répertoire `scripts` du Support de produit Security Access Manager vers le même emplacement temporaire que celui dans lequel vous avez copié le fichier `install_was.sh`. Les fichiers de réponses sont les suivants :

   Linux x86-64
   `WASInstall_linux_x86.xml`

   Linux s390
   `WASInstall_linux_s390x.xml`

   AIX `WASInstall_aix_ppc.xml`

   Solaris
   `WASInstall_solaris_sparc.xml`

9. Ouvrez la copie du fichier `install_was.sh` dans un éditeur de texte.
10. Modifier le chemin d'Installation Manager dans le fichier `install_was.sh` de manière à spécifier l'emplacement où se trouvent les images d'Installation Manager. Par exemple, modifiez la ligne suivante :

    ```
    INSTALL_MGR_DIR=/images/InstallationManager
    ```

11. Modifiez la variable `WAS_RESPONSE_FILE` de manière à spécifier le nom du fichier de réponses à utiliser lors de l'exécution du script. Utilisez le nom du fichier de réponses approprié pour votre plateforme :

    Linux x86-64
    `WASInstall_linux_x86.xml`

    Linux s390
    `WASInstall_linux_s390x.xml`

    AIX `WASInstall_aix_ppc.xml`

    Solaris
    `WASInstall_solaris_sparc.xml`

    Par exemple, sous Linux for x86-64, spécifiez :

    ```
    WAS_RESPONSE_FILE=./WASInstall_linux_x86.xml
    ```

12. Sauvegardez le fichier et fermez-le.
13. Ouvrez la copie du fichier `WASInstall_*.xml` dans un éditeur de texte.
14. Modifiez le chemin d'accès à l'emplacement du référentiel dans le fichier `WASInstall_*.xml` où se trouvent les images de WebSphere Application Server. Par exemple, modifiez la ligne suivante :

    ```
    <repository location='/images/WebSphere'/>
    ```

15. Facultatif : Modifiez l'emplacement dans lequel WebSphere Application Server est installé par le script. Les emplacements d'installation par défaut sont les suivants :

    Linux ou Solaris
    `/opt/IBM/WebSphere/AppServer`

    AIX `/usr/IBM/WebSphere/AppServer`

    Pour changer l'emplacement, modifiez les lignes suivantes dans le fichier `WASInstall_*.xml` :

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
       installLocation='/opt/IBM/WebSphere/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
    ```

16. Enregistrez le fichier de réponses.
17. Exécutez le fichier script.

    ```
    install_was.sh
    ```

Avertissement : Si vous spécifiez le nom d'un fichier de référentiel incorrect à l'étape 14, à la page 302, une erreur s'affiche. Répéter les instructions de modification indiquées à l'étape 14, à la page 302 de manière à corriger le nom de fichier du référentiel. Puis, supprimez le référentiel incorrect dans Installation Manager avant d'exécuter le script :

a. Sur une ligne de commande, placez-vous dans le répertoire d'installation d'Installation Manager :

   ```
   /opt/IBM/InstallationManager/eclipse
   ```

b. Exécutez `IBMIM`.

c. Supprimez le référentiel incorrect.

d. Exécutez à nouveau le script.

18. Une fois l'installation de WebSphere Application Server terminée, créez un profil d'Application Server en exécutant la commande WebSphere Application Server **manageprofiles**.

    Par exemple, tapez :

    ```
    /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -create -templatePath
    /opt/IBM/WebSphere/AppServer/profileTemplates/default
    ```

    Pour plus de détails sur la commande **manageprofiles**, consultez le centre de documentation de WebSphere Application Server :

    http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

19. Démarrez le serveur d'applications.

    Par exemple, tapez :

    ```
    /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/startServer.sh server1
    ```

20. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis.

    a. Localisez le groupe de correctifs sur la page de support de WebSphere Application Server. http://www.ibm.com/support/docview.wss?uid=swg27004980

    b. Téléchargez le groupe de correctifs et utilisez les instructions contenues dans le fichier Readme joint pour l'installer.

Que faire ensuite

Passez à l'étape «Automatisation de l'installation d'un serveur de gestion de sessions (AIX, Linux ou Solaris)», à la page 305.

Automatisation de l'installation de WebSphere Application Server (Windows)

Utilisez le fichier script pour automatiser l'installation de WebSphere Application Server sous Windows.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*). WebSphere Application Server est un produit prérequis pour les composants suivants:

- Web Portal Manager
- Attribute Retrieval Service
- Session Management Server

Installation Manager est requis pour l'installation de WebSphere Application Server.

Procédure

1. Obtenez les fichiers d'installation de WebSphere Application Server et du référentiel du produit à partir de l'un des emplacements suivants :
   - Les supports produit de WebSphere Application Server fournis avec les DVD de Security Access Manager.
   - Le site Passport Advantage.
2. Copiez les fichiers de WebSphere Application Server sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
3. Extrayez dans un répertoire tous les fichiers de WebSphere Application Server à partir de leurs fichiers compressés.
4. Obtenez Installation Manager à partir de l'un des emplacements suivants :
   - Le site Passport Advantage.
   - Le site Web de téléchargement d'IBM Installation Manager :

     http://www.ibm.com/support/entry/portal/All_download_links/Software/Rational/IBM_Installation_Manager
5. Copiez les fichiers d'Installation Manager sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
6. Extrayez les fichiers Installation Manager dans son propre répertoire.
7. Copiez le fichier `install_was.bat` depuis le répertoire `scripts` situé sur le support du produit Security Access Manager et collez-le dans un emplacement temporaire sur l'ordinateur sur lequel vous souhaitez installer WebSphere Application Server.
8. Copiez le fichier `WASInstall.xml` depuis le répertoire `scripts` du support de produit Security Access Manager vers le même emplacement temporaire que celui dans lequel vous avez copié le fichier `install_was.bat`.
9. Ouvrez la copie du fichier `install_was.bat` dans un éditeur de texte.
10. Modifier le chemin d'Installation Manager dans le fichier `install_was.bat` de manière à spécifier l'emplacement où se trouvent les images d'Installation Manager. Par exemple, modifiez la ligne suivante :

    ```
    set INSTALL_MGR_DIR=C:\images\Installation Manager
    ```
11. Sauvegardez le fichier et fermez-le.
12. Ouvrez la copie du fichier `WASInstall.xml` dans un éditeur de texte.
13. Modifiez le chemin d'accès à l'emplacement du référentiel dans le fichier `WASInstall.xml` où se trouvent les images de WebSphere Application Server. Par exemple, modifiez la ligne suivante :

    ```
    <repository location='C:\images\WebSphere'/>
    ```
14. Facultatif : Modifiez l'emplacement dans lequel WebSphere Application Server est installé par le script. Par exemple, modifiez les lignes suivantes :

    ```
    <profile id='IBM WebSphere Application Server Network Deployment V8.0'
      installLocation='C:\Program Files\IBM\WebSphere\AppServer'/>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
    ```
15. Exécutez le fichier script.

    ```
    install_was.bat
    ```
16. Une fois l'installation de WebSphere Application Server terminée, créez un profil d'Application Server en exécutant la commande WebSphere Application Server **manageprofiles**.

    Par exemple, tapez la commande ci-après.

```
C:\Program Files\IBM\WebSphere\AppServer\bin\manageprofiles.bat -create
  -templatePath "C:\Program Files\IBM\WebSphere\AppServer\
   profileTemplates\default"
```

Pour plus de détails sur la commande **manageprofiles**, consultez le centre de documentation de WebSphere Application Server :

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

17. Démarrez le serveur d'applications.

    Par exemple, tapez :

    ```
    C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\
    startServer.bat server1
    ```

18. Installez le groupe de correctifs le plus récent pour votre installation. Consultez la page relative à la configuration matérielle et logicielle requise dans le centre de documentation d'IBM Security Access Manager pour connaître le niveau du groupe de correctifs minimum requis.
    a. Localisez le groupe de correctifs sur la page de support de WebSphere Application Server. http://www.ibm.com/support/docview.wss?uid=swg27004980
    b. Téléchargez le groupe de correctifs et utilisez les instructions contenues dans le fichier Readme joint pour l'installer.

Que faire ensuite

Passez à l'étape «Automatisation de l'installation d'un serveur de gestion de sessions (Windows)», à la page 306.

Automatisation de l'installation d'un serveur de gestion de sessions (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation d'un serveur de gestion de sessions Security Access Manager.

Avant de commencer

Un serveur de gestion de sessions requiert WebSphere Application Server. Avant de commencer cette tâche, installez et configurez WebSphere Application Server, si ce n'est déjà fait. Utilisez l'une des tâches suivantes :

- «Installation de WebSphere Application Server», à la page 47 pour l'installation et la configuration manuelles.
- «Configuration de WebSphere Application Server à l'aide de fichiers scripts», à la page 300 pour automatiser l'installation et la configuration.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i SMS -d chemin_packages -a [accept|display]
   ```

où :

- `SMS` est le nom du composant.
- *`chemin_packages`* est l'emplacement des packages du composant d'installation.

  Par exemple, si vous effectuez l'installation à partir d'un DVD :

  AIX *`point_montage_dvd`*`/usr/sys/inst.images`

  Linux x86-64
  `/point_montage_dvd``/linux_x86`

  Linux on System z
  `/point_montage_dvd``/linux_x390`

  Solaris
  `/point_montage_dvd``/solaris`
- `-a [accept|display]`

  L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

Par exemple, sur Linux x86-64, entrez la commande suivante pour installer un serveur de gestion de sessions :

```
./install_isam.sh -i SMS -d /mnt/dvd/linux_x86 -a accept
```

Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l SMS
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur de gestion de sessions», à la page 307.

Automatisation de l'installation d'un serveur de gestion de sessions (Windows)

Utilisez le fichier script pour automatiser l'installation d'un serveur de gestion de sessions Security Access Manager sous Windows.

Avant de commencer

Un serveur de gestion de sessions requiert WebSphere Application Server. Avant de commencer cette tâche, installez et configurez WebSphere Application Server, si ce n'est déjà fait. Utilisez l'une des tâches suivantes :

- «Installation de WebSphere Application Server», à la page 47 pour l'installation et la configuration manuelles.
- «Automatisation de l'installation de WebSphere Application Server (Windows)», à la page 303 pour automatiser l'installation et la configuration.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i SMS /d chemin_packages
   ```

   où :

   - `SMS` est le nom du composant.
   - *`chemin_packages`* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.

   Par exemple, pour installer le serveur de gestion de sessions, entrez :

   ```
   install_isam.bat /i SMS /d c:\images_isam
   ```

   où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.
4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `/l`.

   ```
   install_isam.bat /l SMS
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'un serveur de gestion de sessions».

Automatisation de la configuration d'un serveur de gestion de sessions

Utilisez le fichier script pour automatiser l'installation d'un serveur de gestion de sessions.

Avant de commencer

- Effectuez l'installation du serveur de gestion de sessions. Voir :
  - «Automatisation de l'installation d'un serveur de gestion de sessions (Windows)», à la page 306
  - «Automatisation de l'installation d'un serveur de gestion de sessions (AIX, Linux ou Solaris)», à la page 305
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant. Deux fichiers sont nécessaires pour le serveur de gestion de sessions. Exécutez le script de déploiement en premier.

      AIX, Linux ou Solaris

      Répertoire : `/opt/PolicyDirector/example/config/`

      Modèle de déploiement : `deploy_sms.options.template`

      Modèle de configuration : `configure_sms.options.template`

      Windows

      Répertoire : `C:\Program Files\Tivoli\PDSMS\etc`

      Modèle de déploiement : `deploy_sms.options.template.cmd`

      Modèle de configuration : `configure_sms.options.template.cmd`

   b. Copiez les deux fichiers dans un répertoire temporaire. Vous pouvez copier les fichiers dans le répertoire temporaire, puis les renommer d'après les noms spécifiques à votre environnement.

      Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

   c. Modifiez le contenu des fichiers pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans les fichiers expliquent les paramètres et fournissent des exemples.

   d. Enregistrez les fichiers.

2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :
   a. Copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options. Le fichier est situé dans les emplacements suivants :

      AIX, Linux ou Solaris

      `/opt/PolicyDirector/example/config/`

      Windows

      `C:\Program Files\Tivoli\Policy Director\example\config\`

   b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.

   c. Revenez à ces instructions pour exécuter le script de configuration.

3. Copiez le fichier script depuis son emplacement d'origine vers le même répertoire que celui où vous avez copié les fichiers d'options. Les fichiers script se trouvent dans les emplacements suivants :

   AIX, Linux ou Solaris

   Répertoire : `/opt/PolicyDirector/example/config/`

   Nom de fichier : `configure_isam.sh`

   Windows

   Répertoire : `C:\Program Files\Tivoli\Policy Director\example\config\`

   Nom de fichier : `configure_isam.cmd`

4. Exécutez le script WebSphere Application Server **setupCmdLine** pour configurer l'environnement d'exécution correct pour l'outil de configuration du serveur Session Management Server.

   AIX

   ```
   . /usr/IBM/WebSphere/AppServer/profiles/nom_profil/bin/setupCmdLine.sh
   ```

   Linux ou Solaris

   ```
   . /opt/IBM/WebSphere/AppServer/profiles/nom_profil/bin/setupCmdLine.sh
   ```

   Windows

   ```
   C:\Program Files\IBM\WebSphere\AppServer\profiles\nom_profil\bin\setupCmdLine.bat
   ```

   où *nom_profil* est le nom de votre profil WebSphere Application Server, tel que `appsrv01`.

5. Exécutez le script de configuration et utilisez le fichier `deploy_sms.options` comme entrée.

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

   Par exemple :

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f my_deploy_sms.options
   ```

   Windows

   ```
   configure_isam.cmd -f my_deploy_sms.options.cmd
   ```

6. Exécutez le script de configuration et utilisez le fichier `configure_sms.options` comme entrée.

   AIX, Linux ou Solaris

   ```
   ./configure_isam.sh -f fichier_options
   ```

   Windows

   ```
   configure_isam.cmd -f fichier_options.cmd
   ```

   où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

Par exemple :

AIX, Linux ou Solaris

```
./configure_isam.sh -f my_configure_sms.options
```

Windows

```
configure_isam.cmd -f my_configure_sms.options.cmd
```

Chapitre 18. Configuration de la ligne de commande de gestion de session

Vous pouvez administrer le serveur de gestion de session via le composant Security Access Manager Session Management Command Line. Exécutez au choix l'utilitaire de ligne de commande **pdadmin** sur le serveur d'autorisations Security Access Manager spécifié, ou l'utilitaire **pdsmsadmin**.

Remarque : Si vous souhaitez utiliser **pdadmin** pour administrer le serveur de gestion de session, vous devez installer et configurer le serveur d'autorisation avant d'installer l'interface de ligne de commande.

Exigences de préinstallation

Avant d'installer et de configurer le serveur de gestion de sessions Security Access Manager via une lign de commande, vous devez effectuer plusieurs tâches de préinstallation.

- Lors de la configuration de Security Access Manager sur des systèmes d'exploitation Linux, l'exécution des scripts peut échouer avec un message indiquant que `/bin/ksh` est introuvable. Sur certaines versions de SUSE Linux Enterprise Server, l'installation basée sur Yast n'installe pas le shell Korn à l'emplacement `/bin/ksh`.

  Installez le fichier `pdksh .rpm` qui correspond au matériel sur lequel vous allez installer Security Access Manager. Le `.rpm` adéquat se trouve sur le support d'installation de SUSE Linux Enterprise Server ou peut être téléchargé à partir des sites Web de support de SUSE Linux Enterprise Server ou de Novell.
- La configuration requiert le nom et le numéro de port du serveur Web utilisé pour accéder au serveur WebSphere Application Server qui héberge le serveur session management server.
- Déterminez si vous souhaitez activer SSL (Secure Sockets Layer) pour les communications avec l'interface de ligne de commande de gestion de sessions. Vous pouvez activer SSL entre Session Management Server et Security Access Manager authorization server pour que toutes les communications de la commande **pdadmin** soient sécurisées.
- Si vous prévoyez d'utiliser l'utilisateur Security Access Manager `sec_master` (ou d'autres utilisateurs et groupes définis dans le suffixe `secAuthority=Default`) pour administrer SMS à l'aide de session management command line, annulez la configuration du nom distinctif de base dans le registre d'utilisateurs LDAP utilisé par WebSphere Application Server.

  Des informations sur la modification du nom distinctif de base pour le registre d'utilisateurs de WebSphere Application Server sont disponibles dans le centre de documentation WebSphere Application Server dans la rubrique consacrée à la configuration de Lightweight Directory Access Protocol, à l'adresse :

  http://www.ibm.com/software/webservers/appserv/was/library/

© Copyright IBM Corp. 2001, 2013

Configuration du serveur de gestion de sessions via les utilitaires de ligne de commande

Vous pouvez installer et configurer un système de gestion de session Security Access Manager via une ligne de commande en utilisant la ligne de commande.

Pour configurer le système de gestion de session via une ligne de commande, utilisez l'utilitaire **pdsmsclicfg**. Si vous souhaitez administrer le serveur de gestion de sessions à l'aide de l'utilitaire **pdadmin**, exécutez la commande **pdsmsclicfg** depuis le système qui héberge le serveur d'autorisations. L'utilitaire **pdsmsclicfg** écrit dans le fichier de configuration du serveur d'autorisation hôte, `ivacld.conf`

Vous pouvez configurer un système de gestion de sessions via une ligne de commande en utilisant l'une des méthodes d'installation suivantes.

Exécutez les instructions qui s'appliquent à votre système d'exploitation.

Remarque : Les packages Security Access Manager Runtime (PD.RTE) et Security Access Manager Authorization Server (PD.Acld) sont uniquement requis si vous souhaitez effectuer l'administration à l'aide de l'utilitaire **pdadmin**.

AIX : Installation de la ligne de commande de gestion des sessions

Utilisez le programme **installp** pour installer les progiciels et l'utilitaire **pdsmsclicfg** pour les configurer sous AIX.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 311.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit) s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Global Security Kit (GSKit)», à la page 35.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «AIX : Installation du client IBM Tivoli Directory Server», à la page 44.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «AIX : Installation d'IBM Security Utilities», à la page 40.
9. Installez les packages Security Access Manager suivants :

   ```
   installp -acgYXd chemin_package/usr/sys/inst.images packages
   ```

où :

- *chemin_package* est le répertoire dans lequel le DVD est monté ou dans lequel se trouvent les fichiers
- *packages* représente les packages suivants :

  PD.RTE Spécifie le package Security Access Manager Runtime.

  PD.Acld
  Indique le package Security Access Manager Authorization Server.

  PD.SMSCLI
  Spécifie le package Security Access Manager Session Management Server Command Line.

10. Démontez, le cas échéant, le DVD.
11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
12. Configurez les packages Security Access Manager Runtime et Security Access Manager Authorization Server packages comme suit :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer, l'un après l'autre.
       Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, appuyez sur **Entrée** pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.
13. Configurez le package Security Access Manager Session Management Command Line en exécutant l'utilitaire **pdsmsclicfg** :

    ```
    pdsmsclicfg –action config
    ```

    Pour obtenir de l'aide sur les options de configuration, consultez le manuel *IBM Security Access Manager for Web Command Reference*.
14. Vous devez démarrer manuellement le serveur d'autorisations qui héberge session management command line après la configuration.

Résultats

Cette étape termine la configuration du système de gestion via une ligne de commande de Security Access Manager Session Management Server. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Linux : Installation de la ligne de commande de gestion des sessions

Utilisez le programme **rpm** pour installer les progiciels et l'utilitaire **pdsmsclicfg** pour les configurer sous Linux.

Pourquoi et quand exécuter cette tâche

Remarque à l'attention des utilisateurs de Linux sur System z : Vous devez tout d'abord obtenir l'accès aux fichiers `rpm` Linux qui se trouvent dans le répertoire */chemin_package*/`linux_s390`.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 311.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Accédez au répertoire *chemin_package*/*distribution*,

   où :

   - *chemin_package* est le point de montage de votre lecteur de DVD ou l'emplacement des fichiers
   - *distribution* spécifie `linux_x86` pour x86-64 ou `linux_s390` pour System z
6. Installez IBM Global Security Kit (GSKit) s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Global Security Kit (GSKit)», à la page 36.
7. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Linux : Installation du client IBM Tivoli Directory Server», à la page 45.
8. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
9. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Linux : Installation d'IBM Security Utilities», à la page 41.
10. Installez les packages Security Access Manager :

    `rpm -ihv` *packages*

    où *packages* désigne les packages suivants :

Package	Linux sur x86-64	Linux on System z
Package Security Access Manager Runtime	`PDRTE-PD-7.0.0-0.x86_64.rpm`	`PDRTE-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Authorization Server	`PDAcld-PD-7.0.0-0.x86_64.rpm`	`PDAcld-PD-7.0.0-0.s390.rpm`
Package Security Access Manager Session Management Command Line	`PDSMS-CLI-7.0.0-0.x86_64.rpm`	`PDSMS-CLI-7.0.0-0.s390.rpm`

11. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

12. Configurez les packages Security Access Manager Runtime et Access Manager Authorization Server de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
       Sélectionnez le numéro de menu du package à configurer.
       Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.
13. Configurez le package Security Access Manager Session Management Command Line en exécutant l'utilitaire **pdsmsclicfg** :

    ```
    pdsmsclicfg –action config
    ```

    Pour plus d'informations sur ces options de configuration, consultez le manuel *IBM Security Access Manager for Web Command Reference*.
14. Démarrez manuellement le serveur d'autorisations qui héberge session management command line après la configuration.

Résultats

Lorsqu'un message s'affiche indiquant que le package a été configuré avec succès, sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système de gestion via une ligne de commande de Security Access Manager Session Management Server. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Solaris : Installation de session management command line

Utilisez **pkgadd** pour installer les progiciels et l'utilitaire **pdsmsclicfg** pour les configurer sur Solaris.

Pourquoi et quand exécuter cette tâche

Avertissement : Si vous procédez à une installation sur des systèmes Solaris, utilisez l'option **-G** avec l'utilitaire **pkgadd**. L'option **-G** ajoute le package uniquement dans la zone en cours.

Procédure

1. Connectez-vous en tant qu'utilisateur **root**.
2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 311.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit) s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Global Security Kit (GSKit)», à la page 37.

6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, si ce n'est déjà fait. Pour obtenir des instructions, voir la page «Solaris : Installation du client IBM Tivoli Directory Server», à la page 46.
7. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «AIX, Linux, Solaris : Installation de la licence IBM Security Access Manager», à la page 38.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Solaris : Installation d'IBM Security Utilities», à la page 42.
9. Installez les packages Security Access Manager :

   ```
   pkgadd -d /chemin_package/solaris -a /chemin_package/solaris/pddefault
   -G packages
   ```

   où :

   /*chemin_package*/solaris
   Indique l'emplacement du package.

   /*chemin_package*/solaris/pddefault
   Indique l'emplacement du script d'administration de l'installation.

   et où les *packages* sont les suivants :

   PDRTE Spécifie le package Security Access Manager Runtime.

   PDAcld Indique le package Security Access Manager Authorization Server.

   PDSMSCLI
   Spécifie le package Security Access Manager Session Management Command Line.

   Lorsque le processus d'installation est terminé pour chaque package, le message suivant s'affiche :

   ```
   Installation of package successful.
   ```
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.
11. Configurez les packages Security Access Manager Runtime et Access Manager Authorization Server de la manière suivante :
    a. Démarrez l'utilitaire de configuration comme suit.

       ```
       pdconfig
       ```

       Le menu d'installation de Security Access Manager s'affiche.
    b. Entrez le numéro de menu 1 pour **Configuration du module**. Le menu de configuration de Security Access Manager s'affiche.
    c. Sélectionnez le numéro de menu du package à configurer.
12. Configurez le package Security Access Manager Session Management Command Line en exécutant l'utilitaire **pdsmsclicfg** :

    ```
    pdsmsclicfg –action config
    ```

    Pour plus d'informations sur ces options de configuration, consultez le manuel *IBM Security Access Manager for Web Command Reference*.
13. Vous devez démarrer manuellement le serveur d'autorisations qui héberge session management command line après la configuration.

Résultats

Lorsqu'un message est affiché signalant que le package a été configuré, appuyez sur Entrée pour configurer un autre package ou sélectionnez l'option **x** deux fois pour fermer l'utilitaire de configuration.

Cette étape termine la configuration du système de gestion via une ligne de commande de Security Access Manager Session Management Server. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Windows : Installation de la ligne de commande de gestion des sessions

Utilisez le programme **setup.exe** pour installer les progiciels et l'utilitaire **pdsmsclicfg** pour les configurer sous Windows.

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de droits d'administrateur.
2. Effectuez les tâches de préinstallation répertoriées dans «Exigences de préinstallation», à la page 311.
3. Vérifiez que le serveur de registre et le serveur de règles sont allumés et en cours d'exécution (en mode normal).
4. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers ne comporte aucun espace.
5. Installez IBM Global Security Kit (GSKit), s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Global Security Kit (GSKit)», à la page 37.
6. Si vous utilisez un registre d'utilisateurs basé sur LDAP, installez le client IBM Tivoli Directory Server, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation du client IBM Tivoli Directory Server», à la page 47.
7. Installez la licence de Security Access Manager, si ce n'est déjà fait. Pour plus d'instructions, voir «Windows : Installation de la licence IBM Security Access Manager», à la page 40.
8. Installez IBM Security Utilities, s'il ne l'est pas déjà. Pour obtenir des instructions, voir la page «Windows : Installation d'IBM Security Utilities», à la page 42.
9. Installez les packages Security Access Manager. Pour ce faire, exécutez le programme **setup.exe** à partir du répertoire suivant `:\windows\PolicyDirector\Disk Images\Disk1`
   Suivez les instructions en ligne et choisissez d'installer le package suivant :
   - Access Manager Session Management Command Line

     En outre, sélectionnez les packages suivants si l'infrastructure de Security Access Manager (**pdadmin**) est utilisés pour gérer le serveur de gestion de sessions :
   - Security Access Manager Runtime
   - Security Access Manager Authorization Server
10. Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue

nationale *avant* de configurer les packages. Pour plus d'instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

11. Configurez les packages de l'une des manières suivantes :
    - Si vous utilisez l'infrastructure de Security Access Manager session Management pour gérer le serveur de gestion de sessions, exécutez l'utilitaire de configuration graphique **pdconfig**.
      a. Ouvre une nouvelle fenêtre de ligne de commande.
      b. Démarrez l'utilitaire. Entrez : `pdconfig`
      c. Si vous avez installé le composant Runtime, sélectionnez le package **Security Access Manager Runtime**.
      d. Cliquez sur **Configurer**.
      e. Si vous avez installé le composant Authorization Server, sélectionnez le package **Security Access Manager Authorization Server**.
      f. Cliquez sur **Configurer**.
      g. Sélectionnez la package **Session Management Server Command Line Interface**.
      h. Cliquez sur **Configurer**.
    - Sinon, exécutez l'utilitaire de configuration graphique **pdsmsclicfg** : `pdsmsclicfg`. Pour plus d'informations sur ces options de configuration, consultez le manuel *IBM Security Access Manager for Web Command Reference*.

    Vous êtes invité à entrer les options de configuration.

Résultats

Cette étape termine la configuration du système de gestion via une ligne de commande de Security Access Manager Session Management Server. Pour configurer un autre système Security Access Manager, suivez la procédure indiquée dans Chapitre 3, «Organigramme d'installation», à la page 21.

Configuration d'une ligne de commande de gestion de sessions avec le tableau de bord (Windows)

Utilisez la méthode d'installation du tableau de bord pour installer et configurer le logiciel de ligne de commande de gestion de sessions sous Windows au moyen d'une interface graphique.

Avant de commencer

Assurez-vous d'avoir effectué les tâches prérequises suivantes :

- «Préparation du système d'exploitation», à la page 28
- Si vous envisagez d'utiliser un registre d'utilisateurs autre qu'IBM Tivoli Directory Server, passez à l'étape Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Pourquoi et quand exécuter cette tâche

Le tableau de bord utilise une interface graphique pour effectuer l'installation étape par étape et la configuration initiale.

Cette tâche installe les composants suivants :

- IBM GSKit

- Client IBM Tivoli Directory Server
- IBM Security Utilities
- Security Access Manager License
- Security Access Manager Runtime
- Security Access Manager Authorization Server
- Security Access Manager Session Management Command Line

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.

   Avertissement : Assurez-vous que le chemin de répertoire des fichiers image du tableau de bord ne comporte aucun espace.
2. Lancez le tableau de bord.
   a. Recherchez le fichier `launchpad64.exe`.
   b. Cliquez deux fois sur ce fichier pour lancer le tableau de bord.
3. Sélectionnez la langue à utiliser durant l'installation.
4. Cliquez sur **OK**. La fenêtre de bienvenue du tableau de bord s'affiche.
5. Cliquez sur **Suivant**.
6. Sélectionnez le composant **Session Management Server Command Line Interface**.
7. Cliquez sur **Suivant**. Une liste affiche le composant que vous avez sélectionné, ainsi que tous les logiciels prérequis que requiert ce composant mais qui ne sont pas encore installés.
8. Cliquez sur **Suivant**. Une flèche à gauche du nom d'un composant indique que ce composant est en cours d'installation. Une coche en regard d'un nom de composant signifie que ce composant est installé.
9. Si le composant courant est IBM Global Security Kit, cliquez sur **Installer IBM Global Security Kit** pour l'installer. Une fois l'opération terminée, passez à l'étape 10.
10. Cliquez sur **Suivant**.
11. Répondez aux invites qui s'affichent au cours de l'installation.
12. Cliquez sur **Suivant** dans la partie inférieure du tableau de bord pour continuer.
13. Terminez l'installation.
    - Si l'installation échoue, corrigez l'erreur décrite dans le message d'erreur et relancez le tableau de bord.
    - Si l'installation a abouti, passez à l'étape 14.
14. Cliquez sur **Suivant** pour commencer la configuration.

    Remarque : L'outil de configuration est affiché dans la langue que vous avez sélectionnée pour l'environnement local de votre système d'exploitation. Si l'outil est affiché en anglais et non dans la langue de votre système d'exploitation, consultez le journal d'installation du module de langue : `%USERPROFILE%\ISAMLangPacksInstall.log`. Corrigez les éventuelles erreurs signalées dans le fichier journal. Installez ensuite le module de langue, comme décrit à la section Annexe E, «Installation du support de langue», à la page 363.
15. Cliquez sur **Configurer la ligne de commande du serveur de gestion de sessions**. L'outil de configuration s'affiche.

16. Sélectionnez le composant
17. Cliquez sur **Configurer**.
18. Terminez la configuration. Pour obtenir de l'aide, voir Annexe D, «Options pdconfig», à la page 339. Lorsque toutes les installations et toutes les configurations sont terminées, un message s'affiche pour indiquer si l'opération a abouti ou échoué.
19. Effectuez l'une des actions suivantes :
    - Si la configuration a abouti, cliquez sur **Suivant**.
    - Si la configuration a échoué ou si une erreur est affichée, consultez le fichier journal à l'emplacement par défaut `%USERPROFILE%` (par exemple, `C:\Users\Administrator\LaunchPDConfigforISAM.log`).

      Apportez les corrections indiquées dans le fichier journal. Configurez ensuite le composant en utilisant l'utilitaire **pdconfig** dans une invite de ligne de commande ou en cliquant sur **Démarrer** > **Programmes** > **IBM Security Access Manager for Web** > **Configuration**.
20. Cliquez sur **Terminer** pour fermer le tableau de bord.

Configuration d'une ligne de commande de gestion de sessions à l'aide de fichiers scripts

Les scripts d'installation et de configuration automatiques automatisent les installations et configurations sans assistance (en mode *silencieux*). Utilisez les scripts tels qu'ils sont fournis ou modifiez-les pour répondre aux exigences de votre environnement.

Automatisation de l'installation d'une ligne de commande de gestion de sessions (AIX, Linux ou Solaris)

Utilisez le fichier script pour automatiser l'installation de la ligne de commande de gestion de sessions.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.sh` dans le répertoire `scripts`.
3. Exécutez le script comme suit :

   ```
   ./install_isam.sh -i SMSCLI -d chemin_packages -a [accept|display]
   ```

   où :
   - `SMSCLI` est le nom du composant.
   - *`chemin_packages`* est l'emplacement des packages du composant d'installation. Par exemple, si vous effectuez l'installation à partir d'un DVD :

     AIX *`point_montage_dvd`*`/usr/sys/inst.images`

     Linux x86-64
     `/point_montage_dvd``/linux_x86`

Linux on System z
/point_montage_dvd/linux_s390

Solaris
/point_montage_dvd/solaris

- `-a [accept|display]`

  L'option `-a accept` permet d'accepter automatiquement la licence dans l'afficher. L'option `-a display` affiche la licence, que vous devez accepter manuellement.

Par exemple, sur Linux x86-64, entrez la commande suivante pour installer un serveur de gestion de sessions :

```
./install_isam.sh -i SMSCLI -d /mnt/dvd/linux_x86 -a accept
```

Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `-l`.

   ```
   ./install_isam.sh -l SMSCLI
   ```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'une ligne de commande de gestion de sessions», à la page 322.

Automatisation de l'installation d'une ligne de commande de gestion de sessions (Windows)

Utilisez le fichier script pour automatiser l'installation d'une ligne de commande de gestion de session pour Security Access Manager sous Windows.

Pourquoi et quand exécuter cette tâche

Les installations automatisées permettent d'effectuer des installations sans surveillance (*en mode silencieux*).

Avertissement : Le script d'installation requiert des droits d'administrateur. Exécutez la commande du fichier script, `install_isam.bat`, après vous être connecté avec un ID administrateur ou à partir de la ligne de commande, ouverte avec **Exécuter en tant qu'administrateur**.

Procédure

1. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
2. Recherchez le fichier script `install_isam.bat` dans le répertoire `scripts`. Ce répertoire se trouve sur le DVD du produit ou dans le répertoire dans lequel vous avez extrait les fichiers du produit. Assurez-vous que le fichier `.bat` et tous les fichiers `.iss` se trouvent dans le même répertoire.
3. Exécutez le script comme suit :

   ```
   install_isam.bat /i SMSCLI /d chemin_packages
   ```

   où :

   - `SMSCLI` est le nom du composant.

- *chemin_packages* correspond au chemin d'accès au DVD du produit ou au répertoire dans lequel vous avez extrait les fichiers du produit.

Par exemple, pour installer la ligne de commande de gestion de sessions, entrez :

```
install_isam.bat /i SMSCLI /d c:\images_isam
```

où `c:\images_isam` est le répertoire dans lequel se trouvent les sous-répertoires et les fichiers du produit extraits. Le script associé à chaque composant installe tous les prérequis pour ce composant. Si les prérequis sont déjà installés, le script passe à l'installation du composant suivant.

4. Facultatif : Pour afficher la liste des packages requis sans les installer, utilisez l'option `/l`.

```
install_isam.bat /l SMSCLI
```

Que faire ensuite

Une fois l'installation terminée, passez à l'étape «Automatisation de la configuration d'une ligne de commande de gestion de sessions».

Automatisation de la configuration d'une ligne de commande de gestion de sessions

Utilisez le fichier script pour automatiser la configuration de la ligne de commande de gestion de sessions.

Avant de commencer

- Effectuez l'installation de la ligne de commande de gestion de sessions. Voir :
  - «Automatisation de l'installation d'une ligne de commande de gestion de sessions (Windows)», à la page 321
  - «Automatisation de l'installation d'une ligne de commande de gestion de sessions (AIX, Linux ou Solaris)», à la page 320
- Pour afficher le statut et les messages dans une autre langue que l'anglais, qui est la langue par défaut, installez votre programme de support de langue nationale *avant* de configurer les packages. Pour obtenir des instructions, voir «Installation des modules de support de langue dans Security Access Manager», à la page 364.

Si vous exécutez ce script sous Windows, ouvrez une nouvelle fenêtre de commande. N'effectuez pas cette tâche dans la même fenêtre que celle dans laquelle vous avez lancé le script d'installation.

Pourquoi et quand exécuter cette tâche

La configuration automatisée permet d'effectuer une configuration sans assistance (*en mode silencieux*).

Procédure

1. Créez un fichier d'options pour le composant que vous souhaitez configurer.
   a. Recherchez le modèle de fichier d'options pour le composant.

      AIX, Linux ou Solaris

      ```
      /opt/PolicyDirector/example/config/
      configure_smscli.options.template
      ```

Windows

```
C:\Program Files\Tivoli\PDSMS\etc\
configure_smscli.options.template.cmd
```

b. Copiez le fichier dans un répertoire temporaire. Vous pouvez copier le fichier dans un répertoire temporaire ayant un nom unique pour votre environnement.

Avertissement : Vous devez conserver l'extension `.cmd` pour les fichiers modèles Windows. Les fichiers modèles Windows sont exécutés en tant que commandes.

c. Modifiez le contenu du fichier pour spécifier les paramètres correspondant à votre environnement. Les commentaires présents dans le fichier expliquent les paramètres et fournissent des exemples.

d. Sauvegardez le fichier.

2. Facultatif : Par défaut, les mots de passe que vous spécifiez dans les fichiers d'options sont stockés sous la forme de texte en clair. Pour masquer ces mots de passe :

a. Copiez le fichier `configure_isam.conf` dans le même répertoire que celui où vous avez copié les fichiers d'options. Le fichier est situé dans les emplacements suivants :

AIX, Linux ou Solaris

```
/opt/PolicyDirector/example/config/
```

Windows

```
C:\Program Files\Tivoli\Policy Director\example\config\
```

b. Voir Annexe F, «Gestion des mots de passe», à la page 375 pour obtenir des instructions sur l'utilisation de l'option `-obfuscate` avec l'outil `pdconf` pour masquer les mots de passe dans les fichiers d'option. Pour plus d'informations sur `pdconf`, voir : *IBM Security Access Manager for Web Command Reference*.

c. Revenez à ces instructions pour exécuter le script de configuration.

3. Copiez le fichier script depuis son emplacement d'origine vers le même répertoire que celui où vous avez copié les fichiers d'options. Les fichiers script se trouvent dans les emplacements suivants :

AIX, Linux ou Solaris

Répertoire : `/opt/PolicyDirector/example/config/`

Nom de fichier : `configure_isam.sh`

Windows

Répertoire : `C:\Program Files\Tivoli\Policy Director\example\config\`

Nom de fichier : `configure_isam.cmd`

4. Exécutez le script de configuration et le fichier d'options.

AIX, Linux ou Solaris

```
./configure_isam.sh -f fichier_options
```

Windows

```
configure_isam.cmd -f fichier_options.cmd
```

où *fichier_options* et *fichier_options*`.cmd` sont les fichiers texte contenant les options de configuration.

