Publique listas de revogação de certificado para o ISE em um exemplo de configuração do Microsoft CA server

Índice

Introdução

Este documento descreve a configuração de um server de Microsoft Certificate Authority (CA) que execute o Internet Information Services (IIS) para publicar atualizações do Certificate Revocation List (CRL). Igualmente explica como configurar o Cisco Identity Services Engine (ISE) (versões 1.1 e mais recente) para recuperar as atualizações para o uso na validação certificada. O ISE pode ser configurado para recuperar CRL para os vários certificados de raiz que de CA se usa na validação certificada.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Liberação 1.1.2.145 do Cisco Identity Services Engine
- ® 2008 R2 do server do ® de Microsoft Windows

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Configurações

Este documento utiliza as seguintes configurações:

- A seção 1. cria e configura um dobrador em CA para abrigar os arquivos CRL
- A seção 2. cria um local no IIS para expor o CRL Distribution Point novo
- A seção 3. configura o Microsoft CA server para publicar arquivos CRL ao ponto de distribuição
- A seção 4. verifica que o arquivo CRL existe e é acessível através do IIS
- A seção 5. configura o ISE para usar o CRL Distribution Point novo

A seção 1. cria e configura um dobrador em CA para abrigar os arquivos CRL

A primeira tarefa é configurar um lugar no server de CA para armazenar os arquivos CRL. À revelia, o Microsoft CA server publica os arquivos a C:\Windows\system32\CertSrv\CertEnroll\. Um pouco do que usa esta pasta de sistema, criam um dobrador novo para os arquivos.

1. No servidor IIS, escolha um lugar no sistema de arquivos e crie um dobrador novo. Neste exemplo, o dobrador C:\CRLDistribution é criado.
2. Para que CA redija os arquivos CRL ao dobrador novo, compartilhando deve ser permitido. Clicar com o botão direito o dobrador novo, escolha **propriedades**, clique a aba de **partilha**, e clique então **partilha avançada**.
3. A fim compartilhar do dobrador, verifique a **parte esta** caixa de verificação do **dobrador** e adicionar então um sinal de dólar ($) ao fim do nome da parte no campo de nome da parte esconder a parte.
4. Clique **permissões** (1), o clique **adiciona** (2), clica os **tipos de objeto** (3), e verifica a caixa de verificação dos **computadores** (4).
5. A fim retornar ao indicador seleto dos usuários, dos computadores, das contas de serviço,

ou de grupos, **APROVAÇÃO do** clique. Na entrada os nomes de objeto para selecionar o campo, para incorporar o nome de computador do server e do clique de CA **verificam nomes**. Se o nome dado entrada com é válido, o nome refresca e parece sublinhado. Clique em **OK**.

6. No grupo ou no campo de nomes de usuário, escolha o computador de CA. A verificação **permite o** controle total conceder o acesso direto à **APROVAÇÃO do** clique CA. Clique a **APROVAÇÃO** outra vez para fechar o indicador de partilha avançado e para retornar à janela de propriedades.
7. A fim permitir que CA redija os arquivos CRL ao dobrador novo, configurar as permissões de segurança apropriadas. Clique a **ABA de segurança** (1), o clique **edita** (2), o clique **adiciona** (3), clica os **tipos de objeto** (4), e verifica a caixa de verificação dos **computadores** (5).
8. Na entrada os nomes de objeto para selecionar o campo, para incorporar o nome de computador do server e do clique de CA **verificam nomes**. Se o nome dado entrada com é válido, o nome refresca e parece sublinhado. Clique em **OK**.
9. Escolha o computador de CA no grupo ou no campo de nomes de usuário e verifique-o então **permitem o** controle total conceder o acesso direto à **APROVAÇÃO do** clique CA e clicar então **perto de** completo a tarefa.

A seção 2. cria um local no IIS para expor o CRL Distribution Point novo

Para que o ISE alcance os arquivos CRL, faça o diretório que abriga os arquivos CRL acessíveis através do IIS.

