Dell Data Protection

Guía de configuración

2014-02

Contenido

1

Configuración de Compatibility Server

Este capítulo explica en detalle los parámetros que se pueden modificar a fin de ajustar el servidor Compatibility Server a su sistema. Siempre haga una copia de seguridad de los archivos de configuración antes de modificarlos.

En estos archivos cambie solo parámetros documentados. Si se cambia algún otro dato de estos archivos, incluso las etiquetas, el sistema podría dañarse y presentar fallas. Dell no puede garantizar que los problemas derivados de modificaciones no autorizadas de estos archivos se puedan resolver sin reinstalar Compatibility Server.

server_config.xml

Se pueden cambiar algunos de los parámetros indicados a continuación, en el archivo **<Directorio de instalación de Compatibility Server>\conf\server_config.xml**. Los parámetros que no se deben modificar están señalados como tales. Si Compatibility Server se está ejecutando, se debe detener el servicio Compatibility Server Service, modificar el archivo server_config.xml y luego reiniciar el servicio Compatibility Server Service para que las modificaciones realizadas tengan efecto.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
secrets.location	$dell.home$/conf/secretKeyStore	Ubicación predeterminada del archivo "secretkeystore". Actualice este parámetro si mueve este archivo de su ubicación predeterminada.
archive.location	$dell.home$/conf/archive	Ubicación predeterminada del archivo "archive". Actualice este parámetro si mueve este archivo de su ubicación predeterminada.
domain.qualified.authentication	true	Indica si se requiere de un nombre de usuario de inicio de sesión para hacer solicitudes al Servidor. Si se modifica ese valor, se debe reiniciar el servidor Device Server para que la modificación realizada tenga efecto.
directory.max.search.size	1000	Límite de las *búsquedas* en directorios; por encima de ese valor se inicia una excepción.
directory.server.search.timeout.seconds	60	Tiempo de espera del servidor de las búsquedas LDAP, en segundos.
directory.client.search.timeout	60	Tiempo de espera del cliente de las búsquedas LDAP, en segundos.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
rmi.recovery.host		Para utilizar la recuperación de EMS en diversos servidores: <!-- - quite la marca de comentario y modifique los nombres de host a sus nombres de dominio completamente autorizados para realizar una recuperación en cadena <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	El nombre predeterminado del grupo al que pertenecen, como opción predeterminada, todos los proxy de políticas. Este nombre se puede modificar aquí, y también en el archivo "context.properties" del Device Server. Si se cambia el nombre del grupo aquí, también hay que cambiarlo en el Device Server, si usted planea: • Habilitar Shield para dispositivos Windows • Utilizar CREDActivate Recomendamos que todos los proxy de políticas pertenezcan al mismo grupo.
rsa.securid.enabled	false	Si en su sistema está utilizando RSA SecurID para Microsoft Windows versión 6 como reemplazo de GINA, establezca este campo a "true" (verdadero), y luego detenga y reinicie el servicio Compatibility Server Service. Cuando los usuarios de Shield se activan en un entorno en el que se reemplazó RSA GINA, la autenticación RSA reemplaza a la autenticación LDAP.
inv.queue.task.worker.size	10	Cantidad de subprocesos que procesan la cola de inventario.
inv.queue.task.timeout.seconds	900	Cantidad de segundos antes de que se produzca el vencimiento del tiempo de espera.
inv.queue.task.retry.count	3	Cantidad de veces que el servidor intenta procesar el inventario antes de descartarlo.
report.retry.max	120	Cantidad máxima de reintentos.
report.retry.wait.millis	250	Cantidad de milisegundos de espera entre un reintento y otro.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
triage.execute.time	0 0 0/6 * *	Se denomina triage al proceso de reconciliar a los usuarios y a los grupos que ya el servidor conoce. La configuración predeterminada es 0 0 0/6 * * ?, que significa que se hace triage cada 6 horas a partir de medianoche (medianoche, 6 AM, mediodía, 6 PM, medianoche...)
gatekeeper.service.max.sessions	5	Cantidad máxima de sesiones del servidor Policy Proxy de políticas.
gatekeeper.service.max.session.timeout	5	Tiempo de espera de la cantidad máxima de las sesiones del Policy Proxy.
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	Función necesaria para actualizar las funciones administrativas de grupos y usuarios.
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	Función necesaria para actualizar las funciones administrativas de grupos y usuarios
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin,LogAdmin	Funciones necesarias para recuperar las sesiones de los registros.
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin,LogAdmin	Funciones necesarias para recuperar los registros.
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin,LogAdmin	Funciones necesarias para recuperar la lista de columnas de los registros.
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin,LogAdmin	Funciones necesarias para recuperar la lista de categorías de los registros.
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin,LogAdmin	Funciones necesarias para recuperar la lista de prioridades de los registros.
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin,SecAdmin,HelpDeskAdmin,SystemAdmin	Funciones necesarias para recuperar los nombres ID únicos.
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	Función necesaria para recuperar la lista de administradores del sistema.
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	Función necesaria para configurar la contraseña del superadministrador.
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	Función necesaria para restablecer la contraseña del superadministrador.
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin,SecAdmin	Funciones necesarias para agregar dominios.
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin,SecAdmin	Funciones necesarias para quitar dominios.
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin,SecAdmin	Funciones necesarias para actualizar dominios.
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin,SecAdmin	Funciones necesarias para agregar grupos.
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin,SecAdmin	Funciones necesarias para quitar grupos.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin,SecAdmin	Funciones necesarias para encontrar grupos LDAP.
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin,SecAdmin	Funciones necesarias para encontrar usuarios LDAP.
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin,SecAdmin	Funciones necesarias para agregar usuarios.
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	Función necesaria para agregar licencias Enterprise.
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	Función necesaria para ver la licencia Enterprise.
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin,SecAdmin	Funciones necesarias para recuperar dispositivos.
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin,SecAdmin	Funciones necesarias para suspender usuarios.
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	Funciones necesarias para activar dispositivos por proxy.
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin,SecAdmin	Funciones necesarias para recuperar dispositivos manualmente por proxy.
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Función necesaria para recuperar el recurso de archivos de Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Función necesaria para aprobar el recurso de archivos de Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Funciones necesarias para aprobar la configuración de Gatekeeper.
policy.arbiter.security.mode	most-restrictive	Esta propiedad controla el modo de funcionamiento del algoritmo de asignación (mapeo) de políticas de los elementos de políticas, que tienen una preferencia de seguridad cuando la política tenga múltiples nodos padre. Valores: Least-restrictive (la menos restrictiva) - se utiliza el valor del elemento menos restrictivo del padre Most-restrictive (la más restrictiva) - se utiliza el valor del elemento más restrictivo del padre
policy.set.synchronization.sync-unmodified	true	Este indicador señala que se debe agregar o reasignar, en la próxima sincronización externa, todos los elementos de política, sin configurar el indicador modificado a "true" (verdadero). En cada sincronización se alterna el valor de este indicador, de modo que es necesario reiniciarlo si el administrador de seguridad quiere agregar sin modificaciones. Esta es una opción avanzada.
db.schema.version.major		Esquema principal de la base de datos.
db.schema.version.minor		Esquema secundario de la base de datos.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
db.schema.version.patch		Versión de la revisión del esquema de la base de datos.
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	Ubicación predeterminada del controlador de la base de datos. Actualice este parámetro si mueve este archivo de su ubicación predeterminada.
dao.db.host		El nombre de host de su servidor de base de datos. Este parámetro se cambia mediante la herramienta de configuración.
dao.db.name		El nombre de su base de datos. Este parámetro se cambia mediante la herramienta de configuración.
dao.db.user		El nombre de usuario que tiene acceso completo a la base de datos. Este parámetro se cambia mediante la herramienta de configuración.
dao.db.password		La contraseña del nombre de usuario que tiene acceso completo a la base de datos. Este parámetro se cambia mediante la herramienta de configuración.
dao.db.max.retry.count	10	La cantidad máxima de veces que Compatibility Server intenta reconectarse a SQL Server cuando ocurre un error especificado de socket.
dao.db.connection.retry.wait.seconds	5	El primer intento de reconexión ocurre de inmediato. El segundo intento ocurre luego de la cantidad especificada de segundos. El tercer intento ocurre luego de la cantidad especificada de segundos multiplicada por dos, el cuarto en la cantidad multiplicada por tres y así sucesivamente.
dao.connection.pool.max.uses	10000	Permite el retiro de conexiones, el valor "0" indica que no se retiren.
dao.connection.pool.inactive.threshold.seconds	900	Se utiliza para determinar si no se ha utilizado una conexión, y por lo tanto se puede cerrar.
dao.db.driver.socket.errors	0	Compatibility Server intenta reconectarse a SQL Server cuando ocurren los errores que corresponden a los códigos que se encuentran en esta lista, separados por comas. "0" es el código de error de los errores de socket de Microsoft SQL Server. También se puede agregar a la lista el código 17142 que corresponde a errores del servidor en pausa, y el 6002 que corresponde a errores de servidor cerrando.
dao.db.mssql.compatability.level	90	Valor correspondiente a SQL Server 2005 o posterior.
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	Controlador del archivo de autorizaciones.
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	Controlador del archivo de inventarios.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	Controlador del archivo de eventos.
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Actualice este parámetro si mueve el archivo de recursos de Gatekeeper de su ubicación predeterminada.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Actualice este parámetro si mueve el archivo de recursos de Gatekeeper de su ubicación predeterminada.
rmi.server.registry.host	localhost	La propiedad Host se utiliza solamente para que los programas cliente puedan determinar en qué lugar se encuentra el registro. No se utiliza durante la creación del registro RMI ni de los objetos remotos. Se creará en localhost.
rmi.server.registry.port	1099	El puerto del registro RMI se configura durante la instalación. Este parámetro también se puede utilizar para cambiar el puerto después de la instalación. Si se cambia ese valor, también se debe configurar los servicios Gatekeeper Web Services.
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones requeridas para configurar las autorizaciones de los informes del servidor.
security.authorization.method.IReportingService.removeEntity	SystemAdmin	Función necesaria para quitar las entidades del servidor.
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	Función necesaria para configurar la visibilidad de las entidades del servidor.
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver la página de detalles de los dispositivos.
security.authorization.method.IReportingService.openSession	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para abrir una sesión del servidor.
security.authorization.method.IReportingService.getPagedReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe paginado.
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe de tipos de dispositivos.
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe del sistema operativo.
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver los informes de modelos de dispositivos.
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe detallado de las políticas.
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe detallado de las estaciones de trabajo.
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe de fallas en la encriptación.
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe de resumen de la encriptación.

