Módulo 10

Implementação e administração do AD FS

Sumário:

Lição 1: Visão geral do AD FS 2

Lição 2: Requisitos e planejamento do AD FS 4

Lição 3: Implantação e configuração do AD FS 7

Lição 4: Visão geral do Proxy de Aplicativo Web 11

Revisão do módulo e informações complementares 15

Perguntas e respostas da revisão do laboratório 16

Lição 1

Visão geral do AD FS

Sumário:

Perguntas e respostas 3

Perguntas e respostas

Pergunta: Uma relação de confiança federada é igual a uma relação de confiança da floresta que as organizações podem configurar entre florestas do AD DS.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

Uma relação de confiança federada não é igual a uma relação de confiança da floresta que as organizações podem configurar entre florestas do AD DS. Em uma relação de confiança federada, os servidores AD FS em duas organizações nunca precisam se comunicar diretamente um com o outro. Além disso, toda a comunicação em uma implantação de federação ocorre por HTTPS, de modo que você não precisa abrir várias portas em algum firewall para permitir a federação.

Lição 2

Requisitos e planejamento do AD FS

Sumário:

Perguntas e respostas 5
Demonstração: Instalação da função de servidor AD FS 5

Perguntas e respostas

Pergunta: No Windows Server 2016, a funcionalidade do proxy do servidor de federação faz parte da função Proxy de Aplicativo Web.

( ) Verdadeiro

( ) Falso

Resposta:

(√) Verdadeiro

( ) Falso

Comentários:

O proxy do servidor de federação é um componente opcional que você normalmente implanta em uma rede de perímetro. Ele não adiciona funcionalidade à implantação do AD FS, mas fornece uma camada de aprimoramento de segurança para conexões da Internet com o servidor de federação. No Windows Server 2016, a funcionalidade do proxy do servidor de federação faz parte do Proxy de Aplicativo Web.

Demonstração: Instalação da função de servidor AD FS

Etapas da demonstração

Instalar o AD FS

1. Em **LON-DC1**, clique em Iniciar, clique com o botão direito do mouse em **Windows PowerShell** e, depois, clique em **Executar como Administrador**.
2. No prompt de comando, digite o seguinte comando e pressione Enter:

   ```
   Add-KdsRootKey –EffectiveTime ((Get-Date).AddHours (-10))
   ```

   Esse comando cria a chave raiz do Serviço de Distribuição de Chave de Grupo da Microsoft para gerar as senhas gMSA (Conta de Serviço Gerenciado do grupo) para a conta que será usada posteriormente neste laboratório. Você deve receber um GUID (identificador global exclusivo) como uma resposta a esse comando.
3. Na **LON-DC1**, no Gerenciador do Servidor, clique em **Gerenciar** e em **Adicionar Funções e Recursos**.
4. No **Assistente de Adição de Funções e Recursos**, na página **Antes de começar,** clique em **Próximo**.
5. Na página **Selecionar tipo de instalação**, clique em **Instalação baseada em função ou recurso** e em **Próximo**.
6. Na página **Selecionar servidor de destino**, clique em **LON-DC1.Adatum.com** e em **Próximo**.
7. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Serviços de Federação do Active Directory (AD FS)** e clique em **Próximo**.
8. Na página **Selecionar recursos**, clique em **Próximo**.
9. Na página **Serviços de Federação do Active Directory (AD FS)**, clique em **Próximo**.
10. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
11. Aguarde a instalação ser concluída e clique em **Fechar**.

Adicionar um registro DNS para o AD FS

1. Em **LON-DC1**, no Gerenciador do Servidor, clique em **Ferramentas** e em **DNS**.
2. No Gerenciador DNS, expanda **LON-DC1**, expanda **Zonas de Pesquisa Direta** e clique em **Adatum.com**.
3. Clique com o botão direito do mouse em **Adatum.com** e clique em **Novo Host (A ou AAAA)**.
4. Na janela **Novo Host**, na caixa **Nome**, digite **adfs**.
5. Na caixa **Endereço IP**, digite **172.16.0.10** e clique em **Adicionar Host**.
6. Na janela **DNS**, clique em **OK** e em **Concluído**.
7. Feche o Gerenciador DNS.