Par exemple :

AIX, Linux ou Solaris

```
./configure_isam.sh -f my_configure_smscli.options
```

Windows

```
configure_isam.cmd -f my_configure_smscli.options.cmd
```

Partie 6. Annexes

© Copyright IBM Corp. 2001, 2013

Annexe A. Configuration de la sécurité SSL (Secure Sockets Layer)

Vous pouvez activer la sécurité SSL (Secure Sockets Layer) entre les serveurs Security Access Manager et votre serveur de registre d'utilisateurs.

Lorsque SSL est activé, les données échangées entre les serveurs Security Access Manager et le serveur de registre d'utilisateurs sont chiffrées. L'authentification de serveur et de client sont prises en charge.

Lorsque vous activez les communications SSL, vous configurez SSL sur les systèmes suivants dans l'ordre indiqué :

1. Le serveur du registre d'utilisateurs. Pour plus d'informations, voir Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.
2. Chaque instance de serveur Security Access Manager.
3. Tout autre système qui communique avec le serveur du registre d'utilisateurs via le client IBM Tivoli Directory Server.

Configuration de SSL sur les serveurs Security Access Manager

Après avoir activé l'accès SSL sur le serveur LDAP, vous pouvez configurer l'accès SSL sur les systèmes clients. Dans ce contexte, ce sont les *systèmes clients* sur lesquels s'exécutent les composants Security Access Manager.

Vous devez créer un fichier de base de données de clés sur le système client afin de stocker le certificat de signataire du serveur LDAP. Le certificat signataire est soit le certificat autosigné, soit un certificat de serveur est émis par une autorité de certification (CA). Le client SSL LDAP valide le certificat de serveur LDAP en garantissant que celui-ci est signé par l'un des certificats de signataires dans sa base de données de clés.

Le processus de configuration d'un système client est le suivant :

1. «Création d'une base de données et ajout du certificat de signataire».
2. «Configuration des communications SSL», à la page 328.
3. «Test de l'accès SSL», à la page 329.

Création d'une base de données et ajout du certificat de signataire

Créez un fichier de clés sur le client et ajoutez le certificat de signataire à partir du serveur LDAP à l'aide de l'utilitaire de gestion des clés GSKit, **GSKCapiCmd**.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur **GSKCapiCmd**, voir le manuel *GSKCapiCmd User's Guide*.

Procédure

1. Ouvrez une invite de commande.
2. Localisez le fichier **gsk8capicmd_64** dans le répertoire d'installation de GSKit et placez-vous dans ce répertoire.

© Copyright IBM Corp. 2001, 2013

3. Exécutez la commande **gsk8capicmd_64** pour créer la base de données de clés. Par exemple, tapez :

```
gsk8capicmd_64 -keydb -create -db /key/isam.kdb -pw passw0rd
  -type cms -stash -empty
```

4. Ajoutez le certificat de serveur LDAP à la base de données de clés.
   a. Copiez le certificat de signataire sur le système client.
      - Si le serveur utilise un certificat émis par une autorité de certification (AC), copiez le fichier contenant le certificat de signataire vers le système client.
      - Si le serveur utilise un certificat autosigné, copiez le certificat que vous avez extrait du fichier de base de données de clés sur le serveur sur le système client.

   b. Exécutez la commande **gsk8capicmd_64** pour ajouter le certificat de signataire à la base de données de clés. Par exemple, pour ajouter un certificat de signataire au format ASCII PEM, saisissez :

```
gsk8capicmd_64 -cert -add -db /key/isam.kdb -pw passw0rd -type cms -file
  /temp/LDAPserver-cert.pem -trust enable -format ascii -label ldapsigner
```

5. Vérifiez que l'accès SSL a été activé. Entrez la commande suivante sur le système Security Access Manager sur lequel vous avez configuré SSL :

```
idsldapsearch -h nom_serveur -Z -K fichier_clés_client
-P motdepasse_fichier_clés
-p port_ldap -b "" -s base objectclass=*
```

   Les variables de commande sont les suivantes :

   nom_serveur
   Nom d'hôte DNS du serveur LDAP.

   fichier_clés_client
   Nom de chemin qualifié complet de la base de données de clés générée pour le client.

   motdepasse_fichier_clés
   Mot de passe du fichier de la base de données de clés généré.

   -p *port_ldap*
   Désigne le porte d'écoute du serveur LDAP. S'il n'est pas spécifié, la valeur par défaut du port SSL LDAP 636 est utilisée.

   -Z Indique que SSL doit être utilisé pour établir la connexion avec le serveur LDAP.

   Cette commande renvoie les informations de base de LDAP, qui incluent les suffixes du serveur LDAP.

Que faire ensuite

Passez à l'étape «Configuration des communications SSL».

Configuration des communications SSL

Utilisez l'utilitaire **pdconfig** de Security Access Manager pour déconfigurer puis reconfigurer un composant Security Access Manager.

L'utilitaire **pdconfig** de Security Access Manager est utile lorsque vous :

- N'avez pas activé SSL.
- Souhaitez modifier la configuration SSL. Vous pouvez par exemple sélectionner un autre fichier de base de données de clés ou spécifier un autre label de certificat.

Pour obtenir une description des options de configuration, voir «Security Access Manager Runtime : LDAP», à la page 339.

Plusieurs valeurs sont requises par la configuration. La plupart proviennent des précédentes tâches de configuration SSL. L'une d'elles (un numéro de port) provient du serveur LDAP.

Tableau 19. Valeurs de configuration SSL

Valeurs de configuration SSL	Descriptions et exemples
Nom du fichier de clés SSL et chemin complet Le fichier et l'emplacement du fichier de clés que vous avez créé sur le composant Security Access Manager.	`/key/isam.kdb`
Mot de passe du fichier des clés SSL Le mot de passe du fichier de clés.	`passw0rd`
Port SSL du serveur LDAP La valeur du port sécurisé du serveur du registre d'utilisateurs.	`636`
Libellé de certificat Le label est affecté lorsque le certificat serveur est importé dans la base de données de clés client.	`sds`

Test de l'accès SSL

Testez l'accès à SSL pour vous assurer que la configuration est terminée.

Entrez la commande suivante sur le système Security Access Manager sur lequel vous avez configuré SSL :

```
idsldapsearch -h nom_serveur -Z -K fichier_clés_client
-P motdepasse_fichier_clés
-p port_ldap -b "" -s base objectclass=*
```

Les variables de commande sont les suivantes :

nom_serveur
: Nom d'hôte DNS du serveur LDAP.

fichier_clés_client
: Nom de chemin qualifié complet de la base de données de clés générée pour le client.

motdepasse_fichier_clés
: Mot de passe du fichier de la base de données de clés généré.

-p *port_ldap*
: Désigne le porte d'écoute du serveur LDAP. S'il n'est pas spécifié, la valeur par défaut du port SSL LDAP 636 est utilisée.

-Z
: Indique que SSL doit être utilisé pour établir la connexion avec le serveur LDAP.

Cette commande renvoie les informations de base de LDAP, qui incluent les suffixes du serveur LDAP.

Configuration du client Tivoli Directory Server pour l'authentification de client

Lors de la configuration de votre serveur LDAP en vue d'activer l'accès SSL, vous devez choisir entre *l'authentification serveur* et *l'authentification serveur et client*. Si vous avez choisi l'*authentification serveur et client*, vous devez créer un certificat pour le système client (c'est-à-dire le système de composants Security Access Manager). Avec ce mode d'authentification, une fois le serveur authentifié par le client, le serveur demande le certificat du client et l'utilise pour vérifier son identité.

Avant de commencer

Installez et configurez le client Tivoli Directory Server sur l'ordinateur sur lequel sont installés vos composants Security Access Manager.

Pourquoi et quand exécuter cette tâche

Les étapes générales suivantes sont requises pour activer l'authentification de client sur Security Access Manager. Consultez les informations relatives à la sécurisation des communications dans le manuel *IBM Tivoli Directory Server Administration Guide* afin de connaître les détails de chaque étape.

Procédure

1. Effectuez *l'une* des actions suivantes :
   - Demandez un certificat personnel à une autorité de certification (AC) et enregistrez-le dans le fichier de la base de données de clés. Il peut également s'avérer utile d'ajouter un certificat de signataire au fichier de la base de données de clés.
   - Créez un certificat autosigné, extrayez-le et mettez-le à disposition sur tous les systèmes clients qui communiquent de façon sécurisée avec le serveur.
2. Créez la base de données de clés, le fichier de mot de passe secret associé, ainsi que le mot de passe, sur le système client. Par exemple, utilisez **gsk8capicmd** pour créer la base de données, le fichier de dissimulation et le mot de passe.
3. Après avoir créé le fichier de base de données de clés sur le système client, définissez l'utilisateur `ivmgr` et le groupe `ivmgr` comme propriétaires du fichier de la base de données de clés. Utilisez la commande de système d'exploitation appropriée pour modifier la propriété du fichier. Par exemple, sur les systèmes AIX, Linux et Solaris, entrez la commande suivante : `chown ivmgr:ivmgr fichier_de_clés_client`
4. Entrez ce certificat dans la base de données de clés.
5. Configurez le client Tivoli Directory Server et activez SSL.
6. Copiez le certificat de signataire sur l'ordinateur Tivoli Directory Server avec lequel vous souhaitez activer les communications SSL.

Que faire ensuite

Passez à l'étape «Test de l'accès SSL lors de l'utilisation de l'authentification de serveur et de client», à la page 331.

Test de l'accès SSL lors de l'utilisation de l'authentification de serveur et de client

Une fois que le serveur LDAP reconnaît le certificat personnel du client, testez l'accès SSL.

Exécutez la commande suivante sur le client LDAP :

```
idsldapsearch -h nom_serveur -Z -K fichier_clés_serveur
-P motdepasse_fichier_clés -N \
libellé_client -p port_ldap -b "" -s base objectclass=*
```

Les variables de commande sont les suivantes :

nom_serveur
: Nom d'hôte DNS du serveur LDAP.

fichier_clés_client
: Nom de chemin qualifié complet de la base de données de clés générée pour le client.

motdepasse_fichier_clés
: Mot de passe du fichier de la base de données de clés généré.

libellé_client
: Le libellé associé à la clé, s'il existe. Cette zone est requise uniquement lorsque le serveur LDAP est configuré pour effectuer l'authentification de serveur et de clients.

-p *port_ldap*
: Désigne le porte d'écoute du serveur LDAP. S'il n'est pas spécifié, la valeur par défaut du port SSL LDAP 636 est utilisée.

-Z
: Indique que SSL doit être utilisé pour établir la connexion avec le serveur LDAP.

La commande **idsldapsearch** renvoie les informations de base de LDAP, qui incluent les suffixes du serveur LDAP. Notez que le paramètre **–N** indique le libellé spécifié lors de l'ajout du certificat personnel du client au fichier de la base de données de clés du client.

Remarque : *Ne spécifiez pas le libellé du certificat de signataire du serveur LDAP.* L'option **–N** indique au GSKit quel certificat de client est envoyé au serveur lorsqu'il est demandé. Si aucun libellé n'est spécifié, le certificat personnel par défaut est envoyé lorsque le serveur demande le certificat du client.

Annexe B. Identités des groupes et administrateurs sur les systèmes AIX, Linux et Solaris

Les ID utilisateur et les groupes sont créés automatiquement par le processus d'installation s'ils n'existent pas encore. Si vous souhaitez attribuer des ID groupe spécifiques ou des ID utilisateur à ces groupes et ces utilisateurs, vous pouvez les créer avant l'installation.

Le tableau 20 répertorie les ID utilisateur et les groupes utilisés par Security Access Manager et ses logiciels prérequis lors de l'installation sur les systèmes AIX, Linux ou Solaris.

Tableau 20. Utilisateurs et groupes requis par Security Access Manager

ID	Type	Description	Appartenance au groupe
`ivmgr`	groupe	Security Access Manager Runtime installe les fichiers et répertoires appartenant au groupe `ivmgr`. Le processus d'installation crée le groupe à l'aide du prochain ID groupe disponible. Pour choisir votre propre ID groupe pour Security Access Manager Runtime : **Linux et Solaris :** `groupadd –g ID_groupe ivmgr` **AIX :** `mkgroup id=ID_groupe ivmgr`	`ivmgr, root`
`ivmgr`	utilisateur	Security Access Manager installe les fichiers et les répertoires appartenant à l'utilisateur `ivmgr`. Le processus d'installation crée l'utilisateur à l'aide du prochain ID utilisateur disponible. Pour choisir votre propre ID utilisateur pour Security Access Manager Runtime : **Linux et Solaris :** `useradd –u ID_util –g ivmgr` `-s /bin/false` `–d /opt/PolicyDirector` `–c "Security Access Manager User" ivmgr` **AIX :** `mkuser id=ID_util groups=ivmgr` `gecos="Security Access Manager User"` `home=/opt/PolicyDirector ivmgr`	

© Copyright IBM Corp. 2001, 2013

Tableau 20. Utilisateurs et groupes requis par Security Access Manager (suite)

ID	Type	Description	Appartenance au groupe
`tivoli`	groupe	Security Access Manager Runtime crée également un ID groupe appelé `tivoli` à utiliser avec le schéma Tivoli Common Directory. Notez que d'autres produits Tivoli peuvent créer l'ID groupe `tivoli` et que sa création n'est pas unique à Security Access Manager Runtime. Le processus d'installation crée l'ID groupe à l'aide du prochain ID groupe disponible. Pour choisir votre propre ID groupe pour Security Access Manager Runtime à utiliser avec Tivoli Common Directory, procédez comme suit. **Linux et Solaris :** `groupadd –g ID_groupe tivoli` **AIX :** `mkgroup id=ID_groupe tivoli`	`tivoli, ivmgr, root`
`tivoli`	utilisateur	Security Access Manager Runtime crée également un ID utilisateur appelé `tivoli` à utiliser avec le schéma Tivoli Common Directory. Notez que d'autres produits Tivoli peuvent créer l'ID utilisateur `tivoli` et que sa création n'est pas unique à Security Access Manager Runtime. Le processus d'installation crée l'ID utilisateur `tivoli` à l'aide du prochain ID utilisateur disponible. Pour choisir votre propre ID utilisateur pour Security Access Manager Runtime à utiliser avec Tivoli Common Directory, procédez comme suit. **Linux et Solaris :** `useradd –u ID_util –g tivoli –c "Owner of Tivoli Common Files" tivoli` `usermod –G tivoli ivmgr` **AIX :** `mkuser id=ID_util groups=tivoli gecos="Owner of Tivoli Common Files" tivoli` `chuser pgrp=staff groups=ivmgr,tivoli ivmgr`	`tivoli`
`idsldap`	groupe	IBM Tivoli Directory Server installe les fichiers et répertoires appartenant au groupe `idsldap`. Le processus d'installation crée le groupe à l'aide du prochain ID groupe disponible. Pour choisir votre propre ID utilisateur, procédez comme suit. **Linux et Solaris :** `groupadd –g ID_groupe idsldap` **AIX :** `mkgroup id=ID_groupe idsldap`	

Tableau 20. Utilisateurs et groupes requis par Security Access Manager (suite)

ID	Type	Description	Appartenance au groupe
idsldap	utilisateur	IBM Tivoli Directory Server installe les fichiers et répertoires appartenant à l'utilisateur idsldap. Le processus d'installation crée l'utilisateur à l'aide du prochain ID utilisateur disponible. Pour choisir votre propre ID utilisateur, procédez comme suit. **Linux et Solaris :** useradd –u *ID_util* –g idsldap –d /home/idsldap –s /bin/ksh idsldap **AIX :** mkuser id=*ID_util* pgrp=staff groups=idsldap	idsldap
sys	groupe	Le processus d'installation crée le groupe pour IBM Global Security Kit (GSKit).	root

L'installation d'IBM Tivoli Directory Server requiert également un ID utilisateur local auquel appartient l'instance de serveur d'annuaire et l'instance de DB2.

Annexe C. Numéros de port par défaut

L'installation utilise plusieurs numéros de port par défaut.

Tableau 21. Numéros de port par défaut utilisés durant l'installation de Security Access Manager

Composants d'installation	Zones à renseigner	Port par défaut
Security Access Manager Policy Server	Port du serveur de règles	7135
Security Access Manager Policy Server Security Access Manager Runtime Security Access Manager Runtime for Java Security Access Manager Web Portal Manager	Port SSL du serveur de règles	7135
Security Access Manager Authorization Server	Port de requête d'autorisation	7136
Security Access Manager Authorization Server	Port de requête d'administration	7137
Security Access Manager Policy Proxy Server	Port de demande de règle	7138
Security Access Manager Policy Proxy Server	Port de requête d'autorisation	7139
Security Access Manager WebSEAL	Port d'écoute de WebSEAL	7234
Security Access Manager Session Management Server	Port d'IBM WebSphere Application Server	8879
Serveurs LDAP	Port non SSL	389
Serveurs LDAP	Port SSL	636
Security Access Manager WebSEAL	Port HTTP	80
Security Access Manager WebSEAL	Port HTTPS	443

© Copyright IBM Corp. 2001, 2013

Annexe D. Options pdconfig

Durant la configuration de Security Access Manager via l'utilitaire **pdconfig**, vous êtes invité à entrer plusieurs options.

Utilisez les descriptions pour vous aider à spécifier les valeurs correctes. Selon que vous effectuez l'installation sur une plateforme Windows, AIX, Linux ou Solaris, il est possible que ces options soient demandées dans un ordre autre que celui qui est répertorié.

Security Access Manager Runtime : LDAP

Le tableau 22 répertorie les options que vous êtes invité à indiquer pendant la configuration du module Security Access Manager Runtime avec un registre LDAP Directory.

Tableau 22. Options de configuration de Security Access Manager Runtime – LDAP. * indique une option obligatoire.

Option de configuration	Description
Allez-vous installer le serveur de règles sur cette machine ?	Indique si le serveur de règles sera installé sur la même machine.
Activer Tivoli Common Directory pour la consignation	Sélectionnez cette option pour activer Tivoli Common Directory. Tivoli Common Directory est un emplacement central sur les systèmes exécutant les logiciels IBM Tivoli pour la sauvegarde des fichiers, notamment les journaux de trace et de messages.

© Copyright IBM Corp. 2001, 2013

Tableau 22. Options de configuration de Security Access Manager Runtime – LDAP (suite). ***** indique une option obligatoire.

Option de configuration	Description
Nom de répertoire (pour Tivoli Common Directory)	Spécifie le chemin complet de Tivoli Common Directory. • Si l'emplacement du répertoire Tivoli Common Directory a été créé antérieurement sur le système suite à l'installation d'une autre application Tivoli, l'emplacement du répertoire s'affiche dans la zone mais ne peut pas être modifié. • Si l'emplacement du répertoire Tivoli Common Directory n'a pas été créé antérieurement sur le système, vous pouvez spécifier un emplacement. Si Tivoli Common Directory est activé et que l'emplacement du répertoire n'a pas été établi antérieurement, les noms des répertoires communs par défaut sont : • Windows : `C :\Program Files\ibm\tivoli\common` • AIX, Linux ou Solaris : `/var/ibm/tivoli/common` Dans Tivoli Common Directory, chaque produit Tivoli stocke ses propres informations dans un sous-répertoire qui lui est spécifique. Les répertoires spécifiques à chaque produit sont désignés par un identifiant à 3 caractères. Par exemple, pour IBM Security Access Manager for Web : *`rép_commun_tivoli`*`/HPD` Voir *IBM Security Access Manager for Web Troubleshooting Guide* pour une liste complète des identificateurs comportant 3 caractères. Si Tivoli Common Directory n'est pas encore activé, Security Access Manager écrit ses messages et données de journal à l'emplacement suivant : • Windows : `C:\Program Files\Tivoli\Policy Director\log` • AIX, Linux ou Solaris : `/var/PolicyDirector/log`
Registre	Spécifie le type de serveur de registre à configurer pour Security Access Manager. Sélectionnez **LDAP**.
Nom d'hôte du serveur LDAP	Spécifie le nom d'hôte ou l'adresse IP du type LDAP du registre du serveur. Vous pouvez spécifier le nom d'hôte complet avec ou sans suffixe de domaine. Exemples : `ldapserver` ou `ldapserver.example.com`
Port du serveur LDAP	Spécifie le numéro de port sur lequel le type de serveur de registre LDAP écoute. Le numéro de port par défaut est **389**.

Tableau 22. Options de configuration de Security Access Manager Runtime – LDAP (suite). ***** indique une option obligatoire.

Option de configuration	Description
Si le serveur de règles Security Access Manager n'est *pas* installé sur le même système que Security Access Manager Runtime, vous êtes invité à entrer les deux valeurs suivantes :	
Nom d'hôte du serveur de règles	Indique le nom d'hôte ou l'adresse IP du serveur de règles Security Access Manager (`pdmgrd`). Le serveur de règles gère la base de données de règles (également appelée *base de données d'autorisation principale*), met à jour les répliques de la base en cas de modification de la base de données principale et duplique les informations de règles dans tous les domaines. Le serveur de règles gère également les informations d'emplacement des autres gestionnaires de ressources dans le domaine. Au moins un serveur de règles doit être défini pour chaque domaine. Vous pouvez spécifier le nom d'hôte complet avec ou sans suffixe de domaine. Exemples : `pdmgr` `pdmgr.example.com`
Port SSL du serveur de règles	Spécifie le numéro du port sur lequel le serveur de règles intercepte des requêtes SSL. Le numéro de port par défaut est **7135**.
Domaine	Spécifie le nom du domaine par défaut de Security Access Manager, également appelé *domaine de gestion*. Ce domaine est créé lors de la configuration du serveur de règles. Le domaine par défaut applique les règles de sécurité pour l'authentification, l'autorisation et le contrôle d'accès. Une règle de sécurité appliquée dans un domaine affecte uniquement les objets se trouvant dans ce domaine. Les utilisateurs autorisés à exécuter des tâches dans un domaine n'ont pas forcément l'autorité nécessaire pour exécuter ces tâches dans d'autres domaines. La valeur par défaut est **Default**, c'est-à-dire, le domaine de gestion.
Sur les systèmes différents de Windows, vous pouvez activer les connexions SSL entre ce système d'exécution Security Access Manager et le serveur LDAP. S'il est sélectionné, vous êtes invité à sélectionner les valeurs suivantes :	
Port non SSL *	Spécifie le numéro de port sur lequel le type de serveur LDAP écoute. Le numéro de port par défaut est **389**.
Numéro de port *	Spécifie le numéro du port sur lequel le serveur LDAP intercepte des requêtes SSL. Le numéro de port par défaut est **636**.

Tableau 22. Options de configuration de Security Access Manager Runtime – LDAP (suite). ***** indique une option obligatoire.

Option de configuration	Description
Fichier de clés et chemin complet *	Spécifie le chemin complet qui contient le fichier de clés client SSL existant ou, si la case **Créer un fichier de clés SSL** est cochée, emplacement du fichier de clés SSL nouvellement créé. Le fichier de clés contient les certificats utilisés dans les communications SSL. L'extension de fichier est toujours `.kdb`. Copiez le fichier de clés SSL sur un répertoire de votre système local. Ce fichier de clés doit être extrait (copié) du serveur LDAP.
Mot de passe du fichier de clés	Spécifie le mot de passe existant associé au fichier de clés SSL indiqué. Le mot de passe du fichier de clés client a été défini lors de la première création du fichier de clés. Changez ce mot de passe à l'aide de l'utilitaire **`gsk8capicmd`** (inclus dans GSKit 8) ou de l'utilitaire **`ikeyman`** (fourni avec IBM Java). Si vous modifiez ce mot de passe, vous devez vous le rappeler.
Libellé de certificat	Spécifie le libellé du certificat client SSL. Ce libellé n'est valide que lorsque SSL est utilisé et que le serveur LDAP est configuré pour que l'authentification client soit exigée. Par exemple : `PDLDAP`. Utilisez un libellé de certificat pour faire la distinction entre plusieurs certificats dans le fichier de clés SSL ou lors de l'utilisation d'un certificat autre que le certificat par défaut du fichier de clés. Dans le cas contraire, ne complétez pas cette zone.
Créez un fichier de clés SSL	Cochez cette case pour créer un fichier de clés SSL. Le fichier de clés contient les certificats utilisés dans les communications SSL. L'utilitaire **`pdconfig`** utilise IBM Global Security Kit (GSKit) pour générer le certificat et le fichier de clés SSL. Valeur par défaut : activée (case cochée)

Tableau 22. Options de configuration de Security Access Manager Runtime – LDAP (suite). * indique une option obligatoire.

Option de configuration	Description
Activer FIPS, NIST SP800-131 ou Suite B	Vous pouvez configurer Security Access Manager pour le mettre en conformité à diverses normes de sécurité. Pour activer la configuration, définissez la valeur de `[ssl] ssl-compliance` dans `pd.conf` après avoir configuré l'environnement d'exécution, mais avant de configurer le serveur de règles. L'utilitaire **pdconfig** crée tous les clés et certificats au moyen d'algorithmes appropriés selon le type de configuration. Lorsque la valeur `[ssl] ssl-compliance` est définie, le client IBM Tivoli Directory Server est configuré pour utiliser le protocole de communication sécurisé approprié suivant le type de conformité sélectionné. **Remarque :** Tous les environnements d'exécution doivent être définis sur la même valeur de `[ssl] ssl-compliance`, car ils ne peuvent pas être mélangés. Valeur par défaut : `[ssl] ssl-compliance='none'`. Cette valeur signifie qu'aucune conformité n'est activée.

Security Access Manager Runtime : Active Directory

Le tableau 23 répertorie les options que vous êtes invité à indiquer pendant la configuration du module Security Access Manager Runtime avec un registre Active Directory.

Tableau 23. Options de configuration de Security Access Manager Runtime – Active Directory. * indique une option obligatoire.

Option de configuration	Description
Registre	Spécifie le type de serveur de registre à configurer pour Security Access Manager. Sélectionnez **Active Directory**.
Configuration dans plusieurs domaines Active Directory	Cochez cette case pour configurer plusieurs domaines Active Directory. Sinon, Security Access Manager est configuré pour un seul domaine. Un exemple de domaines Microsoft Active Directory multiples est un domaine Security Access Manager unique contenant plusieurs domaines Microsoft Active Directory. Lorsqu'elle est configurée pour plusieurs domaines Microsoft Active Directory, la ligne de commande affiche l'ID administrateur Security Access Manager (valeur par défaut **sec_master**) **secmaster@***nom_domaine*. Valeur par défaut : non activée (Security Access Manager est configuré pour un seul domaine).

Tableau 23. Options de configuration de Security Access Manager Runtime – Active Directory (suite). ***** indique une option obligatoire.

Option de configuration	Description
Nom d'hôte Active Directory *	Spécifie le nom du serveur du contrôleur de domaine Active Directory. Par exemple : `adserver.example.com`
Domaine Active Directory	Spécifie le nom du domaine Active Directory. Dans le cas d'une configuration sur plusieurs domaines, le nom est affiché automatiquement. Exemple : `dc=tivoli,dc=com`
Activer les connexions chiffrées	Indique si les communications chiffrées avec Microsoft Active Directory doivent être utilisées. Si la case est cochée, Kerberos est utilisé dans l'interface ADSI (Microsoft Active Directory Service Interface) pour chiffrer les données échangées avec le serveur Microsoft Active Directory. Ce paramètre équivaut à l'activation d'une connexion SSL dans un environnement système qui utilise le client LDAP pour communiquer avec le serveur Active Directory. La valeur par défaut n'est pas activée (Security Access Manager n'est pas configuré pour le chiffrement).
Indiquez l'emplacement du serveur de règles Security Access Manager. Si vous sélectionnez l'option **Le serveur de règles Access Manager Policy est installé sur une autre machine**, vous êtes invité à entrer les valeurs du nom d'hôte et du port d'écoute :	
Nom d'hôte	Indique le nom d'hôte ou l'adresse IP du serveur de règles Security Access Manager (`pdmgrd`). Le serveur de règles gère la base de données de règles (également appelée *base de données d'autorisation principale*), met à jour les répliques de la base en cas de modification de la base de données principale et duplique les informations de règles dans tous les domaines. Le serveur de règles gère également les informations d'emplacement des autres gestionnaires de ressources dans le domaine. Au moins un serveur de règles doit être défini pour chaque domaine. Vous pouvez spécifier le nom d'hôte complet avec ou sans suffixe de domaine. Vous pouvez spécifier le nom d'hôte complet avec ou sans suffixe de domaine. Exemples : `pdmgr` `pdmgr.example.com`
Port d'écoute	Spécifie le numéro du port sur lequel le serveur de règles Security Access Manager intercepte les requêtes SSL. Le numéro de port par défaut est **7135**.

Tableau 23. Options de configuration de Security Access Manager Runtime – Active Directory (suite). ***** indique une option obligatoire.

Option de configuration	Description
Sur les systèmes sur lesquels le client LDAP est utilisé pour communiquer avec le serveur Active Directory, vous pouvez activer les connexions SSL entre le client LDAP et le serveur Active Directory. Si l'option Activer les connexions chiffrées est sélectionnée, vous êtes invité à spécifier les quatre valeurs suivantes :	
Numéro de port	Indique le numéro du port sur lequel le serveur de registres intercepte les requêtes SSL. Le numéro de port par défaut est **636**.
Fichier de clés et chemin complet	Spécifie le chemin qualifié complet qui contient le fichier de clés client SSL existant ou, si la case **Créer un fichier de clés SSL** est cochée, l'emplacement dans lequel vous souhaitez que le fichier de clés SSL soit créé. Le fichier de clés contient les certificats utilisés dans les communications SSL. L'extension de fichier est toujours `.kdb`. Ce fichier de clés doit être obtenu à l'aide de l'utilitaire **gsk8capicmd** (inclus dans GSKit 8) ou de l'utilitaire **ikeyman** (fourni avec IBM Java) et du certificat d'une autorité de certification pour le serveur Active Directory. Si le fichier de clés SSL est créé automatiquement par l'utilitaire **pdconfig**, le chemin complet et le nom de fichier de clés correspond à `C:\Program Files\IBM\LDAP\`*`version`*`\lib\am_key.kdb` ou au chemin et au nom de fichier clés SSL de votre choix. Si vous activez SSL à l'aide d'un fichier de clés SSL existant, copiez le fichier de clés SSL dans un répertoire quelconque de votre système local. Ce fichier de clés doit être extrait (copié) du serveur LDAP.
Libellé de certificat	Spécifie le libellé du certificat client SSL. Ce libellé n'est valide que lorsque SSL est utilisé et que le serveur LDAP est configuré pour que l'authentification client soit exigée. Par exemple : `PDLDAP`. Utilisez un libellé de certificat pour faire la distinction entre plusieurs certificats dans un fichier de clés SSL ou lors de l'utilisation d'un certificat autre que le certificat par défaut du fichier de clés. Dans le cas contraire, ne complétez pas cette zone.
Mot de passe du fichier de clés	Spécifie le mot de passe existant associé au fichier de clés SSL indiqué. Le mot de passe du fichier de clés client a été défini lors de la première création du fichier de clés. Changez ce mot de passe à l'aide de l'utilitaire **gsk8capicmd** (inclus dans GSKit 8) ou de l'utilitaire **ikeyman** (fourni avec IBM Java). Si vous modifiez ce mot de passe, vous devez vous le rappeler.

Tableau 23. Options de configuration de Security Access Manager Runtime – Active Directory (suite). ***** indique une option obligatoire.

Option de configuration	Description
ID Administrateur Active Directory	Spécifie l'identificateur du compte administrateur du domaine Microsoft Active Directory. Cet ID administrateur a été créé en même temps que le domaine Microsoft Active Directory. Il a dû être ajouté aux groupes Administrateurs, Administrateurs de domaine, Administrateurs d'entreprise et Administrateur de schéma. Notez que ce compte administrateur ne s'applique qu'à un utilisateur Microsoft Active Directory et non à un utilisateur Security Access Manager.
Mot de passe administrateur Active Directory	Spécifie le mot de passe de l'ID administrateur du domaine Microsoft Active Directory. Ce mot de passe administrateur a été défini lors de la création de votre compte administrateur Microsoft Active Directory.
Activer l'utilisation d'une adresse électronique en tant qu'ID utilisateur	Active l'utilisation d'une adresse électronique en tant qu'ID utilisateur `userPrincipalname`.
Nom d'hôte du serveur Global Catalog (en mode Active Directory LDAP uniquement)	Spécifie le nom d'hôte Active Directory pour le serveur Global Catalog.
Port du serveur Global Catalog (en mode Active Directory LDAP uniquement)	Spécifie le port Active Directory Global Catalog. Pour une activation non-SSL, la valeur par défaut est 3268. Pour une activation SSL, la valeur par défaut est 3269.
Nom distinctif de l'emplacement des données Security Access Manager	Spécifie le nom distinctif utilisé par Microsoft Active Directory pour indiquer l'endroit où vous voulez stocker des données Security Access Manager. La valeur par défaut est la valeur d'entrée du domaine Active Directory. Exemple : `dc=tivoli,dc=com` Si Security Access Manager est configuré à l'aide de plusieurs domaines Active Directory, cette valeur est automatiquement définie sur le domaine principal d'Active Directory. Notez qu'il ne vous est demandé de remplir cette zone que lorsque la case **Configurer sur plusieurs domaines Active Directory** n'est pas cochée.
Activer Tivoli Common Directory pour la consignation	Sélectionnez cette option pour activer Tivoli Common Directory. Tivoli Common Directory est un emplacement central sur les systèmes exécutant les logiciels Tivoli pour la sauvegarde des fichiers, notamment les journaux de trace et de messages.

Tableau 23. Options de configuration de Security Access Manager Runtime – Active Directory (suite). ***** indique une option obligatoire.

Option de configuration	Description
Nom de répertoire (pour Tivoli Common Directory)	Spécifie le chemin complet de Tivoli Common Directory. • Si l'emplacement du répertoire Tivoli Common Directory a été créé antérieurement sur le système suite à l'installation d'une autre application Tivoli, l'emplacement du répertoire s'affichera dans la zone mais ne pourra pas être modifié. • Si l'emplacement du répertoire Tivoli Common Directory n'a pas été créé antérieurement sur le système, vous pouvez spécifier un emplacement. Si Tivoli Common Directory est activé et que l'emplacement du répertoire n'a pas été établi antérieurement, les noms des répertoires communs par défaut sont : • Windows : `C :\Program Files\ibm\tivoli\ common` • AIX, Linux ou Solaris : `/var/ibm/tivoli/common` Dans Tivoli Common Directory, chaque produit stocke ses propres informations dans un sous-répertoire qui lui est spécifique. Les répertoires spécifiques à chaque produit sont désignés par un identifiant à 3 caractères. Par exemple, pour IBM Security Access Manager for Web : *`rép_commun_tivoli`*`/HPD` Voir *IBM Security Access Manager for Web Troubleshooting Guide* pour une liste complète des identificateurs comportant 3 caractères. Si Tivoli Common Directory n'est pas activé, Security Access Manager consigne ses données de journaux de message et de trace à l'emplacement suivant : • Windows : `C:\Program Files\Tivoli\Policy Director\log` • AIX, Linux ou Solaris : `/var/PolicyDirector/log`
Nom du répertoire	Spécifie le répertoire de journaux du premier logiciel installé. Lors de la première configuration de Tivoli Common Directory, vous pouvez indiquer le répertoire dans lequel vous souhaitez placer les fichiers journaux. Ensuite, vous pouvez configurer le logiciel pour utiliser ce répertoire.

Tableau 23. Options de configuration de Security Access Manager Runtime – Active Directory (suite). * indique une option obligatoire.

Option de configuration	Description
Activer FIPS, NIST SP800-131 ou Suite B	Vous pouvez configurer Security Access Manager pour le mettre en conformité à des normes de sécurité. Pour activer la configuration, définissez la valeur de `[ssl] ssl-compliance` dans `pd.conf` après avoir configuré l'environnement d'exécution, mais avant de configurer le serveur de règles. L'utilitaire **pdconfig** crée tous les clés et certificats au moyen d'algorithmes appropriés selon le type de configuration. Lorsque la valeur `[ssl] ssl-compliance` est définie, le client IBM Tivoli Directory Server est configuré pour utiliser le protocole de communication sécurisé approprié suivant le type de conformité sélectionné. **Remarque :** Tous les environnements d'exécution doivent être définis sur la même valeur de `[ssl] ssl-compliance`, car ils ne peuvent pas être mélangés. Valeur par défaut : `[ssl] ssl-compliance='none'`. Cette valeur signifie qu'aucune conformité n'est activée.

Si vous utilisez Active Directory comme registre, un fichier `activedir.conf` est créé dans le répertoire suivant :

%REP_INSTALL_PD%`\etc`

où *REP_INSTALL_PD* est le répertoire d'installation de Security Access Manager et `C:\Program Files\Tivoli\Policy Director` est le répertoire par défaut pour Windows.

Security Access Manager Attribute Retrieval Service

tableau 24 répertorie les options que vous êtes invité à indiquer pendant la configuration du package Security Access Manager Attribute Retrieval Service.

Tableau 24. Security Access Manager Attribute Retrieval Service. * indique une option obligatoire.

Option de configuration	Description
Nom de noeud	Spécifie le nom du noeud WebSphere utilisé pour l'administration. Il doit être unique dans son groupe de noeuds (cellule). Il correspond au nom DNS ou à l'adresse IP de votre système local.
Nom d'hôte local	Spécifie le nom qualifié complet du système hôte sur lequel se trouve Security Access Manager Attribute Retrieval Service.
ID administrateur local	Spécifie l'ID administrateur avec lequel vous êtes connecté. (Sous AIX, Linux ou Solaris, il s'agit de **root**, sous Windows il s'agit de **Administrateur**).
Mot de passe administrateur local	Spécifie le mot de passe de l'administrateur local.

Security Access Manager Authorization Server

Le tableau 25 répertorie les options que vous êtes invité à indiquer pendant la configuration du package Security Access Manager Authorization Server.

Remarque : Configurez le package Security Access Manager Runtime, puis le package Security Access Manager Server.

Tableau 25. Options de configuration de Security Access Manager Authorization Server. * indique une option obligatoire.

