

Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[SCP](#)

[Sottoscrizione log SWA](#)

[Archiviazione dei file di log](#)

[Configurare LogRetrieval tramite SCP sul server remoto](#)

[Configurare SWA per l'invio dei log al server remoto SCP dalla GUI](#)

[Configurare Microsoft Windows come server remoto SCP](#)

[Push dei registri SCP su un'unità diversa](#)

[Risoluzione dei problemi di push del log SCP](#)

[Visualizza log in SWA](#)

[Visualizza log nel server SCP](#)

[Verifica della chiave host non riuscita](#)

[Autorizzazione negata \(chiave pubblica, password, tastiera-interattiva\)](#)

[Impossibile trasferire SCP](#)

[Riferimenti](#)

Introduzione

In questo documento viene descritto come configurare Secure Copy (SCP) per copiare automaticamente i log in Secure Web Appliance (SWA) su un altro server.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come funziona SCP.
- Amministrazione della SWA.
- Amministrazione del sistema operativo Microsoft Windows o Linux.

Cisco raccomanda:

- SWA fisico o virtuale installato.

- Licenza attivata o installata.
- Installazione guidata completata.

- Accesso amministrativo all'interfaccia grafica (GUI) SWA.
- Microsoft Windows (almeno Windows Server 2019 o Windows 10 (build 1809).) o Linux System Installed.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

SCP

Il comportamento di Secure Copy (SCP) è simile a quello di Remote Copy (RCP), che proviene dalla suite di r-tool Berkeley (il set di applicazioni di rete di proprietà dell'Università di Berkeley), con la differenza che SCP si basa su Secure Shell (SSH) per la sicurezza. Inoltre, SCP richiede che l'autorizzazione di autenticazione, autorizzazione e accounting (AAA) sia configurata in modo che il dispositivo possa determinare se l'utente dispone del livello di privilegi corretto

Il metodo SCP su server remoto (equivalente al metodo SCP Push) invia periodicamente i file di registro tramite il protocollo di copia sicura a un server SCP remoto. Questo metodo richiede un server SSH SCP su un computer remoto con protocollo SSH2. La sottoscrizione richiede un nome utente, una chiave SSH e una directory di destinazione nel computer remoto. I file di log vengono trasferiti in base a una pianificazione di rolover impostata dall'utente.

Sottoscrizione log SWA

È possibile creare più sottoscrizioni di log per ogni tipo di file di log. Le sottoscrizioni includono i dettagli di configurazione per l'archiviazione e l'archiviazione, tra cui:

- Impostazioni di rolover, che determinano quando archiviare i file di log.
- Impostazioni di compressione per i log archiviati.
- Impostazioni di recupero per i registri archiviati, che specificano se i registri vengono archiviati in un server remoto o archiviati nell'accessorio.

Archiviazione dei file di log

Le sottoscrizioni dei log degli archivi AsyncOS (rollover) vengono eseguite quando un file di log corrente raggiunge un limite specificato dall'utente per le dimensioni massime del file o il tempo massimo dall'ultimo rolover.

Le seguenti impostazioni di archiviazione sono incluse nelle sottoscrizioni dei log:

- Rollover per dimensioni file
- Rollover per ora
- Compressione log
- Metodo di recupero

È inoltre possibile archiviare manualmente (eseguire il rollover) i file di registro.

Passaggio 1. Scegliete Amministrazione di sistema > Registra sottoscrizioni.

Passaggio 2. Selezionare la casella di spunta nella colonna Rollover delle sottoscrizioni di log da archiviare oppure selezionare la casella di spunta Tutte per selezionare tutte le sottoscrizioni.

3. Fare clic su Esegui rollover ora per archiviare i log selezionati.

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](#)

Configurazione del recupero del log tramite SCP sul server remoto

Per il recupero del log su un server remoto con SCP da SWA, è necessario eseguire due passaggi principali:

1. Configurare SWA per eseguire il push dei log.
2. Configurare il server remoto per la ricezione dei registri.

Configurare SWA per l'invio dei log al server remoto SCP dalla GUI

Passaggio 1. Accedere a SWA e, da Amministrazione sistema, scegliere Registra sottoscrizioni.

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

System Time

Time Zone

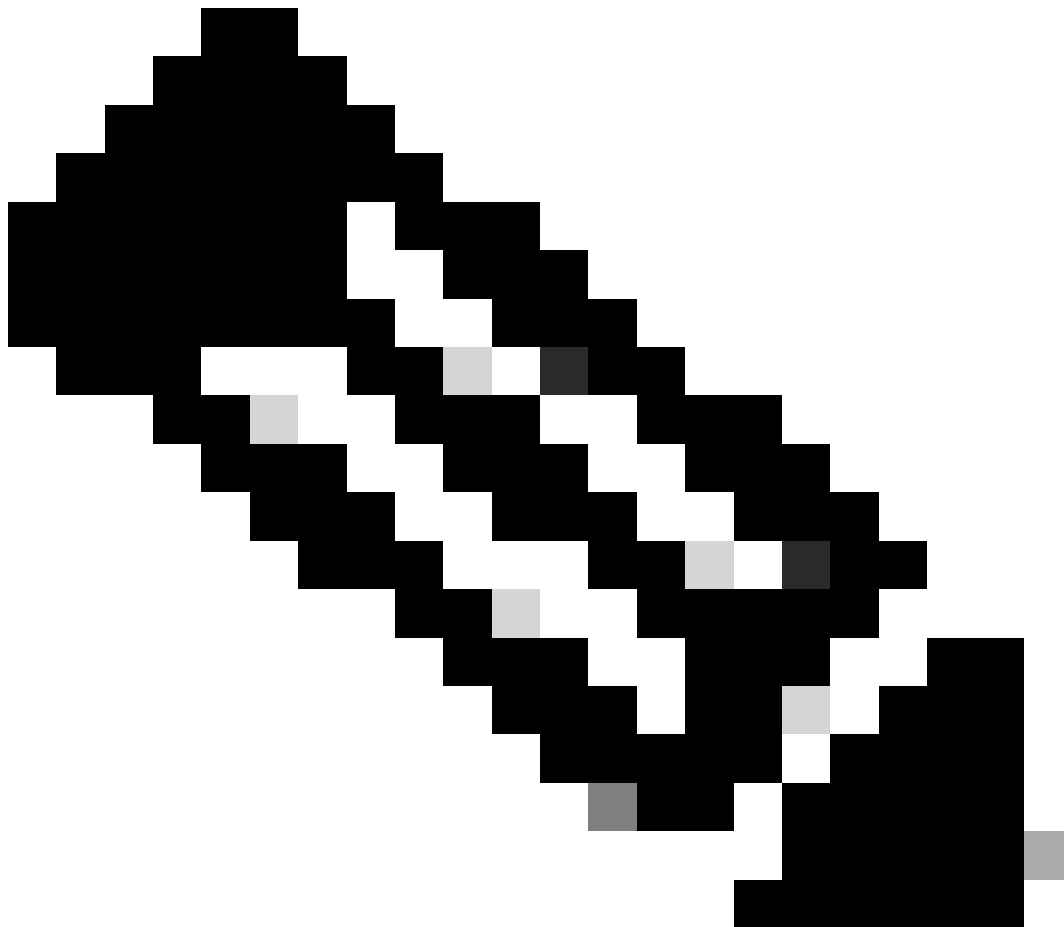
Time Settings

Configuration

Configuration Summary

Configuration File

Salvare la chiave SSH in un file di testo per poterla usare nella sezione di configurazione del server SCP remoto.



