ISE에서 Azure SFTP Blob 저장소 리포지토리 구성 및 문제 해결

목차

소개

이 문서에서는 Azure Blob 저장소를 ISE(Identity Services Engine)를 통한 공개 키 인프라 인증을 통해 SFTP 서버로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 일반 ISE 지식
- ISE 리포지토리 컨피그레이션
- PKI(Public Key Infrastructure) 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Azure의 ISE 3.3, 3.4, 3.5 VM
- 저장소 센터에 액세스하기 위한 Azure 구독

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

클라우드 네이티브 서비스인 Azure Blob Storage SFTP 리포지토리는 배포가 쉽고 Azure 기반 ISE 구현에 이상적입니다. 이 솔루션은 온프레미스 접속 문제를 없애고, 자동으로 확장하여 변화하는 스토리지 요구 사항을 충족하며, 대규모 데이터 세트에 대한 고가용성과 내구성을 보장하는 동시에 수동 인프라 관리가 필요하지 않습니다.

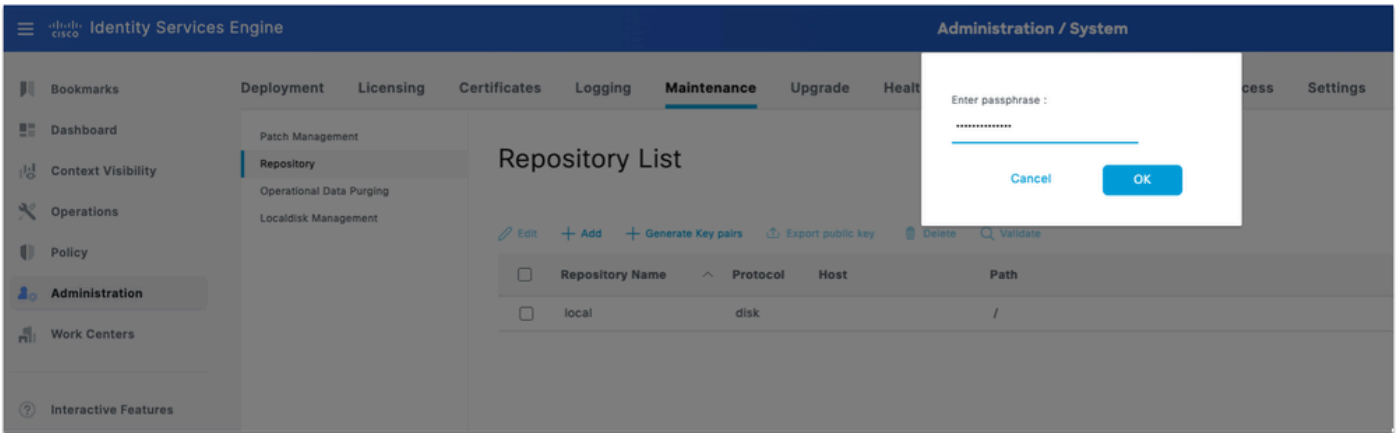
구성

ISE 사전 컨피그레이션

1. ISE에서 키 쌍을 생성합니다. 기본 관리 노드 GUI에 로그인합니다. Administration > System > Maintenance > Repository로 이동합니다.

2. 저장소 목록에서 [키 쌍 생성] 옵션을 클릭합니다.

3. 패스프레이즈(13자 이상)를 입력하고 확인을 클릭합니다. 키 쌍을 보호하려면 이 작업이 필요합니다.



