Dell Data Protection

Guia de configuração

2014-02

Índice

1

Configurar o Compatibility Server

Este capítulo debruça-se sobre os parâmetros que podem ser alterados para ajustar o Compatibility Server ao seu ambiente. Antes da edição, faça sempre uma cópia de segurança dos ficheiros de configuração.

Altere apenas os parâmetros documentados deste ficheiro. A alteração de outros dados deste ficheiro, incluindo etiquetas, pode provocar danos e falha do sistema. A Dell não pode garantir que é possível solucionar os problemas resultantes de alterações não autorizadas através da reinstalação do Compatibility Server.

server_config.xml

Pode alterar alguns dos parâmetros seguintes em **<Compatibility Server install dir>\conf\server_config.xml**. Os parâmetros que não devem ser alterados encontram-se devidamente identificados. Se o Compatibility Server estiver em execução, deve parar o Compatibility Server Service, editar o ficheiro server_config.xml e, em seguida, reiniciar o Compatibility Server Service para que as alterações realizadas neste ficheiro surtam efeito.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
secrets.location	$dell.home$/conf/secretKeyStore	Localização predefinida de secretkeystore. Se mover este ficheiro da localização predefinida, actualize este parâmetro.
archive.location	$dell.home$/conf/archive	Localização predefinida do arquivo. Se mover este ficheiro da localização predefinida, actualize este parâmetro.
domain.qualified.authentication	verdadeiro	Indica se é necessário o nome de início de sessão de um utilizador totalmente qualificado para todos os pedidos ao Server. Se este valor for alterado, é necessário reiniciar o Device Server para o novo valor surtir efeito.
directory.max.search.size	1000	Limite de uma *pesquisa* no directório, após a qual é executada uma excepção.
directory.server.search.timeout.seconds	60	Tempo limite do servidor em segundos para pesquisas LDAP.
directory.client.search.timeout	60	Tempo limite do cliente em segundos para pesquisas LDAP.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
rmi.recovery.host		Para utilizar o EMS Recovery para vários servidores: <!-- - remova os comentários e altere os nomes de anfitrião para os seus nomes de domínio totalmente qualificados para iniciar a recuperação <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 predefinido do Grupo a que pertencem todos os Policy Proxies por predefinição. É possível alterar este nome aqui ou em context.properties do Device Server. Se alterar aqui o nome do grupo, deve alterá-lo também no Device Server se planear: • Proteger dispositivos Windows • Utilizar o CREDActivate Recomendamos que todos os Policy Proxies pertençam a um único grupo.
rsa.securid.enabled	falso	Se estiver a utilizar o RSA SecurID para Microsoft Windows versão 6 como substituto do GINA, defina este parâmetro como verdadeiro e, em seguida, pare e reinicie o Compatibility Server Service. Quando a activação é realizada pelos utilizadores do Shield num ambiente de substituição GINA RSA, a autenticação RSA substitui a autenticação LDAP.
inv.queue.task.worker.size	10	Número de threads que processam a fila de inventário.
inv.queue.task.timeout.seconds	900	Número de segundos até atingir o tempo limite.
inv.queue.task.retry.count	3	Número de vezes que o servidor tenta processar o inventário até este ser eliminado.
report.retry.max	120	Número máximo de tentativas.
report.retry.wait.millis	250	Número de milissegundos a aguardar antes das tentativas.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
triage.execute.time	0 0 0/6 * *	A triagem é o processo de reconciliação de utilizadores e grupos já conhecidos do servidor. A predefinição é 0 0 0/6 * * ?, o que significa que realizamos a triagem a cada 6 horas, começando à meia-noite (0h, 6h, 12h, 18h, 0h...)
gatekeeper.service.max.sessions	5	Número máximo de sessões de Policy Proxy.
gatekeeper.service.max.session.timeout	5	Tempo limite do número máximo de sessões de Policy Proxy.
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	Função necessária para actualizar as funções administrativas de um utilizador ou grupo.
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	Função necessária para actualizar as funções administrativas de um utilizador ou grupo
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin,LogAdmin	Funções necessárias para recuperar sessões de registo.
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin,LogAdmin	Funções necessárias para recuperar registos.
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin,LogAdmin	Funções necessárias para recuperar a lista de colunas do registo.
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin,LogAdmin	Funções necessárias para recuperar a lista de categorias do registo.
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin,LogAdmin	Funções necessárias para recuperar a lista de prioridades do registo.
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin,SecAdmin,HelpDeskAdmin,SystemAdmin	Funções necessárias para recuperar nomes de ID única.
security.authorization.method.IAdministrativeService.getAdministrators	AcctAdmin	Função necessária para recuperar a lista de administradores do sistema.
security.authorization.method.IAdministrativeService.setSuperAdminPassword	SuperAdmin	Função necessária para definir a palavra-passe superadmin.
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	Função necessária para redefinir a palavra-passe superadmin.
security.authorization.method.IAdministrativeService.addDomain	SystemAdmin,SecAdmin	Funções necessárias para adicionar domínios.
security.authorization.method.IAdministrativeService.removeDomain	SystemAdmin,SecAdmin	Funções necessárias para remover domínios.
security.authorization.method.IAdministrativeService.updateDomain	SystemAdmin,SecAdmin	Funções necessárias para actualizar domínios.
security.authorization.method.IAdministrativeService.addGroups	SystemAdmin,SecAdmin	Funções necessárias para adicionar grupos.
security.authorization.method.IAdministrativeService.removeGroup	SystemAdmin,SecAdmin	Funções necessárias para remover grupos.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
security.authorization.method.IAdministrativeService.findLdapGroups	SystemAdmin,SecAdmin	Funções necessárias para encontrar grupos LDAP.
security.authorization.method.IAdministrativeService.findLdapUsers	SystemAdmin,SecAdmin	Funções necessárias para encontrar utilizadores LDAP.
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin,SecAdmin	Funções necessárias para adicionar utilizadores.
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	Função necessária para adicionar licenças empresariais.
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	Função necessária para ver a licença empresarial.
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin,SecAdmin	Funções necessárias para recuperar um dispositivo.
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin,SecAdmin	Funções necessárias para suspender utilizadores.
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	Funções necessárias para activar dispositivos por proxy.
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin,SecAdmin	Funções necessárias para recuperar um dispositivo por proxy.
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Função necessária para recuperar o ficheiro de recursos do Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Função necessária para aprovar o ficheiro de recursos do Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Funções necessárias para aprovar a configuração do Gatekeeper.
policy.arbiter.security.mode	mais restritivo	Esta propriedade controla a forma como o algoritmo de mapeamento de políticas funciona com elementos de política com compensação de segurança quando a política possui diversos nós principais. Valores: Menos restritivo - é utilizado o elemento menos restritivo dos componentes principais Mais restritivo - é utilizado o elemento mais restritivo de todos os componentes principais
policy.set.synchronization.sync-unmodified	verdadeiro	Este sinalizador indica que a próxima sincronização externa deve adicionar ou mapear novamente todos os elementos de políticas sem definir o sinalizador modificado como verdadeiro. Este sinalizador alterna para falso após cada sincronização e, por isso, deve ser redefinido se o administrador de segurança pretender adicionar sem modificações. Trata-se de uma opção avançada.
db.schema.version.major		Esquema principal da base de dados.
db.schema.version.minor		Esquema secundário da base de dados.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
db.schema.version.patch		Versão patch do esquema da base de dados.
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	Localização predefinida do controlador da base de dados. Se mover este ficheiro da localização predefinida, actualize este parâmetro.
dao.db.host		Nome de anfitrião do seu servidor de base de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.name		Nome da sua base de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.user		Nome de utilizador com permissões completas na sua base de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.password		Palavra-passe do nome de utilizador com permissões completas na sua base de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.max.retry.count	10	Número máximo de vezes que o Compatibility Server tenta ligar-se novamente ao SQL Server quando ocorre um erro de socket específico.
dao.db.connection.retry.wait.seconds	5	A primeira tentativa de ligar novamente é imediata. A segunda ocorre após o número de segundos especificado. A terceira ocorre após o dobro do número de segundos especificados, a quarta ocorre após o triplo, e assim sucessivamente.
dao.connection.pool.max.uses	10000	Permite extinguir as ligações. 0 significa "não extinguir".
dao.connection.pool.inactive.threshold.seconds	900	Utilizado para determinar quando uma ligação não é utilizada e pode ser fechada.
dao.db.driver.socket.errors	0	O Compatibility Server tenta ligar-se novamente ao SQL Server quando ocorrem os erros correspondentes aos códigos desta lista separada por vírgulas. 0 refere-se ao código de erro dos erros de socket do Microsoft SQL. Poderá também adicionar 17142 para erros de suspensão de servidor e 6002 para erros de encerramento de servidor.
dao.db.mssql.compatability.level	90	Valor do SQL 2005 ou posterior.
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	Processador do ficheiro de autorização.
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	Processador do ficheiro de inventário.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	Processador do ficheiro de eventos.
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Se mover o ficheiro de recursos do Gatekeeper da localização predefinida, actualize este parâmetro.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Se mover o ficheiro de recursos do Gatekeeper da localização predefinida, actualize este parâmetro.
rmi.server.registry.host	localhost	A propriedade do anfitrião destina-se apenas à determinação da localização do registo por parte de programas clientes. Não é utilizada durante a criação do registo RMI e de objectos remotos. Será criado no anfitrião local.
rmi.server.registry.port	1099	A porta do registo RMI é configurável durante a instalação. Pode também utilizar este parâmetro para alterar a porta após a instalação. Se alterar este valor, também tem de configurar os Gatekeeper Web Services.
security.authorization.method.IServerReports.getOverviewReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para definir a autorização de relatórios do servidor.
security.authorization.method.IReportingService.removeEntity	SystemAdmin	Função necessária para remover entidades do servidor.
security.authorization.method.IReportingService.setEntityVisibility	SystemAdmin	Função necessária para definir a visibilidade das entidades do servidor.
security.authorization.method.IReportingService.getHardwareDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver a página de detalhes do dispositivo.
security.authorization.method.IReportingService.openSession	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para abrir uma sessão no servidor.
security.authorization.method.IReportingService.getPagedReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver as páginas de relatório.
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de tipo de dispositivo.
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório do sistema operativo.
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver os relatórios de modelo de dispositivo.
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de detalhes da política.
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de detalhes da estação de trabalho.
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de falha de encriptação.
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de resumo de encriptação.