server_config.xml		
Parámetro	**Valor predeterminado**	**Descripción**
security.authorization.method.IReportingService.getUserDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe de información detallada de los usuarios.
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para ver el informe de información detallada de los grupos.
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funciones necesarias para el informe de la lista de dominios.
security.authorization.method.IKeyService.getKeys	ForensicAdmin	Esta configuración se utiliza con los complementos de integración forense. Comuníquese con el departamento de apoyo técnico de Dell si necesita la integración con una herramienta forense.
accountType.nonActiveDirectory.enabled	false	Habilitar las activaciones fuera del dominio es una configuración avanzada que tiene consecuencias amplias. *ANTES* de habilitar esta configuración, póngase en contacto con el departamento de apoyo al cliente para analizar las necesidades específicas de su entorno. Reinicie el servicio de Compatibility Server después de modificar este valor. Además de esta configuración, cree o modifique el parámetro de registro de la computadora con Windows de la siguiente manera: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations=REG_DWORD:1

gkresource.xml

Se pueden cambiar los parámetros en <Directorio de instalación de Compatibility Server>\conf\gkresource.xml.

Recomendamos que indique la secuencia de los cambios realizados, mediante comentarios al comienzo del archivo. Eso le permitirá trasladar de manera sencilla los cambios al nuevo archivo cuando haga una actualización.

NOTA: El archivo gkresource.xml debe ser un archivo XML de formato correcto. Si no está familiarizado con los archivos XML, Dell recomienda que no intente modificar este archivo. Asegúrese de utilizar referencias a entidades cuando corresponda, en vez de caracteres especiales no precedidos por una secuencia de escape.

Todo cambio al archivo de recursos de Gatekeeper debe ser aprobado por un Administrador del Sistema antes de su implementación.

Habilitar el formato dominio/nombre de usuario

Agregue la siguiente cadena para habilitar (o deshabilitar) el formato dominio\nombre de usuario. El formato queda deshabilitado si la cadena no existe en el archivo. También se puede configurar el valor a "0" para deshabilitarlo.

1. Vaya a <Directorio de instalación de Compatibility Server>\conf.
2. Abra el archivo gkresource.xml con un editor de archivos .xml.
3. Agregue la cadena:

   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. Haga clic en Guardar y cierre el archivo.

run-service.conf

Se pueden cambiar algunos de los parámetros indicados a continuación, en el archivo **<Directorio de instalación de Compatibility Server>\conf\run-service.conf**. Estos parámetros se configuran automáticamente durante la instalación. Para personalizar o cambiar la configuración de cualquier servicio:

1. Detenga el servicio.
2. Quite el servicio.
3. Modifique y guarde el archivo **run-service.conf**. Recomendamos que indique la secuencia de los cambios realizados, mediante comentarios al comienzo del archivo.
4. Vuelva a instalar el servicio.
5. Arranque el servicio.

run-service.conf		
Parámetro	**Valor predeterminado**	**Descripción**
JAVA_HOME	Dell\Java Runtime\jreX.x	Ubicación del directorio de instalación de Java.
wrapper.java.additional.5	n/a	La dirección MAC indicada en este renglón es la dirección MAC de la tarjeta de la red local. Si el servidor tiene varias tarjetas de red, o si desea enlazar a una tarjeta distinta de la tarjeta principal del sistema, escriba aquí la dirección MAC de la tarjeta deseada, sin guiones.
wrapper.ntservice.name	EpmCompatSvr	Nombre del servicio.
wrapper.ntservice.displayname	Dell Compatibility Server	Nombre para mostrar del servicio.
wrapper.ntservice.description	Enterprise Compatibility Server	Descripción del servicio.
wrapper.ntservice.dependency.1		Dependencias del servicio. Agregue las dependencias del servicio, según sea necesario, a partir de 1.
wrapper.ntservice.starttype	AUTO_START	Modo en el que el servicio está instalado: AUTO_START o bien DEMAND_START.
wrapper.ntservice.interactive	false	Cuando se configura a "true", el servicio puede interactuar con el escritorio.

2

Configuración de Core Server

Este capítulo explica en detalle los parámetros que se pueden modificar para ajustar el servidor Core Server de núcleo a su sistema.

En estos archivos cambie solo parámetros documentados. Si se cambia algún otro dato de estos archivos, incluso las etiquetas, el sistema podría dañarse y presentar fallas. Dell no puede garantizar que los problemas derivados de modificaciones no autorizadas de estos archivos se puedan resolver sin reinstalar Core Server.

Cambio del arbitraje de políticas, de La más segura a La menos segura

PolicyService.config

Modifique este parámetro para cambiar el arbitraje de políticas, de "la más segura" a "la menos segura". Cambie la configuración en **<Directorio de instalación de Core Server>\PolicyService.config**. Si Core Server está en ejecución, se debe detener el servicio, modificar el archivo PolicyService.config y luego reiniciar el servicio, para que los cambios realizados al archivo tengan efecto.

Recomendamos que indique la secuencia de los cambios realizados, mediante comentarios al comienzo del archivo. Eso le permitirá trasladar de manera sencilla los cambios al nuevo archivo PolicyServiceConfig.xml cuando haga una actualización.

Modifique la siguiente sección:

```
<!-- 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" /> [Cambie este valor de “0” a “1” para configurar a la opción La menos segura]
</object>
```

Deshabilitar los servicios web

NOTA: Esta es una configuración avanzada que solo debe modificarse con la guía del departamento de apoyo técnico al cliente.

Para deshabilitar los servicios web en Core Server (por ejemplo, si se cuenta con una segunda instalación de Core Server que solo realiza el procesamiento de inventarios), modifique los parámetros de configuración en:

<Directorio de instalación de Core Server>

Credant.Server2.WindowsService.exe.Config

y

<Directorio de instalación de Core Server>\Spring.config

Si Core Server está en ejecución, se debe detener el servicio, modificar los parámetros de configuración de estos dos archivos y luego reiniciar el servicio, para que los cambios realizados al archivo tengan efecto.

Credant.Server2.WindowsService.exe.Config

Elimine la siguiente sección:

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

Spring.config

Elimine lo siguiente:

Elimine todas las definiciones <object> </object> en los encabezados de **AOP Advice**, **Web Service Target Definition** y **Web Service Host Definition**.

Habilitación del servidor SMTP para el envío de notificaciones de licencia por correo electrónico

Si se utiliza Dell Data Protection | Cloud Edition, estos parámetros de configuración se automatizan usando la herramienta de configuración del servidor. Utilice este procedimiento si necesita habilitar el servidor SMTP para el envío de notificaciones de licencia por correo electrónico por otros motivos no relacionados con Dell Data Protection | Cloud Edition.

NotificationObjects.config

Para configurar su servidor SMTP para el envío de notificaciones de licencia por correo electrónico, modifique el archivo **NotificationObjects.config** que se encuentra en el **<Directorio de instalación de Core Server>**.

Modifique lo siguiente:

```
<object name="EmailNotification" singleton="false" type="Credant.Notification.EmailNotification,
Credant.Notification"> [No cambie este valor]
  <property name="NotificationDataFactory" ref="NotificationDataFactory"/> [No cambie este valor]
  <property name="Host" value="test.dell.com"/>
  <property name="Port" value="25"/>
  <property name="Username" value="username"/>
  <property name="Password" value="${SmtpPassword}"/> [No cambie este valor]
  <property name="Logger" ref="NotificationLogger"/> [No cambie este valor]
</object>
```

Notification.config

Si su servidor de correo electrónico requiere de autenticación, modifique el archivo **Notification.config** que se encuentra en el **<Directorio de instalación de Core Server>**.

