

Módulo 12

Implementação da sincronização do AD DS com o Microsoft Azure AD

Sumário:

Lição 1: Planejamento e preparação para a sincronização de diretório	2
Lição 2: Implementação da sincronização de diretório usando o Azure AD Connect	4
Lição 3: Gerenciamento de identidades com a sincronização de diretório	7
Revisão do módulo e informações complementares	10
Perguntas e respostas da revisão do laboratório	12

Lição 1

Planejamento e preparação para a sincronização de diretório

Sumário:

Perguntas e respostas	3
Recursos	3

Perguntas e respostas

Pergunta: Quando você implementa a sincronização de diretório, as contas de usuário e os grupos são movidas do seu AD DS local para o Azure AD.

☐ Verdadeiro

☐ Falso

Resposta:

☐ Verdadeiro

☒ Falso

Comentários:

A sincronização de diretório não move objetos. Ela copia objetos do AD DS local com um subconjunto de seus atributos e cria novos objetos no Azure AD.

Recursos

Planejamento da sincronização de diretório



Leitura adicional: para obter mais informações, consulte o Azure Hybrid Identity Design Considerations Guide em: <http://aka.ms/ibuqek>

Pré-requisitos e preparação para a sincronização de diretório



Leitura adicional: para obter mais informações, consulte: "Você recebe o erro "Esta empresa excedeu o número de objetos que podem ser sincronizados" em um relatório de sincronização de diretório" em: <http://aka.ms/r4x1q4>

Lição 2

Implementação da sincronização de diretório usando o Azure AD Connect

Sumário:

Perguntas e respostas	5
Recursos	5
Demonstração: Instalação e configuração do Azure AD Connect	5


Perguntas e respostas

Pergunta: Ao implementar a sincronização entre o AD DS e o Azure AD, onde você controla os objetos do AD DS?


Resposta: Se tiver implantado o Azure AD Connect para a sincronização do Active Directory, você estará controlando os objetos de dentro do seu AD DS local usando ferramentas, como Usuários e Computadores do Active Directory ou o Windows PowerShell — a origem da autoridade é o AD DS local.

Recursos

Sincronização personalizada do Azure AD Connect

 **Leitura adicional:** para obter mais informações, consulte: “Configurando o ID de logon alternativo” em: <http://aka.ms/nqh5gc>


Recursos de monitoramento do Azure AD Connect

 **Leitura adicional:** para obter mais informações, consulte: “Monitorar infraestrutura de identidade local e serviços de sincronização na nuvem” em: <http://aka.ms/dqaaps>

Demonstração: Instalação e configuração do Azure AD Connect

Etapas da demonstração

1. Em **LON-SVR1**, entre como **Adatum\Administrador** com a senha **Pa55w.rd**.
2. Abra o Internet Explorer e acesse <http://www.microsoft.com/en-us/download/details.aspx?id=47594>.
3. Na página **Microsoft Azure Active Directory Connect**, clique em **Baixar**.
4. Clique em **Executar**. Aguarde alguns minutos até que o download seja concluído.

 **Observação:** se tiver qualquer problema para iniciar o download, adicione o site <https://download.microsoft.com> aos seus sites confiáveis.

5. No **Assistente do Microsoft Azure Active Directory Connect**, na página **Bem-vindo ao Azure AD Connect**, selecione **Concordo com os termos de licença e o aviso de privacidade** e clique em **Continuar**.
6. Na página **Configurações Expressas**, clique em **Personalizar**.
7. Na página **Instalar componentes necessários**, examine as opções disponíveis, mas não faça alterações e, em seguida, clique em **Instalar**.
8. Na página **Entrada do usuário**, selecione **Sincronização de Senha** e clique em **Avançar**.
9. Na página **Conectar ao Azure AD**, nas caixas de texto **NOME DE USUÁRIO** e **SENHA**, digite **SYNC@seudomínio.onmicrosoft.com** para o nome de usuário da conta, digite **Pa55w.rd1** como a senha e clique em **Avançar**. Pode demorar alguns minutos para que a conexão seja estabelecida.

