Configurar e Solucionar Problemas do Repositório de Armazenamento de Blob do SFTP do Azure no ISE

Contents

Introdução

Este documento descreve a configuração do Armazenamento de Blob do Azure como servidor SFTP com autenticação de Infraestrutura de Chave Pública com o Identity Services Engine.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento geral do ISE
- configuração do repositório ISE
- Autenticação de infraestrutura de chave pública (PKI)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- ISE 3.3, 3.4, 3.5 VM no Azure
- Assinatura do Azure para acessar o Centro de Armazenamento

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Como um serviço nativo na nuvem, o repositório SFTP do Azure Blob Storage é fácil de implantar e ideal para implementações do ISE baseadas no Azure. Ele elimina problemas de conectividade no local, é escalado automaticamente para atender às demandas flutuantes de armazenamento e garante alta disponibilidade e durabilidade para grandes conjuntos de dados — tudo isso enquanto elimina a necessidade de gerenciamento manual da infraestrutura.

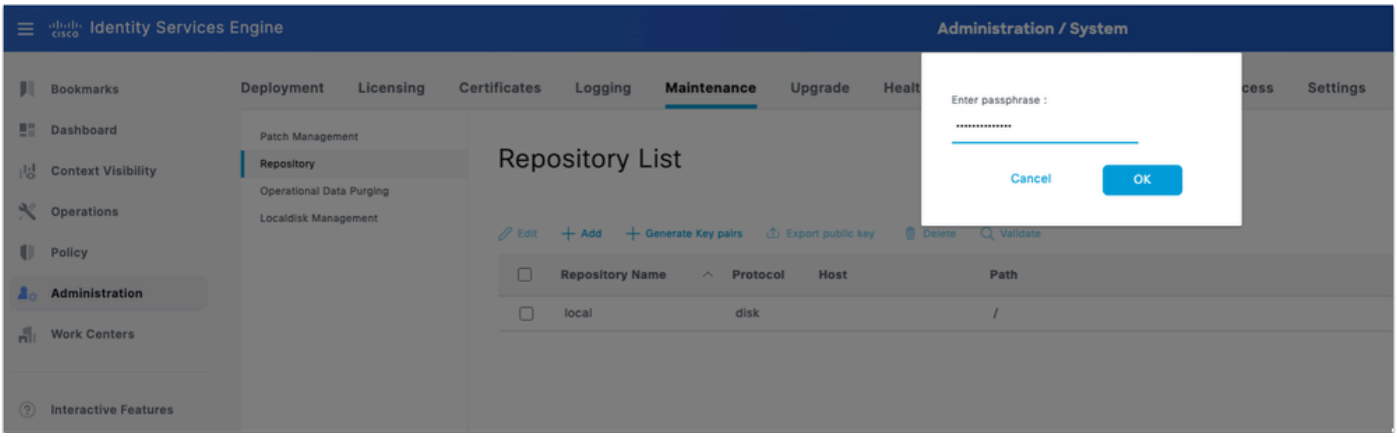
Configurar

Pré-configuração do ISE

1. Gerar pares de chaves no ISE: Efetue login na GUI do nó de administração principal. Navegue até Administração > Sistema > Manutenção > Repositório.

