Dell Data Protection

Konfigurationsleitfaden

2014-02

Inhalt

1

Compatibility Server konfigurieren

In diesem Kapitel sind die Parameter aufgeführt, die Sie ändern können, um den Compatibility Server optimal an Ihre Umgebung anzupassen. Erstellen Sie vor der Bearbeitung von Konfigurationsdateien eine Sicherungskopie.

Ändern Sie nur dokumentierte Parameter in dieser Datei. Wenn Sie andere Daten in dieser Datei ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. Dell kann nicht gewährleisten, dass sich Probleme als Folge nicht autorisierter Änderungen an diesen Dateien ohne Neuinstallation des Compatibility Servers beheben lassen.

server_config.xml

Einige der folgenden Parameter können in **<Compatibility Server install dir>\conf\server_config.xml** geändert werden. Parameter, die unverändert bleiben sollten, sind entsprechend gekennzeichnet. Wenn der Compatibility Server ausgeführt wird, müssen Sie den Compatibility Server Service beenden, die Datei „server_config.xml“ bearbeiten und dann den Compatibility Server Service neu starten, damit die Änderungen an dieser Datei in Kraft treten.

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
secrets.location	$dell.home$/conf/secretKeyStore	Standardspeicherort der Datei „secretkeystore“. Wenn Sie den Speicherort dieser Datei ändern, müssen Sie diesen Parameter entsprechend aktualisieren.
archive.location	$dell.home$/conf/archive	Standardspeicherort des Archivs. Wenn Sie den Speicherort dieser Datei ändern, müssen Sie diesen Parameter entsprechend aktualisieren.
domain.qualified.authentication	true	Gibt an, ob ein vollständiger Benutzeranmeldename für sämtliche an den Server gerichteten Anfragen erforderlich ist. Bei Änderung dieses Werts muss der Device Server neu gestartet werden, damit der neue Wert in Kraft treten kann.
directory.max.search.size	1000	Grenzwert für einen *Verzeichnissuchvorgang*. Bei Überschreitung des Werts wird eine Ausnahme ausgelöst.
directory.server.search.timeout.seconds	60	Server-Zeitüberschreitung in Sekunden für LDAP-Suchvorgänge.
directory.client.search.timeout	60	Client-Zeitüberschreitung in Sekunden für LDAP-Suchvorgänge.

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
rmi.recovery.host		So wird EMS-Wiederherstellung für mehrere Server eingesetzt: <!-- – Entfernen Sie die Kommentarmarkierung und ändern Sie die Hostnamen zu Ihren vollständigen Domänennamen für die Kettenwiederherstellung <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	Standardname der Gruppe, der alle Richtlinien-Proxys standardmäßig angehören. Sie können diesen Namen hier oder in der Device Server-Datei „context.properties“ ändern. Sollten Sie den Gruppennamen hier ändern, müssen Sie ihn im Device Server ebenfalls anpassen, falls Sie Folgendes beabsichtigen: • Windows-Geräte mit Shield schützen • CREDActivate verwenden Es empfiehlt sich, alle Richtlinien-Proxys in einer einzigen Gruppe unterzubringen.
rsa.securid.enabled	False	Falls Sie RSA SecurID für Microsoft Windows Version 6 als GINA-Ersatz verwenden, setzen Sie diesen Parameter auf „false“. Beenden Sie anschließend den Compatibility Server Service und starten Sie ihn erneut. Wenn Shield-Benutzer eine Aktivierung in einer RSA-GINA-Ersatzumgebung vornehmen, wird die LDAP-Authentifizierung durch die RSA-Authentifizierung ersetzt.
inv.queue.task.worker.size	10	Anzahl der Threads, die die Bestandswarteschlange verarbeiten.
inv.queue.task.timeout.seconds	900	Anzahl der Sekunden, bevor eine Zeitüberschreitung auftritt.
inv.queue.task.retry.count	3	Anzahl der Versuche, die der Server zur Verarbeitung des Bestands unternimmt, bevor dieser verworfen wird.
report.retry.max	120	Maximale Anzahl der Wiederholungsversuche.
report.retry.wait.millis	250	Anzahl der Millisekunden, die vor Wiederholungsversuchen gewartet wird.
triage.execute.time	0 0 0/6 * *	Bei der Triage werden die Benutzer und Gruppen, die der Server bereits kennt, abgeglichen. Die Standardeinstellung ist 0 0 0/6 * * ?, was bedeutet, dass die Triage ab Mitternacht alle sechs Stunden erfolgt (0.00 Uhr, 6.00 Uhr, 12.00 Uhr, 18.00 Uhr, 0.00 Uhr...).

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
gatekeeper.service.max.sessions	5	Maximale Anzahl der Richtlinien-Proxy-Sitzungen.
gatekeeper.service.max.session.timeout	5	Zeitüberschreitung für die maximale Anzahl der Richtlinien-Proxy-Sitzungen.
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	Rolle, die zur Aktualisierung von Gruppen- oder Benutzeradministratorrollen erforderlich ist.
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	Rolle, die zur Aktualisierung von Gruppen- oder Benutzeradministratorrollen erforderlich ist
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin,LogAdmin	Rollen, die zum Abrufen von Protokollsitzungen erforderlich sind.
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin,LogAdmin	Rollen, die zum Abrufen von Protokollen erforderlich sind.
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin,LogAdmin	Rollen, die zum Abrufen der Protokollspaltenliste erforderlich sind.
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin,LogAdmin	Rollen, die zum Abrufen der Protokollkategorieliste erforderlich sind.
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin,LogAdmin	Rollen, die zum Abrufen der Protokollprioritätenliste erforderlich sind.
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin,SecAdmin,HelpDeskAdmin,SystemAdmin	Rollen, die zum Abrufen der Namen eindeutiger IDs erforderlich sind.
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	Rolle, die zum Abrufen der Liste von Administratoren im System erforderlich ist.
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	Rolle, die zum Festlegen des Superadmin-Passworts erforderlich ist.
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	Rolle, die zum Zurücksetzen des Superadmin-Passworts erforderlich ist.
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin,SecAdmin	Rollen, die zum Hinzufügen von Domänen erforderlich sind.
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin,SecAdmin	Rollen, die zum Entfernen von Domänen erforderlich sind.
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin,SecAdmin	Rollen, die zum Aktualisieren von Domänen erforderlich sind.
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin,SecAdmin	Rollen, die zum Hinzufügen von Gruppen erforderlich sind.
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin,SecAdmin	Rollen, die zum Entfernen von Gruppen erforderlich sind.
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin,SecAdmin	Rollen, die zum Suchen nach LDAP-Gruppen erforderlich sind.
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin,SecAdmin	Rollen, die zum Suchen nach LDAP-Benutzern erforderlich sind.
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin,SecAdmin	Rollen, die zum Hinzufügen von Benutzern erforderlich sind.

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	Rolle, die zum Hinzufügen von Enterprise-Lizenzen erforderlich ist.
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	Rolle, die zum Anzeigen der Enterprise-Lizenz erforderlich ist.
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin,SecAdmin	Rollen, die zum Wiederherstellen eines Geräts erforderlich sind.
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin,SecAdmin	Rollen, die zum Sperren von Benutzern erforderlich sind.
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	Rollen, die zum Aktivieren von Geräten nach Proxy erforderlich sind.
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin,SecAdmin	Rollen, die zum manuellen Wiederherstellen eines Geräts nach Proxy erforderlich sind.
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Rolle, die zum Abrufen der Gatekeeper-Ressourcendatei erforderlich ist.
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Rolle, die zum Genehmigen der Gatekeeper-Ressourcendatei erforderlich ist.
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Rollen, die zum Genehmigen der Gatekeeper-Konfiguration erforderlich sind.
policy.arbiter.security.mode	most-restrictive	Diese Eigenschaft regelt den Algorithmus zur Richtlinienzuordnung für Richtlinienelemente, die bei Richtlinien mit mehreren übergeordneten Knoten sicherheitsrelevant sind. Werte: Least-restrictive: Der am wenigsten restriktive Elementwert aller übergeordneten Knoten wird verwendet Most-restrictive: Der restriktivste Elementwert aller übergeordneten Knoten wird verwendet
policy.set.synchronization.sync-unmodified	true	Dieses Flag gibt an, dass die nächste externe Synchronisierung alle Richtlinienelemente hinzufügen oder neu zuordnen soll, ohne das modified-Flag auf „true“ zu setzen. Dieses Flag wird nach jeder Synchronisierung auf „false“ umgeschaltet, sodass es zurückgesetzt werden muss, falls der Sicherheitsadministrator die Hinzufügung ohne Änderungen vornehmen möchte. Hierbei handelt es sich um eine erweiterte Option.
db.schema.version.major		Hauptdatenbankschema.
db.schema.version.minor		Untergeordnetes Datenbankschema.
db.schema.version.patch		Patchversion des Datenbankschemas.
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	Standardspeicherort des Datenbanktreibers. Wenn Sie den Speicherort dieser Datei ändern, müssen Sie diesen Parameter entsprechend aktualisieren.
dao.db.host		Hostname des Datenbankservers. Dieser Parameter wird im Konfigurationstool geändert.

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
dao.db.name		Name der Datenbank. Dieser Parameter wird im Konfigurationstool geändert.
dao.db.user		Benutzername mit sämtlichen Berechtigungen für die Datenbank. Dieser Parameter wird im Konfigurationstool geändert.
dao.db.password		Passwort für den Benutzernamen mit sämtlichen Berechtigungen für die Datenbank. Dieser Parameter wird im Konfigurationstool geändert.
dao.db.max.retry.count	10	Maximale Anzahl der Versuche, die der Compatibility Server unternimmt, um die Verbindung mit dem SQL Server nach einem angegebenen Socketfehler wiederherzustellen.
dao.db.connection.retry.wait.seconds	5	Der erste Versuch zur Wiederherstellung der Verbindung erfolgt sofort. Der zweite wird nach der angegebenen Anzahl von Sekunden unternommen. Der dritte erfolgt nach der doppelten Anzahl von angegebenen Sekunden, der vierte nach der dreifachen Anzahl und so weiter.
dao.connection.pool.max.uses	10000	Ermöglicht das Beenden von Verbindungen. 0 bedeutet nicht beenden.
dao.connection.pool.inactive.threshold.seconds	900	Wird verwendet, um zu bestimmen, ob eine Verbindung nicht mehr in Verwendung ist und geschlossen werden kann.
dao.db.driver.socket.errors	0	Der Compatibility Server versucht, die Verbindung mit dem SQL Server bei Fehlern wiederherzustellen, die den Codes in dieser Liste mit Kommatrennzeichen entsprechen. 0 ist der Fehlercode für Socketfehler in Bezug auf Microsoft SQL. Sie können auch 17142 für Fehler in Bezug auf Serverunterbrechungen und 6002 für Fehler in Bezug auf heruntergefahrene Server hinzufügen.
dao.db.mssql.compatability.level	90	Wert für SQL 2005 oder höher.
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	Autorisierungsdateihandler.
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	Bestandsdateihandler.
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	Ereignisdateihandler.
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Aktualisieren Sie diesen Parameter, wenn Sie die Gatekeeper-Ressourcendatei aus dem Standardspeicherort verschieben.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Aktualisieren Sie diesen Parameter, wenn Sie die Gatekeeper-Ressourcendatei aus dem Standardspeicherort verschieben.

