Azure SFTP Blob Storage Repository auf der ISE konfigurieren und Fehlerbehebung durchführen

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Azure Blob Storage als SFTP-Server mit Public Key Infrastructure-Authentifizierung mit Identity Services Engine beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Allgemeine ISE-Kenntnisse
- ISE-Repository-Konfiguration
- PKI-Authentifizierung (Public Key Infrastructure)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- ISE 3.3, 3.4, 3.5 VM auf Azure
- Azure-Abonnement für den Zugriff auf Storage Center

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Als Cloud-nativer Service ist das Azure Blob Storage SFTP-Repository einfach bereitzustellen und ideal für Azure-basierte ISE-Implementierungen. Es beseitigt Verbindungsprobleme vor Ort, lässt sich automatisch skalieren, um schwankenden Speicheranforderungen gerecht zu werden, und gewährleistet hohe Verfügbarkeit und Dauerhaftigkeit für große Datensätze. Gleichzeitig entfällt das manuelle Infrastrukturmanagement.

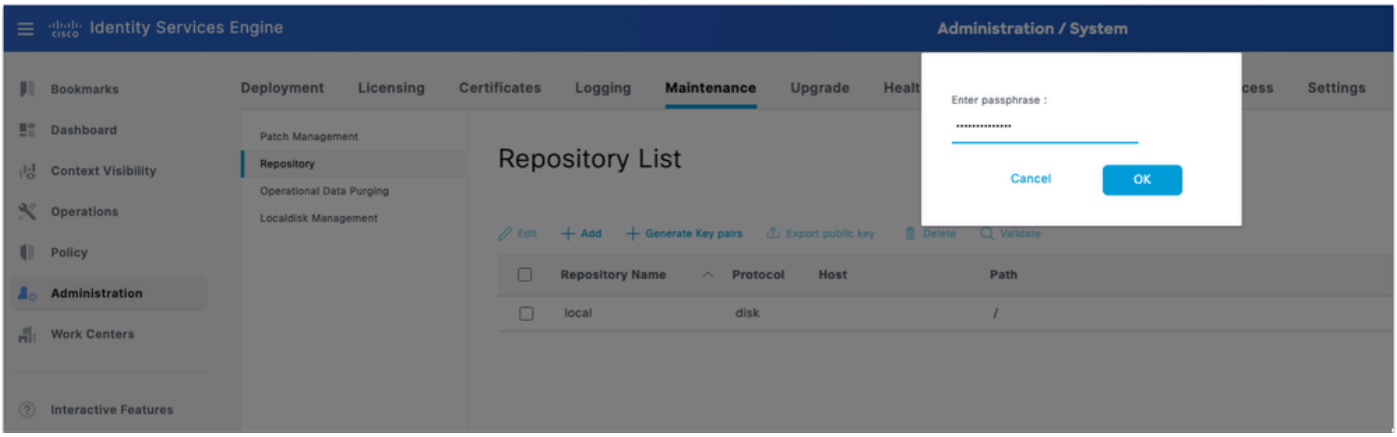
Konfigurieren

ISE-Vorkonfiguration

1. Schlüsselpaare auf der ISE generieren: Melden Sie sich bei der GUI des primären Admin-Knotens an. Navigieren Sie zu Administration > System > Maintenance > Repository.

2. Klicken Sie unter Repository-Liste auf die Option Schlüsselpaare generieren.

3. Geben Sie eine Passphrase (mehr als 13 Zeichen) ein, und klicken Sie auf OK. Dies ist erforderlich, um das Schlüsselpaar zu schützen.



