Módulo 7

Proteção do Active Directory Domain Services

Sumário:

Lição 1: Proteção dos controladores de domínio 2

Lição 2: Implementação de segurança da conta 6

Lição 3: Implementação da autenticação de auditoria 10

Lição 4: Configuração de contas de serviço gerenciado 13

Revisão do módulo e informações complementares 15

Perguntas e respostas da revisão do laboratório 17

Lição 1

Proteção dos controladores de domínio

Sumário:

Perguntas e respostas 3
Demonstração: Configuração de uma política de replicação de senha 3

Perguntas e respostas

Pergunta: Como fornecer maior segurança para unidades de disco rígido nos controladores de domínio?

> **Resposta:** Para fornecer um nível a mais de segurança, use a criptografia de unidade de disco BitLocker para criptografar discos rígidos do controlador de domínio.

Demonstração: Configuração de uma política de replicação de senha

Etapas da demonstração

Preparar uma instalação delegada de um RODC

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Serviços e Sites do Active Directory**.
2. Em **Serviços e Sites do Active Directory**, no painel de navegação, clique em **Sites**. No menu **Ação**, clique em **Novo Site**.
3. Na caixa de diálogo **Novo Objeto – Site**, no campo **Nome**, digite **Munique**, selecione o objeto de link de site **DEFAULTIPSITELINK** e clique em **OK**.
4. Na caixa de mensagem **Active Directory Domain Services**, clique em **OK**.
5. Alterne para **Gerenciador do Servidor**, clique em **Ferramentas** e em **Central Administrativa do Active Directory**.
6. Em **Central Administrativa do Active Directory**, no painel de navegação, clique em **Adatum (local)** e, no painel de detalhes, clique duas vezes na unidade organizacional (UO) **Domain Controllers**.
7. No painel **Tarefas**, na seção **Domain Controllers**, clique em **Pré-criar uma conta do controlador de domínio Somente leitura**.
8. No **Assistente para Instalação do Active Directory Domain Services**, na página **Assistente de Instalação dos Serviços de Domínio Active Directory**, clique em **Avançar**.
9. Na página **Credenciais de Rede**, clique em **Avançar**.
10. Na página **Especifique o Nome do Computador**, digite o nome do computador como **MUC-RODC1** e clique em **Avançar**.
11. Na página **Selecione um Site**, clique em **Munique** e em **Avançar**.
12. Na página **Opções Adicionais de Controlador de Domínio**, aceite a configuração padrão, marque as caixas de seleção **Servidor DNS** e **Catálogo global** e clique em **Avançar**.
13. Na página **Instalação e Administração de Delegação de RODC,** clique em **Definir**.
14. Na caixa de diálogo **Selecionar Usuário ou Grupo**, no campo **Digite o nome do objeto a ser selecionado**, digite **Bill**, e clique em **Verificar Nomes**.
15. Verifique se Bill Norman está resolvido e clique em **OK**.
16. Na página **Instalação e Administração de Delegação de RODC**, clique em **Avançar**.
17. Na página **Resumo**, revise sua seleção e clique em **Avançar**.
18. Na página **Concluindo o Assistente para Instalação do Active Directory Domain Services**, clique em **Concluir**.

Exibir uma política de replicação de senha de RODC

1. No **Central Administrativa do Active Directory**, na UO **Controladores de Domínio**, selecione **MUC-RODC1**.
2. No painel **Tarefas**, na seção **MUC-RODC1**, clique em **Propriedades**.
3. Na caixa de diálogo **Propriedades** do **MUC-RODC1 (Desabilitado)**, role para baixo até **Extensões**, e clique na guia **Política de Replicação de Senha**.
4. Examine os grupos, usuários e computadores padrão na Política de Replicação de Senha.
5. Deixe a caixa de diálogo aberta.

