Dell Data Protection

Guia de configuração

2014-02

Índice

1

Configurar o Servidor de compatibilidade

Este capítulo detalha os parâmetros que podem ser alterados para ajustar o Servidor de compatibilidade para o seu ambiente. Sempre faça um backup dos arquivos de configuração antes de editá-los.

Altere somente os parâmetros documentados neste arquivo. Alterar outros dados neste arquivo, incluindo tags, pode causar falha e corromper o sistema. A Dell não garante que os problemas resultantes de alterações não autorizadas nesse arquivo possam ser resolvidas sem reinstalar o Servidor de compatibilidade.

server_config.xml

Você pode mudar alguns dos parâmetros a seguir no **<Diretório de instalação do servidor de compatibilidade>\conf\server_config.xml**. Os parâmetros que não devem ser alterados estão indicados. Se o Servidor de compatibilidade estiver em execução, você deve parar o serviço do servidor de compatibilidade, editar o arquivo server_config.xml e, em seguida, reiniciar o serviço do servidor de compatibilidade para que as alterações deste arquivo tenham efeito.

server_config.xml		
Parâmetro	**Padrão**	**Descrição**
secrets.location	$dell.home$/conf/secretKeyStore	Localização padrão do secretkeystore. Se você mudar esse arquivo da localização padrão, atualize este parâmetro.
archive.location	$dell.home$/conf/archive	Localização padrão do arquivo. Se você mudar esse arquivo da localização padrão, atualize este parâmetro.
domain.qualified.authentication	true	Indica se um nome de login do usuário totalmente qualificado é necessário para todas as solicitações no servidor. Se este valor for alterado, o servidor de dispositivo deverá ser reiniciado antes que o novo valor entre em vigor.
directory.max.search.size	1000	Limita a ação de *Localizar* em um diretório, após a qual uma exceção é gerada.
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	**Padrão**	**Descrição**
rmi.recovery.host		Para usar o Multi-Server EMS Recovery: <!-- - remove comentários e altera os nomes de host para os nomes de domínios totalmente qualificados para a recuperação da cadeia <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	O nome padrão do Grupo ao qual todos os proxies de política pertencem por padrão. Você pode alterar esse nome aqui ou no context.properties do servidor do dispositivo. Se você alterar o nome do grupo aqui, precisará alterá-lo no servidor de dispositivo, se pretender: • Usar dispositivos Shield do Windows • Usar o CREDActivate Recomendamos que todos os seus proxies de políticas pertençam a um único grupo.
rsa.securid.enabled	false	Se você estiver usando o RSA SecurID para Microsoft Windows versão 6 como seu substituto GINA, defina este parâmetro como true, e, em seguida, pare e reinicie o serviço de servidor de compatibilidade. Quando forem ativados os usuários Shield em um ambiente de substituição RSA GINA, a autenticação RSA substituirá a autenticação LDAP.
inv.queue.task.worker.size	10	Número de threads processando a fila de inventário.
inv.queue.task.timeout.seconds	900	Número de segundos antes de ocorrer o tempo limite.
inv.queue.task.retry.count	3	Número de vezes que o servidor tenta processar o inventário antes de descartá-lo.
report.retry.max	120	Número máximo de tentativas de repetição.
report.retry.wait.millis	250	Número de milisegundos aguardados antes de tentar novamente.

server_config.xml		
Parâmetro	**Padrão**	**Descrição**
triage.execute.time	0 0 0/6 * *	Triagem é o processo de reconciliar os usuários e grupos que o servidor já conhece. A configuração padrão é 0 0 0/6 * * ?, o que significa que fazemos a triagem a cada 6 horas a partir de meia-noite (meia-noite, 6:00, meio-dia, 18:00, meia-noite...)
gatekeeper.service.max.sessions	5	Número máximo de sessões proxy de política.
gatekeeper.service.max.session.timeout	5	Tempo de espera para o número máximo de sessões proxy de política.
security.authorization.method.IAdministrativeService.updateAdminRoles	AcctAdmin	Função necessária para atualizar as funções administrativas de um grupo ou usuário.
security.authorization.method.IAdministrativeService.getAdministrativeAccountGroups	AcctAdmin	Função necessária para atualizar as funções administrativas de um grupo ou usuário
security.authorization.method.IAdministrativeService.openGetLogsSession	SystemAdmin,LogAdmin	Funções necessárias para recuperar sessões de log.
security.authorization.method.IAdministrativeService.getLogs	SystemAdmin,LogAdmin	Funções necessárias para recuperar os logs.
security.authorization.method.IAdministrativeService.getLogColumnList	SystemAdmin,LogAdmin	Funções necessárias para recuperar a lista de coluna de log.
security.authorization.method.IAdministrativeService.getLogCategoryList	SystemAdmin,LogAdmin	Funções necessárias para recuperar a lista de categoria de log.
security.authorization.method.IAdministrativeService.getLogPriorityList	SystemAdmin,LogAdmin	Funções necessárias para recuperar a lista de prioridade de log.
security.authorization.method.IAdministrativeService.getUniqueIdName	AcctAdmin,SecAdmin,HelpDeskAdmin,SystemAdmin	Funções necessárias para recuperar nomes de ID exclusivo.
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 senha de superadmin.
security.authorization.method.IAdministrativeService.resetSuperAdminPassword	SecAdmin	Função necessária para redefinir a senha de 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 atualizar 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	**Padrão**	**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 usuários LDAP.
security.authorization.method.IAdministrativeService.addUsers	SystemAdmin,SecAdmin	Funções necessárias para adicionar usuários.
security.authorization.method.IAdministrativeService.addLicense	SystemAdmin	Função necessária para adicionar licenças enterprise.
security.authorization.method.IAdministrativeService.getLicense	SystemAdmin	Função necessária para visualizar licenças enterprise.
security.authorization.method.IDeviceManager.recoverDevice	HelpDeskAdmin,SecAdmin	Funções necessárias para recuperar um dispositivo.
security.authorization.method.IDeviceManager.isUserSuspended	HelpDeskAdmin,SecAdmin	Funções necessárias para suspender usuários.
security.authorization.method.DeviceManagerService.proxyActivate	SecAdmin	Funções necessárias para ativar dispositivos por proxy.
security.authorization.method.DeviceManagerService.proxiedDeviceManualAuth	HelpDeskAdmin,SecAdmin	Funções necessárias para recuperar manualmente um dispositivo por proxy.
security.authorization.method.IFileManager.getGatekeeperResource	SystemAdmin	Função necessária para recuperar o arquivo de recurso do Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperResource	SystemAdmin	Função necessária para aprovar o arquivo de recurso do Gatekeeper.
security.authorization.method.IFileManager.approveGatekeeperConfig	SystemAdmin	Funções necessárias para aprovar a configuração do Gatekeeper.
policy.arbiter.security.mode	more-restrictive	Esta propriedade controla a forma como o algoritmo de mapeamento de política funciona para os elementos políticos que têm um viés de segurança quando a política tem vários nós pai. Valores: Menos restritivo - é usado o valor do elemento menos restritivo dos pais Mais restritivo - é usado o valor do elemento mais restritivo dos pais
policy.set.synchronization.sync-unmodified	true	Este indicador sinaliza que a próxima sincronização externa deve adicionar ou remapear todos os elementos de política sem definir o indicador modificado para true. Este indicador é alterado para false depois de cada sincronização, por isso deve ser reiniciado caso o administrador de segurança deseje adicionar sem modificações. Esta é uma opção avançada.
db.schema.version.major		Esquema de banco de dados principal.
db.schema.version.minor		Esquema de banco de dados secundário.

server_config.xml		
Parâmetro	**Padrão**	**Descrição**
db.schema.version.patch		Versão do patch do esquema de banco de dados.
dao.db.driver.dir	$dell.home$/lib/mssql-microsoft	Localização padrão do driver do banco de dados. Se você mudar esse arquivo da localização padrão, atualize este parâmetro.
dao.db.host		Nome de host do seu servidor de banco de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.name		O nome do seu banco de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.user		O nome de usuário com permissões completas para seu banco de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.password		A senha para o nome de usuário com permissões completas para seu banco de dados. Este parâmetro é alterado na Ferramenta de configuração.
dao.db.max.retry.count	10	O número máximo de vezes que o servidor de compatibilidade tenta se reconectar com o SQL Server, quando ocorre um erro de soquete especificado.
dao.db.connection.retry.wait.seconds	5	A primeira tentativa de reconexão é imediata. A segunda acontece depois do número especificado de segundos. A terceira acontece depois do dobro do número de segundos especificados, o quarto depois do triplo, e assim por diante.
dao.connection.pool.max.uses	10000	Permite que as conexões sejam desativadas, 0 significa não desativar.
dao.connection.pool.inactive.threshold.seconds	900	Usado para determinar quando uma conexão não foi utilizada e pode ser fechada.
dao.db.driver.socket.errors	0	O servidor de compatibilidade tenta se reconectar com o SQL Server quando ocorrerem os erros correspondentes aos códigos desta lista separada por vírgulas. 0 é o código de erro para erros de soquete do Microsoft SQL. Você também pode adicionar 17142 para os erros de pausa do servidor e 6002 para erros de desligamento do servidor.
dao.db.mssql.compatability.level	90	Valor para o SQL 2005 ou posterior.
vfs.file.handler.auth	com.credant.guardian.server.vfs.AuthFileHandler	Handler de arquivo de autorização.
vfs.file.handler.inventory	com.credant.guardian.server.vfs.InventoryFileHandler	Handler de arquivo de inventário.