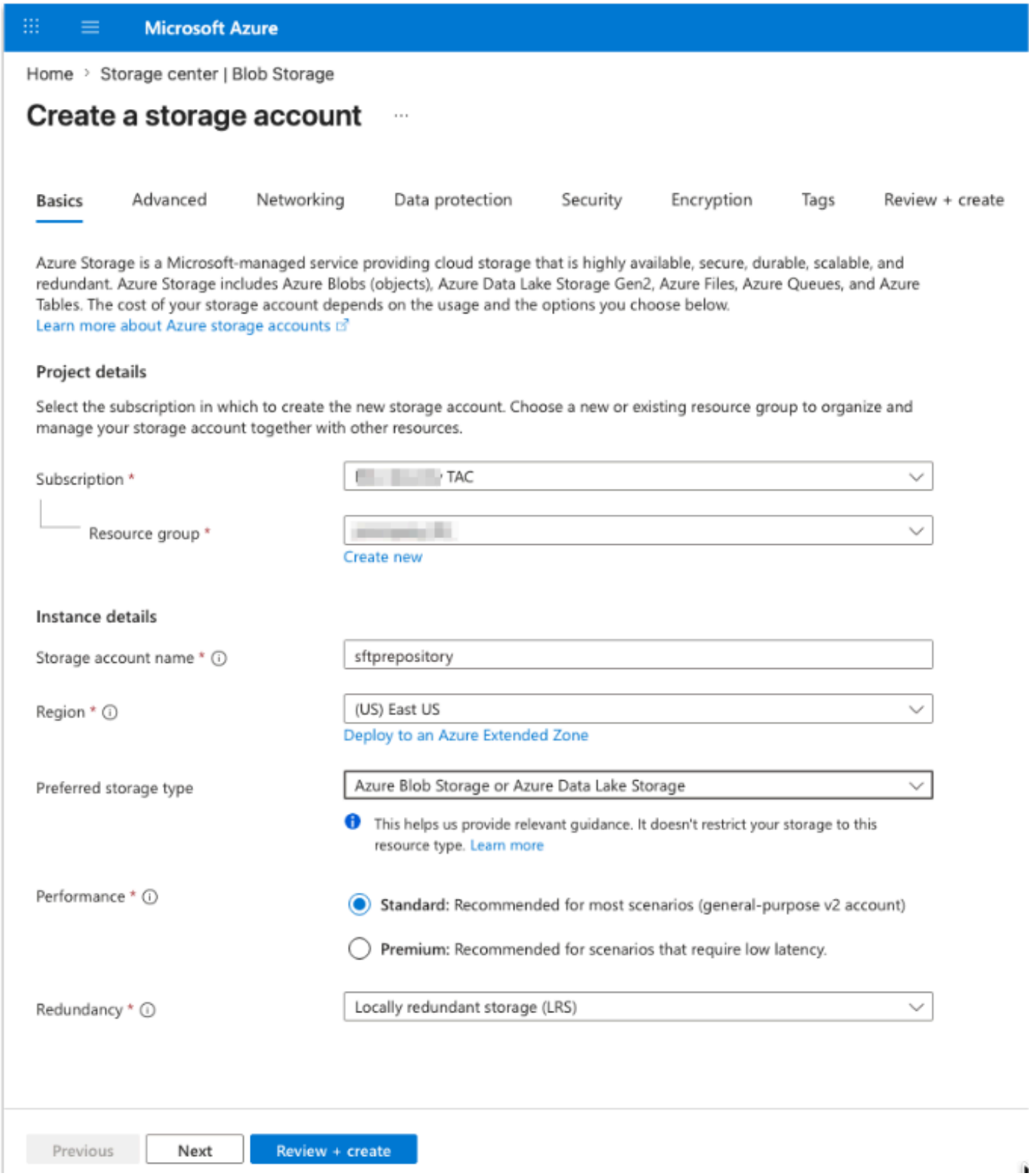
Schlüsselpaar auf ISE generieren

4. Klicken Sie auf Öffentlichen Schlüssel exportieren und laden Sie den id_rsa.pub-Schlüssel auf Ihren Computer herunter (stellen Sie sicher, dass dieser für zukünftige Referenzen gespeichert wird).

Azure SFTP-Konfiguration

1. Azure-Speicherkonto erstellen und konfigurieren: Melden Sie sich beim Azure-Portal an, und navigieren Sie zu Speicherkonten. Klicken Sie auf der Registerkarte Ressourcen auf Erstellen, um ein neues Speicherkonto zu erstellen. Füllen Sie die Felder aus:

Feld	Wert
Abonnement	Ihr Azure-Abonnement
Ressourcengruppe	Vorhandenen auswählen oder neuen erstellen
Name des Speicherkontos	Global einzigartig
Region	Wählen Sie Ihre bevorzugte Region aus
Redundanz	Lokal redundanter Speicher (LRS) - geeignet für Labor/Nicht-Hersteller

