Configurazione e risoluzione dei problemi del repository di archiviazione BLOB SFTP di Azure su ISE

Sommario

Introduzione

In questo documento viene descritta la configurazione di Archiviazione BLOB di Azure come server SFTP con autenticazione infrastruttura a chiave pubblica con motore Identity Services.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze generali di ISE
- Configurazione del repository ISE
- Autenticazione PKI (Public Key Infrastructure)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- ISE 3.3, 3.4, 3.5 VM in Azure
- Sottoscrizione di Azure per accedere a Centro archiviazione

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Come servizio nativo del cloud, l'archivio SFTP di Archiviazione BLOB di Azure è facile da distribuire e ideale per le implementazioni ISE basate su Azure. Elimina i problemi di connettività locali, offre la scalabilità automatica per soddisfare le fluttuanti esigenze di storage e garantisce elevata disponibilità e durata per dataset di grandi dimensioni, eliminando al contempo la necessità di una gestione manuale dell'infrastruttura.

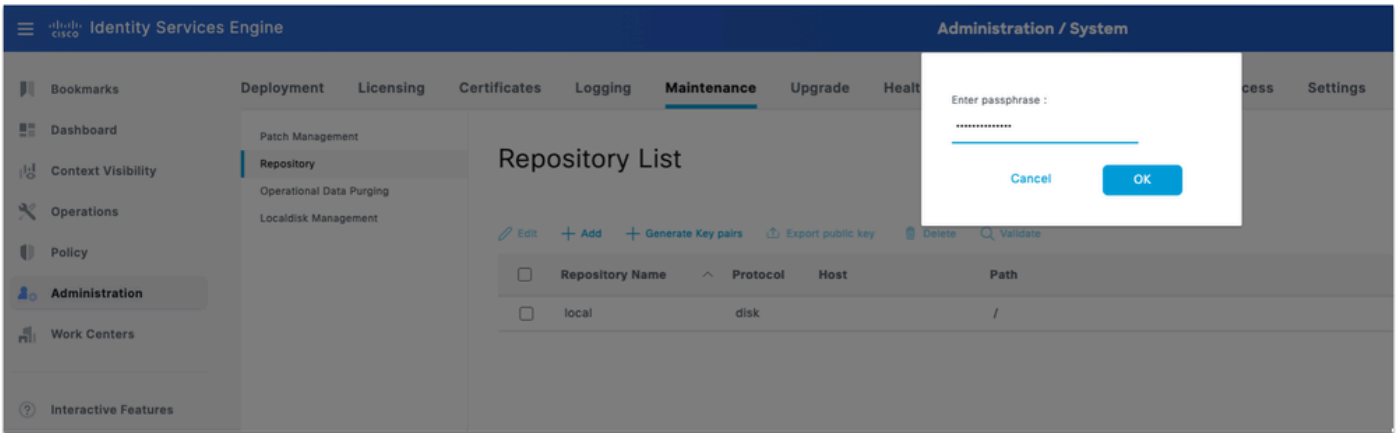
Configurazione

Preconfigurazione ISE

1. Genera una coppia di chiavi sull'ISE: Accedere alla GUI del nodo di amministrazione principale. Passare a Amministrazione > Sistema > Manutenzione > Repository.

2. In Elenco repository, fare clic sull'opzione Genera coppie di chiavi.

3. Immettere la passphrase (più lunga di 13 caratteri) e fare clic su OK. Questa operazione è necessaria per proteggere la coppia di chiavi.



