Configurer et dépanner le référentiel de stockage d'objets blob SFTP Azure sur ISE

Table des matières

Introduction

Ce document décrit la configuration d'Azure Blob Storage en tant que serveur SFTP avec l'authentification Public Key Infrastructure avec Identity Services Engine.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances générales d'ISE
- Configuration du référentiel ISE
- Authentification par infrastructure à clé publique (PKI)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- ISE 3.3, 3.4, 3.5 VM sur Azure
- Abonnement Azure pour accéder à Storage Center

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

En tant que service natif du cloud, le référentiel SFTP Azure Blob Storage est facile à déployer et idéal pour les mises en oeuvre ISE basées sur Azure. Elle élimine les problèmes de connectivité sur site, évolue automatiquement pour répondre aux fluctuations des demandes de stockage et garantit une disponibilité et une durabilité élevées pour les grands ensembles de données, tout en éliminant le besoin de gestion manuelle de l'infrastructure.

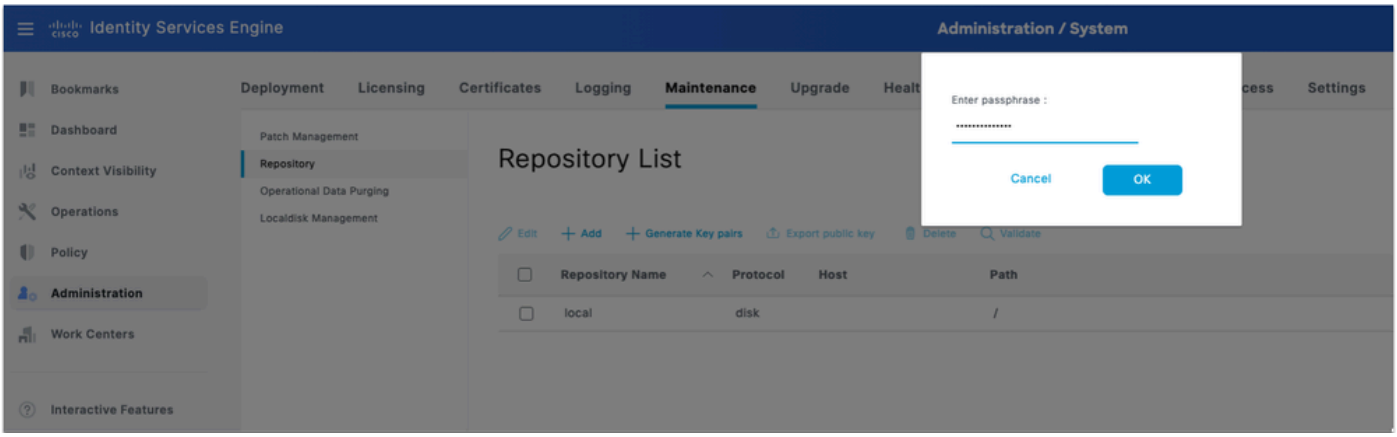
Configurer

Pré-configuration ISE

1. Générez des paires de clés sur ISE : Connectez-vous à l'interface utilisateur graphique du noeud d'administration principal. Accédez à Administration > System > Maintenance > Repository.

2. Sous Liste des référentiels, cliquez sur l'option Générer des paires de clés.

3. Entrez une phrase de passe (supérieure à 13 caractères) et cliquez sur OK. Ceci est nécessaire pour protéger la paire de clés.