Configurar o AD FS

1. Na **LON-DC1**, no Gerenciador do Servidor, clique no ícone **Notificações** e clique em **Configure o serviço de federação neste servidor**.
2. No **Assistente de Configuração dos Serviços de Federação do Active Directory**, na página **Bem-vindo**, clique em **Criar o primeiro servidor de federação em um farm de servidores de federação** e em **Próximo**.
3. Na página **Conectar ao Active Directory Domain Services**, clique em **Próximo** para usar **Adatum\Administrador** para realizar a configuração.
4. Na página **Especificar Propriedades do Serviço**, na caixa de diálogo **Certificado SSL**, selecione **adfs.adatum.com**.
5. Na caixa **Nome para Exibição do Serviço de Federação**, digite **A. Datum Corporation** e clique em **Próximo**.
6. Na página **Especificar Conta de Serviço**, clique em **Criar uma Conta de Serviço Gerenciado de Grupo**.
7. Na caixa **Nome da Conta**, digite **ADFSService** e clique em **Próximo**.
8. Na página **Especificar Banco de Dados de Configuração**, clique em **Crie um banco de dados neste servidor que utiliza o Banco de Dados Interno do Windows** e em **Próximo**.
9. Na página **Examinar Opções**, clique em **Próximo**.
10. Na página **Verificações de Pré-requisitos**, clique em **Configurar**.
11. Na página **Resultados**, clique em **Fechar**.

Lição 3

Implantação e configuração do AD FS

Sumário:

Perguntas e respostas 8
Recursos 8
Demonstração: Configuração dos objetos de confiança de terceira parte confiável e das relações de confiança do provedor de declarações 8
Demonstração: Configuração das regras de declarações 10

Perguntas e respostas

Pergunta: O que são regras de declaração? Qual é a finalidade das regras de declaração?

Resposta: As regras de declaração definem como os servidores AD FS enviam e consomem declarações. As regras de declaração definem a lógica de negócios aplicada às declarações fornecidas pelos provedores de declarações e aceitas pelas terceiras partes confiáveis. Você pode usar as regras de declaração para:

- Definir quais declarações de entrada são aceitas de um ou mais provedores de declarações.
- Definir quais declarações de saída são fornecidas a uma ou mais terceiras partes confiáveis.
- Aplicar regras de autorização a fim de permitir o acesso a uma terceira parte confiável específica de um ou mais usuários ou grupos de usuários.

Recursos

Como funciona a descoberta de realm inicial

 **Leitura adicional:** Para saber mais sobre *RelayState*, consulte "Como oferecer suporte a RelayState iniciado pelo provedor de identidade" em: http://aka.ms/Df8hqs

Demonstração: Configuração dos objetos de confiança de terceira parte confiável e das relações de confiança do provedor de declarações

Etapas da demonstração

Configurar uma relação de confiança do provedor de declarações

1. Na **LON-DC1**, no Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento do AD FS**.
2. No console de gerenciamento do **AD FS**, clique em **Confiança do Provedor de Declarações**.
3. Clique com o botão direito do mouse em **Active Directory** e clique em **Editar Regras de Declaração**.
4. Na janela **Editar Regras de Declaração para Active Directory**, na guia **Regras de Transformação de Aceitação**, clique em **Adicionar Regra**.
5. No **Assistente para Adicionar Regra de Declaração de Transformação**, na página **Selecionar Modelo de Regra**, na lista **Modelo de regra de declaração**, clique em **Enviar Atributos LDAP como Declarações** e em **Avançar**.
6. Na página **Configurar Regra**, na caixa **Nome da regra de declaração**, digite **Regra de Atributos LDAP de Saída**.
7. Na lista **Repositório de atributos**, clique em **Active Directory**.
8. Na seção **Mapeamento de atributos LDAP para tipos de declaração de saída**, selecione os seguintes valores para o **Atributo LDAP** e o **Tipo de Declaração de Saída**:
   - Endereços de Email: **Endereço de Email**
   - Nome Principal do Usuário: **UPN**
9. Clique em **Concluir** e em **OK**.