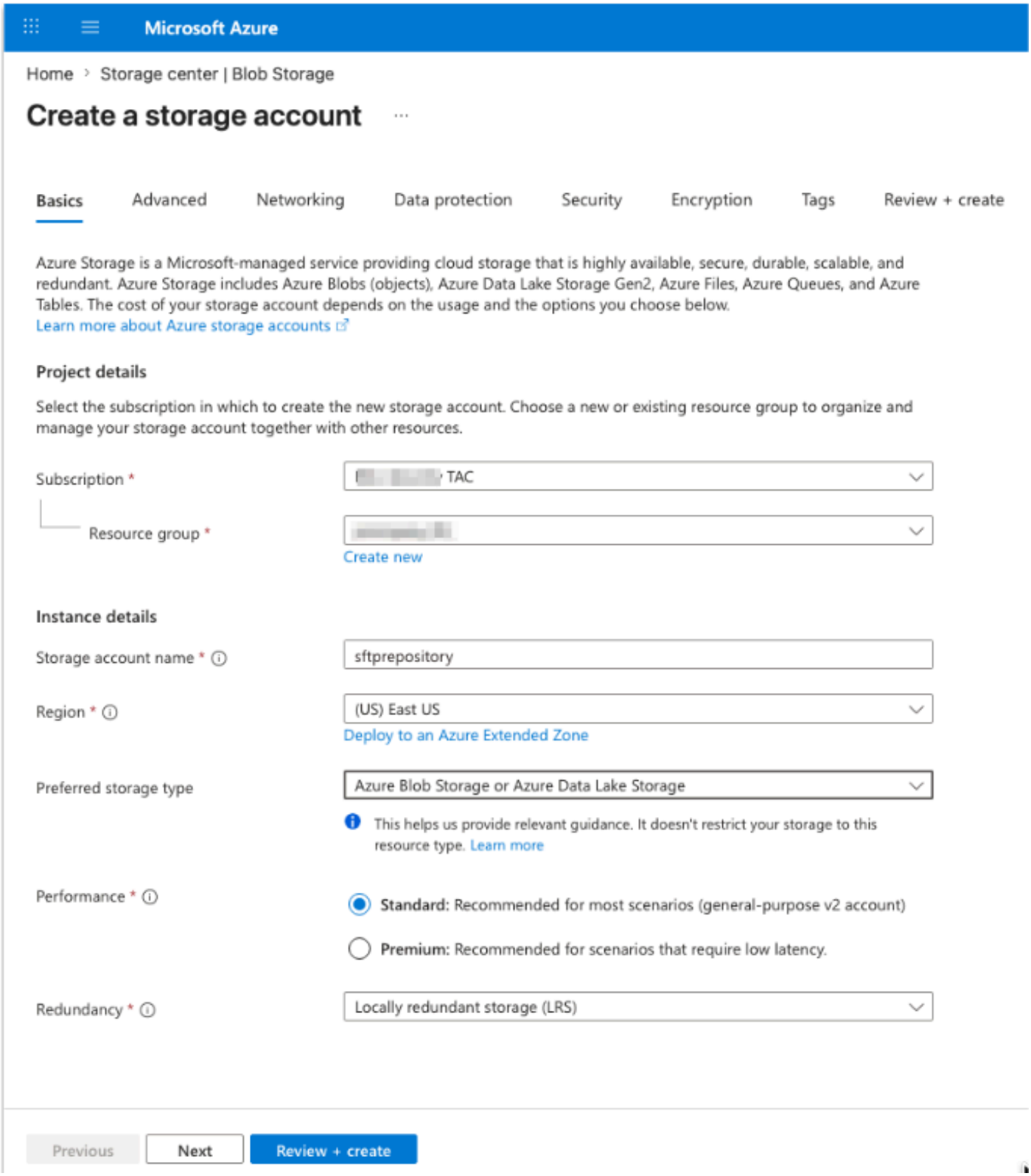
Genera coppia di chiavi su ISE

4. Fare clic su Esporta chiave pubblica e scaricare la chiave id_rsa.pub sul computer (assicurarsi che sia stata salvata per riferimenti futuri).

Configurazione SFTP di Azure

1. Creare e configurare l'account di archiviazione di Azure: Accedere al portale di Azure e passare agli account di archiviazione. Nella scheda Risorse fare clic su Crea per creare un nuovo account di archiviazione. Compila i dettagli:

Campo	Valore
Abbonamento	Sottoscrizione di Azure
Gruppo di risorse	Seleziona esistente o crea nuovo
Nome account di archiviazione	Deve essere univoco a livello globale
Regione	Seleziona la tua regione preferita
Ridondanza	Storage con ridondanza locale (LRS): accettabile per ambienti lab/non prod