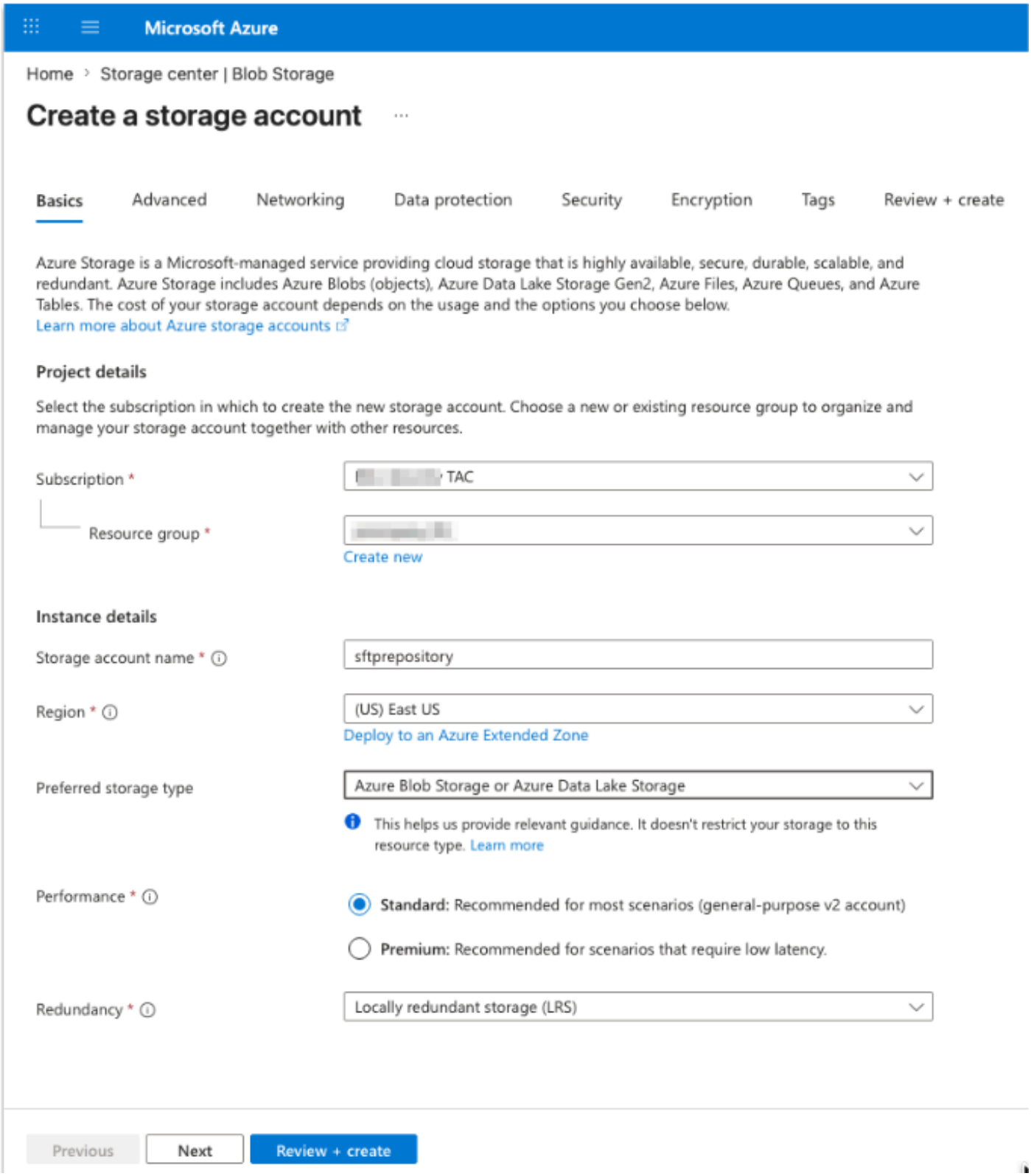
Générer une paire de clés sur ISE

4. Cliquez sur Exporter la clé publique et téléchargez la clé id_rsa.pub sur votre ordinateur (assurez-vous qu'elle est enregistrée pour de futures références).

Configuration SFTP Azure

1. Créez et configurez un compte de stockage Azure : Connectez-vous au portail Azure et accédez aux comptes de stockage. Sous l'onglet Resources, cliquez sur Create pour créer un nouveau compte de stockage. Renseignez les détails :

Champ	Valeur
Abonnement	Votre abonnement Azure
Groupe de ressources	Sélectionner un fichier existant ou en créer un nouveau
Nom du compte de stockage	Doit être unique au niveau mondial
Région	Sélectionnez votre région préférée
Redondance	Stockage redondant local (LRS) : acceptable pour les travaux pratiques/non prod

