Konfigurieren von SCP-Push-Protokollen in der sicheren Web-Appliance mit Microsoft Server

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren von Secure Copy (SCP) beschrieben, um Protokolle in Secure Web Appliance (SWA) automatisch auf einen anderen Server zu kopieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Funktionsweise von SCP
- SWA-Verwaltung.
- Administration des Betriebssystems Microsoft Windows oder Linux

Cisco empfiehlt Folgendes:

- Installierte physische oder virtuelle SWA.
- Lizenz aktiviert oder installiert.
- Der Setup-Assistent ist abgeschlossen.

- Administrator-Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Microsoft Windows (mindestens Windows Server 2019 oder Windows 10 (Build 1809)) oder Linux System installiert.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

SCP

Das Verhalten von Secure Copy (SCP) ähnelt dem von Remote Copy (RCP), das aus der Berkeley r-tools Suite (Berkeley University Own Set of Networking Applications) stammt, mit der Ausnahme, dass SCP aus Sicherheitsgründen auf Secure Shell (SSH) basiert. Darüber hinaus muss die AAA-Autorisierung (Authentication, Authorization, Accounting) gemäß SCP konfiguriert werden, damit das Gerät feststellen kann, ob der Benutzer über die richtige Privilegstufe verfügt.

Die SCP on Remote Server-Methode (entspricht SCP Push) überträgt regelmäßig Protokolldateien des Protokolls für sichere Kopien an einen entfernten SCP-Server. Für diese Methode ist ein SSH-SCP-Server auf einem Remotecomputer mit SSH2-Protokoll erforderlich. Das Abonnement erfordert einen Benutzernamen, einen SSH-Schlüssel und ein Zielverzeichnis auf dem Remotecomputer. Protokolldateien werden basierend auf einem von Ihnen festgelegten Rollover-Zeitplan übertragen.

SWA-Protokoll-Abonnement

Sie können für jeden Protokolldateityp mehrere Protokoll-Subscriptions erstellen. Abonnements enthalten Konfigurationsdetails für Archivierung und Speicherung, darunter:

- Rollover-Einstellungen, die bestimmen, wann Protokolldateien archiviert werden.
- Komprimierungseinstellungen für archivierte Protokolle.
- Abrufeinstellungen für archivierte Protokolle, die angeben, ob Protokolle auf einem Remote-Server archiviert oder auf der Appliance gespeichert werden.

Archivieren von Protokolldateien

AsyncOS archiviert (rollt über) Protokoll-Subscriptions, wenn eine aktuelle Protokolldatei eine vom Benutzer angegebene maximale Dateigröße oder maximale Zeit seit dem letzten Rollover erreicht.

Diese Archivierungseinstellungen sind in Protokoll-Subscriptions enthalten:

- Rollover nach Dateigröße
- Rollover nach Zeit
- Protokollkomprimierung
- Retrieval-Methode

Sie können Protokolldateien auch manuell archivieren (Rollover).
Schritt 1: Wählen Sie Systemverwaltung > Protokollabonnements aus.
Schritt 2: Aktivieren Sie das Kontrollkästchen in der Spalte Rollover der zu archivierenden Protokoll-Subscriptions, oder aktivieren Sie das Kontrollkästchen Alle, um alle Subscriptions auszuwählen.
Schritt 3 . Klicken Sie auf Rollover Now, um die ausgewählten Protokolle zu archivieren.

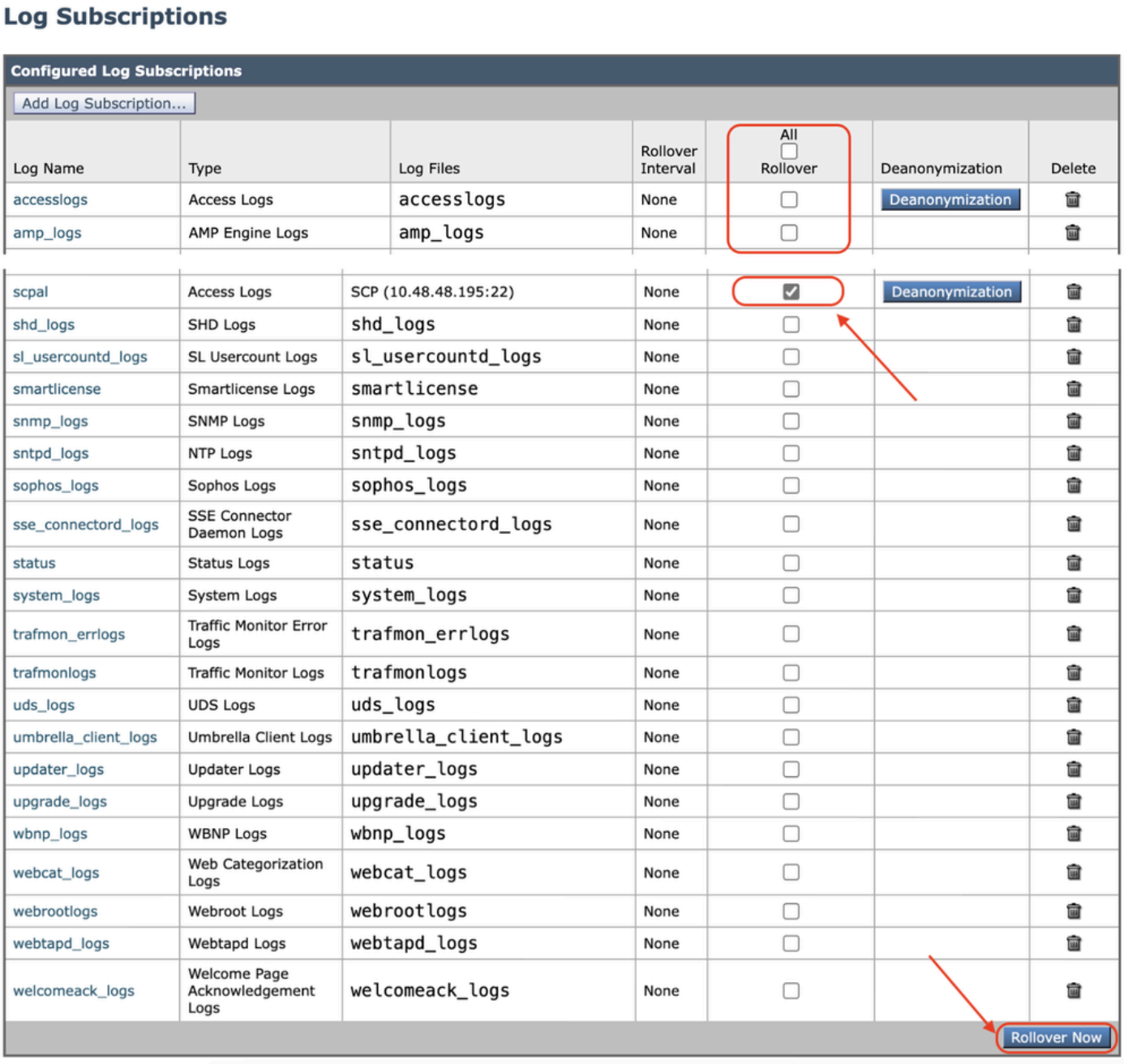


Bild - Benutzeroberfläche für Rollover jetzt

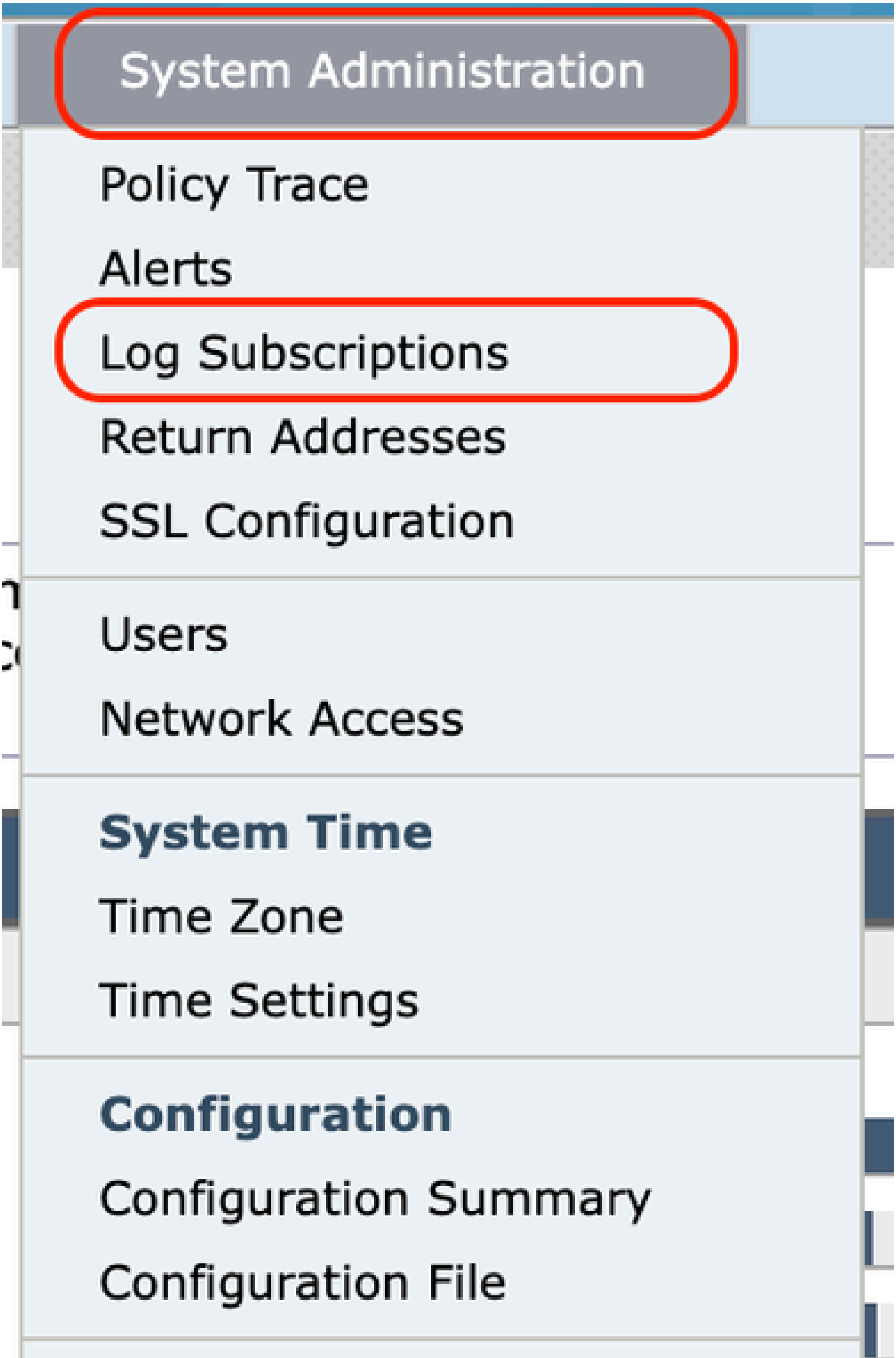
Konfigurieren des Protokollabrufs über SCP auf dem Remote-Server