2. Em Lista de Repositórios, clique na opção Gerar Pares de Chaves.

3. Insira a senha (com mais de 13 caracteres) e clique em OK. Isso é necessário para proteger o par de chaves.



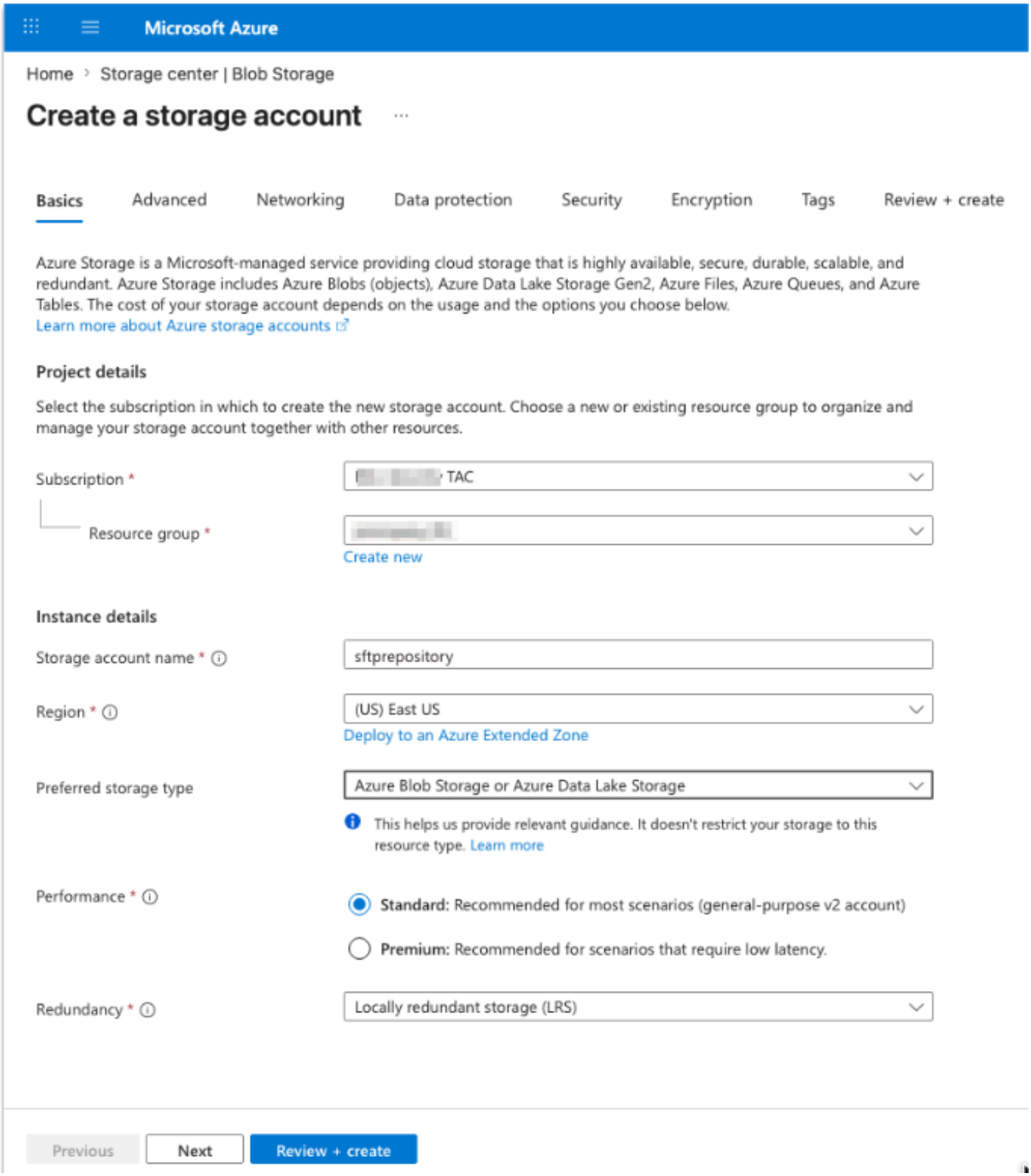
Gerar par de chaves no ISE

4. Clique em Exportar chave pública e faça o download da chave id_rsa.pub em seu computador (Certifique-se de que ela esteja salva para referências futuras).

Configuração do SFTP do Azure

1. Criar e Configurar a Conta de Armazenamento do Azure: Faça logon no Portal do Azure e navegue para Contas de armazenamento. Na guia Resources, clique em Create para criar uma nova conta de armazenamento. Preencha os detalhes:

Campo	Valor
Assinatura	Sua assinatura do Azure
Grupo de recursos	Selecionar existente ou criar novo
Nome da Conta de Armazenamento	Deve ser globalmente exclusivo
Região	Selecione sua região preferencial
Redundância	Local Redundant Storage (LRS) — aceitável para laboratório/não-produção