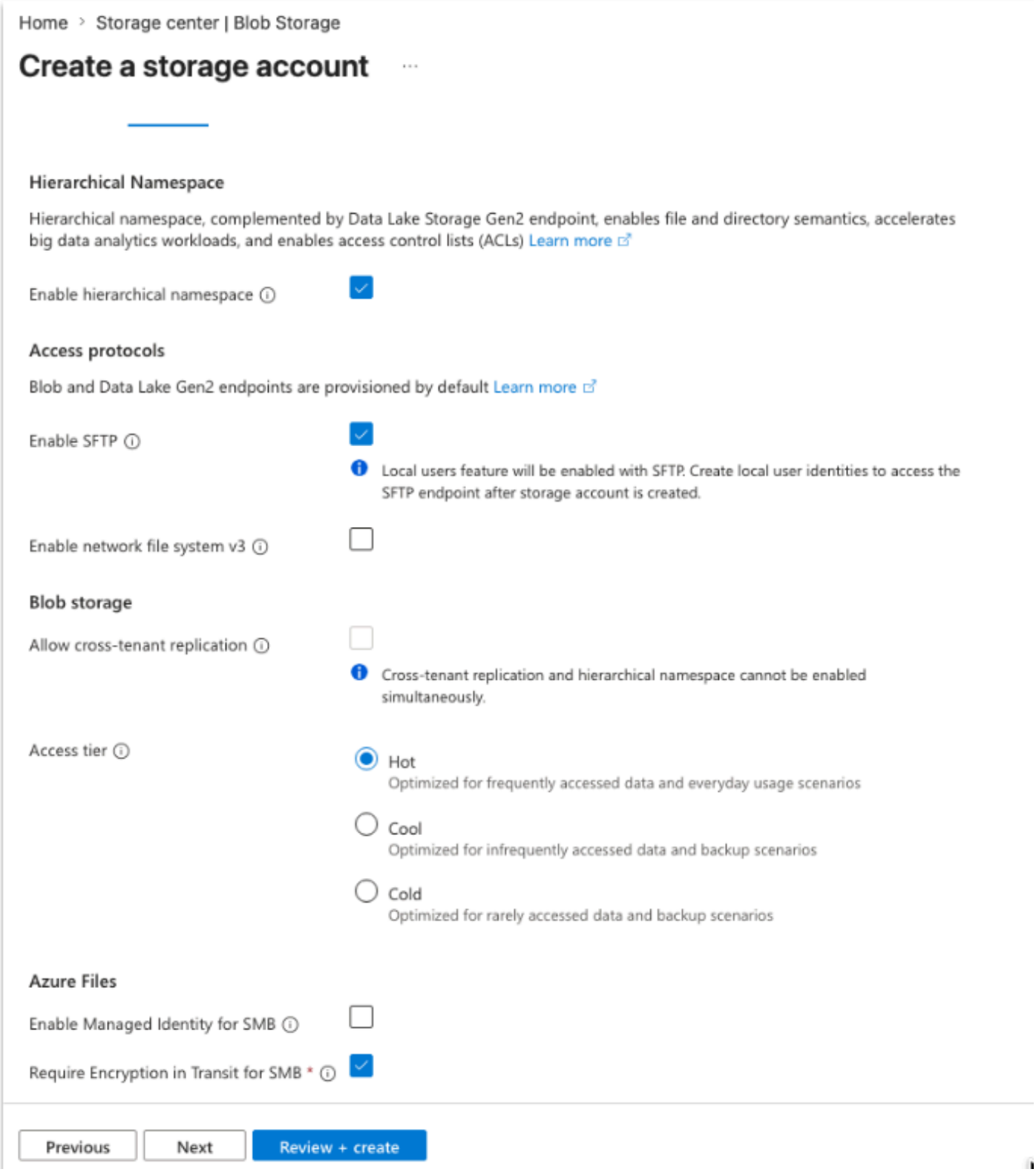


Speicherkonto erstellen

2. Klicken Sie auf Weiter und aktivieren Sie auf der Registerkarte Erweitert das Kontrollkästchen Hierarchischen Namespace aktivieren. Diese Option ist obligatorisch. SFTP kann nur für hierarchische Namespacekonten aktiviert werden.