server_config.xml		
Parâmetro	**Padrão**	**Descrição**
vfs.file.handler.event	com.credant.guardian.server.vfs.EventFileHandler	Handler de arquivo de evento.
gatekeeper.resource	$dell.home$/conf/gkresource.xml	Se você mover o arquivo de recurso Gatekeeper da localização padrão, atualize este parâmetro.
gatekeeper.config	$dell.home$/conf/gkconfig.xml	Se você mover o arquivo de recurso Gatekeeper da localização padrão, atualize este parâmetro.
rmi.server.registry.host	localhost	A propriedade host é apenas para o benefício de programas do cliente e para determinar onde está o registro. Ele não é usado durante a criação do registro RMI e de objetos remotos. Ele será criado no localhost.
rmi.server.registry.port	1099	A porta de registro RMI é configurável durante a instalação. Você também pode alterar a porta após a instalação usando este parâmetro. Se você alterar esse valor, também precisará configurar o Serviço da Web do Gatekeeper.
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 as 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 visualizar 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 visualizar o relatório paginado.
security.authorization.method.IReportingService.getDeviceTypeReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório do tipo de dispositivo.
security.authorization.method.IReportingService.getDeviceOsReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório do sistema operacional.
security.authorization.method.IReportingService.getDeviceModelReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar os relatórios do modelo de dispositivo.
security.authorization.method.IReportingService.getPolicyDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório de detalhes da política.
security.authorization.method.IReportingService.getWorkstationDetailReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório de detalhes da estação de trabalho.
security.authorization.method.IReportingService.getEncryptionFailuresReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório de falha de criptografia.
security.authorization.method.IReportingService.getEncryptionSummaryReport	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório do resumo de criptografia.

server_config.xml		
Parâmetro	**Padrão**	**Descrição**
security.authorization.method.IReportingService.getUserDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório de detalhes do usuário.
security.authorization.method.IReportingService.getGroupDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar o relatório de detalhes do grupo.
security.authorization.method.IReportingService.getDomainDetail	AcctAdmin,HelpDeskAdmin,SystemAdmin,SecAdmin	Funções necessárias para visualizar a lista de relatórios dos domínios.
security.authorization.method.IKeyService.getKeys	ForensicAdmin	Esta configuração é usada com um plug-in de integração forense. Entre em contato com o suporte Dell se for necessária a integração da ferramenta forense.
accountType.nonActiveDirectory.enabled	false	Habilitar ativações sem domínio é uma configuração avançada, com consequências de grande alcance. *ANTES* de habilitar esta configuração, entre em contato com o suporte ao cliente para discutir suas necessidades específicas de ambiente. Reinicie o serviço de servidor de compatibilidade depois de alterar este valor. Além dessa definição, crie ou modifique a configuração do registro no computador com o Windows da seguinte forma: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield AllowNonDomainActivations= REG_DWORD:1

gkresource.xml

Você pode alterar os parâmetros em <Diretório de instalação do servidor de compatibilidade>\conf\gkresource.xml.

Recomendamos que você rastreie suas alterações nos comentários no início do arquivo, o que permitirá que você transfira facilmente as suas alterações para o novo arquivo ao atualizar.

OBSERVAÇÃO: O arquivo gkresource.xml deve ser um arquivo XML bem formado. A Dell recomenda que você não tente editar este arquivo se não estiver familiarizado com XML. Certifique-se de usar referências de entidade, se for o caso, em vez de caracteres especiais brutos (sem escape).

Um administrador de sistema deve aprovar as alterações no arquivo de recurso Gatekeeper antes que elas tenham efeito.

Habilitar formato de nome de usuário/domínio

Adicione a seguinte sequência para ativar (ou desativar) o formato de nome de usuário/domínio. O formato está desativado se não existir a string no arquivo. Ele também pode ser desativado configurando o valor em 0.

1. Acesse <Diretório de instalação do servidor de compatibilidade>\conf.
2. Abra o gkresource.xml com um editor de .xml.
3. Adicione a string:

   <string name="EnableGKProbeMultiDomainSupport">1</string>
4. Salve e feche o arquivo.

run-service.conf

Você pode mudar alguns dos seguintes parâmetros em **<Diretório de instalação do servidor de compatibilidade>\conf\run-service.conf**. Estes parâmetros são ajustados automaticamente durante a instalação. Para personalizar ou fazer alterações de configuração para qualquer serviço:

1. Pare o serviço.
2. Remova o serviço.
3. Edite e salve o arquivo **run-service.conf**. Recomendamos que você rastreie suas alterações nos comentários no início do arquivo,
4. Reinstale o serviço.
5. Inicie o serviço.

run-service.conf

Parâmetro	Padrão	Descrição
JAVA_HOME	Dell\Java Runtime\jreX.x	Localização do diretório de instalação do Java.
wrapper.java.additional.5	n/d	O endereço MAC nesta linha é o endereço MAC do adaptador ethernet local. Se um servidor tiver várias NICS ou se você quiser vincular a um adaptador diferente do adaptador primário, digite o endereço físico MAC da NIC aqui, sem traços.
wrapper.ntservice.name	EpmCompatSvr	Nome do serviço.
wrapper.ntservice.displayname	Servidor de compatibilidade Dell	Exibe o nome do serviço.
wrapper.ntservice.description	Servidor de compatibilidade Enterprise	Descrição do serviço.
wrapper.ntservice.dependency.1		Dependências do serviço. Adicione dependências conforme necessário, iniciando com 1.
wrapper.ntservice.starttype	AUTO_START	Modo em que o serviço está instalado: AUTO_START ou DEMAND_START.
wrapper.ntservice.interactive	false	A definição true permite que o serviço interaja com a área de trabalho.

2

Configurar o Servidor central

Este capítulo detalha os parâmetros que podem ser alterados para ajustar o Servidor central para o seu ambiente.

Altere somente os parâmetros documentados neste arquivo. Alterar outros dados neste arquivo, incluindo tags, pode causar falha e corromper o sistema. A Dell não garante que os problemas resultantes de alterações não autorizadas nesse arquivo possam ser resolvidas sem reinstalar o Servidor central.

Alterar a Arbitragem de política de Mais seguro para Menos seguro

PolicyService.config

Modifique essa configuração para mudar a arbitragem da política de mais seguro para menos seguro. Altere a configuração em **<diretório de instalação do servidor central>\PolicyService.config**. Se o Servidor central estiver em execução, você deve parar o serviço, editar o arquivo PolicyService.config e, em seguida, reiniciar o serviço para que as alterações deste arquivo tenham efeito.

Recomendamos que você rastreie suas alterações nos comentários no início do arquivo, o que permitirá transferir facilmente as suas alterações para o novo arquivo PolicyServiceConfig.xml ao atualizar.

Modifique a seguinte seção:

```
<!-- Alvos de serviços da Web -->
<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 como menos seguro]
</object>
```

Desativar serviços da web

OBSERVAÇÃO: Esta é uma configuração avançada que só deve ser alterada sob a orientação do Suporte ao cliente.

Para desativar serviços da web no Servidor central (por exemplo, se houver uma segunda instalação do Servidor central, que só faz o processamento do inventário), altere as configurações em:

<diretório de instalação do servidor central>

Credant.Server2.WindowsService.exe.Config

e

<diretório de instalação do servidor central>\Spring.config

Se o Servidor central estiver em execução, você deve parar o serviço, editar as configurações nestes dois arquivos e, em seguida, reiniciar o serviço para que as alterações deste arquivo tenham efeito.