server_config.xml		
Parâmetro	**Predefinido**	**Descrição**
security.authorization.method.IReportingService.getUserDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de detalhes de utilizador.
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de detalhes de grupo.
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para ver o relatório de lista de domínio.
security.authorization.method.IKeyService.getKeys	ForensicAdmin	Esta definição é utilizada com um plug-in de integração de nível superior. Contacte a Assistência Dell se necessitar de integração da ferramenta de nível superior.
accountType.nonActiveDirectory.enabled	falso	A permissão de activações fora do domínio constitui uma configuração avançada, com consequências muito variadas. *ANTES* de activar esta configuração, contacte a Assistência ao cliente para debater as necessidades específicas do seu ambiente. Reinicie o Compatibility Server Service depois de alterar este valor. Além desta definição, crie ou altere as definições do registo no computador com Windows da seguinte forma: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations= REG_DWORD:1

gkresource.xml

Pode alterar os parâmetros em <Compatibility Server install dir>\conf\gkresource.xml.

Recomendamos a utilização de registo de alterações nos comentários situados no início do ficheiro. Desta forma, poderá transferir facilmente as alterações para o novo ficheiro quando fizer alguma actualização.

NOTA: o ficheiro gkresource.xml deve ser um ficheiro XML bem constituído. A Dell recomenda que a edição deste ficheiro apenas seja realizada por utilizadores familiarizados com XML. Utilize referências a entidades, onde tal seja adequado, em vez de utilizar caracteres especiais não processados (sem escape).

Todas as alterações ao ficheiro de recursos do Gatekeeper devem ser aprovadas por um Administrador do sistema antes de serem aplicadas.

Enable Domain\Username Format

Adicione a seguinte string para activar (ou desactivar) o formato domínio/nome de utilizador. O formato é desactivado se a string não existir no ficheiro. Pode também ser desactivado definindo o valor como 0.

1. Aceda a <Compatibility Server install dir>\conf.
2. Abra gkresource.xml com um editor de .xml.
3. Adicione a string:
   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. Guarde e feche o ficheiro.

run-service.conf

Pode alterar alguns dos parâmetros seguintes em **<Compatibility Server install dir>\conf\run-service.conf**. Estes parâmetros são definidos automaticamente na instalação. Para personalizar ou alterar as configurações de qualquer serviço:

1. Pare o serviço.
2. Remova o serviço.
3. Edite e guarde o ficheiro **run-service.conf**. Recomendamos a utilização de registo de alterações nos comentários situados no início do ficheiro.
4. Instale novamente o serviço.
5. Inicie o serviço.

run-service.conf		
Parâmetro	**Predefinido**	**Descrição**
JAVA_HOME	Dell\Java Runtime\jreX.x	Localização do directório de instalação do Java.
wrapper.java.additional.5	n/a	O endereço MAC desta linha corresponde ao endereço MAC do adaptador de Ethernet local. Se um servidor possuir diversos NICS ou se quiser vincular-se a um adaptador que não seja o adaptador primário, introduza aqui o endereço MAC físico do NIC, sem travessão.
wrapper.ntservice.name	EpmCompatSvr	Nome do serviço.
wrapper.ntservice.displayname	Dell Compatibility Server	Apresentar o nome do serviço.
wrapper.ntservice.description	Enterprise Compatibility Server	Descrição do serviço.
wrapper.ntservice.dependency.1		Dependências do serviço. Adicione dependências conforme necessário, começando em 1.
wrapper.ntservice.starttype	AUTO_START	Modo no qual é instalado o serviço: AUTO_START ou DEMAND_START.
wrapper.ntservice.interactive	falso	A definição "verdadeiro" permite ao serviço interagir com o ambiente de trabalho.

2

Configurar o Core Server

Este capítulo debruça-se sobre os parâmetros que podem ser alterados para ajustar o Core Server ao seu ambiente.

Altere apenas os parâmetros documentados deste ficheiro. A alteração de outros dados deste ficheiro, incluindo etiquetas, pode provocar danos e falha do sistema. A Dell não pode garantir que é possível solucionar os problemas resultantes de alterações não autorizadas a este ficheiro através da reinstalação do Core Server.

Alterar a Arbitragem de políticas da mais segura para a menos segura

PolicyService.config

Altere esta definição para alterar a Arbitragem de políticas da mais segura para a menos segura. Altere a definição em **<Core Server install dir>\PolicyService.config**. Se o Core Server estiver em execução, deve parar o serviço, editar o ficheiro PolicyServiceConfig e, em seguida, reiniciar o serviço para que as alterações ao ficheiro surtam efeito.

Recomendamos a utilização de registo de alterações nos comentários situados no início do ficheiro. Desta forma, poderá transferir facilmente as alterações para o novo ficheiro PolicyServiceConfig.xml quando fizer uma actualização.

Altere a seguinte secção:

```
<!-- 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" /> [altere este valor de "0" para "1" para definir o valor para a menos segura]
</object>
```

Desactivar serviços da Web

NOTA: trata-se de uma definição avançada que apenas deve ser alterada com orientação da Assistência a clientes.

Para desactivar os serviços da Web no Core Server (por exemplo, se existir uma segunda instalação do Core Server que apenas faça o processamento de inventário), altere as definições em:

<Core Server install dir>

Credant.Server2.WindowsService.exe.Config

e

<Core Server install dir>\Spring.config

Se o Core Server estiver em execução, deve parar o serviço, editar as definições destes dois ficheiros e, em seguida, reiniciar o serviço para que as alterações realizadas neste ficheiro surtam efeito.

Credant.Server2.WindowsService.exe.Config

Remova a seguinte secção:

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

Spring.config

Remova o seguinte:

Remova todas as definições <object> </object> sob os cabeçalhos **Recomendação AOP**, **Definição de alvo de serviço da Web** e **Definição de anfitrião de serviço da Web**.

Activar o servidor SMTP para notificações de licenças por e-mail

Se utilizar o Dell Data Protection | Cloud Edition, estas definições são automáticas se utilizar a Ferramenta de configuração do servidor. Utilize este procedimento se precisar de activar o servidor SMTP para notificações de licenças por e-mail para fins externos ao Dell Data Protection | Cloud Edition.

NotificationObjects.config

Para configurar o servidor SMTP para notificações de licenças por e-mail, altere o ficheiro **NotificationObjects.config**, que se encontra em **<Core Server install dir>**.

Altere o seguinte:

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

Notification.config

Se o seu servidor de e-mail necessitar de autenticação, altere o ficheiro **Notification.config**, que se encontra em **<Core Server install dir>**.

Altere o seguinte:

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

Adicione a localização do Compatibility Server ao ficheiro de configuração do Core Server

O Core Server, enquanto aplicação .Net, pode por vezes ser impedido de aceder a informações do registo, devido às permissões. O problema é que, para ler o secretkeystore (chave de encriptação da base de dados), o Core Server necessita de aceder às informações de configuração do registo para a localização de secretkeystore. Se as permissões do registo bloquearem este acesso, o Core Server não consegue autenticar os utilizadores da Consola. Esta definição adiciona a localização da pasta do Compatibility Server ao ficheiro de configuração do Core Server em caso de problemas de acesso ao registo.

1. Navegue até <Core Server install dir>\EntityDataAccessObjects.config.
2. Altere o seguinte item a **negrito**:

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

   Remova os comentários desta linha e defina o caminho totalmente qualificado até ao Compatibility Server.