Modifique lo siguiente:

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

Agregar la ubicación de la carpeta de Compatibility Server al archivo de configuración de Core Server

Dado que Core Server es una aplicación .Net, el acceso a la información de registro puede bloquearse en ocasiones, a causa de los permisos. El problema es que, para que Core Server pueda leer secretkeystore (la clave de encriptación de la base de datos), necesita acceso a la información de la configuración de registro de Compatibility Server para encontrar la ubicación de secretkeystore. Si los permisos del registro bloquean este acceso, Core Server no puede autenticar a los usuarios de la consola. Esta configuración agrega la ubicación de la carpeta de Compatibility Server a la carpeta de configuración de Core Server en caso de problemas de acceso al registro.

1. Navegue hasta el <Directorio de instalación de Core Server>\EntityDataAccessObjects.config.
2. Cambie el siguiente elemento en **negrita**:

   <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"/> -->
   Quite la marca de comentario de esta línea y establezca la ruta de acceso completa a Compatibility Server.

   </object>
3. Haga clic en Guardar y cierre el archivo.
4. Reinicie los servicios de Core Server y Compatibility Server.

Permitir que Core Server utilice un proceso de iteración para los métodos de autenticación

El controlador de dominio puede bloquear los intentos de autenticación de Core Server debido a políticas configuradas en los métodos de autenticación permitidos. La mejora se realizó para implementar un "interruptor" en el archivo de configuración de Core Server para permitir que Core Server repita (iteración) diversos métodos de autenticación, en un intento por encontrar uno que funcione.

1. Navegue hasta el <Directorio de instalación de Core Server>\Spring.config.
2. Cambie el siguiente elemento en **negrita**:

   <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" /> ***Cambie este valor a "true" para habilitar esta función.***

   <!-- Used to change the AuthType per domain: key is domain's CID and value is the System.DirectoryServices.AuthenticationTypes value

   <property name="DomainAuthType">

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

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

   </dictionary>

   </property>

   -->

   </object>

3 Haga clic en Guardar y cierre el archivo.

4 Reinicie el servicio de Core Server.

3

Configuración de Device Server

Este capítulo explica en detalle los parámetros que se pueden modificar para ajustar el servidor Device Server de dispositivos a su sistema.

En estos archivos cambie solo parámetros documentados. Si se cambia algún otro dato de estos archivos, incluso las etiquetas, el sistema podría dañarse y presentar fallas. Dell no puede garantizar que los problemas derivados de modificaciones no autorizadas de estos archivos se puedan resolver sin reinstalar Device Server.

eserver.properties

Se pueden cambiar los siguientes parámetros en <Directorio de instalación de Device Server>\conf\eserver.properties.

Recomendamos que indique la secuencia de los cambios realizados, mediante comentarios al comienzo del archivo. Eso le permitirá trasladar de manera sencilla los cambios al nuevo archivo cuando haga una actualización.

eserver.properties		
Parámetro	**Valor predeterminado**	**Descripción**
eserver.default.host	Servicio Device Server	El FQDN de la ubicación en la que está instalado Device Server.
eserver.default.port	Enterprise Server v7.7 o posterior: 8443 Enterprise Server anterior a v7.7: 8081	El puerto en el que Device Server estará atento a solicitudes entrantes de activación provenientes de los dispositivos.
eserver.use.ssl	True	Los protocolos SSL están habilitados como opción predeterminada. Para deshabilitar SSL, cambie el valor de este parámetro a "False".
eserver.keystore.location	${context['server.home']}/conf/cacerts	La ubicación del certificado SSL que utiliza Device Server.
eserver.keystore.password	changeit	Este parámetro se modifica cuando se modifica la contraseña de cacerts mediante la herramienta de configuración. Si se modifica el cacert del sistema mediante la herramienta de configuración en algún momento después de la configuración inicial, actualice este parámetro con la contraseña Keystore que usted utiliza.

eserver.properties		
Parámetro	**Valor predeterminado**	**Descripción**
eserver.ciphers		Configura la lista de algoritmos de encriptación. Coloque una coma entre cada uno de los algoritmos. Si se deja vacío, el socket sólo permitirá los algoritmos compatibles con Tomcat. Quite la marca de comentario en el ejemplo a continuación para configurar la lista de algoritmos de encriptación. Coloque una coma entre cada uno de los algoritmos. Consulte la guía de referencia de JSSE de Sun para conocer la lista de nombres válidos de los paquetes de algoritmos de encriptación. #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

Se pueden cambiar algunos de los parámetros indicados a continuación, en el archivo **<Directorio de instalación de Device Server>\conf\run-service.conf**. Estos parámetros se configuran automáticamente durante la instalación. Para personalizar o cambiar la configuración de cualquier servicio:

1. Detenga el servicio.
2. Quite el servicio.
3. Modifique y guarde el archivo **run-service.conf**. Recomendamos que indique la secuencia de los cambios realizados, mediante comentarios al comienzo del archivo.
4. Vuelva a instalar el servicio.
5. Arranque el servicio.

run-service.conf		
Parámetro	**Valor predeterminado**	**Descripción**
JAVA_HOME	Dell\Java Runtime\jreX.x	Ubicación del directorio de instalación de Java.
wrapper.ntservice.name	EpmDeviceSvr	Nombre del servicio.
wrapper.ntservice.displayname	Dell Device Server	Nombre para mostrar del servicio.
wrapper.ntservice.description	Enterprise Device Server	Descripción del servicio.
wrapper.ntservice.dependency.1		Dependencias del servicio. Agregue las dependencias del servicio, según sea necesario, a partir de 1.
wrapper.ntservice.starttype	AUTO_START	Modo en el que el servicio está instalado: AUTO_START o bien DEMAND_START.
wrapper.ntservice.interactive	false	Cuando se configura a "true", el servicio puede interactuar con el escritorio.

4

Configuración de Security Server

Este capítulo explica en detalle los parámetros que se pueden modificar a fin de ajustar el servidor Security Server a su sistema.

En estos archivos cambie solo parámetros documentados. Si se cambia algún otro dato de estos archivos, incluso las etiquetas, el sistema podría dañarse y presentar fallas. Dell no puede garantizar que los problemas derivados de modificaciones no autorizadas de estos archivos se puedan resolver sin reinstalar Security Server.

context.properties

Se pueden cambiar los siguientes parámetros en **<Directorio de instalación de Security Server>\webapps\xapi\WEB-INF\context.properties**.

Recomendamos que indique la secuencia de los cambios realizados, mediante comentarios al comienzo del archivo. Eso le permitirá trasladar de manera sencilla los cambios al nuevo archivo cuando haga una actualización.

context.properties		
Parámetro	**Valor predeterminado**	**Descripción**
default.gatekeeper.group.remote	CMGREMOTE	Nombre del grupo remoto del dispositivo. **Evite modificarlo.**
xmlrpc.max.threads	250	Cantidad máxima de subprocesos simultáneos en este Device Server.
default.auth.upn.suffix		El sufijo UPN que se añade al nombre del usuario a fin de iniciar una sesión, si el servidor requiere de un nombre completo y la solicitud no lo incluye.
device.manual.auth.enable	true	Indica si las autenticaciones manuales están habilitadas o deshabitadas. **Evite modificarlo.**
service.activation.enable	true	Indica si el servidor Device Server maneja las activaciones. **Evite modificarlo.**
service.policy.enable	true	Indica si la política está habilitada o deshabitada. **Evite modificarlo**.
service.auth.enable	true	Indica si el servidor Device Server maneja las autenticaciones.
service.forensic.enable	true	Esta configuración se utiliza con los complementos de integración forense. Comuníquese con el departamento de apoyo técnico de Dell si necesita la integración con una herramienta forense.
service.support.enable	true	Habilita la recuperación de metainformación del servidor.

context.properties		
Parámetro	**Valor predeterminado**	**Descripción**
service.device.enable	true	Habilita la compatibilidad con servicios Shield tales como el almacenamiento de claves SDE.

5

Configuración de las funciones de encriptación

Esta sección explica cómo se puede controlar de manera independiente las funciones de encriptación.

Prevención de la eliminación de archivos temporales

Como opción predeterminada, todos los archivos temporales que se encuentren en el directorio c:\windows\temp serán eliminados automáticamente al hacer instalaciones y actualizaciones de DDPE. La eliminación de los archivos temporales agiliza la encriptación inicial, y se realiza antes del barrido inicial de encriptación.

No obstante, si en su sistema se utilizan aplicaciones de terceros que requieren que se conserve la estructura de archivos contenida en el directorio \temp, no se debe realizar dicha eliminación.

Para deshabilitar la eliminación de archivos temporales, cree o modifique la configuración de registro de la siguiente manera:

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

Tome en cuenta que si **no** se eliminan los archivos temporales aumentará la duración de la encriptación inicial.

Ocultar iconos superpuestos

Como opción predeterminada, durante la instalación todos los iconos de encriptado superpuestos están configurados para mostrarse. Utilice los siguientes parámetros de registro para ocultar los iconos de encriptado superpuestos para todos los usuarios administrados en una computadora después de la instalación original.