Credant.Server2.WindowsService.exe.Config

Remova a seguinte seção:

```
<!-- Configurações de serviços da web -->
<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 de <objeto> </objeto> nos cabeçalhos de **Aviso AOP**, **Definição de alvo de serviço da web** e **Definição de host de serviço da web**.

Ative o servidor SMTP para licenciar notificações de e-mail

Se você estiver usando o Dell Data Protection | Cloud Edition, essas configurações serão automatizadas usando a ferramenta de configuração do servidor. Utilize este procedimento se você precisar habilitar o servidor SMTP para licenciar as notificações de e-mail para fins fora do Dell Data Protection | Cloud Edition.

NotificationObjects.config

Para configurar o servidor SMTP para notificações de e-mail de licença, modifique o arquivo **NotificationObjects.config** localizado no **<diretório de instalação do servidor central>**.

Modifique 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 requer autenticação, modifique o arquivo **Notification.config** localizado no **<diretório de instalação do servidor central>**.

Modifique o seguinte:

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

Adicionar localização da pasta do servidor de compatibilidade no arquivo de configuração do servidor central

O servidor central, sendo um aplicativo .Net, às vezes pode ser impedido de acessar informações de registro devido as permissões. O problema é que o servidor central, para ler o secretkeystore (a chave de criptografia de banco de dados), precisa acessar informações de configuração do registro do servidor de compatibilidade para obter a localização do secretkeystore. Se as permissões do registro bloquearem esse acesso, então o servidor central não consegue autenticar os usuários do console. Essa configuração adiciona a localização da pasta do servidor de compatibilidade no arquivo de configuração do servidor central em caso de problemas de acesso ao registro.

1. Navegue até o <diretório de instalação do servidor central>\EntityDataAccessObjects.config.
2. Altere o seguinte item **em 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 o comentário desta linha e defina o caminho totalmente qualificado para o servidor de compatibilidade.

   </object>
3. Salve e feche o arquivo.
4. Reiniciar os serviços do servidor central e do servidor de compatibilidade.

Permitir que o servidor central faça iteração através dos métodos de autenticação

As tentativas de autenticação do servidor central podem ser bloqueadas pelo controlador de domínio devido a políticas que são configuradas nos métodos de autenticação permitidos. A melhoria foi a implementação de um "interruptor" no arquivo de configuração do servidor central para permitir que o servidor central faça iteração com vários métodos de autenticação em uma tentativa de encontrar um que funcione.

1. Navegue até o <diretório de instalação do servidor central>\Spring.config.
2. Altere o seguinte item **em 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 habilitar a funcionalidade.***

   <!-- Usada para mudar o AuthType por domínio: chave é o CID do domínio e 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. Salve e feche o arquivo.
4. Reinicie o serviço de servidor central.

3

Configurar o Servidor de dispositivo

Este capítulo detalha os parâmetros que podem ser alterados para ajustar o Servidor de dispositivo para o seu ambiente.

Altere somente os parâmetros documentados neste arquivo. Alterar outros dados neste arquivo, incluindo tags, pode causar falha e corromper o sistema. A Dell não garante que os problemas resultantes de alterações não autorizadas nesse arquivo possam ser resolvidas sem reinstalar o Servidor de dispositivo.

eserver.properties

Você pode alterar os seguintes parâmetros em **<diretório de instalação do servidor de dispositivo>\conf\eserver.properties**.

Recomendamos que você rastreie suas alterações nos comentários no início do arquivo, o que permitirá que você transfira facilmente as suas alterações para o novo arquivo ao atualizar.

eserver.properties

Parâmetro	Padrão	Descrição
eserver.default.host	Serviço do servidor de dispositivo	FQDN de onde o Serviço do servidor de dispositivo está instalado.
eserver.default.port	Enterprise Server v7.7 ou posterior - 8443 Enterprise Server pré-v7.7 - 8081	A porta que o servidor de dispositivo escutará para entrada das solicitações de ativação dos dispositivos.
eserver.use.ssl	true	O SSL está ativado por padrão. Para desativar o SSL, altere este parâmetro para false.
eserver.keystore.location	${context['server.home']}/conf/cacerts	Localização do certificado do SSL usado pelo servidor de dispositivo.
eserver.keystore.password	changeit	Se você modificou a senha cacerts na ferramenta de configuração, consequentemente este parâmetro será atualizado. Se você modificar seu cacert na ferramenta de configuração a qualquer momento após a configuração inicial, atualize este parâmetro com a sua senha do Keystore.

eserver.properties		
Parâmetro	**Padrão**	**Descrição**
eserver.ciphers		Define a lista de cifras de criptografia. Cada cifra deve ser separada por uma vírgula. Se for deixado vazio, o soquete permitirá qualquer cifra disponível suportada pelo Tomcat. Remova o comentário do exemplo abaixo para definir a lista de cifras de criptografia. Separe cada cifra com uma vírgula. Consulte o guia de referência JSSE da Sun para obter a lista de nomes dos conjuntos de cifras válidas. #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

Você pode mudar alguns dos seguintes parâmetros em **<diretório de instalação do servidor de dispositivo>\conf\run-service.conf**. Estes parâmetros são ajustados automaticamente durante a instalação. Para personalizar ou fazer alterações de configuração para qualquer serviço:

1. Pare o serviço.
2. Remova o serviço.
3. Edite e salve o arquivo **run-service.conf**. Recomendamos que você rastreie suas alterações nos comentários no início do arquivo,
4. Reinstale o serviço.
5. Inicie o serviço.

run-service.conf		
Parâmetro	**Padrão**	**Descrição**
JAVA_HOME	Dell\Java Runtime\jreX.x	Localização do diretório de instalação do Java.
wrapper.ntservice.name	EpmDeviceSvr	Nome do serviço.
wrapper.ntservice.displayname	Servidor de dispositivo Dell	Exibe o nome do serviço.
wrapper.ntservice.description	Servidor de dispositivo Enterprise	Descrição do serviço.
wrapper.ntservice.dependency.1		Dependências do serviço. Adicione dependências conforme necessário, iniciando com 1.
wrapper.ntservice.starttype	AUTO_START	Modo em que o serviço está instalado: AUTO_START ou DEMAND_START.
wrapper.ntservice.interactive	false	A definição verdadeiro permite que o serviço interaja com a área de trabalho.

4

Configurar o Servidor de segurança

Este capítulo detalha os parâmetros que podem ser alterados para ajustar o Servidor de segurança para o seu ambiente.