Configurar uma política de replicação de senha específica de RODC

1. Alterne para **Gerenciador do Servidor**, clique em **Ferramentas** e em **Usuários e Computadores do Active Directory**.
2. No painel de navegação, expanda **Adatum.com** e clique em **Usuários**.
3. No menu **Ação**, clique em **Novo** e em Grupo.
4. Na caixa de diálogo **Novo Objeto – Grupo**, digite o nome do grupo como **Grupo de Replicação de Senha RODC Permitido de Munique** e clique em **OK**.
5. Clique duas vezes em **Grupo de Replicação de Senha RODC Permitido de Munique**, clique na guia **Membros** e clique em **Adicionar**.
6. Na caixa de diálogo **Selecionar Usuários, Contatos, Computadores, Contas de Serviço ou Grupos**, na caixa de texto **Digite os nomes de objeto a serem selecionados**, digite **Ana** e clique em **Verificar Nomes**.
7. Na caixa de diálogo **Diversos Nomes Encontrados**, selecione **Ana Cantrell** e clique em **OK**.
8. Na caixa de diálogo **Selecionar Usuários, Contatos, Computadores, Contas de Serviço ou Grupos**, clique em **OK** e, na caixa de diálogo **Propriedades de Grupo de Replicação de Senha RODC Permitido de Munique**, clique em **OK**.
9. Feche **Usuários e Computadores do Active Directory**.
10. Alterne para **Centro Administrativo do Active Directory** e abra as propriedades de **MUC-RODC1**. Na seção **Extensões**, na guia **Política de Replicação de Senha**, clique em **Adicionar**.
11. Na caixa de diálogo **Adicionar Grupos, Usuários e Computadores**, selecione a opção **Permitir a replicação de senhas da conta para este RODC** e clique em **OK**.
12. Na caixa de diálogo **Selecionar Usuários, Computadores, Contas de Serviço ou Grupos**, na caixa de texto **Digite os nomes de objeto a serem selecionados**, digite **Munique**, clique em **Verificar Nomes** e em **OK**.
13. Na caixa de diálogo **MUC-RODC1 (Desabilitado)**, clique em **OK**.

Verificar a política de senha resultante

1. No **Centro Administrativo do Active Directory**, no painel **Tarefas,** na seção **MUC-RODC1**, clique em **Propriedades**.
2. Na caixa de diálogo **Propriedades de MUC-RODC1 (Desabilitado)**, na seção **Extensões** da guia **Política de Replicação de Senha**, clique em **Avançado**.

 **Observação:** a caixa de diálogo **Política de Replicação de Senha Avançada para MUC-RODC1** exibe todas as contas com senhas armazenadas neste RODC.

3. Na lista suspensa **Exibir usuários e computadores que atendam aos seguintes critérios**, clique em **Contas que foram autenticadas para este Controlador de Domínio Somente Leitura** e informe aos alunos que esta página mostrará apenas as contas que têm as permissões solicitadas e autenticadas pelo RODC.
4. Na guia **Política Resultante**, clique em **Adicionar** e, na caixa de diálogo **Selecionar Usuários ou Computadores**, no campo **Digite o nome do objeto a ser selecionado**, digite **Ana**, clique em **Verificar Nomes** e em **OK** duas vezes.
5. Observe que Ana tem uma **Configuração Resultante Permitir**.
6. Feche ou cancele todas as caixas de diálogo.

Lição 2

Implementação de segurança da conta

Sumário:

Perguntas e respostas 6
Recursos 6
Demonstração: Configuração de políticas de conta de domínio 6
Demonstração: Configuração de uma política de senha refinada 8

Perguntas e respostas

Pergunta: Qual tecnologia permite usar a funcionalidade biométrica para entrar nos dispositivos Windows?

> **Resposta:** Windows Hello é uma nova tecnologia no Windows 10 e Windows 10 Mobile que permite autenticação usando impressões digitais, varredura de íris ou outros dados biométricos.