Nota: è necessario copiare entrambe le righe iniziando con ssh- e terminando con root@<nome host SWA> .

Log Subscriptions

Success — Log Subscription "SCP_Access_Logs" was added.

Please place the following SSH key(s) into your authorized_keys file:

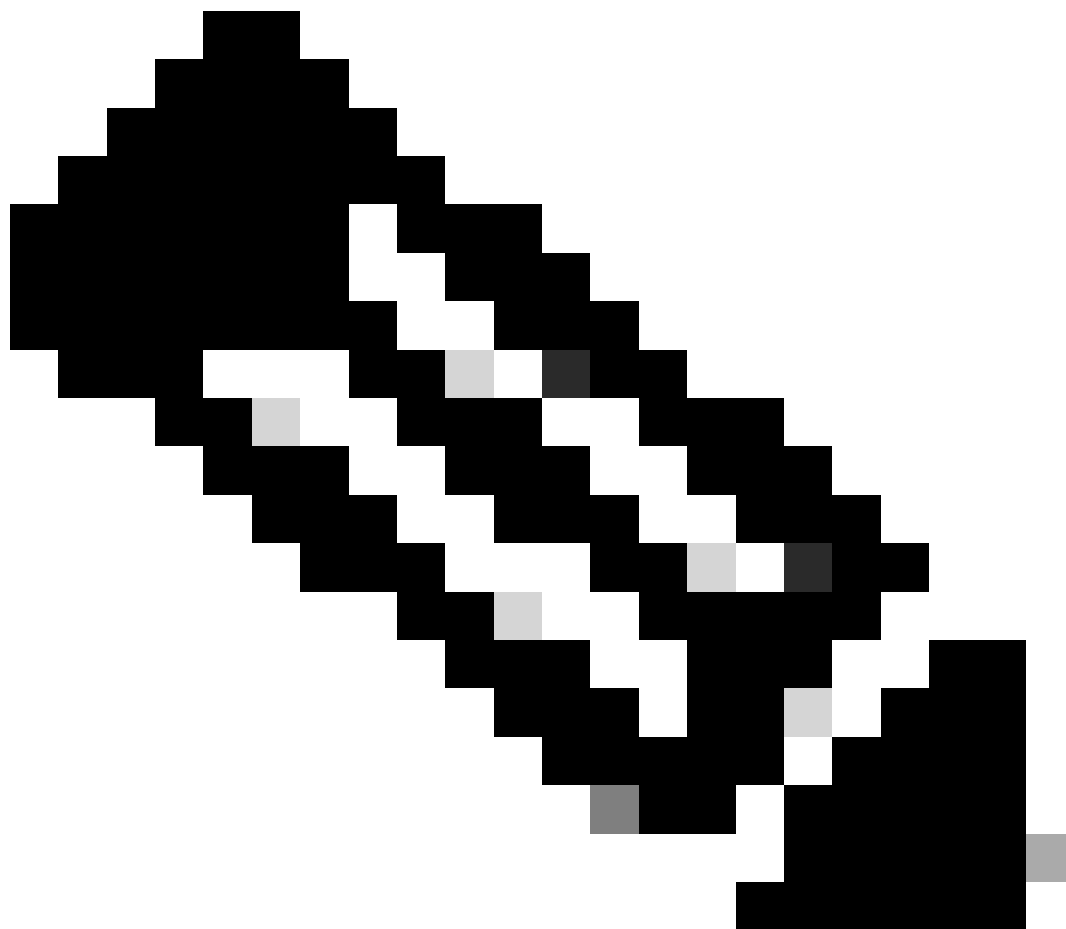
```
ssh-dss  
AAAAB3NzaC1kc3MAAACBAOuNX6TUOmzIWolPkVQ5I7LC/9yv:  
root@122[REDACTED]le.com  
  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACwbJziB4AE7H
```

Image (Immagine) - Salvare la chiave SSH per un ulteriore utilizzo.

Passaggio 10. Eseguire il commit delle modifiche.

Configurare Microsoft Windows come server remoto SCP

Passaggio 10. Per creare un utente per il servizio SCP, passare a Gestione computer:



Nota: se si dispone già di un utente per SCP, andare al passo 16.

Passaggio 11. Selezionare Utenti e gruppi locali e scegliere Utenti dal riquadro di sinistra.

Passaggio 12. Fare clic con il pulsante destro del mouse sulla pagina principale e scegliere nuovo utente.

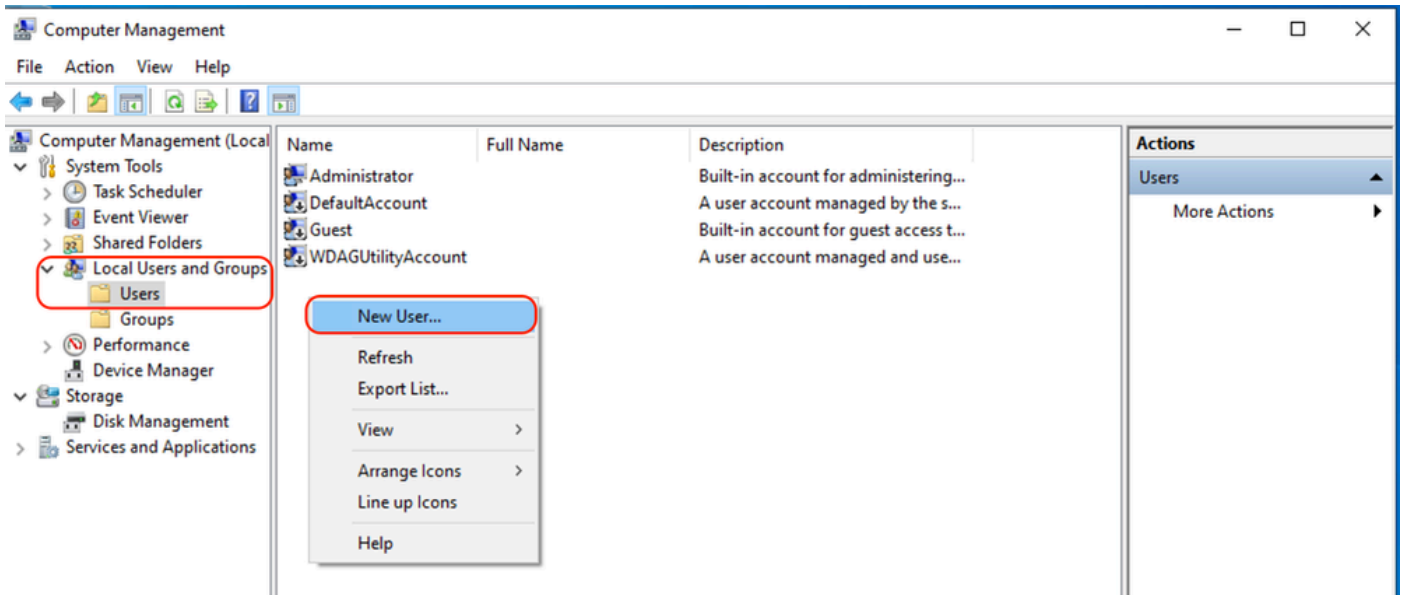


Immagine - Crea un utente per il servizio SCP.