   ```
   </object>
   ```

3. Guarde e feche o ficheiro.
4. Reinicie os serviços do Core Server e do Compatibility Server.

Permitir que o Core Server percorra vários métodos de autenticação

As tentativas de autenticação do Core Server podem ser bloqueadas pelo controlador do domínio, uma vez que as políticas são definidas com base nos métodos de autenticação permitidos. A melhoria consiste na implementação de um "interruptor" no ficheiro de configuração do Core Server para permitir ao Core Server percorrer vários métodos de autenticação, numa tentativa de encontrar um que funcione.

1. Navegue até <Core Server install dir>\Spring.config.
2. Altere o seguinte item a **negrito**:

   ```
   <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" />
   ```

   Altere este valor para "true" para activar esta funcionalidade.

   ```
     <!-- Utilizado para alterar o AuthType por domínio: a chave é o CID do domínio e o valor é o valor
     System.DirectoryServices.AuthenticationTypes
     <property name="DomainAuthType">
       <dictionary key-type="string" value-type="int" >
         <entry key="5A23TPM2" value="0" />
       </dictionary>
     </property>
     -->
   </object>
   ```

3. Guarde e feche o ficheiro.
4. Reinicie o Core Server Service.

3

Configurar o Device Server

Este capítulo debruça-se sobre os parâmetros que podem ser alterados para ajustar o Device Server ao seu ambiente.

Altere apenas os parâmetros documentados deste ficheiro. A alteração de outros dados deste ficheiro, incluindo etiquetas, pode provocar danos e falha do sistema. A Dell não pode garantir que é possível solucionar os problemas resultantes de alterações não autorizadas através da reinstalação do Device Server.

eserver.properties

Pode alterar os seguintes parâmetros em **<Device Server install dir>\conf\eserver.properties**.

Recomendamos a utilização de registo de alterações nos comentários situados no início do ficheiro. Desta forma, poderá transferir facilmente as alterações para o novo ficheiro quando fizer uma actualização.

eserver.properties

Parâmetro	Predefinido	Descrição
eserver.default.host	Device Server Service	FQDN do local onde o Device Server Service está instalado.
eserver.default.port	Enterprise Server v7.7 ou posterior - 8443 Anterior ao Enterprise Server v7.7 - 8081	A porta verificada pelo Device Server para entrada de pedidos de activação enviados pelos dispositivos.
eserver.use.ssl	Verdadeiro	O SSL está activo por predefinição. Para desactivar o SSL, altere este parâmetro para falso.
eserver.keystore.location	${context['server.home']}/conf/cacerts	Localização do certificado SSL utilizado pelo Device Server.
eserver.keystore.password	changeit	Se tiver alterado a palavra-passe cacerts na Ferramenta de configuração, este parâmetro é actualizado de forma correspondente. Se alterar cacert na Ferramenta de configuração em qualquer momento após a configuração inicial, atualize este parâmetro com a palavra-passe Keystore que utiliza.

eserver.properties		
Parâmetro	**Predefinido**	**Descrição**
eserver.ciphers		Define a lista de cifras de encriptação. Cada cifra deve ser separada por vírgula. Se ficar vazio, o socket permite qualquer cifra disponível suportada pelo Tomcat. Remova os comentários do exemplo abaixo para definir a lista de cifras de encriptação. Separe as cifra com vírgulas. Consulte o guia de referência JSSE da Sun para obter a lista de nomes de conjuntos de cifras válidos. #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

Pode alterar alguns dos parâmetros seguintes em **<Device Server install dir>\conf\run-service.conf**. Estes parâmetros são definidos automaticamente na instalação. Para personalizar ou alterar as configurações de qualquer serviço:

1. Pare o serviço.
2. Remova o serviço.
3. Edite e guarde o ficheiro **run-service.conf**. Recomendamos a utilização de registo de alterações nos comentários situados no início do ficheiro.
4. Instale novamente o serviço.
5. Inicie o serviço.

run-service.conf		
Parâmetro	**Predefinido**	**Descrição**
JAVA_HOME	Dell\Java Runtime\jreX.x	Localização do directório de instalação do Java.
wrapper.ntservice.name	EpmDeviceSvr	Nome do serviço.
wrapper.ntservice.displayname	Dell Device Server	Apresentar o nome do serviço.
wrapper.ntservice.description	Enterprise Device Server	Descrição do serviço.
wrapper.ntservice.dependency.1		Dependências do serviço. Adicione dependências conforme necessário, começando em 1.
wrapper.ntservice.starttype	AUTO_START	Modo no qual é instalado o serviço: AUTO_START ou DEMAND_START.
wrapper.ntservice.interactive	falso	A definição “true” permite ao serviço interagir com o ambiente de trabalho.

4

Configurar o Security Server

Este capítulo debruça-se sobre os parâmetros que podem ser alterados para ajustar o Security Server ao seu ambiente.

Altere apenas os parâmetros documentados deste ficheiro. A alteração de outros dados deste ficheiro, incluindo etiquetas, pode provocar danos e falha do sistema. A Dell não pode garantir que é possível solucionar os problemas resultantes de alterações não autorizadas através da reinstalação do Security Server.

context.properties

Pode alterar os seguintes parâmetros em **<Security Server install dir>\webapps\xapi\WEB-INF\context.properties**.

Recomendamos a utilização de registo de alterações nos comentários situados no início do ficheiro. Desta forma, poderá transferir facilmente as alterações para o novo ficheiro quando fizer uma actualização.

context.properties		
Parâmetro	**Predefinido**	**Descrição**
default.gatekeeper.group.remote	CMGREMOTE	Nome do grupo remoto de dispositivos. **Não altere.**
xmlrpc.max.threads	250	Número máximo de threads simultâneas neste Device Server.
default.auth.upn.suffix		Sufixo UPN anexado ao nome de início de sessão de um utilizador se o servidor exigir um nome de início de sessão totalmente qualificado e este não for fornecido no pedido.
device.manual.auth.enable	verdadeiro	Indica se as autenticações manuais estão activas ou desactivadas. **Não altere**
service.activation.enable	verdadeiro	Indica se as activações são processadas pelo Device Server. **Não altere**
service.policy.enable	verdadeiro	Indica se a política está activa ou desactivada. **Não altere**.
service.auth.enable	verdadeiro	Indica se as autenticações são processadas pelo Device Server.
service.forensic.enable	verdadeiro	Esta definição é utilizada com um plug-in de integração de nível superior. Contacte a Assistência Dell se necessitar de integração da ferramenta de nível superior.
service.support.enable	verdadeiro	Activa a recuperação de meta informação sobre o servidor.
service.device.enable	verdadeiro	Activa o suporte de serviços Shield, como o armazenamento de chaves SDE.

5

Configurar funcionalidades de encriptação

Esta secção debruça-se sobre como controlar funcionalidades de encriptação de forma independente.

Impedir a eliminação temporária de ficheiros

Por predefinição, todos os ficheiros temporários do directório c:\windows\temp são eliminados automaticamente durante a instalação/actualização do DDPE. A eliminação dos ficheiros temporários acelera a encriptação inicial e ocorre antes do varrimento de encriptação inicial.

No entanto, se a sua organização utilizar uma aplicação de terceiros que exija que a estrutura de ficheiros dentro do directório \temp seja preservada, deverá evitar esta eliminação.

Para desactivar a eliminação dos ficheiros temporários, crie ou altere a definição do registo da seguinte forma:

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

Tenha em atenção que, ao **não** eliminar os ficheiros temporários, aumenta o tempo de encriptação inicial.

Ocultar ícones sobrepostos

Por predefinição, durante a instalação, todos os ícones de sobreposição de encriptação estão definidos para ser exibidos. Utilize a seguinte definição do registo para ocultar os ícones de sobreposição de encriptação para todos os utilizadores geridos num computador após a instalação original.

Crie ou modifique a definição do registo da seguinte forma:

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)=1

Se um utilizador (com os privilégios adequados) optar por exibir os ícones de sobreposição de encriptação, essa definição substitui este valor do registo.

Ocultar o ícone do tabuleiro do sistema

Por predefinição, durante a instalação, é exibido o ícone do tabuleiro do sistema. Utilize a seguinte definição do registo para ocultar o ícone do tabuleiro do sistema para todos os utilizadores geridos num computador após a instalação original.

Crie ou modifique a definição do registo da seguinte forma:

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)=1

Activação temporizada

A activação temporizada é uma funcionalidade que lhe permite distribuir as activações de Shields durante um período de tempo definido para aliviar a carga do servidor durante uma implementação em massa. As activações são atrasadas com base em períodos de tempo gerados por algoritmos, para distribuir uniformemente os tempos de activação.

A Activação temporizada é activada e configurada através do instalador do Shield ou através da estação de trabalho do Shield.

