Módulo 8

Implantação e gerenciamento do AD CS

Sumário:

Lição 1

Implantação de ACs

Sumário:

Perguntas e respostas

Pergunta: Quais das opções a seguir descrevem as vantagens de implantar uma AC corporativa em vez de uma AC autônoma?

( ) Fornece várias maneiras pelas quais usuários e dispositivos podem receber certificados.

( ) Não exige o AD DS.

( ) As solicitações de certificado podem ser emitidas ou negadas automaticamente com base na política.

( ) Pode ficar offline para evitar comprometimento.

( ) Pode usar modelos para emitir certificados com base em dados no AD DS.

Resposta:

(√) Fornece várias maneiras pelas quais usuários e dispositivos podem receber certificados.

( ) Não exige o AD DS.

(√) As solicitações de certificado podem ser emitidas ou negadas automaticamente com base na política.

( ) Pode ficar offline para evitar comprometimento.

(√) Pode usar modelos para emitir certificados com base em dados no AD DS.

Comentários:

As vantagens de uma AC corporativa incluem as várias maneiras para se registrar para certificados, incluindo o registro automático usando modelos de certificado. As ACs corporativas também permitem a aprovação ou negação automática de solicitações com base nas políticas de emissão. As ACs corporativas, no entanto, exigem o AD DS (Active Directory Domain Services) e devem ficar online para facilitar o registro de certificado.

Pergunta: Quais das opções a seguir são motivos pelos quais convém implantar várias ACs subordinadas?

( ) Você deseja segmentar a emissão de certificados com base em políticas de uso exclusivas.

( ) Você tem vários domínios no ambiente do AD DS, e cada domínio exige sua própria AC subordinada.

( ) Você deseja segmentar a emissão de certificados com base na divisão organizacional ou na região geográfica.

( ) Você deseja várias ACs subordinadas para alta disponibilidade e balanceamento de carga de solicitações.

( ) Você precisa publicar vários modelos de certificado, e cada modelo exige sua própria AC subordinada.

Resposta:

(√) Você deseja segmentar a emissão de certificados com base em políticas de uso exclusivas.

( ) Você tem vários domínios no ambiente do AD DS, e cada domínio exige sua própria AC subordinada.

(√) Você deseja segmentar a emissão de certificados com base na divisão de organizacional ou na região geográfica.

(√) Você deseja várias ACs subordinadas para alta disponibilidade e balanceamento de carga de solicitações.

( ) Você precisa publicar vários modelos de certificado, e cada modelo exige sua própria AC subordinada.

Comentários:

Você pode implantar várias ACs para políticas de uso exclusivas, divisões organizacionais ou regiões geográficas. Além disso, você pode implantar várias ACs para garantir a alta disponibilidade de balanceamento de carga de solicitações.

Não são necessárias várias ACs subordinadas em um ambiente AD DS de vários domínios, embora você possa usar essa abordagem se seus domínios AD DS já se alinham às regiões geográficas ou divisões organizacionais. Não são necessárias várias ACs subordinadas se você precisar publicar modelos de certificado diferentes porque uma AC pode ser configurada para emitir certificados de mais de um modelo.

Demonstração: Implantação de uma AC raiz corporativa

Etapas da demonstração

1. Em **LON-SVR1**, clique em **Iniciar** e em **Gerenciador de Servidores**.
2. No **Gerenciador do Servidor**, clique em **Adicionar funções e recursos**.
3. Na página **Antes de começar**, clique em **Próximo**.
4. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
5. Na página **Selecionar servidor de destino**, clique em **Próximo**.
6. Na página **Selecionar funções de servidor**, selecione **Serviços de Certificados do Active Directory**.
7. No **Assistente de Adição de Funções e Recursos**, clique em **Adicionar Recursos** e, depois, em **Próximo**.
8. Na página **Selecionar recursos**, clique em **Próximo**.
9. Na página **Serviços de Certificados do Active Directory**, clique em **Próximo**.
10. Na página **Selecionar serviços de função**, verifique se a **Autoridade de Certificação** está selecionada e clique em **Próximo**.
11. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
12. Na página **Progresso da instalação**, após a instalação ser concluída, clique no texto **Configurar Serviços de Certificados do Active Directory** no servidor de destino.
13. No **Assistente de** configuração do AD CS, na **página** Credenciais, clique em **Próximo**.
14. Na página **Serviços de função**, selecione **Autoridade de certificação** e clique em **Próximo**.
15. Na página **Tipo de instalação**, selecione **AC corporativa** e clique em **Próximo**.
16. Na **página** Tipo de Autoridade de Certificação, clique na opção **AC raiz** e clique em **Próximo**.
17. Na página **Chave Privada**, verifique se a opção **Criar uma nova chave privada** está selecionada e clique em **Avançar**.

