

# 在ISE上配置Azure SFTP Blob儲存庫並對其進行故障排除

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

### [設定](#)

#### [ISE預配置](#)

#### [Azure SFTP配置](#)

#### [ISE GUI儲存庫配置](#)

#### [ISE CLI儲存庫配置](#)

### [驗證](#)

### [疑難排解](#)

#### [解析](#)

#### [解析](#)

---

## 簡介

本文檔介紹如何將Azure Blob儲存配置為SFTP伺服器，使用身份服務引擎進行公鑰基礎結構身份驗證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 一般ISE知識
- ISE儲存庫配置
- 公開金鑰基礎架構(PKI)驗證

## 採用元件

本文件的資訊是以下列軟體版本為依據：

- Azure上的ISE 3.3、3.4、3.5 VM
- 用於訪問Storage Center的Azure訂閱

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

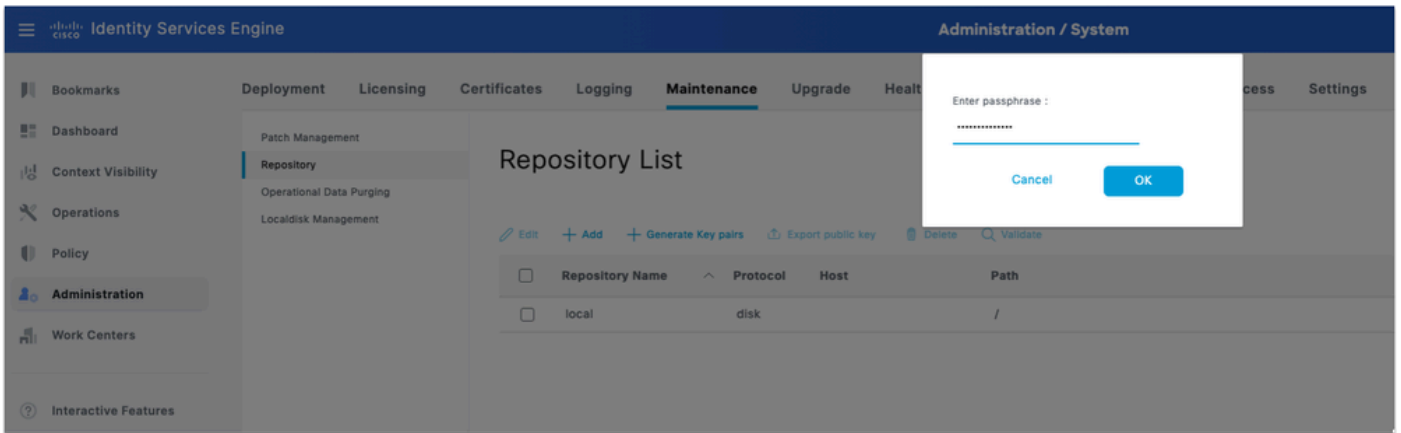
## 背景資訊

作為雲原生服務，Azure Blob儲存SFTP儲存庫易於部署，非常適合基於Azure的ISE實施。它消除了本地連線問題，自動擴展以滿足波動的儲存需求，並確保了大型資料集的高可用性和耐用性 — 同時消除了手動基礎架構管理的需要。

## 設定

### ISE預配置

- 1.在ISE上生成金鑰對：登入到主管理節點GUI。導覽至Administration > System > Maintenance > Repository。
- 2.在「資料庫清單」下，按一下生成金鑰對選項。
- 3.輸入密碼短語（大於13個字元），然後按一下OK。這是保護金鑰對所必需的。



在ISE上生成金鑰對

4. 按一下Export public key，然後在電腦上下載id\_rsa.pub金鑰（確保儲存此金鑰以供將來參考）。

## Azure SFTP配置

1. 建立和配置Azure儲存帳戶：登入到Azure門戶並導航到儲存帳戶。在Resources頁籤下，按一下Create以建立新的儲存帳戶。填寫詳細資訊：

欄位	價值
訂閱	你的Azure訂閱
資源組	選擇現有或新建
儲存帳戶名稱	必須是全域性唯一的
地區	選擇您的首選區域
備援	本地冗餘儲存(LRS) — 實驗室/非生產裝置可以接受

Microsoft Azure

Home > Storage center | Blob Storage

## Create a storage account

Basics | Advanced | Networking | Data protection | Security | Encryption | Tags | Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below.  
[Learn more about Azure storage accounts](#)

### Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \*

Resource group \*   
[Create new](#)

### Instance details

Storage account name \*

Region \*   
[Deploy to an Azure Extended Zone](#)

Preferred storage type

**i** This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance \*  Standard: Recommended for most scenarios (general-purpose v2 account)  
 Premium: Recommended for scenarios that require low latency.