Option de configuration	Description
Domaine	Spécifie le nom de domaine. La valeur par défaut est **Default**, c'est-à-dire, le domaine de gestion.
Nom d'hôte du serveur de règles	Indique le nom d'hôte utilisé par le serveur de règles pour contacter ce serveur. La valeur par défaut est le nom d'hôte du système local.
Port du serveur de règles	Spécifie le numéro du port sur lequel le serveur de règles intercepte des requêtes. Le numéro de port par défaut est **7135**.
Administrateur Security Access Manager (ou ID administrateur pour le domaine Default)	Spécifie l'identificateur de l'administrateur Security Access Manager du domaine de gestion. L'ID administrateur par défaut est **sec_master**.
Mot de passe	Spécifie le mot de passe associé à l'ID administrateur Security Access Manager.
Nom d'instance	Spécifie le nom d'instance du serveur d'autorisations. Le nom d'instance du serveur d'autorisations par défaut n'est jamais renseigné. Entrez un nom unique pour la configuration de chaque serveur d'autorisations additionnel. Les noms d'instance peuvent contenir les caractères suivants : 'a' à 'z' , '0' à '9' , '-' et '_' (sans apostrophes). Le nom d'instance ne doit pas commencer par un tiret ('-').
Nom d'hôte local	Spécifie le nom complet du système hôte sur lequel se trouve le serveur d'autorisation.
Port de requête d'administration	Spécifie le port de requête d'administration. Le port par défaut est **7137**.
Port de requête d'autorisation	Spécifie le numéro du port de requête d'autorisation. Le numéro de port par défaut est **7136**.

IBM Security Access Manager Runtime for Java

Le tableau 26 répertorie les options que vous êtes invité à indiquer pendant la configuration du package IBM Security Access Manager Runtime for Java.

Tableau 26. options de configuration IBM Security Access Manager Runtime for Java. ***** indique une option obligatoire.

Option de configuration	Description
Type de configuration	Pour configurer IBM Security Access Manager Runtime for Java pour l'utilisation avec l'environnement JRE (Java Runtime Environment) actuel, sélectionnez un type de configuration : **Complète** : sélectionnez ce type si vous configurez Web Portal Manager ou si vous activez les applications Java pour gérer et utiliser la sécurité Security Access Manager. >**Autonome** : sélectionnez cette option si vous êtes développeur et que vous utilisez des classes de Runtime for Java. Vous n'êtes pas invité à entrer les informations du serveur de règles.
Chemin complet de Java Runtime Environment (JRE) en vue d'une configuration pour Security Access Manager	Spécifie le chemin d'accès au composant IBM Java Runtime fourni avec Security Access Manager. Par exemple : `/opt/ibm/java-x86_64-60/jre` Si vous installez un système Web Portal Manager, assurez-vous que vous spécifiez l'environnement Java Runtime Environment qui est installé avec IBM WebSphere Application Server. Par exemple : `/usr/WebSphere/AppServer/java/jre`
Nom d'hôte de la machine du serveur de règles Security Access Manager	Définit le nom d'hôte qualifié complet du serveur de règles. Par exemple : `pdmgr.example.com`
Numéro de port de la machine du serveur de règles Security Access Manager	Spécifie le numéro du port sur lequel le serveur de règles intercepte des requêtes SSL. Le numéro de port par défaut est **7135**.
Informations sur le domaine Security Access Manager Policy Server	null
Activer Tivoli Common Directory pour la consignation	Sélectionnez cette option pour activer Tivoli Common Directory. Tivoli Common Directory est un emplacement central sur les systèmes exécutant les logiciels Tivoli pour la sauvegarde des fichiers, notamment les journaux de trace et de messages.

Tableau 26. options de configuration IBM Security Access Manager Runtime for Java (suite). * indique une option obligatoire.

Option de configuration	Description
Nom du répertoire	Spécifie le chemin complet de Tivoli Common Directory. • Si l'emplacement du répertoire Tivoli Common Directory a été créé antérieurement sur le système suite à l'installation d'une autre application Tivoli, l'emplacement du répertoire s'affichera dans la zone mais ne pourra pas être modifié. • Si l'emplacement du répertoire Tivoli Common Directory n'est pas déjà créé antérieurement sur le système, vous pouvez spécifier un emplacement. Si Tivoli Common Directory est activé et que l'emplacement du répertoire n'a pas encore été établi, le nom de répertoire commun par défaut est : • Windows : `C :\Program Files\ibm\tivoli\ common` • AIX, Linux ou Solaris : `/var/ibm/tivoli/common` Dans Tivoli Common Directory, chaque produit Tivoli stocke ses propres informations dans un sous-répertoire qui lui est spécifique. Les répertoires spécifiques à chaque produit sont désignés par un identifiant à 3 caractères. Par exemple, pour IBM Security Access Manager for Web : *`rép_commun_tivoli`*`/HPD` Voir *IBM Security Access Manager for Web Troubleshooting Guide* pour une liste complète des identificateurs comportant 3 caractères. Si Tivoli Common Directory n'est pas encore activé, Security Access Manager écrit ses messages et données de journal à l'emplacement suivant : • Windows : `C:\Program Files\Tivoli\Policy Director\log` • AIX, Linux ou Solaris : `/var/PolicyDirector/log`

Security Access Manager Plug-in for Web Servers sur AIX, Linux ou Solaris

tableau 27 répertorie les options de configuration pour le module Plug-in for Web Servers sur les plateformes AIX, Linux ou Solaris.

Tableau 27. Plug-in for Web Servers sur AIX, Linux ou Solaris. * indique une option obligatoire.

Option de configuration	Description
Chemin d'accès complet au répertoire contenant le fichier de configuration de serveur Web	Spécifie le chemin d'installation par défaut du serveur Web. Acceptez ce chemin ou entrez-en un autre.

Tableau 27. Plug-in for Web Servers sur AIX, Linux ou Solaris (suite). * indique une option obligatoire.

Option de configuration	Description
Hôtes virtuels à protéger	Spécifiez le numéro de l'option de menu ou entrez **x** pour sortir. Vous avez trois options : • Si vous souhaitez protéger un seul hôte virtuel avec le plug-in, entrez le numéro qui désigne l'hôte virtuel dans la liste affichée. • Pour sécuriser plusieurs hôtes virtuels, entrer les valeurs correspondant à leurs positions dans la liste affichée. Séparez les numéros entrés par des espaces. • Entrez `all` pour que le plug-in protège tous les hôtes virtuels connus sur le serveur.
ID administrateur de Security Access Manager	Spécifie l'identificateur de l'administrateur Security Access Manager du domaine de gestion. L'ID administrateur par défaut est **sec_master**. Pour les domaines Active Directory multiples, il s'agit de **sec_master@***nom_domaine*.
Mot de passe associé à l'ID administrateur de Security Access Manager	Spécifie le mot de passe associé à l'ID administrateur Security Access Manager.
Numéro de port à utiliser pour les mises à jour des règles d'autorisation	Une mise à jour d'autorisation est le transfert de paquets delta d'informations de règles à partir serveur de règle d'autorisation pendant le fonctionnement de l'application. Entrez le numéro de port sur le quel intercepter les mises à jour d'autorisation ou acceptez la valeur par défaut de **7237**.
Pour les registres LDAP sous AIX, Linux ou Solaris uniquement, vous êtes invité à indiquer si la communication SSL doit être activée.	
Activer la communication SSL entre le serveur d'autorisation Security Access Manager Plug-in for Web Servers et le serveur LDAP	L'activation de SSL n'est pas nécessaire dans les environnements dans lesquels le serveur Web et le serveur de registre se trouvent sur le même réseau sécurisé. Si vous pouvez être sûr de l'intégrité et de la sécurité des données envoyées entre le serveur Web et votre registre, le choix de ne pas utiliser SSL améliore la bande passante réseau en supprimant le temps système de sécurité.
Si vous activez SSL entre le serveur d'autorisation Security Access Manager Plug-in for Web Servers et le serveur LDAP, vous êtes invité à entrer les quatre valeurs suivantes :	
Emplacement du fichier de clés du client SSL LDAP	Spécifie où le fichier de clés client doit être placé. L'emplacement par défaut est `/usr/ldap/lib/ldapkey.kdb`. **Remarque :** Lorsque Security Access Manager Plug-in for Web Servers est installé sur la même machine que le serveur de règles et configuré avec SSL sur LDAP, le fichier client LDAP ne peut pas être partagé.Les droits de fichier AIX, Linux ou Solaris sont essentiels pour protéger les fichiers contre les accès non autorisés. Le fichier de clés client LDAP peut être partagé si les droits de fichier autorisent l'accès aux fichiers par les utilisateurs du Plug-in.

Tableau 27. Plug-in for Web Servers sur AIX, Linux ou Solaris (suite). * indique une option obligatoire.

Option de configuration	Description
Libellé de certificat client SSL	Spécifie le libellé dans le fichier de base de données de clés du client LDAP correspondant au certificat client à envoyer au serveur. Ce libellé est uniquement requis si le serveur est configuré pour demander l'authentification client pendant l'établissement de la connexion SSL ou si vous souhaitez utiliser un certificat qui n'est pas celui par défaut dans votre fichier de clés. En règle générale, le serveur LDAP requiert uniquement les certificats côté client spécifiés pendant la création du fichier client `.kdb` file. Si le libellé du fichier de clé client SSL n'est pas demandé, laissez cette zone vide.
Mot de passe du fichier de clés du client SSL du serveur LDAP	Spécifie le mot de passe existant associé au fichier de clés SSL indiqué. Le mot de passe du fichier de clés client a été défini lors de la première création du fichier de clés. Changez ce mot de passe à l'aide de l'utilitaire **gsk8capicmd** (inclus dans GSKit 8) ou de l'utilitaire **ikeyman** (fourni avec IBM Java). Si vous modifiez ce mot de passe, vous devez vous le rappeler.
Numéro de port SSL du serveur LDAP*	Spécifie le numéro du port sur lequel le serveur LDAP intercepte des requêtes SSL. Le numéro de port par défaut est **636**.

Security Access Manager Plug-in for Web Servers sous Windows

Le tableau 28 répertorie les options de configuration pour le plug-in for Web Servers sur les plateformes Windows.

Tableau 28. Plug-in for Web Servers sous Windows. * indique une option obligatoire.

Option de configuration	Description
Hôtes virtuels à protéger	Spécifie la liste des hôtes virtuels à protéger. Effectuez une sélection dans la liste pour indiquer l'hôte virtuel à protéger.
ID administrateur de Security Access Manager *	Spécifie l'identificateur de l'administrateur Security Access Manager du domaine de gestion. L'ID administrateur par défaut est **sec_master**. Pour les domaines Active Directory multiples, il s'agit de **sec_master@***nom_domaine*.
Mot de passe associé à l'ID administrateur de Security Access Manager *	Spécifie le mot de passe associé à l'ID administrateur Security Access Manager.
Numéro de port d'écoute à utiliser pour les mises à jour des règles d'autorisation *	Spécifie le numéro de port pour intercepter les mises à jour d'autorisations. Une mise à jour d'autorisation est le transfert de paquets delta d'informations de règles à partir serveur de règle d'autorisation pendant le fonctionnement de l'application. La valeur par défaut est **7237**.

Security Access Manager Policy Server

Le tableau suivant répertorie les options de configuration pour le serveur de règles.

Remarque :

1. Vous êtes invité à configurer le module Security Access Manager Runtime avant de configurer le module Security Access Manager Policy Server.
2. Si vous reconfigurez le serveur de règles Security Access Manager, vous devez également reconfigurer Security Access Manager Runtime ou IBM Security Access Manager Runtime for Java pour utiliser les certificats pour le nouveau serveur de règles.
3. Le serveur de règles n'est pas pris en charge sur les plateformes AIX, Linux ou Solaris pour le serveur de registre Active Directory.

Tableau 29. Options de configuration de Security Access Manager Policy Server. * indique une option obligatoire.

Option de configuration	Description
ID administrateur de Security Access Manager *	Spécifie l'identificateur de l'administrateur Security Access Manager du domaine de gestion. L'ID administrateur par défaut est **sec_master**. Pour les domaines Active Directory multiples, il s'agit de **sec_master@***nom_domaine*.
Mot de passe associé à l'ID administrateur de Security Access Manager *	Spécifie le mot de passe associé à l'ID administrateur Security Access Manager.
Confirmer le mot de passe *	Spécifiez une nouvelle fois le mot de passe de l'ID administrateur Security Access Manager pour confirmation.
Port SSL du serveur de règles *	Spécifie le numéro du port sur lequel le serveur de règles intercepte des requêtes SSL. Le numéro de port par défaut est **7135**.
Cycle de vie du certificat SSL *	Spécifie le nombre de jours de validité du fichier de certificat SSL. Le nombre de jours par défaut est **365**.
Délai d'expiration de la connexion SSL *	Indique la délai d'attente de réponse (exprimé en secondes) d'une connexion SSL avant son arrivée à expiration. Le nombre de secondes par défaut est **7200**.

Tableau 29. Options de configuration de Security Access Manager Policy Server (suite). ***** indique une option obligatoire.

Option de configuration	Description
Activer FIPS, NIST SP800-131 ou Suite B	Vous pouvez configurer Security Access Manager pour le mettre en conformité à diverses normes de sécurité. Pour activer la configuration, définissez la valeur de `[ssl] ssl-compliance` dans `pd.conf` après avoir configuré l'environnement d'exécution, mais avant de configurer le serveur de règles. L'utilitaire **pdconfig** crée tous les clés et certificats au moyen d'algorithmes appropriés selon le type de configuration. Lorsque la valeur `[ssl] ssl-compliance` est définie, le client IBM Tivoli Directory Server est configuré pour utiliser le protocole de communication sécurisé approprié suivant le type de conformité sélectionné. **Remarque :** Tous les environnements d'exécution doivent être définis sur la même valeur de `[ssl] ssl-compliance`, car ils ne peuvent pas être mélangés. Valeur par défaut : `[ssl] ssl-compliance='none'`. Cette valeur signifie qu'aucune conformité n'est activée.
Nom du domaine de gestion	Nom du domaine de gestion. Le domaine administratif initial créé lors de la configuration du serveur de règles est appelé domaine de gestion. Le nom du domaine de gestion doit être unique sur le serveur LDAP. Ce nom doit être une chaîne alphanumérique d'une longueur maximale de 64 caractères et n'est pas sensible à la casse. La valeur par défaut est **Default**.
Nom de domaine de l'emplacement du domaine de gestion LDAP	Le nom distinctif de l'emplacement du serveur LDAP où seront stockées les métadonnées Security Access Manager. Les informations du domaine de gestion sont stockées par défaut dans son propre suffixe au format secAuthority=*nom_domaine_gestion*. Que le nom distinctif utilisé ait été spécifié ou que ce soit celui par défaut, l'emplacement doit exister sur le serveur LDAP.

Security Access Manager Policy Proxy Server

Le tableau 30, à la page 356 répertorie les options que vous êtes invité à indiquer pendant la configuration du package Security Access Manager Policy Proxy Server.

Remarque : Configurez le package Security Access Manager Runtime, puis le package Security Access Proxy Server.

Tableau 30. Options de configuration de Security Access Manager Policy Proxy Server. * indique une option obligatoire.

Option de configuration	Description
Nom d'hôte du serveur de règles *	Définit le nom d'hôte qualifié complet du serveur de règles. Par exemple : `pdmgr.example.com`
Port du serveur de règles *	Spécifie le numéro du port sur lequel le serveur de règles intercepte des requêtes. Le numéro de port par défaut est **7135**.
ID administrateur *	Spécifie l'identificateur de l'administrateur Security Access Manager du domaine de gestion. L'ID administrateur par défaut est **sec_master**. Pour les domaines Active Directory multiples, il s'agit de **sec_master@***nom_domaine*.
Mot de passe *	Spécifie le mot de passe associé à l'ID administrateur Security Access Manager.
Nom d'hôte local *	Spécifie le nom complet du système hôte sur lequel se trouve le serveur proxy de règles. Par exemple : `pdproxy.example.com`
Port de requête d'administration *	Spécifie le port de requête d'administration. Le port par défaut est **7139**.
Port de requête proxy *	Spécifie le port de requête de proxy. Le port par défaut est **7138**.

Security Access Manager Web Portal Manager

Le tableau 31 répertorie les options que vous êtes invité à indiquer pendant la configuration du package Security Access Manager Web Portal Manager.

Tableau 31. Options de configuration de Security Access Manager Web Portal Manager. * indique une option obligatoire.

Option de configuration	Description
Chemin complet * (répertoire d'installation d'IBM WebSphere Application Server)	Spécifie le répertoire d'installation existant d'IBM WebSphere Application Server. Entrez le chemin qualifié complet de l'emplacement d'un des types suivants de serveur IBM WebSphere Application Server : • Dans le cas de clusters, indiquez les informations relatives au déploiement existant d'IBM WebSphere Application Server Network Deployment. • En cas de serveur unique, indiquez les informations relatives au serveur IBM WebSphere Application Server. Valeur par défaut : `C:\Program Files\IBM\WebSphere\AppServer`

Tableau 31. Options de configuration de Security Access Manager Web Portal Manager (suite). ***** indique une option obligatoire.

Option de configuration	Description
Nom d'hôte * (IBM WebSphere Application Server)	Spécifie le nom d'hôte ou l'adresse IP de l'un des types d'instance IBM WebSphere Application Server : • Dans le cas de clusters, indiquez les informations relatives au déploiement existant d'IBM WebSphere Application Server Network Deployment. • En cas de serveur unique, indiquez les informations relatives au serveur IBM WebSphere Application Server. Par exemple, : `was01`
Port * (IBM WebSphere Application Server)	Spécifie le numéro de port sur lequel IBM WebSphere Application Server écoute les demandes d'administration SOAP pour l'un des types d'instance IBM WebSphere Application Server suivants : • Dans le cas de clusters, indiquez les informations relatives au déploiement existant d'IBM WebSphere Application Server Network Deployment. • En cas de serveur unique, indiquez les informations relatives au serveur IBM WebSphere Application Server. Utilisez la valeur de numéro de port par défaut qui est fonction du serveur. Le numéro de port IBM WebSphere Application Server par défaut est **8800**. **Remarque :** Ne modifiez cette valeur que si le serveur est déjà configuré pour utiliser un numéro de port différent. Ce processus n'essaie pas de définir cette valeur pour le serveur.
Activer SSL avec IBM WebSphere Application Server	Cochez la case pour activer les communications SSL (Secure Sockets Layer) avec IBM WebSphere Application Server. Valeur par défaut : non activée (case non cochée.)
ID administrateur du serveur d'application * IBM WebSphere	L'identificateur d'un compte administrateur existant d'IBM WebSphere Application Server. Tous les ID administrateur doivent respecter les règles d'affectation de noms d'IBM WebSphere Application Server.
IBM WebSphere Mot de passe administrateur du serveur d'application *	Spécifie le mot de passe associé à l'ID administrateur IBM WebSphere Application Server indiqué. Ce mot de passe administrateur a été créé lors de la création du compte administrateur IBM WebSphere Application Server.

Tableau 31. Options de configuration de Security Access Manager Web Portal Manager (suite). ***** indique une option obligatoire.

Option de configuration	Description
Fichier de clés certifiées SSL et chemin complet *	Indique le chemin complet de l'emplacement du fichier de clés certifiées existant. Servez-vous du fichier de clés certifiées pour gérer les certificats utilisés dans les communications SSL. Le fichier de clés certifiées vérifie le certificat présenté par le serveur. Le signataire du certificat SSL doit être reconnu comme étant une autorité de certification digne de confiance. Pour indiquer le fichier de clés du client SSL, entrez son chemin complet et son nom ou faites une recherche parmi les fichiers de clés certifiées existants.
Mot de passe du fichier de clés certifiées SSL	Spécifie le mot de passe existant qui protège le fichier de clés certifiées si une connexion sécurisée à IBM WebSphere Application Server est utilisée. Le mot de passe du fichier de clés certifiées a été défini lors de la première création du fichier de clés.
Fichier de clés SSL et chemin complet	Spécifie le chemin complet qui contient le fichier de clés existant. Le fichier de clés contient les certificats utilisés dans les communications SSL. Pour indiquer le fichier de clés du client SSL, entrez son chemin complet et son nom ou faites une recherche parmi les fichiers de clés existants.
Mot de passe du fichier des clés SSL	Spécifie le mot de passe existant associé au fichier de clés client indiqué. Le mot de passe du fichier de clés a été défini lors de la première création du fichier de clés.
Clusters *	Sélectionnez un cluster existant dans lequel Web Portal Manager doit être déployé depuis la liste affichée. Vous devez sélectionner au moins un cluster ou serveur d'application. Par exemple : `WPM_Cluster`
Serveurs d'applications *	Sélectionnez dans la liste un serveur d'applications existant dans lequel Web Portal Manager doit être déployé. Vous devez sélectionner au moins un cluster ou serveur d'application. Par exemple : `WebSphere:cell-was01Cell01,node=was01Node01,server==server1`
Serveurs Web	Sélectionnez dans la liste un serveur Web existant sur lequel Web Portal Manager doit être déployé. Par exemple : `WPM_WebServer`

Tableau 31. Options de configuration de Security Access Manager Web Portal Manager (suite). ***** indique une option obligatoire.

Option de configuration	Description
Nom d'hôte * (serveur de règles Security Access Manager ou serveur proxy de règles)	Indique le nom d'hôte ou l'adresse IP du serveur de règles (ou du serveur proxy de règles) Security Access Manager. Le serveur de règles gère la base de données de règles (parfois appelée *base de données d'autorisation principale*), met à jour les répliques de la base de données en cas de modification de la base de données principale et réplique les informations de règles dans tous les domaines. Le serveur de règles gère également les informations d'emplacement des autres gestionnaires de ressources dans le domaine. Au moins un serveur de règles doit être défini pour chaque domaine. Par exemple : `WPM_PolServer`
Port * (serveur de règles Security Access Manager ou serveur proxy de règles)	Spécifie le numéro du port sur lequel le serveur (ou le serveur proxy) de règles Security Access Manager intercepte les requêtes SSL. Utilisez la valeur de numéro de port par défaut qui est fonction du serveur. Le numéro de port par défaut du serveur de règles est **7135**. Le numéro de port par défaut du serveur proxy de règles est **7138**.
Security Access Manager Authorization Server est-il configuré ?	Cochez cette case pour configurer le serveur d'autorisations Security Access Manager. Valeur par défaut : non activée (case non cochée.)
Nom d'hôte *	Spécifie le nom d'hôte complet ou l'adresse IP existante pour configurer le serveur d'autorisations Security Access Manager à utiliser par Web Portal Manager. Par exemple : `WPM_AuthServer`
Port *	Spécifie le numéro du port sur lequel le serveur d'autorisations Security Access Manager intercepte les requêtes SSL. Utilisez la valeur de numéro de port par défaut qui est fonction du serveur. Le numéro de port par défaut du serveur d'autorisation est **7136**.
ID administrateur *	Spécifie l'identificateur d'un compte administrateur existant du domaine Security Access Manager spécifié. L'ID administrateur par défaut du domaine Security Access Manager est **sec_master**.
Mot de passe administrateur *	Indique le mot de passe associé à l'ID administrateur Security Access Manager spécifié. Ce mot de passe administrateur a été créé lors de la création du compte administrateur.

Tableau 31. Options de configuration de Security Access Manager Web Portal Manager (suite). ***** indique une option obligatoire.

Option de configuration	Description
Domaine *	Indique le nom du domaine. Ce domaine doit déjà exister. Une règle de sécurité appliquée dans un domaine affecte uniquement les objets se trouvant dans ce domaine. Les utilisateurs qui sont autorisés à exécuter des tâches dans un domaine n'ont nécessairement pas le droit d'exécuter ces tâches dans d'autres domaines. Le domaine par défaut est **Default**, c'est-à-dire, le domaine de gestion.

Security Access Manager WebSEAL

Le tableau 32 répertorie les options que vous êtes invité à indiquer pendant la configuration du package Security Access Manager WebSEAL.

Remarque : Configurez le package Security Access Manager Runtime, puis le package Security Access Manager WebSEAL.

Tableau 32. Options de configuration de Security Access Manager WebSEAL. ***** indique une option obligatoire.

Option de configuration	Description
Nom d'instance WebSEAL *	Indique le nom d'hôte complet utilisé par le serveur de règles pour contacter le serveur WebSEAL.
Utilisation de l'interface de réseau logique	Spécifie l'utilisation d'une interface réseau logique. Si vous indiquez **oui**, vous êtes invité à entrer l'adresse IP de l'interface réseau logique.
Nom d'hôte WebSEAL *	Spécifie le nom d'hôte du serveur WebSEAL.
Port d'écoute WebSEAL *	Spécifie le numéro du port sur lequel le serveur WebSEAL intercepte des requêtes. Le numéro de port par défaut est **7234**.
ID administrateur *	Spécifie l'identificateur de l'administrateur Security Access Manager du domaine de gestion. L'ID administrateur par défaut est **sec_master**.
Mot de passe administrateur *	Spécifie le mot de passe associé à l'ID administrateur Security Access Manager.
Autoriser l'accès HTTP (y/n)	Spécifie si l'accès HTTP doit être activé. Si cette option est sélectionnée, vous devez spécifier le numéro de port HTTP. L'accès HTTP est activé par défaut.
Port HTTP [80]	Spécifie le port HTTP. Le numéro de port par défaut est **80**. En cas de conflit avec le port, la configuration le détecte et augmente le numéro de port de manière incrémentielle.

Tableau 32. Options de configuration de Security Access Manager WebSEAL (suite). ***** indique une option obligatoire.

Option de configuration	Description
Autoriser l'accès HTTPS sécurisé (y/n)	Spécifie si l'accès HTTPS doit être activé. Si cette option est sélectionnée, vous devez spécifier le numéro de port HTTPS. L'accès HTTPS est activé par défaut.
Port HTTPS [443]	Spécifie le port HTTPS. Le numéro de port par défaut est **443**. En cas de conflit avec le port, la configuration le détecte et augmente de manière incrémentiellele choix du numéro de port.
Répertoire principal des documents Web [opt/pdweb/www-default/docs]	Les répertoires par défaut sont les suivants : • AIX, Linux et Solaris : `/opt/pdweb/www-default/docs` • Windows : `C:\Progam Files\Tivoli\PolicyDirector \PDWeb\www-default\docs`
Activer SSL avec le serveur de registre	Indique s'il est nécessaire d'activer les connexions SSL (Secure Sockets Layer) chiffrées avec un serveur LDAP. **Remarque :** Vous devez d'abord configurer le serveur LDAP pour accéder à SSL. Valeur par défaut: activée (la case est cochée)
Fichier de clés et chemin complet	Indique le chemin qualifié complet sous lequel le fichier de base de données de clés du client SSL se trouve dans le système d'exécution. Ce fichier de clés doit être extrait du serveur LDAP. N'importe quelle extension de fichier est valide (l'extension `.kdb` est utilisée en général). Servez-vous du fichier de clés SSL pour gérer les certificats utilisés dans les communications SSL. Le signataire du certificat SSL doit être reconnu comme étant une autorité de certification dans la base de données de clés client.
Mot de passe du fichier de clés	Spécifie le mot de passe existant associé au fichier de clés SSL indiqué. Le mot de passe du fichier de clés client a été défini lors de la première création du fichier de clés. Changez ce mot de passe à l'aide de l'utilitaire **gsk8capicmd** (inclus dans GSKit 8) ou de l'utilitaire **ikeyman** (fourni avec IBM Java). Si vous modifiez ce mot de passe, vous devez vous le rappeler.

Tableau 32. Options de configuration de Security Access Manager WebSEAL (suite). ***** indique une option obligatoire.

Option de configuration	Description
Libellé de certificat	Spécifie le libellé du certificat SSL du certificat client dans la base de données de clés SSL qui est envoyé au serveur de registre si ce dernier est configuré pour effectuer l'autorisation du client et du serveur pendant l'établissement de la connexion SSL. Ce libellé n'est valide que lorsque SSL est utilisé et que le serveur de registre a été configuré pour que l'autorisation client soit exigée. En règle générale, le serveur de registre requiert uniquement les certificats côté serveur spécifiés pendant la création du fichier client `.kdb`. Le libellé de certificat correspond à une chaîne alphanumérique sensible à la casse que vous choisissez. Les caractères des valeurs de chaîne doivent faire partie de la page de codes locale. Par exemple : `PDLDAP` Cette zone nécessite l'entrée d'un caractère. Etant donné que vous n'avez pas besoin de configurer l'authentification de certificat côté client, le caractère que vous spécifiez est ignoré.
Port SSL	Spécifie le numéro du port sur lequel le serveur LDAP intercepte des requêtes SSL. Un numéro de port valide peut être tout nombre positif autorisé par le protocole TCP/IP et n'étant pas en cours d'utilisation par une autre application.

Annexe E. Installation du support de langue

Security Access Manager est traduit en plusieurs langues. Les traductions de ces langues sont fournies comme programmes de support de langue nationale pour chaque composant du produit. Pour utiliser les composants du produit dans une langue autre que l'anglais, vous devez installer le support de langue nationale de ce composant.

Utilisez ces instructions pour installer le programme de support de langue nationale si vous appliquez la méthode d'installation via une ligne de commande ou le script d'installation pour installer les composants Security Access Manager.

Si vous utilisez les méthodes d'installation à partir du tableau de bord pour installer les composants Security Access Manager, le programme de support de langue nationale est installé automatiquement et vous n'avez pas besoin d'exécuter ces instructions.

Avant de poursuivre l'installation, veillez à consulter les rubriques relatives au support de langue nationale sur le site Web de support.

Présentation du support de langue

Le logiciel Security Access Manager est traduit dans les langues suivantes :

- Arabe
- Portugais (Br)
- Tchèque
- Chinois (simplifié)
- Chinois (Traditionnel)
- Français
- Allemand
- Hébreu
- Hongrois
- Italien
- Japonais
- Coréen
- Polonais
- Espagnol
- Russe

Remarque :

1. Seuls les panneaux de Web Portal Manager prennent en charge l'hébreu ; les messages et l'aide en ligne s'affichent en anglais.

Les traductions de ces langues sont fournies comme programmes de support de langue nationale pour le produit. Pour obtenir le support de langue de Security Access Manager, vous devez installer le programme de support de langue de ce produit. Chaque langue est une image d'installation de produit distincte.

© Copyright IBM Corp. 2001, 2013

- Si vous utilisez les utilitaires d'installation natifs pour installer Security Access Manager, vous devez installer le module de langue *après* avoir installé les composants Security Access Manager, mais *avant* de les configurer. Si vous n'installez pas le programme de support de langue, le texte du produit associé s'affiche entièrement en anglais.
- Si vous installez Security Access Manager Session Management Server ou Session Management Command Line sous Windows, vous devez installer le module de langue *après* avoir installé le composant Session Management.

Si le support de langue nationale d'un produit est installé et que vous mettez à niveau le produit, vous devez également installer le produit de support de langue correspondant, s'il existe. Consultez la documentation de mise à niveau du produit spécifique pour savoir si le support de langue est requis. Si vous n'installez pas le support de langue après la mise à niveau, il se peut que le produit associé affiche des zones et des messages en anglais.

Installation des modules de support de langue dans Security Access Manager

Activez le support de langue pour Security Access Manager en installant un ou plusieurs programmes de support de langue nationale.

Avant de commencer

Avertissement : Lorsque vous installez les modules linguistiques Security Access Manager, si un jeu de caractères codé sur deux octets est utilisé pour l'installation de la langue, définissez l'environnement local du système d'exploitation de sorte qu'il corresponde à la langue utilisée par le programme d'installation.

Procédure

1. Connectez-vous en tant que **root** ou administrateur.
2. Accédez au DVD du produit ou extrayez les fichiers depuis le fichier archive que vous avez téléchargé à partir de Passport Advantage.
3. Assurez-vous que le module IBM Java Runtime fourni avec Security Access Manager est installé sur votre système d'exploitation spécifique. Pour plus d'informations, consultez l'une des procédures suivantes :
   - «AIX : Installation d'IBM Java Runtime», à la page 32.
   - «Linux : Installation d'IBM Java Runtime», à la page 33.
   - «Solaris : Installation d'IBM Java Runtime», à la page 33.
   - «Windows : Installation d'IBM Java Runtime», à la page 34.
4. En fonction du composant Security Access Manager que vous souhaitez installer, exécutez un ou plusieurs scripts de configuration parmi les suivants.
   - Pour effectuer l'installation à l'aide d'un assistant :
     a. Vérifiez qu'IBM Java Runtime est disponible sur le chemin d'exécution de commande (ou placez le répertoire JRE comme préfixe de commande).
     b. Exécutez la commande suivante :

        ```
        java -jar module_linguistique.jar
        ```

        où *module_linguistique.jar* est le nom du module linguistique à installer :

        carslp.jar
        Installe les modules linguistiques de Service commun de contrôle et de rapport.

pdjrte_lp_setup.jar
Installe les modules linguistiques d'IBM Security Access Manager Runtime for Java.

pdrte_lp_setup.jar
Installe les modules linguistiques de Security Access Manager Runtime.

pdweb_lp_setup.jar
Installe les modules linguistiques de Security Access Manager WebSEAL.

pdwbpi_lp_setup.jar
Installe les modules linguistiques de Security Access Manager Plug-in for Web Servers.

pdwebrte_lp_setup.jar
Installe les modules linguistiques de Security Access Manager Web Security Runtime.

smslp.jar
Installe les modules linguistiques de Security Access Manager Session Management Server, ainsi que Security Access Manager Session Management Command Line.

c. Cliquez sur **Suivant** pour lancer l'installation. La fenêtre Software License Agreement s'affiche.
d. Pour accepter le contrat de licence, cochez la case **I accept** si vous en acceptez les termes.
e. Cliquez sur **Suivant**. Une boîte de dialogue affiche la liste des langues.
f. Sélectionnez les modules linguistiques que vous souhaitez installer.
g. Cliquez sur **Suivant**. Une boîte de dialogue indiquant l'emplacement et les fonctions des langues que vous sélectionnez s'affiche.
h. Pour accepter les langues sélectionnées, cliquez sur **Suivant**. L'assistant d'installation confirme que l'espace disponible sur le disque est suffisant.
i. Pour installer les langues sélectionnées, cliquez sur **Suivant**.
j. Lorsque l'installation du module linguistique de Security Access Manager a abouti, cliquez sur **Terminer** pour fermer l'assistant.

- Pour installer en mode console :
  a. Vérifiez qu'IBM Java Runtime est disponible sur le chemin d'exécution de commande (ou placez le répertoire JRE comme préfixe de commande).
  b. Exécutez la commande suivante :

```
java -jar module_linguistique.jar -console
```

où *module_linguistique.jar* est le nom du module linguistique à installer :

carslp.jar
Installe les modules linguistiques de Service commun de contrôle et de rapport.

pdjrte_lp_setup.jar
Installe les modules linguistiques d'IBM Security Access Manager Runtime for Java.

pdrte_lp_setup.jar
Installe les modules linguistiques de Security Access Manager Runtime.

pdweb_lp_setup.jar
Installe les modules linguistiques de Security Access Manager WebSEAL.

pdwbpi_lp_setup.jar
Installe les modules linguistiques de Security Access Manager Plug-in for Web Servers.

pdwebrte_lp_setup.jar
Installe les modules linguistiques de Security Access Manager Web Security Runtime.

smslp.jar
Installe les modules linguistiques de Security Access Manager Session Management Server, ainsi que Security Access Manager Session Management Command Line.

c. Répondez aux invites qui s'affichent pour installer les modules linguistiques.

- Pour installer en mode silencieux à l'aide d'un fichier de réponses :

  Remarque : La méthode d'installation en mode silencieux n'est pas prise en charge sur les systèmes Linux.

  a. Créez un fichier de réponses.

     Sous AIX ou Solaris :

     1) Ouvrez un éditeur de texte et créez un fichier avec une extension `.rsp`.
     2) Dans le fichier, fournissez les informations spécifiques à votre installation. Basez-vous sur le modèle suivant :

```
########################################
# Auto-accept the license
# Note: By setting this to true you are accepting the terms
# and conditions of the license.
-G licenseAccepted=true
#
# Select languages to install by setting the feature to true.
# Set to false if you do not want to install a language.
#
-P arLangfeature.active=true
-P csLangfeature.active=true
-P deLangfeature.active=true
-P esLangfeature.active=true
-P frLangfeature.active=true
-P huLangfeature.active=true
-P itLangfeature.active=true
-P jaLangfeature.active=true
-P koLangfeature.active=true
-P plLangfeature.active=true
-P pt_BRLangfeature.active=true
-P ruLangfeature.active=true
-P zh_CNLangfeature.active=true
-P zh_TWLangfeature.active=true
```

        Remarque : vérifiez que la ligne suivante a été inclue dans le fichier de réponses :

```
-G licenseAccepted=true
```

     3) Sauvegardez le fichier.

Sous Windows :

1) Sur le support d'installation, localisez le fichier de réponses exemple appelé `\bin\isamLangPack.rsp`.
2) Editez le fichier à l'aide d'un éditeur de texte et utilisez les instructions du fichier pour fournir les informations spécifiques à votre installation.
3) Vérifiez que la ligne suivante a été inclue dans le fichier de réponses :

   ```
   -G licenseAccepted=true
   ```

4) Sauvegardez le fichier.

b. Vérifiez qu'IBM Java Runtime est disponible sur le chemin d'exécution de commande (ou placez le répertoire JRE comme préfixe de commande).

c. Exécutez la commande suivante :

   ```
   java -jar module_linguistique.jar -silent -options fichier_réponses.rsp
   ```

   où *module_linguistique.jar* est le nom du module linguistique à installer :

   carslp.jar
   Installe les modules linguistiques de Service commun de contrôle et de rapport.

   pdjrte_lp_setup.jar
   Installe les modules linguistiques d'IBM Security Access Manager Runtime for Java.

   pdrte_lp_setup.jar
   Installe les modules linguistiques de Security Access Manager Runtime.

   pdweb_lp_setup.jar
   Installe les modules linguistiques de Security Access Manager WebSEAL.

   pdwbpi_lp_setup.jar
   Installe les modules linguistiques de Security Access Manager Plug-in for Web Servers.

   pdwebrte_lp_setup.jar
   Installe les modules linguistiques de Security Access Manager Web Security Runtime.

   smslp.jar
   Installe les modules linguistiques de Security Access Manager Session Management Server, ainsi que Security Access Manager Session Management Command Line.

   et où *fichier_réponses.*.rsp correspond au chemin et au nom du fichier de réponses créé à la première étape.