Recursos

Opções de segurança da conta no Windows Server 2016

 **Leitura adicional:** Para obter mais informações sobre a proteção de credenciais e gerenciamento, consulte: http://aka.ms/R5bfid

Demonstração: Configuração de políticas de conta de domínio

Etapas da demonstração

Configurar uma política de senha baseada em domínio

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. No console de **Gerenciamento de Política de Grupo,** expanda **Floresta: Adatum.com\Domains\Adatum.com\Objetos de Política de Grupo**, clique com o botão direito do mouse em **Política de Domínio Padrão** e clique em **Editar**.
3. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, em **Configuração do Computador**, expanda **Políticas\Configurações do Windows\Configurações de Segurança\Políticas de Conta**, clique duas vezes em **Política de Senha** e duas vezes em **Aplicar histórico de senhas**.
4. Na caixa de diálogo de propriedades de **Aplicar histórico de senhas**, no campo **Manter histórico da senha por** , digite **20**, clique em **OK** e clique duas vezes em **Tempo de vida máximo da senha**.
5. Na caixa de diálogo de propriedades de **Tempo de vida máximo da senha**, no campo **A senha expirará em**, digite **45**, clique em **OK** e clique duas vezes em **Tempo de vida mínimo da senha**.
6. Na caixa de diálogo de propriedades de **Tempo de vida mínimo da senha**, verifique se o campo **A senha pode ser alterada após** está definido como **1**, clique em **OK** e clique duas vezes em **Comprimento mínimo da senha**.
7. Na caixa de diálogo de propriedades de **Comprimento mínimo da senha**, no campo **A senha deve ter pelo menos**, digite **10**, clique em **OK** e clique duas vezes em **A senha deve atender aos requisitos de complexidade**.
8. Na caixa de diálogo de propriedades de **A senha deve atender aos requisitos de complexidade**, clique em **Habilitado** e em **OK**.
9. Não feche a janela **Editor de Gerenciamento de Política de Grupo**.

Configurar uma política de bloqueio de conta

1. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, clique em **Política de Bloqueio de Conta** e clique duas vezes em **Duração do bloqueio de conta**.
2. Na caixa de diálogo **Propriedades de Duração do bloqueio de conta**, clique em **Definir esta configuração de política** e, no campo **Minutos**, digite **30** e clique em **OK**.
3. Na caixa de diálogo **Alterações de valor sugeridas**, observe os valores sugeridos, inclusive a configuração automática de **Limite de bloqueio de conta**, clique em **OK** e clique duas vezes em **Zerar contador de bloqueios de conta após**.
4. Na caixa de diálogo de propriedades de **Zerar contador de bloqueios de conta após**, no campo **Zerar contador de bloqueios de conta após**, digite **15** e clique em **OK**.
5. Feche a janela **Editor de Gerenciamento de Política de Grupo** e o console de **Gerenciamento de Política de Grupo**.

Demonstração: Configuração de uma política de senha refinada

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Centro Administrativo do Active Directory**.
2. No **Centro Administrativo do Active Directory**, no painel de navegação, clique em **Adatum (local)**.
3. No painel de detalhes, clique duas vezes na UO **Gerentes**.
4. No painel de detalhes, clique com o botão direito do mouse no grupo **Gerentes** e clique em **Propriedades**.

 **Observação:** verifique se você abriu a caixa de diálogo **Propriedades** do grupo Gerentes, não da UO Gerentes.

5. Na caixa de diálogo **Managers**, em **Escopo do grupo**, clique em **Global** e em **OK**.
6. No Central Administrativa do Active Directory, no painel de navegação, clique em **Adatum (local)**.
7. No painel de detalhes, clique duas vezes no contêiner **System**.
8. No painel de detalhes, clique com o botão direito do mouse em **Passowrd settings container**, clique em **Novo** e em **Password Settings**.
9. Na janela **Criar Configurações de Senha**, conclua as seguintes etapas:
   a. No campo **Nome**, digite **ManagersPSO**.
   b. No campo **Precedência**, digite **10**.
   c. Marque a caixa de seleção **Impor comprimento mínimo da senha** e, no campo **Comprimento mínimo da senha (caracteres)**, digite **15**.
   d. Marque a caixa de seleção **Impor histórico de senhas** e, no campo **Número de senhas lembradas**, digite **20**.

e. Marque a caixa de seleção **A senha deve atender aos requisitos de complexidade**, caso ainda não esteja marcada.

f. Marque a caixa de seleção **Impor duração mínima da senha**, caso ainda não esteja marcada e, no campo **O usuário não pode alterar a senha dentro de (dias)**, digite **1**.

g. Marque a caixa de seleção **Impor duração máxima da senha** caso ainda não esteja marcada e, no campo **O usuário deve alterar a senha após (dias)**, digite **30**.

h. Marque a caixa de seleção **Impor política de desbloqueio de conta**.

i. No campo **Número de tentativas de logon com falha permitido**, digite **3**.

j. No campo **Redefinir contagem de tentativas de logon com falha após (min)**, digite **30** e clique em **Até que um administrador desbloqueie manualmente a conta**.

