在ISE上配置并排除Azure SFTP Blob存储库故障

目录

简介

本文档介绍如何将Azure Blob存储配置为SFTP服务器，以使用身份服务引擎进行公钥基础结构身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 一般ISE知识
- ISE存储库配置
- 公钥基础设施(PKI)身份验证

使用的组件

本文档中的信息基于以下软件版本：

- Azure上的ISE 3.3、3.4、3.5 VM
- 用于访问存储中心的Azure订阅

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

作为云本机服务，Azure Blob存储SFTP存储库易于部署，是基于Azure的ISE实施的理想之选。它消除了本地连接问题，可自动扩展以满足波动的存储需求，并确保大型数据集的高可用性和持久性 — 同时消除了手动基础架构管理的需要。

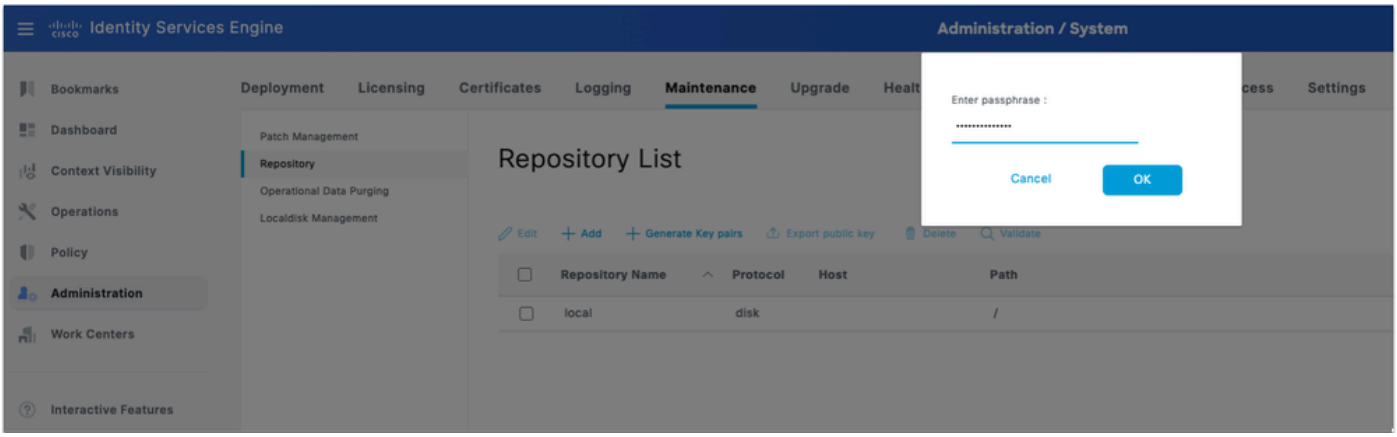
