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

Inhalt

Finleitung
voraussetzungen
Anforderungen
Verwendete Komponenten
<u>SCP</u>
SWA-Protokoll-Abonnement
Archivieren von Protokolldateien
Konfigurieren von LogRetrieval über SCP auf dem Remote-Server
Konfigurieren von SWA zum Senden der Protokolle von der GUI an den SCP Remote-Server
Konfigurieren von Microsoft Windows als SCP-Remote-Server
Push-SCP-Protokolle auf ein anderes Laufwerk
Fehlerbehebung: SCP-Protokoll-Push
Protokolle in SWA anzeigen
Protokolle auf dem SCP-Server anzeigen
Host-Schlüsselüberprüfung fehlgeschlagen
Berechtigung verweigert (publickey.password.keyboard-interactive)
SCP konnte nicht übertragen werden.
Referenzen

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.

Log Subscriptions

Configured Log Subscriptions									
Add Log Subscription									
Log Name	Туре		Log Files	Rollover Interval		All Rollover		Deanonymization	Delete
accesslogs	Access Logs		accesslogs	None				Deanonymization	Ē
amp_logs	AMP Engine Logs		amp_logs	None					ŵ
		-							
scpal	Access Logs	SCP (10.48.48.195:22)	None	C			Deanonymization	Ŵ
shd_logs	SHD Logs	shd_	logs	None					ŵ
sl_usercountd_logs	SL Usercount Logs	sl_u	isercountd_logs	None					ŵ
smartlicense	Smartlicense Logs	smar	rtlicense	None				\mathbf{i}	Ŵ
snmp_logs	SNMP Logs	snmp	_logs	None					ŵ
sntpd_logs	NTP Logs	sntp	od_logs	None					Ŵ
sophos_logs	Sophos Logs	soph	nos_logs	None					Ŵ
sse_connectord_logs	SSE Connector Daemon Logs	sse_	_connectord_logs	None					ŵ
status	Status Logs	stat	tus	None					Ŵ
system_logs	System Logs	syst	em_logs	None					ŵ
trafmon_errlogs	Traffic Monitor Error Logs	traf	fmon_errlogs	None					ŵ
trafmonlogs	Traffic Monitor Logs	traf	fmonlogs	None					ŵ
uds_logs	UDS Logs	uds_	logs	None					ŵ
umbrella_client_logs	Umbrella Client Logs	umbr	rella_client_logs	None					ŵ
updater_logs	Updater Logs	upda	ater_logs	None					ŵ
upgrade_logs	Upgrade Logs	upgr	rade_logs	None					ŵ
wbnp_logs	WBNP Logs	wbnp	_logs	None					ŵ
webcat_logs	Web Categorization Logs	webc	cat_logs	None					ŵ
webrootlogs	Webroot Logs	webr	rootlogs	None					<u>ت</u>
webtapd_logs	Webtapd Logs	webt	apd_logs	None					Ŵ
welcomeack_logs	Welcome Page Acknowledgement Logs	weld	comeack_logs	None					Ŵ
								Rol	lover Now

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	
	System Auministration	100
	Policy Trace	
	Alerts	
	Log Subscriptions	
	Return Addresses	
_	SSL Configuration	L
1 2(Users	
	Network Access	L
	System Time	
	Time Zone	
	Time Settings	
	Configuration	L

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> .

Log Subscriptions

Success — Log Subscription "SCP_Access_Logs" was added.

Please place the following SSH key(s) into your authorized_ke

ssh-dss AAAAB3NzaC1kc3MAAACBAOuNX6TUOmzIWolPkVQ5I7LC/9vv root@122 le.com

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwbJziB4AE7F

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.

New User			?	×					
User name:	wsaso								
Full name:	WSA	WSA SCP							
Description:	SCP usemame for SWA logs								
Password:		•••••							
Confirm password:									
User must char	nge pa	word at next logon							
User cannot ch	nange (assword							
Password neve	er expir	3							
Account is disa	bled								
Help		Create	Clos	se					