10. Na seção **Aplica-se Diretamente a**, clique em **Adicionar**.
11. Na caixa de texto **Digite os nomes de objeto a serem selecionados**, digite **Adatum\Managers**, clique em **Verificar Nomes** e em **OK**.
12. Na janela **Criar Configurações de Senha: ManagersPSO**, clique em **OK**.
13. Feche o **Central Administrativa do Active Directory**.

Lição 3

Implementação da autenticação de auditoria

Sumário:

Perguntas e respostas 11
Demonstração: Configuração de políticas de auditoria relacionadas à autenticação 11
Demonstração: Exibição de eventos de logon 12

Perguntas e respostas

Pergunta: Quando um usuário entra em um controlador de domínio, é gerado um evento de logon.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

Quando um usuário entra em um controlador de domínio, é gerado um evento de logon de conta, não um evento de logon.

Demonstração: Configuração de políticas de auditoria relacionadas à autenticação

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique no menu **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. No console de **Gerenciamento de Política de Grupo**, no painel de navegação, expanda **Floresta: Adatum.com\Domains\Adatum.com\Objetos de Política de Grupo** e selecione a **Política de Controladores de Domínio Padrão**.
3. Clique com o botão direito do mouse em **Política de Controladores de Domínio Padrão** e clique em **Editar**.
4. Na janela **Editor de Gerenciamento de Políticas de Grupo**, no painel de navegação, expanda **Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Políticas Locais** e clique em **Política de Auditoria**.
5. No painel de detalhes, clique duas vezes em **Auditoria de eventos de logon de conta** e explique as seguintes opções de configuração:
   - Se você marcar a caixa de seleção **Definir estas configurações de políticas**, a política será aplicada.
   - Se você selecionar **Êxito**, somente as auditorias com êxito serão registradas.
   - Se você selecionar **Falha**, somente as auditorias com falha serão registradas.

   Se várias políticas contiverem a configuração e ela estiver definida de forma diferente, as opções de êxito e falha serão aplicadas com base na última política aplicada que definiu essas configurações. Se uma política definir auditorias com êxito e a outra definir auditorias com falha, elas não serão mescladas. Clique em **Definir estas configurações de políticas**, marque as caixas de seleção **Êxito** e **Falha** e clique em **OK**.
6. No painel de detalhes, clique duas vezes em **Auditoria de eventos de logon de conta**. Clique na guia **Explicar** e mostre e discuta a explicação. Clique em **Cancelar** para fechar a caixa de diálogo de propriedades de **Auditoria de eventos de logon de conta**.
7. Repita as etapas 5 e 6 com a política de **Auditoria de eventos de logon**.
8. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, vá para **Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Configuração Avançada de Política de Auditoria\Políticas de Auditoria** e clique em **Políticas de Auditoria**.

9. Na política **Políticas de Auditoria**, mostre as 10 principais categorias e clique duas vezes em **Logon de Conta**.
10. Mostre as quatro subcategorias e clique duas vezes em **Auditoria de Serviço de Autenticação Kerberos**.
11. Mostre que a subcategoria tem as mesmas configurações que **Logon de Conta de Auditoria da Política de Auditoria** e explique que agora elas estão em nível mais detalhado, permitindo uma auditoria mais seletiva.
12. Selecione **Configurar estes eventos de auditoria**, selecione **Êxito** e **Falha** e clique em **Aplicar**.
13. Na guia **Explicar**, mostre e discuta a explicação, as configurações padrão e o volume de auditoria previsto.
14. Para fechar a caixa de diálogo de propriedades de **Auditoria de Serviço de Autenticação Kerberos**, clique em **OK**.

