

SCP Push Logs in Secure Web Applicatie configureren met Microsoft Server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[SCP](#)

[SWA Log-abonnement](#)

[Logbestanden archiveren](#)

[Log ophalen configureren via SCP op externe server](#)

[SWA configureren om de logbestanden via GUI naar SCP Remote Server te verzenden](#)

[Microsoft Windows configureren als SCP Remote Server](#)

[SCP-logbestanden naar DifferentDrive drukken](#)

[Probleemoplossing voor SCP log Push](#)

[Logbestanden in SWA bekijken](#)

[Logs in SCP-server bekijken](#)

[Verificatie hostsleutel mislukt](#)

[Toestemming geweigerd \(public key, wachtwoord, toetsenbord-interactief\)](#)

[SCP niet overgezet](#)

[Referenties](#)

Inleiding

Dit document beschrijft de stappen om Secure Copy (SCP) te configureren om logs in Secure Web Applicatie (SWA) automatisch te kopiëren naar een andere server.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe SCP werkt.
- Toediening van SWA.
- Beheer van Microsoft Windows of Linux.

Cisco raadt u aan het volgende te doen:

- Fysieke of virtuele SWA geïnstalleerd.

- Licentie geactiveerd of geïnstalleerd.
- De setup-wizard is voltooid.
- Administratieve toegang tot de grafische gebruikersinterface van de SWA (GUI).
- Microsoft Windows (ten minste Windows Server 2019 of Windows 10 (build 1809).) of Linux-systeem geïnstalleerd.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

SCP

Het gedrag van Secure Copy (SCP) is vergelijkbaar met dat van Remote Copy (RCP), dat afkomstig is uit de Berkeley r-tools-reeks (eigen reeks netwerktoepassingen van de universiteit van Berkeley), behalve dat SCP voor beveiliging op Secure Shell (SSH) vertrouwt. Daarnaast vereist SCP dat verificatie-, autorisatie- en accounting (AAA)-autorisatie wordt geconfigureerd, zodat het apparaat kan bepalen of de gebruiker het juiste prioriteitsniveau heeft

De methode SCP op Remote Server (gelijk aan SCP Push) duwt periodiek logbestanden door het protocol voor een beveiligde kopie naar een externe SCP-server. Voor deze methode is een SSH SCP-server op een externe computer met een SSH2-protocol vereist. Het abonnement vereist een gebruikersnaam, SSH-sleutel en doelmap op de externe computer. Logbestanden worden overgedragen op basis van een rollover-schema dat door u is ingesteld.

SWA Log-abonnement

U kunt meerdere logabbonementen maken voor elk type logbestand. Abbonementen bevatten configuratiegegevens voor archivering en opslag, waaronder deze:

- Instellingen voor rollover, die bepalen wanneer logbestanden worden gearcheveerd.
- Compressie-instellingen voor gearcheveerde logbestanden.
- Ophaalinstellingen voor gearcheveerde logbestanden, waarbij wordt aangegeven of logbestanden worden gearcheveerd op een externe server of op het apparaat worden opgeslagen.

Logbestanden archiveren

AsyncOS archiveert (rolls over) logabbonementen wanneer een huidig logbestand een door de gebruiker opgegeven limiet van maximale bestandsgrootte of maximale tijd sinds de laatste rollover bereikt.

Deze archiefinstellingen zijn opgenomen in logabonnementen:

- Bewaren op bestandsgrootte
- Beweeg de muis over tijd
- Logcompressie
- Retrieval-methode

U kunt logbestanden ook handmatig archiveren (rollover).

Stap 1. Kies Systeembeheer > Logabonnementen.

Stap 2. Schakel het selectievakje in in de kolom Rollover van de logabonnementen in om te archiveren of controleer het selectievakje All om alle abonnementen te selecteren.

Stap 3. Klik op Rollover Now om de geselecteerde logs te archiveren.

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](#)

Log ophalen via SCP op externe server configureren

Er zijn twee belangrijke stappen om logopvraging te hebben naar een externe server met SCP van SWA:

1. Configureer SWA om de logbestanden te drukken.
2. Configureer de externe server om de logbestanden te ontvangen.

SWA configureren om de logbestanden via GUI naar SCP Remote Server te verzenden

Stap 1. Meld u aan bij SWA en kies Logabonnementen uit Systeembeheer.

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

System Time

Time Zone

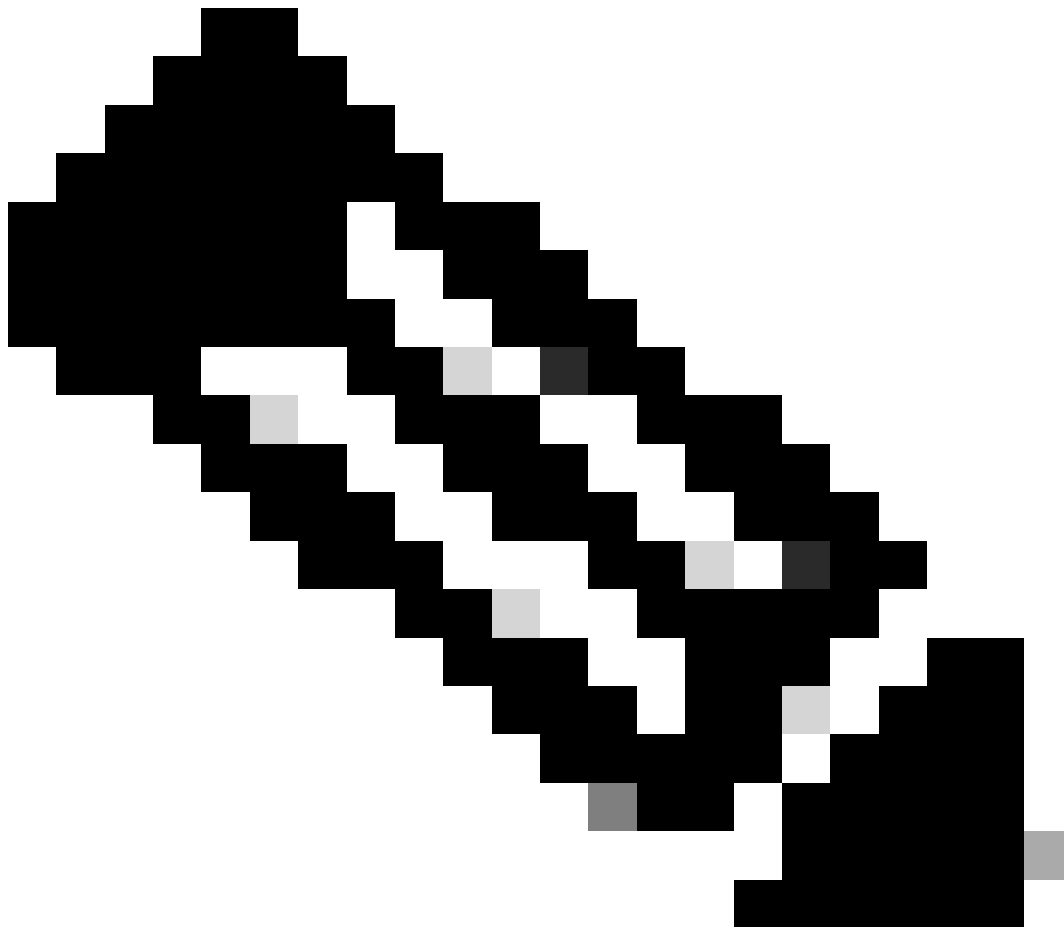
Time Settings

Configuration

Configuration Summary

Configuration File

Sla de SSH-toets in een tekstbestand op voor verder gebruik in het vak Configuratie externe SCP-server.



Opmerking: u moet beide regels kopiëren, beginnend met ssh- en eindigend met root@<SWA hostname> .

Log Subscriptions

Success — Log Subscription "SCP_Access_Logs" was added.