Passaggio 13. Immettere il nome utente e la password desiderati.

Passaggio 14. Scegliere Password Never Expired.

Passaggio 15. Fare clic su Crea, quindi chiudere la finestra.

New User ? X

User name: wsascp

Full name: WSA SCP |

Description: SCP username for SWA logs

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

Help Create Close

Image (Immagine) - Consente di immettere le informazioni sul nuovo utente.

Passaggio 16. Accedere al server SCP remoto con l'utente appena creato per creare la directory dei profili.

Nota: se OpenSSL è installato sul server SCP remoto, andare al passaggio 19.

Passaggio 17. Aprire PowerShell con privilegi di amministratore (Esegui come amministratore) ed eseguire questo comando per verificare i prerequisiti:

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

Se l'output è True, è possibile procedere. In caso contrario, rivolgersi al team di supporto Microsoft,

Passaggio 18. Per installare OpenSSH utilizzando PowerShell con privilegi di amministratore (Esegui come amministratore), eseguire :

```
# Install the OpenSSH Client
```

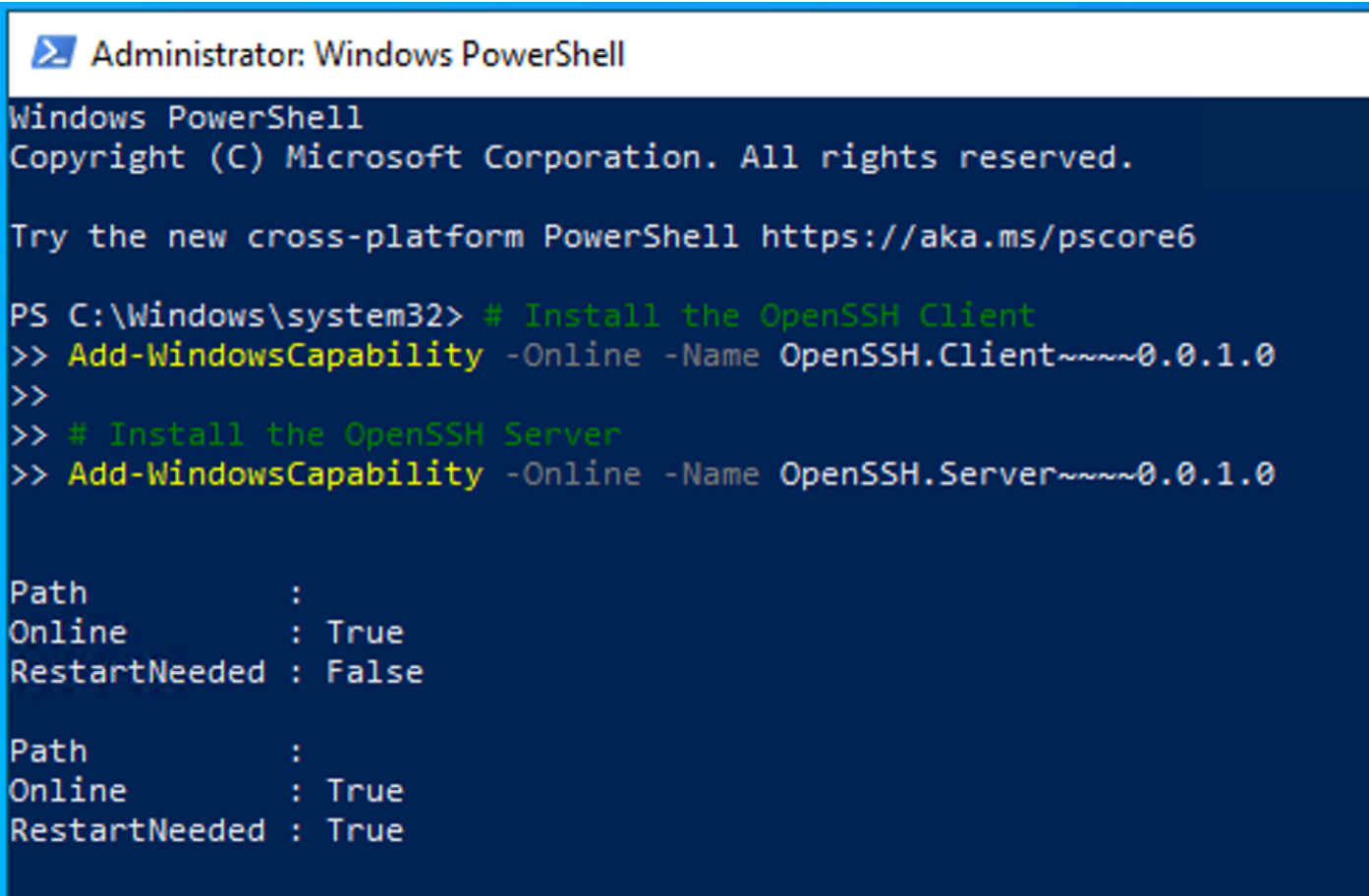
```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

