Dell Data Protection

Guide de configuration

2014-02

Sommaire

1 Configuration de Compatibility Server 5

server_config.xml **5**

gkresource.xml **11**

Activation du format Domaine\Nom d'utilisateur 12

run-service.conf **12**

2 Configuration de Core Server 13

Remplacement de l'arbitrage des règles le plus sécurisé par l'arbitrage des règles le moins sécurisé . . **13**

PolicyService.config. 13

Désactiver des Services Web **13**

Activation des notifications de licence par e-mail sur le serveur SMTP. **14**

NotificationObjects.config 14

Notification.config. 14

Ajouter l'emplacement du dossier Compatibility Server au fichier de configuration du Core Server **15**

Donner la permission au Core Server d'effectuer une itération via des méthodes d'authentification. . . . **15**

3 Configuration de Device Server. 17

eserver.properties **17**

run-service.conf **18**

4 Configuration de Security Server 19

context.properties **19**

5 Configuration des fonctionnalités de cryptage 21

Empêcher la suppression des fichiers temporaires. **21**

Masquer des icônes en transparence **21**

Masquer une icône de barre d'état système. **21**

Activation par plages horaires. **21**

Interrogation forcée 23

Options d'inventaire 23

Activations hors domaine 23

6 Configuration des composants pour l'authentification/autorisation Kerberos 25

Configuration des composants pour l'authentification/autorisation Kerberos 25

Instructions pour les services Windows 25

Instructions pour le fichier de configuration Key Server 25

Exemple de fichier de configuration : 26

Instructions pour les services Windows 26

Instructions pour la Console de gestion à distance 27

7 Attribuer le rôle d'administrateur Forensic 29

Instructions pour la Console de gestion à distance 29

Désactiver l'autorisation Forensic 29

8 Expressions Cron 31

Présentation des expressions Cron 31

Syntaxe des expressions Cron 31

Caractères spéciaux 31

Exemples 33

9 Créer un certificat auto-signé avec Keytool et générer une demande de signature de certificat (CSR) 35

Générer une nouvelle paire de clés et un certificat auto-signé 35

Demander un certificat signé par une autorité de certification 36

Importer un certificat racine 37

Exemple de méthode pour demander un certificat 37

1

Configuration de Compatibility Server

Ce chapitre décrit les paramètres que vous pouvez modifier afin d'adapter Compatibility Server à votre environnement. Faites toujours une copie de sauvegarde des fichiers de configuration avant de les modifier.

Ne modifiez que les paramètres documentés dans ce fichier. Vous risquez de corrompre ou d'endommager le système si vous modifiez les autres données contenues dans ces fichiers, notamment les balises. Dell n'est pas en mesure de garantir que les problèmes résultant de l'apport de modifications non autorisées à ces fichiers pourront être résolus sans procéder à une réinstallation de Compatibility Server.

server_config.xml

Vous pouvez modifier certains des paramètres décrits ci-après dans **<répertoire d'installation du Compatibility Server>\conf\server_config.xml**. Les paramètres qui ne doivent pas être modifiés sont identifiés comme tel. Si Compatibility Server est en cours d'exécution, vous devez arrêter ce service avant de modifier le fichier server_config.xml. Redémarrez ensuite le service Compatibility Server pour permettre aux modifications apportées à ce fichier de prendre effet.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
secrets.location	$dell.home$/conf/secretKeyStore	Emplacement par défaut du fichier secretkeystore. Mettez à jour ce paramètre si vous modifiez l'emplacement par défaut de ce fichier.
archive.location	$dell.home$/conf/archive	Emplacement par défaut de l'archive. Mettez à jour ce paramètre si vous modifiez l'emplacement par défaut de ce fichier.
domain.qualified.authentication	vrai	Indique si le nom de connexion complet d'un utilisateur est requis pour toutes les requêtes envoyées au serveur. Si vous modifiez cette valeur, vous devez redémarrer Device Server pour permettre à la nouvelle valeur de prendre effet.
directory.max.search.size	1000	Limite d'une *recherche* de répertoire au-delà de laquelle une exception est levée.
directory.server.search.timeout.seconds	60	Délai d'expiration (en secondes) du serveur pour les recherches LDAP.
directory.client.search.timeout	60	Délai d'expiration (en secondes) du client pour les recherches LDAP.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
rmi.recovery.host		Pour utiliser la fonction de récupération EMS multi-serveur : <!-- - supprimez le commentaire et modifiez les noms d'hôtes en ajoutant les noms complets de vos domaines pour activer la récupération <property name="rmi.recovery.host"> <value>rmi://foo.fabrikam.com:1099</value> </property> <property name="rmi.recovery.host"> <value>rmi://foo.fabrikam2.com:1099</value> </property> -->
default.gatekeeper.group.remote	CMGREMOTE	Nom par défaut du groupe auquel appartiennent par défaut toutes les Proxy règles. Vous pouvez modifier ce nom ici ou dans le fichier context.properties de Device Server. Si vous modifiez le nom du groupe ici, vous devez également le modifier dans Device Server si vous prévoyez : • de protéger des périphériques Windows ; • d'utiliser CREDActivate. Nous vous recommandons de regrouper toutes vos Proxy règles dans un seul groupe.
rsa.securid.enabled	faux	Si vous utilisez RSA SecurID pour Microsoft Windows version 6 comme remplacement de votre GINA, définissez ce paramètre sur vrai, puis arrêtez et redémarrez le service Compatibility Server. Lorsque les utilisateurs de Shield activent un environnement RSA de remplacement de GINA, l'authentification LDAP est alors remplacée par une authentification RSA.
inv.queue.task.worker.size	10	Nombre de threads utilisés pour traiter la file d'attente de l'inventaire.
inv.queue.task.timeout.seconds	900	Nombre de secondes avant le délai d'expiration.
inv.queue.task.retry.count	3	Nombre de tentatives de traitement de l'inventaire exécutées par le serveur avant abandon.
report.retry.max	120	Nombre maximal de nouvelles tentatives.
report.retry.wait.millis	250	Délai d'attente en millièmes de secondes avant toute nouvelle tentative.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
triage.execute.time	0 0 0/6 * *	Le triage est un processus qui consiste à rapprocher les utilisateurs et les groupes que le serveur connaît déjà. Le paramètre par défaut est « 0 0 0/6 * * ? », ce qui signifie que le triage est effectué toutes les 6 heures à partir de minuit (minuit, 6h00, midi, 18h00, minuit...)
gatekeeper.service.max.sessions	5	Nombre maximal de sessions Proxy règles.
gatekeeper.service.max.session.timeout	5	Délai d'expiration pour le nombre maximal de sessions Proxy règles.
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	Rôle requis pour mettre à jour des rôles d'administrateur de groupe ou d'utilisateur.
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	Rôle requis pour mettre à jour des rôles d'administrateur de groupe ou d'utilisateur.
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin, LogAdmin	Rôles requis pour récupérer les sessions de rapport.
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin, LogAdmin	Rôles requis pour récupérer les rapports.
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin, LogAdmin	Rôles requis pour récupérer la liste des colonnes du rapport.
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin, LogAdmin	Rôles requis pour récupérer la liste des catégories du rapport.
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin, LogAdmin	Rôles requis pour récupérer la liste des priorités du rapport.
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin, SecAdmin, HelpDeskAdmin, SystemAdmin	Rôles requis pour récupérer les noms associés aux ID uniques.
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	Rôle requis pour récupérer la liste des administrateurs du système.
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	Rôle requis pour définir le mot de passe superadmin.
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	Rôle requis pour réinitialiser le mot de passe superadmin.
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin, SecAdmin	Rôles requis pour ajouter des domaines.
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin, SecAdmin	Rôles requis pour supprimer des domaines.
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin, SecAdmin	Rôles requis pour mettre à jour des domaines.
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin, SecAdmin	Rôles requis pour ajouter des groupes.
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin, SecAdmin	Rôles requis pour supprimer des groupes.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin, SecAdmin	Rôles requis pour rechercher des groupes LDAP.
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin, SecAdmin	Rôles requis pour rechercher des utilisateurs LDAP.
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin, SecAdmin	Rôles requis pour ajouter des utilisateurs.
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	Rôle requis pour ajouter des licences d'entreprise.
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	Rôle requis pour afficher la licence d'entreprise.
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin, SecAdmin	Rôles requis pour récupérer un périphérique.
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin, SecAdmin	Rôles requis pour suspendre des utilisateurs.
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	Rôle requis pour activer des périphériques par proxy.
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin, SecAdmin	Rôles requis pour récupérer manuellement un périphérique par proxy.
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Rôle requis pour récupérer le fichier de ressources Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Rôle requis pour approuver le fichier de ressources Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Rôle requis pour approuver la configuration de Gatekeeper.
policy.arbiter.security.mode	most-restrictive	Cette propriété contrôle le fonctionnement de l'algorithme de mappage de règle pour les éléments de règle auxquels une préférence de sécurité est appliquée lorsque la règle possède plusieurs nœuds parents. Valeurs : Least-restrictive – La valeur d'élément la moins restrictive des parents est utilisée. Most-restrictive – La valeur d'élément la plus restrictive de tous les parents est utilisée.
policy.set.synchronization.sync-unmodified	vrai	Cet indicateur signale que la prochaine synchronisation externe doit ajouter ou remapper tous les éléments de règle sans définir l'indicateur modifié sur vrai. Cet indicateur bascule sur faux après chaque synchronisation. Il doit donc être réinitialisé si l'administrateur de sécurité souhaite ajouter des éléments sans apporter de modification. Il s'agit d'une option avancée.
db.schema.version.major		Schéma de la base de données principale.
db.schema.version.minor		Schéma de la base de données secondaire.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
db.schema.version.patch		Version du correctif du schéma de la base de données.
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	Emplacement par défaut du pilote de base de données. Mettez à jour ce paramètre si vous modifiez l'emplacement par défaut de ce fichier.
dao.db.host		Nom d'hôte de votre serveur de base de données. Ce paramètre peut être modifié dans l'outil de configuration.
dao.db.name		Nom de votre base de données. Ce paramètre peut être modifié dans l'outil de configuration.
dao.db.user		Nom d'utilisateur possédant les autorisations maximales pour votre base de données. Ce paramètre peut être modifié dans l'outil de configuration.
dao.db.password		Mot de passe associé au nom d'utilisateur possédant les autorisations maximales pour votre base de données. Ce paramètre peut être modifié dans l'outil de configuration.
dao.db.max.retry.count	10	Nombre maximal de tentatives de reconnexion à SQL Server exécutées par Compatibility Server lorsqu'une erreur de socket spécifiée se produit.
dao.db.connection.retry.wait.seconds	5	La première tentative de reconnexion est immédiate. La deuxième tentative est exécutée dès que le délai (en secondes) indiqué est écoulé. La troisième tentative est exécutée lorsque le double du délai indiqué est écoulé, la quatrième est exécutée lorsque le triple du délai indiqué est écoulé, et ainsi de suite.
dao.connection.pool.max.uses	10000	Permet d'interrompre les connexions. 0 signifie que les connexions ne sont pas interrompues.
dao.connection.pool.inactive.threshold.seconds	900	Utilisé pour déterminer si une connexion n'est pas utilisée et peut donc être fermée.
dao.db.driver.socket.errors	0	Compatibility Server tente de se reconnecter à SQL Server lorsque des erreurs correspondant aux codes répertoriés dans cette liste de valeurs séparées par des virgules se produisent. 0 correspond au code d'erreur pour les erreurs de socket rencontrées par Microsoft SQL. Vous pouvez également ajouter 17142 pour les erreurs de pause du serveur et 6002 pour les erreurs d'arrêt du serveur.
dao.db.mssql.compatability.level	90	Valeur pour SQL version 2005 ou ultérieure.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	Gestionnaire du fichier d'autorisation.
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	Gestionnaire du fichier d'inventaire.
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	Gestionnaire du fichier d'événements.
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Mettez à jour ce paramètre si vous modifiez l'emplacement par défaut du fichier de ressources Gatekeeper.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Mettez à jour ce paramètre si vous modifiez l'emplacement par défaut du fichier de ressources Gatekeeper.
rmi.server.registry.host	localhost	La propriété hôte est uniquement utilisée pour les programmes clients afin de déterminer l'emplacement du registre. Elle n'est pas utilisée lors de la création du registre RMI et des objets distants. Elle sera créée dans localhost.
rmi.server.registry.port	1099	La configuration du port du registre RMI peut être effectuée au moment de l'installation. Il est également possible de modifier le port une fois l'installation terminée à l'aide de ce paramètre. Si vous modifiez cette valeur, vous devez également configurer Gatekeeper Web Services.
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour définir l'autorisation pour les rapports du serveur.
security.authorization.method.IReportingService.removeEntity	SystemAdmin	Rôle requis pour supprimer les entités du serveur.
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	Rôle requis pour définir la visibilité des entités du serveur.
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher la page de détails du périphérique.
security.authorization.method.IReportingService.openSession	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour ouvrir une session sur le serveur.
security.authorization.method.IReportingService.getPagedReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport paginé.
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur les types de périphériques.
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur le système d'exploitation.
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher les rapports sur les modèles de périphériques.
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur les détails des règles.