Es gibt zwei Hauptschritte für den Protokollabruf auf einem Remote-Server mit SCP von SWA:

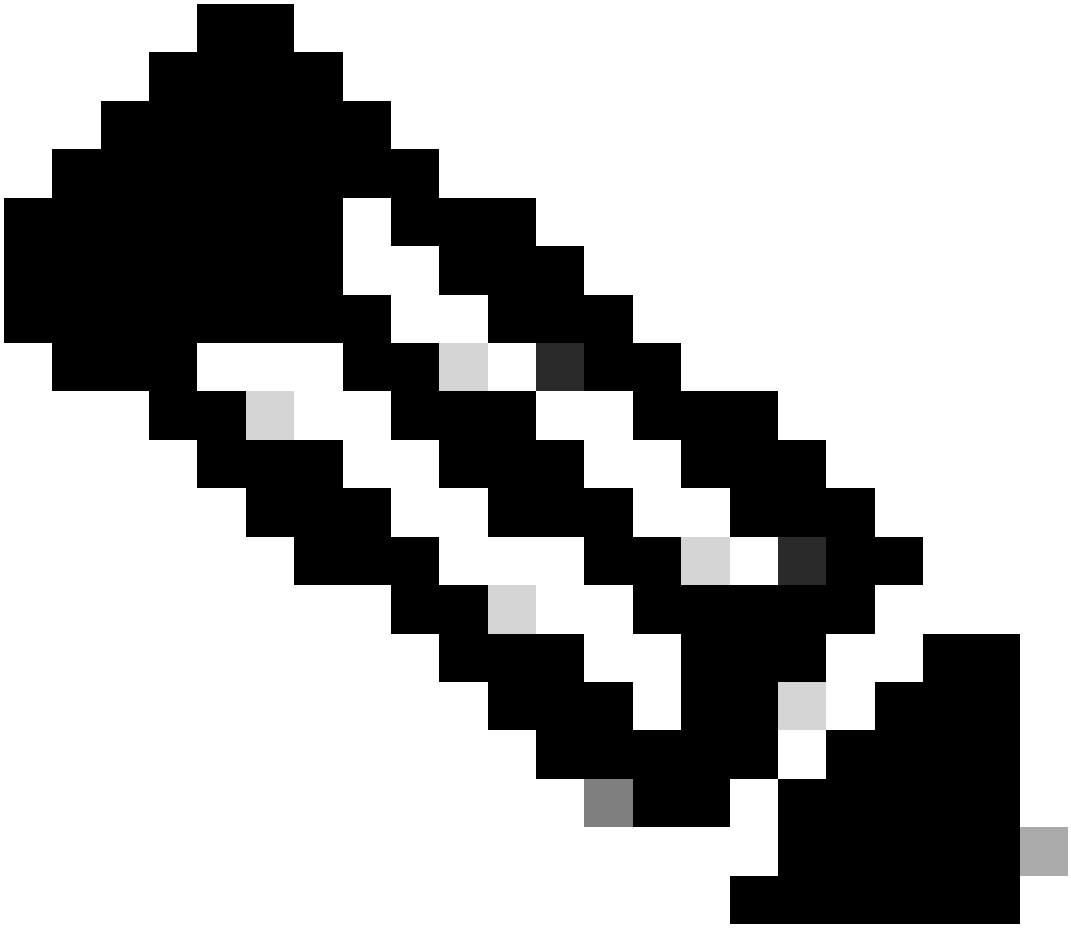
1. Konfigurieren Sie SWA so, dass die Protokolle übertragen werden.
2. Konfigurieren Sie den Remote-Server so, dass er die Protokolle empfängt.

Konfigurieren von SWA zum Senden der Protokolle von der GUI an den SCP Remote-Server

Schritt 1: Melden Sie sich bei SWA an, und wählen Sie unter Systemverwaltung die Option Protokoll-Subscriptions aus.


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

Speichern Sie den SSH-Schlüssel in einer Textdatei für die weitere Verwendung im Konfigurationsabschnitt des Remote-SCP-Servers.



Hinweis: Sie müssen beide Zeilen kopieren, beginnend mit ssh- und endend mit root@<SWA hostname> .

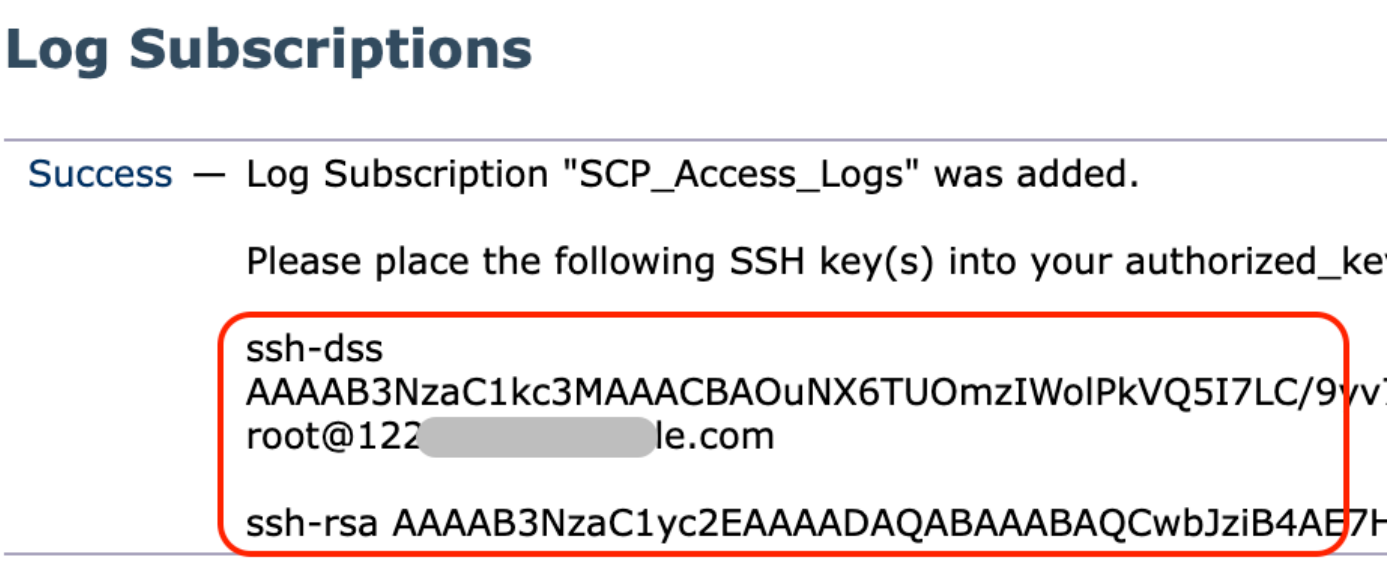
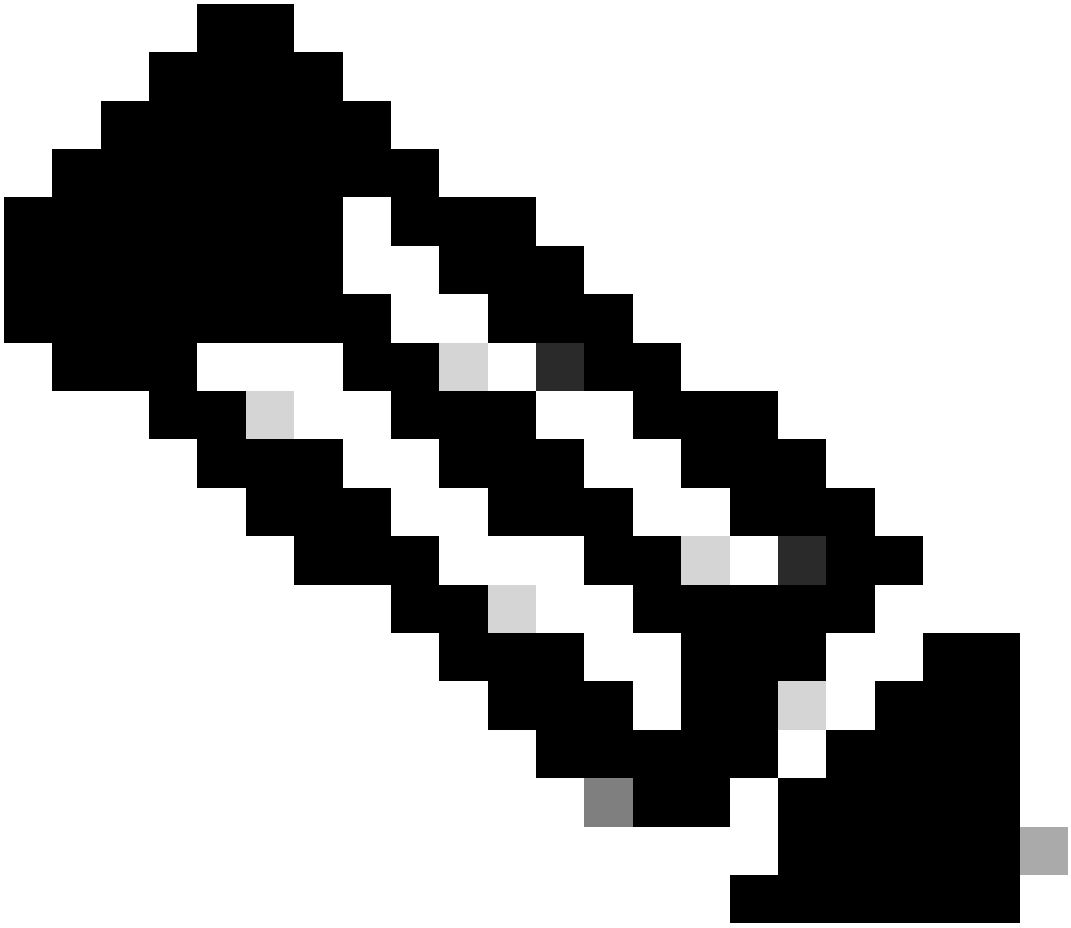


Bild - Speichern Sie den SSH-Schlüssel zur weiteren Verwendung.

