

在带有Microsoft Server的安全Web设备中配置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](#)

[在远程服务器上配置通过SCP的日志检索](#)

[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](#)

[主机密钥验证失败](#)

[权限被拒绝\(publickey , password , keyboard-interactive\)](#)

[SCP无法传输](#)

[参考](#)

简介

本文档介绍将安全复制(SCP)配置为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)的管理权限。
- 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)的行为与远程复制(RCP)类似,后者来自Berkeley r-tools套件(伯克利大学自有的一组网络应用程序),不同之处在于SCP依赖安全外壳(SSH)来确保安全性。此外,SCP要求配置身份验证、授权和记帐(AAA)授权,以便设备可以确定用户是否具有正确的权限级别

远程服务器上的SCP方法(相当于SCP推送)通过安全复制协议定期将日志文件推送到远程SCP服务器。此方法要求远程计算机上使用SSH2协议的SSH SCP服务器。订用需要远程计算机上的用户名、SSH密钥和目标目录。日志文件将根据您设置的滚动更新计划进行传输。

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:

- 滚动更新设置,用于确定日志文件的存档时间。
- 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:

- 按文件大小回滚
- 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。

第二步：选中要存档的日志订用的“滚动”列中的复选框，或选中全部复选框以选择所有订用。
 第3步.点击立即滚动(Rollover Now)以存档所选日志。

Log Subscriptions

Configured Log Subscriptions						
Add Log Subscription...						
Log Name	Type	Log Files	Rollover Interval	All Rollover	Deanonimization	Delete
accesslogs	Access Logs	access_logs	None	<input type="checkbox"/>	Deanonimization	
amp_logs	AMP Engine Logs	amp_logs	None	<input type="checkbox"/>		
scpal	Access Logs	SCP (10.48.48.195:22)	None	<input checked="" type="checkbox"/>	Deanonimization	
shd_logs	SHD Logs	shd_logs	None	<input type="checkbox"/>		
sl_usercountd_logs	SL Usercount Logs	sl_usercountd_logs	None	<input type="checkbox"/>		
smartlicense	Smartlicense Logs	smartlicense	None	<input type="checkbox"/>		
snmp_logs	SNMP Logs	snmp_logs	None	<input type="checkbox"/>		
sntpd_logs	NTP Logs	sntpd_logs	None	<input type="checkbox"/>		
sophos_logs	Sophos Logs	sophos_logs	None	<input type="checkbox"/>		
sse_connectord_logs	SSE Connector Daemon Logs	sse_connectord_logs	None	<input type="checkbox"/>		
status	Status Logs	status	None	<input type="checkbox"/>		
system_logs	System Logs	system_logs	None	<input type="checkbox"/>		
trafmon_errlogs	Traffic Monitor Error Logs	trafmon_errlogs	None	<input type="checkbox"/>		
trafmonlogs	Traffic Monitor Logs	trafmonlogs	None	<input type="checkbox"/>		
uds_logs	UDS Logs	uds_logs	None	<input type="checkbox"/>		
umbrella_client_logs	Umbrella Client Logs	umbrella_client_logs	None	<input type="checkbox"/>		
updater_logs	Updater Logs	updater_logs	None	<input type="checkbox"/>		
upgrade_logs	Upgrade Logs	upgrade_logs	None	<input type="checkbox"/>		
wbnp_logs	WBNP Logs	wbnp_logs	None	<input type="checkbox"/>		
webcat_logs	Web Categorization Logs	webcat_logs	None	<input type="checkbox"/>		
webrootlogs	Webroot Logs	webrootlogs	None	<input type="checkbox"/>		
webtapd_logs	Webtapd Logs	webtapd_logs	None	<input type="checkbox"/>		
welcomeack_logs	Welcome Page Acknowledgement Logs	welcomeack_logs	None	<input type="checkbox"/>		

[Rollover Now](#)

图像-立即回滚GUI

通过远程服务器上的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:登录到SWA，然后从系统管理选择日志订阅。