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

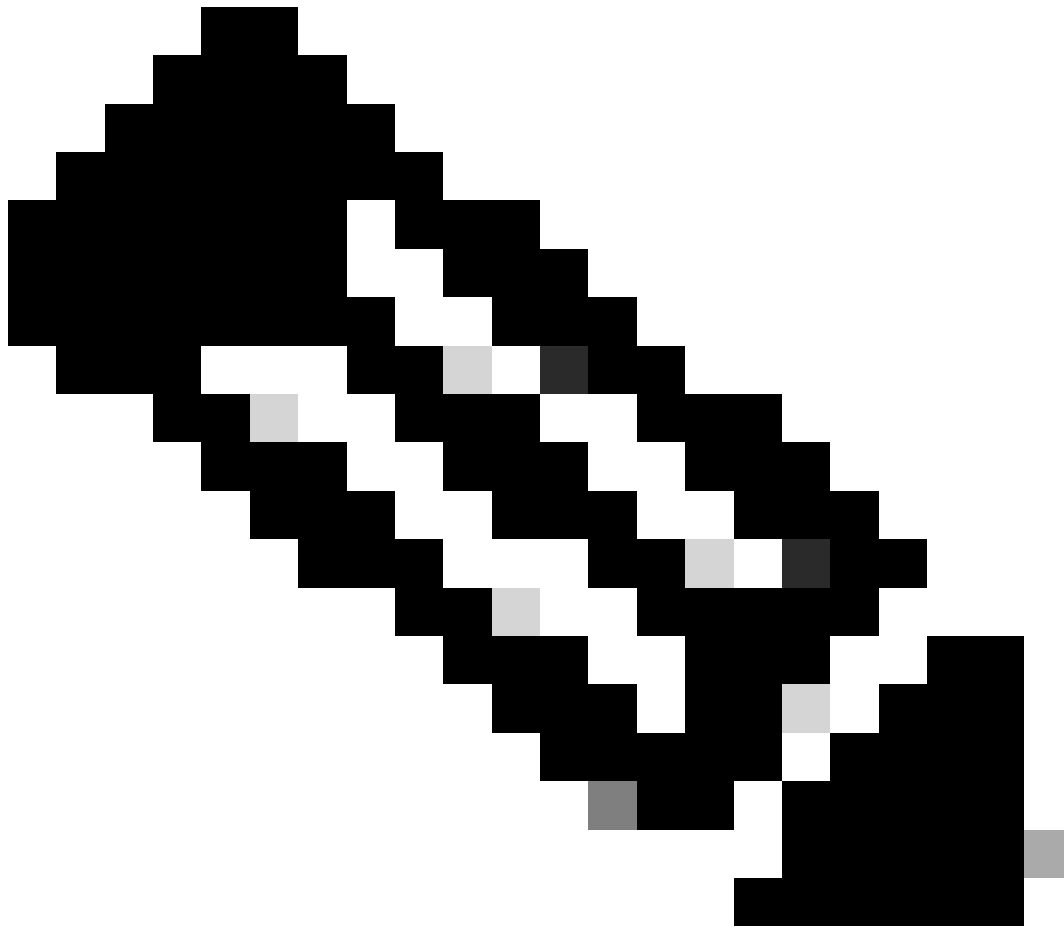
```
ssh-dss  
AAAAB3NzaC1kc3MAAACBAOuNX6TUOmzIWolPkVQ5I7LC/9yv:  
root@122[REDACTED]le.com  
  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACwbJziB4AE7H
```

Afbeelding - Sla de SSH-toets op voor verder gebruik.

Stap 10. Wijzigingen doorvoeren.

Microsoft Windows configureren als SCP Remote Server

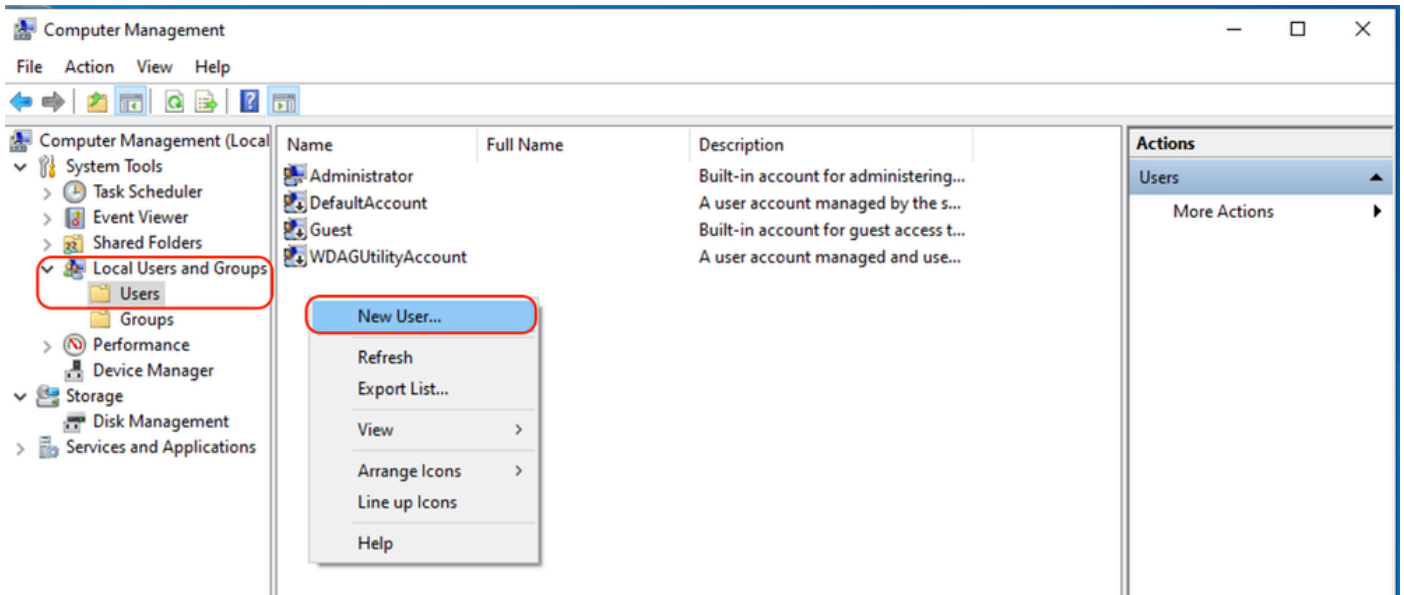
Stap 10. Om een gebruiker voor uw SCP-service te maken, navigeer naar Computer Management:



Opmerking: als u al een gebruiker voor SCP hebt, gaat u naar Stap 16.

Stap 11. Selecteer Lokale gebruikers en groep en kies Gebruikers in het linker deelvenster.

Stap 12. Klik met de rechtermuisknop op de hoofdpagina en kies een nieuwe gebruiker.



Afbeelding - Een gebruiker voor SCP-service maken.

Stap 13. Voer de gebruikersnaam en het gewenste wachtwoord in.

Stap 14. Kies een wachtwoord dat nooit is verlopen.

Stap 15. Klik op Aanmaken en sluit het venster.

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

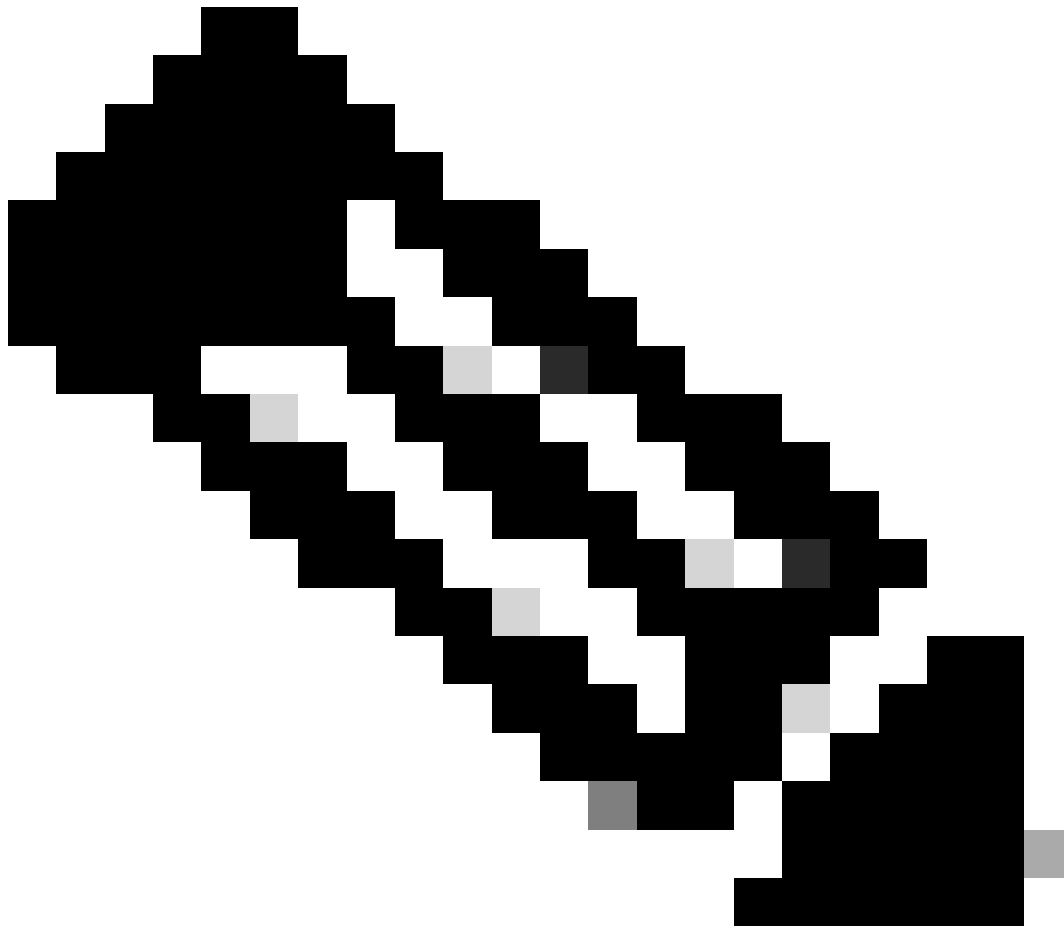
Password never expires

Account is disabled

Help Create Close

Afbeelding - Voer nieuwe gebruikersinformatie in.