Demonstração: Exibição de eventos de logon

Etapas da demonstração

1. Em **LON-DC1**, na tela inicial, digite **cmd** e clique em **Prompt de Comando**.
2. Digite **gpupdate /force** e pressione Enter.
3. Espere até a política ser atualizada.
4. Alterne para a tela Iniciar. Clique no ícone **Administrador** e em **Sair**.
5. Em **LON-DC1**, tente entrar como **Adatum\Aidan** com a senha **123456**.

   Você receberá uma mensagem informando que o nome de usuário ou a senha está incorreta. Clique em **OK**.
6. Entre como **Adatum\Administrador** com a senha **Pa55w.rd**.
7. Aguarde até o logon ser finalizado e o **Gerenciador do Servidor** ser iniciado.
8. No **Gerenciador do Servidor**, clique em **Ferramentas** e em **Visualizador de Eventos**.
9. No Visualizador de Eventos, no painel de navegação, expanda **Logs do Windows** e clique em **Segurança**.
10. No painel de detalhes, localize o **ID do Evento 4771** e mostre que esse evento é de Falha de Auditoria. Clique duas vezes no evento **Falha de Auditoria**. Mostre que esse evento foi registrado quando Adatum\Aidan tentou entrar com a senha incorreta. Clique em **Fechar**.
11. Localize o evento com o **ID do Evento 4768**. Mostre que se trata de um evento de Êxito de Auditoria. Clique duas vezes no evento **Êxito de Auditoria**. Mostre que esse evento foi registrado quando Adatum\Administrador entrou com êxito. Clique em **Fechar**.
12. Feche o Visualizador de Eventos.

Lição 4

Configuração de contas de serviço gerenciado

Sumário:

Perguntas e respostas 14
Demonstração: Configuração de MSAs de grupo 14

Perguntas e respostas

Pergunta: Qual é a diferença entre MSAs de grupo e MSAs padrão?

> **Resposta:** As MSAs de grupo permitem estender os recursos das MSAs padrão para mais de um servidor no domínio.

Demonstração: Configuração de MSAs de grupo

Etapas da demonstração

Criar a chave raiz KDS para o domínio

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e abra o console do **Módulo Active Directory do Windows PowerShell**.
2. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
```

Criar e associar uma MSA

1. No prompt de comando, digite o seguinte comando e pressione Enter:

```
New-ADServiceAccount –Name SampleApp_SVR1 –DNSHostname LON-DC1.Adatum.com -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
```

2. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Add-ADComputerServiceAccount –identity LON-SVR1 –ServiceAccount SampleApp_SVR1
```

3. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Get-ADServiceAccount -Filter *
```

4. Verifique se a conta de serviço **SampleApp_SVR1** está listada.

Instalar uma MSA

1. Em **LON-SVR1**, clique em **Iniciar** e em **Gerenciador do Servidor**, em seguida, no menu **Ferramentas**, abra o console do **Módulo Active Directory do Windows PowerShell**.
2. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Install-ADServiceAccount -Identity SampleApp_SVR1
```

3. Em **Gerenciador do Servidor**, na barra de ferramentas **Menu**, clique em **Ferramentas** e em **Serviços**.
4. No console de **Serviços**, clique com o botão direito do mouse em **Serviço de Compartilhamento de Dados** e clique em **Propriedades**.

 **Observação:** nesta demonstração, o Serviço de Compartilhamento de Dados é usado como exemplo. Em um ambiente de produção, você usaria o serviço real atribuído à MSA.

5. Na caixa de diálogo de propriedades de **Serviço de Compartilhamento de Dados (Computador Local)**, clique na guia **Logon**.
6. Na guia **Logon**, clique em **Esta conta** e digite **Adatum\SampleApp_SVR1$**.
7. Limpe a senha nas caixas **Senha** e **Confirmar senha** e clique em **OK**.
8. Clique em **OK** em todos os avisos.

Revisão do módulo e informações complementares

Perguntas de revisão

Pergunta: Por que a segurança física é tão importante, principalmente nos controladores de domínio do AD DS?

> **Resposta:** Os controladores de domínio do AD DS armazenam todas as informações sobre todos os usuários, computadores, grupos e quaisquer outros objetos do domínio. Se uma pessoa obtiver acesso físico ao servidor ou à sua unidade de disco rígido, ela poderá desviar da proteção de segurança com facilidade e recuperar todas essas informações. Essa pessoa poderá usar as informações para atacar a rede ou modificar o controlador de domínio e colocá-lo de volta na rede com más intenções.