配置

ISE预配置

1.在ISE上生成密钥对：登录到主管理节点GUI。导航到管理 > 系统 > 维护 > 存储库。

2.在“资料库列表”下，单击生成密钥对选项。

3.输入口令（大于13个字符），然后单击确定。这是保护密钥对所必需的。



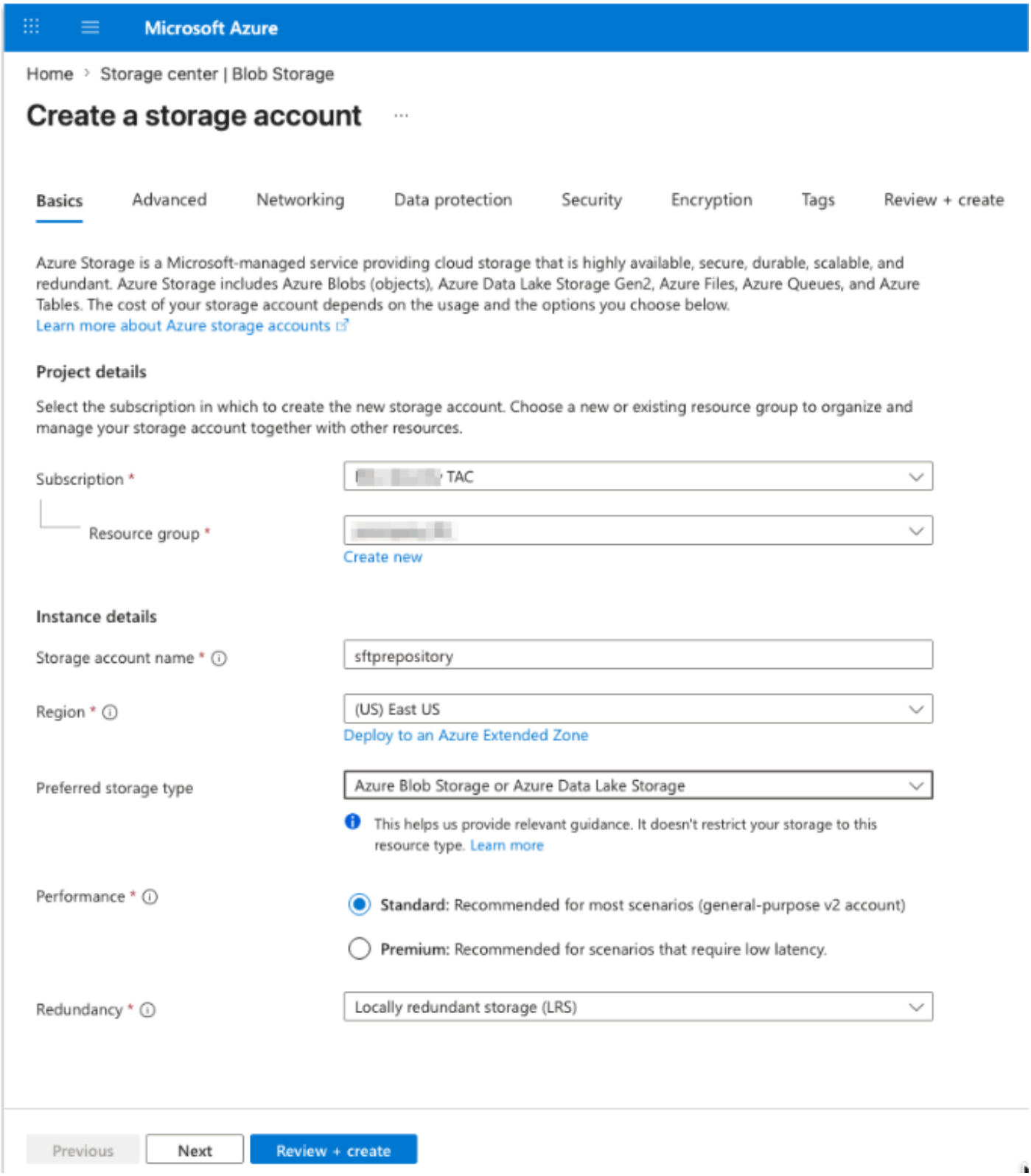
在ISE上生成密钥对

4.单击Export public key，然后在计算机上下载id_rsa.pub密钥（确保保存此密钥以供将来参考）。

Azure SFTP配置

1.创建和配置Azure存储帐户：登录到Azure门户并导航到Storage accounts。在Resources选项卡下，单击Create以创建新的存储帐户。填写详细信息：

字段	价值
订用	你的Azure订阅
资源组	选择现有或新建
存储帐户名称	必须是全局唯一的
地区	选择您的首选地区
冗余	本地冗余存储(LRS) — 适用于实验室/非生产环境

