ISEでのAzure SFTP BLOBストレージリポジトリの構成およびトラブルシューティング

内容

はじめに

このドキュメントでは、Identity Services Engineで公開キーインフラストラクチャ(PKI)認証を使用してSFTPサーバーとしてAzure Blob Storageを構成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISEに関する一般的な知識
- ISEリポジトリの設定
- 公開キーインフラストラクチャ(PKI)認証

使用するコンポーネント

本書の情報は、次のソフトウェアのバージョンに基づくものです。

- ISE 3.3、3.4、3.5 VM on Azure
- Storage CenterにアクセスするためのAzureサブスクリプション

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

クラウドネイティブサービスであるAzure Blob Storage SFTPリポジトリは、簡単にデプロイでき、AzureベースのISE実装に最適です。これにより、オンプレミスの接続に関する問題が解消され、変化するストレージ要件に合わせて自動的に拡張されます。また、大規模なデータセットに対して高可用性と耐久性が確保されるため、インフラストラクチャを手動で管理する必要がなくなります。

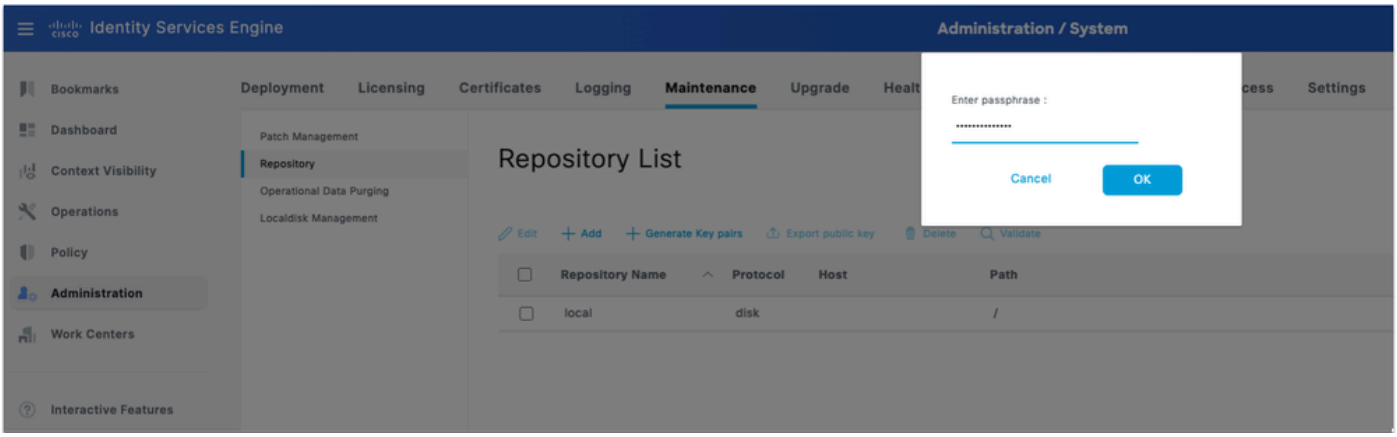
設定

ISEの事前設定

1. ISEでキーペアを生成します。プライマリ管理ノードのGUIにログインします。Administration > System > Maintenance > Repositoryの順に移動します。

2.「リポジトリ・リスト」で、「キー・ペアの生成」オプションをクリックします。

3. パスフレーズ（13文字を超える文字列）を入力して、OKをクリックします。 これは、キーペアを保護するために必要です。



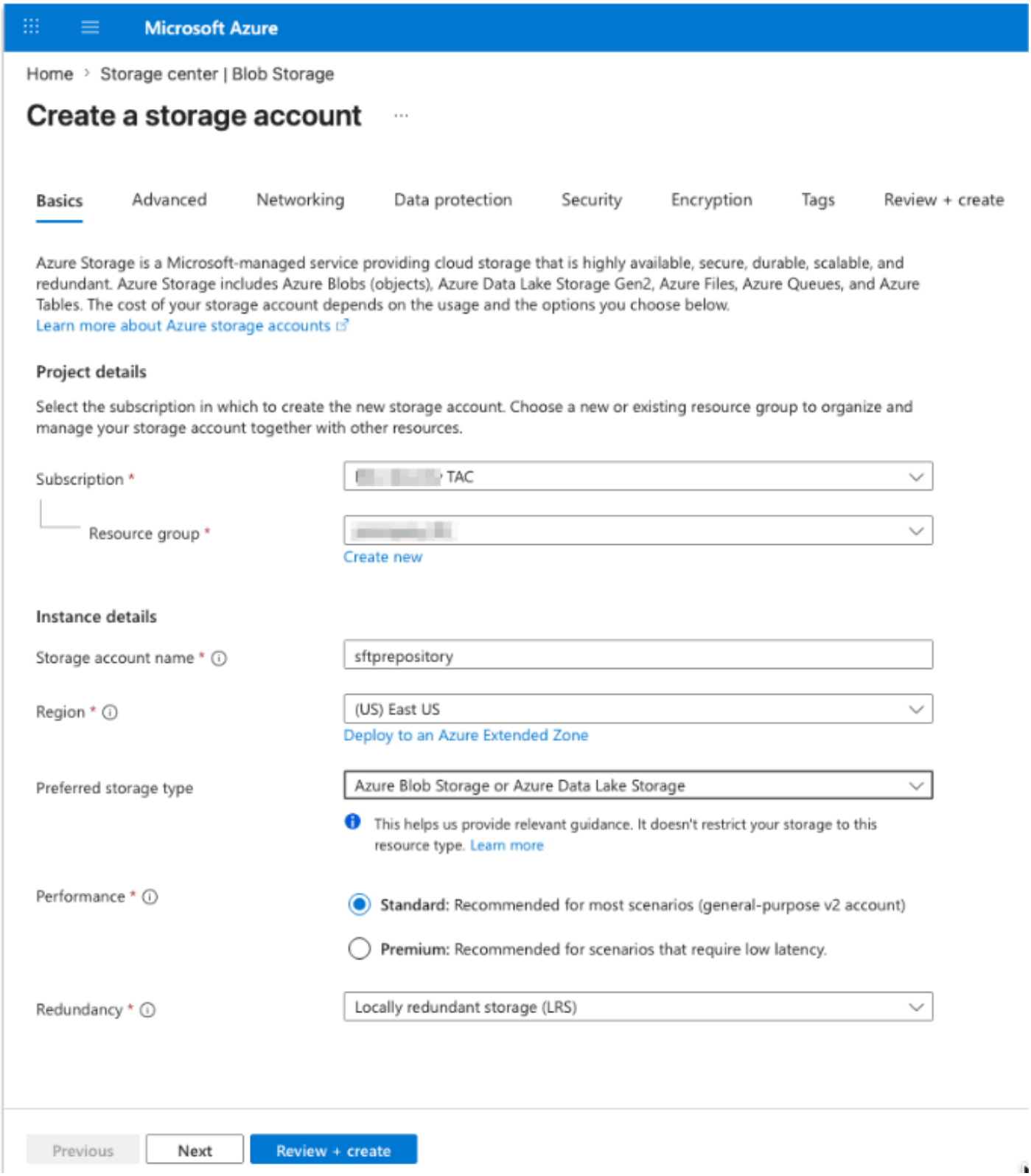
ISEでのキーペアの生成

4. Export public keyをクリックし、コンピュータにid_rsa.pubキーをダウンロードします（今後の参照用に保存しておいてください）。

Azure SFTP構成

1. Azureストレージアカウントを作成および構成する： Azureポータルにログインし、ストレージアカウントに移動します。ResourcesタブでCreateをクリックし、新しいストレージアカウントを作成します。詳細を入力します。

フィールド	値
定期購読	Azureサブスクリプション
リソースグループ	既存のものを選択または新規作成
ストレージアカウント名	グローバルに一意である必要がある
地域	お好みの地域を選択してください
冗長性	ローカル冗長ストレージ(LRS)：ラボ/非実稼働モデルで使用可能

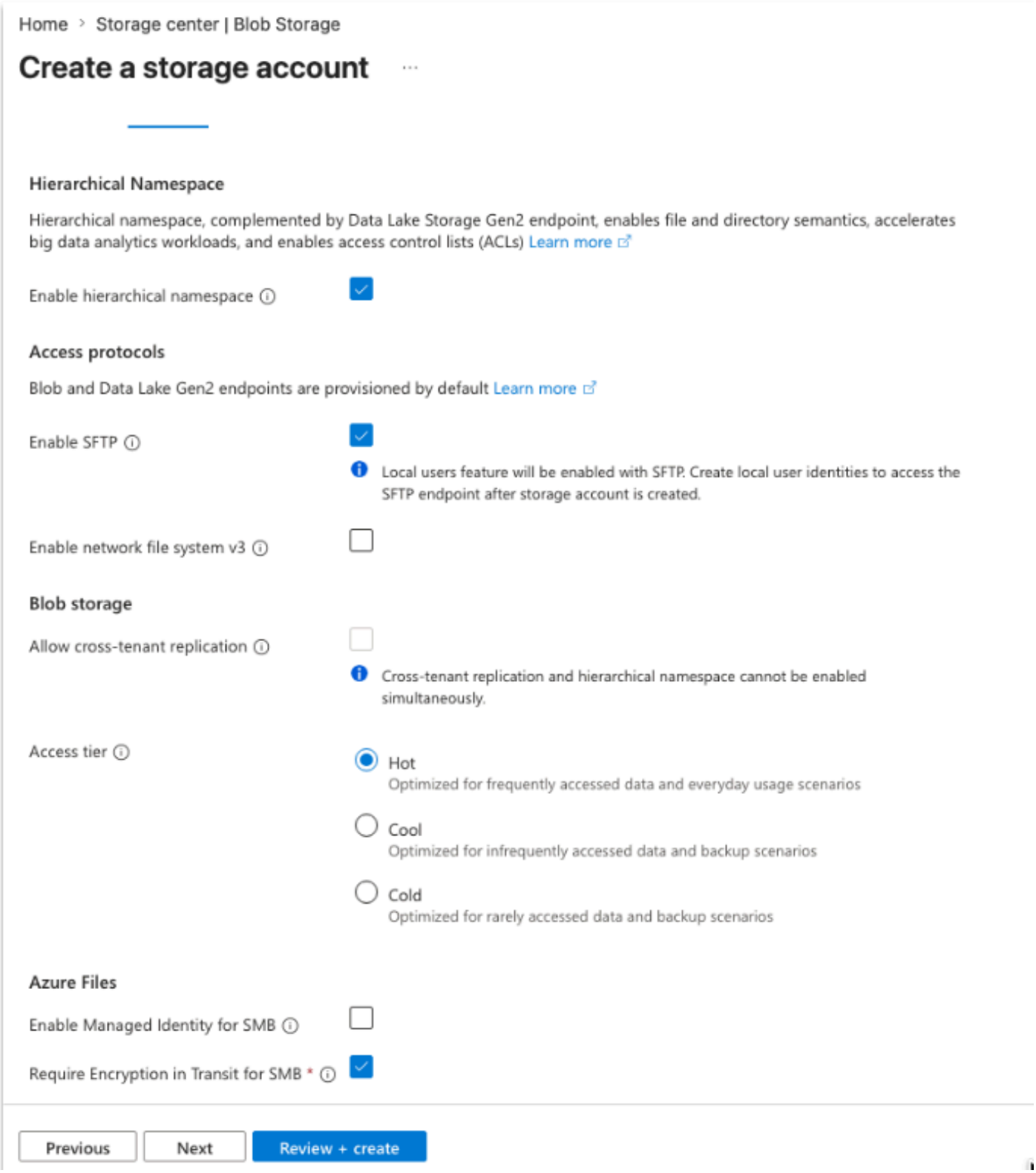


ストレージアカウントの作成

2. Nextをクリックし、AdvancedタブでEnable Hierarchical Namespaceチェックボックスを選択します。 このオプションは必須です。SFTPは、階層型名前空間アカウントに対してのみ有効にできます。

3. 「SFTPの有効化」チェックボックスを選択します。

4. 残りのオプションはデフォルトのままにするか、必要に応じて調整します。



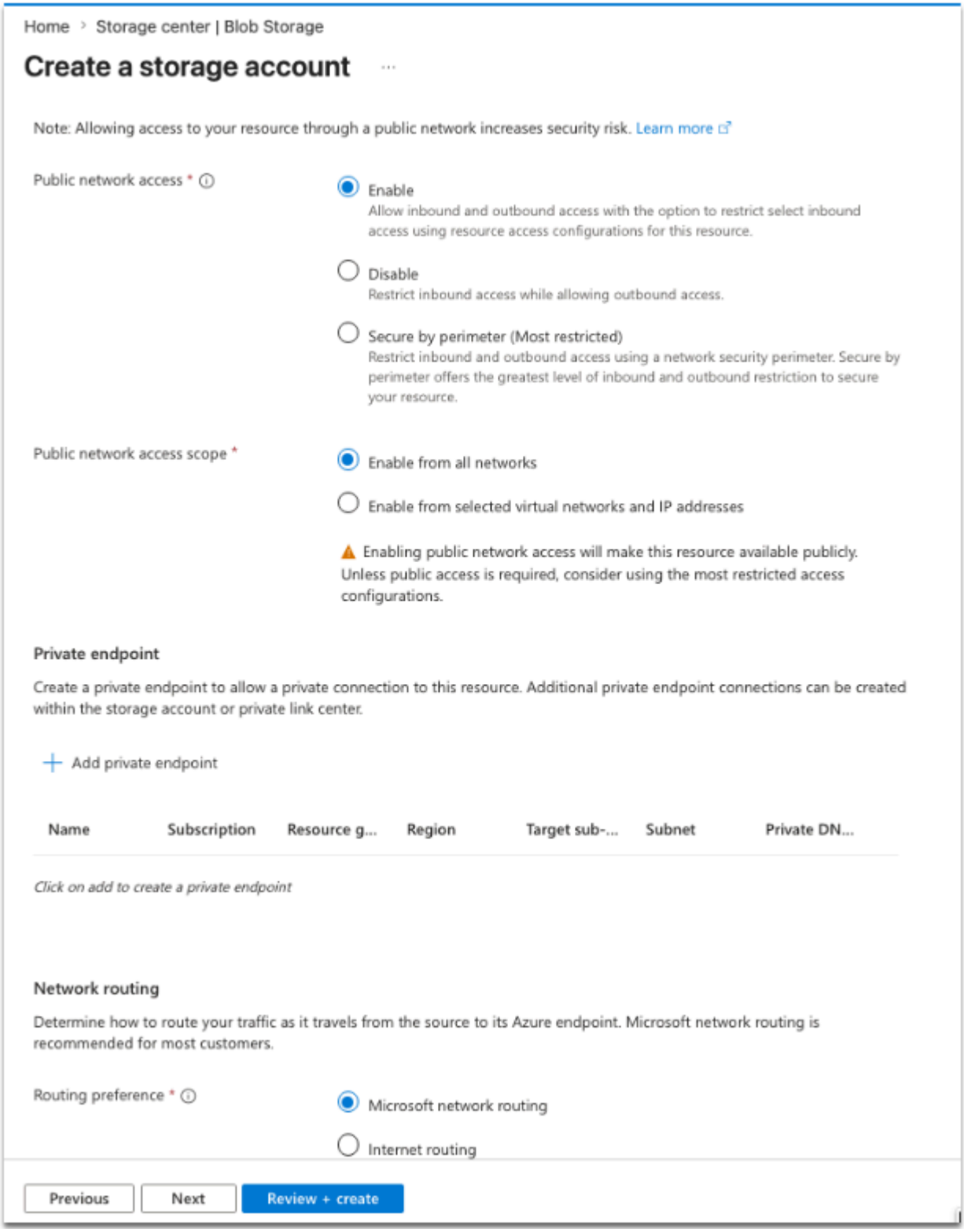
ストレージアカウントの構成

5. Nextをクリックして、Networkingを設定します。

6. Network accessをEnable public access from all networksに設定します。

7. Routing preferenceをMicrosoft network routingに設定します。

注：注：実稼働環境では、ストレージアカウントのファイアウォールルールを使用して、特定のIP範囲（ISEノードのIPアドレス）へのアクセスを制限することを検討してください。



8. Nextをクリックし、Data protection、Security、およびEncryptionをデフォルトのままにします。 ラボまたは標準の導入では、追加の設定は必要ありません。

9. 「レビュー+作成」をクリックします。検証に合格したら、Createをクリックします。

10. デプロイが完了するのを待ってから、Go to resourceをクリックします。

11. AzureストレージアカウントでSFTPを構成する：新しく作成したストレージアカウントで、データストレージ> コンテナー > コンテナーの追加に移動して、コンテナーを追加します

12. コンテナ名を入力します。[Create] をクリックします。

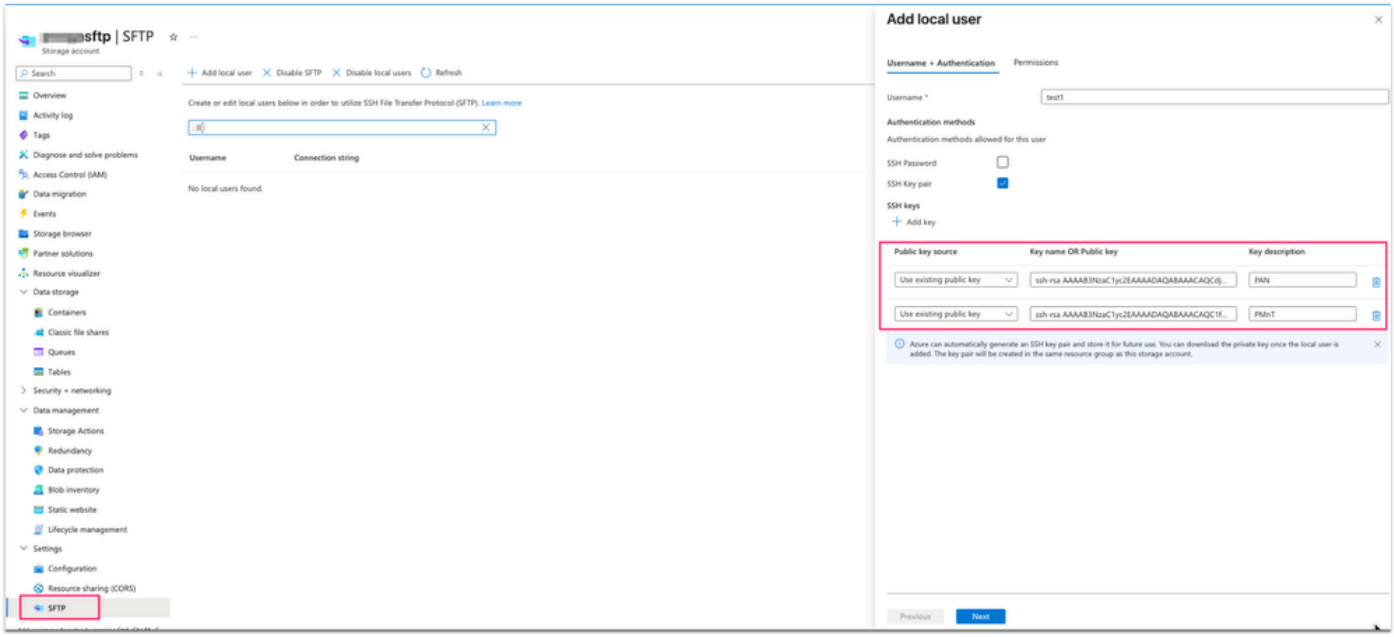
13. 左側のメニューでSettings > SFTPに移動して、sftpユーザを追加します。Add local userをクリックして、次のように設定します。

フィールド	値
ユーザ名	記述名
認証方式	SSHキーペア：パスワードを使用しない
SSH公開キーソース	既存のキーを使用（ステップ1で生成、id_rsa.pubキー）

注：マルチノード展開では、プライマリPANとプライマリMnTが別々のノードである場合、id_rsa.pubファイルにはプライマリPANとプライマリMnTの両方のノードからのRSA公開キーが含まれます。

14. SSHキーオプションで既存の公開キーを使用する場合は、任意のテキストエディタでid_rsa.pubファイルを開き、Add keyオプションを2回クリックして、両方のノードキー(ssh-rsaで始まり、root@your_node_nameで終わる)を個別にコピーペーストします。

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



Azureに公開キーを追加しています

15. Permissionsをクリックします。最初にこの手順で作成したコンテナを選択し、コンテナの権限を読み取り、書き込み、リスト、削除、作成に設定します。

16. ホームディレクトリをコンテナのルートに設定します。

17. ユーザを保存します。

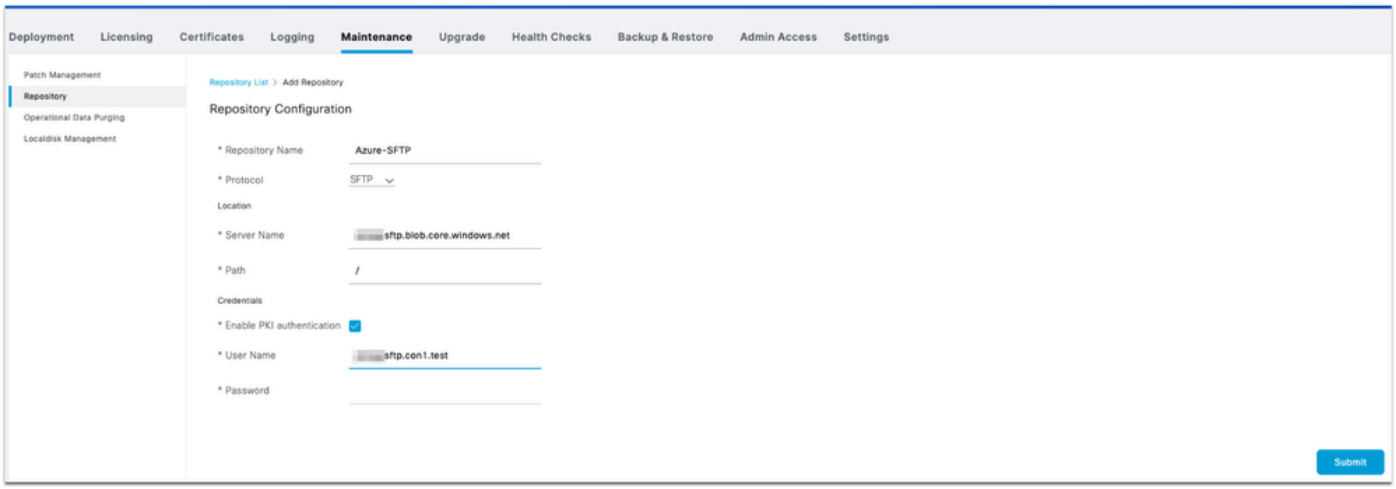
ISE GUIリポジトリの設定

1. Administration > System > Maintenance > Repositoryに移動し、Addをクリックします。次のようにフィールドに入力します。

フィールド	値
リポジトリ名	説明ラベル（Azure-SFTPなど）
プロトコル	SFTP
サーバ名	<storage_account_name>.blob.core.windows.net
パス	/（ルートディレクトリ）

認証	PKI
ユーザ名	<storage_account_name>.<container_name>.<sftp_local_username>
[パスワード（Password）]	空白のままにします。

2. Submitをクリックして、リポジトリを保存します。



ISE SFTPリポジトリの設定

警告：このリポジトリを使用するには、CLIでcrypto host_key add実行可能コマンドを使用して、sftpサーバのホストキーを追加する必要があります。また、ホストのキー文字列が、リポジトリ設定のURLで使用されているホスト名と一致していることを確認します。PKI対応リポジトリにアクセスするには、GUIからキーペアを生成し、公開キーをローカルマシンにエクスポートします。この公開キーをPKI対応SFTPサーバにコピーし、「authorized_keys」ファイルに追加します。

---

3. プライマリ管理ノードとプライマリ監視ノードの両方にログインし、crypto host_key ad host <sftp server >コマンドを使用して暗号化ホストキーを追加します。ISEノードがsftpホスト名を解決できることを確認します。

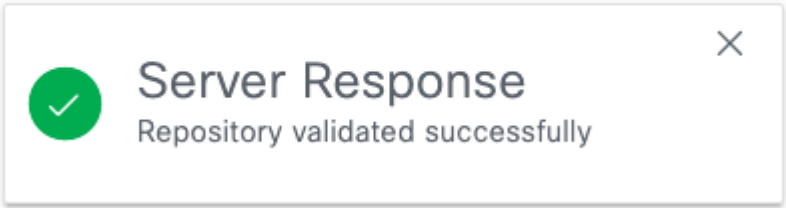
<#root>

```
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. ISE GUIのRepositoryの下に戻り、新しく作成したリポジトリを選択して、Validateをクリックします。リポジトリが正常に検証されました。



正常なリポジトリ検証

注意：リポジトリ検証オプションは、プライマリ管理ノードでのみリポジトリ構成を検証します。

注：RSA公開キーを使用して作成されたSFTPリポジトリの場合、GUIを使用して作成されたリポジトリはCLIで複製されず、CLIを使用して作成されたリポジトリはGUIで複製されません。CLIとGUIで同じリポジトリを設定するには、CLIとGUIの両方でRSA公開キーを生成し、両方のキーをSFTPサーバにエクスポートします。

ISE CLIリポジトリの設定

1. プライマリ管理ノードのCLI（コマンドラインインターフェイス）にSSH接続します。CLIからPKIベースのSFTPリポジトリにアクセスする展開内の各ノードに暗号キーを追加します。

2. CLIのrsa公開キーを生成します。

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

3. 生成された公開キーファイルをローカルディスクリポジトリ（ファイルをダウンロードするためのアクセス権を持つ任意のリポジトリ）にエクスポートします。

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

4. リポジトリからこのファイルをダウンロードし、テキストエディタで開いてCLIアクセス用の公開キーをコピーします。

5. SSH公開キーをAzureにアップロードします。これは、Azure SFTPローカルユーザー作成画面で追加したGUIキーと同じです（手順3から）。

6. Add keyをクリックし、完全なSSH公開キーを(SSH public keyフィールドに)ペーストします。

7. オプションで、キーの説明を入力します(例：ISE-CLI-Key)。

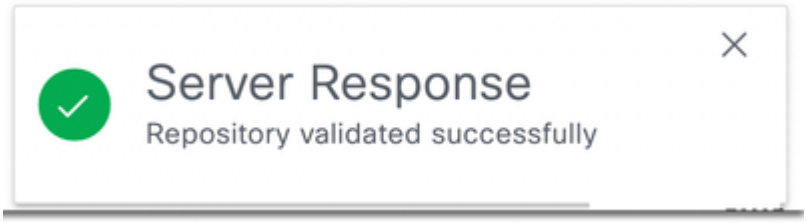
8. Nextをクリックし、Saveをクリックします。

確認

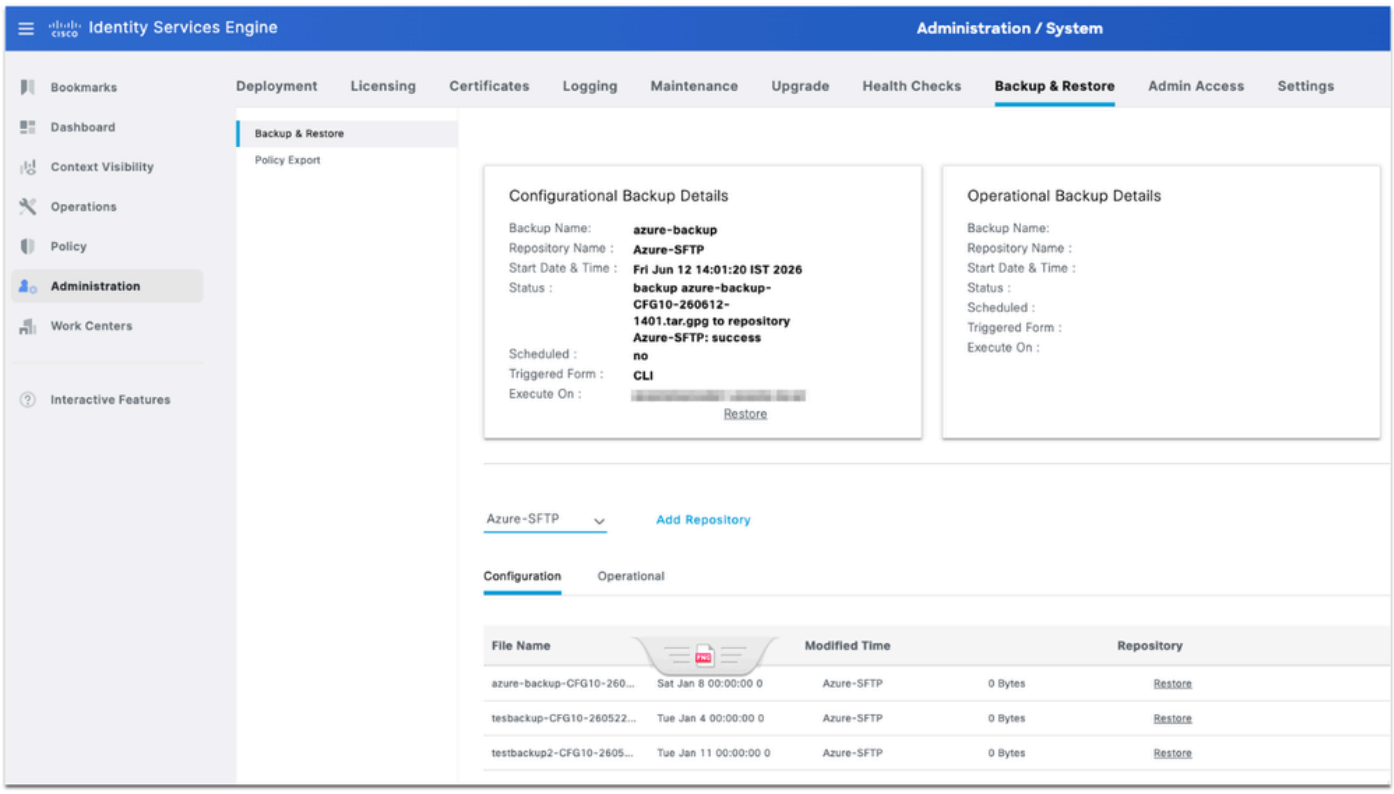
1. show repository <Repository name>コマンドを使用して、sftpリポジトリへのCLIアクセスを確認します。 このsftpサーバに保存されているファイルが表示されます。

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

2. Repositoryに移動して、新しく作成されたリポジトリを選択し、Validateをクリックして、sftpリポジトリへのGUIアクセスを確認します。リポジトリが正常に検証されました。



3. Administration > System > Backup and Restoreの順に移動します。設定のバックアップを作成し、このページの下部に移動します。SFTPリポジトリを選択し、設定の下で、最新のバックアップを復元できます。

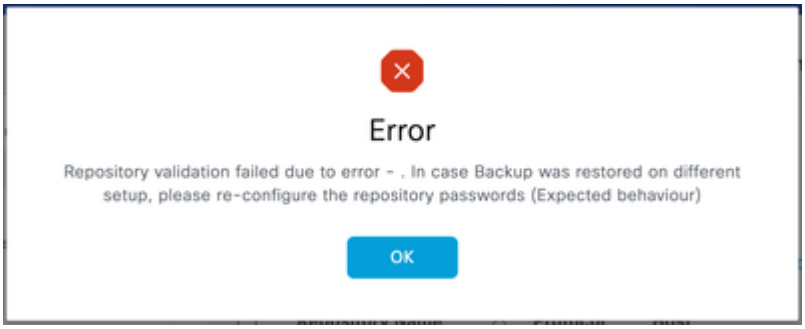


sftpリポジトリの検証

注：表面的なCisco Bug IDCSCwu68863の問題により、Azureストレージ上のバックアップのサイズは0バイトと表示されますが、機能的な影響はありません。これらのバックアップは、必要に応じて正常に復元できます。

トラブルシュート

1. ISE GUIでリポジトリ検証を行うと、次のエラーが表示されます。



エラー メッセージ

解決策

正しい公開キーがSSHキーでSFTPサーバーにインポートされていることを確認します（「AzureストレージアカウントでのSFTPの構成」の手順2を参照）。 このエラーは、リポジトリの検証が成功した後に、ユーザがGUIで新しいキーペアを再度生成した場合に発生します。

2. GUIリポジトリの検証は成功しましたが、show repository <sftp repository>コマンドからの出力がありません。

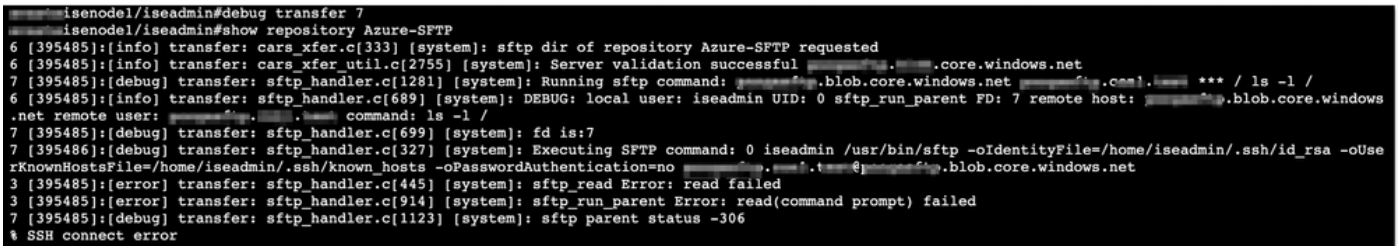
エラースクリーンショット

解決策

CLIから生成されたRSA公開キーがAzure ssh構成に追加されていることを確認します。

3. SFTPリポジトリの問題をさらにトラブルシューティングするには、debugコマンドを有効にします。

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



デバッグログ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。