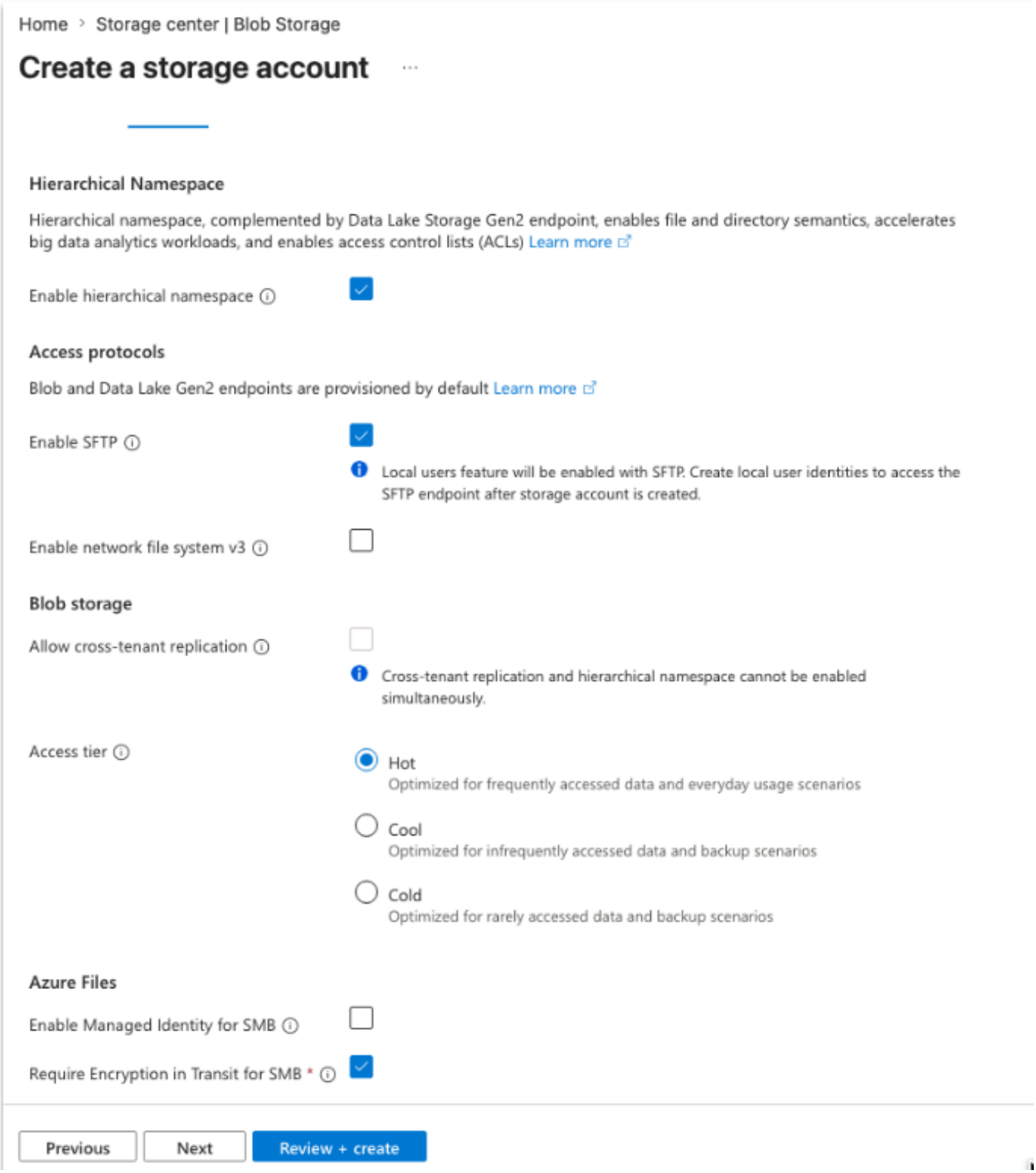


Criar uma Conta de Armazenamento

2. Clique em Próximo e, na guia Avançado, marque a caixa de seleção Ativar Namespace Hierárquico. Essa opção é obrigatória. O SFTP só pode ser habilitado para contas de namespace hierárquicas.