server_config.xml		
Paramètre	**Valeur par défaut**	**Description**
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur les détails des postes de travail.
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport d'échec du cryptage.
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport de résumé du cryptage.
security.authorization.method.IReportingService.getUserDetail	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur les détails des utilisateurs.
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur les détails des groupes.
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin, HelpDeskAdmin, SystemAdmin, SecAdmin	Rôles requis pour afficher le rapport sur la liste des domaines.
security.authorization.method.IKeyService.getKeys	ForensicAdmin	Ce paramètre est utilisé avec un module d'extension d'intégration forensic. Veuillez contacter le support Dell pour savoir si un outil d'intégration forensic est nécessaire.
accountType.nonActiveDirectory.enabled	faux	L'autorisation des activations hors domaine est une configuration avancée qui a d'importantes répercussions. *AVANT* d'activer cette configuration, contactez le service clientèle pour aborder vos besoins spécifiques en termes d'environnement. Redémarrez le service Compatibility Server après avoir modifié cette valeur. En plus de ce paramètre, créez ou modifiez le paramètre de répertoire sur l'ordinateur Windows comme suit : HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations=REG_DWORD:1

gkresource.xml

Vous pouvez modifier les paramètres dans <rép. d'installation de Compatibility Server>\conf\gkresource.xml.

Nous vous recommandons d'insérer des commentaires au début du fichier pour effectuer le suivi des modifications que vous apportez. Vous pourrez ainsi facilement transférer vos modifications vers le nouveau fichier lorsque vous effectuerez une mise à niveau.

REMARQUE : Le fichier gkresource.xml doit être un fichier XML bien formé. Si vous ne maîtrisez pas le format XML, Dell vous recommande de ne pas essayer de modifier ce fichier. Le cas échéant, veillez à utiliser les références des entités plutôt que des caractères spéciaux bruts (sans programmation spéciale).

Pour pouvoir prendre effet, les modifications apportées au fichier de ressources Gatekeeper doivent être approuvées par un administrateur système.

Activation du format Domaine\Nom d'utilisateur

Insérez la chaîne de caractères suivante pour activer (ou désactiver) le format domaine\nom d'utilisateur. Ce format est désactivé si la chaîne de caractères n'existe pas dans le fichier. Vous pouvez également désactiver ce format en définissant la valeur sur 0.

1. Naviguez jusqu'à <rép. d'installation de Compatibility Server>\conf.
2. Ouvrez le fichier gkresource.xml à l'aide d'un éditeur XML.
3. Insérez la chaîne de caractères :
   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. Enregistrez le fichier, puis fermez-le.

run-service.conf

Vous pouvez modifier certains des paramètres décrits ci-après dans **<répertoire d'installation du Compatibility Server>\conf\run-service.conf**. Ces paramètres sont configurés automatiquement au moment de l'installation. Pour personnaliser les paramètres ou modifier la configuration de n'importe quel service :

1. Arrêtez le service.
2. Supprimez le service.
3. Modifiez puis enregistrez le fichier **run-service.conf**. Nous vous recommandons d'insérer des commentaires au début du fichier pour effectuer le suivi des modifications que vous apportez.
4. Réinstallez le service.
5. Démarrez le service.

run-service.conf		
Paramètre	**Valeur par défaut**	**Description**
JAVA_HOME	Dell\Java Runtime\jreX.x	Emplacement du répertoire d'installation de Java.
wrapper.java.additional.5	Sans objet	L'adresse Mac indiquée dans cette ligne correspond à l'adresse Mac de la carte Ethernet locale. Si un serveur possède plusieurs cartes réseau ou si vous souhaitez effectuer une liaison vers une autre carte que la carte principale, saisissez ici l'adresse physique (Mac) de la carte réseau en supprimant les tirets.
wrapper.ntservice.name	EpmCompatSvr	Nom du service.
wrapper.ntservice.displayname	Dell Compatibility Server	Nom d'affichage du service.
wrapper.ntservice.description	Enterprise Compatibility Server	Description du service.
wrapper.ntservice.dependency.1		Dépendances du service. Ajoutez les dépendances nécessaires en commençant par 1.
wrapper.ntservice.starttype	AUTO_START	Mode dans lequel le service est installé : AUTO_START ou DEMAND_START.
wrapper.ntservice.interactive	faux	Lorsque ce paramètre est configuré sur vrai, le service est autorisé à interagir avec le bureau.

2

Configuration de Core Server

Ce chapitre décrit les paramètres que vous pouvez modifier afin d'adapter Core Server à votre environnement.

Ne modifiez que les paramètres documentés dans ce fichier. Vous risquez de corrompre ou d'endommager le système si vous modifiez les autres données contenues dans ces fichiers, notamment les balises. Dell n'est pas en mesure de garantir que les problèmes résultant de l'apport de modifications non autorisées à ces fichiers pourront être résolus sans procéder à une réinstallation du Core Server.

Remplacement de l'arbitrage des règles le plus sécurisé par l'arbitrage des règles le moins sécurisé

PolicyService.config

Modifiez ce paramètre pour remplacer l'arbitrage des règles le plus sécurisé par l'arbitrage des règles le moins sécurisé. Modifiez le paramètre dans **<répertoire d'installation du Core Server>\PolicyService.config**. Si le Core Server est en cours de fonctionnement, vous devez arrêter le Service, modifier le fichier PolicyService.config, puis redémarrer le Service pour que les modifications à ce fichier prennent effet.

Nous vous recommandons d'insérer des commentaires au début du fichier pour effectuer le suivi des modifications que vous apportez. Vous pourrez ainsi facilement transférer vos modifications vers le nouveau fichier PolicyServiceConfig.xml lorsque vous effectuerez une mise à niveau.

Modifiez la section suivante :

```
<!-- Web Service Targets -->
<object id="PolicyService" singleton="false" type="Credant.Policy.Service.PolicyService,
Credant.Policy.ServiceImplementation">
    <property name="TemplateDataAccess" ref="TemplateDataAccess"/>
    <property name="PolicyDataAccess" ref="PolicyDataAccess"/>
    <property name="SupportDataAccess" ref="SupportDataAccess"/>
    <property name="AuditLog" ref="ServiceAuditLog"/>
    <property name="GlobalArbitrationBias" value="1" /> [remplacez la valeur « 0 » par la valeur « 1 » pour définir la valeur sur le paramètre le moins sécurisé]
</object>
```

Désactiver des Services Web

REMARQUE : Il s'agit d'un paramètre avancé qui doit impérativement être modifié conformément aux consignes du service clientèle.

Pour désactiver des services web sur le Core Server (par exemple, si une seconde installation Core Server est chargée exclusivement du traitement de l'inventaire), modifiez les paramètres dans :

<répertoire d'installation du Core Server>

Credant.Server2.WindowsService.exe.Config

et

<répertoire d'installation du Core Server>\Spring.config

Si le Core Server est en cours de fonctionnement, vous devez arrêter le Service, modifier les paramètres dans ces deux fichiers, puis redémarrer le Service afin que les changements prennent effet.