10. Na página **Conecte seus diretórios**, na caixa de texto **NOME DE USUÁRIO**, digite **Adatum\administrador** e, na caixa de texto **SENHA**, digite **Pa55w.rd**. Clique em **Adicionar Diretório** e, em seguida, clique em **Avançar**.
11. Na página **Configuração de entrada do Azure AD**, selecione **Continuar sem nenhum domínio verificado**, e clique em **Avançar**.
12. Na página **Filtragem de domínio e UO**, clique em **Avançar**.
13. Na página **Identificar com exclusividade seus usuários**, examine e explique as opções disponíveis, mas não faça alterações.
14. Clique em **Avançar**.
15. Na página **Filtrar usuários e dispositivos**, clique em **Sincronização selecionada**. Na caixa de texto **GRUPO**, digite **Pesquisa** e clique em **Resolver**. Verifique se uma marca de seleção verde é exibida depois que você clica em **Resolver**.
16. Clique em **Avançar**.
17. Na página **Recursos opcionais**, selecione **Write-back de senha**, explique as outras opções aos alunos e clique em **Avançar**.
18. Na página **Pronto para configurar**, clique em **Instalar** e, quando a instalação for concluída, clique em **Sair**.

A sincronização de objetos a partir do seu AD DS local e do Azure AD deve começar. Espere aproximadamente cinco minutos para que esse processo seja concluído.

19. Abra o Internet Explorer no seu computador host e, em seguida, abra o portal do Azure acessando **<https://portal.azure.com>**.
20. Entre com a sua conta criada durante o provisionamento da avaliação do Office 365.
21. No painel esquerdo, clique em **Azure Active Directory**.
22. Clique em **Usuários e grupos** na lista de opções **GERENCIAR**.
23. Clique em **Todos os usuários**.
24. Verifique se você pode ver as contas de usuário do seu AD DS local. Você deve ser capaz de ver todos os usuários do seu domínio **adatum.com** local.
25. Em **LON-SVR1**, clique em **Iniciar** e, em seguida, clique em **Azure AD Connect**. Expanda **Azure AD Connect** e clique em **Serviço de Sincronização**.
26. Na janela **Synchronization Service Manager em LON-SVR1**, clique na guia **Operações**.
27. Certifique-se de que você veja as tarefas **Exportação**, **Sincronização Completa** e **Importação Completa**.
28. Verifique se todas as tarefas têm a hora e a data atuais nas colunas **Hora de Início** e **Hora de Término**. Além disso, certifique-se de que todas as tarefas exibam **êxito** na coluna **Status**.

Lição 3

Gerenciamento de identidades com a sincronização de diretório

Sumário:

Perguntas e respostas	8
Recursos	9

Perguntas e respostas

Pergunta: Se quiser ter SSO para o serviço baseado em nuvem e o serviço local, o que você precisa implantar? Escolha todas as opções aplicáveis.

- ☐ Azure AD Connect Health
- ☐ AD FS
- ☐ Azure AD Connect
- ☐ Office 365
- ☐ Azure AD

Resposta:

- ☐ Azure AD Connect Health
- ☒ AD FS
- ☒ Azure AD Connect
- ☐ Office 365
- ☐ Azure AD

Pergunta: Se implementar o AD FS e a federação entre o AD DS implantado localmente e o Azure AD, você não precisará usar o Azure AD Connect.

- ☐ Verdadeiro
- ☐ Falso

Resposta:

- ☐ Verdadeiro
- ☒ Falso

Comentários:

O AD DS local executa a autenticação e, em seguida, passa essas informações para o Azure AD. A senha do Azure AD não é usada. No entanto, as contas nos dois serviços de diretório devem coincidir. Portanto, é necessário que você use tanto o Azure AD Connect quanto o AD FS.