```
# Install the OpenSSH Server
```

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

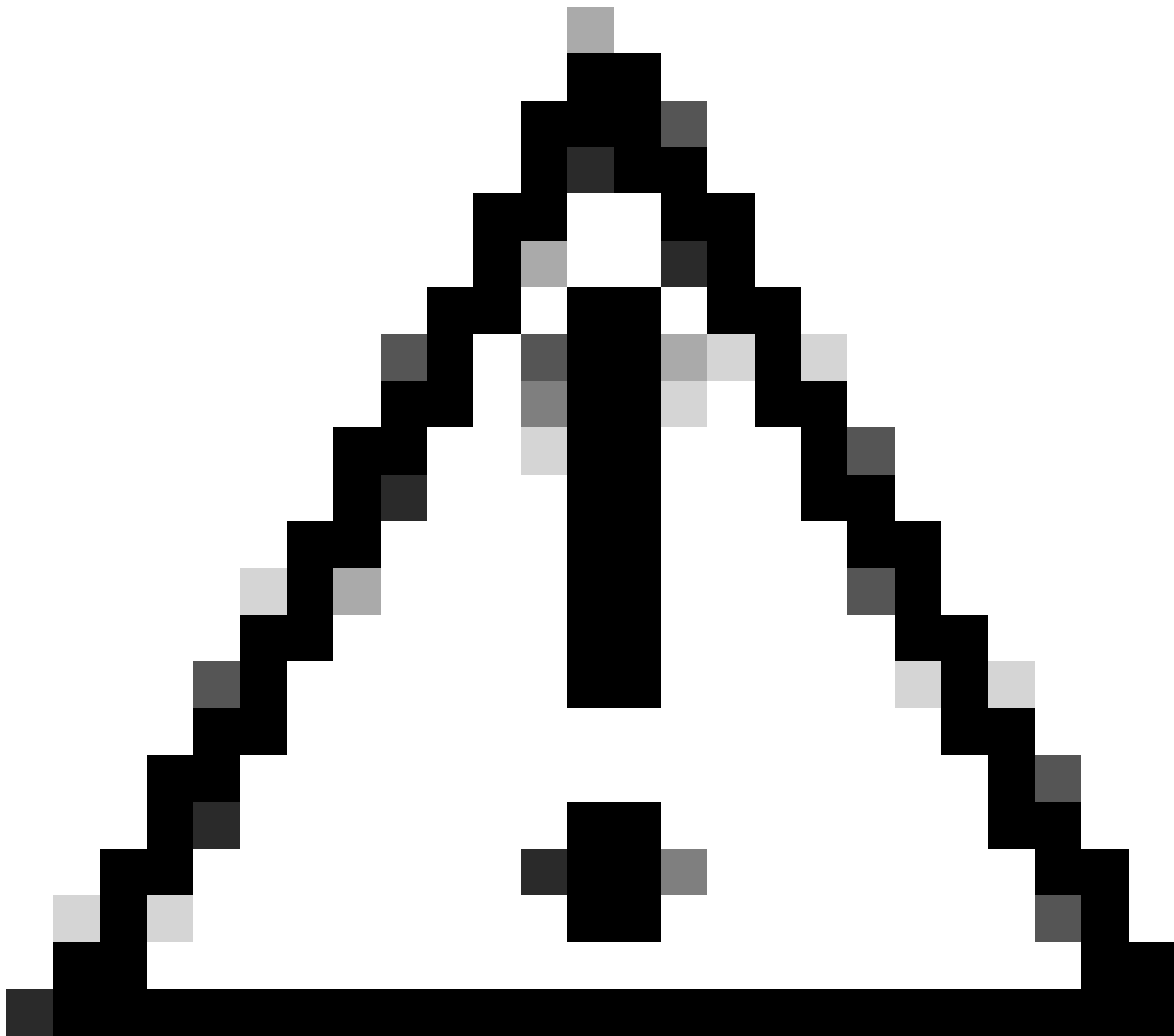
Di seguito è riportato un esempio di risultati positivi:

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



```
Administrator: Windows PowerShell  
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
```

Immagine: installazione di OpenSSH in PowerShell



Attenzione: se `RestartNeeded` è impostato su `True`, riavviare Windows.

Per ulteriori informazioni sull'installazione in altre versioni di Microsoft Windows, visitare questo collegamento: [Introduzione a OpenSSH per Windows | Microsoft Learn](#)

Passaggio 19. Aprire una sessione PowerShell normale (senza privilegi elevati) e generare una coppia di chiavi RSA utilizzando il comando:

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

Al termine del comando, è possibile verificare che la cartella `.ssh` ha creato la directory del profilo utente.

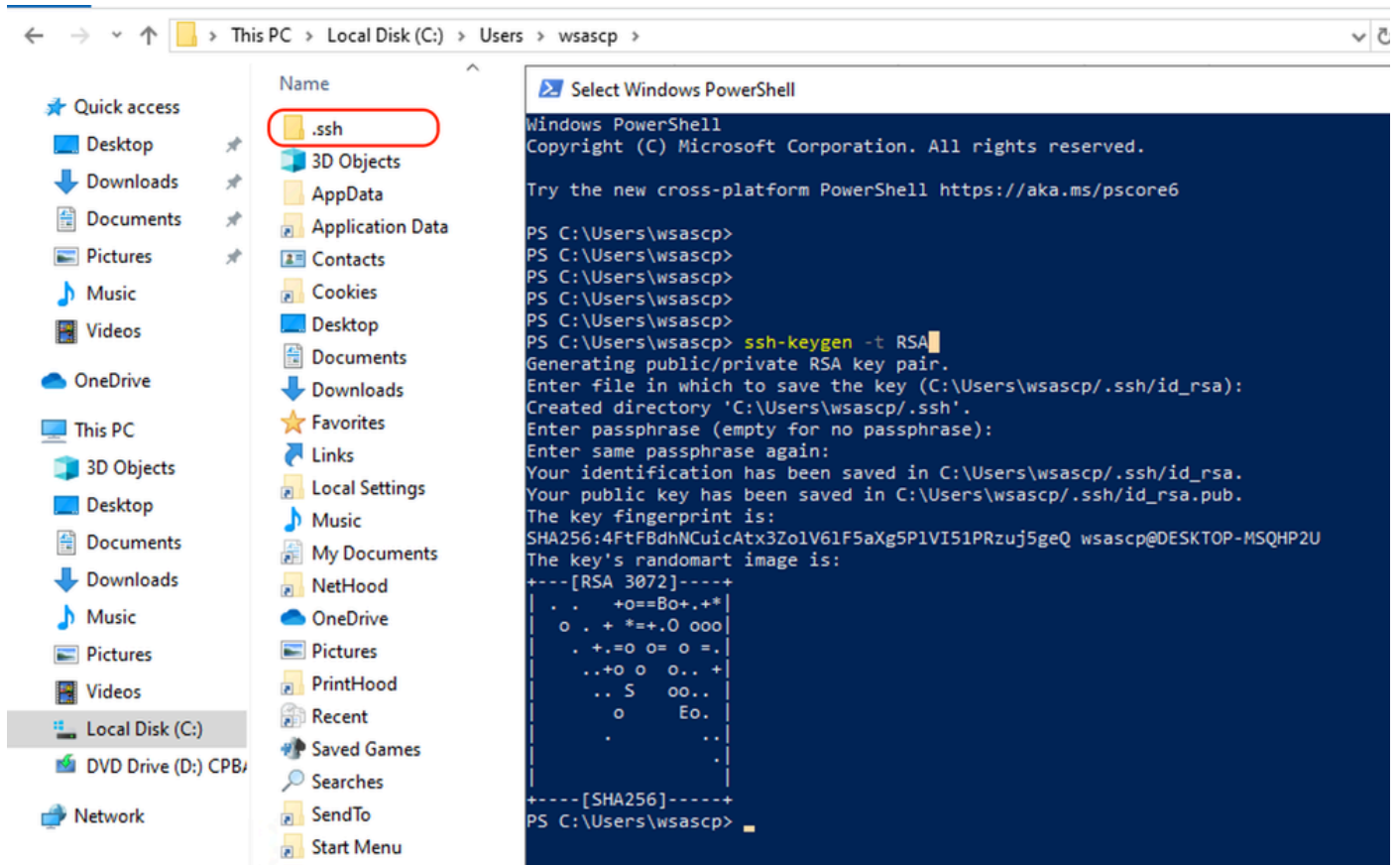


Immagine - Genera chiave RSA

Passaggio 20. Avviare il servizio SSH da PowerShell con il privilegio di amministratore (Esegui come amministratore).

```
Start-Service sshd
```

Passaggio 21. (Facoltativo ma consigliato) Impostare il tipo di avvio del servizio su Automatico, con il privilegio di amministratore (Esegui come amministratore).

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

Passaggio 22. Confermare la creazione della regola firewall per consentire l'accesso alla porta TCP 22.