Configurar um aplicativo WIF (Windows Identity Foundation) para AD FS

1. Na **LON-SVR1**, abra o Gerenciador do Servidor, clique em **Ferramentas** e em **Windows Identity Foundation federation utility**.
2. Na página **Bem-vindo ao Assistente do Utilitário de Federação**, na caixa **Local de configuração do aplicativo**, digite **C:\inetpub\wwwroot\AdatumTestApp\web.config** para o local do arquivo **Web.config** de exemplo.
3. Na caixa **URI do Aplicativo**, digite **https://lon-svr1.adatum.com/AdatumTestApp/** de modo a indicar o caminho para o aplicativo de exemplo que confiará nas declarações de entrada do servidor de federação e clique em **Avançar**.
4. Na página **Serviço de Token de Segurança**, clique em **Usar um STS existente** e, na caixa **Local do documento de metadados da Web Services Federation do STS**, digite **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**. Clique em **Avançar**.
5. Na página **STS signing certificate chain validation error**, clique em **Disable certificate chain validation** e clique em **Avançar**.
6. Na página **Security token encryption**, clique em **No encryption** e em **Avançar**.
7. Na página **Offered claims**, examine as declarações que serão oferecidas pelo servidor de federação e clique em **Next**.
8. Na página **Resumo**, examine as alterações que serão feitas no aplicativo de exemplo pelo **Assistente do Utilitário de Federação**, percorra os itens para entender a função de cada um e clique em **Concluir**.
9. Na janela **Êxito**, clique em **OK**.

Configurar um objeto de confiança de terceira parte confiável

1. Na **LON-DC1**, no prompt de comando do **Windows PowerShell**, digite o seguinte comando para adicionar um objeto de confiança de terceira parte confiável e pressione Enter:

```
Add-ADFSRelyingPartyTrust –Name ‘A. Datum Corporation Test App’ –MetadataURL ‘https:
//lon-svr1.adatum.com/AdatumTestApp/federationmetadata/2007-06/federationmetadata.xml’
```

2. No console de gerenciamento do **AD FS**, na lista de **Confianças da Terceira Parte Confiável**, clique em **Aplicativo de Teste da A. Datum Corporation** e selecione **Editar Política de Emissão de Declaração**.
3. Na janela **Editar Política de Emissão de Declaração para Aplicativo de Teste da A. Datum Corporation**, na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
4. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
5. Na caixa **Nome da regra de declaração**, digite **Passar nome da conta do Windows**.
6. Na lista **Tipo de declaração de entrada**, clique em **Nome de conta do Windows** e em **Concluir**.
7. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
8. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
9. Na caixa **Nome da regra de declaração**, digite **Passar Endereço de Email**.
10. Na lista **Tipo de declaração de entrada**, clique em **Endereço de Email** e em **Concluir**.
11. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.

12. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
13. Na caixa **Nome da regra de declaração**, digite **Passar UPN**.
14. Na lista **Tipo de declaração de entrada**, clique em **UPN** e em **Concluir**.
15. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
16. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
17. Na caixa **Nome da regra de declaração**, digite **Passar Nome**.
18. Na lista **Tipo de declaração de entrada**, clique em **Nome** e em **Concluir**.
19. Na guia **Regras de Transformação de Emissão**, clique em **OK**.