Altere somente os parâmetros documentados neste arquivo. Alterar outros dados neste arquivo, incluindo tags, pode causar falha e corromper o sistema. A Dell não garante que os problemas resultantes de alterações não autorizadas nesse arquivo possam ser resolvidas sem reinstalar o Servidor de segurança.

context.properties

Você pode alterar os seguintes parâmetros em **<diretório de instalação do servidor de segurança>\webapps\xapi\WEB-INF\context.properties**.

Recomendamos que você rastreie suas alterações nos comentários no início do arquivo, o que permitirá que você transfira facilmente as suas alterações para o novo arquivo ao atualizar.

context.properties		
Parâmetro	**Padrão**	**Descrição**
default.gatekeeper.group.remote	CMGREMOTE	Nome do grupo remoto do dispositivo. **Não modifique.**
xmlrpc.max.threads	250	Número máximo de threads simultâneos dentro deste servidor de dispositivo.
default.auth.upn.suffix		Sufixo UPN é anexado a um nome de login do usuário se o servidor requer um nome de usuário totalmente qualificado e um deles não é fornecido na solicitação.
device.manual.auth.enable	true	Indica se as autenticações manuais estão ativadas ou desativadas. **Não modifique.**
service.activation.enable	true	Indica se as ativações são processadas pelo servidor de dispositivo. **Não modifique.**
service.policy.enable	true	Indica se a política está ativada ou desativada. **Não modifique**.
service.auth.enable	true	Indica se as autenticações são processadas pelo servidor de dispositivo.
service.forensic.enable	true	Esta configuração é usada com um plug-in de integração forense. Entre em contato com o suporte Dell se for necessária a integração da ferramenta forense.
service.support.enable	true	Permite a recuperação de meta-informações sobre o servidor.
service.device.enable	true	Ativa o suporte de serviços shield, como o armazenamento de chaves SDE.

5

Configurar recursos de criptografia

Esta seção explica como controlar os recursos de criptografia de forma independente.

Evitar exclusão de arquivo temporário

Por padrão, todos os arquivos temporários no diretório c:\windows\temp são excluídos automaticamente durante a instalação/atualização do DDPE. A exclusão de arquivos temporários acelera a criptografia inicial e ocorre antes da varredura de criptografia inicial.

No entanto, se a sua organização usar um aplicativo de terceiros que requer que a estrutura de arquivos dentro do diretório \temp seja preservada, será necessário evitar essa exclusão.

Para desabilitar a exclusão do arquivo temporário, crie ou modifique a configuração do registro da seguinte forma:

HKLM\SOFTWARE\CREDANT\CMGShield

DeleteTempFiles (REG_DWORD)=0

Observe que **não** excluir os arquivos temporários, aumentará o tempo de criptografia inicial.

Ocultar ícones de sobreposição

Por padrão, durante a instalação, todos os ícones de sobreposição de criptografia são definidos para serem exibidos. Use a seguinte configuração de registro para ocultar os ícones de sobreposição de criptografia para todos os usuários gerenciados em um computador após a instalação original.

Crie ou modifique a configuração do registro conforme segue:

HKLM\Software\CREDANT\CMGShield

HideOverlayIcons (DWORD value)=1

Se um usuário (com os privilégios apropriados) optar por mostrar os ícones de sobreposição de criptografia, essa definição substituirá esse valor do registro.

Ocultar o ícone de bandeja do sistema

Por padrão, durante a instalação, o ícone da bandeja do sistema é exibido. Use a seguinte configuração de registro para ocultar os ícones da bandeja do sistema para todos os usuários gerenciados em um computador após a instalação original.

Crie ou modifique a configuração do registro conforme segue:

HKLM\Software\CREDANT\CMGShield

HIDESYSTRAYICON (DWORD value)=1

Ativação com intervalo

Ativação com intervalo é um recurso que permite espalhar ativações de Shields durante um determinado período de tempo a fim de aliviar a carga do servidor durante uma implantação em massa. As ativações são atrasadas com base em intervalos de tempo gerados por algoritmos para proporcionar uma distribuição regular de tempos de ativação.

A ativação com intervalo é habilitada e configurada através do instalador Shield ou da estação de trabalho Shield.

Para os usuários que necessitam de ativação por VPN, a configuração de ativação com intervalo para o Shield pode ser obrigada a adiar a ativação inicial por tempo suficiente para que haja tempo para o software cliente VPN estabelecer uma conexão de rede.

ATENÇÃO: Configure a ativação com intervalo apenas com o auxílio do suporte ao cliente. A configuração com intervalo de tempo impróprio pode resultar em um grande número de clientes tentando ativar ao mesmo tempo, com potencial de criar graves problemas de desempenho.

As seguintes chaves de registro são usadas p ara configurar a ativação com intervalo. As alterações nessas chaves do registro requerem uma reinicialização da estação de trabalho Shield para que as alterações tenham efeito.

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

  Esta configuração habilita ou desabilita o recurso de ativação com intervalo.
  Desativado=0 (padrão)
  Ativado=1

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

  O período de tempo em segundos em que ocorrerá o intervalo de ativação. Você pode usar essa propriedade para substituir o período de tempo em segundos durante o qual ocorrerá o intervalo de ativação. 25200 segundos estão disponíveis para ativações com intervalo durante um período de sete horas. A configuração padrão é 86400 segundos, o que representa uma repetição diária.

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

  O intervalo dentro da repetição, ACTIVATION_SLOT_CALREPEAT, quando ocorrem todos os intervalos de tempo de ativação. Só é permitido um intervalo. Esta configuração deve ser 0,<CalRepeat>. O desvio de 0 pode produzir resultados inesperados. A configuração padrão é 0,86400. Para definir a repetição de sete horas, use a configuração 0,25200. CALREPEAT é ativado quando um usuário Shield efetua login.

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

  O número de intervalos de ativação que podem ser perdidos antes que o computador tente ativar no próximo login do usuário cuja ativação foi intercalada. Se a ativação falhar durante esta tentativa imediata, o Shield retoma as tentativas de ativação com intervalo. Se a ativação falhar devido a uma falha de rede, a ativação será tentada após a reconexão da rede, mesmo que não tenha excedido o valor em MISSTHRESHOLD. Se um usuário desconectar antes de atingir o tempo do intervalo de ativação, um novo intervalo é atribuído no próximo login.

- HKCU/Software/CREDANT/ActivationSlot (por dados de usuário)

  O tempo adiado para tentar a ativação de intervalo, que é definido quando o usuário faz login na rede pela primeira vez após a ativação com intervalo ser habilitada. O intervalo de ativação é recalculado para cada tentativa de ativação.

