Dell Data Protection

Guida alla configurazione

2014-02

Contenuto

1

Configurare Compatibility Server

In questo capitolo vengono forniti dettagli relativi ai parametri che è possibile modificare per adattare Compatibility Server all'ambiente in uso. Prima di eseguire qualsiasi modifica, effettuare sempre il backup dei file di configurazione.

Modificare esclusivamente i parametri documentati in questo file. La modifica di altri dati in questi file, inclusi i tag, può determinare danneggiamenti e guasti del sistema. Dell non può garantire la risoluzione dei problemi derivanti da modifiche non autorizzate a questi file senza dover reinstallare Compatibility Server.

server_config.xml

È possibile modificare alcuni tra i parametri indicati di seguito in **<directory di installazione di Compatibility Server>\conf\server_config.xml**. È presente un'indicazione per i parametri che non è opportuno modificare. Se Compatibility Server è in esecuzione, è necessario arrestare il servizio Compatibility Server, modificare il file server_config.xml e riavviare il servizio Compatibility Server per rendere effettive le modifiche a questo file.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
secrets.location	$dell.home$/conf/secretKeyStore	Percorso predefinito di secretkeystore. Se si modifica questo file dalla posizione predefinita, aggiornare questo parametro.
archive.location	$dell.home$/conf/archive	Percorso predefinito dell'archivio. Se si modifica questo file dalla posizione predefinita, aggiornare questo parametro.
domain.qualified.authentication	true	Indica se è richiesto un nome di accesso utente completo per tutte le richieste al server. Se il valore viene modificato, sarà necessario riavviare Device Server per rendere effettivo il nuovo valore.
directory.max.search.size	1000	Limite in una directory *find* dopo il quale verrà generata un'eccezione.
directory.server.search.timeout.seconds	60	Timeout del server in secondi per ricerche LDAP.
directory.client.search.timeout	60	Timeout del client in secondi per ricerche LDAP.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
rmi.recovery.host		Per utilizzare il recupero EMS multiserver: <!-- - rimuovere i commenti e modificare i nomi host nei nomi di dominio completi per concatenare il recupero <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	Nome predefinito del gruppo a cui appartengono tutti i proxy criteri per impostazione predefinita. È possibile modificare questo nome qui oppure in context.properties all'interno di Device Server. Se si modifica il nome del gruppo qui, sarà necessario modificarlo anche in Device Server se si intende: • proteggere i dispositivi Windows; • utilizzare CREDActivate. È consigliabile che tutti i proxy criteri appartengano a un unico gruppo.
rsa.securid.enabled	false	Se si utilizza RSA SecurID versione 6 per Microsoft Windows come sostituzione di GINA, impostare questo parametro su true, quindi arrestare e riavviare il servizio Compatibility Server. Quando gli utenti di Shield eseguono l'attivazione in un ambiente RSA di sostituzione di GINA, l'autenticazione RSA sostituisce l'autenticazione LDAP.
inv.queue.task.worker.size	10	Numero di thread che elaborano la coda di inventario.
inv.queue.task.timeout.seconds	900	Numero di secondi prima che si verifichi il timeout.
inv.queue.task.retry.count	3	Numero di tentativi di elaborazione dell'inventario da parte del server prima che venga ignorato.
report.retry.max	120	Numero massimo di nuovi tentativi.
report.retry.wait.millis	250	Numero di millisecondi di attesa prima di un nuovo tentativo.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
triage.execute.time	0 0 0/6 * *	La valutazione è il processo di riconciliazione degli utenti e dei gruppi già noti al server. L'impostazione predefinita è 0 0 0/6 * * ?, ovvero viene effettuata una valutazione ogni 6 ore a partire da mezzanotte (mezzanotte, 6.00, mezzogiorno, 18.00, mezzanotte...)
gatekeeper.service.max.sessions	5	Numero massimo di sessioni di proxy criteri.
gatekeeper.service.max.session.timeout	5	Timeout per il numero massimo di sessioni di proxy criteri.
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	Ruolo richiesto per aggiornare i ruoli amministrativi di un utente o un gruppo.
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	Ruolo richiesto per aggiornare i ruoli amministrativi di un utente o un gruppo
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin,LogAdmin	Ruoli richiesti per recuperare sessioni di registro.
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin,LogAdmin	Ruoli richiesti per recuperare registri.
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin,LogAdmin	Ruoli richiesti per recuperare l'elenco di colonne del registro.
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin,LogAdmin	Ruoli richiesti per recuperare l'elenco di categorie del registro.
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin,LogAdmin	Ruoli richiesti per recuperare l'elenco di priorità del registro.
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin,SecAdmin,HelpDeskAdmin,SystemAdmin	Ruoli richiesti per recuperare nomi ID univoci.
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	Ruolo richiesto per recuperare l'elenco di amministratori nel sistema.
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	Ruolo richiesto per impostare la password amministratore con privilegi avanzati.
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	Ruolo richiesto per reimpostare la password amministratore con privilegi avanzati.
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin,SecAdmin	Ruoli richiesti per aggiungere domini.
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin,SecAdmin	Ruoli richiesti per rimuovere domini.
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin,SecAdmin	Ruoli richiesti per aggiornare domini.
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin,SecAdmin	Ruoli richiesti per aggiungere gruppi.
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin,SecAdmin	Ruoli richiesti per rimuovere gruppi.
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin,SecAdmin	Ruoli richiesti per trovare gruppi LDAP.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin,SecAdmin	Ruoli richiesti per trovare utenti LDAP.
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin,SecAdmin	Ruoli richiesti per aggiungere utenti.
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	Ruolo richiesto per aggiungere licenze Enterprise.
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	Ruolo richiesto per visualizzare la licenza Enterprise.
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin,SecAdmin	Ruoli richiesti per ripristinare un dispositivo.
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin,SecAdmin	Ruoli richiesti per sospendere utenti.
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	Ruoli richiesti per attivare dispositivi in base al proxy.
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin,SecAdmin	Ruoli richiesti per ripristinare manualmente un dispositivo in base al proxy.
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Ruolo richiesto per recuperare il file di risorse di Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Ruolo richiesto per approvare il file di risorse di Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Ruoli richiesti per approvare la configurazione di Gatekeeper.
policy.arbiter.security.mode	most-restrictive	Questa proprietà controlla il funzionamento dell'algoritmo di mappatura per gli elementi dei criteri che presentano differenze nei livelli di sicurezza se un criterio include più nodi padre. Valori: Least-restrictive: viene utilizzato il valore dell'elemento meno restrittivo degli elementi padre Most-restrictive: viene utilizzato il valore dell'elemento più restrittivo di tutti gli elementi padre
policy.set.synchronization.sync-unmodified	true	Questo flag indica che la successiva sincronizzazione esterna dovrà aggiungere o eseguire nuovamente la mappatura di tutti gli elementi dei criteri senza impostare il flag modificato su true. Il flag viene impostato su false in seguito a ogni sincronizzazione, pertanto dovrà essere reimpostato se l'amministratore della sicurezza desidera aggiungere elementi senza modifiche. Si tratta di un'opzione avanzata.
db.schema.version.major		Schema database principale.
db.schema.version.minor		Schema database secondario.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
db.schema.version.patch		Versione di patch dello schema database.
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	Percorso predefinito del driver del database. Se si modifica questo file dalla posizione predefinita, aggiornare questo parametro.
dao.db.host		Nome host del server database. Questo parametro viene modificato nello strumento di configurazione.
dao.db.name		Nome del database. Questo parametro viene modificato nello strumento di configurazione.
dao.db.user		Nome utente con autorizzazioni complete per il database. Questo parametro viene modificato nello strumento di configurazione.
dao.db.password		Password del nome utente con autorizzazioni complete per il database. Questo parametro viene modificato nello strumento di configurazione.
dao.db.max.retry.count	10	Numero massimo di tentativi di riconnessione a SQL Server da parte di Compatibility Server se si verifica un errore di socket specificato.
dao.db.connection.retry.wait.seconds	5	Il primo tentativo di riconnessione è immediato. Il secondo tentativo si verifica dopo il numero di secondi specificato. Il terzo si verifica dopo il numero raddoppiato di secondi specificato, il quarto dopo il numero triplicato e così via.
dao.connection.pool.max.uses	10000	Consente il ritiro delle connessioni. Un valore pari a 0 indica nessun ritiro.
dao.connection.pool.inactive.threshold.seconds	900	Consente di determinare se una connessione non è stata utilizzata e può essere chiusa.
dao.db.driver.socket.errors	0	Compatibility Server tenta di riconnettersi a SQL Server se si verificano errori corrispondenti ai codici inclusi in questo elenco separato da virgole. 0 è il codice per gli errori di socket relativi a Microsoft SQL. È inoltre possibile aggiungere 17142 per gli errori di sospensione del server e 6002 per gli errori di arresto del server.
dao.db.mssql.compatability.level	90	Valore per SQL 2005 o versioni successive.
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	Gestore file di autorizzazione.
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	Gestore file di inventario.
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	Gestore file di eventi.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Se si sposta il file di risorse di Gatekeeper dal percorso predefinito, aggiornare questo parametro.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Se si sposta il file di risorse di Gatekeeper dal percorso predefinito, aggiornare questo parametro.
rmi.server.registry.host	localhost	La proprietà host è utile esclusivamente ai programmi client per determinare la posizione del registro. Non viene utilizzata durante la creazione di oggetti remoti e del registro RMI. Verrà creata in localhost.
rmi.server.registry.port	1099	La porta del registro RMI è configurabile durante l'installazione. Sarà inoltre possibile modificare la porta in seguito all'installazione mediante questo parametro. Se si modifica questo valore, sarà necessario configurare anche Gatekeeper Web Services.
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per impostare l'autorizzazione dei rapporti del server.
security.authorization.method.IReportingService.removeEntity	SystemAdmin	Ruolo richiesto per rimuovere entità del server.
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	Ruolo richiesto per impostare la visibilità delle entità del server.
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare la pagina relativa ai dettagli del dispositivo.
security.authorization.method.IReportingService.openSession	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per aprire una sessione server.
security.authorization.method.IReportingService.getPagedReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto in pagine.
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per il tipo di dispositivo.
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per il sistema operativo.
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare i rapporti per i modelli di dispositivo.
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per i dettagli dei criteri.
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per i dettagli della workstation.
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per gli errori di crittografia.
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per il riepilogo della crittografia.
security.authorization.method.IReportingService.getUserDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per i dettagli dell'utente.