```
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction SilentlyContinue | Select-Object Name) {
    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 True
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and exists."
}
```

Passaggio 23. Modificare il file di configurazione SSH situato in :

%programdata%\ssh\sshd_config nel Blocco note e rimuovere il simbolo di errore # per RSA e 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
```

Passaggio 24. Modificare le condizioni di connessione in %programdata%\ssh\sshd_config. In questo esempio, l'indirizzo di ascolto è per tutti gli indirizzi di interfacce. È possibile personalizzarlo in base al progetto.

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

Passaggio 25. Contrassegnare le due righe seguenti alla fine del file %programdata%\ssh\sshd_config aggiungendo # all'inizio di ogni riga:

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

Passaggio 26.(Facoltativo) Modificare le modalità rigorose in %programdata%\ssh\sshd_config. Per impostazione predefinita, questa modalità è abilitata e impedisce l'autenticazione basata su chiave SSH se le chiavi pubblica e privata non sono protette correttamente.

Rimuovere il commento dalla riga #StrictModes yes e modificarla in StrictModes no:

```
StrictModes No
```

Passaggio 27. Rimuovere # da questa riga in %programdata%\ssh\sshd_config per consentire l'autenticazione con chiave pubblica

```
PubkeyAuthentication yes
```

Passaggio 28. Creare un file di testo "authorized_keys" nella cartella .ssh e incollare la chiave RSA pubblica SWA (raccolta nel passaggio 9)

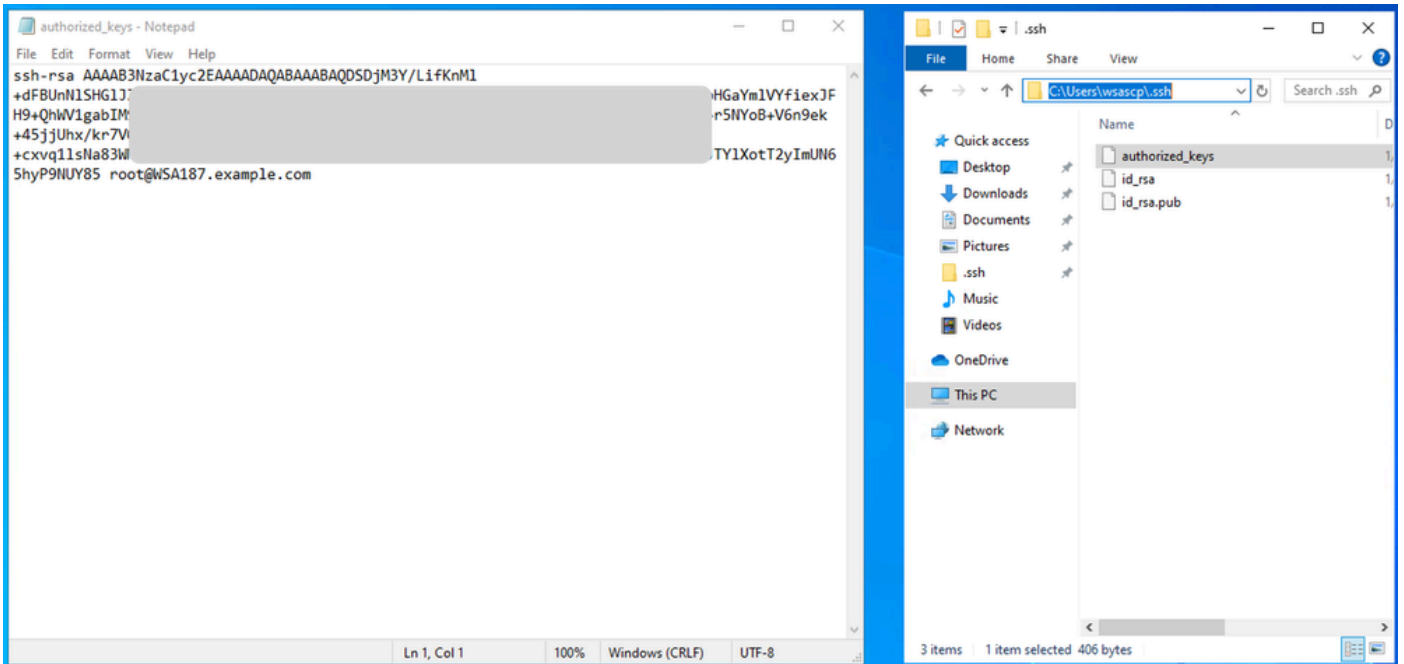
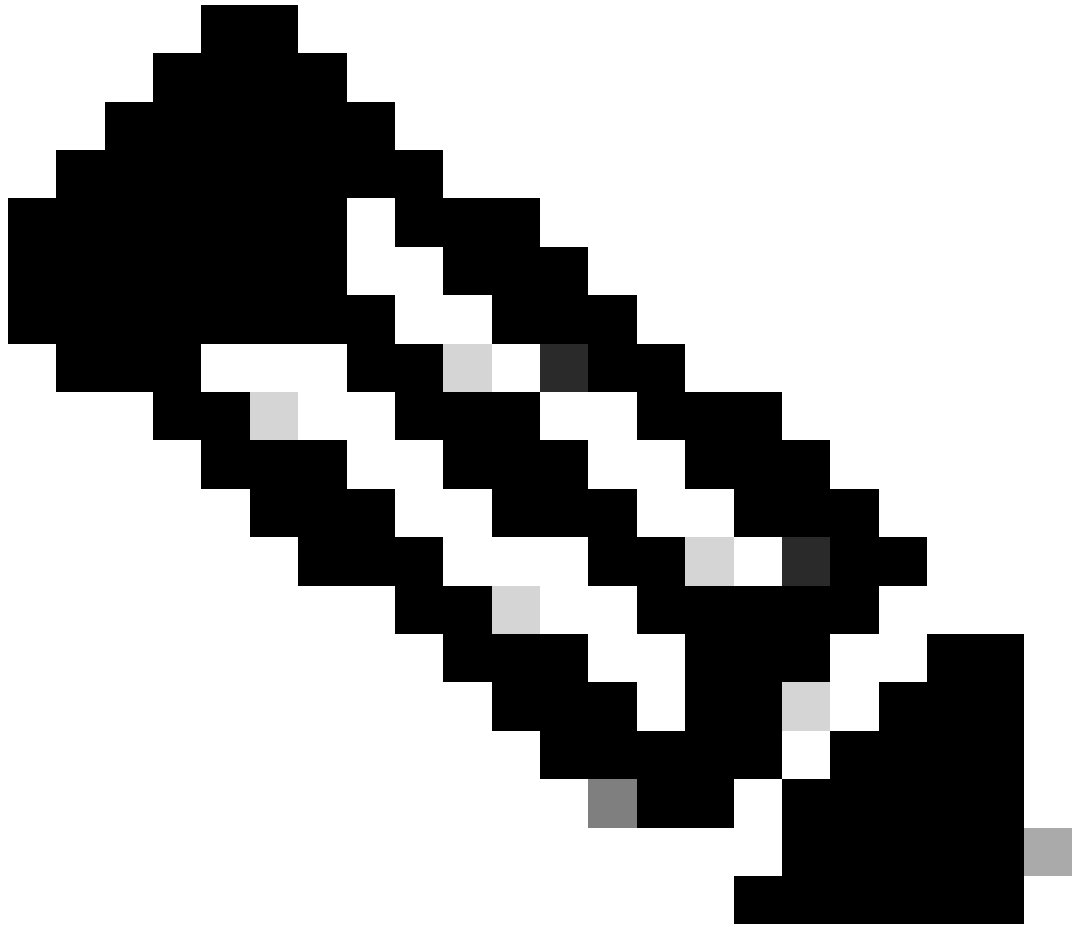
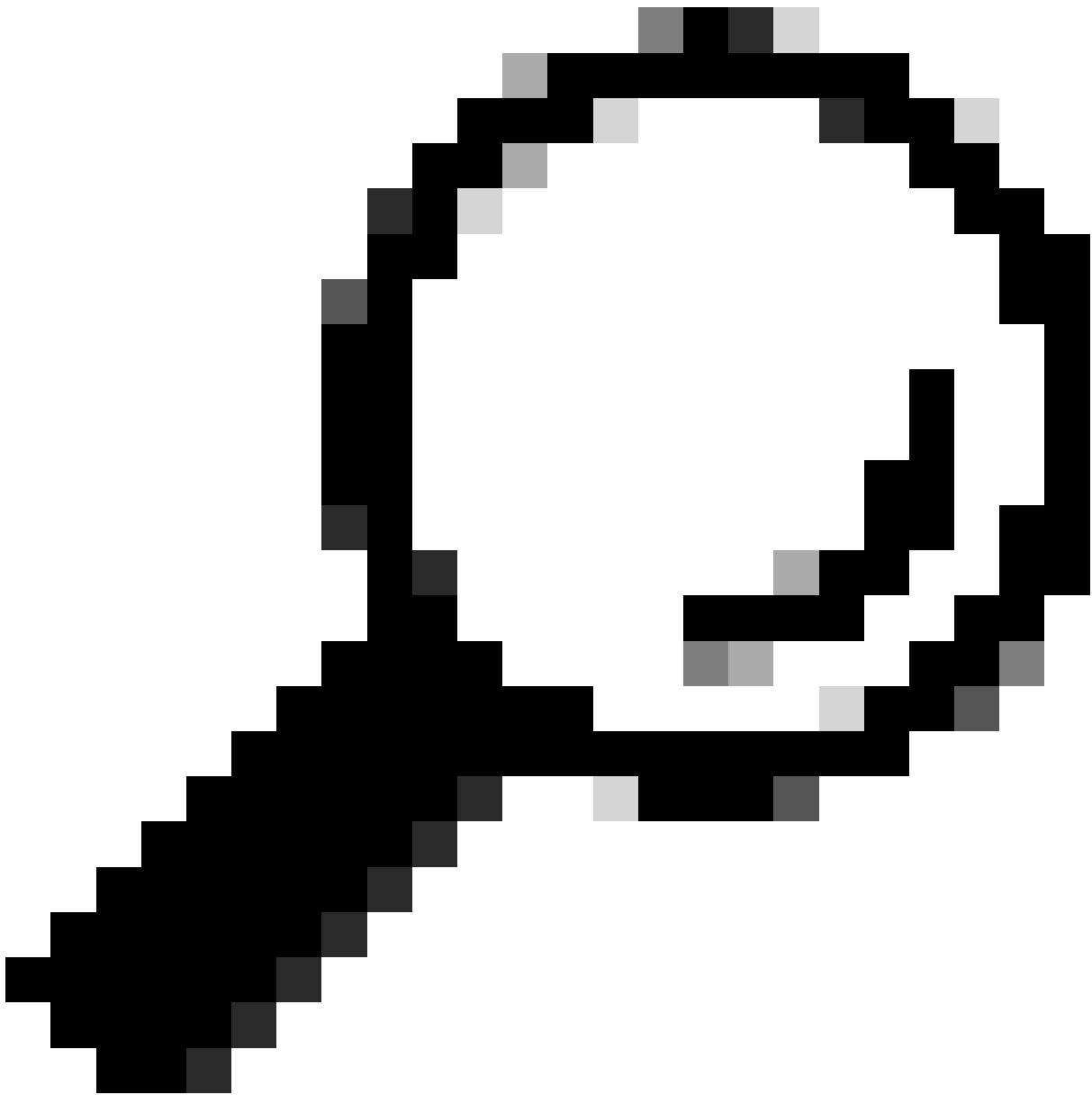