- HKCU/Software/CREDANT/SlotAttemptCount (por dados de usuário)

  O número de tentativas fracassadas ou perdidas, quando o horário de intervalo chega e é tentado, mas a tentativa falha. Quando este número atingir o valor definido em ACTIVATION_SLOT_MISSTHRESHOLD, o computador tenta uma ativação imediata após a conexão com a rede.

Para habilitar a ativação com intervalo através da linha de comando, use um comando semelhante ao seguinte:

setup.exe /v"SLOTTEDACTIVATION=1 CALREPEAT=25200 SLOTINTERVALS=0.25200 <outros parâmetros>"

OBSERVAÇÃO: Certifique-se de incluir um valor que contenha um ou mais caracteres especiais, como um espaço em branco, entre aspas com escape.

Sondagem forçada

Use a seguinte configuração do registro para o Shield sondar o servidor para uma atualização de política forçada.

Crie ou modifique a configuração do registro conforme segue:

HKLM\SOFTWARE\Credant\CMGShield\Notify

PingProxy (DWORD valor)=1

Dependendo da versão do Shield, a configuração do registro desaparecerá automaticamente *ou* alterará de 1 para 0 após a conclusão da sondagem.

Dependendo do conjunto de permissões de um usuário administrador, uma alteração de permissões pode ser necessária para criar essa configuração de registro. Se surgirem problemas durante a tentativa de criar uma nova DWORD, siga as etapas abaixo para fazer a mudança de permissões.

1. No registro do Windows, vá para HKLM\SOFTWARE\Credant\CMGShield\Notify.
2. Clique com o botão direito em **Notificar** > **Permissões**.
3. Ao abrir a janela *Permissões para notificar*, marque a caixa de seleção **Controle total**.
4. Clique em **OK**.

Agora você pode criar sua nova configuração do Registro.

Opções de inventário

Use as seguintes configurações de registro para permitir que o Shield envie um inventário otimizado para o servidor, envie um inventário completo para o servidor ou envie um inventário completo de todos os usuários ativados para o servidor.

Enviar inventário otimizado para o servidor

Crie ou modifique a configuração do registro conforme segue:

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

OnlySendInvChanges (REG_DWORD)=1

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

Enviar inventário completo para o servidor

Crie ou modifique a configuração do registro conforme segue:

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

OnlySendInvChanges (REG_DWORD)=0

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

Enviar um inventário completo de todos os usuários ativados

Crie ou modifique a configuração do registro conforme segue:

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

RefreshInventory (REG_DWORD)=1

Essa entrada é excluída do registro assim que for processada. O valor é salvo no vault, por isso, mesmo se o computador for reiniciado antes que ocorra o upload do inventário, o Shield ainda processará esta solicitação com sucesso no próximo upload de inventário.

Esta entrada substitui o valor do registro OnlySendInvChanges.

Ativações sem domínio

Habilitar ativações sem domínio é uma configuração avançada, com consequências de grande alcance. Entre em contato com o suporte ao cliente para discutir suas necessidades específicas de ambiente e para obter instruções para ativar esse recurso.

6

Configurar os componentes para autorização/autenticação do Kerberos

Esta seção explica como configurar os componentes para uso com autenticação/autorização do Kerberos.

Configurar os componentes para autorização/autenticação do Kerberos

OBSERVAÇÃO: Se a autorização/autenticação do Kerberos for usada, então o servidor que contém o componente do servidor de chaves terá de fazer parte do domínio afetado.

O servidor de chaves é um serviço que escuta os clientes conectarem em um soquete. Assim que um cliente se conecta, uma conexão segura é negociada, autenticada e criptografada usando APIs Kerberos (se uma conexão segura não puder ser negociada, o cliente será desconectado).

Em seguida o servidor de chaves verifica com o servidor de dispositivo para ver se o usuário que está executando o cliente tem permissão para acessar as chaves. Este acesso é concedido no Console de gerenciamento remoto via domínios *individuais*.

Instruções de serviço do Windows

1. Navegue até o painel Serviços do Windows (Iniciar > Executar... > services.msc > OK).
2. Clique com o botão direito no servidor de chaves Dell e selecione Propriedades.
3. Vá para a guia Log On e selecione o botão de opção Esta conta:.
4. No campo Esta conta:, adicione o usuário de domínio desejado. Este usuário do domínio deve ter no mínimo direitos de administrador local para a pasta do servidor de chaves (deve poder gravar no arquivo de configuração do servidor de chaves, bem como poder gravar no arquivo log.txt.).
5. Clique em OK.
6. Reinicie o serviço (saia do painel de serviço do Windows aberto para continuar a operação).
7. Navegue até <Diretório de instalação do servidor de chave> log.txt para verificar se o serviço foi iniciado corretamente.

Instruções de arquivo de configuração do servidor de chave

1. Navegue até <Diretório de instalação do servidor de chave>.
2. Abra o Credant.KeyServer.exe.config com um editor de texto.
3. Vá para <add key="user" value="superadmin" /> e altere o valor "superadmin" para o nome do usuário apropriado (você também pode deixar como "superadmin").

   O formato "superadmin" pode ser qualquer método que possa autenticar no servidor. O nome de conta SAM, UPN ou domínio\nome de usuário são aceitáveis. Qualquer método que puder autenticar no servidor é aceitável porque a validação é necessária para *aquela* conta de usuário de autorização em relação aos diretórios ativos.

   Por exemplo, em um ambiente multi-domínio, a simples digitação de um nome de conta SAM, como "jsilva", provavelmente falhará porque o servidor não poderá autenticar "jsilva" porque ele não consegue encontrar "jsilva". Em um ambiente multi-domínio, o UPN é recomendado, apesar do formato domínio\nome de usuário ser aceitável.

   Em um ambiente de domínio único, o nome da conta SAM é aceitável.

4 Vá até <add key="epw" value="<valor criptografado da senha>" /> e altere "epw" para "senha". Depois altere "<valor criptografado da senha>" para a senha do usuário na etapa 3. Esta senha é re-criptografada quando o servidor for reiniciado.

Se estiver usando "superadmin" na etapa 3 e a senha superadmin não for "changeit", ela deverá ser alterado aqui.

5 Salve suas alterações e feche o arquivo.

Exemplo de arquivo de configuração:

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<appSettings>

<add key="port" value=8050" /> *[Que é a porta TCP que o servidor escutará. O padrão é 8050, altere se necessário.]*

<add key="maxConnections" value="2000" /> *[Quantas conexões de soquetes ativos o servidor permitirá.]*