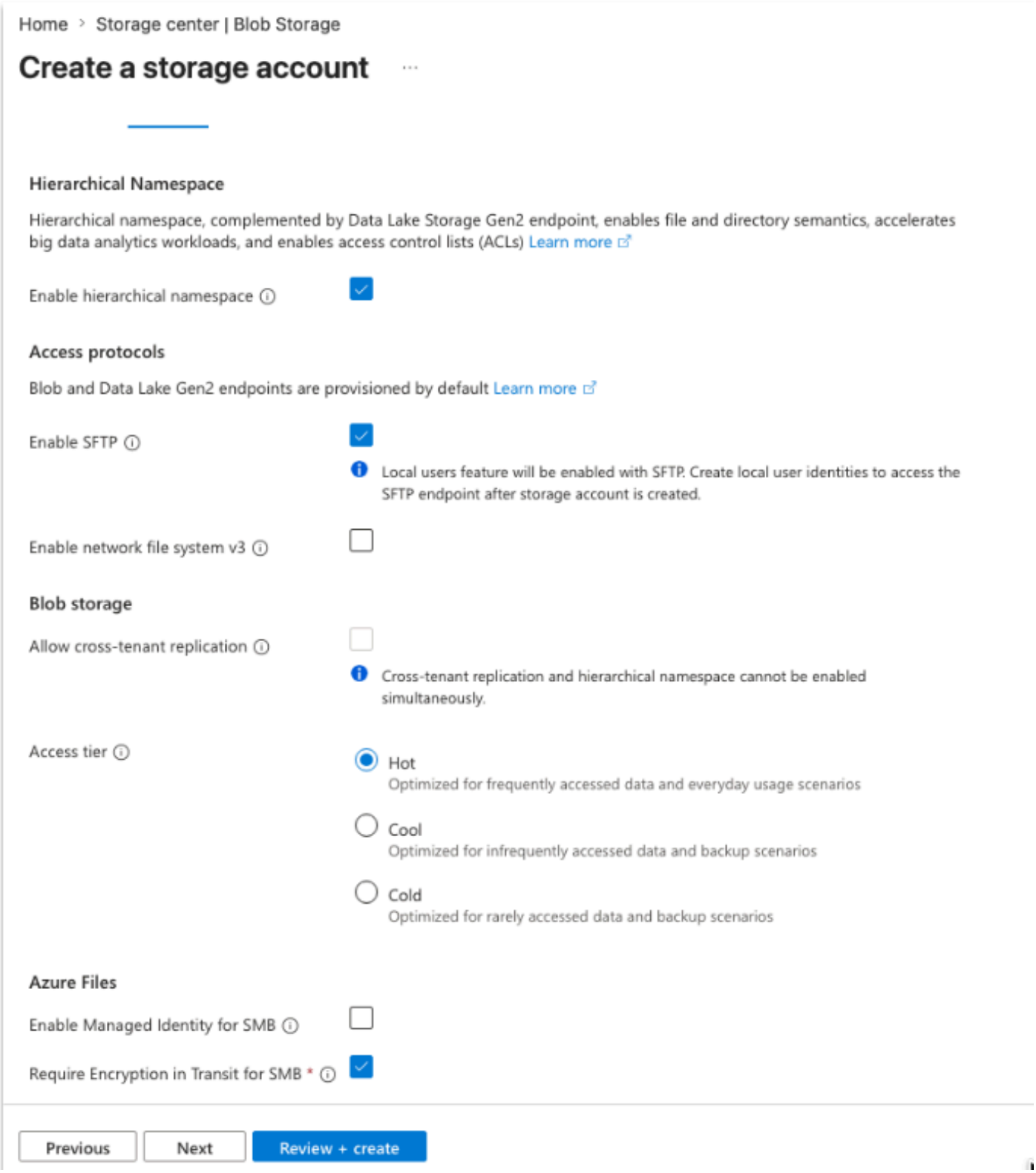


创建存储帐户

2.单击下一步，然后在高级选项卡下，选中启用分层名称空间复选框。此选项是必需的。只能为分层命名空间帐户启用SFTP。

3.选中启用SFTP复选框。

4.保留其余选项为默认选项或根据需要进行微调。



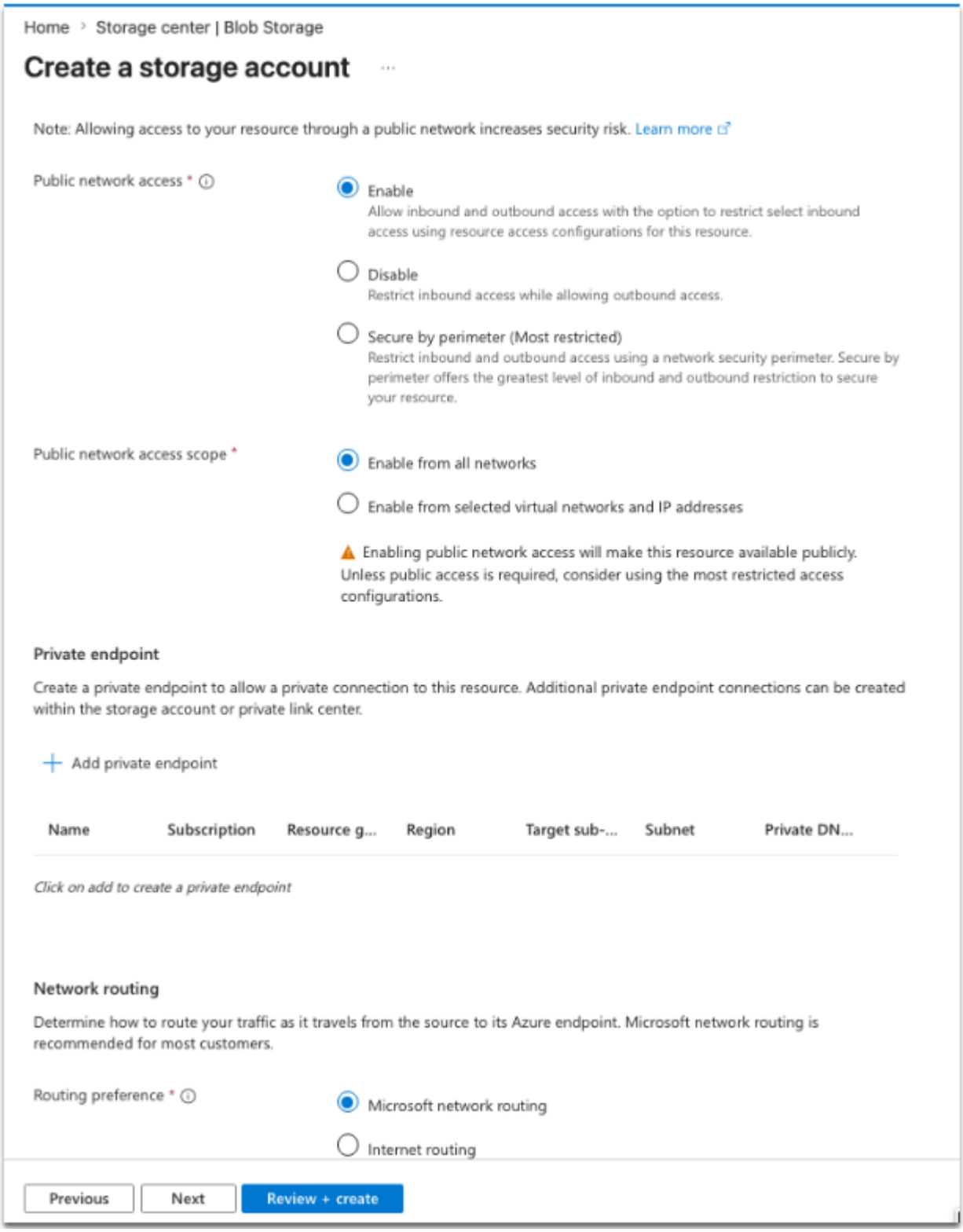
配置存储帐户

5.单击下一步配置网络。

6.将Network access设置为Enable public access from all networks。

7.将Routing preference设置为Microsoft network routing。

注意：注意：在生产环境中，考虑使用存储帐户上的防火墙规则限制对特定IP范围（ISE节点IP地址）的访问。



网络设置

8.单击下一步，将数据保护、安全性和加密保留为默认值。实验室或标准部署不需要其他配置。

9.单击复查+创建。验证通过后，单击Create。

10.等待部署完成，然后单击转至资源。

11.在Azure存储帐户上配置SFTP:在新创建的存储帐户中，通过导航到数据存储 > 容器 > 添加容器来添加容器

12.提供容器名称。Click Create.