Stap 16. Log in op de Remote SCP-server met de nieuwe gebruiker om de profielmap te maken.



Opmerking: als u OpenSSL op uw Remote SCP-server hebt geïnstalleerd, gaat u verder met stap 19.

Stap 17. Open PowerShell met beheerdersrechten (Als beheerder uitvoeren) en voer deze opdracht uit om de vereisten te controleren:

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

Als de uitvoer Waar is, kunt u verdergaan. Anders kunt u contact opnemen met het Microsoft-ondersteuningsteam.

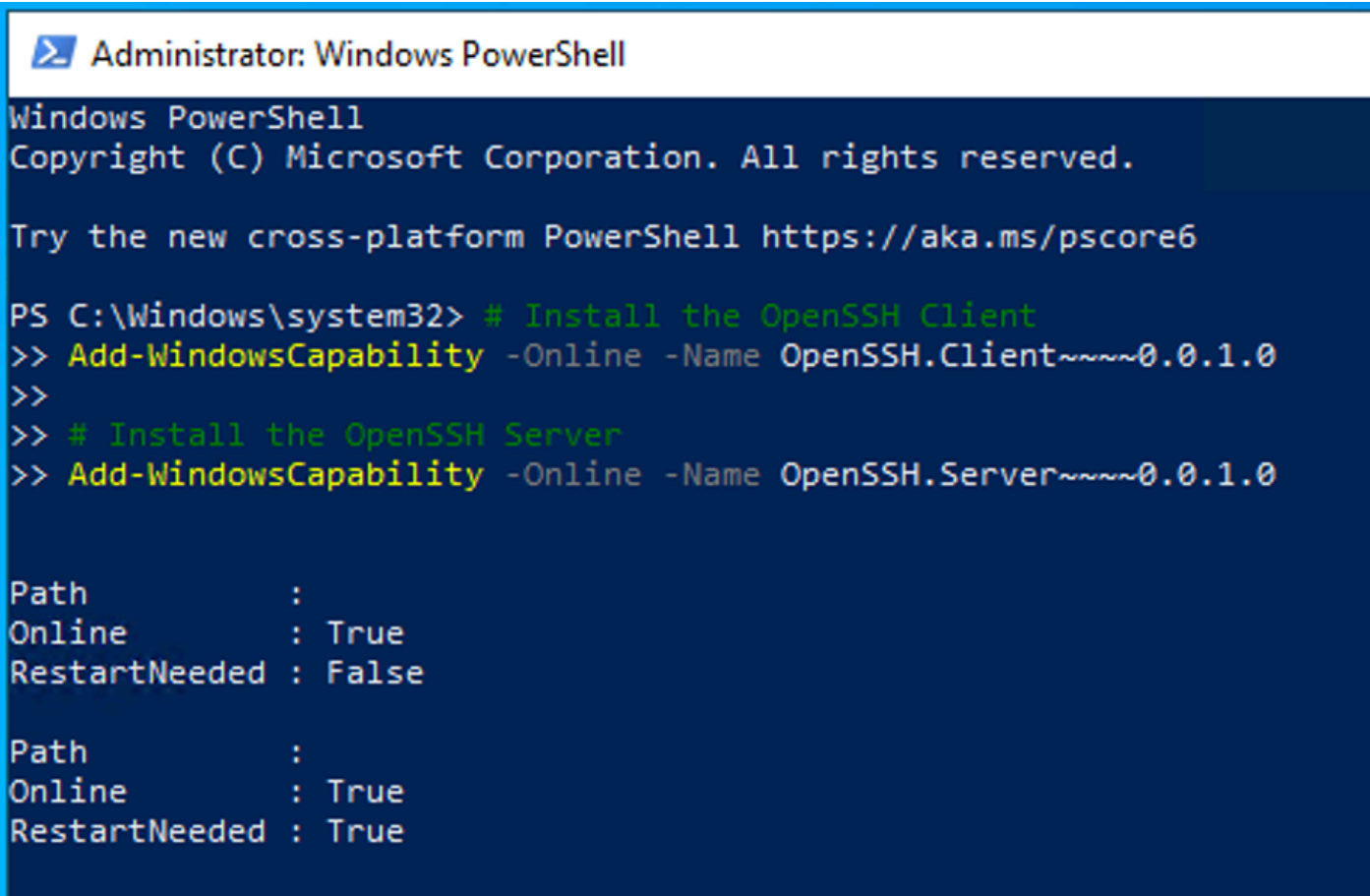
Stap 18. Als u OpenSSH wilt installeren met PowerShell met beheerdersrechten (uitgevoerd als beheerder), voert u het volgende uit:

```
# 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
```

Hier is een voorbeeld van succesvolle resultaten:

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



```
Administrator: Windows PowerShell

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

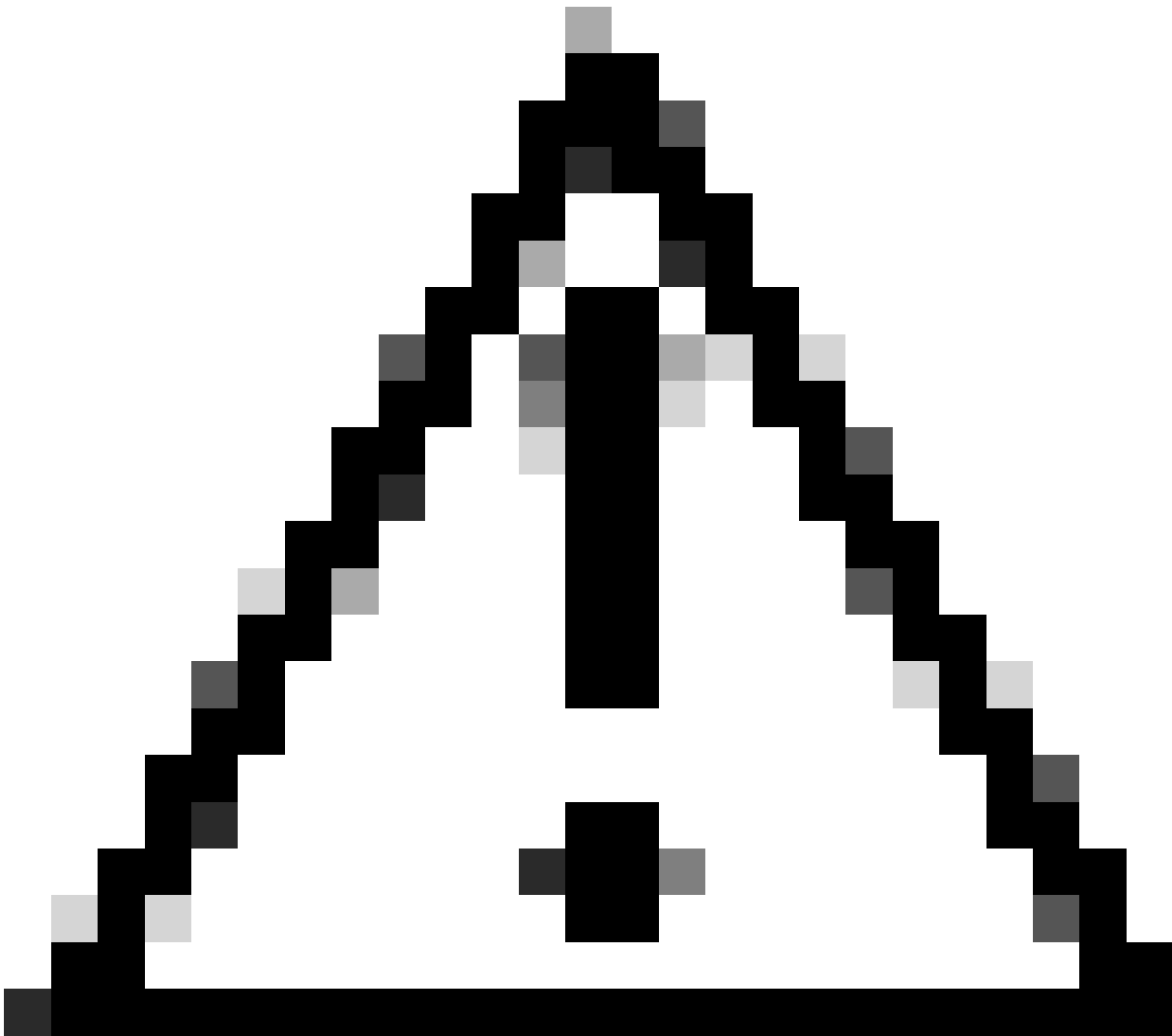
Try the new cross-platform PowerShell https://aka.ms/pscore6

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
```