3. Aktivieren Sie das Kontrollkästchen SFTP aktivieren.

4. Belassen Sie die restlichen Optionen als Standard oder gemäß Ihren Anforderungen angepasst.



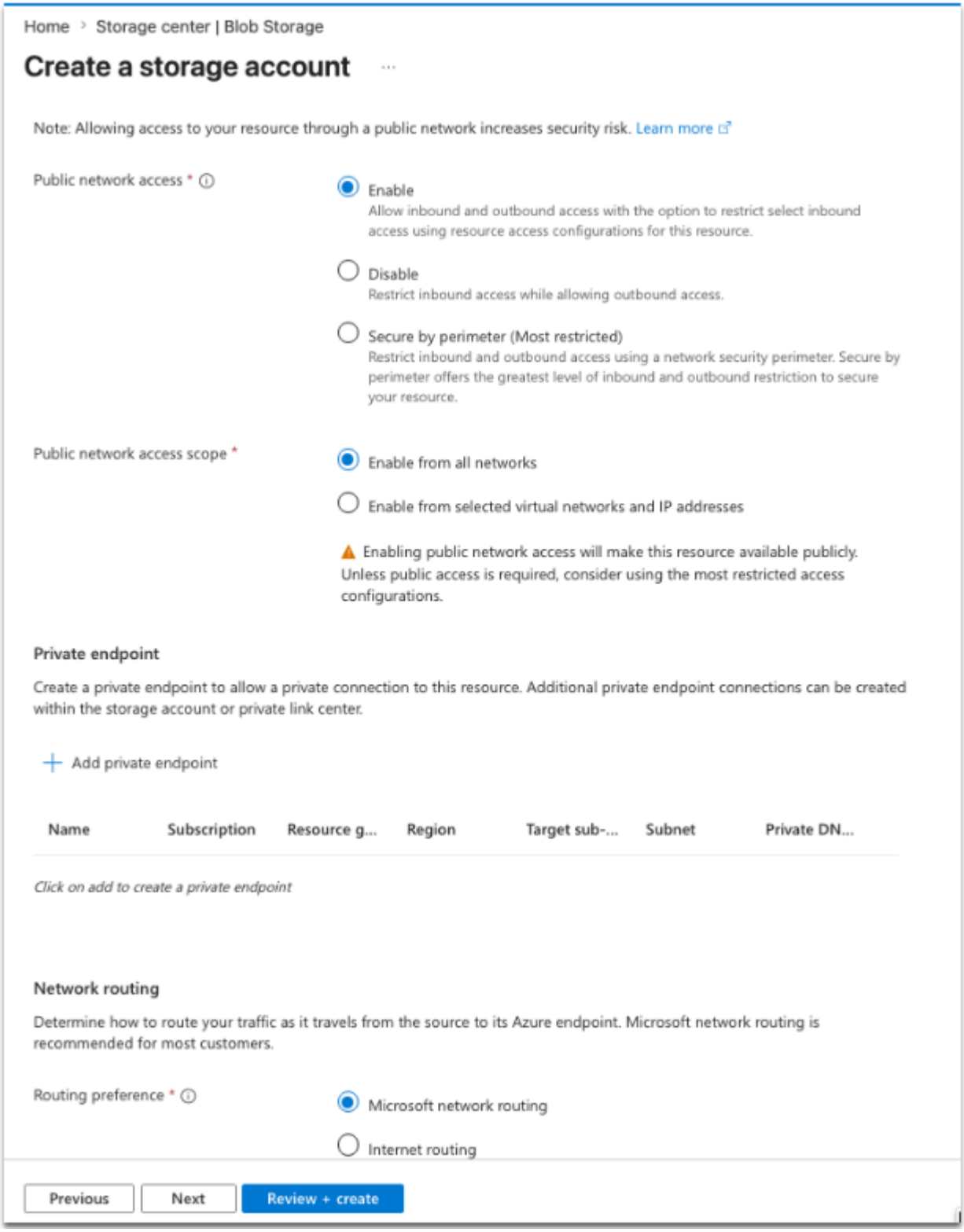
Speicherkonto konfigurieren

5. Klicken Sie auf Weiter, um Networking zu konfigurieren.

6. Legen Sie Netzwerkzugriff auf öffentlichen Zugriff aus allen Netzwerken fest.

7. Legen Sie die Routing-Voreinstellung auf Microsoft-Netzwerk-Routing fest.

Anmerkung: Anmerkung: Erwägen Sie in Produktionsumgebungen, den Zugriff auf bestimmte IP-Bereiche (die ISE-Knoten-IP-Adressen) mithilfe von Firewall-Regeln auf dem Speicherkonto zu beschränken.



Netzwerkeinstellungen

8. Klicken Sie auf Weiter und belassen Sie Datenschutz, Sicherheit und Verschlüsselung als Standard. Für Übungs- oder Standardbereitstellungen ist keine zusätzliche Konfiguration erforderlich.

9. Klicken Sie auf Prüfen + erstellen. Klicken Sie nach der Validierung auf Erstellen.

10. Warten Sie, bis die Bereitstellung abgeschlossen ist, und klicken Sie dann auf Zur Ressource wechseln.

11. Konfigurieren Sie SFTP auf dem Azure-Speicherkonto: Fügen Sie in Ihrem neu erstellten Speicherkonto einen Container hinzu, indem Sie zu Datenspeicher > Container > Container hinzufügen navigieren.