Redundancy \*

[Previous](#) [Next](#) [Review + create](#)

建立儲存帳戶

2.按一下下一步，然後在高級頁籤下選中啟用分層名稱空間覈取方塊。此選項是必需的。只能為層次結構名稱空間帳戶啟用SFTP。

3.選中啟用SFTP覈取方塊。

4.保留其餘選項為預設選項或根據需要進行微調。

Home > Storage center | Blob Storage

## Create a storage account

---

### Hierarchical Namespace

Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs) [Learn more](#)

Enable hierarchical namespace

### Access protocols

Blob and Data Lake Gen2 endpoints are provisioned by default [Learn more](#)

Enable SFTP   
**i** Local users feature will be enabled with SFTP. Create local user identities to access the SFTP endpoint after storage account is created.

Enable network file system v3

### Blob storage

Allow cross-tenant replication   
**i** Cross-tenant replication and hierarchical namespace cannot be enabled simultaneously.

Access tier  Hot  
Optimized for frequently accessed data and everyday usage scenarios

Cool  
Optimized for infrequently accessed data and backup scenarios

Cold  
Optimized for rarely accessed data and backup scenarios

### Azure Files

Enable Managed Identity for SMB

Require Encryption in Transit for SMB \*

---

[Previous](#) [Next](#) [Review + create](#)

配置儲存帳戶

5.按一下下一步配置網路。

6.將Network access設定為Enable public access from all networks。

## 7.將Routing preference設定為Microsoft network routing。



附註：附註：在生產環境中，考慮使用儲存帳戶上的防火牆規則限制對特定IP範圍（ISE節點IP地址）的訪問。

Home > Storage center | Blob Storage

### Create a storage account

Note: Allowing access to your resource through a public network increases security risk. [Learn more](#)

Public network access \* ⓘ

Enable  
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.

Disable  
Restrict inbound access while allowing outbound access.

Secure by perimeter (Most restricted)  
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

Public network access scope \*

Enable from all networks

Enable from selected virtual networks and IP addresses

▲ Enabling public network access will make this resource available publicly. Unless public access is required, consider using the most restricted access configurations.

**Private endpoint**

Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.

+ Add private endpoint

Name	Subscription	Resource g...	Region	Target sub-...	Subnet	Private DN...
------	--------------	---------------	--------	----------------	--------	---------------

Click on add to create a private endpoint

**Network routing**

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference \* ⓘ

Microsoft network routing

Internet routing

Previous Next Review + create

8. 按一下下一步，將資料保護、安全和加密保留為預設值。實驗室或標準部署不需要其他配置。
9. 按一下複查+建立。驗證通過後，按一下Create。
10. 等待部署完成，然後按一下轉至資源。
11. 在Azure儲存帳戶上配置SFTP:在新建立的儲存帳戶中，導航到Data storage > Containers > Add container以新增容器
12. 提供容器名稱。按一下「Create」。
13. 導航到左側選單中的設定> SFTP以新增sftp使用者。按一下Add local user並配置以下內容：