18. Na página **Criptografia para AC**, mantenha as seleções padrão para **Selecione um provedor criptográfico** e **Selecione o algoritmo de hash para certificados de autenticação emitidos por esta autoridade de certificação**, mas configure o **Comprimento da chave** para **4096** e clique em **Próximo**.
19. Na página **Nome da Autoridade de Certificação**, na caixa de texto **Nome comum da autoridade de certificação**, digite **AdatumRootCA** e clique em **Próximo**.
20. Na página **Período de validade**, clique em **Próximo**.
21. Na página **Banco de dados de AC**, clique em **Próximo**.
22. Na página **Confirmação**, clique em **Configurar**.
23. Na página **Resultados**, clique em **Fechar**.
24. Na página **Progresso da instalação**, clique em **Fechar**.

Lição 2

Administração de ACs

Sumário:

Perguntas e respostas

Pergunta: Qual das opções a seguir é verdadeira sobre a administração baseada em funções da implantação do AD CS?

( ) O AD CS cria automaticamente três funções e grupos internos para Administrador de AC, Gerenciador de certificados e Usuário registrado.

( ) Você pode conceder aos grupos de função do AD CS uma ou mais das seguintes permissões de AC: Gerenciar AC, Emitir e Gerenciar certificados, Ler e Solicitar certificados.

( ) Você pode limitar a permissão de AC para Emitir e gerenciar certificados a um determinado modelo ou conjunto de modelos.

( ) Você pode criar grupos de função do AD CS personalizados com base em necessidades específicas de sua organização.

( ) A Entidade de segurança de usuários autenticados pode se registrar para qualquer certificado que seja publicado em uma AC.

Resposta:

( ) O AD CS cria automaticamente três funções e grupos internos para Administrador de AC, Gerenciador de certificados e Usuário registrado.

(√) Você pode conceder aos grupos de função do AD CS uma ou mais das seguintes permissões de AC: Gerenciar a AC. Emitir e Gerenciar certificados, Ler e Solicitar certificados.

(√) Você pode limitar a permissão de AC Emitir e gerenciar certificados a um determinado modelo ou conjunto de modelos.

(√) Você pode criar grupos de função do AD CS personalizados com base em necessidades específicas de sua organização.

( ) A entidade de segurança Usuários autenticados pode se registrar para qualquer certificado que seja publicado em uma AC.

Comentários:

A Administração baseada em funções no AD CS é um conceito, não um recurso instalado automaticamente. Portanto, você deve criar qualquer função de grupos manualmente. Após criar um grupo de função, você pode atribuir a ele uma ou mais das seguintes permissões de AC: Gerenciar AC, Emitir e gerenciar certificados, Ler e Solicitar certificados. Você pode personalizar as funções de acordo com as necessidades da sua organização, incluindo a restrição da permissão para Emitir e gerenciar certificados para determinado modelo ou conjunto de modelos.
A **Entidade de segurança** de usuários autenticados pode solicitar qualquer certificado, mas o modelo de certificado controla a capacidade de registrar, não a AC.

Pergunta: Qual das opções a seguir é verdadeira sobre as extensões de AIA e CPD de uma AC?

( ) Cada extensão exige, no mínimo, duas URLs válidas e acessíveis para que a validação do certificado funcione corretamente.

( ) Você pode publicar certificados de AC offline e autônoma e CRLs em um ambiente do AD DS manualmente.

( ) A ordem na qual você especifica URLs de AIA e CPD não é tão importante quanto o mecanismo de encadeamento de certificados que ordena automaticamente os locais com base na conexão mais rápida.

( ) Para facilitar a validação de certificados para clientes externos, você deve publicar URLs de AIA e CPD externas usando HTTP por meio de um Proxy de Aplicativo Web do Windows Server 2016.

( ) Se você estiver usando uma AC corporativa, a validação de certificados internos funcionará sem nenhuma configuração adicional.

Resposta:

( ) Cada extensão exige, no mínimo, duas URLs válidas e acessíveis para que a validação do certificado funcione corretamente.

(√) Você pode publicar manualmente certificados de AC offline e autônoma e CRLs em um ambiente do AD DS.