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

中的“严格模式”。默认情况下，此模式处于启用状态，并且如果私钥和公钥未得到正确保护，它将阻止基于SSH密钥的身份验证。

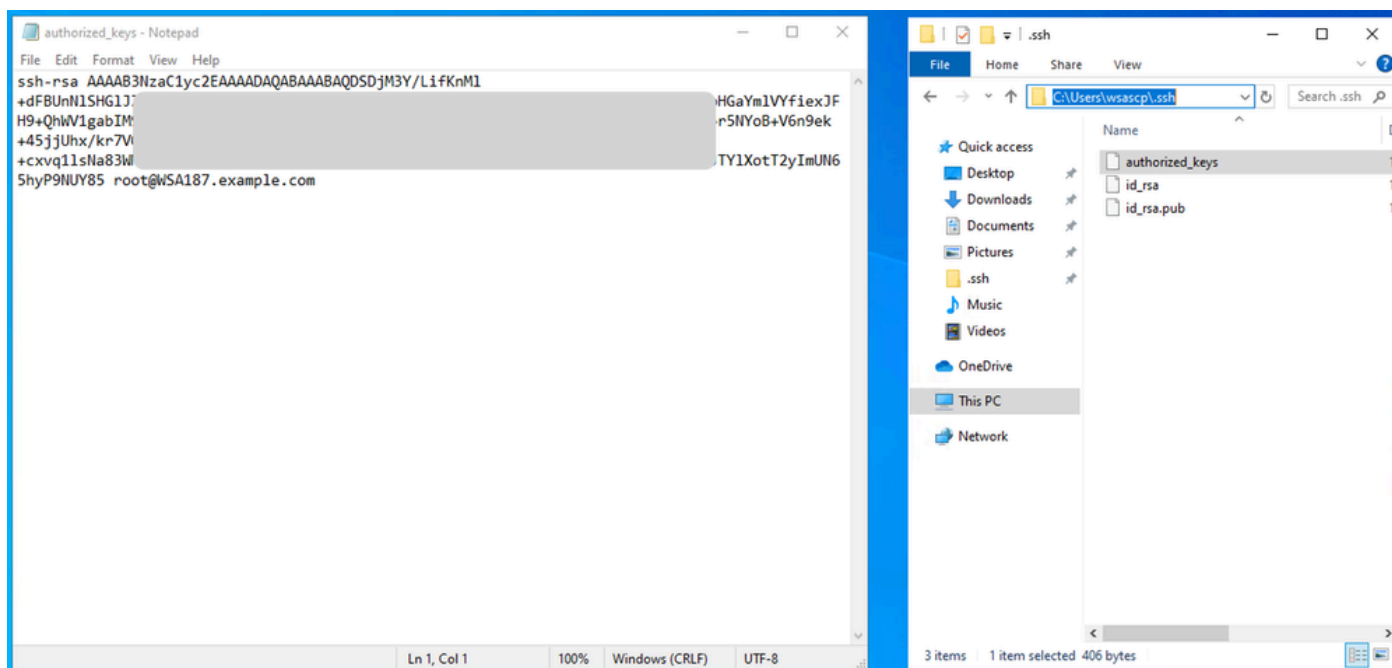
取消注释该行#StrictModesyes，并将其更改为StrictModes no：

```
StrictModes No
```