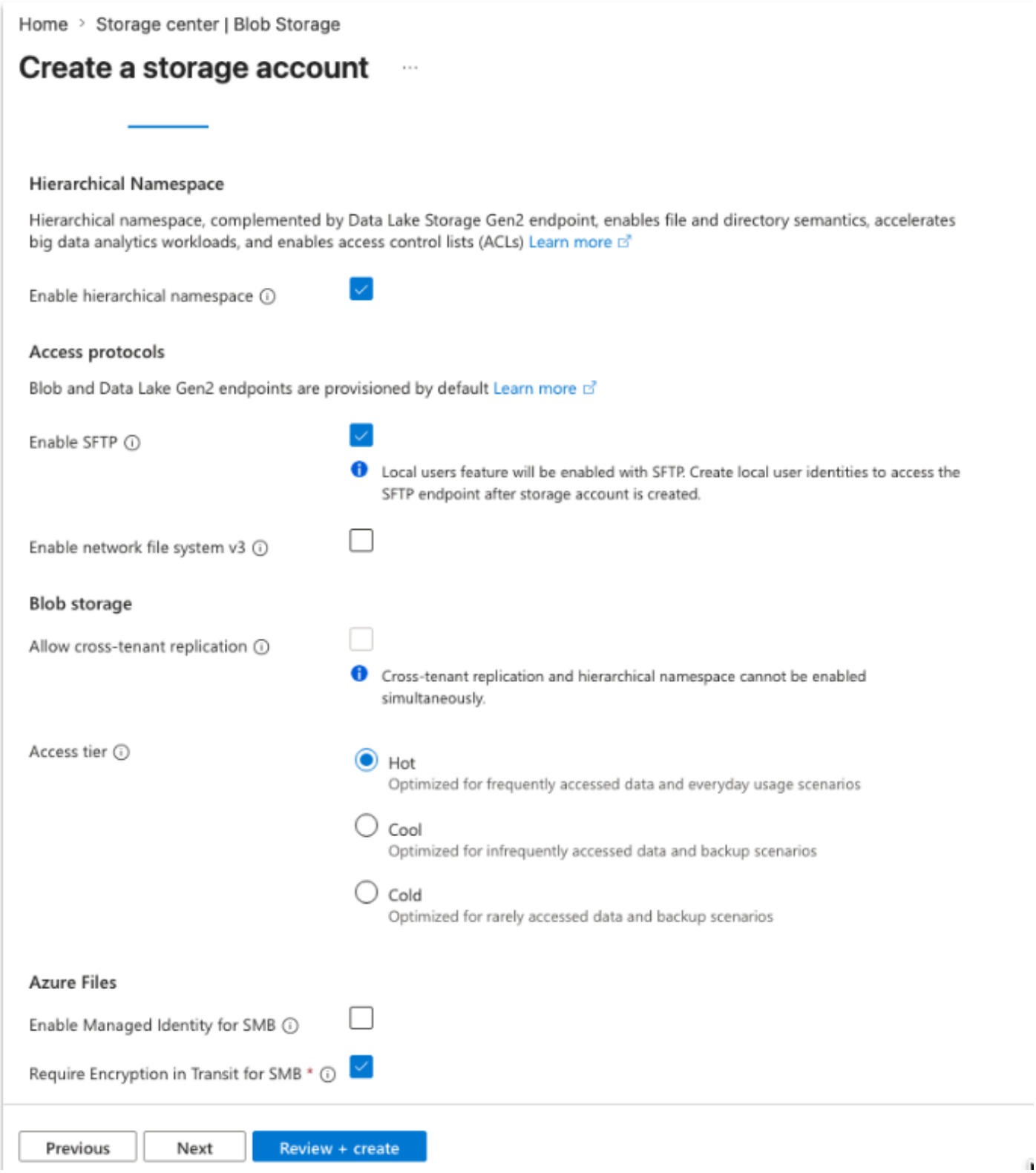


Créer un compte de stockage

2. Cliquez sur Suivant et sous l'onglet Avancé, cochez la case Activer l'espace de noms hiérarchique. Cette option est obligatoire. SFTP ne peut être activé que pour les comptes d'espace de noms hiérarchiques.