Credant.Server2.WindowsService.exe.Config

Supprimez la section suivante :

```
<!-- Web Services Configuration -->
<system.serviceModel>
    <services configSource="Services.config"/>
    <behaviors configSource="Behaviors.config"/>
    <bindings configSource="Bindings.config"/>
</system.serviceModel>
```

Spring.config

Supprimez les éléments suivants :

Supprimez toutes les définitions <object> </object> sous les en-têtes **AOP Advice**, **Web Service Target Definition**, et **Web Service Host Definition**.

Activation des notifications de licence par e-mail sur le serveur SMTP

Si vous utilisez Dell Data Protection | Cloud Edition, ces paramètres sont automatisés en utilisant l'Outil de configuration serveur. Utilisez cette procédure si vous devez activer le Serveur SMTP pour les notifications de licence par e-mail à d'autres fins que Dell Data Protection | Cloud Edition.

NotificationObjects.config

Pour configurer les notifications de licence par e-mail sur votre serveur SMTP, modifiez le fichier **NotificationObjects.config** qui se trouve à l'emplacement suivant : **<rép. d'installation de Core Server>**.

Effectuez les modifications suivantes :

```
<object name="EmailNotification" singleton="false" type="Credant.Notification.EmailNotification,
Credant.Notification"> [Ne modifiez pas cette valeur]
  <property name="NotificationDataFactory" ref="NotificationDataFactory"/> [Ne modifiez pas cette valeur]
  <property name="Host" value="test.dell.com"/>
  <property name="Port" value="25"/>
  <property name="Username" value="username"/>
  <property name="Password" value="${SmtpPassword}"/> [Ne modifiez pas cette valeur]
  <property name="Logger" ref="NotificationLogger"/> [Ne modifiez pas cette valeur]
</object>
```

Notification.config

Si votre serveur e-mail requiert une authentification, modifiez le fichier **Notification.config** qui se trouve à l'emplacement suivant : **<rép. d'installation de Core Server>**.

Effectuez les modifications suivantes :

```
<notification>
    <add key="SmtpPassword" value="your_email_server_password"/>
</notification>
```

Ajouter l'emplacement du dossier Compatibility Server au fichier de configuration du Core Server

Le Core Server est une application .Net, ce qui signifie que l'accès aux informations du répertoire peut parfois être interdit, en raison des autorisations. Cependant, pour lire le secretkeystore (la clé de cryptage de base), le Core Server doit accéder aux informations de configuration du répertoire du Compatibility Server pour l'emplacement du secretkeystore. Si les autorisations de répertoire bloquent cet accès, le Core Server ne parvient pas à authentifier les utilisateurs de la Console. Ce paramètre ajoute l'emplacement du dossier du Compatibility Server dans le fichier de configuration du Core Server en cas de problèmes d'accès au répertoire.

1. Rendez-vous sur <répertoire d'installation du Core Server>\EntityDataAccessObjects.config.
2. Changez l'élément en gras :

   <object id="DomainDataAccess" singleton="false" type="Credant.Entity.DataAccess.DomainDataAccess, Credant.Entity.DataAccess">

   <property name="Logger" ref="DataAccessLogger"/>

   <!--<property name="CompatibilityServerPath" value="PATH_TO_COMPATIBILITY_SERVER"/> --> *Supprimez le commentaire de cette ligne et définissez le chemin d'accès complet du Compatibility Server.*

   </object>
3. Enregistrez le fichier, puis fermez-le.
4. Redémarrez les Services Core Server et Compatibility Server.

Donner la permission au Core Server d'effectuer une itération via des méthodes d'authentification

Les tentatives d'authentification Core Server peuvent être bloquées par le contrôleur de domaine, dans le cadre des règles définies quant aux méthodes d'authentification autorisées. L'amélioration a consisté à mettre en œuvre un « commutateur » dans le fichier de configuration Core Server afin de permettre à celui-ci d'effectuer une itération via diverses méthodes d'authentification, dans le but d'en identifier une qui fonctionne.

1. Rendez-vous sur <répertoire d'installation du Core Server >\Spring.config.
2. Changez l'élément en gras :

   <object id="DomainCache" singleton="true" type="Credant.Authorization.DomainCache.DomainCache, Credant.Authorization.DomainCache">

   <!-- Change this logger? -->

   <property name="Logger" ref="DataAccessLogger" />

   <property name="DomainDataAccess" ref="DomainDataAccess" />

   <property name="RefreshFrequency" value="300" />

   <property name="TryAllAuthTypes" value="false" /> *Changez cette valeur en « true » pour activer cette fonctionnalité.*

   <!-- Utilisé pour modifier AuthType par domaine : la clé est le CID du domaine et la valeur est System.DirectoryServices.AuthenticationTypes

   <property name="DomainAuthType">

   <dictionary key-type="string" value-type="int" >

   <entry key="5A23TPM2" value="0" />

   </dictionary>

   </property>

   -->

   </object>
3. Enregistrez le fichier, puis fermez-le.
4. Redémarrez le service Core Server.

3

Configuration de Device Server

Ce chapitre décrit les paramètres que vous pouvez modifier afin d'adapter Device Server à votre environnement.

Ne modifiez que les paramètres documentés dans ce fichier. Vous risquez de corrompre ou d'endommager le système si vous modifiez les autres données contenues dans ces fichiers, notamment les balises. Dell n'est pas en mesure de garantir que les problèmes résultant de l'apport de modifications non autorisées à ces fichiers pourront être résolus sans procéder à une réinstallation du Device Server.

eserver.properties

Vous pouvez modifier les paramètres décrits ci-après dans **<rép. d'installation de Device Server>\conf\eserver.properties**.

Nous vous recommandons d'insérer des commentaires au début du fichier pour effectuer le suivi des modifications que vous apportez. Vous pourrez ainsi facilement transférer vos modifications vers le nouveau fichier lorsque vous effectuerez une mise à niveau.

eserver.properties		
Paramètre	**Valeur par défaut**	**Description**
eserver.default.host	Device Server Service	Nom complet du domaine sur lequel le service Device Server est installé.
eserver.default.port	Enterprise Server version 7.7 ou ultérieure - 8443 Enterprise Server antérieur à la version 7.7 - 8081	Port d'écoute qui sera utilisé par Device Server pour les demandes d'activation entrantes envoyées par les périphériques.
eserver.use.ssl	Vrai	SSL est activé par défaut. Configurez ce paramètre sur Faux pour désactiver SSL.
eserver.keystore.location	${context['server.home']}/conf/cacerts	Emplacement du certificat SSL utilisé par Device Server.
eserver.keystore.password	changeit	Si vous avez modifié le mot de passe cacerts dans l'outil de configuration, ce paramètre est mis à jour en conséquence. Pour modifier votre cacert dans l'outil de configuration à tout moment après la configuration initiale, mettez à jour ce paramètre en saisissant le mot de passe Keystore que vous utilisez.

eserver.properties		
Paramètre	**Valeur par défaut**	**Description**
eserver.ciphers		Définit la liste des chiffrements de cryptage. Tous les chiffrements doivent être séparés par une virgule. Si vous laissez ce paramètre vide, le socket autorisera uniquement les chiffrements disponibles pris en charge par Tomcat. Supprimez le commentaire dans l'exemple ci-dessous pour définir la liste des chiffrements de cryptage. Séparez tous les chiffrements par une virgule. Consultez le guide de référence des JSSE de Sun pour connaître la liste des noms de suites de chiffrement valides. #eserver.ciphers= SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

run-service.conf

Vous pouvez modifier certains des paramètres décrits ci-après dans **<répertoire d'installation du Device Server>\conf\run-service.conf**. Ces paramètres sont configurés automatiquement au moment de l'installation. Pour personnaliser les paramètres ou modifier la configuration de n'importe quel service :

1. Arrêtez le service.
2. Supprimez le service.
3. Modifiez puis enregistrez le fichier **run-service.conf**. Nous vous recommandons d'insérer des commentaires au début du fichier pour effectuer le suivi des modifications que vous apportez.
4. Réinstallez le service.
5. Démarrez le service.

run-service.conf		
Paramètre	**Valeur par défaut**	**Description**
JAVA_HOME	Dell\Java Runtime\jreX.x	Emplacement du répertoire d'installation de Java.
wrapper.ntservice.name	EpmDeviceSvr	Nom du service.
wrapper.ntservice.displayname	Dell Device Server	Nom d'affichage du service.
wrapper.ntservice.description	Enterprise Device Server	Description du service.
wrapper.ntservice.dependency.1		Dépendances du service. Ajoutez les dépendances nécessaires en commençant par 1.
wrapper.ntservice.starttype	AUTO_START	Mode dans lequel le service est installé : AUTO_START ou DEMAND_START.
wrapper.ntservice.interactive	faux	Lorsque ce paramètre est configuré sur vrai, le service est autorisé à interagir avec le bureau.

4

Configuration de Security Server

Ce chapitre décrit les paramètres que vous pouvez modifier afin d'adapter Security Server à votre environnement.

Ne modifiez que les paramètres documentés dans ce fichier. Vous risquez de corrompre ou d'endommager le système si vous modifiez les autres données contenues dans ces fichiers, notamment les balises. Dell n'est pas en mesure de garantir que les problèmes résultant de l'apport de modifications non autorisées à ces fichiers pourront être résolus sans procéder à une réinstallation de Security Server.

context.properties

Vous pouvez modifier les paramètres décrits ci-après dans **<rép. d'installation de Security Server>\webapps\xapi\WEB-INF\context.properties**.

Nous vous recommandons d'insérer des commentaires au début du fichier pour effectuer le suivi des modifications que vous apportez. Vous pourrez ainsi facilement transférer vos modifications vers le nouveau fichier lorsque vous effectuerez une mise à niveau.

context.properties		
Paramètre	**Valeur par défaut**	**Description**
default.gatekeeper.group.remote	CMGREMOTE	Nom de groupe du périphérique distant. **Ne modifiez pas cette valeur.**
xmlrpc.max.threads	250	Nombre max. de threads simultanés dans ce Device Server.
default.auth.upn.suffix		Suffixe UPN ajouté au nom de connexion d'un utilisateur si le serveur requiert un nom de connexion complet et si aucun nom de connexion n'est fourni dans la requête.
device.manual.auth.enable	vrai	Indique si les authentifications manuelles sont activées ou désactivées. **Ne modifiez pas cette valeur.**
service.activation.enable	vrai	Indique si les activations sont gérées par Device Server. **Ne modifiez pas cette valeur.**
service.policy.enable	vrai	Indique si la règle est activée ou désactivée. **Ne modifiez pas cette valeur**.
service.auth.enable	vrai	Indique si les authentifications sont gérées par Device Server.
service.forensic.enable	vrai	Ce paramètre est utilisé avec un module d'extension d'intégration forensic. Veuillez contacter le support Dell pour savoir si un outil d'intégration forensic est nécessaire.
service.support.enable	vrai	Autorise la récupération des méta-informations relatives au serveur.
service.device.enable	vrai	Autorise la prise en charge des services du Shield tels que le stockage des clés SDE.