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

```
🔀 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: 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 : <u>Erste Schritte mit OpenSSH für Windows | Microsoft - Informationen</u>

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).

authorized_keys - Notepad		– 🗆 🗙		_ ⊘ _ ∓ .s	ssh		-		×
File Edit Format View Help				File Home	Share	View			0
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSDjM3Y/LifKnM1		^					_		-
+dFBUnN1SHG1J7		HGaYmlVYfiexJF		$\leftarrow \rightarrow \land \uparrow$	C:\Users\	\wsascp\.ssh	ڻ ~	Search .ssh	P
H9+QhWV1gabIM		r5NYoB+V6n9ek				Name	^		D
+45jjUhx/kr7V				🖈 Quick access		0			
+CXVQ11SN885W		IYIXot I 2y1mUN6		Desktop	*	authorized_keys			1,
ShyP9N0185 PootgwSA187.example.com				Downloads		id_rsa			1,
				Decuments	<u>_</u>	id_rsa.pub			1,
				Documents	*				
				Pictures	R				
				.ssh	*				
				Music					
				Videos					
				 OneDrive 					
				This PC					
				- Network					
		~			<			_	>
Ln 1, Col 1	100% Windows (CRLF)	UTF-8	-	3 items 1 item s	elected 406 l	bytes		8	

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-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rsa-cert-v01@openssh.com,ssh-rsa-cert-v01@openss

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

Select Administrator: Command Prompt	- 0	×	📙 🔄 📃 🖛 WSA01		- 0	×
C:\>mklink /d c:\users\wsascp\wsa01 D:\WSA_Logs\WSA01 symbolic link created for c:\users\wsascp\wsa01 <<==>> D:\WSA_Logs\WSA01	←──	^	File Home Share	View		~ 🔞
C:\>dir c:\Users\wsascp Volume in drive C has no label. Volume Serial Number is DA21-1860			← → * ↑ ► DAWSA ★ Quick access	LogsWSA01 √ ♂ Name ^ ☐ aclog.@20240103T111359.1.s	Search WSA01 Date modified 1/3/2024 10:52 AM	رم Type S File
Directory of c:\Users\wsascp 01/03/2024 10:49 AM <dir> . 01/03/2024 10:49 AM <dir> . 01/03/2024 10:67 AM <dir> .ssh 01/03/2024 10:67 AM <dir> .ssh 01/03/2024 09:55 AM <dir> 3D 0bjects 01/03/2024 09:55 AM <dir> Desktop 01/03/2024 09:55 AM <dir> Documents 01/03/2024 09:55 AM <dir> Documents 01/03/2024 09:55 AM <dir> Documents 01/03/2024 09:55 AM <dir> Favorites 01/03/2024 09:55 AM <dir> Links 01/03/2024 09:55 AM <dir> Links 01/03/2024 09:55 AM <dir> Music 01/03/2024 09:55 AM <dir> Music 01/03/2024 09:55 AM <dir> Music 01/03/2024 09:55 AM <dir> Music 01/03/2024 09:55 AM <dir> Decuments 01/03/2024 09:55 AM <dir> Music 01/03/2024 09:55 AM <dir> Music</dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir></dir>			ConeDrive This PC 3D Objects Desktop Documents Downloads Music Pictures Videos Local Dick (C)			
01/03/2024 09:55 AM <0IR> Pictures 01/03/2024 09:55 AM <0IR> Saved Games 01/03/2024 09:55 AM <0IR> Searches 01/03/2024 09:55 AM <0IR> Videos 01/03/2024 10:49 AM <5YMLINKD> Wsa01 [D:\WSA_Logs\WSA01] ◀ 01/03/2024 10:35 AM <0IR> Wsa01 01/03/2024 10:35 AM <0IR> Wsa01 0 File(s) 0 bytes 18 Dir(s) 64,076,275,712 bytes free C:\>			Local Disk (C:) New Volume (D:) WSA_Logs VSA01 DVD Drive (E:) CPBA.; Network	٢		>

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: <u>mklink | Microsoft -</u> 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

Event Viewer							- 0	×
File Action View Help								
💠 🔿 🔁 📷 🖬 🖬								
Event Viewer (Local) Operat	tional Numb	er of events: 273 (!) New ev		Actions				
> Gustom Views	D	te and Time	Source	Event ID	Tack Category		Operational	
> Windows Logs	provation 1/	2/2024 4-25-19 DM	OpenSSH	Eventito	Nege		Open Swed Log	
Applications and Services Logs	ormation 1/	2/2024 4:25:15 PM	OpenSSH	4	None			
Internet Explorer	ormation 1/	2/2024 4:25:17 PM	OpenSSH	4	None		Create Custom View	
Key Management Service	ormation 1/	2/2024 4:25:17 PM	OpenSSH	4	None		Import Custom View	
> Microsoft	ormation 1/	2/2024 4:24:35 PM	OpenSSH	4	None		Clear Log	
✓ ☐ OpenSSH	ormation 1/	2/2024 4:24:17 PM	OpenSSH	4	None		Filter Current Log	
Admin () Info	ormation 1/	2/2024 4:24:17 PM	OpenSSH	4	None		Properties	
() Info	ormation 1/	2/2024 4:23:16 PM	OpenSSH	4	None		Dirable Log	