Immagine - Chiave pubblica SWA



Nota: copiare l'intera riga iniziando con ssh-rsa e terminando con
root@<your_SWA_hostname>



Consiglio: poiché RSA è installato sul server SCP, non è necessario incollare la chiave ssh-dss

Passaggio 29. Abilitare "Agente di autenticazione OpenSSH" in PowerShell con privilegi di amministratore (Esegui come amministratore).

```
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> █
```

Immagine - Abilitazione dell'agente di autenticazione SSH Open

Passaggio 30.(Facoltativo) Aggiungere questa riga a %programdata%\ssh\sshd_config per consentire i tipi di chiave:

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

Passaggio 31. Riavviare il servizio SSH. È possibile utilizzare questo comando da PowerShell con privilegi di amministratore (Esegui come amministratore)

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

Passaggio 32. Per verificare se il push SCP è configurato correttamente, eseguire il rollover dei log configurati, è possibile farlo dalla GUI o dalla CLI (comando rollover now):

```
WSA_CLI> rollovernow scp1
```



Nota: in questo esempio il nome del log è "scpal".

È possibile confermare che i log vengano copiati nella cartella definita, che in questo esempio era `c:/Users/wsascp/wsa01`

Push dei registri SCP su un'unità diversa

nel caso sia necessario eseguire il push dei registri in un'unità diversa da C:, creare un collegamento dalla cartella profilo utente all'unità desiderata. In questo esempio, i log vengono spostati su `D:\WSA_Logs\WSA01` .

