Configure SCP Push Logs in Secure Web Appliance with Microsoft Server

Contents

Introduction

This document describes the steps to configure Secure Copy (SCP) to automatically copy logs in Secure Web Appliance (SWA) to another server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- How SCP works.
- SWA administration.
- Administration of Microsoft Windows or Linux Operating system.

Cisco recommends that you have:

- Physical or Virtual SWA Installed.
- License activated or installed.
- The setup wizard is completed.

- Administrative Access to the SWA Graphical User Interface (GUI).
- Microsoft Windows (at least Windows Server 2019 or Windows 10 (build 1809).) or Linux System Installed.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

SCP

The behavior of Secure Copy (SCP) is similar to that of remote copy (RCP), which comes from the Berkeley r-tools suite (Berkeley university own set of networking applications), except that SCP relies on Secure Shell (SSH) for security. In addition, SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so that the device can determine whether the user has the correct privilege level

The SCP on Remote Server method (equivalent to SCP Push) periodically pushes log files by the secure copy protocol to a remote SCP server. This method requires an SSH SCP server on a remote computer with SSH2 protocol. The subscription requires a user name, SSH key, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by you.

SWA Log Subscription

You can create multiple log subscriptions for each type of log file. Subscriptions include configuration details for archiving and storage, including these:

- Rollover settings, which determine when log files are archived.
- Compression settings for archived logs.
- Retrieval settings for archived logs, which specify whether logs are archived onto a remote server or stored on the appliance.

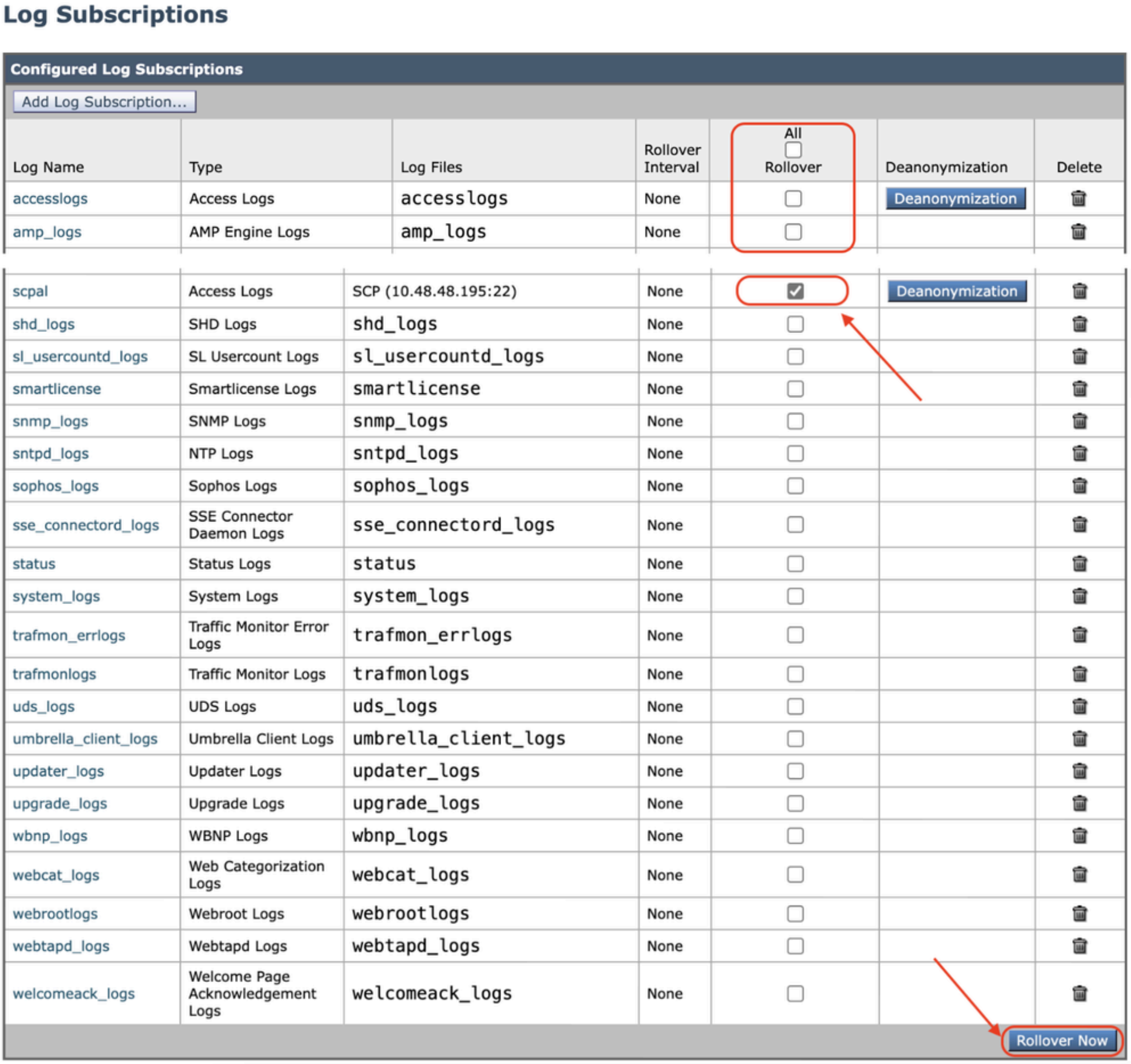
Archiving Log Files

AsyncOS archives (rolls over) log subscriptions when a current log file reaches a user-specified limit of maximum file size or maximum time since last rollover.

These archive settings are included in log subscriptions:

- Rollover by File Size
- Rollover by Time
- Log Compression
- Retrieval Method

You can also manually archive (rollover) log files.
Step 1. Choose **System Administration** > **Log Subscriptions**.
Step 2. Check the checkbox in the Rollover column of the log subscriptions to archive, or check the **All** checkbox to select all the subscriptions.
Step 3 .Click **Rollover Now** to archive the selected logs.



Log Subscriptions

Configured Log Subscriptions

Add Log Subscription...