3. Cochez la case Enable SFTP.

4. Laissez le reste des options par défaut ou modifiez-les selon vos besoins.



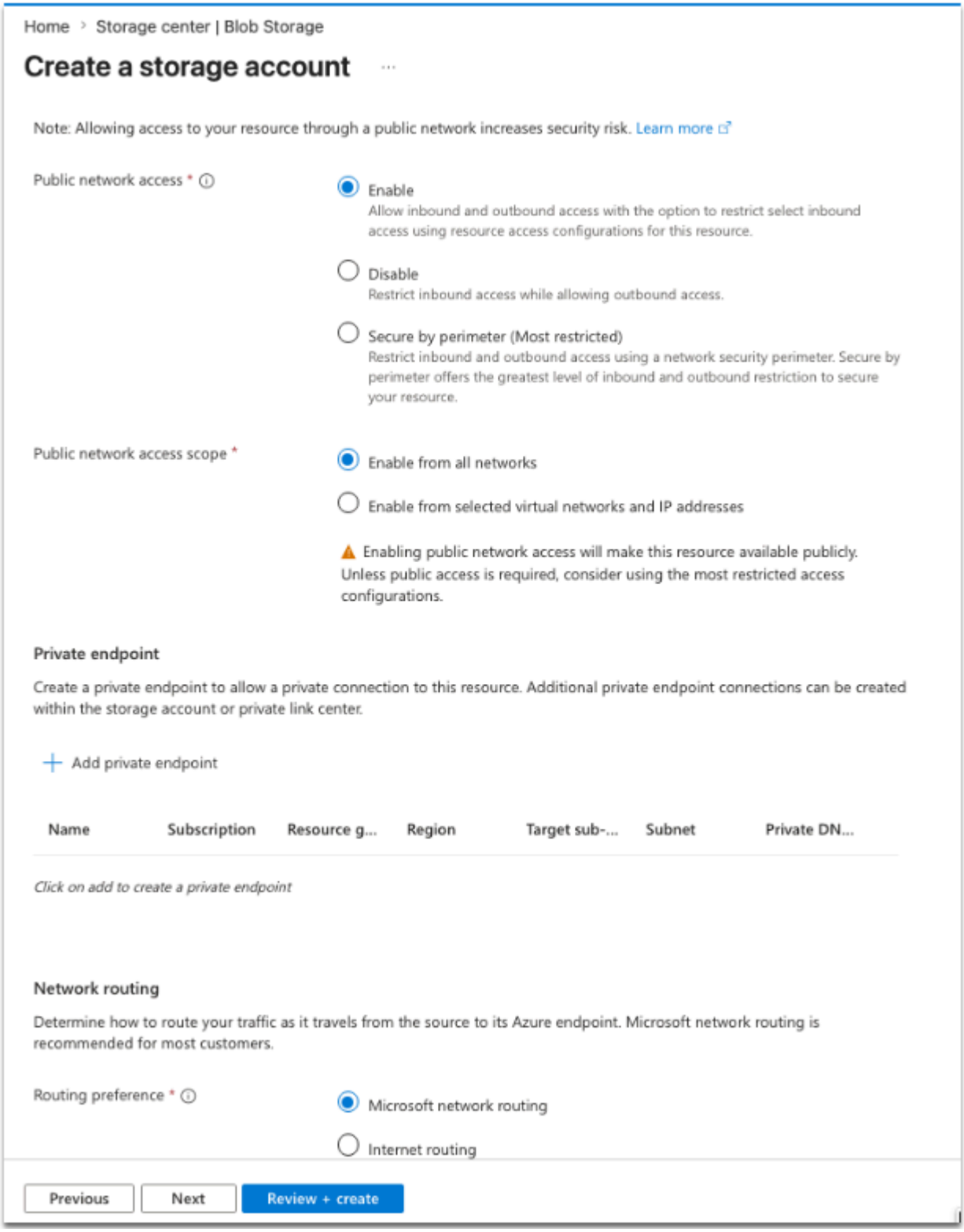
Configurer le compte de stockage

5. Cliquez sur Next pour configurer Networking.

6. Définissez Accès réseau sur Activer l'accès public à partir de tous les réseaux.

7. Définissez la préférence de routage sur Routage réseau Microsoft.

Remarque : Remarque : Dans les environnements de production, pensez à restreindre l'accès à des plages IP spécifiques (les adresses IP du noeud ISE) à l'aide de règles de pare-feu sur le compte de stockage.



8. Cliquez sur Next et conservez la valeur par défaut Data protection, Security and Encryption. Aucune configuration supplémentaire n’est requise pour les déploiements de travaux pratiques ou standard.

9. Cliquez sur Vérifier + créer. Une fois la validation passée, cliquez sur Create.

10. Attendez la fin du déploiement, puis cliquez sur Accéder à la ressource.

11. Configurez SFTP sur le compte de stockage Azure : Dans le compte de stockage que vous venez de créer, ajoutez un conteneur en accédant à Stockage de données > Conteneurs > Ajouter un conteneur

