Módulo 9

Implantação e gerenciamento de certificados

Sumário:

Lição 1

Implantação e gerenciamento de modelos de certificado

Sumário:

Perguntas e respostas

Pergunta: Quais afirmações a seguir são verdadeiras em relação à versão 2 dos modelos de certificado no AD CS? (Escolha todas as opções aplicáveis.)

( ) Os modelos versão 2 dão suporte ao registro automático.

( ) Você só pode modificar a guia Segurança no modelo versão 2.

( ) Você pode atualizar para o modelo versão 2 duplicando um modelo versão 1.

( ) Apenas o Windows Server 2008, o Windows Vista e sistemas operacionais posteriores dão suporte aos modelos versão 2.

( ) Apenas o Windows Server 2012, o Windows 8 e sistemas operacionais posteriores dão suporte aos modelos versão 2.

Resposta:

(√) Os modelos versão 2 dão suporte ao registro automático.

( ) Você só pode modificar a guia Segurança no modelo versão 2.

(√) Você pode atualizar para o modelo versão 2 duplicando um modelo versão 1.

( ) Apenas Windows Server 2008, Windows Vista e sistemas operacionais superiores oferecem suporte a modelos versão 2.

( ) Apenas Windows Server 2012, Windows 8 e sistemas operacionais superiores oferecem suporte a modelos versão 2.

Comentários:

Um importante aspecto dos modelos versão 2 é que eles dão suporte ao registro automático pelos computadores e usuários do Active Directory Domain Services (AD DS). Ao contrário dos modelos versão 1, você pode modificar todos os aspectos do modelo versão 2. Para atualizar para o modelo versão 2, é possível duplicar um modelo versão 1. Os modelos versão 2 têm suporte no Windows Server 2003 Enterprise Edition, no Windows Server 2008 Enterprise e no Windows Server 2008 R2 e posterior.

Pergunta: Você é o administrador do AD CS na A. Datum Corporation. Vários usuários no seu ambiente do AD DS registraram automaticamente um certificado de usuário. Você deseja diminuir o prazo de validade do certificado de usuário e precisa garantir que os usuários consigam um novo certificado imediatamente sem que haja quebra de validade do certificado existente. Quais das ações a seguir devem ser executadas? (Escolha todas as opções aplicáveis.)

( ) Duplicar o modelo existente e fornecer um novo nome de modelo. Modificar o prazo de validade do novo modelo.

( ) Modificar o prazo de validade do modelo existente.

( ) Modificar as configurações do registro automático do modelo existente.

( ) Revogar todos os certificados de usuário emitidos a partir do modelo existente.

( ) Modificar o novo modelo para que ele substitua o modelo existente. Publicar o novo modelo.

Resposta:

(√) Duplicar o modelo existente e fornecer um novo nome de modelo. Modificar o período de validade do novo modelo.

( ) Modificar o prazo de validade do modelo existente.

( ) Modificar as configurações do registro automático do modelo existente.

(√) Revogar todos os certificados de usuário emitidos a partir do modelo existente.

(√) Modificar o novo modelo para que ele substitua o modelo existente. Publicar o novo modelo.

Comentários:

Nessa situação, você deve duplicar o modelo existente, fornecendo um novo nome do modelo e prazo de validade. Além disso, você deve atualizar o novo modelo para que ele substitua o anterior. Depois de publicar o novo modelo em uma AC corporativa, os usuários que tinham se registrado automaticamente em relação ao modelo anterior vão se registrar automaticamente novamente para o novo modelo. Assim que os novos certificados com prazo de validade correto tiverem substituído os certificados emitidos anteriormente, revogue todos os certificados de usuário do modelo existente para que os usuários não possam utilizá-los.

Se você modificar o prazo de validade do modelo existente, novas inscrições no modelo terão as configurações corretas, mas certificados emitidos anteriormente ainda terão o prazo de validade indesejado. Não é necessário modificar as configurações de registro automático no modelo existente, e isso não alcançaria o efeito desejado.