5

Configuration des fonctionnalités de cryptage

Cette section vous explique comment vous pouvez contrôler indépendamment les fonctionnalités de cryptage..

Empêcher la suppression des fichiers temporaires

Par défaut, tous les fichiers temporaires qui se trouvent dans le répertoire c:\windows\temp directory sont automatiquement supprimés au cours de l'installation/la mise à niveau de DDPE. La suppression des fichiers temporaires permet de réduire la durée initiale du cryptage et est effectuée avant l'analyse de cryptage initiale.

Cependant, si votre entreprise utilise une application tierce qui nécessite de conserver la structure des fichiers qui se trouvent dans le répertoire \temp directory, vous devez empêcher la suppression de ces fichiers.

Pour désactiver la suppression des fichiers temporaires, créez ou modifiez le paramètre registre en suivant les indications ci-après :

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

Remarque : le fait de ne **pas** supprimer les fichiers temporaires augmente la durée de cryptage initiale.

Masquer des icônes en transparence

Lors de l'installation, toutes les icônes de cryptage en transparence sont affichées par défaut. Utilisez le paramètre de répertoire suivant pour masquer les icônes de cryptage en transparence pour tous les utilisateurs gérés sur un ordinateur après l'installation initiale.

Créez ou modifiez le paramètre registre suivant :

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)=1

Si un utilisateur (doté des privilèges appropriés) choisit d'afficher les icônes de cryptage en transparence, ce paramètre écrasera cette valeur de répertoire.

Masquer une icône de barre d'état système

Par défaut, lors de l'installation, l'icône de barre d'état système est affichée. Utilisez le paramètre suivant de répertoire pour masquer les icônes de barre d'état système pour tous les utilisateurs gérés sur un ordinateur après l'installation initiale.

Créez ou modifiez le paramètre registre suivant :

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)=1

Activation par plages horaires

La fonctionnalité d'activation par plages horaires vous permet d'échelonner les activations des Shields sur une période définie en vue de diminuer la charge du serveur lors d'un déploiement de masse. Les activations sont différées en fonction de plages horaires générées par des algorithmes pour permettre une répartition fluide des heures d'activation.

L'activation et la configuration de la fonctionnalité d'activation par plages horaires s'effectuent dans le programme d'installation du Shield ou via le poste de travail du Shield.

Pour les utilisateurs nécessitant une activation via VPN, la configuration d'une activation par plages horaires pour le Shield peut être nécessaire pour différer l'activation initiale pendant une durée suffisamment importante pour permettre au logiciel client VPN d'établir une connexion au réseau.

ATTENTION : Ne configurez l'activation par plages horaires qu'avec l'aide du service clientèle. Si la configuration des plages horaires n'est pas correctement effectuée, un grand nombre de tentatives d'activation de clients peuvent être exécutées simultanément, ce qui risque de ralentir considérablement les performances du système.

Les clés de registre suivantes sont utilisées pour configurer l'activation par plages horaires. Il est nécessaire de redémarrer le poste de travail du Shield pour permettre aux modifications apportées à ces clés de registre de prendre effet.

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\SlottedActivation

  Ce paramètre active ou désactive la fonction d'Activation par plages horaires.
  Désactivé=0 (défaut)
  Activé=1
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat

  Durée en secondes de l'intervalle défini pour votre plage d'horaire d'activation. Vous pouvez utiliser cette propriété pour modifier la durée en secondes de l'intervalle défini pour votre plage d'horaire d'activation. Pour une période de sept heures, les plages horaires d'activation peuvent être réparties sur 25 200 secondes. Le paramètre par défaut est 86400 secondes, ce qui correspond à une répétition quotidienne.
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals

  Durée de l'intervalle dans la répétition, ACTIVATION_SLOT_CALREPEAT, qui correspond au moment où toutes les activations par plages horaires se produisent. Un seul intervalle est autorisé. Ce paramètre doit être 0,<CalRepeat>. Une valeur autre que 0 peut provoquer des résultats inattendus. Le paramètre par défaut est 0,86400. Pour configurer une répétition toutes les sept heures, utilisez le paramètre 0,25200. CALREPEAT est activé lorsqu'un utilisateur du Shield se connecte.
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold

  Nombre maximal de plages horaires d'activation qui peuvent être manquées avant que l'ordinateur tente de procéder à l'activation lors de la prochaine connexion de l'utilisateur pour lequel une plage horaire d'activation a été définie. Si l'activation échoue lors de cette tentative immédiate, le Shield reprend les tentatives d'activation par plages horaires. Si l'activation échoue en raison d'une défaillance du réseau, une nouvelle tentative d'activation est exécutée une fois la connexion au réseau rétablie, et ce même si la valeur du paramètre MISSTHRESHOLD n'a pas été dépassée. Si un utilisateur se déconnecte avant le début de la plage horaire de l'activation, une nouvelle plage horaire est définie pour sa prochaine connexion.
- HKCU/Software/CREDANT/ActivationSlot (en fonction des données utilisateur)

  Heure différée pour la tentative d'activation par plages horaires qui est définie lorsque l'utilisateur se connecte pour la première fois au réseau après l'activation de la fonctionnalité d'activation par plages horaires. La plage horaire de l'activation est recalculée à chaque tentative d'activation.
- HKCU/Software/CREDANT/SlotAttemptCount (en fonction des données utilisateur)

  Nombre de tentatives échouées ou manquées qui se produisent lorsque la plage horaire arrive à échéance et que la tentative d'activation échoue. Lorsque ce nombre atteint la valeur définie dans le paramètre ACTIVATION_SLOT_MISSTHRESHOLD, l'ordinateur exécute immédiatement une tentative d'activation dès qu'une connexion au réseau est établie.

Pour permettre l'activation par plages horaires via la ligne de commande, utilisez une commande basée sur l'exemple suivant :

setup.exe /v"SLOTTEDACTIVATION=1 CALREPEAT=25200 SLOTINTERVALS=0,25200 <autres paramètres>"

REMARQUE : Veillez à placer une valeur contenant un ou plusieurs caractères spéciaux, tels qu'un espace, entre des guillemets d'échappement (sans programmation spéciale).

Interrogation forcée

Utilisez le paramètre registre suivant pour autoriser le Shield à interroger le serveur pour procéder à une mise à niveau forcée des règles.

Créez ou modifiez le paramètre registre suivant :

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD value)=1

Selon la version Shield, le paramètre de répertoire disparaîtra automatiquement *ou* passera de 1 à 0 une fois l'interrogation terminée.

Selon les permissions d'un utilisateur Admin, il est possible qu'une modification des permissions s'impose pour créer ce paramètre de répertoire. En cas de problèmes pendant la tentative de création d'un nouveau DWORD, procédez comme suit pour modifier les permissions.

1. Dans le répertoire Windows, rendez-vous sur HKLM\SOFTWARE\Credant\CMGShield\Notifier.
2. Cliquez avec le bouton droit de la souris sur Notifier > Autorisations.
3. Quand la fenêtre *Permission de notifier* s'ouvre, cochez la case Contrôle total.
4. Cliquez sur OK.

Vous pouvez créer le paramètre de votre nouveau répertoire.

Options d'inventaire

Utilisez les paramètres suivants du registre pour permettre au Shield d'envoyer au serveur, au choix, un inventaire optimisé, un inventaire complet ou un inventaire complet pour tous les utilisateurs activés.

Envoyer un inventaire optimisé au serveur

Créez ou modifiez le paramètre registre suivant :

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

OnlySendInvChanges (REG_DWORD)=1

Si aucune entrée n'existe, l'inventaire optimisé est envoyé au serveur.

Envoyer un inventaire complet au serveur

Créez ou modifiez le paramètre registre suivant :

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

OnlySendInvChanges (REG_DWORD)=0

Si aucune entrée n'existe, l'inventaire optimisé est envoyé au serveur.

Envoyer un inventaire complet pour tous les utilisateurs activés

Créez ou modifiez le paramètre registre suivant :

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield

RefreshInventory (REG_DWORD)=1

Cette entrée est supprimée du registre une fois traitée. Cependant, la valeur est enregistrée dans le coffre. Par conséquent, même si vous redémarrez l'ordinateur avant le chargement de l'inventaire, le Shield honorera cette requête lors du prochain chargement réussi de l'inventaire.

Cette entrée remplace la valeur de répertoire OnlySendInvChanges.

Activations hors domaine

L'autorisation des activations hors domaine est une configuration avancée qui a d'importantes répercussions. Contactez le service clientèle pour aborder vos besoins environnementaux spécifiques et obtenir des instructions afin d'activer cette fonction.

6

Configuration des composants pour l'authentification/autorisation Kerberos

Cette section vous explique comment configurer les composants requis pour l'utilisation de l'authentification/autorisation Kerberos.

Configuration des composants pour l'authentification/autorisation Kerberos

REMARQUE : Pour utiliser l'authentification/autorisation Kerberos, il est nécessaire d'intégrer le serveur qui contient le composant Key Server dans le domaine concerné.

Key Server est un service qui écoute les clients qui se connectent à un socket. Dès qu'un client est connecté, une connexion sécurisée est négociée, authentifiée et cryptée grâce aux API Kerberos (en cas d'échec de la négociation de la connexion sécurisée, le client est déconnecté).

Key Server vérifie ensuite auprès de Device Server si l'utilisateur exécutant le client est autorisé à accéder aux clés. Cet accès est accordé dans la Console de gestion à distance via des domaines *individuels*.