3. Marque a caixa de seleção Enable SFTP.

4. Deixe o resto das opções como padrão ou ajuste conforme suas necessidades.



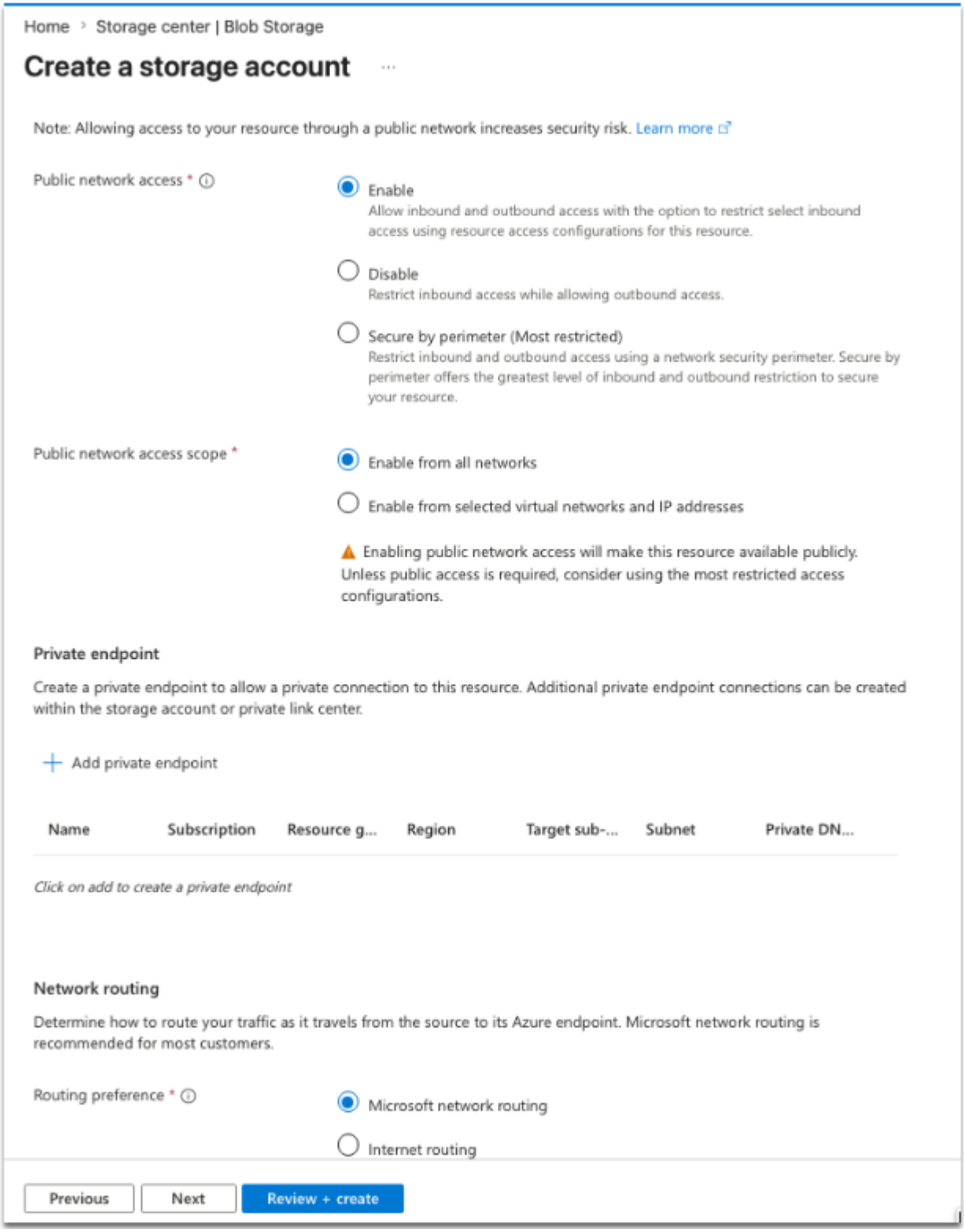
Configurar conta de Armazenamento

5. Clique em Próximo para configurar Rede.

6. Defina Acesso à rede para Habilitar acesso público de todas as redes.

7. Defina a preferência de Roteamento para o roteamento de rede da Microsoft.

Note: Note: Em ambientes de produção, considere restringir o acesso a intervalos de IP específicos (os endereços IP do nó ISE) usando regras de firewall na conta de armazenamento.



8. Clique em Próximo e deixe Proteção de Dados, Segurança e Criptografia como padrão. Nenhuma configuração adicional é necessária para implantações de laboratório ou padrão.

9. Clique em Revisar + criar. Depois que a validação for aprovada, clique em Criar.

10. Aguarde a conclusão da disponibilização e clique em Ir para o recurso.

11. Configurar o SFTP na Conta de Armazenamento do Azure: Em sua conta de armazenamento recém-criada, adicione um contêiner navegando até Armazenamento de dados > Contêineres > Adicionar contêiner

12. Forneça um nome de contêiner. Clique em Criar.

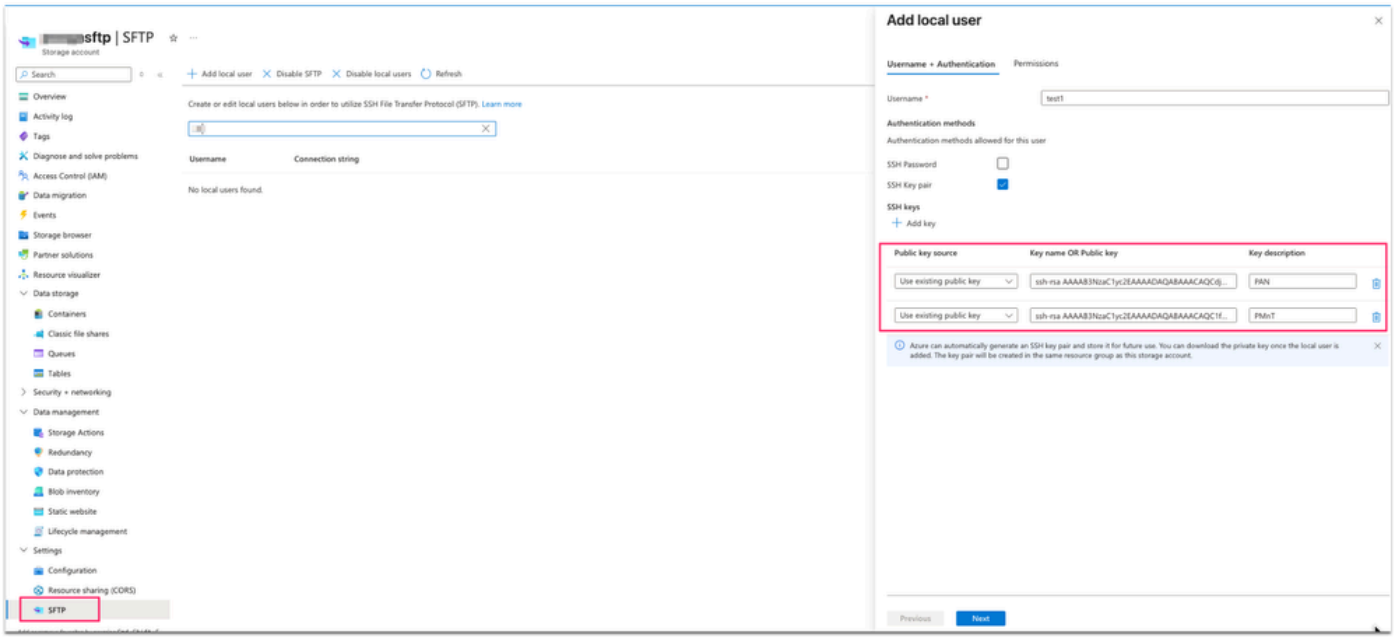
13. Adicione o usuário sftp navegando até Settings > SFTP no menu à esquerda. Clique em Adicionar usuário local e configure o seguinte:

Campo	Valor
Nome de usuário	Um nome descritivo
Método de autenticação	Par de chaves SSH — NÃO usar senha
origem de chave pública SSH	Usar chave existente (Gerada na etapa 1, a chave id_rsa.pub)

Note: Em uma implantação de vários nós, quando o PAN primário e o MnT primário são nós separados, o arquivo id_rsa.pub tem chaves públicas RSA do PAN primário e dos nós MnT primários.

14. Para usar a chave pública existente sob a opção de chaves SSH, abra o arquivo id_rsa.pub em um editor de texto de sua escolha e copie e cole a chave de nós (começando com ssh-rsa e terminando com root@your_node_name) separadamente clicando na opção Add key duas vezes.

```
Sample key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCdjUFU6QaMQfxuR/yzbw1QWZ8EwUJjN/COcNNMlkMOQE9flJQ6GoC
```



Adicionando chave pública no Azure

15. Clique em Permissões. Selecione inicialmente o Contêiner criado nesta etapa e defina a permissão para o contêiner como Ler, Gravar, Listar, Excluir e Criar.

16. Defina o diretório Home para a raiz do contêiner.

17. Salve o usuário.

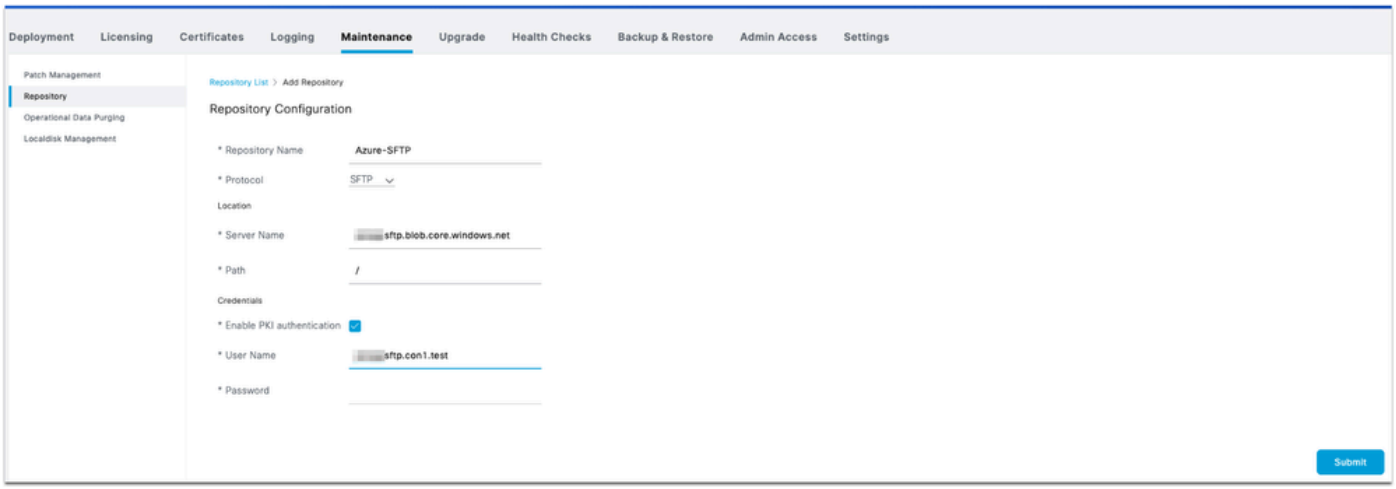
Configuração do repositório GUI do ISE

1. Navegue até Administração > Sistema > Manutenção > Repositório e clique em Adicionar. Preencha os campos da seguinte maneira:

Campo	Valor
Nome do Repositório	Um rótulo descritivo (como Azure-SFTP)
Protocolo	SFTP
Nome do servidor	<storage_account_name>.blob.core.windows.net
Caminho	/ (diretório raiz)

Autenticação	PKI
User Name	<storage_account_name>.<container_name>.<sftp_local_username>
Senha	Deixar em branco

2. Clique em Enviar para salvar o repositório.



Configuração do repositório SFTP do ISE

---

aviso: A chave de host do servidor sftp deve ser adicionada por meio da CLI usando o comando executável crypto host_key add antes que este repositório possa ser usado. Certifique-se também de que a string da chave do host corresponda ao nome do host usado na URL da configuração do repositório. Para acessar o repositório habilitado para PKI, gere pares de chaves a partir da GUI e exporte a chave pública para sua máquina local. Copie essa chave pública no servidor SFTP habilitado para PKI e adicione-a ao arquivo 'authorized_keys'.

---

3. Efetue login nos nós Principal admin e Principal monitoring e adicione a chave do host de criptografia usando o comando crypto host_key and host <sftp server>. Verifique se o nó ISE pode resolver o nome de host sftp.

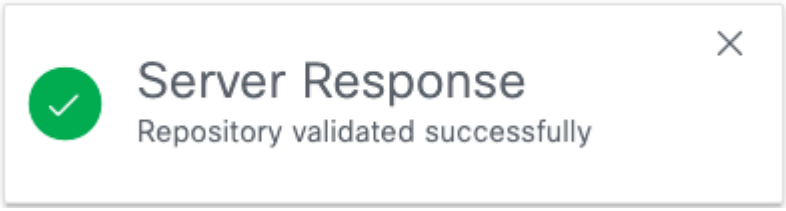
<#root>

```
isenode1/iseadmin#
```

crypto host_key add host xxxxxsftp.blob.core.windows.net

```
host key fingerprint added
# Host xxxxxsftp.blob.core.windows.net found: line 1
xxxxxsftp.blob.core.windows.net RSA SHA256:sP18dIvbSZgtEa5a2ea+Fy4P54Wd2ocEkToBq6xG74g
```

4. Volte para a GUI do ISE em Repository (Repositório) e selecione o repositório recém-criado e clique em Validate. Repositório validado com êxito.



Validação de repositório bem-sucedida

Note: A opção de validação do repositório valida a configuração do repositório apenas no nó Administrador principal.

Note: No caso do repositório SFTP criado com chave pública RSA, os repositórios criados através da GUI não são replicados na CLI e os repositórios criados através da CLI não são replicados na GUI. Para configurar o mesmo repositório na CLI e na GUI, gere chaves públicas RSA na CLI e na GUI e exporte ambas as chaves para o servidor SFTP.

Configuração do repositório CLI do ISE

1. SSH na CLI (interface de linha de comando) do nó admin primário. Adicione a chave de criptografia em cada nó na implantação onde você deseja acessar o repositório SFTP baseado em PKI a partir da CLI.