Log Name	Type	Log Files	Rollover Interval	All □ Rollover	Deanonymization	Delete
accesslogs	Access Logs	accesslogs	None	□	Deanonymization	🗑
amp_logs	AMP Engine Logs	amp_logs	None	□		🗑
scpal	Access Logs	SCP (10.48.48.195:22)	None	☑	Deanonymization	🗑
shd_logs	SHD Logs	shd_logs	None	□		🗑
sl_usercountd_logs	SL Usercount Logs	sl_usercountd_logs	None	□		🗑
smartlicense	Smartlicense Logs	smartlicense	None	□		🗑
snmp_logs	SNMP Logs	snmp_logs	None	□		🗑
sntpd_logs	NTP Logs	sntpd_logs	None	□		🗑
sophos_logs	Sophos Logs	sophos_logs	None	□		🗑
sse_connectord_logs	SSE Connector Daemon Logs	sse_connectord_logs	None	□		🗑
status	Status Logs	status	None	□		🗑
system_logs	System Logs	system_logs	None	□		🗑
trafmon_errlogs	Traffic Monitor Error Logs	trafmon_errlogs	None	□		🗑
trafmonlogs	Traffic Monitor Logs	trafmonlogs	None	□		🗑
uds_logs	UDS Logs	uds_logs	None	□		🗑
umbrella_client_logs	Umbrella Client Logs	umbrella_client_logs	None	□		🗑
updater_logs	Updater Logs	updater_logs	None	□		🗑
upgrade_logs	Upgrade Logs	upgrade_logs	None	□		🗑
wbnp_logs	WBNP Logs	wbnp_logs	None	□		🗑
webcat_logs	Web Categorization Logs	webcat_logs	None	□		🗑
webrootlogs	Webroot Logs	webrootlogs	None	□		🗑
webtapd_logs	Webtapd Logs	webtapd_logs	None	□		🗑
welcomeack_logs	Welcome Page Acknowledgement Logs	welcomeack_logs	None	□		🗑

Rollover Now

Image - Rollover now GUI

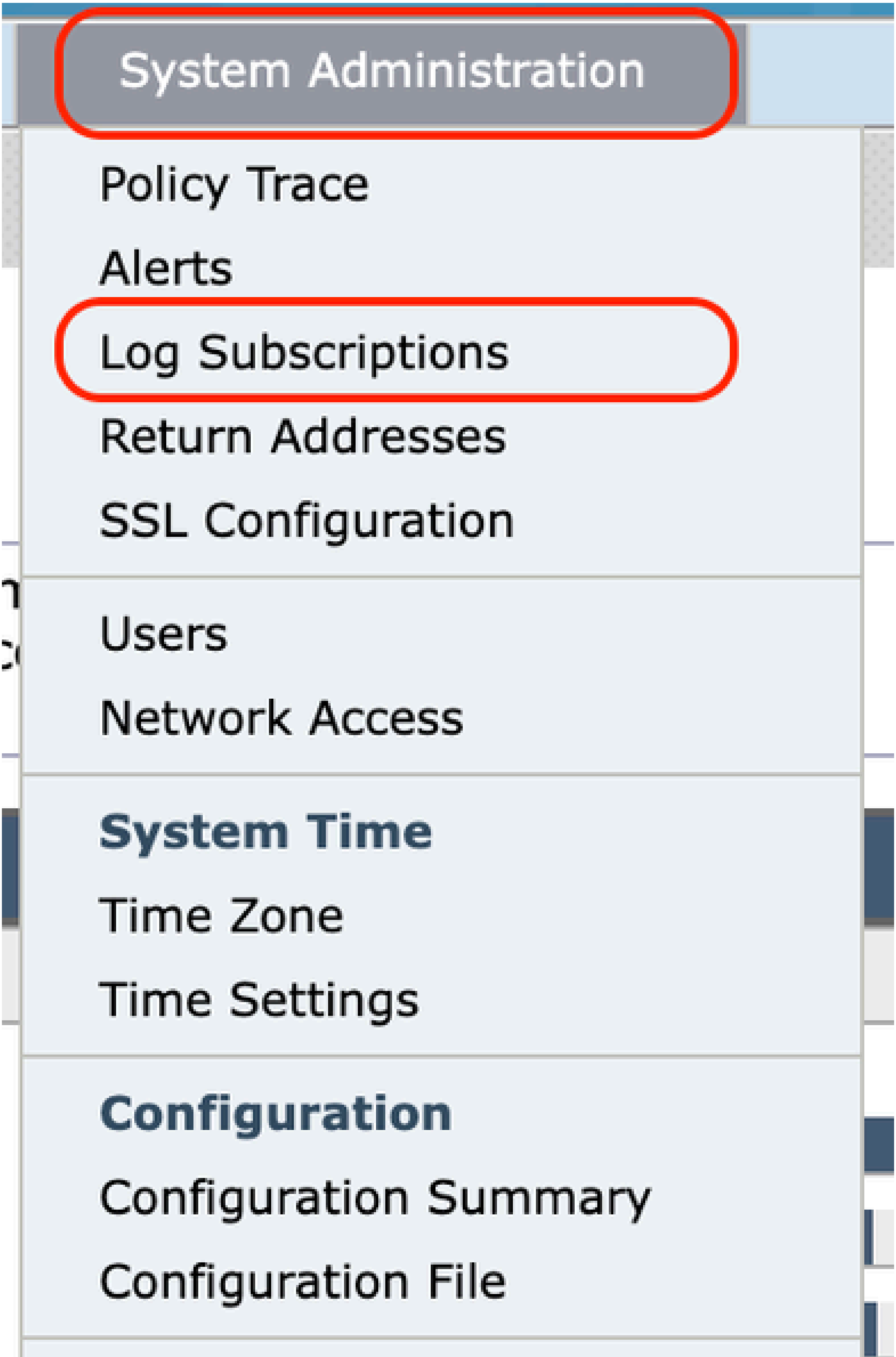
Configure Log Retrieval via SCP on Remote Server

There are two main steps to have log retrieval to a remote server with SCP from SWA:

1. Configure SWA to push the logs.
2. Configure remote server to receive the logs.

Configure SWA to Send The Logs to SCP Remote Server From GUI

Step 1. Log in to SWA and, from **System Administration,** choose **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

Open PowerShell with Administrator privileges (Run as Administrator) and run this command to check the prerequisites:

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

If the output is True, you can proceed. Otherwise, check with Microsoft support team,

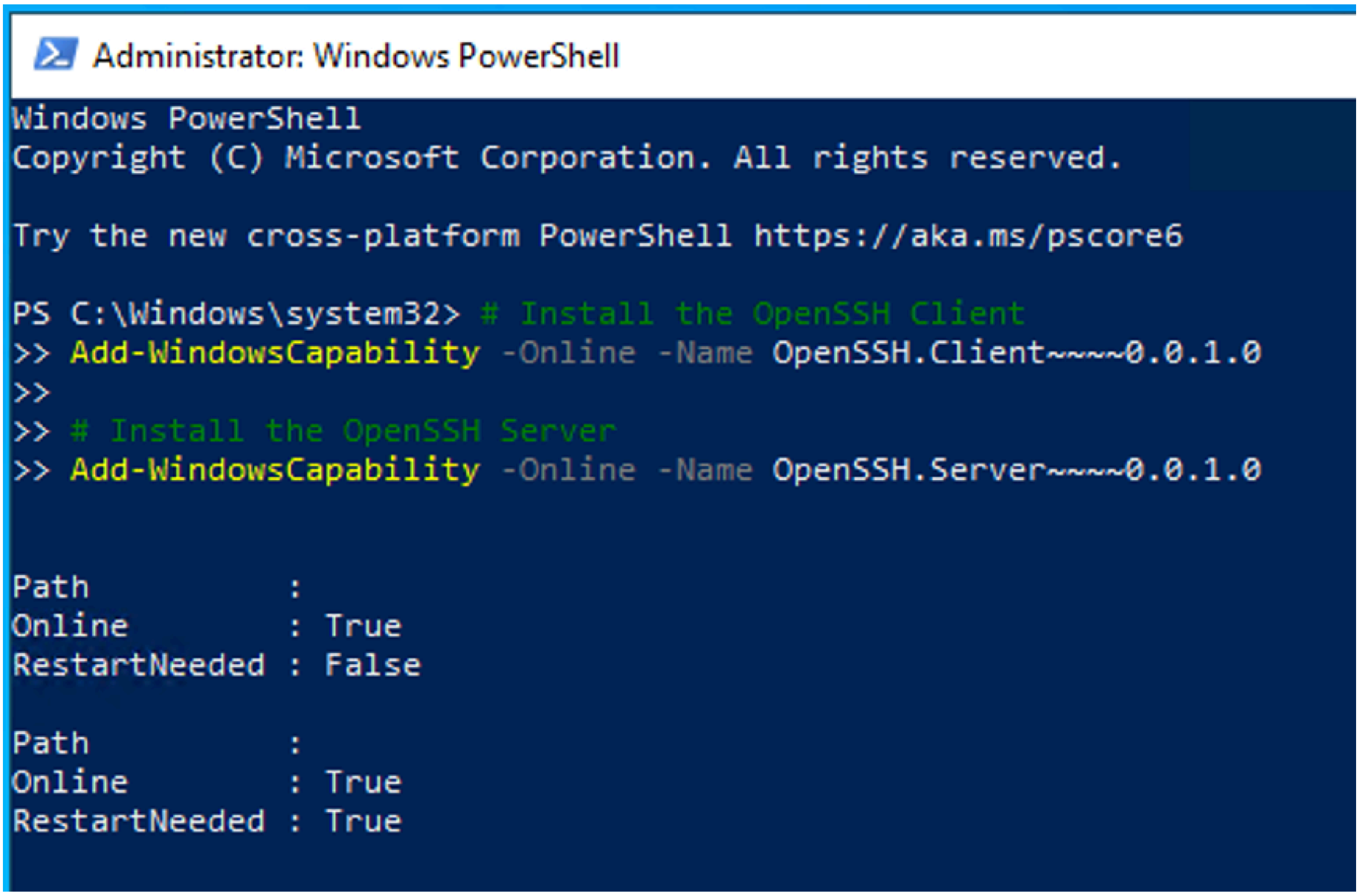
Step 18. To install OpenSSH using PowerShell with Administrator privilege (Run as Administrator), run :

```
# 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
```

Here is a sample of successful results:

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



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> # 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