Demonstração: Modificação e habilitação de um modelo de certificado

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **certification authority**.
2. No console **Autoridade de Certificação**, expanda **AdatumCA**, clique com o botão direito do mouse em **Modelos de Certificado** e clique em **Gerenciar**.
3. Examine a lista de modelos padrão. Examine os modelos e suas propriedades.
4. No painel de detalhes, clique duas vezes em **IPsec**.
5. Na caixa de diálogo **Propriedades IPsec** clique nas guias e observe o que você pode modificar em cada uma. Observe que, na guia **Segurança**, é possível definir as permissões para registro. Clique em **Cancelar** para fechar o modelo.
6. No console **Modelos de Certificado**, no painel de detalhes, clique com o botão direito do mouse no modelo de certificado **Usuário do Exchange** e clique em **Modelo Duplicado**.
7. Na caixa de diálogo **Propriedades do Novo Modelo**, examine as opções na guia **Compatibilidade**.
8. Clique na guia **Geral** e, na caixa de texto **Nome para exibição do modelo** digite **Usuário do Exchange Teste 1**.
9. Clique na guia **Modelos Obsoletos** e clique em **Adicionar**.
10. Clique no modelo **Usuário do Exchange** e clique em **OK**.
11. Clique na guia **Segurança** e em **Usuários Autenticados**.
12. No nó **Permissões para Usuários Autenticados**, marque as caixas de seleção **Permitir** para **Registrar** e **Registrar automaticamente** e clique em **OK**.
13. Feche o **Console de Modelos de Certificado**.
14. No console **Autoridade de Certificação**, clique com o botão direito em **Modelos de Certificado**, aponte para **Novo** e clique em **Modelo de Certificado a Ser Emitido**.
15. Na caixa de diálogo **Ativar Modelos de Certificado**, selecione o certificado **Usuário do Exchange Teste 1** e clique em **OK**.

Lição 2

Gerenciamento de implantação, revogação e recuperação de certificados

Sumário:

Perguntas e respostas

Pergunta: Ao revogar um certificado, onde está a impressão digital do certificado publicado?

( ) CPD (ponto de distribuição de CRL)

( ) AIA (acesso às informações da autoridade)

( ) CRL (lista de certificados revogados)

( ) AD DS

( ) O serviço Respondente Online

Resposta:

( ) CPD (ponto de distribuição de CRL)

( ) AIA (acesso às informações da autoridade)

(√) CRL (lista de certificados revogados)

( ) AD DS

( ) O serviço Respondente Online

Comentários:

Quando você revoga um certificado, a impressão digital do certificado é publicada na CRL (lista de certificados revogados). Um CPD (Ponto de distribuição de CRL) é o local da URL onde a CRL está armazenada. O AIA (acesso às informações de autoridade) é a URL onde está localizado o certificado de AC. O AD DS é um local válido para um CPD, mas certificados revogados não publicam diretamente no AD DS. Um serviço Respondente Online valida o status de um certificado específico usando a cópia local da CRL, mas os certificados revogados não publicam diretamente em um serviço Respondente Online.

Pergunta: Quais das ações a seguir você deve realizar para configurar o arquivamento de chave em uma AC do AD CS? (Escolha todas as opções aplicáveis.)

( ) Configurar o modelo de certificado KRA.

( ) Registrar um usuário designado para um certificado KRA.

( ) Publicar a chave pública KRA usando a Política de Grupo.

( ) Configurar um agente de recuperação na AC.

( ) Configurar os modelos de certificado desejados para arquivamento de chave.

Resposta:

(√) Configurar o modelo de certificado KRA.

(√) Registrar um usuário designado para um certificado KRA.

( ) Publicar a chave pública KRA usando a Política de Grupo.

(√) Configurar um agente de recuperação na AC.

(√) Configurar os modelos de certificado desejados para arquivamento de chave.

Comentários:

Para configurar o arquivamento de chave, é necessário:

1. Configurar o certificado KRA para que somente os usuários confiáveis possam se registrar para um certificado.
2. Registrar um usuário confiável para o certificado KRA.
3. Configurar um agente de recuperação na AC usando o certificado KRA.
4. Configurar os modelos de certificado desejados para arquivamento de chave.