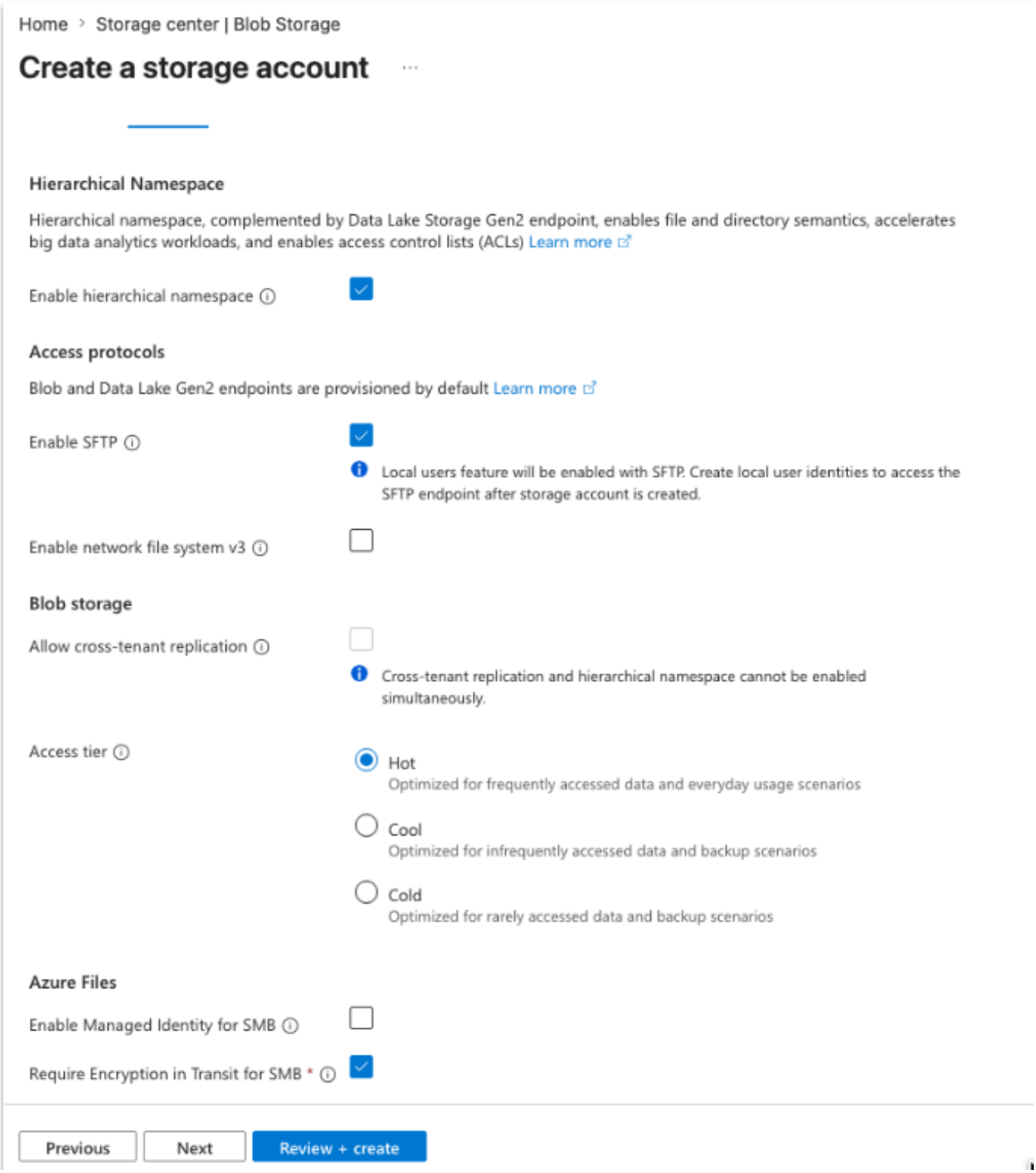


Crea un account di archiviazione

2. Fare clic su Avanti e in Avanzate scheda, selezionare la casella di controllo Abilita spazio dei nomi gerarchico. Questa opzione è obbligatoria. SFTP può essere abilitato solo per gli account namespace gerarchici.