<add key="url" value="https://keyserver.domain.com:8081/xapi" /> *[URL do servidor de dispositivo. Se o Enterprise Server for versão 7.7 ou posterior, o formato será https://keyserver.domain.com:8443/xapi/ -- Se o Enterprise Server for anterior à versão 7.7, o formato será https://keyserver.domain.com:8081/xapi (sem a barra final.]*

<add key="verifyCertificate" value="false" /> *[O valor true verifica certificados/definir para false para não verificar ou se estiver usando certificados auto-assinado]*

<add key="user" value="superadmin" /> *[Nome de usuário usado para se comunicar com o servidor de dispositivo. Este usuário deve ter o tipo Administrador forense selecionado no Console de gerenciamento remoto. O formato "superadmin" pode ser qualquer método que possa autenticar no servidor. O nome de conta SAM, UPN ou domínio\nome de usuário são aceitáveis. Qualquer método que puder autenticar no servidor é aceitável porque a validação é necessária para aquela conta de usuário de autorização em relação aos diretórios ativos. Por exemplo, em um ambiente multi-domínio, a simples digitação de um nome de conta SAM, como "jsilva", provavelmente falhará porque o servidor não poderá autenticar "jsilva" porque ele não consegue encontrar "jsilva". Em um ambiente multi-domínio, o UPN é recomendado, apesar do formato domínio\nome de usuário ser aceitável. Em um ambiente de domínio único, o nome da conta SAM é aceitável.]*

<add key="cacheExpiration" value="30" /> *[Com que frequência (em segundos) o serviço deve verificar para ver quem está autorizado a pedir as chaves. O serviço mantém um cache e registra quantos tempo tem. Assim que o cache for mais velho do que o valor (em segundos), ele obtém uma nova lista. Quando um usuário se conecta, o servidor de chave precisa baixar os usuários autorizados do servidor de dispositivo. Se não houver um cache desses usuários ou a lista não foi baixada nos últimos "x" segundos, ela será baixada novamente. Não há sondagem, mas esse valor configura o quão obsoleta a lista pode se tornar antes de ser atualizada quando for necessária.]*

<add key="epw" value="valor criptografado da senha" /> *[Senha usada para se comunicar com o servidor de dispositivo. Se for necessário alterar a senha superadmin, ela deverá ser alterada aqui.]*

</appSettings>

</configuração>

Instruções de serviço do Windows

1 Retorne ao painel de serviços do Windows.

2 Reinicie o serviço do servidor de chave Dell.

3 Navegue até <Diretório de instalação do servidor de chave> log.txt para verificar se o serviço foi iniciado corretamente.

4 Feche o painel de Serviços do Windows.

Instruções do Console de gerenciamento remoto

1. Se necessário, efetue login no Console de gerenciamento remoto.
2. Clique em **Domínios** e clique no ícone **Detalhes**.
3. Clique no **Servidor de chave**.
4. Na lista de contas do servidor de chaves, adicione o usuário que realizará as atividades de administrador. O formato é domínio\nome de usuário. Clique em **Adicionar conta**.
5. Clique em **Usuários** no menu esquerdo. Na caixa de pesquisa, procure o nome de usuário adicionado na Etapa 4. Clique em **Pesquisar**.
6. Assim que o usuário correto for localizado, clique no ícone **Detalhes**.
7. Selecione **Administrador forense**. Clique em **Atualizar**.

Agora os componentes estão configurados para a autorização/autenticação do Kerberos.

7

Atribuir função Administrador Forense

Por padrão, a Autorização forense está ativada em servidores de back-end e desativada em servidores front-end. Essas configurações são posicionadas adequadamente no momento da instalação no Servidor de dispositivo e no Servidor de segurança.

Instruções do Console de gerenciamento remoto

1. Se necessário, efetue login no Console de gerenciamento remoto.
2. No painel esquerdo, clique em **Gerenciar** > **Usuários**.
3. Na página *Pesquisar usuários*, insira o nome do usuário que você deseja fornecer a função de Administrador forense e clique em **Pesquisar** (as credenciais deste usuário são fornecidas durante a execução dos utilitários CMGAd, CMGAu, CMGAlu e no Decryption Agent no modo Forense).
4. Na página *Resultados da pesquisa de usuários*, clique no ícone **Detalhes**.
5. Na página *Detalhes do usuário: <Nome do usuário>*, selecione **Admin**.
6. Na coluna Usuário, marque **Administrador forense** e clique em **Atualizar**.

A função Administrador Forense foi definida.

Desativar Administrador Forense

1. No seu servidor de back-end, acesse **<diretório de instalação do servidor de segurança>\webapps\xapi\WEB-INF\context.properties** e altere a seguinte propriedade:

   service.forensic.enable=true

   para

   service.forensic.enable=false
2. **Reinicie** o serviço do Servidor de Segurança.
3. Navegue até <diretório de instalação do servidor de dispositivo>\webapps\ROOT\WEB-INF\web.xml. Modifique o seguinte:

   <init-param>

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

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

   </init-param>
4. **Reinicie** o serviço de servidor de dispositivo.
5. Como prática recomendada, remova a função Administrador Forense de qualquer usuário que não esteja usando as permissões da função.

8

Expressões Cron

Esta seção explica como usar formatos de expressão cron e caracteres especiais.

Introdução às expressões Cron

Cron é uma ferramenta UNIX que está presente a um longo tempo, então as suas capacidades de agendamento são poderosas e comprovadas. A classe CronTrigger baseia-se nos recursos de agendamento do cron.

O CronTrigger usa expressões cron, que podem criar agendamentos de disparos, como às 8h00 de segunda a sexta-feira ou à 1:30 toda última sexta-feira do mês.

As expressões cron são poderosas, mas podem ser confusas. Este documento visa clarear um pouco do mistério da criação de uma expressão cron, proporcionando um recurso para usar antes de procurar ajuda externa.

Formatos das expressões Cron

As expressões cron são compostas de seis campos obrigatórios e um campo opcional, separados por espaço em branco. Os campos podem conter qualquer um dos valores desejados, em conjunto com várias combinações de caracteres especiais autorizados para aquele campo.

As expressões cron pode ser tão simples como * * * * ? *.

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

Os campos são descritos a seguir.

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 caractere * é usado para especificar todos os valores. Por exemplo, * no campo minutos significa todos os minutos.
- O caractere ? (nenhum valor específico) é útil quando você precisa especificar algo em um dos dois campos em que o caractere é permitido, mas não no outro. Por exemplo, para disparar um alarme em um determinado dia do mês (dia 10), mas você não se importa em qual dia da semana será, use 10 no campo o dia do mês e ? no campo de dia da semana.
- O caractere - é usado para especificar intervalos. Por exemplo, 10-12 no campo horas significa as horas 10, 11 e 12.
- O caractere , é usado para especificar valores adicionais. Por exemplo, MON,WED,FRI no campo de dia da semana significa os dias de segunda, quarta e sexta-feira.