Não é necessário publicar a chave pública KRA usando a Política de Grupo.

Demonstração: Configuração da AC para arquivamento de chave

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Autoridade de Certificação**. No console **Autoridade de Certificação**, expanda o nó **AdatumCA**, clique com o botão direito na pasta **Modelos de Certificado** e clique em **Gerenciar**.
2. No painel de detalhes, clique com o botão direito do mouse no certificado **Agente de Recuperação de Chave** e clique em **Propriedades**.
3. Na caixa de diálogo **Propriedades do Agente de Recuperação de Chave** clique na guia **Requisitos de Emissão** desmarque a caixa de seleção **Aprovação do gerenciador de certificados de autoridade de certificação** e clique na guia **Segurança**. Observe que os grupos **Admins. do Domínio** e **Administradores de Empresa** são os únicos que têm a permissão Registrar. Em seguida, clique em **OK**.
4. Feche o **Console de Modelos de Certificado**.
5. No console **Autoridade de Certificação**, clique com o botão direito em **Modelos de Certificado**, aponte para **Novo** e clique em **Modelo de Certificado a Ser Emitido**.
6. Na caixa de diálogo **Ativar Modelos de Certificado** clique no modelo **Agente de Recuperação de Chave** e clique em **OK**.
7. Clique em **Iniciar** e no ícone **Windows PowerShell**.
8. No prompt de comando do Windows PowerShell, digite **mmc.exe** e pressione Enter.
9. No console **Console1-[Raiz do Console]** clique em **Arquivo** e clique em **Adicionar/Remover Snap-in**.
10. Na caixa de diálogo **Adicionar ou Remover Snap-ins** clique em **Certificados** e em **Adicionar**.
11. Na caixa de diálogo **Snap-in de certificados** selecione **Minha conta de usuário**, clique em **Concluir** e em **OK**.
12. Expanda o nó **Certificados – Usuário Atual**, clique com o botão direito do mouse em **Pessoal**, aponte para **Todas as Tarefas** e clique em **Solicitar Novo Certificado**.
13. No **Assistente de Registro de Certificado**, na página **Antes de Começar**, clique em **Avançar**.
14. Na página **Selecionar política de registro de certificado**, clique em **Avançar**.
15. Na página **Solicitar Certificados**, marque a caixa de seleção **Agente de Recuperação de Chave**, clique em **Registrar** e em **Concluir**.
16. Atualize o console e, em seguida, exiba o KRA no repositório pessoal; isto é, percorra as propriedades de certificado e verifique se o modelo de certificado com a finalidade específica **Agente de Recuperação de Chave** está presente.
17. Feche o **Console1** sem salvar as alterações.
18. Retorne ao console **Autoridade de Certificação** clique com o botão direito do mouse em **AdatumCA** e clique em **Propriedades**.
19. Na caixa de diálogo **Propriedades de AdatumCA** clique na guia **Agentes de Recuperação** e selecione **Arquivar a chave**.
20. Em Certificados do agente de recuperação de chave, clique em **Adicionar**.
21. Na caixa de diálogo **Seleção de Agente de Recuperação de Chave** clique em **Mais Opções** e clique no certificado com a finalidade KRA (provavelmente é o último na lista emitido para o **Administrador**) e clique duas vezes em **OK**.
22. Quando for solicitado a reiniciar a AC, clique em **Sim**.

Lição 3

Uso de certificados em um ambiente de negócios

Sumário:

Perguntas e respostas

Pergunta: Quais destas opções são afirmações verdadeiras sobre o uso de certificados em um ambiente empresarial? (Escolha todas as opções aplicáveis.)

( ) Os certificados podem ser usados para criptografar o tráfego HTTP entre um servidor Web e o navegador.

( ) Os usuários podem usar certificados para assinar digitalmente documentos.

( ) Os documentos assinados digitalmente são inválidos se alguém modifica o conteúdo.

( ) Para enviar email criptografado para um destinatário externo que não faz parte da sua PKI interna, você deve usar um certificado de criptografia emitido por uma AC pública.