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
rmi.server.registry.host	localhost	Der einzige Zweck der Hosteigenschaft besteht darin, dass Clientprogramme bestimmen können, wo sich die Registrierung befindet. Sie kommt während der Erstellung der RMI-Registrierung und von Remoteobjekten nicht zum Einsatz. Wird in localhost erstellt.
rmi.server.registry.port	1099	Der RMI-Registrierungsport kann während der Installation konfiguriert werden. Sie können den Port auch nach der Installation mithilfe dieses Parameters ändern. Wenn Sie diesen Wert ändern, müssen Sie auch die Gatekeeper Web Services konfigurieren.
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Festlegen der Autorisierung für Serverberichte erforderlich sind.
security.authorization.method.IReportingService.removeEntity	SystemAdmin	Rolle, die zum Entfernen von Serverobjekten erforderlich ist.
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	Rolle, die zum Festlegen der Sichtbarkeit von Serverobjekten erforderlich ist.
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen der Gerätedetailseite erforderlich sind.
security.authorization.method.IReportingService.openSession	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Öffnen einer Serversitzung erforderlich sind.
security.authorization.method.IReportingService.getPagedReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Seitenberichts erforderlich sind.
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Gerätetypberichts erforderlich sind.
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Betriebssystemberichts erforderlich sind.
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Gerätemodellberichts erforderlich sind.
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Richtlinien-Detailberichts erforderlich sind.
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Workstation-Detailberichts erforderlich sind.
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Verschlüsselungsfehlerberichts erforderlich sind.
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Verschlüsselungsübersichtsberichts erforderlich sind.
security.authorization.method.IReportingService.getUserDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Benutzerdetailberichts erforderlich sind.
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen des Gruppendetailberichts erforderlich sind.
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Rollen, die zum Anzeigen der Liste der Domänenberichte erforderlich sind.

server_config.xml		
Parameter	**Standardeinstellung**	**Erläuterung**
security.authorization.method.IKeyService.getKeys	ForensicAdmin	Diese Einstellung wird mit einem forensischen Integrationsplugin verwendet. Wenden Sie sich an den Dell-Support, wenn die Integration eines forensischen Tools benötigt wird.
accountType.nonActiveDirectory.aktiviert	False	Das Zulassen von Nicht-Domänen-Aktivierungen ist eine erweiterte Konfiguration mit weitreichenden Konsequenzen. Wenden Sie sich *VOR* dem Durchführen dieser Maßnahme an den Kundensupport, um die spezifischen Anforderungen Ihrer Umgebung zu besprechen. Starten Sie den Compatibility Server Service nach der Änderung dieses Werts neu. Erstellen oder ändern Sie die Registrierungseinstellungen des Windows-Computers zusätzlich zu dieser Einstellung wie folgt: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations=REG_DWORD:1

gkresource.xml

Die Parameter in <Compatibility Server-Installationsverzeichnis>\conf\gkresource.xml können geändert werden.
Es empfiehlt sich, die Änderungen in Form von Kommentaren am Anfang der Datei festzuhalten. So können Sie die Änderungen bei einem Upgrade schnell in die neue Datei übertragen.

HINWEIS: Die Datei „gkresource.xml“ muss ein gültiges XML-Format aufweisen. Wenn Sie mit XML nicht vertraut sind, sollten Sie diese Datei nicht bearbeiten. Stellen Sie sicher, dass Sie gegebenenfalls Objektverweise anstatt von (nicht durch Escapezeichen geschützten) Sonderzeichen verwenden.

Die Änderungen an der Gatekeeper-Ressourcendatei müssen vor Inkrafttreten durch einen Systemadministrator genehmigt werden.

Format „Domäne\Benutzername“ aktivieren

Fügen Sie die folgende Zeichenfolge hinzu, um das Format „Domäne\Benutzername“ zu aktivieren (oder zu deaktivieren). Das Format ist deaktiviert, wenn die Zeichenfolge in der Datei nicht vorkommt. Sie können das Format auch durch Festlegen des Werts auf 0 deaktivieren.

1. Wechseln Sie zu <Compatibility Server-Installationsverzeichnis>\conf.
2. Öffnen Sie die Datei „gkresource.xml“ mit einem XML-Editor.
3. Fügen Sie folgende Zeichenfolge hinzu:
   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. Speichern und schließen Sie die Datei.

run-service.conf

Einige der folgenden Parameter können in **<Compatibility Server-Installationsverzeichnis>\conf\run-service.conf** geändert werden. Diese Parameter werden bei der Installation automatisch festgelegt. So passen Sie Dienste an bzw. nehmen daran Konfigurationsänderungen vor:

1. Beenden Sie den Dienst.
2. Entfernen Sie den Dienst.
3. Bearbeiten und speichern Sie die Datei **run-service.conf**. Es empfiehlt sich, die Änderungen in Form von Kommentaren am Anfang der Datei festzuhalten.
4. Installieren Sie den Dienst neu.
5. Starten Sie den Dienst.

run-service.conf

Parameter	Standardeinstellung	Erläuterung
JAVA_HOME	Dell\Java Runtime\jreX.x	Speicherort des Java-Installationsverzeichnisses.
wrapper.java.additional.5	k.A.	Die MAC-Adresse in dieser Zeile ist die MAC-Adresse des lokalen Ethernet-Adapters. Wenn ein Server über mehrere NICs verfügt oder Sie eine Bindung zu einem anderen Adapter als dem primären Adapter wünschen, geben Sie die MAC-Adresse der NIC hier ohne Bindestriche ein.
wrapper.ntservice.name	EpmCompatSvr	Name des Diensts.
wrapper.ntservice.displayname	Dell Compatibility Server	Anzeigename des Diensts.
wrapper.ntservice.description	Enterprise Compatibility Server	Beschreibung des Diensts.
wrapper.ntservice.dependency.1		Dienst-Dependencys. Fügen Sie Dependencys bei Bedarf hinzu und beginnen Sie bei 1.
wrapper.ntservice.starttype	AUTO_START	Modus, in dem der Dienst installiert wurde: AUTO_START oder DEMAND_START.
wrapper.ntservice.interactive	False	Mit der Einstellung „true“ lassen Sie zu, dass der Dienst mit dem Desktop interagiert.

2

Core Server konfigurieren

In diesem Kapitel sind die Parameter aufgeführt, die Sie ändern können, um den Core Server optimal an Ihre Umgebung anzupassen.

Ändern Sie nur dokumentierte Parameter in dieser Datei. Wenn Sie andere Daten in dieser Datei ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. Dell kann nicht gewährleisten, dass sich Probleme als Folge nicht autorisierter Änderungen an dieser Datei ohne Neuinstallation des Core Servers beheben lassen.

Richtlinienvermittlung von der höchsten Sicherheitsstufe in die niedrigste Sicherheitsstufe ändern

PolicyService.config

Passen Sie diese Einstellung an, um die Richtlinienvermittlung von der höchsten Sicherheitsstufe in die niedrigste Sicherheitsstufe zu ändern. Ändern Sie die Einstellung in **<Core Server-Installationsverzeichnis>\PolicyService.config**. Falls der Core Server ausgeführt wird, müssen Sie den Dienst beenden, die Datei „PolicyService.config“ bearbeiten und dann den Dienst neu starten, damit die Änderungen an dieser Datei in Kraft treten.

Es empfiehlt sich, die Änderungen in Form von Kommentaren am Anfang der Datei festzuhalten. So können Sie die Änderungen bei einem Upgrade schnell in die neue Datei „PolicyServiceConfig.xml“ übertragen.

Ändern Sie den folgenden Abschnitt:

```
<!-- 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" /> [Ändern Sie diesen Wert von „0“ in „1“, um ihn auf die niedrigste Sicherheitsstufe zu setzen.]
</object>
```

Web Services deaktivieren

HINWEIS: Es handelt sich hierbei um erweiterte Einstellungen, die nur unter Anleitung des Kundensupports geändert werden sollten.

Ändern Sie zur Deaktivierung der Web Services auf dem Core Server (wenn es z. B. eine zweite Core Server-Installation nur für die Bestandsverarbeitung gibt) die Einstellungen in:

<Core Server-Installationsverzeichnis>

Credant.Server2.WindowsService.exe.Config

und

<Core Server-Installationsverzeichnis>\Spring.config

Falls der Core Server ausgeführt wird, müssen Sie den Dienst beenden, die Einstellungen in diesen beiden Dateien bearbeiten und dann den Dienst neu starten, damit die Änderungen an diesen Dateien in Kraft treten.

Credant.Server2.WindowsService.exe.Config

Entfernen Sie den folgenden Abschnitt:

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

Spring.config

Entfernen Sie Folgendes:

Entfernen Sie alle <object> </object>-Definitionen unter den Überschriften **AOP Advice**, **Web Service Target Definition** und **Web Service Host Definition**.

SMTP-Server für Lizenz-E-Mail-Benachrichtigungen aktivieren

Bei Verwendung von Dell Data Protection | Cloud Edition werden diese Einstellungen über das Serverkonfigurationstool automatisch vorgenommen. Verwenden Sie dieses Verfahren daher nur, wenn Sie den SMTP-Server für Lizenz-E-Mail-Benachrichtigungen außerhalb von Dell Data Protection | Cloud Edition aktivieren.

NotificationObjects.config

Wenn Sie Ihren SMTP-Server für Lizenz-E-Mail-Benachrichtigungen konfigurieren möchten, ändern Sie die Datei **NotificationObjects.config** unter **<Core Server-Installationsverzeichnis>**.

Ändern Sie Folgendes:

```
<object name="EmailNotification" singleton="false" type="Credant.Notification.EmailNotification,
Credant.Notification"> [Ändern Sie diesen Wert nicht.]
  <property name="NotificationDataFactory" ref="NotificationDataFactory"/> [Ändern Sie diesen Wert nicht.]
  <property name="Host" value="test.dell.com"/>
  <property name="Port" value="25"/>
  <property name="Username" value="Benutzername"/>
  <property name="Password" value="${SmtpPassword}"/> [Ändern Sie diesen Wert nicht.]
  <property name="Logger" ref="NotificationLogger"/> [Ändern Sie diesen Wert nicht.]
</object>
```

Notification.config

Falls für Ihren E-Mail-Server eine Authentifizierung benötigt wird, ändern Sie die Datei **Notification.config** unter **<Core Server-Installationsverzeichnis>**.