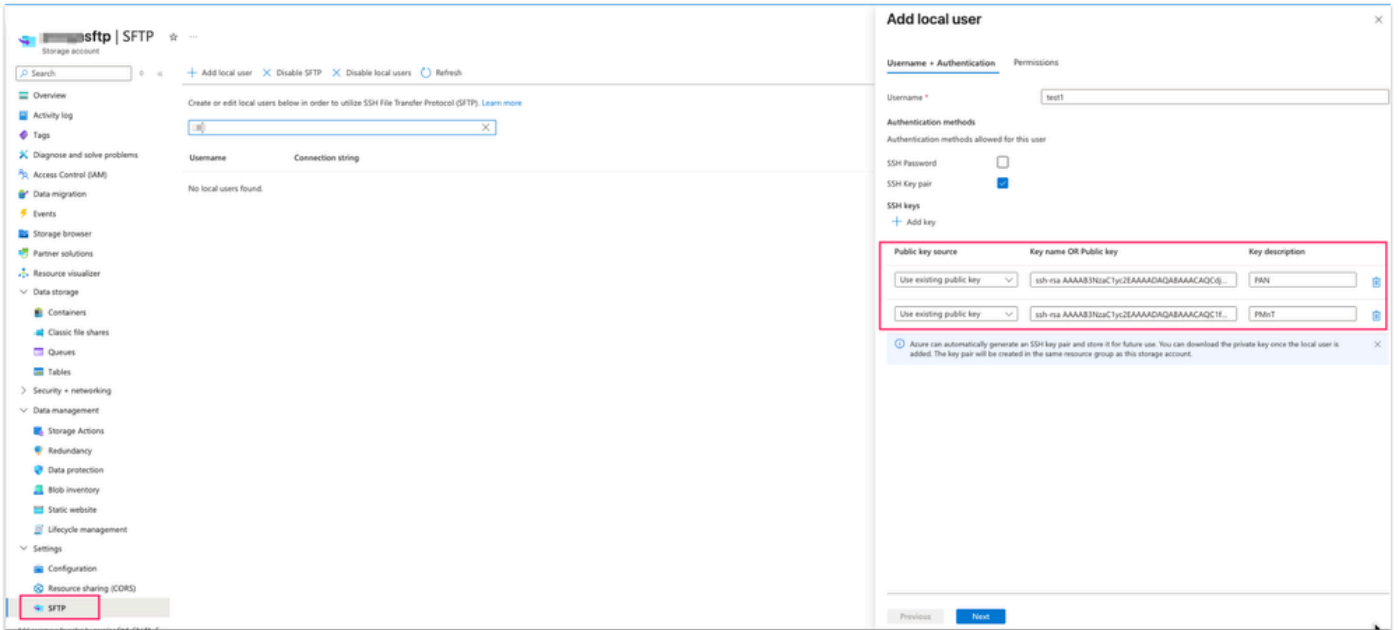
欄位	價值
使用者名稱	描述性名稱
認證方法	SSH金鑰對 — 不使用密碼
SSH公鑰源	使用現有金鑰 ( 在步驟1中生成，即id_rsa.pub金鑰 )



附註：在多節點部署中，當主PAN和主MnT是單獨的節點時，id\_rsa.pub檔案具有來自主PAN和主MnT節點的RSA公鑰。

14. 要使用SSH金鑰選項下的現有公鑰，請在您選擇的文本編輯器中開啟id\_rsa.pub檔案，然後通過兩次按一下Add key選項分別複製貼上兩個節點金鑰(從ssh-rsa開始並以root@your\_node\_name結束)。

Sample key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQcdjUFU6QaMQfxuR/yzbw1QWZ8EwUJjN/C0cNNM1kMOQE9f1JQ6GoC



在Azure上新增公鑰

15. 按一下「權限」。最初選擇在此步驟中建立的容器，並將容器的許可權設定為「讀取」、「寫入」、「清單」、「刪除」和「建立」。

16. 將Home目錄設定為容器的根。

17. 保存使用者。

## ISE GUI儲存庫配置

1. 導航至「管理」>「系統」>「維護」>「儲存庫」，然後按一下Add。按如下方式填寫欄位：

欄位	價值
儲存庫名稱	描述性標籤 ( 如Azure-SFTP )
通訊協定	SFTP
伺服器名稱	<storage_account_name>.blob.core.windows.net
Path	/ ( 根目錄 )
驗證	PKI