( ) A ordem na qual você especifica URLs de CPD e AIA não é tão importante quanto o mecanismode encadeamento de certificados que classifica automaticamente locais com base na conexão mais rápida.

(√) Para facilitar a validação de certificado para clientes externo, você deve publicar URLs de AIA e CPD externas usando HTTP por meio de um Proxy de Aplicativo Web do Windows Server 2016.

(√) Se você estiver usando uma AC corporativa, a validação de certificados internos funcionará sem nenhuma configuração adicional.

Comentários:

Para que o certificado de validação funcione, as extensões de CPD e AIA devem conter um mínimo de uma URL válida e acessível. Para ACs offline e autônomas, você pode publicar o certificado e a CRL da AC no AD DS manualmente. A ordem das URLs de AIA e CPD é importante, pois o mecanismo de encadeamento de certificado mecanismo os procura sequencialmente. Você deve colocar as URLs com maior probabilidade de estarem disponíveis na parte superior da ordem de URL. Para facilitar a validação de certificados para clientes externos, você pode publicar URLs de AIA e CPD externas usando HTTP por meio de um Proxy de Aplicativo Web do Windows Server 2016 ou outra solução de proxy reverso de terceiros. Se você estiver usando uma AC corporativa, a validação do certificado trabalhará automaticamente para os clientes internos, mas pode exigir configuração adicional em outros cenários.

Recursos

Gerenciamento de ACs

 **Leitura adicional:** Para obter mais informações, consulte:

- Cmdlets de implantação do AD CS no Windows PowerShell http://aka.ms/Giih2g
- Cmdlets de implantação do AD CS no Windows PowerShell http://aka.ms/Dekm5i

Demonstração: configuração de propriedades de AC

Etapas da demonstração

1. Em **LON-SVR1**, abra o **Gerenciador do Servidor**, clique em **Ferramentas** e depois em **certification authority**.
2. No Console de **autoridade de certificação**, clique com o botão direito do mouse em **AdatumRootCA** e selecione **Propriedades**.
3. Na guia **Geral**, clique em **Exibir certificado**. Quando a janela do certificado abrir, revise os dados nas guias **Detalhes**, **gerais** e **Caminho de certificação** e clique em **OK**.
4. Na guia **Módulo de política**, clique em **Propriedades**. Analise as configurações disponíveis para o **Módulo de** política padrão e clique em **OK**.

5. Na guia **Módulo de saída**, clique em **Propriedades**. Mostre as **Configurações de publicação** disponíveis no Módulo de saída padrão e clique em **OK**.
6. Na guia **Extensões**, analise as opções disponíveis para a extensão de CPD e AIA **na lista suspensa** Selecionar extensão.
7. Na guia **Segurança**, analise as opções disponíveis na lista de controle de acesso (ACL) e as permissões padrão.
8. Na guia **Gerenciadores de certificado**, analise as opções e explique como restringir entidades de segurança para modelos de certificado específicos e clique em **Cancelar**.
9. Feche o console Certsrv.

Lição 3

Solução de problemas e manutenção de ACs

Sumário:

Perguntas e respostas

Pergunta: Qual dos seguintes problemas pode impedir que o registro automático funcione corretamente no AD CS?

( ) O computador que você pretende registrar automaticamente para um certificado está em uma unidade organizacional (UO) do AD DS, onde a herança de políticas está bloqueada.

( ) O usuário que você pretende registrar automaticamente para um certificado está em uma UO do AD DS, onde a configuração de Política de Grupo necessária não está vinculada ou não é herdada.

( ) A AC é autônoma.

( ) O modelo de certificado não é publicado em uma AC.

( ) A URL de AIA está configurada incorretamente na guia de extensões da AC.

Resposta:

(√) O computador que você pretende registrar automaticamente para um certificado está em uma unidade organizacional (UO) do AD DS, onde a herança de políticas está bloqueada.

(√) O usuário que você pretende registrar automaticamente para um certificado está em uma OU do AD DS, onde a configuração de Política de Grupo necessária não está vinculada ou não é herdada.

(√) A AC é autônoma.

(√) O modelo de certificado não é publicado em uma AC.

( ) A URL de AIA está configurada incorretamente na guia de extensões da AC.