12. Geben Sie einen Containernamen an. Klicken Sie auf Erstellen.

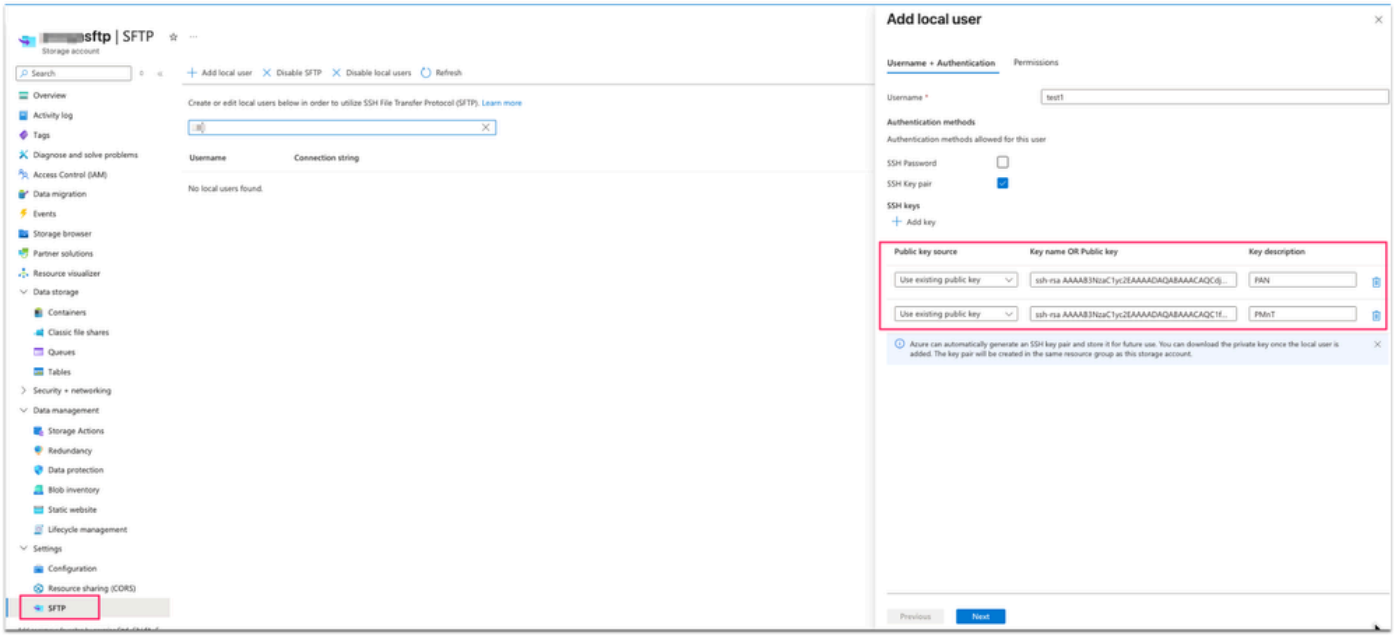
13. Fügen Sie einen SFTP-Benutzer hinzu, indem Sie im linken Menü zu Settings > SFTP (Einstellungen > SFTP) navigieren. Klicken Sie auf Lokalen Benutzer hinzufügen, und konfigurieren Sie Folgendes:

Feld	Wert
Benutzername	Einen beschreibenden Namen
Authentifizierungsmethode	SSH-Schlüsselpaar - Kennwort NICHT verwenden
Quelle des öffentlichen SSH-Schlüssels	Vorhandenen Schlüssel verwenden (Generiert in Schritt 1, der Schlüssel id_rsa.pub)

Anmerkung: Wenn in einer Bereitstellung mit mehreren Knoten das primäre PAN und das primäre MnT separate Knoten sind, verfügt die Datei "id_rsa.pub" über öffentliche RSA-Schlüssel sowohl vom primären PAN als auch vom primären MnT-Knoten.

14. Um den vorhandenen öffentlichen Schlüssel unter SSH keys Option zu verwenden, öffnen Sie die Datei id_rsa.pub in einem Texteditor Ihrer Wahl und kopieren Sie die beiden Knoten Schlüssel (beginnend mit ssh-rsa und endet mit root@your_node_name) separat durch Klicken Schlüssel hinzufügen Option zweimal.

```
Sample key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCdjUFU6QaMQfxuR/yzbw1QWZ8EwUJjN/C0cNNMlkMOQE9flJQ6GoC
```



Hinzufügen eines öffentlichen Schlüssels in Azure

15. Klicken Sie auf Berechtigungen. Wählen Sie zunächst den in diesem Schritt erstellten Container aus, und legen Sie die Berechtigung für den Container auf Lesen, Schreiben, Auflisten, Löschen und Erstellen fest.