Schritt 10. Änderungen bestätigen.

Konfigurieren von Microsoft Windows als SCP-Remote-Server

Schritt 10. So erstellen Sie einen Benutzer für den SCP-Dienst:



Hinweis: Wenn Sie bereits einen Benutzer für die SCP haben, fahren Sie mit Schritt 16 fort.

Schritt 11. Wählen Sie Lokale Benutzer und Gruppe aus, und wählen Sie Benutzer aus dem linken Bereich aus.

Schritt 12: Klicken Sie mit der rechten Maustaste auf die Hauptseite, und wählen Sie einen neuen Benutzer aus.

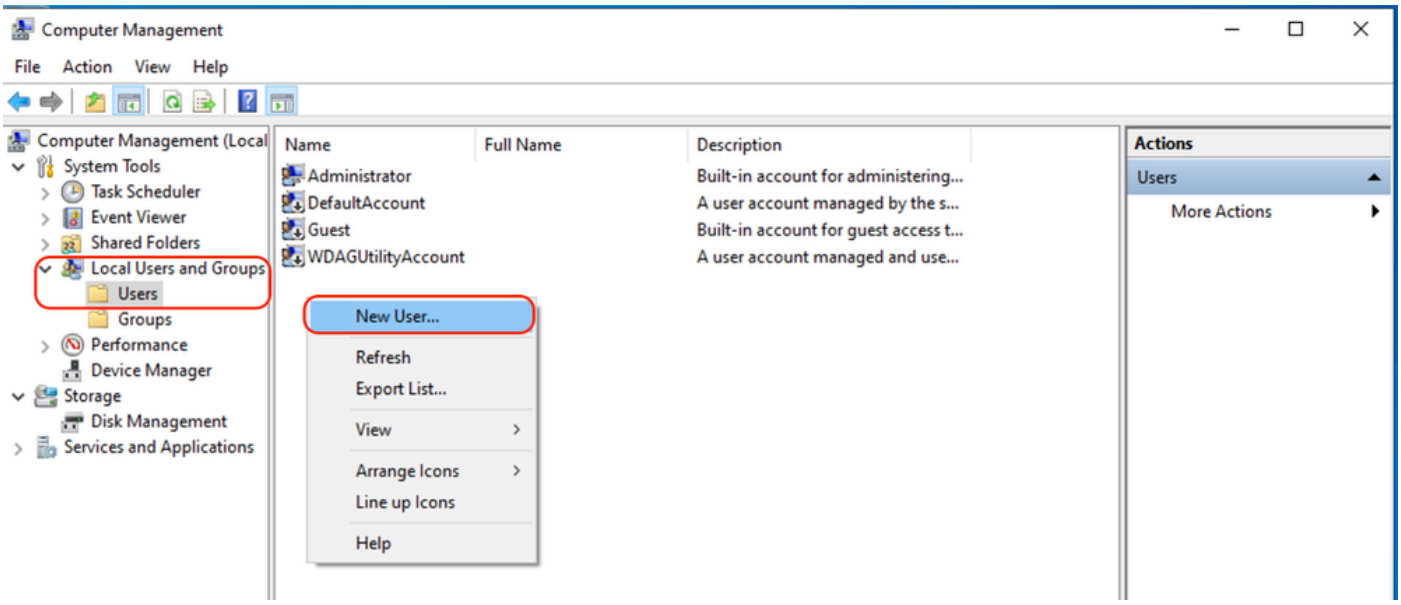


Image - Erstellen eines Benutzers für den SCP-Service.

Schritt 13: Geben Sie den Benutzernamen und das gewünschte Kennwort ein.

Schritt 14: Wählen Sie Kennwort ist nie abgelaufen aus.

Schritt 15: Klicken Sie auf Erstellen, und schließen Sie das Fenster.

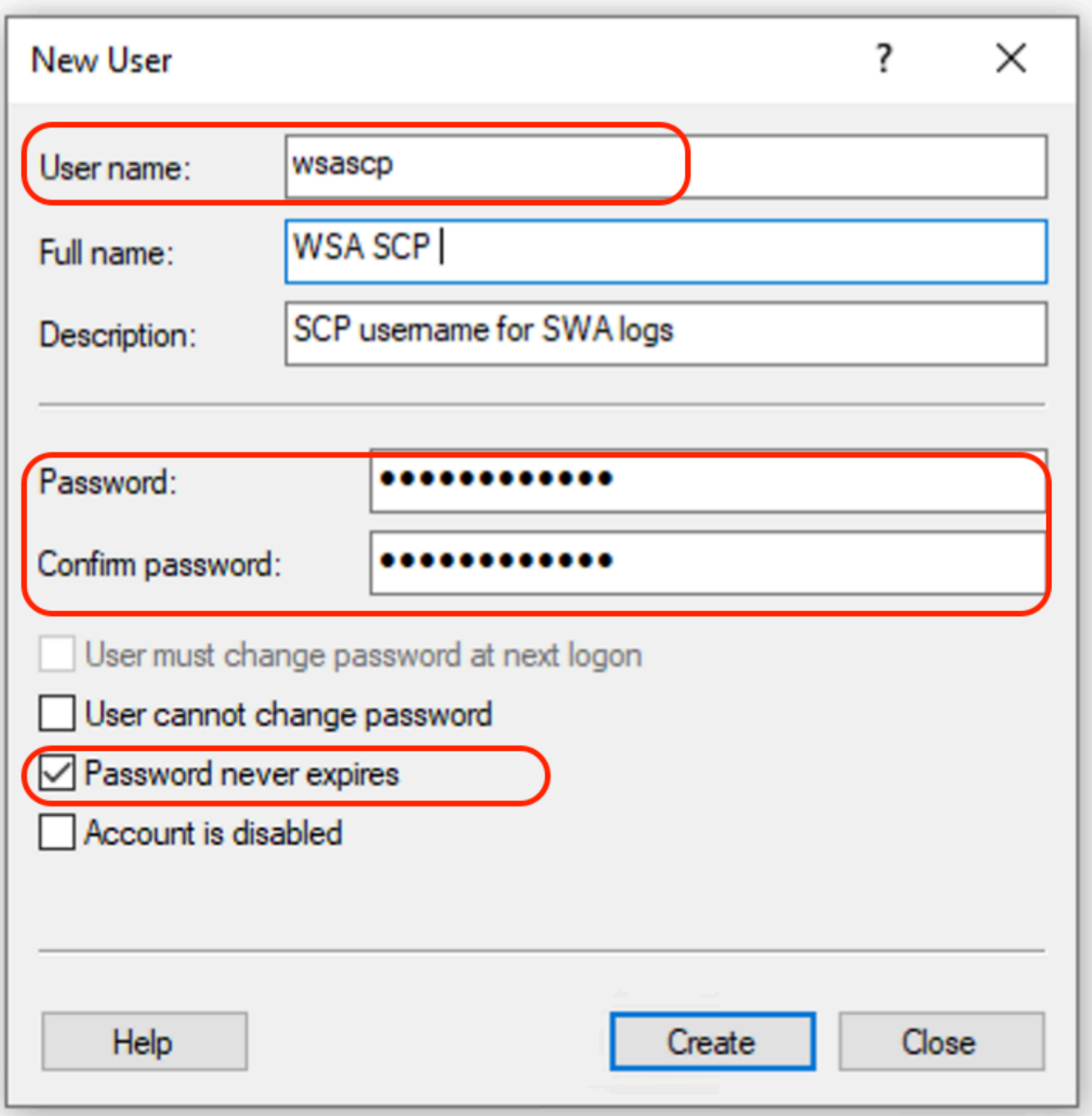
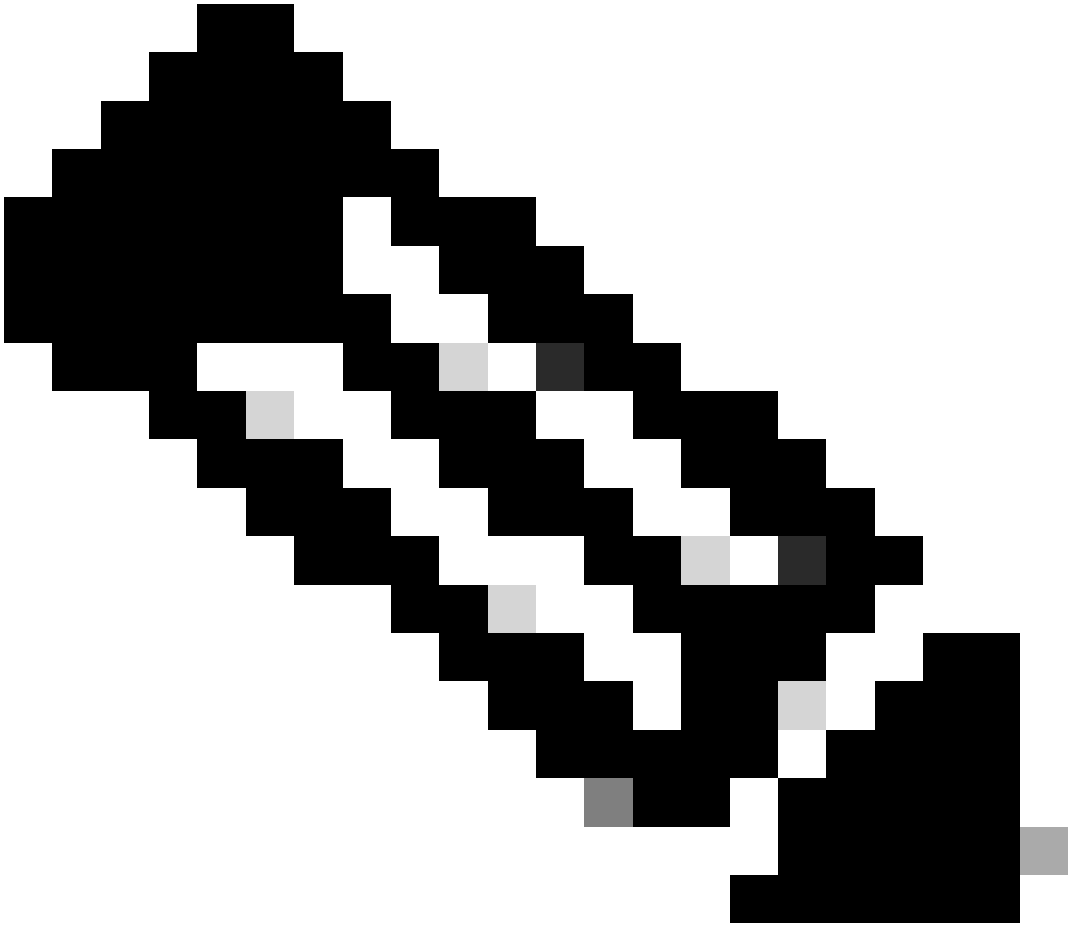


Bild: Geben Sie neue Benutzerinformationen ein.