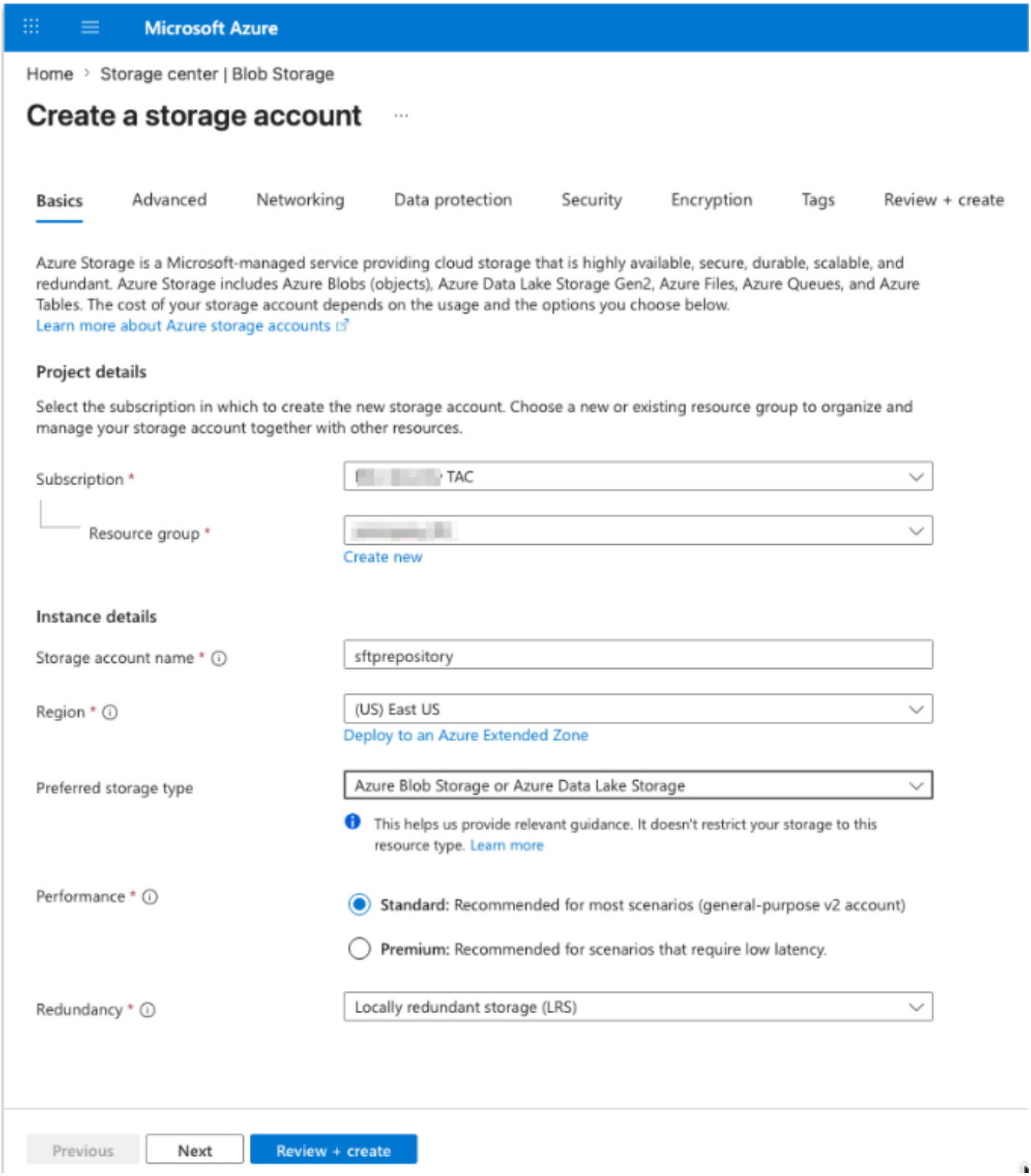
ISE에서 키 쌍 생성

4. Export public key(공개 키 내보내기)를 클릭하고 컴퓨터에서 id_rsa.pub 키를 다운로드합니다(나중에 참조할 수 있도록 저장되었는지 확인).

Azure SFTP 구성

1. Azure 저장소 계정을 만들고 구성합니다. Azure 포털에 로그인하고 저장소 계정으로 이동합니다. Resources(리소스) 탭에서 Create(생성)를 클릭하여 새 스토리지 계정을 생성합니다. 세부 정보를 입력합니다.

필드	가치
서브스크립션	Azure 구독
리소스 그룹	기존 항목 선택 또는 새 항목 만들기
저장소 계정 이름	전역적으로 고유해야 함
지역	원하는 지역을 선택하십시오.
이중화	LRS(Locally Redundant Storage) - 실습/비실습에 적합