Image - Installeer OpenSSH in PowerShell



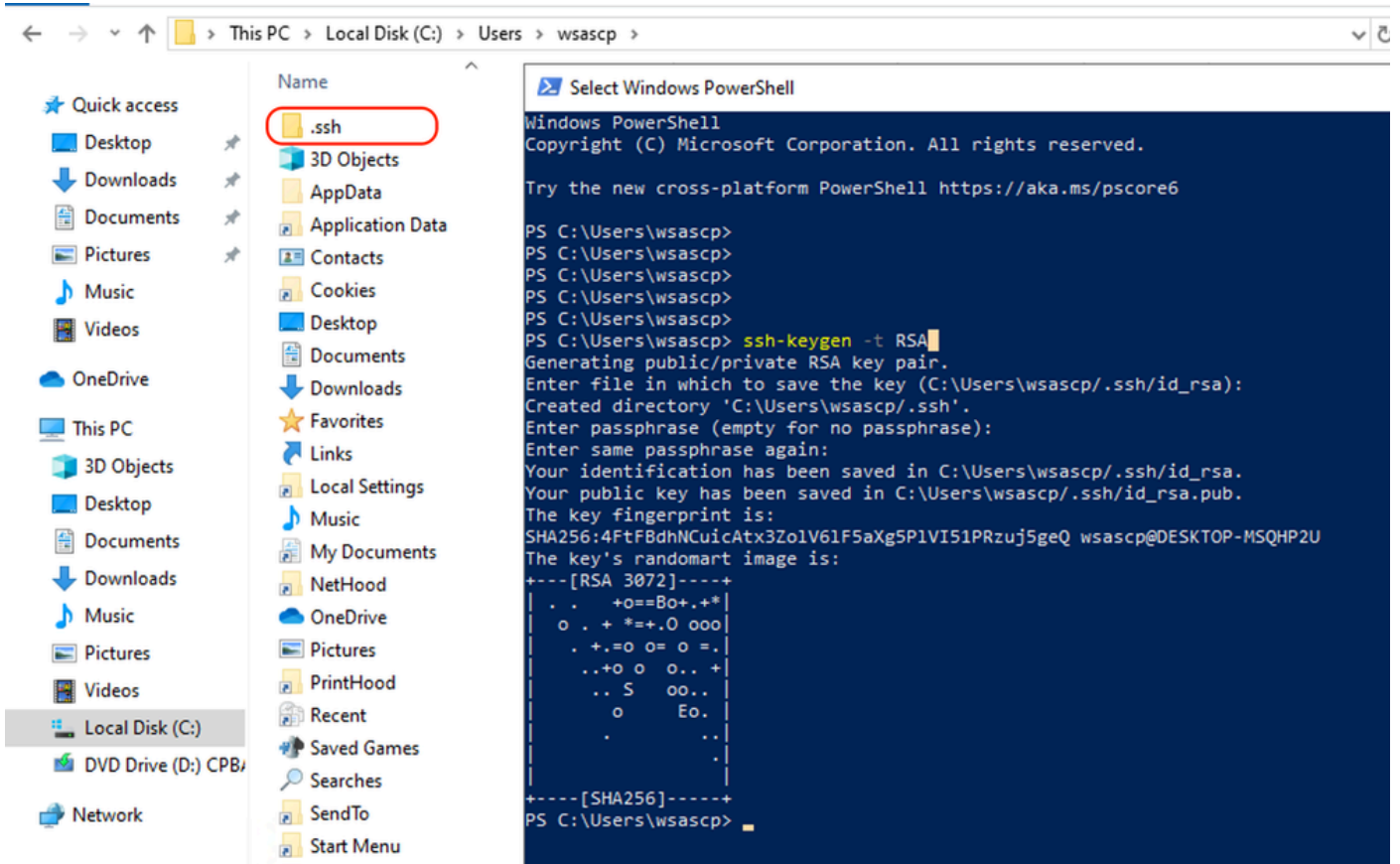
Waarschuwing: als HerstartNoodzakelijk is ingesteld op True, moet u Windows opnieuw opstarten.

Ga voor meer informatie over de installatie op andere versies van Microsoft Windows naar deze link: [Aan de slag met OpenSSH voor Windows | Microsoft Learn](#)

Stap 19. Open een normale (niet-verhoogde) PowerShell-sessie en genereer een paar RSA-toetsen met behulp van de opdracht:

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

Als de opdracht is voltooid, kunt u zien dat de map .ssh uw gebruikersprofielmap heeft gemaakt.



Afbeelding - Generate RSA-toets

Stap 20. Start de SSH-service vanuit PowerShell met beheerdersrechten (als beheerder uitvoeren).

```
Start-Service sshd
```

Stap 21. (optioneel maar aanbevolen) Wijzig het opstarttype voor de service in Automatisch, met beheerdersrechten (Als beheerder uitvoeren).

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

Stap 22. Bevestig dat de firewallregel om toegang tot TCP-poort 22 te verlenen is gemaakt.

```
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."
}
```

Stap 23. Bewerk SSH-configuratiebestand in: %programdata%\ssh\sshd_config in blocnote en verwijder # voor de RSA en 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
```

Stap 24. Bewerk de verbindingsvoorwaarden in %programdata%\ssh\sshd_config. In dit voorbeeld, is het luisteradres voor al interfaceadres. Je kunt het aanpassen aan je ontwerp.

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

Stap 25. Merk deze twee lijnen aan het eind van het %programdata%\ssh\sshd_config- bestand door # aan het begin van elke regel toe te voegen:

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

Stap 26.(Optioneel) Bewerk de strikte modi in %programdata%\ssh\sshd_config, Deze modus is standaard ingeschakeld en voorkomt SSH-sleutelgebaseerde verificatie als privaat- en openbare sleutels niet goed zijn beveiligd.

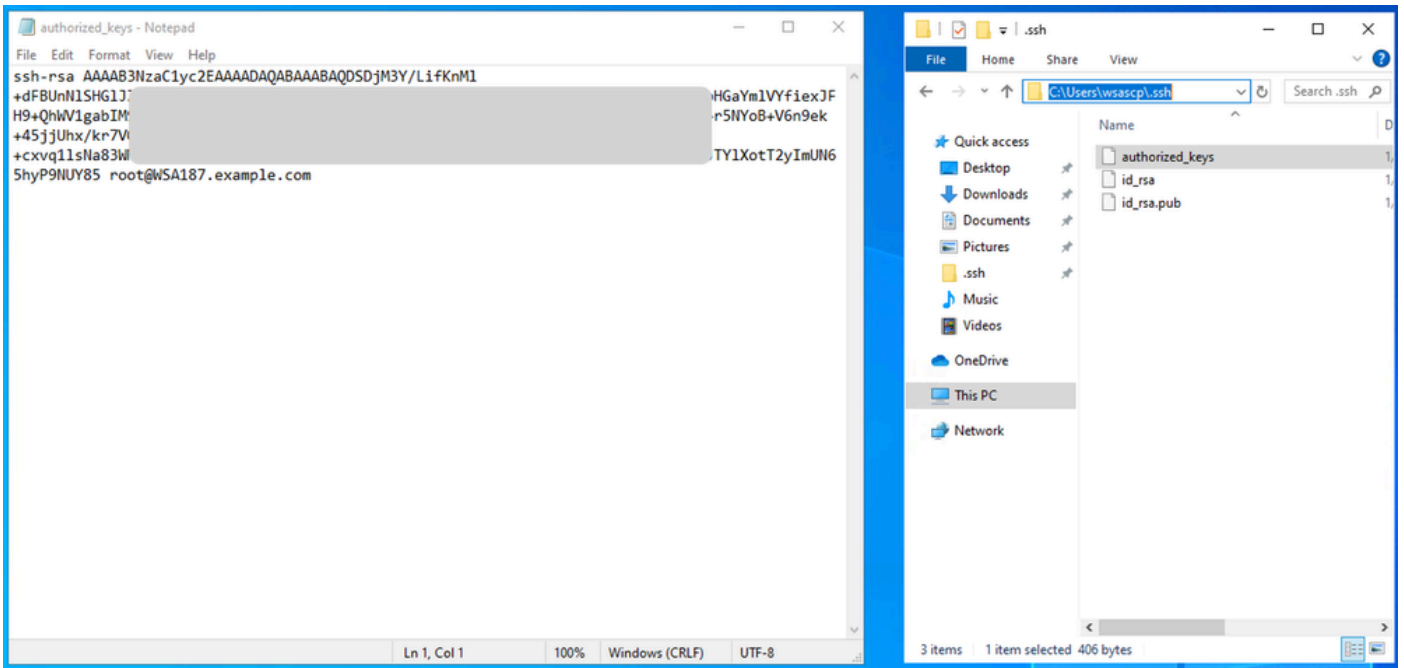
Schakel de regel #StrictModes ja in en wijzig deze naar StrictModes no:

```
StrictModes No
```

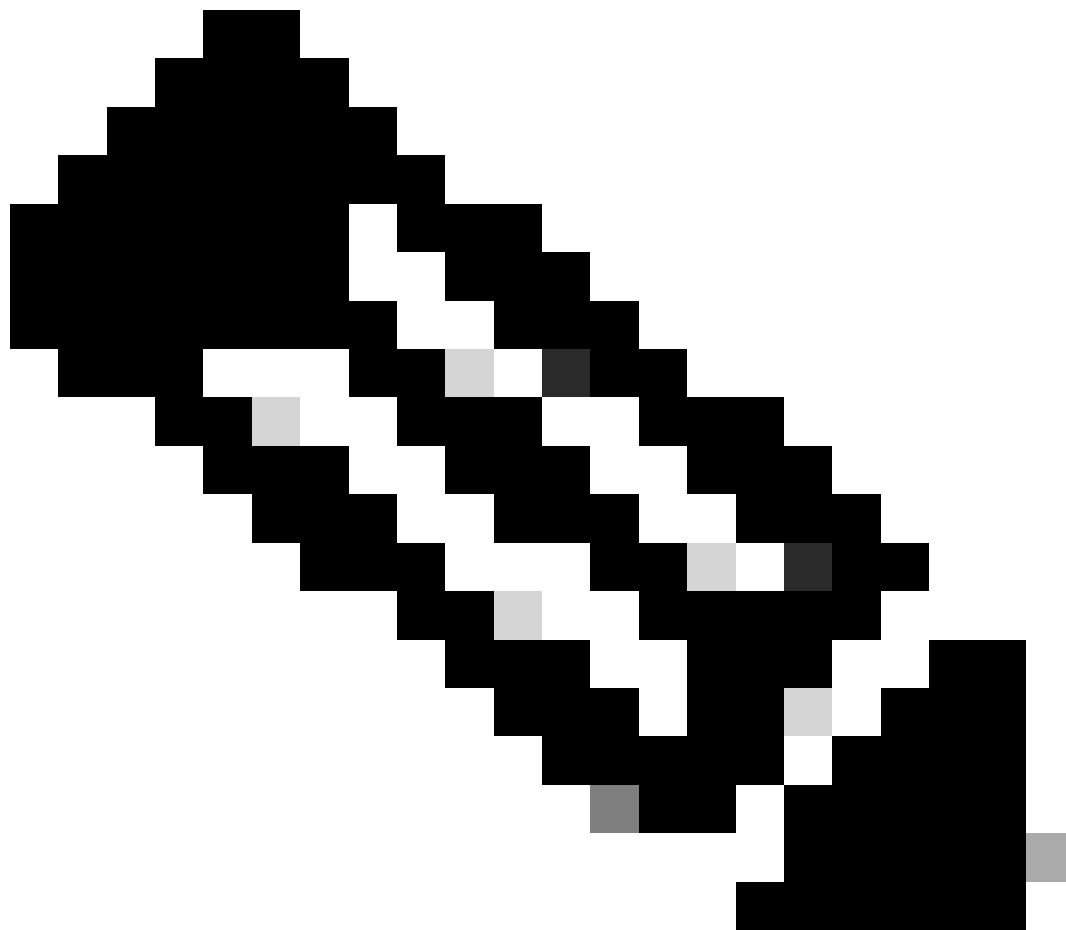
Stap 27. Verwijder de # van deze regel naar %programdata%\ssh\sshd_config om openbare toetsverificatie toe te staan

```
PubkeyAuthentication yes
```

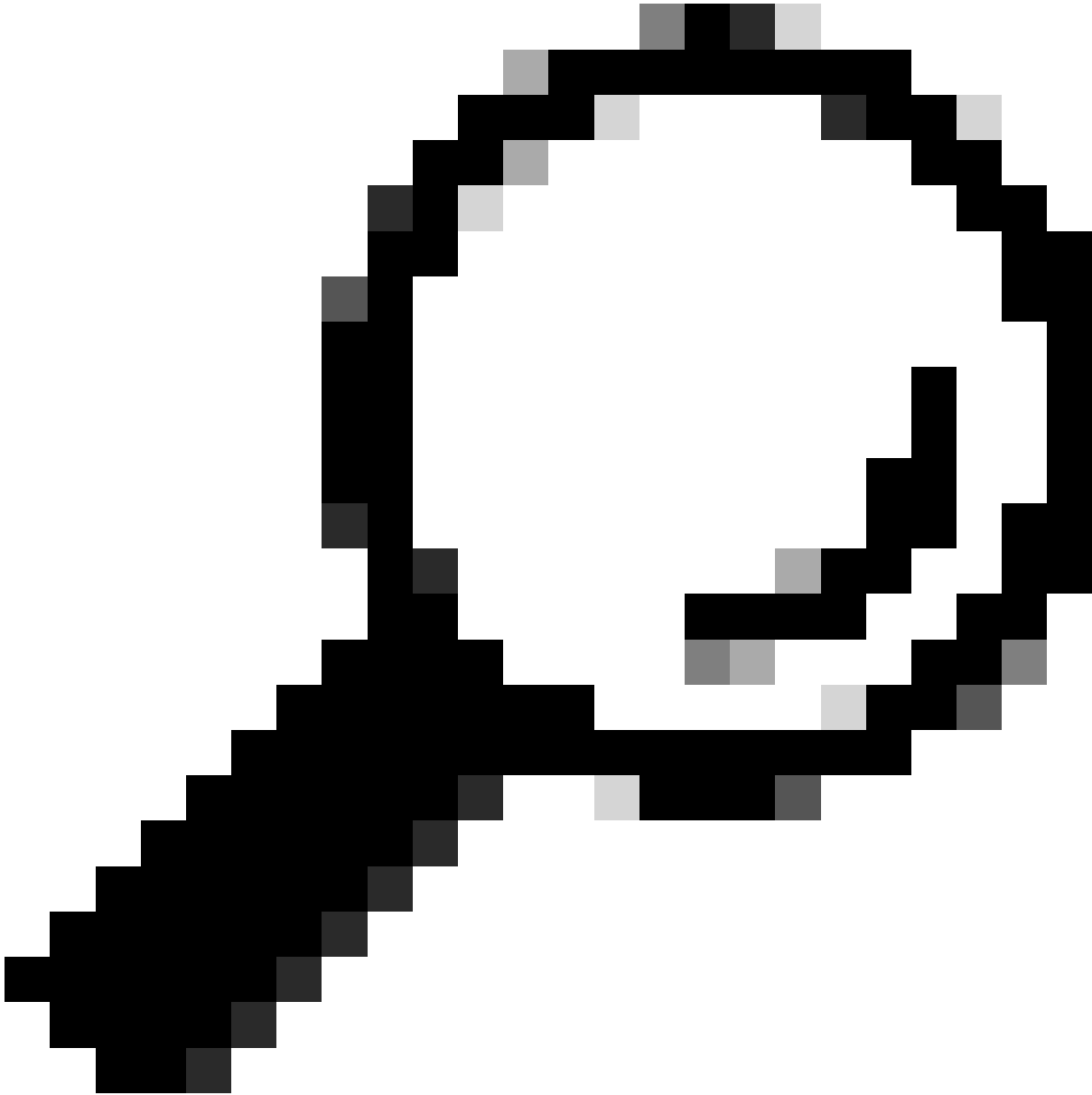
Stap 28. Maak een tekstbestand "authorised_keys" in .ssh-map en plak de SWA public RSA-toets (die is verzameld op stap 9)



Afbeelding - SWA Public Key



Opmerking: kopieer de hele regel die begint met ssh-rsa en eindigt met root@<your_SWA_hostname>



Tip: Aangezien RSA is geïnstalleerd op de SCP-server, hoeft de ssh-dss-toets niet te worden geplakt

Stap 29. Schakel "OpenSSH-verificatieagent" in PowerShell met beheerdersrechten in (als beheerder uitvoeren).