Installation des programmes de support de langue nationale pour IBM Tivoli Directory Server

Outre l'installation de modules de langue sur le logiciel Security Access Manager, vous devez installer les modules sur le registre d'utilisateurs, comme IBM Tivoli Directory Server.

Ces modules linguistiques sont fournis sur le support du produit Security Access Manager pour les plateformes prises en charge.

Sur IBM Tivoli Directory Server, au moins un module linguistique doit être installé sur tous les systèmes AIX, Linux ou Solaris pour que le client et les utilitaires d'administration IBM Tivoli Directory Server fonctionnent correctement. Pour déterminer si un module linguistique est installé, voir «Variable LANG sur les systèmes AIX, Linux ou Solaris», à la page 369.

Après avoir installé les modules linguistiques de Tivoli Directory Server, vous devez installer le groupe de correctifs pour le module linguistique. L'image du groupe de correctifs image est incluse dans le support de Security Access Manager, sous le répertoire `imagepath/platform/tdsV6.3FP/LangPack`. Voir le fichier Readme contenu dans le répertoire `LangPack` pour obtenir des instructions d'installation.

Après avoir installé les modules linguistiques de Tivoli Directory Server, vous devez installer les modules linguistiques d'IBM DB2.

Utilisez les instructions d'installation du module linguistique contenues dans le centre de documentation d'IBM Tivoli Directory Server : http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml

Avertissement : Lorsque vous installez le produit IBM Tivoli Directory Server, ou ses modules linguistiques, ou les modules linguistiques Security Access Manager, si un jeu de caractères codé sur deux octets est utilisé pour l'installation de la langue, définissez l'environnement local du système d'exploitation de sorte qu'il corresponde à la langue utilisée par le programme d'installation.

Variables d'environnement local

Comme sur la plupart des systèmes d'exploitation courants, vous pouvez localiser le comportement en définissant l'environnement local souhaité. Pour les logiciels Security Access Manager, définissez la variable d'environnement **LANG** sur le nom d'environnement local souhaité tel qu'indiqué par POSIX, X/Open, ou d'autres normes de système ouvert.

Remarque : Si vous travaillez dans un environnement Windows, vous pouvez également modifier le paramètre de langue dans les **Paramètres régionaux** du **Panneau de configuration**.

Si vous définissez la variable d'environnement **LANG** et modifiez les paramètres régionaux, la variable **LANG** remplace ce paramètre régional.

Comme indiqué dans les normes des systèmes ouverts, d'autres variables d'environnement remplacent **LANG** pour tout ou partie des catégories d'environnement local. Les variables possibles sont les suivantes :

- **LC_COLLATE**
- **LC_CTYPE**
- **LC_MONETARY**
- **LC_NUMERIC**
- **LC_TIME**
- **LC_MESSAGES**
- **LC_ALL**

Si l'une de ces variables est définie, vous devez supprimer sa valeur dans la variable **LANG** pour qu'elle soit prenne effet.

Variable LANG sur les systèmes AIX, Linux ou Solaris

La plupart des systèmes AIX, Linux et Solaris utilisent la variable **LANG** pour spécifier l'environnement local souhaité. Toutefois, les différents systèmes d'exploitation AIX, Linux et Solaris requièrent des noms d'environnement local différents pour paramétrer la même langue. Assurez-vous d'indiquer une valeur **LANG** prise en charge par le système d'exploitation AIX, Linux ou Solaris que vous utilisez.

Pour obtenir les noms d'environnements locaux correspondant à votre système AIX, Linux ou Solaris, entrez la commande suivante :

```
locale –a
```

Sur IBM Tivoli Directory Server, au moins un module linguistique doit être installé sur tous les systèmes AIX, Linux et Solaris pour que le client et les utilitaires d'administration IBM Tivoli Directory Server (par exemple **idscfgdb** ou **db2dif**) fonctionnent correctement. Pour vous assurer qu'un module linguistique est installé sur votre système AIX, Linux ou Solaris, entrez la commande suivante :

```
locale
```

Si vous avez chargé un module linguistique (par exemple, **bos.loc.iso.en_us**), la sortie de la commande **locale** sera :

```
LANG=en_US
LC_COLLATE="en_US"
LC_CTYPE="en_US"
LC_MONETARY="en_US"
LC_NUMERIC="en_US"
LC_TIME="en_US"
LC_MESSAGES="en_US"
LC_ALL=
```

Si aucun module linguistique n'est installé, la sortie sera :

```
LANG=en_US
LC_COLLATE="C"
LC_CTYPE="C"
LC_MONETARY="C"
LC_NUMERIC="C"
LC_TIME="C"
LC_MESSAGES="C"
LC_ALL=
```

Variable LANG sur les systèmes Windows

La plupart des systèmes d'exploitation n'utilisent pas la variable d'environnement **LANG**. Toutefois, le logiciel Security Access Manager peut faire appel à la variable **LANG** pour déterminer la langue souhaitée. Pour ce faire, définissez la variable d'environnement **LANG** sur le nom d'environnement canonique basé sur le langage ISO ou les codes de territoire sans suffixe de jeu de code. Par exemple :

- **fr** est le nom d'environnement local pour le français standard
- **ja** est le nom d'environnement local pour le japonais
- **pt_BR** est le nom d'environnement local pour le portugais (Brésil)
- **C** est le nom d'environnement local pour l'anglais dans l'environnement local C

Utilisation de variantes d'environnement local

Même si le logiciel Security Access Manager propose actuellement une version traduite pour chaque langue, vous pouvez utiliser une variante préférentielle d'environnement local. Security Access Manager trouve alors la version traduite correspondante. Par exemple, Security Access Manager propose une traduction pour le français, mais chacun des paramètres d'environnement local suivant permet de rechercher la traduction appropriée :

- **fr** est le nom de l'environnement local pour le français standard
- **fr_FR** est le nom d'environnement local pour le français de France
- **fr_CA** est le nom d'environnement local pour le français du Canada
- **fr_CH** est le nom d'environnement local pour le français de Suisse

Catalogues de messages

Les catalogues de messages sont généralement installés dans un sous-répertoire `msg` ; chacun de ces catalogues de messages est installé dans un sous-répertoire spécifique à la langue. Par exemple, les composants de base de Security Access Manager se trouvent dans les répertoires suivants :

- Sur les systèmes AIX, Linux ou Solaris :
  `/opt/PolicyDirector/nls/msg/`*`locale`*
- Sur les systèmes Windows :
  `rép_install``/nls/msg/`*`locale`*

D'autres composants Security Access Manager utilisent des répertoires similaires pour leurs catalogues de messages.

Security Access Manager détecte les différences entre les noms d'environnements locaux sur AIX, Linux ou Solaris et peut généralement mapper la valeur spécifiée avec le catalogue de messages approprié.

La variable d'environnement **NLSPATH** permet de rechercher le répertoire du catalogue de messages approprié, tel qu'indiqué par les normes des systèmes ouverts. Par exemple, si les catalogues de messages se trouvent dans `/opt/PolicyDirector/nls/msg`, la variable **NLSPATH** est définie comme suit :

```
/opt/PolicyDirector/nls/msg/%L/%N.cat:/opt/PolicyDirector/nls/msg/%L/%N
```

Remarque : Sous Windows, utilisez un point-virgule (**;**) au lieu des deux points (**:**) comme séparateur. Par exemple :

```
C:\Program Files\PolicyDirector\nls\msg\%L\%N.cat;C:\Program
Files\PolicyDirector\nls\msg\%L\%N
```

La directive **%L** est étendue au répertoire de catalogue de messages qui correspond le plus à la sélection de langue actuelle de l'utilisateur, et **%N.cat** est étendue au catalogue de messages souhaité.

Si le catalogue de messages n'est pas trouvé pour la langue souhaitée, les catalogues de messages en anglais **C** sont utilisés.

Par exemple, si vous travaillez sur AIX et indiquez un environnement local suisse allemand comme suit :

```
LANG=De_CH.IBM-850
```

La directive **%L** est étendue dans l'ordre suivant afin de trouver l'environnement local spécifié :

1. **de_CH**
2. **de**
3. **C**

Security Access Manager ne propose pas de module linguistique suisse allemand. L'environnement local **de_CH** est donc introuvable. Si le module linguistique allemand de Security Access Manager est installé, **de** est utilisé. Sinon, l'environnement local par défaut **C** est utilisé. Le texte s'affiche alors en anglais.

Support de codage de texte (jeu de codes)

Les divers systèmes d'exploitation codent souvent le texte de façons différentes. Par exemple, les systèmes Windows utilisent **SJIS** (page de code 932) pour le texte en japonais, tandis que les systèmes AIX, Linux ou Solaris utilisent souvent le système **eucjp**.

En outre, plusieurs environnements locaux peuvent être pris en charge avec une seule langue. Différents jeux de codes peuvent donc être utilisés pour la même langue sur la même machine. Le fait de proposer plusieurs environnements locaux pour la même langue peut entraîner des problèmes lorsque le texte est déplacé d'un système à un autre ou entre deux environnements locaux différents.

Security Access Manager traite ces problèmes en utilisant Unicode et UTF-8 (la forme multi-octets d'Unicode) comme représentation canonique interne du texte.

Les catalogues de messages sont codés en UTF-8 et le texte est converti via le codage de l'environnement local avant d'être affiché à l'écran. Ainsi, les mêmes fichiers de catalogues de messages français peuvent être utilisés pour prendre en charge plusieurs jeux de codes Latin 1, comme ISO8859-1, Microsoft 1252, IBM PC 850, et IBM MVS™ 1047.

UTF-8 permet également de garantir l'interopérabilité du texte. Par exemple, les chaînes COBRA (Common Object Request Broker Architecture) sont transmises au format UTF-8. Cela permet d'effectuer une gestion à distance sur un réseau hétérogène où le codage de texte d'environnement local peut varier. Par exemple, les noms de fichiers japonais peuvent être manipulés sur des noeuds finaux de PC japonais à partir d'un poste de travail exécutant l'environnement local AIX, Linux ou Solaris japonais EUC.

En outre, pour assurer l'interopérabilité du texte sur un domaine sécurisé, les chaînes sont stockées au format UTF-8 dans la base de données d'objets Tivoli. Les chaînes sont converties via le codage d'environnement local pour permettre de les afficher et de les manipuler sous des applications s'exécutant sur différents jeux de code de système d'exploitation.

Emplacement des fichiers de jeu de codes

L'interopérabilité sur l'ensemble du domaine sécurisé dépend des fichiers de jeux de codes, utilisés pour effectuer les conversions UTF-8 et d'autres types de traitement de texte relatifs au codage. Ces fichiers sont installés dans les répertoires suivants :

- Sur les systèmes AIX, Linux ou Solaris :
  `/opt/PolicyDirector/nls/TIS`
- Sur les systèmes Windows :
  rép_install`\nls\TIS`

Désinstallation des programmes de support de langue nationale Security Access Manager

Appliquez la procédure suivante pour désinstaller les programmes de support de langue nationale pour Security Access Manager.

Avant de commencer

Annulez la configuration de tous les composants Security Access Manager avant de désinstaller les modules linguistiques. Voir Annexe K, «Désinstallation», à la page 429.

Procédure

1. Sélectionnez le répertoire de désinstallation du module que vous souhaitez désinstaller :
   - Sur les systèmes AIX, Linux ou Solaris :

     Web Security Runtime
     `/AMWebRTELP/lp_uninst`

     Plug-in for Web Servers
     `/PDWpiLP/lp_uninst`

     Runtime
     `/opt/PolicyDirector/PDBLP/lp_uninst`

Runtime for Java
/opt/PolicyDirector/PDJrtLP/lp_uninst

Session Management Server et Session Management Command Line
/opt/pdsms/SMSLP/lp_uninst

WebSEAL
/opt/pdweb/PDWebLP/lp_uninst

- Sur les systèmes Windows :

Web Security Runtime
c:\Program Files\Tivoli\PDWebRTE\AMWebRTELP\lp_uninst

Plug-in for Web Servers
c:\Program Files\Tivoli\PDWebPI\PDWpiLP/lp_uninst

Runtime
c:\Program Files\Tivoli\Policy Director/PDBLP/lp_uninst

Runtime for Java
c:\Program Files\Tivoli\Policy Director\PDJrtLP/lp_uninst

Session Management Server et Session Management Command Line
c:\Program Files\Tivoli\PDSMS\SMSLP\lp_uninst

WebSEAL
c:\Program Files\Tivoli\PDWeb/PDWebLP/lp_uninst

2. Pour désinstaller les programmes de support de langue, entrez l'une des commandes suivantes :
   - Sur les systèmes AIX, Linux ou Solaris :
     chemin_jre/java -jar *module*
   - Sur les systèmes Windows :
     chemin_jre\java -jar *module*

   où *chemin_jre* désigne le chemin d'accès au fichier Java et *package* désigne l'une des options suivantes :

   Remarque : Si le fichier Java se trouve sous ce chemin d'accès, vous n'avez pas besoin de spécifier la variable *chemin_jre*.

   cars_lp_uninstall.jar
   Désigne l'emplacement des modules linguistiques des composants Service commun de contrôle et de rapport.

   pdrte_lp_uninstall.jar
   Désigne l'emplacement des modules linguistiques de Security Access Manager Runtime.

   pdjrte_lp_uninstall.jar
   Désigne le module linguistique d'IBM Security Access Manager Runtime for Java.

   pdsms_lp_uninstall.jar
   Désigne l'emplacement des modules linguistiques de Security Access Manager Session Management Server et de Security Access Manager Session Management Command Line.

   pdwbpi_lp_uninstall.jar
   Désigne le module linguistique pour Plug-in for Web Servers.

pdweb_lp_uninstall.jar
Désigne le module linguistique pour Security Access Manager WebSEAL.

pdwebrte_lp_uninstall.jar
Désigne le module linguistique pour Security Access Manager Web Security Runtime.

Remarque : Si un message s'affiche indiquant qu'un fichier de propriétés existe pour une langue et vous demande si vous souhaitez supprimer le fichier, cliquez sur **Yes to All**. Poursuivez la désinstallation. Si le texte qui apparaît en fin de désinstallation affiche des erreurs en relation avec la suppression de fichiers, vérifiez les répertoires de désinstallation et assurez-vous que les fichiers ont bien été supprimés. Si les fichiers existent toujours, supprimez-les.

Annexe F. Gestion des mots de passe

L'utilitaire `pdconf` vous permet de masquer ou supprimer les mots de passe qui sont stockés dans un fichier de configuration.

Les mots de passe qui sont utilisés lors de la configuration automatisée sont inscrits et stockés dans un fichier d'options. Vous pouvez masquer ces mots de passe à tout moment. Vous pouvez également supprimer ces mots de passe dans un fichier d'options après avoir terminé la configuration.

Pour gérer les mots de passe de configuration dans les fichiers d'options, voir les activités suivantes :

Tableau 33. Tâches liées aux mots de passe de configuration automatisée

Objectif	Tâche
Masquer un mot de passe sous AIX, Linux ou Solaris	«Masquage des mots de passe sous AIX, Linux ou Solaris», à la page 376
Masquer un mot de passe sous Windows	«Masquage des mots de passe sous Windows», à la page 377
Supprimer un mot de passe sous AIX, Linux ou Solaris	«Suppression d'un mot de passe stocké sous AIX, Linux et Solaris», à la page 379
Supprimer un mot de passe sous Windows	«Suppression d'un mot de passe enregistré sous Windows», à la page 380

A propos des fichiers d'options de configuration

Un fichier d'*options* contient des variables, telles que des mots de passe. Le script de configuration automatique utilise le contenu du fichier d'options afin de faciliter une configuration en mode silencieux.

Par défaut, les valeurs incluses dans le fichier d'options sont vides. Avant d'utiliser le script de configuration automatique, complétez le modèle de fichier d'options avec les mots de passe requis.

- Sous Windows, le fichier d'options `configure_isam.conf` stocke les mots de passe de configuration.
- Sous AIX, Linux ou Solaris, chaque composant possède un fichier d'options de configuration par défaut, qui porte le nom

  `configure_`*`composant`*`.options.template`

  où *composant* désigne un composant installé.

  Voir la section «Masquage des mots de passe sous AIX, Linux ou Solaris», à la page 376, qui contient un tableau de noms de fichiers pour les systèmes AIX, Linux et Solaris.

Meilleures pratiques pour la sécurité des mots de passe de configuration

Le fichier d'options de configuration utilisé par le script de configuration automatique stocke par défaut les mots de passe en texte clair. Vous pouvez, en

© Copyright IBM Corp. 2001, 2013

option, masquer les mots de passe. Voir «Masquage des mots de passe sous AIX, Linux ou Solaris» ou «Masquage des mots de passe sous Windows», à la page 377

Toutefois, les mots de passe masqués sont renvoyés en texte clair lorsque vous spécifiez les options `pdconf`, `getstanza` ou `getentry`.

Pour réduire les problèmes de sécurité concernant les mots de passe stockés, vous pouvez supprimer l'entrée qui contient le mot de passe dans le fichier d'options de configuration. Voir «Suppression d'un mot de passe stocké sous AIX, Linux et Solaris», à la page 379 or «Suppression d'un mot de passe enregistré sous Windows», à la page 380.

Masquage des mots de passe sous AIX, Linux ou Solaris

Exécutez l'utilitaire `pdconf` pour masquer les mots de passe stockés dans les fichiers d'options de configuration sous AIX, Linux ou Solaris.

Avant de commencer

Vous devez modifier le fichier modèle d'options par défaut contenant les mots de passe pour que le script de configuration automatique achève la configuration automatisée. Reportez-vous aux instructions de configuration relatives au composant que vous installez :

- «Automatisation de la configuration d'un serveur de règles», à la page 126
- «Automatisation de la configuration d'un serveur d'autorisations», à la page 140
- «Automatisation de la configuration d'un système d'exécution pour un système Java», à la page 165
- «Automatisation de la configuration d'un serveur proxy de règles», à la page 178
- «Automatisation de la configuration d'un système d'exécution», à la page 191
- «Automatisation de la configuration de Web Portal Manager», à la page 217
- «Automatisation de la configuration du plug-in de serveur Apache ou IBM HTTP Server», à la page 248
- «Automatisation de la configuration d'un serveur de gestion de sessions», à la page 307
- «Automatisation de la configuration d'une ligne de commande de gestion de sessions», à la page 322

Pourquoi et quand exécuter cette tâche

Les mots de passe requis sont affichés dans le fichier d'options afin de faciliter les configurations automatisées.

Vous pouvez exécuter l'utilitaire `pdconf` pour masquer n'importe quel un mot de passe spécifié. Par défaut, le fichier `pdconf` se trouve dans le sous-répertoire `/opt/PolicyDirector/sbin/`.

Procédure

1. Localisez le fichier d'options sur votre système. Vous devez connaître son emplacement pour pouvoir accomplir les étapes suivantes. L'emplacement par défaut du fichier modèle est :

   `/opt/PolicyDirector/example/config`

Le tableau suivant indique le nom par défaut du fichier modèle d'options sous AIX, Linux ou Solaris pour chaque composant :

Tableau 34. Fichiers modèles d'options de composant par défaut sous AIX, Linux, ou Solaris

Composant	Fichier d'options sous AIX, Linux ou Solaris
Serveur de règles	`configure_policysvr.options.template`
Serveur d'autorisations	`configure_authzsvr.options.template`
Système Java	`configure_javarte.options.template`
Serveur de règles proxy	`configure_policysvproxy.options.template`
Système d'exécution	`configure_runtime.options.template`
Web Portal Manager	`configure_wpm.options.template`
Attribute Retrieval Service	`configure_webars.options.template`
Plug-in for Web servers	`configure_webpi.options.template`
Serveur de gestion de sessions - configuration	`configure_sms.options.template`
Serveur de gestion de sessions - déploiement	`deploy_sms.options.template`
WebSEAL	`configure_webseal.options.template`

2. Ouvrez le fichier et notez les valeurs d'entrée et de mot de passe que vous souhaitez masquer.
3. Exécutez la commande suivante :

   ```
   /opt/PolicyDirector/sbin/pdconf -f configure_composant.options.template
   setentry -obfuscate config entrée mot de passe
   ```

   Où :

   configure_*composant*.**options.template**
   Est le modèle de fichier d'options contenant les mots de passe du script de configuration automatique. *composant* est le composant Security Access Manager. Ce fichier peut être enregistré sous un nom différent.

   -obfuscate
   Indique de ne pas enregistrer la valeur sous forme de texte en clair.

   config Est le nom de la strophe dans laquelle la valeur est inscrite.

   Remarque : Le nom de cette strophe doit être `config`.

   entrée Est la clé correspondant à la variable d'environnement dans le fichier modèle. Par exemple, `SECMASTERPWD`.

   mot de passe
   Est le mot de passe à masquer.

Masquage des mots de passe sous Windows

Exécutez l'utilitaire `pdconf.exe` pour masquer les mots de passe contenus dans les fichiers d'options de configuration sous Windows.

Avant de commencer

Vous devez modifier le fichier modèle d'options par défaut contenant les mots de passe pour que le script de configuration automatique achève la configuration automatisée. Reportez-vous aux instructions de configuration relatives au composant que vous installez :

- «Automatisation de la configuration d'un serveur de règles», à la page 126
- «Automatisation de la configuration d'un serveur d'autorisations», à la page 140
- «Automatisation de la configuration d'un système d'exécution pour un système Java», à la page 165
- «Automatisation de la configuration d'un serveur proxy de règles», à la page 178
- «Automatisation de la configuration d'un système d'exécution», à la page 191
- «Automatisation de la configuration de Web Portal Manager», à la page 217
- «Automatisation de la configuration du plug-in Internet Information Service», à la page 249
- «Automatisation de la configuration d'un serveur de gestion de sessions», à la page 307
- «Automatisation de la configuration d'une ligne de commande de gestion de sessions», à la page 322

Pourquoi et quand exécuter cette tâche

Les mots de passe requis sont affichés dans le fichier d'options afin de faciliter les configurations automatisées.

Vous pouvez exécuter l'utilitaire `pdconf` pour masquer n'importe quel un mot de passe spécifié. Par défaut, le fichier `pdconf` se trouve dans le sous-répertoire `C:\Program Files\Tivoli\Policy Director\sbin\`.

Procédure

1. Localisez le fichier d'options sur votre système. Vous devez connaître son emplacement pour pouvoir accomplir les étapes suivantes. Par défaut, ces fichiers modèles sont installés à l'emplacement suivant:

   ```
   C:\Program Files\Tivoli\PolicyDirector\example\config
   ```

2. Ouvrez le fichier `configure_isam.conf` et notez les valeurs de l'entrée et du mot de passe que vous souhaitez masquer.
3. Exécutez la commande suivante :

   ```
   C:\Program Files\Tivoli\Policy Director\sbin\pdconf -f configure_isam.conf
   setentry -obfuscate config entrée mot de passe
   ```

   Où :

   configure_isam.conf
   Est le modèle de fichier d'options contenant les mots de passe du script de configuration automatique.

   -obfuscate
   Indique que la valeur ne doit pas être stockée sous forme de texte en clair.

   config Est le nom de la strophe dans laquelle la valeur est inscrite.

   Remarque : Ce nom de strophe nom doit être `config`.

entrée Est la clé correspondant à la variable d'environnement dans le fichier modèle. Par exemple, `SECMASTERPWD`.

mot de passe
Est le mot de passe à masquer.

Suppression d'un mot de passe stocké sous AIX, Linux et Solaris

Exécutez l'utilitaire `pdconf` pour supprimer les mots de passe stockés dans un fichier de configuration sous AIX, Linux ou Solaris.

Avant de commencer

Vous devez modifier le fichier modèle d'options par défaut contenant les mots de passe pour que le script de configuration automatique achève la configuration automatisée. Reportez-vous à la procédure "Automatisation de la configuration d'un *composant*" relative au composant concerné dans le manuel *IBM Security Access Manager for Web : Guide d'installation*.

Pourquoi et quand exécuter cette tâche

Les mots de passe requis sont affichés dans le fichier d'options afin de faciliter les configurations automatisées.

Les mots de passe masqués sont renvoyés sous forme de texte en clair lorsque l'option `pdconf` de `getstanza` ou `getentry` est spécifiée.

Pour éviter l'exposition d'un mot de passe, supprimez tous les mots de passe lorsque vous avez fini d'utiliser le script de configuration.

Procédure

1. Localisez le fichier d'options sur votre système. Vous devez connaître son emplacement pour pouvoir accomplir les étapes suivantes. L'emplacement par défaut du fichier d'options est `/opt/PolicyDirector/example/config`.
2. Exécutez l'outil `pdconf` :

   ```
   chemin_outil_pdconf/pdconf -f chemin_fichier_options/fichier_options
   deleteentry strophe entrée
   ```

   Où :

   chemin_outil_pdconf
   Désigne le répertoire dans lequel se trouve l'outil `pdconf.exe`. Par défaut, ce chemin d'accès est `opt/PolicyDirector/sbin/pdconf`.

   fichier_options
   Spécifie le nom du fichier d'options de configuration qui contient le mot de passe. Le modèle par défaut des fichiers d'options pour chaque composant est appelé `configure_`*`composant`*`.options.template`, mais il se peut que vous l'ayez renommé.

   deleteentry
   Supprime l'entrée et la valeur dans la strophe spécifiée par le fichier d'options.

   strophe Indique le nom de la strophe dans laquelle vous souhaitez supprimer le mot de passe.

entrée Indique l'entrée du fichier d'options de configuration spécifié et la strophe. Par exemple, `SECMASTERPWD`.

Suppression d'un mot de passe enregistré sous Windows

L'utilitaire `pdconf` vous permet de supprimer les mots de passe qui sont stockés dans un fichier d'options de configuration sous Windows.

Avant de commencer

Vous devez modifier le fichier modèle d'options par défaut contenant les mots de passe pour que le script de configuration automatique achève la configuration automatisée. Reportez-vous à la procédure "Automatisation de la configuration d'un *composant*" relative au composant concerné dans le manuel *IBM Security Access Manager for Web : Guide d'installation*.

Pourquoi et quand exécuter cette tâche

Les mots de passe requis sont affichés dans le fichier d'options afin de faciliter les configurations automatisées.

Les mots de passe masqués sont renvoyés sous forme de texte en clair lorsque l'option `pdconf` de `getstanza` ou `getentry` est spécifiée.

Pour éviter l'exposition d'un mot de passe, supprimez tous les mots de passe lorsque vous avez fini d'utiliser le script de configuration.

Procédure

1. Localisez le fichier d'options sur votre système. Vous devez connaître son emplacement pour pouvoir accomplir les étapes suivantes.

   L'emplacement par défaut des fichiers d'options est : `C:\Program Files\Tivoli\Policy Director\examples\config\configure_isam.conf`.
2. Exécutez l'outil `pdconf` :

   ```
   chemin_outil_pdconf\pdconf -f
   "chemin_fichier_options\configure_isam.conf" deleteentry strophe entrée
   ```

   Où :

   chemin_outil_pdconf
   Désigne le répertoire dans lequel se trouve l'outil `pdconf.exe`. Par défaut, ce chemin d'accès est `C:\Program Files\Tivoli\Policy Director\sbin\pdconf`.

   "*chemin_fichier_options**fichier_options*"
   Spécifie le chemin d'accès et le nom du fichier d'options de configuration qui contient le mot de passe. Cette donnée doit être mise entre guillemets si le chemin contient des espaces. Le fichier d'options est appelé `configure_isam.conf`.

   deleteentry
   Supprime l'entrée et la valeur dans la strophe spécifiée par le fichier d'options.

   strophe Indique le nom de la strophe dans laquelle vous souhaitez supprimer le mot de passe.

   entrée Indique l'entrée du fichier d'options de configuration spécifié et la strophe. Par exemple, `SECMASTERPWD`.

Annexe G. Configuration du serveur de règles de secours (AIX)

Vous pouvez configurer un serveur de secours pour prendre en charge les fonctions de serveur de règles en cas de panne système ou d'indisponibilité non planifiée.

Lorsque le serveur de règles s'arrête, le serveur de règles de secours agit comme serveur de règles jusqu'à ce que le serveur de règles primaire remplisse son rôle d'origine. A son tour, le serveur de règles de secours remplit à nouveau un rôle de secours. A un moment donné, il n'y a *qu'un seul* serveur de règles actif et *qu'une seule* copie partagée des bases de données de règles.

Security Access Manager prend en charge l'utilisation d'un serveur de règles de secours sur les plateformes AIX prises en charge. De plus, le déploiement d'un serveur de règles de secours requiert l'installation et la configuration du logiciel High Availability Cluster Multi-Processing (IBM PowerHA, anciennement HACMP), une solution de groupement conçue pour proposer un accès de grande disponibilité aux données de métier et à l'application via la redondance des composants et au basculement de l'application.

Le scénario PowerHA est fourni comme un guide général qui vous explique comment installer et configurer un environnement PowerHA pour la capacité du serveur de règles de secours. Une fois que vous avez configuré votre environnement PowerHA, suivez les instructions spécifiques au produit concernant la création d'un serveur de règles de secours dans un domaine sécurisé Security Access Manager. Des scripts et des exemples vous sont proposés et vous les utilisez à votre convenance.

Pour obtenir des informations sur l'installation et la configuration PowerHA, voir :

- IBM PowerHA SystemMirror 7.1 : http://pic.dhe.ibm.com/infocenter/aix/v7r1/topic/com.ibm.aix.powerha.navigation/powerha_main.htm
- IBM PowerHA SystemMirror 6.1 : http://pic.dhe.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.powerha.navigation/powerha_main.htm
- IBM PowerHA for AIX Cookbook : http://www.redbooks.ibm.com/redbooks/pdfs/sg247739.pdf
- L'aide-mémoire PowerHA for AIX (anciennement HACMP) : http://www.ibm.com/developerworks/aix/library/au-hacmpcheatsheet/index.html

Règles

- Vous pouvez créer un serveur de règles primaire et un serveur de règles de secours.
- Les serveurs de règles à la fois primaires et de secours doivent être placés sur les systèmes AIX qui font partie d'un environnement High Availability Cluster Multi-Processing (PowerHA).
- Chaque système AIX doit avoir accès à une grappe de disques partagée configurée pour la redondance de données.
- La base de données de règles et les fichiers de configuration utilisés par le serveur de règles doivent se trouver sur une batterie de disques partagée.

© Copyright IBM Corp. 2001, 2013

- Le serveur de registre, tel que IBM Tivoli Directory Server, doit être disponible et installé sur un système distinct.
- Sauvegardez les données partagées ou toute autre base de données de règles partagées avant de configurer les serveurs primaire et de secourssur le système de fichiers partagé.

Scénario d'environnement IBM PowerHA

Ce scénario est simplement un exemple de la façon d'installer et de configurer un environnement PowerHA pour la capacité du serveur de règles de secours. Dans cet exemple de scénario, comme dans les autres environnements PowerHA qui prennent en charge une capacité de serveur de règles de secours, vous devez configurer l'environnement PowerHA pour la reprise de l'adresse IP du service de système primaire, ainsi que pour l'accès partagé à un système de fichiers externe.

Pour des détails complets sur l'installation et la configuration de ces environnements, consultez les documents de PowerHA inclus lorsque vous avez acheté votre produit PowerHA. En cas de problème de service impliquant PowerHA, contactez le support IBM pour les produits concernés.

Ce scénario fournit des instructions de configuration d'un serveur de règles sur chacun des deux systèmes AIX. Les systèmes hôte utilisés dans ce scénario sont les suivants :

- `tucana` possède une adresse IP de service `192.168.2.13`, une adresse IP de démarrage `192.168.2.79` et une adresse IP de secours qui doivent se trouver sur un sous-réseau différent des adresses IP de service et de démarrage `192.168.3.2`. Ces adresses IP exigent que deux adaptateurs de réseau, tels que des adaptateurs Ethernet, soient disponibles sur `tucana`. Seuls deux adaptateurs de réseau sont nécessaires car, dans un environnement PowerHA, l'adresse IP de service est activée et l'adresse IP de démarrage est désactivée *après* que le cluster PowerHA a été démarré sur un noeud PowerHA.
- `perseus` possède une adresse IP de service `192.168.2.14`, une adresse IP de démarrage `192.168.2.80` et une adresse IP de secours qui doivent se trouver sur un sous-réseau différent des adresses IP de service et de démarrage `192.168.3.3`. Ces adresses IP exigent que deux adaptateurs de réseau, tels que des adaptateurs Ethernet, soient disponibles sur `perseus`.

Remarque : Les adresses IP de service et de démarrage de *chaque* système AIX utilisent le *même* adaptateur de réseau. L'adresse IP de secours de chaque système AIX utilise le second adaptateur de réseau.

Le serveur de règles primaire est installé et configuré sur le système AIX primaire. Le système hôte primaire de ce scénario est `tucana`.

Le serveur de règles de secours est installé et configuré sur le système AIX de secours. L'autre système hôte de ce scénario est `perseus`.

Installation et configuration d'IBM PowerHA pour AIX

Appliquez le scénario suivant pour configurer un environnement IBM PowerHA de base sur IBM AIX.

Procédure

1. Installez le système d'exploitation AIX à l'aide des CD d'installation AIX, y compris tous les packages `rsct` et le module de mise à jour adéquat.

2. Installez le logiciel PowerHA et les composants prérequis du système d'exploitation AIX. Suivez les instructions fournies avec le logiciel.
3. Configurez le cluster PowerHA.

Que faire ensuite

Une fois le cluster PowerHA configuré, passez à l'étape «Création d'un environnement de serveur de règles de secours».

Création d'un environnement de serveur de règles de secours

Vous pouvez créer un environnement de serveur de règles de secours à utiliser en cas de reprise nécessaire du serveur de règles principal.

Procédure

1. Sur les *deux* systèmes de serveur de règles primaire et de secours, créez un ID utilisateur **ivmgr**, un ID groupe **ivmgr** et un ID utilisateur **tivoli** ainsi qu'un ID groupe **tivoli**. Avant de créer ces ID, vérifiez que le fichier `/etc/security/limits` de chaque système possède les mêmes paramètres par défaut (lors de la création des ID utilisateur et groupe). Ces paramètres permettent de s'assurer que les ID utilisateur et groupe sont créés avec les mêmes caractéristiques sur ces deux systèmes.
   Pour créer ces ID, procédez de l'une des manières suivantes :
   - Utilisez l'utilitaire SMIT afin de vérifier que *les deux* systèmes AIX utilisent le même numéro pour chaque ID. Par exemple, les deux systèmes doivent posséder le même numéro d'ID pour l'ID utilisateur **ivmgr**. De plus, les numéros d'ID doivent être différents pour chacun des quatre ID.
   - Créez un script identique au modèle présenté dans «Script : paramétrage des ID utilisateur pour les systèmes primaires et de secours», à la page 387. Exécutez ce script pour paramétrer les ID pour les utilisateurs et les groupes **ivmgr** > **tivoli**. Par exemple, si ce script a été nommé **`setivug`**, la commande suivante crée un groupe **ivmgr** avec un ID `250`, un utilisateur **ivmgr** avec un ID `251`, un groupe **tivoli** avec un ID `260`, ainsi qu'un utilisateur **tivoli** avec un ID `261` :

     ```
     ./setivug 250 251 260 261
     ```

     Remarque : Assurez-vous que les quatre valeurs des ID utilisateur ne sont pas en cours d'utilisation sur système *avant* de les créer.
2. Après avoir configuré et démarré le cluster PowerHA sur vos deux systèmes, créez un répertoire tel que `/share` dans le système de fichiers partagé qui peut être installé sur ces systèmes. Par exemple, créez un répertoire `/share` sur la tour de stockage SSA externe partagée. Pour ce faire, procédez comme suit.
   a. Sur le système qui héberge le serveur de règles principal, créez un répertoire `/share` dans le système de fichiers partagé. Ce répertoire partagé, situé dans la tour de stockage SSA externe, contient des informations importantes qui doivent être partagées entre les serveurs de règles primaire et de secours.
   b. Créez un sous-répertoire `/share` nommé `/PolicyDirector` (`/share/PolicyDirector`). Vérifiez également que **ivmgr** est le propriétaire et que **ivmgr** est le groupe associé aux *deux* répertoires.
   c. Utilisez les menus SMIT HACMP pour simuler un scénario de reprise de protocole IP. Pour ce faire, arrêtez les services de cluster sur la machine de serveur de règles principal en utilisant l'option **Arrêter les services de cluster**. Une fois le cluster arrêté sur le serveur de règles primaire, le

serveur de règles de secours prend en charge l'adresse ID de service du serveur de règles primaire et peut accéder aux répertoires `/share` et `/share/PolicyDirector` dans le système de fichiers partagé.

d. A partir du système de serveur de règles de secours, exécutez la commande **ls –l** pour valider le fait que ces deux répertoires sont associés à l'utilisateur **ivmgr** et au groupe **ivmgr**.

e. Redémarrez le cluster sur le serveur de règles primaire. Une fois le redémarrage effectué, l'adresse IP de service est restaurée sur le système du serveur de règles principal et le système de fichiers partagé est installé sur le système du serveur de règles principal.

3. ***Sur le serveur de règles principal***, procédez comme suit :

a. Installez et configurez les composants Security Access Manager requis. Pour obtenir des instructions, voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109. figure 1 présente l'emplacement des fichiers de clés une fois le serveur de règles primaire installé et configuré.

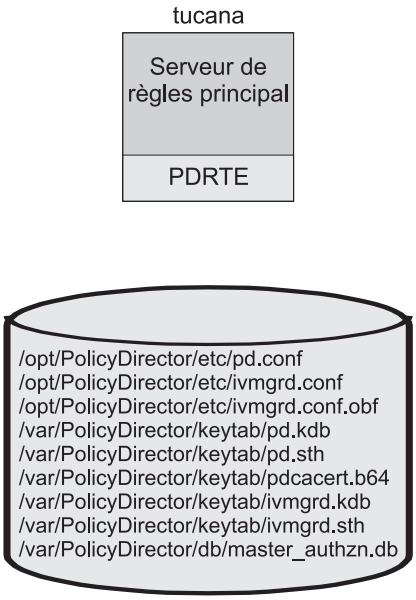


Figure 1. Serveur de règles primaire après la configuration initiale

b. Arrêtez le serveur de règles principal.

c. Editez le fichier `/opt/PolicyDirector/etc/ivmgrd.conf` et procédez comme suit.

1) Dans la section `[ssl]`, changez la valeur de l'entrée `ssl-io-inactivity-timeout` en `300`.