Pergunta: Você precisa implementar políticas de auditoria para autenticação de domínio e alterações nos serviços de diretório. Qual é a melhor maneira de implementar essas configurações de auditoria?

> **Resposta:** Se você deseja habilitar a auditoria, é muito importante definir as mesmas configurações de auditoria para todos os servidores pertinentes nos quais o evento possa ocorrer. Se você deseja configurar a auditoria para autenticação de domínio ou alterações no AD DS, defina essas configurações na Política de Controladores de Domínio Padrão ou um GPO que esteja vinculado à UO de Controladores de Domínio.

Pergunta: Sua organização exige que seja mantida uma infraestrutura AD DS altamente confiável e segura. E também que os usuários tenham acesso ao email corporativo pela Internet, usando o Outlook Web Access. Você está pensando em implementar configurações de bloqueio de conta. O que deve ser considerado?

> **Resposta:** As configurações de bloqueio de conta não são apenas um recurso de segurança. Elas também fornecem aos invasores uma interface DoS de fácil acesso. Se o Outlook Web Access for acessado pela Internet, configure protocolos ou serviços adicionais para garantir que somente os usuários do seu domínio poderão inserir credenciais de logon. Outros usuários não devem ser autorizados a usar o site da Web para inserir senhas falsas e bloquear contas de usuário válidas.

Ferramentas

A tabela a seguir lista as ferramentas mencionadas neste módulo.

Ferramenta	Use para	Onde encontrar
Usuários e Computadores do Active Directory	Gerenciar objetos dentro do AD DS, por exemplo, usuários, grupos e computadores.	**Gerenciador do Servidor**
Central Administrativa do Active Directory	Gerenciar objetos dentro do AD DS, por exemplo, usuários, grupos e computadores.	**Gerenciador do Servidor**
Gerenciamento de Política de Grupo	Gerenciar, emitir relatório, fazer backup e restaurar GPOs.	**Gerenciador do Servidor**
Gpupdate.exe	Atualizar manualmente os GPOs de máquinas locais.	Linha de comando

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Você definiu configurações de política de auditoria avançada, mas elas não se aplicam.	Verifique se você definiu **Auditoria: forçar configurações de subcategorias de políticas de auditoria (Windows Vista ou superior) para substituir configurações de categorias de políticas de auditoria** em **Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Políticas Locais\Opções de Segurança**.
Você configurou a auditoria de alterações em logon de conta ou serviços de diretório. Agora, você está testando-os, mas não consegue localizar os eventos no log de eventos do servidor.	Se você tiver vários controladores de domínio, verifique o log de segurança de cada controlador de domínio. Além disso, certifique-se de que você tenha a política de auditoria configurada para cada controlador de domínio.

Perguntas e respostas da revisão do laboratório

Laboratório: Segurança do AD DS

Perguntas e respostas

Pergunta: No laboratório, você definiu as configurações de senha para todos os usuários dentro da Política de Domínio Padrão e também para os administradores dentro de um PSO. Que outras opções estavam disponíveis para ajudá-lo na solução?

Resposta: Você poderia ter criado um PSO com configurações específicas para todos os usuários, configurado com precedência bastante elevada e vinculado ao grupo de segurança Usuários do Domínio. O benefício é haver somente uma interface de gerenciamento de políticas de senha de domínio, e as configurações padrão para contas locais nos membros do domínio podem ser definidas de modo diferente em todo o domínio.

Pergunta: No laboratório, você estava usando precedência para o PSO administrativo com valor 10. Por quê?

Resposta: O PSO administrativo é muito restritivo, portanto, a precedência precisa ser baixa. No entanto, futuramente, poderá haver grupos de administradores com configurações mais restritivas, por exemplo, um subconjunto de administradores para acessar dados de recursos humanos, ou contas de serviço às quais você pode impor senhas mais longas com direitos administrativos que mudem com menos frequência. Por esses motivos, usando o valor 10, haverá espaço para implementar PSOs que sejam mais precisos.