Path          :
Online        : True
RestartNeeded : False

Path          :
Online        : True
RestartNeeded : True
```

Image- Install OpenSSH in PowerShell

⚠

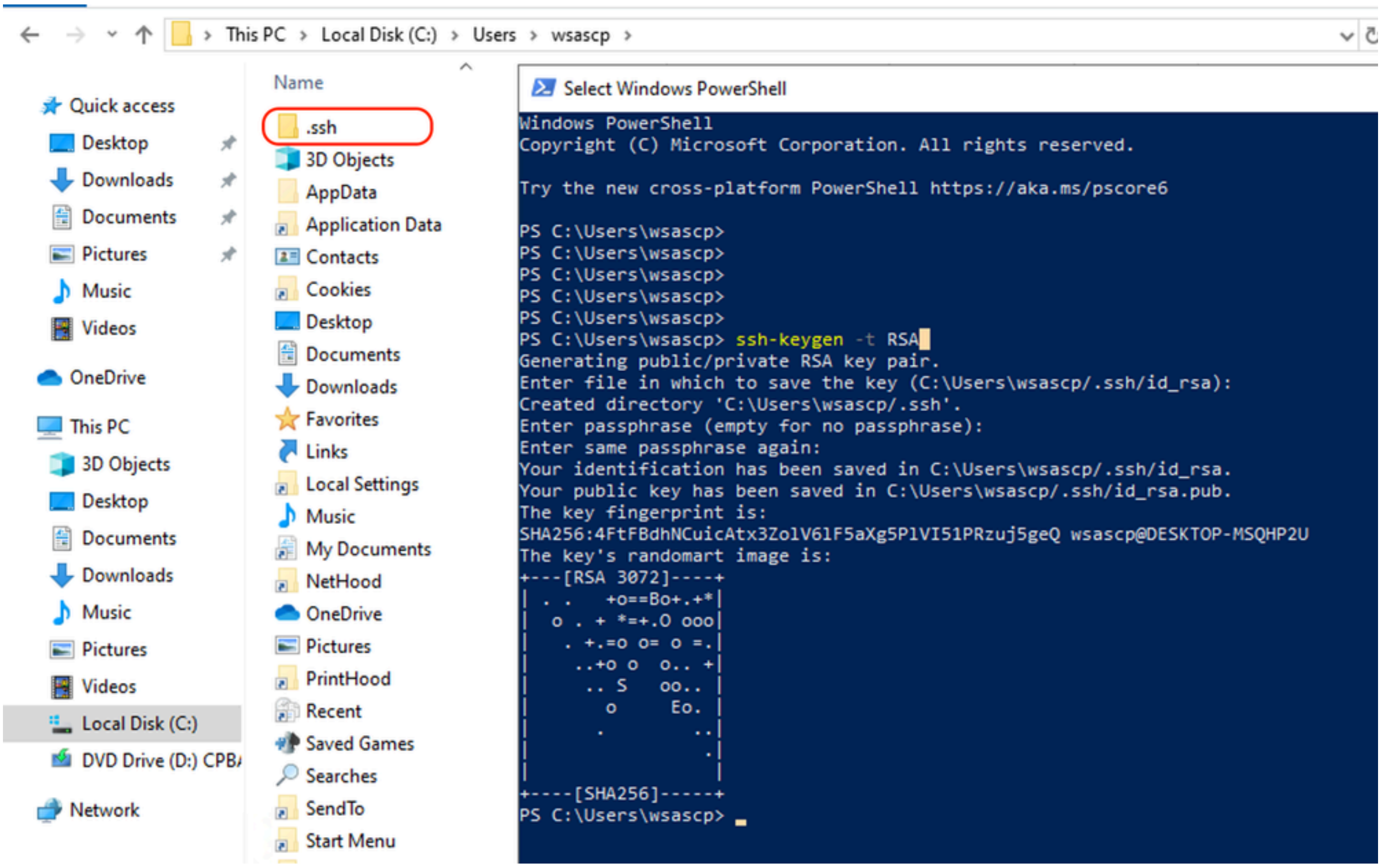
Caution: If **RestartNeeded** is set to True, please reboot the Windows .

For more information about the installation on other versions of Microsoft Windows, visit this link : Get started with OpenSSH for Windows | Microsoft Learn

Step 19. Open a normal (non-elevated) PowerShell session and generate a pair of RSA keys by using the command:

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

After the command is finished, you can see the **.ssh** folder has created your user profile directory.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\wsascp>
PS C:\Users\wsascp>
PS C:\Users\wsascp>
PS C:\Users\wsascp>
PS C:\Users\wsascp>
PS C:\Users\wsascp> ssh-keygen -t RSA
Generating public/private RSA key pair.
Enter file in which to save the key (C:\Users\wsascp/.ssh/id_rsa):
Created directory 'C:\Users\wsascp/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\wsascp/.ssh/id_rsa.
Your public key has been saved in C:\Users\wsascp/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:4FtFBdhNCuicAtx3ZolV6lF5aXg5PlVI51PRzuj5geQ wsascp@DESKTOP-MSQHP2U
The key's randomart image is:
+---[RSA 3072]----+
| . .   +o==Bo+.+*|
|  o . + *=+.O ooo|
|   . +.=o o= o =.|
|    ..+o o  o.. +|
|     .. S   oo.. |
|       o    Eo.  |
|      .        ..|
|                .|
|                 |
+----[SHA256]-----+
PS C:\Users\wsascp>
```

Image - Generate RSA Key

Step 20. Start the SSH service from PowerShell with Administrator privilege (Run as Administrator).

```
Start-Service sshd
```

Step 21. (Optional but recommended) Change the service Startup type to Automatic, with Administrator privilege (Run as Administrator).

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

Step 22. Confirm the firewall rule to allow access to TCP port 22 has been created.

```
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction SilentlyContinue | Select-Object N
    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."
}
```

Step 23. Edit SSH configuration file located in : **%programdata%\ssh\sshd_config** in notepad and remove the # for the RSA and DSA.

```
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
```

Step 24. Edit the connection conditions in **%programdata%\ssh\sshd_config**. In this example, the listen address is for all interfaces address. You can customize it due to your design.

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

Step 25. Mark these two lines at the end of the **%programdata%\ssh\sshd_config** file by adding # at the beginning of each line:

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

Step 26.(Optional) Edit the Strict Modes in **%programdata%\ssh\sshd_config**, By default, this mode is enabled and prevents SSH key-based authentication if private and public keys are not properly protected.