Para os utilizadores que necessitam de activação através de VPN, poderá ser necessária uma configuração de activação temporizada para o Shield, para atrasar a activação inicial por tempo suficiente para permitir que o software cliente VPN estabeleça uma ligação de rede.

ATENÇÃO: para configurar a Activação temporizada, é necessário o apoio da Assistência ao cliente. A configuração inadequada dos períodos de tempo poderá resultar na tentativa de activação por muitos clientes em simultâneo, criando problemas de desempenho potencialmente graves.

As seguintes Chaves de registo são utilizadas para configurar a Activação temporizada. Para que as actualizações surtam efeito, a estação de trabalho do Shield deve ser reiniciada após as alterações às Chaves de registo.

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

  Esta definição activa ou desactiva a funcionalidade de Activação temporizada.
  Desactivado=0 (predefinido)
  Activado=1

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

  Período de tempo, em segundos, em que ocorre o intervalo de activação. Esta propriedade pode ser utilizada para substituir o período de tempo, em segundos, durante o qual ocorre o intervalo de activação. Estão disponíveis 25 200 segundos para activações temporizadas durante um período de sete horas. A predefinição é de 86 400 segundos, o que representa uma repetição diária.

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

  Intervalo de repetição, ACTIVATION_SLOT_CALREPEAT, em que ocorrem todos os períodos de activação. Apenas é permitido um intervalo. Esta definição deve ser 0,<CalRepeat>. Um valor diferente de 0 pode provocar resultados inesperados. A predefinição é de 0,86400. Para definir uma repetição de sete horas, utilize a definição 0,25200. CALREPEAT activa-se quando um utilizador Shield inicia sessão.

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

  O número de períodos de activação que podem ser perdidos antes de o computador tentar activar no próximo início de sessão do utilizador cuja activação foi temporizada. Se a activação falhar durante esta tentativa imediata, o Shield retoma as tentativas de Activação temporizada. Se a activação falhar devido a falha de rede, ocorre uma tentativa de activação ao ligar novamente à rede, mesmo se o valor de MISSTHRESHOLD não tiver sido excedido. Se um utilizador terminar sessão antes de ser atingido o tempo de activação, é atribuído um novo tempo no próximo início de sessão.

- HKCU/Software/CREDANT/ActivationSlot (dados por utilizador)

  Tempo diferido para tentar a Activação temporizada, definido quando o utilizador inicia sessão na rede pela primeira vez após a Activação temporizada ser activada. O tempo de activação é recalculado para cada tentativa de activação.

- HKCU/Software/CREDANT/SlotAttemptCount (dados por utilizador)

  Número de tentativas falhadas ou perdidas; quando chega o momento do intervalo de tempo e a tentativa de activação falha. Quando este número atinge o valor definido em ACTIVATION_SLOT_MISSTHRESHOLD, o computador tenta uma activação imediata ao ligar à rede.

Para activar a Activação temporizada através da linha de comandos, utilize um comando semelhante ao seguinte:

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

NOTA: certifique-se de que inclui um valor que contém um ou mais caracteres especiais, como um espaço em branco, entre aspas de escape.

Análise forçada

Utilize a seguinte definição do registo para que o Shield analise o servidor em busca de uma actualização de política forçada.

Crie ou modifique a definição do registo da seguinte forma:

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD value)=1

Consoante a versão do Shield, a definição do registo desaparece automaticamente *ou* altera-se de 1 para 0 após a realização da análise.

Consoante o conjunto de permissões de um utilizador Administrador, poderá ser necessária uma alteração das permissões para criar esta definição do registo. Se ocorrerem problemas ao tentar criar um novo DWORD, siga os passos abaixo para alterar as permissões.

1. No registo do Windows, aceda a HKLM\SOFTWARE\Credant\CMGShield\Notify.
2. Clique com o botão direito em **Notificar** > **Permissões**.
3. Quando abrir a janela *Permissão para notificar*, seleccione a caixa de verificação de **Controlo total**.
4. Clique em **OK**.

Já pode criar uma nova definição do registo.

Opções de inventário

Utilize as seguintes definições do registo para permitir ao Shield enviar um inventário otimizado para o servidor, enviar um inventário completo para o servidor ou enviar um inventário completo para todos os utilizadores activos no servidor.

Enviar inventário otimizado para o servidor

Crie ou modifique a definição do registo da seguinte forma:

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

OnlySendInvChanges (REG_DWORD)=1

Se não estiver presente qualquer entrada, é enviado o inventário otimizado para o servidor.

Enviar inventário completo para o servidor

Crie ou modifique a definição do registo da seguinte forma:

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

OnlySendInvChanges (REG_DWORD)=0

Se não estiver presente qualquer entrada, é enviado o inventário otimizado para o servidor.

Enviar inventário completo para todos os utilizadores activos

Crie ou modifique a definição do registo da seguinte forma:

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

RefreshInventory (REG_DWORD)=1

Esta entrada é eliminada do registo assim que é processada. Como o valor é guardado no Vault, o Shield atende a este pedido no próximo carregamento com êxito do inventário mesmo que o computador seja reiniciado antes de ser realizado o inventário.

Esta entrada tem prioridade sobre o valor do registo OnlySendInvChanges.

Activações fora do domínio

A permissão de activações fora do domínio constitui uma configuração avançada, com consequências muito variadas. Contacte a Assistência ao cliente para debater as necessidades específicas do seu ambiente e para obter instruções sobre como activar esta funcionalidade.

6

Configurar componentes para autenticação/autorização Kerberos

Esta secção debruça-se sobre a configuração de componentes para utilização com autenticação/autorização Kerberos.

Configurar componentes para autenticação/autorização Kerberos

NOTA: se for utilizada a autenticação/autorização Kerberos, o servidor que contém o componente Key Server tem de fazer parte do domínio afectado.

O Key Server consiste num serviço que verifica os clientes que se ligam a um socket. Depois de um cliente se ligar, é estabelecida, autenticada e encriptada uma ligação segura através de APIs Kerberos (se não for possível estabelecer uma ligação segura, o cliente é desligado).

O Key Server verifica então junto do Device Server se o utilizador que está a executar o cliente tem permissão para aceder às chaves. Este acesso é concedido na Consola de gestão remota através de domínios *individuais*.

Instruções para o serviço Windows

1. Navegue até ao painel do serviço Windows (Iniciar > Executar... > services.msc > OK).
2. Clique com o botão direito do rato no Dell Key Server e seleccione **Propriedades**.
3. Aceda ao separador **Iniciar sessão** e seleccione o botão da opção **Esta conta:**.
4. No campo **Esta conta:**, adicione o utilizador do domínio pretendido. Este utilizador do domínio deve possuir, pelo menos, direitos administrativos locais da pasta do Key Server (deve poder gravar no ficheiro de configuração do Key Server e também no ficheiro log.txt).
5. Clique em **OK**.
6. Reinicie o serviço (deixe o painel do serviço Windows aberto para continuar a utilizá-lo).
7. Navegue até <Key Server install dir>\log.txt para verificar se o serviço foi iniciado adequadamente.

Instruções para o ficheiro de configuração do Key Server

1. Navegue até <Key Server install dir>.
2. Abra Credant.KeyServer.exe.config com um editor de texto.
3. Aceda a <add key="user" value="superadmin" /> e altere o valor "superadmin" para o nome do utilizador pretendido (também pode deixar "superadmin").

   O formato "superadmin" pode consistir em qualquer método que possa ser autenticado no servidor. São aceitáveis o nome de conta SAM, UPN ou o domínio/nome de utilizador. É aceite qualquer método que possa ser autenticado no servidor uma vez que a validação é obrigatória para *essa* conta de utilizador, para autenticação face ao Active Directory.

   Por exemplo, num ambiente de vários domínios, a introdução de apenas o nome de conta SAM "jdoe" irá provavelmente falhar, uma vez que o servidor não consegue autenticar "jdoe" porque não consegue encontrar "jdoe". Num ambiente de vários domínios, é recomendada a utilização do UPN, embora também seja aceitável o formato domínio\nome de utilizador.

   Num ambiente de domínio único, é aceitável o nome de conta SAM.

4 Aceda a <add key="epw" value="<encrypted value of the password>" /> e altere "epw" para "password". Em seguida, altere "<encrypted value of the password>" para a palavra-passe do utilizador do Passo 3. Esta palavra-passe é encriptada novamente ao reiniciar o servidor.

Se, no Passo 3, utilizou "superadmin" e a palavra-passe do superadmin não for "changeit", deve ser alterada aqui.