Ändern Sie Folgendes:

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

Verzeichnis des Compatibility Servers zur Core Server-Konfigurationsdatei hinzufügen

Weil es sich beim Core Server um eine .NET-Anwendung handelt, kann aufgrund der Berechtigungen der Zugriff auf Registrierungsinformationen gesperrt sein. Der Core Server benötigt zum Lesen des secretkeystore (des Datenbank-Verschlüsselungsschlüssels) Zugriff auf die Registrierungsinformationen des Compatibility Servers, die den Speicherpfad des secretkeystore enthalten. Wird dieser Zugriff aufgrund der Registrierungsberechtigungen gesperrt, kann der Core Server die Console-Benutzer nicht authentifizieren. Mit dieser Einstellung wird das Verzeichnis des Compatibility Servers zur Konfigurationsdatei des Core Servers hinzugefügt, um Probleme mit dem Registrierungszugriff zu vermeiden.

1. Navigieren Sie zu <Core Server-Installationsverzeichnis>\EntityDataAccessObjects.config.
2. Ändern Sie die **fettgedruckten** Einträge:

   <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"/> --> *Entfernen Sie die Kommentarmarkierung und geben Sie den vollständigen Pfad zum Compatibility Server ein.*

   </object>
3. Speichern und schließen Sie die Datei.
4. Starten Sie den Core Server und die Compatibility Server Services neu.

Core Server die Ausführung der Authentifizierungsverfahren gestatten

Die Authentifizierungsversuche des Core Servers werden u. U. durch den Domänencontroller gesperrt, wenn Richtlinien für die zulässigen Authentifizierungsverfahren gelten. Damit sollte ein „Schalter“ in der Konfigurationsdatei des Core Servers implementiert werden, der dem Core Server die Ausführung mehrerer Authentifizierungsverfahren gestattet, um das richtige zu finden.

1. Navigieren Sie zu <Core Server-Installationsverzeichnis>\Spring.config.
2. Ändern Sie die **fettgedruckten** Einträge:

   <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" /> *Setzen Sie diesen Wert auf „true“, um diese Funktion zu aktivieren.*

   <!-- Zur domänenspezifischen Änderung des AuthType: Der Schlüssel ist die CID der Domäne, der Wert ist der unter System.DirectoryServices.AuthenticationTypes

   <property name="DomainAuthType">

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

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

   </dictionary>

   </property>

   -->

   </object>
3. Speichern und schließen Sie die Datei.
4. Führen Sie einen Neustart des Core Server Service durch.

3

Device Server konfigurieren

In diesem Kapitel sind die Parameter aufgeführt, die Sie ändern können, um den Device Server optimal an Ihre Umgebung anzupassen.

Ändern Sie nur dokumentierte Parameter in dieser Datei. Wenn Sie andere Daten in dieser Datei ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. Dell kann nicht gewährleisten, dass sich Probleme als Folge nicht autorisierter Änderungen an dieser Datei ohne Neuinstallation des Device Servers beheben lassen.

eserver.properties

Die folgenden Parameter in **<Device Server-Installationsverzeichnis>\conf\eserver.properties** können geändert werden.

Es empfiehlt sich, die Änderungen in Form von Kommentaren am Anfang der Datei festzuhalten. So können Sie die Änderungen bei einem Upgrade schnell in die neue Datei übertragen.

eserver.properties		
Parameter	**Standardeinstellung**	**Erläuterung**
eserver.default.host	Device Server Service	Der vollständige Domänenname des Installationsspeicherorts des Device Server Service.
eserver.default.port	Versionen ab Enterprise Server v7.7 – 8443 Ältere Versionen als Enterprise Server v7.7 – 8081	Port, der vom Device Server auf eingehende Aktivierungsanfragen von Geräten abgehört wird.
eserver.use.ssl	True	SSL ist standardmäßig aktiviert. Um SSL zu deaktivieren, ändern Sie diesen Parameter in „False“.
eserver.keystore.location	${context['server.home']}/conf/cacerts	Speicherort des SSL-Zertifikats, das vom Device Server verwendet wird.
eserver.keystore.password	changeit	Wenn Sie das Cacerts-Passwort im Konfigurationstool ändern, wird dieser Parameter entsprechend aktualisiert. Sollten Sie Cacerts im Konfigurationstool zu einem Zeitpunkt nach der Erstkonfiguration ändern, müssen Sie diesen Parameter mit dem verwendeten Keystore-Passwort aktualisieren.

eserver.properties		
Parameter	**Standardeinstellung**	**Erläuterung**
eserver.ciphers		Legt die Liste der Verschlüsselungschiffren fest. Die einzelnen Chiffren sollten durch Kommas getrennt werden. Bleibt die Zeile leer, lässt das Socket jede verfügbare Chiffre zu, die von Tomcat unterstützt wird. Entfernen Sie die Kommentarmarkierung im Beispiel unten, um die Liste der Verschlüsselungschiffren festzulegen. Trennen Sie die einzelnen Chiffren durch Kommas. Eine Liste der gültigen Namen von Chiffresammlungen finden Sie im JSSE-Referenzhandbuch von Sun. #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

Einige der folgenden Parameter können in **<Device Server-Installationsverzeichnis>\conf\run-service.conf** geändert werden. Diese Parameter werden bei der Installation automatisch festgelegt. So passen Sie Dienste an bzw. nehmen daran Konfigurationsänderungen vor:

1. Beenden Sie den Dienst.
2. Entfernen Sie den Dienst.
3. Bearbeiten und speichern Sie die Datei **run-service.conf**. Es empfiehlt sich, die Änderungen in Form von Kommentaren am Anfang der Datei festzuhalten.
4. Installieren Sie den Dienst neu.
5. Starten Sie den Dienst.

run-service.conf		
Parameter	**Standardeinstellung**	**Erläuterung**
JAVA_HOME	Dell\Java Runtime\jreX.x	Speicherort des Java-Installationsverzeichnisses.
wrapper.ntservice.name	EpmDeviceSvr	Name des Diensts.
wrapper.ntservice.displayname	Dell Device Server	Anzeigename des Diensts.
wrapper.ntservice.description	Enterprise Device Server	Beschreibung des Diensts.
wrapper.ntservice.dependency.1		Dienst-Dependencys. Fügen Sie Dependencys bei Bedarf hinzu und beginnen Sie bei 1.
wrapper.ntservice.starttype	AUTO_START	Modus, in dem der Dienst installiert wurde: AUTO_START oder DEMAND_START.
wrapper.ntservice.interactive	False	Mit der Einstellung „true“ lassen Sie zu, dass der Dienst mit dem Desktop interagiert.

4

Security Server konfigurieren

In diesem Kapitel sind die Parameter aufgeführt, die Sie ändern können, um den Security Server optimal an Ihre Umgebung anzupassen.

Ändern Sie nur dokumentierte Parameter in dieser Datei. Wenn Sie andere Daten in dieser Datei ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. Dell kann nicht gewährleisten, dass sich Probleme als Folge nicht autorisierter Änderungen an diesen Dateien ohne Neuinstallation des Security Servers beheben lassen.

context.properties

Die folgenden Parameter in **<Security Server-Installationsverzeichnis>\webapps\xapi\WEB-INF\context.properties** können geändert werden.

Es empfiehlt sich, die Änderungen in Form von Kommentaren am Anfang der Datei festzuhalten. So können Sie die Änderungen bei einem Upgrade schnell in die neue Datei übertragen.

context.properties		
Parameter	**Standardeinstellung**	**Erläuterung**
default.gatekeeper.group.remote	CMGREMOTE	Gruppenname der Remote-Gruppe. **Nehmen Sie daran keine Änderung vor.**
xmlrpc.max.threads	250	Maximale Anzahl der gleichzeitigen Threads in diesem Device Server.
default.auth.upn.suffix		UPN-Suffix, das an einen Benutzeranmeldenamen angehängt wird, falls der Server einen vollständigen Anmeldenamen benötigt und dieser in der Anfrage nicht bereitgestellt wird.
device.manual.auth.enable	true	Gibt an, ob manuelle Authentifizierungen aktiviert oder deaktiviert sind. **Nehmen Sie daran keine Änderung vor.**
service.activation.enable	true	Gibt an, ob Aktivierungen vom Device Server bearbeitet werden. **Nehmen Sie daran keine Änderung vor.**
service.policy.enable	true	Gibt an, ob die Richtlinie aktiviert oder deaktiviert ist. **Nehmen Sie daran keine Änderung vor**.
service.auth.enable	true	Gibt an, ob Authentifizierungen vom Device Server bearbeitet werden.
service.forensic.enable	true	Diese Einstellung wird mit einem forensischen Integrationsplugin verwendet. Wenden Sie sich an den Dell-Support, wenn die Integration eines forensischen Tools benötigt wird.

context.properties		
Parameter	**Standardeinstellung**	**Erläuterung**
service.support.enable	true	Aktiviert den Abruf von Metainformationen über den Server.
service.device.enable	true	Aktiviert die Unterstützung von Shield-Diensten wie die SDE-Schlüsselspeicherung.

5

Verschlüsselungsfunktionen konfigurieren

In diesem Abschnitt wird beschrieben, wie Verschlüsselungsfunktionen eigenständig geregelt werden.

Löschen temporärer Dateien verhindern

Standardmäßig werden alle temporären Dateien im Verzeichnis c:\windows\temp bei Installation/Upgrade von DDPE automatisch gelöscht. Durch das Löschen der temporären Dateien vor der ersten Verschlüsselungssuche wird die Verschlüsselungsdauer verkürzt.

Wenn Ihre Organisation jedoch eine Drittanbieter-Anwendung einsetzt, die auf die Dateistruktur im Verzeichnis \Temp angewiesen ist, sollten Sie das Löschen verhindern.

Durch die Erstellung oder Änderung des folgenden Registrierungseintrags können Sie das Löschen temporärer Dateien verhindern:

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

Werden temporäre Dateien **nicht** gelöscht, verlängert sich die Verschlüsselungsdauer.

Overlay-Symbole ausblenden

Standardmäßig werden bei der Installation alle Verschlüsselungs-Overlay-Symbole angezeigt. Verwenden Sie die folgenden Registrierungseinstellungen, um die Verschlüsselungs-Overlay-Symbole für alle verwalteten Benutzer nach der ursprünglichen Installation auf einem Computer auszublenden.

Erstellen oder ändern Sie die Registrierungseinstellungen wie folgt:

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)=1

Wenn ein Benutzer (mit der entsprechenden Berechtigung) die Verschlüsselungs-Overlay-Symbole anzeigen möchte, wird dieser Registrierungswert durch die neue Einstellung aufgehoben.