server_config.xml		
Parametro	**Predefinito**	**Descrizione**
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per i dettagli del gruppo.
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Ruoli richiesti per visualizzare il rapporto per l'elenco di domini.
security.authorization.method.IKeyService.getKeys	ForensicAdmin	Impostazione utilizzata con un plug-in di integrazione Forensic. Se è necessaria l'integrazione di uno strumento Forensic, contattare l'assistenza Dell.
accountType.nonActiveDirectory.enabled	false	L'abilitazione di attivazioni non di dominio è una configurazione avanzata con conseguenze di vario tipo. *PRIMA* di abilitare questa configurazione, contattare il servizio di assistenza clienti per discutere delle esigenze specifiche dell'ambiente. Una volta modificato questo valore, riavviare il servizio Compatibility Server. Oltre a questa impostazione, creare o modificare l'impostazione del Registro di sistema nel computer Windows, come indicato di seguito. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations=REG_DWORD:1

gkresource.xml

È possibile modificare i parametri in <directory di installazione di Compatibility Server>\conf\gkresource.xml.

È consigliabile tenere traccia delle modifiche con commenti all'inizio del file. In questo modo sarà più semplice trasferire le modifiche al nuovo file in fase di aggiornamento.

NOTA: il file gkresource.xml dovrà essere un file XML ben formato. Dell sconsiglia di modificare questo file se non si è esperti di XML. Accertarsi di utilizzare riferimenti di entità laddove appropriato, anziché caratteri speciali (senza escape) non elaborati.

Un amministratore di sistema deve approvare le modifiche al file di risorse di Gatekeeper affinché vengano rese effettive.

Abilitare il formato dominio\nome utente

Aggiungere la seguente stringa per abilitare o disabilitare il formato dominio/nome utente. Il formato è disabilitato se la stringa non è presente nel file. Può inoltre essere disabilitato impostando il valore su 0.

1. Passare a <directory di installazione di Compatibility Server>\conf.
2. Aprire il file gkresource.xml con un editor XML.
3. Aggiungere la stringa:

   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. Salvare e chiudere il file.

run-service.conf

È possibile modificare alcuni tra i seguenti parametri in **<directory di installazione di Compatibility Server>\conf\run-service.conf**. Questi parametri vengono automaticamente impostati durante l'installazione. Per personalizzare o apportare modifiche di configurazione a qualsiasi servizio, attenersi alla procedura descritta di seguito.

1. Arrestare il servizio.
2. Rimuovere il servizio.
3. Modificare e salvare il file **run-service.conf**. È consigliabile tenere traccia delle modifiche con commenti all'inizio del file.
4. Reinstallare il servizio.
5. Avviare il servizio.

run-service.conf		
Parametro	**Predefinito**	**Descrizione**
JAVA_HOME	Dell\Java Runtime\jreX.x	Percorso della directory di installazione di Java.
wrapper.java.additional.5	n/d	L'indirizzo MAC in questa riga corrisponde a quello della scheda Ethernet locale. Se il server include più schede di interfaccia di rete o si desidera eseguire l'associazione a una scheda diversa da quella principale, immettere qui l'indirizzo MAC fisico della scheda dell'interfaccia di rete senza trattini.
wrapper.ntservice.name	EpmCompatSvr	Nome del servizio.
wrapper.ntservice.displayname	Dell Compatibility Server	Nome visualizzato del servizio.
wrapper.ntservice.description	Enterprise Compatibility Server	Descrizione del servizio.
wrapper.ntservice.dependency.1		Dipendenze del servizio. Aggiungere dipendenze in base alle esigenze, a partire da 1.
wrapper.ntservice.starttype	AUTO_START	Modalità di installazione del servizio: AUTO_START o DEMAND_START.
wrapper.ntservice.interactive	false	Se si imposta su true, il servizio potrà interagire con il desktop.

2

Configurare Core Server

In questo capitolo vengono forniti dettagli relativi ai parametri che è possibile modificare per adattare Core Server all'ambiente in uso.

Modificare esclusivamente i parametri documentati in questo file. La modifica di altri dati in questi file, inclusi i tag, può determinare danneggiamenti e guasti del sistema. Dell non può garantire la risoluzione dei problemi derivanti da modifiche non autorizzate a questi file senza dover reinstallare Core Server.

Modificare l'arbitraggio dei criteri dal livello più sicuro al livello meno sicuro

PolicyService.config

Modificare questa impostazione per cambiare l'arbitraggio dei criteri dal livello più sicuro al meno sicuro. Modificare l'impostazione in **<directory di installazione di Core Server>\PolicyService.config**. Se Core Server è in esecuzione, arrestare il servizio, modificare il file PolicyService.config, quindi riavviare il servizio affinché le modifiche vengano rese effettive.

È consigliabile tenere traccia delle modifiche con commenti all'inizio del file. In questo modo sarà più semplice trasferire le modifiche al nuovo file PolicyServiceConfig.xml in fase di aggiornamento.

Modificare la seguente sezione:

```
<!-- 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" /> [modificare questo valore da "0" a "1" per impostarlo su un livello meno sicuro]
</object>
```

Disabilitare i servizi Web

NOTA: è consigliabile modificare questa impostazione avanzata solo con il supporto del servizio di assistenza clienti.

Per disabilitare i servizi Web in Core Server (ad esempio in presenza di una seconda installazione di Core Server esclusivamente per l'elaborazione dell'inventario), modificare le impostazioni in:

<directory di installazione di Core Server>

Credant.Server2.WindowsService.exe.Config

e

<directory di installazione di Core Server>\Spring.config

Se Core Server è in esecuzione, arrestare il servizio, modificare le impostazioni in questi due file, quindi riavviare il servizio affinché le modifiche a questo file vengano rese effettive.

Credant.Server2.WindowsService.exe.Config

Rimuovere la seguente sezione:

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

Spring.config

Rimuovere quanto segue:

Rimuovere tutte le definizioni <object> </object> nelle intestazioni **AOP Advice**, **Web Service Target Definition** e **Web Service Host Definition**.

Abilitare il server SMTP per le notifiche e-mail sulle licenze

Se si utilizza Dell Data Protection | Cloud Edition, queste impostazioni vengono automatizzate mediante lo strumento di configurazione server. Attenersi alla procedura descritta di seguito se è necessario abilitare il server SMTP per le notifiche e-mail sulle licenze per scopi al di fuori dell'ambito di Dell Data Protection | Cloud Edition.

NotificationObjects.config

Per configurare il server SMTP per le notifiche e-mail sulle licenze, modificare il file **NotificationObjects.config** in **<directory di installazione di Core Server>**.

Modificare quanto segue:

```
<object name="EmailNotification" singleton="false" type="Credant.Notification.EmailNotification,
Credant.Notification"> [non modificare questo valore]
  <property name="NotificationDataFactory" ref="NotificationDataFactory"/> [non modificare questo valore]
  <property name="Host" value="test.dell.com"/>
  <property name="Port" value="25"/>
  <property name="Username" value="nomeutente"/>
  <property name="Password" value="${SmtpPassword}"/> [non modificare questo valore]
  <property name="Logger" ref="NotificationLogger"/> [non modificare questo valore]
</object>
```

Notification.config

Se il server della posta richiede l'autenticazione, modificare il file **Notification.config** in **<directory di installazione di Core Server>**.