5 Guarde as alterações e feche o ficheiro.

Exemplo de ficheiro de configuração:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <appSettings>
        <add key="port" value="8050" /> [A porta TCP verificada pelo servidor. A predefinição é 8050; altere se for necessário.]
        <add key="maxConnections" value="2000" /> [Quantas ligações de socket ativas o servidor permite.]
        <add key="url" value="https://keyserver.domain.com:8081/xapi" /> [URL do Device Server. Se o seu Enterprise Server for v7.7 ou posterior, o formato é https://keyserver.domain.com:8443/xapi/ -- se o seu Enterprise Server for anterior à v7.7, o formato é https://keyserver.domain.com:8081/xapi (sem a barra final).]
        <add key="verifyCertificate" value="false" /> [Se verdadeiro, verifica certificados/defina como falso para não verificar ou se utilizar certificados auto-assinados]
        <add key="user" value="superadmin" /> [Nome de utilizador usado para comunicar com o Device Server. Este utilizador deve ser do tipo de Administrador de nível superior seleccionado na Consola de gestão remota. O formato "superadmin" pode consistir em qualquer método que possa ser autenticado no servidor. São aceitáveis o nome de conta SAM, UPN ou o domínio/nome de utilizador. É aceite qualquer método que possa ser autenticado no servidor uma vez que a validação é obrigatória para essa conta de utilizador, para autenticação face ao Active Directory. Por exemplo, num ambiente de vários domínios, a introdução de apenas o nome de conta SAM "jdoe" irá provavelmente falhar, uma vez que o servidor não consegue autenticar "jdoe" porque não consegue encontrar "jdoe". Num ambiente de vários domínios, é recomendada a utilização do UPN, embora também seja aceitável o formato domínio\nome de utilizador. Num ambiente de domínio único, é aceitável o nome de conta SAM.]
        <add key="cacheExpiration" value="30" /> [A frequência (em segundos) com que o serviço deve verificar quem tem permissão para pedir chaves. O serviço mantém uma cache e regista o tempo que esta tem. Quando a cache tiver mais tempo que o valor (em segundos), é obtida uma nova lista. Quando um utilizador se liga, o Key Server tem de transferir utilizadores autorizados do Device Server. Se estes utilizadores não estiverem em cache, ou se a lista não tiver sido transferida nos últimos "x" segundos, esta será transferida novamente. Não existe análise, mas este valor configura o tempo máximo que a lista pode ter antes de ser actualizada quando necessário.]
        <add key="epw" value="encrypted value of the password" /> [Palavra-passe utilizada para comunicar com o Device Server. Se a palavra-passe de superadmin tiver sido alterada, deve ser alterada aqui.]
    </appSettings>
</configuration>
```

Instruções para o serviço Windows

1 Regresse ao painel do serviço Windows.

2 Reinicie o Dell Key Server Service.

3 Navegue até <Key Server install dir>\log.txt para verificar se o serviço foi iniciado adequadamente.

4 Feche o painel do serviço Windows.

Instruções para a Consola de gestão remota

1. Caso necessário, inicie a sessão na Consola de gestão remota.
2. Clique em **Domínios** e clique no ícone **Detalhe**.
3. Clique em **Key Server**.
4. Na lista de contas do Key Server, adicione o utilizador que irá realizar as actividades de administrador. O formato é Domínio\nome de utilizador. Clique em **Adicionar conta**.
5. Clique em **Utilizadores** no menu principal. Na caixa de pesquisa, procure o nome de utilizador adicionado no Passo 2. Clique em **Pesquisar**.
6. Depois de encontrar o utilizador correto, clique no ícone **Detalhe**.
7. Seleccione **Administrador de nível superior**. Clique em **Actualizar**.

Os componentes estão agora configurados para autenticação/autorização Kerberos.

7

Atribuir função de Administrador Forense

Por predefinição, a Autorização de nível superior está activa em servidores back-end e desactivada em servidores front-end. Estas definições são introduzidas da forma adequada durante a instalação do Device Server e do Security Server.

Instruções para a Consola de gestão remota

1. Caso necessário, inicie a sessão na Consola de gestão remota.
2. No painel esquerdo, clique em **Gerir** > **Utilizadores**.
3. Na página *Pesquisar utilizadores*, introduza o nome do utilizador a quem pretende conferir a função de administrador de nível superior e clique em **Pesquisar** (as credenciais deste utilizador são fornecidas durante a execução dos utilitários CMGAd, CMGAu e CMGAlu, e do Decryption Agent no modo de nível superior).
4. Na página *Resultados da pesquisa de utilizadores*, clique no ícone **Detalhe**.
5. Na página *Detalhe de utilizador de: <Username>*, seleccione **Admin**.
6. Na coluna Utilizador, seleccione **Administrador de nível superior** e clique em **Actualizar**.

A função de Administrador Forense foi agora definida.

Desativar Autorização Forense

1. No seu servidor de back-end, navegue até **<Security Server install dir>\webapps\xapi\WEB-INF\context.properties** e altere a seguinte propriedade:

   service.forensic.enable=true

   para

   service.forensic.enable=false
2. **Reinicie** o serviço Servidor de segurança.
3. Navegue até **<Device Server install dir>webapps\ROOT\WEB-INF\web.xml**. Altere o seguinte:

   <init-param>

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

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

   </init-param>
4. **Reinicie** o Device Server Service.
5. Como prática recomendada, elimine a função de Administrador Forense a qualquer utilizador que não utilize activamente as permissões da função.