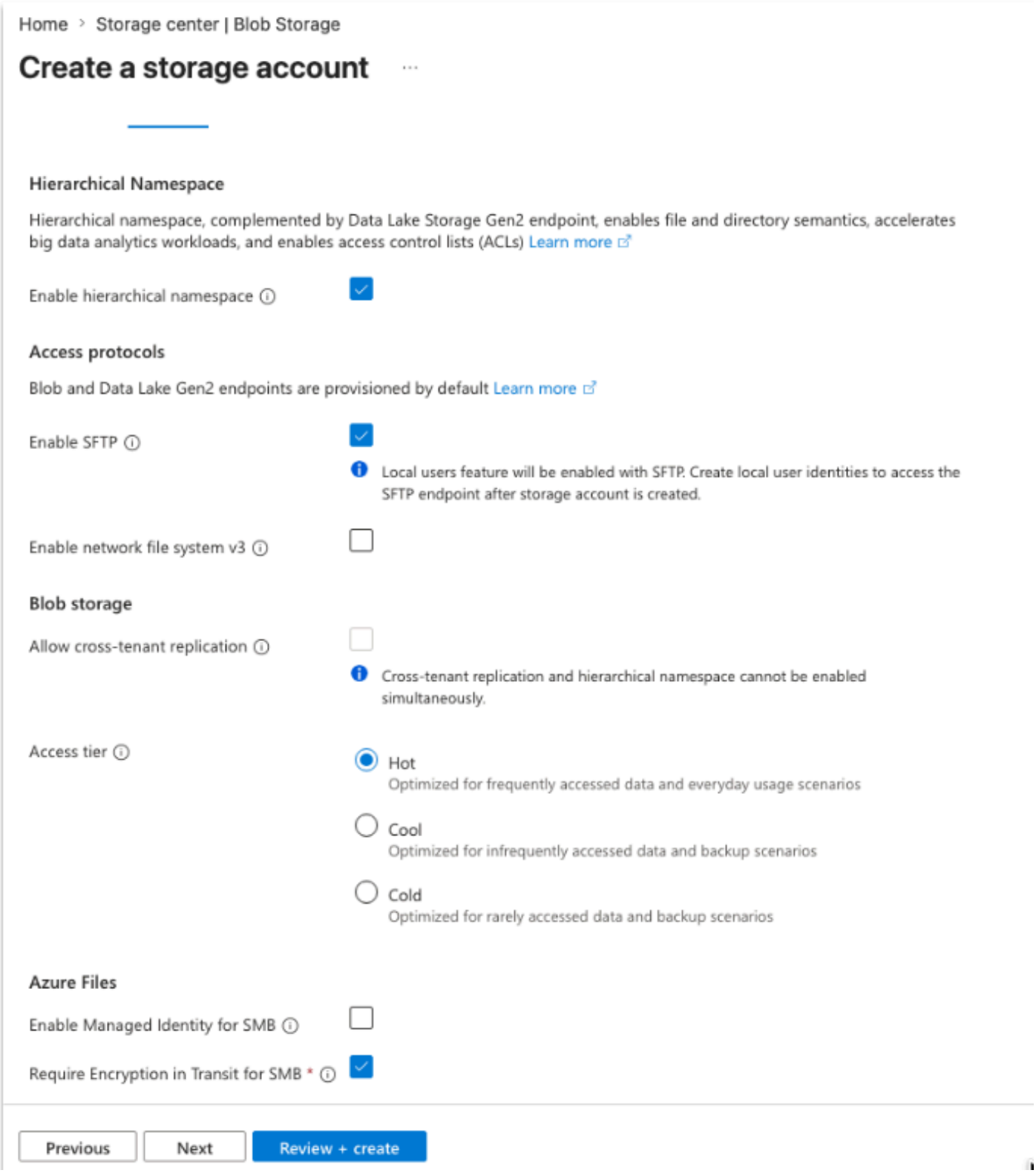


저장소 계정 만들기

2. 다음을 누르고 고급 탭에서 계층 네임스페이스 사용 체크박스를 선택합니다. 이 옵션은 필수입니다. SFTP는 계층적 네임스페이스 계정에만 활성화할 수 있습니다.

3. SFTP 사용 확인란을 선택합니다.

4. 나머지 옵션은 기본값으로 두거나 필요에 따라 조정합니다.