16. Legen Sie das Home-Verzeichnis auf den Stamm des Containers fest.

17. Speichern Sie den Benutzer.

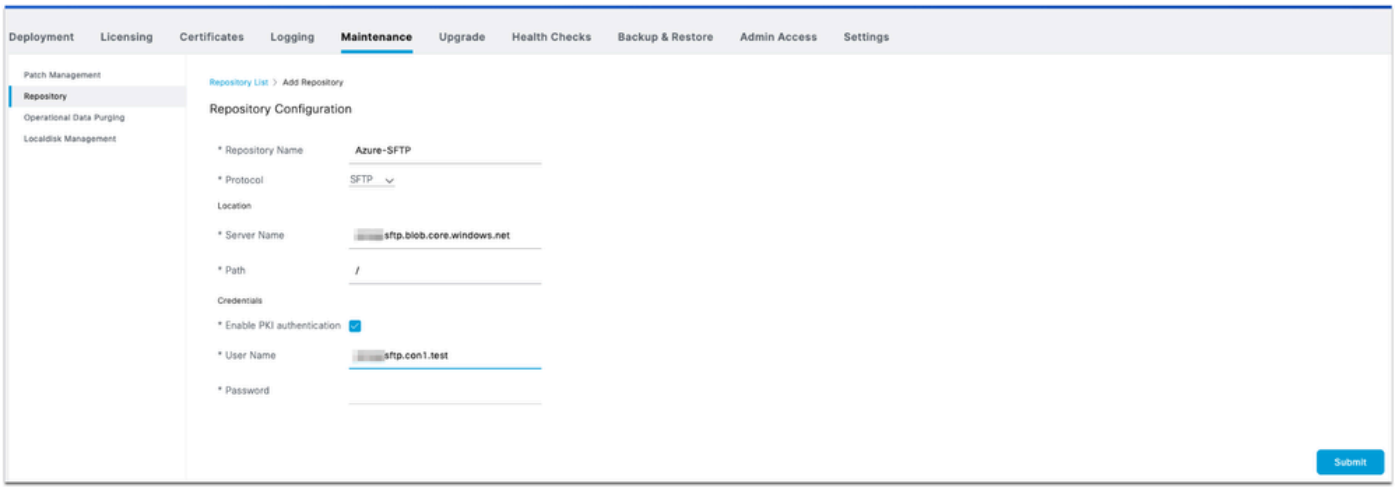
Konfiguration des ISE-GUI-Repository

1. Navigieren Sie zu Administration > System > Maintenance > Repository, und klicken Sie auf Add (Hinzufügen). Füllen Sie die Felder wie folgt aus:

Feld	Wert
Repository-Name	Ein beschreibendes Label (z. B. Azure-SFTP)
Protokolle	SFTP
Servername	<Name des Speicherkontos>.blob.core.windows.net
Pfad	/ (Stammverzeichnis)

Authentifizierung	PKI
Benutzername	<storage_account_name>.<container_name>.<sftp_local_useraname>
Kennwort	Leer lassen

2. Klicken Sie auf Senden, um das Repository zu speichern.



ISE SFTP-Repository - Konfiguration

Warnung: Der Host-Schlüssel des SFTP-Servers muss über die CLI mithilfe des ausführbaren Befehls crypto host_key add hinzugefügt werden, bevor dieses Repository verwendet werden kann. Stellen Sie außerdem sicher, dass die Hostschlüsselzeichenfolge mit dem Hostnamen übereinstimmt, der in der URL der Repository-Konfiguration verwendet wird. Um auf das PKI-aktivierte Repository zuzugreifen, generieren Sie Schlüsselpaare aus der GUI, und exportieren Sie den öffentlichen Schlüssel auf Ihren lokalen Computer. Kopieren Sie diesen öffentlichen Schlüssel auf den PKI-fähigen SFTP-Server und fügen Sie ihn der Datei "authorized_keys" hinzu.

---

3. Melden Sie sich sowohl beim primären Admin-Knoten als auch beim primären Überwachungsknoten an, und fügen Sie den Krypto-Host-Schlüssel mit dem Befehl crypto host_key und host <sftp server> hinzu. Stellen Sie sicher, dass der ISE-Knoten den SFTP-Hostnamen auflösen kann.