3. Selezionare la casella di controllo Abilita SFTP.

4. Lasciare le altre opzioni come predefinite o modificare in base alle proprie esigenze.



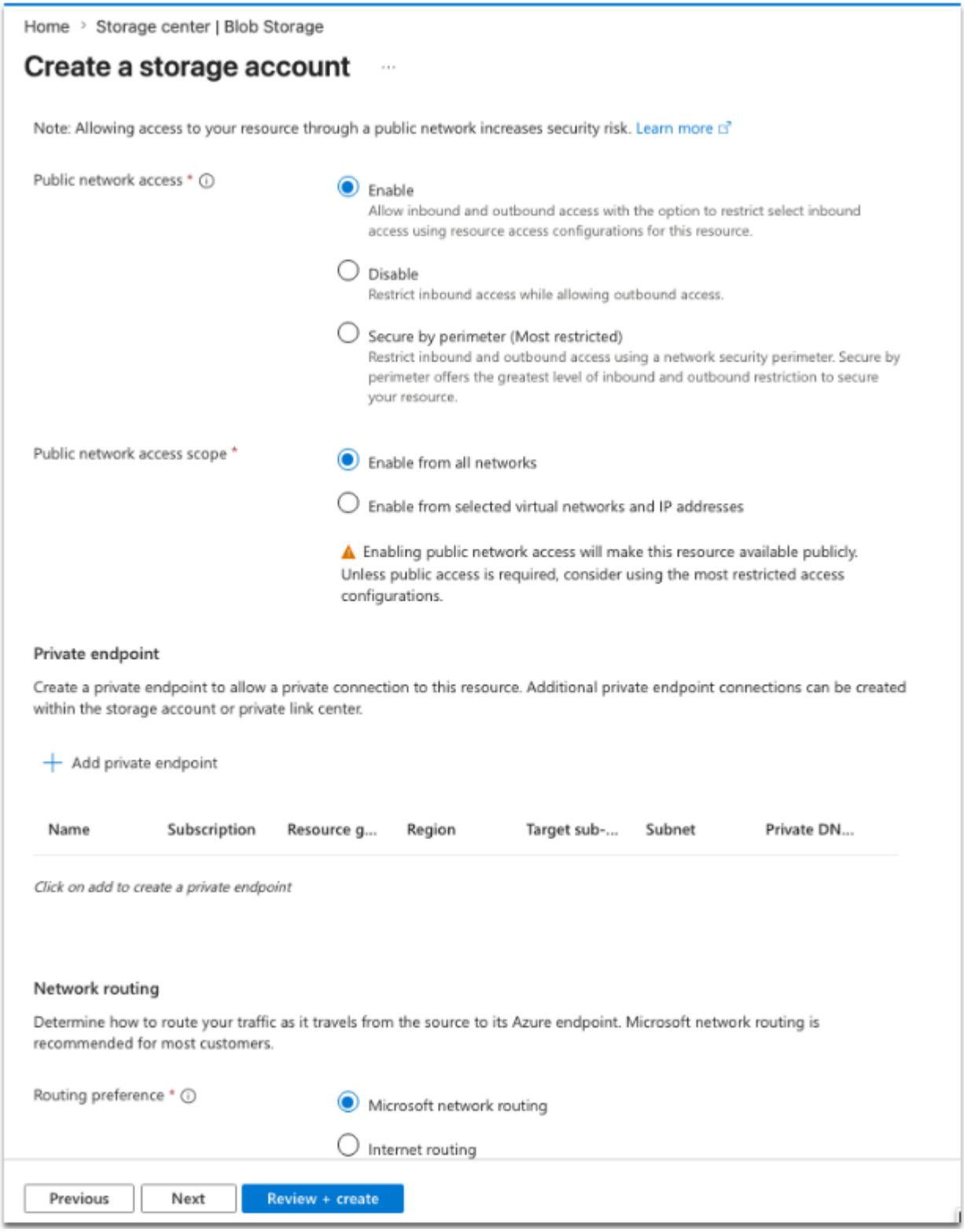
Configura account di archiviazione

5. Fare clic su Next (Avanti) per configurare la rete.

6. Impostare Accesso alla rete su Abilita accesso pubblico da tutte le reti.

7. Impostare la preferenza di instradamento su Instradamento rete Microsoft.

Nota: Nota: Negli ambienti di produzione, prendere in considerazione la possibilità di limitare l'accesso a intervalli IP specifici (gli indirizzi IP del nodo ISE) utilizzando le regole firewall sull'account di storage.



8. Fare clic su Avanti e lasciare le impostazioni Protezione dati, Sicurezza e Crittografia predefinite. Non è necessaria alcuna configurazione aggiuntiva per distribuzioni lab o standard.

9. Fare clic su Rivedi + crea. Una volta superata la convalida, fare clic su Crea.

10. Attendere il completamento della distribuzione, quindi fare clic su Vai alla risorsa.

11. Configurare SFTP sull'account di archiviazione di Azure: Nel nuovo account di archiviazione creato, aggiungere un contenitore passando a Archiviazione dati > Contenitori > Aggiungi contenitore