1. Na barra de tarefas do servidor IIS, clique o **começo**. Escolha **ferramentas administrativas > gerente do Internet Information Services (IIS)**.
2. No painel esquerdo (conhecido como a árvore de console), expanda o nome de servidor IIS e expanda então **locais.**
3. Clicar com o botão direito a **website padrão** e escolha-a **adicionam o diretório virtual**.
4. No campo do pseudônimo, dê entrada com um nome de site para o CRL Distribution Point. Neste exemplo, CRLD é incorporado.
5. Clique a elipse (…) à direita do campo do caminho físico e consulte ao dobrador criado na seção 1. seleta o dobrador e clique a **APROVAÇÃO**. **APROVAÇÃO do** clique para fechar o indicador do diretório virtual adicionar.
6. O nome de site dado entrada com em etapa 4 deve ser destacado no painel esquerdo. Se não, escolha-o agora. No centro placa, **diretório do** clique duas vezes que **consulta**.
7. No painel correto, o clique **permite** de permitir o diretório que consulta.
8. No painel esquerdo, escolha o nome de site outra vez. No centro placa, **editor da configuração do** clique duas vezes.
9. Na lista de drop-down da seção, escolha **system.webServer/Segurança/requestFiltering.** Na lista de drop-down allowDoubleEscaping, escolha verdadeiro**.** No painel correto, o clique aplica-se**.**

O dobrador deve agora ser acessível através do IIS.

A seção 3. configura o Microsoft CA server para publicar arquivos CRL ao ponto de distribuição

Agora que um dobrador novo esteve configurado para abrigar os arquivos CRL e o dobrador esteve exposto no IIS, configurar o Microsoft CA server para publicar os arquivos CRL ao lugar

novo.

1. Na barra de tarefas do server de CA, clique o **começo**. Escolha **ferramentas administrativas > Certificate Authority**.
2. No painel esquerdo, clicar com o botão direito o nome de CA. Escolha **propriedades** e clique então a aba dos **Ramais**. A fim adicionar um CRL Distribution Point novo, o clique **adiciona**.
3. No campo do lugar, entre no trajeto ao dobrador criado e compartilhado na seção 1. No exemplo na seção 1, o trajeto é:`\\RTPAAA-DC1\CRLDistribution$\`
4. Com o campo do lugar povoado, escolha o **<CaName> da** lista de drop-down variável e clique então a **inserção.**
5. Da lista de drop-down variável, escolha o **<CRLNameSuffix>** e clique então a **inserção**.
6. No campo do lugar, adicione .crl à extremidade do trajeto. Neste exemplo, o lugar é:`\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`
7. Clique a **APROVAÇÃO** para retornar à aba dos Ramais. Verifique a **publicação CRL a esta** caixa de verificação do **lugar** (1) e clique então a **APROVAÇÃO** (2) para fechar a janela de propriedades. Uma alerta aparece para que a permissão reinicie serviços certificados do diretório ativo. Clique **sim** (3).
8. No painel esquerdo, clicar com o botão direito **Certificados revogados**. Escolha **todas as tarefas > publicam**. Assegure-se de que o CRL novo esteja selecionado e clique-se então a **APROVAÇÃO.**

O Microsoft CA server deve criar um arquivo novo .crl no dobrador criado na seção 1. Se o arquivo novo CRL é criado com sucesso não haverá nenhum diálogo depois que APROVADO está clicado. Se um erro é retornado com respeito ao dobrador novo do ponto de distribuição, repita com cuidado cada etapa nesta seção.

A seção 4. verifica que o arquivo CRL existe e é acessível através do IIS

Verifique que os arquivos novos CRL existem e isso são acessíveis através do IIS de uma outra estação de trabalho antes que você comece esta seção.

1. No servidor IIS, abra o dobrador criado na seção 1. Deve haver um único arquivo .crl atual com o formulário <CANAME>.crl onde <CANAME> é o nome do server de CA. Neste exemplo, o nome de arquivo é:`rtpaaa-CA.crl`
2. De uma estação de trabalho na rede (idealmente na mesma rede que o nó preliminar ISE Admin), abra um navegador da Web e consulte a http:// <SERVER>/<CRLSITE> onde <SERVER> é o nome do servidor do servidor IIS configurado na seção 2 e <CRLSITE> é o nome de site escolhido para o ponto de distribuição na seção 2. Neste exemplo, a URL é:`http://RTPAAA-DC1/CRLD`Os indicadores do deslocamento predeterminado do diretório, que inclui o arquivo observaram em etapa 1.

A seção 5. configura o ISE para usar o CRL Distribution Point novo

Antes que o ISE esteja configurado para recuperar o CRL, defina o intervalo para publicar o CRL. A estratégia para determinar este intervalo é além do alcance deste documento. Os valores potenciais (em Microsoft CA) têm 1 hora a 411 anos, inclusivos. O valor padrão é 1 semana. Uma vez que um intervalo apropriado para seu ambiente foi determinado, ajuste o intervalo com estas instruções:

1. Na barra de tarefas do server de CA, clique o **começo**. Escolha **ferramentas administrativas**

> Certificate Authority.