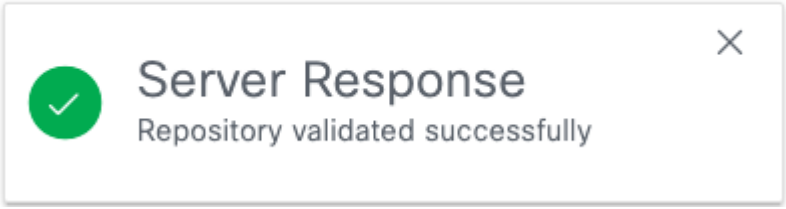
<#root>

```
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. Gehen Sie zurück zur ISE-GUI unter Repository, und wählen Sie das neu erstellte Repository aus, und klicken Sie auf Validieren. Repository erfolgreich validiert.



Erfolgreiche Repository-Validierung

Anmerkung: Mit der Option zur Repository-Validierung wird die Repository-Konfiguration nur auf dem primären Admin-Knoten validiert.

Anmerkung: Wenn ein SFTP-Repository mit einem öffentlichen RSA-Schlüssel erstellt wurde, werden die über die GUI erstellten Repositories nicht in der CLI repliziert, und die über die CLI erstellten Repositories werden nicht in der GUI repliziert. Um dasselbe Repository auf der CLI und der GUI zu konfigurieren, generieren Sie die öffentlichen RSA-Schlüssel auf der CLI und der GUI, und exportieren Sie beide Schlüssel auf den SFTP-Server.

ISE CLI Repository-Konfiguration

1. SSH in die CLI (Befehlszeilenschnittstelle) des primären Admin-Knotens integrieren. Fügen Sie den Kryptografieschlüssel auf jedem Knoten in der Bereitstellung hinzu, auf den Sie über die CLI auf das PKI-basierte SFTP-Repository zugreifen möchten.

2. Generieren Sie einen öffentlichen RSA-Schlüssel für CLI.

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

3. Exportieren Sie die generierte Public Key-Datei in das lokale Festplatten-Repository (jedes Repository, auf das Sie Zugriff haben, um die Datei herunterzuladen).

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

4. Laden Sie diese Datei aus dem Repository herunter und öffnen Sie sie in einem Texteditor, um den öffentlichen Schlüssel für den CLI-Zugriff zu kopieren.

5. Laden Sie den öffentlichen SSH-Schlüssel auf Azure hoch. Dies entspricht dem GUI-Schlüssel, der unter dem Bildschirm zum Erstellen des lokalen Azure SFTP-Benutzers (aus Schritt 3) hinzugefügt wurde.

6. Klicken Sie auf Schlüssel hinzufügen und fügen Sie den vollständigen öffentlichen SSH-Schlüssel (in das Feld für den öffentlichen SSH-Schlüssel) ein.

7. Geben Sie optional eine Schlüsselbeschreibung an (z. B. ISE-CLI-Key).

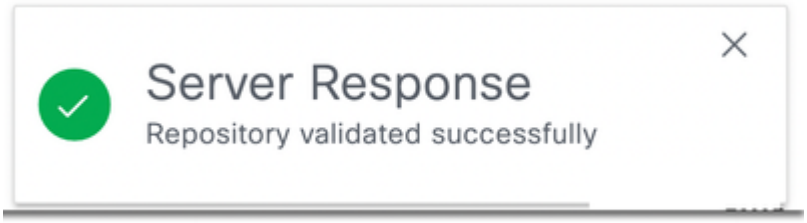