Comentários:

A herança do Objeto de Política de Grupo (GPO) é um problema comum que pode impedir o registro automático. Usuários e computadores devem estar em uma organização de AD DS onde você vinculou as configurações de GPO necessárias e a herança de política não bloqueada. Além disso, as ACs devem ser corporativas para funcionarem corretamente, pois os clientes usam o AD DS para determinar ACs e modelos disponíveis. Você deve publicar modelos em uma AC corporativa e o usuário ou computador deve ter as permissões de registro automático configuradas no modelo. Uma URL de AIA ou CPD inválida na AC não impedirá o registro automático, mas pode impedir que o certificado seja validado corretamente ao ser usado por um aplicativo cliente ou serviço.

Pergunta: Qual das opções a seguir é verdadeira sobre a ferramenta PKIVIew?

( ) O PKIView mostra todas as suas ACs corporativas e a integridade atual delas.

( ) Você pode usar o PKIView para adicionar ACs autônomas manualmente.

( ) Você pode usar o PKIView para configurar o registro automático para usuários e computadores.

( ) O PKIView avalia o estado de CPD ou AIA para cada local definido em cada AC.

( ) O PKIView pode avaliar o status do serviço da função Respondente Online do AD CS.

Resposta:

(√) O PKIView mostra todas as suas ACs corporativas e a integridade atual delas.

( ) Você pode usar o PKIView para adicionar ACs autônomas manualmente.

( ) Você pode usar o PKIView para configurar o registro automático para usuários e computadores.

(√) O PKIView avalia o estado de CPD ou AIA para cada local definido em cada AC.

(√) O PKIView pode avaliar o status do serviço da função Respondente Online do AD CS.

Comentários:

Você pode usar o PKIView para ver todas as suas ACs corporativas e a integridade atual delas, mas ele não mostra o status de uma AC autônoma. Você configura o registro automático para usuários e computadores por meio da Política de Grupo, não com a ferramenta PKIView.
O PKIVIew permite avaliar o estado de CPD e AIA para cada local definido em cada AC, além do status do serviço da função Respondente Online do AD CS, caso o tenha implantado.

Revisão do módulo e informações complementares

Práticas recomendadas

- Ao implantar uma infraestrutura de AC, implante uma AC raiz autônoma (não adicionada ao domínio) e uma AC corporativa subordinada (AC emissora). Depois que a AC corporativa subordinada receber um certificado da AC raiz, coloque a AC raiz offline.
- Analise o tempo de validação das listas de certificados revogados (CRLs) da AC raiz.
- Forneça mais de um local para AIA e CRL.

Perguntas de revisão

Pergunta: Por quais motivos uma organização utilizaria uma PKI?

> **Resposta:** Alguns dos motivos para usar uma PKI incluem melhorar a segurança, aumentar o controle de identidade e fazer assinatura digital de código.

Pergunta: Por que você deve implantar módulos personalizados de política e saída?

> **Resposta:** Se você tiver um aplicativo adicional para o gerenciamento de certificado, como o Gerenciamento de certificado MIM, você terá que instalar módulos de política e de saída personalizados para integrar seu aplicativo com a AC.

Ferramentas

- **Console de** autoridade de certificação
- Ferramenta de linha de comando CertUtil
- Windows PowerShell
- PKIView.msc
- Gerenciador do Servidor

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
O local do certificado de AC especificado na extensão de AIA não está configurado para incluir o sufixo do nome de certificado. Os clientes podem não conseguir localizar a versão correta do certificado da AC emissora para compilar uma cadeia de certificados e a validação do certificado pode falhar.	Use o Console de **autoridade de certificação** para configurar a extensão do AIA e incluir o sufixo do nome do certificado em cada local.
AC não está configurada para incluir os locais de CPD nas extensões de certificados emitidos. Os clientes podem não conseguir localizar uma CRL para verificar o status de revogação de um certificado, e a validação de certificado pode falhar.	Use o Console da **autoridade de certificação** para configurar a extensão do CPD e para especificar o local de rede da CRL.

Perguntas e respostas da revisão do laboratório

Laboratório: Implantação e configuração de uma hierarquia de AC de duas camadas

Perguntas e respostas

Pergunta: Por que não é recomendado instalar somente uma AC raiz corporativa?

Resposta: Por motivos de segurança, AC raiz deve ficar offline e não deve ter qualquer acesso à rede. Como a AC raiz corporativa não pode estar offline, você não pode fornecer máxima proteção para a chave e a identidade dela.

Pergunta: Por quais motivos uma organização usaria uma AC raiz corporativa?

Resposta: Se uma organização desejar usar só uma AC e modelos de certificado e registro automático, então uma AC raiz corporativa será a única escolha.