Instructions pour les services Windows

1. Accédez au panneau de configuration des services Windows (Démarrer > Exécuter... > services.msc > OK).
2. Effectuez un clic droit sur Dell Key Server, puis sélectionnez Propriétés.
3. Accédez à l'onglet Connexion et cochez la case d'option Ce compte :.
4. Dans le champ Ce compte :, ajoutez l'utilisateur de domaine de votre choix. Cet utilisateur de domaine doit au minimum disposer des droits d'administrateur local pour le dossier Key Server (il doit disposer de droits d'écriture sur le fichier de configuration Key Server ainsi que sur le fichier log.txt).
5. Cliquez sur OK.
6. Redémarrez le service (laissez le panneau de configuration des services Windows ouvert pour pouvoir y retourner ultérieurement).
7. Naviguez jusqu'au fichier log.txt qui se trouve dans le <rép. d'installation de Key Server> pour vérifier que le service a correctement démarré.

Instructions pour le fichier de configuration Key Server

1. Naviguez jusqu'au <rép. d'installation de Key Server>.
2. Ouvrez le fichier Credant.KeyServer.exe.config à l'aide d'un éditeur de texte.
3. Naviguez jusqu'à <add key="user" value="superadmin" /> et remplacez la valeur « superadmin » par le nom de l'utilisateur concerné (vous pouvez également laisser la valeur « superadmin »).

   Le format « superadmin » peut correspondre à n'importe quelle méthode permettant l'authentification sur le serveur. Vous pouvez utiliser le nom de compte SAM, l'UPN ou le format domaine\nom d'utilisateur. Toutes les méthodes permettant l'authentification sur le serveur sont acceptées car la validation est requise pour *ce* compte utilisateur pour une autorisation en fonction d'Active Directory.

   Par exemple, dans un environnement à domaines multiples, si vous saisissez uniquement un nom de compte SAM tel que « jdoe », l'authentification risque d'échouer car le serveur ne pourra pas authentifier « jdoe » car « jdoe » est introuvable. Bien que le format domaine\nom d'utilisateur soit accepté, nous vous recommandons d'utiliser l'UPN dans un environnement à domaines multiples.

   Dans un environnement à domaine unique, vous pouvez utiliser le nom de compte SAM.

4 Accédez à <add key="epw" value="<valeur cryptée du mot de passe>" /> et remplacez « epw » par « password ». Puis remplacez la « <valeur cryptée du mot de passe> » par le mot de passe de l'utilisateur de l'étape 3. Ce mot de passe est re-crypté dès que le serveur redémarre.

Si vous avez utilisé « superadmin » à l'étape 3, et si le mot de passe superadmin n'est pas « changeit », vous devez le modifier ici.

5 Enregistrez vos modifications, puis fermez le fichier.

Exemple de fichier de configuration :