Recursos

Modificação da sincronização de diretório



Leitura adicional: para obter mais informações, consulte: "Sincronização do Azure AD Connect: configurar a filtragem" em: <http://aka.ms/au8smo>

Monitoramento da sincronização de diretório



Leitura adicional: para obter mais informações, consulte: "Azure Active Directory PowerShell Module" em: <http://aka.ms/pfsm1x>

Solução de problemas da sincronização de diretório



Leitura adicional: para obter mais informações, consulte: "Integração das suas identidades locais com o Azure Active Directory" em: <http://aka.ms/cdm2kk>



Leitura adicional: para obter mais informações, consulte: "How to troubleshoot Azure Active Directory Sync tool installation and Configuration Wizard errors" em: <http://aka.ms/bz5cjw>

Revisão do módulo e informações complementares

Práticas recomendadas

- Para ambientes simples, use as configurações expressas do Azure AD Connect.
- Habilite os usuários para usarem a funcionalidade de autoatendimento de redefinição de senha com pelo menos dois métodos de autenticação.
- Considere o uso de funcionalidades de write-back.
- Implemente o Azure AD Connect Health se tiver uma assinatura Premium do Azure AD.

Problemas e cenários reais

Como a sincronização de diretório é o vínculo entre seus objetos do AD DS local e os serviços no Azure AD, tenha cuidado ao fazer alterações no Azure AD Connect ou no Synchronization Service Manager após a implantação de produção. Por exemplo, um pequeno erro na filtragem pode excluir acidentalmente todas as caixas de correio de usuário no Office 365.

Em alguns ambientes, por exemplo, em um ambiente de teste, você pode testar todas as alterações em um outro servidor de sincronização de diretório que esteja conectado a um locatário separado do Azure AD (avaliação). Além disso, você deve iniciar manualmente os perfis de execução para cada agente de gerenciamento no Synchronization Service Manager e observar as ações pendentes antes de exportar para o Azure AD. Em alguns casos, convém criar um novo perfil de execução para a exportação para o Azure AD que inclui um limite máximo ao número de exclusões permitidas.

Pergunta de revisão

Pergunta: Qual recurso você precisa configurar para que os objetos sejam sincronizados do Azure AD com seu AD DS local?

Resposta: Você precisa implantar funcionalidades de write-back. No momento, você pode usar o write-back de senha, o write-back de grupo e o write-back de dispositivos.

Ferramentas

A tabela a seguir lista as ferramentas mencionadas neste módulo:

Ferramenta	Use para	Onde encontrar
Azure AD Connect	Estabelecer a sincronização entre o AD DS e o Azure AD	Centro de Download da Microsoft
Azure AD Connect Health	Monitorar a integridade da sincronização do AD DS com o Azure AD	O portal clássico do Azure
O portal clássico do Azure	Gerenciamento do Azure AD	http://aka.ms/n2l3cb

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
A filtragem de sincronização de diretório não está mais funcionando.	É importante ter a última versão da ferramenta de sincronização de diretório. No entanto, ao atualizar para uma nova versão da ferramenta, todos os filtros e outras personalizações do agente de gerenciamento não serão importados automaticamente para a nova instalação. Se você estiver atualizando para uma versão mais recente da sincronização de diretório, sempre reapply manualmente as configurações de filtragem após a atualização, mas antes de executar o primeiro ciclo de sincronização.
Após a instalação do Azure AD Connect, um prompt poderá ser exibido com a seguinte mensagem de erro quando você abrir o Synchronization Service Manager: "Unable to connect to the Synchronization Service."	Adicione a conta de usuário apropriada do domínio do Azure AD Connect ao grupo ADSyncAdmins, saia e entre novamente. A conta de usuário do domínio que você usa para entrar durante a instalação do Azure AD Connect será adicionada automaticamente ao grupo, mas você ainda precisará sair e depois entrar novamente antes de conseguir abrir o Synchronization Service Manager com êxito.

Perguntas e respostas da revisão do laboratório

Laboratório: Configuração da sincronização de diretório

Perguntas e respostas

Pergunta: O que você precisa fazer antes de começar a configurar o Azure AD Connect?

Resposta: Você deve criar uma conta de sincronização no Azure AD e, em seguida, adicionar seu domínio ao locatário do Azure AD.

Pergunta: Qual cmdlet devo usar para alterar a agenda de sincronização do Azure AD Connect?

Resposta: Você deve usar o cmdlet **Set-ADSyncScheduler** no computador de instalação do Azure AD Connect.