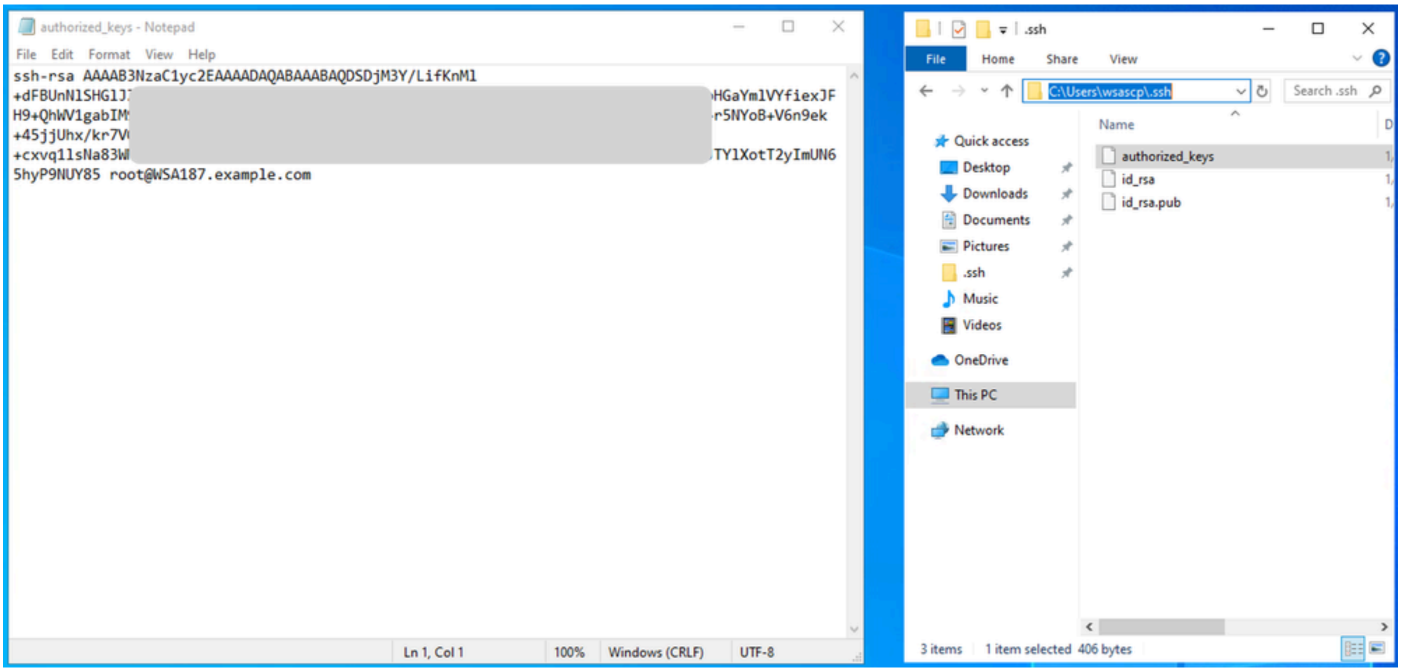
Un-comment the line #StrictModes yes and change it to StrictModes no:

```
StrictModes No
```

Step 27. Remove the # from this line to **%programdata%\ssh\sshd_config** to permit Public Key Authentication

```
PubkeyAuthentication yes
```

Step 28. Create a text file "**authorized_keys**" in .ssh folder and paste the SWA public RSA key (which was collected on step 9)



```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSDjM3Y/LifKnMl
+dFBUnN1SHG1J[redacted]HGaYmlVYfiexJF
H9+QhWV1gabIM                                                      r5NYoB+V6n9ek
+45jjUhx/kr7V
+cxvq1lsNa83W                                                      TY1XotT2yImUN6
5hyP9NUY85 root@WSA187.example.com
```

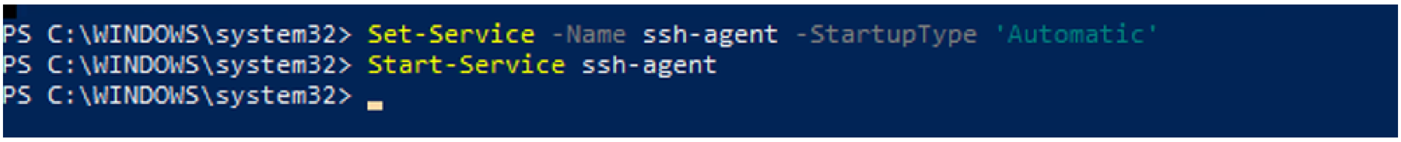
Image - SWA Public Key

Note: copy the whole line starting with **ssh-rsa** and ending with **root@<your_SWA_hostname>**

Tip: Since RSA is installed on the SCP server there is no need to paste the **ssh-dss** key

Step 29. Enable "OpenSSH Authentication Agent" in PowerShell with Administrator privilege (Run as Administrator).

```
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>
```

Image - Enable Open SSH Authentication Agent

Step 30.(Optional) Add this line to **%programdata%\ssh\sshd_config** to permit key types:

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

Step 31. Restart SSH service. You can use this command from PowerShell with Administrator privilege (Run as Administrator)

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

Step 32. To test if the SCP push is configured correct, rollover the configured logs, you can do it from both GUI or CLI (**rollovernow** command):

```
WSA_CLI> rollovernow scpal
```

Note: In this example the log name is "scpal".

You can confirm the logs are copied to the defined folder, which in this example was **c:/Users/wsascp/wsa01**

Push SCP Logs to Different Drive

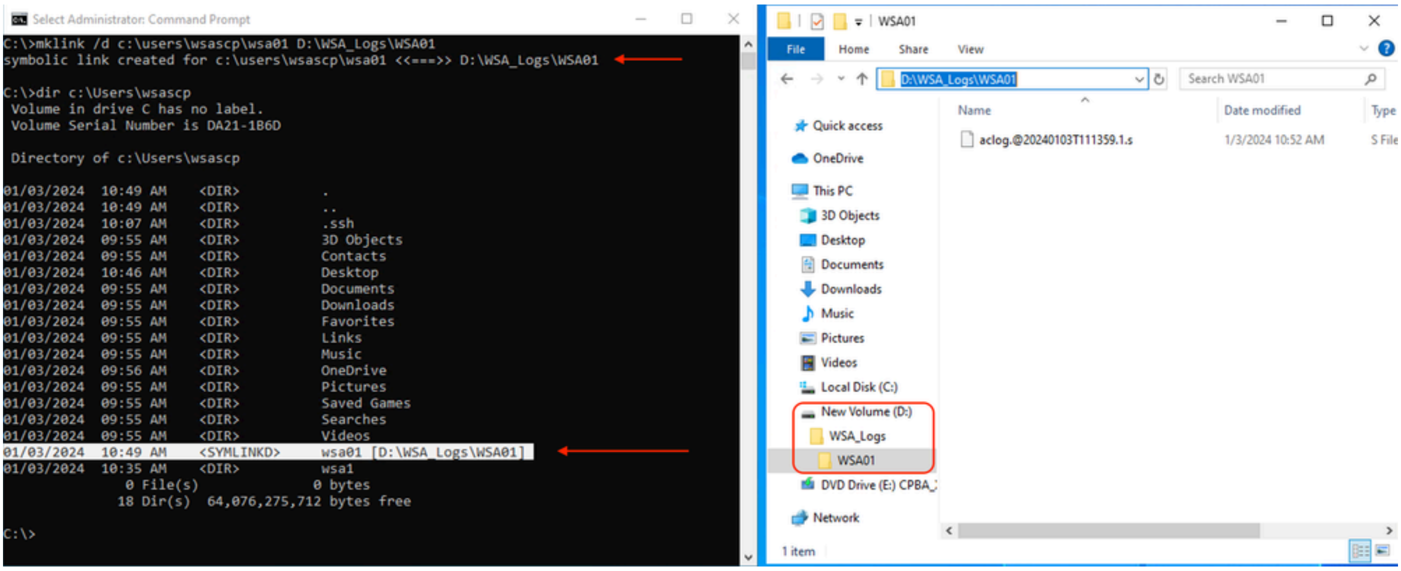
in case you need to push the logs to a different drive other than C:, create a link from user profile folder to desired drive. In this example the logs are pushed to **D:\WSA_Logs\WSA01** .