Modificare quanto segue:

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

Aggiungere il percorso della cartella di Compatibility Server al file di configurazione di Core Server

Core Server è un'applicazione .NET e pertanto può non essere in grado di accedere alle informazioni del Registro di sistema per via delle autorizzazioni. Il problema risiede nel fatto che, per poter leggere secretkeystore (chiave di crittografia del database), Core Server deve accedere alle informazioni di configurazione del Registro di sistema di Compatibility Server per il percorso di secretkeystore. Se le relative autorizzazioni impediscono l'accesso, Core Server non potrà autenticare gli utenti della console. Con questa impostazione il percorso della cartella di Compatibility Server viene aggiunto al file di configurazione di Core Server in caso di problemi di accesso al Registro di sistema.

1. Passare a <directory di installazione di Core Server>\EntityDataAccessObjects.config.
2. Modificare il seguente elemento in **grassetto**:

   ```
   <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"/> -->
   ```

   Rimuovere i commenti in questa riga e impostare il percorso completo su Compatibility Server.

   ```
   </object>
   ```

3. Salvare e chiudere il file.
4. Riavviare i servizi Core Server e Compatibility Server.

Consentire l'iterazione di Core Server attraverso metodi di autenticazione

I tentativi di autenticazione di Core Server possono essere bloccati dal controller di dominio a causa dei criteri impostati nei metodi di autenticazione consentiti. Il miglioramento consiste nell'implementare uno "switch" nel file di configurazione di Core Server per consentirne l'iterazione attraverso vari metodi di configurazione, nel tentativo di individuarne uno appropriato.

1. Passare a <directory di installazione di Core Server>\Spring.config.
2. Modificare il seguente elemento in **grassetto**:

   ```
   <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" />
   ```

   Impostare questo valore su "true" per abilitare la funzionalità.

   ```
     <!-- 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 Salvare e chiudere il file.

4 Riavviare il servizio Core Server.

3

Configurare Device Server

In questo capitolo vengono forniti dettagli relativi ai parametri che è possibile modificare per adattare Device Server all'ambiente in uso.

Modificare esclusivamente i parametri documentati in questo file. La modifica di altri dati in questi file, inclusi i tag, può determinare danneggiamenti e guasti del sistema. Dell non può garantire la risoluzione dei problemi derivanti da modifiche non autorizzate a questi file senza dover reinstallare Device Server.

eserver.properties

È possibile modificare i parametri indicati di seguito in **<directory di installazione di Device Server>\conf\eserver.properties**.

È consigliabile tenere traccia delle modifiche con commenti all'inizio del file. In questo modo sarà più semplice trasferire le modifiche al nuovo file in fase di aggiornamento.

eserver.properties		
Parametro	**Predefinito**	**Descrizione**
eserver.default.host	Servizio Device Server	Nome di dominio completo in cui è installato il servizio Device Server.
eserver.default.port	Enterprise Server 7.7 o versioni successive - 8443 Enterprise Server (versioni precedenti alla 7.7) - 8081	Porta in cui Device Server è in ascolto di richieste di attivazione in ingresso da dispositivi.
eserver.use.ssl	True	SSL è abilitato per impostazione predefinita. Per disabilitare SSL, impostare il parametro su False.
eserver.keystore.location	${context['server.home']}/conf/cacerts	Percorso del certificato SSL utilizzato da Device Server.
eserver.keystore.password	changeit	Se è stata modificata la password dell'Autorità di certificazione nello strumento di configurazione, il parametro verrà automaticamente aggiornato. Se si modifica l'Autorità di certificazione nello strumento di configurazione in qualsiasi momento dopo la configurazione iniziale, aggiornare questo parametro con la password KeyStore utilizzata.

eserver.properties		
Parametro	**Predefinito**	**Descrizione**
eserver.ciphers		Imposta l'elenco di crittografie. Ogni crittografia deve essere separata da una virgola. Se non viene indicato alcun valore, il socket consentirà qualsiasi crittografia supportata da Tomcat. Rimuovere i commenti dall'esempio indicato di seguito per impostare l'elenco di crittografie. Separare ogni crittografia con una virgola. Per un elenco dei nomi di suite di crittografia validi, consultare la guida di riferimento JSSE di 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

È possibile modificare alcuni tra i seguenti parametri in **<directory di installazione di Device Server>\conf\run-service.conf**. Questi parametri vengono automaticamente impostati durante l'installazione. Per personalizzare o apportare modifiche di configurazione a qualsiasi servizio, attenersi alla procedura descritta di seguito.

1. Arrestare il servizio.
2. Rimuovere il servizio.
3. Modificare e salvare il file **run-service.conf**. È consigliabile tenere traccia delle modifiche con commenti all'inizio del file.
4. Reinstallare il servizio.
5. Avviare il servizio.

run-service.conf		
Parametro	**Predefinito**	**Descrizione**
JAVA_HOME	Dell\Java Runtime\jreX.x	Percorso della directory di installazione di Java.
wrapper.ntservice.name	EpmDeviceSvr	Nome del servizio.
wrapper.ntservice.displayname	Dell Device Server	Nome visualizzato del servizio.
wrapper.ntservice.description	Enterprise Device Server	Descrizione del servizio.
wrapper.ntservice.dependency.1		Dipendenze del servizio. Aggiungere dipendenze in base alle esigenze, a partire da 1.
wrapper.ntservice.starttype	AUTO_START	Modalità di installazione del servizio: AUTO_START o DEMAND_START.
wrapper.ntservice.interactive	false	Se si imposta su true, il servizio potrà interagire con il desktop.

4

Configurare Security Server

In questo capitolo vengono forniti dettagli relativi ai parametri che è possibile modificare per adattare Security Server all'ambiente in uso.

Modificare esclusivamente i parametri documentati in questo file. La modifica di altri dati in questi file, inclusi i tag, può determinare danneggiamenti e guasti del sistema. Dell non può garantire la risoluzione dei problemi derivanti da modifiche non autorizzate a questi file senza dover reinstallare Security Server.

context.properties

È possibile modificare i parametri indicati di seguito in **<directory di installazione di Security Server>\webapps\xapi\WEB-INF\context.properties**.

È consigliabile tenere traccia delle modifiche con commenti all'inizio del file. In questo modo sarà più semplice trasferire le modifiche al nuovo file in fase di aggiornamento.

context.properties		
Parametro	**Predefinito**	**Descrizione**
default.gatekeeper.group.remote	CMGREMOTE	Nome del gruppo remoto di dispositivi. **Non modificare.**
xmlrpc.max.threads	250	Numero massimo di thread simultanei con questo Device Server.
default.auth.upn.suffix		Suffisso UPN aggiunto a un nome di accesso utente se il server richiede un nome di accesso completo non fornito nella richiesta.
device.manual.auth.enable	true	Indica se le autenticazioni manuali sono abilitate o disabilitate. **Non modificare**
service.activation.enable	true	Indica se le attivazioni sono gestite da Device Server. **Non modificare**
service.policy.enable	true	Indica se i criteri sono abilitati/disabilitati. **Non modificare**.
service.auth.enable	true	Indica se le autenticazioni sono gestite da Device Server.
service.forensic.enable	true	Impostazione utilizzata con un plug-in di integrazione Forensic. Se è necessaria l'integrazione di uno strumento Forensic, contattare l'assistenza Dell.
service.support.enable	true	Consente il recupero di metadati sul server.
service.device.enable	true	Consente il supporto di servizi Shield, ad esempio l'archiviazione delle chiavi SDE.

5

Configurare funzioni di crittografia

In questa sezione viene descritto come controllare in modo indipendente le funzioni di crittografia.

Impedire l'eliminazione dei file temporanei

Per impostazione predefinita, tutti i file temporanei nella directory c:\windows\temp vengono automaticamente eliminati durante l'installazione o l'aggiornamento di DDPE. L'eliminazione dei file temporanei velocizza il processo di crittografia iniziale e si verifica prima della procedura di ricerca crittografia.

Tuttavia, se l'organizzazione utilizza un'applicazione di terze parti che richiede di preservare la struttura dei file nella directory \temp, è opportuno evitare l'eliminazione di questi file.

Per disabilitare l'eliminazione dei file temporanei, creare o modificare l'impostazione del Registro di sistema come segue:

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

Se **non** si eliminano i file temporanei, la durata del processo di crittografia iniziale risulterà maggiore.

Nascondere le icone sovrapposte

Per impostazione predefinita, in fase di installazione tutte le icone di crittografia sovrapposte sono impostate come visibili. Utilizzare la seguente impostazione del Registro di sistema per nasconderle per tutti gli utenti gestiti in un computer in seguito all'installazione originale.

Creare o modificare l'impostazione del Registro di sistema come segue:

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)=1

Se un utente con privilegi appropriati sceglie di mostrare le icone di crittografia sovrapposte, l'impostazione sostituirà il valore del Registro di sistema.

Nascondere l'icona della barra di sistema

Per impostazione predefinita, in fase di installazione l'icona della barra di sistema è visibile. Utilizzare la seguente impostazione del Registro di sistema per nasconderla per tutti gli utenti gestiti in un computer in seguito all'installazione originale.

Creare o modificare l'impostazione del Registro di sistema come segue:

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)=1

Attivazione in slot

L'attivazione in slot è una funzione che consente di distribuire le attivazioni di Shield in un periodo di tempo preimpostato per agevolare il carico del server durante una distribuzione di massa. Le attivazioni vengono ritardate in base a periodi di tempo generati da un algoritmo, per garantire una distribuzione lineare dei tempi di attivazione.

L'attivazione in slot è abilitata e configurata tramite il programma di installazione o la workstation di Shield.

Per gli utenti che necessitano dell'attivazione tramite VPN, è possibile richiedere la configurazione di un'attivazione in slot per Shield al fine di ritardare l'attivazione iniziale in modo da garantire al software del client VPN il tempo necessario a stabilire una connessione di rete.

ATTENZIONE: configurare l'attivazione in slot esclusivamente con il servizio di assistenza clienti. Una configurazione in slot inappropriata potrebbe determinare l'attivazione simultanea di un numero elevato di client e causare seri problemi di prestazioni.

Per configurare l'attivazione in slot vengono utilizzate le seguenti chiavi del Registro di sistema. Le modifiche a queste chiavi verranno rese effettive solo in seguito al riavvio della workstation di Shield.

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

  Questa impostazione consente di abilitare o disabilitare la funzione di attivazione in slot.
  Disabilitata=0 (impostazione predefinita)
  Abilitata=1

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

  Periodo di tempo in secondi in cui si verificherà l'intervallo dell'attivazione in slot. È possibile utilizzare questa proprietà per ignorare il periodo di tempo in secondi in cui si verificherà tale intervallo. In un periodo di sette ore sono disponibili 25.200 secondi per le attivazioni in slot. L'impostazione predefinita è 86.400 secondi, ovvero una ripetizione giornaliera.

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

  Intervallo nella ripetizione, ACTIVATION_SLOT_CALREPEAT, in cui si verificano tutti gli slot dell'attivazione. È consentito un solo intervallo. È consigliabile impostare il valore 0,<CalRepeat>. Un valore diverso da 0 potrebbe generare risultati imprevisti. L'impostazioni predefinita è 0,86400. Per impostare una ripetizione ogni sette ore, utilizzare l'impostazione 0,25200. CALREPEAT verrà attivato all'accesso di un utente di Shield.

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

  Numero di slot di attivazione che è possibile ignorare prima che il computer tenti di attivarsi al successivo accesso dell'utente la cui attivazione è stata divisa in slot. Se l'attivazione ha esito negativo durante questo tentativo immediato, Shield riprenderà i tentativi di attivazione in slot. Se l'attivazione ha esito negativo per un errore di rete, verrà effettuato un nuovo tentativo alla riconnessione della rete, anche se il valore in MISSTHRESHOLD non è stato superato. Se un utente si disconnette prima del raggiungimento del periodo degli slot di attivazione, all'accesso successivo verrà assegnato un nuovo slot.

- HKCU/Software/CREDANT/ActivationSlot (dati per utente)

  Tempo posticipato per tentare l'attivazione in slot, impostata quando l'utente accede per la prima volta alla rete in seguito all'abilitazione dell'attivazione in slot. Lo slot di attivazione viene ricalcolato per ogni tentativo di attivazione.

- HKCU/Software/CREDANT/SlotAttemptCount (dati per utente)

  Numero di tentativi non riusciti o ignorati, quando sopraggiunge lo slot temporale e viene eseguito un tentativo di attivazione che ha esito negativo. Se il numero raggiunge il valore impostato in ACTIVATION_SLOT_MISSTHRESHOLD, il computer tenterà un'attivazione immediata al momento della connessione alla rete.

Per abilitare l'attivazione in slot tramite riga di comando, utilizzare un comando simile al seguente:

```
setup.exe /v"SLOTTEDACTIVATION=1 CALREPEAT=25200 SLOTINTERVALS=0,25200 <other parameters>"
```

NOTA: è importante ricordare che tutti i valori contenenti uno o più caratteri speciali, ad esempio uno spazio, devono essere racchiusi tra virgolette con escape.

Polling forzato

Utilizzare la seguente impostazione del Registro di sistema per fare in modo che Shield esegua il polling del server per un aggiornamento forzato dei criteri.

Creare o modificare l'impostazione del Registro di sistema come segue:

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD value)=1

A seconda della versione di Shield in uso, l'impostazione del Registro di sistema sparirà *o* passerà automaticamente da **1** a **0** al completamento del polling.

A seconda del gruppo di autorizzazioni di un utente amministratore, potrebbe essere necessario modificare le autorizzazioni per creare questa impostazione del Registro di sistema. Se si verificano problemi durante la creazione di un nuovo valore DWORD, attenersi alla procedura descritta di seguito per modificare le autorizzazioni.

1. Nel Registro di sistema di Windows passare a HKLM\SOFTWARE\Credant\CMGShield\Notify.
2. Fare clic con il pulsante destro del mouse su **Notifica** e scegliere **Autorizzazioni**.
3. All'apertura della finestra *Autorizzazione per Notifica* selezionare la casella di controllo **Controllo completo**.
4. Fare clic su **OK**.

È ora possibile creare la nuova impostazione del Registro di sistema.

Opzioni di inventario

Utilizzare le seguenti impostazioni del Registro di sistema per consentire l'invio da parte di Shield di un inventario ottimizzato al server, l'invio di un inventario completo al server o l'invio di un inventario completo per tutti gli utenti attivati al server.

Inviare l'inventario ottimizzato al server

Creare o modificare l'impostazione del Registro di sistema come segue:

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

OnlySendInvChanges (REG_DWORD)=1

Se non sono presenti voci, l'inventario ottimizzato verrà inviato al server.

Inviare l'inventario completo al server

Creare o modificare l'impostazione del Registro di sistema come segue:

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

OnlySendInvChanges (REG_DWORD)=0

Se non sono presenti voci, l'inventario ottimizzato verrà inviato al server.

Inviare l'inventario completo per tutti gli utenti attivati

Creare o modificare l'impostazione del Registro di sistema come segue:

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

RefreshInventory (REG_DWORD)=1

Questa voce verrà eliminata dal Registro di sistema nel momento in cui verrà elaborata. Il valore viene salvato nell'insieme di credenziali, pertanto anche se il computer viene riavviato prima del caricamento dell'inventario, Shield soddisferà comunque questa richiesta al successivo tentativo di caricamento riuscito.

Questa voce sostituisce il valore OnlySendInvChanges del Registro di sistema.

Attivazioni non di dominio

L'abilitazione di attivazioni non di dominio è una configurazione avanzata con conseguenze di vario tipo. Contattare il servizio di assistenza clienti per discutere delle esigenze specifiche dell'ambiente e ottenere istruzioni per abilitare questa funzione.

6

Configurare componenti per l'autenticazione/autorizzazione Kerberos

In questa sezione viene descritto come configurare componenti per l'utilizzo con l'autenticazione/autorizzazione Kerberos.

Configurare componenti per l'autenticazione/autorizzazione Kerberos

NOTA: se è necessario utilizzare l'autenticazione/autorizzazione Kerberos, il server contenente il componente Key Server dovrà essere parte integrante del dominio coinvolto.

Key Server è un servizio in ascolto dei client per la connessione tramite un socket. Al momento della connessione di un client, una connessione sicura verrà negoziata, autenticata e crittografata mediante API Kerberos (se non è possibile negoziare una connessione sicura, il client verrà disconnesso).

Key Server verificherà quindi con Device Server se l'utente che esegue il client è autorizzato ad accedere alle chiavi. Questo accesso viene consentito nella console di gestione remota tramite *singoli* domini.

Istruzioni per Servizi di Windows

1. Passare al pannello Servizi di Windows (Start > Esegui... > services.msc > OK).
2. Fare clic con il pulsante destro del mouse su Dell Key Server e scegliere **Proprietà**.
3. Accedere alla scheda **Connessione** e selezionare il pulsante di opzione **Account**.
4. Nel campo **Account** aggiungere l'utente di dominio desiderato. Questo utente dovrà disporre almeno dei diritti di amministratore locale per la cartella Key Server (deve essere in grado di scrivere nel file di configurazione di Key Server e nel file log.txt).
5. Fare clic su **OK**.
6. Riavviare il servizio (lasciare aperto il pannello Servizi di Windows per ulteriori operazioni).
7. Passare al file log.txt in <directory di installazione di Key Server> per verificare che il servizio sia stato avviato.

Istruzioni per il file di configurazione di Key Server

1. Passare a <directory di installazione di Key Server>.
2. Aprire il file Credant.KeyServer.exe.config con un editor di testo.
3. Accedere a <add key="user" value="superadmin" /> e modificare il valore "superadmin" con il nome dell'utente appropriato (è possibile mantenere "superadmin").

   Il formato di "superadmin" può essere qualsiasi metodo in grado di eseguire l'autenticazione al server. È accettabile il nome dell'account SAM, l'UPN o il formato dominio\nome utente. È accettabile qualsiasi metodo in grado di eseguire l'autenticazione al server, poiché la convalida è richiesta per l'account utente *specifico* ai fini dell'autorizzazione rispetto ad Active Directory.

   Ad esempio, in un ambiente multidominio, se si immette solo un nome di account SAM come "jdoe", l'operazione potrebbe avere esito negativo, in quanto il server non sarà in grado di autenticare "jdoe" poiché non riuscirà a trovarlo. In un ambiente multidominio è consigliabile utilizzare l'UPN, sebbene sia accettabile anche il formato dominio\nome utente.

In un ambiente con un solo dominio è accettabile l'utilizzo del nome dell'account SAM.

4 Accedere a <add key="epw" value="<valore crittografato della password>" /> e modificare "epw" in "password". Modificare quindi "<valore crittografato della password>" con la password dell'utente al passaggio 3. La password verrà nuovamente crittografata al riavvio del server.

Se si utilizza "superadmin" (passaggio 3) e la password superadmin non è "changeit", dovrà essere modificata in questo punto.

5 Salvare le modifiche e chiudere il file.

File di configurazione di esempio:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [porta TCP su cui sarà in ascolto il server. L'impostazione predefinita è 8050, ma può essere modificata.]
        <add key="maxConnections" value="2000" /> [numero di connessioni socket attive consentite dal server.]
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [URL di Device Server. Se si dispone di Enterprise Server 7.7 o versioni successive, il formato è https://keyserver.domain.com:8443/xapi/; se si dispone di una versione precedente, il formato è https://keyserver.domain.com:8081/xapi (senza barra finale).]
        <add key="verifyCertificate" value="false" /> [true abilita la verifica dei certificati. Impostare su false per non eseguire la verifica o in caso di utilizzo di certificati autofirmati.]
        <add key="user" value="superadmin" /> [nome utente utilizzato per comunicare con Device Server. Il tipo di amministratore Forensic dell'utente deve essere selezionato nella console di gestione remota. Il formato di "superadmin" può essere qualsiasi metodo in grado di eseguire l'autenticazione al server. È accettabile il nome dell'account SAM, l'UPN o il formato dominio|nome utente. È accettabile qualsiasi metodo in grado di eseguire l'autenticazione al server, poiché la convalida è richiesta per l'account utente specifico ai fini dell'autorizzazione rispetto ad Active Directory. Ad esempio, in un ambiente multidominio, se si immette solo un nome di account SAM come "jdoe", l'operazione potrebbe avere esito negativo, in quanto il server non sarà in grado di autenticare "jdoe" poiché non riuscirà a trovarlo. In un ambiente multidominio è consigliabile utilizzare l'UPN, sebbene sia accettabile anche il formato dominio|nome utente. In un ambiente con un solo dominio è accettabile l'utilizzo del nome dell'account SAM.]
        <add key="cacheExpiration" value="30" /> [durata (in secondi) in cui il servizio verificherà quali utenti sono autorizzati a chiedere chiavi. Il servizio mantiene una cache e tiene traccia della data di creazione. Una volta che la data della cache avrà superato il valore indicato (in secondi), verrà creato un nuovo elenco. Nel momento in cui un utente si connette, Key Server dovrà scaricare gli utenti autorizzati da Device Server. Se non è presente una cache per questi utenti o l'elenco non è stato scaricato negli ultimi "x" secondi, verrà nuovamente effettuato il download. Non si verificherà alcun polling, ma questo valore configurerà il livello di obsolescenza consentito per l'elenco prima che venga aggiornato.]
        <add key="epw" value="encrypted value of the password" /> [password utilizzata per comunicare con Device Server. Se la password superadmin è stata modificata, sarà necessario cambiarla in questo punto.]
    </appSettings>
</configuration>
```