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [Port TCP sur lequel le serveur écoutera. Le port par défaut est 8050, modifiez-le si nécessaire.]
        <add key="maxConnections" value="2000" /> [Nombre de connexions de socket actives que le serveur autorisera]
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [URL de votre Device Server] Si votre Enterprise Server est à la version 7.7 ou une version ultérieure, le format est https://keyserver.domain.com:8443/xapi/ -- Si Enterprise Server est antérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8081/xapi https://keyserver.domain.com:8081/xapi (sans la dernière barre oblique.]
        <add key="verifyCertificate" value="false" /> [la valeur « vrai » vérifie les certificats ; définissez-la sur « faux » si vous ne souhaitez pas vérifier les certificats ou si vous utilisez des certificats auto-signés]
        <add key="user" value="superadmin" /> [Nom d'utilisateur utilisé pour communiquer avec Device Server. Notez que le type Administrateur Forensic doit être sélectionné pour cet utilisateur dans la Console de gestion à distance. Le format « superadmin » peut correspondre à n'importe quelle méthode permettant l'authentification sur le serveur. Vous pouvez utiliser le nom de compte SAM, l'UPN ou le format domaine|nom d'utilisateur. Toutes les méthodes permettant l'authentification sur le serveur sont acceptées car la validation est requise pour ce compte utilisateur pour une autorisation en fonction d'Active Directory. Par exemple, dans un environnement à domaines multiples, si vous saisissez uniquement un nom de compte SAM tel que « jdoe », l'authentification risque d'échouer car le serveur ne pourra pas authentifier « jdoe » car « jdoe » est introuvable. Bien que le format domaine|nom d'utilisateur soit accepté, nous vous recommandons d'utiliser l'UPN dans un environnement à domaines multiples. Dans un environnement à domaine unique, vous pouvez utiliser le nom de compte SAM.]
        <add key="cacheExpiration" value="30" /> [Fréquence (en secondes) à laquelle le service doit vérifier les personnes autorisées à demander des clés. Le service conserve un cache et assure le suivi de son ancienneté. Lorsque l'ancienneté du cache dépasse la valeur définie (en secondes), le service établit alors une nouvelle liste. Lorsqu'un utilisateur se connecte, Key Server doit télécharger les utilisateurs autorisés à partir du Device Server. S'il n'existe aucun cache pour ces utilisateurs, ou si la liste n'a pas été téléchargée au cours des « x » dernières secondes, la liste est alors téléchargée à nouveau. Aucune interrogation n'est exécutée, mais cette valeur permet de configurer le délai d'expiration de la liste après lequel une actualisation est nécessaire.]
        <add key="epw" value="encrypted value of the password" /> [Mot de passe utilisé pour communiquer avec le Device Server. Si vous avez modifié le mot de passe superadmin, vous devez également le modifier ici.]
    </appSettings>
</configuration>
```

Instructions pour les services Windows

1 Retournez au panneau de configuration des services Windows.

2 Redémarrez le service Dell Key Server.

3 Naviguez jusqu'au fichier log.txt qui se trouve dans le <rép. d'installation de Key Server> pour vérifier que le service a correctement démarré.

4 Fermez le panneau de configuration des services Windows.

Instructions pour la Console de gestion à distance

1. Si nécessaire, connectez-vous à la Console de gestion à distance.
2. Cliquez sur **Domaines**, puis sur l'icône **Détails**.
3. Cliquez sur **Key Server**.
4. Dans la liste des comptes Key Server, ajoutez l'utilisateur qui exécutera les opérations d'administration. Le format à utiliser est Domaine\Nom d'utilisateur. Cliquez sur **Ajouter un compte**.
5. Cliquez sur **Utilisateurs** dans le menu de gauche. Dans la zone de recherche, recherchez le nom d'utilisateur que vous avez ajouté à l'étape 4. Cliquez sur **Rechercher**.
6. Une fois que vous avez localisé l'utilisateur approprié, cliquez sur l'icône **Détails**.
7. Sélectionnez **Administrateur Forensic**. Cliquez sur **Mettre à jour**.

La configuration des composants pour l'authentification/autorisation Kerberos est maintenant terminée.

7

Attribuer le rôle d'administrateur Forensic

Par défaut, l'autorisation Forensic est activée sur les serveurs dorsaux et désactivée sur les serveurs frontaux. Ces paramètres sont définis correctement lors de l'installation du Device Server et du serveur de sécurité.

Instructions pour la Console de gestion à distance

1. Si nécessaire, connectez-vous à la Console de gestion à distance.
2. Dans le volet de gauche, cliquez sur **Gérer** > **Utilisateurs**.
3. Dans la page *Rechercher les utilisateurs*, saisissez le nom de l'utilisateur auquel vous souhaitez accorder le rôle d'administrateur Forensic, puis cliquez sur **Rechercher** (les identifiants de cet utilisateur sont fournis au moment de l'exécution des utilitaires CMGAd, CMGAu et CMGAlu et de Decryption Agent en mode Forensic).
4. Dans la page *Résultats de la recherche d'utilisateur*, cliquez sur l'icône **Détails**.
5. Dans la page *Détails de l'utilisateur : <Nom d'utilisateur>*, sélectionnez **Admin**.
6. Dans la colonne Utilisateur, cochez la case **Administrateur Forensic**, puis cliquez sur **Mettre à jour**.

Le rôle d'administrateur Forensic est désormais défini.

Désactiver l'autorisation Forensic

1. Sur votre serveur principal, naviguez jusqu'à **<répertoire d'installation du serveur de sécurité>\webapps\xapi\WEB-INF\context.properties** et modifiez la propriété suivante :

   service.forensic.enable=true

   en

   service.forensic.enable=false
2. **Redémarrez** le service du serveur de sécurité.
3. Naviguez jusqu'à <rép. d'installation de Device Server>\webapps\ROOT\WEB-INF\web.xml et effectuez la modification suivante :

   <init-param>

   <param-name>forensic</param-name>

   <param-value>**@FORENSIC_DISABLE@**</param-value>

   </init-param>
4. **Redémarrez** le service Device Server.
5. La méthode recommandée consiste à supprimer le rôle d'administrateur Forensic pour les utilisateurs qui n'utilisent pas activement les permissions de rôle.

8

Expressions Cron

Cette section vous explique comment utiliser la syntaxe des expressions Cron et les caractères spéciaux.

Présentation des expressions Cron

Cron est un outil disponible depuis de nombreuses années sous UNIX. Ses puissantes fonctionnalités de planification sont donc éprouvées. La classe CronTrigger est basée sur les fonctionnalités de planification de Cron.

CronTrigger utilise les expressions Cron qui permettent de planifier le déclenchement de règles, par exemple à 8h00 tous les matins du lundi au vendredi, ou à 1h30 du matin tous les derniers vendredis du mois.

Les expressions Cron constituent un outil puissant mais qui peut parfois prêter à confusion. Ce document a pour objectif de dissiper certains des mystères qui entourent la création d'une expression Cron en vous apportant quelques points de repères auxquels vous pourrez vous référer avant d'avoir à solliciter une aide extérieure.

Syntaxe des expressions Cron

Les expressions Cron se composent de six champs obligatoires et d'un champ facultatif séparés par un espace. Ces champs peuvent contenir toutes les valeurs autorisées ainsi que différentes combinaisons de caractères spéciaux autorisés qui sont spécifiques à chaque champ.

La syntaxe des expressions Cron peut être aussi simple que * * * * ? *.

Ou plus complexe, par exemple 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010.

Les différents champs sont décrits dans le tableau ci-dessous.

Nom du champ	Obligatoire ?	Valeurs autorisées	Caractères spéciaux autorisés
Minutes	Oui	0-59	, - * /
Hours	Oui	0-23	, - * /
Day of month	Oui	1-31	, - * ? / L W C
Month	Oui	1-12 ou JAN-DEC	, - * /
Day of week	Oui	1-7 ou SUN-SAT	, - * ? / L C #
Year	Non	vide, 1970-2099	, - * /

Caractères spéciaux

- Le caractère * permet de spécifier toutes les valeurs. Par exemple, * dans le champ « Minutes » signifie chaque minute.
- Le caractère ? (aucune valeur précise) est utile lorsque vous devez spécifier une valeur dans l'un des deux champs où ce caractère est autorisé mais pas dans l'autre. Par exemple, si vous souhaitez déclencher une règle à un jour précis du mois (le 10), mais que le jour de la semaine auquel il correspond n'a aucune importance, saisissez 10 dans le champ « Day of month » et ? dans le champ « Day of week ».
- Le caractère - permet de spécifier des plages de valeurs. Par exemple, 10-12 dans le champ « Hours » permet de spécifier les heures suivantes : 10 heures, 11 heures et 12 heures.
- Le caractère , permet de spécifier des valeurs supplémentaires. Par exemple, MON,WED,FRI dans le champ « Day of week » signifie les jours suivants : lundi, mercredi et vendredi.

- Le caractère / permet de spécifier des incréments.

  0/15 dans le champ « Seconds » signifie les secondes suivantes : 0, 15, 30 et 45.

  5/15 dans le champ « Seconds » signifie les secondes suivantes : 5, 20, 35 et 50.

  Faire précéder le caractère / du caractère * équivaut à spécifier 0 comme valeur de départ.

  1/3 dans le champ « Day of month » signifie que la règle est déclenchée tous les 3 jours à partir du premier jour du mois.

  L'essentiel à retenir est qu'il existe un ensemble de nombres qui peuvent être activés ou désactivés pour chaque champ de l'expression. Pour les secondes et les minutes, les numéros vont de 0 à 59. Pour les heures, de 0 à 23, pour les jours du mois, de 0 à 31. Pour les mois, de 1 à 12. Le caractère / vous permet d'activer facilement la fréquence dans l'ensemble correspondant. Ainsi, 7/6 dans le champ « Month » permet de déclencher la règle uniquement le septième mois, et non tous les six mois.
- Le caractère L est autorisé dans les champs « Day of month » et « Day of week ». Ce caractère signifie « dernier » mais il peut avoir des significations différentes selon qu'il est employé dans l'un ou l'autre de ces champs.

  La valeur L dans le champ « Day of month » signifie le dernier jour du mois (le 31 pour le mois de janvier, le 28 pour le mois de février dans le cas des années non bissextiles).

  S'il est utilisé seul dans le champ « Day of week », ce caractère signifie le septième jour de la semaine ou SAT (samedi).

  S'il succède à une autre valeur dans le champ « Day of week », il signifie alors le dernier xxxème jour de la semaine dans le mois. Par exemple, 6L signifie le dernier vendredi du mois. Pour éviter d'obtenir des résultats prêtant à confusion lorsque vous utilisez l'option L, il est important de ne pas spécifier de listes ou de plages de valeurs.
- Le caractère W est autorisé dans le champ « Day of month ». Ce caractère permet de spécifier le jour de semaine (du lundi au vendredi) le plus proche d'une date donnée. Par exemple, si vous spécifiez la valeur 15W dans le champ « Day of month », cela signifie le jour de semaine le plus proche du 15 du mois. Si le 15 du mois correspond à un samedi, la règle sera déclenchée le vendredi 14. Si le 15 du mois correspond à un dimanche, la règle sera déclenchée le lundi 16. Si le 15 du mois correspond à un mardi, la règle sera déclenchée le mardi 15. Cependant, si vous définissez la valeur 1W dans le champ « Day of month » et si le premier jour du mois correspond à un samedi, la règle sera déclenchée le lundi 3 car il n'est pas possible de dépasser la limite du mois. Le caractère W peut uniquement être utilisé lorsque vous spécifiez un seul jour, et non une plage ou une liste de jours, dans le champ « Day of month ».

  Il est également possible d'associer les caractères L et W dans une expression correspondant à un « Day of month » pour créer l'expression LW, qui signifie alors le dernier jour de semaine du mois.
- Le caractère # est autorisé dans le champ « Day of week ». Ce caractère permet de spécifier le « nième » jour du mois. Par exemple, la valeur 6#3 dans le champ « Day of week » signifie le troisième vendredi du mois (jour 6 = vendredi et #3 = le troisième du mois).

  Autres exemples :
  2#1 = le premier lundi du mois
  4#5 = le cinquième mercredi du mois.

  Notez que si vous spécifiez la valeur #5 et qu'il n'existe pas de cinquième occurrence du jour de la semaine spécifié dans le mois concerné, la règle ne sera pas déclenchée pendant le mois en question.
- Le caractère C est autorisé pour le calendrier. Lorsque ce caractère est utilisé, les valeurs sont alors calculées en fonction du calendrier associé, le cas échéant. Si aucun calendrier n'est associé, l'utilisation de ce caractère équivaut à utiliser un calendrier englobant tous les événements. Si vous définissez la valeur 5C dans le champ « Day of month », cela signifie le premier jour du calendrier correspondant au 5 du mois ou au premier jour suivant le 5 du mois. Si vous définissez la valeur 1C dans le champ « Day of week », cela signifie le premier jour du calendrier correspondant au dimanche ou au premier jour suivant le dimanche.

REMARQUE : La définition d'une valeur correspondant à la fois au jour de la semaine et au jour du mois n'est pas totalement prise en charge. Utilisez le caractère ? dans l'un de ces champs. La définition des fonctionnalités décrites pour le caractère C n'est pas totalement prise en charge. Les caractères autorisés et les noms des mois et des jours de la semaine ne sont pas sensibles à la casse. Vous pouvez indifféremment saisir « MON » ou « mon » (pour lundi). Faites bien attention aux effets des ? et * dans les champs « Day of week » et « Day of month ».
Soyez particulièrement vigilant lorsque vous spécifiez les heures de déclenchement des règles entre minuit et 1 h 00 du matin. Le changement d'heure peut entraîner l'omission (ou la répétition) d'un déclenchement, selon qu'il s'agit d'un passage à l'heure d'été ou à l'heure d'hiver.

Exemples

Expression	Signification
0 0 12 * * ?	Déclenchement de la règle tous les jours à 12h00 (midi)
0 15 10 ? * *	Déclenchement de la règle tous les jours à 10h15
0 15 10 * * ?	Déclenchement de la règle tous les jours à 10h15
0 15 10 * * ? *	Déclenchement de la règle tous les jours à 10h15
0 15 10 * * ? 2005	Déclenchement de la règle tous les jours à 10h15 pendant l'année 2005
0 * 14 * * ?	Déclenchement de la règle toutes les minutes de 14h00 à 14h59, tous les jours
0 0/5 14 * * ?	Déclenchement de la règle toutes les 5 minutes de 14h00 à 14h55, tous les jours
0 0/5 14,18 * * ?	Déclenchement de la règle toutes les 5 minutes de 14h00 à 14h55 ET déclenchement de la règle toutes les 5 minutes de 18h00 à 18h55, tous les jours
0 0-5 14 * * ?	Déclenchement de la règle toutes les minutes de 14h00 à 14h05, tous les jours
0 10,44 14 ? 3 WED	Déclenchement de la règle à 14h10 et à 14h44 tous les mercredis du mois de mars.
0 15 10 ? * MON-FRI	Déclenchement de la règle à 10h15 tous les lundis, mardis, mercredis, jeudis et vendredis
0 15 10 15 * ?	Déclenchement de la règle à 10h15 le 15 de chaque mois
0 15 10 L * ?	Déclenchement de la règle à 10h15 le dernier jour de chaque mois
0 15 10 ? * 6L	Déclenchement de la règle à 10h15 le dernier vendredi de chaque mois
0 15 10 ? * 6L	Déclenchement de la règle à 10h15 le dernier vendredi de chaque mois
0 15 10 ? * 6L 2002-2005	Déclenchement de la règle à 10h15 chaque dernier vendredi de chaque mois pendant les années 2002, 2003, 2004 et 2005
0 15 10 ? * 6#3	Déclenchement de la règle à 10h15 le troisième vendredi de chaque mois
0 0 12 1/5 * ?	Déclenchement de la règle à 12h (midi) tous les 5 jours de chaque mois à partir du premier jour du mois.
0 11 11 11 11 ?	Déclenchement de la règle tous les 11 novembre à 11h11.

9

Créer un certificat auto-signé avec Keytool et générer une demande de signature de certificat (CSR)

REMARQUE : Cette section décrit les étapes à suivre pour créer un certificat auto-signé pour des composants Java. Ce processus *ne peut pas* être utilisé pour créer un certificat auto-signé pour les composants basés sur .NET.

Nous recommandons un certificat auto-signé *uniquement* dans un environnement hors production.

Si votre entreprise nécessite un certificat de serveur SSL, ou si vous avez besoin de créer un certificat pour d'autres raisons, cette section décrit le processus de création d'un magasin de clés java à l'aide de l'outil Keytool.

Keytool crée les clés privées qui sont transmises sous le format d'une demande de signature de certificat (CSR) à une autorité de certification, telle que VeriSign® ou Entrust®. Sur la base de cette CSR, l'autorité de certification créera ensuite un certificat de serveur signé. Le certificat de serveur est ensuite téléchargé sur un fichier avec le certificat de l'autorité de signature. Les certificats sont ensuite importés dans le fichier cacerts.

Générer une nouvelle paire de clés et un certificat auto-signé

1. Naviguez vers le répertoire conf de Compliance Reporter, Console Web Services, Device Server, ou Gatekeeper Web Services.
2. Sauvegardez la base de données de certificats par défaut :

   Cliquez sur Démarrer > Exécuter et tapez move cacerts cacerts.old.
3. Ajoutez Keytool au chemin d'accès au système. Tapez la commande suivante dans une invite de commande :

   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. Pour générer un certificat, exécutez Keytool comme indiqué :

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Saisissez les informations suivantes, quand l'outil keytool vous invite à le faire.

REMARQUE : Faites une copie de sauvegarde des fichiers de configuration avant de les modifier. Modifiez uniquement les paramètres spécifiés. Vous risquez de corrompre ou d'endommager le système si vous modifiez les autres données contenues dans ces fichiers, notamment les balises. Dell n'est pas en mesure de garantir que les problèmes résultant de l'apport de modifications non autorisées à ces fichiers pourront être résolus sans procéder à une réinstallation de l'Enterprise Server.

- *Mot de passe du magasin de clés :* saisissez un mot de passe (les caractères non pris en charge sont les suivants : <>;&” ’), et définissez la variable dans le composant de fichier conf à la même valeur, comme suit :

  <répertoire d'installation du Compliance Reporter>\conf\eserver.properties. Définissez la valeur eserver.keystore.password =

  <répertoire d'installation des Console Web Services>\conf\eserver.properties. Définissez la valeur eserver.keystore.password =

  <répertoire d'installation du Device Server>\conf\eserver.properties. Définissez la valeur eserver.keystore.password =
- *Nom et prénom :* saisissez le nom complet du serveur sur lequel le composant avec lequel vous travaillez est installé. Ce nom complet comprend le nom d'hôte et le nom de domaine (par exemple, server.dell.com).
- *Service :* saisissez la valeur appropriée (par exemple, Sécurité).
- *Entreprise :* saisissez la valeur appropriée (par exemple, Dell).

- *Ville ou localité :* saisissez la valeur appropriée (par exemple, Austin).
- *État ou province :* saisissez le nom non-abrégé de l'État ou de la province (par exemple, Texas).
- Code de deux lettres du pays :
  États-Unis = US

  Canada = CA

  Suisse = CH

  Allemagne = DE

  Espagne = ES

  France = FR

  Grande-Bretagne = GB

  Irlande = IE

  Italie = IT

  Pays-Bas = NL
- L'utilitaire demande confirmation que l'information est correcte. Si c'est le cas, saisissez `oui`.
  Si ce n'est pas le cas, saisissez `non`. Le Keytool affiche toutes les valeurs saisies précédemment. Cliquez sur **OK** pour accepter la valeur ou modifiez la valeur, puis cliquez sur **OK**.
- *Mot de passe clé pour alias :* si vous ne saisissez pas un autre mot de passe ici, ce mot de passe sera par défaut celui du magasin de clés.

Demander un certificat signé par une autorité de certification

Utilisez cette procédure pour générer une demande de signature de certificat (CSR) pour le certificat auto-signé créé dans Générer une nouvelle paire de clés et un certificat auto-signé.

1. Substituez la même valeur que celle utilisée précédemment pour **<certificatealias>** :
   ```
   keytool -certreq -sigalg MD5withRSA -alias <certificate-alias> -keystore
   .\cacerts -file <csr-filename>
   ```
   Exemple :
   ```
   keytool -certreq -sigalg MD5withRSA -alias dell -keystore .\cacerts -file
   credant.csr
   ```
   Le fichier .csr contiendra une paire BEGIN/END qui sera utilisée lors de la création du certificat de l'autorité de certification.

Schéma 9-1. Exemple de fichier .CSR

2. Suivez votre processus organisationnel pour l'acquisition d'un certificat de serveur SSL auprès d'une autorité de certification. Envoyer le contenu de <csr-filename> pour la signature.

REMARQUE : Il existe plusieurs méthodes pour demander un certificat valide. Un **exemple** de méthode est disponible dans Exemple de méthode pour demander un certificat.

3 Lorsque le certificat signé est reçu, enregistrez-le dans un fichier.

4 La méthode recommandée consiste à sauvegarder ce certificat dans le cas où une erreur se produise pendant le processus d'importation. Cette sauvegarde pourra éviter d'avoir à reprendre le processus depuis le début.

Importer un certificat racine

REMARQUE : Si l'Autorité de certification du certificat racine est Verisign (mais pas Verisign Test), passez à la procédure suivante et importez le certificat signé.

Le certificat racine de l'autorité de certification valide les certificats signés.

1 Effectuez l'une des opérations suivantes :

- Téléchargez le certificat racine de l'autorité de certification et enregistrez-le dans un fichier.
- Obtenez le certificat racine du serveur de l'annuaire d'entreprise.

2 Effectuez l'une des opérations suivantes :

- Si vous activez SSL pour Compliance Reporter, Console Web Services, Device Server ou Legacy Gatekeeper Connector, utilisez le répertoire de composantconf.
- Si vous activez SSL entre le serveur et le serveur de répertoire d'entreprise, remplacez par <Répertoire d'installation Dell>\Java Runtimes\jre1.x.x_xx\lib\security (le mot de passe par défaut de JRE cacerts est changeit).

3 Exécutez Keytool comme suit pour installer le certificat racine :

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file
<ca-cert-filename>
```