Schritt 16: Melden Sie sich mit dem neu erstellten Benutzer beim Remote-SCP-Server an, um das Profilverzeichnis erstellen zu lassen.



Hinweis: Wenn Sie OpenSSL auf Ihrem Remote SCP-Server installiert haben, fahren Sie mit Schritt 19 fort.

Schritt 17: Öffnen Sie PowerShell mit Administratorrechten (Als Administrator ausführen), und führen Sie diesen Befehl aus, um die Voraussetzungen zu überprüfen:

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

Wenn die Ausgabe True lautet, können Sie fortfahren. Wenden Sie sich andernfalls an das Microsoft-Supportteam,

Schritt 18: Führen Sie Folgendes aus, um OpenSSH mit PowerShell mit Administratorrechten (Ausführen als Administrator) zu installieren:

```
# 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 ein Beispiel für erfolgreiche Ergebnisse:

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

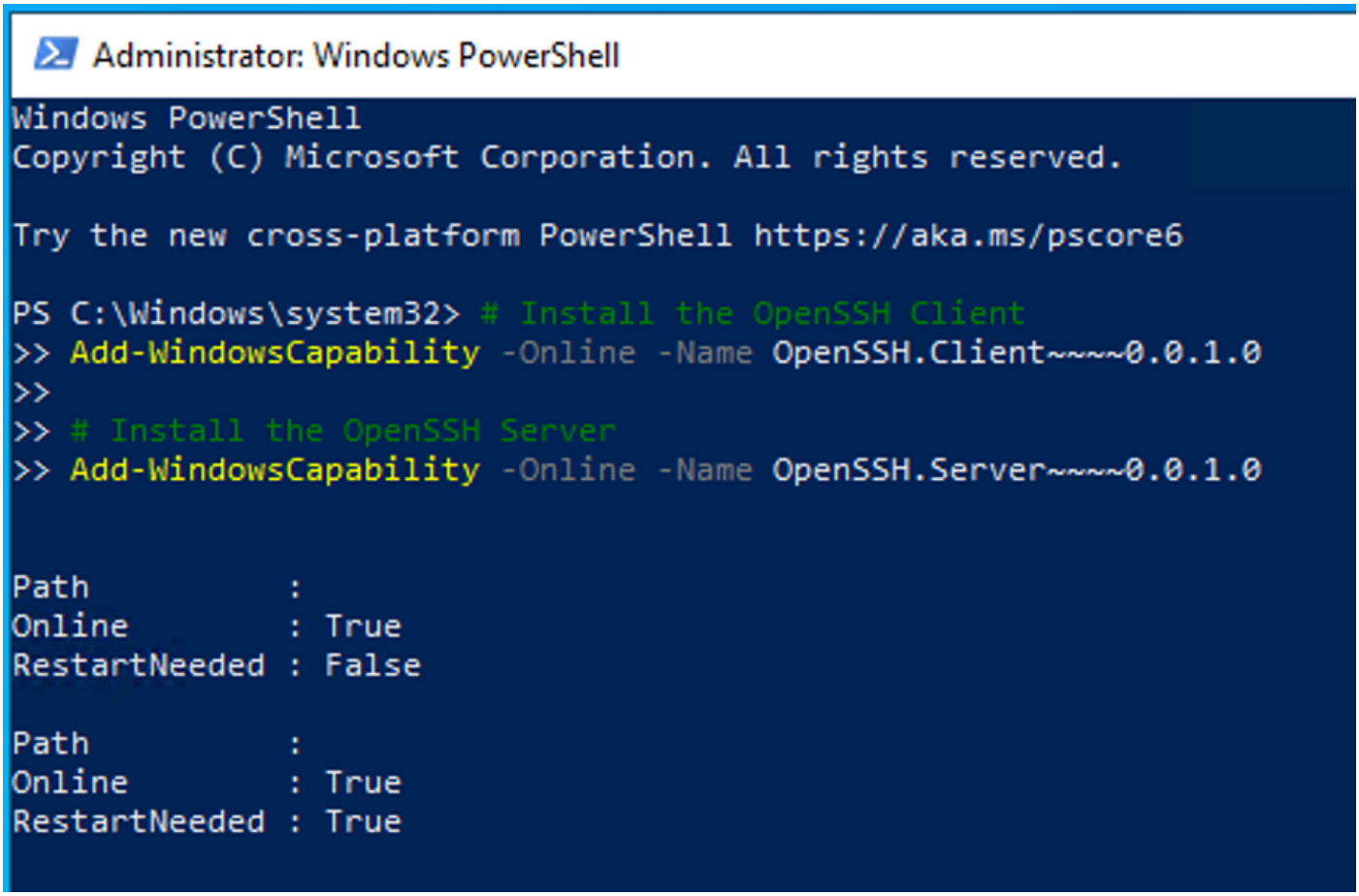
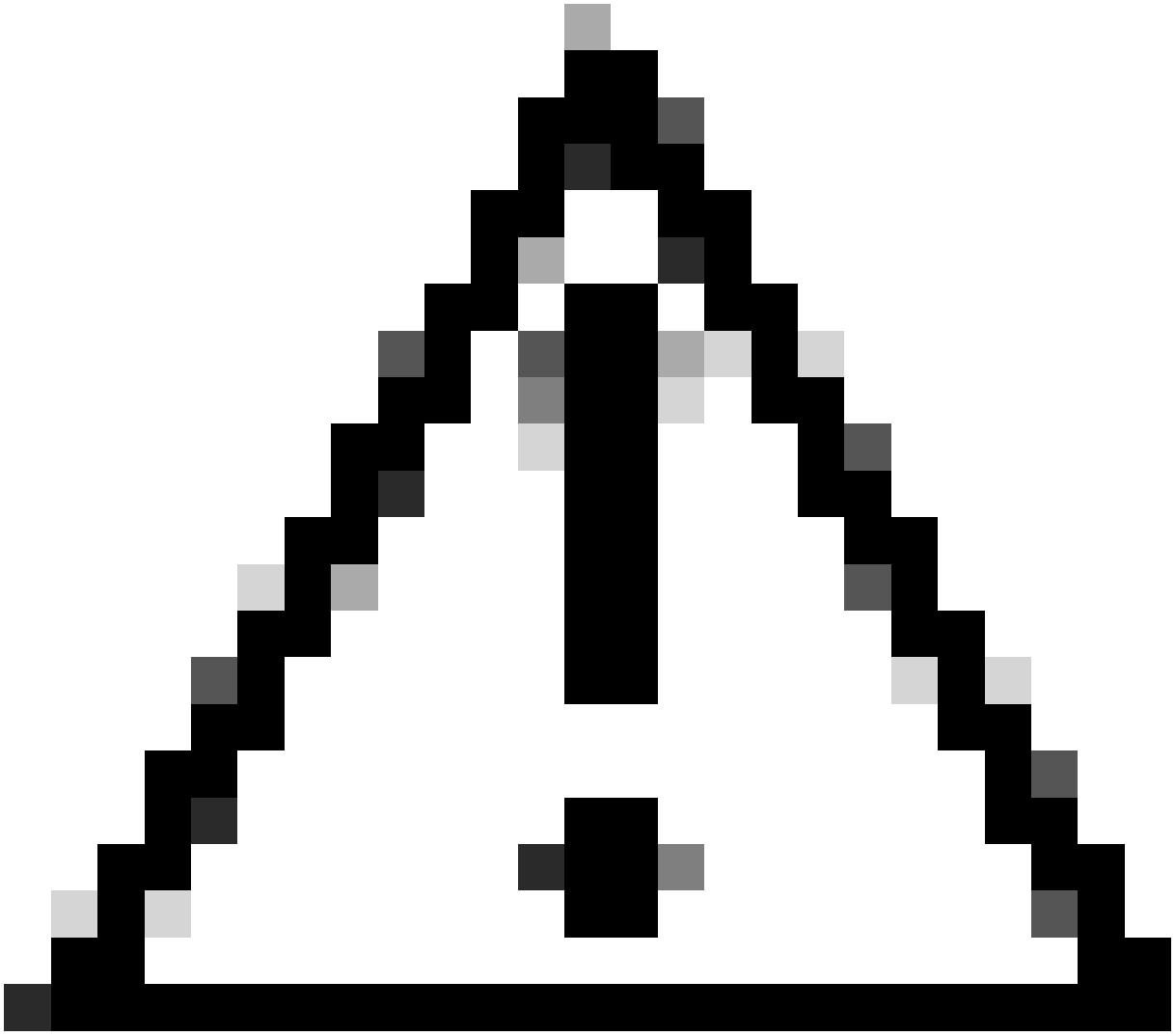


Image: Installation von OpenSSH in PowerShell



Achtung: Wenn RestartNeeded auf True festgelegt ist, starten Sie Windows neu.

Weitere Informationen zur Installation auf anderen Versionen von Microsoft Windows finden Sie unter diesem Link : [Erste Schritte mit OpenSSH für Windows | Microsoft - Informationen]

Schritt 19: Öffnen Sie eine normale (nicht erhöhte) PowerShell-Sitzung, und generieren Sie ein Paar RSA-Schlüssel mit dem folgenden Befehl:

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

Nachdem der Befehl beendet ist, können Sie sehen, dass der Ordner .ssh Ihr Benutzerprofilverzeichnis erstellt hat.

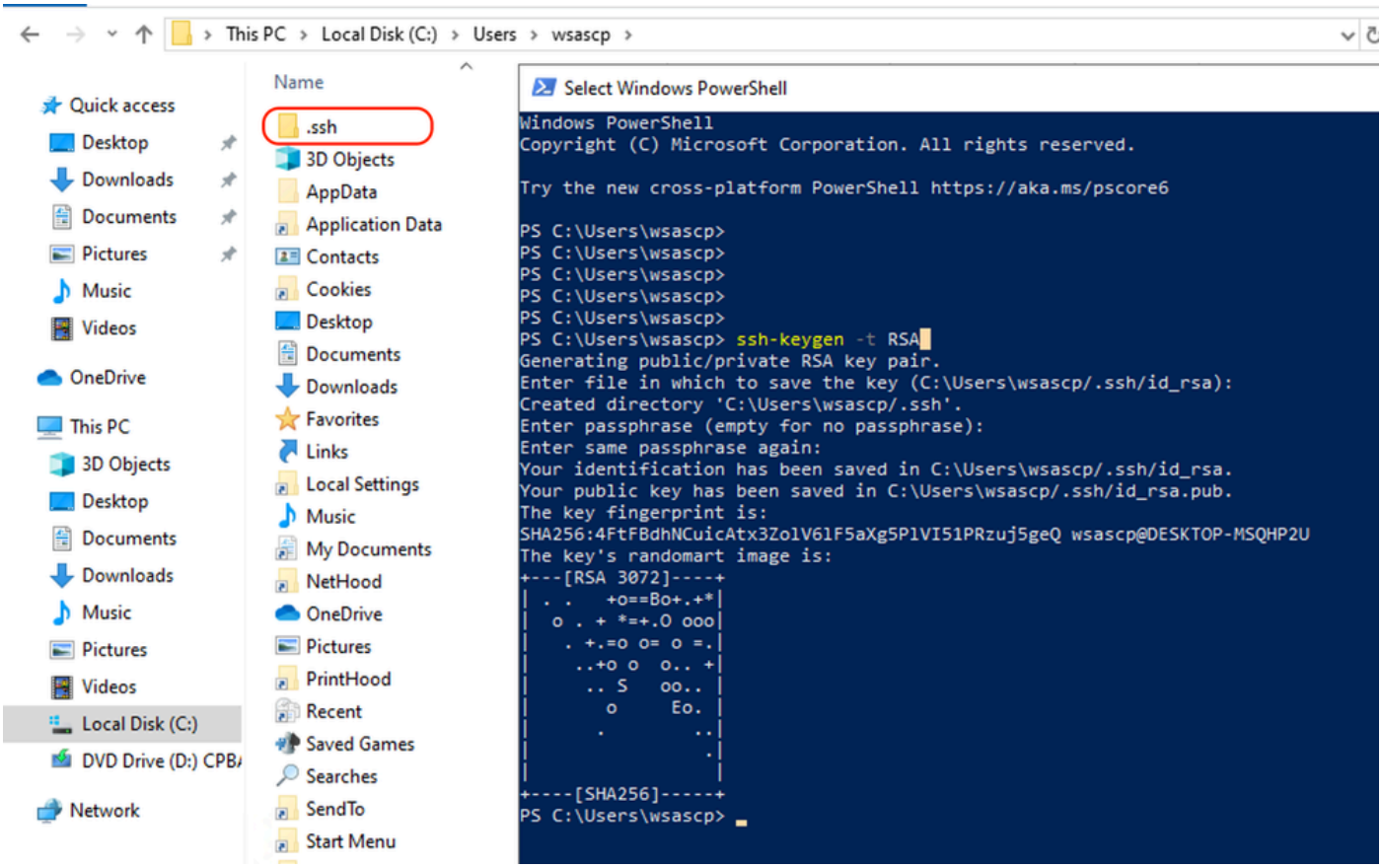


Bild - RSA-Schlüssel generieren

Schritt 20: Starten Sie den SSH-Dienst von PowerShell mit Administratorberechtigung (Als Administrator ausführen).