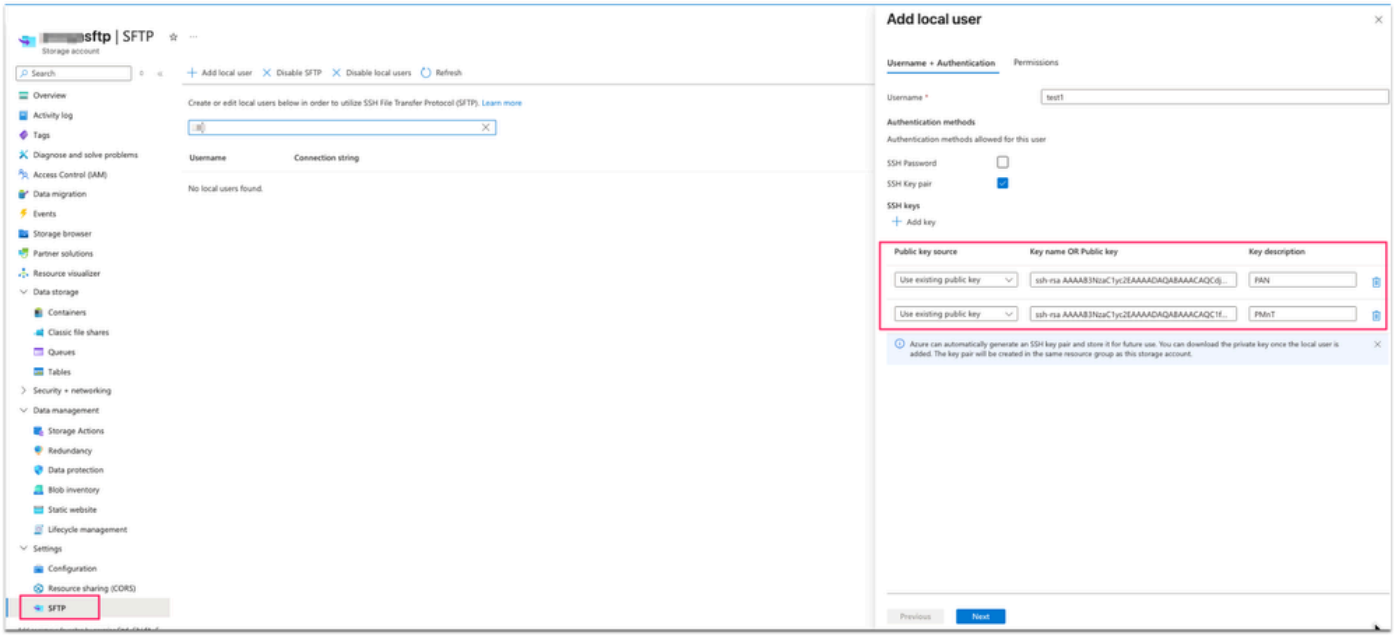
13.导航到左侧菜单中的设置>SFTP，添加sftp用户。单击Add local user并配置以下项：

字段	价值
用户名	描述性名称
认证方法	SSH密钥对 — 不使用密码
SSH公钥源	使用现有密钥（在步骤1中生成，即id_rsa.pub密钥）

注意：在多节点部署中，当主PAN和主MnT是单独的节点时，id_rsa.pub文件具有来自主PAN和主MnT节点的RSA公钥。

14.要使用SSH密钥选项下的现有公钥，请在您选择的文本编辑器中打开id_rsa.pub文件，然后通过两次点击Add key选项复制粘贴两个节点密钥(从ssh-rsa开始并以root@your_node_name)分别粘贴这两个节点密钥。