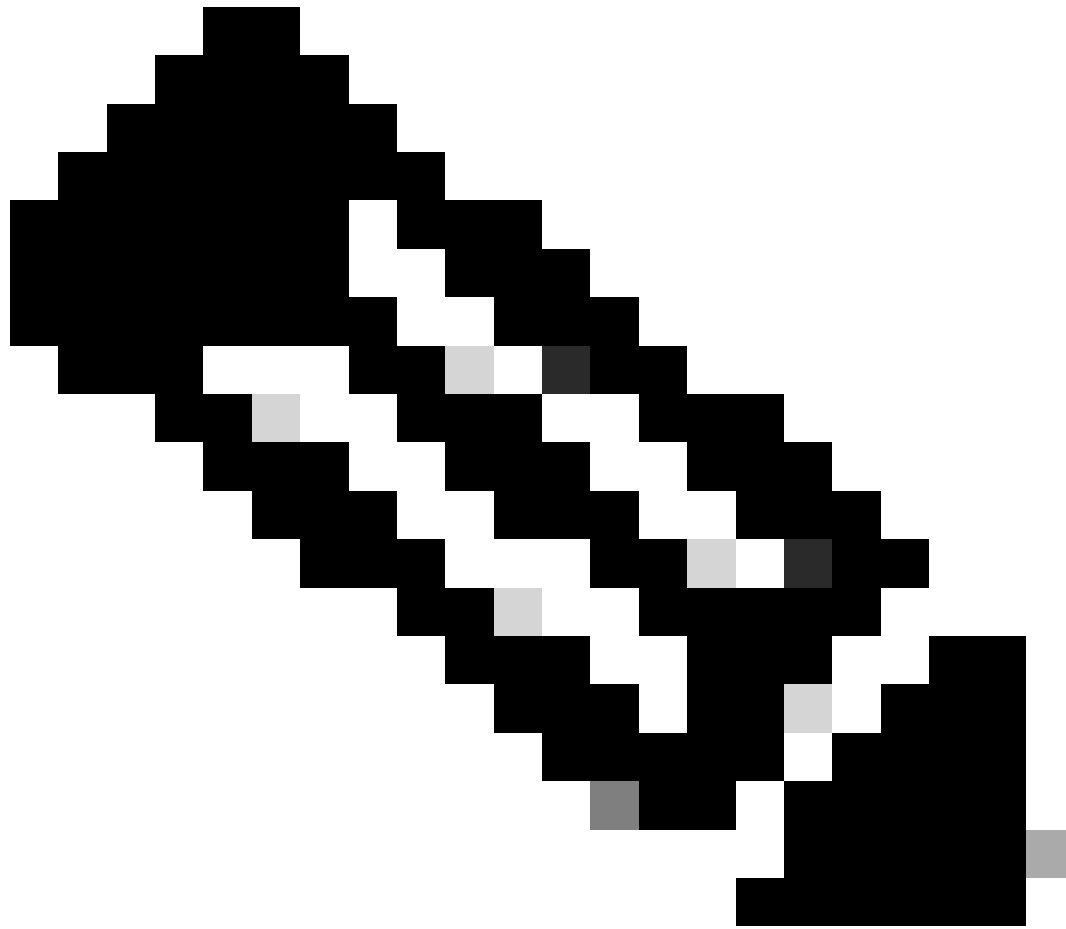
步骤 27将#从此行中删除到%programdata%\ssh\sshd_config，以便允许进行公钥身份验证

```
PubkeyAuthentication yes
```

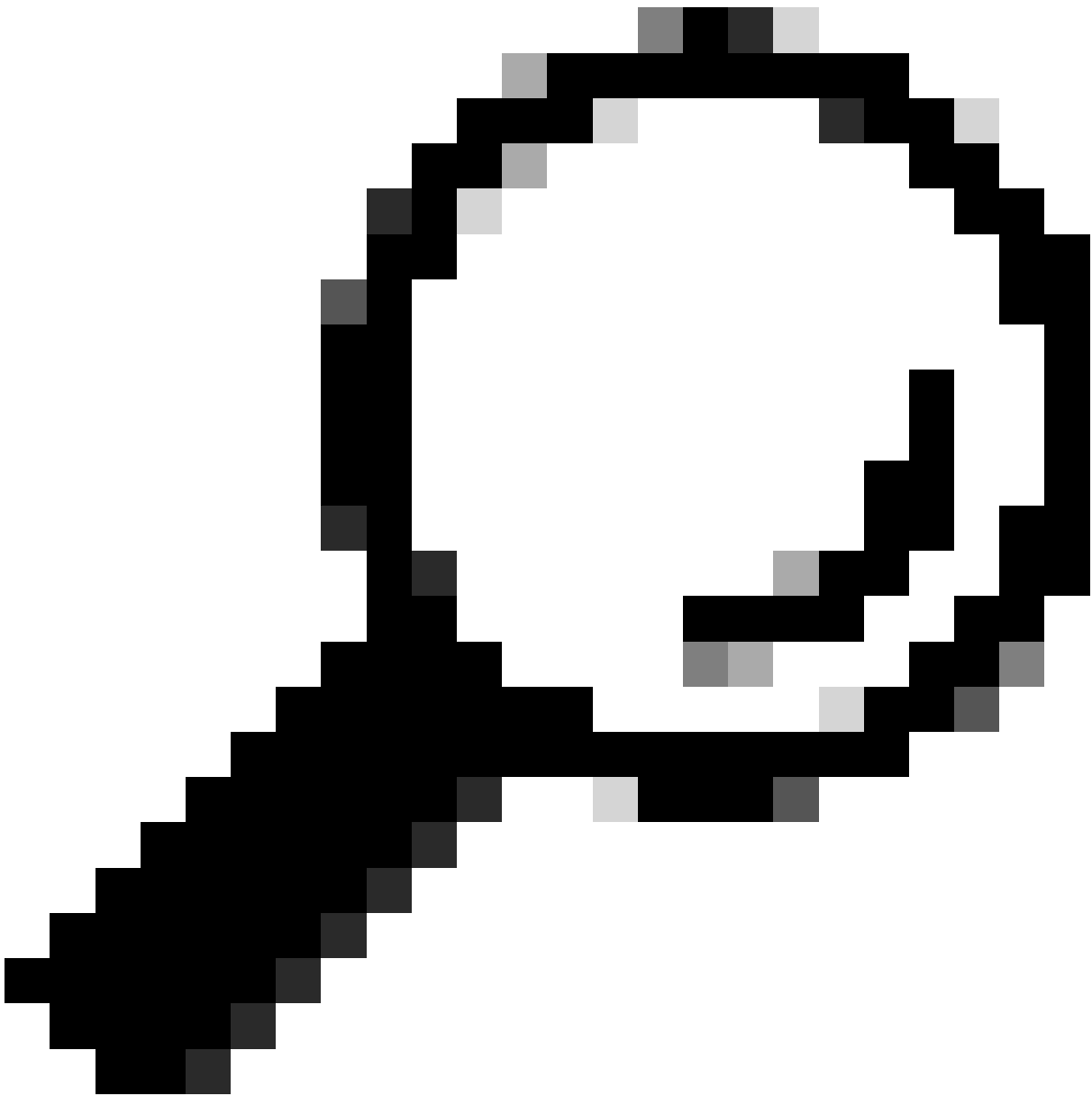
步骤 28在.ssh文件夹中创建文本文件“authorized_keys”，然后粘贴SWA公共RSA密钥（已于步骤9中收集）