```
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> █
```

Afbeelding - Open SSH-verificatieagent inschakelen

Stap 30.(Optioneel) Voeg deze regel toe aan %programdata%\ssh\sshd_config om de volgende sleuteltypen toe te staan:

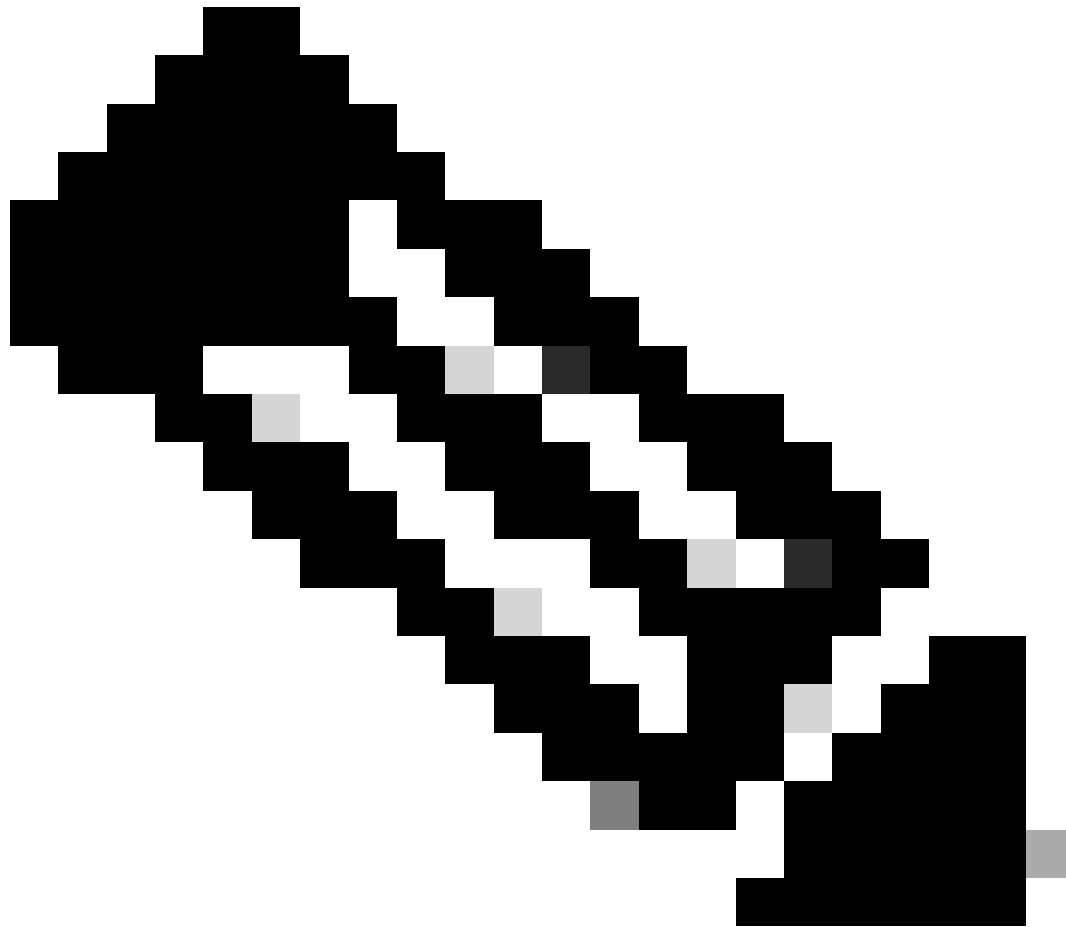
```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rs
```

Stap 31. Start de SSH-service opnieuw. U kunt deze opdracht gebruiken vanuit PowerShell met beheerdersrechten (Als beheerder uitvoeren)

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

Stap 32. Om te testen als de SCP-druk correct is geconfigureerd, kunt u de geconfigureerde logbestanden kantelen via zowel GUI als CLI (rollover now-opdracht):