使用者名稱	<storage_account_name>.<container_name>.<sftp_local_username>
密碼	留空

2. 按一下提交以儲存儲存庫。

ISE SFTP儲存庫配置



**警告：**必須先使用 `crypto host_key add executable` 命令通過CLI新增sftp伺服器的主機金鑰，然後才能使用此儲存庫。此外，請確保主機金鑰字串與資料庫配置URL中使用的主機名相匹配。要訪問啟用PKI的儲存庫，請從GUI生成金鑰對，並將公鑰匯出到本地電腦上。將此公鑰複製到啟用了PKI的SFTP伺服器，並將其新增到「authorized\_keys」檔案中。

3. 登入到主管理節點和主監控節點，並使用 `crypto host_key ad host <sftp server>` 命令新增加密主機密鑰。確保ISE節點能夠解析sftp主機名。

```
<#root>
```

```
isenode1/iseadmin#
```

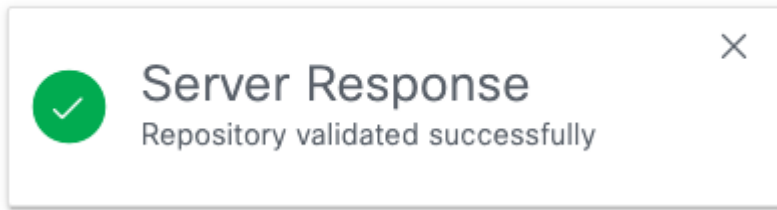
```
crypto host_key add host xxxxsftp.blob.core.windows.net
```

```
host key fingerprint added
```

```
# Host xxxxsftp.blob.core.windows.net found: line 1
```

```
xxxxsftp.blob.core.windows.net RSA SHA256:sP18dIvbSZgtEa5a2ea+Fy4P54Wd2ocEkToBq6xG74g
```

4. 返回Repository下的ISE GUI，選擇新建立的儲存庫，然後按一下Validate。已成功驗證儲存庫。



儲存庫驗證成功



附註：儲存庫驗證選項僅在主管理節點上驗證儲存庫配置。



附註：在使用RSA公鑰建立的SFTP儲存庫的情況下，通過GUI建立的儲存庫不會在CLI中複製，而通過CLI建立的儲存庫不會在GUI中複製。要在CLI和GUI上配置相同的儲存庫，請在CLI和GUI上生成RSA公鑰，並將這兩個金鑰匯出到SFTP伺服器。

## ISE CLI儲存庫配置

1.通過SSH連線到主管理節點的CLI（命令列介面）。在要從CLI訪問基於PKI的SFTP儲存庫的部署中的每個節點上新增加密金鑰。

2.為CLI生成rsa公鑰。

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

3.將生成的公鑰檔案匯出到本地磁碟儲存庫（您有權下載該檔案的所有儲存庫）。

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

4.從儲存庫下載此檔案，然後在文本編輯器中將其開啟，以複製公鑰以進行CLI訪問。

5.將SSH公鑰上傳到Azure，與在Azure SFTP本地使用者建立螢幕下新增的GUI金鑰相同（來自步驟3）。

6.按一下Add key並貼上完整的SSH公鑰（貼上到SSH公鑰欄位中）。

7. ( 可選 ) 提供金鑰說明(例如ISE-CLI-Key)。

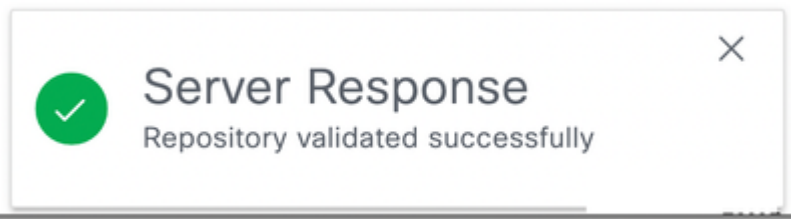
8.按一下Next和Save。

## 驗證

1.使用「show repository <Repository name>」命令驗證對sftp儲存庫的CLI訪問許可權。它顯示此sftp伺服器上儲存的檔案。

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

2.通過導航到「儲存庫」並選擇「新建立的儲存庫」並按一下「驗證」來驗證GUI對sftp儲存庫的訪問。已成功驗證儲存庫。



3.導覽至Administration > System > Backup and Restore。進行配置備份，然後轉到此頁底部，選擇SFTP儲存庫，在配置下，可以顯示要還原的最新備份。

The screenshot shows the Cisco Identity Services Engine Administration / System Backup & Restore page. The left sidebar contains navigation options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is divided into two panels: 'Configurational Backup Details' and 'Operational Backup Details'. Below these panels, there is a section for 'Azure-SFTP' with an 'Add Repository' button and tabs for 'Configuration' and 'Operational'. A table lists backup files with their names, modified times, repository names, and sizes (all 0 Bytes).