图像- SWA公钥



注意：复制以ssh-rsa开头并以root@<your_SWA_hostname>结尾的整行



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 29在PowerShell中启用具有管理员权限的“OpenSSH Authentication Agent”（以管理员身份运行）。

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

```
PS C:\WINDOWS\system32> Set-Service -Name ssh-agent -StartupType 'Automatic'  
PS C:\WINDOWS\system32> Start-Service ssh-agent  
PS C:\WINDOWS\system32> █
```

映像-启用开放式SSH身份验证代理

第30步 (可选) 将此行添加到%programdata%\ssh\sshd_config以允许密钥类型 :

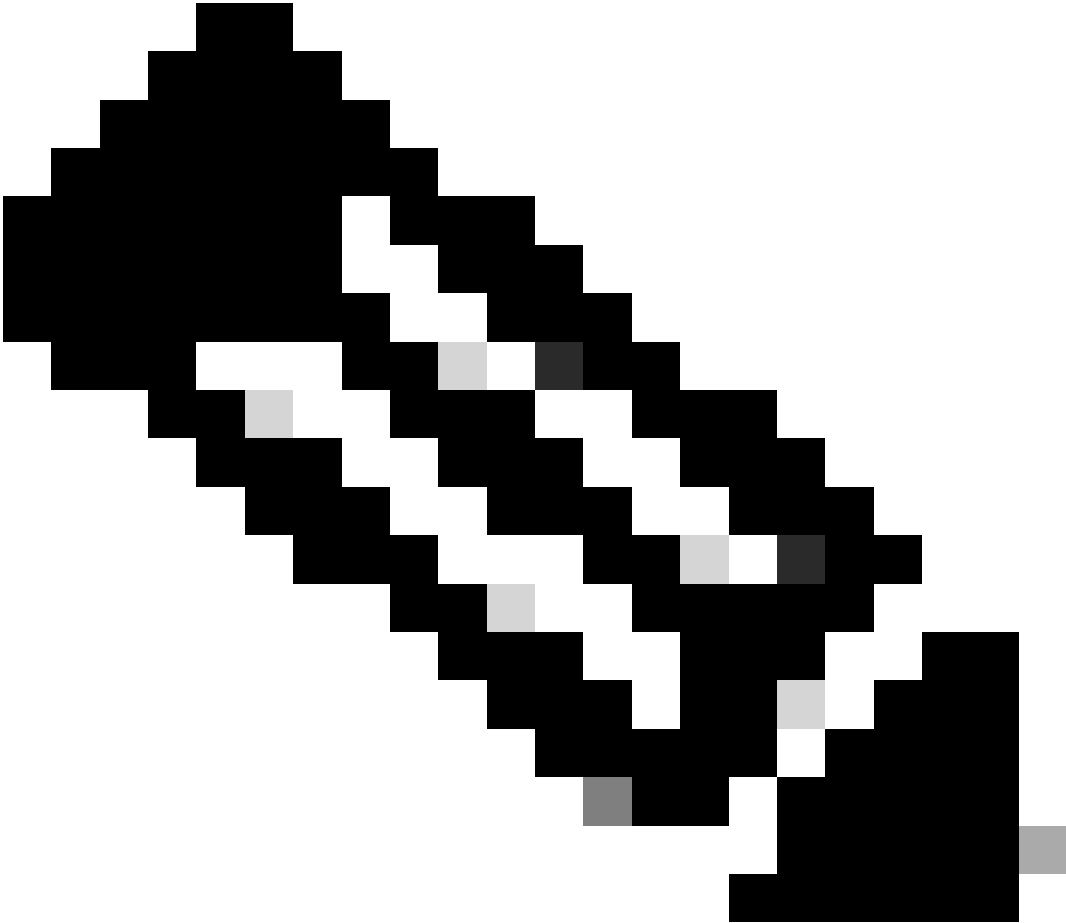
```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rs
```