- O caractere / é usado para especificar incrementos.

  0/15 no campo segundos significa os segundos 0, 15, 30 e 45.

  5/15 no campo segundos significa os segundos 5, 20, 35 e 50.

  Especificar * antes de / equivale a especificar 0 como o valor para começar.

  1/3 no campo de dia do mês significa disparar a cada 3 dias, começando no primeiro dia do mês.

  Basicamente, para cada campo na expressão, há um conjunto de números que podem ser ativados ou desativados. Para segundos e minutos, os números variam de 0 a 59. Para horas, de 0 a 23, para os dias do mês, de 0 a 31. Para os meses, de 1 a 12. O caractere / simplesmente ajuda a ativar cada valor 'enésimo' em um dado conjunto. Assim, 7/6 no campo mês só é ativado no mês 7, mas isso não significa a cada 6 meses.

- O caractere L é permitido para os campos dia da semana e dia do mês. Esta caractere significa último (ou last em inglês), mas tem um significado diferente em cada um dos dois campos.

  O valor L no campo dia do mês significa o último dia do mês (dia 31 de janeiro, dia 28 de fevereiro em anos não-bissextos).

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

  Se usado no campo de dia da semana após outro valor, isso significa o último dia xxx do mês. Por exemplo, 6L significa a última sexta-feira do mês. Ao usar a opção L, é importante não especificar listas ou intervalos de valores, já que você obterá resultados confusos.

- O caractere W é permitido para o campo o dia do mês. Este caractere é usado para especificar o dia da semana (de segunda a sexta-feira) mais próximo do dia determinado. Por exemplo, se você especificar 15W como o valor para o campo do dia do mês, isso significa o dia da semana mais próximo ao dia 15 do mês. Assim, se o dia 15 for um sábado, o disparo será acionado na sexta-feira dia 14. E se o dia 15 for um domingo, o disparo será acionado na segunda-feira dia 16. Já se o dia 15 é uma terça-feira, o disparo será acionado na terça-feira dia 15. No entanto, se você especificar 1W como o valor para o dia do mês e o primeiro dia for um sábado, o gatilho será acionado na segunda-feira dia 3, pois ele não vai "saltar" sobre o limite de dias de um mês. O caractere W só pode ser especificado quando o dia do mês for um único dia, não podendo ser um intervalo ou lista de dias.

  Os caracteres L e W também podem ser combinados na expressão dia do mês para originar LW, o que significa o último dia da semana do mês.

- O caractere # é permitido para o campo o dia do mês. Este caractere é usado para especificar o 'enésimo' xxx dia do mês. Por exemplo, o valor de 6#3 no campo de dia da semana, significa a terceira sexta-feira do mês (dia 6 = sexta e #3 = o terceiro do mês).

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

  Note que se você especificar #5 e não houver o quinto determinado dia da semana, no mês, então o disparo não ocorrerá nesse mês.

- O caractere C é permitido para o calendário. Usar este carácter significa que os valores são calculados no calendário associado, se houver. Se nenhum calendário estiver associado, equivale a ter um calendário com tudo incluído. O valor 5C no campo o dia do mês significa o primeiro dia incluído no calendário ou a partir da quinta-feira. O valor 1C no campo o dia do mês significa o primeiro dia incluído no calendário ou a partir do domingo.

OBSERVAÇÃO: O suporte para especificar tanto um valor de dia da semana e do dia do mês não está completo. Use o caractere ? em um destes campos. O suporte para as funções descritas para o caractere C não está completo. Os caracteres legais e os nomes dos meses e dias da semana não diferenciam maiúsculas de minúsculas. MON é o mesmo que mon. Preste muita atenção para os efeitos do ? e * nos campos de dia da semana e de dia do mês.
Tenha cuidado ao definir horários de disparo entre meia-noite e 1:00h. O horário de verão pode provocar um salto (ou repetição), dependendo se o tempo for adiantado ou atrasado.

Exemplos

Expressão	Significado
0 0 12 * * ?	Disparo às 12h (meio-dia) todos os dias
0 15 10 ? * *	Disparo às 10:15h todos os dias
0 15 10 * * ?	Disparo às 10:15h todos os dias
0 15 10 * * ? *	Disparo às 10:15h todos os dias
0 15 10 * * ? 2005	Disparo às 10:15h todos os dias no ano de 2005
0 * 14 * * ?	Disparo a cada minuto a partir das 14:00h e terminando às 14:59h, todos os dias
0 0/5 14 * * ?	Disparo a cada 5 minutos a partir das 14:00h e terminando às 14:55h, todos os dias
0 0/5 14,18 * * ?	Disparo a cada cinco minutos a partir das 14:00h e terminando às 14:55h E disparo a cada 5 minutos a partir das 18:00h e terminando às 18:55h, todos os dias
0 0-5 14 * * ?	Disparo a cada minuto a partir das 14:00h e terminando às 14:05h, todos os dias
0 10,44 14 ? 3 WED	Disparo às 14:10h e às 14:44h toda quarta-feira no mês de março.
0 15 10 ? * MON-FRI	Disparo às 10:15h toda segunda, terça, quarta, quinta e sexta-feira.
0 15 10 15 * ?	Disparo às 10:15h no dia 15 de cada mês
0 15 10 L * ?	Disparo às 10:15h no último dia de cada mês
0 15 10 ? * 6L	Disparo às 10:15h na última sexta-feira de cada mês
0 15 10 ? * 6L	Disparo às 10:15h na última sexta-feira de cada mês
0 15 10 ? * 6L 2002-2005	Disparo às 10:15h em toda sexta-feira de cada mês durante os anos de 2002, 2003, 2004 e 2005
0 15 10 ? * 6#3	Disparo às 10:15h na terceira sexta-feira de cada mês
0 0 12 1/5 * ?	Disparo às 12h (meio-dia) a cada 5 dias todo mês, começando no primeiro dia do mês.
0 11 11 11 11 ?	Disparo a cada dia 11 de novembro às 11:11h.

9

Criar um certificado autoassinado usando Keytool e gerar uma solicitação de assinatura de certificado

OBSERVAÇÃO: Esta seção detalhe as etapas necessárias para criar um certificado autoassinado para componentes baseados em Java. Este processo *não* pode ser usado para criar um certificado autoassinado para componentes .NET.

Recomendamos um certificado autoassinado *somente* em um ambiente que não seja de produção.

Se sua organização precisar de um certificado de servidor SSL ou você precisar criar um certificador para outros motivos, esta seção descreve o processo para criar um armazenamento de chave java com Keytool.

O Keytool cria chaves privadas passadas no formato de uma CSR (solicitação de assinatura de certificado) para uma CA (Autoridade de Certificação), como VeriSign® ou Entrust®. Baseado nesta CSR, a CA criará um certificado de servidor que assina. Aí então o certificado de servidor pode ser baixado em um arquivo com o certificado de autoridade de assinatura. Os certificados são importados no arquivo cacerts.

Gerar um novo par de chaves e um certificado de autoassinado

1. Acesse o diretório **conf** do Compliance Reporter, Console Web Services, Device Server, ou Gatekeeper Web Services.
2. Faça o backup do banco de dados de certificado padrão:

   Clique em **Iniciar** > **Executar** e digite **move cacerts cacerts.old**.