12. Entrez un nom de conteneur. Cliquez sur Créer.

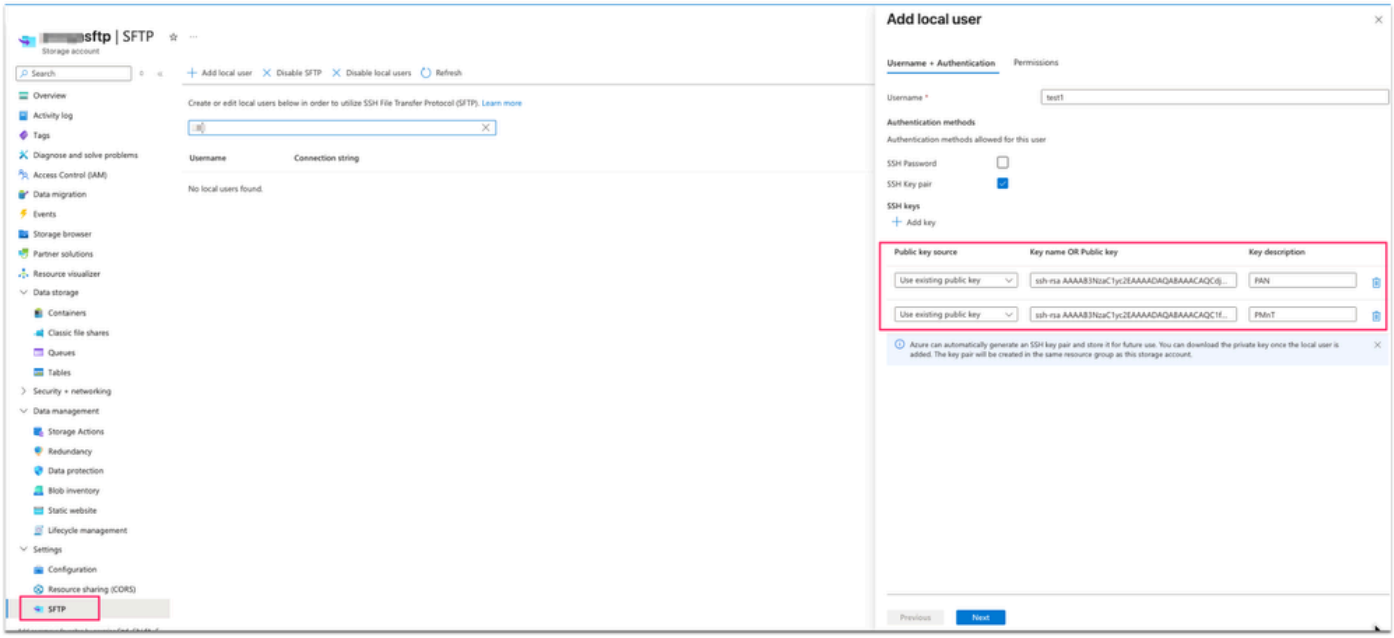
13. Ajoutez un utilisateur sftp en accédant à Paramètres > SFTP dans le menu de gauche. Cliquez sur Add local user et configurez les éléments suivants :

Champ	Valeur
Nom d’utilisateur	Un nom descriptif
Méthode d'authentification	Paire de clés SSH — Ne pas utiliser de mot de passe
Source de clé publique SSH	Utiliser la clé existante (générée à l'étape 1, la clé id_rsa.pub)

Remarque : Dans un déploiement multinoeud, lorsque le PAN principal et le MnT principal sont des noeuds distincts, le fichier id_rsa.pub possède des clés publiques RSA à la fois du PAN principal et du MnT principal.

14. Pour utiliser une clé publique existante sous l'option SSH keys, ouvrez le fichier id_rsa.pub dans un éditeur de texte de votre choix et copiez-collez les deux clés de noeuds (en commençant par ssh-rsa et en terminant par root@your_node_name) séparément en cliquant sur l'option Add key deux fois.

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



Ajout d'une clé publique sur Azure

15. Cliquez sur Autorisations. Sélectionnez initialement le conteneur créé à cette étape et définissez l'autorisation de lecture, d'écriture, de liste, de suppression et de création pour le conteneur.