8

Expressões Cron

Esta secção debruça-se sobre a utilização de formatos de expressão Cron e caracteres especiais.

Introdução às expressões Cron

Cron é uma ferramenta UNIX existente há bastante tempo, cujas capacidades de agendamento são potentes e comprovadas. A classe CronTrigger baseia-se nas capacidades de agendamento do Cron.

A CronTrigger utiliza expressões Cron que podem criar agendas de accionamento, como, por exemplo, às 8h00 todas as segundas a sextas-feiras, ou às 1h30 de cada última sexta-feira do mês.

As expressões Cron são potentes, mas podem ser confusas. O objectivo deste documento é desmistificar a criação de uma expressão Cron, proporcionando-lhe um recurso a utilizar antes de procurar ajuda externa.

Formatos das expressões Cron

As expressões Cron são constituídas por 6 campos obrigatórios e 1 campo opcional, separados por espaços. Os campos podem conter qualquer um dos valores permitidos, em conjunto com várias combinações dos caracteres especiais permitidos nesse campo.

As expressões Cron podem ser tão simples como * * * * ? *.

Ou mais complexas, como 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010.

Segue-se uma descrição dos campos.

Nome do campo	Obrigatório?	Valores permitidos	Caracteres especiais permitidos
Minutos	Sim	0-59	, - * /
Horas	Sim	0-23	, - * /
Dia do mês	Sim	1-31	, - * ? / L W C
Mês	Sim	1-12 ou JAN-DEC	, - * /
Dia da semana	Sim	1-7 ou SUN-SAT	, - * ? / L C #
Ano	Não	vazio, 1970-2099	, - * /

Caracteres especiais

- O carácter * é utilizado para especificar todos os valores. Por exemplo, no campo de minutos, * indica qualquer minuto.
- O carácter ? (sem valor específico) é útil quando necessita de especificar algo num dos dois campos em que o carácter é permitido, mas não no outro. Por exemplo, para accionar um processo num dia específico do mês (dia 10), independentemente do dia da semana a que corresponde, utilize 10 no campo de dia do mês e ? no campo de dia da semana.
- O carácter - é utilizado para especificar intervalos. Por exemplo, no campo de hora, 10-12 refere-se às horas 10, 11 e 12.
- O carácter , é utilizado para especificar valores adicionais. Por exemplo, no campo de dia da semana, MON,WED,FRI refere-se a segunda-feira, quarta-feira e sexta-feira.

- O carácter / é utilizado para especificar incrementos.

  No campo de segundos, 0/15 refere-se aos segundos 0, 15, 30 e 45.

  No campo de segundos, 5/20 refere-se aos segundos 5, 15, 35 e 50.

  Especificar * antes de / equivale a especificar 0 como valor inicial.

  No campo de dia do mês, 1/3 refere-se a cada 3 dias começando no primeiro dia de cada mês.

  Essencialmente, para cada campo da expressão existe um conjunto de números que podem ser activados ou desactivados. Para os segundos e minutos, os números situam-se entre 0 e 59; para as horas, de 0 a 23; para dias do mês, de 0 a 31; para meses, 1 a 12. O carácter / serve apenas para o ajudar a accionar a cada ".º" valor no conjunto determinado. Desta forma, no campo de mês, 7/6 apenas acciona no 7.º mês; não significa a cada 6 meses.

- O carácter L é permitido para os campos de dia do mês e dia da semana. Este carácter refere-se a "último", mas tem diferentes significados em cada um destes campos.

  O valor L do campo de dia do mês refere-se ao último dia do mês (dia 31 em janeiro, dia 28 em fevereiro, em anos comuns).

  Se for utilizado no campo de dia da semana por si só, significa 7 ou SAT.

  Se utilizado no campo de dia da semana após outro valor, refere-se ao último dia xxx do mês. Por exemplo, 6L refere-se à última sexta-feira do mês. Ao utilizar a opção L, é importante não especificar listas nem intervalos de valores, caso contrário obterá resultados confusos.

- O carácter W é permitido para o campo de dia do mês. Este carácter é utilizado para especificar o dia útil (segunda a sexta-feira) mais próximo do dia introduzido. Por exemplo, se especificar 15W como o valor do campo de dia do mês, refere-se ao dia útil mais próximo do dia 15 do mês. Por isso, se o dia 15 for um sábado, o processo será accionado na sexta-feira dia 14. Se o dia 15 for um domingo, o processo será accionado na segunda-feira dia 16. Se o dia 15 for uma terça-feira, o processo será accionado na terça-feira dia 15. No entanto, se especificar 1W como valor para o dia do mês, e o dia 1 for um sábado, o processo será accionado na segunda-feira dia 3, uma vez que o limite do mês não é ultrapassado. Apenas é possível especificar o carácter W quando o dia do mês for um dia único e não um intervalo ou lista de dias.

  Também é possível combinar os caracteres L e W para a expressão de dia do mês, com LW, que se refere ao último dia útil do mês.

- O carácter # é permitido para o campo de dia da semana. Este carácter é utilizado para especificar o xxx ".º" dia do mês. Por exemplo, o valor 6#3 no campo de dia da semana refere-se à terceira sexta-feira do mês (dia 6 = sexta-feira e #3 = a 3.ª do mês).

  Outros exemplos:
  2#1 = a primeira segunda-feira do mês
  4#5 = a quinta quarta-feira do mês.

  Tenha em atenção que, se especificar #5 e não existir esse dia da semana pela 5.ª vez nesse mês, não será accionado o processo nesse mês.

- O carácter C é permitido para calendário. A utilização deste carácter significa que os valores são calculados face ao calendário associado, caso exista. Se não existir qualquer calendário associado, é o equivalente a ter um calendário com tudo incluído. No campo de dia do mês, um valor de 5C refere-se ao primeiro dia incluído no calendário no dia 5 ou após este. No campo de dia da semana, um valor de 1C refere-se ao primeiro dia incluído no calendário num domingo ou após este dia.