步骤 31重新启动SSH服务。您可以从PowerShell中通过管理员权限 (以管理员身份运行) 使用此命令

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

步骤 32要测试SCP推送配置是否正确，请将鼠标指针置于已配置的日志上，可以通过GUI或CLI执行此操作(rollovernow命令) :

```
WSA_CLI> rollovernow scp1
```



注意：在本示例中，日志名称为“scpal”。

您可以确认是否将日志复制到已定义的文件夹(在本示例中为c : /Users/wsascp/wsa01)

将SCP日志推送到其他驱动器

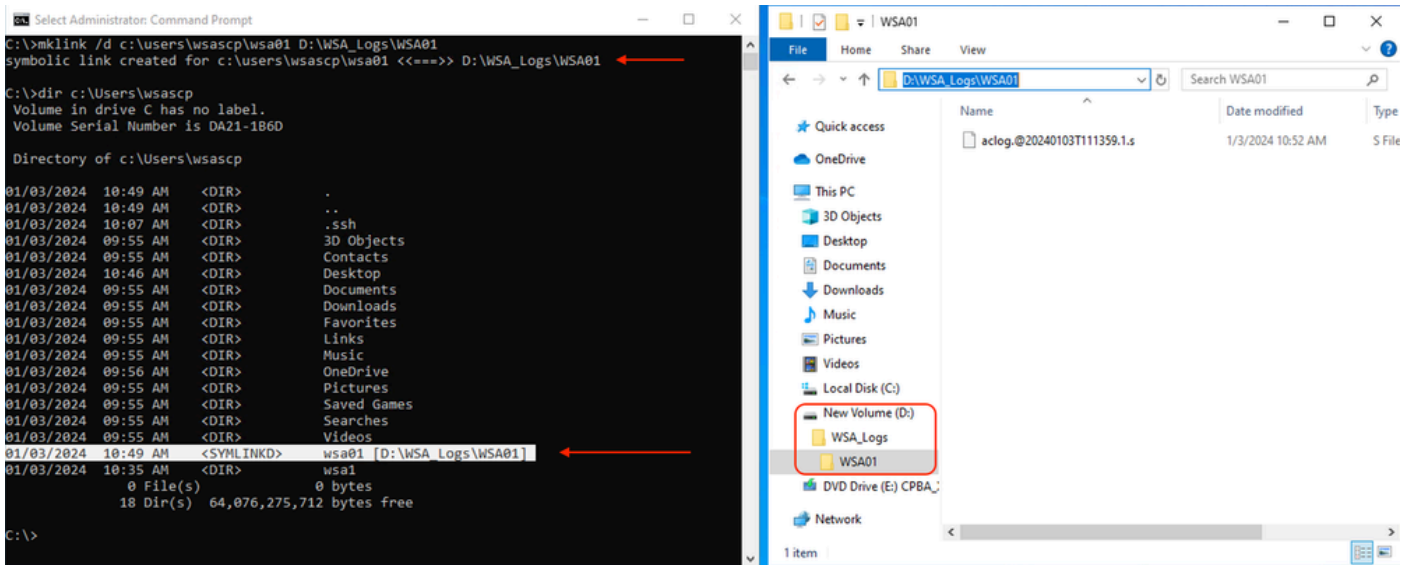
如果您需要将日志推送到除C：以外的其他驱动器，请从用户配置文件文件夹创建指向所需驱动器的链接。在本示例中，日志被推送到D:\WSA_Logs\WSA01。