Passaggio 1. creare le cartelle nell'unità desiderata, in questo esempio

Passaggio 2. Apri prompt dei comandi con privilegi di amministratore (Esegui come amministratore)

Passaggio 3. Eseguire questo comando per creare il collegamento:

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

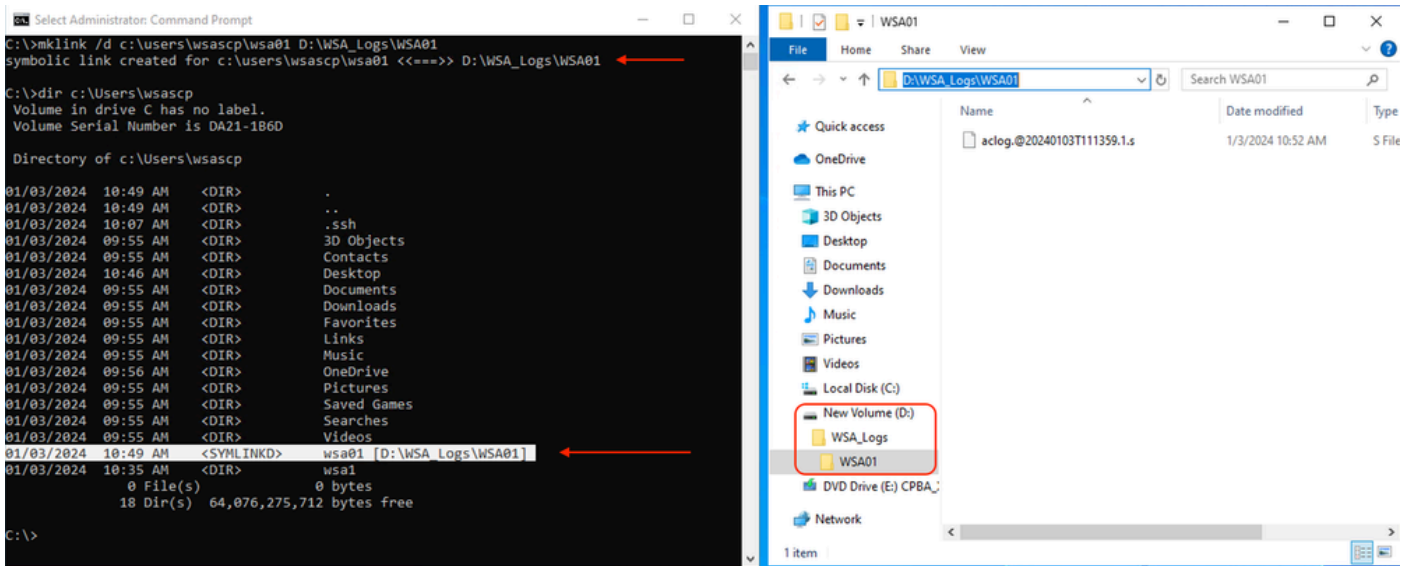


Immagine - Crea collegamento SYM



Nota: in questo esempio SWA è configurato per eseguire il push dei log nella cartella WSA01 in C:\Users\wsascp e il server SCP ha la cartella WSA01 come collegamento simbolico a D:\WSA_Logs\WSA01

Per ulteriori informazioni su Microsoft Symbol Link, visitare: [mmlink | Microsoft Learn](#)

Risoluzione dei problemi di push del log SCP

Visualizza log in SWA

Per risolvere il problema relativo al push del log SCP, controllare gli errori in:

1. CLI > visualizza avvisi
2. Registri_sistema



Nota: per leggere `system_logs`, è possibile usare il comando `grep` nella CLI, scegliere il numero associato a `system_logs` e rispondere alla domanda nella procedura guidata.

Visualizza log nel server SCP

È possibile leggere i registri del server SCP nel Visualizzatore eventi di Microsoft, in Registri applicazioni e servizi > OpenSSH > Operativo

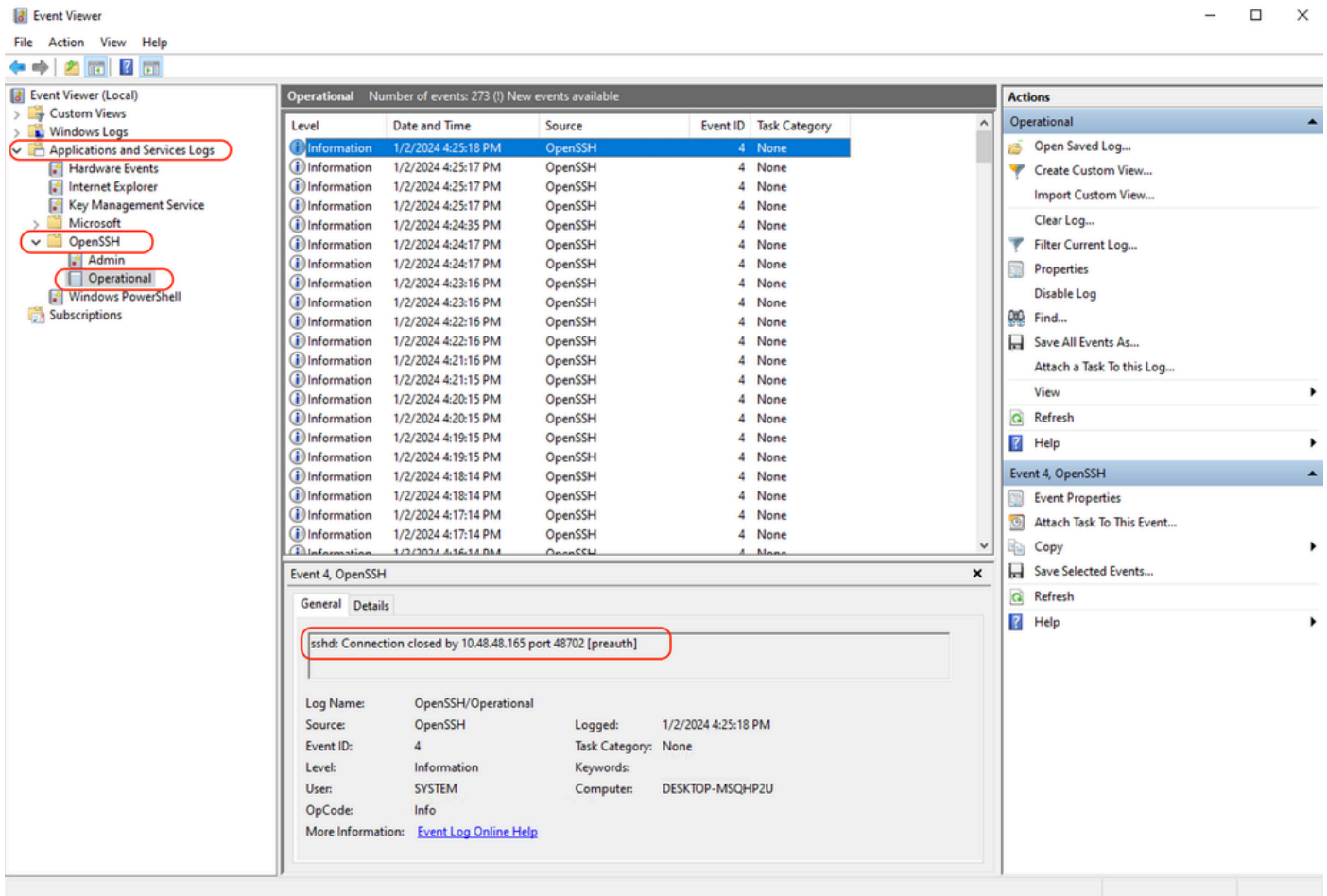


Immagine - PreAuth non riuscita

Verifica della chiave host non riuscita

Questo errore indica che la chiave pubblica del server SCP archiviata in SWA non è valida.