( ) Arquivos criptografados com EFS só podem ser lidos pela pessoa que os criptografou primeiro.

Resposta:

(√) Os certificados podem ser usados para criptografar o tráfego HTTP entre um servidor Web e o navegador.

(√) Os usuários podem usar certificados para assinar digitalmente documentos.

(√) Os documentos assinados digitalmente são inválidos se alguém modifica o conteúdo.

( ) Para enviar email criptografado para um destinatário externo que não faz parte da sua PKI interna, você deve usar um certificado de criptografia que um público da autoridade de certificação emitiu.

( ) Arquivos criptografados com EFS só podem ser lidos pela pessoa que os criptografou primeiro.

Comentários:

Os certificados podem ser usados para criptografar o tráfego HTTP, assinar digitalmente e criptografar documentos e emails, e para autenticação de cliente/servidor. Os documentos assinados digitalmente são inválidos se alguém modifica o conteúdo. Para enviar email criptografado para um destinatário externo, você pode usar um certificado interno ou emitido publicamente, caso tenha acesso à chave pública do destinatário. Os arquivos criptografados usando o EFS podem ser lidos pela pessoa que os criptografou e por usuários explicitamente designados para o compartilhamento do EFS. Se a chave privada de criptografia individual for perdida ou excluída, um agente de recuperação de dados pode acessar o arquivo ou um agente de recuperação de chave pode recuperar a chave privada, se você tiver configurado o arquivamento de chave no modelo de certificado EFS e na AC emissora.

Pergunta: Você é o administrador de AD CS da A. Datum. Você deseja habilitar os usuários do AD DS para realizar assinatura digital e criptografia usando certificados da sua PKI interna. Quais das etapas a seguir são necessárias?

( ) Habilitar um agente de recuperação de chave.

( ) Habilitar um agente de recuperação de dados.

( ) Publicar o modelo de certificado do Usuário e configurar os grupos de usuários desejados para registro automático.

( ) Habilitar EFS nos computadores do domínio AD DS usando a Política de Grupo.

( ) Atualizar todos os computadores do domínio AD DS para o Windows Server 2016 ou Windows 10.

Resposta:

( ) Habilitar um agente de recuperação de chave.

( ) Habilitar um agente de recuperação de dados.

(√) Publicar o modelo de certificado do Usuário e configurar os grupos de usuários desejados para registro automático.

( ) Habilitar EFS nos computadores do domínio AD DS usando a Política de Grupo.

( ) Atualizar todos os computadores do domínio AD DS para o Windows Server 2016 ou Windows 10.

Comentários:

Para habilitar a assinatura digital e a criptografia, só será necessário publicar o modelo de certificado do usuário e configurá-lo para registro automático. Embora o uso de um agente de recuperação de chave e um agente de recuperação de dados sejam práticas recomendadas, elas não são necessárias para habilitar assinaturas digitais e criptografia. Você não precisa habilitar o EFS em computadores de domínio AD DS, nem precisa atualizar todos os computadores do domínio AD DS para o Windows Server 2016 ou Windows 10.

Demonstração: Como assinar digitalmente um documento

Etapas da demonstração

1. Em **LON-CL1**, abra a interface de linha de comando do Windows PowerShell.
2. No prompt de comando do **Windows PowerShell** digite **mmc.exe** e pressione Enter.
3. Na janela **Console1 – [Raiz do Console]**, clique no menu **Arquivo** e selecione **Adicionar/Remover Snap-in**.
4. Selecione **Certificados**, clique em **Adicionar**, selecione **Minha conta de usuário**, clique em **Concluir** e clique em **OK**.
5. Expanda **Certificados - Usuário Atual**, clique com o botão direito do mouse em **Pessoal**, selecione **Todas as Tarefas** e clique em **Solicitar Novo Certificado**.
6. No **Assistente de Registro de Certificado**, clique duas vezes em **Avançar**.
7. Na página **Registro de Certificado** na lista de modelos disponíveis, selecione **Usuário**, clique em **Registrar** e clique em **Concluir**.
8. Feche a janela **Console1 – [Raiz do Console]** sem salvar as alterações.
9. Abra o Word 2016.