Step 1. create the folders in desired drive, in this example

Step 2. Open Command Prompt with Administrator privilege (Run as Administrator)

Step 3. Run this command to create the link:

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



```
C:\>mklink /d c:\users\wsascp\wsa01 D:\WSA_Logs\WSA01
symbolic link created for c:\users\wsascp\wsa01 <<===>> D:\WSA_Logs\WSA01

C:\>dir c:\Users\wsascp
 Volume in drive C has no label.
 Volume Serial Number is DA21-1B6D

 Directory of c:\Users\wsascp

01/03/2024  10:49 AM    <DIR>          .
01/03/2024  10:49 AM    <DIR>          ..
01/03/2024  10:07 AM    <DIR>          .ssh
01/03/2024  09:55 AM    <DIR>          3D Objects
01/03/2024  09:55 AM    <DIR>          Contacts
01/03/2024  10:46 AM    <DIR>          Desktop
01/03/2024  09:55 AM    <DIR>          Documents
01/03/2024  09:55 AM    <DIR>          Downloads
01/03/2024  09:55 AM    <DIR>          Favorites
01/03/2024  09:55 AM    <DIR>          Links
01/03/2024  09:55 AM    <DIR>          Music
01/03/2024  09:56 AM    <DIR>          OneDrive
01/03/2024  09:55 AM    <DIR>          Pictures
01/03/2024  09:55 AM    <DIR>          Saved Games
01/03/2024  09:55 AM    <DIR>          Searches
01/03/2024  09:55 AM    <DIR>          Videos
01/03/2024  10:49 AM    <SYMLINKD>     wsa01 [D:\WSA_Logs\WSA01]
01/03/2024  10:35 AM    <DIR>          wsa1
               0 File(s)              0 bytes
              18 Dir(s)  64,076,275,712 bytes free

C:\>
```

Image - Create SYM link

Note: In this Example SWA is configured to push the logs to WSA01 folder in C:\Users\wsascp , and the SCP server has folder WSA01 as Symbolic link to D:\WSA_Logs\WSA01

For more information about Microsoft Symbol Link please visit : mklink | Microsoft Learn

Troubleshoot SCP Log Push

View Logs in SWA

To troubleshoot the SCP log push, check the errors in:

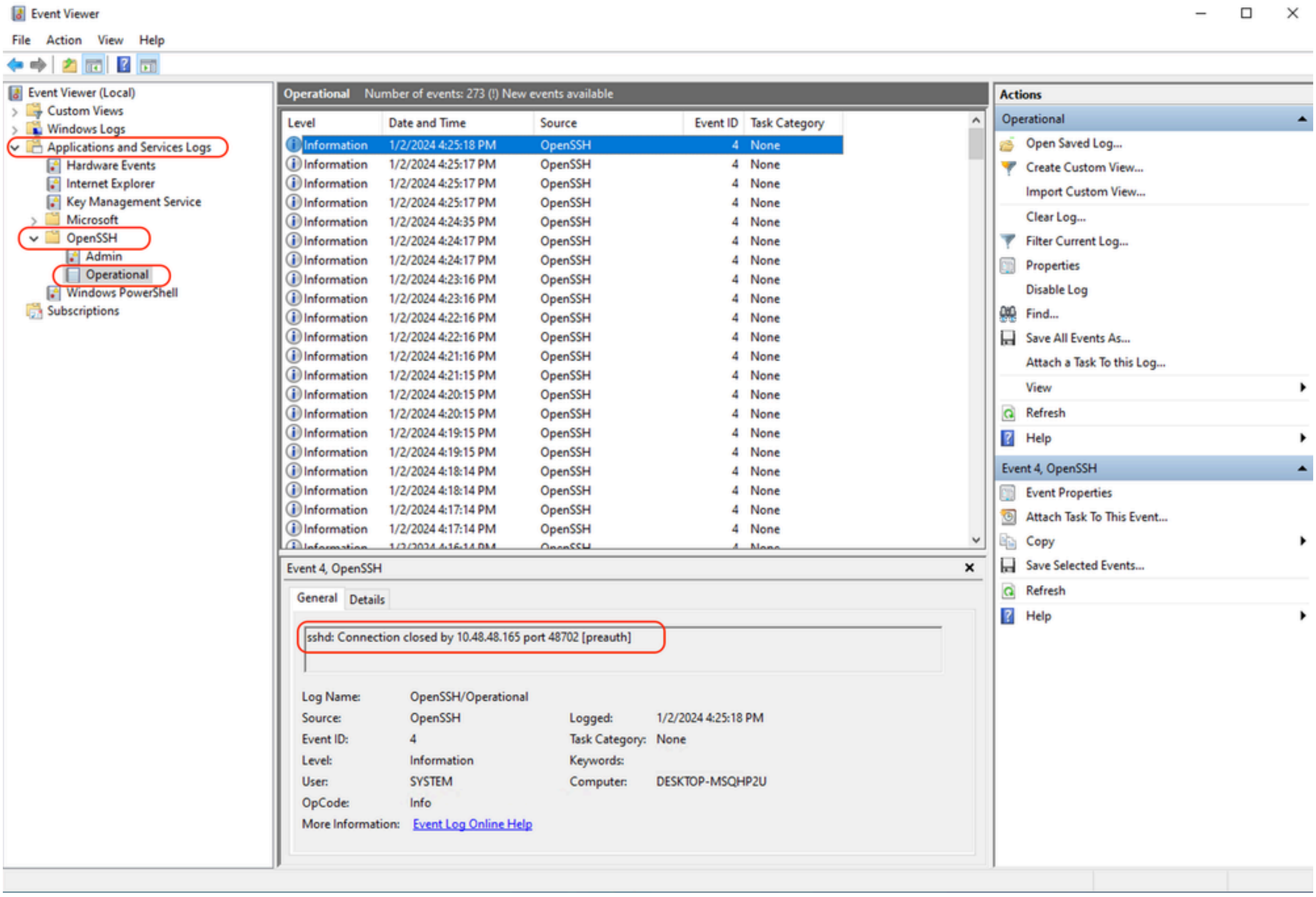
1. CLI > **displayalerts**

2. System_logs

Note: To read **system_logs**, you can use grep command in CLI , choose the number associated with **system_logs** and answer the question in the wizard.

View Logs in SCP server

You can read the SCP server logs in Microsoft Event Viewer, in **Applicataions and Services Logs** > **OpenSSH** > **Operational**



Level	Date and Time	Source	Event ID	Task Category
Information	1/2/2024 4:25:18 PM	OpenSSH	4	None
Information	1/2/2024 4:25:17 PM	OpenSSH	4	None
Information	1/2/2024 4:25:17 PM	OpenSSH	4	None
Information	1/2/2024 4:25:17 PM	OpenSSH	4	None
Information	1/2/2024 4:24:35 PM	OpenSSH	4	None
Information	1/2/2024 4:24:17 PM	OpenSSH	4	None
Information	1/2/2024 4:24:17 PM	OpenSSH	4	None
Information	1/2/2024 4:23:16 PM	OpenSSH	4	None
Information	1/2/2024 4:23:16 PM	OpenSSH	4	None
Information	1/2/2024 4:22:16 PM	OpenSSH	4	None
Information	1/2/2024 4:22:16 PM	OpenSSH	4	None
Information	1/2/2024 4:21:16 PM	OpenSSH	4	None
Information	1/2/2024 4:21:15 PM	OpenSSH	4	None
Information	1/2/2024 4:20:15 PM	OpenSSH	4	None
Information	1/2/2024 4:20:15 PM	OpenSSH	4	None
Information	1/2/2024 4:19:15 PM	OpenSSH	4	None
Information	1/2/2024 4:19:15 PM	OpenSSH	4	None
Information	1/2/2024 4:18:14 PM	OpenSSH	4	None
Information	1/2/2024 4:18:14 PM	OpenSSH	4	None
Information	1/2/2024 4:17:14 PM	OpenSSH	4	None
Information	1/2/2024 4:17:14 PM	OpenSSH	4	None

```
sshd: Connection closed by 10.48.48.165 port 48702 [preauth]
```

Log Name: OpenSSH/Operational
Source: OpenSSH   Logged: 1/2/2024 4:25:18 PM
Event ID: 4   Task Category: None
Level: Information   Keywords:
User: SYSTEM   Computer: DESKTOP-MSQHP2U
OpCode: Info
More Information: Event Log Online Help

Image - PreAuth Failed

Host key verification failed

This Error indicates that the SCP server public key stored in SWA is invalid.

Here is a sample of error from **displayalerts** output in CLI:

```
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.
```

Here are some sample of Error in system_logs :

```
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
```

To solve this issue, you can copy the Host from SCP server and paste it in SCP logs subscription page.

Refer to step 7 in **Configure SWA** to **Send The Logs to SCP Remote Server From GUI** or you can contact Cisco TAC to remove the Host Key from backend.

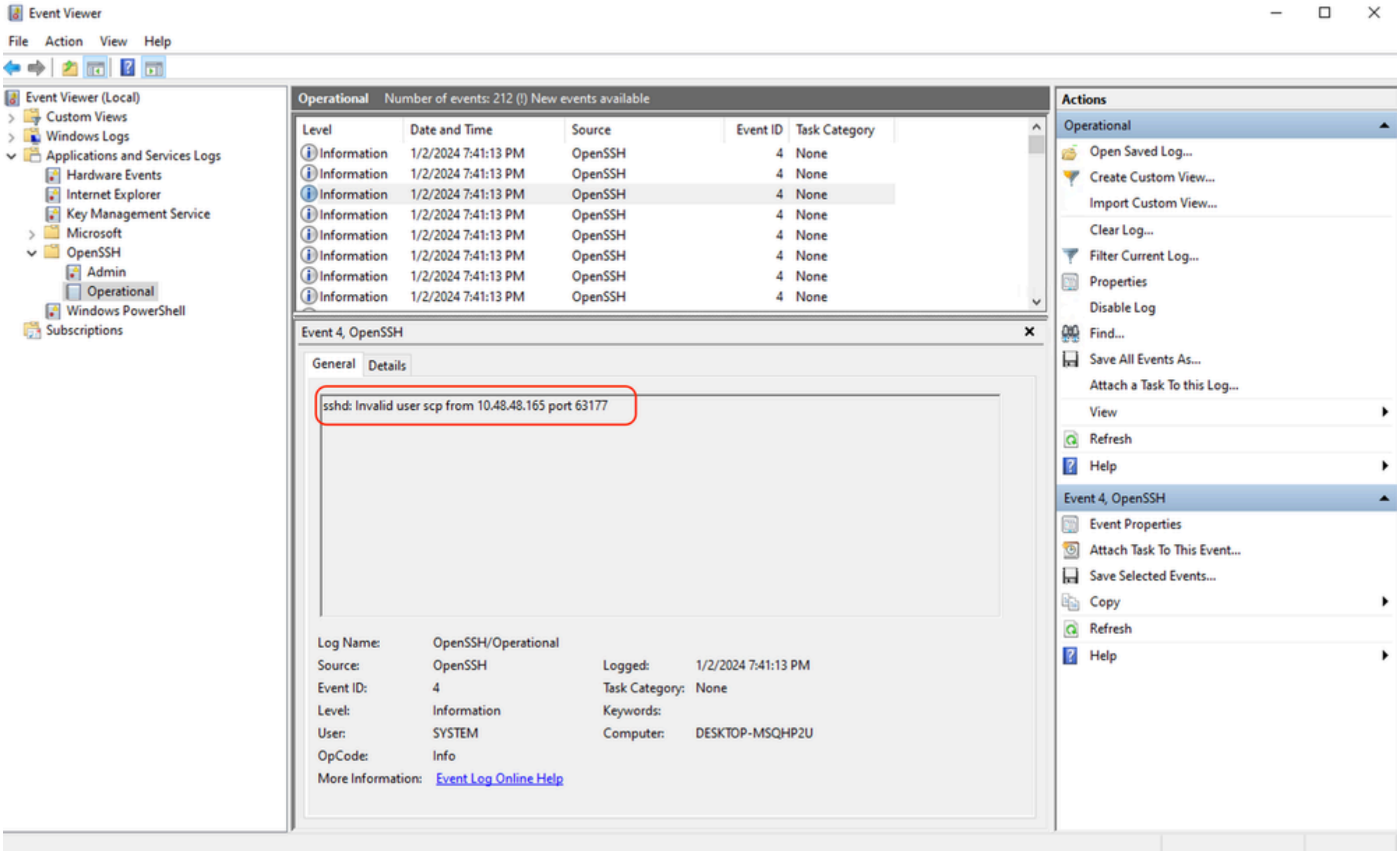
Permission denied (publickey,password,keyboard-interactive)