Istruzioni per Servizi di Windows

1. Tornare al pannello Servizi di Windows.
2. **Riavviare** il servizio Dell Key Server.
3. Passare al file log.txt in <directory di installazione di Key Server> per verificare che il servizio sia stato avviato.
4. Chiudere il pannello Servizi di Windows.

Istruzioni per la console di gestione remota

1. Se necessario, accedere alla console di gestione remota.
2. Fare clic su **Domini** e quindi sull'icona **Dettaglio**.
3. Fare clic su **Key Server**.
4. Nell'elenco degli account Key Server aggiungere l'utente che eseguirà le attività di amministratore. Il formato è dominio\nome utente. Fare clic su **Aggiungi account**.
5. Fare clic su **Utenti** nel menu a sinistra. Nell'apposita casella cercare il nome utente aggiunto nel passaggio 4. Fare clic su **Cerca**.
6. Una volta individuato l'utente corretto, fare clic sull'icona **Dettaglio**.
7. Selezionare **Amministratore Forensic**. Fare clic su **Aggiorna**.

I componenti sono ora configurati per l'autenticazione/autorizzazione Kerberos.

7

Assegnazione del ruolo di Amministratore Forensic

Per impostazione predefinita, l'autorizzazione Forensic è abilitata nei server back-end e disabilitata nei server front-end. Queste impostazioni vengono posizionate in modo appropriato in fase di installazione per Device Server e Security Server.

Istruzioni per la console di gestione remota

1. Se necessario, accedere alla console di gestione remota.
2. Nel riquadro sinistro fare clic su **Gestisci** > **Utenti**.
3. Nella pagina *Ricerca utenti* immettere il nome dell'utente a cui associare il ruolo di amministratore Forensic, quindi fare clic su **Cerca** (le credenziali di questo utente vengono fornite durante l'esecuzione delle utilità CMGAd, CMGAu, CMGAlu e dell'agente decrittografia in modalità Forensic).
4. Nella pagina *Risultati ricerca utenti* fare clic sull'icona **Dettaglio**.
5. Nella pagina *Dettaglio utente per: <nome utente>* selezionare **Amministrazione**.
6. Nella colonna Utente selezionare **Amministratore Forensic** e fare clic su **Aggiorna**.

Il ruolo di Amministratore Forensic è ora impostato.

Disattivazione dell'autorizzazione Forensic

1. Dal server back-end, accedere a **<directory di installazione di Security Server>\webapps\xapi\WEB-INF\context.properties** e modificare la proprietà seguente:

   service.forensic.enable=true

   in

   service.forensic.enable=false
2. **Riavviare** il servizio Security Server.
3. Passare a **<directory di installazione di Device Server>\webapps\ROOT\WEB-INF\web.xml** e modificare la seguente:

   <init-param>

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

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

   </init-param>
4. **Riavviare** il servizio Device Server.
5. È consigliabile rimuovere il ruolo di Amministratore Forensic per gli utenti che non utilizzano attivamente le autorizzazioni per i ruoli.

8

Espressioni Cron

In questa sezione viene descritto come utilizzare formati di espressioni Cron e caratteri speciali.

Introduzione alle espressioni Cron

Cron è uno strumento UNIX in commercio da diverso tempo, pertanto le sue funzionalità di pianificazione sono efficaci e comprovate. La classe CronTrigger si basa sulle funzionalità di pianificazione di Cron.

CronTrigger utilizza espressioni Cron, che consentono di creare pianificazioni di attivazione, ad esempio alle ore 8.00 dal lunedì al venerdì oppure alle ore 1.30 ogni ultimo venerdì del mese.

Si tratta di espressioni efficaci, ma che possono creare confusione. L'obiettivo di questo documento è quello di tentare di fare chiarezza sulla creazione di un'espressione Cron, una risorsa a cui attingere prima di richiedere assistenza.

Formati di espressioni Cron

Le espressioni Cron sono costituite da 6 campi obbligatori e 1 campo facoltativo, separati da spazi. I campi possono contenere qualsiasi valore autorizzato, oltre a una serie di combinazioni di caratteri speciali consentiti per il campo specifico.

Le espressioni Cron possono essere semplici, come * * * * ? *,

o più complesse, ad esempio 0 0/5 14,18,3-39,52 ? GEN,MAR,SET LUN-VEN 2002-2010.

Di seguito vengono descritti i campi.

Nome del campo	Obbligatorio?	Valori consentiti	Caratteri speciali consentiti
Minutes	Sì	0-59	, - * /
Hours	Sì	0-23	, - * /
Day of month	Sì	1-31	, - * ? / L W C
Month	Sì	1-12 o JAN-DEC	, - * /
Day of week	Sì	1-7 o SUN-SAT	, - * ? / L C #
Year	No	vuoto, 1970-2099	, - * /

Caratteri speciali

- Il carattere * consente di specificare tutti i valori. Ad esempio, * nel campo dei minuti indica ogni minuto.
- Il carattere ? (nessun valore specifico) risulta utile in caso sia necessario specificare un valore in uno dei due campi in cui il carattere è consentito, ma non nell'altro. Ad esempio, per eseguire un'attivazione in un giorno specifico del mese (10), indipendentemente dal giorno della settimana, utilizzare 10 nel campo relativo al giorno del mese e ? in quello del giorno della settimana.
- Il carattere - consente di specificare intervalli. Ad esempio, 10-12 nel campo delle ore indica 10.00, 11.00 e 12.00.
- Il carattere , consente di specificare valori aggiuntivi. Ad esempio, MON,WED,FRI nel campo del giorno della settimana indica i giorni lunedì, mercoledì e venerdì.

- Il carattere / consente di specificare incrementi.