 **Observação:** Se o **Assistente para Ativação do Microsoft Office** aparecer, clique em **Fechar**. Clique em **Pergunte–me mais tarde** e clique em **Aceitar**.

10. Em um documento em branco, digite algum texto e, em seguida, salve o arquivo na área de trabalho.
11. Na barra de ferramentas, clique em **Inserir** e, no painel **Texto**, na lista suspensa **Linha de Assinatura**, clique em **Linha de Assinatura do Microsoft Office**.
12. Na janela **Configuração de Assinatura**, digite seu nome na caixa de texto **Signatário sugerido**, digite **Administrador** na caixa de texto **Cargo do signatário sugerido**, digite **Administrator@adatum.com** na caixa de texto **Endereço de email do signatário sugerido** e clique em **OK**.

13. Clique com o botão direito do mouse na linha de assinatura no documento e, em seguida, clique em **Assinar**.
14. Na janela **Assinar**, clique em **Alterar**.
15. Na janela **Segurança do Windows** em **Selecione um certificado**, selecione o certificado de **Administrador** com a data de hoje e clique em **OK**.
16. Na caixa de texto à direita do X, digite seu nome e clique em **Assinar** e em **OK**.

 **Observação:** explique aos alunos que é possível selecionar uma imagem em vez de digitar seu nome. Essa imagem pode ser sua assinatura manual digitalizada.

17. Certifique-se de que você não pode editar mais o documento.
18. Feche o Word 2016 e salve as alterações quando solicitado.
19. Continue conectado para a próxima demonstração.

Demonstração: Criptografia de um arquivo com EFS

Etapas da demonstração

1. Em **LON-CL1**, clique com o botão direito do mouse no documento do Microsoft Word que você salvou na área de trabalho na demonstração anterior e, em seguida, clique em **Propriedades**.
2. Na guia **Geral** da caixa de diálogo **Propriedades**, clique em **Avançado**, clique em **Criptografar o conteúdo para proteger os dados** e clique duas vezes em **OK**.
3. Na janela de prompt, selecione **Criptografar somente o arquivo** e clique em **OK**.
4. Mova o documento que você criptografou para a pasta **C:\Users\Public\Public Documents**.
5. Saia de **LON-CL1**.
6. Entre com o **Adatum\Aidan** com a senha **Pa55w.rd**.
7. Abra o Explorador de Arquivos e acesse **C:\Users\Public\Public Documents**.
8. Tente abrir o documento criptografado.
9. Verifique se não é possível abrir o documento.
10. Saia de **LON-CL1**.

Lição 4

Implementação e gerenciamento de cartões inteligentes

Sumário:

Perguntas e respostas

Pergunta: Qual destas afirmações é verdadeira sobre cartões inteligentes?

( ) Os cartões inteligentes são uma opção para a autenticação multifator.

( ) Você não pode usar cartões inteligentes para fazer logon interativo.

( ) Os cartões inteligentes contêm um certificado e uma chave privada que você pode acessar apenas usando um PIN.

( ) Os cartões inteligentes fornecem segurança aprimorada, além de uma senha.

( ) É possível usar os cartões inteligentes somente para assinatura digital e criptografia.

Resposta:

(√) Os cartões inteligentes são uma opção para a autenticação multifator.

( ) Você não pode usar cartões inteligentes para fazer logon interativo.

(√) Os cartões inteligentes contêm um certificado e uma chave privada que você pode acessar apenas usando um PIN.

(√) Os cartões inteligentes fornecem segurança aprimorada, além de uma senha.

( ) É possível usar os cartões inteligentes somente para assinatura digital e criptografia.

Comentários:

Os cartões inteligentes são uma opção para a autenticação multifator: os usuários devem ter a posse física do cartão inteligente e também devem saber seu PIN. Inserindo o PIN, os certificados e as chaves privadas armazenadas no cartão inteligente se tornam disponíveis para autenticação, assinatura digital e criptografia. O uso de cartões inteligentes para fazer logon interativo fornece segurança aprimorada, além da senha.