Demonstração: Configuração das regras de declarações

Etapas da demonstração

1. Na **LON-DC1**, no Gerenciador do AD FS, selecione **Confianças da Terceira Parte Confiável**, clique com o botão direito do mouse em **Aplicativo de Teste da A. Datum Corporation** e clique em **Editar Política de Emissão de Declaração**.
2. Na janela **Editar Política de Emissão de Declaração para Aplicativo A. Datum Corporation Test App**, na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
3. Na caixa de diálogo **Modelo de Regra de Declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
4. Na caixa **Nome da regra de declaração**, digite **Regra de Envio de Nome de Grupo**.
5. Na lista **Tipo de declaração de entrada**, clique em **Grupo** e em **Concluir**.
6. Clique em **OK**.
7. Clique com o botão direito do mouse em **Aplicativo de Teste da A. Datum Corporation** e clique em **Editar Política de Controle de Acesso**
8. Na janela **Editar Política de Controle de Acesso para Aplicativo de Teste da A. Datum Corporation**, na guia **Política de controle de acesso**, clique na regra **Permitir um grupo específico**.
9. Em **Política**, clique no link **<parâmetro>**.
10. Clique em **Adicionar** e, na caixa **Selecionar Grupos**, digite **Pesquisa** e clique em **OK**. Clique em **OK** novamente para fechar a caixa **Selecionar Grupos**.
11. Clique em **OK** para fechar a caixa de diálogo **Política de Controle de Acesso**.
12. Clique com o botão direito do mouse em **Aplicativo de Teste da A. Datum Corporation** e clique em **Editar Política de Emissão de Declaração**.
13. Na guia **Regras de Transformação de Emissão**, clique em **Passar UPN** e em **Editar Regra**.
14. Na lista **Tipo de declaração de entrada**, verifique se **UPN** está selecionado.
15. Selecione **Passar apenas um valor de declaração específico**.
16. Na caixa **Valor da declaração de entrada**, digite **@adatum.com**.
17. Clique em **Exibir Idioma da Regra**.
18. Clique em **OK** e em **OK** novamente.
19. Na janela **Editar Política de Emissão de Declaração para Aplicativo de Teste da A. Datum Corporation**, clique em **OK**.

Lição 4

Visão geral do Proxy de Aplicativo Web

Sumário:

Perguntas e respostas 12
Recursos 12
Demonstração: Instalação e configuração do Proxy de Aplicativo Web 13

Perguntas e respostas

Pergunta: Qual das seguintes afirmações sobre a configuração do Proxy de Aplicativo Web é verdadeira? (Escolha todas as opções aplicáveis.)

( ) Para instalar o Proxy de Aplicativo Web, primeiramente, você deve implementar o AD FS na sua organização.

( ) Para instalar o Proxy de Aplicativo Web, você não precisa implementar o AD FS na sua organização.

( ) Para cada aplicativo que você publica, é preciso configurar uma URL externa e uma URL de servidor interna.

( ) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL interna.

( ) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL externa.

Resposta:

(√) Para instalar o Proxy de Aplicativo Web, primeiramente, você deve implementar o AD FS na sua organização.

( ) Para instalar o Proxy de Aplicativo Web, você não precisa implementar o AD FS na sua organização.

(√) Para cada aplicativo que você publica, é preciso configurar uma URL externa e uma URL de servidor interna.

( ) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL interna.

(√) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL externa.

Comentários:

A Opção 4 está incorreta. O certificado deve conter o nome do host da URL externa.

A Opção 2 está incorreta. Para instalar o Proxy de Aplicativo Web, você já deve ter o AD FS instalado.

Recursos

Cenários de uso do Proxy de Aplicativo Web

Leitura adicional: para obter mais informações sobre como configurar um site para usar IWA e delegação restrita de Kerberos, consulte "Configurar um site para usar a autenticação integrada do Windows" em: http://aka.ms/Nbsbll

Leitura adicional: para obter mais informações sobre como configurar a autenticação Kerberos para servidores Exchange com carga balanceada, consulte "Configurando a autenticação Kerberos para servidores de Acesso para Cliente com carga balanceada" em: http://aka.ms/Nd2avi

Leitura adicional: para obter mais informações sobre como publicar o Gateway de Área de Trabalho Remota por meio do Proxy de Aplicativo Web, consulte Publicando aplicativos com SharePoint, Exchange e RDG: http://aka.ms/C7f0wn