Windows PowerShell	ormation 1/	2/2024 4:23:16 PM	OpenSSH	4	None		Disable Log	
U Info	ormation 1/	2/2024 4:22:16 PM	OpenSSH	4	None		Find	
(i) Info	ormation 1/	2/2024 4:22:16 PM	OpenSSH	4	None		Save All Events As	
(i) Info	ormation 1/	2/2024 4:21:16 PM	OpenSSH	4	None		Attach a Task To this Log	
() Info	ormation 1/	2/2024 4:21:15 PM	OpenSSH	4	None		View	•
() Into	ormation 1/	2/2024 4:20:15 PM	OpenSSH	4	None		Defeath	
	ormation 1/	2/2024 4:20:15 PM	OpenSSH	4	None		Ci Kerresh	
() Infe	ormation 1/	2/2024 4:19:15 PM	OpenSSH	4	None		P Help	•
(i) Infe	ormation 1/	2/2024 4:18:19 PM	OpenSSH	4	None		Event 4, OpenSSH	
(i) Info	ormation 1/	2/2024 4:18:14 PM	OpenSSH	4	None		Event Properties	
(i) Info	ormation 1/	2/2024 4:17:14 PM	OpenSSH	4	None		Attack Task To This Grant	
(1) Info	ormation 1/	2/2024 4:17:14 PM	OpenSSH	4	None		Attach lask to This Event	
Black	armation 1/	2/2024 A-16-14 DM	U22aaaO		Nana	~	Сору	•
Event 4	4, OpenSSH					×	Save Selected Events	
Gen	tral Details						Refresh	
				<u>`</u>			Help	•
sst	nd: Connection	closed by 10.48.48.165 po	rt 48702 [preauth]	J				
Log	Name:	OpenSSH/Operational						
Sou	irce:	OpenSSH	Logged:	1/2/2024 4:25:18	PM			
Eve	nt ID:	4	Task Category:	None				
Lev	el:	Information	Keywords:					
Use	n	SYSTEM	Computer:	DESKTOP-MSQH	IP2U			
Opt	Code:	Info						
Mo	re Information:	Event Log Online Help						

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: 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>

Event Viewer (Local)	Event Viewer (Local) Operational Number of events: 212 (!) New events available										
 Event Viewer (Local) Event Viewer (Local) Quarter Views Applications and Services Logs Hardware Events Internet Explorer Key Management Service Microsoft OpenSSH Admin Operational Windows PowerShell Subscriptions 	Operational Numb Level Dr Information 1/ Information 1/ Information 1/ Information 1/ Information 1/ Information 1/ Information 1/ Event 4, OpenSSH General Details schd: Invalid user	er of events: 212 (!) New te and Time 2/2024 7:41:13 PM 2/2024 7:41:13 PM	events available Source OpenSSH OpenSSH OpenSSH OpenSSH OpenSSH OpenSSH OpenSSH OpenSSH OpenSSH	Event ID 4 4 4 4 4 4 4 4 4	Task Category None None None None None None	×	Actions Operational Image: Create Custom View Import Custom View Import Custom View Clear Log Filter Current Log Properties Disable Log Image: Find Attach a Task To this Log View Refresh Image: Help	•			
	Log Name: Source: Event ID: Level: User: OpCode: More Information:	OpenSSH/Operationa OpenSSH 4 Information SYSTEM Info <u>Event Log Online Hel</u>	l Logged: Task Category: Keywords: Computer: R	1/2/2024 7:41:13 None DESKTOP-MSQH	1PM 4P2U		Event 4, OpenSSH Event Properties Attach Task To This Event Save Selected Events Copy Refresh Help	•			

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:

- PW	o. ime	Source	Destination	Protocol	Lengt stream	Into
-	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
Т	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	<pre>0 Client: Protocol (SSH-2.0-OpenSSH_7.5 FreeBSD-20170903)</pre>
1	5 2024-01-03 13:42:47.590566	10.48.48.195	10.48.48.187	SSHv2	87	<pre>& Server: Protocol (SSH-2.0-OpenSSH_for_Windows_8.1)</pre>
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
1	7 2024-01-03 13:42:47.590801	10.48.48.187	10.48.48.195	SSHv2	1110	0 Client: Key Exchange Init
1	8 2024-01-03 13:42:47.633579	10.48.48.195	10.48.48.187	SSHv2	1102	Server: Key Exchange Init
1	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
1	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
Т	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
П	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:
1	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:
1	22 2024-01-03 13:42:47.732044	10.48.48.195	10.48.48.187	SSHv2	386	0 Server:
1	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
1	24 2024-01-03 13:42:47.734405	10.48.48.187	10.48.48.195	SSHv2	706	0 Client:
10	25 2024-01-03 13:42:47 760459	10.48.48.195	10.48.48.187	SSHv2	82	@ 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.