2) Dans la section `[configuration-database]`, mettez à jour l'entrée `file=` pour indiquer l'emplacement complet qualifié du fichier `ivmgrd.conf.obf` dans le système de fichiers externe SHARED. Par exemple : `file=/share/PolicyDirector/etc/ivmgrd.conf.obf`

d. Editez le fichier `/opt/PolicyDirector/pd.conf` et changez le nom d'hôte du serveur de règles primaire afin qu'il corresponde au nom d'hôte de l'interface IP de service qui a été configurée dans votre configuration PowerHA pour ce système. Dans l'exemple présenté dans «Installation et configuration d'IBM PowerHA pour AIX», à la page 382, cette valeur du nom d'hôte est `tucana`.

e. Une fois les changements enregistrés dans les fichiers de configuration, créez un script identique au modèle présenté dans «Script : création de liens entre fichiers et répertoires sur le système principal», à la page 389. Exécutez ce script sur le serveur de règles primaire afin d'associer les fichiers et les répertoires requis au système de fichiers partagé (`/share`). La figure 2 illustre l'emplacement des fichiers de clés une fois qu'ils ont été déplacés dans le système de fichiers partagé. Notez que le serveur de règles de secours n'est pas encore configuré.

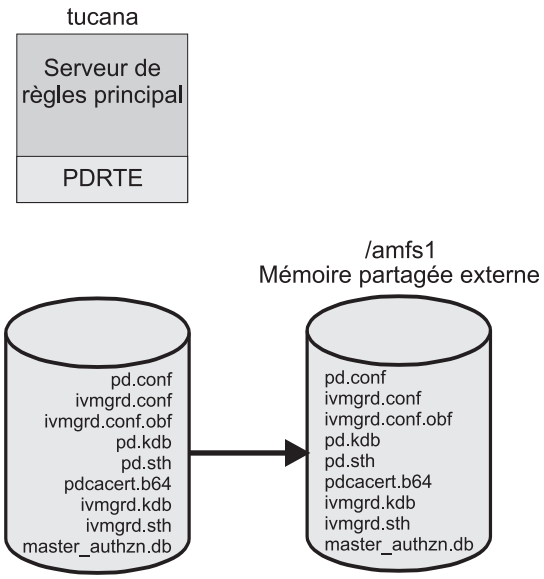


Figure 2. Serveur de règles principal après l'intégration de l'utilisation du système de fichiers partagé

f. Redémarrez le serveur de règles principal.

g. Vérifiez la structure du répertoire, l'emplacement du fichier, les liens lointains et les autorisations des fichiers, comme le montre la page «Exemple : vérification des répertoires de serveur primaire, des liens lointains et des autorisations», à la page 390.

4. ***Sur le serveur de règles de secours***, procédez comme suit.

   a. Installez (*sans les configurer*) les composants Security Access Manager requis à l'aide de l'utilitaire d'installation native, tel que **`installp`**. Pour obtenir des instructions, voir «AIX : Installation du serveur de règles», à la page 113.

   b. Vérifiez que le cluster PowerHA est exécuté sur ce système et validez le fait que le système de fichiers externe partagé (`/share/PolicyDirector`) est accessible.

      Cette étape est nécessaire pour que le processus de configuration puisse accéder aux fichiers `.conf` qui sont stockés dans le système de fichiers.

      Pour que le serveur de règles de secours puisse accéder à ce système de fichiers externe partagé, le serveur de règles primaire doit être arrêté. Pour ce faire, utilisez les menus SMIT HACMP pour arrêter les services de cluster en sélectionnant l'option **Arrêter les services de cluster** sur le système du serveur de règles principal.

      Une fois le cluster arrêté sur ce système et une fois l'opération de reprise de PowerHA exécutée (ce qui prend moins d'une minute), vérifiez que le système de serveur de règles de secours a pris en charge l'adresse IP de

service du serveur de règles principal et que le système de fichiers partagé est installé sur le système de serveur de règles de secours.

c. Configurez le serveur de règles de secours, y compris le composant d'exécution, à l'aide de l'utilitaire **pdconfig**. Pour obtenir des instructions, voir «AIX : Installation du serveur de règles», à la page 113 et «AIX : Installation de Security Access Manager Runtime», à la page 182.

   Remarque : Le serveur de règles principal n'a pas besoin d'être en cours d'exécution pour qu'un serveur de règles de secours puisse être configuré. Cependant, le serveur de registre utilisé par le serveur de règles primaire doit être disponible et exécuté sur un système différent du système de serveur de règles primaire.
   Lors de la configuration, l'utilitaire **pdconfig** détecte qu'il existe déjà une configuration de serveur de règles. Répondez y (Oui) aux invites suivantes :
   `Un serveur de règles est déjà configuré sur ce serveur LDAP. Un second serveur de règles peut être configuré uniquement à des fins de migration ou de secours. Voulez-vous configurer un second serveur de règles pour ce serveur LDAP ? (y/n) [Non] y Utilisation du serveur de règles pour la fonction de secours (y=oui/n=non) [No] : y`
   Lorsque vous y êtes invité, tapez l'emplacement “complet qualifié” du fichier `ivmgrd.conf` (fichier de configuration du serveur de règles existant). Par exemple, si le répertoire partagé est `/share`, tapez ce qui suit :`/share/PolicyDirector/ivmgrd.conf`
   L'utilitaire **pdconfig** établit un lien vers ce fichier dans le répertoire `/opt/PolicyDirector/etc` et modifie le fichier `ivmgrd.conf` pour activer l'opération de secours.
   Remarque : Après une configuration effectuée avec succès du serveur de règles de secours, celui-ci *n'est pas* démarré. Il est automatiquement démarré *uniquement* après qu'un état de basculement a été détecté par le logiciel PowerHA exécuté sur le serveur de règles de secours. Sinon, de graves erreurs et des conflits peuvent se produire si *à la fois* les serveurs de règles primaires et de secours tentent une exécution simultanée.

d. Créez un script identique au modèle présenté dans «Script : création d'un lien allant des fichiers système AIX vers le répertoire partagé sur le système de secours», à la page 392. Exécutez ce script pour établir un lien allant des fichiers système AIX vers le répertoire partagé.

e. Vérifiez la structure du répertoire, l'emplacement du fichier, les liens lointains et les autorisations des fichiers, comme le montre la page «Exemple : vérification des répertoires de serveur de secours, des liens lointains et des autorisations», à la page 393.

   Remarque : Etant donné que les deux systèmes partagent ce répertoire, le contenu de `/share/PolicyDirector` sur le serveur de secours doit être identique au contenu affiché pour le serveur primaire.

Résultats

La configuration des serveurs de règles primaire et de secours est désormais terminée. A ce stade, le cluster PowerHA est arrêté sur le système de serveur de règles principal et en cours de fonctionnement sur le système de serveur de règles de secours.

Avant de tester les capacités de basculement du serveur de règles, une vérification doit être effectuée pour s'assurer que le serveur de règles exécutable est bien défini dans la configuration PowerHA comme un serveur d'applications. Pour effectuer

une vérification à l'aide de l'utilitaire SMIT, sélectionnez **Show Cluster Resources** dans le panneau PowerHA Cluster Resources pour afficher les ressources du cluster.

Pour définir un serveur d'applications, sélectionnez l'option **Add an Application Server** dans le panneau PowerHA Define Application Servers. Une fois ce panneau sélectionné, le script de démarrage (`/usr/bin/pd_start start`) et le script d'arrêt (`/usr/bin/pd_start stop`) de l'exécutable du serveur de règles sont définis.

La figure 3 illustre l'emplacement des fichiers de clés après l'utilisation d'une méthode d'installation native pour configurer le serveur de règles de secours. Des liens adéquats vers ces fichiers de clés dans le système partagé sont également créés.

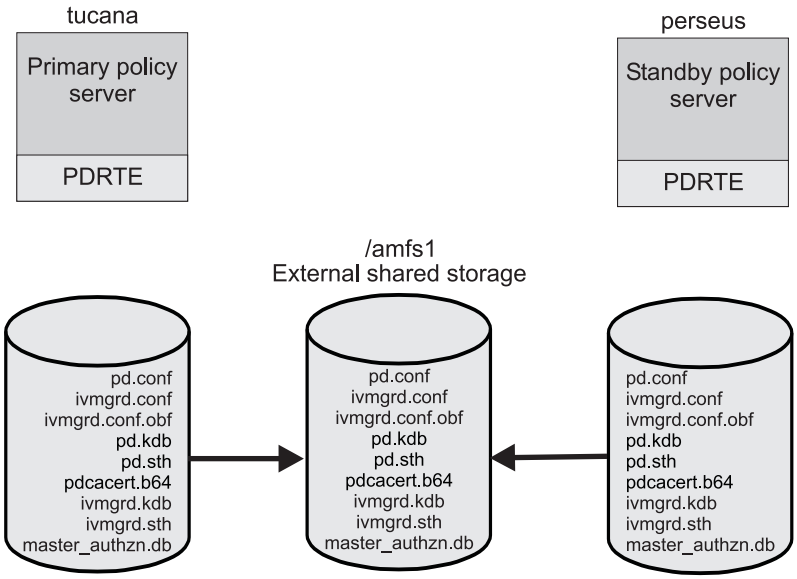


Figure 3. Environnement de serveur de règles principal ou de secours exécuté

Une fois que la configuration du serveur d'applications a été vérifiée, il est désormais possible d'activer entièrement la configuration du serveur de règles PowerHA primaire ou de secours. Pour activer cette configuration, le cluster PowerHA du système de serveur de règles principal doit être redémarré. Cette action démarre le serveur de règles principal et fait passer le serveur de règles de secours en mode secours.

Script : paramétrage des ID utilisateur pour les systèmes primaires et de secours

Utilisez un script pour définir les IDU des utilisateurs et groupes **ivmgr** et **tivoli** sur les systèmes de serveurs de règles primaires et de secours.

Utilisez le script suivant à titre de guide.

```
#!/bin/ksh
#
# Ce script paramètre les valeurs des ID utilisateur pour l'utilisateur ivmgr et le groupe ivmgr
# sur des valeurs définies sur la ligne de commande lorsque ce script est exécuté. De plus,
# ce script définit l'ID utilisateur de groupe tivoli et l'ID utilisateur d'utilisateur tivoli.
#
# Le premier paramètre ($1) est l'ID utilisateur du groupe ivmgr. Le second paramètre ($2) est
# l'ID utilisateur de l'utilisateur ivmgr. Le troisième paramètre ($3) est l'ID utilisateur du
# groupe tivoli. Le quatrième paramètre ($4) est destiné à l'ID utilisateur de l'utilisateur
# tivoli. Avant d'exécuter ce script, vérifiez que les quatre valeurs d'ID utilisateur ne sont PAS
# déjà utilisées sur un des systèmes.
#
# Compte tenu de l'importance de ces valeurs, il est ABSOLUMENT nécessaire, sur le système qui est
# exécuté comme serveur de règles de secours, de paramétrer l'ID utilisateur du groupe ivmgr
# et l'ID utilisateur de l'utilisateur ivmgr pour comparer les paramètres correspondants de ces
# entités sur le système qui joue le rôle de serveur de règles primaire. De plus, étant
# donné que la définition de l'utilisateur ivmgr appartient au groupe tivoli, il est également
# nécessaire de créer le groupe tivoli. Enfin, étant donné que le groupe tivoli contient
# l'utilisateur tivoli, l'utilisateur tivoli, avec l'ID utilisateur adéquat, doit également être
# défini. Ces paramètres d'utilisateur ou de groupe assurent une certaine cohérence à travers les
# deux serveurs de règles, ce qui permet à chaque système d'assumer le rôle de serveur de règles
# primaire le cas échéant. Sinon, le serveur de règles de secours n'est pas exécuté ou n'effectue
# pas de configuration correcte si ces valeurs ne sont pas identiques sur les DEUX systèmes.
#
# Notez que ce script, setivug, DOIT être exécuté AVANT que le serveur de règles de secours
# ne soit installé. En fait, il est conseillé d'exécuter ce script AVANT qu'un logiciel Security
# Access Manager ne soit installé sur le serveur de règles primaire OU de secours. Ainsi, ces quatre
# ID sont cohérentes dans les DEUX systèmes.
#
set -e
set -x
#
# Créez les groupes ivmgr et tivoli avec les ID utilisateur adéquats
#
mkgroup -'A' id="$1" ivmgr
mkgroup -'A' id="$3" tivoli
x() {
LIST=
SET_A=
for i in "$@"
do
if [ "$i" = "admin=true" ]
then
SET_A="-a"
continue
fi
LIST="$LIST \"$i\""
done
eval mkuser $SET_A $LIST
}
#
# Définissez maintenant l'ID utilisateur ivmgr pour qu'il fasse partie des groupes staff,
# tivoli et ivmgr. (Entrez la commande suivante sur une ligne continue.)
#
x id="$2" pgrp='staff' groups='staff,tivoli,ivmgr' home='/opt/PolicyDirector'
shell='/usr/bin/ksh' gecos='Policy Director Manager' ivmgr
#
# Définissez maintenant l'ID utilisateur tivoli pour qu'il fasse partie des groupes staff et tivoli.
# (Entrez la commande suivante sur une ligne continue.)
#
x id="$4" pgrp='staff' groups='staff,tivoli' home='/home/tivoli' shell='/usr/bin/ksh'
gecos='Owner of Tivoli Common Files' tivoli
#
```

Script : création de liens entre fichiers et répertoires sur le système principal

Utilisez un script pour créer des liens entre les fichiers et les répertoires requis sur le système du serveur de règles principal.

Utilisez le script suivant à titre de guide.

```
#!/bin/ksh
#

# Enregistrez une copie des 3 fichiers ci-dessous sous l'extension .bkp
cp -p /opt/PolicyDirector/etc/pd.conf /opt/PolicyDirector/etc/pd.conf.bkp
cp -p /opt/PolicyDirector/etc/ivmgrd.conf /opt/PolicyDirector/etc/ivmgrd.conf.bkp
cp -p /opt/PolicyDirector/etc/ivmgrd.conf.obf /opt/PolicyDirector/etc/ivmgrd.conf.obf.bkp

# Déplacez les fichiers de configuration vers le répertoire partagé du système de fichiers externe
mv /opt/PolicyDirector/etc/pd.conf /share/PolicyDirector
mv /opt/PolicyDirector/etc/ivmgrd.conf /share/PolicyDirector/ivmgrd.conf
mv /opt/PolicyDirector/etc/ivmgrd.conf.obf /share/PolicyDirector/ivmgrd.conf.obf

# Créez à nouveau un lien entre les fichiers de configuration et le répertoire d'installation d'origine
# et changez la propriété et le groupe de ces liens en ivmgr.
ln -s /share/PolicyDirector/pd.conf /opt/PolicyDirector/etc
ln -s /share/PolicyDirector/ivmgrd.conf /opt/PolicyDirector/etc
ln -s /share/PolicyDirector/ivmgrd.conf.obf /opt/PolicyDirector/etc
chown -h ivmgr /share/PolicyDirector/files/ivmgrd.conf
chown -h ivmgr /share/PolicyDirector/files/ivmgrd.conf.obf
chown -h ivmgr /share/PolicyDirector/files/pd.conf
chgrp -h ivmgr /share/PolicyDirector/files/ivmgrd.conf
chgrp -h ivmgr /share/PolicyDirector/files/ivmgrd.conf.obf
chgrp -h ivmgr /share/PolicyDirector/files/pd.conf

# Pour les sous-répertoires keytab, db et lock, créez une copie de sauvegarde de ces répertoires,
# déplacez leur contenu dans le système de fichiers externe partagé et créez à nouveau un lien
# pour les fichiers de
ces répertoires vers le répertoire d'installation d'origine.

cp -R -p /var/PolicyDirector/keytab /var/PolicyDirector/keytab_bkp
mv /var/PolicyDirector/keytab /share/PolicyDirector
ln -s /share/PolicyDirector/keytab /var/PolicyDirector

cp -R -p /var/PolicyDirector/db /var/PolicyDirector/db_bkp
mv /var/PolicyDirector/db /share/PolicyDirector
ln -s /share/PolicyDirector/db /var/PolicyDirector

cp -R -p /var/PolicyDirector/lock /var/PolicyDirector/lock_bkp
mv /var/PolicyDirector/lock /share/PolicyDirector
ln -s /share/PolicyDirector/lock /var/PolicyDirector

# Changez la propriété et le groupe de ces liens en ivmgr.
chown -h ivmgr /share/PolicyDirector/files/db
chown -h ivmgr /share/PolicyDirector/files/keytab
chown -h ivmgr /share/PolicyDirector/files/lock
chgrp -h ivmgr /share/PolicyDirector/files/db
chgrp -h ivmgr /share/PolicyDirector/files/keytab
chgrp -h ivmgr /share/PolicyDirector/files/lock
```

Exemple : vérification des répertoires de serveur primaire, des liens lointains et des autorisations

Utilisez l'exemple suivant pour vérifier les répertoires, liens et autorisations.

Dans le répertoire /opt/PolicyDirector/etc :

```
==> ls -l
total 3714
-rw-r-----1 ivmgrivmgr1682440 Oct 10 11:48 AccessManagerBaseAutoTraceDatabaseFile.obfuscated
-rw-r--r--1 ivmgrivmgr2703 Oct 14 13:16 activedir_ldap.conf
-rw-r-----1 ivmgrivmgr2703 Jul 14 14:21 activedir_ldap.conf.template
-rw-r-----1 ivmgrivmgr18195 Jul7 10:46 additional_licenses.txt
drw-rw----2 ivmgrivmgr512 Dec 31 1969blades
-rw-r-----1 ivmgrivmgr5890 Jan 24 2003config
-rw-r-----1 ivmgrivmgr114 Oct 10 11:48 ffdc
lrwxrwxrwx1 ivmgrivmgr36 Oct 15 13:45 ivmgrd.conf -> /amfs1/PolicyDirector/ivmgrd.conf
-rw-r-----1 ivmgrivmgr16949 Oct 14 13:19 ivmgrd.conf.bkp
lrwxrwxrwx1 ivmgrivmgr40 Oct 15 13:45 ivmgrd.conf.obf -> /amfs1/PolicyDirector/ivmgrd.conf.obf
-rw-r-----1 ivmgrivmgr64 Oct 14 13:19 ivmgrd.conf.obf.bkp
-rw-r-----1 ivmgrivmgr16731 Oct 10 11:29 ivmgrd.conf.template
-rw-r--r--1 ivmgrivmgr2319 Oct 14 13:18 ldap.conf
-rw-r-----1 ivmgrivmgr2187 Oct 10 11:21 ldap.conf.template
-rw-r--r--1 ivmgrivmgr36544 Sep 29 12:45 novschema.def
-rw-r--r--1 ivmgrivmgr26260 Sep 29 12:45 nsschema.def
lrwxrwxrwx1 ivmgrivmgr32 Oct 15 13:45 pd.conf -> /amfs1/PolicyDirector/pd.conf
-rw-r--r--1 ivmgrivmgr3736 Oct 14 13:20 pd.conf.bkp
-rw-r-----1 ivmgrivmgr3645 Oct 10 11:29 pd.conf.template
-rw-r-----1 ivmgrivmgr5576 Oct 10 10:05 pdbackup.lst
-rw-r-----1 ivmgrivmgr7448 Oct 10 10:05 pdinfo.lst
-rw-r--r--1 ivmgrivmgr5354 Oct 14 13:19 pdmgrd_routing
-rw-r--r--1 ivmgrivmgr5255 Oct 10 11:36 pdmgrd_routing.template
-rw-r--r--1 ivmgrivmgr1492 Oct 14 12:49 pdversion.dat
-rw-r--r--1 ivmgrivmgr1492 Aug 18 11:37 pdversion.dat.template
-rw-r-----1 ivmgrivmgr1466 Jan 24 2003product
-rw-r--r--1 ivmgrivmgr5827 Oct 14 13:16 routing
-rw-r--r--1 ivmgrivmgr5674 Oct 10 11:36 routing.template
-rw-r--r--1 ivmgrivmgr14035 Sep 29 12:45 secschema.def
-rw-r--r--1 ivmgrivmgr11236 Jan 24 2003secschema390.def
-rw-r--r--1 ivmgrivmgr1 Oct 14 12:49 startup
-rw-r--r--1 ivmgrivmgr1 Jun 24 10:48 startup.template
-rw-r--r--1 ivmgrivmgr1233 Jan 24 2003upgrade3.7_ibm_schema.def
-rw-r--r--1 ivmgrivmgr1938 Jan 24 2003upgrade3.7_ibm_schema390.def
-rw-r--r--1 ivmgrivmgr1744 Jan 24 2003upgrade3.7_netscape_schema.def
```

Dans le répertoire /var/PolicyDirector **:**

```
==> ls -Rl
total 7
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969audit
lrwxrwxrwx1 ivmgrivmgr27 Oct 15 13:45 db -> /amfs1/PolicyDirector/db
drwxrwxr-x2 ivmgrivmgr512 Oct 14 13:19 db_bkp
lrwxrwxrwx1 ivmgrivmgr31 Oct 16 15:48 keytab -> /amfs1/PolicyDirector/keytab
drwxr-xr-x2 ivmgrivmgr512 Oct 16 15:42 keytab_bkp
lrwxrwxrwx1 ivmgrivmgr29 Oct 15 13:45 lock -> /amfs1/PolicyDirector/lock
drwxr-x---2 ivmgrivmgr512 Dec 31 1969lock_bkp
drwxrwxrwx3 ivmgrivmgr512 Oct 16 13:40 log
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969pdbackup
drwxr-x---2 ivmgrivmgr512 Oct 14 12:49 pdmgrd
./audit:
total 0

./db_bkp:
total 1056
-rw-------1 ivmgrivmgr540672 Oct 15 13:45 master_authzn.db

./keytab_bkp:
total 35
-rw-------1 ivmgrivmgr10080 Oct 14 13:19 ivmgrd.kdb
-rw-------1 ivmgrivmgr129 Oct 14 13:18 ivmgrd.sth
-rw-rw-rw-1 rootsystem5080 Oct 14 13:19 pd.kdb
-rw-rw-rw-1 rootsystem129 Oct 14 13:19 pd.sth
-rw-------1 rootsystem1070 Oct 14 13:18 pdcacert.b64

./lock_bkp:
total 0
```

Dans le répertoire partagé, /share/PolicyDirector**, sur le système de fichiers externe :**

```
==> ls -Rl
total 80
drwxrwxr-x2 ivmgrivmgr512 Oct 14 13:19 db
-rw-r-----1 ivmgrivmgr16950 Oct 16 13:32 ivmgrd.conf
-rw-r-----1 ivmgrivmgr64 Oct 16 13:32 ivmgrd.conf.obf
drwxr-xr-x2 ivmgrivmgr512 Oct 16 15:42 keytab
drwxr-x---2 ivmgrivmgr512 Dec 31 1969lock
-rw-r--r--1 ivmgrivmgr3736 Oct 14 13:20 pd.conf

./db:
total 1056
-rw-------1 ivmgrivmgr540672 Oct 16 16:18 master_authzn.db

./keytab:
total 64
-rw-------1 ivmgrivmgr10080 Oct 14 13:19 ivmgrd.kdb
-rw-------1 ivmgrivmgr129 Oct 14 13:18 ivmgrd.sth
-rw-rw-rw-1 rootsystem5080 Oct 14 13:19 pd.kdb
-rw-rw-rw-1 rootsystem129 Oct 14 13:19 pd.sth
-rw-------1 rootsystem1070 Oct 14 13:18 pdcacert.b64

./lock:
total 0
```

Script : création d'un lien allant des fichiers système AIX vers le répertoire partagé sur le système de secours

Utilisez un script pour établir un lien entre les fichiers système AIX et le répertoire partagé sur le système du serveur de règles de secours.

Utilisez l'exemple de script suivant à titre de guide.

```
#!/bin/ksh
#

# Le serveur de règles de secours doit utiliser les mêmes fichiers de configuration que le
# serveur de règles primaire. C'est la raison pour laquelle les liens suivants doivent être créés
# pour que le serveur de règles de secours fonctionne correctement.
#
# Notez que le logiciel de configuration de Security Access Manager crée automatiquement
# un lien vers le fichier ivmgrd.conf stocké dans le système de fichiers externe partagé.

# Enregistrez pd.conf sous pd.bkp et créez un lien vers pd.conf dans le système de fichiers externe
# partagé
mv /opt/PolicyDirector/etc/pd.conf /opt/PolicyDirector/etc/pd.conf.bkp
ln -s /share/PolicyDirector/pd.conf /opt/PolicyDirector/etc

# Enregistrez les répertoires keytab, db et lock et créez un lien entre les répertoires keytab,
# db et lock
et leurs fichiers correspondants dans le système de fichiers externe partagé.

mv /var/PolicyDirector/keytab /var/PolicyDirector/keytab_bkp
ln -s /share/PolicyDirector/keytab /var/PolicyDirector

mv /var/PolicyDirector/db /var/PolicyDirector/db_bkp
ln -s /share/PolicyDirector/db /var/PolicyDirector

mv /var/PolicyDirector/lock /var/PolicyDirector/lock_bkp
ln -s /share/PolicyDirector/lock /var/PolicyDirector

# Changez le groupe et la propriété des cinq liens ci-dessus en ivmgr.
chown -h ivmgr /share/PolicyDirector/files/etc/pd.conf
chown -h ivmgr /share/PolicyDirector/files/db
chown -h ivmgr /share/PolicyDirector/files/keytab
chown -h ivmgr /share/PolicyDirector/files/lock
chgrp -h ivmgr /share/PolicyDirector/files/pd.conf
chgrp -h ivmgr /share/PolicyDirector/files/db
chgrp -h ivmgr /share/PolicyDirector/files/keytab
chgrp -h ivmgr /share/PolicyDirector/files/lock
```

Exemple : vérification des répertoires de serveur de secours, des liens lointains et des autorisations

Utilisez l'exemple suivant pour vérifier les répertoires, liens et autorisations.

Dans le répertoire /opt/PolicyDirector/etc :

```
==> ls -l
total 3668
-rw-r-----   1 ivmgr  ivmgr    1682440 Oct 10 11:48 AccessManagerBaseAutoTraceDatabaseFile.obfuscated
-rw-r--r-- 1 ivmgr ivmgr2703 Oct 16 13:26 activedir_ldap.conf
-rw-r----- 1 ivmgr ivmgr2703 Jul 14 14:21 activedir_ldap.conf.template
-rw-r----- 1 ivmgr ivmgr18195 Jul 07 10:46 additional_licenses.txt
drw-rw---- 2 ivmgr ivmgr512 Dec 31 1969blades
-rw-r----- 1 ivmgr ivmgr5890 Jan 24 2003config
-rw-r----- 1 ivmgr ivmgr114 Oct 10 11:48 ffdc
lrwxrwxrwx 1 rootsystem36 Oct 16 13:32 ivmgrd.conf -> /amfs1/PolicyDirector/ivmgrd.conf
lrwxrwxrwx 1 rootsystem40 Oct 16 13:32 ivmgrd.conf.obf -> /amfs1/PolicyDirector/ivmgrd.conf.obf
-rw-r----- 1 ivmgr ivmgr16731 Oct 10 11:29 ivmgrd.conf.template
-rw-r--r-- 1 ivmgr ivmgr2319 Oct 16 13:31 ldap.conf
-rw-r----- 1 ivmgr ivmgr2187 Oct 10 11:21 ldap.conf.template
-rw-r--r-- 1 ivmgr ivmgr36544 Sep 29 12:45 novschema.def
-rw-r--r-- 1 ivmgr ivmgr26260 Sep 29 12:45 nsschema.def
lrwxrwxrwx 1 ivmgr ivmgr32 Oct 16 13:36 pd.conf -> /amfs1/PolicyDirector/pd.conf
-rw-r--r-- 1 ivmgr ivmgr3741 Oct 16 13:32 pd.conf.bkp
-rw-r----- 1 ivmgr ivmgr3645 Oct 10 11:29 pd.conf.template
-rw-r----- 1 ivmgr ivmgr5576 Oct 10 10:05 pdbackup.lst
-rw-r----- 1 ivmgr ivmgr7448 Oct 10 10:05 pdinfo.lst
-rw-r--r-- 1 ivmgr ivmgr5255 Oct 10 11:36 pdmgrd_routing.template
-rw-r--r-- 1 ivmgr ivmgr1492 Oct 16 13:27 pdversion.dat
-rw-r--r-- 1 ivmgr ivmgr1492 Aug 18 11:37 pdversion.dat.template
-rw-r----- 1 ivmgr ivmgr1466 Jan 24 2003product
-rw-r--r-- 1 ivmgr ivmgr5810 Oct 16 13:27 routing
-rw-r--r-- 1 ivmgr ivmgr5674 Oct 10 11:36 routing.template
-rw-r--r-- 1 ivmgr ivmgr14035 Sep 29 12:45 secschema.def
-rw-r--r-- 1 ivmgr ivmgr11236 Jan 24 2003secschema390.def
-rw-r--r-- 1 ivmgr ivmgr1 Oct 16 13:27 startup
-rw-r--r-- 1 ivmgr ivmgr1 Jun 24 10:48 startup.template
-rw-r--r-- 1 ivmgr ivmgr1233 Jan 24 2003upgrade3.7_ibm_schema.def
-rw-r--r-- 1 ivmgr ivmgr1938 Jan 24 2003upgrade3.7_ibm_schema390.def
-rw-r--r-- 1 ivmgr ivmgr1744 Jan 24 2003upgrade3.7_netscape_schema.def
```

Dans le répertoire /var/PolicyDirector :

```
==> ls -Rl
total 7
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969audit
lrwxrwxrwx1 ivmgrivmgr27 Oct 16 13:36 db -> /amfs1/PolicyDirector/db
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969db_bkp
lrwxrwxrwx1 ivmgrivmgr31 Oct 16 13:36 keytab -> /amfs1/PolicyDirector/keytab
drwxrwxrwx2 ivmgrivmgr512 Dec 31 1969keytab_bkp
lrwxrwxrwx1 ivmgrivmgr29 Oct 16 13:36 lock -> /amfs1/PolicyDirector/lock
drwxr-x---2 ivmgrivmgr512 Dec 31 1969lock_bkp
drwxrwxrwx2 ivmgrivmgr512 Dec 31 1969log
drwxrwxr-x2 ivmgrivmgr512 Dec 31 1969pdbackup
drwxr-x---2 ivmgrivmgr512 Oct 16 13:24 pdmgrd
./audit:
total 0

./db_bkp:
total 0

./keytab_bkp:
total 0

./lock_bkp:
total 0
```

Gestion de la haute disponibilité

Les tâches suivantes visent à vous assurer que vous avez correctement suivi les premières procédures de configuration de Security Access Manager pour la configuration des serveurs HACMP Security Access Manager principal et de secours.

Vérification de la configuration du serveur de règles pour la haute disponibilité

Pour vérifier que les procédures d'installation et de configuration ont correctement été suivies, assurez-vous que les tâches principales suivantes ont été effectuées :

- Assurez-vous de configurer les liens lointains à partir du serveur principal actif vers le serveur de secours.
- Assurez-vous que vous avez modifié les options de configuration appropriées dans les fichiers de configuration `ivmgrd.conf` et `pd.conf` sur le noeud principal et les serveurs de secours. Ces fichiers de configuration doivent avoir les mêmes paramètres par défaut pour les ID d'utilisateur et de groupe requis suivants :
  - ID utilisateur **ivmgr**
  - ID utilisateur **tivoli**
  - ID groupe **ivmgr**
  - ID groupe **tivoli**
- Assurez-vous de copier les fichiers du système de fichiers AIX pour le serveur principal et le serveur de secours vers le système de fichiers partagé. Vérifiez que le système de fichiers partagé se trouve dans un répertoire commun et que chaque utilisateur et chaque groupe dispose des droits d'accès nécessaires.

Si l'un de ces éléments n'est pas correctement défini, revenez à la procédure de configuration d'un serveur de règles de secours. Voir Annexe G, «Configuration du serveur de règles de secours (AIX)», à la page 381.

Consultation des fichiers journaux

Vous pouvez surveiller le processus de transition entre le serveur de règles principal et le serveur de secours en examinant le fichier `hacmp.log` afin de vérifier que toutes les opérations de reprise HACMP et PowerHA ont été exécutées.

La procédure de consultation des fichiers journaux HACMP et PowerHA est décrite dans la documentation relative à HACMP et PowerHA. Le fichier `hacmp.log` se trouve dans le répertoire `/tmp`.

Si des erreurs d'opérations de lecture ou d'écriture se sont produites lors de la fonction de secours du serveur de règles, vous pouvez consulter les fichiers journaux du serveur de règles principal. L'emplacement des fichiers journaux Security Access Manager dépend de l'utilisation ou non du logicielTivoli Common Directory. Reportez-vous au manuel *IBM Security Access Manager for Web Troubleshooting Guide* pour plus d'informations sur ces fichiers journaux et sur le visualiseur de fichiers XML.

Annexe H. Configuration d'un serveur de règles de secours avec IBM Tivoli System Automation for Multiplatforms

Vous pouvez configurer un serveur de secours pour prendre en charge les fonctions de serveur de règles lors d'une panne système ou d'une indisponibilité non planifiée.

Lorsque le serveur de règles s'arrête, le serveur de règles de secours agit comme le serveur de règles primaire jusqu'à ce que le serveur de règles primaire remplisse son rôle d'origine. A son tour, le serveur de règles de secours remplit à nouveau un rôle serveur de secours. A un moment donné, il n'y a qu'un seul serveur de règles actif et qu'une seule copie partagée des bases de données de règles.

Security Access Manager prend en charge l'utilisation d'un serveur de règles de secours sur les plateformes AIX, Linux ou Windows prises en charge. En outre, le déploiement d'un serveur de règles de secours nécessite un équilibrage de charge réseau, ainsi qu'IBM Tivoli System Automation for Multiplatforms.

Ce scénario est indiqué à titre de guide général. Il explique comment installer et configurer un système Tivoli Environment Automation for Multiplatforms pour utiliser les capacités du serveur de règles.

Remarque : Si vous configurez un serveur de règles de secours sur AIX, vous pouvez utiliser le scénario dans Annexe G, «Configuration du serveur de règles de secours (AIX)», à la page 381.

Composants du scénario

Ce scénario relatif aux règles de secours utilise un serveur d'exécution, un serveur LDAP et un équilibreur de charge, un serveur principal, ainsi qu'un serveur de secours. IBM Tivoli System Automation for Multiplatforms fait office à la fois de serveur principal et de serveur de secours. Il assure les fonctionnalités de haute disponibilité et d'automatisation basée sur des règles pour l'environnement.

© Copyright IBM Corp. 2001, 2013

Le graphique suivant illustre l'organisation de ces composants :

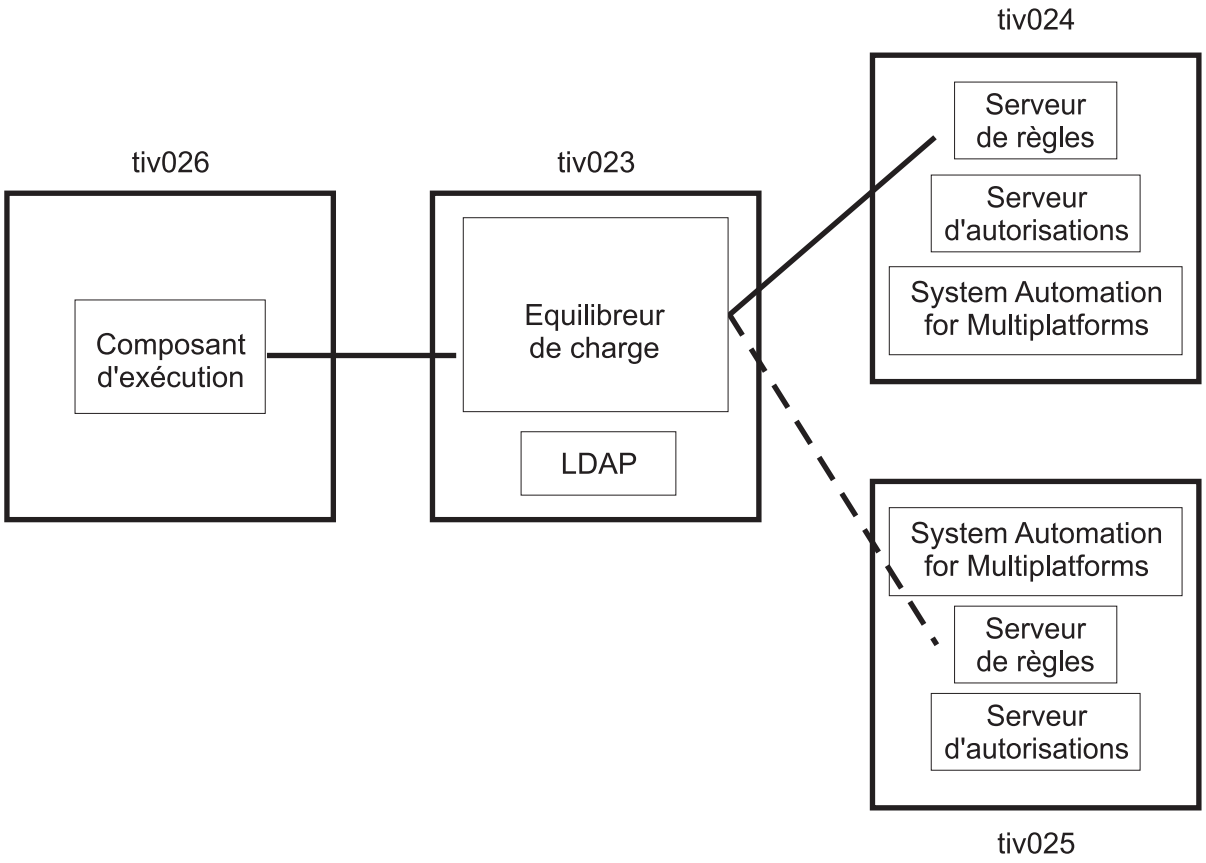


Tableau 35. Composants du scénario utilisant IBM Tivoli System Automation for Multiplatforms

Nom	Utilisation
tiv023	Serveur LDAP et équilibreur de charge pour la reprise
tiv024	Serveur de règles principal équipé d'IBM Tivoli System Automation Application Manager
tiv025	Serveur de règles en veille équipé d'IBM Tivoli System Automation Application Manager
tiv026	Serveur d'exécution et client LDAP **Remarque :** Le composant d'exécution utilisé dans ce scénario peut être n'importe quel composant Security Access Manager nécessitant l'accès au serveur de règles. Vous pouvez par exemple remplacer le serveur d'exécution indiqué dans le scénario par un serveur WebSEAL.