```
Start-Service sshd
```

Schritt 21. (Optional, aber empfohlen) Ändern Sie den Starttyp des Diensts in Automatisch mit Administratorrechten (Als Administrator ausführen).

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

Schritt 22: Bestätigen Sie, dass die Firewall-Regel für den Zugriff auf den TCP-Port 22 erstellt wurde.

```
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."
}
```

Schritt 23: Bearbeiten Sie die SSH-Konfigurationsdatei im Verzeichnis %programdata%\ssh\sshd_config im Notepad, und entfernen Sie die # für RSA und 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
```

Schritt 24: Bearbeiten Sie die Verbindungsbedingungen in %programdata%\ssh\sshd_config. In diesem Beispiel gilt die Listen-Adresse für alle Schnittstellen-Adressen. Sie können es aufgrund Ihres Designs anpassen.

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

Schritt 25. Markieren Sie diese beiden Zeilen am Ende der Datei %programdata%\ssh\sshd_config, indem Sie # am Anfang jeder Zeile hinzufügen:

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

Schritt 26.(Optional) Bearbeiten Sie die strikten Modi in %programdata%\ssh\sshd_config. Dieser Modus ist standardmäßig aktiviert und verhindert die auf dem SSH-Schlüssel basierende Authentifizierung, wenn private und öffentliche Schlüssel nicht ordnungsgemäß geschützt sind.

Kommentarlose Eingabe der Zeile #StrictModes yes und Änderung in StrictModes no:

```
StrictModes No
```

Schritt 27: Entfernen Sie die # aus dieser Zeile in %programdata%\ssh\sshd_config, um die Authentifizierung mit öffentlichem Schlüssel zu ermöglichen.

```
PubkeyAuthentication yes
```

Schritt 28: Erstellen Sie eine Textdatei "authorized_keys" im Ordner ".ssh", und fügen Sie den öffentlichen SWA-RSA-Schlüssel ein (der in Schritt 9 erfasst wurde).

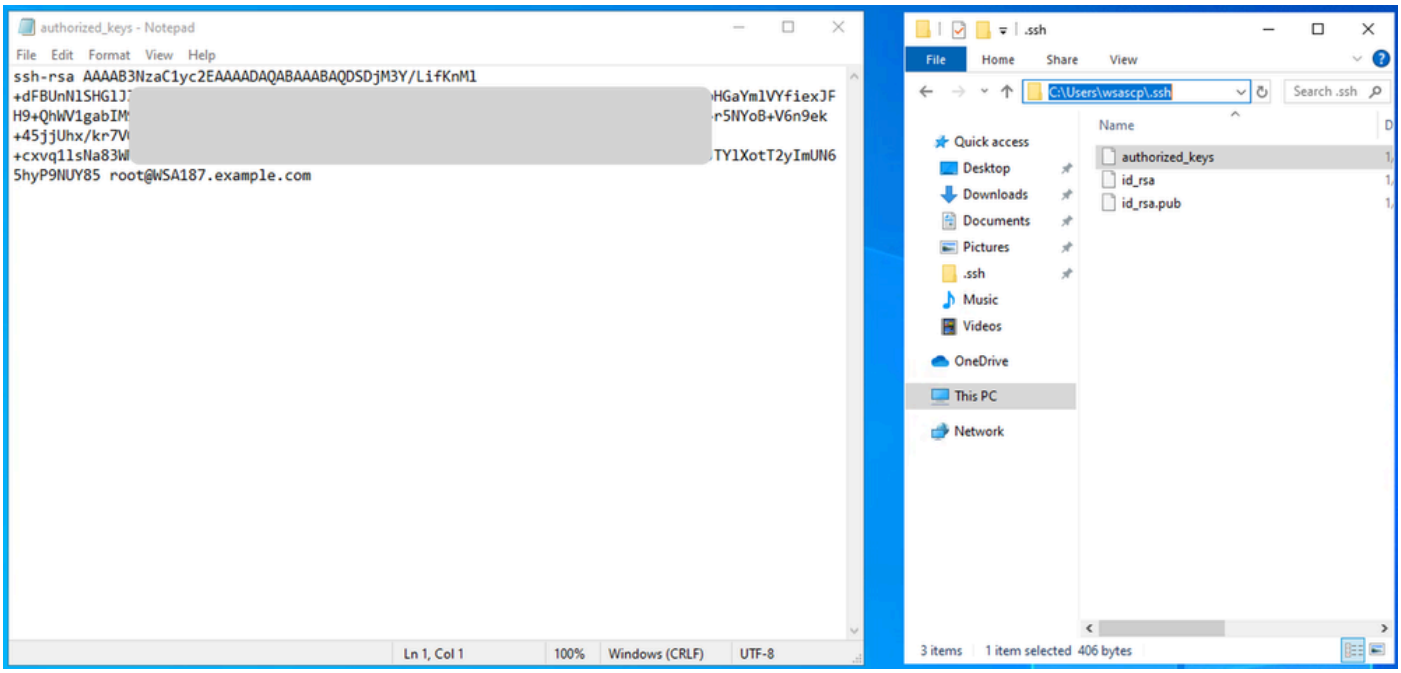
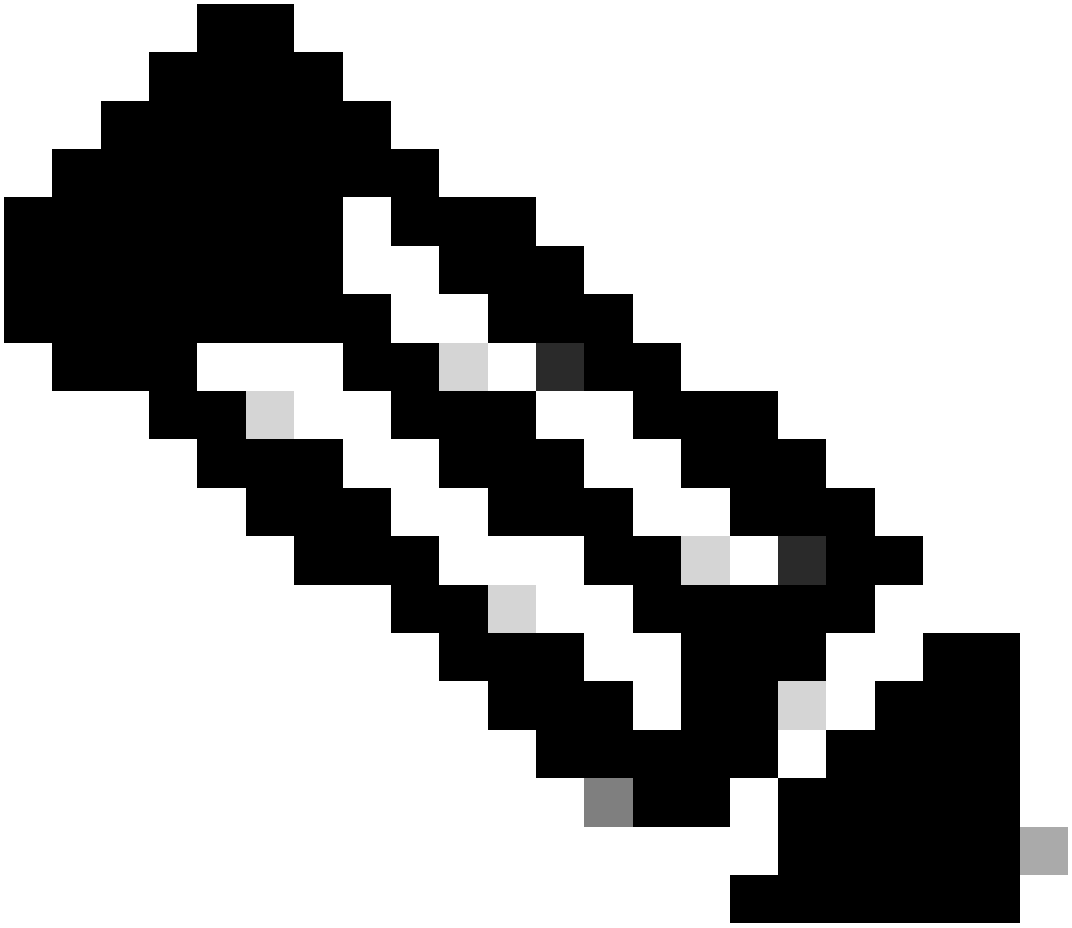
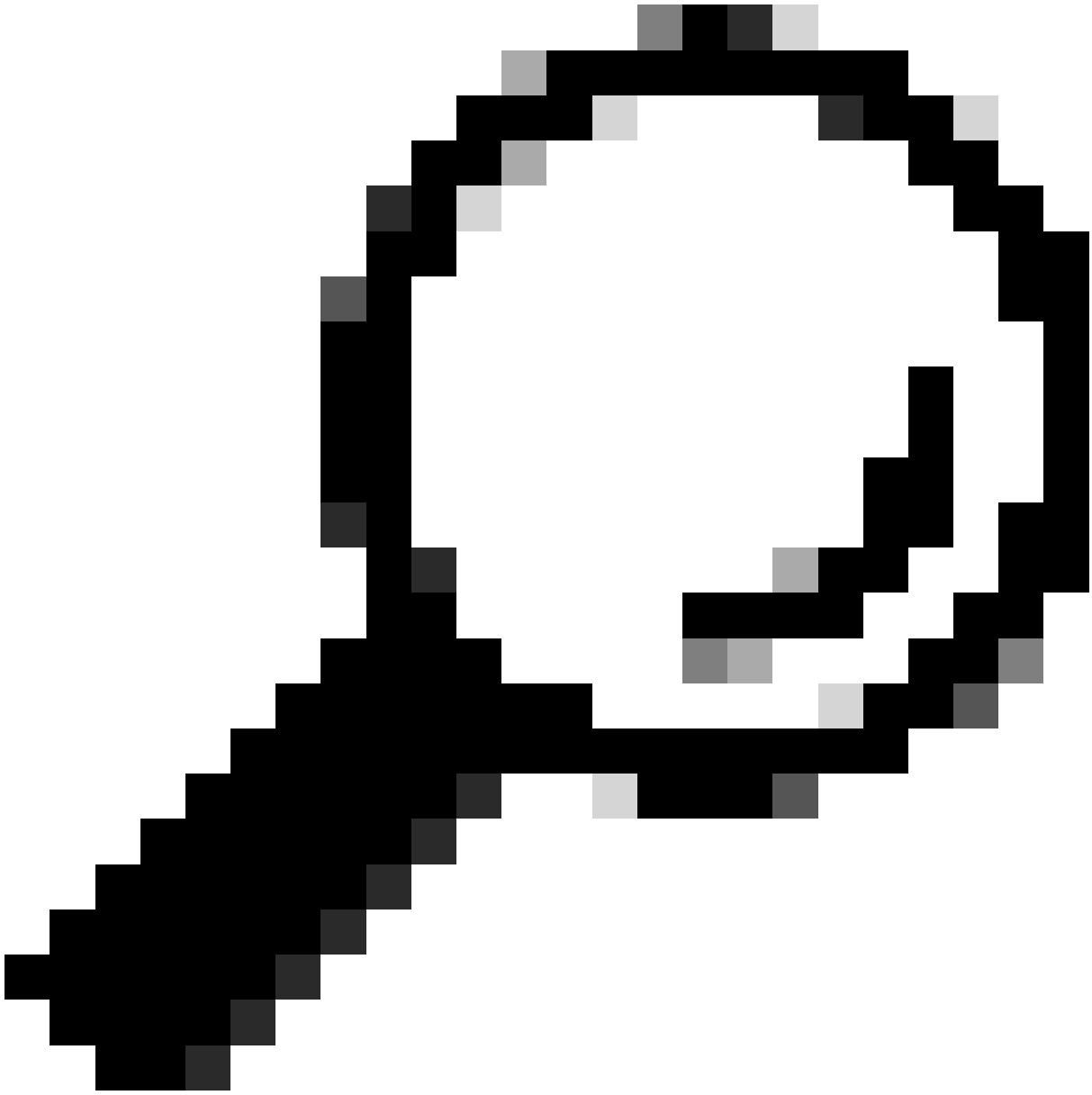