12. Fornire un nome di contenitore. Fare clic su Crea.

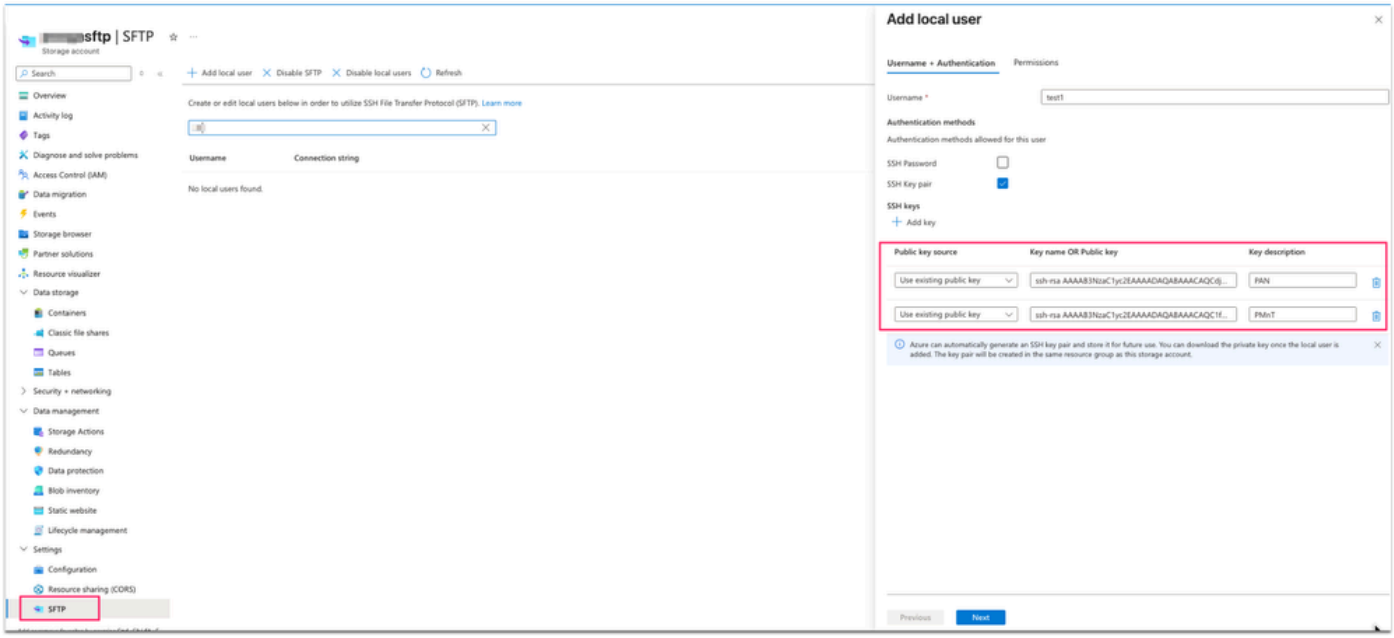
13. Aggiungere un utente sftp selezionando Impostazioni > SFTP nel menu a sinistra. Fare clic su Aggiungi utente locale e configurare quanto segue:

Campo	Valore
Username	Un nome descrittivo
Metodo di autenticazione	Coppia di chiavi SSH - NON utilizzare password
Origine chiave pubblica SSH	Usa chiave esistente (generata nel passaggio 1, la chiave id_rsa.pub)

Nota: In una distribuzione a più nodi, quando la PAN primaria e la MnT primaria sono nodi separati, il file id_rsa.pub dispone di chiavi pubbliche RSA provenienti sia dal nodo PAN primario che dal nodo MnT primario.

14. Per usare la chiave pubblica esistente sotto l'opzione SSH keys, aprire il file id_rsa.pub in un editor di testo a scelta e copiare e incollare separatamente la chiave dei nodi (iniziando con ssh-rsa e terminando con root@your_node_name) facendo clic due volte su Add key option (Aggiungi chiave).

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



Aggiunta della chiave pubblica in Azure

15. Fare clic su Permissions. Selezionare inizialmente il contenitore creato in questo passaggio e impostare l'autorizzazione per il contenitore su Lettura, Scrittura, Elenca, Elimina e Crea.