La ligne continue désigne le chemin d'accès normal au système Security Access Manager. La ligne discontinue correspond au chemin d'accès pour la reprise sur le système de secours.

Exigences de préinstallation

Cet environnement à haute disponibilité implique des exigences en termes de configuration logicielle.

Assurez-vous que les logiciels suivants sont disponibles pour votre installation :

- Un serveur LDAP pris en charge, tel qu'IBM Tivoli Directory Server
- IBM Security Access Manager
- Equilibreur de charge pour la reprise
- IBM Tivoli System Automation for Multiplatforms

Effectuez les tâches préalables à l'installation sur chaque serveur. Voir Chapitre 4, «Plan des installations et configurations prérequises», à la page 27.

Exigences relatives à LDAP et à l'équilibreur de charge

Ce scénario requiert l'installation du protocole LDAP et du logiciel d'équilibrage de charge (pour la reprise). Dans ces instructions, le serveur LDAP est installé sur le même serveur que celui qui héberge le serveur d'exécution. Toutefois, vous pouvez les installer sur des serveurs distincts.

Pour plus d'informations sur les conditions requises pour le registre d'utilisateurs, voir Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs» , à la page 51.

Configuration requise pour le serveur principal

Le serveur principal requiert un serveur de règles et un serveur d'autorisations Security Access Manager, ainsi qu'IBM Tivoli System Automation for Multiplatforms.

Serveur de règles et serveur d'autorisations

Pour plus d'informations sur les prérequis, consultez «Security Access Manager - systèmes de base», à la page 13.

Tivoli System Automation for Multiplatforms

Pour plus d'informations sur les prérequis, consultez http://www.ibm.com/software/tivoli/products/sys-auto-linux/platforms.html.

Exigences applicables au serveur de secours

Le serveur de secours requiert un serveur de règles et un serveur d'autorisations Security Access Manager, ainsi qu'IBM Tivoli System Automation for Multiplatforms.

Serveur de règles et serveur d'autorisations

Pour plus d'informations sur les prérequis, consultez «Security Access Manager - systèmes de base», à la page 13.

Tivoli System Automation for Multiplatforms

Pour plus d'informations sur les prérequis, consultez http://www.ibm.com/software/tivoli/products/sys-auto-linux/platforms.html.

Exigences applicables au serveur d'exécution

Le serveur d'exécution requiert le composant Security Access Manager Runtime. Le composant d'exécution utilisé dans ce scénario peut être n'importe quel composant Security Access Manager nécessitant l'accès au serveur de règles. Vous pouvez par exemple remplacer le serveur d'exécution indiqué dans le scénario par un serveur WebSEAL.

Composant d'exécution

Pour plus d'informations sur les prérequis, consultez «Security Access Manager - systèmes de base», à la page 13.

Client LDAP

Pour plus d'informations sur les prérequis, consultez Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51.

Installation du protocole LDAP et de l'équilibreur de charge

Pour commencer votre déploiement, installez les logiciels LDAP et d'équilibrage de charge sur le serveur afin de permettre le basculement entre les serveurs de règles principal et de secours.

Avant de commencer

Assurez-vous que votre environnement satisfait aux exigences décrites à la section «Exigences relatives à LDAP et à l'équilibreur de charge», à la page 399.

Procédure

1. Installez LDAP. Suivez les instructions de la section Chapitre 5, «Installation et configuration du serveur de registres d'utilisateurs», à la page 51. Durant l'installation, veillez à conservez les valeurs par défaut dans les zones suivantes :
   - **Valeur de départ de chiffrement**
   - **Port non SSL**
   - **Port SSL**
   - **Fichier de clés SSL et chemin complet**
   - **Libellé de certificat**
2. Installez le logiciel d'équilibrage de charge. Pour obtenir des instructions sur l'installation de l'équilibreur de charge, utilisez la documentation fournie avec le produit.

Que faire ensuite

Passez à l'étape «Installation du serveur principal».

Installation du serveur principal

La configuration initiale du serveur principal comprend l'installation du serveur de règles et du serveur d'autorisations de Security Access Manager. Au cours d'une tâche ultérieure, vous devrez installer IBM Tivoli System Automation for Multiplatforms sur ce serveur.

Avant de commencer

Assurez-vous que votre environnement satisfait aux exigences décrites à la section «Configuration requise pour le serveur principal», à la page 399.

Procédure

1. Installez le client LDAP. Voir «Installation du client IBM Tivoli Directory Server», à la page 43.
2. Installez le composant Global Security Kit. Voir «Installation d'IBM Global Security Kit (GSKit)», à la page 35.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez le composant IBM Security Utilities. Voir «Installation d'IBM Security Utilities», à la page 40.
5. Installez le composant d'exécution. Voir Chapitre 11, «Configuration d'un système d'exécution», à la page 181.
6. Installez le serveur de règles. Voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109.
7. Installez le serveur d'autorisations. Voir Chapitre 7, «Configuration du serveur d'autorisation», à la page 129.
8. Configurez uniquement les serveurs d'exécution et de règles pour utiliser le protocole LDAP précédemment installé. Voir Chapitre 11, «Configuration d'un système d'exécution», à la page 181 et Chapitre 6, «Configuration d'un serveur de règles», à la page 109.
9. Créez les domaines Security Access Manager éventuellement requis en plus du domaine de gestion Security Manager par défaut. Exécutez la commande **pdadmin domain create**. Voir *IBM Security Access Manager for Web Command Reference*.
10. Clonez le serveur de règles principal en créant une sauvegarde de celui-ci. Exécutez la commande **pdbackup**. Voir *IBM Security Access Manager for Web Command Reference*. Un fichier `.tar` est créé sur les systèmes AIX et Linux. Par exemple :`pdbackup.tiv024.tar`. Un fichier `.dar` est créé sur les systèmes Windows.
11. Configurez un serveur d'autorisations pour le domaine de gestion de Security Access Manager. Voir Chapitre 7, «Configuration du serveur d'autorisation», à la page 129.
12. Si vous créez des domaines Security Access Manager supplémentaires, configurez des instances additionnelles du serveur d'autorisations, à raison d'une par domaine. Envisagez d'utiliser pour ces domaines des noms d'instance qui soient aisément reconnaissables. Par exemple, utilisez le nom de domaine pour lequel l'instance est en cours de configuration.

Que faire ensuite

Passez à l'étape «Installation du serveur de secours», à la page 402.

Installation du serveur de secours

La configuration du serveur de secours implique plusieurs tâches. Vous devez installer Security Access Manager sur le serveur, cloner le serveur principal, restaurer le clone sur le serveur de secours, puis configurer un serveur d'autorisations unique sur le serveur de secours. Au cours d'une tâche ultérieure, vous devrez également installer IBM Tivoli System Automation for Multiplatforms sur ce serveur.

Avant de commencer

Effectuez les tâches requises décrites à la section «Configuration requise pour le serveur principal», à la page 399.

Procédure

1. Installez le client LDAP. Voir «Installation du client IBM Tivoli Directory Server», à la page 43.
2. Installez le composant Global Security Kit. Voir «Installation d'IBM Global Security Kit (GSKit)», à la page 35.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez le composant IBM Security Utilities. Voir «Installation d'IBM Security Utilities», à la page 40.
5. Installez le composant d'exécution. Voir Chapitre 11, «Configuration d'un système d'exécution», à la page 181.
6. Installez le serveur de règles. Voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109.
7. Installez le serveur d'autorisations. Voir Chapitre 7, «Configuration du serveur d'autorisation», à la page 129.
8. Configurer *uniquement* l'environnement d'exécution (pdrte) sur le serveur de secours. Voir Chapitre 6, «Configuration d'un serveur de règles», à la page 109.
9. Copiez la sauvegarde du serveur principal sur le serveur de secours.
   a. Copiez le fichier `.tar` à partir du serveur principal sur le serveur de secours, dans un répertoire temporaire.
   b. Restaurer la copie de sauvegarde sur le serveur de secours en utilisant l'action `restore` avec la commande **pdbackup**. Par exemple, sur AIX ou Linux, entrez :

      ```
      pdbackup -action restore -file /tmp/pdbackup.tiv024.tar
      ```

      Par exemple, sous Windows, tapez :

      ```
      pdbackup -action restore -file %TEMP%pdbackup.tiv024.dar
      ```
10. Affichez les fichiers du serveur de règles. Par exemple, sur AIX et Linux, dans le répertoire `/var/PolicyDirector/db`, entrez :

    ```
    ls -l
    ```

    Le résultat attendu est similaire à l'exemple suivant :

    ```
    -rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 master_authzn.db
    ```

    Si vous avez créé des domaines supplémentaires, vous pouvez également vous attendre à un résultat similaire à l'exemple suivant.

```
-rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 domain2.db
-rw------- 1 ivmgr ivmgr 540672 Oct 19 10:38 domain3.db
```

11. Vérifiez le statut des serveurs sur le serveur de secours. Par exemple, sous AIX ou Linux, entrez :

    ```
    pdconfig
    ```

    Lorsque vous y êtes invité, sélectionnez **3. Afficher le statut de configuration**. Le résultat attendu est similaire à l'exemple suivant :

    ```
    Security Access Manager Runtime Yes
    Security Access Manager Policy Server Yes
    Security Access Manager Authorization Server No
    ```

12. Configurez des serveurs d'autorisation uniques sur le serveur de secours.
    a. Configurer un serveur d'autorisations pour le domaine de gestion de Security Access Manager.
    b. Si vous avez créé des domaines Security Access Manager supplémentaires, configurez des instances additionnelles du serveur d'autorisations, à raison d'une par domaine. Envisagez d'utiliser pour ces domaines des noms d'instance qui soient aisément reconnaissables. Par exemple, utilisez le nom de domaine pour lequel l'instance est en cours de configuration.
13. Vérifiez que la configuration a abouti en exécutant la commande **`server list`**. Pour plus de détails, voir *IBM Security Access Manager for Web Command Reference*. Le serveur principal et le serveur de secours figurent tous deux dans la liste qui est affichée par la commande. Un seul serveur de règles est répertorié.

Que faire ensuite

Passez à l'étape «Vérification des serveurs Security Access Manager».

Vérification des serveurs Security Access Manager

Avant de poursuivre les tâches de configuration restantes, assurez-vous que l'installation et la configuration des serveurs Security Access Manager sont correctes. Puis, mettez à jour certains paramètres répliqués de sorte qu'ils pointent vers les serveurs appropriés.

Pourquoi et quand exécuter cette tâche

Les serveurs de règles et d'autorisations situés sur le serveur principal et le serveur de secours utilisent la même base de données de règles. Par conséquent, les mises à jour effectuées depuis l'un ou l'autre serveur sont répliquées dans les bases de données de règles et doivent être accessibles via les deux serveurs. Cette tâche a pour but de vérifier cette accessibilité.

Remarque : Sur les systèmes Microsoft Windows, utilisez la fenêtre Services du Panneau de configuration pour démarrer et arrêter manuellement les processus des serveurs. Dans la fenêtre Services, changez le type de démarrage du service Access Manager d'Automatique à Manuel.

Les fichiers avec lesquels vous travaillez pour cette tâche se trouvent par défaut dans les emplacements suivants.

AIX, Linux et Solaris :

```
/opt/PolicyDirector/etc/pd.conf
/opt/PolicyDirector/etc/ivmgrd.conf
```

Windows :

```
C:\Program Files\Tivoli\Policy Director\etc\pd.conf
C:\Program Files\Tivoli\Policy Director\etc\imgmrd.conf
```

Remplacez les informations relatives au chemin d'accès dans les exemples de cette tâche par le chemin d'accès approprié pour votre environnement.

Procédure

1. Créez une liste de contrôle d'accès sur le serveur principal :
   a. Assurez-vous que le serveur de règles et le serveur d'autorisations hébergés sur le serveur principal sont démarrés. Par exemple, sur AIX ou Linux, tapez :

      ```
      pd_start start
      ```

      Pour s'assurer qu'ils sont démarrés, entrez `pd_start status`.
   b. Créer une liste de contrôle d'accès en exécutant la commande **pdadmin acl create**. Par exemple, sur AIX ou Linux, tapez :

      ```
      pdadmin -a sec_master -p passw0rd
      pdadmin sec_master> acl create testacl
      pdadmin sec_master> acl show testacl
      ```

      Le résultat est similaire à l'exemple suivant :

      ```
      ACL Name: testacl
      Description:
      Entries:
      User sec_master TcmdbsvaBRl
      ```
   c. Arrêtez le serveur de règles et le serveur d'autorisations. Par exemple, sur AIX ou Linux, tapez :

      ```
      pd_start stop
      ```
2. Vérifiez la réplication sur le serveur de secours :
   a. Arrêtez le serveur d'autorisations sur le serveur de secours. Par exemple, tapez :

      ```
      pd_start stop
      ```
   b. Modifiez le paramètre "master-host" dans le fichier `pd.conf` en mettant en commentaires les entrées correspondant au serveur de règles et en ajoutant une entrée correspondant au serveur de secours. Modifiez le fichier `pd.conf` de manière à ce qu'il se présente comme suit, "tiv024" désignant le serveur principal et "tiv025" le serveur de secours :

      ```
      # Hostname of the server.
      # This parameter is set by the bassslcfg utility.
      #master-host = <Server host name>
      #master-host = tiv024
      master-host = tiv025
      ```
   c. Dans le même fichier, désactivez le démarrage du serveur d'autorisations. Modifiez le paramètre suivant :

      ```
      [pdrte]
      boot-start-ivacld=no
      ```

      Si vous avez configuré des serveurs d'autorisations supplémentaires, arrêtez-les également :

      ```
      [pdrte]
      boot-start-domain2-ivacld=no
      boot-start-domain3-ivacld=no
      ```
   d. Modifiez le paramètre "database-path" dans le fichier `ivmgrd.conf`. Editez le fichier `ivmgrd.conf` comme suit.

Remarque : Sous Windows, remplacez `/var/PolicyDirector/db/` par le répertoire approprié.

```
# Database file
#database-path=/var/PolicyDirector/db/master_authzn.db
database-path=/var/PolicyDirector/db/ivacld.db
```

Si vous avez créé des domaines supplémentaires, mettez à jour les entrées correspondant à leur chemin de base de manière à spécifier les fichiers de base de données correspondants sur le serveur d'autorisations :

```
[domain=domain2]
#database-path=/var/PolicyDirector/db/domain2.db
database-path=/var/PolicyDirector/db/domain2-ivacld.db
[domain=domain3]
#database-path=/var/PolicyDirector/db/domain3.db
database-path=/var/PolicyDirector/db/domain3-ivacld.db
```

e. Démarrez le serveur de règles, mais *pas* les serveurs d'autorisations. Par exemple, sur AIX ou Linux, tapez :

```
pd_start start
```

Remarque : La commande **pd_start start** peut être utilisée ici puisqu'elle a été désactivée, au cours d'une étape précédente, sur les serveurs d'autorisations.

f. Sur le serveur de secours (tiv025 dans cet exemple), connectez-vous à **pdadmin** et recherchez la liste de contrôle d'accès qui a été créée sur le serveur principal. Par exemple, sur AIX ou Linux, tapez :

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> acl list
```

Localisez le nom de la liste de contrôle d'accès que vous avez ajoutée sur le serveur principal, talle que `testacl`.

3. Sur le serveur de secours, mettez à jour la liste de contrôle d'accès.

a. Sur le serveur principal, modifier le paramètre "master-host" dans le fichier `pd.conf`. Ouvrez le fichier `pd.conf` dans un éditeur de texte. Puis, éditez le fichier de manière à ce qu'il se présente comme suit, "tiv024" désignant le serveur principal et "tiv025" le serveur de secours :

```
# Hostname of the server.
# This parameter is set by the bassslcfg utility.
#master-host = <Server host name>
#master-host = tiv024
master-host = tiv025
```

b. Dans le même fichier, désactivez le démarrage du serveur de règles. Modifiez le paramètre suivant :

```
[pdrte]
boot-start-ivmgrd=no
```

c. Modifiez le paramètre "master-host" dans le fichier `ivacld.conf`. Modifiez le fichier `ivacld.conf` de manière à ce qu'il se présente comme suit, "tiv024" désignant le serveur principal et "tiv025" le serveur de secours :

```
# Hostname of the server.
# This parameter is set by the svrsslcfg utility.
#master-host = <Server host name>
#master-host = tiv024
master-host = tiv025
```

d. Démarrez les serveurs d'autorisations, mais *pas* le serveur de règles. Par exemple, sur AIX ou Linux, tapez :

```
pd_start start
```

Remarque : La commande **pd_start start** peut être utilisée ici puisqu'elle a été désactivée, au cours d'une étape précédente, sur le serveur de règles. Pour vous assurer que le démarrage a bien eu lieu, entrez `pd_start status`.

4. Sur le serveur de secours, ajoutez un utilisateur à la liste de contrôle d'accès.
   a. Affichez la liste de contrôle d'accès que vous avez précédemment créée. Par exemple, tapez :

      ```
      pdadmin -a sec_master -p passw0rd
      pdadmin sec_master> acl show testacl
      ```

   b. Créez un utilisateur à l'aide de la commande **pdadmin user create** et ajoutez l'utilisateur à la liste de contrôle d'accès précédemment créée. Par exemple, tapez :

      ```
      pdadmin sec_master> user create bobsm cn=bobsm,o=ibm,c=us
          Bob Smith passw0rd
      pdadmin sec_master> user modify bobsm account-valid yes
      pdadmin sec_master> acl modify testacl set user bobsm Tr
      pdadmin sec_master> acl show testacl
      ```

      Le résultat est similaire à l'exemple suivant :

      ```
      ACL Name: testacl
      Description:
      Entries:
      User sec_master TcmdbsvaBRl
      User bobsm Tr
      ```

5. Sur le serveur de secours, arrêtez le serveur de règles.

   ```
   pd_start stop
   ```

6. Sur le serveur de secours, arrêtez le serveur d'autorisations.

   ```
   pd_start stop
   ```

7. Sur le serveur principal, modifiez les paramètres du serveur de règles de sorte que celui-ci pointe vers le serveur d'autorisations sur le serveur principal.
   a. Modifiez le paramètre "master-host" dans le fichier `pd.conf` en mettant en commentaires les entrées correspondant au serveur de règles et en ajoutant une entrée correspondant au serveur de secours. Modifiez le fichier `pd.conf` de manière à ce qu'il se présente comme suit, "tiv024" désignant le serveur principal et "tiv025" le serveur de secours :

      ```
      # Hostname of the server.
      # This parameter is set by the bassslcfg utility.
      #master-host = <Server host name>
      master-host = tiv024
      ```

   b. Dans le même fichier, activez le démarrage du serveur de règles et désactivez le démarrage du serveur d'autorisations. Modifiez le paramètre suivant :

      ```
      [pdrte]
      boot-start-ivmgrd=yes
      boot-start-ivacld=no
      ```

      Si vous avez configuré des serveurs d'autorisations supplémentaires, arrêtez-les également :

      ```
      [pdrte]
      boot-start-domain2-ivacld=no
      boot-start-domain3-ivacld=no
      ```

   c. Modifiez le paramètre "database-path" dans le fichier `ivmgrd.conf`. Editez le fichier `ivmgrd.conf` comme suit.

Remarque : Sous Windows, remplacez /var/PolicyDirector/db/ par le répertoire approprié.

```
# Database file
#database-path=/var/PolicyDirector/db/master_authzn.db
database-path=/var/PolicyDirector/db/ivacld.db
```

Si vous avez créé des domaines supplémentaires, mettez à jour les entrées correspondant à leur chemin de base de manière à spécifier les fichiers de base de données correspondants sur le serveur d'autorisations :

```
[domain=domain2]
#database-path=/var/PolicyDirector/db/domain2.db
database-path=/var/PolicyDirector/db/domain2-ivacld.db
[domain=domain3]
#database-path=/var/PolicyDirector/db/domain3.db
database-path=/var/PolicyDirector/db/domain3-ivacld.db
```

8. Sur le serveur principal, démarrez le serveur de règles.

   ```
   pd_start start
   ```

9. Sur le serveur principal, connectez-vous à **pdadmin** et recherchez la liste de contrôle d'accès qui a été créée sur le serveur de secours. Par exemple, tapez :

   ```
   pdadmin -a sec_master -p passw0rd
   pdadmin sec_master> acl show testacl
   ```

   Le résultat est similaire à l'exemple suivant :

   ```
   ACL Name: testacl
   Description:
   Entries:
   User sec_master TcmdbsvaBRl
   User bobsm Tr
   ```

   La modification effectuée sur la liste de contrôle d'accès du serveur de secours est visible sur le serveur principal.

10. Restaurez la configuration initiale sur le serveur de secours.
    a. Modifiez le paramètre "master-host" dans le fichier pd.conf en mettant en commentaires les entrées correspondant au serveur de règles et en ajoutant une entrée correspondant au serveur de secours. Modifiez le fichier pd.conf de manière à ce qu'il se présente comme suit, "tiv024" désignant le serveur principal et "tiv025" le serveur de secours :

       ```
       # Hostname of the server.
       # This parameter is set by the bassslcfg utility.
       #master-host = <Server host name>
       master-host = tiv024
       ```

    b. Dans le même fichier, désactivez le démarrage du serveur de règles et activez le démarrage du serveur d'autorisations. Modifiez le paramètre suivant :

       ```
       [pdrte]
       boot-start-ivmgrd=no
       boot-start-ivacld=yes
       ```

       Si vous avez configuré des serveurs d'autorisations supplémentaires, activez-les également :

       ```
       [pdrte]
       boot-start-domain2-ivacld=yes
       boot-start-domain3-ivacld=yes
       ```

    c. Démarrez le serveur d'autorisations, mais *pas* le serveur de règles. Par exemple, sur AIX ou Linux, tapez :

       ```
       pd_start start
       ```

d. Pour vous assurer que le démarrage a bien eu lieu, entrez `pd_start status`.
e. Utilisez les commandes **pdadmin** pour vous assurer que les serveurs fonctionnent correctement. Par exemple, tapez :

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> server list
```

Configuration de l'équilibreur de charge

Le logiciel d'équilibrage de charge doit être configuré pour permettre le basculement du serveur de règles principal vers le serveur de secours lorsque ce dernier détecte que le serveur principal ne répond pas. L'équilibreur de charge doit pas tenter d'envoyer des requêtes aux deux serveurs simultanément, mais doit fournir uniquement la prise en charge du basculement, car un seul serveur de règles est actif à la fois.

Installation et configuration du serveur d'exécution

La configuration du serveur d'exécution comprend l'installation du client LDAP et le serveur Security Access Manager Runtime.

Pourquoi et quand exécuter cette tâche

Effectuez les tâches requises décrites à la section «Exigences applicables au serveur d'exécution», à la page 400.

Le fichier pour cette tâche se trouve à l'emplacement par défaut suivant :

AIX, Linux et Solaris :

```
/opt/PolicyDirector/etc/pd.conf
```

Windows :

```
C:\Program Files\Tivoli\Policy Director\etc\pd.conf
```

Remplacez les informations relatives au chemin d'accès dans les exemples de cette tâche par le chemin d'accès approprié pour votre environnement.

Procédure

1. Installez le client LDAP. Voir «Installation du client IBM Tivoli Directory Server», à la page 43.
2. Installez le composant Global Security Kit. Voir «Installation d'IBM Global Security Kit (GSKit)», à la page 35.
3. Installez IBM Security Access Manager License, s'il ne l'est pas déjà. Pour obtenir des instructions, voir «Installation de la licence IBM Security Access Manager», à la page 38.
4. Installez le composant IBM Security Utilities. Voir «Installation d'IBM Security Utilities», à la page 40.
5. Installez le composant d'exécution. Voir Chapitre 11, «Configuration d'un système d'exécution», à la page 181.
6. Configurez le serveur d'exécution en vue d'utiliser l'annuaire LDAP que vous avez précédemment installé.
7. Vérifiez la retransmission des requêtes par l'équilibreur de charge.
   a. Connectez-vous à **pdadmin** et vérifiez que les serveurs principal et de secours sont listés. Par exemple, tapez :

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> server list
```

b. Sur le serveur d'exécution, modifiez le paramètre "master-host" dans le fichier `pd.conf` de manière à pointer vers l'adresse IP du cluster. Modifiez le fichier `pd.conf` de manière à ce qu'il se présente comme suit, "tiv024" désignant le serveur principal et "tiv026" le serveur d'exécution.

```
# Hostname of the server.
# This parameter is set by the bassslcfg utility.
#master-host = <Server host name>
#master-host = <tiv024_ip_address>
master-host = <ip_address_of_Edge_server_cluster>
```

c. Connectez-vous à **pdadmin** et vérifiez les modifications dans la liste de serveurs et la liste de contrôle d'accès. Par exemple, tapez :

```
pdadmin -a sec_master -p passw0rd
pdadmin sec_master> server list
```

d. Vérifiez que les serveurs principal et de secours sont listés. Entrez ensuite :

```
pdadmin sec_master> acl list
```

e. Vérifiez que toutes les listes de contrôle d'accès (y compris la liste ACL qui a été créée, appelée `testacl` dans cet exemple) sont répertoriées. Entrez ensuite :

```
pdadmin sec_master> acl show testacl
```

f. Vérifiez que tous les utilisateurs membres de cette liste de contrôle d'accès sont répertoriés.

Que faire ensuite

Passez à l'étape «Installation et configuration de Tivoli System Automation for Multiplatforms».

Installation et configuration de Tivoli System Automation for Multiplatforms

Installez et configurez IBM Tivoli System Automation for Multiplatforms à la fois sur le serveur principal et le serveur de secours. IBM Tivoli System Automation for Multiplatforms assure assure des fonctionnalités de haute disponibilité et d'automatisation basée sur des règles pour l'environnement.

Pourquoi et quand exécuter cette tâche

Pour plus de détails sur l'installation et la configuration de Tivoli System Automation for Multiplatforms, reportez-vous aux instructions d'installation disponibles à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.samp.doc_3.2.2/HALICG23.pdf.

Les exemples de commandes utilisent les variables suivantes. Remplacez ces variables par les noms qui correspondent à votre installation :

tiv024 Nom du serveur principal.

tiv025 Nom du serveur de secours.

tiv023 Nom du serveur LDAP et de l'équilibreur de charge.

mynetwork
Nom utilisé pour représenter votre réseau.

Procédure

1. Installez à la fois sur le serveur principal et sur le serveur de secours le composant Tivoli System Automation for Multiplatforms. Reportez-vous aux instructions fournies sur le centre de documentation de Tivoli System Automation for Multiplatforms : http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.samp.doc_3.2.2/HALICG23.pdf
2. Une fois l'installation du produit terminée, suivez les instructions pour terminer la configuration.
3. Sur le serveur principal, créez un cluster à deux noeuds.

   Remarque : Sous Windows, exécutez toutes les commandes à partir du programme IBM Tivoli System Automation Shell. Pour démarrer cet interpréteur de commandes, cliquez sur **Démarrer** > **Tous les programmes** > **SA for Multiplatforms** > **IBM Tivoli System Automation-Shell**.

   a. Exécutez **preprpnode** avec les noms des noeuds principal et de secours. Par exemple, tapez :

      ```
      preprpnode tiv024 tiv025
      ```

   b. Créez un cluster et spécifiez à la fois les noeuds principal et de secours. Utilisez un nom de votre choix. SA_DOMAIN est le nom qui est utilisé dans cet exemple. Par exemple, tapez :

      ```
      mkrpdomain SA_DOMAIN tiv024 tiv025
      ```

   c. Vérifiez la mise hors ligne du cluster. Affichez les informations relatives au cluster. Par exemple, tapez :

      ```
      lsrpdomain SA_DOMAIN
      ```

   d. Connectez le cluster. Par exemple, tapez :

      ```
      startrpdomain SA_DOMAIN
      ```

      Patientez quelques minutes le temps que le cluster soit mis en ligne. Exécutez à nouveau la commande **lsrpdomain SA_DOMAIN** jusqu'à ce que la mise en ligne soit indiquée.
4. Vérifiez le statut du cluster sur le serveur de secours. Par exemple, sur le serveur de secours, entrez :

   ```
   lsrpdomain SA_DOMAIN
   ```

5. Configurez la condition de départage du réseau sur le serveur principal.

   a. Obtenez la liste des types de condition de départage disponibles. Par exemple, tapez :

      ```
      lsrsrc -c IBM.TieBreaker AvailableTypes
      ```

   b. Créez une condition de départage. Par exemple, tapez :

      ```
      mkrsrc IBM.TieBreaker Type="EXEC" Name="mynetwork"
      DeviceInfo='PATHNAME=/usr/sbin/rsct/bin/samtb_net Address=tiv023_ip_address
      Log=1' PostReserveWaitTime=30;
      ```

   c. Activez la condition de départage. Par exemple, tapez :

      ```
      chrsrc -c IBM.PeerNode OpQuorumTieBreaker="mynetwork"
      ```

   d. Sur le serveur de secours, affichez les informations relatives à la condition de départage. Par exemple, sur le serveur de secours, entrez :

      ```
      lsrsrc IBM.TieBreaker
      ```

Que faire ensuite

Passez à l'étape «Activation de l'automatisation de la reprise en ligne», à la page 411.

Activation de l'automatisation de la reprise en ligne

IBM Tivoli System Automation for Multiplatforms utilise des *ressources d'application* pour activer l'automatisation des fonctions de basculement. Une ressource d'application est un élément matériel ou logiciel que vous pouvez définir dans System Automation for Multiplatforms.

Pourquoi et quand exécuter cette tâche

Ce déploiement utilise une ressource d'application que vous devez créer sur le serveur principal. En outre, vous devez créer des scripts pour démarrer, arrêter et surveiller le serveur principal et le serveur de secours.

Sous Windows, exécutez toutes les commandes de cette tâche dans le programme IBM Tivoli System Automation Shell. Pour démarrer cet interpréteur de commandes, cliquez sur **Démarrer** > **Tous les programmes** > **SA for Multiplatforms** > **IBM Tivoli System Automation-Shell**.

Procédure

1. Utilisez les exemples de scripts situés aux emplacements suivants pour créer les scripts nécessaires au serveur principal et au serveur de secours:
   - **Pour AIX, Linux et Solaris :**
     - Principal : `/opt/PolicyDirector/example/primaryscripts`
     - Secours : `/opt/PolicyDirector/example/standbyscripts`
   - **Pour Windows :**
     - Principal : `C:\Program Files\Tivoli\Policy Director\example\primaryscripts`

       Secours : `C:\Program Files\Tivoli\Policy Director\example\standbyscripts`

   Créez chacun des scripts suivants à la fois sur le serveur principal et sur le serveur de secours :

   polup Script de démarrage de la ressource en ligne. Utilisez l'exemple de script fourni dans les rubriques suivantes pour créer votre propre fichier :
   - «Script Polup pour le serveur principal», à la page 413
   - «Script Polup pour le serveur de secours», à la page 414

   poldown Script de mise hors ligne de la ressource. Utilisez l'exemple de script fourni dans les rubriques suivantes pour créer votre propre fichier :
   - «Script Poldown pour le serveur principal», à la page 416
   - «Script Poldown pour le serveur de secours», à la page 418

   polmon Script de surveillance de la ressource en ligne. Utilisez l'exemple de script fourni dans les rubriques suivantes pour créer votre propre fichier :
   - «Script Polmon pour le serveur principal», à la page 419
   - «Script Polmon pour le serveur de secours», à la page 420
2. Placez les scripts dans le répertoire `/opt/PolicyDirector/etc` ou `C:\Program Files\Tivoli\Policy Director/etc` sous Windows.

3. Créez une ressource d'application flottante sur le serveur de règles principal. Une *ressource flottante* est une ressource qui peut fonctionner sur plusieurs noeuds d'un cluster, mais à raison d'un seul noeud à la fois.
   a. Créez un fichier texte appelé `pdmgrd-rs.def` dans le répertoire `/opt/PolicyDirector/etc` ou `C:\Program Files\Tivoli\Policy Director/etc` sous Windows.
   b. Incluez le contenu et les définitions suivantes dans le fichier.

      Sur AIX ou Linux :

      ```
      PersistentResourceAttributes :
      Name="pdmgrd-rs"
      StartCommand="/opt/PolicyDirector/etc/polup"
      StopCommand="/opt/PolicyDirector/etc/poldown"
      MonitorCommand="/opt/PolicyDirector/etc/polmon"
      MonitorCommandPeriod=5
      MonitorCommandTimeout=30
      NodeNameList={'tiv024','tiv025'}
      StartCommandTimeout=30
      StopCommandTimeout=30
      UserName="root"
      ResourceType=1
      ```

      Sous Windows :

      ```
      PersistentResourceAttributes :
      Name="pdmgrd-rs"
      StartCommand="/dev/fs/C/Progra~1/Tivoli/Policy~1/etc/polup"
      StopCommand="/dev/fs/C/Progra~1/Tivoli/Policy~1/etc/poldown"
      MonitorCommand="/dev/fs/C/Progra~1/Tivoli/Policy~1/etc/polmon"
      MonitorCommandPeriod=5
      MonitorCommandTimeout=30
      NodeNameList={'tiv024','tiv025'}
      StartCommandTimeout=30
      StopCommandTimeout=30
      UserName="Administrateur"
      ResourceType=1
      ```

      Remarque : ResourceType=1 spécifie une ressource flottante ; la ressource peut être exécutée n'importe quel noeud, mais à raison d'une seule ressource à la fois.
   c. Sauvegardez le fichier.
   d. Exécutez la commande suivante :

      ```
      mkrsrc -f pdmgrd-rs.def IBM.Application
      ```
4. Créez un groupe de ressources. Par exemple, sur AIX ou Linux, tapez :

   ```
   mkrg pdmgrd-rg
   ```
5. Ajoutez la ressource d'application au groupe de ressources. Par exemple, sur AIX ou Linux, tapez :

   ```
   addrgmgr -g pdmgrd-rg IBM.Application:pdmgrd-rs
   ```
6. Connectez la ressource. Par exemple, sur AIX ou Linux, tapez :

   ```
   chrg -o online pdmgrd-rg
   ```
7. Testez l'automatisation du basculement :
   a. Arrêtez le serveur principal. Le programme pdmgrd démarre automatiquement sur le serveur de secours.
   b. Exécutez la commande **lssam** sur le serveur de secours. Si le basculement s'effectue, le serveur principal (pdmgrd) est indiqué comme étant hors ligne, tandis que le serveur de secours (pdmgrd) est en ligne.
   c. Testez la commande **pdadmin** sur le serveur d'exécution pour vous assurer que la fonction pdadmin est active.

d. Puis, arrêtez le serveur de secours. Le programme pdmgrd démarre automatiquement sur le serveur principal.
e. Testez à nouveau la commande **pdadmin** sur le serveur d'exécution pour vous assurer que la fonction pdadmin est active.
f. Si ces tests aboutissent, l'automatisation fonctionne. S'ils échouent, passez en revue les étapes précédentes et votre configuration jusqu'à ce que vous ayez déterminé l'origine de l'erreur.

Script Polup pour le serveur principal

Utilisez cet exemple de script pour créer un programme permettant de démarrer le serveur principal.

Script AIX ou Linux

```
#!/bin/sh

#
# Set the hostname or IP address for the standby policy server
#
STANDBY_SERVER=<standby_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop authorization server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Alias the loopback interface for the cluster IP address
#
ifconfig lo:1 <cluster_ip_address> netmask 255.255.255.255 up
logger -i -t "POLUP" "lo:1 interface UP"

#
# Start policy server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Script Windows

```
#!/bin/sh

#
# Set the hostname for the primary policy server
#
PRIMARY_SERVER=tiv024

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop authorization server
#
net stop IVAcld >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Start policy server
#
net start IVMgr >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Script Polup pour le serveur de secours

Utilisez cet exemple de script pour créer un programme permettant de démarrer le serveur de secours.

Script AIX ou Linux

```
#!/bin/sh

#
# Set the hostname or IP address for the standby policy server
#
STANDBY_SERVER=<standby_policy_server>
```

```
#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop authorization server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Alias the loopback interface for the cluster IP address
#
ifconfig lo:1 <cluster_ip_address> netmask 255.255.255.255 up
logger -i -t "POLUP" "lo:1 interface UP"

#
# Start policy server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Script Windows

```
#!/bin/sh

#
# Set the hostname for the standby policy server
#
STANDBY_SERVER=tiv025

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
```

```
# Stop authorization server
#
net stop IVAcld >/dev/null 2>&1
logger -i -t "POLUP" "Authorization server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd yes
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld no

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld no
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld no

logger -i -t "POLUP" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
# Start policy server
#
net start IVMgr >/dev/null 2>&1
logger -i -t "POLUP" "Policy server started"

exit 0
```

Script Poldown pour le serveur principal

Utilisez cet exemple de script pour créer un programme permettant d'arrêter le serveur principal.

Script AIX ou Linux

```
#!/bin/sh

#
# Set the hostname or IP address for the primary policy server
#
PRIMARY_SERVER=<primary_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop policy server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf -f pd.conf setentry pdrte boot-start-ivacld yes

#
```

```
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Unalias the loopback interface
#
ifconfig lo:1 down
logger -i -t "POLDOWN" "lo:1 interface DOWN"

#
# Start authorization server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Script Windows

```
#!/bin/sh

#
# Set the hostname for the standby policy server
#
STANDBY_SERVER=tiv025

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop policy server
#
net stop IVMgr >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $STANDBY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $STANDBY_SERVER"

#
```

```
# Start authorization server
#
net start IVAcld >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Script Poldown pour le serveur de secours

Utilisez cet exemple de script pour créer un programme permettant d'arrêter le serveur de secours.