Exemple :

```
keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer
```

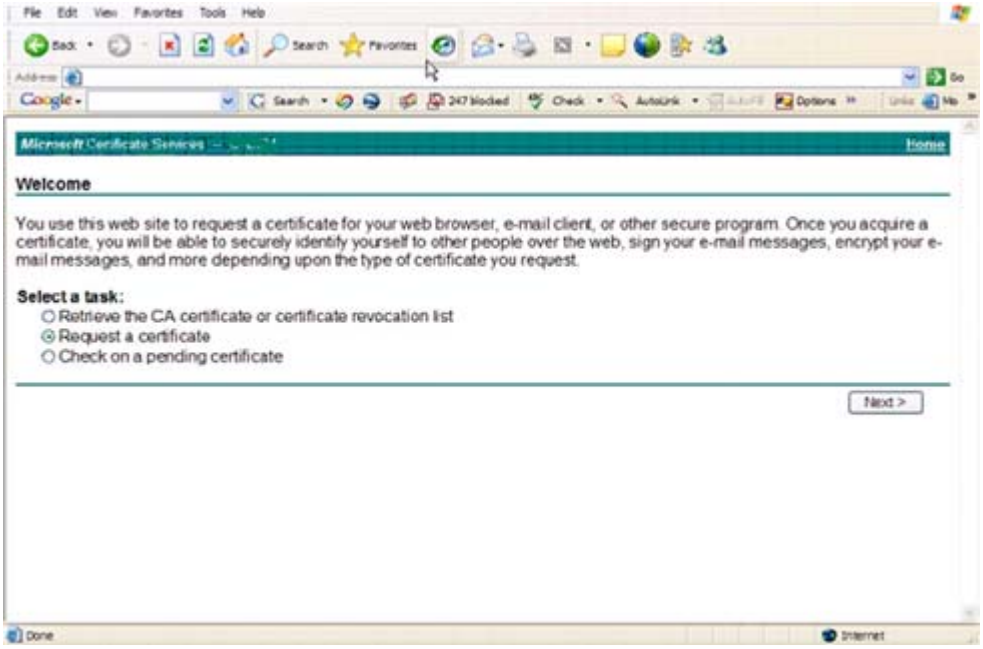
Exemple de méthode pour demander un certificat

Exemple de méthode pour demander un certificat : utiliser un navigateur web pour accéder au Serveur CA Microsoft, qui sera mis en place en interne par votre entreprise.

1 Naviguez jusqu'au serveur CA Microsoft. L'adresse IP sera fournie par votre entreprise.

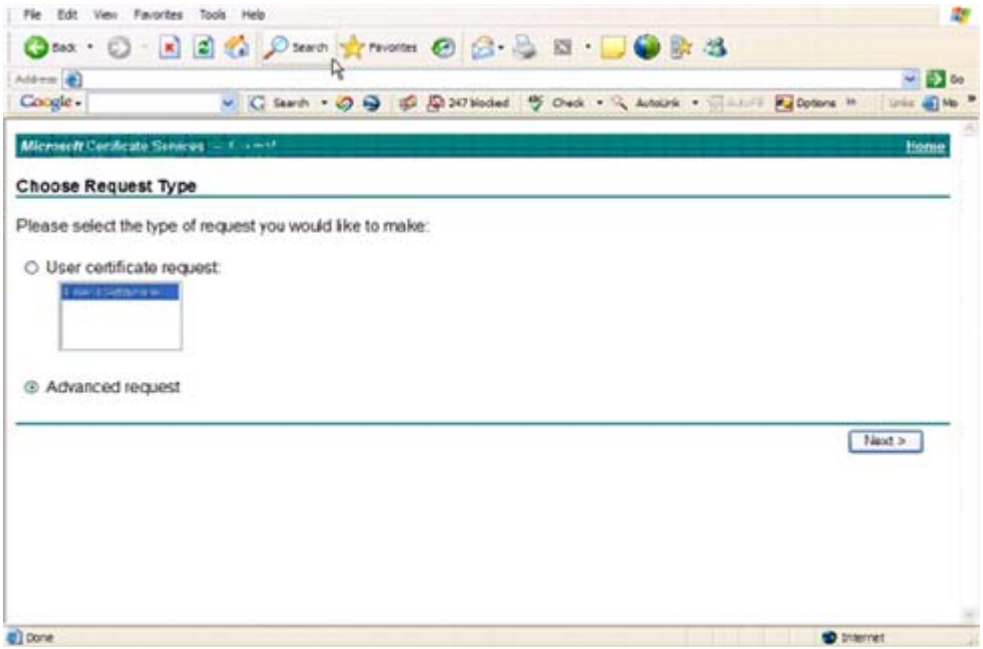
2 Sélectionnez Demander un certificat et cliquez sur Suivant >.