第1步：在所需驱动器中创建文件夹，在本例中

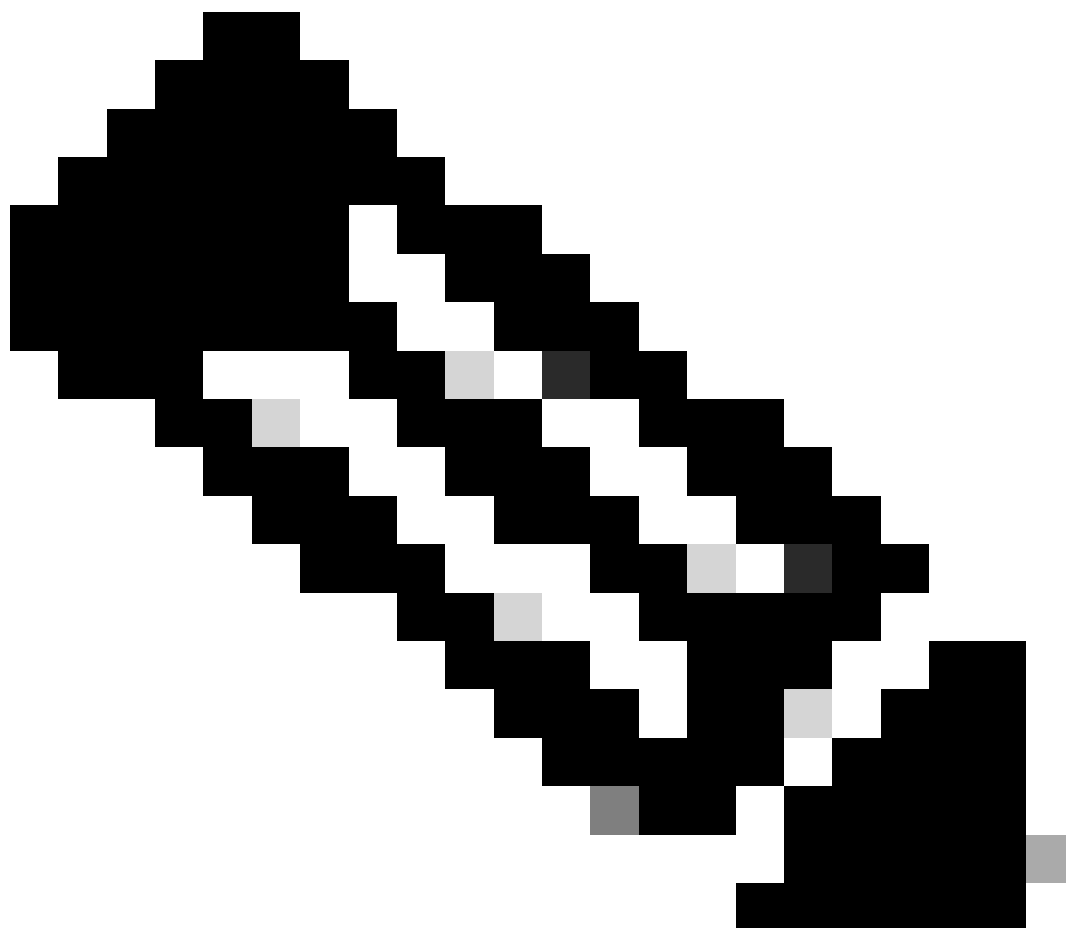
第二步：以管理员权限打开命令提示符（以管理员身份运行）

第三步：运行以下命令以创建链路：

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



映像-创建SYM链路



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（这是

您寻找缓存缺失可以使用的隐藏命令)，并且SCP服务器将文件夹WSA01配置为指向D:\WSA_Logs\WSA01的符号链接

有关Microsoft Symbol链接的详细信息，请访问：[mmlink | Microsoft学习](#)