Taskleistensymbol ausblenden

Standardmäßig wird das Taskleistensymbol während der Installation angezeigt. Verwenden Sie die folgenden Registrierungseinstellungen , um das Taskleistensymbol für alle verwalteten Benutzer nach der ursprünglichen Installation auf einem Computer auszublenden.

Erstellen oder ändern Sie die Registrierungseinstellungen wie folgt:

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)=1

Aktivierung mit Zeitfenster

Die Aktivierung mit Zeitfenster ist eine Funktion, mit der Sie Aktivierungen von Shield über einen vorgegebenen Zeitraum verteilen können, um während einer Massenimplementierung eine Serverüberlastung zu vermeiden. Aktivierungen werden basierend auf Zeitfenstern verzögert, die durch Algorithmen generiert werden, um eine gleichmäßige Verteilung der Aktivierungszeiten zu erreichen.

Die Aktivierung und Konfiguration der Aktivierung mit Zeitfenster erfolgt über das Shield-Installationsprogramm oder die Shield-Workstation.

Für Benutzer, die eine Aktivierung durch VPN benötigen, kann eine Aktivierungskonfiguration mit Zeitfenster erforderlich sein, damit die anfängliche Aktivierung lange genug verzögert wird, um der VPN-Client-Software den Aufbau einer Netzwerkverbindung zu erlauben.

ACHTUNG: Konfigurieren Sie die Aktivierung mit Zeitfenster nur mit Hilfe des Kundensupports. Werden die Zeitfenster falsch konfiguriert, kann möglicherweise eine große Anzahl von Clients gleichzeitig versuchen, sich zu aktivieren, was schwere Leistungseinbußen zur Folge haben kann.

Die folgenden Registrierungsschlüssel werden zur Konfiguration der Aktivierung mit Zeitfenster verwendet. Änderungen an diesen Registrierungsschlüsseln treten erst nach einem Neustart der Shield-Workstation in Kraft.

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

  Mit dieser Einstellung wird die Aktivierung mit Zeitfenster aktiviert oder deaktiviert.
  Deaktiviert = 0 (Standard)
  Aktiviert = 1

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\CalRepeat

  Der Zeitraum in Sekunden, in dem Ihr Aktivierungszeitintervall auftritt. Mit dieser Einstellung überschreiben Sie den Zeitraum in Sekunden, in dem das Aktivierungszeitintervall auftritt. 25200 Sekunden stehen zur Verfügung, um Aktivierungen während eines Zeitraums von sieben Stunden einzuplanen. Die Standardeinstellung ist 86400 Sekunden, was einer täglichen Wiederholung entspricht.

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\SlotIntervals

  Das Intervall innerhalb der Wiederholung, ACTIVATION_SLOT_CALREPEAT, in dem alle Aktivierungszeitfenster auftreten. Es ist nur ein Intervall erlaubt. Diese Einstellung sollte 0,<CalRepeat> sein. Eine Verschiebung von 0 kann zu unerwarteten Ergebnissen führen. Die Standardeinstellung ist 0,86400. Für eine Wiederholung alle sieben Stunden stellen Sie 0,25200 ein. CALREPEAT wird aktiviert, sobald sich ein Shield-Benutzer anmeldet.

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\ActivationSlot\MissThreshold

  Die Anzahl der Aktivierungszeitfenster, die verpasst werden können, bevor der Computer bei der nächsten Anmeldung des Benutzers, dessen Aktivierung eingeplant wurde, eine Aktivierung durchführt. Wenn die Aktivierung während dieses unmittelbaren Versuchs fehlschlägt, nimmt Shield die Aktivierungsversuche mit Zeitfenster wieder auf. Wenn die Aktivierung aufgrund eines Netzwerkfehlers fehlschlägt, wird die Aktivierung bei Wiederherstellung der Netzwerkverbindung erneut versucht, auch wenn der Wert in MISSTHRESHOLD nicht überschritten wurde. Wenn ein Benutzer sich abmeldet, bevor das Aktivierungszeitfenster erreicht ist, wird bei der nächsten Anmeldung ein neues Zeitfenster zugewiesen.

- HKCU/Software/CREDANT/ActivationSlot (Daten pro Benutzer)

  Verzögerungszeit bis zum Versuch der Aktivierung mit Zeitfenster, die eingestellt wird, wenn sich der Benutzer zum ersten Mal beim Netzwerk anmeldet, nachdem die Aktivierung mit Zeitfenster aktiviert wurde. Das Aktivierungszeitfenster wird für jeden Aktivierungsversuch neu berechnet.

- HKCU/Software/CREDANT/SlotAttemptCount (Daten pro Benutzer)

  Anzahl der fehlgeschlagenen oder verpassten Versuche, wenn das Zeitfenster beginnt und ein Aktivierungsversuch gestartet wird, aber fehlschlägt. Wenn diese Anzahl den in ACTIVATION_SLOT_MISSTHRESHOLD festgelegten Wert erreicht, versucht der Computer bei der Verbindung mit dem Netzwerk noch eine einzige Aktivierung.

Um die Aktivierung mit Zeitfenster über die Befehlszeile zu aktivieren, geben Sie einen Befehl wie den folgenden ein:

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

HINWEIS: Stellen Sie sicher, dass ein Wert eingegeben wird, der ein oder mehrere Sonderzeichen, z. B. eine Leerstelle, zwischen in Escape-Zeichen gesetzten Anführungszeichen enthält.

Erzwungene Abfrage

Über die folgende Registrierungseinstellung lässt sich von Shield eine Richtlinienaktualisierung erzwingen.

Erstellen oder ändern Sie die Registrierungseinstellungen wie folgt:

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD-Wert) = 1

Je nach der Shield-Version werden die Registrierungseinstellungen entweder automatisch geschlossen *oder* sie ändern sich nach der Abfrage von **1** auf **0**.

Je nach den Zugriffsrechten des Administrators kann für die Erstellung dieser Registrierungseinstellungen eine Änderung der Zugriffsrechte erforderlich sein. Falls beim Versuch, ein neues DWORD zu erstellen, Probleme auftreten, befolgen Sie die nachstehenden Schritte, um die Zugriffsrechte zu ändern.

1. Gehen Sie in der Windows-Registrierung zu HKLM\SOFTWARE\Credant\CMGShield\Notify.
2. Klicken Sie mit der rechten Maustaste auf **Benachrichtigen** > **Berechtigungen**.
3. Wählen Sie im *Berechtigungsfenster für die Benachrichtigungen* das Kontrollkästchen für den **Vollzugriff** aus.
4. Klicken Sie auf **OK**.

Jetzt können Sie Ihre neuen Registrierungseinstellungen vornehmen.

Bestandsoptionen

Verwenden Sie die folgenden Registrierungseinstellungen, um Shield das Senden optimierter Bestandsinformationen an den Server, das Senden vollständiger Bestandsinformationen an den Server oder das Senden vollständiger Bestandsinformationen an den Server für alle aktivierten Benutzer zu ermöglichen.

Senden optimierter Bestandsinformationen an den Server

Erstellen oder ändern Sie die Registrierungseinstellungen wie folgt:

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

OnlySendInvChanges (REG_DWORD) = 1

Wenn kein Eintrag vorhanden ist, werden optimierte Bestandsinformationen an den Server gesendet.

Senden vollständiger Bestandsinformationen an den Server

Erstellen oder ändern Sie die Registrierungseinstellungen wie folgt:

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

OnlySendInvChanges (REG_DWORD) = 0

Wenn kein Eintrag vorhanden ist, werden optimierte Bestandsinformationen an den Server gesendet.

Senden vollständiger Bestandsinformationen für alle aktivierten Benutzer

Erstellen oder ändern Sie die Registrierungseinstellungen wie folgt:

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

RefreshInventory (REG_DWORD) = 1

Dieser Eintrag wird nach der Verarbeitung aus der Registrierung gelöscht, der Wert wird jedoch gespeichert. Dadurch ist Shield in der Lage, die Anfrage beim nächsten Upload zu erfüllen, selbst wenn der Computer neu gestartet wird, bevor die Bestandsinformationen hochgeladen wurden.

Dieser Eintrag ersetzt den Registrierungswert für OnlySendInvChanges.

Nicht-Domänen-Aktivierungen

Das Zulassen von Nicht-Domänen-Aktivierungen ist eine erweiterte Konfiguration mit weitreichenden Konsequenzen. Wenden Sie sich an den Kundensupport, um die spezifischen Anforderungen Ihrer Umgebung zu besprechen und eine Anleitung zur Aktivierung dieser Funktion zu erhalten.

6

Komponenten für die Kerberos-Authentifizierung/-Autorisierung konfigurieren

In diesem Abschnitt wird beschrieben, wie Komponenten zur Verwendung mit der Kerberos-Authentifizierung/-Autorisierung konfiguriert werden.

Komponenten für die Kerberos-Authentifizierung/-Autorisierung konfigurieren

HINWEIS: Wenn die Kerberos-Authentifizierung/-Autorisierung verwendet werden soll, muss der Server, der die Key Server-Komponente enthält, zur betroffenen Domäne gehören.

Key Server ist ein Dienst, der überwacht, ob Clients eine Verbindung über ein Socket herstellen. Wenn ein Client einen Verbindungsversuch unternimmt, wird mithilfe von Kerberos-APIs eine sichere Verbindung ausgehandelt, authentifiziert und verschlüsselt (wenn keine sichere Verbindung ausgehandelt werden kann, wird die Client-Verbindung getrennt).

Der Key Server überprüft dann auf dem Device Server, ob der Benutzer, der den Client ausführt, auf Schlüssel zugreifen darf. Dieser Zugriff wird in der Remote Management Console über *einzelne* Domänen gewährt.

Anleitungen für das Windows-Dialogfeld „Dienste“

1. Navigieren Sie zum Windows-Dialogfeld „Dienste“ (Start > Ausführen... > services.msc > OK).
2. Klicken Sie mit der rechten Maustaste auf „Dell Key Server“ und wählen Sie Eigenschaften aus.
3. Rufen Sie die Registerkarte Anmelden auf und wählen Sie das Optionsfeld Dieses Konto: aus.
4. Geben Sie in das Feld Dieses Konto: den gewünschten Domänenbenutzer ein. Dieser Domänenbenutzer muss mindestens über lokale Administratorrechte für den Key Server-Ordner verfügen (er muss Schreibzugriff für die Key Server-Konfigurationsdatei und die Datei „log.txt“ besitzen).
5. Klicken Sie auf OK.
6. Starten Sie den Dienst neu (lassen Sie das Windows-Dialogfeld „Dienste“ für weitere Arbeitsschritte geöffnet).
7. Navigieren Sie zu „<Key Server-Installationsverzeichnis> log.txt“, um zu überprüfen, ob der Dienst korrekt gestartet wurde.