Cree o modifique las siguientes configuraciones de registro:

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)=1

Si un usuario (con los privilegios apropiados) decide mostrar los iconos de encriptado superpuestos, esa configuración anulará este valor del registro.

Ocultar el icono de la bandeja del sistema

De forma predeterminada, durante la instalación se muestra el icono de la bandeja del sistema. Utilice los siguientes parámetros de registro para ocultar el icono de la bandeja del sistema para todos los usuarios administrados en una computadora después de la instalación original.

Cree o modifique las siguientes configuraciones de registro:

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)=1

Activación escalonada

La Activación escalonada es una función que permite repartir las activaciones de Shield a lo largo de un período determinado de tiempo, a fin de reducir las cargas sobre el servidor al realizar implementaciones masivas. Las activaciones se retrasan con base en escalones de tiempo generados algorítmicamente, a fin de permitir una distribución homogénea de los lapsos de activación.

La Activación escalonada se habilita y configura a través del instalador de Shield, y a través de la estación de trabajo de Shield.

En el caso de usuarios que requieran de activación a través de redes VPN, podría ser necesaria una configuración de Activación escalonada de Shield, a fin de retrasar la activación inicial durante el lapso necesario que permita que el software cliente de la VPN establezca una conexión de red.

PRECAUCIÓN: Configure la Activación escalonada sólo con la asistencia del departamento de apoyo técnico al cliente. Si el escalonamiento de tiempo se configura de manera incorrecta, es posible que una gran cantidad de clientes intenten la activación de forma simultánea, lo que puede generar problemas graves de rendimiento.

En la configuración de la Activación escalonada se utilizan las siguientes claves de registro. Todo cambio a estas claves de registro requieren del reinicio de la estación de trabajo de Shield para que las actualizaciones tengan efecto.

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

  Esta configuración habilita o deshabilita la función de Activación escalonada.
  Deshabilitada=0 (predeterminado)
  Habilitada=1

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

  El lapso de tiempo, en segundos, en que ocurrirá el intervalo entre escalones de la activación. Se puede utilizar esta propiedad a fin de reemplazar el período de tiempo, en segundos, durante el que ocurre el intervalo entre escalones de la activación. Están disponibles 25200 segundos para las activaciones escalonadas, durante un período de siete horas. La configuración predeterminada es de 86400 segundos, lo que representa una repetición diaria.

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

  El intervalo dentro de la repetición, ACTIVATION_SLOT_CALREPEAT, en el que se producen todos los escalones de tiempo de activación. Sólo se permite un intervalo. El valor de esa configuración debe ser de "0",<CalRepeat>. Toda desviación del valor 0 podría arrojar resultados inesperados. La configuración predeterminada es 0,86400. Para configurar una repetición de siete horas, utilice la configuración 0,25200. CALREPEAT se activa cuando un usuario de Shield inicia una sesión.

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

  La cantidad de escalones de activación que pueden ser omitidos antes de que la computadora intente hacer la activación, durante el siguiente inicio de sesión del usuario cuya activación haya sido escalonada. Si la activación no se realiza durante ese intento inmediato, Shield reinicia los intentos de Activación escalonada. Si la activación no se realiza debido a una falla en la red, se intentará la activación al reconectarse la red, aunque no se haya superado el valor del parámetro MISSTHRESHOLD. Si un usuario cierra su sesión antes de haberse alcanzado el lapso del escalón de activación, se asigna un nuevo escalón cuando el usuario inicie una nueva sesión.

- HKCU/Software/CREDANT/ActivationSlot (según la información de usuario)

  El tiempo diferido en el que se intentará la Activación escalonada, que se configura cuando el usuario inicia una sesión en la red por primera vez después de haberse habilitado la Activación escalonada. El escalón de activación se vuelve a calcular después de cada uno de los intentos de activación.

- HKCU/Software/CREDANT/SlotAttemptCount (según la información de usuario)

  La cantidad de intentos fallidos u omitidos, cuando se llega al escalón de tiempo y se intenta la activación pero falla. Cuando esa cifra alcanza el valor configurado en el parámetro ACTIVATION_SLOT_MISSTHRESHOLD, la computadora intenta una activación inmediata al momento de la conexión a la red.

Para activar la Activación escalonada mediante la línea de comandos, utilice un comando similar al siguiente:

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

NOTA: Asegúrese de incorporar un valor que contenga uno o más caracteres especiales, como un espacio, en comillas no precedidas por una secuencia de escape.

Sondeo forzado

Utilice la configuración de registro a continuación para que Shield sondee al servidor para una actualización forzada de política.

Cree o modifique las siguientes configuraciones de registro:

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD value)=1

Según la versión de Shield, la configuración de registro desaparecerá automáticamente *o* se modificará de **1** a **0** una vez que el sondeo esté terminado.

Según el conjunto de permisos de un usuario administrador, podría necesitarse realizar una modificación en los permisos para crear este parámetro de configuración de registro. Si surgen problemas al intentar crear un DWORD nuevo, siga los pasos que se detallan a continuación para realizar la modificación de permisos.

1. En el registro de Windows vaya a HKLM\SOFTWARE\Credant\CMGShield\Notify.
2. Haga clic con el botón derecho en **Notificar** > **Permisos**.
3. Una vez que se abre la ventana *Permiso para notificar*, seleccione la casilla de **Control total**.
4. Haga clic en **Aceptar**.

Ya puede crear su nueva configuración de registro.

Opciones de inventario

Utilice los siguientes parámetros de registro para permitir que Shield envíe un inventario optimizado al servidor, envíe un inventario completo al servidor o envíe un inventario completo para todos los usuarios activados al servidor.

Enviar inventario optimizado al servidor

Cree o modifique las siguientes configuraciones de registro:

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

OnlySendInvChanges (REG_DWORD)=1

Si no hay ninguna entrada, se envía el inventario optimizado al servidor.

Enviar inventario completo al servidor

Cree o modifique las siguientes configuraciones de registro:

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

OnlySendInvChanges (REG_DWORD)=0

Si no hay ninguna entrada, se envía el inventario optimizado al servidor.

Enviar inventario completo para todos los usuarios activados

Cree o modifique las siguientes configuraciones de registro:

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

RefreshInventory (REG_DWORD)=1

Esta entrada se quita del registro tras ser procesada. El valor se guarda en el almacén, de forma que incluso si se reinicia la computadora antes de que se cargue el inventario, Shield seguirá cumpliendo la solicitud en la próxima carga de inventario satisfactoria.

Esta entrada tiene precedencia sobre el valor de registro OnlySendInvChanges.

Activaciones fuera del dominio

Habilitar las activaciones fuera del dominio es una configuración avanzada que tiene consecuencias amplias. Póngase en contacto con el departamento de apoyo al cliente para analizar las necesidades específicas de su entorno y obtener instrucciones para activar esta función.

6

Configuración de los componentes a fin de utilizarlos con la autenticación/autorización Kerberos

Esta sección explica la manera de configurar los componentes a fin de utilizarlos con la autenticación/autorización Kerberos.

Configuración de los componentes a fin de utilizarlos con la autenticación/autorización Kerberos

NOTA: Si se va a utilizar la autenticación/autorización Kerberos, entonces el servidor que contiene el componente servidor de claves (Key Server) deberá formar parte del dominio afectado.

Key Server es un servicio que está atento a la conexión de clientes a sockets. Al conectarse un cliente, se negocia, autentica y encripta una conexión segura, con el uso de las interfaces API de Kerberos (si no se puede negociar una conexión segura, se desconecta al cliente).

Key Server comprueba con Device Server si el usuario que ejecuta el cliente tiene el permiso de acceso a las claves. Dicho acceso se otorga a través de la consola de administración remota mediante dominios *individuales*.

Instrucciones del Servicio de Windows

1. Navegue hasta el panel del Servicio de Windows (Inicio > Ejecutar... > services.msc > Aceptar).
2. Haga clic con el botón de la derecha sobre Dell Key Server y seleccione **Propiedades**.
3. Vaya a la pestaña **Iniciar sesión** y seleccione el botón de opción **Esta cuenta:**.
4. En el campo **Esta cuenta:**, agregue el usuario deseado de dominio. Este usuario de dominio debe tener al menos los derechos de administrador local a la carpeta de Key Server (debe poder escribir en el archivo de configuración de Key Server, y también escribir en el archivo log.txt).
5. Haga clic en **Aceptar**.
6. Reinicie el servicio (deje abierto el panel del Servicio de Windows para operaciones posteriores).
7. Navegue hasta <Directorio de instalación de Key Server> log.txt a fin de verificar que el servicio arrancó correctamente.

Instrucciones del archivo de configuración de Key Server

1. Navegue hasta el <Directorio de instalación de Key Server>.
2. Abra Credant.KeyServer.exe.config con un editor de texto.
3. Vaya a <add key="user" value="superadmin" /> y cambie el valor de "superadmin" al nombre del usuario correspondiente (también puede dejar el valor de "superadmin").

   El formato "superadmin" puede ser cualquier método que pueda autenticarse con el servidor. El nombre de la cuenta del SAM, el nombre UPN y también el formato "dominio/nombre de usuario" son aceptables. Todo método que pueda autenticar con el servidor es aceptable, debido que se requiere la validación de *esa* cuenta de usuario a fin de obtener la autorización con Active Directory.

Por ejemplo, en un entorno multi-dominios, si sólo se coloca el nombre de la cuenta del SAM, "jdoe", probablemente fallará porque el servidor no podrá autenticar "jdoe" ya que no puede encontrar "jdoe". En un entorno multi-dominios, se recomienda el formato UPN, aunque el formato "dominio/nombre de usuario" también es aceptable.

En un entorno de dominio único, es aceptable el nombre de la cuenta del SAM.

4 Vaya a <add key="epw" value="<valor encriptado de la contraseña>" /> y cambie "epw" a "password". Luego cambie "<valor encriptado de la contraseña>" a la contraseña del usuario según el Paso 3. El valor de la contraseña del usuario será encriptado cuando se reinicie el servidor.

Si se utiliza "superadmin" en el paso 3, y la contraseña del superadministrador no es "changeit",se debe cambiar aquí.

5 Guarde los cambios y cierre el archivo.

Ejemplo de archivo de configuración:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [El puerto TCP en el que el servidor estará atento. La opción predeterminada es 8050, modifique de ser necesario.]
        <add key="maxConnections" value="2000" /> [Máxima cantidad de conexiones activas al socket permitidas por el servidor].
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [URL de Device Server. Si su Enterprise Server es v7.7 o posterior, el formato es https://keyserver.domain.com:8443/xapi/ -- Si su Enterprise Server es anterior a v7.7, el formato es https://keyserver.domain.com:8081/xapi (sin la barra diagonal al final)].
        <add key="verifyCertificate" value="false" /> [El valor "true" verifica los certificados. Configure el valor en "false" si desea omitir la verificación o si utiliza certificados de firma automática].
        <add key="user" value="superadmin" /> [El nombre de usuario que se utiliza para comunicarse con el servidor Device Server. Este usuario debe ser del tipo "Administrador forense", seleccionado en la consola de administración remota. El formato "superadmin" puede ser cualquier método que pueda autenticarse con el servidor. El nombre de la cuenta del SAM, el nombre UPN y también el formato "dominio/nombre de usuario" son aceptables. Todo método que pueda autenticar con el servidor es aceptable, debido que se requiere la validación de esa cuenta de usuario a fin de obtener la autorización con Active Directory. Por ejemplo, en un entorno multi-dominios, si sólo se coloca el nombre de la cuenta del SAM, "jdoe", probablemente fallará porque el servidor no podrá autenticar "jdoe" ya que no puede encontrar "jdoe". En un entorno multi-dominios, se recomienda el formato UPN, aunque el formato "dominio/nombre de usuario" también es aceptable. En un entorno de dominio único, es aceptable el nombre de la cuenta del SAM.]
        <add key="cacheExpiration" value="30" /> [Qué tan a menudo (en segundos) el servicio debe comprobar quiénes tienen permiso de pedir claves. El servicio mantiene una memoria caché y lleva el seguimiento de la antigüedad. Una vez que la información en la caché tenga más antigüedad que el valor de este parámetro (en segundos), obtiene una nueva lista. Al conectarse un usuario, Key Server debe descargar del Device Server la información de los usuarios autorizados. Si no hay información de los usuarios en la caché, o si la lista no se ha descargado en los últimos "x" segundos, se volverá a descargar. No se hace sondeo, sino que este valor configura qué tan antigua puede llegar a ser la lista antes de que sea actualizada, cuando sea necesaria.]
        <add key="epw" value="encrypted value of the password" /> [Contraseña que se utiliza para comunicarse con Device Server. Si la contraseña "superadmin" fue cambiada, se debe cambiar aquí.]
    </appSettings>
</configuration>
```

Instrucciones del Servicio de Windows

1. Regrese al panel del Servicio de Windows.
2. **Reinicie** el servicio Dell Key Server Service.
3. Navegue hasta <Directorio de instalación de Key Server> log.txt a fin de verificar que el servicio arrancó correctamente.
4. Cierre el panel del Servicio de Windows.

Instrucciones de la Consola de Administración Remota

1. De ser necesario, inicie una sesión en la Consola de Administración Remota.
2. Haga clic en **Dominios** y luego en el icono **Detalle**.
3. Haga clic en **Key Server**.
4. En la lista de cuentas de Key Server, agregue al usuario que realizará las actividades de Administrador. El formato es dominio\nombre de usuario. Haga clic en **Agregar cuenta**.
5. Haga clic en **Usuarios** en el menú a la izquierda. En la casilla de búsqueda, escriba el nombre de usuario que fue agregado en el Paso 4. Haga clic en **Buscar**.
6. Una vez que haya encontrado el usuario correcto, haga clic en el icono **Detalle**.
7. Seleccione **Administrador forense**. Haga clic en **Actualizar**.

Los componentes estarán ya configurados para la autenticación/autorización Kerberos.

7

Asignar función de administrador forense

De forma predeterminada, la autorización forense está habilitada en los servidores de base de datos y deshabilitada en los servidores de aplicaciones. Estas configuraciones se establecen apropiadamente al momento de la instalación tanto de Device Server como de Security Server.

Instrucciones de la Consola de Administración Remota

1. De ser necesario, inicie una sesión en la Consola de Administración Remota.
2. En el panel izquierdo, haga clic en **Controlar** > **Usuarios**.
3. En la página de *Búsqueda de usuarios*, introduzca el nombre del usuario al que quiere asignar la función de administrador forense, y luego haga clic en **Buscar** (las credenciales de este usuario se suministran durante la ejecución de las utilidades CMGAd, CMGAu, CMGAlu, y durante la ejecución del agente Decryption Agent en el modo Forense).
4. En la página *Resultados de la búsqueda de usuarios*, haga clic en el icono **Detalle**.
5. En la página *Detalles de usuario de: <Nombre de usuario>*, seleccione **Admin**.
6. En la columna "Usuario", marque **Administrador forense**, y haga clic en **Actualizar**.

La función del administrador forense ya está configurada.

Deshabilitar autorización forense

1. En su servidor de base de datos, vaya a **<Directorio de instalación de Security Server>\webapps\xapi\WEB-INF\context.properties** y cambie la siguiente propiedad:

   service.forensic.enable=true

   a

   service.forensic.enable=false
2. **Reinicie** el servicio del Servidor de Seguridad.
3. Navegue hasta **<Directorio de instalación de Device Server>\webapps\ROOT\WEB-INF\web.xml** y modifique lo siguiente:

   <init-param>

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

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

   </init-param>
4. **Reinicie** el servicio de Device Server.
5. La práctica recomendada es eliminar la función de administrador forense de cualquier usuario que no utilice activamente los permisos que otorga la función.

8

Expresiones cron

Esta sección explica la manera de utilizar los formatos y los caracteres especiales de las expresiones cron.

Introducción a las expresiones cron

La herramienta cron es una herramienta de UNIX que ha estado en uso durante mucho tiempo, de modo que sus capacidades de planificación en el tiempo son poderosas y están demostradas. La clase CronTrigger se basa en las capacidades de planificación en el tiempo de cron.

CronTrigger utiliza expresiones cron, con las que se puede crear cronogramas de activación, del estilo "8:00 am de lunes a viernes" o "la 1:30 am todos los últimos viernes del mes".

Las expresiones cron son muy poderosas pero también pueden ser muy confusas. Este documento busca eliminar algunos de los misterios de la creación de expresiones cron, lo que le da un recurso que puede utilizar antes de buscar ayuda de otros.

Formatos de las expresiones cron

Las expresiones cron constan de 6 campos obligatorios y de 1 campo opcional, separados por espacios en blanco.
Los campos pueden contener cualquiera de los valores permitidos, junto con diversas combinaciones de los caracteres especiales permitidos para cada campo en particular.

Las expresiones cron puede ser tan sencillas como * * * * ? *.

O más complicadas, como 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010.

La descripción de los campos es como sigue.

Nombre del campo	¿Obligatorio?	Valores permitidos	Caracteres especiales permitidos
Minutos	Sí	0-59	, - * /
Horas	Sí	0-23	, - * /
Día del mes	Sí	1-31	, - * ? / L W C
Mes	Sí	1-12 o bien JAN-DEC	, - * /
Día de la semana	Sí	1-7 o bien SUN-SAT	, - * ? / L C #
Año	No	Vacío, 1970-2099	, - * /

Caracteres especiales

- El caracter "*" se utiliza para especificar todos los valores. Por ejemplo, "*" en el campo de minutos significa todos los minutos.
- El caracter "?" (sin valor especificado) es útil cuando se quiere especificar algo en alguno de los dos campos en los que se permite el uso de dicho caracter, pero no en el otro. Por ejemplo, para desencadenar una activación en un día particular del mes (el día 10), sin importar qué día de la semana sea la fecha, coloque "10" en el campo del día del mes y "?" en el campo del día de la semana.

- El caracter "-" se utiliza para especificar intervalos. Por ejemplo, "10-12" en el campo de horas significa las horas 10, 11 y 12.
- El caracter "," se utiliza para especificar valores adicionales. Por ejemplo, MON,WED,FRI en el campo del día de la semana significa los días lunes, miércoles y viernes.
- El caracter "/" se utiliza para especificar incrementos.

  "0/15" en el campo de segundos significa los segundos 0, 15, 30 y 45.

  "5/15" en el campo de segundos significa los segundos 5, 20, 35 y 50.

  Colocar "*" antes de "/" equivale a especificar "0" como el valor inicial.

  "1/3" en el campo del día del mes significa activar cada 3 días a partir del primer día del mes.

  En pocas palabras, existe un conjunto de números para cada uno de los campos de la expresión que se pueden poner en uso y en desuso. Para segundos y minutos, los números van de 0 a 59; para las horas, de 0 a 23; para los días del mes, de 0 a 31; y para los meses, de 1 a 12. El caracter / simplemente le ayuda a activar cada valor ordinal (nº) en un conjunto dado. De ese modo, "7/6" en el campo del mes sólo activa los meses 7, no significa cada 6º mes.
- El caracter "L" es un caracter permitido en los campos de día del mes y de día de la semana. El significado de este carácter es "último" (last), pero tiene un significado diferente en cada uno de los dos campos.

  El valor "L" en el campo del día del mes significa el último día del mes (el día 31 del mes de enero, el día 28 del mes de febrero en los años no bisiestos, etc).

  Si se utiliza por sí solo en el campo del día de la semana, significa 7 o SAT (sábado).

  Si se utiliza en el campo del día de la semana después de otro valor, significa el último día XXX del mes. Por ejemplo, "6L" significa el último viernes del mes. Cuando se utiliza la opción "L", es importante que no se especifique listas ni intervalos de valores, ya que los resultados obtenidos serán confusos.
- El caracter "W" es un caracter permitido en el campo del día del mes. Este caracter se utiliza para especificar el día de la semana (lunes-viernes) más cercano al día dado. Por ejemplo, si se coloca "15W" en el campo del día del mes, significa el día de la semana (lunes-viernes) más cercano al día 15 del mes. De modo que si el día 15 es un sábado, el desencadenador se activará el día viernes 14. Si el día 15 es un domingo, el desencadenador se activará el día lunes 16. Si el día 15 es un martes, el desencadenador se activará el día martes 15. No obstante, si se especifica "1W" como el valor del campo del día del mes, y el día 1º es un sábado, el desencadenador se activará el lunes 3, ya que no 'saltará' la demarcación de los días de un mes. El caracter "W" sólo se puede utilizar cuando el día del mes sea un día único, no un intervalo ni una lista de días.

  Los caracteres "L" y "W" también se pueden combinar en las expresiones del día del mes, para crear la expresión "LW" que significa el último día de la semana (lunes-viernes) del mes.
- El caracter "#" es un caracter permitido en el campo del día de la semana. Este caracter se utiliza para especificar el 'nº' día XXX del mes. Por ejemplo, la expresión "6#3" en el campo del día de la semana significa el tercer viernes del mes (día 6 = viernes, y #3 = el 3º del mes).

  Ejemplos adicionales:
  2#1 = el primer lunes del mes
  4#5 = el quinto miércoles del mes.

  Tome en cuenta que si coloca "#5" y no hay un día 5º del día dado en ese mes, no se producirá la activación en dicho mes.

- El caracter "C" se utiliza en expresiones de calendario. Al utilizar este caracter se indica que los valores se calculan en relación al calendario asociado, si existe. Si no existe un calendario asociado, entonces es equivalente a tener un calendario total. Por ejemplo, la expresión "5C" en el campo del día del mes significa el primer día incluido en el calendario que caiga en la fecha 5 del mes o con posterioridad a dicha fecha. Por ejemplo, la expresión "1C" en el campo de la semana del mes significa el primer día incluido en el calendario que caiga en domingo o después de un domingo.

NOTA: La compatibilidad para especificar valores tanto del día de la semana como del día del mes todavía no está finalizada. En dichos campos, utilice el caracter "?". La compatibilidad de las funciones asociadas al caracter "C" todavía no está finalizada. Los caracteres permitidos y los nombres de los meses y los días no distinguen entre mayúsculas y minúsculas. "MON" es lo mismo que "mon". Preste atención a los efectos de ? y * en los campos de día de la semana y día del mes.
Tenga cuidado cuando establezca las horas de disparo entre la medianoche y la 1:00 de la mañana. Los horarios de verano pueden causar saltos (o repeticiones) en función de si la hora se atrasa o si adelanta.

Ejemplos

Expresión	Significado
0 0 12 * * ?	Activar a las 12 pm (mediodía) todos los días
0 15 10 ? * *	Activar a las 10:15 am todos los días
0 15 10 * * ?	Activar a las 10:15 am todos los días
0 15 10 * * ? *	Activar a las 10:15 am todos los días
0 15 10 * * ? 2005	Activar a las 10:15 am todos los días durante el año 2005
0 * 14 * * ?	Activar cada minuto a partir de las 2 pm hasta las 2:59 pm, todos los días
0 0/5 14 * * ?	Activar cada 5 minutos a partir de las 2 pm hasta las 2:55 pm, todos los días
0 0/5 14,18 * * ?	Activar cada 5 minutos a partir de las 2 pm hasta las 2:55 pm, Y activar cada 5 minutos a partir de las 6 pm hasta las 6:55 pm, todos los días
0 0-5 14 * * ?	Activar cada minuto a partir de las 2 pm hasta las 2:05 pm, todos los días
0 10,44 14 ? 3 WED	Activar a las 2:10 pm y a las 2:44 pm todos los miércoles del mes de marzo.
0 15 10 ? * MON-FRI	Activar a las 10:15 am todos los lunes, martes, miércoles, jueves y viernes
0 15 10 15 * ?	Activar a las 10:15 am el día 15 de cada mes
0 15 10 L * ?	Activar a las 10:15 am el último día de cada mes
0 15 10 ? * 6L	Activar a las 10:15 am el último viernes de cada mes
0 15 10 ? * 6L	Activar a las 10:15 am el último viernes de cada mes
0 15 10 ? * 6L 2002-2005	Activar a las 10:15 am todos los últimos viernes de cada mes durante los años 2002, 2003, 2004 y 2005
0 15 10 ? * 6#3	Activar a las 10:15 am el tercer viernes de cada mes
0 0 12 1/5 * ?	Activar a las 12 pm (mediodía) cada 5 días todos los meses, a partir del primer día del mes.
0 11 11 11 11 ?	Activar todos los días 11 de noviembre a las 11:11 am.

9

Creación de un certificado autofirmado con Keytool y generación de una solicitud de firma de certificado

NOTA: Esta sección explica los pasos necesarios para crear un certificado autofirmado para componentes basados en Java. Este proceso *no puede usarse* para crear un certificado autofirmado en componentes basados en .NET.

Recomendamos los certificados autofirmados *solamente* en entornos que no sean de producción.

Si su organización exige un certificado de servidor SSL, o si necesita crear un certificado por cualquier otro motivo, esta sección describe el proceso para crear un keystore de java usando la herramienta Keytool.

Keytool crea claves privadas que se transmiten en un formato de Solicitud de firma de certificado (CSR) a una Autoridad de certificación (CA), como puede ser VeriSign® o Entrust®. La CA, basada en esta CSR, crea y firma un certificado de servidor. El certificado de servidor se descarga entonces a un archivo, junto con el certificado de la autoridad de firma. Los certificados se importan luego al archivo cacerts.

Generación de un nuevo par de claves y un certificado autofirmado

1. Vaya hasta el directorio conf de Compliance Reporter, Console Web Services, Device Server, o Gatekeeper Web Services.
2. Realice una copia de seguridad de la base de datos de certificados predeterminada:

   Haga clic en Inicio > Ejecutar, y escriba move cacerts cacerts.old.
3. Agregue Keytool a la ruta del sistema. Escriba el siguiente comando en la línea de comandos:

   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. Para generar un certificado, ejecute Keytool como se muestra:

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Introduzca la siguiente información cuando Keytool se la solicite.

NOTA: Haga una copia de seguridad de los archivos de configuración antes de modificarlos. Cambie únicamente los parámetros especificados. Si se cambia algún otro dato de estos archivos, incluso las etiquetas, el sistema podría dañarse y presentar fallas. Dell no puede garantizar que los problemas derivados de modificaciones no autorizadas de estos archivos se puedan resolver sin reinstalar Enterprise Server.

- *Contraseña de keystore:* Ingrese una contraseña (los caracteres no compatibles son <>;&" '), y configure la variable en el archivo de componente conf al mismo valor, como se muestra:

  <Directorio de instalación de Compliance Reporter>\conf\eserver.properties. Configure el valor eserver.keystore.password =

  <Directorio de instalación de Console Web Services>\conf\eserver.properties. Configure el valor eserver.keystore.password =

  <Directorio de instalación de Device Server>\conf\eserver.properties. Configure el valor eserver.keystore.password =

- *Nombre completo:* Introduzca el nombre completo del servidor en el que está instalado el componente con el que está trabajando. Este nombre completo incluye el nombre de host y el nombre de dominio (ejemplo: server.dell.com).
- *Unidad organizacional:* Introduzca el valor apropiado (ejemplo: Seguridad).
- *Organización:* Introduzca el valor apropiado (ejemplo: Dell).
- *Ciudad o localidad:* Introduzca el valor apropiado (ejemplo: Austin).
- *Estado o provincia:* Introduzca el nombre de la provincia o el estado sin abreviar (ejemplo: Texas).
- Código de dos letras del país:

  Estados Unidos = US

  Canadá = CA

  Suiza = CH

  Alemania = DE

  España = ES

  Francia = FR

  Gran Bretaña = GB

  Irlanda = IE

  Italia = IT

  Países Bajos = NL
- La utilidad solicita la confirmación de que la información es correcta. De ser así, escriba `yes`.
  Si no lo es, escriba `no`. Keytool muestra cada valor ingresado previamente. Haga clic en **Intro** para aceptar el valor o cambie el valor y haga clic en **Intro**.
- *Contraseña clave para alias:* Si no introduce aquí otra contraseña, de forma predeterminada se utilizará la de Keystore.

Solicitud de certificado firmado a una Autoridad de certificación

Utilice este procedimiento para generar una solicitud de firma de certificado (CSR) para el certificado autofirmado creado en Generación de un nuevo par de claves y un certificado autofirmado.

1 Sustituya el mismo valor usado anteriormente para **<certificate-alias>**:

```
keytool -certreq -sigalg MD5withRSA -alias <certificate-alias> -keystore
.\cacerts -file <csr-filename>
```

Ejemplo:

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

El archivo .csr contendrá un par BEGIN/END que se usará durante la creación del certificado por parte de la CA.

Figura 9-1. Ejemplo de archivo .CSR

2 Siga el proceso de su organización para la adquisición de un certificado de servidor SSL de una autoridad de certificación. Envíe el contenido de <csr-filename> para su firma.

NOTA: Hay varios métodos para solicitar un certificado válido. Puede ver un método de **ejemplo** en Ejemplo de un método para solicitar un certificado.

3 Cuando reciba el certificado firmado, guárdelo en un archivo.

4 La práctica recomendada es realizar una copia de seguridad de este certificado, en caso de que ocurra un error durante el proceso de importación. Esta copia de seguridad evitará tener que comenzar todo el proceso otra vez.

Importación de un certificado raíz

NOTA: Si la autoridad de certificación del certificado raíz es Verisign (no Verisign Test), pase al siguiente procedimiento e importe el certificado firmado.

El certificado raíz de la autoridad de certificación valida los certificados firmados.

1 Haga una de las siguientes acciones:

- Descargue el certificado raíz de la autoridad de certificación y guárdelo en un archivo.
- Obtenga el certificado raíz del servidor de directorios empresarial.

2 Haga una de las siguientes acciones:

- Si está habilitando SSL para Compliance Reporter, Console Web Services, Device Server o Legacy Gatekeeper Connector, cambie al directorio del componente **conf**.
- Si está habilitando SSL entre el servidor y el servidor de directorios empresarial, cambie a **<Directorio de instalación de Dell>\Java Runtimes\jre1.x.x_xx\lib\security** (La contraseña predeterminada para el cacerts JRE es **changeit**).

3 Ejecute Keytool de la siguiente manera, para instalar el certificado raíz:

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

Ejemplo:

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

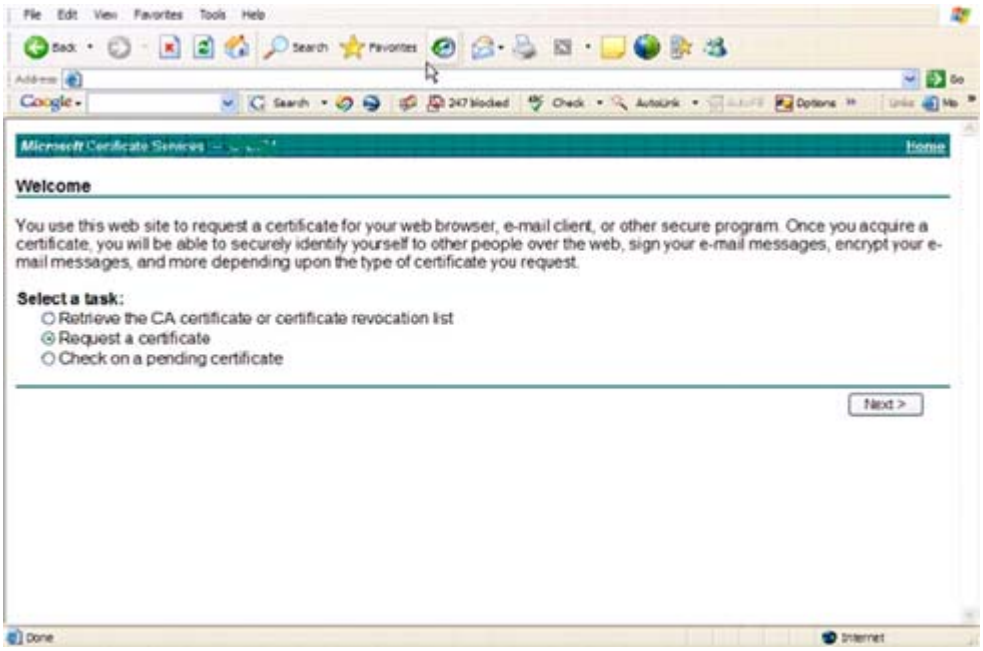
Ejemplo de un método para solicitar un certificado

Un ejemplo de un método para solicitar un certificado es usar un navegador web para acceder al servidor de CA de Microsoft, que su organización habría configurado internamente.