16. Définissez le répertoire Home à la racine du conteneur.

17. Enregistrez l'utilisateur.

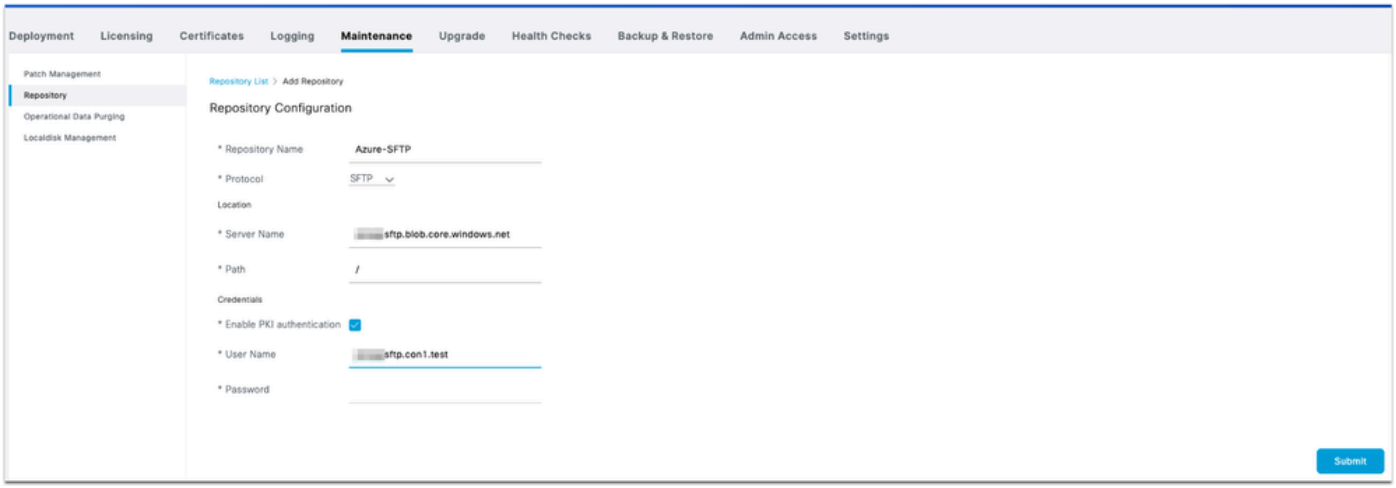
Configuration du référentiel ISE GUI

1. Accédez à Administration > Système > Maintenance > Référentiel et cliquez sur Ajouter. Renseignez les champs comme suit :

Champ	Valeur
Nom du référentiel	Une étiquette descriptive (comme, Azure-SFTP)
Protocol	SFTP
Nom du serveur	<nom_compte_stockage>.blob.core.windows.net

Chemin	/ (répertoire racine)
Authentification	PKI
Nom d'utilisateur	<nom_compte_stockage>.<nom_conteneur>.<nom_utilisateur_local_sftp>
Mot de passe	Laisser vide

2. Cliquez sur Soumettre pour enregistrer le référentiel.



Configuration du référentiel ISE SFTP

Avertissement : La clé d'hôte du serveur sftp doit être ajoutée via l'interface de ligne de commande en utilisant la commande crypto host_key add executable avant que ce référentiel puisse être utilisé. Assurez-vous également que la chaîne de clé d'hôte correspond au nom d'hôte utilisé dans l'URL de la configuration du référentiel. Pour accéder au référentiel PKI, générez des paires de clés à partir de l'interface utilisateur graphique et exportez la clé publique sur votre ordinateur local. Copiez cette clé publique sur le serveur SFTP PKI et ajoutez-la au fichier « authorized_keys ».

---

3. Connectez-vous au noeud d'administration principal et au noeud de surveillance principal et ajoutez la clé d'hôte de chiffrement à l'aide de la commande crypto host_key et host <sftp server>. Assurez-vous que le noeud ISE peut résoudre le nom d'hôte sftp.