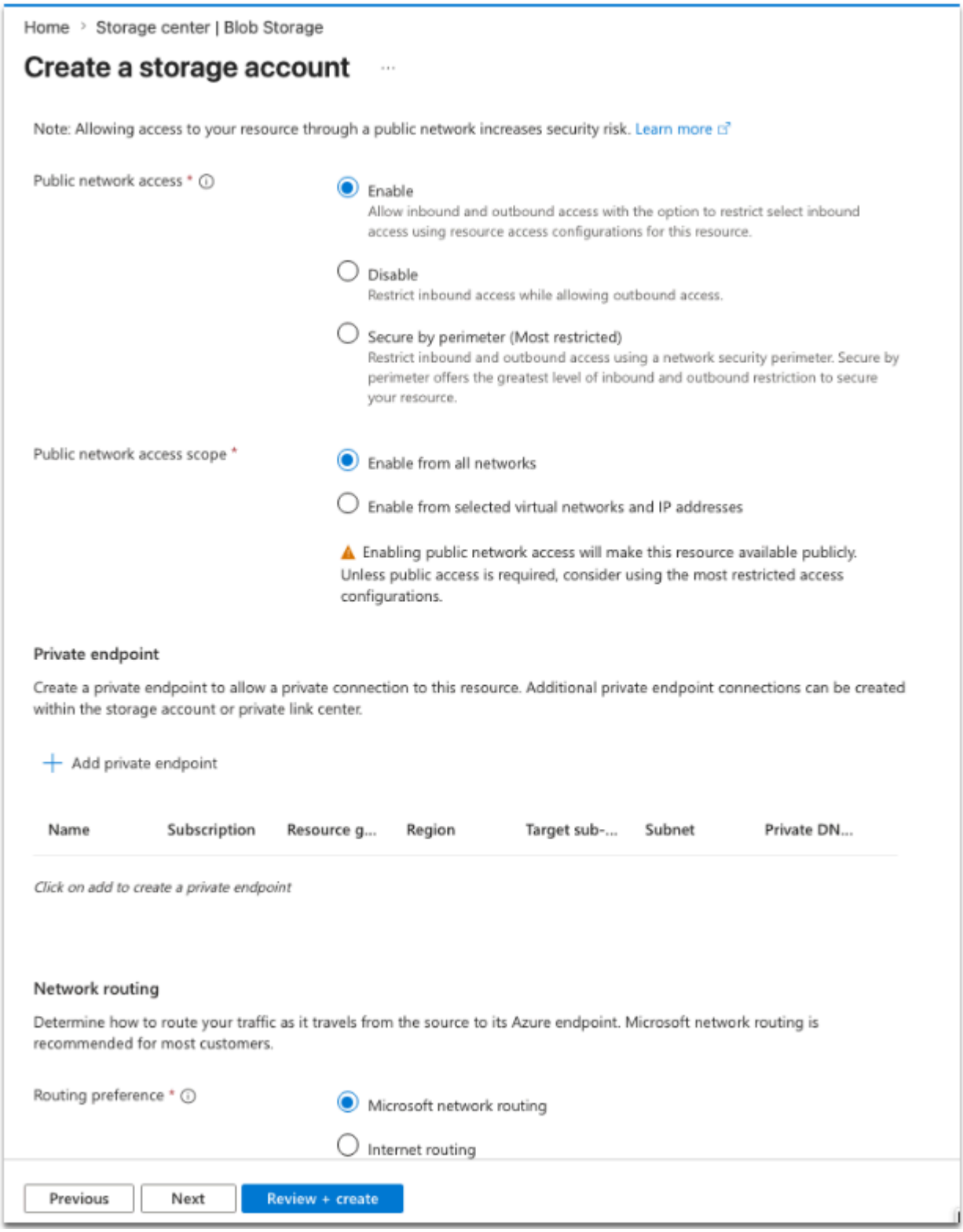
저장소 계정 구성

5. [다음]을 클릭하여 네트워킹을 구성합니다.

6. 모든 네트워크에서 공용 액세스를 사용하도록 네트워크 액세스를 설정합니다.

7. 라우팅 기본 설정을 Microsoft 네트워크 라우팅으로 설정합니다.

참고: 참고: 프로덕션 환경에서는 스토리지 계정의 방화벽 규칙을 사용하여 특정 IP 범위(ISE 노드 IP 주소)에 대한 액세스를 제한하는 것이 좋습니다.



네트워크 설정

8. 다음을 클릭하고 데이터 보호, 보안 및 암호화를 기본값으로 둡니다. 실습 또는 표준 배포에 추가 구성이 필요하지 않습니다.

9. 검토 + 생성을 클릭합니다. 검증이 통과되면 생성을 클릭합니다.

10. 구축이 완료될 때까지 기다린 후 리소스로 이동을 클릭합니다.

11. Azure 저장소 계정에 SFTP를 구성합니다. 새로 만든 저장소 계정에서 데이터 저장소 > 컨테이너 > 컨테이너 추가로 이동하여 컨테이너를 추가합니다

12. 컨테이너 이름을 입력합니다. Create(생성)를 클릭합니다.