```
WSA_CLI> rollovernow scpall
```



Opmerking: in dit voorbeeld is de lognaam "scpal".

U kunt bevestigen dat de logbestanden worden gekopieerd naar de gedefinieerde map, die in dit voorbeeld `c:/Gebruikers/wsascp/wsa01` was

SCP-logbestanden naar andere station drukken

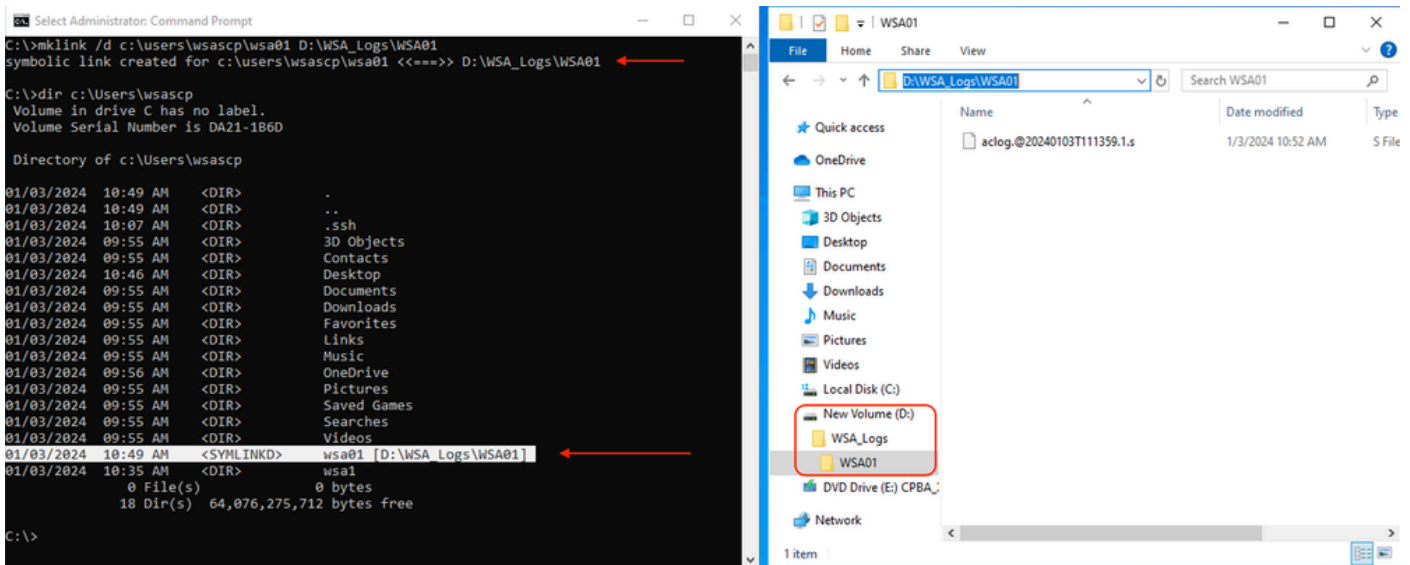
als u de logbestanden moet duwen naar een ander station dan C:, maakt u een koppeling van de map gebruikersprofielen naar het gewenste station. In dit voorbeeld worden de logs naar `D:\WSA_Logs\WSA01` gedrukt .

Stap 1. maak de mappen aan op het gewenste station, in dit voorbeeld

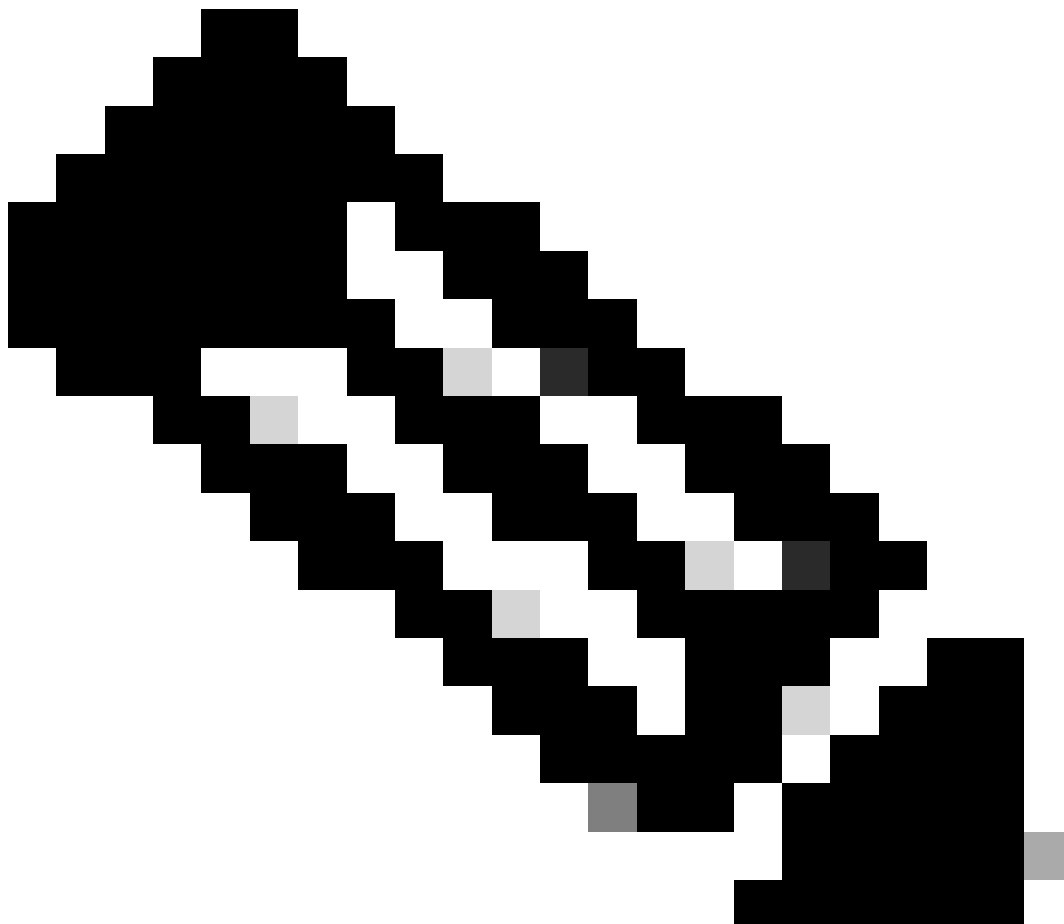
Stap 2. Opdrachtprompt met beheerdersrechten openen (als beheerder uitvoeren)

Stap 3. Voer deze opdracht uit om de koppeling te maken:

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



Afbeelding - Sym-link maken



Opmerking: in dit voorbeeld SWA is geconfigureerd om de logbestanden te duwen naar WSA01 map in C:\Users\wsascp , en de SCP-server heeft map WSA01 als symbolische link naar D:\WSA_Logs\WSA01

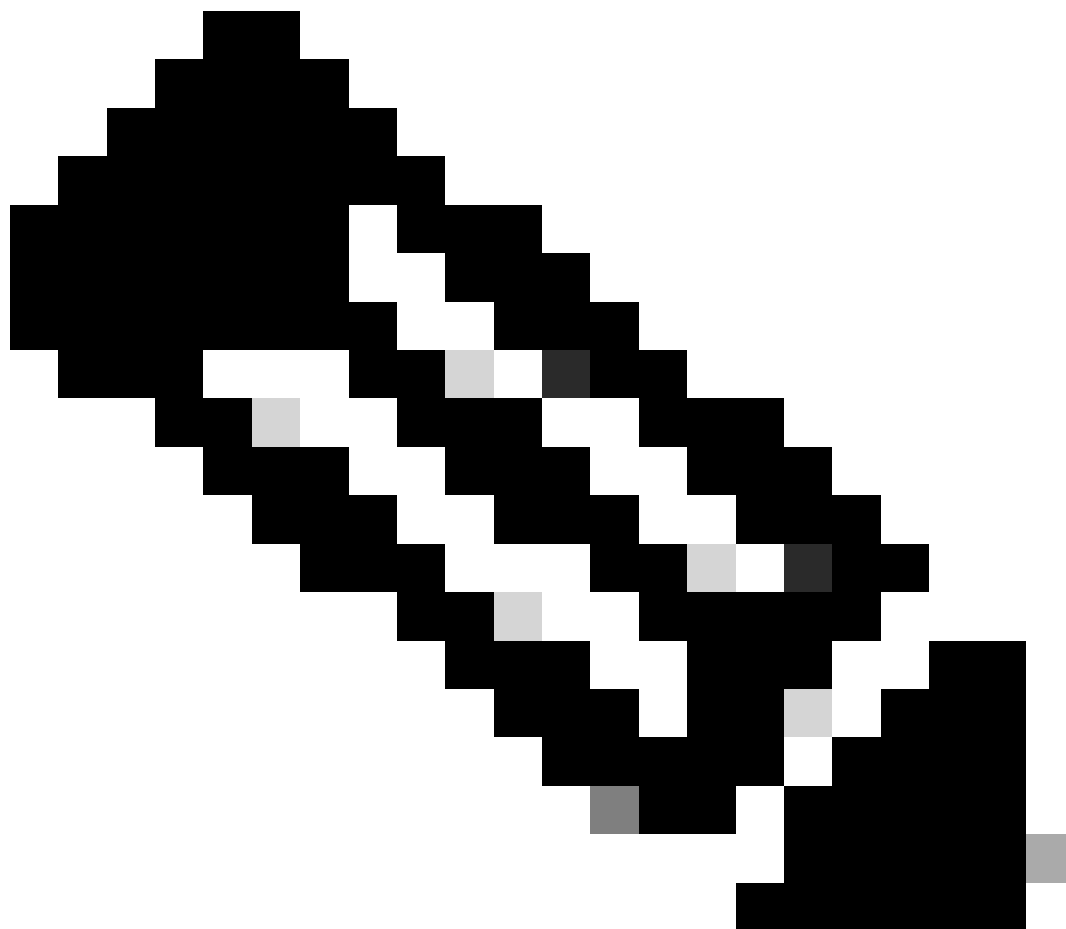
Voor meer informatie over Microsoft Symbol Link gaat u naar: [mklink | Microsoft Learn](#)

Probleemoplossing voor SCP log Push

Logbestanden in SWA bekijken

Om de SCP log push op te lossen, controleer de fouten in:

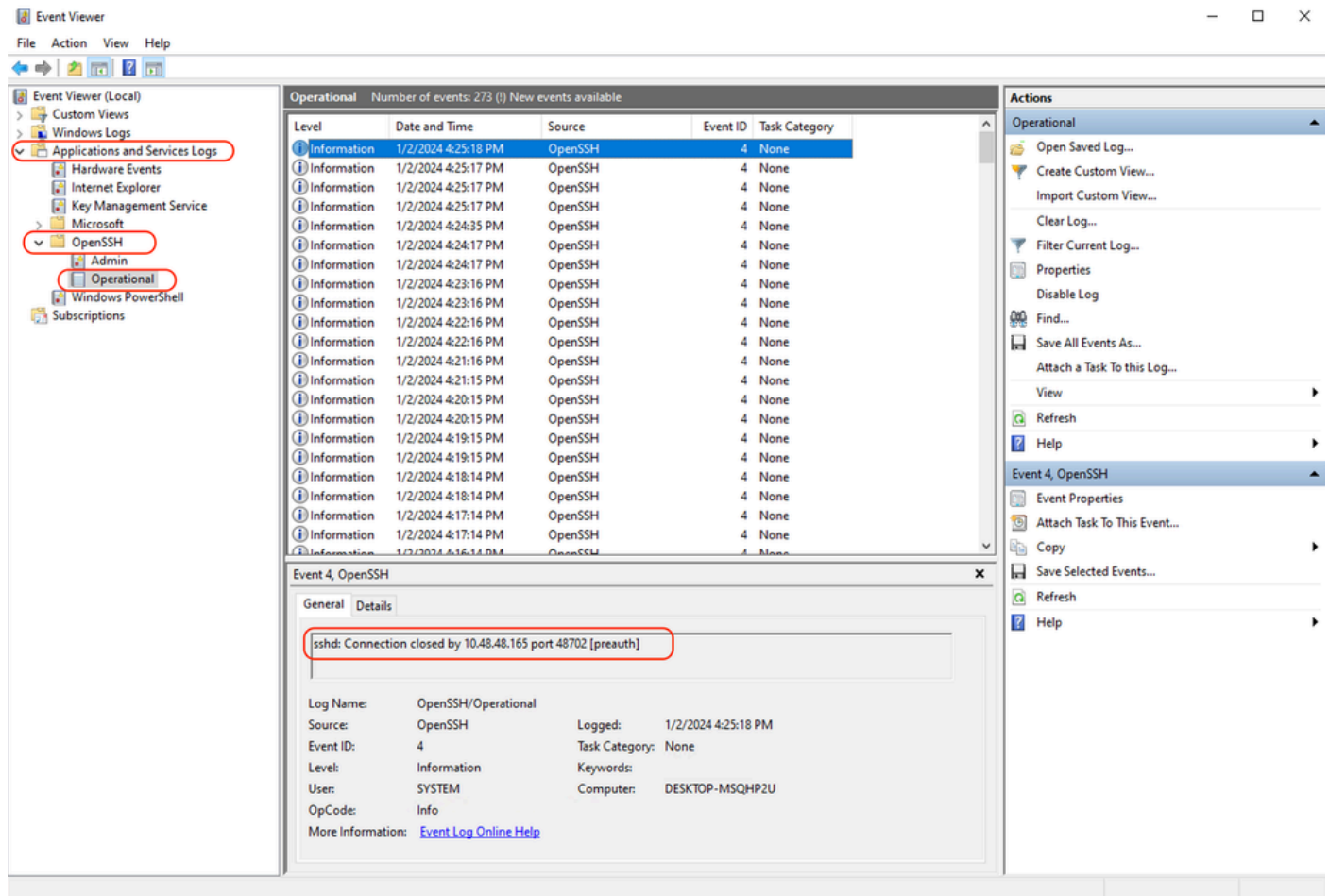
1. CLI > displays
 2. System_logs
-



Opmerking: Om system_logs te lezen, kunt u grep commando in CLI gebruiken, het nummer kiezen dat gekoppeld is aan system_logs en de vraag in de wizard beantwoorden.

Logs in SCP-server bekijken

U kunt de SCP server logt in Microsoft Event Viewer lezen, in applicaties en services logs > OpenSSH > Operationeel



Afbeelding - PreAuth is mislukt

Verificatie hostsleutel mislukt

Deze fout geeft aan dat de in SWA opgeslagen openbare sleutel van de SCP-server ongeldig is.

Hier is een voorbeeld van een fout in de weergave van waarschuwingen in CLI:

```
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
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
Last message occurred 22 times between Tue Jan 2 15:53:01 2024 and Tue Jan 2 16:29:18 2024.

Hier zijn een paar voorbeelden van Fout in system_logs :

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

Om dit probleem op te lossen, kunt u de host kopiëren van SCP server en plakken in SCP logs abonnementspagina.

Zie stap 7 in Configureren SWA om de logbestanden te verzenden naar SCP Remote Server vanuit GUI of u kunt contact opnemen met Cisco TAC om de hostsleutel uit een backend te verwijderen.

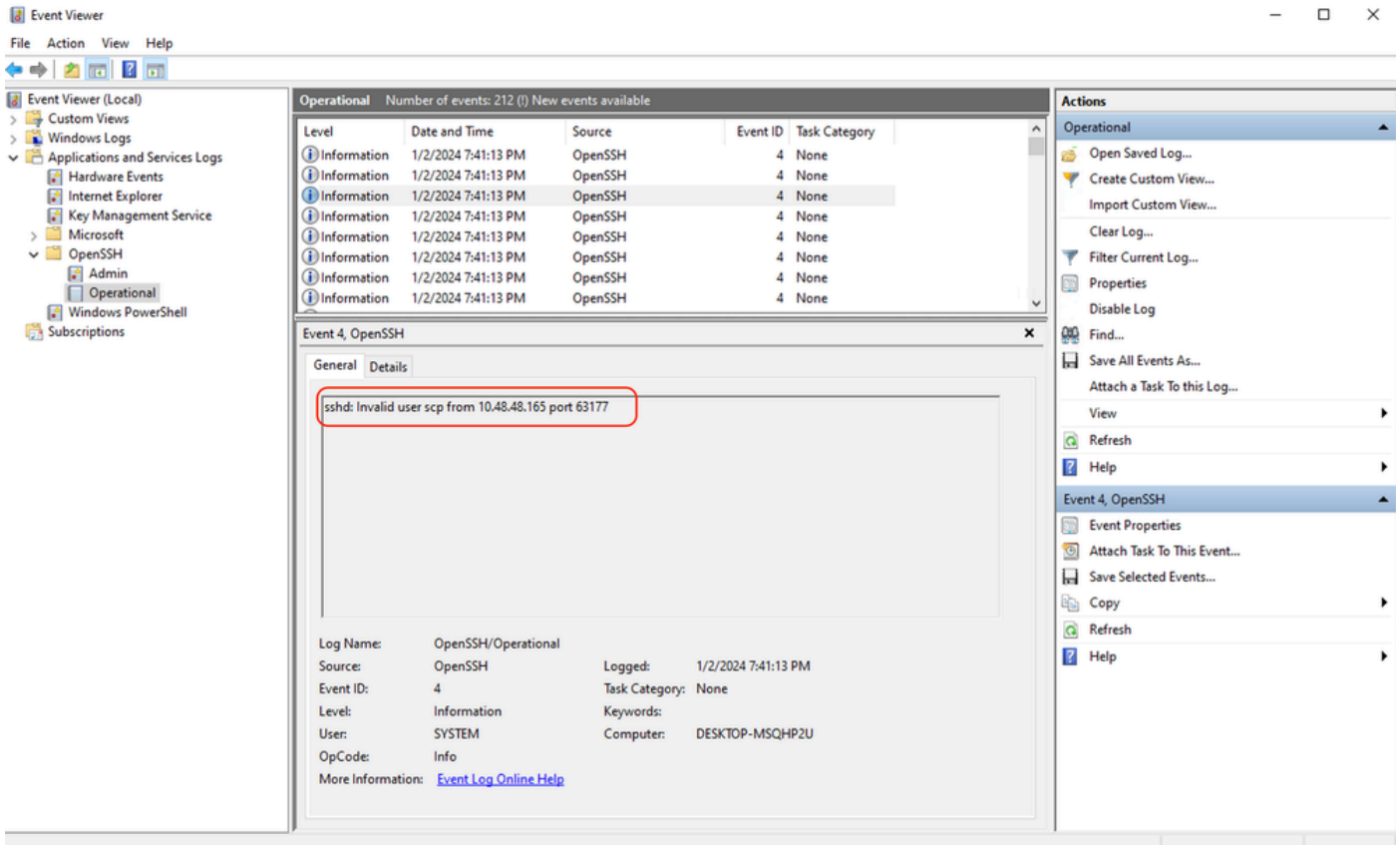
Toestemming geweigerd (public key, wachtwoord, toetsenbord-interactief)

Deze fout geeft meestal aan dat de gebruikersnaam in SWA ongeldig is.

Hier is een voorbeeld van error log in system_logs:

```
Tue Jan 2 20:41:40 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer  
Tue Jan 2 20:41:40 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer  
Tue Jan 2 20:41:40 2024 Critical: Log Error: Push error for subscription scp1: SCP failed to transfer
```

Hier is een voorbeeld van een fout van SCP server: Ongeldige gebruiker SCP van <SWA_IP address> poort <TCP-poort: SWA maakt verbinding met SCP server>



Afbeelding - Ongeldige gebruiker

Om deze fout op te lossen, controleer gelieve de spelling en te verifiëren dat de gebruiker (die in SWA wordt gevormd om de logboeken te duwen) in SCP server wordt toegelaten.

Geen dergelijk bestand of map

Deze fout geeft aan dat het pad dat in de sectie SWA logs abonnement wordt geboden, niet geldig is.

Hier is een voorbeeld van een fout uit 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
```

Om dit probleem op te lossen, verifieert u de spelling en controleert u of het pad correct en geldig is in de SCP-server.

SCP niet overgezet

deze fout zou een indicator van een communicatiefout kunnen zijn. Hier is de steekproef van fout:

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


Om de connectiviteit problemen op te lossen, gebruik het Telnet bevel 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 dit voorbeeld is de verbinding niet tot stand gebracht. De succesvolle verbinding is als:

```
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
```

Als het telnet niet is aangesloten:

- [1] Controleer of de SCP-serverfirewall de toegang blokkeert.
- [2] Controleer of er firewalls zijn in het pad van SWA naar SCP server die de toegang blokkeren.
- [3] Controleer of TCP-poort 22 zich in een luisterstatus op SCP-server bevindt.
- [4] Start pakketopname in zowel SWA- als SCP-server voor verdere analyse.

Hier is een voorbeeld van pakketvastlegging van succesvolle verbinding:

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:

Afbeelding - Succesvolle Connection-pakketopname

Referenties

[Richtlijnen voor beste praktijken van Cisco Web Security Applicatie - Cisco](#)

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

[Gebruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Applicatie - GD \(Algemene implementatie\) - Verbinden, installeren en configureren \[Cisco Secure Web Applicatie\] - Cisco](#)

[Aan de slag met OpenSSH voor Windows | Microsoft Learn](#)

[SSH Public Key-verificatie configureren op Windows | Windows OS Hub \(woshub.com\)](#)

[Key-gebaseerde verificatie in OpenSSH voor Windows | Microsoft Learn](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.