NOTA: a possibilidade de especificar um valor de dia da semana e de dia do mês em simultâneo ainda não está concluída. Utilize o carácter ? num destes campos. As funcionalidades descritas para o carácter C anda não está concluídas. Os caracteres legais e os nomes de meses e dias da semana não são sensíveis a maiúsculas e minúsculas. MON equivale a mon. Preste especial atenção aos efeitos de ? e * nos campos de dia da semana e dia do mês.
Tenha cuidado ao definir horas de activação entre a meia-noite e a 1h00. A hora de verão pode provocar um avanço (ou repetição) consoante a hora adianta ou atrasa.

Exemplos

Expressão	Significado
0 0 12 * * ?	Accionar às 12h00 (meio-dia) todos os dias
0 15 10 ? * *	Accionar às 10h15 todos os dias
0 15 10 * * ?	Accionar às 10h15 todos os dias
0 15 10 * * ? *	Accionar às 10h15 todos os dias
0 15 10 * * ? 2005	Accionar às 10h15 todos os dias durante o ano de 2005
0 * 14 * * ?	Accionar a cada minuto, começando às 14h00 e terminando às 14h59, todos os dias
0 0/5 14 * * ?	Accionar a cada 5 minutos, começando às 14h00 e terminando às 14h55, todos os dias
0 0/5 14,18 * * ?	Accionar a cada 5 minutos começando às 14h00 e terminando às 14h55 E accionar a cada 5 minutos começando às 18h00 e terminando às 18h55, todos os dias
0 0-5 14 * * ?	Accionar a cada minuto, começando às 14h00 e terminando às 14h05, todos os dias
0 10,44 14 ? 3 WED	Accionar às 14h10 e às 14h44 todas as quartas-feiras do mês de março.
0 15 10 ? * MON-FRI	Accionar às 10h15 todas as segundas, terças, quartas, quintas e sextas
0 15 10 15 * ?	Accionar às 10h15 do 15.º dia de cada mês
0 15 10 L * ?	Accionar às 10h15 do último dia de cada mês
0 15 10 ? * 6L	Accionar às 10h15 da última sexta-feira de cada mês
0 15 10 ? * 6L	Accionar às 10h15 da última sexta-feira de cada mês
0 15 10 ? * 6L 2002-2005	Accionar às 10h15 de cada última sexta-feira de cada mês durante os anos de 2002, 2003, 2004 e 2005
0 15 10 ? * 6#3	Accionar às 10h15 da terceira sexta-feira de cada mês
0 0 12 1/5 * ?	Accionar às 12h00 (meio-dia) a cada 5.º dia de cada mês, começando no primeiro dia do mês.
0 11 11 11 11 ?	Accionar a cada dia 11 de Novembro às 11h11.

9

Criar um certificado auto-assinado utilizando o Keytool e gerar uma Solicitação de assinatura de certificado

NOTA: esta secção debruça-se sobre os passos necessários para criar um certificado auto-assinado para componentes baseados em Java. *Não é possível* utilizar este processo para criar um certificado auto-assinado para componentes baseados em .NET.

Recomendamos os certificados auto-assinados *apenas* em ambientes que não sejam de produção.

Se a sua organização necessitar de um certificado do servidor SSL, ou se necessitar de criar um certificado por outros motivos, esta secção descreve o processo para criar um Keystore Java utilizando o Keytool.

O Keytool cria chaves privadas emitidas sob a forma de uma Solicitação de assinatura de certificado (CSR) para uma Autoridade de certificação (AC), como VeriSign® ou Entrust®. Com base neste CSR, a AC irá criar um certificado do servidor assinado. O certificado do servidor é então transferido para um ficheiro em conjunto com o certificado da autoridade de assinatura. Os certificados são então importados para o ficheiro cacerts.

Gerar um novo par de chaves e um certificado auto-assinado

1. Navegue até ao directório conf do Compliance Reporter, Console Web Services, Device Server ou Gatekeeper Web Services.
2. Faça uma cópia de segurança da base de dados de certificados predefinida:

   Clique em Iniciar > Executar e introduza move cacerts cacerts.old.
3. Adicione o Keytool ao caminho do sistema. Introduza o seguinte comando numa linha de comandos:

   ```
   set path=%path%;%dell_java_home%\bin
   ```
4. Para gerar um certificado, execute o Keytool da forma apresentada:

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Introduza as seguintes informações quando forem solicitadas pelo Keytool.

NOTA: antes da edição, faça uma cópia de segurança dos ficheiros de configuração. Altere apenas os parâmetros especificados. A alteração de outros dados destes ficheiros, incluindo etiquetas, pode provocar danos e falha do sistema. A Dell não pode garantir que é possível solucionar os problemas resultantes de alterações não autorizadas a estes ficheiros através da reinstalação do Enterprise Server.

- *Palavra-passe Keystore:* introduza uma palavra-passe (os caracteres não suportados são <>;&" ') e defina a variável do ficheiro conf de componentes para o mesmo valor, da seguinte forma:

  <Compliance Reporter install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =

  <Console Web Services install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =

  <Device Server install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =
- *Primeiro e último nome:* introduza o nome totalmente qualificado do servidor onde está instalado o componente com o qual está a trabalhar. Este nome totalmente qualificado inclui o nome do anfitrião e o nome do domínio (exemplo: server.dell.com).

- *Unidade organizacional:* introduza o valor adequado (exemplo: Segurança).
- *Organização:* introduza o valor adequado (exemplo: Dell).
- *Cidade ou localidade:* introduza o valor adequado (exemplo: Austin).
- *Estado ou província:* introduza o nome não abreviado do estado ou província (exemplo: Texas).