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



在Azure上添加公钥

15.单击“权限”。首先选择在此步骤中创建的容器，然后将容器的权限设置为读取、写入、列表、删除和创建。

16.将Home目录设置为容器的根。

17.保存用户。

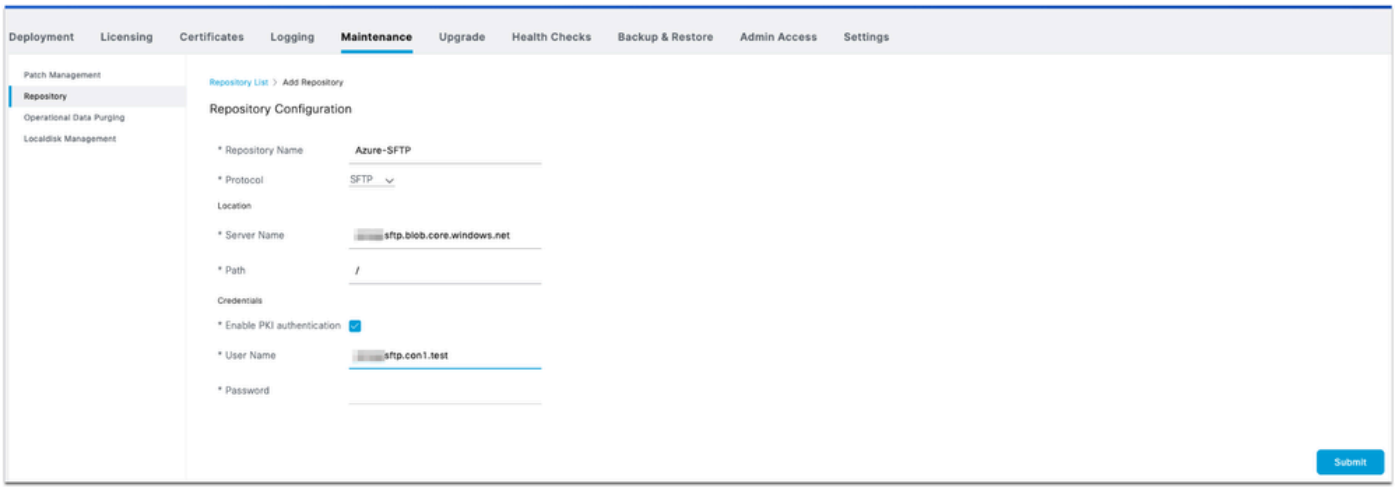
ISE GUI存储库配置

1.导航到“管理”(Administration)>“系统”(System)>“维护”(Maintenance)>“存储库”(Repository)，然后单击添加。按如下方式填写字段：

字段	价值
存储库名称	描述性标签（如Azure-SFTP）
协议	SFTP
服务器名称	<storage_account_name>.blob.core.windows.net
路径	/（根目录）

身份验证	PKI
用户名	<storage_account_name>.<container_name>.<sftp_local_useraname>
密码	留空

2.单击提交以保存存储库。



ISE SFTP存储库配置

警告：必须先使用crypto host_key add executable命令通过CLI添加sftp服务器的主机密钥，然后才能使用此存储库。此外，请确保主机密钥字符串与存储库配置的URL中使用的主机名相匹配。要访问启用PKI的存储库，请从GUI生成密钥对并将公钥导出到本地计算机上。将此公钥复制到启用PKI的SFTP服务器，并将其添加到“authorized_keys”文件。

3.登录到主管理节点和主监控节点并使用crypto host_key ad host <sftp server>命令添加加密主机密钥。确保ISE节点能够解析sftp主机名。

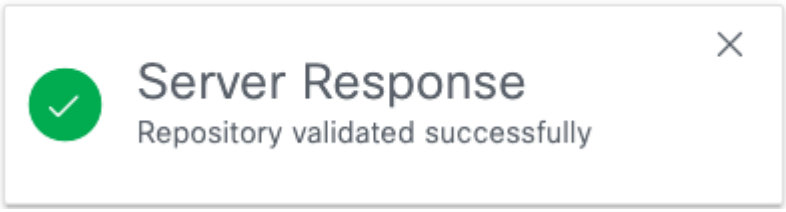
<#root>

```
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. 返回Repository下的ISE GUI，选择新创建的存储库，然后单击Validate。已成功验证存储库。



存储库验证成功

注意：存储库验证选项仅验证主管理节点上的存储库配置。

注意：如果使用RSA公钥创建SFTP存储库，则通过GUI创建的存储库不会在CLI中复制，通过CLI创建的存储库也不会在GUI中复制。要在CLI和GUI上配置相同的存储库，请在CLI和GUI上生成RSA公钥，并将这两个密钥导出到SFTP服务器。

ISE CLI存储库配置

1.通过SSH连接到主管理节点的CLI（命令行界面）。在部署中要从CLI访问基于PKI的SFTP存储库的每个节点上添加加密密钥。

2.生成CLI的rsa公钥。

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

3.将生成的公钥文件导出到本地磁盘存储库（您有权下载该文件的所有存储库）。

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

4.从存储库下载此文件，然后在文本编辑器中将其打开，以复制公钥以进行CLI访问。

5.将SSH公钥上载到Azure，与在Azure SFTP本地用户创建屏幕下添加的GUI密钥相同（从第3步开始）。

6.单击Add key并粘贴完整的SSH公钥(粘贴到SSH公钥字段中)。

7.（可选）提供密钥说明(例如ISE-CLI-Key)。

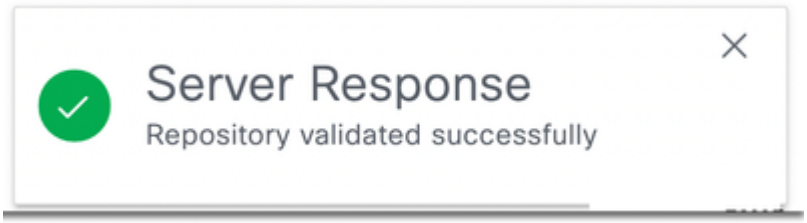
8.单击下一步和保存。

验证

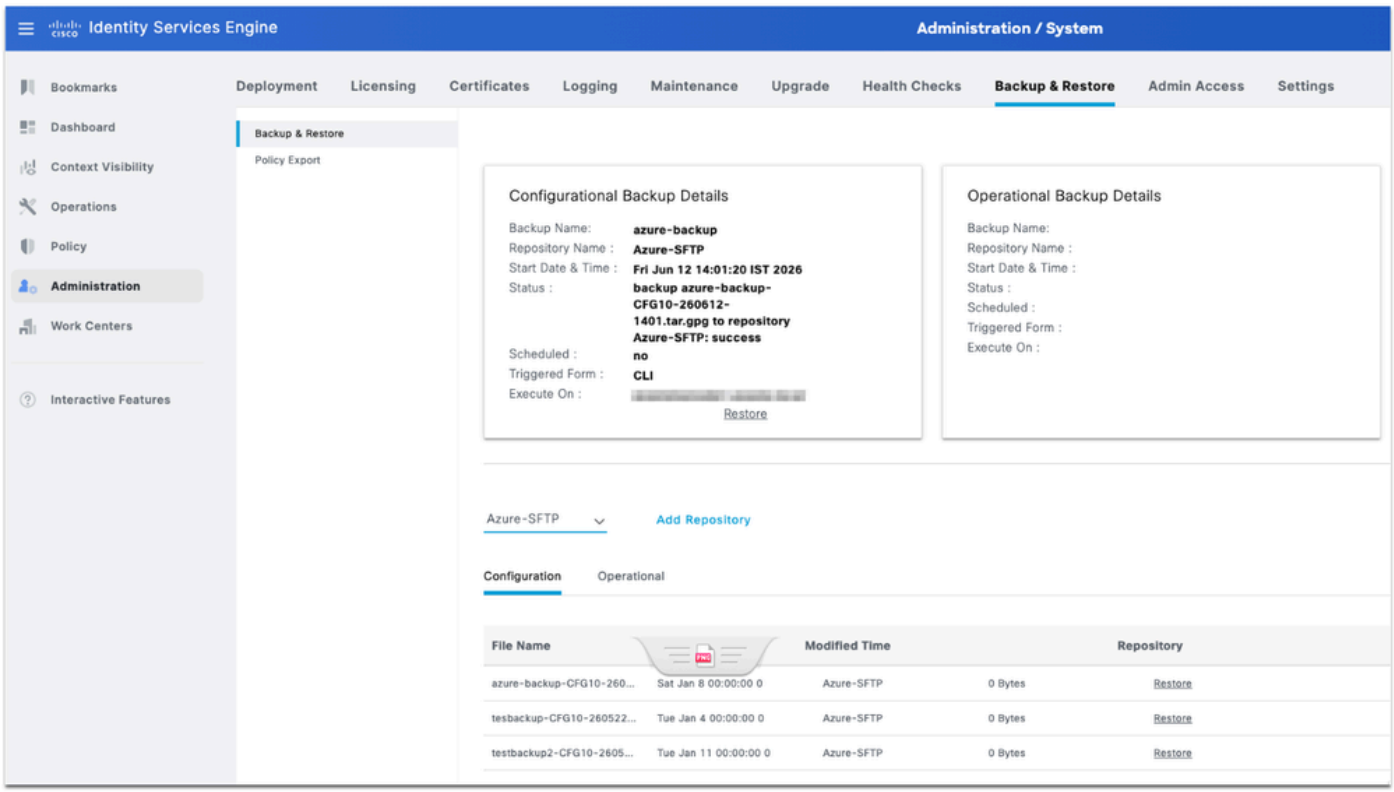
1.使用命令“show repository <Repository name>”验证对sftp存储库的CLI访问。 显示此sftp服务器上存储的文件。

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

2.通过导航到“存储库”并选择“新建的存储库”并单击验证，验证对sftp存储库的GUI访问。已成功验证存储库。



3.导航到管理 > 系统 > 备份和还原。执行配置备份，然后转到此页面底部，选择SFTP存储库，在配置下，可以看到要还原的最新备份。

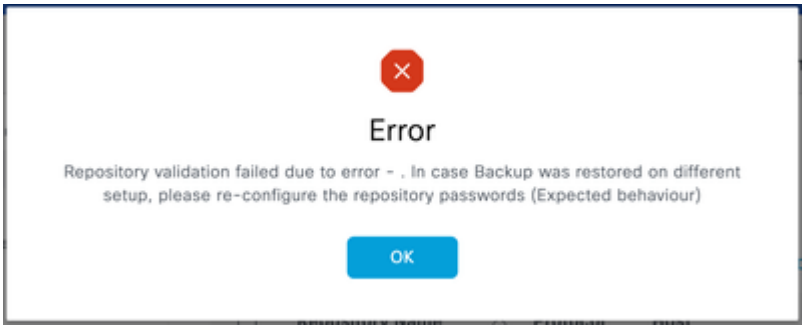


sftp存储库验证

注意：由于表面的Cisco bug IDCSCwu68863，此处将Azure存储上的备份大小视为0字节，但不会造成功能影响。如果需要，可以成功恢复这些备份。

故障排除

1.在ISE GUI中，系统信息库验证将产生以下错误：



错误消息

分辨率

检查在SFTP服务器上使用SSH密钥导入正确的公钥（请参阅在Azure存储帐户上配置SFTP的步骤2）。 如果用户在成功验证存储库后在GUI中再次生成新的密钥对，则会出现此错误。

2. GUI存储库验证成功，但show repository <sftp repository>命令没有输出。

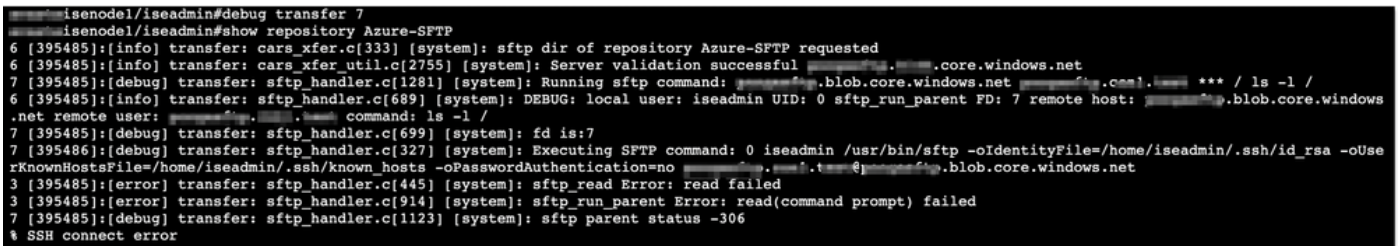
错误屏幕截图

分辨率

检查从CLI生成的RSA公钥是否已添加到Azure ssh配置下。

3.要进一步排除SFTP存储库问题，请启用debug命令：

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



调试日志

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。