Bild - Öffentlicher SWA-Schlüssel



Hinweis: Kopieren Sie die gesamte Zeile, beginnend mit ssh-rsa und endend mit root@<Ihr_SWA_Hostname>



Tipp: Da RSA auf dem SCP-Server installiert ist, muss der Schlüssel ssh-dss nicht eingefügt werden.

Schritt 29: Aktivieren Sie "OpenSSH Authentication Agent" in PowerShell mit Administratorrechten (Als Administrator ausführen).

```
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: Open SSH Authentication Agent aktivieren

Schritt 30.(Optional) Fügen Sie diese Zeile zu %programdata%\ssh\sshd_config hinzu, um folgende Schlüsseltypen zuzulassen:

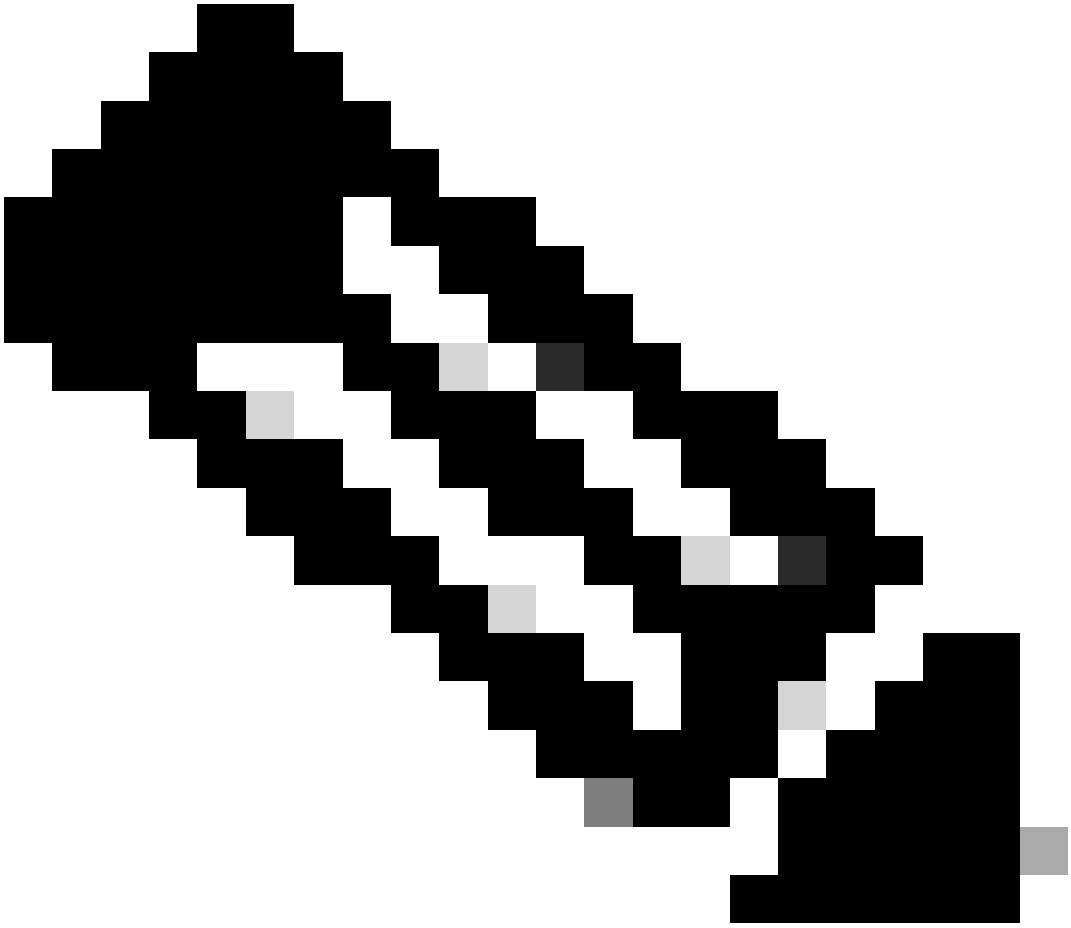
```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rs
```

Schritt 31: Starten Sie den SSH-Dienst neu. Sie können diesen Befehl in PowerShell mit Administratorrechten verwenden (Als Administrator ausführen).

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

Schritt 32: Um zu testen, ob der SCP-Push richtig konfiguriert ist, führen Sie ein Rollover der konfigurierten Protokolle durch, und zwar über die GUI oder die CLI (rollovernow-Befehl):