1 Navegue hasta el servidor de CA de Microsoft. Su organización le proporcionará la dirección IP.

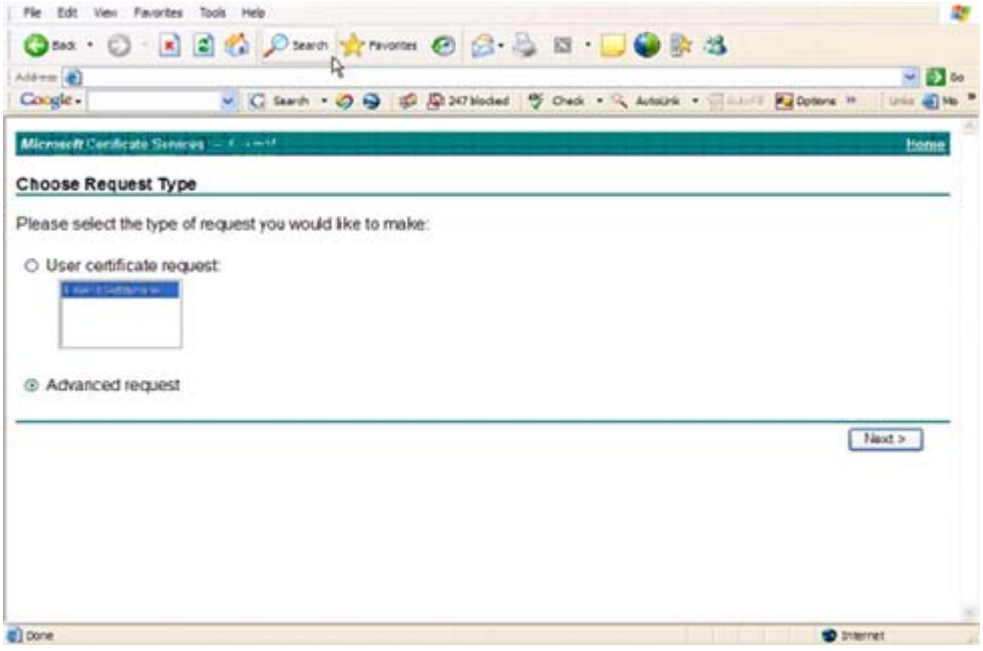
2 Seleccione **Request a certificate** y haga clic en **Next >**.

Figura 9-2. Servicios de certificación de Microsoft



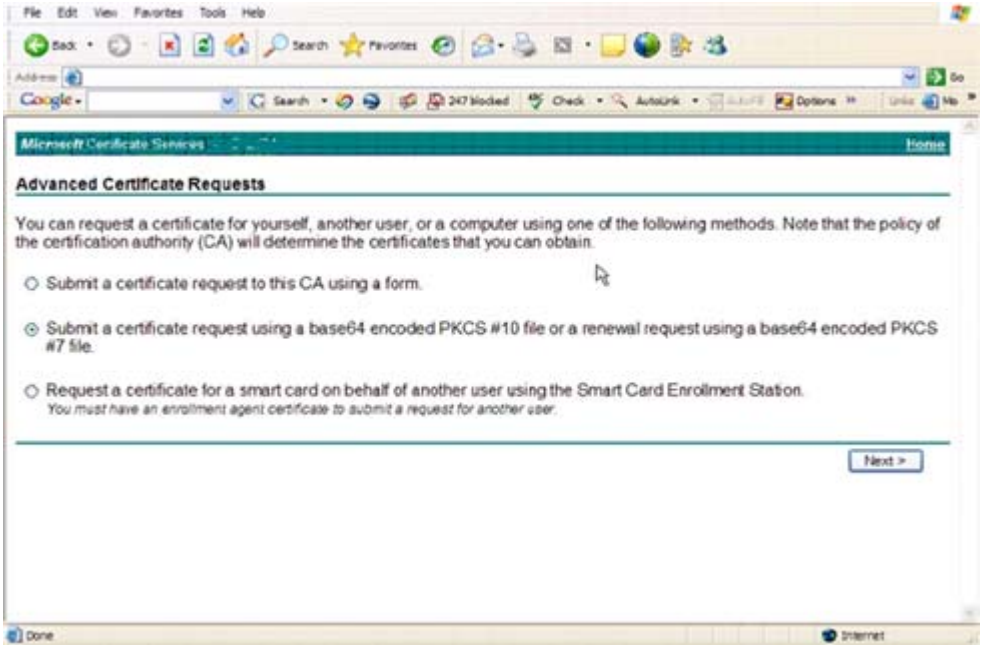
3 Seleccione **Advanced Request** y haga clic en **Next >**.

Figura 9-3. Selección del tipo de solicitud



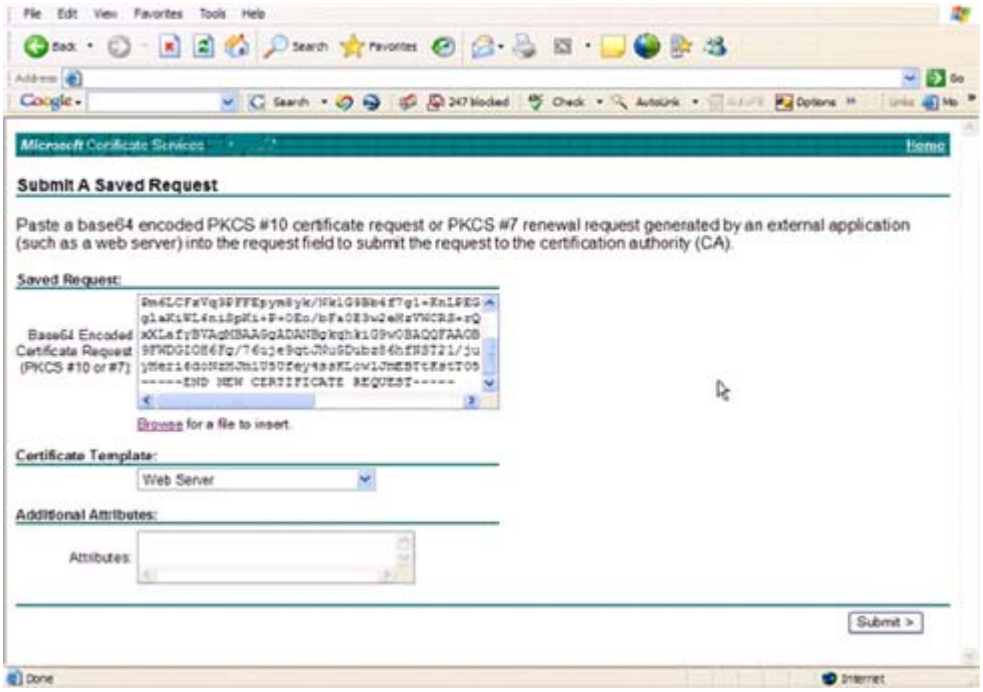
4 Seleccione la opción **Submit a certificate request using a base64 encode PKCS #10 file** y haga clic en **Next >**.

Figura 9-4. Solicitud de certificado avanzada



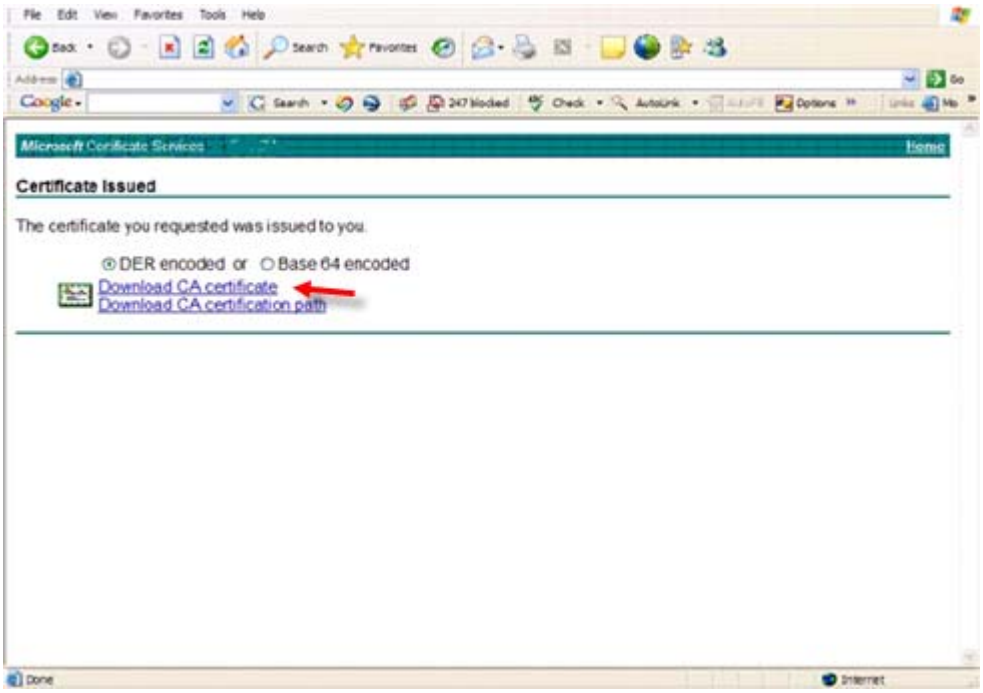
5 Pegue el contenido de la solicitud CSR en el cuadro de texto. Seleccione una plantilla de certificado de **Web Server** haga clic en **Submit >**.

Figura 9-5. Envío de una solicitud guardada



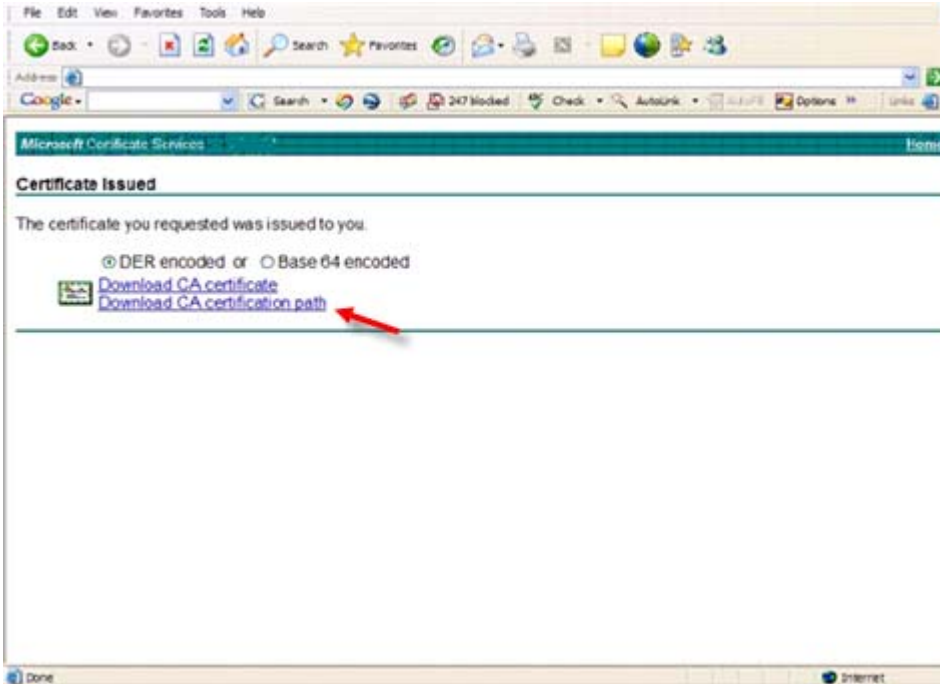
6 Guarde el certificado. Seleccione **DER encoded** y haga clic en **Download CA certificate**.

Figura 9-6. Descarga del certificado de la CA



7 Guarde el certificado. Seleccione **DER encoded** y haga clic en **Download CA certification path**.

Figura 9-7. Descarga de la ruta de certificación de la CA



8 Importe el certificado de la autoridad de firma convertido. Volver a la ventana de DOS. Escriba:

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

9 Ahora que ya ha importado el certificado de la autoridad de firma, puede importar el certificado del servidor (puede establecerse la cadena de confianza). Escriba:

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

Utilice el alias del certificado autofirmado para emparejar la solicitud de CSR con el certificado del servidor.

10 Al listar el archivo cacerts se verá que el certificado del servidor tiene una **longitud de cadena de certificado** de **2**, lo que indica que el certificado no es autofirmado. Escriba:

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

Observe que la huella digital del segundo certificado en la cadena es el certificado importado de la autoridad de certificación (que también aparece en el listado bajo el certificado del servidor en la lista).

El certificado del servidor se ha importado correctamente, junto con el certificado de la autoridad de firma.


0 XXXXXA0 X