排除SCP日志推送故障

在SWA中查看日志

要排除SCP日志推送的故障，请检查：

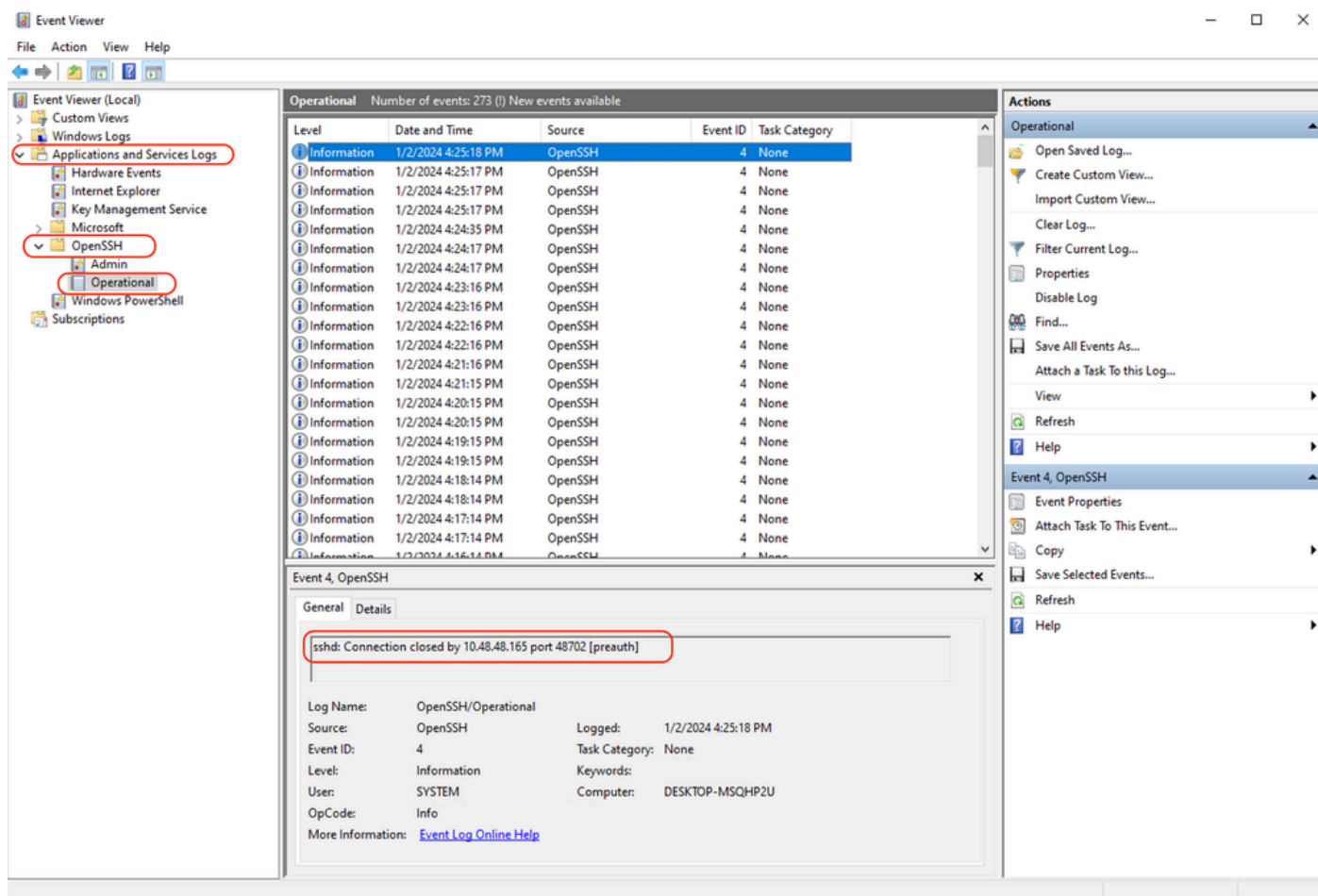
1. CLI > displayalerts
 2. 系统日志
-

注意：要读取system_logs，可以在CLI中使用grep命令（在CLI中为System_logs选择一个

关联数字) , 然后在向导中回答问题。

在SCP服务器中查看日志

您可以在Microsoft事件查看器的应用和服务日志 > OpenSSH > Operational中读取SCP服务器日志



映像- PreAuth失败

主机密钥验证失败

此错误表示存储在SWA中的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 scp1: SCP failed to transfer to 10.48.48.195:22: Host key verification failed
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 scp1: SCP failed to transfer to 10.48.48.195:22: Host key verification failed
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 scp1: SCP failed to transfer to 10.48.48.195:22: lost connection to SCP server
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 scp1: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
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 to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
Tue Jan 2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
Tue Jan 2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
```

要解决此问题，可以从SCP服务器复制主机，并将其粘贴到SCP日志订阅页面中。

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Cisco TAC从后端删除主机密钥。

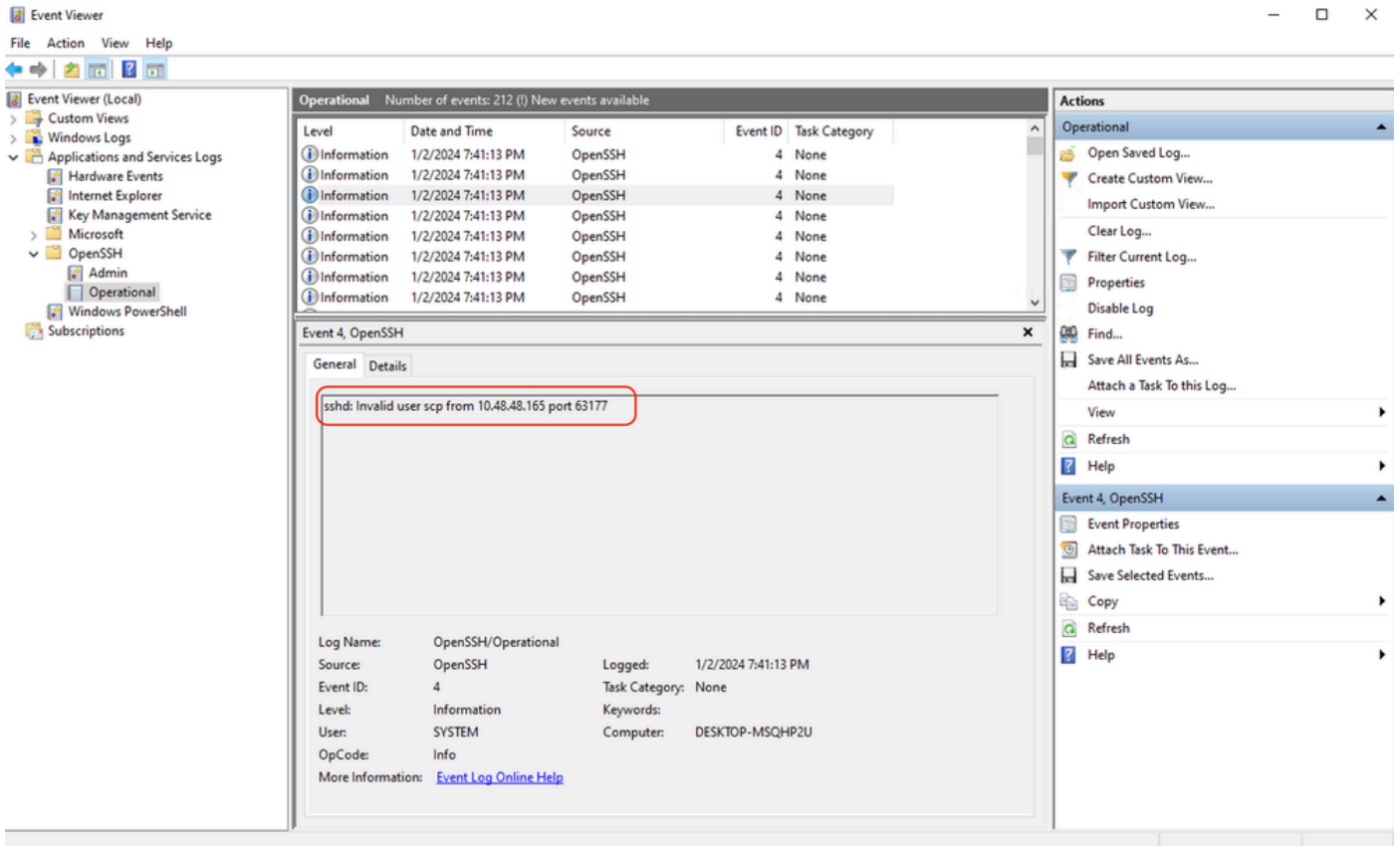
权限被拒绝(publickey , password , keyboard-interactive)

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 scp1: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
Tue Jan 2 20:41:40 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
Tue Jan 2 20:41:40 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused
```

以下是SCP服务器的错误示例：<SWA_IP地址> port <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，请检查拼写并验证在SCP服务器中是否已启用用户（在SWA中配置为推送日志）。

无此类文件或目录

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 scp: SCP failed to transfer
Tue Jan 2 20:47:18 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer
Tue Jan 2 20:47:18 2024 Critical: Log Error: Push error for subscription scp: 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器。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，未建立连接。成功的连接输出为：

```
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	Length	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 13:42:47.635001	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:

映像-成功捕获连接数据包

参考

[思科网络安全设备最佳实践指南-思科](#)

[BRKSEC-3303 \(ciscolive\)](#)

[思科安全网络设备AsyncOS 14.5用户指南- GD \(通用部署\) -连接、安装和配置\[思科安全网络设备\]-思科](#)

[Windows版OpenSSH入门 | Microsoft学习](#)

[在Windows上配置SSH公钥身份验证 | Windows OS中心\(woshub.com\)](#)

[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）。