16. Impostare la home directory sulla radice del contenitore.

17. Salvare l'utente.

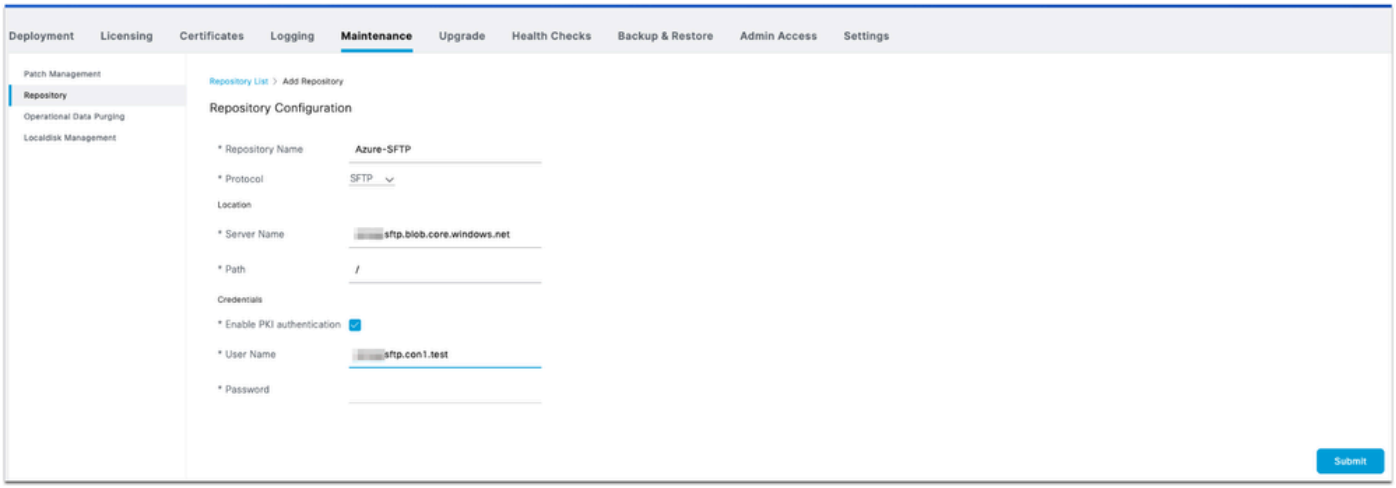
Configurazione ISE GUI Repository

1. Passare a Amministrazione > Sistema > Gestione > Repository e fare clic su Aggiungi. Compilare i campi come segue:

Campo	Valore
Nome repository	Un'etichetta descrittiva (come Azure-SFTP)
Protocollo	SFTP
Nome del server	<nome_account_archiviazione>.blob.core.windows.net

Percorso	/ (directory principale)
Autenticazione	PKI
Nome utente	<nome_account_archiviazione>.<nome_contenitore>.<nomeutente_locale_sftp>
Password	Lasciare vuoto

2. Fare clic su Sottometti per salvare il repository.



Configurazione repository ISE SFTP

Avviso: La chiave host del server sftp deve essere aggiunta tramite CLI utilizzando il comando crypto host_key add executable prima di poter utilizzare questo repository. Verificare inoltre che la stringa della chiave host corrisponda al nome host utilizzato nell'URL della configurazione del repository. Per accedere al repository abilitato per PKI, generare una coppia di chiavi dalla GUI ed esportare la chiave pubblica nel computer locale. Copiare la chiave pubblica sul server SFTP abilitato per PKI e aggiungerla al file 'authorized_keys'.

---

3. Accedere a entrambi i nodi Admin primario e Monitoraggio primario e aggiungere la chiave host crittografica utilizzando il comando crypto host_key e host <sftp server >. Accertarsi che il nodo ISE sia in grado di risolvere il nome host sftp.