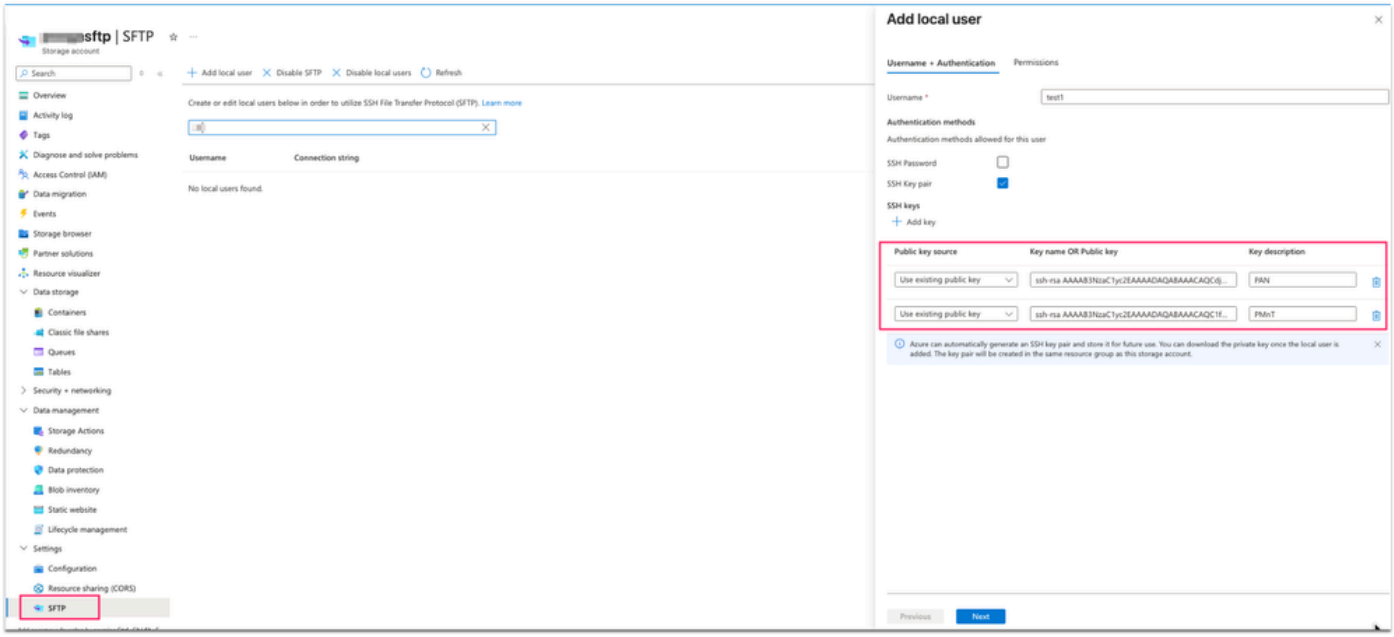
13. 왼쪽 메뉴에서 Settings(설정) > SFTP로 이동하여 sftp 사용자를 추가합니다. Add local user(로컬 사용자 추가)를 클릭하고 다음을 구성합니다.

필드	가치
사용자 이름	설명이 포함된 이름
인증 방법	SSH 키 쌍 — 비밀번호 사용 안 함
SSH 공개 키 소스	기존 키 사용(1단계에서 생성된 id_rsa.pub 키)

참고: 다중 노드 구축에서 주 PAN과 주 MnT가 별도의 노드인 경우 id_rsa.pub 파일은 주 PAN 및 주 MnT 노드 모두의 RSA 공개 키를 가집니다.

14. SSH 키 옵션에서 기존 공개 키를 사용하려면 선택한 텍스트 편집기에서 id_rsa.pub 파일을 열고 두 노드 키(ssh-rsa로 시작하여 root@your_node_name으로 끝나음)를 모두 복사하여 키 추가 옵션을 두 번 클릭하여 각각 붙여넣습니다.

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



Azure에 공개 키를 추가하는 중

15. 권한을 클릭합니다. 처음에 이 단계에서 만든 컨테이너를 선택하고 컨테이너에 대한 사용 권한을 Read, Write, List, Delete 및 Create로 설정합니다.

16. 홈 디렉토리를 컨테이너의 루트로 설정합니다.

17. 사용자를 저장합니다.