Pergunta: Ao implementar uma infraestrutura de cartão inteligente, qual dos seguintes processos deve fazer parte da sua estrutura de gerenciamento de certificados?

( ) Emissão

( ) Revogação

( ) Renovação

( ) Bloqueio e desbloqueio

( ) Suspensão

Resposta:

(√) Emissão

(√) Revogação

(√) Renovação

(√) Bloqueio e desbloqueio

(√) Suspensão

Comentários:

Todas as opções acima são processos corretos que você deve incluir no seu plan o de gerenciamento de certificados. É possível executar alguns dos processos com ferramentas internas. No entanto, devido à complexidade envolvida, é recomendável que você implemente uma solução dedicada para o gerenciamento de certificados e cartões inteligentes, com o a MIM.

Revisão do módulo e informações complementares

Práticas recomendadas

- Ao substituir os modelos de certificado antigos, use os modelos substitutos.
- Sempre arquive certificados que servem para criptografia.
- Use o registro automático para implantação em mass a de certificados.
- Se você estiver usando cartões inteligentes, certifique-se de que os usuários alterem seus PINs regularmente.
- Se você estiver usando cartões inteligentes, implemente uma solução de gerenciamento de cartão inteligente.

Perguntas de revisão

Pergunta: Liste os requisitos para usar o registro automático em certificados.

> **Resposta:** Para usar o registro automático em certificados, você deve ter uma AC corporativa e deve configurar as opções da Política de Grupo. Além disso, você deve habilitar o registro automático nos modelos de certificado desejados e deve configurar os Objetos de Política de Grupo.

Pergunta: Como os cartões virtuais funcionam?

> **Resposta:** Os Cartões inteligentes virtuais emulam a funcionalidade dos cartões inteligentes tradicionais, mas em vez de exigirem a compra de hardware adicional, eles utilizam uma tecnologia que os usuários já possuem.

Problemas e cenários reais

A Contoso, Ltd. deseja implantar uma PKI para dar suporte e proteger vários serviços. Foi decidido usar o AD CS do Windows Server 2016 como uma plataforma para PKI. A Contoso usará certificados principalmente para EFS, assinatura digital e servidores Web. Como os documentos criptografados são importantes, é essencial ter uma estratégia de recuperação de desastres no caso de perda da chave. Além disso, os clientes que terão acesso às partes seguras do site da empresa não devem receber nenhum aviso nos seus navegadores. Considere as seguintes perguntas:

- Que tipo de implantação a Contoso deve escolher?
- Que tipo de certificados a Contoso deve usar para EFS e assinatura digital?
- Que tipo de certificados a Contoso deve usar para um site?
- Como a Contoso assegurará que dados com criptografia EFS não serão perdidos se um usuário perder um certificado?

Ferramentas

- O console **Autoridade de Certificação**
- O Console de **Modelos de Certificado**
- O console **Certificados**
- **Certutil.exe**

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
O modelo de certificado não é visível durante o registro.	Verifique se você configurou corretamente as permissões Leitura e Registro no modelo.
O registro automático não funciona.	Verifique se você configurou as opções de registro automático na Política de Grupo e se atribuiu as permissões de Ler, Registar e Registrar automaticamente ao grupo apropriado de computadores ou de usuários.
O usuário que criptografou um arquivo não pode descriptografá-lo.	Verifique se o usuário possui a chave privada do par de chaves. Além disso, verifique se o certificado não expirou. Se a chave privada foi perdida ou o certificado expirou, use KRA ou DRA.

Perguntas e respostas da revisão do laboratório

Laboratório: Implantação e uso de certificados

Perguntas e respostas

Pergunta: O que você deve fazer para recuperar chaves privadas?

Resposta: Para recuperar chaves privadas, você deve configurar a AC para arquivar chaves privadas de modelos específicos e emitir o certificado KRA.

Pergunta: Qual é o benefício de usar um Agente de registro restrito?

Resposta: O agente de registro permite que você limite as permissões de usuários designados com o agentes de registro para que se registrem em certificados de cartão inteligente em nome de outros usuários.