  0/15 nel campo dei secondi indica i secondi 0, 15, 30 e 45.

  5/15 nel campo dei secondi indica i secondi 5, 20, 35 e 50.

  Specificare * prima di / corrisponde a specificare 0 come valore di partenza.

  1/3 nel campo del giorno del mese indica l'attivazione ogni 3 giorni a partire dal primo giorno del mese.

  In sostanza, per ogni campo dell'espressione è disponibile un insieme di numeri che possono essere attivati o disattivati. Per i secondi e i minuti, il numero varia da 0 a 59, per le ore da 0 a 23, per i giorni del mese da 0 a 31 e per i mesi da 1 a 12. Il carattere / consente di attivare ogni valore numerico nell'insieme specifico. Pertanto, 7/6 nel campo del mese consente di attivare semplicemente il mese 7 e non ogni sesto mese.

- Il carattere L è consentito per i campi del giorno del mese e della settimana. Questo carattere significa "last" (ultimo), ma cambia di significato a seconda del campo.

  Il valore L nel campo del giorno del mese indica l'ultimo giorno del mese (31 per gennaio, 28 per febbraio negli anni non bisestili).

  Se utilizzato nel campo del giorno della settimana, indica 7 o domenica.

  Se utilizzato nel campo del giorno della settimana dopo un altro valore, indica l'ultimo giorno xxx del mese. Ad esempio, 6L indica l'ultimo sabato del mese. Se si utilizza l'opzione L, è importante non specificare elenchi o intervalli di valori, in quanto si otterrebbero risultati poco chiari.

- Il carattere W è consentito per il campo del giorno del mese. Significa "weekday" (giorno feriale) e consente di specificare il giorno feriale (lunedì/venerdì) più vicino al giorno indicato. Se ad esempio si specifica 15W come valore per il campo del giorno del mese, indica il giorno feriale più vicino al 15 del mese. Se il giorno 15 è un sabato, l'attivazione avrà luogo venerdì 14, se è una domenica, avverrà lunedì 16, mentre se è un martedì, si verificherà martedì 15. Se tuttavia si specifica 1W come valore per il giorno del mese e il giorno 1 è un sabato, l'attivazione avrà luogo lunedì 3, poiché non verrà eseguito il passaggio da un mese all'altro. Il carattere W può essere specificato solo se il giorno del mese è indicato come singolo giorno e non come un intervallo o un elenco di giorni.

  I caratteri L e W possono inoltre essere combinati per generare l'espressione del giorno del mese LW, a indicare l'ultimo giorno feriale del mese.

- Il carattere # è consentito per il campo del giorno della settimana. Consente di specificare il valore numerico del giorno xxx del mese. Ad esempio, il valore 6#3 nel campo del giorno della settimana indica il terzo sabato del mese (giorno 6 = sabato e #3 = il terzo del mese).

  Altri esempi:
  2#1 = primo martedì del mese
  4#5 = quinto giovedì del mese.

  Se si specifica #5, ma non è presente il quinto giorno della settimana nel mese specifico, l'attivazione non avrà luogo nel mese in corso.

- Il carattere C è consentito per il calendario e indica che i valori vengono calcolati in base a un eventuale calendario associato. Se non è associato alcun calendario, verrà considerato un calendario globale. Il valore 5C nel campo del giorno del mese indica il primo giorno incluso nel calendario corrispondente al 5 o dopo di esso. Il valore 1C nel campo del giorno della settimana indica il primo giorno incluso nel calendario corrispondente alla domenica o dopo di essa.

NOTA: il supporto per indicare un valore per il giorno della settimana e del mese non è completo. Utilizzare il carattere ? in uno di questi campi. Il supporto per le funzioni descritte per il carattere C non è completo. I caratteri e i nomi dei mesi e dei giorni della settimana validi non fanno distinzione tra lettere maiuscole e minuscole. MON è uguale a mon. Prestare massima attenzione agli effetti dei caratteri ? e * nei campi del giorno della settimana e del mese.
Procedere con la massima cautela nel caso in cui si specifichi l'attivazione tra la mezzanotte e l'una. L'ora legale può determinare il salto o la ripetizione di un'ora a seconda della situazione specifica.

Esempi

Espressione	Significato
0 0 12 * * ?	Attivazione alle 12.00 (mezzogiorno) ogni giorno
0 15 10 ? * *	Attivazione alle 10.15 ogni giorno
0 15 10 * * ?	Attivazione alle 10.15 ogni giorno
0 15 10 * * ? *	Attivazione alle 10.15 ogni giorno
0 15 10 * * ? 2005	Attivazione alle 10.15 ogni giorno del 2005
0 * 14 * * ?	Attivazione ogni minuto a partire dalle 14.00 e fino alle 14.59 di ogni giorno
0 0/5 14 * * ?	Attivazione ogni 5 minuti a partire dalle 14.00 e fino alle 14.55 di ogni giorno
0 0/5 14,18 * * ?	Attivazione ogni 5 minuti a partire dalle 14.00 e fino alle 14.55 E ogni 5 minuti a partire dalle 18.00 e fino alle 18.55 ogni giorno
0 0-5 14 * * ?	Attivazione ogni minuto a partire dalle 14.00 e fino alle 14.05 di ogni giorno
0 10,44 14 ? 3 WED	Attivazione alle 14.10 e alle 14.44 ogni mercoledì di marzo.
0 15 10 ? * MON-FRI	Attivazione alle 10.15 ogni lunedì, martedì, mercoledì, giovedì e venerdì
0 15 10 15 * ?	Attivazione alle 10.15 il giorno 15 di ogni mese
0 15 10 L * ?	Attivazione alle 10.15 l'ultimo giorno di ogni mese
0 15 10 ? * 6L	Attivazione alle 10.15 l'ultimo sabato di ogni mese
0 15 10 ? * 6L	Attivazione alle 10.15 l'ultimo sabato di ogni mese
0 15 10 ? * 6L 2002-2005	Attivazione alle 10.15 l'ultimo sabato di ogni mese durante gli anni 2002, 2003, 2004 e 2005
0 15 10 ? * 6#3	Attivazione alle 10.15 il terzo sabato di ogni mese
0 0 12 1/5 * ?	Attivazione alle 12.00 (mezzogiorno) ogni 5 giorni di ogni mese, a partire dal primo giorno del mese.
0 11 11 11 11 ?	Attivazione ogni 11 novembre alle 11.11.

9

Creare un certificato autofirmato mediante Keytool e generare una richiesta di firma del certificato

NOTA: in questa sezione sono illustrati in dettaglio i passaggi per creare un certificato autofirmato per i componenti basati su Java. Questo processo *non* può essere utilizzato per creare un certificato autofirmato per componenti basati su .NET.

È consigliabile utilizzare un certificato autofirmato *solo* in un ambiente non di produzione.

Se l'organizzazione richiede un certificato server SSL oppure è necessario creare un certificato per altri motivi, in questa sezione viene descritto il processo per creare un archivio chiavi Java mediante Keytool.

Keytool consente di creare chiavi private passate nel formato CSR (Certificate Signing Request, richiesta di firma del certificato) a un'Autorità di certificazione, come VeriSign® o Entrust®. L'Autorità, in base a questa richiesta, creerà quindi un certificato server per la firma. Il certificato server verrà scaricato in un file insieme a quello dell'autorità di firma. Entrambi verranno infine importati nel file dell'Autorità di certificazione.

Generare una nuova coppia di chiavi e un certificato autofirmato

1. Passare alla directory **conf** di Compliance Reporter, Console Web Services, Device Server o Gatekeeper Web Services.
2. Eseguire il backup del database di certificati predefinito:

   Fare clic sul pulsante **Start** > scegliere **Esegui** e digitare **move cacerts cacerts.old**.
3. Aggiungere Keytool al percorso di sistema. Al prompt dei comandi digitare il seguente comando:

   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. Per generare un certificato, eseguire Keytool come illustrato di seguito:

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Immettere le seguenti informazioni quando richiesto da Keytool.

NOTA: prima di modificare i file di configurazione, eseguirne il backup. Modificare esclusivamente i parametri specificati. La modifica di altri dati in questi file, inclusi i tag, può determinare danneggiamenti e guasti del sistema. Dell non può garantire la risoluzione dei problemi derivanti da modifiche non autorizzate a questi file senza dover reinstallare Enterprise Server.

- *Password Keystore:* immettere una password (<>;&" ' sono caratteri non supportati) e impostare la variabile nel file **conf** del componente sullo stesso valore, come segue:

  <directory di installazione di Compliance Reporter>\conf\eserver.properties. Impostare il valore eserver.keystore.password =

  <directory di installazione di Console Web Services>\conf\eserver.properties. Impostare il valore eserver.keystore.password =

  <directory di installazione di Device Server>\conf\eserver.properties. Impostare il valore eserver.keystore.password =
- *Nome e cognome:* immettere il nome completo del server in cui è installato il componente in uso. Questo nome completo include il nome host e il nome di dominio (ad esempio, server.dell.com).