Script AIX ou Linux

```
#!/bin/sh

#
# Set the hostname or IP address for the primary policy server
#
PRIMARY_SERVER=<primary_policy_server>

#
# Add Security Access Manager CLI to PATH
#
PATH=$PATH:/opt/PolicyDirector/bin
PATH=$PATH:/opt/PolicyDirector/sbin
export PATH

#
# Stop policy server
#
pd_start stop >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /opt/PolicyDirector/etc

pdconf -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Unalias the loopback interface
#
ifconfig lo:1 down
logger -i -t "POLDOWN" "lo:1 interface DOWN"

#
# Start authorization server
#
pd_start start >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Script Windows

```
#!/bin/sh

#
# Set the hostname for the primary policy server
#
PRIMARY_SERVER=tiv024

#
# Add Security Access Manager dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/bin
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/Policy~1/sbin
export PATH

#
# Add IBM Security Utilities dll location to PATH
#
PATH=$PATH:/dev/fs/C/Progra~1/Tivoli/TivSecUtl/bin
export PATH

#
# Stop policy server
#
net stop IVMgr >/dev/null 2>&1
logger -i -t "POLDOWN" "Policy server stopped"

#
# Change pd.conf
#
cd /dev/fs/C/Progra~1/Tivoli/Policy~1/etc

pdconf.exe -f pd.conf setentry manager master-host $PRIMARY_SERVER
pdconf.exe -f pd.conf setentry pdrte boot-start-ivmgrd no
pdconf.exe -f pd.conf setentry pdrte boot-start-ivacld yes

#
# Add lines for additional authorization servers used for additional domains
#
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain2-ivacld yes
#pdconf.exe -f pd.conf setentry pdrte boot-start-domain3-ivacld yes

logger -i -t "POLDOWN" "pd.conf modified: master-host set to $PRIMARY_SERVER"

#
# Start authorization server
#
net start IVAcld >/dev/null 2>&1
logger -i -t "POLDOWN" "Authorization server started"

exit 0
```

Script Polmon pour le serveur principal

Utilisez cet exemple de script pour créer un programme permettant de surveiller le serveur principal.

Script AIX ou Linux

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -ef | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
```

```
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Script Windows

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -e | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Script Polmon pour le serveur de secours

Utilisez cet exemple de script pour créer un programme permettant de surveiller le serveur de secours.

Script AIX ou Linux

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -ef | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Script Windows

```
#!/bin/sh

OPSTATE_ONLINE=1
OPSTATE_OFFLINE=2

ps -e | grep -v "grep" | grep "pdmgrd" >/dev/null
if [ $? == 0 ]
then
    RC=${OPSTATE_ONLINE}
else
    RC=${OPSTATE_OFFLINE}
fi

exit $RC
```

Annexe I. Configuration de l'environnement de proxy Tivoli Directory Server

Un proxy Tivoli Directory Server est un type spécial d'instance IBM Tivoli Directory Server qui fournit le routage des requêtes, l'équilibrage de charge, la reprise en ligne, l'authentification distribuée et la prise en charge des groupes distribués ou de propriété, ainsi que le partitionnement des conteneurs.

Avertissement : Les clients d'IBM Security Access Manager qui souhaitent utiliser le serveur proxy Tivoli Directory Server doivent acheter une autorisation Tivoli Directory Server séparée. La version de Tivoli Directory Server qui fait partie du module Security Access Manager ne permet pas l'utilisation par les clients IBM Security Access Manager du serveur proxy Tivoli Directory Server.

Si vous disposez des droits appropriés, utiliser les instructions relatives au serveur proxy décrites dans le manuel *IBM Tivoli Directory Server Administration Guide* pour configurer le serveur proxy : http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/admin_gd.htm.

Puis, revenez à ce document pour obtenir des instructions concernant la configuration du serveur proxy en vue du fonctionnement avec IBM Security Access Manager.

Security Access Manager stocke ses métadonnées dans un suffixe obligatoire appelé `secAuthority=Default`. Les métadonnées incluent des informations utilisées pour suivre les informations de statut sur l'utilisateur et le groupe spécifiques à Security Access Manager. Lorsque vous utilisez un proxy, l'objet `secAuthority=Default` en lui-même ne peut pas être modifié à l'aide du proxy car l'objet situé au niveau d'un point de fractionnement d'une partition de proxy ne peut pas être modifié via le proxy. Par conséquent, Security Access Manager ne peut pas être configuré directement via le proxy car Security Access Manager doit modifier l'objet `secAuthority=Default` lors de la configuration.

Dans un environnement proxy, l'administrateur doit décider sur quel serveur d'arrière-plan la sous-arborescence `secAuthority=Default` sera hébergée et configurer ce serveur d'arrière plan et les informations de partition du proxy de sorte à refléter cette topologie. Cet exemple explique la configuration du `Serveur A` pour héberger la sous-arborescence `secAuthority=Default`.

Les données se trouvant sous un point de fractionnement d'une partition de proxy (par exemple, `o=ibm,c=us`) sont hachées pour déterminer le serveur d'arrière-plan qui contient la sous- arborescence. Dans cet exemple, le `Proxy` est configuré pour hacher les valeurs RDN immédiatement après `o=ibm,c=us` sur deux serveurs. Cela signifie également que les valeurs RDN supérieures de plus de 1 à `o=ibm,c=us` seront mappées au même serveur que les valeurs immédiatement après `o=ibm,c=us`. Pour cette raison, il est généralement plus avantageux de configurer le proxy avec une partition unique pour le suffixe `secAuthority=Default`.

Si vous souhaitez distribuer les métadonnées de Security Access Manager dans le suffixe `secAuthority=Default` sur plusieurs serveurs d'arrière plan, il est préférable de diviser la partition sous le conteneur `cn=Users,secAuthority=Default`. Les entrées sont effectuées au nom de chaque utilisateur défini sous le conteneur

© Copyright IBM Corp. 2001, 2013

cn=Users,secAuthority=Default. Par conséquent, le fractionnement de ces informations utilisateur peut permettre de distribuer les données de manière plus équilibrée sur les serveurs d'arrière plan. Cet exemple ne distribuera pas les données mais conservera la totalité de la sous-arborescence secAuthority=Default sur le Serveur A.

Ajout du suffixe Security Access Manager au proxy

Pour le proxy destiné à fonctionner avec Security Access Manager, vous devez configurer le suffixe secAuthority=Default.

Procédure

1. Connectez-vous au Serveur A en tant qu'administrateur LDAP local (par exemple, cn=root).
2. Sélectionnez **Server administration** > → > **Manage server properties**. Sélectionnez la propriété Suffixes.
3. Dans la zone **Suffix DN**, entrez Default.
4. Cliquez sur **Add**.
5. Lorsque vous avez terminé, cliquez sur **Apply** pour sauvegarder vos modifications sans quitter la page, ou sur **OK** pour appliquer vos modifications et fermer la fenêtre.
6. Le suffixe ne sera pas disponible tant que le serveur n'a pas été redémarré. Dans le panneau de navigation, sélectionnez **Server administration**, puis **Start/stop/restart server**.
7. Assurez-vous que la case **Start/restart in configuration only mode** *n'est pas* cochée.
8. Cliquez sur **Restart**.
9. Après que le message indiquant que la demande de redémarrage a été envoyée s'est affiché, accédez à **Server administration**, puis vérifiez le statut du serveur. Attendez que le serveur redémarre, puis soit en cours d'exécution avant de poursuivre.
10. Connectez-vous au Proxy en tant qu'administrateur LDAP local (par exemple, cn=root).
11. Dans le panneau de navigation, développez **Proxy administration**.
12. Dans la page Proxy administration, cliquez sur **Manage proxy properties**.
13. Dans la zone **Suffix DN**, entrez Default.
14. Cliquez sur **Add**.
15. Cliquez sur **OK** pour sauvegarder vos changements et revenir à la fenêtre Introduction.
16. Dans le panneau de navigation, cliquez sur **Proxy administration**, puis sur **Manage partition bases**.
17. Dans le menu **Manage partition bases**, cliquez sur **Ajouter**.
18. Dans la zone **Split Name**, entrez Split 1.
19. Dans la zone **Partition base DN**, saisissez : secAuthority=Default
20. Dans la zone **Number of partitions**, saisissez : 1
21. Dans la table **Partition bases**, sélectionnez le bouton d'option **secAuthority=Default**.
22. Cliquez sur **View servers**, puis vérifiez que secAuthority=Default s'affiche dans la zone **Partition base DN**.
23. Dans la table **Back-end directory servers for partition base**, cliquez sur **Add**.

24. Dans le menu **Add Back-end directory server**, cliquez sur **Back-end directory server** > ➔ > **Serveur A**.
25. Vérifiez que 1 s'affiche dans la zone **Partition index**.
26. Cliquez sur **OK**.
27. Lorsque vous avez terminé, cliquez sur **Close**.
28. Redémarrez le serveur `Proxy` pour que les changements prennent effet.

Configuration de Security Access Manager pour utiliser le proxy

Une fois que le serveur proxy Tivoli Directory Server et les serveurs d'arrière-plan sont configurés avec la configuration du fractionnement DIT, Security Access Manager peut être configuré pour utiliser le proxy. Le serveur proxy fournit une vue unifiée du répertoire et empêche l'application LDAP (Security Access Manager par exemple) d'être consciente du fractionnement DIT.

Lorsqu'il est configuré pour utiliser le serveur proxy Tivoli Directory Server, Security Access Manager est uniquement conscient du proxy et exécute toutes les opérations via le proxy, comme s'il représentait la totalité de l'espace de nom DIT.

Pour offrir un support de reprise en ligne, plusieurs serveurs proxy Tivoli Directory Server peuvent également être configurés. Pour obtenir des informations sur la configuration de plusieurs serveurs proxy Tivoli Directory Server en vue d'offrir le support de reprise en ligne, voir le manuel *IBM Tivoli Directory Server : Guide d'administration*. Lors de la configuration de plusieurs serveurs proxy pour offrir le support de reprise en ligne, Security Access Manager doit être configuré de sorte à traiter chacun des serveurs proxy comme une réplique du serveur d'annuaire. L'exemple de scénario décrit ci-dessous suppose qu'il n'existe qu'un seul proxy.

Etant donné que Security Access Manager ne peut pas être configuré directement sur le serveur proxy Tivoli Directory Server, Security Access Manager doit d'abord être configuré sur le serveur d'arrière-plan qui héberge la sous-arborescence `secAuthority=Default`. Lors de la configuration du composant Security Access Manager Runtime pour l'utiliser avec ce serveur d'arrière-plan, sélectionnez **LDAP** en tant que type de registre. Lorsque l'utilitaire **`pdconfig`** demande le **nom d'hôte LDAP**, saisissez le nom d'hôte et le **numéro de port LDAP** du `Serveur A` (le serveur d'arrière-plan qui héberge la sous-arborescence `secAuthority=Default`). Ne saisissez pas le nom d'hôte du serveur proxy Tivoli Directory Server (`Proxy`).

Configurez les informations SSL pour définir une connexion SSL avec le `Serveur A`, si SSL doit être utilisé. Lorsque vous utilisez SSL, le `Proxy` doit être configuré avec un certificat de serveur qui est généré par la même autorité de certification (AC) que celle utilisée pour créer le certificat de serveur du `Serveur A`. Indiquez le nom distinctif LDAP (par exemple, `cn=root`) et le mot de passe de l'administrateur LDAP pour le `Serveur A`. Une fois que le serveur de règles Security Access Manager est configuré avec succès sur le serveur d'arrière-plan (`Serveur A`), vous pouvez recibler le système de serveur de règles Security Access Manager sur le serveur proxy Tivoli Directory Server. Quittez l'utilitaire **`pdconfig`**.

Redirection du serveur de règles vers le proxy

Pour recibler le système de serveur de règles Security Access Manager sur le proxy, arrêtez le serveur de règles à l'aide de la commande **`pd_start stop`** sous AIX,

Linux ou Solaris, ou à l'aide des services Windows. Editez le serveur de règles `ldap.conf` et les fichiers de configuration `pd.conf` à l'aide de la commande **pdadmin config**.

Procédure

1. Démarrez l'utilitaire **pdadmin**.
2. Connectez-vous au système local à l'aide de la commande **login –l**.
3. Après vous être connecté localement, modifiez la valeur de l'hôte et du port dans les fichiers de configuration pour indiquer le nom d'hôte et le port du serveur proxy Tivoli Directory Server à l'aide des commandes suivantes : **Pour AIX, Linux ou Solaris** :

```
config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf ldap host nom_hôte_proxy
config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf ldap port port_proxy
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf pdrte user-reg-server nom_hôte_proxy
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf pdrte user-reg-host nom_hôte_proxy
config modify keyvalue set /opt/PolicyDirector/etc/pd.conf pdrte user-reg-hostport port_proxy
```

Pour Windows : **Remarque :** cet exemple suppose que Security Access Manager est installé à l'emplacement par défaut. Modifiez les commandes suivantes pour correspondre à l'emplacement d'installation pour votre système si nécessaire.

```
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
   ldap host nom_hôte_proxy
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
   ldap port port_proxy
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-server nom_hôte_proxy
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-host nom_hôte_proxy
config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
  pdrte user-reg-hostport port_proxy
```

où :

nom_hôte_proxy
Est le nom d'hôte du serveur proxy Tivoli Directory Server.

port_proxy
Est le numéro de port du serveur proxy Tivoli Directory Server.

4. Une fois que les fichiers de configuration sont modifiés, le serveur de règles peut être redémarré à l'aide de l'utilitaire **pd_start start** sous AIX, Linux ou Solaris, ou des services Windows.

Résultats

Pour plus d'informations sur ces commandes et utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

Configuration des contrôles d'accès pour le proxy

Comme indiqué précédemment, les listes de contrôle d'accès (ACL) ne peuvent pas être gérées à partir du serveur proxy Tivoli Directory Server. Lorsqu'un serveur proxy est utilisé, c'est le serveur d'arrière-plan qui applique le contrôle d'accès. L'administrateur LDAP est responsable de s'assurer que les ACL adéquates sont créées sur chaque serveur d'arrière-plan si les ACL existent sur l'objet de niveau supérieur du point de fractionnement de la partition.

Pourquoi et quand exécuter cette tâche

Security Access Manager doit disposer d'un contrôle d'accès pour lui permettre de gérer les utilisateurs et les groupes au sein des suffixes dans lesquels les définitions de groupe et d'utilisateur sont conservées. Pour définir les listes de contrôle d'accès sur les serveurs d'arrière-plan afin de permettre à Security Access Manager de gérer les suffixes de partition, exécutez l'utilitaire Security Access Manager **ivrgy_tool** en spécifiant le paramètre **add-acls**.

Procédure

1. Exécutez l'utilitaire **ivrgy_tool** à partir de n'importe quel système sur lequel Security Access Manager Runtime est installé, par exemple le système sur lequel le serveur de règles est installé.
2. Pour appliquer les ACL adéquates sur chaque serveur d'arrière-plan, exécutez la commande suivante :

   ```
   ivrgy_tool -h hôte_arrière-plan -p port_arrière-plan -D ND_admin_ldap \
   -w mdp_admin_ldap -d [-Z] [-K fichier_clés_ssl] [-P mdp_fichier_clés_ldap] \
   [-N label] add-acls domaine
   ```

   Pour plus d'informations sur l'utilitaire **ivrgy_tool**, voir *IBM Security Access Manager for Web Command Reference*.

Résultats

Le serveur de règles est le seul composant Security Access Manager qui doit être reciblé sur le serveur proxy Tivoli Directory Server comme décrit dans la section «Configuration de Security Access Manager pour utiliser le proxy», à la page 423. Les autres composants Security Access Manager, notamment le serveur d'autorisations ou WebSEAL, ne doivent pas être reciblés.

Une fois que le serveur de règles est configuré, les autres composants Security Access Manager peuvent être configurés normalement.

Lors de la configuration de Security Access Manager Runtime pour les autres composants, le nom d'hôte et le port du serveur proxy Tivoli Directory Server doivent être indiqués pour le nom d'hôte LDAP. Il n'est pas nécessaire d'indiquer l'un des serveurs d'arrière-plan.

Annulation de la configuration de Security Access Manager à partir du proxy

Avant de pouvoir annuler la configuration du serveur de règles, il doit être reciblé sur le serveur d'arrière-plan qui héberge la sous-arborescence `secAuthority=Default`. Avant de tenter de recibler et d'annuler la configuration du serveur de règles, vérifiez que tous les autres composants Security Access Manager sont arrêtés et que leur configuration est annulée.

Pourquoi et quand exécuter cette tâche

Il est possible d'annuler normalement la configuration de tous les composants de Security Access Manager *autres* que le serveur de règles lorsque l'environnement est configuré avec le serveur proxy Tivoli Directory Server (comme décrit à la rubrique «Configuration de Security Access Manager pour utiliser le proxy», à la page 423).

Une fois que la configuration de tous les composants Security Access Manager est annulée, le serveur de règles peut être reciblé sur le serveur d'arrière-plan qui héberge la sous-arborescence `secAuthority=Default`.

Pour recibler le système du serveur de règles sur le serveur d'arrière-plan, arrêtez le serveur de règles à l'aide de la commande **pd_start stop** sous AIX, Linux ou Solaris, ou à l'aide des services Windows. Editez le serveur de règles `ldap.conf` et les fichiers de configuration `pd.conf` à l'aide de la commande **pdadmin config**.

Procédure

1. Lancez la commande **pdadmin**.
2. Connectez-vous au système local à l'aide de la commande **login –l**.
3. Modifiez la valeur de l'hôte et du port dans les fichiers de configuration pour spécifier le nom d'hôte et le port du serveur d'arrière-plan qui héberge la sous-arborescence `secAuthority=Default` (`Serveur A` dans cet exemple) :

   Pour AIX, Linux ou Solaris :

   ```
   config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf
      \ldap host nom_hôte_serveurA
   config modify keyvalue set /opt/PolicyDirector/etc/ldap.conf
     \ldap port port_serveurA
   config modify keyvalue set /opt/PolicyDirector/etc/pd.conf
     \pdrte user-reg-server nom_hôte_serveurA
   config modify keyvalue set /opt/PolicyDirector/etc/pd.conf
     \pdrte user-reg-host nom_hôte_serveurA
   config modify keyvalue set /opt/PolicyDirector/etc/pd.conf
     \pdrte user-reg-hostport port_serveurA
   ```

   Pour Windows

   Cet exemple suppose que Security Access Manager est installé à l'emplacement par défaut. Modifiez les commandes suivantes pour correspondre à l'emplacement d'installation de votre système si nécessaire :

   ```
   config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
     ldap host nom_hôte_serveurA
   config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\ldap.conf"
     ldap port port_serveurA
   config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
     pdrte user-reg-server nom_hôte_serveurA
   config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
     pdrte user-reg-host nom_hôte_serveurA
   config modify keyvalue set "c:\Program Files\Tivoli\Policy Director\etc\pd.conf"
     pdrte user-reg-hostport port_serveurA
   ```

   où :

   nom_hôte_serveurA
   : Nom d'hôte du serveur d'arrière-plan.

   port_serveurA
   : Numéro de port du serveur d'arrière-plan.
4. Une fois que les fichiers de configuration sont modifiés, le serveur de règles peut être redémarré à l'aide de l'utilitaire **pd_start start** sous AIX, Linux ou Solaris, ou des services Windows.
5. Une fois que le serveur d'arrière-plan a été redémarré avec succès, sa configuration peut être annulée à l'aide de l'utilitaire **pdconfig**.

Résultats

Pour plus d'informations sur ces commandes et utilitaires, voir : *IBM Security Access Manager for Web Command Reference*.

Annexe J. Adaptateur de registre Security Access Manager pour les référentiels fédérés WebSphere

L'adaptateur de registre Security Access Manager pour les référentiels fédérés WebSphere utilise l'API Java Security Access Manager Registry Direct pour effectuer des opérations liées au registre.

L'adaptateur :

- Est un adaptateur VMM (gestionnaire de membre virtuel). Pour obtenir des informations détaillées sur VMM, voir la documentation sur les gestionnaires de membres virtuels dans le centre de documentation IBM IBM WebSphere Application Server à l'adresse http://www.ibm.com/software/webservers/appserv/was/library/.
- Prend en charge un seul domaine Security Access Manager. Toutefois, Security Access Manager prend en charge le support pour les domaines sécurisés multiples lorsqu'il est configuré avec le registre LDAP.
- Prend en charge les registres Security Access Manager pris en charge par l'API Java Registry Direct.

© Copyright IBM Corp. 2001, 2013

Annexe K. Désinstallation

La désinstallation de Security Access Manager est un processus en trois étapes.

Vous devez annuler la configuration des composants, supprimer les packages Security Access Manager, puis redémarrer le système.

Avertissement : N'annulez la configuration du composant Security Access Manager Runtime que si la configuration de toutes les applications Security Access Manager installées sur le système, comme WebSEAL et d'autres plug-ins de serveur Web a déjà été annulée. Sinon, l'application Security Access Manager reste dans un état inutilisable.

Annulez la configuration et supprimez le système de serveur de règles en dernier.

Annulation de la configuration des composant Security Access Manager

Avant de supprimer les packages Security Access Manager, vous devez vous assurer que la configuration du composant est annulée (le cas échéant).

Procédure

1. Sur les systèmes AIX, Linux ou Solaris, connectez-vous en tant que **root**. Sous Windows, connectez-vous en tant qu'utilisateur ayant des droits d'administrateur Windows.
2. Pour démarrer l'utilitaire de configuration, entrez la commande suivante :
   ```
   pdconfig
   ```
   Remarque : Vous pouvez également, sur le système Windows, sélectionner **Démarrer → Programmes → IBM Security Access Manager → Configuration**. Le menu de configuration de Security Access Manager s'affiche.
3. Annulez la configuration des composants dans l'ordre suivant :
   a. Security Access Manager Attribute Retrieval Service
   b. Interface de ligne de commande de gestion des sessions Security Access Manager, ou service de gestion de sessions de Security Access Manager
   c. Security Access Manager Web Portal Manager, Access Manager WebSEAL, ou Security Access Manager Plug-in for Web Servers
   d. Instances de Security Access Manager Authorization Server
   e. Security Access Manager Policy Proxy Server, Standby Security Access Manager Policy Server
   f. Security Access Manager Policy Server
   g. Security Access Manager Runtime et Security Access Manager Runtime for Java

   Pour annuler la configuration d'un composant sous AIX, Linux ou Solaris, entrez le numéro de l'élément de menu du composant Security Access Manager. Pour annuler la configuration d'un composant sous Windows, sélectionnez un composant et cliquez sur **Annuler la configuration**. Répétez cette procédure pour chaque package dont la configuration doit être annulée.

© Copyright IBM Corp. 2001, 2013

Remarque :

a. Si vous utilisez un registre d'utilisateurs LDAP et que vous annulez la configuration d'un serveur de règles ou d'un serveur proxy de règles, vous êtes invité à entrer le nom distinctif (**cn=root**) et le mot de passe de l'administrateur LDAP.

b. Pendant l'annulation de la configuration du serveur de règles :
   - Vous êtes averti que les informations de configuration et d'autorisation de tous les serveurs et applications Security Access Manager installés dans le domaine de gestion seront supprimées. Entrez **y** pour poursuivre.
   - Vous êtes invité à indiquer si vous souhaitez supprimer définitivement les informations de domaine du registre. Entrez **y** pour supprimer toutes les informations de domaine, y compris les informations d'utilisateur et de groupe. Entrez **n** pour supprimer les informations de domaine mais pour conserver les informations d'utilisateur et de groupe pour pouvoir recréer le domaine ultérieurement, le cas échéant.

c. Si vous avez installé le composant Security Access Manager Runtime for Java ou Web Portal Manager, mais *pas* le composant Security Access Manager Runtime, lancez l'utilitaire **pdjrtecfg** sous le chemin `/opt/PolicyDirector/sbin/` pour annuler la configuration de Security Access Manager Runtime for Java. Entrez :

   ```
   /opt/PolicyDirector/sbin/pdjrtecfg -action unconfig -interactive
   ```

   Lancez l'utilitaire **amwpmcfg** dans le chemin `/opt/PolicyDirector/sbin/` pour annuler la configuration de Security Access Manager Web Portal Manager. Entrez :

   ```
   /opt/PolicyDirector/sbin/amwpmcfg -action unconfig -interactive
   ```

Annulation de la configuration d'IBM Tivoli Directory Server

L'annulation de la configuration d'IBM Tivoli Directory Server implique celle de la base de données sur l'instance de serveur d'annuaire, ainsi que la suppression de cette instance.

Sauvegardez votre annuaire et les fichiers de schéma existants avant de commencer cette procédure.

Annulation de la configuration de la base de données

La configuration de la base de données associée à une instance de serveur d'annuaire peut être annulée à l'aide de l'outil de configuration ou de la ligne de commande.

Utilisation de l'outil de configuration

Utilisez l'outil de configuration pour annuler la configuration de la base de données qui est associée à une instance de serveur d'annuaire.

Procédure

1. Sur les systèmes AIX, Linux ou Solaris, connectez-vous en tant que **root**. Sur les systèmes Windows, connectez-vous avec un ID utilisateur membre du groupe Administrateurs.
2. Démarrez l'outil de configuration en entrant la commande suivante : `idsxcfg`
3. Cliquez sur **Annuler la configuration de la base de donnée** dans le panneau de navigation.

4. Dans la fenêtre **Annuler la configuration de la base de donnée**, sélectionnez l'une des options suivantes :

   Annuler la configuration de la base de données
   Supprime les informations sur la base de données du fichier de configuration pour l'instance de serveur d'annuaire. Toutefois, la base de données et ses données restent intactes. La base de données devient inaccessible pour l'instance de serveur d'annuaire mais les données qu'elle contient ne sont pas supprimées.

   Annuler la configuration et supprimer la base de données
   Supprime la base de données et son contenu ainsi que les informations sur la base de données du fichier de configuration pour l'instance de serveur d'annuaire.
5. Cliquez sur **Annuler la configuration**.
6. Cliquez sur **Oui** pour confirmer l'opération.

Utilisation de la ligne de commande

Utilisez la commande **idsucfgdb** pour annuler la configuration d'une base de données pour une instance de serveur d'annuaire.

Par défaut, **idsucfgdb** annule la configuration de la base de données du fichier `ibmslapd.conf`, mais ne supprime pas la base de données. Vous pouvez facultativement spécifier une suppression de la base de données.

Remarque : Sur les systèmes AIX, Linux ou Solaris, connectez-vous en tant que **root**. Sur les systèmes Windows, connectez-vous avec un ID utilisateur membre du groupe Administrateurs.

Par exemple :

- Pour annuler la configuration de la base de données pour une instance de serveur d'annuaire `my_instance`, entrez la commande :

  ```
  idsucfgdb -n -I my_instance
  ```

  Remarque : L'option -n indique de ne pas inviter l'utilisateur à confirmer l'opération avant l'annulation de la configuration
- Pour annuler la configuration et supprimer la base de données pour une instance de serveur d'annuaire `my_instance`, entrez la commande :

  ```
  idsucfgdb –r –n -I myinstance
  ```

  Remarque :
  1. L'option `-n` indique que l'utilisateur n'est pas invité à confirmer l'opération avant l'annulation de la configuration
  2. L'option `-r` spécifie la suppression de la base de données

Voir le manuel *IBM Tivoli Directory Server Command Reference* pour obtenir des informations détaillées sur la commande **idsucfgdb**.

Suppression d'une instance de serveur d'annuaire

Vous pouvez supprimer une instance de serveur d'annuaire et son instance de base de données associée à l'aide de l'outil d'administration d'instance ou de la ligne de commande.

Utilisation de l'outil d'administration d'instance

Utilisez l'outil d'administration d'instance pour supprimer une instance de serveur d'annuaire et, facultativement, son instance de base de données associée.

Procédure

1. Sur les systèmes AIX, Linux ou Solaris, connectez-vous en tant que **root**. Sur les systèmes Windows, connectez-vous avec un ID utilisateur membre du groupe Administrateurs.
2. Arrêtez l'instance d'annuaire, si elle est en cours d'exécution.
3. Démarrez l'outil d'administration d'instance,le cas échéant.
   - Sur les systèmes AIX, Linux ou Windows, entrez la commande suivante : `idsxinst`.
   - Sur les systèmes Windows, vous pouvez également cliquer sur **Démarrer** > **Programmes** > **IBM Tivoli Directory Server** > **Outil d'administration d'instance**.
4. Dans la fenêtre **IBM Tivoli Directory Server Instance Administration Tool**, sélectionnez l'instance à supprimer et cliquez sur **Supprimer...**.
5. Dans la fenêtre **Delete directory server instance**, sélectionnez l'une des options suivantes :

   Delete directory server instance only
   Pour supprimer l'instance de serveur d'annuaire mais laisser l'instance de base de données intacte.

   Delete directory server instance and destroy associated database instance
   Pour supprimer l'instance de serveur d'annuaire et l'instance de base de données.
6. Cliquez sur **Supprimer**. Des messages sont affichés dans le panneau Task Messages lorsque l'opération est en cours.
7. Cliquez sur **Fermer** à la fin de l'opération pour fermer la fenêtre et revenir à la fenêtre principale de l'outil d'administration d'instance.
8. Si vous avez terminé d'utiliser l'outil d'administration d'instance, cliquez sur **Fermer** pour quitter l'outil.

Utilisation de la ligne de commande

Utilisez la commande **idsidrop** pour supprimer une instance de serveur d'annuaire.

Procédure

1. Sur les systèmes AIX, Linux ou Solaris, connectez-vous en tant que **root**. Sur les systèmes Windows, connectez-vous avec un ID utilisateur membre du groupe Administrateurs.
2. Arrêtez l'instance d'annuaire à supprimer.
3. Entrez la commande qui permet de supprimer l'instance. Indiquez les options appropriées pour la commande.

   Exemples :
   - Pour supprimer l'instance de serveur d'annuaire mais conserver l'instance de base de données associée :

     ```
     idsidrop -I <nom_instance>
     ```
   - Pour supprimer une instance de serveur d'annuaire et détruire l'instance de base de données associée :

     ```
     idsidrop -I <nom_instance> -r
     ```

- Pour annuler la configuration de l'instance de base de données associée sans supprimer une instance de serveur d'annuaire :