```
WSA_CLI> rollovernow scpal
```



Hinweis: In diesem Beispiel lautet der Protokollname "scpal".

Sie können bestätigen, dass die Protokolle in den definierten Ordner kopiert werden, der in diesem Beispiel c:/Users/wsascp/wsa01 war.

Push-SCP-Protokolle auf ein anderes Laufwerk

Falls Sie die Protokolle auf ein anderes Laufwerk als C: übertragen müssen, erstellen Sie einen Link vom Benutzerprofilordner zum gewünschten Laufwerk. In diesem Beispiel werden die Protokolle an die Adresse D:\WSA_Logs\WSA01 gesendet.

Schritt 1. Erstellen Sie die Ordner in der gewünschten Festplatte, in diesem Beispiel

Schritt 2: Öffnen der Eingabeaufforderung mit Administratorrechten (Als Administrator ausführen)

Schritt 3: Führen Sie den folgenden Befehl aus, um den Link zu erstellen:

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

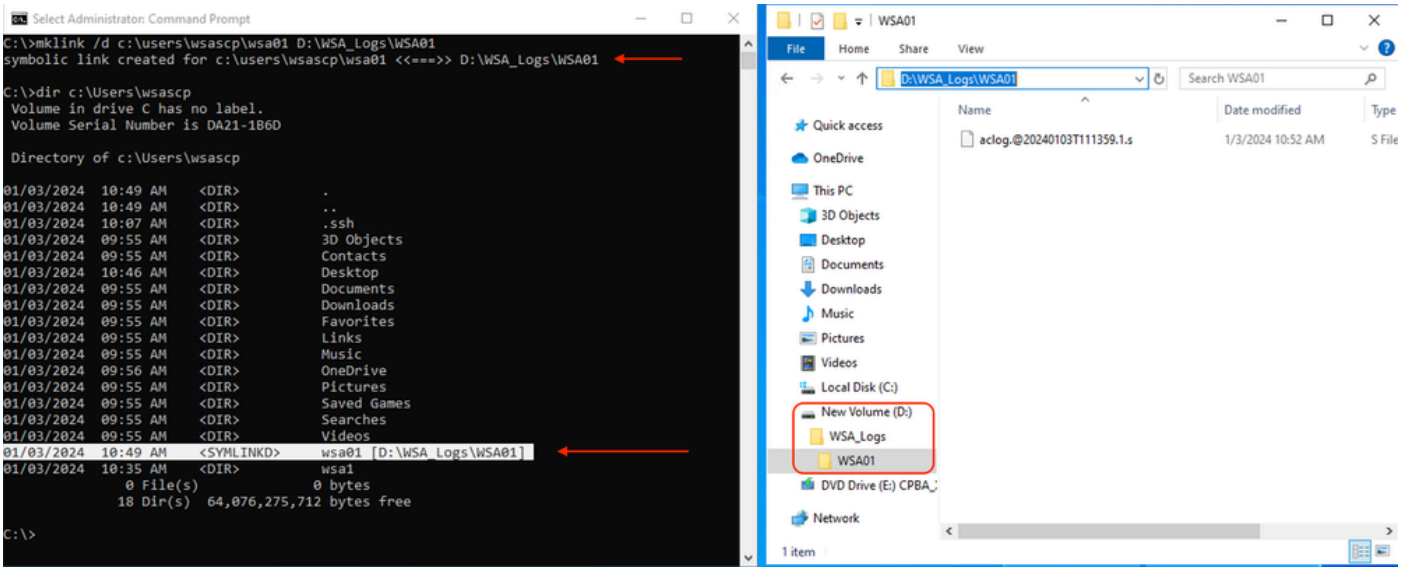
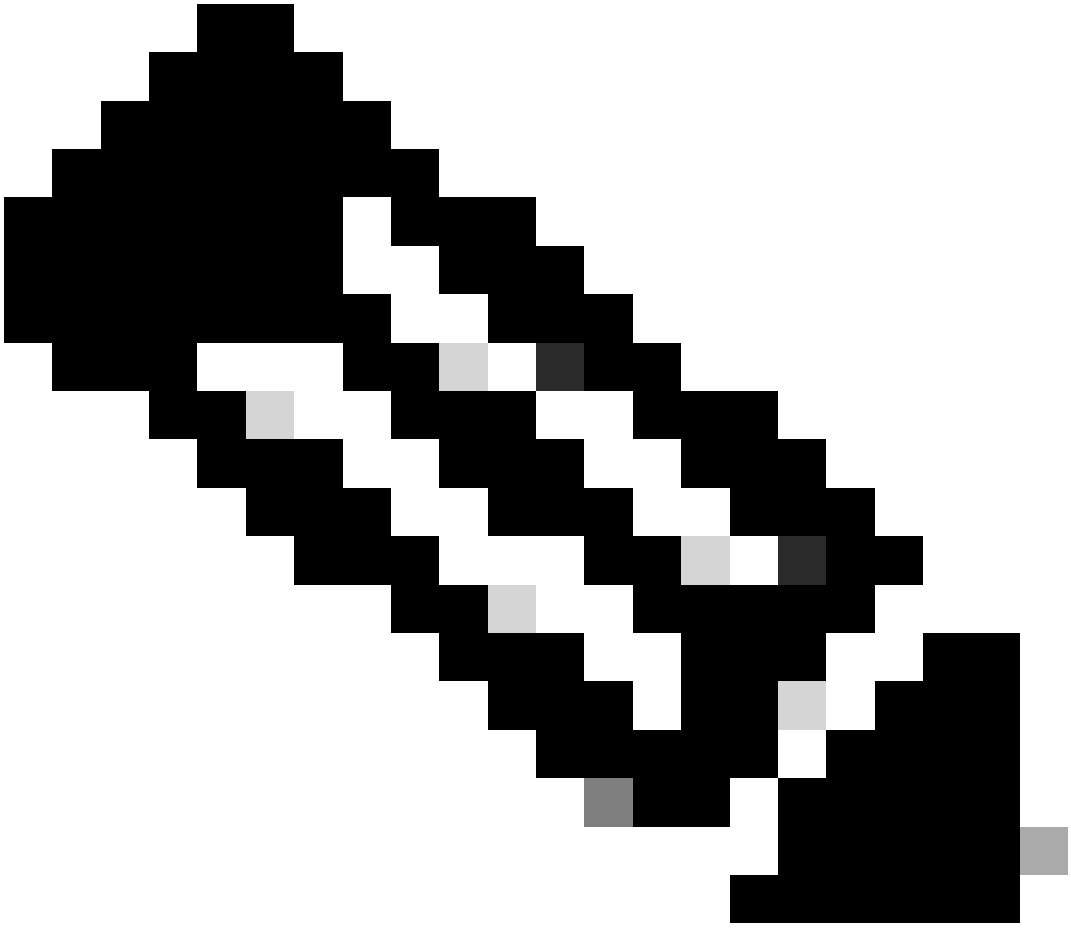


Bild - SYM-Link erstellen



Hinweis: In diesem Beispiel ist SWA so konfiguriert, dass die Protokolle in den Ordner "WSA01" in "C:\Users\wsascp" verschoben werden. Der SCP-Server verfügt über den Ordner "WSA01" als symbolischen Link zu "D:\WSA_Logs\WSA01".

Weitere Informationen zu Microsoft Symbol Link finden Sie unter: [mklink | Microsoft - Informationen]

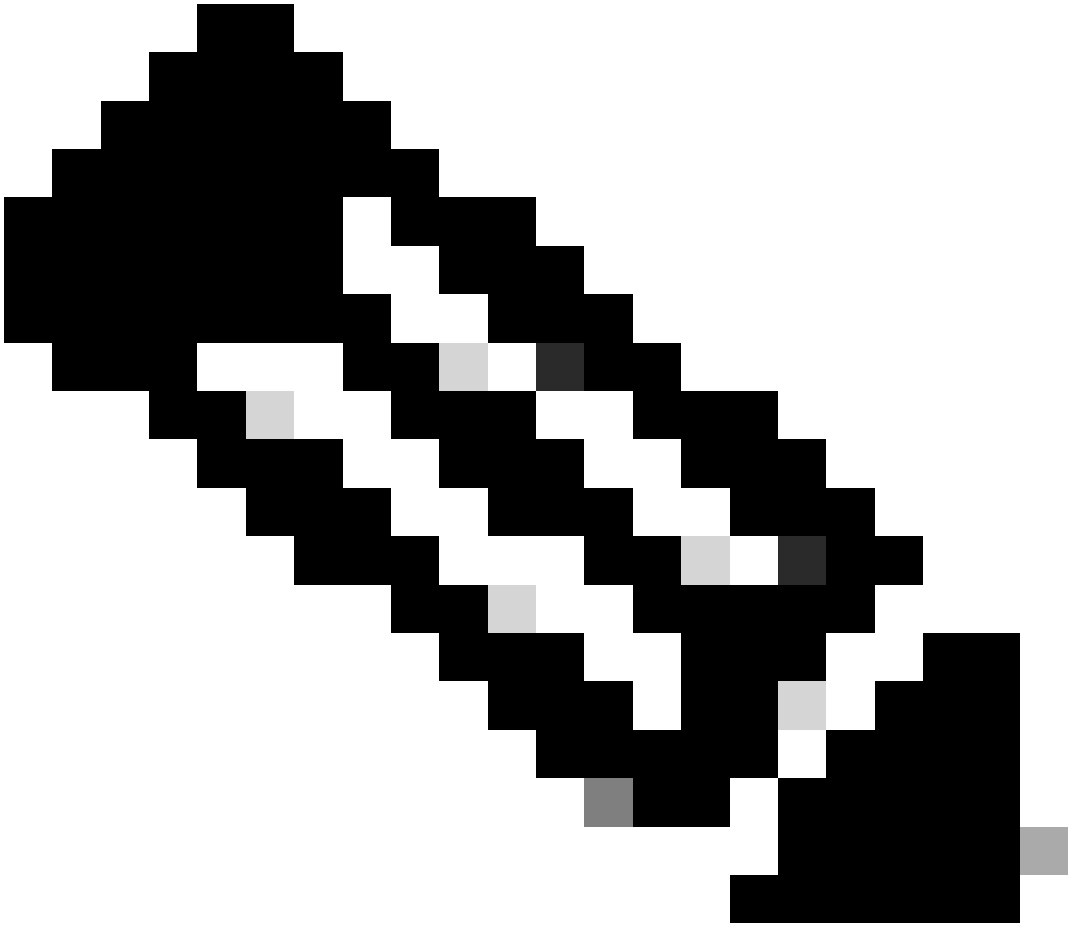
Fehlerbehebung: SCP-Protokoll-Push

Protokolle in SWA anzeigen

Prüfen Sie zur Fehlerbehebung beim SCP-Protokoll-Push die Fehler in:

1. CLI > zeigtWarnungen an

2. System_logs



Hinweis: Um system_logs zu lesen, können Sie den Befehl grep in der CLI verwenden, die mit system_logs verknüpfte Nummer auswählen und die Frage im Assistenten beantworten.

Protokolle auf dem SCP-Server anzeigen

Sie können die SCP-Serverprotokolle in der Microsoft Event Viewer unter Anwendungen und Dienstprotokolle lesen > OpenSSH > Betriebsbereit

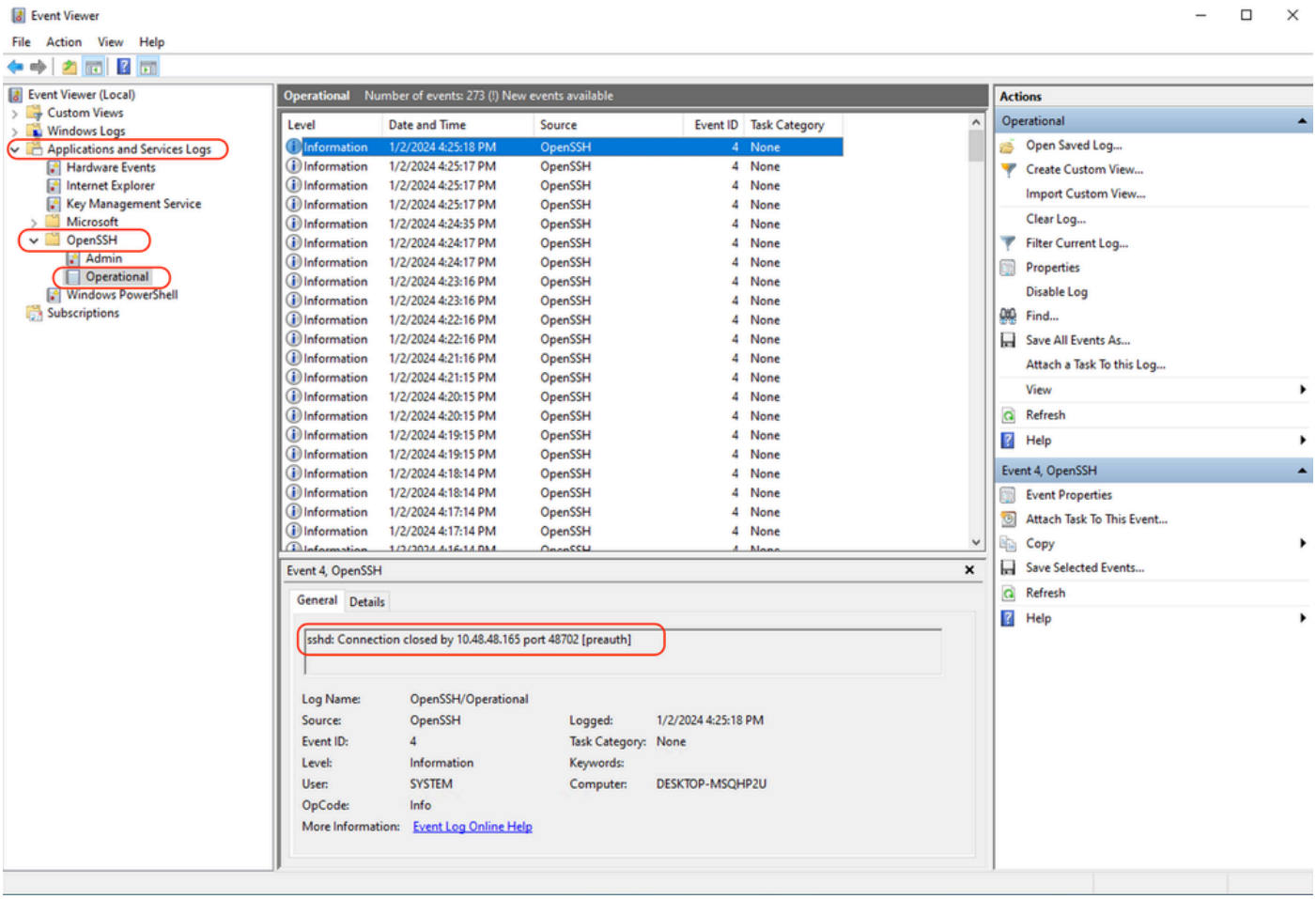


Bild - PreAuth fehlgeschlagen

Host-Schlüsselüberprüfung fehlgeschlagen

Dieser Fehler zeigt an, dass der öffentliche Schlüssel des SCP-Servers, der in SWA gespeichert ist, ungültig ist.

Nachfolgend finden Sie ein Beispiel für einen Fehler bei der Anzeige von Warnmeldungen in der 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.
```