This error usually indicates that the username provided in SWA is invalid.

Here is a sample of error log in system_logs :

```
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
```

Here is a sample of error from SCP server: **Invalid user SCP from <SWA_IP address> port <TCP port SWA conencts to SCP server>**



Operational Number of events: 212 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None
Information	1/2/2024 7:41:13 PM	OpenSSH	4	None

Event 4, OpenSSH

General Details

```
sshd: Invalid user scp from 10.48.48.165 port 63177
```

Log Name: OpenSSH/Operational
Source: OpenSSH Logged: 1/2/2024 7:41:13 PM
Event ID: 4 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-MSQHP2U
OpCode: Info
More Information: Event Log Online Help

Image- Invalid User

To solve this error, please check the spelling and verify that the user (configured in SWA to push the logs) is Enabled in SCP server.

No such file or directory

This Error Indicates that the path provided in SWA logs subscription section is not valid, Here is a sample of error from system_logs:

```
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
```

To solve this issue, verify the spelling and make sure the path is correct and valid in SCP server.

SCP failed to transfer

this error could be an indicator of a communication error. Here is the sample of error:

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

To troubleshoot the connectivity, use the telnet command in SWA CLI:

```
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...
```

In this example the connection is not established. The successful connection out is like:

```
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
```

If the telnet is not connected:

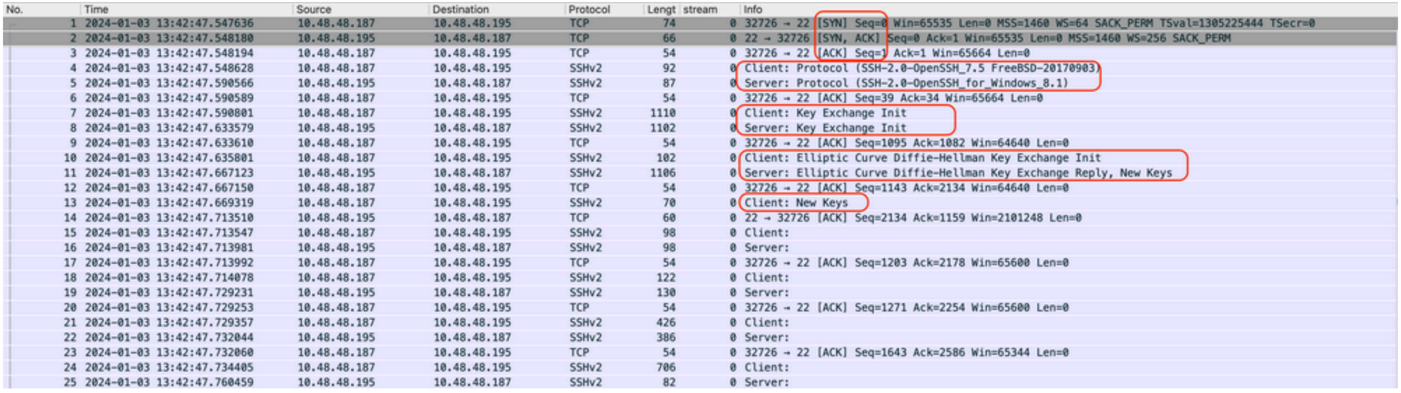
[1] Check If the SCP server firewall is blocking the access.

[2] Check if there are any firewalls in the path from SWA to SCP server blocking the access.

[3] Check if the TCP port 22 is in a listen state in SCP server .

[4] Run packet capture in both SWA ans SCP server for further analysis.

Here is a sample of Packet Capture of successful connection:



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:

Image - Successful Connection Packet Capture

References

Cisco Web Security Appliance Best Practices Guidelines - Cisco

BRKSEC-3303 (ciscolive)

User Guide for AsyncOS 14.5 for Cisco Secure Web Appliance - GD (General Deployment) - Connect, Install, and Configure [Cisco Secure Web Appliance] - Cisco

Get started with OpenSSH for Windows | Microsoft Learn

Configuring SSH Public Key Authentication on Windows | Windows OS Hub (woshub.com)

Key-based authentication in OpenSSH for Windows | Microsoft Learn