Di seguito è riportato un esempio di errore dall'output di displayalert nella CLI:

```
02 Jan 2024 16:52:35 +0100 Log Error: Push error for subscription scpal: 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 scpal: 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 scpal: SCP failed to transfer to 10.48.48.195:22: lost connection to host. 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 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.
```

Di seguito sono riportati alcuni esempi di errori nei log_di_sistema:

```
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: Host key verification failed.
```


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

Per risolvere il problema, è possibile copiare l'host dal server SCP e incollarlo nella pagina di sottoscrizione dei log SCP.

Fare riferimento al passaggio 7 di Configurazione SWA per inviare i log al server remoto SCP dalla GUI o è possibile contattare Cisco TAC per rimuovere la chiave host dal back-end.

Autorizzazione negata (chiave pubblica, password, tastiera-interattiva)

Questo errore in genere indica che il nome utente fornito nell'SWA non è valido.

Di seguito è riportato un esempio di log degli errori in system_logs:

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

Di seguito è riportato un esempio di errore restituito dal server SCP: SCP utente non valido dalla <indirizzo_SWA> porta <porta TCP SWA connette al server SCP>

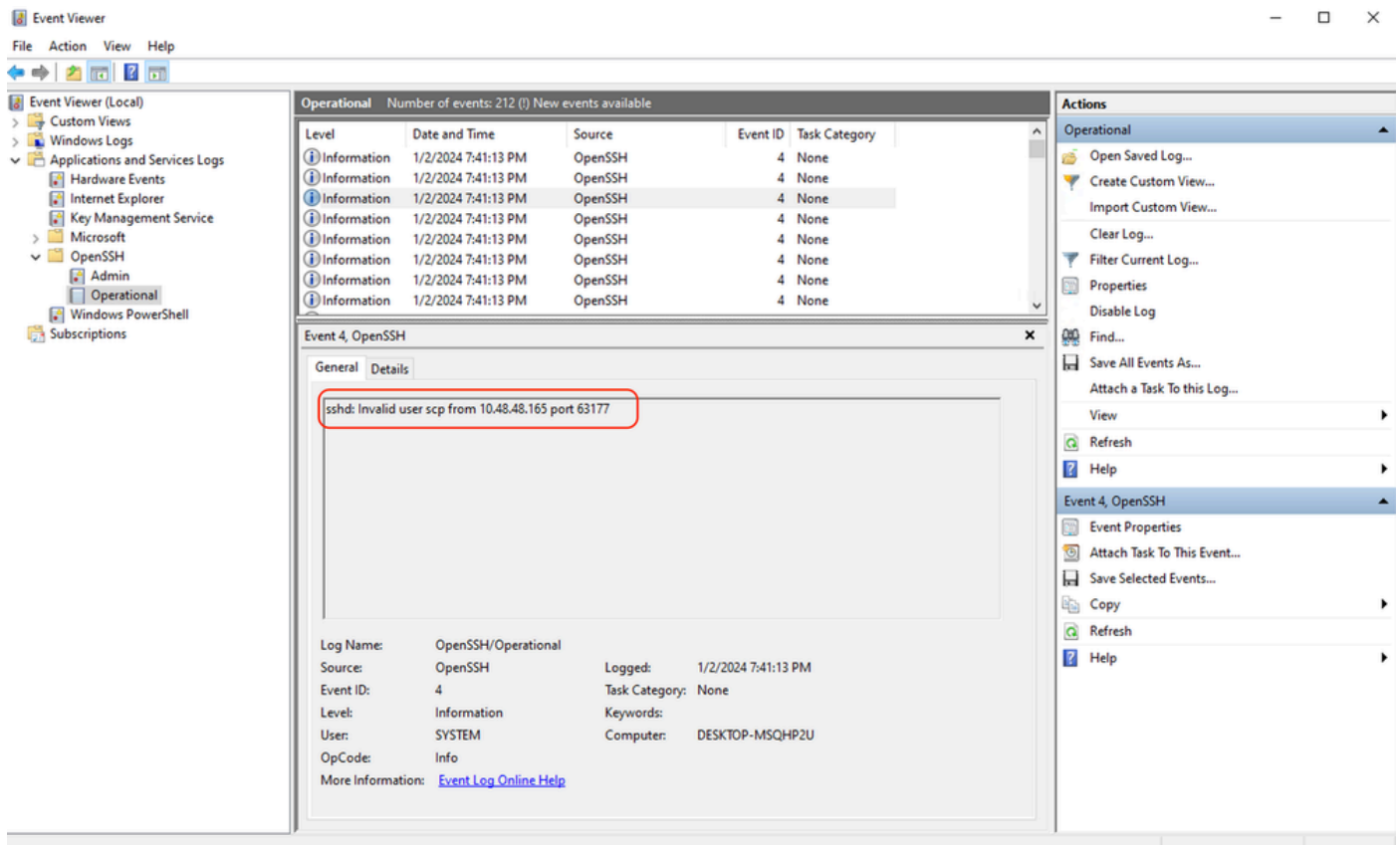


Immagine - Utente non valido

Per risolvere questo errore, controllare l'ortografia e verificare che l'utente (configurato in SWA per il push dei log) sia abilitato nel server SCP.

File o directory non esistente

Questo errore indica che il percorso specificato nella sezione di sottoscrizione dei log SWA non è valido,

Di seguito è riportato un esempio di errore da system_logs:

```
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer
Tue Jan  2 20:47:18 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer
```

Per risolvere il problema, verificare l'ortografia e assicurarsi che il percorso sia corretto e valido nel server SCP.

Impossibile trasferire SCP

questo errore potrebbe indicare un errore di comunicazione. Di seguito è riportato un esempio di errore:

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

Per risolvere i problemi di connettività, usare il comando telnet nella CLI SWA:

```
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 questo esempio la connessione non viene stabilita. L'output della connessione è simile al seguente:

```
SWA_CLI> telnet
```

Please select which interface you want to telnet from.

1. Auto
2. Management (10.48.48.187/24: rishi2Man.ca1o.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

Se la rete telnet non è collegata:

[1] Verificare se il firewall del server SCP blocca l'accesso.

[2] Verificare se nel percorso dal server SWA al server SCP sono presenti firewall che bloccano l'accesso.

[3] Verificare se la porta TCP 22 è in stato di ascolto nel server SCP.

[4] Eseguire l'acquisizione dei pacchetti in entrambi i server SWA e SCP per ulteriori analisi.

Di seguito è riportato un esempio di Packet Capture per la connessione riuscita:

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=1385225444 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 13:42:47.713901	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 13:42:47.732844	10.48.48.195	10.48.48.187	SSHv2	386	0	Server:
23	2024-01-03 13:42:47.732860	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:

Immagine - Acquisizione del pacchetto di connessione riuscita

Riferimenti

[Linee guida sulle best practice di Cisco Web Security Appliance - Cisco](#)

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

[Guida per l'utente di AsyncOS 14.5 for Cisco Secure Web Appliance - GD \(General Deployment\) - Connessione, installazione e configurazione \[Cisco Secure Web Appliance\] - Cisco](#)

[Introduzione a OpenSSH per Windows | Microsoft Learn](#)

[Configurazione dell'autenticazione con chiave pubblica SSH su Windows | Hub del sistema operativo Windows \(woshub.com\)](#)

[Autenticazione basata su chiavi in OpenSSH per Windows | Microsoft Learn](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).