Hier sind einige Beispiele für Fehler 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
```

Um dieses Problem zu beheben, können Sie den Host vom SCP-Server kopieren und in die Abonnementseite für SCP-Protokolle einfügen.

Siehe Schritt 7 in SWA konfigurieren, um die Protokolle von der GUI an den SCP Remote-Server zu senden, oder wenden Sie sich an das Cisco TAC, um den Host-Schlüssel vom Backend zu entfernen.

Berechtigung verweigert (publickey,password,keyboard-interactive)

Dieser Fehler weist normalerweise darauf hin, dass der in SWA angegebene Benutzername ungültig ist.

Beispiel für ein Fehlerprotokoll 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
```

Beispiel für einen Fehler des SCP-Servers: Ungültiger Benutzer-SCP von <SWA_IP-Adresse> Port <TCP-Port SWA-Verbindungen zum SCP-Server>

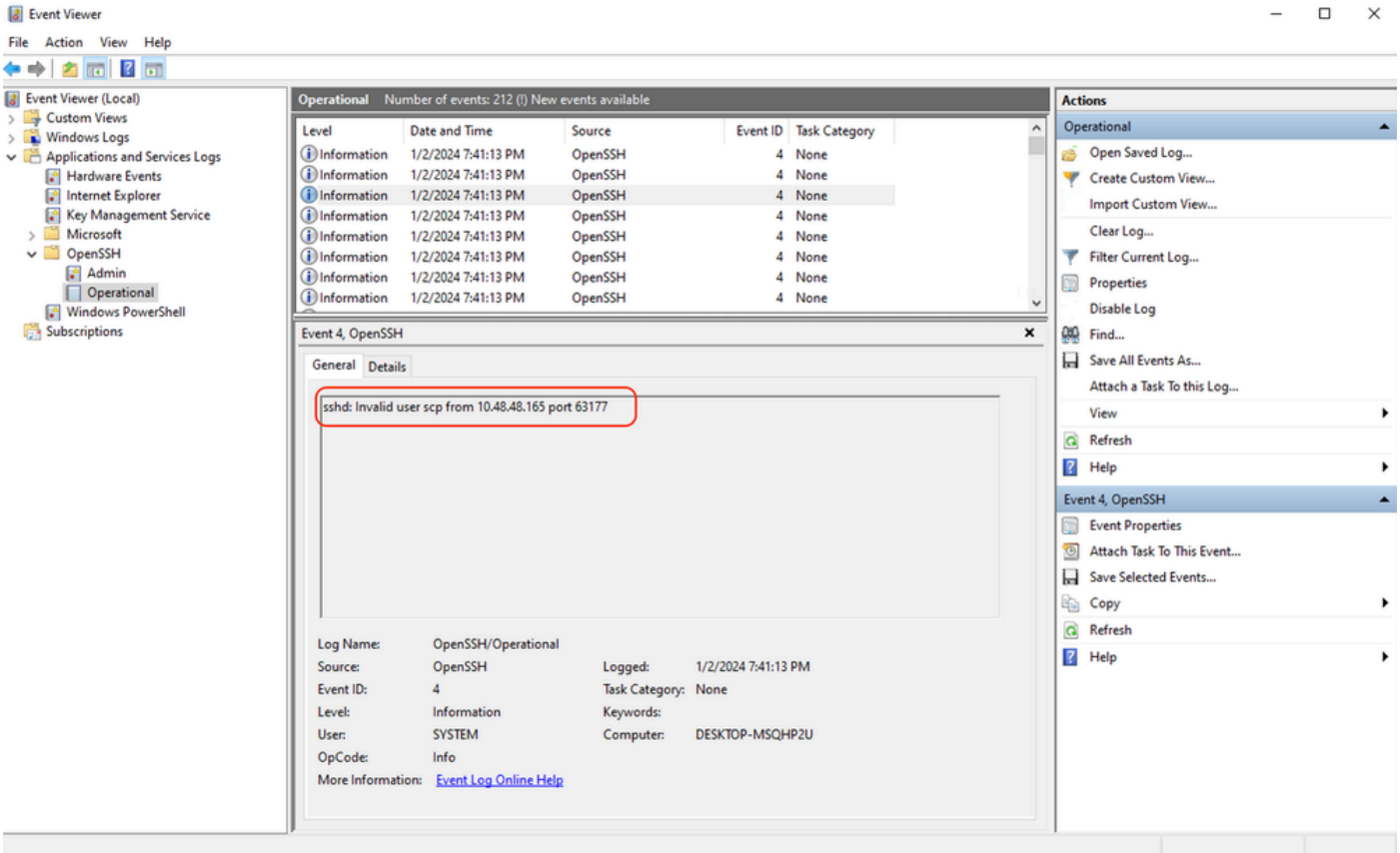


Bild - Ungültiger Benutzer

Um diesen Fehler zu beheben, überprüfen Sie die Rechtschreibung und stellen Sie sicher, dass der Benutzer (der in SWA konfiguriert wurde, um die Protokolle zu übertragen) im SCP-Server aktiviert ist.

Keine solche Datei oder solches Verzeichnis

Dieser Fehler zeigt an, dass der im SWA-Protokoll-Abonnementabschnitt angegebene Pfad ungültig ist.

Beispiel für einen Fehler in 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
```

Um dieses Problem zu lösen, überprüfen Sie die Rechtschreibung und vergewissern Sie sich, dass der Pfad im SCP-Server richtig und gültig ist.

SCP konnte nicht übertragen werden.

Dieser Fehler kann ein Hinweis auf einen Kommunikationsfehler sein. Beispiel für einen Fehler:

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

Verwenden Sie den Befehl telnet in der SWA-CLI, um Probleme mit der Verbindung zu beheben:

```
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 diesem Beispiel ist die Verbindung nicht hergestellt. Der erfolgreiche Verbindungsausgang sieht

wie folgt aus:

```
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
```

Wenn das Telnet nicht verbunden ist:

[1] Aktivieren Sie diese Option, wenn die SCP-Server-Firewall den Zugriff blockiert.

[2] Überprüfen Sie, ob Firewalls im Pfad von SWA zum SCP-Server den Zugriff blockieren.

[3] Überprüfen Sie, ob sich der TCP-Port 22 im SCP-Server im Listen-Status befindet.

[4] Führen Sie die Paketerfassung für weitere Analysen sowohl auf dem SWA- als auch auf dem SCP-Server aus.

Nachfolgend finden Sie ein Beispiel für eine erfolgreiche Verbindung mit der Paketerfassung:

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:

Bild - Erfolgreiche Paketerfassung

Referenzen

Best Practices-Richtlinien für Cisco Web Security Appliances - Cisco

BRKSEC-3303 (Cisco Live)

Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD (Allgemeine Bereitstellung) - Verbinden, Installieren und Konfigurieren [Cisco Secure Web Appliance] - Cisco

Erste Schritte mit OpenSSH für Windows | Microsoft - Informationen

Konfigurieren der SSH-Authentifizierung mit öffentlichem Schlüssel unter Windows | Windows-Betriebssystem-Hub (woshub.com)

Schlüsselbasierte Authentifizierung in OpenSSH für Windows | Microsoft - Informationen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.