Schéma 9-2. Services de certificats Microsoft



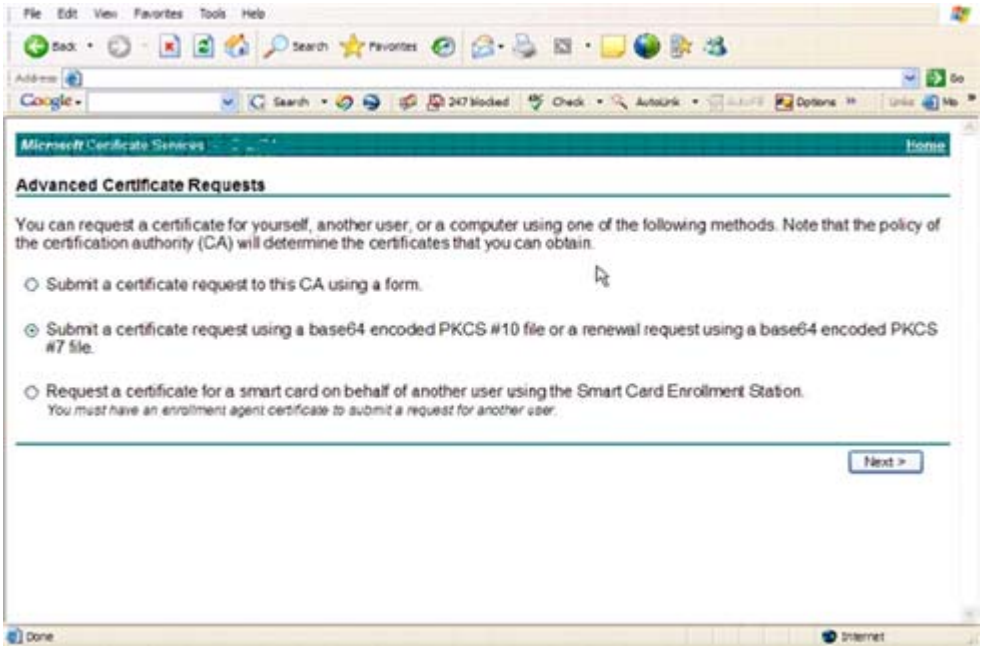
3 Sélectionnez Demandes avancées puis cliquez sur Suivant >.

Schéma 9-3. Choisissez le type de demande



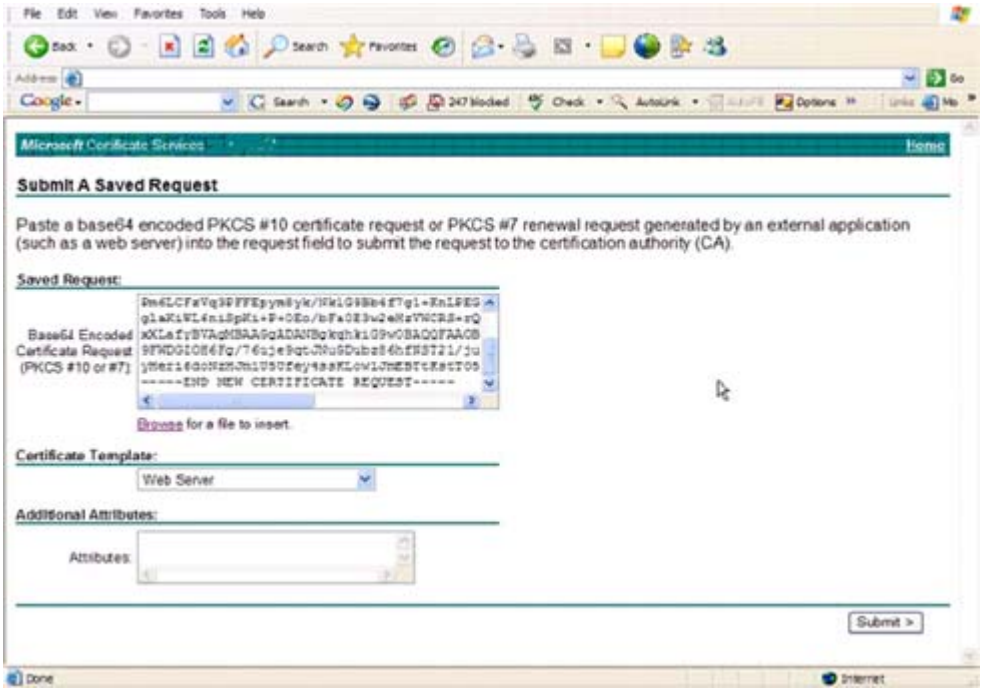
4 Sélectionnez l'option de **Soumettre une demande de certificat avec un fichier PKCS #10 à encodage base64** et cliquez sur **Suivant >**.

Schéma 9-4. Demande de certificat avancée



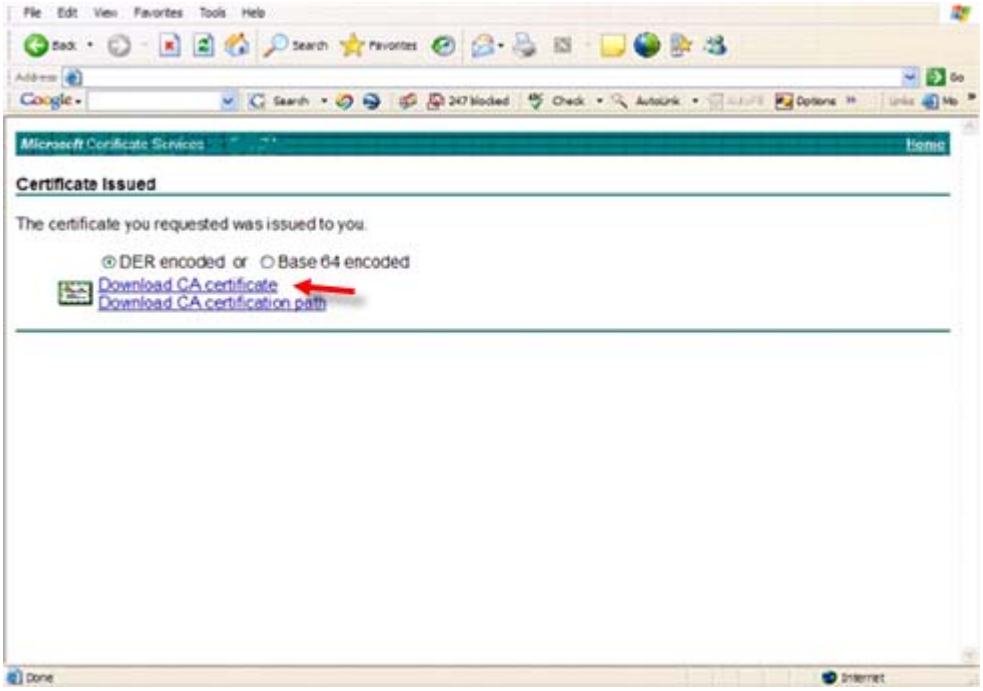
5 Collez le contenu de la demande CSR dans la zone de texte. Sélectionnez un modèle de certificat de **serveur Web** et cliquez sur **Envoyer >**.

Schéma 9-5. Soumettre une requête enregistrée



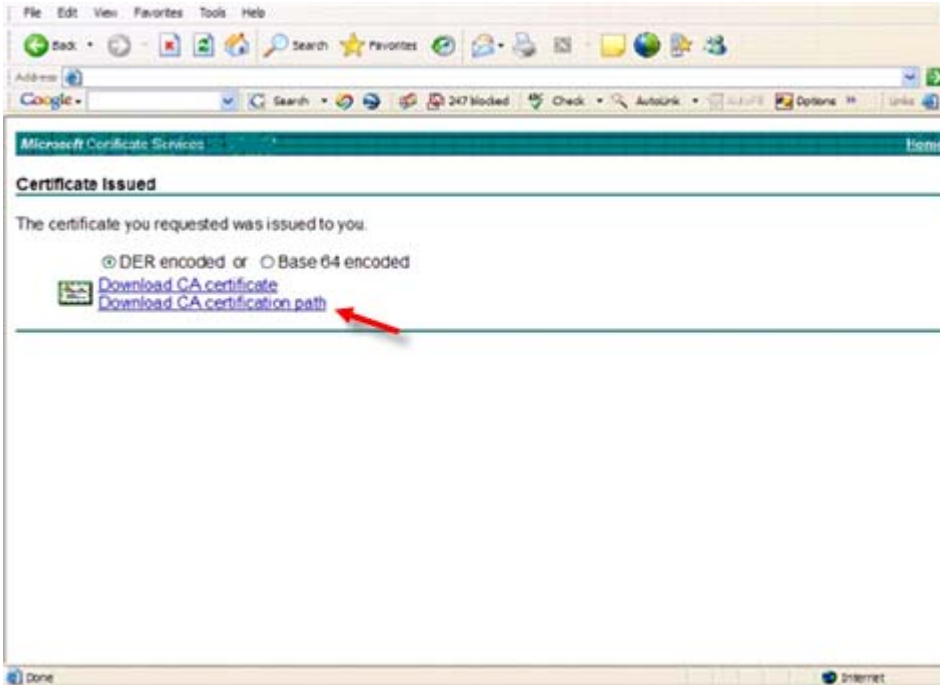
6 Enregistrez le certificat. Sélectionnez **Binaire encodé** et cliquez sur **Télécharger certificat CA**.

Schéma 9-6. Télécharger un certificat CA



7 Enregistrez le certificat. Sélectionnez **Binaire encodé** et cliquez sur **Télécharger chemin de certification CA**.

Schéma 9-7. Télécharger chemin de certification CA



8 Importez les certificats d'autorité de signature convertis. Retournez à la fenêtre DOS. Tapez :

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Après que le certificat de l'autorité de signature a été importé, le certificat du serveur peuvent être importés (la chaîne de confiance peut être établie). Tapez :

```
keytool -import -alias dell -file <csr-filename> -keystore cacerts
```

Utilisez l'alias du certificat auto-signé pour combiner la demande CSR avec le certificat du serveur.

10 La liste du fichier cacerts montrera que le certificat du serveur a une **longueur de chaîne de certificat** de **2**, ce qui indique que le certificat n'est pas auto-signé. Tapez :

```
keytool -list -v -keystore cacerts
```

Notez que l'empreinte de certificat du deuxième certificat de la chaîne est le certificat d'autorité de signature importé (qui est également répertorié ci-dessous comme certificat du serveur dans la liste).

Le certificat du serveur a été importé, ainsi que le certificat de l'autorité de signature.


0 XXXXXA0 X