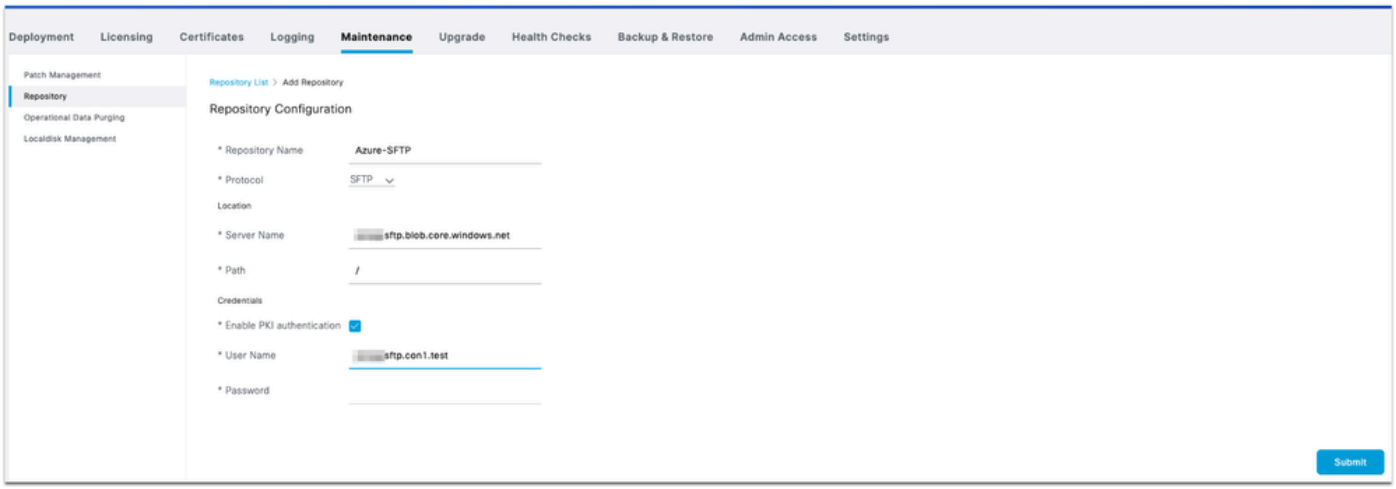
ISE GUI 저장소 컨피그레이션

1. Administration(관리) > System(시스템) > Maintenance(유지 관리) > Repository(저장소)로 이동하여 Add(추가)를 클릭합니다Add(추가)를 클릭합니다. 다음과 같이 필드를 채웁니다.

필드	가치
저장소 이름	설명 레이블(예: Azure-SFTP)
프로토콜	SFTP
서버 이름	<storage_account_name>.blob.core.windows.net
경로	/(루트 디렉토리)

인증	피키
사용자 이름	<storage_account_name>.<container_name>.<sftp_local_useraname>
암호	비워 둠

2. 제출을 눌러 저장소를 저장합니다.



ISE SFTP 저장소 컨피그레이션

경고: 이 리포지토리를 사용하려면 crypto host_key add executable 명령을 사용하여 sftp 서버의 호스트 키를 CLI를 통해 추가해야 합니다. 또한 호스트 키 문자열이 리포지토리 구성의 URL에 사용된 호스트 이름과 일치하는지 확인합니다. PKI 지원 리포지토리에 액세스하려면 GUI에서 키 쌍을 생성하고 로컬 시스템으로 공개 키를 내보냅니다. 이 공개 키를 PKI 지원 SFTP 서버에 복사하고 'authorized_keys' 파일에 추가합니다.

---

3. 기본 관리 노드와 기본 모니터링 노드에 모두 로그인하고 crypto host_key 및 host <sftp server> 명령을 사용하여 암호화 호스트 키를 추가합니다. ISE 노드가 sftp 호스트 이름을 확인할 수 있는지 확인합니다.