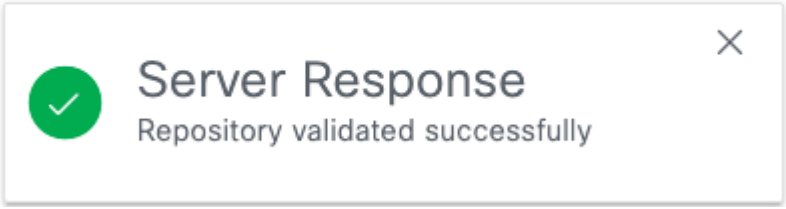
<#root>

```
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. Revenez à l'interface utilisateur graphique ISE sous Référentiel et sélectionnez le référentiel nouvellement créé et cliquez sur Valider. Validation du référentiel réussie.



Validation du référentiel réussie

Remarque : L'option de validation du référentiel valide la configuration du référentiel uniquement sur le noeud d'administration principal.

Remarque : Dans le cas d'un référentiel SFTP créé avec une clé publique RSA, les référentiels créés via l'interface utilisateur graphique ne sont pas répliqués dans l'interface de ligne de commande et les référentiels créés via l'interface de ligne de commande ne sont pas répliqués dans l'interface utilisateur graphique. Pour configurer le même référentiel sur l'interface de ligne de commande et l'interface utilisateur graphique, générez des clés publiques RSA sur l'interface de ligne de commande et l'interface utilisateur graphique et exportez les deux clés vers le serveur SFTP.

Configuration du référentiel ISE CLI

1. Connectez SSH à l'interface de ligne de commande (CLI) du noeud d'administration principal. Ajoutez la clé de chiffrement sur chaque noeud du déploiement où vous souhaitez accéder au référentiel SFTP basé sur l'ICP à partir de l'interface de ligne de commande.

2. Générez une clé publique rsa pour CLI.

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

3. Exportez le fichier de clé publique généré vers le référentiel de disque local (tout référentiel auquel vous avez accès pour télécharger le fichier).

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

4. Téléchargez ce fichier à partir du référentiel et ouvrez-le dans l'éditeur de texte pour copier la clé publique pour l'accès CLI.

5. Téléchargez la clé publique SSH sur Azure, comme la clé GUI ajoutée sous l'écran de création d'utilisateur local Azure SFTP (à partir de l'étape 3).

6. Cliquez sur Add key et collez la clé publique SSH complète (dans le champ SSH public key).

7. Fournissez éventuellement une description de clé (par exemple, ISE-CLI-Key).

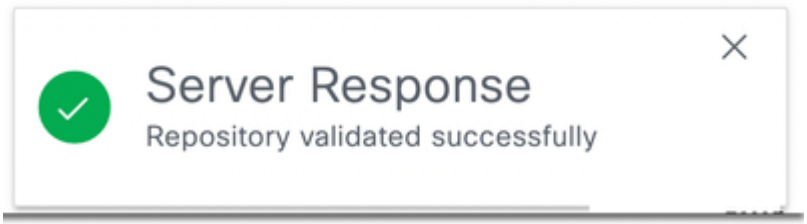