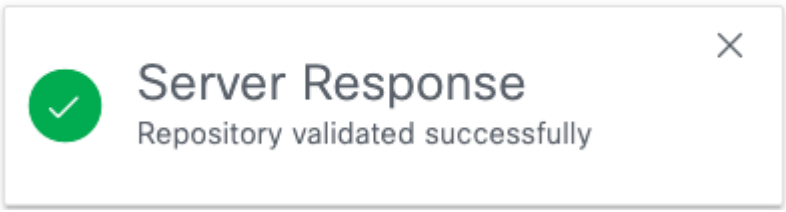
<#root>

```
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. Tornare alla GUI di ISE in Repository e selezionare il repository appena creato e fare clic su Convalida. Convalida del repository completata.



Convalida del repository riuscita

Nota: L'opzione di convalida del repository convalida la configurazione del repository solo sul nodo di amministrazione principale.

Nota: Nel caso di un repository SFTP creato con la chiave pubblica RSA, i repository creati tramite la GUI non vengono replicati nella CLI e i repository creati tramite la CLI non vengono replicati nella GUI. Per configurare lo stesso repository sulla CLI e sulla GUI, generare le chiavi pubbliche RSA sia sulla CLI che sulla GUI ed esportare entrambe le chiavi sul server SFTP.

Configurazione del repository CLI ISE

1. SSH nella CLI (interfaccia della riga di comando) del nodo di amministrazione primario. Aggiungere la chiave crittografica su ciascun nodo della distribuzione in cui si desidera accedere al repository SFTP basato su PKI dalla CLI.

2. Generare la chiave pubblica rsa per la CLI.

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

3. Esportare il file di chiave pubblica generato nel repository del disco locale (qualsiasi repository che sia possibile scaricare).

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

4. Scaricare il file dal repository e aprirlo in un editor di testo per copiare la chiave pubblica per l'accesso CLI.

5. Caricare la chiave pubblica SSH in Azure, come la chiave GUI aggiunta nella schermata di creazione dell'utente locale SFTP di Azure (dal passaggio 3).

6. Fare clic su Add key (Aggiungi chiave) e incollare la chiave pubblica SSH completa (nel campo SSH public key).

7. Facoltativamente, fornire una descrizione della chiave (ad esempio, ISE-CLI-Key).

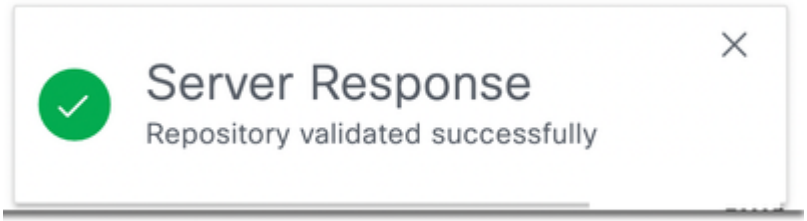
8. Fare clic su Avanti e su Salva.

Verifica

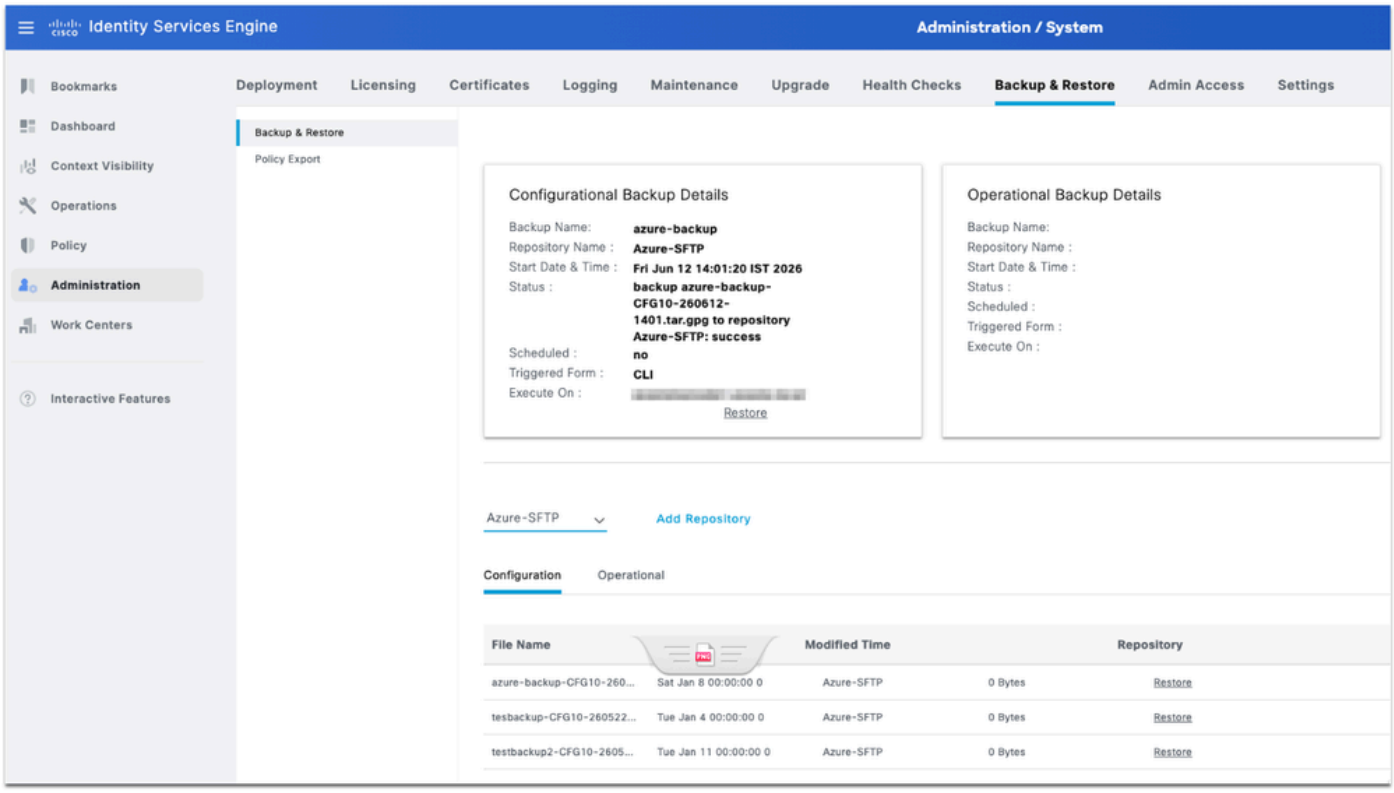