<#root>

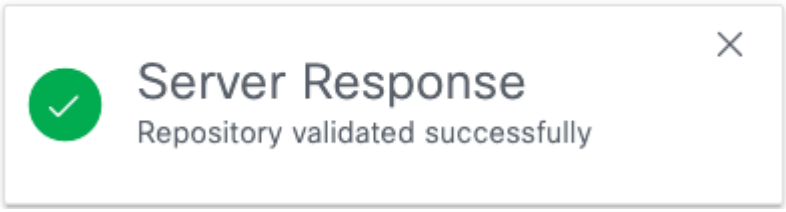
```
isenode1/iseadmin#

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. Repository(저장소) 아래의 ISE GUI로 돌아가 새로 생성된 저장소를 선택하고 Validate(검증)를 클릭합니다. 리포지토리의 유효성을 검사했습니다.



저장소 유효성 검사 성공

참고: 저장소 검증 옵션은 기본 관리 노드에서만 저장소 구성을 검증합니다.

참고: RSA 공개 키를 사용하여 만든 SFTP 저장소의 경우 GUI를 통해 만든 저장소는 CLI에서 복제되지 않으며 CLI를 통해 만든 저장소는 GUI에서 복제되지 않습니다. CLI 및 GUI에서 동일한 리포지토리를 구성하려면 CLI 및 GUI 모두에서 RSA 공개 키를 생성하고 두 키를 SFTP 서버로 내보냅니다.

ISE CLI 저장소 컨피그레이션

1. 기본 관리 노드의 CLI(Command Line Interface)에 SSH를 적용합니다. CLI에서 PKI 기반 SFTP 리포지토리에 액세스하려는 구축의 각 노드에 암호화 키를 추가합니다.

2. CLI용 rsa 공개 키를 생성합니다.

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

3. 생성된 공개 키 파일을 로컬 디스크 저장소(파일을 다운로드할 수 있는 액세스 권한이 있는 저장소)로 내보냅니다.

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

4. 저장소에서 이 파일을 다운로드하고 텍스트 편집기에서 열어 CLI 액세스를 위한 공개 키를 복사합니다.

5. Azure SFTP 로컬 사용자 생성 화면(3단계)에 추가된 GUI 키와 같은 SSH 공개 키를 Azure에 업로드합니다.

6. Add key(키 추가)를 클릭하고 전체 SSH 공개 키(SSH 공개 키 필드)를 붙여넣습니다.

7. 선택적으로, 주요 설명(예: ISE-CLI-Key)을 제공합니다.

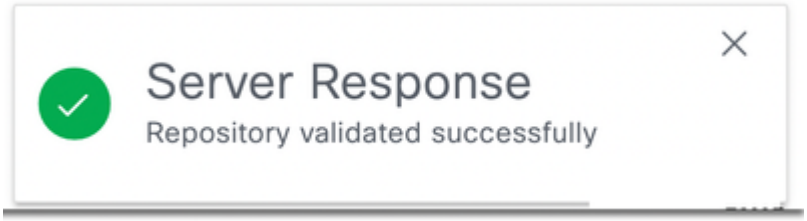
8. 다음을 클릭하고 저장합니다.

다음을 확인합니다.

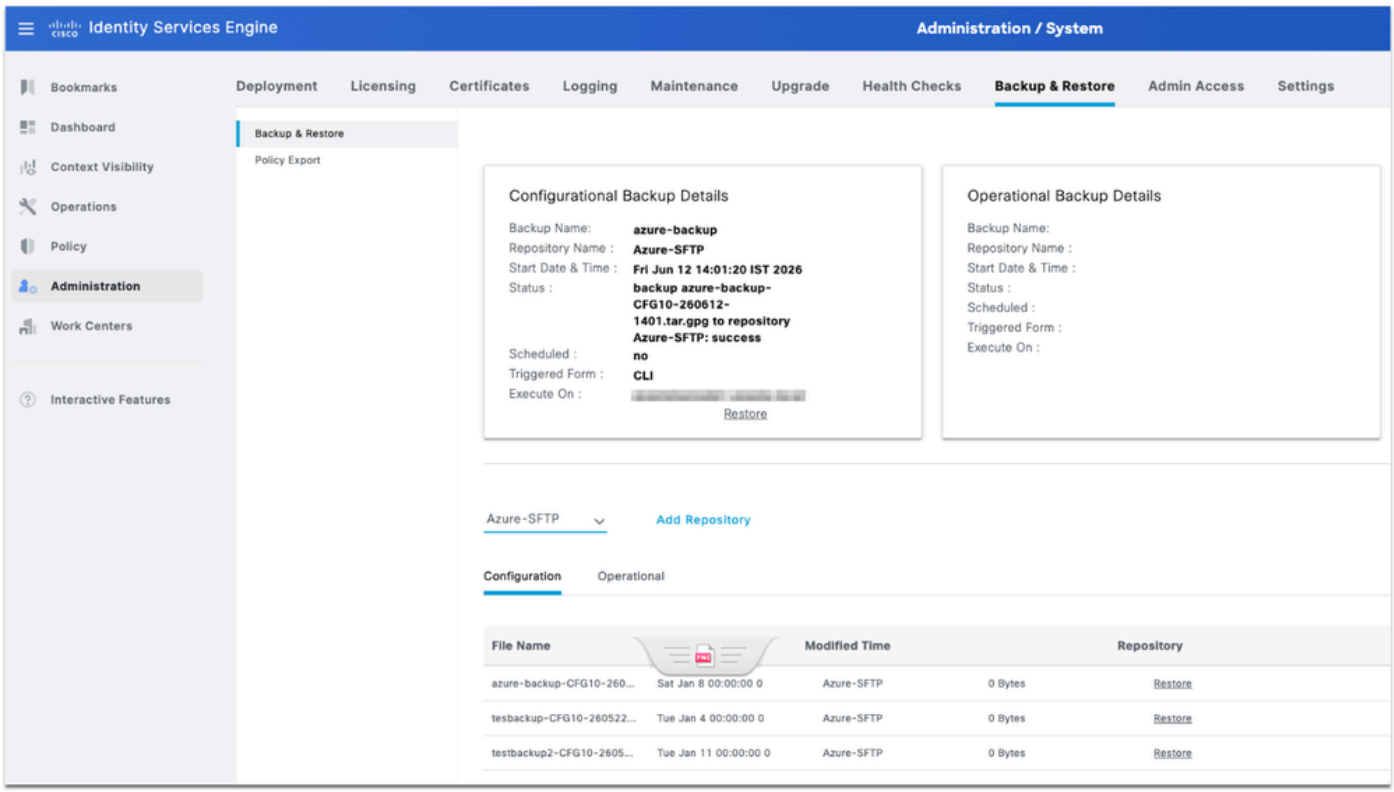