File Name	Modified Time	Repository	Size
azure-backup-CFG10-260...	Sat Jan 8 00:00:00 0	Azure-SFTP	0 Bytes
testbackup-CFG10-260522...	Tue Jan 4 00:00:00 0	Azure-SFTP	0 Bytes
testbackup2-CFG10-2605...	Tue Jan 11 00:00:00 0	Azure-SFTP	0 Bytes

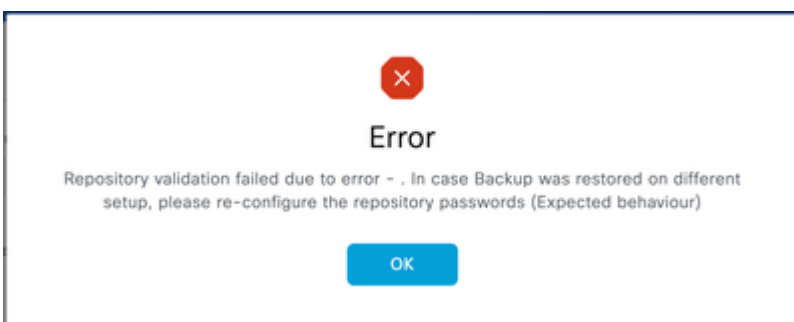
sftp儲存庫驗證



附註：由於修飾的Cisco錯誤[IDCSCwu6863](#)，此處將Azure儲存上的備份大小視為0位元組，但不會影響功能。如果需要，可以成功恢復這些備份。

## 疑難排解

1.在ISE GUI中，系統資訊庫驗證將產生以下錯誤：



錯誤消息

## 解析

檢查是否在SSH金鑰下在SFTP伺服器上匯入了正確的公鑰 ( 請參閱在Azure儲存帳戶上配置SFTP的步驟2 )。 如果使用者在成功驗證儲存庫後在GUI上再次生成新的金鑰對，則會發生此錯誤。

2. GUI儲存庫驗證成功，但show repository <sftp repository>命令沒有輸出。

```
isenode1/iseadmin#show repository Azure-SFTP
% SSH connect error
```

錯誤螢幕截圖

### 解析

檢查從CLI生成的RSA公鑰是否已新增到Azure ssh配置中。

3.為了進一步排除SFTP資料庫問題，請啟用debug命令：

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

```
isenode1/iseadmin#debug transfer 7
isenode1/iseadmin#show repository Azure-SFTP
6 [395485]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository Azure-SFTP requested
6 [395485]:[info] transfer: cars_xfer_util.c[2755] [system]: Server validation successful .core.windows.net
7 [395485]:[debug] transfer: sftp_handler.c[1281] [system]: Running sftp command: .blob.core.windows.net *** / ls -l /
6 [395485]:[info] transfer: sftp_handler.c[689] [system]: DEBUG: local user: iseadmin UID: 0 sftp_run_parent FD: 7 remote host: .blob.core.windows.net remote user: . command: ls -l /
7 [395485]:[debug] transfer: sftp_handler.c[699] [system]: fd is:7
7 [395486]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 iseadmin /usr/bin/sftp -oIdentityFile=/home/iseadmin/.ssh/id_rsa -oUseKnownHostsFile=/home/iseadmin/.ssh/known_hosts -oPasswordAuthentication=no .t @.blob.core.windows.net
3 [395485]:[error] transfer: sftp_handler.c[445] [system]: sftp_read Error: read failed
3 [395485]:[error] transfer: sftp_handler.c[914] [system]: sftp_run_parent Error: read(command prompt) failed
7 [395485]:[debug] transfer: sftp_handler.c[1123] [system]: sftp parent status -306
% SSH connect error
```

調試日誌

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。