Demonstração: Instalação e configuração do Proxy de Aplicativo Web

Etapas da demonstração

Instalar o Proxy de Aplicativo Web

1. Na **LON-SVR2**, abra o Gerenciador do Servidor, clique em **Gerenciar** e em **Adicionar Funções e Recursos**.
2. No **Assistente de Adição de Funções e Recursos**, na página **Antes de começar,** clique em **Próximo**.
3. Na página **Selecionar tipo de instalação**, clique em **Instalação baseada em função ou recurso** e em **Próximo**.
4. Na página **Selecionar servidor de destino**, clique em **LON-SVR2.Adatum.com** e em **Próximo**.
5. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Acesso Remoto** e clique em **Próximo**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Acesso Remoto**, clique em **Próximo**.
8. Na página **Selecionar serviços de função**, selecione **Proxy de Aplicativo Web**.
9. No **Assistente de Adição de Funções e Recursos**, clique em **Adicionar Recursos**.
10. Na página **Selecionar serviços de função**, clique em **Próximo**.
11. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
12. Na página **Progresso da instalação**, clique em **Fechar**.

Exportar o certificado adfs.adatum.com da LON-DC1

1. Na Tela inicial da **LON-DC1**, digite **mmc** e pressione Enter.
2. No **Console1 – [Raiz do Console]**, clique em **Arquivo** e em **Adicionar/Remover Snap-in**.
3. Na janela **Adicionar ou Remover Snap-ins**, na coluna **Snap-ins disponíveis**, clique duas vezes em **Certificados**.
4. Na janela **Snap-in de certificados**, clique em **Conta de computador** e em **Próximo**.
5. Na janela **Selecionar Computador**, clique em **Computador Local (o computador em que este console está em execução)** e em **Concluir**.
6. Na janela **Adicionar ou Remover Snap-ins**, clique em **OK**.
7. No **Console1 – [Raiz do Console]**, expanda **Certificados (Computador Local)**, expanda **Pessoal** e clique em **Certificados**.
8. Clique com o botão direito do mouse em **adfs.adatum.com**, aponte para **Todas as Tarefas** e clique em **Exportar**.
9. No **Assistente para Exportação de Certificados**, clique em **Próximo**.
10. Na página **Exportar Chave Privada**, clique em **Sim, exportar a chave privada** e clique em **Próximo**.
11. Na página **Formato do Arquivo de Exportação**, clique em **Próximo**.
12. Na página **Segurança**, marque a caixa de seleção **Senha**.
13. Nas caixas **Senha** e **Confirmar senha**, digite **Pa55w.rd** e clique em **Próximo**.
14. Na página **Arquivo a Ser Exportado**, na caixa **Nome do arquivo**, digite **C:\adfs.pfx** e clique em **Próximo**.

15. Na página **Concluindo o Assistente para Exportação de Certificados**, clique em **Concluir** e em **OK** para fechar a mensagem de êxito.
16. Feche o **Console1 – [Raiz do Console]** e não salve as alterações.

Importar o certificado adfs.adatum.com na LON-SVR2

1. Na Tela inicial da **LON-SVR2**, digite **mmc** e pressione Enter.
2. No **Console1 – [Raiz do Console]**, clique em **Arquivo** e em **Adicionar/Remover Snap-in**.
3. Na janela **Adicionar ou Remover Snap-ins**, na coluna **Snap-ins disponíveis**, clique duas vezes em **Certificados**.
4. Na janela **Snap-in de certificados**, clique em **Conta de computador** e em **Avançar**.
5. Na janela **Selecionar Computador**, clique em **Computador Local (o computador em que este console está em execução)** e em **Concluir**.
6. Na janela **Adicionar ou Remover Snap-ins**, clique em **OK**.
7. No **Console1 – [Raiz do Console]**, expanda **Certificados (Computador Local)** e clique em **Pessoal**.
8. Clique com o botão direito do mouse em **Pessoal**, aponte para **Todas as Tarefas** e clique em **Importar**.
9. No **Assistente para Importação de Certificados**, clique em **Próximo**.
10. Na página **Arquivo a Ser Importado**, na caixa **Nome do arquivo**, digite **\\LON-DC1\c$\adfs.pfx** e clique em **Próximo**.
11. Na página **Proteção de chave privada**, na caixa **Senha**, digite **Pa55w.rd**.
12. Marque a caixa de seleção **Marcar esta chave como exportável. Isso possibilitará o backup ou o transporte das chaves posteriormente** e clique em **Próximo**.
13. Na página **Repositório de Certificados**, clique em **Colocar todos os certificados no repositório a seguir**.
14. Na caixa **Repositório de certificados**, selecione **Pessoal** e clique em **Próximo**.
15. Na página **Concluindo o Assistente para Importação de Certificados**, clique em **Concluir**.
16. Clique em **OK** para limpar a mensagem de êxito.
17. Feche o **Console1 – [Raiz do Console]** e não salve as alterações.