1. "show repository <Repository name>" 명령을 사용하여 sftp 리포지토리에 대한 CLI 액세스를 확인합니다. 이 sftp 서버에 저장된 파일이 표시됩니다.

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

2. 리포지토리로 이동하여 sftp 리포지토리에 대한 GUI 액세스를 확인하고 새로 생성된 리포지토리를 선택한 후 Validate(검증)를 클릭합니다. 리포지토리의 유효성을 검사했습니다.



3. Administration > System > Backup and Restore로 이동합니다. 컨피그레이션 백업을 수행한 다음 이 페이지의 맨 아래로 이동하여 SFTP 저장소를 선택하고 Configuration(컨피그레이션) 아래에 최근 백업이 표시되어 복원할 수 있습니다.

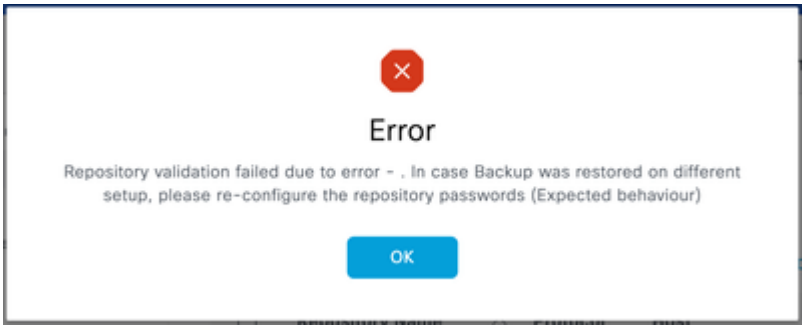


sftp 저장소 검증

참고: 외관상 Cisco 버그 IDCSCwu68863으로 인해 Azure 스토리지의 백업 크기가 0바이트로 표시되지만 기능적인 영향은 없습니다. 필요한 경우 이러한 백업을 성공적으로 복원할 수 있습니다.

문제 해결

1. ISE GUI에서 리포지토리 검증은 다음 오류를 제공합니다.



오류 메시지

해결

SSH 키 아래의 SFTP 서버에서 올바른 공개 키를 가져왔는지 확인합니다(Azure 저장소 계정에 SFTP 구성의 2단계 참조). 이 오류는 사용자가 리포지토리의 유효성을 검사한 후 GUI에서 새 키 쌍을 다시 생성한 경우 발생합니다.

2. GUI 리포지토리 검증에 성공했지만 show repository <sftp repository> 명령의 출력이 없습니다.

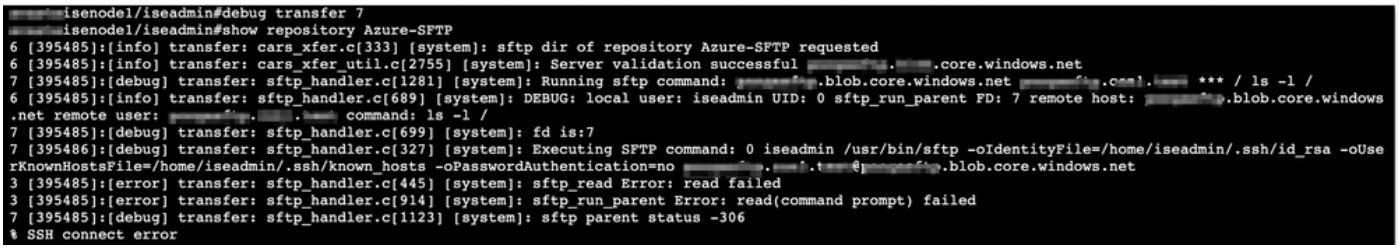
오류 스크린샷

해결

CLI에서 생성된 RSA 공개 키가 Azure ssh 구성에 추가되었는지 확인합니다.

3. SFTP 리포지토리 문제를 더 자세히 해결하려면 debug 명령을 활성화하십시오.

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



디버그 로그

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.