3. Adicione Keytool ao caminho do sistema. Digite o seguinte comando em um prompt de comando:

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

   ```
   keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias dell -keystore
   .\cacerts
   ```
5. Insira as seguintes informações conforme o Keytool solicita.

OBSERVAÇÃO: Sempre faça um backup dos arquivos de configuração antes de editá-los. Altere somente os parâmetros especificados. Alterar outros dados nesses arquivos, incluindo tags, pode causar falha e corromper o sistema. A Dell não garante que os problemas resultantes de alterações não autorizadas nesses arquivos possam ser resolvidas sem reinstalar o Enterprise Server.

- *Senha do armazenamento de chaves:* Insira uma senha (caracteres incompatíveis: <>;&" ') e defina a variável no arquivo **conf** do componente para o mesmo valor, conforme a seguir:

  <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 =
- *Nome completo:* Insira o nome totalmente qualificado do servidor no qual o componente que você está trabalhando está instalado. Este nome totalmente qualificado inclui o nome do host e o nome do domínio (por exemplo: server.dell.com).

- *Unidade organizacional:* Insira o valor apropriado (por exemplo: Segurança).
- *Organização:* Insira o valor apropriado (por exemplo: Dell).
- *Cidade ou localidade:* Insira o valor apropriado (por exemplo: Austin).
- *Estado ou província:* Insira a abreviatura do estado ou o nome da província (por exemplo: Texas).
- Código de país de duas letras:

  EUA = US

  Canadá = CA

  Suíça = CH

  Alemanha = DE

  Espanha = ES

  França = FR

  Grã-Bretanha = GB

  Irlanda = IE

  Itália = IT

  Holanda = NL
- O utilitário solicita confirmação sobre as informações. Digite `yes` para confirmar as informações. Digite `no` para não confirmar as informações. O Keytool exibe cada valor inserido anteriormente. Clique em **Enter** para aceitar o valor ou altere o valor e clique em **Enter**.
- *Senha da chave para alias:* Se você não inserir outra senha aqui, esta senha vira padrão para a senha do Keystore.

Solicite um certificado assinado de uma autoridade de certificado

Use este procedimento para gerar uma CSR (solicitação de assinatura de certificado) para o certificado autoassinado criado em Gerar um novo par de chaves e um certificado de autoassinado<Default Font>.

1 Troque o mesmo valor usado anteriormente para <**certificatealias**>:

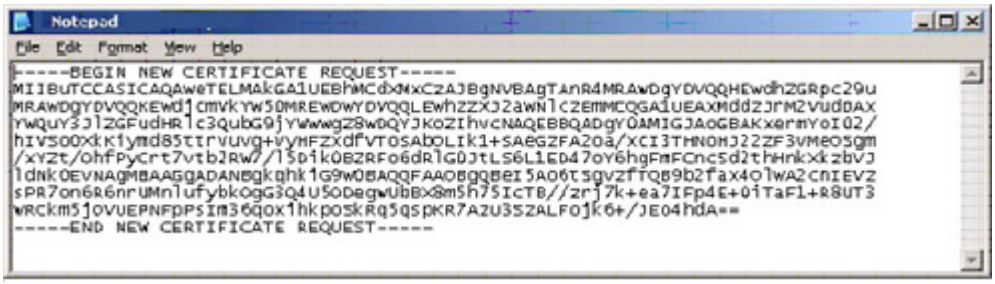
```
keytool -certreq -sigalg MD5withRSA -alias <certificate-alias> -keystore
.\cacerts -file <csr-filename>
```

Por exemplo:

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

O arquivo .csr conterá um par BEGIN/END que será usado durante a criação do certificado na CA.

Figura 9-1. Exemplo de arquivo .CSR



2 Siga o processo da sua organização para adquirir um certificado de servidor SSL de uma Autoridade de Certificado. Envie o conteúdo de <csr-filename> para assinatura.

OBSERVAÇÃO: Há vários métodos para solicitar um certificado válido. Um método de **exemplo** é mostrado em Exemplo de método para solicitar um certificado<Default Font>.

3 Quando o certificado assinado é recebido, armazene-o em um arquivo.

4 Como prática recomendada, faça o backup deste certificado para a eventualidade de ocorrer um erro no processo de importação. Com o backup você não precisará iniciar o processo de novo.

Importar um certificado raiz

OBSERVAÇÃO: Se a Autoridade de Certificação do certificado raiz for a Verisign (não a Verisign Test), ignore o próximo procedimento e importe o certificado assinado.

O certificado raiz da Autoridade de Certificação valida certificado assinados.

1 Execute **uma** das seguintes ações:

- Faça o download do certificado raiz da Autoridade de Certificação e armazene-o em um arquivo.
- Obtenha o certificado raiz do servidor do diretório corporativo.

2 Execute **uma** das seguintes ações:

- Se você estiver habilitando SSL para Compliance Reporter, Console Web Services, Device Server ou Legacy Gatekeeper Connector, mude para o componente **conf**.
- Se você habilitar SSL entre o servidor e o servidor do diretório corporativo, mude para **<Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (a senha padrão para JRE cacerts é **changeit**).

3 Execute o Keytool conforme a seguir para instalar o certificado raiz:

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

Por exemplo:

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

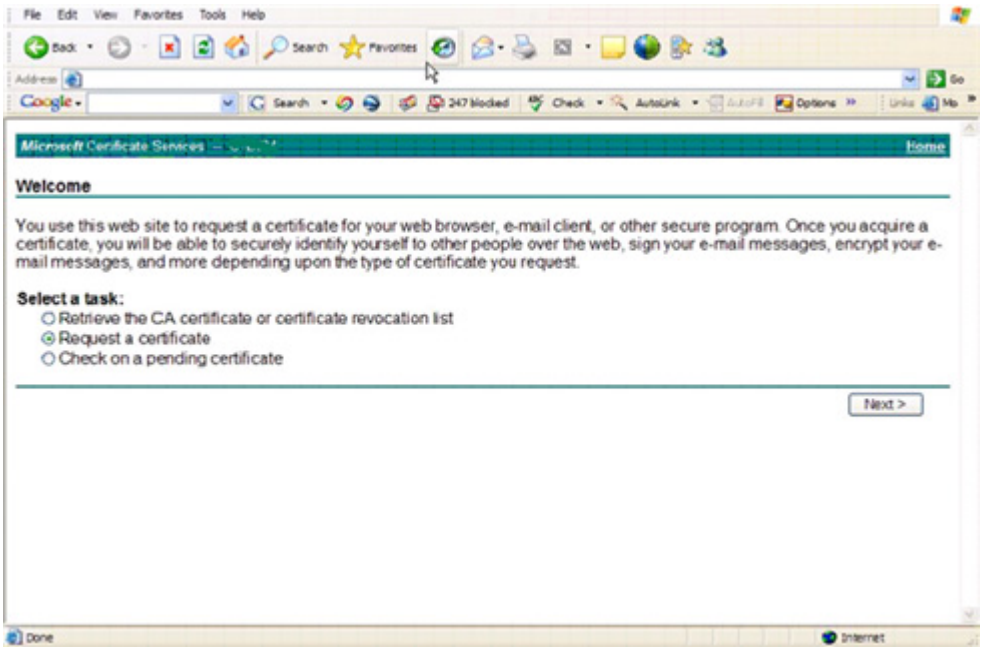
Exemplo de método para solicitar um certificado

Um exemplo de método para solicitar um certificado é usar um navegador da web para acessar o Microsoft CA Server, o que será configurado internamente pela sua organização.

1 Acesse o Microsoft CA Server. O endereço de IP será fornecido pela sua organização.

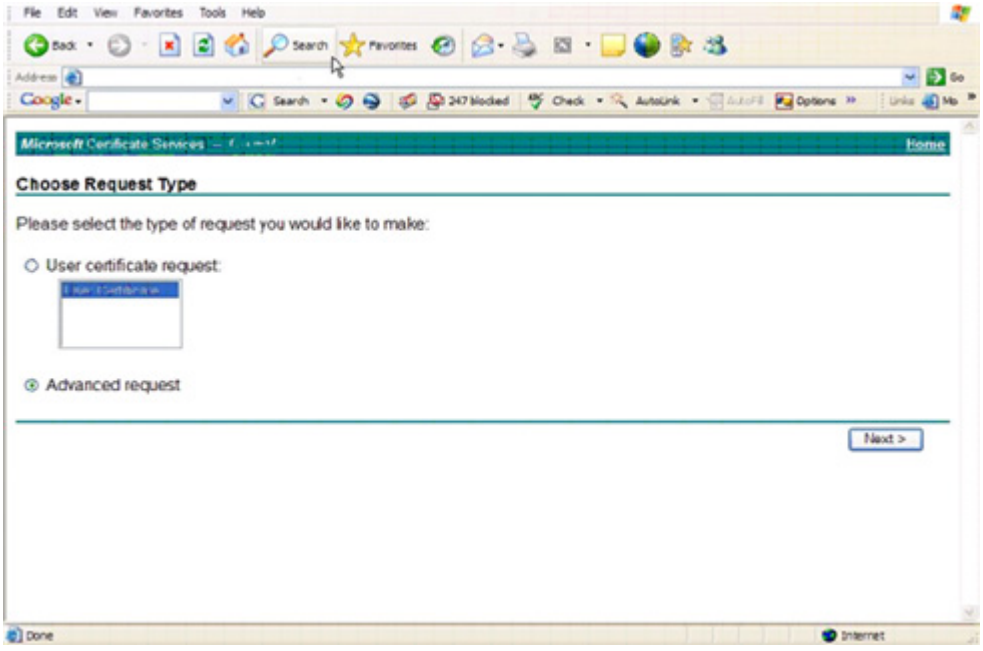
2 Selecione **Solicitar um certificado** e clique em **Avançar >**.

Figura 9-2. Microsoft Certificate Services



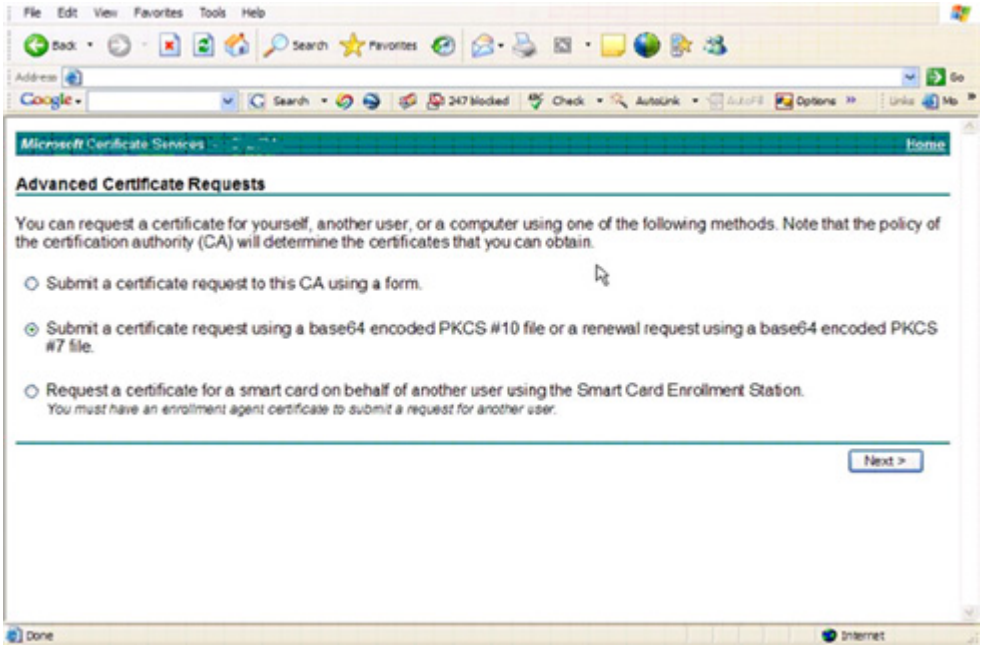
3 Selecione **Solicitação avançada** e clique em **Avançar >**.

Figura 9-3. Selecione o tipo de solicitação



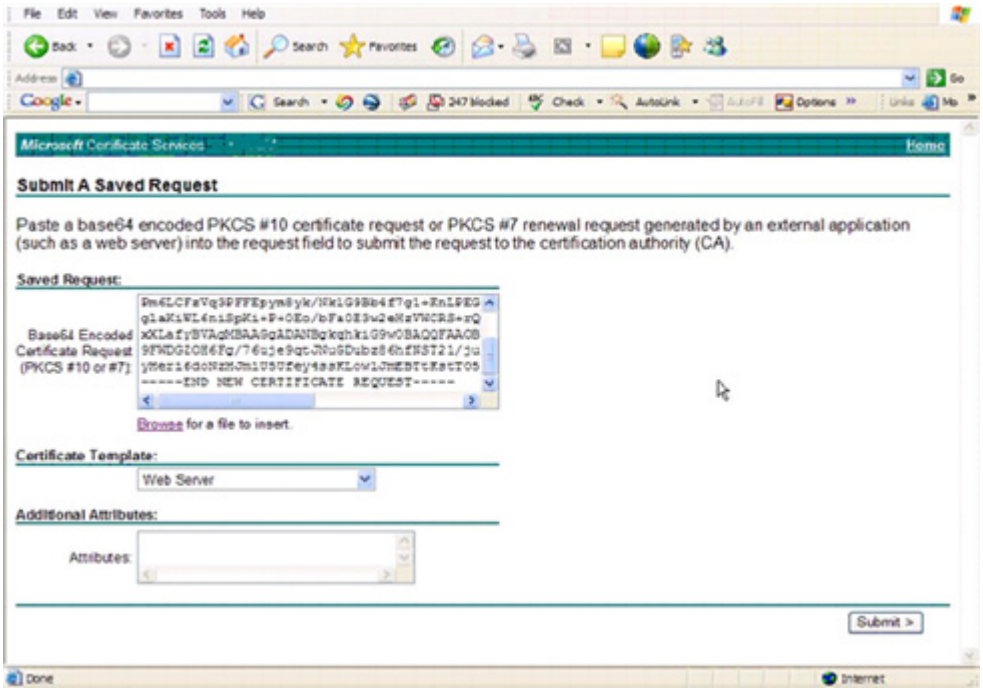
4 Selecione a opção para **Enviar uma solicitação de certificado usando um arquivo base64 encode PKCS #10** e clique em **Avançar >**.

Figura 9-4. Solicitação de certificado avançado



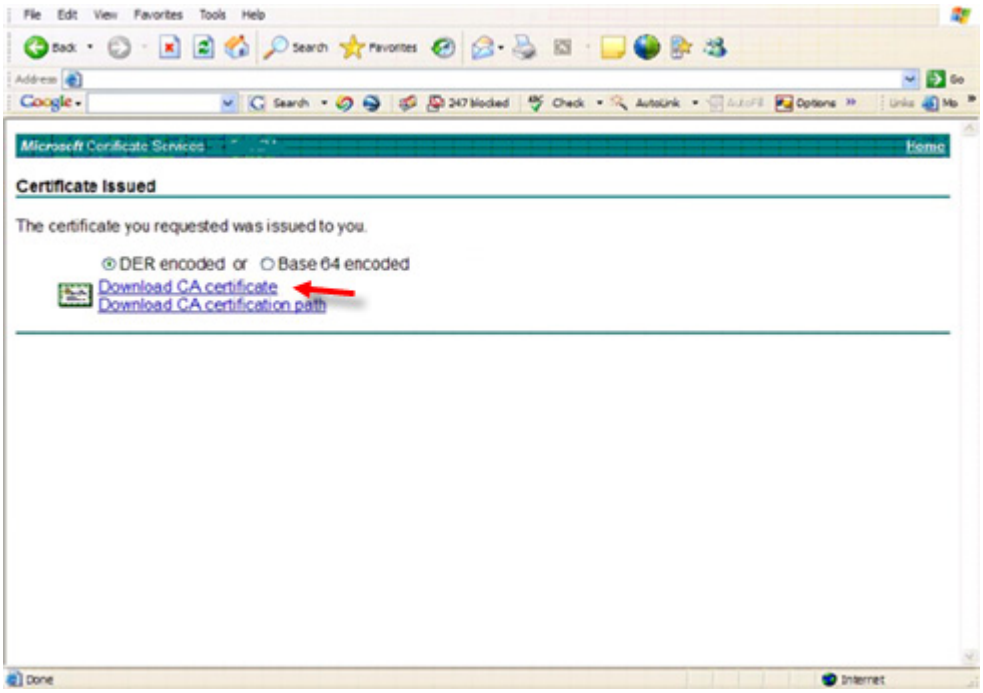
5 Cole o conteúdo da solicitação CSR na caixa de texto. Selecione um template de certificado do **Web Server** e clique em **Enviar >**.

Figura 9-5. Envie uma solicitação salva



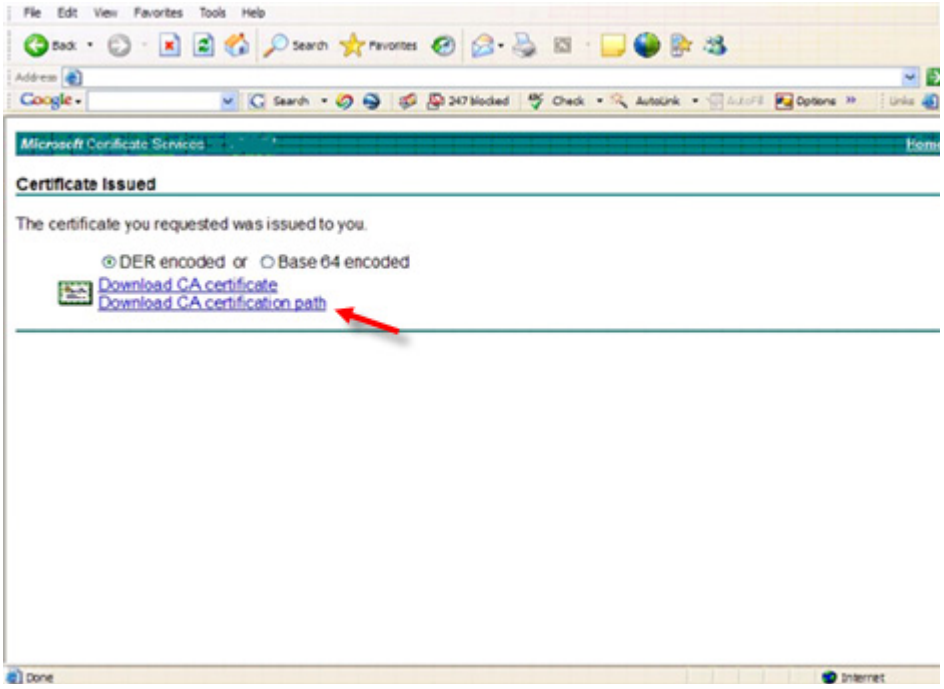
6 Salve o certificado. Selecione **Codificado por DER** e clique em **Baixar certificado da CA**.

Figura 9-6. Faça o download do certificado da CA



7 Salve o certificado. Selecione **Codificado por DER** e clique em **Baixar caminho do certificado da CA**.

Figura 9-7. Faça o download do caminho do certificado da CA



8 Importe o certificado da autoridade de assinatura convertido. Volte à janela do DOS. Digite:

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

9 Agora que o certificado de autoridade de assinatura foi importado, o certificado do servidor pode ser importado (a cadeia de confiança pode ser estabelecida). Digite:

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

Use o alias do certificado autoassinado para emparelhar a solicitação da CSR com o certificado do servidor.

10 Uma lista do arquivo cacerts mostrará que o certificado do servidor tem um **comprimento de cadeia de certificado** igual a **2**, o que indica que o certificado não é autoassinado. Digite:

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

A impressão digital do segundo certificado na cadeia é o certificado da autoridade de assinatura importada (também relacionado abaixo do certificado de servidor na lista).

O certificado do servidor foi importada com êxito, além do certificado da autoridade de assinatura.


0 XXXXXA0 X