2. Gerar chave pública rsa para CLI.

```
isenode1/iseadmin#crypto key generate rsa passphrase <passphrase>
```

3. Exporte o arquivo de chave pública gerado para o repositório do disco local (qualquer repositório ao qual você tenha acesso para fazer download do arquivo).

```
isenode1/iseadmin#crypto key export <give a name for this file> repository <repository name>
```

4. Baixe este arquivo do repositório e abra-o no editor de texto para copiar a chave pública para acesso CLI.

5. Carregue a chave pública SSH para o Azure, a mesma que a chave GUI adicionada na tela de criação de usuário local do SFTP do Azure (da Etapa 3).

6. Clique em Adicionar chave e Cole a chave pública SSH completa (no campo Chave pública SSH).

7. Opcionalmente, forneça uma descrição-chave (Por exemplo, ISE-CLI-Key).

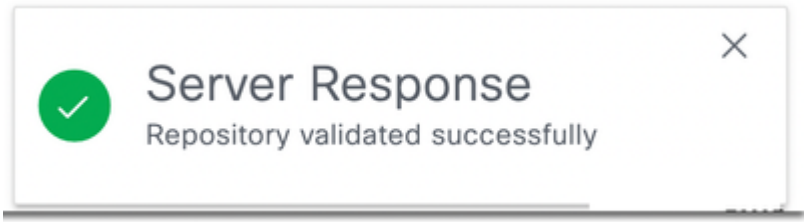
8. Clique em Próximo e em Salvar.

Verificar

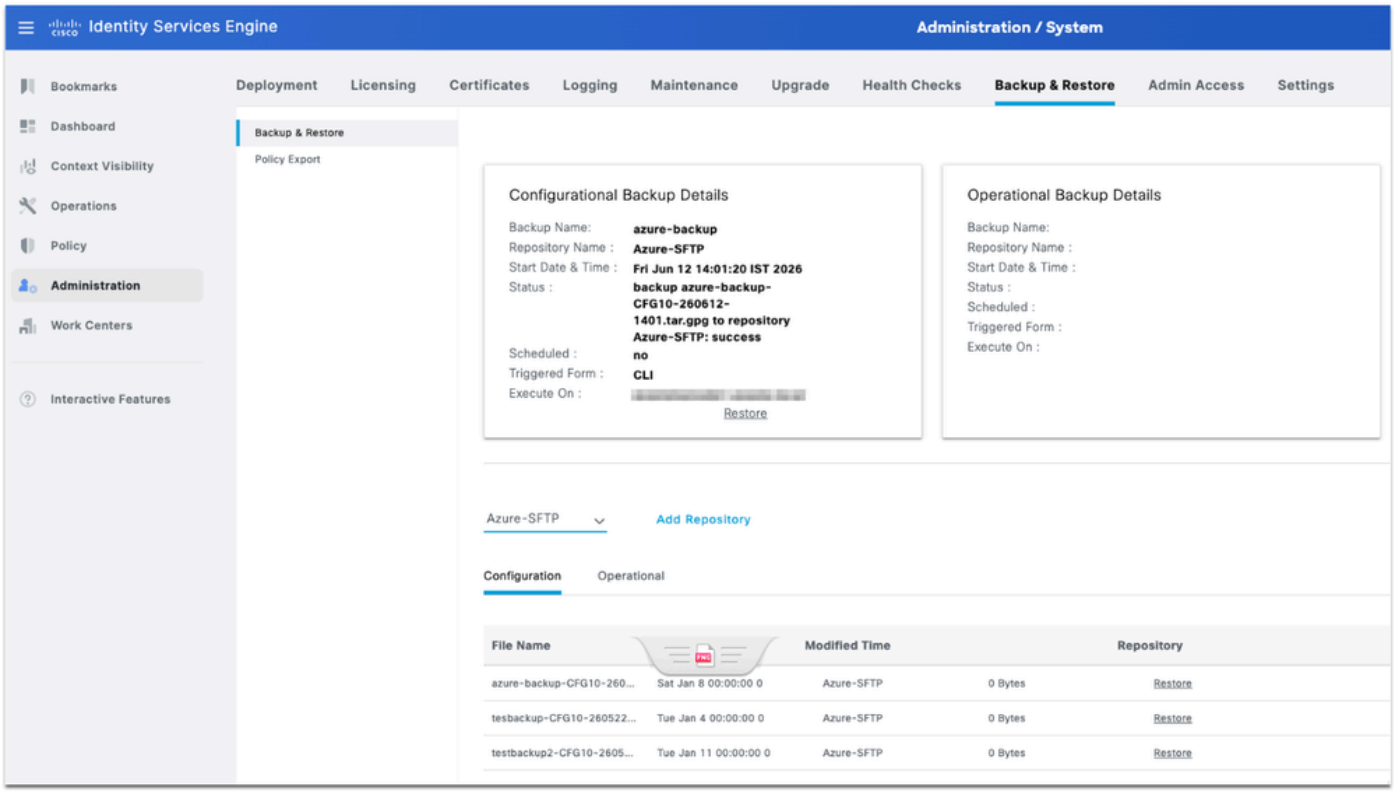
1. Verifique o acesso do CLI ao repositório sftp usando o comando "show repository <Nome do repositório>". Ele mostra os arquivos armazenados neste servidor sftp.

```
isenode1/iseadmin#show repository Azure-SFTP
SB-pk-260522-2236.tar.gpg
ops-OPS10-260525-1026.tar.gpg
```