Configurar o Proxy de Aplicativo Web

1. Na **LON-SVR2**, no Gerenciador do Servidor, clique no ícone **Notificações** e em **Abrir o Assistente de Proxy do Aplicativo Web**.
2. No **Assistente de Configuração do Proxy de Aplicativo Web**, na página **Bem-vindo**, clique em **Próximo**.
3. Na página **Servidor de Federação**, digite as seguintes informações e clique em **Próximo**:
   - Nome do serviço de federação: **adfs.adatum.com**
   - Nome de usuário: **Adatum\Administrador**
   - Senha: **Pa55w.rd**
4. Na página **Certificado de Proxy do AD FS**, na caixa de diálogo **Selecione um certificado a ser usado pelo proxy do AD FS**, selecione **adfs.adatum.com** e clique em **Próximo**.
5. Na página **Confirmação**, clique em **Configurar**.
6. Na página **Resultados**, clique em **Fechar**.

Revisão do módulo e informações complementares

Prática recomendada

Nas versões anteriores do AD FS, era comum usar o SCW (Assistente de Configuração de Segurança) para aplicar práticas recomendadas de segurança específicas do AD FS aos servidores de federação e aos computadores do proxy do servidor de federação. No Windows Server 2016, o SCW foi removido porque os recursos tiveram a segurança aprimorada por padrão. Consequentemente, se precisar controlar as configurações de segurança específicas, você poderá usar a Política de Grupo ou o Gerenciador de Conformidade de Segurança da Microsoft (acesse http://aka.ms/Ncq8jm).

Perguntas de revisão

Pergunta: Sua organização está planejando implementar o AD FS. No curto prazo, somente clientes internos usarão o AD FS para acessar os aplicativos internos. No entanto, posteriormente, você deverá fornecer aos usuários domésticos acesso aos aplicativos baseados na Web que tiveram a segurança aprimorada pelo AD FS. Quantos certificados você deve obter de uma autoridade de certificação de terceiros?

> **Resposta:** Você precisa apenas de um certificado de uma autoridade de certificação de terceiros, pois o único certificado do AD FS que precisa ser confiável é o certificado de comunicação de serviço. Você pode deixar os certificados de autenticação de tokens e de descriptografia do token como autoassinados.

Pergunta: Sua organização implementou com êxito um único servidor AD FS e um único Proxy de Aplicativo Web. Inicialmente, o AD FS era usado apenas para um único aplicativo, mas agora ele é usado para vários aplicativos essenciais aos negócios. O AD FS deve ser configurado para ser altamente disponível.

Durante a instalação do AD FS, você escolheu usar o WID. Você pode usar esse banco de dados em uma configuração altamente disponível?

> **Resposta:** Sim, é possível usar o WID (Banco de Dados Interno do Windows) para dar suporte a até cinco servidores AD FS. O primeiro servidor AD FS é o servidor principal, onde todas as alterações da configuração ocorrem. As alterações no servidor principal são replicadas nos outros servidores AD FS.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do AD FS

Perguntas e respostas

Pergunta: Por que configurar adfs.adatum.com para uso como um nome de host é importante para o serviço AD FS?

Resposta: Se você usar o nome do host de um servidor existente para o servidor AD FS, não será possível adicionar mais servidores ao seu farm de servidores. Todos os servidores no farm de servidores devem compartilhar o mesmo nome de host ao fornecer serviços AD FS. Os servidores proxy do AD FS também usam o nome do host para AD FS.

Pergunta: Como você pode verificar se o AD FS está funcionando corretamente?

Resposta: Se você puder acessar **https://hostname/federationmetadata/2007-06/federationmetadata.xml** com êxito no servidor AD FS, isso significa que o AD FS está funcionando corretamente.