- *Unità organizzativa:* immettere il valore appropriato (ad esempio, Sicurezza).
- *Organizzazione:* immettere il valore appropriato (ad esempio, Dell).
- *Città o località:* immettere il valore appropriato (ad esempio, Roma).
- *Stato:* immettere il nome esteso dello stato (ad esempio, Italia).
- Codice paese di due lettere:

  Stati Uniti = US

  Canada = CA

  Svizzera = CH

  Germania = DE

  Spagna = ES

  Francia = FR

  Gran Bretagna = GB

  Irlanda = IE

  Italia = IT

  Paesi Bassi = NL
- Verrà richiesta la conferma dell'immissione delle informazioni. In questo caso, digitare `yes`, altrimenti `no`. In Keytool verrà visualizzato ciascun valore precedentemente immesso. Premere INVIO per accettare il valore oppure modificarlo e premere INVIO.
- *Password della chiave per l'alias:* se non si immette un'altra password in questa posizione, verrà utilizzata la password Keystore.

Richiedere un certificato firmato da un'Autorità di certificazione

Attenersi alla procedura descritta di seguito per generare una richiesta di firma del certificato per il certificato autofirmato creato in Generare una nuova coppia di chiavi e un certificato autofirmato.

1 Sostituire lo stesso valore precedentemente utilizzato per <certificate-alias>:

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

Esempio:

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

Il file .csr conterrà una coppia BEGIN/END che verrà utilizzata durante la creazione del certificato nell'Autorità di certificazione.

Figura 9-1. File CSR di esempio

2 Attenersi alla procedura dell'organizzazione per l'acquisizione di un certificato server SSL da un'Autorità di certificazione. Inviare i contenuti del file <csr-filename> per la firma.

NOTA: è possibile richiedere un certificato valido in diversi modi. Un metodo di **esempio** è illustrato in Metodo di esempio per richiedere un certificato.

3 Alla ricezione del certificato firmato, archiviarlo in un file.

4 È consigliabile eseguire il backup del certificato in caso di errori durante il processo di importazione, onde evitare di dover ripetere per intero la procedura.

Importare un certificato radice

NOTA: se l'Autorità di certificazione del certificato radice è Verisign (ma non Verisign Test), passare alla procedura successiva e importare il certificato firmato.

Il certificato radice dell'Autorità di certificazione convalida i certificati firmati.

1 Effettuare una delle seguenti operazioni:

- Scaricare il certificato radice dell'Autorità di certificazione e archiviarlo in un file.
- Ottenere il certificato radice server della directory aziendale.

2 Effettuare una delle seguenti operazioni:

- Se si abilita SSL per Compliance Reporter, Console Web Services, Device Server o Legacy Gatekeeper Connector, passare alla directory conf del componente.
- Se si abilita SSL tra il server e il server della directory aziendale, passare a <directory di installazione Dell>\Java Runtimes\jre1.x.x_xx\lib\security (la password predefinita per l'Autorità di certificazione JRE è changeit).

3 Per installare il certificato radice, eseguire Keytool nel modo seguente:

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

Esempio:

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

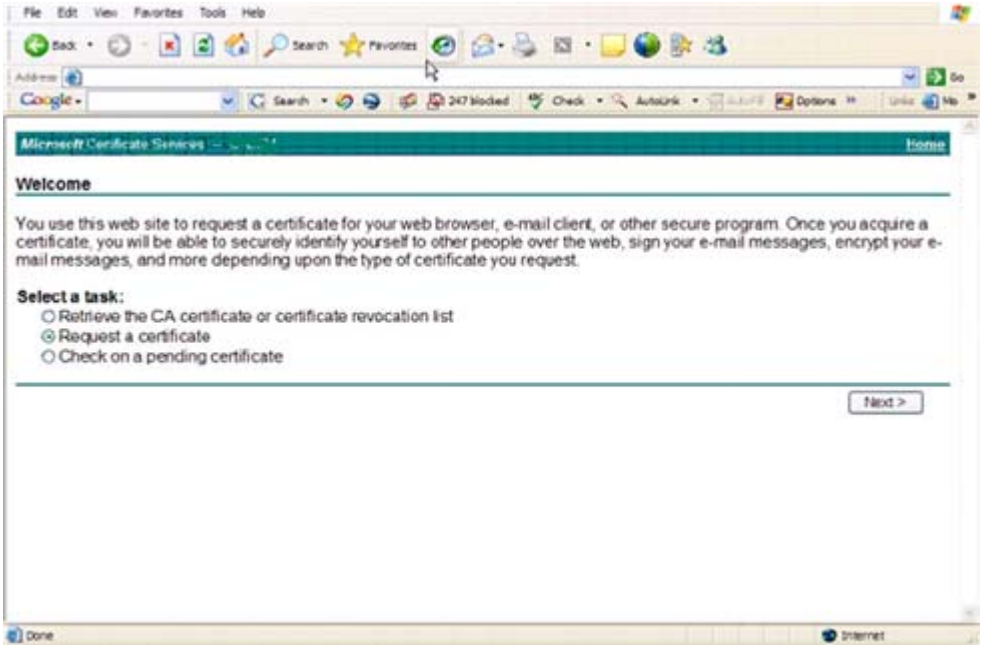
Metodo di esempio per richiedere un certificato

Un metodo di esempio per richiedere un certificato consiste nell'utilizzare un browser Web per accedere al server Microsoft CA, installato internamente dall'organizzazione.

1 Passare al server Microsoft CA. L'indirizzo IP verrà fornito dall'organizzazione.

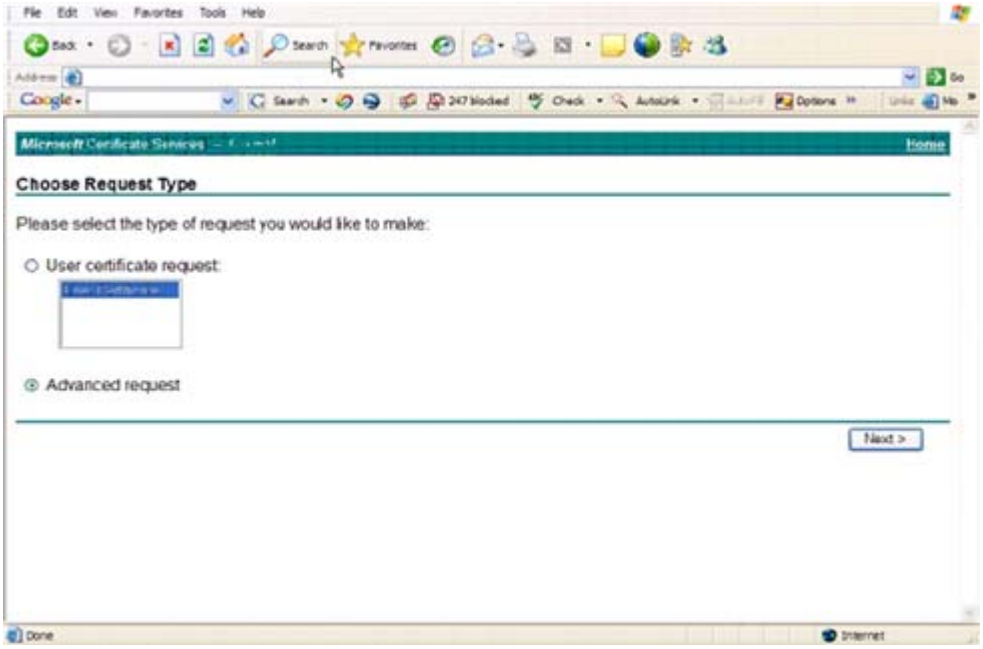
2 Selezionare **Richiedi certificato** e fare clic su **Avanti >**.

Figura 9-2. Servizi certificati Microsoft



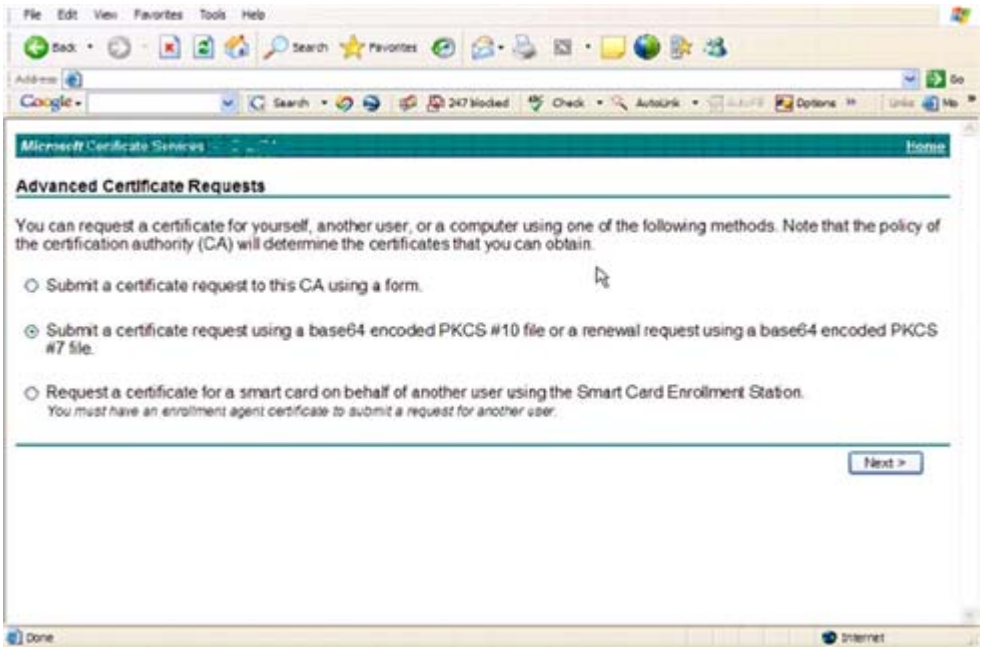
3 Selezionare **Richiesta avanzata** e fare clic su **Avanti >**.