2. No painel esquerdo, expanda o CA clicam com o botão direito o dobrador **revogado dos Certificados** e escolhem **propriedades.**
3. Nos campos do intervalo da publicação CRL, entre no número obrigatório e escolha o período de tempo. Clique a **APROVAÇÃO** para fechar o indicador e para aplicar a mudança. Neste exemplo, um intervalo da publicação dos dias 7 é configurado.Você deve agora confirmar diversos valores de registro, que ajudarão a determinar os ajustes da recuperação CRL no ISE.
4. Incorpore o **certutil - getreg CA ** comando de **Clock*** confirmar o valor de ClockSkew. O valor padrão é os minutos 10.Saídas de exemplo:
```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```
5. Incorpore o **certutil - getreg CA ** comando de **CRLov*** verificar se o CRLOverlapPeriod esteve ajustado manualmente. À revelia o valor de CRLOverlapUnit é 0, que indica que nenhum valor manual esteve ajustado. Se o valor é um valor a não ser 0, grave o valor e as unidades.Saídas de exemplo:
```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```
6. Incorpore o **certutil - getreg CA ** comando de **CRLpe*** verificar o CRLPeriod, que foi ajustado em etapa 3.Saídas de exemplo:
```
Values:
    CRLPeriod      REG_SZ = Days
    CRLUnits        REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```
7. Calcule o período de graça CRL como segue:Se CRLOverlapPeriod foi ajustado na etapa 5: SOBREPOSIÇÃO = CRLOverlapPeriod, nos minutos;Mais: SOBREPOSIÇÃO = (CRLPeriod/10), nos minutosSe SOBREPOSIÇÃO > então SOBREPOSIÇÃO 720 = 720Se SOBREPOSIÇÃO < (1.5 * SOBREPOSIÇÃO de ClockSkewMinutes) então = (1.5 * ClockSkewMinutes)Se SOBREPOSIÇÃO > CRLPeriod, na SOBREPOSIÇÃO dos minutos então = no CRLPeriod nos minutosPeríodo de graça = 720 minutos + o 10 cronometram = 730 minutosExemplo:
```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
CRLOverlapPeriod was not set.

a. OVERLAP = (10248 / 10) = 1024.8 minutes
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```
   O período de graça calculado é a quantidade de tempo entre quando CA publica o CRL seguinte e quando o CRL atual expira. O ISE precisa de ser configurado para recuperar em conformidade os CRL.
8. Entre ao nó preliminar Admin e escolha a **administração > o sistema > os Certificados**. No painel esquerdo, **loja** seleta do **certificado**.
9. Verifique a caixa de verificação da loja do certificado ao lado do certificado de CA para que você pretende configurar CRL. O clique **edita**.
10. Perto da parte inferior do indicador, verifique a caixa de verificação da **transferência CRL**.
11. No campo URL da distribuição de CRL, entre no trajeto ao CRL Distribution Point, que inclui o arquivo .crl, criado na seção 2. Neste exemplo, a URL é:`http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. O ISE pode ser configurado para recuperar em intervalos regulares o CRL ou ser baseado na expiração (que, geralmente, é igualmente um intervalo regular). Quando o CRL publica o intervalo é estática, umas atualizações mais oportunas CRL está obtido quando a última

opção é usada. Clique **automaticamente o** botão de rádio.

13. Ajuste o valor para a recuperação a um valor menos do que o período de graça calculado na etapa 7. Se o conjunto de valores é mais longo do que o período de graça, o ISE verifica o CRL Distribution Point antes que CA publique o CRL seguinte. Neste exemplo, o período de graça é calculado para ser 730 minutos, ou 12 horas e minutos 10. Um valor das horas 10 será usado para a recuperação.
14. Ajuste o intervalo de nova tentativa como apropriado para seu ambiente. Se o ISE não pode recuperar o CRL no intervalo configurado na etapa precedente, experimentará de novo neste intervalo mais curto.
15. Verifique a **verificação do desvio CRL se o CRL não é** caixa de verificação **recebida** para permitir que a autenticação certificado-baseada continue normalmente (e sem uma verificação CRL) se o ISE era incapaz de recuperar o CRL para este CA em sua última tentativa da transferência. Se esta caixa de verificação não é verificada, toda a autenticação certificado-baseada com os Certificados emitidos por este CA falhará se o CRL não pode ser recuperado.
16. Verifique a **ignorância que o CRL não seja** caixa de verificação **ainda válida ou expirada** permitir que o ISE use (ou não ainda válido) arquivos expirados CRL como se eram válidos. Se esta caixa de verificação não é verificada, o ISE considera um CRL ser inválido antes de sua data efetiva e após os seus próximos updates time. **Salvaguarda do** clique para terminar a configuração.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems