使用Microsoft Server配置SWA中的SCP推送日志

目录

简介

先决条件

- 要求
- 使用的组件

SCP

SWA日志订阅

存档日志文件

在远程服务器上通过SCP配置日志检索

- 将SWA配置为从GUI向SCP远程服务器发送日志
- 将Microsoft Windows配置为SCP远程服务器

将SCP日志推送到其他驱动器

排除SCP日志推送故障

- 在SWA中查看日志
- 在SCP服务器中查看日志

相关内容

简介

本文档介绍配置安全复制(SCP)以自动将安全网络设备(SWA)中的日志复制到其他服务器的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- SCP的工作原理
- SWA管理
- Microsoft Windows或Linux操作系统的管理

Cisco 建议您：

- 已安装物理或虚拟SWA。

- 许可证已激活或已安装。
- 安装向导已完成。

- 对SWA图形用户界面(GUI)的管理访问。
- 已安装Microsoft Windows(至少Windows Server 2019或Windows 10(build 1809)。)或Linux系统。

使用的组件

本文档不限于特定的软件和硬件版本。

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。

SCP

安全复制(SCP)的行为类似于远程复制(RCP)，它来自Berkeley r-tools套件（Berkeley大学拥有的一组网络应用程序），不同之处在于SCP依赖安全外壳(SSH)提供安全性。此外，SCP要求配置身份验证、授权和记帐(AAA)授权，以便设备能够确定用户是否具有正确的权限级别

SCP on Remote Server方法（等同于SCP Push）通过使用SCP定期将日志文件复制到远程SCP服务器。此方法需要在使用SSH2协议的远程计算机上安装SSH SCP服务器。该订阅需要远程计算机上的用户名、SSH密钥和目标目录。根据您设置的滚动更新计划传输日志文件。

SWA日志订阅

可以为每种类型的日志文件创建多个日志订阅。订用包括存档和存储的配置详细信息，包括：

- 回滚设置，用于确定日志文件存档的时间。
- 已存档日志的压缩设置。
- 已存档日志的检索设置，用于指定日志是存档到远程服务器上还是存储在设备上。

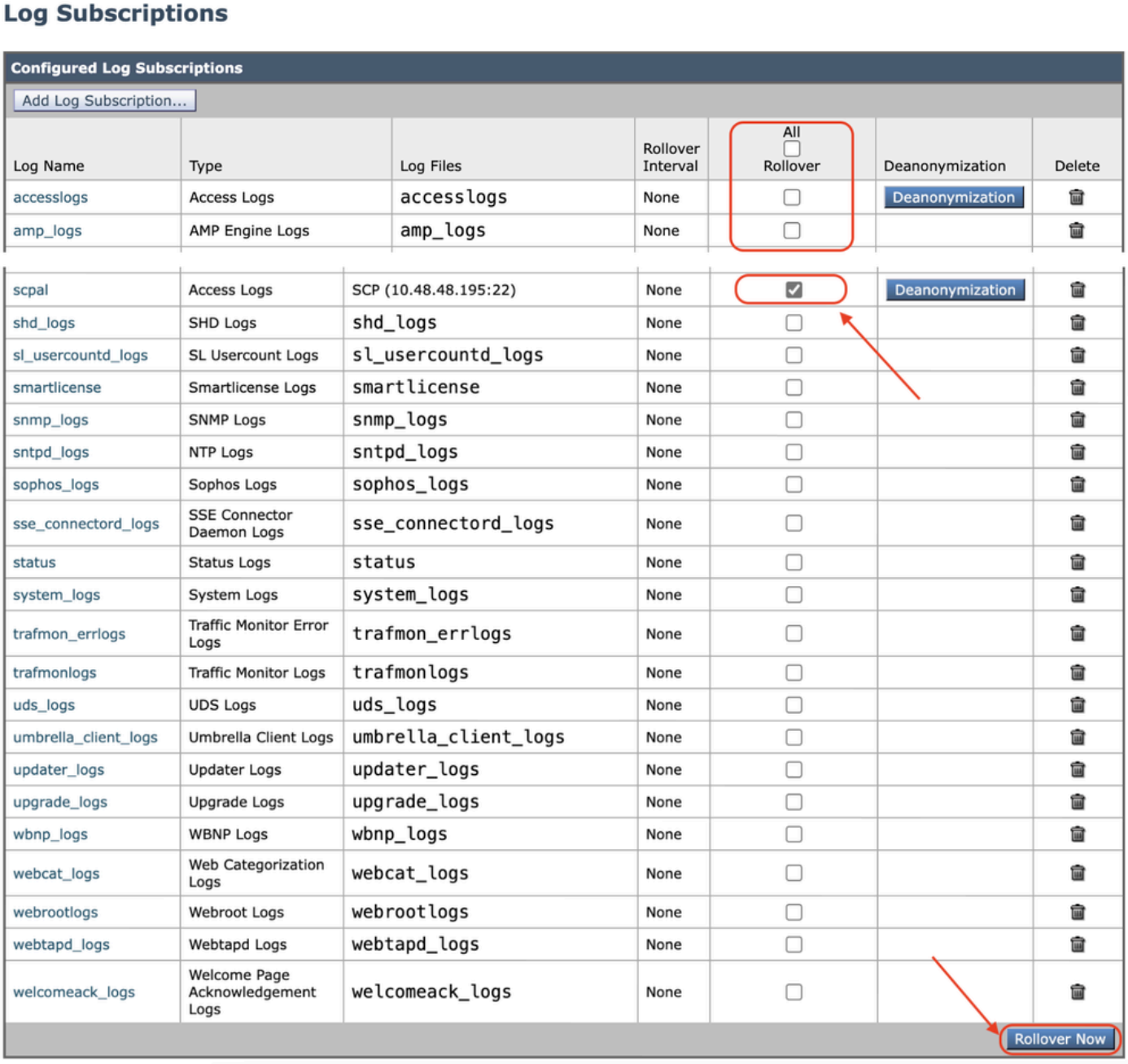
存档日志文件

当当前日志文件达到用户指定的最大文件大小限制或自上次滚动后的最长时间限制时，AsyncOS存档（回滚）日志订阅。

日志订阅中包含以下存档设置：

- 按文件大小滚动更新
- 按时间滚动更新
- 日志压缩
- 检索方法

您还可以手动存档（回滚）日志文件。
步骤1.选择System Administration > Log Subscriptions。
第2步：选中要存档的日志订用的回滚列中的复选框，或选中全部复选框以选择所有订用。
第3步：单击Rollover Now以存档选定的日志。



图像 — 立即回滚GUI

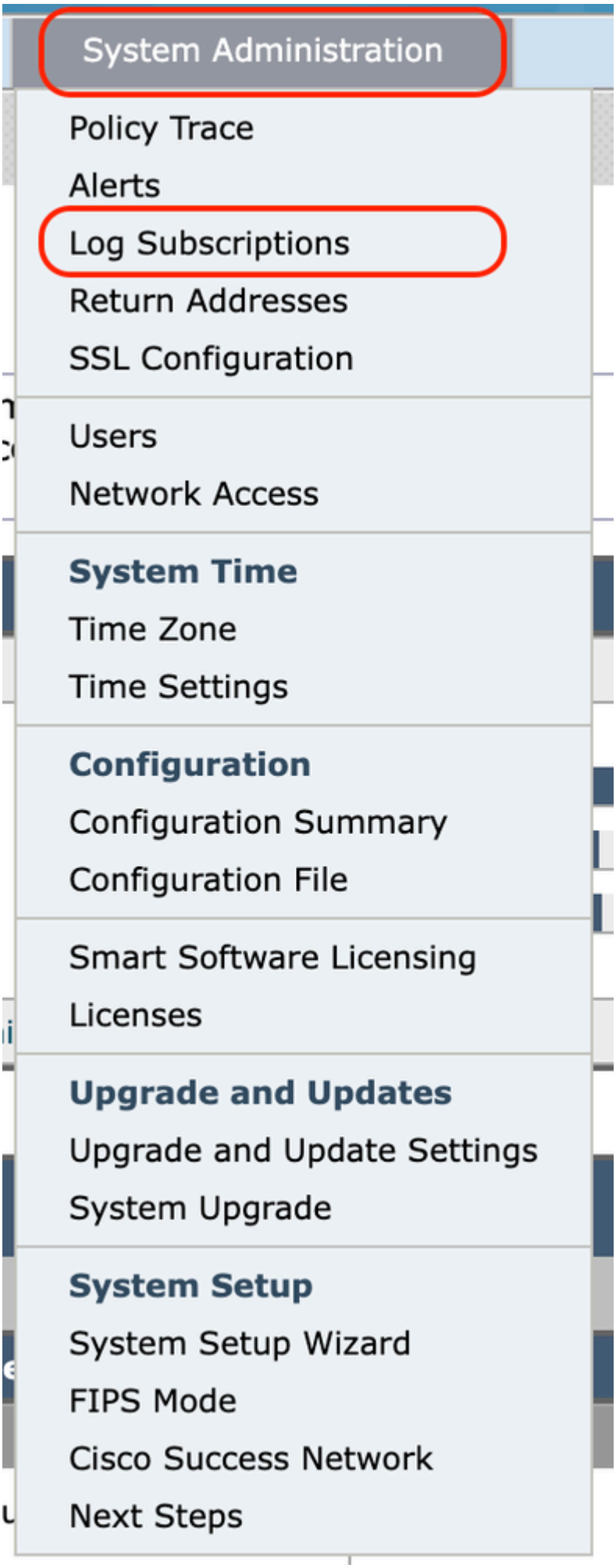
在远程服务器上通过SCP配置日志检索

从SWA使用SCP将日志检索到远程服务器有两个主要步骤：

1. 配置SWA以推送日志。
2. 配置远程服务器以接收日志。

将SWA配置为从GUI向SCP远程服务器发送日志

步骤1.登录SWA，从系统管理中选择Log Subscriptions。


System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary
Configuration File
Smart Software Licensing
Licenses
Upgrade and Updates
Upgrade and Update Settings
System Upgrade
System Setup
System Setup Wizard
FIPS Mode
Cisco Success Network
Next Steps

图像 — 选择日志订阅

第2步：在“日志订阅”页上，选择添加日志订阅:



图像 — 选择添加日志订阅

步骤3.选择日志类型。在本示例中，已选择访问日志。

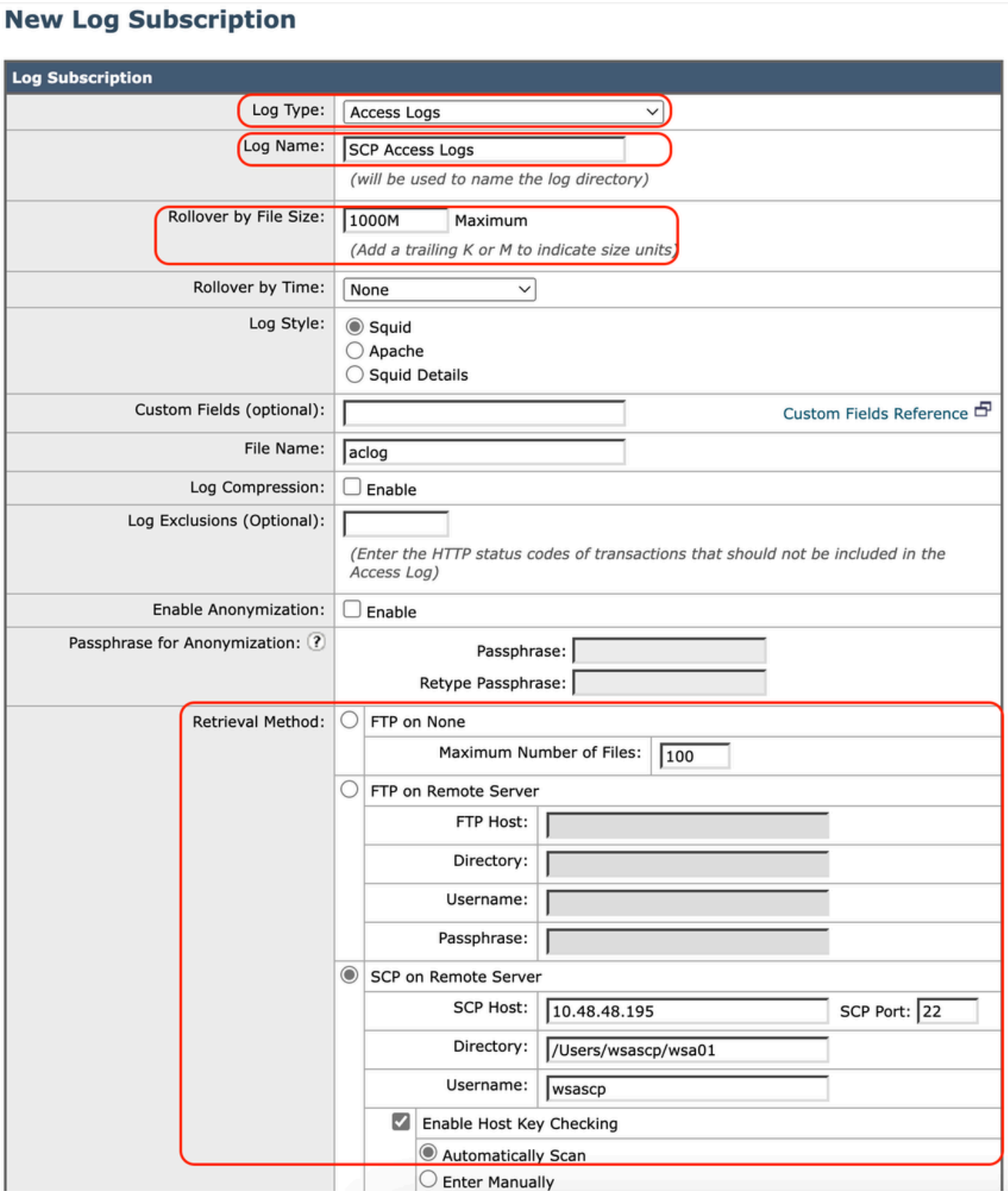
步骤4.输入日志订阅的名称。

步骤5.（可选）您可以按文件大小更改回滚。

步骤6.从Retrieval方法中选择SCP on Remote Server。

步骤7.输入远程服务器的以下信息：

- SCP主机名或IP地址
- 远程服务器上侦听SSH的侦听端口号（默认值为TCP/22）
- 目录名称
- 用于连接到远程服务器的用户名



映像 — 配置日志参数

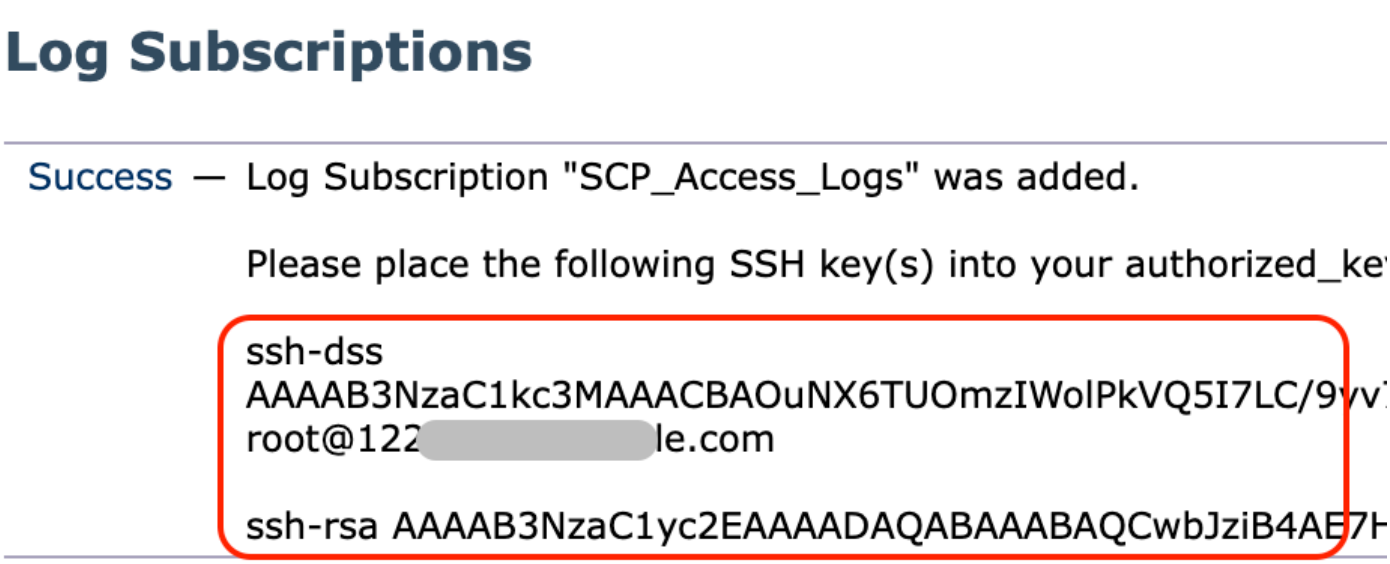
注意：在本示例中，用户名是wsascp，远程服务器是Microsoft Windows操作系统。已在c:\users\wccpscp文件夹（Microsoft中的用户配置文件文件夹）中创建文件夹wsa01。

提示：您只需键入文件夹名称;在本示例中，它是wsa01。

步骤8.提交更改。

步骤9.将SSH密钥保存到文本文件中，以便进一步在远程SCP服务器配置部分使用。

注意：您需要复制以ssh — 开头和以root@<SWA hostname>结束的两行。



映像 — 保存SSH密钥以供进一步使用。

步骤10.提交更改。

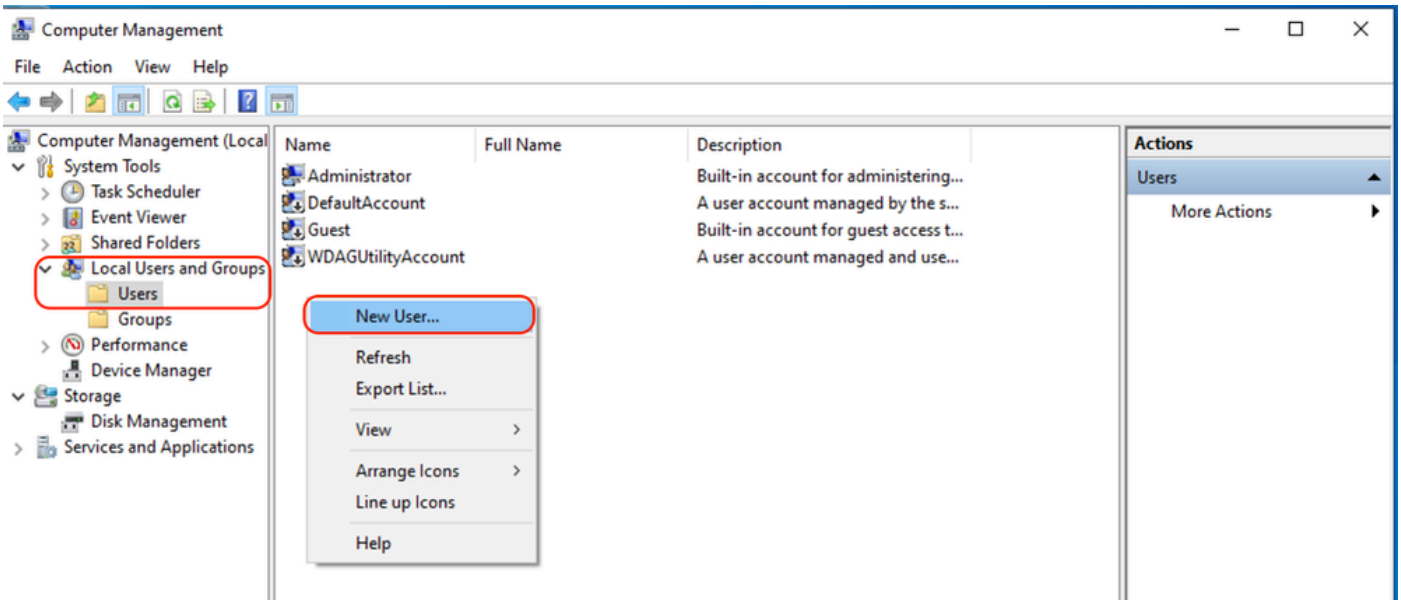
将Microsoft Windows配置为SCP远程服务器

步骤11.要为SCP服务创建用户，请导航到计算机管理:

注意：如果您已经有SCP用户，请跳至步骤16。

步骤12.选择Local Users和Groups，然后从左侧窗格中选择Users。

步骤13.在主页上单击鼠标右键，然后选择new user（新用户）。

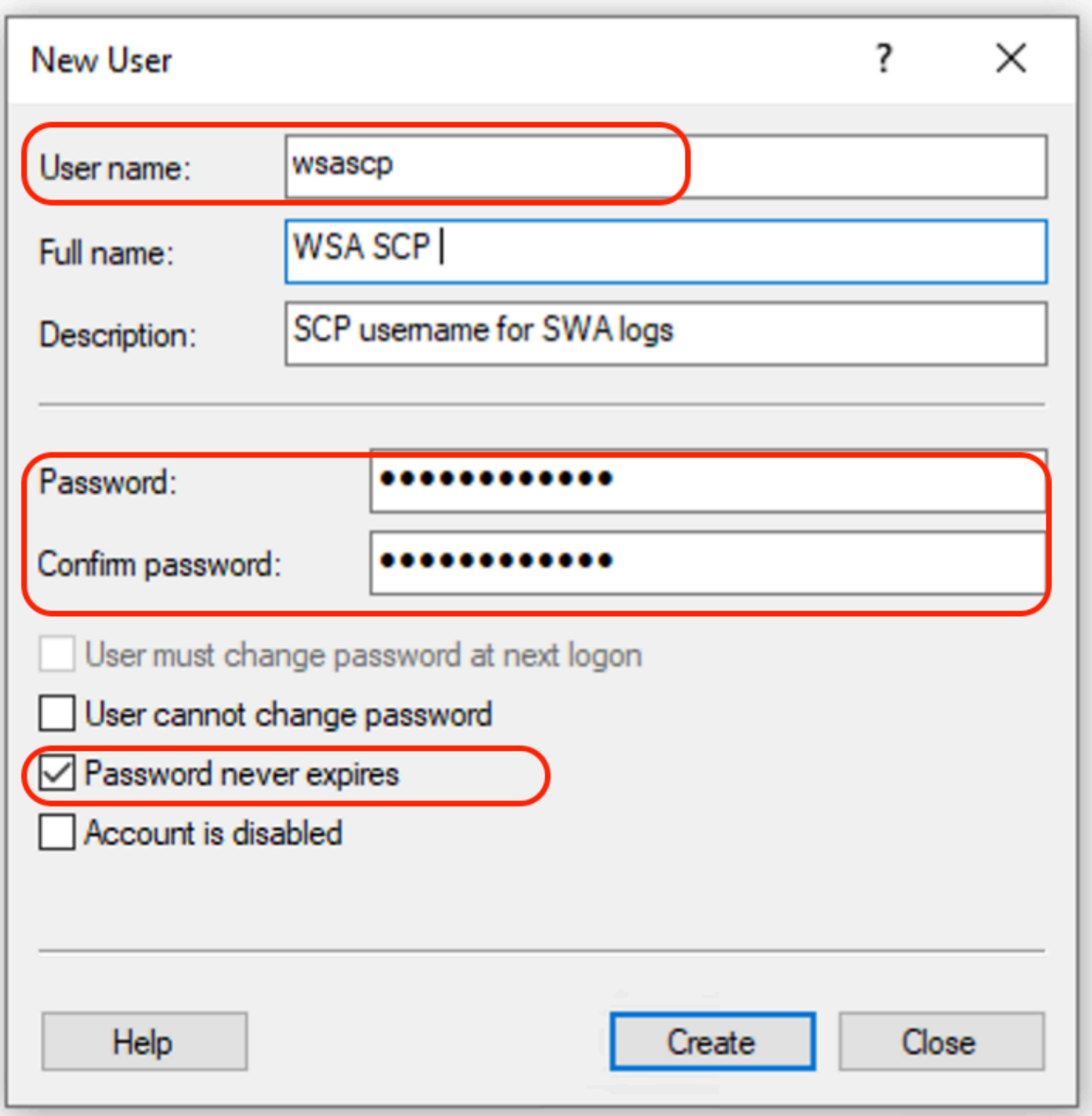


映像 — 为SCP服务创建用户。

步骤14.输入用户名和所需密码。

步骤15.选择Password Never Expires。

步骤16.单击Create，然后关闭窗口。



图像 — 输入新用户信息。

步骤17.使用新创建的用户登录到远程SCP服务器，以创建配置文件目录。

注意：如果远程SCP服务器上安装了OpenSSL，请跳至步骤19。

步骤18.使用管理员权限（以管理员身份运行）打开PowerShell，然后运行此命令以检查先决条件：

```
(New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

如果输出为True，您可以继续。否则，请与Microsoft支持团队联系，

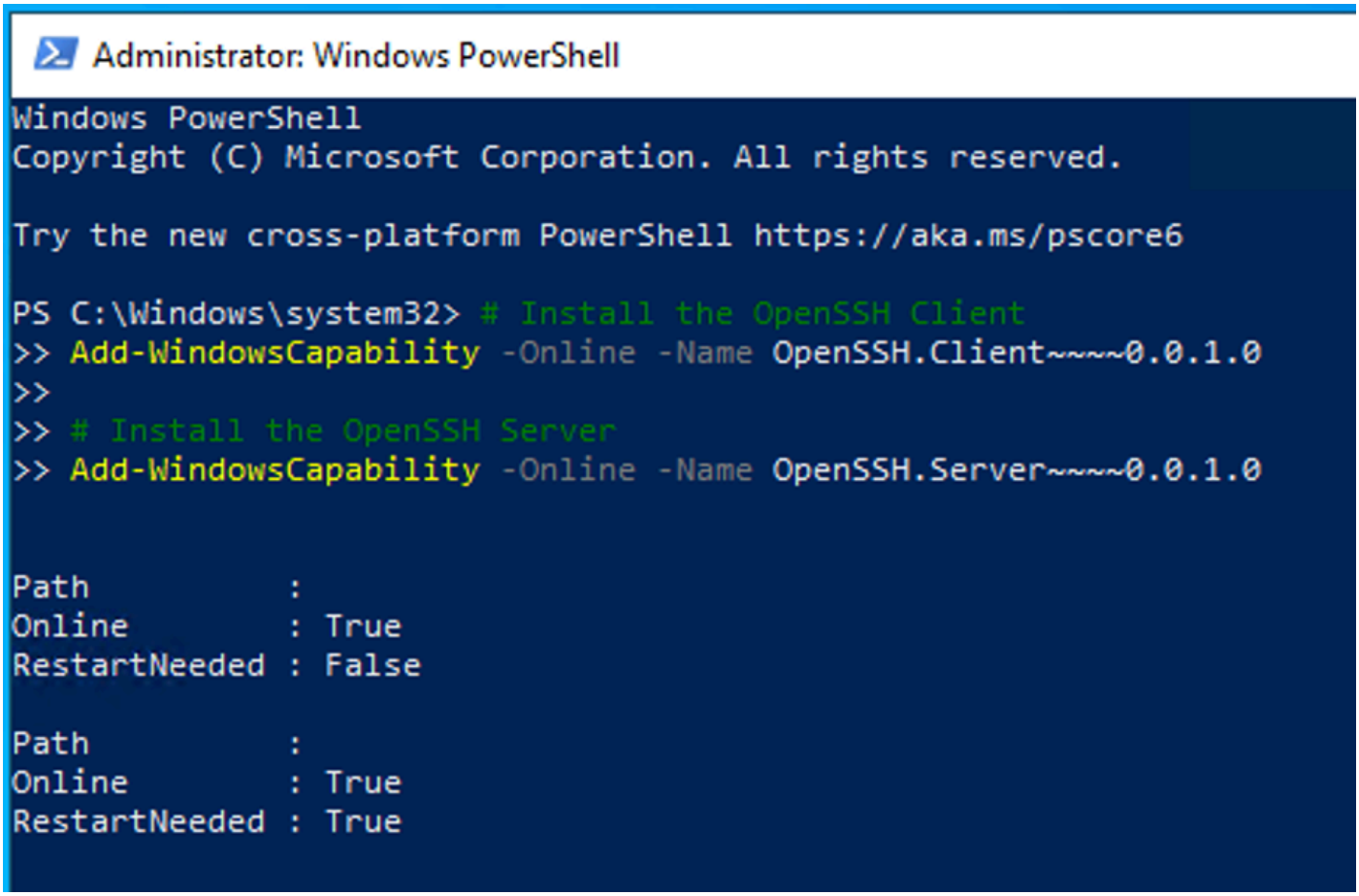
步骤19.要使用具有管理员权限的PowerShell（以管理员身份运行）安装OpenSSH，请运行：

```
# Install the OpenSSH Client
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

# Install the OpenSSH Server
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

以下是成功结果的示例：

```
Path          :
Online        : True
RestartNeeded : False
```



映像 — 在PowerShell中安装OpenSSH

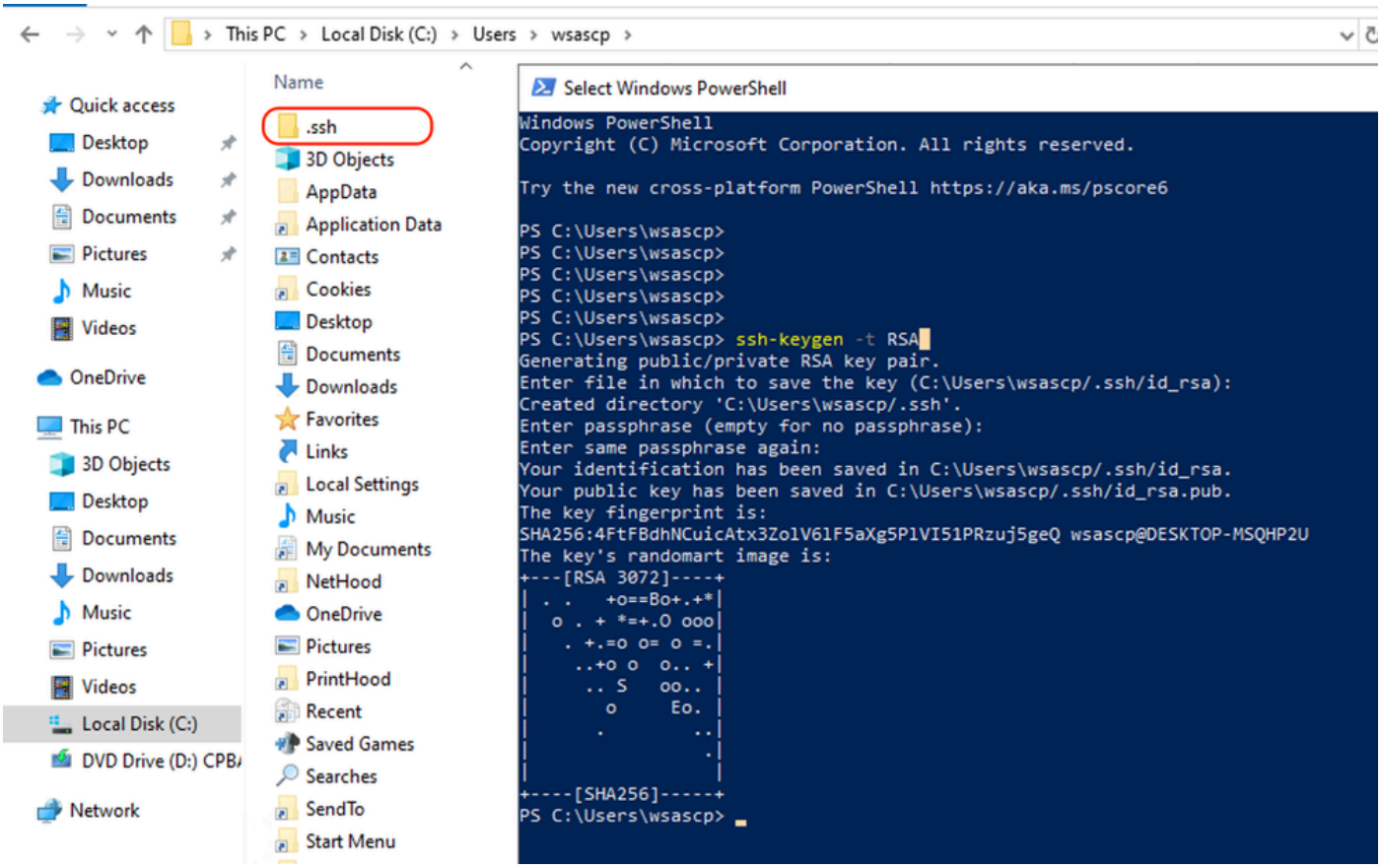
⚠ 警告：如果RestartNeeded设置为True，请重启Windows。

有关在其他版本的Microsoft Windows上安装的更多信息，请访问OpenSSH for Windows入门 | Microsoft Learn。

步骤20.打开一个正常（未提升）的PowerShell会话，并使用以下命令生成一对RSA密钥：

```
ssh-keygen -t RSA
```

命令完成后，您可以看到.ssh文件夹已创建您的用户配置文件目录。



映像 — 生成RSA密钥

步骤21.从PowerShell以管理员权限（以管理员身份运行）启动SSH服务。

```
Start-Service sshd
```

步骤22.（可选，但推荐）使用Administrator权限（以Administrator身份运行）将服务Startup type更改为Automatic。

```
Set-Service -Name sshd -StartupType 'Automatic'
```

步骤23.确认firewall规则已创建，允许访问TCP端口22。

```
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction SilentlyContinue | Select-Object Na
    Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not exist, creating it..."
    New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName 'OpenSSH Server (sshd)' -Enabled Tru
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and exists."
}
```

步骤24.编辑SSH配置文件，该文件位于：%programdata%\ssh\sshd_config在记事本中，删除RSA和DSA的#。

```
HostKey __PROGRAMDATA__/ssh/ssh_host_rsa_key
HostKey __PROGRAMDATA__/ssh/ssh_host_dsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ecdsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ed25519_key
```

步骤25.编辑%programdata%\ssh\sshd_config中的连接条件。在本示例中，侦听地址用于所有接口地址。您可以根据部署设计自定义此设置。

```
Port 22
#AddressFamily any
ListenAddress 0.0.0.0
```

步骤26.通过在%programdata%\ssh\sshd_config文件的末尾添加#，将这两行标记为%programdata%\ssh\sshd_config文件的末尾：

```
# Match Group administrators
#       AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

步骤27.（可选）编辑%programdata%\ssh\sshd_config中的Strict Modes，默认情况下，此模式处于启用状态，并在未正确保护私有密钥和公用密钥的情况下阻止基于SSH密钥的身份验证。

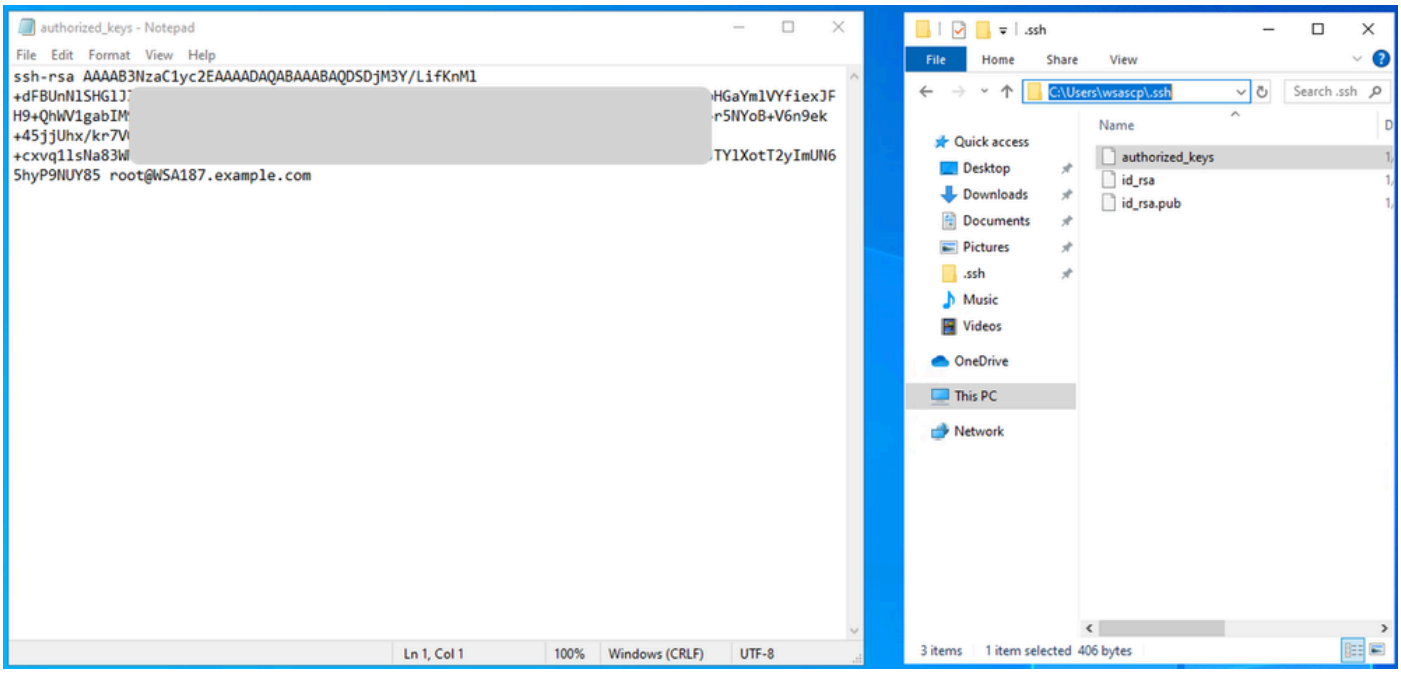
取消对该行的注释#StrictModes是，并将其更改为StrictModes no:

```
StrictModes No
```

步骤28.将#从此行中删除%programdata%\ssh\sshd_config，以允许公钥身份验证

```
PubkeyAuthentication yes
```

步骤29.在.ssh文件夹中创建文本文件authorized_keys，并粘贴SWA public RSA 密钥（在步骤9中收集）：



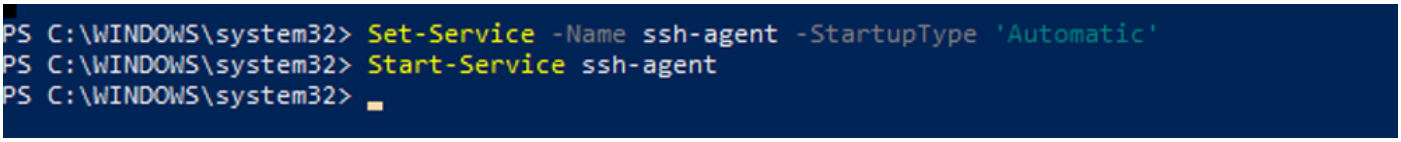
图像 — SWA公钥

注意：复制整行，从ssh-rsa开始并以root@<your_SWA_hostname>结束。

提示：由于RSA安装在SCP服务器上，因此无需粘贴ssh-dss密钥。

步骤30.在PowerShell中启用OpenSSH Authentication Agent，并具有管理员权限（以Administrator身份运行）。

```
Set-Service -Name ssh-agent -StartupType 'Automatic'
Start-Service ssh-agent
```



映像 — 启用开放式SSH身份验证代理

步骤31.（可选）将此行添加到%programdata%\ssh\sshd_config以允许密钥类型：

```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rs
```

步骤32.重新启动SSH服务。您可以从PowerShell with Administrator privilege （以Administrator身份运行）使用此命令。

```
 restart-Service -Name sshd
```

步骤33.要测试是否正确配置了SCP推送，请将鼠标指针置于已配置的日志上，您可以从GUI或CLI（rollovernow命令）执行操作：

```
WSA_CLI> rollovernow scpal
```

注意：在本示例中，日志名称为scpal。

您可以确认日志已复制到定义的文件夹，在本例中为c:/Users/wsascp/wsa01。

将SCP日志推送到其他驱动器

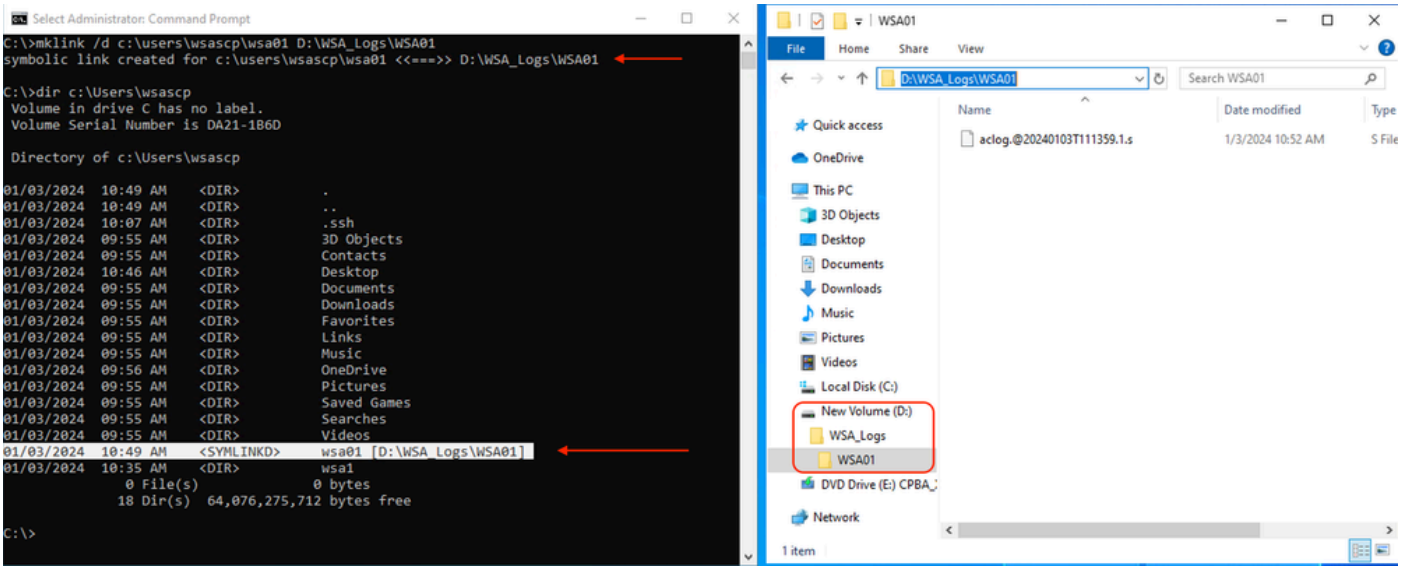
如果需要将日志推送到除C以外的其他驱动器，请创建从用户配置文件文件夹到所需驱动器的链接。在本示例中，日志被推送到D:\WSA_Logs\WSA01。

步骤1.在所需驱动器中创建文件夹。

步骤2.使用Administrator权限打开Command Prompt（以Administrator身份运行）。

步骤3.运行以下命令创建链接：

```
mklink /d c:\users\wsascp\wsa01 D:\WSA_Logs\WSA01
```



图像 — 创建SYM链接

注意：在本示例中，SWA配置为将日志推送到C:\Users\wsascp中的WSA01文件夹，并且SCP服务器将WSA01文件夹作为到D:\WSA_Logs\WSA01的符号链接。

有关Microsoft Symbol链接的详细信息，请访问：[mklink | Microsoft学习]

排除SCP日志推送故障

在SWA中查看日志

要排除SCP日志推送故障，请检查中的错误：

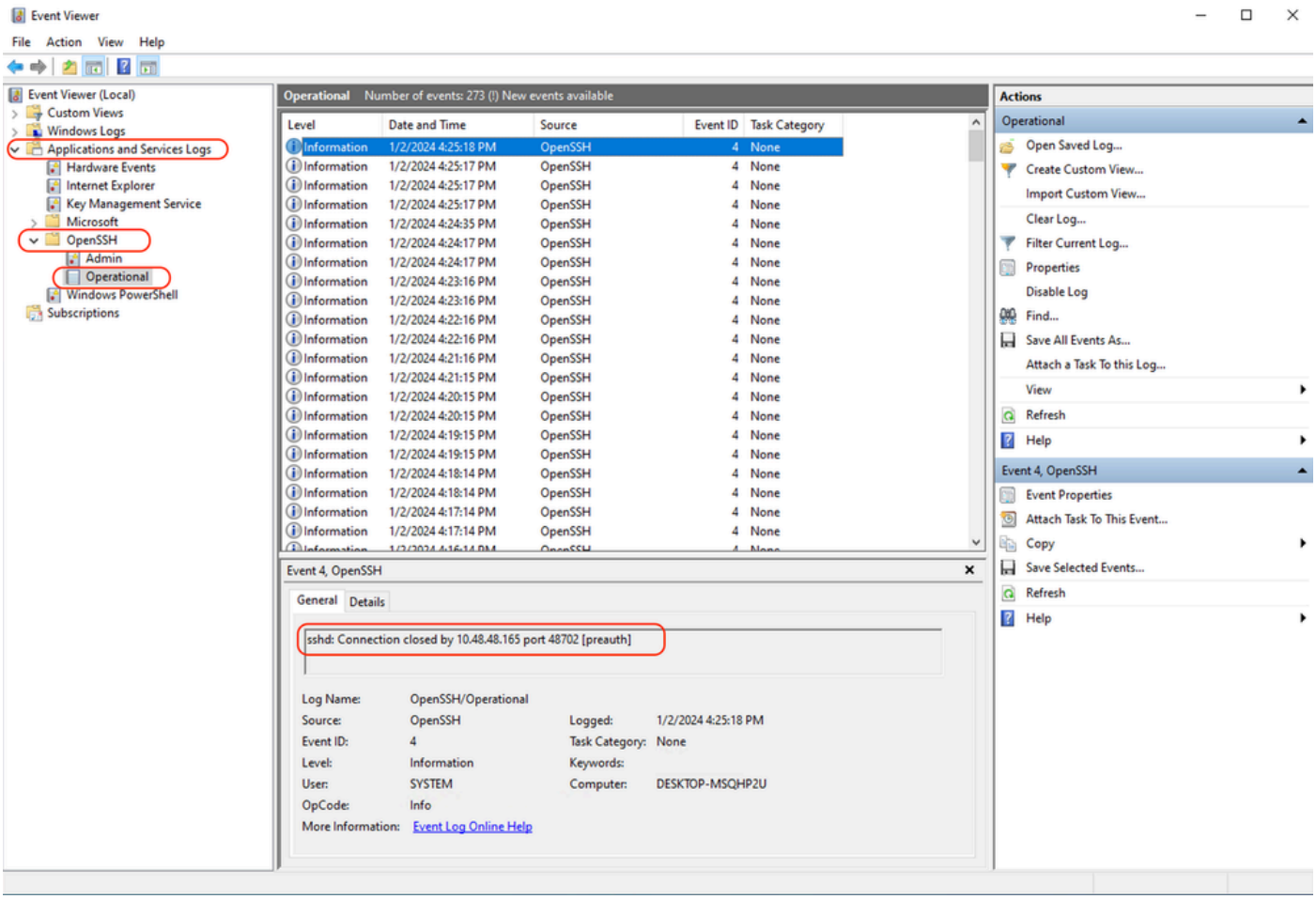
1. CLI > displayalerts

2.系统日志

注意：要读取system_logs，可以在CLI中使用grep命令。选择与system_logs关联的编号，然后回答向导中的问题。

在SCP服务器中查看日志

您可以在Microsoft Event Viewer、Applications and Services Logs > OpenSSH > Operational中读取SCP服务器日志:



映像 — PreAuth失败

"主机密钥验证失败。"

此错误表示SWA中存储的SCP服务器公钥无效。

以下是CLI中displayalerts输出的错误示例：

```
02 Jan 2024 16:52:35 +0100    Log Error: Push error for subscription scpal: SCP failed to transfer to 1
Last message occurred 68 times between Tue Jan  2 15:53:01 2024 and Tue Jan  2 16:52:31 2024.
```

```
Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: Host key verif
Last message occurred 46 times between Tue Jan  2 16:30:19 2024 and Tue Jan  2 16:52:31 2024.

Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: lost connectio
Last message occurred 68 times between Tue Jan  2 15:53:01 2024 and Tue Jan  2 16:52:31 2024.

Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: ssh: connect t
Last message occurred 22 times between Tue Jan  2 15:53:01 2024 and Tue Jan  2 16:29:18 2024.
```

以下是system_logs中的错误示例：

```
Tue Jan  2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer t
Tue Jan  2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer t
Tue Jan  2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer t
```

要解决此问题，可以从SCP服务器复制主机并将其粘贴到SCP logs订用页。请参阅配置SWA以从GUI向SCP远程服务器发送日志中的步骤7，或者您可以联系CiscoTAC从后端删除主机密钥。

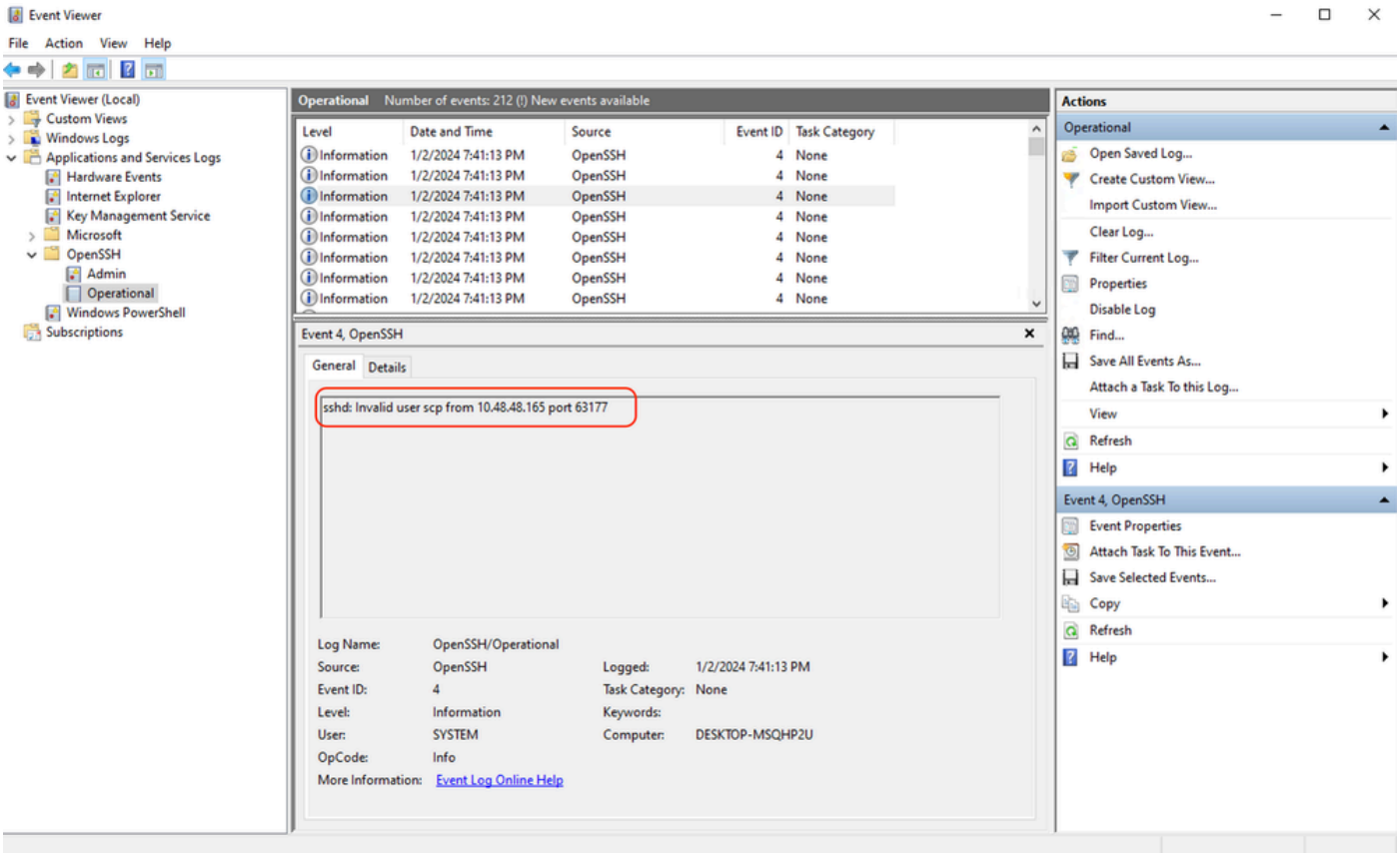
"权限被拒绝(publickey，password，keyboard-interactive)。"

此错误通常表示SWA中提供的用户名无效。

以下是system_logs中的错误日志示例：

```
Tue Jan  2 20:41:40 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:41:40 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:41:40 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
```

以下是SCP服务器中的错误示例：“来自<SWA_IP地址>端口<TCP端口SWA连接到SCP服务器>的用户SCP无效”。



图像 — 无效用户

要解决此错误，请检查拼写，并验证用户（在SWA中配置为推送日志）在SCP服务器中是否已启用。

"没有这样的文件或目录。"

此错误表示SWA日志订阅部分中提供的路径无效，

以下是system_logs的错误示例：

```
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scpal: SCP failed to transfer
```

要解决此问题，请验证拼写，并确保路径在SCP服务器中正确有效。

"SCP无法传输。"

此错误可能是通信错误的指示符。以下是错误示例：

```
03 Jan 2024 13:23:27 +0100    Log Error: Push error for subscription scp: SCP failed to transfer to 10.
```

要排除连接故障，请在SWA CLI中使用telnet命令：

```
SWA_CLI> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (10.48.48.187/24: SWA_man.csico.com)
[1]> 2

Enter the remote hostname or IP address.
[]> 10.48.48.195

Enter the remote port.
[23]> 22

Trying 10.48.48.195...
```

在本示例中，连接未建立。成功的连接方式如下：

```
SWA_CLI> telnet

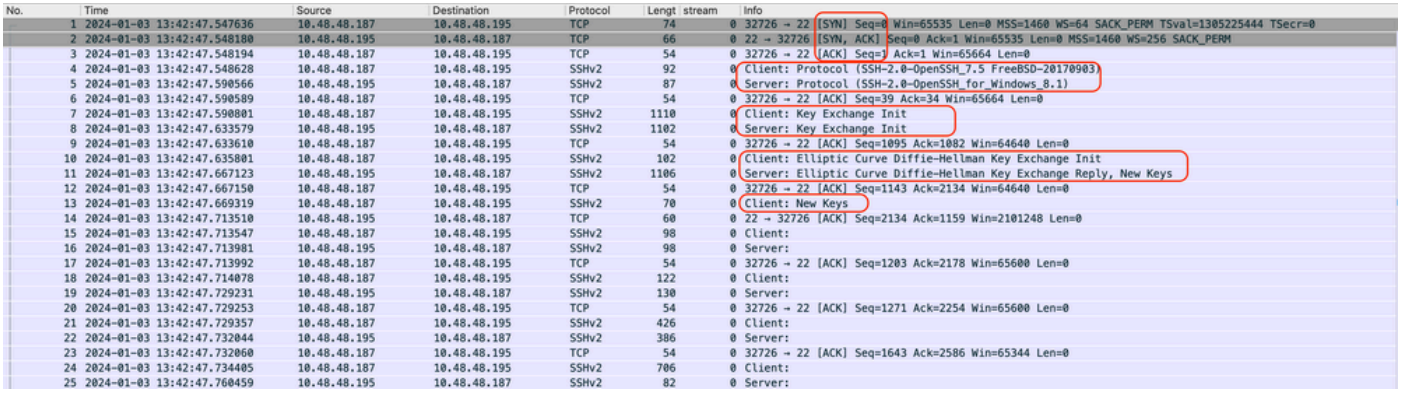
Please select which interface you want to telnet from.
1. Auto
2. Management (10.48.48.187/24: rishi2Man.calo.lab)
[1]> 2
Enter the remote hostname or IP address.
[]> 10.48.48.195
Enter the remote port.
[23]> 22

Trying 10.48.48.195...
Connected to 10.48.48.195.
Escape character is '^]'.
SSH-2.0-OpenSSH_for_Windows_SCP
```

如果telnet未连接：

1. 检查SCP服务器防火墙是否阻止访问。
2. 检查从SWA到SCP服务器的路径中是否有任何防火墙阻止访问。
3. 检查TCP端口22在SCP服务器中是否处于侦听状态。
4. 在两个SWA和SCP服务器中运行数据包捕获以进行进一步分析。

以下是成功连接的数据包捕获示例：



No.	Time	Source	Destination	Protocol	Lengt	stream	Info
1	2024-01-03 13:42:47.547636	10.48.48.187	10.48.48.195	TCP	74	0	32726 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM TSval=1305225444 TSecr=0
2	2024-01-03 13:42:47.548180	10.48.48.195	10.48.48.187	TCP	66	0	22 → 32726 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3	2024-01-03 13:42:47.548194	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1 Ack=1 Win=65664 Len=0
4	2024-01-03 13:42:47.548628	10.48.48.187	10.48.48.195	SSHv2	92	0	Client: Protocol (SSH-2.0-OpenSSH_7.5 FreeBSD-20170903)
5	2024-01-03 13:42:47.590566	10.48.48.195	10.48.48.187	SSHv2	87	0	Server: Protocol (SSH-2.0-OpenSSH_for_Windows_8.1)
6	2024-01-03 13:42:47.590589	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=39 Ack=34 Win=65664 Len=0
7	2024-01-03 13:42:47.590801	10.48.48.187	10.48.48.195	SSHv2	1110	0	Client: Key Exchange Init
8	2024-01-03 13:42:47.633579	10.48.48.195	10.48.48.187	SSHv2	1102	0	Server: Key Exchange Init
9	2024-01-03 13:42:47.633610	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1095 Ack=1082 Win=64640 Len=0
10	2024-01-03 13:42:47.635801	10.48.48.187	10.48.48.195	SSHv2	102	0	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
11	2024-01-03 13:42:47.667123	10.48.48.195	10.48.48.187	SSHv2	1106	0	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
12	2024-01-03 13:42:47.667150	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1143 Ack=2134 Win=64640 Len=0
13	2024-01-03 13:42:47.669319	10.48.48.187	10.48.48.195	SSHv2	70	0	Client: New Keys
14	2024-01-03 13:42:47.713510	10.48.48.195	10.48.48.187	TCP	60	0	22 → 32726 [ACK] Seq=2134 Ack=1159 Win=2101248 Len=0
15	2024-01-03 13:42:47.713547	10.48.48.187	10.48.48.195	SSHv2	98	0	Client:
16	2024-01-03 13:42:47.713981	10.48.48.195	10.48.48.187	SSHv2	98	0	Server:
17	2024-01-03 13:42:47.713992	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1203 Ack=2178 Win=65600 Len=0
18	2024-01-03 13:42:47.714078	10.48.48.187	10.48.48.195	SSHv2	122	0	Client:
19	2024-01-03 13:42:47.729231	10.48.48.195	10.48.48.187	SSHv2	130	0	Server:
20	2024-01-03 13:42:47.729253	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1271 Ack=2254 Win=65600 Len=0
21	2024-01-03 13:42:47.729357	10.48.48.187	10.48.48.195	SSHv2	426	0	Client:
22	2024-01-03 13:42:47.732044	10.48.48.195	10.48.48.187	SSHv2	386	0	Server:
23	2024-01-03 13:42:47.732060	10.48.48.187	10.48.48.195	TCP	54	0	32726 → 22 [ACK] Seq=1643 Ack=2586 Win=65344 Len=0
24	2024-01-03 13:42:47.734405	10.48.48.187	10.48.48.195	SSHv2	706	0	Client:
25	2024-01-03 13:42:47.760459	10.48.48.195	10.48.48.187	SSHv2	82	0	Server:

图像 — 成功捕获连接数据包

"未找到匹配的主机密钥类型"

此错误表示SWA在客户端密钥交换阶段提供的主机密钥算法在SCP服务器中没有匹配项。

```
Wed Feb 12 20:21:40 2025 Critical: Log Error: Push error for subscription al: SCP failed to transfer to
Wed Feb 12 20:21:40 2025 Critical: Log Error: Push error for subscription al: SCP failed to transfer to
Wed Feb 12 20:21:40 2025 Critical: Log Error: Push error for subscription al: SCP failed to transfer to
```

要解决此问题，可以使用以下步骤：

步骤1.在SWA中开始数据包捕获，并过滤SCP服务器IP地址。

步骤2.回滚日志文件，以确保SWA将文件发送到SCP服务器。

步骤3.停止数据包捕获并打开文件。

步骤4.在捕获文件中，查找Client:在Info（信息）部分中进行Key Exchange Init。

步骤5.展开SSH协议，然后导航到算法部分。

步骤6.检查server_host_key_algorithms字符串(例如：server_host_key_algoriths字符串：ssh-rsa)

步骤7.导航到SCP服务器并编辑sshd_config文件。

步骤8.查找以HostKeyAlgorithms开头的行，并将Step 6中提到的受支持的主机密钥添加到文件。(在本例中：HostKeyAlgorithms ssh-rsa)

注意：如果没有以HostKeyAlgorithms开头的行，您可以将该行添加到文件末尾。

步骤9.保存更改并重新启动SSHD服务。

相关内容

- 思科网络安全设备最佳实践指南
- BRKSEC-3303(ciscolive)
- 思科安全Web设备AsyncOS 14.5用户指南 — GD（通用部署）— 连接、安装和配置[思科安全Web设备]
- 开始使用OpenSSH for Windows | Microsoft学习
- 在Windows上配置SSH公钥身份验证 | Windows OS Hub(woshub.com)
- Windows版OpenSSH中基于密钥的身份验证 | Microsoft学习

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）。