Figura 9-3. Scegliere il tipo di richiesta



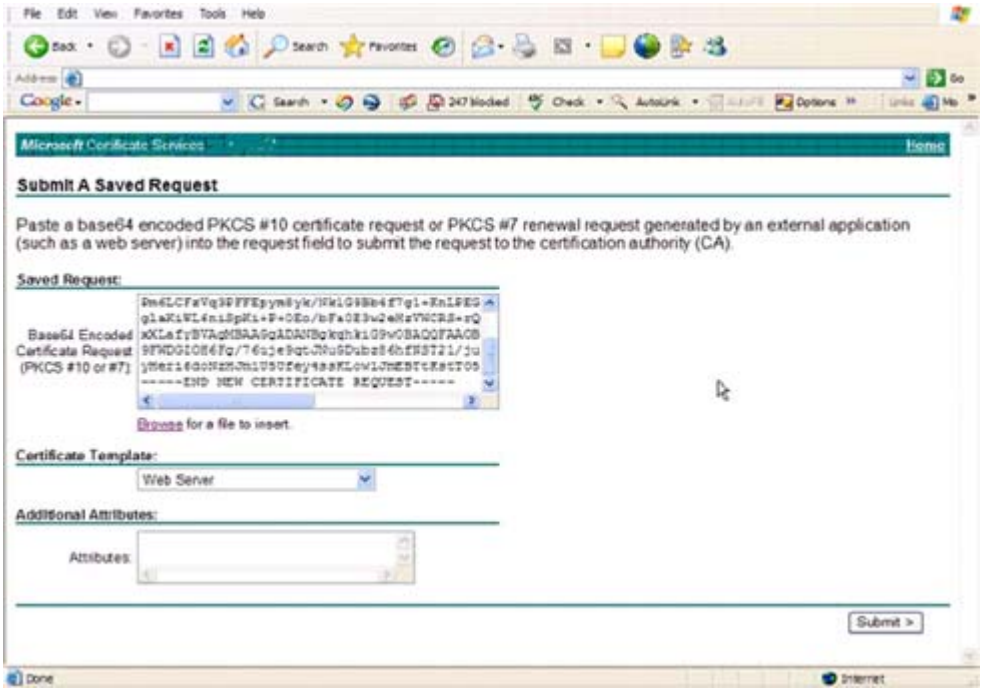
4 Selezionare l'opzione per **inviare una richiesta di certificato mediante un file PKCS #10 con codifica Base64** e fare clic su **Avanti >**.

Figura 9-4. Richiesta certificati avanzata



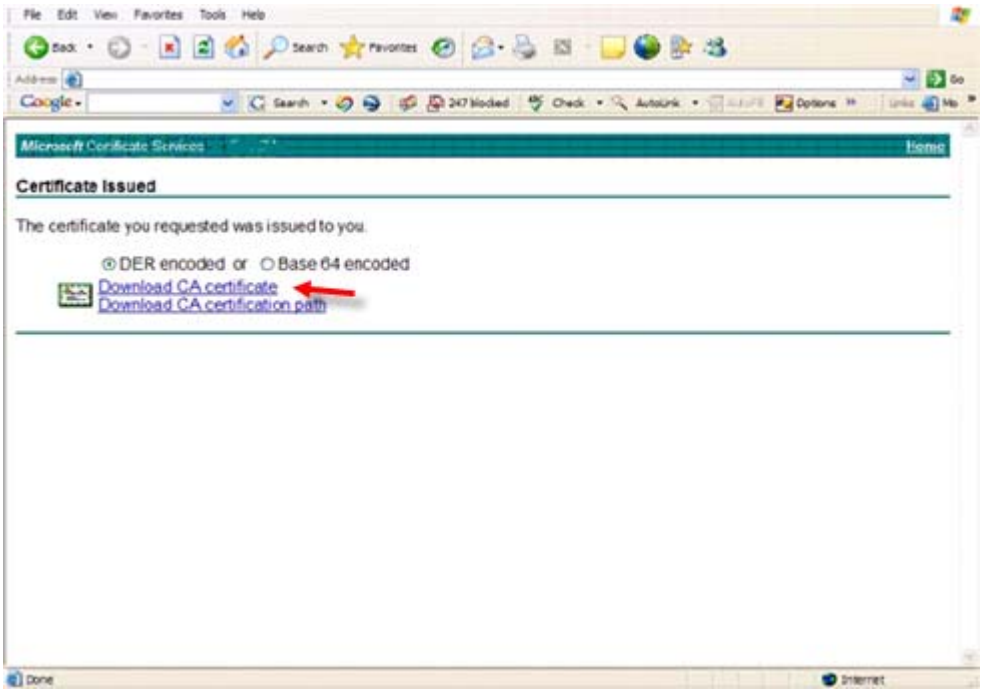
5 Incollare i contenuti della richiesta CSR nella casella di testo. Selezionare un modello di certificato del **server Web** e fare clic su **Invia >**.

Figura 9-5. Inviare una richiesta salvata



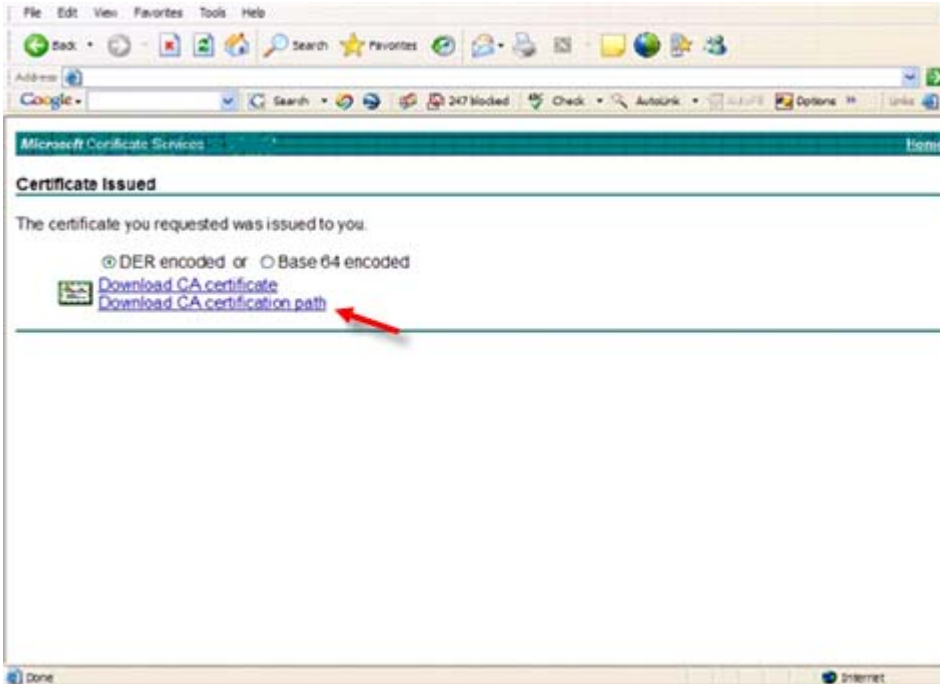
6 Salvare il certificato. Selezionare Codifica DER e fare clic su Scarica certificato CA.

Figura 9-6. Scaricare il certificato CA



7 Salvare il certificato. Selezionare Codifica DER e fare clic su Scarica percorso certificato CA.

Figura 9-7. Scaricare il percorso del certificato CA



8 Importare il certificato dell'autorità di firma convertito. Tornare alla finestra DOS. Digitare:

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

9 Una volta importato il certificato dell'autorità di firma, sarà possibile importare il certificato server (è possibile creare la catena di certificati). Digitare:

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

Utilizzare l'alias del certificato autofirmato per associare la richiesta CSR al certificato server.

10 Un elenco dei file delle Autorità di certificazione indicherà che il certificato server presenta una **lunghezza per la catena di certificati** pari a **2**, ovvero il certificato non è autofirmato. Digitare:

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

L'impronta del secondo certificato nella catena è il certificato dell'autorità di firma importato (elencato anche al di sotto del certificato server nell'elenco).

Il certificato server è stato importato insieme a quello dell'autorità di firma.


0 XXXXXA0 X