- Código de país de duas letras:

  Estados Unidos = US

  Canadá = CA

  Suíça = CH

  Alemanha = DE

  Espanha = ES

  França = FR

  Grã-Bretanha = GB

  Irlanda = IE

  Itália = IT

  Holanda = NL
- O utilitário solicita confirmação de que as informações estão corretas. Em caso afirmativo, introduza `sim`. Em caso negativo, introduza `não`. O Keytool apresenta cada valor apresentado anteriormente. Prima **Enter** para aceitar o valor ou alteração ao valor e prima **Enter**.
- *Palavra-passe chave para alias:* se não introduzir aqui outra palavra-passe, a predefinição será a palavra-passe Keystore.

Solicitar um certificado assinado de uma Autoridade de certificação

Utilize este procedimento para gerar uma Solicitação de assinatura de certificado (CSR) para o certificado auto-assinado criado em Gerar um novo par de chaves e um certificado auto-assinado<Default Font>.

1 Substitua pelo mesmo valor utilizado anteriormente para <**certificatealias**>:

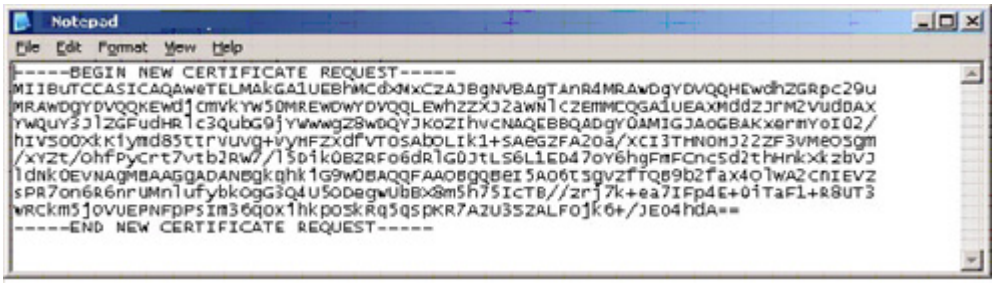
```
keytool -certreq -sigalg MD5withRSA -alias <certificate-alias> -keystore
.\cacerts -file <csr-filename>
```

Exemplo:

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

O ficheiro .csr contém um par BEGIN/END que será utilizado durante a criação do certificado pela AC.

Figura 9-1. Exemplo: ficheiro .CSR



2 Siga o seu processo organizacional para adquirir um certificado do servidor SSL de uma Autoridade de certificação. Envie os conteúdos do <csr-filename> para assinatura.

NOTA: Existem vários métodos para solicitar um certificado válido: Exemplo de método para solicitar um certificado<Default Font> apresenta um método de **exemplo**.

3 Quando receber o certificado assinado, guarde-o num ficheiro.

4 Como boa prática, faça uma cópia de segurança deste certificado para o caso de ocorrer algum erro durante o processo de importação. Esta cópia de segurança evita ter de iniciar novamente o processo.

Importar um certificado de raiz

NOTA: se a Autoridade de certificação de raiz for a Verisign (mas não Verisign Test), avance para o próximo procedimento e importe o certificado assinado.

O certificado de raiz da Autoridade de certificação valida certificados assinados.

1 Siga **um** dos seguintes procedimentos:

- Transfira o certificado de raiz da Autoridade de certificação e guarde-o num ficheiro.
- Obtenha o certificado de raiz do servidor do directório da empresa.

2 Siga **um** dos seguintes procedimentos:

- Se estiver a activar o SSL para o Compliance Reporter, Console Web Services, Device Server ou Legacy Gatekeeper Connector, altere o directório **conf** de componentes.
- Se estiver a activar o SSL entre o Server e o servidor de directório da empresa, altere **<Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (a palavra-passe predefinida do JRE cacerts é **changeit**).

3 Execute o Keytool da seguinte forma para instalar o certificado de raiz:

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

Exemplo:

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

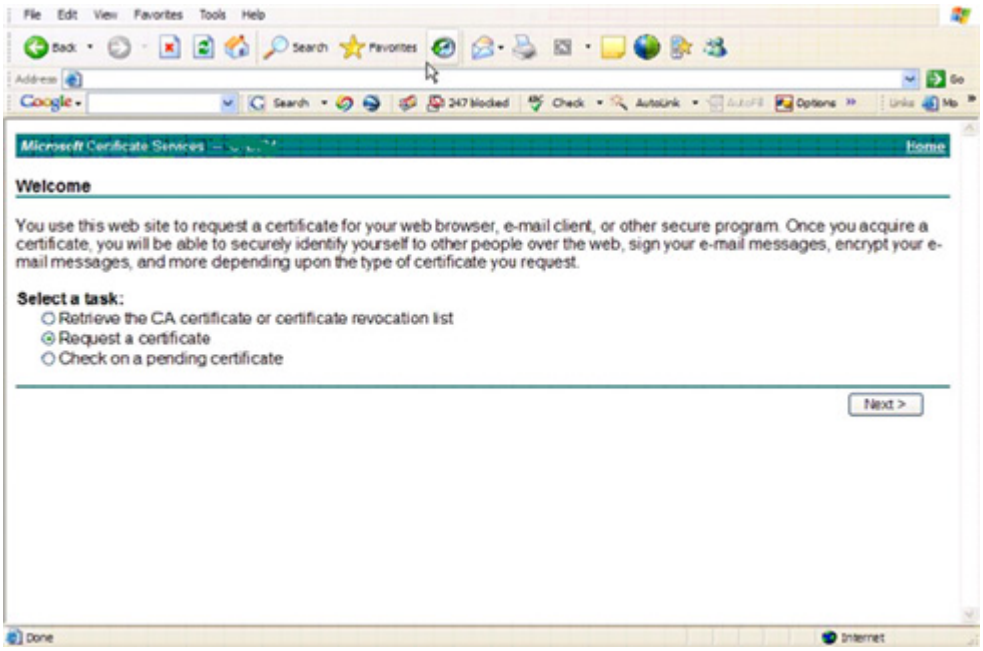
Exemplo de método para solicitar um certificado

A utilização de um navegador da Internet para aceder ao Microsoft CA Server, que será configurado internamente pela sua organização, é um exemplo de um método para solicitar um certificado.

1 Navegue até ao Microsoft CA Server. O endereço IP será fornecido pela sua organização.

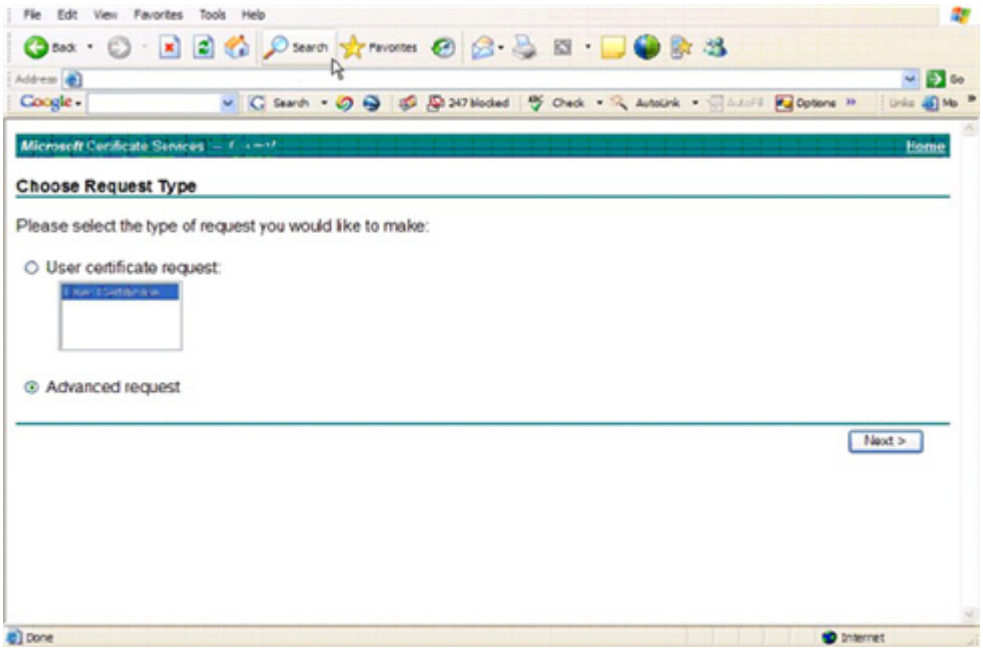
2 Seleccione **Solicitar certificado** e clique em **Seguinte**.

Figura 9-2. Serviços de certificados da Microsoft



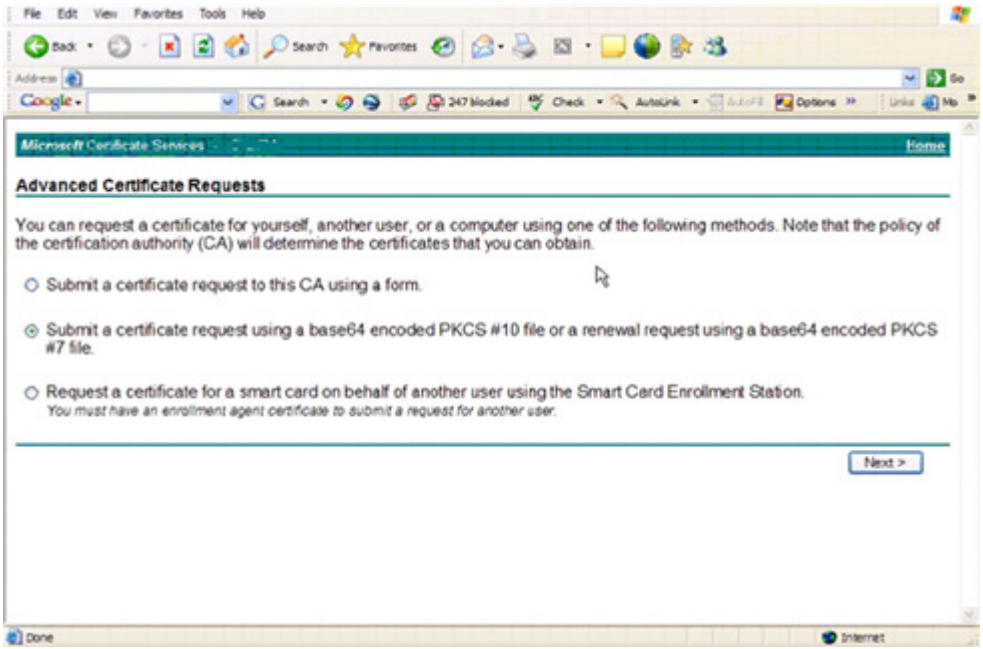
3 Seleccione **Pedido avançado** e clique em **Seguinte**.

Figura 9-3. Seleccione o tipo de pedido



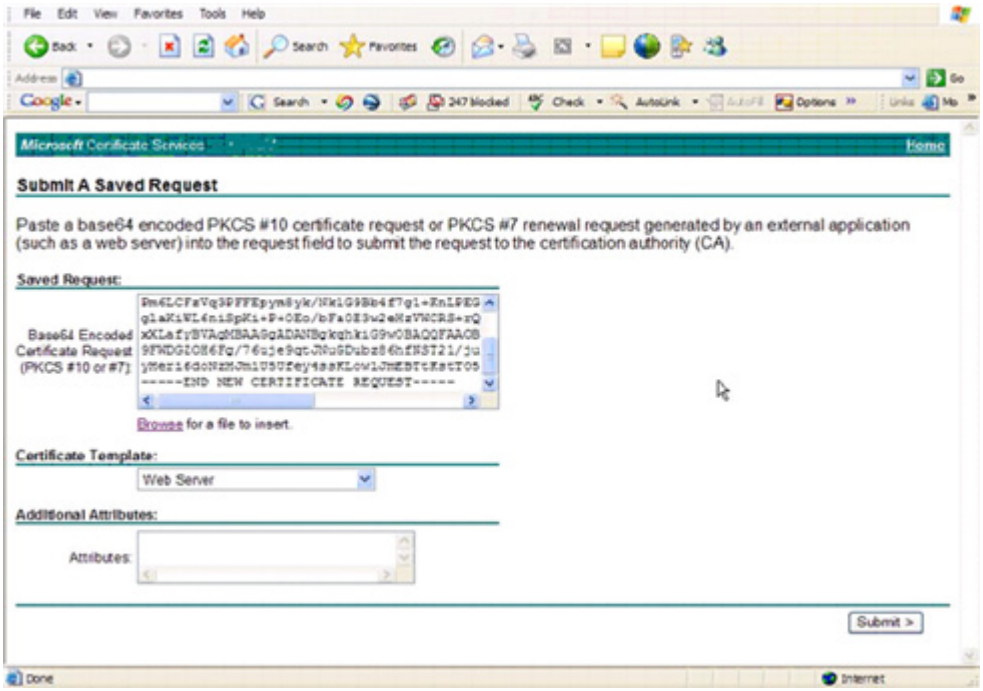
4 Seleccione a opção de **Enviar solicitação de certificado utilizando um ficheiro base64 encode PKCS #10** e clique em **Seguinte >**.

Figura 9-4. Pedido de certificado avançado



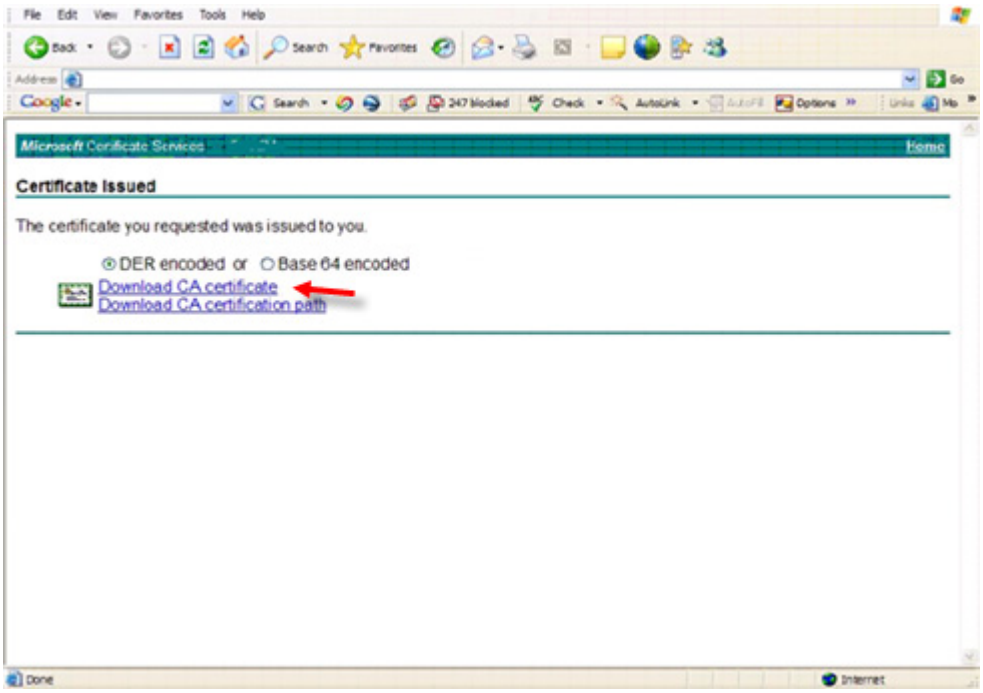
5 Cole o conteúdo do pedido CSR na caixa de texto. Seleccione um modelo de certificado do **Web Server** e clique em **Enviar >**.

Figura 9-5. Enviar um pedido guardado



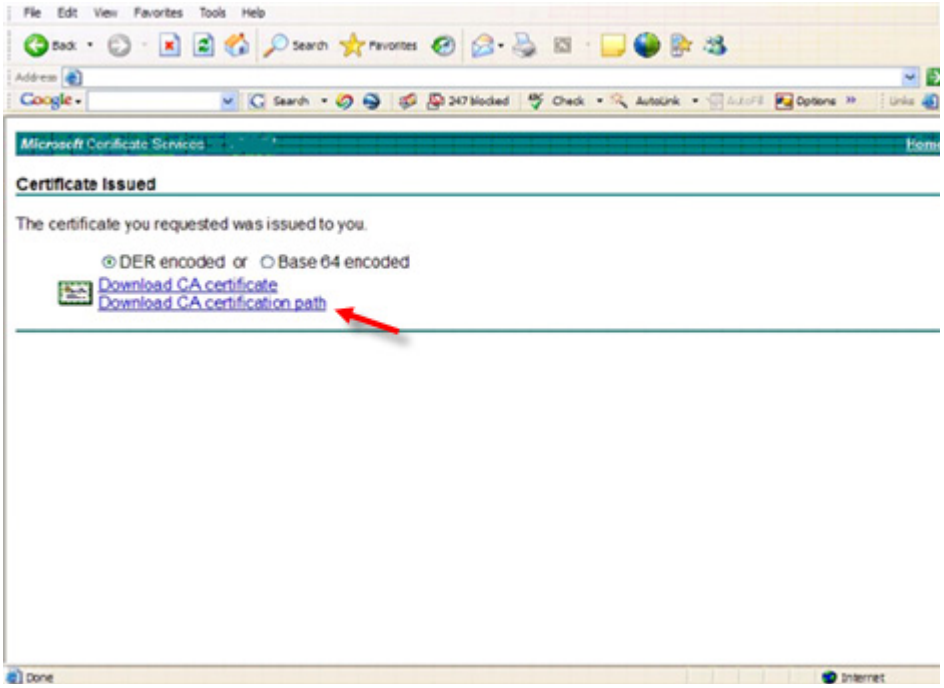
6 Guarde o certificado. Seleccione Codificação DER e clique em Transferir certificado da AC.

Figura 9-6. Transferir o certificado da AC



7 Guarde o certificado. Seleccione Codificação DER e clique em Transferir certificado da AC.

Figura 9-7. Transferir caminho de certificado da AC



8 Importe o certificado convertido da autoridade de assinatura. Regresse à janela DOS. Introduza:

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

9 Depois de importar o certificado da autoridade de assinatura, é possível importar o certificado do servidor (é possível estabelecer a cadeia de confiança). Introduza:

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

Utilize o alias do certificado auto-assinado para emparelhar o pedido CSR com o certificado do servidor.

10 Uma listagem do ficheiro cacerts mostra que o certificado do servidor possui um **comprimento da cadeia de certificação** de **2**, o que indica que o certificado não é auto-assinado. Introduza:

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

Tenha em atenção que a impressão digital do segundo certificado da cadeia consiste no certificado da autoridade de assinatura importado (que também se encontra na listagem de certificados do servidor).

O certificado do servidor foi importado com êxito, em conjunto com o certificado da autoridade de assinatura.


0 XXXXXA0 X