2. Verifique o acesso da GUI ao repositório sftp navegando até Repository (Repositório) e selecione o repositório recém-criado e clique em Validate. Repositório validado com êxito.



3. Navegue até Administração > Sistema > Backup e Restauração . Faça um backup da configuração e vá para o final desta página, selecione o repositório SFTP e, em Configuração, o backup recente estará visível para restauração.

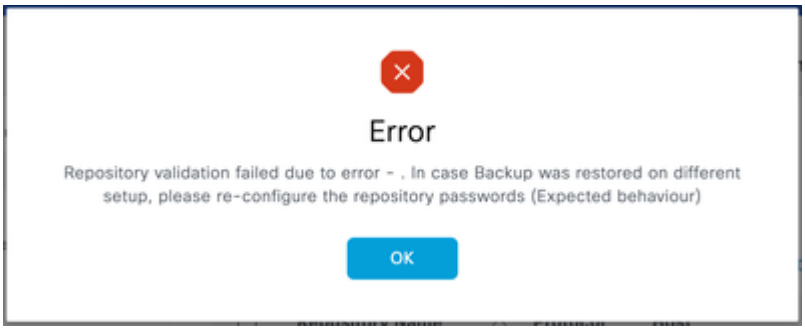


validação do repositório sftp

Note: Devido ao bug cosmético da Cisco IDCSCwu6863, o tamanho dos backups no armazenamento do Azure é visto aqui como 0 bytes, mas não há impacto funcional. Esses backups podem ser restaurados com êxito, se necessário.

Troubleshooting

1. Na GUI do ISE, a validação do repositório apresenta este erro:



Mensagem de erro

Resolução

Verifique se a chave pública correta é importada no servidor SFTP nas chaves SSH (consulte a Etapa 2 de Configurar SFTP na Conta de Armazenamento do Azure). Esse erro ocorrerá se o usuário tiver gerado um novo par de chaves novamente na GUI após a validação bem-sucedida do repositório.

2. Validação do repositório de GUI bem-sucedida, mas sem saída do comando show repository <sftp repository>.

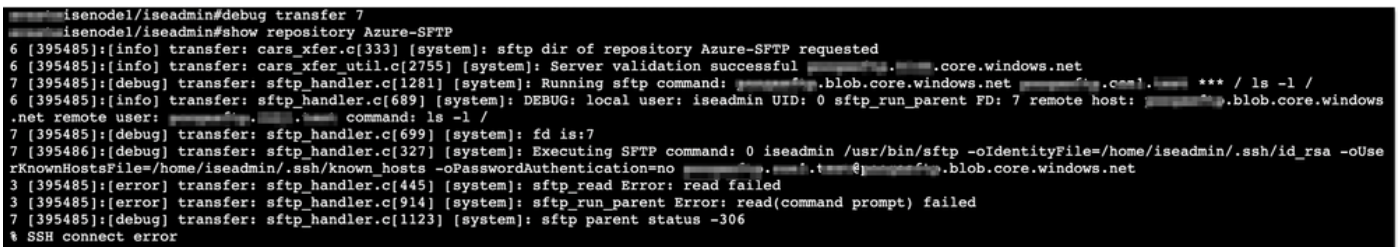
Captura de tela de erro

Resolução

Verifique se a chave pública RSA gerada pelo CLI foi adicionada na configuração ssh do Azure.

3. Para fazer troubleshooting adicional do problema do repositório SFTP, habilite o comando debug:

```
isenode1/iseadmin#debug transfer 7
```



Logs de depuração

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.