1. Verificare l'accesso CLI al repository sftp utilizzando il comando "show repository <nome repository>". Mostra i file archiviati su questo server sftp.

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

2. Verificare l'accesso GUI al repository sftp passando a Repository e selezionare il repository appena creato e fare clic su Convalida. Convalida del repository completata.



3. Passare a Amministrazione > Sistema > Backup e ripristino. Eseguire un backup della configurazione, quindi andare in fondo alla pagina, selezionare il repository SFTP e in Configurazione, il backup recente è visibile per il ripristino.

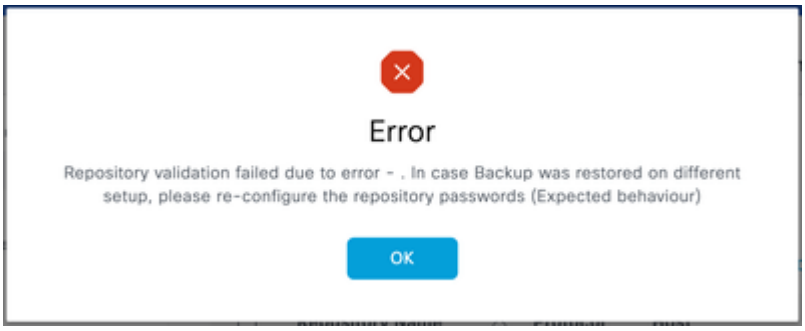


convalida repository sftp

Nota: A causa del bug cosmetico di Cisco IDCSCwu68863, le dimensioni dei backup nell'archiviazione di Azure vengono visualizzate come 0 byte, ma non vi è alcun impatto funzionale. Se necessario, è possibile ripristinare correttamente questi backup.

Risoluzione dei problemi

1. Nella GUI ISE, la convalida del repository fornisce questo errore:



Messaggio di errore

Risoluzione

Verificare che la chiave pubblica corretta sia stata importata nel server SFTP sotto le chiavi SSH (fare riferimento al passaggio 2 di Configurazione SFTP nell'account di archiviazione di Azure). Questo errore si verifica se l'utente ha generato di nuovo una nuova coppia di chiavi sulla GUI dopo la convalida del repository.

2. La convalida del repository GUI è riuscita ma il comando show repository <sftp repository> non restituisce alcun output.

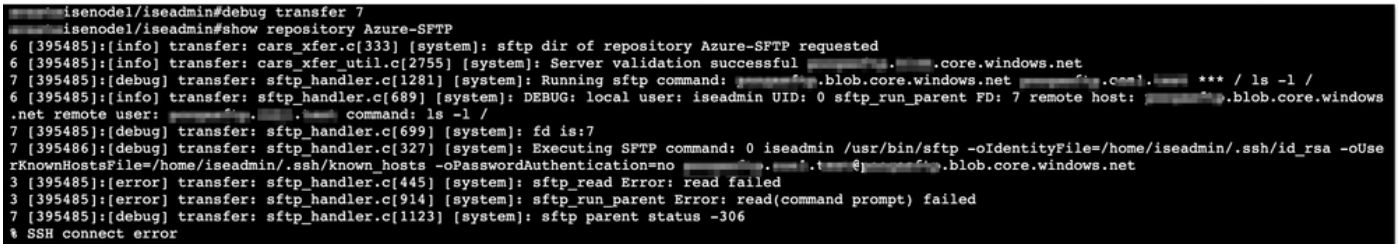
Schermata di errore

Risoluzione

Verificare che la chiave pubblica RSA generata dalla CLI sia stata aggiunta nella configurazione di Azure ssh.

3. Per risolvere ulteriormente il problema dell'archivio SFTP, abilitare il comando debug:

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



Registri di debug

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).