  ```
  idsidrop -I <nom_instance>
  -R
  ```

Résultats

Voir le manuel *IBM Tivoli Directory Server Command Reference* pour obtenir des informations sur la commande **idsidrop**.

Suppression de packages

La désinstallation de Security Access Manager est un processus en trois étapes. Vous devez annuler la configuration des composants, supprimer les packages Security Access Manager, puis redémarrer le système.

Désinstallation d'IBM Tivoli Directory Server

Après avoir annulé la configuration d'IBM Tivoli Directory Server, vous procéder à sa désinstallation.

Avant de commencer

La méthode appropriée pour la désinstallation d'IBM Tivoli Directory Server dépend de la méthode utilisée pour installer Tivoli Directory Server. Utilisez le tableau suivant pour choisir la méthode de désinstallation appropriée.

Tableau 36. Méthodes de désinstallation de Tivoli Directory Server

Méthode utilisée pour installer Tivoli Directory Server	**Méthode utilisée pour désinstaller Tivoli Directory Server**
Assistant d'installation de Tivoli Directory Server «Installation d'IBM Tivoli Directory Server avec l'assistant d'installation Tivoli Directory Server», à la page 60	Utilisez la procédure suivante, qui utilise une interface graphique utilisateur telle que l'assistant d'installation.
Fichier script	Utilisez la méthode correspondant à votre plateforme : • «AIX : suppression de packages», à la page 434 • «Linux : suppression des packages», à la page 436 • «Solaris : suppression de packages», à la page 438 • «Windows : suppression de packages», à la page 439
Tableau de bord «Installation de Tivoli Directory Server avec le tableau de bord (Windows uniquement)», à la page 69	Utilisez la procédure suivante ou celle de la rubrique «Windows : suppression de packages», à la page 439.

Procédure

1. Ouvrez une invite de commande.
2. Accédez au répertoire `_uninst`.

   Windows
   *racine_ldap*_uninst

   où *racine_ldap* est l'emplacement où Tivoli Directory Server est installé.

   AIX et Solaris
   /opt/IBM/ldap/V6.3/_uninst

   Linux
   /opt/IBM/ldap/V6.3/_uninst
3. Lancez la commande de désinstallation :

   Windows
   uninstall_tds.exe

   AIX, Linux ou Solaris
   ./uninstall_tds.bin

AIX : suppression de packages

Suppression des packages sur AIX pour désinstaller Security Access Manager.

Avant de commencer

Avant de supprimer les packages, arrêtez toute instance de services et d'applications Security Access Manager en cours d'exécution.

Procédure

1. Assurez-vous que la configuration des composants a été annulée (le cas échéant). Suivez les instructions dans «Annulation de la configuration des composant Security Access Manager», à la page 429.
2. Entrez la commande suivante : `installp -u -g` *packages*
   où *packages* spécifie un ou plusieurs packages suivants. **Remarque :** utilisez l'option **–g** uniquement si vous souhaitez supprimer un logiciel dépendant du module spécifié.

AIX Certificate and SSL Base Runtime Acme Toolkit IBM Global Security Kit (GSKit)	GSKit8.gsksslб4.ppc.rte GSKit8.gskcrypt64.ppc.rte
IBM Tivoli Directory Server Web Administration Tool (sans SSL)	idsldap.webadmin63
IBM Tivoli Directory Server Web Administration Tool (SSL)	idsldap.webadmin_max_crypto63
Client IBM Tivoli Directory Server	idsldap.cltbase63 idsldap.clt64bit63 idsldap.clt_max_crypto64bit63 idsldap.cltjava63
IBM Tivoli Directory Server	idsldap.srv64bit63 idsldap.srvproxy64bit63 idsldap.srv_max_crypto64bit63 idsldap.srv_max_cryptoproxy64bit63 idsldap.msg63.en_US

Security Access Manager Application Development Kit	PD.AuthADK
Security Access Manager Attribute Retrieval Service	PDWeb.ARS
Security Access Manager Authorization Server	PD.Acld
Security Access Manager License	PD.lic
Security Access Manager Plug-in for IBM HTTP Server	PD.WPIIHS
Security Access Manager Plug-in for Web Servers	PD.WPI
Security Access Manager Policy Proxy Server	PD.MgrPrxy
Security Access Manager Policy Server	PD.Mgr
Security Access Manager Runtime	PD.RTE
IBM Security Access Manager Runtime for Java	PDJ.rte
Security Access Manager Session Management Command Line	PD.SMSCLI
Security Access Manager Session Management Server	PD.SMS
Security Access Manager Web Portal Manager	PD.WPM
Security Access Manager Web Security ADK	PDWeb.ADK
Security Access Manager Web Security Runtime	PDWeb.RTE
Security Access Manager WebSEAL	PDWeb.Web
Security Utilities	TivSec.Utl

3. Lorsque vous avez terminé de supprimer les packages, redémarrez le système.

Suppression de DB2

Exécutez cette tâche pour supprimer DB2 d'un système AIX.

Procédure

1. Connectez-vous comme utilisateur avec des droits `root`.
2. Accédez au répertoire suivant :
   rép_install_db2`/install`

   où *rép_install_db2* est le répertoire dans lequel DB2 est installé.
3. Exécutez la commande suivante :
   `./db2_deinstall -a`

Suppression de WebSphere Application Server, d'IBM HTTP Server ou du composant Plug-in for Web Servers

Pour supprimer WebSphere Application Server et le logiciel WebSphere associé tel qu'IBM HTTP Server ou le composant Plug-in for Web Servers d'un système AIX, voir les instructions du centre de documentation WebSphere Application Server.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Linux : suppression des packages

Suppression des packages sur Linux pour désinstaller Security Access Manager.

Avant de commencer

Avant de supprimer les packages, arrêtez toute instance de services et d'applications Security Access Manager en cours d'exécution.

Procédure

1. Assurez-vous d'avoir annulé la configuration des composants. Suivez les instructions dans «Annulation de la configuration des composant Security Access Manager», à la page 429.
2. Entrez la commande suivante : `rpm -e packages`
   où *packages* spécifie un ou plusieurs packages suivants :

IBM Global Security Kit (GSKit)	`gskcrypt64-8.0.14.26` `gskssl64-8.0.14.26`
IBM Tivoli Directory Server Web Administration Tool	`idsldap-webadmin63-6.3.0-17`
Client IBM Tivoli Directory Server	`idsldap-clt64bit63-6.3.0-17` `idsldap-cltbase63-6.3.0-17` `idsldap-cljava63-6.3.0-17`
IBM Tivoli Directory Server (packages serveur 64 bits et serveur proxy 64 bits)	`idsldap-srv64bit63-6.3.0-17` `idsldap-srvproxy64bit63-6.3.0-17`
Messages en anglais d'IBM Tivoli Directory Server	`idsldap-msg63-en-6.3.0-17`
Security Access Manager Application Development Kit	`PDAuthADK-PD-7.0.0-0`
Security Access Manager Attribute Retrieval Service (Linux on System z et Linux on x86-64 uniquement)	`PDWebARS-PD-7.0.0-0`
Security Access Manager Authorization Server`PDAcld-PD-7.0.0-0`	
Security Access Manager License	`PDlic-PD-7.0.0-0`
Security Access Manager Plug-in for Apache Web Server (Linux on System z uniquement)	`PDWPI-Apache-7.0.0-0`
Security Access Manager Plug-in for IBM HTTP Server (Linux on x86-64 et Linux on System z)	`PDWPI-IHS-7.0.0-0`
Security Access Manager Plug-in for Web Servers (Linux on System z et Linux on x86-64)	`PDWPI-PD-7.0.0-0`
Security Access Manager Policy Proxy Server	`PDMgrPrxy-PD-7.0.0-0`
Security Access Manager Policy Server	`PDMgr-PD-7.0.0-0`

Security Access Manager Runtime	`PDRTE-PD-7.0.0-0`
IBM Security Access Manager Runtime for Java	`PDJrte-PD-7.0.0-0`
Security Access Manager Session Management Command Line (Linux on System z uniquement)	`PDSMS-CLI-7.0.0-0`
Security Access Manager Session Management Server (Linux on System z uniquement)	`PDSMS-PD-7.0.0-0`
Security Access Manager Web Portal Manager	`PDWPM-PD-7.0.0-0`
Security Access Manager Web Security ADK (Linux on System z et Linux on x86-64 uniquement)	`PDWebADK-PD-7.0.0-0`
Security Access Manager Web Security Runtime (Linux on System z et Linux on x86-64 uniquement)	`PDWebRTE-PD-7.0.0-0`
Security Access Manager WebSEAL (Linux on System z et Linux on x86-64 uniquement)	`PDWeb-PD-7.0.0-0`
Security Utilities	`TivSecUtl-TivSec-7.0.0-0`

3. Lorsque vous avez terminé de supprimer les packages, redémarrez le système.

Résultats

Remarque : Certains packages répertoriés ne sont pas disponibles pour toutes les versions de Linux.

Suppression de DB2

Exécutez cette tâche pour supprimer DB2 d'un système Linux.

Procédure

1. Connectez-vous comme utilisateur avec des droits `root`.
2. Accédez au répertoire suivant :

   rép_install_db2`/install`

   où *rép_install_db2* est le répertoire dans lequel DB2 est installé.
3. Exécutez la commande suivante :

   ```
   ./db2_deinstall -a
   ```

Suppression de WebSphere Application Server, d'IBM HTTP Server ou du composant Plug-in for Web Servers

Pour supprimer WebSphere Application Server et le logiciel WebSphere associé tel qu'IBM HTTP Server ou le composant Plug-in for Web Servers d'un système Linux, voir les instructions du centre de documentation WebSphere Application Server.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Solaris : suppression de packages

Suppression des packages sur Solaris pour désinstaller Security Access Manager.

Avant de commencer

Avant de supprimer les packages, arrêtez toute instance de services et d'applications Security Access Manager en cours d'exécution.

Procédure

1. Assurez-vous que la configuration des composants a été annulée. Pour annuler la configuration des composants, suivez les instructions dans «Annulation de la configuration des composant Security Access Manager», à la page 429.
2. Pour supprimer un package, entrez la commande suivante : `pkgrm` *`packages`* où *packages* spécifie un ou plusieurs packages de composants suivants :

IBM Global Security Kit (GSKit)	`gsk8cry64` `gsk8ssl64`
IBM Tivoli Directory Server Web Administration Tool	`IDSlweb63`
Client IBM Tivoli Directory Server	`idsldap.cltbase63` `idsldap.clt64bit63` `idsldap.cltjava63`
IBM Tivoli Directory Server (packages serveur 64 bits et serveur proxy 64 bits)	`IDSl64s63` `IDSl64p63`
Messages en anglais d'IBM Tivoli Directory Server	`IDSlen63`
Security Access Manager Application Development Kit	`PDAuthADK`
Security Access Manager Attribute Retrieval Service	`PDWebARS`
Security Access Manager Authorization Server	`PDAcld`
Security Access Manager License	`PDlic`
Security Access Manager Plug-in for Apache Web Server	`PDWPIapa`
Security Access Manager Plug-in for IBM HTTP Server	`PDWPIihs`
Security Access Manager Plug-in for Web Servers	`PDWPI`
Security Access Manager Policy Proxy Server	`PDMgrPrxy`
Security Access Manager Policy Server	`PDMgr`
Security Access Manager Runtime	`PDRTE`
IBM Security Access Manager Runtime for Java	`PDJrte`
Security Access Manager Session Management Command Line	`PDSMSCLI`
Security Access Manager Session Management Server	`PDSMS`

Security Access Manager Web Portal Manager	`PDWPM`
Security Access Manager Web Security ADK	`PDWebADK`
Access Manager Web Security Runtime	`PDWebRTE`
Security Access Manager WebSEAL	`PDWeb`
Security Utilities	`TivSecUtl`

3. Lorsque vous êtes invité à confirmer la suppression de ces composants, entrez **y**. Une invite s'affiche et indique que le script de pré-suppression est en cours d'exécution. Chaque fichier est répertorié au fur et à mesure de la suppression.
4. Lorsque vous avez terminé de supprimer les packages, redémarrez le système.

Suppression de DB2

Utilisez cette tâche pour supprimer DB2 d'un système Solaris.

Procédure

1. Connectez-vous comme utilisateur avec des droits `root`.
2. Accédez au répertoire suivant :
   rép_install_db2`/install`

   où *rép_install_db2* est le répertoire dans lequel DB2 est installé.
3. Exécutez la commande suivante :
   `./db2_deinstall -a`

Suppression de WebSphere Application Server, d'IBM HTTP Server ou du composant Plug-in for Web Servers

Pour supprimer WebSphere Application Server et le logiciel WebSphere associé tel qu'IBM HTTP Server ou le composant Plug-in for Web Servers d'un système Solaris, voir les instructions du centre de documentation WebSphere Application Server.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Windows : suppression de packages

Suppression des packages sur Solaris pour désinstaller Security Access Manager.

Avant de commencer

Avant de supprimer les packages, arrêtez toute instance de services et d'applications Security Access Manager en cours d'exécution.

Procédure

1. Connectez-vous en tant qu'utilisateur disposant de droits d'administrateur Windows.
2. Sélectionnez **Démarrer → Panneau de configuration**, puis cliquez sur **Programmes et fonctionnalités**.
3. Sélectionnez l'un des composants installés et cliquez sur **Supprimer**. Vous pouvez choisir de désinstaller les packages Security Access Manager suivants :
   - IBM Tivoli Directory Server
   - DB2 Enterprise Server Edition

- Security Access Manager Application Developer Kit
- Security Access Manager Attribute Retrieval Service
- Security Access Manager Authorization Server
- Security Access Manager License
- Security Access Manager for Plug-in for Internet Information Services
- Security Access Manager Plug-in for Web Servers
- Security Access Manager Policy Proxy Server
- Security Access Manager Policy Server
- Security Access Manager Session Management Command Line
- Security Access Manager Session Management Server
- Security Access Manager Runtime
- IBM Security Access Manager Runtime for Java
- Security Access Manager Web Portal Manager
- Security Access Manager Web Security ADK
- Security Access Manager Web Security Runtime
- Security Access Manager WebSEAL
- Security Utilities
- GSKit8 SSL 64 bits

4. Sélectionnez un autre composant dans la liste ou cliquez sur **OK** pour quitter le programme.
5. Lorsque vous avez terminé, redémarrez le système.

Suppression de WebSphere Application Server, d'IBM HTTP Server ou du composant Plug-in for Web Servers

Pour supprimer WebSphere Application Server et le logiciel WebSphere associé tel qu'IBM HTTP Server ou le composant Plug-in for Web Servers d'un système Windows, voir les instructions du centre de documentation WebSphere Application Server.

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welcome_nd.html

Remarques

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, un programme ou un service IBM n'implique pas que seul ce produit, programme ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 Etats-Unis

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

Pour les demandes de licence concernant les informations sur le jeu de caractères codé sur deux octets (DBCS), contactez le Département de la propriété intellectuelle au sujet des licencesIBM de votre pays ou envoyez vos demandes, par courrier, à :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

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 VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS.

Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

© Copyright IBM Corp. 2001, 2013

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document 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.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. 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 Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 Etats-Unis

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 Livret Contractuel IBM, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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 tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

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.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la mise en service ou le fonctionnement de ces programmes. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation IBM.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des échantillons de programmes d'IBM Corp. © Copyright IBM Corp. _entrez l'année ou les années_. Tous droits réservés.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services 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.

Adobe, Acrobat, PostScript et tous les logos incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etat-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans d'autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Cell Broadband Engine et Cell/B.E. sont des marques de Sony Computer Entertainment, Inc., aux Etats-Unis et/ou dans certains autres pays et sont utilisées sous licence.



Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Index

A

accessibilité xx
Active Directory Lightweight Directory Service
  outil d'administration 89
activedir.conf 343
adaptateur de registre
  pour les référentiels fédérés WebSphere 427
ADK
  Voir aussi Web Security ADK
  composants d'installation 13
  configuration d'un système de développement 143
  désinstallation (AIX) 434
  désinstallation (Linux) 436
  désinstallation (Solaris) 438
  désinstallation (Windows) 439
  installation (AIX) 144
  installation (Linux) 145
  installation (Solaris) 146
  installation (Windows) 148
  installation à partir du tableau de bord 149
  installation automatique (AIX, Linux, Solaris) 151
  installation automatique (Windows) 152
  présentation 5
annulation de la configuration
  composants produit 429
Attribute Retrieval Service
  composants d'installation 15
  configuration 223
  désinstallation (AIX) 434
  désinstallation (Linux) 436
  désinstallation (Solaris) 438
  désinstallation (Windows) 439
  installation (AIX) 224
  installation (Linux) 225
  installation (Solaris) 226
  installation (Windows) 227
  nom du système hôte local 348
  options pdconfig 348
authentification de client
  configurer sur un client 330
  libellé de certificat 342
  utilisation dans la sécurité SSL 327
authentification native 79

B

base de données
  annulation de configuration (outil) 430
  annulation de configuration (présentation) 430
  unconfiguring (commande) 431
base de données de connexion
  création pour SMS 288

C

catalogue de messages
  internationalisation 370
  répertoires de langue 370
certificats
  création d'un objet d'autorité 101
  création pour le serveur LDAP 102
  cycle de vie 354
  extraction d'un certificat autosigné pour le serveur Novell eDirectory 102
certificats autosignés
  serveur Novell eDirectory 102
  Tivoli Directory Server 71
client LDAP
  configuration pour l'authentification client 330
  configuration pour SSL 327
  fichier de clés 360
client Tivoli Directory Server
  désinstallation (AIX) 434
  désinstallation (Linux) 436
  désinstallation (Solaris) 438
  installation (AIX) 44
  installation (Linux) 45
  installation (présentation) 43
  installation (Solaris) 46
  installation (Windows) 47
Client Tivoli Directory Server
  présentation 10
codage de texte 371
codage UTF-8 371
commande gskkyman 83
commande idsidrop 432
commande idsldapsearch 331
commande idsucfgdb 431
commande idsxcfg 430
commande idsxinst 432
commande ldapmodify 80
commande pdconfig 339
commande pkmspasswd 79
commandes
  environnement local 369
  gskkyman 83
  idsldapsearch 331
  ivrgy_tool.exe 98
  ldapmodify 80
  pdconfig 339
  pkmspasswd 79
commandes d'installation
  Attribute Retrieval Service 223
  présentation 19
  serveur d'autorisations 130
  serveur d'exécution 181
  serveur de gestion de session 284
  serveur de règles 112
  serveur proxy de règles 167
  système de développement 143
  système de développement de sécurité Web 82, 253
  système Runtime for Java 155
commandes d'installation *(suite)*
  système WebSEAL 265
  Web Portal Manager 195
composants d'installation
  Attribute Retrieval Service 15
  base 5
  commun 4
  conditions requises 13
  développement de sécurité Web (ADK) 15
  exigences de sécurité Web 15
  exigences des systèmes de gestion de sessions 16
  exigences pour les systèmes de base 13
  gestion de session 8
  IBM Tivoli Directory Server 13
  ligne de commande de gestion des sessions 16
  plug-in pour Apache Web Server 15
  plug-in pour IBM HTTP Server 15
  plug-in pour IIS 15
  prérequis 9
  présentation 13
  sécurité Web 7
  Security Access Manager Runtime 13
  serveur d'autorisations 13
  serveur de gestion de sessions 16
  serveur de règles 13
  serveur proxy de règles 13
  système de développement (ADK) 13
  WebSEAL 15
composants de base
  Application Development Kit 5
  exécution 6
  Licence 7
  présentation de la désinstallation 429
  Runtime for Java 6
  Security Utilities 6
  serveur d'autorisation 5
  serveur de règles 5
  serveur proxy de règles 5
  tâches 21
  Web Portal Manager 7
composants de sécurité Web
  installation 223
composants requis
  Access Manager Runtime 13
  Attribute Retrieval Service 15
  développement de sécurité Web (ADK) 15
  IBM Tivoli Directory Server 13
  ligne de commande de gestion des sessions 16
  plug-in pour Apache Web Server 15
  plug-in pour IBM HTTP Server 15
  plug-in pour IIS 15
  serveur d'autorisations 13
  serveur de gestion de sessions 16
  serveur de règles 13

© Copyright IBM Corp. 2001, 2013

composants requis *(suite)*
serveur proxy de règles 13
système de développement (ADK) 13
WebSEAL 15
composants Web Security
Plug-in for Web Servers 7
service d'extraction d'attribut 7
tâches 21
Web Security ADK 8
WebSEAL 8
configuration
Voir aussi installation à l'aide du tableau de bord
Attribute Retrieval Service 223
ligne de commande de gestion des sessions 312
sécurité de WebSphere Application Server 219
serveur d'autorisations 129
serveur d'exécution 181
serveur de gestion de session 284
serveur de règles 112
serveur proxy de règles 167
système de développement de sécurité Web 82
système Runtime for Java 155
système WebSEAL 265
configuration automatique
exécution 192
gestion des mots de passe 375
ligne de commande de gestion des sessions 322
plug-in Apache Server 248
plug-in d'IBM HTTP Server 248
plug-in IIS 250
Runtime for Java 165
serveur d'autorisations 141
serveur de gestion de sessions 307
serveur de règles 126
serveur proxy de règles 178
système WebSEAL 276
Web Portal Manager 217
configuration requise pour l'installation 282
configuration SSL
authentification de client 330
communication du client 328
configuration du serveur 327
pour Active Directory Lightweight Directory Service 84, 94
pour Tivoli Directory Server 71
pour Tivoli Directory Server for z/OS 81
sur le serveur Novell eDirectory 100
console
accès à SMS 291
déploiement de SMS 291
cycle de vie, certificats 354

D

DB2 xviii
assistant d'installation 60
désinstallation (AIX) 435
désinstallation (Linux) 437
désinstallation (Solaris) 439
DB2 *(suite)*
installation à partir du tableau de bord 69
délai d'expiration, connexion 354
délai d'expiration de la connexion 354
dépannage xx
désinstallation
composants (présentation) 429
packages AIX 434
packages Linux 436
packages Solaris 438
packages Windows 439
support de langue 372
Tivoli Directory Server 433
directives de langue 370
directives de langues 370
documentation GSKit xviii
domaine sécurisé
présentation 4
domaines
exécution 339
ID administrateur 349, 351
multiple, Active Directory 343
registres d'utilisateurs 339
serveur d'autorisations 349
serveur de règles 350
domaines de gestion
création 111
emplacement pour le registre Active Directory Lightweight Directory Service 112
options de configuration 339
présentation 4
serveur de règles 110
droits d'accès
serveur PowerHA de secours 393
serveur PowerHA principal 390

E

en ligne
publications xv
terminologie xv
exécution
composants d'installation 13
configuration de Security Access Manager Runtime 181
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 182
installation (Linux) 183
installation (Solaris) 185
installation (Windows) 187
installation à partir du tableau de bord 188
installation automatique (AIX, Linux, Solaris) 190
installation automatique (Windows) 191
installation sur SUSE Linux 184
options pdconfig (Active Directory) 343
options pdconfig (LDAP) 339
exigences de préinstallation
ligne de commande de gestion des sessions 311
serveur de règles de secours (TSAMP) 399
exigences préinstallation
plug-in pour les serveurs Web 229
préparation du système d'exploitation 28
serveur de gestion de sessions 282

F

Federal Information Processing Standard
Voir FIPS
fichier d'options 375
fichier de base de données de clés
création pour le serveur LDAP 83
Fichier de clés
pour Tivoli Directory Server 71
fichier de clés client 351
fichier journal
hacmp.log 395
haute disponibilité 395
fichier PDMdata.nsf 351
fichiers de configuration
activedir.conf 343
httpd.conf 196
serveurs Web sur AIX, Linux ou Solaris 351
slapd.conf 82
fichiers de schéma
mise à jour de Tivoli Directory Server for z/OS 78
FIPS
configuration de LDAP 339
paramètre d'Active Directory 343
présentation 17
formation xx

G

gestion de clés, GSKit xviii
gskcapicmd xviii
gskikm.jar xviii
GSKit
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 36
installation (Linux) 36
installation (présentation) 35
installation (Solaris) 37
installation (Windows) 37
présentation 9

H

HACMP
fichier hacmp.log 395
haute disponibilité
configuration du serveur de règles 394
fichiers journaux 395
gestion 394

haute disponibilité *(suite)*
serveur de règles de secours 394
haute disponibilité (TSAMP)
activation de l'automatisation de la reprise en ligne 411
configuration de l'équilibreur de charge 408
configuration de Tivoli System Automation for Multi-platforms 409
configuration du serveur d'exécution 408
exigences applicables au serveur d'exécution 400
exigences applicables au serveur de secours 399
installation de Tivoli System Automation for Multi-platforms 409
installation du serveur d'exécution 408
installation du serveur principal 401
script Poldown (serveur de secours) 418
script Poldown (serveur principal) 416
script Polmon (serveur de secours) 420
script Polmon (serveur principal) 419
script Polup (serveur de secours) 414
script Polup (serveur principal) 413
vérification des serveurs Access Manager 403
hôtes virtuels
serveurs Web (AIX, Linux ou Solaris) 351
serveurs Web (Windows) 353
HTTP
accès 360
port 360
httpd.conf 196
HTTPS
accès 360
port 360

I

IBM
assistant de support xx
service de support logiciel xx
IBM HTTP Server
Voir aussi plug-in pour IBM HTTP Server
désinstallation (AIX) 436
désinstallation (Linux) 437
désinstallation (Solaris) 439
désinstallation (Windows) 440
IBM Security Access Manager Runtime for Java
composants d'installation 13
configuration 155
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 156
installation (Linux) 157
IBM Security Access Manager Runtime for Java *(suite)*
installation (Solaris) 159
installation (Windows) 160
options pdconfig 350
type de configuration 350
IBM Tivoli Directory Server
Voir Tivoli Directory Server
ID administrateur
Active Directory 343
local 348
pour domaine de gestion
serveur d'autorisations 349
serveur de règles 354
serveur proxy de règles 355
Serveurs Web 351, 353
WebSEAL 360
WPM 356
requisSecurity Access Manager 333
ID groupe 333
ID utilisateur
obligatoire pour Security Access Manager 333
identification des problèmes xx
iKeyman xviii
installation à l'aide du tableau de bord
ADK 149
description 19
ligne de commande de gestion des sessions 318
plug-in pour Internet Information Services 245
Runtime for Java 161
serveur d'autorisations 136
serveur d'exécution 188
serveur de gestion de sessions 295
serveur de règles 121
serveur proxy de règles 174
Tivoli Directory Server 69
Web Portal Manager 206
Web Security ADK 260
WebSEAL 272
installation automatique
ligne de commande de gestion des sessions 320, 321
plug-in pour Apache Server 247
plug-in pour IBM HTTP Server 247
plug-in pour IIS 249
serveur d'autorisations 138, 139
serveur de gestion de sessions 305, 306
serveur de règles 124, 125
système d'exécution 190, 191
système de développement 151, 152
système de développement de sécurité Web 262, 263
système de serveur proxy de règles 176, 177
système Runtime for Java 163, 164
système Web Portal Manager 215, 216
système WebSEAL 274, 275
WebSphere Application Server for SMS 301, 303
WebSphere Application Server for WPM 211, 213
installation native
Voir commandes d'installation
instance de serveur d'annuaire
création 60, 69
suppression (commande) 432
suppression (outil) 432
suppression (présentation) 431
interface réseau logique 360
internationalisation
catalogues de messages 370
désinstallation du support de langue nationale 372
installation du support de langue 364
jeux de codes 371
langues prises en charge 363
support de langue nationale d'IBM Tivoli Directory Server 368
variable LANG 369
Variable LANG sur Windows 369
variables d'environnement local 368
variantes d'environnement local 370
ivrgy_tool.exe 98

J

Java Runtime
chemin d'accès 350
installation (AIX) 32
installation (Linux) 33
installation (présentation) 32
installation (Solaris) 34
installation (Windows) 34
options pdconfig 350
présentation 9
type de configuration 350
jeux de codes
emplacements de répertoire de fichiers 372
support de langue 371
journaux de trace et de message
emplacement du fichier journal commun 350

K

Kit GSK (Global Security Kit)
Voir GSKit

L

LDAP
options d'exécution pdconfig 339
remarques 52
LDAP_ADMINLIMIT_EXCEEDED 53
ldp.exe 89
libellé
Libellé de certificat client SSL 351
libellé de certificat
Active Directory SSL 343
WebSEAL SSL 360
libellé de certificat client
Active Directory 343
WebSEAL 360
licence
désinstallation (AIX) 434

licence *(suite)*
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX, Linux, Solaris) 38
installation (Windows) 40
présentation 7
présentation de l'installation 38
liens lointains
serveur PowerHA de secours 393
serveur PowerHA principal 390
ligne de commande de gestion de session
configuration 311
ligne de commande de gestion de sessions
présentation 9
ligne de commande de gestion des sessions
composants d'installation 16
configuration 312
configuration requise pour l'installation 311
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 312
installation (Linux) 314
installation (Solaris) 315
installation (Windows) 317
installation à partir du tableau de bord 318
installation automatique (AIX, Linux, Solaris) 320
installation automatique (Windows) 321
limite d'exploration 53

M

méthodes d'installation
composants Security Access Manager 19
produits prérequis 27
Microsoft Active Directory
chiffrement des connexions 343
configuration 84
domaines multiples 343
ID administrateur 343
mot de passe de l'administrateur 343
nom d'hôte du contrôleur de domaine 343
nom distinctif de l'emplacement des données 343
options d'exécution pdconfig 343
prise en charge du registre 12
remarques 54
utilisation du registre 343
Microsoft Active Directory Lightweight Directory Service
ajout d'un administrateur 91
autorisation de liaison anonyme 93
configuration 85, 86
configuration de l'emplacement 88
configuration de partition (autre que par défaut) 89
Microsoft Active Directory Lightweight Directory Service *(suite)*
configuration de partition (par défaut) 89
configuration SSL (exemple) 84, 94
emplacement de domaine de gestion de 112
installation de la prise en charge de 86
présentation 86
prise en charge du registre 12
remarques 53
mot de passe
Active Directory 343
gestion 375
masquage 376, 378
supprimer 379, 380
mot de passe de l'administrateur
Active Directory 343
local 348

N

NIST SP800-131 339, 343
nom d'hôte
Active Directory 343
Attribute Retrieval Service 348
Java Runtime 350
serveur d'autorisations 349
serveur de règles (LDAP) 339
serveur LDAP 339
serveur proxy de règles 355
WebSEAL 360
nom d'hôte du contrôleur de domaine 343
nom d'instance, WebSEAL 360
nom de noeud
Attribute Retrieval Service 348
nom distinctif
emplacement des données Active Directory 343
nom distinctif de l'emplacement des données 343
nom du système hôte local
Attribute Retrieval Service 348
serveur d'autorisations 349
serveur proxy de règles 355
noms d'environnements locaux
AIX, Linux, Solaris 369
Windows 369
numéros de port
nécessaire durant l'installation 337

O

ObjectGrid 282
objet d'autorité 101
objet d'autorité de certification 101
objet d'autorité de certification organisationnelle 101
options de configuration
Attribute Retrieval Service 348
JRE 350
pdconfig 339
Plug-in for Web Servers sous Windows 353
options de configuration *(suite)*
Plug-in for Web Servers sur AIX, Linux ou Solaris 351
Runtime for Java 350
Security Access Manager Runtime (Active Directory) 343
Security Access Manager Runtime (LDAP) 339
serveur d'autorisations 349
serveur de règles 354
serveur proxy de règles 355
Web Portal Manager 356
WebSEAL 360
options de sécurité 82
options pdconfig
Attribute Retrieval Service 348
Java Runtime 350
Plug-in for Web Servers sous Windows 353
Plug-in for Web Servers sur AIX, Linux ou Solaris 351
serveur d'autorisations 349
serveur de règles 354
serveur proxy de règles 355
Web Portal Manager 356
WebSEAL 360
Oracle Directory Server
Voir Sun Java System Directory Server
organigramme d'installation 21
outils 89
configuration de la base de données 430
GSKCapiCmd 9
idsxcfg 430
idsxinst 432
instance de base de données 432
ivrgy_tool 98
ldifde.exe 86
pdconf 375
réparation d'eDirectory 98
Tivoli Directory Server Administration 10

P

packages
désinstallation du support de langue nationale 372
support de langue 364
support de langue nationale d'IBM Tivoli Directory Server 368
suppression (présentation) 433
suppression AIX 434
suppression de DB2 435
suppression de WebSphere (AIX) 436
suppression de WebSphere (Linux) 437
suppression de WebSphere (Solaris) 439
suppression de WebSphere (Windows) 440
paramètre régional pour Windows 368
paramètres linguistiques 368
pdcacert.b64 113
planification
installation prérequise 27
méthodes d'installation 19

planification *(suite)*
organigramme 21
présentation 3
tâches 21
plug-in for IBM HTTP Server
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
installation (Linux) 239
installation (Solaris) 241
plug-in for Web Servers
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
exigences préinstallation 229
Plug-in for Web Servers
options pdconfig (AIX, Linux ou Solaris) 351
présentation 7
plug-in pour Apache Web Server
automatisation de l'installation 247
désinstallation (Linux) 436
désinstallation (Solaris) 438
installation (AIX) 230
installation (Linux) 234
installation (Linux x86-64) 232
installation (Solaris) 235
plug-in pour IBM HTTP Server
automatisation de l'installation 247
composants d'installation 15
installation (AIX) 237
plug-in pour Internet Information Services
automatisation de l'installation 249
composants d'installation 15
désinstallation 439
installation à partir du tableau de bord 245
installation via une ligne de commande 243
plug-in pour les serveurs Web
configuration 229
désinstallation (AIX) 436
désinstallation (Linux) 437
désinstallation (Solaris) 439
désinstallation (Windows) 440
installation pour Apache 230
installing pour IBM HTTP Server 237
plug-in pour serveurs Web
désinstallation (Windows) 439
options de pdconfig (Windows) 353
port
demande d'autorisation 349
HTTP 360
HTTPS 360
serveur d'autorisations 349
serveur d'exécution 350
serveur LDAP 339
serveur proxy de règles 355
port d'écoute
mises à jour de règles d'autorisation 351, 353
serveur de registre (Active Directory SSL) 343
serveur de registre (SSL LDAP) 339
serveur de règles (Active Directory) 343
port d'écoute *(suite)*
WebSEAL 360
port de requête d'administration
serveur d'autorisations 349
serveur proxy de règles 355
port de requête de proxy 355
port SSL
serveur de règles 339, 354
serveur LDAP 351
ports de requête
administration 349, 355
autorisation 349
proxy 355
PowerHA
configuration d'un serveur de règles de secours 381
création d'un lien allant des fichiers AIX vers le répertoire partagé 392
création d'un serveur de règles de secours 383
création de liens de fichiers et de répertoires 389
création de liens entre fichiers et répertoires de secours 392
création de liens entre fichiers et répertoires principaux 389
paramétrage des ID utilisateur 387
scénario d'environnement 382
vérification du serveur de secours 393
vérification du serveur primaire 390
préinstallation requise
plan 27
systèmes de base 13
systèmes de gestion de session 16
systèmes de sécurité Web 15
présentation
ADK 5
Client Tivoli Directory Server 10
domaine sécurisé 4
exécution 6
FIPS 17
GSKit 9
IBM Java Runtime 9
installation 3
langues prises en charge 363
Licence 7
ligne de commande de gestion de sessions 9
Plug-in for Web Servers 7
produits prérequis
IBM Java Runtime 9
Runtime for Java 6
Security Utilities 6
serveur d'autorisation 5
serveur de gestion de sessions 8
serveur de règles 5
serveur proxy de règles 5
service d'extraction d'attribut 7
Tivoli Directory Server 10
Web Administration Tool 10
Web Portal Manager 7
Web Security ADK 8
Web security runtime 8
WebSEAL 8
WebSphere Application Server 10
Présentation de GSKCapiCmd 9
présentation de l'installation 3
produits prérequis
Client Tivoli Directory Server 10
descriptions 9
GSKit 9
installation (présentation) 27
installation d'IBM Java Runtime 32
installation d'IBM Security Utilities 40
installation de GSKit 35
installation de la licence (AIX, Linux, Solaris) 38
installation de la licence (Windows) 40
installation de licence 38
installation du client Tivoli Directory Server 43
préparation des systèmes d'exploitation 28
tâches 21
Tivoli Directory Server 10
WebSphere Application Server 10
publications
accès en ligne xv
liste pour ce produit xv

R

registre d'utilisateurs
valeurs maximales 57
registres d'utilisateurs
Active Directory
configuration 84
paramètres 343
port d'écoute SSL 343
remarques 54
support 12
ADLDS
configuration 85
support 12
configuration 51
considérations relatives à ADLDS 53
différences 51
IBM z/OS
support 11
LDAP
différences 51
paramètres pdconfig 339
port d'écoute SSL 339
remarques 52
types de registres d'utilisateurs 51
longueur des noms d'utilisateur 57
Novell eDirectory
configuration 95
support 12
pris en charge 11
remarques 52
Sun Java System Directory
remarques 53
Sun Java System Directory Server
configuration 103
support 12
Tivoli Directory Server
configuration 60
configuration de SSL 71
support 11

registres d'utilisateurs *(suite)*
Tivoli Directory Server for z/OS configuration 78
URAF
différences 51
types 54
types de registres d'utilisateurs 51
utilisation dans un domaine de gestion 4
règle d'autorisation
numéro de port 351
numéro de port d'écoute 353
règle sur les mots de passe
LDAP 52
répertoire racine des documents Web 360
Runtime for Java
installation à partir du tableau de bord 161
installation automatique (AIX, Linux, Solaris) 163
installation automatique (Windows) 164
présentation 6

S

scénario d'environnement, PowerHA 382
scripts
Voir aussi scripts d'installation
création d'un lien allant des fichiers AIX vers le répertoire partagé 392
création de liens de fichiers et de répertoires 389
paramétrage des ID utilisateur 387
scripts d'installation
descriptions 19
environnement d'exécution du serveur proxy de règles 176
ligne de commande de gestion des sessions 320
plug-in du serveur Web 247
Runtime for Java 163
serveur d'autorisations 138
serveur d'exécution 190
serveur de gestion de session 300
serveur de règles 123
système de développement 150
système de développement de sécurité Web 262
système WebSEAL 274
Web Portal Manager 210
WebSphere Application Server for SMS 300
WebSphere Application Server for WPM 210
scripts de configuration
exécution 192
ligne de commande de gestion des sessions 322
plug-in Apache Server 248
plug-in d'IBM HTTP Server 248
plug-in IIS 250
Runtime for Java 165
serveur d'autorisations 141
serveur de gestion de sessions 307
scripts de configuration *(suite)*
serveur de règles 126
serveur proxy de règles 178
système WebSEAL 276
Web Portal Manager 217
Secure Sockets Layer
Voir SSL
Security Access Manager
installation du système de base 109
installation du système de sécurité Web 223
Security Utilities
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 40
installation (Linux) 41
installation (Solaris) 42
installation (Windows) 42
présentation 6
présentation de l'installation 40
serveur d'autorisation
présentation 5
serveur d'autorisations
automatisation de la configuration 141
composants d'installation 13
configuration 129
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 130
installation (Linux) 132
installation (Solaris) 133
installation (Windows) 135
installation à partir du tableau de bord 136
installation automatique (AIX, Linux, Solaris) 138
installation automatique (Windows) 139
nom du système hôte local 349
options pdconfig 349
serveur de gestion de sessions
composants d'installation 16
configuration 281
configuration (console) 294
configuration (présentation) 293
configuration (smcfg) 293
console 291
création de la base de données d'historique de connexion 288
déploiement de l'application (console) 292
déploiement de l'application (présentation) 292
déploiement de l'application (smscfg) 292
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
exigences préinstallation 282
extension de console 291
installation (AIX) 284
serveur de gestion de sessions *(suite)*
installation (Linux) 285
installation (Solaris) 286
installation (Windows) 288
installation à partir du tableau de bord 295
installation automatique (AIX, Linux, Solaris) 305
installation automatique (Windows) 306
présentation 8
serveur de règles
composants d'installation 13
configuration 109
configuration d'un serveur de secours 381
configuration de la haute disponibilité 394
création d'un serveur de secours 383
description 4
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
informations sur le domaine 350
installation (AIX) 113
installation (Linux) 115
installation (Solaris) 117
installation (Windows) 119
installation à partir du tableau de bord 121
installation automatique (AIX, Linux, Solaris) 124
installation automatique (Windows) 125
nom d'hôte 339, 349, 350, 355
nom d'hôte (Active Directory) 343
numéro de port 349, 350, 355
numéro de port SSL 339, 354
options pdconfig 354
port d'écoute (Active Directory) 343
présentation 5
redirection vers le serveur proxy 424
serveur de secours 394
tâches 21
serveur de règles de secours
configuration 381
création 383
serveur de règles de secours (TSAMP)
composants 397
configuration requise pour l'équilibreur de charge 399
exigences applicables au serveur principal 399
exigences de préinstallation 399
installation de LDAP et de l'équilibreur de charge 400
installation du serveur de secours 402
présentation 397
serveur LDAP
fichier de clés client SSL 351
format de données minimal 110
format de données standard 110
nom d'hôte 339
numéro de port 339
numéro de port SSL 351

serveur LDAP *(suite)*
options de configuration 339
sélection du format de données 110
serveur LDAP sur z/OS xviii
serveur Novell eDirectory
configuration 95
configuration SSL 100
création d'objet d'autorité de certification organisationnelle 101
documentation 95
emplacement du domaine 99
extraction d'un certificat autosigné 102
prise en charge du registre 12
utilisation des classes d'objets 98
serveur PowerHA de secours 387, 392, 393
serveur PowerHA principal 387, 389, 390
serveur proxy de règles
composants d'installation 13
configuration 167
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 168
installation (Linux) 170
installation (Solaris) 171
installation (Windows) 173
installation à partir du tableau de bord 174
installation automatique (AIX, Linux, Solaris) 176
installation automatique (Windows) 177
nom du système hôte local 355
options pdconfig 355
présentation 5
serveurs proxy
ajout de suffixe 422
annulation de la configuration 425
configuration 421
configuration pour l'utilisation 423
définition des contrôles d'accès 425
redirection à partir du serveur de règles 424
Serveurs Web
automatisation de l'installation (Apache) 247
chemin d'accès 351
composants d'installation Apache 15
désinstallation sous AIX 434
options de pdconfig (Windows) 353
options pdconfig 351
options pdconfig (AIX, Linux ou Solaris) 351
service d'extraction d'attribut
présentation 7
slapd.conf 82
SSL
activation avec GSKit 35
activation pour les serveurs Web 351
activation pour Novell 103
configuration du client 327
cycle de vie du certificat 354
SSL *(suite)*
délai d'expiration de la connexion 354
fichier de clés du client LDAP 351
libellé de certificat 343
libellé de certificat client 351, 360
pour Tivoli Directory Server for z/OS 81
serveur de règles 339
test d'accès 329
test de l'accès sur le serveur LDAP 331
ssl-compliance 339, 343
suffixes
ajout à Sun Java System Directory Server 103
ajout à Tivoli Directory Server 61, 65, 67
ajout à Tivoli Directory Server for z/OS 78
ajout pour serveur proxy 422
considérations de Microsoft Active Directory 54
dans plusieurs domaines 59
valeur par défaut de Tivoli Directory Server 60, 70
Suite B 339, 343
Sun Java System Directory Server
configuration 103
LDAP_ADMINLIMIT_EXCEEDED 53
limite d'exploration 53
prise en charge du registre 12
remarques 53
support de langue
catalogues de messages 370
désinstallation 372
IBM Tivoli Directory Server 368
jeux de codes 371
modules d'installation 364
nom du paramètre régional sous AIX, Linux, Solaris 369
noms d'environnements locaux de Windows 369
présentation 363
présentation de l'installation 363
service commun de contrôle et de rapport 364
variables d'environnement local 368
variantes d'environnement local, implémentation 370
support de langues
désinstallation 372
installation 364
installation sur IBM Tivoli Directory Server 368
système d'exploitation
préparation d'AIX 29
préparation de l'installation 28
préparation de Linux 30
préparation de Solaris 31
préparation de Windows 31
système de gestion de session
présentation 8
tâches 21

T

terminologie xv
Tivoli Common Directory
activation 339, 343
journaux de trace et de message 350
nom de répertoire 350
répertoire d'installation 343
Tivoli Directory Integrator xviii
Connector for Security Access Manager 21
Tivoli Directory Server
annulation de la configuration 430
automatisation de l'installation 63
composants d'installation 13
configuration SSL 71
création du fichier de la base de données de clés 327
désinstallation 433
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation 60
Installation à l'aide du fichier script 63
installation à partir du tableau de bord 69
présentation 10
présentation de l'installation 59
prise en charge du registre 11
programmes de support de langue nationale (un obligatoire) 368
publication associée xviii
Tivoli Directory Server for z/OS
ajout de suffixes 78
authentification native 79
configuration 78, 79
configuration SSL 81
création du fichier de la base de données de clés 83
documentation 81
mise à jour des fichiers de schéma 78
prise en charge du registre 11

U

Unicode 371
URAF
remarques 54
utilitaire iKeyman
configuration de la variable d'environnement 34
emplacement 35

V

variable d'environnement LANG
AIX, Linux, Solaris 369
Variable d'environnement LANG
description 368
Windows 369
variable d'environnement NLSPATH 370
variable EXTSHM
configuration pour plug-in (HTTP Server) 237

variable EXTSHM *(suite)*
paramètre de plug-in (Apache) 230
variables
LANG avec AIX, Linux, Solaris 369
LANG avec Windows 369
NLSPATH 370
variables d'environnement
environnement local 368
variables d'environnement local 368
variantes, environnements locaux de langue 370
variantes d'environnement local 370

W

Web Administration Tool
présentation 10
Web Portal Manager
composants d'installation 13
configuration 195
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 196
installation (Linux) 199
installation (Solaris) 201
installation (Windows) 204
installation à partir du tableau de bord 206
installation automatique (AIX, Linux, Solaris) 215
installation automatique (Windows) 216
options pdconfig 356
présentation 7
Web Security ADK
composants d'installation 15
configuration d'un système de développement 253
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 254
installation (Linux) 255
installation (Solaris) 257
installation (Windows) 258
installation à partir du tableau de bord 260
présentation 8
Web Security Runtime
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
présentation 8
WebSEAL
composants d'installation 15
configuration 265
désinstallation (AIX) 434
désinstallation (Linux) 436
désinstallation (Solaris) 438
désinstallation (Windows) 439
installation (AIX) 266
installation (Linux) 267
installation (Solaris) 269
WebSEAL *(suite)*
installation (Windows) 271
installation à partir du tableau de bord 272
installation automatique (AIX, Linux, Solaris) 274
installation automatique (Windows) 275
nom d'hôte 360
nom d'instance 360
options pdconfig 360
port d'écoute 360
présentation 8
WebSphere Application Server
automatisation de l'installation pour SMS (AIX, Linux, Solaris) 301
automatisation de l'installation pour SMS (Windows) 303
configuration de la sécurité 219
désinstallation sous AIX 436
désinstallation sous Linux 437
désinstallation sous Solaris 439
désinstallation sous Windows 440
installation 47
installation automatique (AIX, Linux, Solaris) 211
installation automatique (Windows) 213
présentation 10
WebSphere Application Server Network Deployment xviii
WebSphere eXtreme Scale xviii



GC11-6786-02