Anleitungen für die Key Server-Konfigurationsdatei

1. Navigieren Sie zu <Key Server-Installationsverzeichnis>.
2. Öffnen Sie „Credant.KeyServer.exe.config“ mit einem Texteditor.
3. Gehen Sie zu <add key="user" value="superadmin" /> und ändern Sie den Wert „superadmin“ in den Namen des entsprechenden Benutzers (Sie können auch „superadmin“ stehen lassen).

   Das Format von „superadmin“ kann jede Methode sein, die sich beim Server authentifizieren kann. Der SAM-Kontoname, der UPN oder das Format „Domäne\Benutzername“ sind akzeptabel. Jede Methode, die sich beim Server authentifizieren kann, ist akzeptabel, da für *dieses* Benutzerkonto eine Überprüfung zur Autorisierung bei Active Directory erforderlich ist.

   Beispiel: In einer Umgebung mit mehreren Domänen würde die Eingabe eines SAM-Kontonamens wie „jdoe“ vermutlich fehlschlagen, da der Server „jdoe“ nicht authentifizieren kann, weil er den Namen nicht findet. In einer Umgebung mit mehreren Domänen wird der UPN empfohlen, obwohl das Format „Domäne\Benutzername“ akzeptabel ist.

   In einer Umgebung mit einer Domäne kann der SAM-Kontoname verwendet werden.

4 Gehen Sie zu <add key="epw" value="<verschlüsselter Wert des Passworts>" /> und ändern Sie „epw“ in „password“. Ändern Sie dann „<verschlüsselter Wert des Passworts>“ in das Passwort des Benutzers aus Schritt 3. Beim Neustart des Servers wird dieses Passwort neu verschlüsselt.

Wenn Sie in Schritt 3 „superadmin“ verwendet haben und das Superadmin-Passwort nicht „changeit“ lautet, muss es hier geändert werden.