8. Klicken Sie auf Weiter und Speichern.

Überprüfung

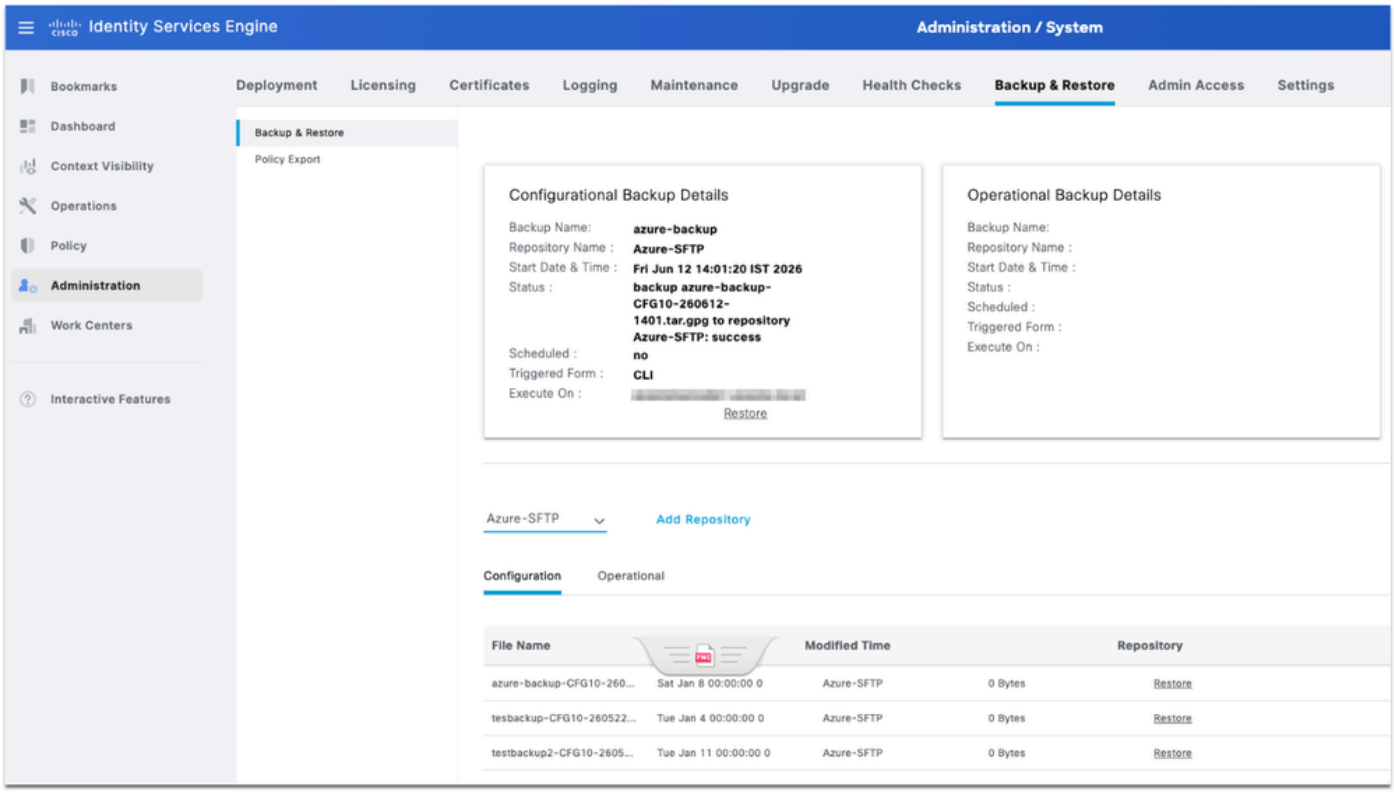
1. Überprüfen Sie den CLI-Zugriff auf das SFTP-Repository mit dem Befehl "show repository <Repository-Name>". Es zeigt die gespeicherten Dateien auf diesem SFTP-Server.

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

2. Überprüfen Sie den GUI-Zugriff auf das SFTP-Repository, indem Sie zu Repository navigieren und das neu erstellte Repository auswählen und auf Validieren klicken. Repository erfolgreich validiert.



3. Navigieren Sie zu Administration > System > Backup and Restore . Nehmen Sie ein Konfigurations-Backup vor, und gehen Sie dann zum Ende dieser Seite, wählen Sie das SFTP-Repository aus, und unter Konfiguration ist das aktuelle Backup sichtbar, um es wiederherzustellen.

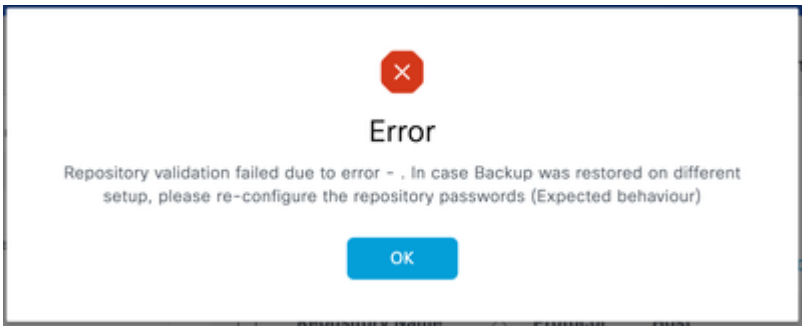


SFTP-Repository-Validierung

Anmerkung: Aufgrund des kosmetischen Cisco Bugs IDCSCwu68863 wird die Größe der Backups auf Azure-Speicher hier als 0 Byte angesehen, es gibt jedoch keine funktionalen Auswirkungen. Diese Sicherungen können bei Bedarf erfolgreich wiederhergestellt werden.

Fehlerbehebung

1. In der ISE-GUI gibt die Repository-Validierung den folgenden Fehler aus:



Fehlermeldung

Auflösung

Überprüfen Sie, ob der richtige öffentliche Schlüssel auf dem SFTP-Server unter SSH-Schlüsseln importiert wird (siehe Schritt 2 unter Konfigurieren von SFTP auf dem Azure-Speicherkonto). Dieser Fehler tritt auf, wenn der Benutzer nach der erfolgreichen Validierung des Repositorys erneut ein neues Schlüsselpaar in der GUI generiert hat.

2. GUI-Repository-Validierung erfolgreich, aber keine Ausgabe des Befehls show repository <sftp repository>

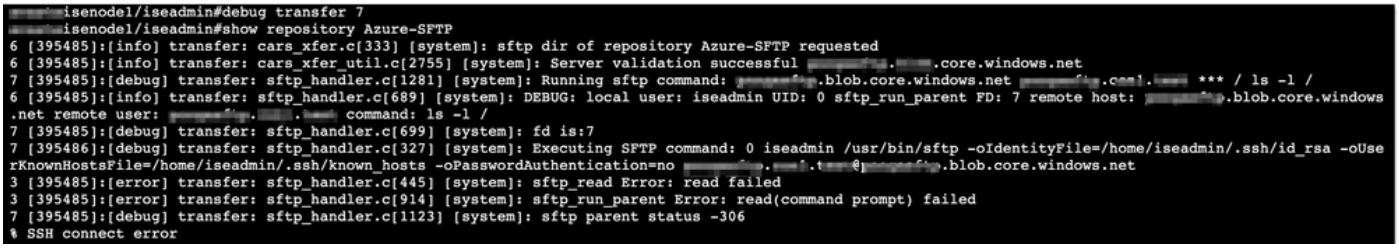
Screenshot des Fehlers

Auflösung

Überprüfen Sie, ob der aus der CLI generierte öffentliche RSA-Schlüssel unter der Azure SSH-Konfiguration hinzugefügt wurde.

3. Um das Problem mit dem SFTP-Repository weiter zu beheben, aktivieren Sie den Befehl debug:

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



Debug-Protokolle

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.