8. Cliquez sur Suivant et sur Enregistrer.

Vérifier

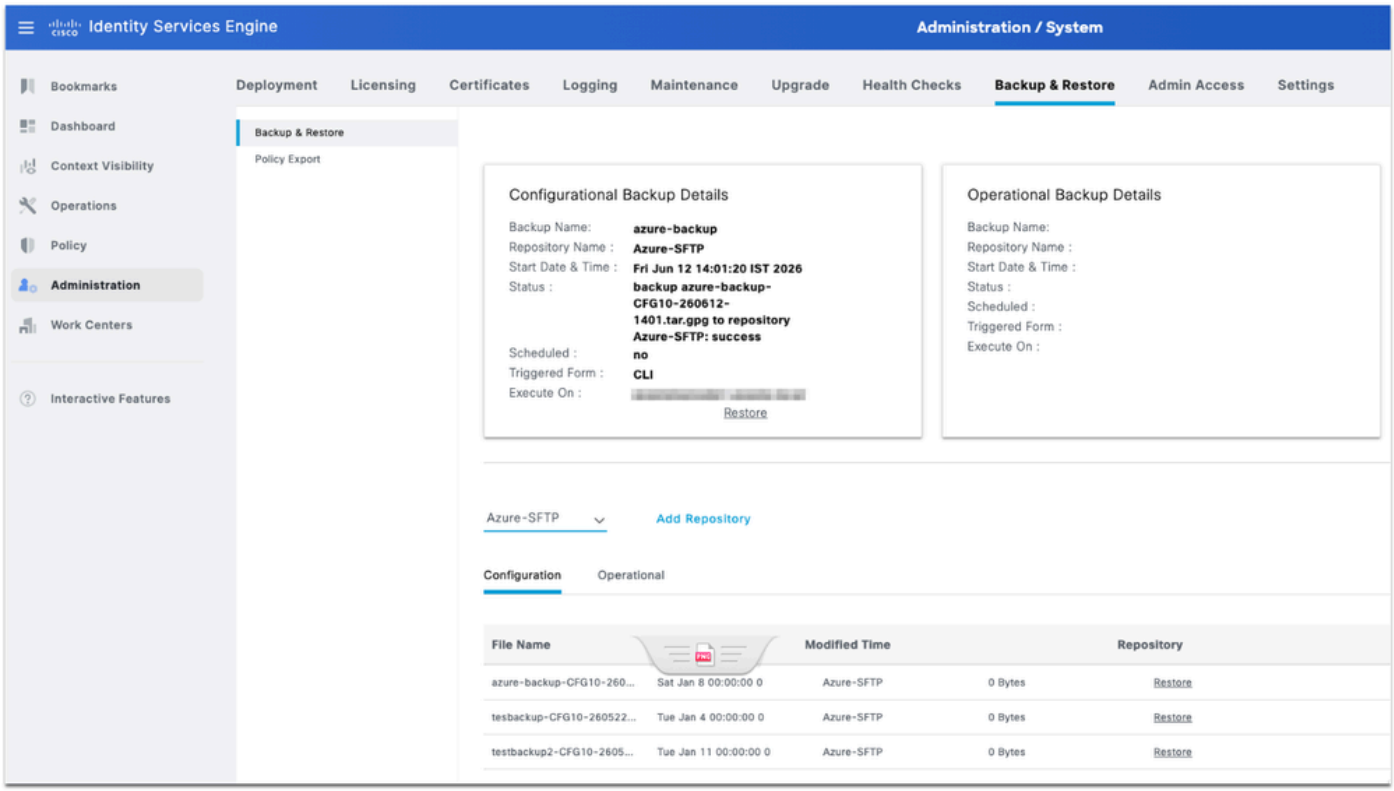
1. Vérifiez l'accès CLI au référentiel sftp à l'aide de la commande « show repository <Nom du référentiel> ». Il affiche les fichiers stockés sur ce serveur sftp.

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

2. Vérifiez l'accès de l'interface utilisateur graphique au référentiel sftp en naviguant jusqu'à Référentiel et sélectionnez le référentiel nouvellement créé et cliquez sur Valider. Validation du référentiel réussie.



3. Accédez à Administration > System > Backup and Restore . Effectuez une sauvegarde de configuration, puis allez au bas de cette page, sélectionnez le référentiel SFTP et sous Configuration, la sauvegarde récente est visible pour restauration.

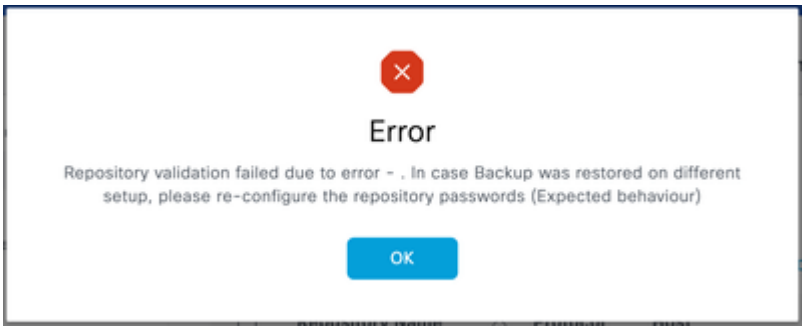


validation du référentiel sftp

Remarque : En raison du bogue cosmétique Cisco IDCSCwu6863, la taille des sauvegardes sur le stockage Azure est considérée ici comme 0 octet, mais il n'y a aucun impact fonctionnel. Ces sauvegardes peuvent être restaurées avec succès si nécessaire.

Dépannage

1. Dans l'interface utilisateur graphique ISE, la validation du référentiel génère l'erreur suivante :



Résolution

Vérifiez que la clé publique appropriée est importée sur le serveur SFTP sous SSH keys (reportez-vous à l'étape 2 de Configuration de SFTP sur un compte de stockage Azure). Cette erreur se produit si l'utilisateur a généré à nouveau une nouvelle paire de clés sur l'interface utilisateur graphique après une validation réussie du référentiel.

2. Validation du référentiel GUI réussie mais aucun résultat de la commande show repository <sftp repository>.

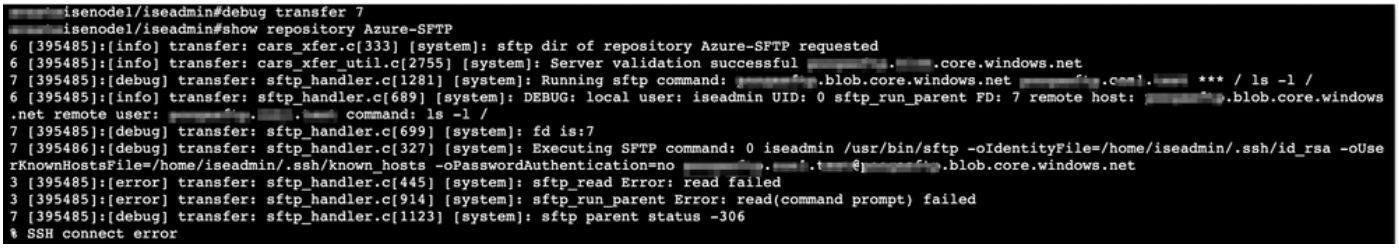
Capture d'écran Erreur

Résolution

Vérifiez que la clé publique RSA générée à partir de l'interface de ligne de commande est ajoutée sous la configuration SSH Azure.

3. Afin de dépanner davantage le problème du référentiel SFTP, activez la commande debug :

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



Journaux de débogage

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.