5 Speichern Sie Ihre Änderungen und schließen Sie die Datei.

Beispielkonfigurationsdatei:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [Der vom Server abgehörte TCP-Port. Die Standardeinstellung ist 8050, die bei Bedarf geändert werden kann.]
        <add key="maxConnections" value="2000" /> Die Anzahl der vom Server zugelassenen Socketverbindungen.]
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [Device Server-URL. Bei Versionen ab Enterprise Server v7.7 gilt das Format https://keyserver.domain.com:8443/xapi/ – bei älteren Versionen als Enterprise Server v7.7 gilt das Format https://keyserver.domain.com:8081/xapi (ohne den folgenden Schrägstrich)].
        <add key="verifyCertificate" value="false" /> [Bei „true“ werden Zertifikate überprüft. Legen Sie „false“ fest, wenn keine Überprüfung erfolgen soll oder selbstsignierte Zertifikate verwendet werden.]
        <add key="user" value="superadmin" /> [Der für die Kommunikation mit dem Device Server verwendete Benutzername. Für diesen Benutzer muss der Typ „Forensischer Administrator“ in der Remote Management Console ausgewählt sein. Das Format von „superadmin“ kann jede Methode sein, die sich beim Server authentifizieren kann. Der SAM-Kontoname, der UPN oder das Format „Domäne\Benutzername“ sind akzeptabel. Jede Methode, die sich beim Server authentifizieren kann, ist akzeptabel, da für dieses Benutzerkonto eine Überprüfung zur Autorisierung bei Active Directory erforderlich ist. Beispiel: In einer Umgebung mit mehreren Domänen würde die Eingabe eines SAM-Kontonamens wie „jdoe“ vermutlich fehlschlagen, da der Server „jdoe“ nicht authentifizieren kann, weil er den Namen nicht findet. In einer Umgebung mit mehreren Domänen wird der UPN empfohlen, obwohl das Format „Domäne\Benutzername“ akzeptabel ist. In einer Umgebung mit einer Domäne kann der SAM-Kontoname verwendet werden.]
        <add key="cacheExpiration" value="30" /> [Wie oft (in Sekunden) der Dienst überprüfen soll, wer Schlüssel abrufen darf. Der Dienst unterhält einen Cache und verfolgt dessen Alter. Wenn der Cache älter ist als der Wert (in Sekunden), erhält er eine neue Liste. Wenn ein Benutzer eine Verbindung herstellt, muss der Key Server autorisierte Benutzer vom Device Server herunterladen. Wenn kein Cache mit diesen Benutzern existiert oder die Liste in den letzten n Sekunden nicht heruntergeladen wurde, wird sie erneut heruntergeladen. Es erfolgt keine Abfrage, doch dieser Wert bestimmt, wie alt die Liste werden kann, bevor sie bei Bedarf aktualisiert wird.]
        <add key="epw" value="encrypted value of the password" /> [Das für die Kommunikation mit dem Device Server verwendete Passwort. Wenn das Superadmin-Passwort geändert wurde, muss es auch hier geändert werden.]
    </appSettings>
</configuration>
```

Anleitungen für das Windows-Dialogfeld „Dienste“

1 Gehen Sie zurück zum Windows-Dialogfeld „Dienste“.

2 Führen Sie einen Neustart des Dell Key Server Service durch.

3 Navigieren Sie zu „<Key Server-Installationsverzeichnis> log.txt“, um zu überprüfen, ob der Dienst korrekt gestartet wurde.

4 Schließen Sie das Windows-Dialogfeld „Dienste“.

Anleitungen für die Remote Management Console

1. Melden Sie sich gegebenenfalls bei der Remote Management Console an.
2. Klicken Sie auf **Domänen** und dann auf das Symbol **Detail**.
3. Klicken Sie auf **Key Server**.
4. Fügen Sie der Key Server-Kontoliste den Benutzer hinzu, der die Administratoraufgaben ausführt. Das Format lautet „Domäne\Benutzername“. Klicken Sie auf **Konto hinzufügen**.
5. Klicken Sie im linken Menü auf **Benutzer**. Geben Sie in das Suchfeld den in Schritt 4 hinzugefügten Benutzernamen ein. Klicken Sie auf **Suchen**.
6. Nachdem der korrekte Benutzer gefunden wurde, klicken Sie auf das Symbol **Detail**.
7. Wählen Sie **Forensischer Administrator** aus. Klicken Sie auf **Aktualisieren**.

Die Komponenten sind nun für die Kerberos-Authentifizierung/-Autorisierung konfiguriert.

7

Forensische Administratorrolle zuweisen

Standardmäßig ist die forensische Autorisierung auf Back-End-Servern aktiviert und auf Front-End-Servern deaktiviert. Diese Einstellungen werden bei der Installation für den Device Server und den Security Server vorgenommen.

Anleitungen für die Remote Management Console

1. Melden Sie sich gegebenenfalls bei der Remote Management Console an.
2. Klicken Sie im linken Bereich auf **Verwalten** > **Benutzer**.
3. Geben Sie auf der Seite *Benutzersuche* den Namen des Benutzers ein, dem die Rolle des forensischen Administrators erteilt werden soll, und klicken Sie auf **Suchen** (die Anmeldeinformationen dieses Benutzers werden während der Ausführung der Dienstprogramme CMGAd, CMGAu und CMGAlu sowie des Decryption Agents im forensischen Modus angegeben).
4. Klicken Sie auf der Seite *Ergebnisse der Benutzersuche* auf das Symbol **Detail**.
5. Wählen Sie auf der Seite *Benutzerdetail für: <Benutzername>* die Option **Administrator** aus.
6. Aktivieren Sie in der Spalte „Benutzer“ die Option **Forensischer Administrator** und klicken Sie auf **Aktualisieren**.

Die forensische Administratorrolle ist nun eingerichtet.

Forensische Autorisierung deaktivieren

1. Gehen Sie auf dem Back-End-Server zu **<Security Server-Installationsverzeichnis>\webapps\xapi\WEB-INF\context.properties** und ändern Sie die folgende Eigenschaft:

   service.forensic.enable=true

   zu

   service.forensic.enable=false
2. Führen Sie einen **Neustart** des Security Server Service durch.
3. Gehen Sie auf dem Back-End-Server zu **<Device Server-Installationsverzeichnis>\webapps\ROOT\WEB-INF\web.xml** und ändern Sie folgende:

   <init-param>

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

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

   </init-param>
4. Führen Sie einen **Neustart** des Device Server Service durch.
5. Es empfiehlt sich, die forensische Administratorrolle von allen Benutzern zu entfernen, die die entsprechenden Berechtigungen nicht aktiv nutzen.

8

Cron-Ausdrücke

In diesem Abschnitt wird beschrieben, wie Cron-Ausdrucksformate und Sonderzeichen verwendet werden.

Einführung in Cron-Ausdrücke

Cron ist ein bewährtes UNIX-Tool, das leistungsstarke Planungsfunktionen bietet. Die CronTrigger-Klasse basiert auf den Planungsfunktionen von Cron.

CronTrigger verwendet Cron-Ausdrücke, mit denen Zeitpläne für die Auslösung von Vorgängen erstellt werden können, beispielsweise um 8.00 Uhr jeden Montag bis Freitag oder um 1.30 Uhr jeden letzten Freitag im Monat.

Cron-Ausdrücke sind leistungsstark, aber manchmal auch verwirrend. Dieses Dokument soll die Erstellung von Cron-Ausdrücken verständlicher machen und Ihnen als Referenz dienen, bevor Sie Hilfe von Dritten in Anspruch nehmen.

Cron-Ausdrucksformate

Cron-Ausdrücke setzen sich aus sechs erforderlichen Feldern und einem optionalen Feld zusammen, die durch Leerzeichen getrennt sind. Die Felder können jeden zulässigen Wert sowie verschiedene Kombinationen der für das Feld zulässigen Sonderzeichen enthalten.

Cron-Ausdrücke können so einfach wie * * * * ? * sein.

Es gibt auch komplexere wie 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010.

Die Felder werden im Folgenden beschrieben.

Feldname	Erforderlich?	Zulässige Werte	Zulässige Sonderzeichen
Minutes	Ja	0–59	, - * /
Hours	Ja	0–23	, - * /
Day of month	Ja	1–31	, - * ? / L W C
Month	Ja	1–12 or JAN–DEC	, - * /
Day of week	Ja	1–7 or SUN–SAT	, - * ? / L C #
Year	Nein	empty, 1970–2099	, - * /

Sonderzeichen

- Mit dem Zeichen * werden alle Werte angegeben. Wenn * beispielsweise im Feld für die Minuten steht, bedeutet dies jede Minute.
- Das Fragezeichen (kein bestimmter Wert) ist nützlich, wenn Sie etwas in einem von zwei Feldern, in denen das Zeichen zulässig ist, angeben möchten, jedoch nicht in dem anderen. Wenn Sie beispielsweise einen Vorgang an einem bestimmten Tag des Monats (dem 10.) auslösen möchten, Ihnen aber egal ist, an welchem Wochentag dies geschieht, geben Sie 10 in das Feld für den Tag des Monats und ? in das Feld für den Wochentag ein.
- Mit dem Zeichen - werden Bereiche angegeben. 10-12 im Feld für die Stunden bedeutet beispielsweise die Stunden 10, 11 und 12.
- Mit dem Zeichen , werden zusätzliche Werte angegeben. MON,WED,FRI im Feld für den Wochentag steht beispielsweise für die Tage Montag, Mittwoch und Freitag.

- Mit dem Zeichen / werden Inkremente angegeben.

  0/15 im Feld für die Sekunden steht für die Sekunden 0, 15, 30 und 45.

  5/15 im Feld für die Sekunden steht für die Sekunden 5, 20, 35 und 50.

  Die Angabe von * vor / entspricht der Angabe von 0 als Startwert.

  1/3 im Feld für den Tag des Monats bedeutet, dass der Vorgang ab dem ersten Tag des Monats alle drei Tage ausgelöst wird.

  Im Grunde gibt es für jedes Feld im Ausdruck eine Reihe von Zahlen, die zur Auslösung des Vorgangs verwendet werden können. Bei Sekunden und Minuten reichen die Zahlen von 0 bis 59, bei Stunden von 0 bis 23, bei den Tagen des Monats von 0 bis 31. Bei Monaten umfasst der Zahlenbereich 1 bis 12. Mit dem Zeichen / können Sie einfach festlegen, dass der Vorgang zu jedem n-ten Wert im jeweiligen Zahlenbereich ausgelöst wird. 7/6 im Feld für den Monat bedeutet daher, dass die Auslösung des Vorgangs im 7. Monat, und nicht alle sechs Monate erfolgt.

- Das Zeichen L ist in den Feldern für den Tag des Monats und den Wochentag zulässig. Dieses Zeichen steht für „letzter“, allerdings hat es in den beiden Feldern eine unterschiedliche Bedeutung.

  Das Zeichen L im Feld für den Tag des Monats steht für den letzten Tag des Monats (31. Januar, 28. Februar in Nicht-Schaltjahren).

  Wenn L allein im Feld für den Wochentag verwendet wird, steht es für 7 oder SAT.

  Folgt L im Feld für den Wochentag auf einen anderen Wert, bedeutet es den letzten Wochentag des Monats. 6L steht beispielsweise für den letzten Freitag im Monat. Bei Verwendung der Option L ist es wichtig, dass keine Listen oder Wertebereiche angegeben werden, da dies zu verwirrenden Ergebnissen führt.

- Das Zeichen W ist im Feld für den Tag des Monats zulässig. Mit diesem Zeichen wird der Werktag (Montag bis Freitag) angegeben, der dem jeweiligen Tag am nächsten liegt. Wenn Sie beispielsweise 15W im Feld für den Tag des Monats angeben, steht dies für den Werktag, der dem 15. des Monats am nächsten liegt. Fällt der 15. also auf einen Samstag, wird der Vorgang am Freitag, dem 14. ausgelöst. Wenn es sich beim 15. um einen Sonntag handelt, erfolgt die Auslösung am Montag, dem 16. Fällt der 15. auf einen Dienstag, wird der Vorgang am Dienstag, dem 15. ausgelöst. Wenn Sie allerdings 1W im Feld für den Tag des Monats angeben und der 1. ein Samstag ist, wird der Vorgang am Montag, dem 3. ausgelöst, da die Auslösung immer im selben Monat erfolgt. Das Zeichen W lässt sich nur angeben, wenn der Tag des Monats ein einzelner Tag ist, kein Bereich bzw. keine Liste von Tagen.

  Die Zeichen L und W können im Ausdruck für den Tag des Monats auch zu LW kombiniert werden, was für den letzten Werktag im Monat steht.

- Das Zeichen # ist im Feld für den Wochentag zulässig. Mit diesem Zeichen wird der n-te jeweilige Tag des Monats angegeben. Wenn Sie beispielsweise 6#3 im Feld für den Wochentag angeben, steht dies für den dritten Freitag des Monats (Tag 6 = Freitag und #3 = der dritte Freitag im Monat).

  Andere Beispiele:
  2#1 = der erste Montag des Monats
  4#5 = der fünfte Mittwoch des Monats.

  Hinweis: Wenn #5 angegeben wird und der jeweilige Wochentag im Monat nicht fünfmal vorkommt, wird der Vorgang in diesem Monat nicht ausgelöst.

- Das Zeichen C ist für Kalender zulässig. Bei Verwendung dieses Zeichens werden Werte auf Basis eines zugeordneten Kalenders (sofern vorhanden) berechnet. Wenn kein Kalender zugeordnet ist, entspricht dies der Verwendung eines allumfassenden Kalenders. Der Wert 5C im Feld für den Tag des Monats steht für den ersten zum Kalender gehörenden Tag am oder nach dem 5. Der Wert 1C im Feld für den Wochentag steht für den ersten zum Kalender gehörenden Tag am oder nach Sonntag.

HINWEIS: Die Angabe eines Werts für den Wochentag sowie für den Tag des Monats wird noch nicht vollständig unterstützt. Verwenden Sie das Fragezeichen in einem dieser Felder. Die Funktionen, die für das Zeichen C beschrieben wurden, werden noch nicht vollständig unterstützt. Bei den zulässigen Zeichen und den Namen von Monaten und Wochentagen muss die Groß-/Kleinschreibung nicht beachtet werden. MON ist gleichbedeutend mit mon. Achten Sie besonders auf die Auswirkung von ? und * in den Feldern für den Tag des Monats und den Wochentag.
Lassen Sie Vorsicht walten, wenn Sie Auslösungszeiten zwischen Mitternacht und 1.00 Uhr festlegen. Die Sommerzeit kann dazu führen, dass die Auslösung eines Vorgangs übersprungen (oder wiederholt) wird, je nachdem, ob die Uhr vor- oder zurückgestellt wird.

Beispiele

Ausdruck	Erläuterung
0 0 12 * * ?	Auslösung um 12.00 Uhr mittags jeden Tag
0 15 10 ? * *	Auslösung um 10.15 Uhr jeden Tag
0 15 10 * * ?	Auslösung um 10.15 Uhr jeden Tag
0 15 10 * * ? *	Auslösung um 10.15 Uhr jeden Tag
0 15 10 * * ? 2005	Auslösung um 10.15 Uhr jeden Tag während des Jahres 2005
0 * 14 * * ?	Auslösung jede Minute, beginnend um 14.00 Uhr und endend um 14.59 Uhr jeden Tag
0 0/5 14 * * ?	Auslösung alle fünf Minuten, beginnend um 14.00 Uhr und endend um 14.55 Uhr jeden Tag
0 0/5 14,18 * * ?	Auslösung alle fünf Minuten, beginnend um 14.00 Uhr und endend um 14.55 Uhr UND Auslösung alle fünf Minuten, beginnend um 18.00 Uhr und endend um 18.55 Uhr jeden Tag
0 0-5 14 * * ?	Auslösung jede Minute, beginnend um 14.00 Uhr und endend um 14.05 Uhr jeden Tag
0 10,44 14 ? 3 WED	Auslösung um 14.10 Uhr und um 14.44 Uhr jeden Mittwoch im Monat März
0 15 10 ? * MON-FRI	Auslösung um 10.15 Uhr jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag
0 15 10 15 * ?	Auslösung um 10.15 Uhr am 15. Tag jedes Monats
0 15 10 L * ?	Auslösung um 10.15 Uhr am letzten Tag jedes Monats
0 15 10 ? * 6L	Auslösung um 10.15 Uhr am letzten Freitag jedes Monats
0 15 10 ? * 6L	Auslösung um 10.15 Uhr am letzten Freitag jedes Monats
0 15 10 ? * 6L 2002-2005	Auslösung um 10.15 Uhr jeden letzten Freitag jeden Monats während der Jahre 2002, 2003, 2004 und 2005
0 15 10 ? * 6#3	Auslösung um 10.15 Uhr am dritten Freitag jedes Monats
0 0 12 1/5 * ?	Auslösung um 12.00 Uhr mittags alle fünf Tage jeden Monat, beginnend am ersten Tag des Monats
0 11 11 11 11 ?	Auslösung an jedem 11. November um 11.11 Uhr

9

Selbstsignierte Zertifikate mit Keytool erstellen und Anfragen zum Signieren von Zertifikaten erstellen

HINWEIS: In diesem Abschnitt werden die Schritte zum Erstellen eines selbstsignierten Zertifikats für die Java-basierten Komponenten beschrieben. Anhand dieses Verfahrens können *keine* selbstsignierten Zertifikate für .NET-basierte Komponenten erstellt werden.

Für Produktionsumgebungen sind selbstsignierte Zertifikate *nicht* zu empfehlen.

Falls Ihre Organisation ein SSL-Serverzertifikat benötigt oder Sie aus anderen Gründen ein Zertifikat erstellen müssen, wird in diesem Abschnitt das Verfahren zum Erstellen eines Java-Keystore mit Keytool beschrieben.

Keytool erstellt private Schlüssel, die im CSR-Format (Certificate Signing Request) an eine Zertifizierungsstelle wie VeriSign® oder Entrust® übertragen werden. Anhand dieser CSR erstellt die Zertifizierungsstelle dann ein Serverzertifikat und signiert es. Danach wird das Serverzertifikat zusammen mit dem Zertifikat der Zertifizierungsstelle in eine Datei heruntergeladen. Anschließend werden die Zertifikate in die cacerts-Datei importiert.

Neue Key-Paare und selbstsignierte Zertifikate erstellen

1. Navigieren Sie zum **conf**-Verzeichnis von Compliance Reporter, Console Web Services, Device Server oder Gatekeeper Web Services.
2. Erstellen Sie eine Sicherungskopie der Standard-Zertifikatsdatenbank:
   Klicken Sie auf **Start** > **Ausführen** und geben Sie **move cacerts cacerts.old** ein.
3. Fügen Sie Keytool in den Systempfad ein. Geben Sie den folgenden Befehl in eine Eingabeaufforderung ein:
   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. Führen Sie zum Erstellen eines Zertifikats Keytool wie folgt aus:
   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Geben Sie nach der entsprechenden Aufforderung in Keytool die folgenden Informationen ein.

HINWEIS: Erstellen Sie vor der Bearbeitung von Konfigurationsdateien eine Sicherungskopie. Ändern Sie nur die angegebenen Parameter. Wenn Sie andere Daten in diesen Dateien ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. Dell kann nicht gewährleisten, dass sich Probleme als Folge nicht autorisierter Änderungen an diesen Dateien ohne Neuinstallation des Enterprise Servers beheben lassen.

- *Keystore-Passwort:* Geben Sie ein Passwort ein (die Zeichen <>;&" ' sind nicht zulässig) und setzen Sie die Variable in der Datei component **conf** auf denselben Wert, wie hier gezeigt:

  <Compliance Reporter-Installationsverzeichnis>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

  <Console Web Services-Installationsverzeichnis>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

  <Device Server-Installationsverzeichnis>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

- *Vor- und Nachname:* Geben Sie den vollständigen Namen des Servers ein, auf dem die Komponente, mit der Sie arbeiten, installiert ist. Zum vollständigen Namen gehören der Hostname und der Domänenname (Beispiel: server.dell.com).
- *Organisationseinheit:* Geben Sie den entsprechenden Wert ein (Beispiel: Sicherheit).
- *Organisation:* Geben Sie den entsprechenden Wert ein (Beispiel: Dell).
- *Ort:* Geben Sie den entsprechenden Wert ein (Beispiel: München).
- *Bundesstaat bzw. Bundesland:* Geben Sie den Namen des Bundesstaats oder -landes ohne Abkürzungen ein (Beispiel: Bayern).
- Zweistelliger Ländercode:

  USA = US

  Kanada = CA

  Schweiz = CH

  Deutschland = DE

  Spanien = ES

  Frankreich = FR

  Großbritannien = GB

  Irland = IE

  Italien= IT

  Niederlande = NL
- Sie müssen im Dienstprogramm bestätigen, dass die Angaben stimmen. Wenn dem so ist, geben Sie `Ja` ein. Wenn nicht, geben Sie `Nein` ein. Keytool zeigt jeden zuvor eingegebenen Wert an. Drücken Sie die **Eingabetaste**, um den Wert zu akzeptieren, oder ändern Sie den Wert und drücken Sie anschließend die **Eingabetaste**.
- *Schlüsselpasswort für Alias:* Wenn Sie hier kein anderes Passwort eingeben, wird automatisch das Keystore-Passwort verwendet.

Signierte Zertifikate von einer Zertifizierungsstelle anfordern

Verwenden Sie dieses Verfahren, um eine Anfrage zum Signieren von Zertifikaten (CSR) für das in Neue Key-Paare und selbstsignierte Zertifikate erstellen erstellte selbstsignierte Zertifikat zu erstellen.

1 Verwenden Sie denselben Wert wie zuvor für <**Zertifikat-Alias**>:

```
keytool -certreq -sigalg MD5withRSA -alias <Zertifikat-Alias> -keystore .\cacerts
-file <CSR-Dateiname>
```

Beispiel:

```
keytool -certreq -sigalg MD5withRSA -alias dell -keystore .\cacerts -file
credant.csr
```

Die .csr-Datei enthält ein BEGIN/END-Paar, das während der Erstellung des Zertifikats bei der Zertifizierungsstelle verwendet wird.

Abbildung 9-1. .csr-Beispieldatei

2 Befolgen Sie Ihr Organisationsverfahren zum Erwerb eines SSL-Serverzertifikats bei einer Zertifizierungsstelle. Senden Sie den Inhalt von <CSR-Dateiname> zum Signieren.

HINWEIS: Es gibt verschiedene Methoden zur Anforderung eines gültigen Zertifikats. Ein **Beispiel** finden Sie unter Beispielmethode zur Anforderung eines Zertifikats.

3 Speichern Sie das signierte Zertifikat nach Erhalt in einer Datei.

4 Wir empfehlen, immer eine Sicherungskopie dieses Zertifikats anzufertigen, falls beim Import ein Fehler auftritt. Die Sicherungskopie verhindert, dass der Vorgang noch einmal von vorn begonnen werden muss.

Stammzertifikate importieren

HINWEIS: Wenn die Zertifizierungsstelle für das Stammzertifikat Verisign (aber nicht Verisign Test) ist, gehen Sie zum nächsten Verfahren weiter und importieren Sie das signierte Zertifikat.

Mit dem Stammzertifikat der Zertifizierungsstelle werden signierte Zertifikate validiert.

1 Führen Sie einen der nachfolgenden Schritte aus:

- Laden Sie das Stammzertifikat der Zertifizierungsstelle herunter und speichern Sie es in einer Datei.
- Rufen Sie das Stammzertifikat vom Unternehmensverzeichnisserver ab.

2 Führen Sie einen der nachfolgenden Schritte aus:

- Wenn Sie SSL für Compliance Reporter, Console Web Services, Device Server, Gatekeeper Web Services oder Legacy Gatekeeper Connector aktivieren, wechseln Sie zum component conf-Verzeichnis.
- Wenn Sie SSL zwischen dem Server und dem Unternehmensverzeichnisserver aktivieren, wechseln Sie zu **<Dell-Installationsverzeichnis>\Java Runtimes\jre1.x.x_xx\lib\security** (das Standardpasswort für JRE cacerts ist **changeit**).

3 Führen Sie Keytool wie folgt aus, um das Stammzertifikat zu installieren:

```
keytool -import -trustcacerts -alias <Alias des
Zertifizierungsstellen-Zertifikats> -keystore .\cacerts -file <Dateiname des
Zertifizierungsstellen-Zertifikats>
```

Beispiel:

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

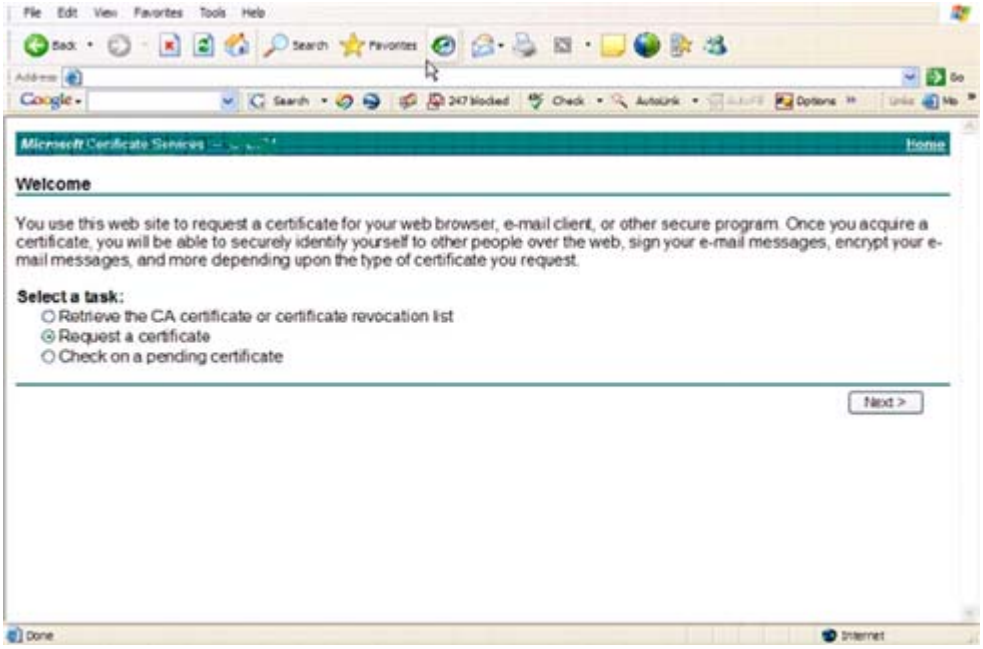
Beispielmethode zur Anforderung eines Zertifikats

Eine Methode zur Anforderung eines Zertifikats besteht darin, über einen Webbrowser auf den Microsoft-Zertifizierungsstellenserver zuzugreifen, der intern von Ihrer Organisation eingerichtet wird.

1 Navigieren Sie zum Microsoft-Zertifizierungsstellenserver. Die IP-Adresse wird von Ihrer Organisation bereitgestellt.

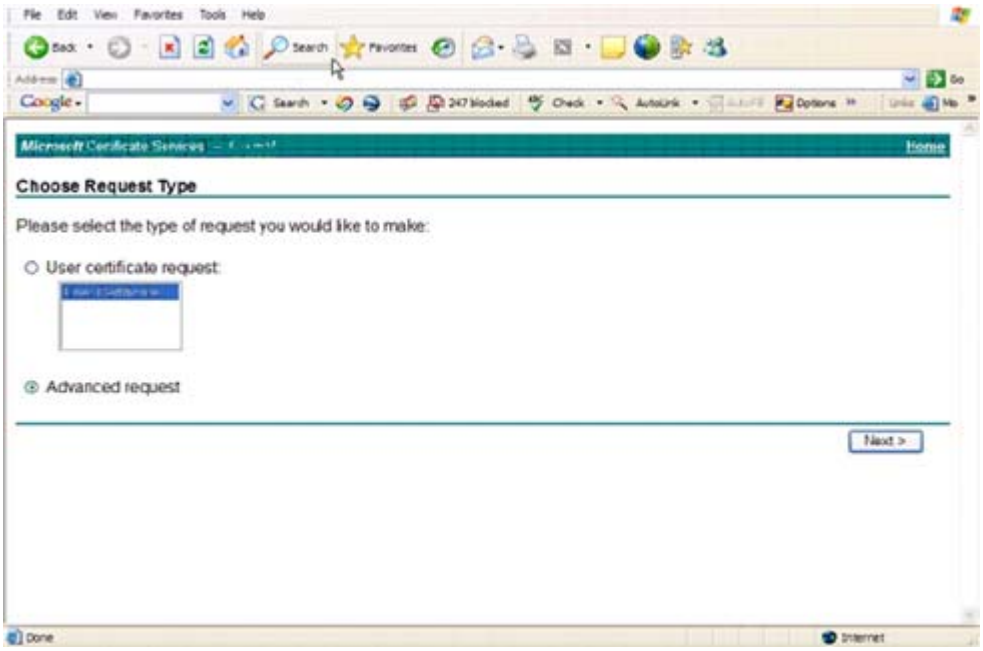
2 Wählen Sie **Request a certificate (Zertifikat anfordern)** aus und klicken Sie auf **Next >** (Weiter).

Abbildung 9-2. Microsoft-Zertifikatdienste



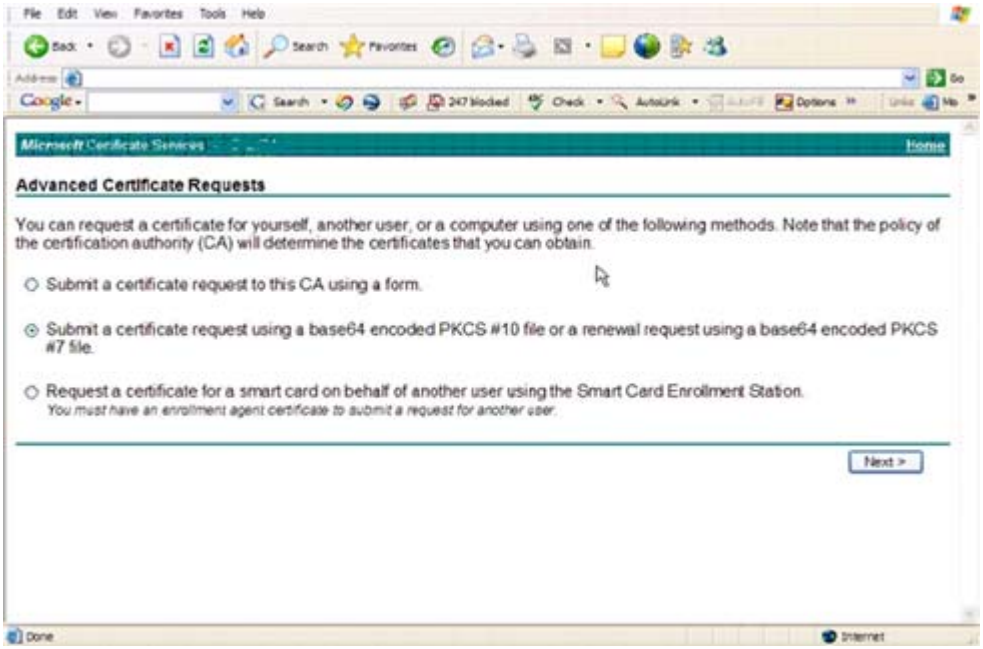
3 Wählen Sie **Advanced Request** (Erweiterte Anforderung) aus und klicken Sie auf **Next > (Weiter).**

Abbildung 9-3. Art der Anforderung auswählen



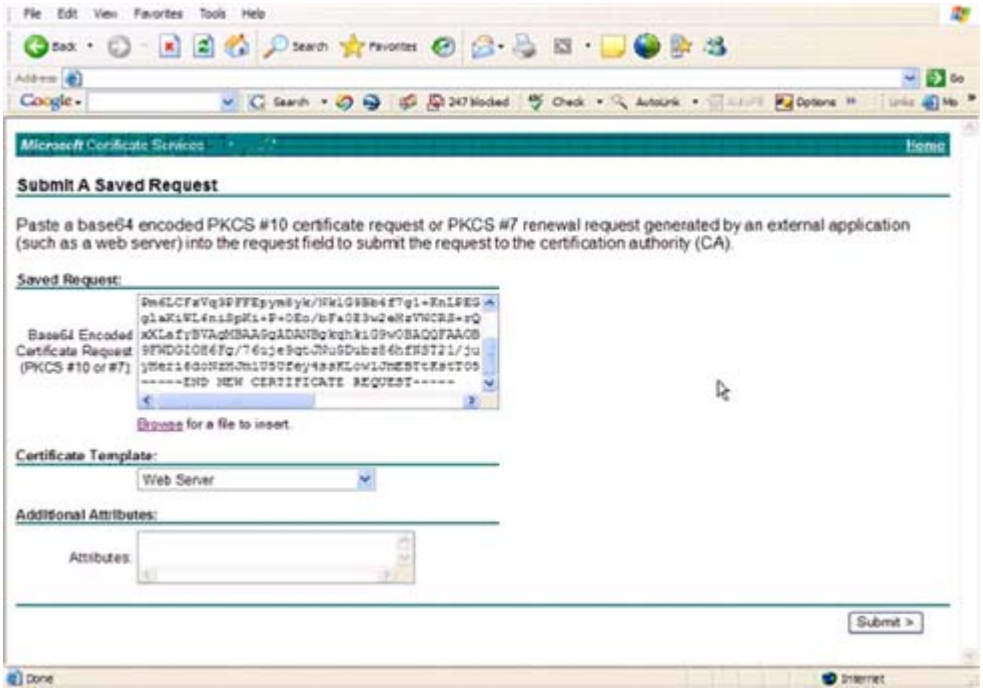
4 Wählen Sie die Option zum **Einreichen einer Zertifikatanforderung**, die eine Base64-codierte PKCS10-Datei verwendet, und klicken Sie auf **Next >** (Weiter).

Abbildung 9-4. Erweiterte Zertifikatanforderung



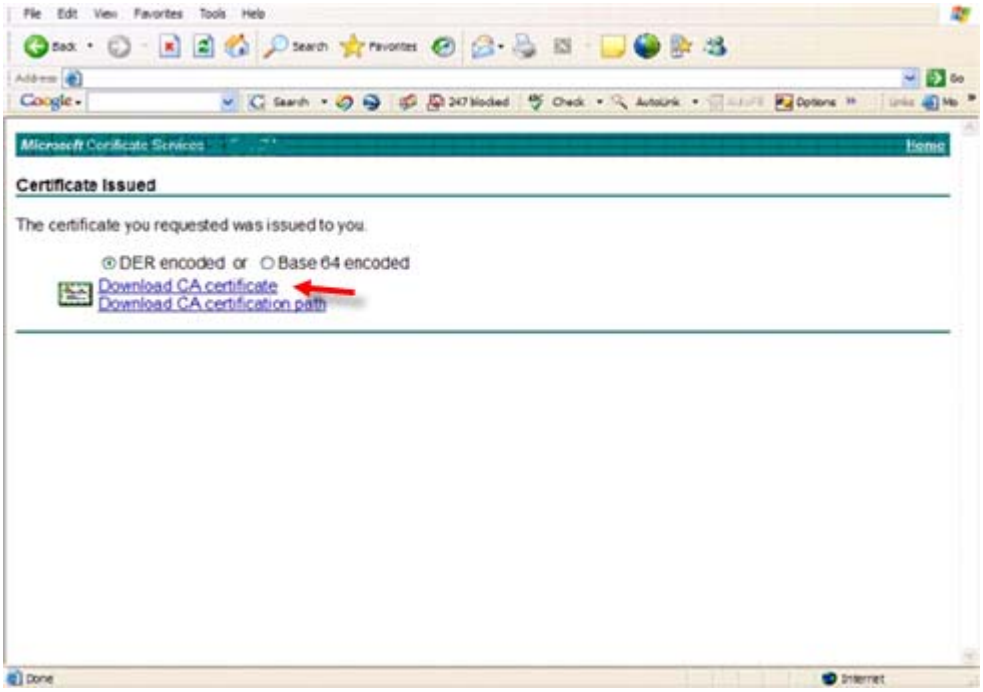
5 Kopieren Sie den Inhalt der CSR-Anforderung in das Textfeld. Wählen Sie die Zertifikatvorlage **Web Server** (Webserver) aus und klicken Sie auf **Submit >** (Senden).

Abbildung 9-5. Gespeicherte Anforderung senden



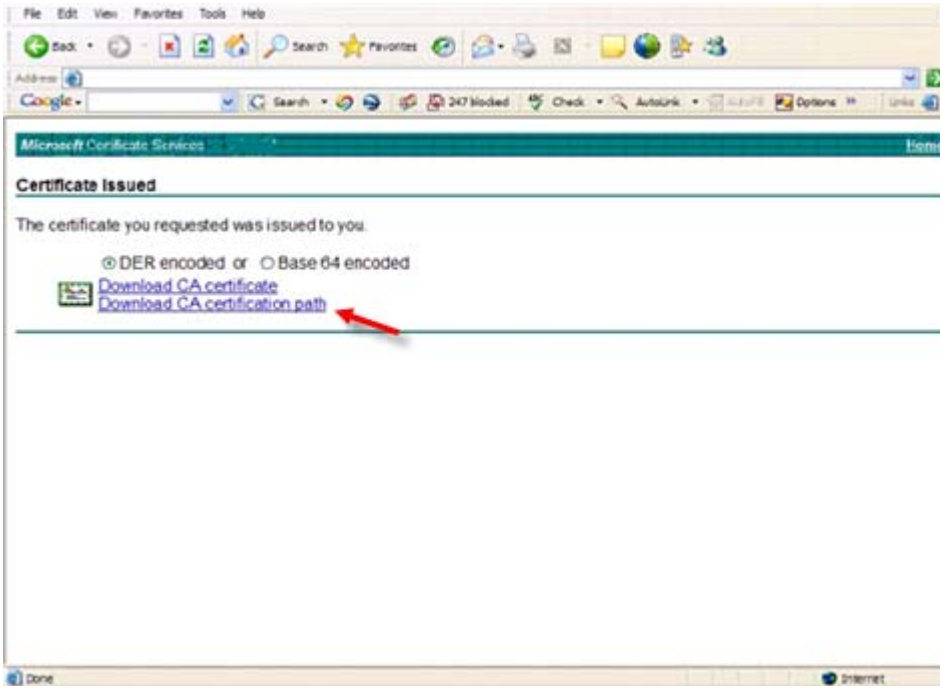
6 Speichern Sie das Zertifikat. Wählen Sie **DER encoded** (DER-codiert) aus und klicken Sie auf **Download CA certificate** (Download des Zertifizierungsstellenzertifikats).

Abbildung 9-6. Download des Zertifizierungsstellenzertifikats



7 Speichern Sie das Zertifikat. Wählen Sie **DER encoded** (DER-codiert) aus und klicken Sie auf **Download CA certification path** (Download des Zertifizierungsstellen-Zertifizierungspfads).

Abbildung 9-7. Download des Zertifizierungsstellen-Zertifizierungspfads



8 Importieren Sie das konvertierte Zertifikat der Zertifizierungsstelle. Kehren Sie zum DOS-Fenster zurück. Geben Sie Folgendes ein:

```
keytool -import -trustcacerts -file <CSR-Dateiname> -keystore cacerts
```

9 Nach dem Import des Zertifikats der Zertifizierungsstelle kann nun das Serverzertifikat importiert werden (die Zertifikatkette kann eingerichtet werden). Geben Sie Folgendes ein:

```
keytool -import -alias dell -file <CSR-Dateiname> -keystore cacerts
```

Verwenden Sie das Alias des selbstsignierten Zertifikats, um die CSR-Anforderung mit dem Serverzertifikat zu verknüpfen.

10 Eine Auflistung der cacerts-Datei zeigt, dass das Serverzertifikat eine **Zertifikatkettenlänge** von **2** hat. Daran ist erkennbar, dass das Zertifikat nicht selbstsigniert ist. Geben Sie Folgendes ein:

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

Beachten Sie, dass der Zertifikat-Fingerabdruck des zweiten Zertifikats in der Kette das importierte Zertifikat der Zertifizierungsstelle ist (außerdem unter dem Serverzertifikat in der Auflistung aufgeführt).

Das Serverzertifikat wurde zusammen mit dem Zertifikat der Zertifizierungsstelle erfolgreich importiert.


0 XXXXXA0 X