# نمآلا بيو زاهج يف SCP عفد تالجس نيوكت مداخ مادختساب

### تايوتحملا

<u>ةمدق مل ا</u>
<u>قي، س اس أل ا ت ابل طت مل ا</u>
<u>ةمدختسمل اتانبوكمل ا</u>
<u>SCP</u>
<u>SWA لچس يف كارتشال ا</u>
لچسل ا تافل م ةفش رأ
<u>ديعبانا مداخلنا عاليع SCP ربع ل چسانا دادرتسا نيوكت</u>
(GUI) قېموس،زل،ا مردختس،مل،ا قەچاۋ نىم دېغېل،ا SCP مداخ ىل،ا تال.چس,ل،ا ل،اس،زال، SWA نېيوكت
<u>ديعبل Microsoft Windows مِداخِك SCP المنعبوكت</u>
<u>SCP الجس عفد SCP الجس عفد SCP الجس عفد</u>
<u>امحال،صاو SCP لچس عفد ءاطخاً فاشكتساً</u>
<u>SWA يف تالجسلا ضرع SWA</u>
<u>SCP مداخ يف تال چس ل ا ض دع</u>
<u>فيضمل احات فم قيق حتا الشف</u>
<u>رجيتافملا قحول عم publicKey،password.password.interactive) نذالاا ضفر مت</u>
<u>القان ل شف SCP</u>
عجارمل

### ةمدقملا

يف ةدوجوملا تالجسلا خسنل "(SCP) نمآلا خسنلا" ةزيم نيوكت تاوطخ دنتسملا اذه فصي رخآ مداخ ىلإ ايئاقلت (SWA) نمآلا بيو زاهج.

# ةيساسألا تابلطتملا

### تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- .SCP لمع ةيفيك •
- ./اوس/ ەرادأ •
- . Linux وأ Microsoft Windows ليغشتلا ماظن ةرادإ

:كيدل نوكي نأب Cisco يصوت

• ةيضارتفالا وأ ةيداملا SWA تيبثت مت.

- ەتيبثت وأ صيخرتلا طيشنت مت.
- دادعإلا جلاعم لمتكا.
- ال (GUI) ةيموسرلا مدختسملا ةمجاو يلإ يرادإلا لوصولا (GUI) ما SWA.
- Microsoft Windows (لق ال ا ى ل ع) Windows Server 2019 وأ Windows (اطن وأ د) Windows (ال ا ى ل ع) Windows (ال ا Linux ل ت ب ث م ل

ةمدختسملا تانوكملا

ةنيعم ةيدام تانوكمو جمارب تارادصإ ىلع دنتسملا اذه رصتقي ال.

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

### SCP

يتأي يذلاو ،(RCP) دعب نع خسنلاا كولسل الثامم (SCP) نمآلا خسنلا لوكوتورب كولس دعي ، Berkeley ةعماجب ةصاخلا تاكبشلا تاقيبطت ةعومجم) Berkeley نم تاودأ ةعومجم نم .نامألا ريفوتل (SSH) نامألا ةقبط لوكوتورب ىلع دمتعي SCP لوكوتورب نأ ءانثتساب ضيوفتلاو ةقداصملا ضيوفت نيوكت SCP لوكوتورب بلطتي ،كلذ ىلإ ةفاضإلابو زايتمالا ىوتسم هيدل مدختسملا ناك اذإ ام ديدحت زاهجلل نكمي ثيوب (AAA) قبساحملاو حيحصلا

عفدب ايرود (SCP طغضل لداعملا) ديعبلا مداخلا بولسأب صاخلا SCP لوكوتورب موقي ةقيرطلا هذه بلطتت .ديعبلا SCP مداخ ىلإ نمآلا خسنلا لوكوتورب ةطساوب لجسلا تافلم مدختسم مسا كارتشالا بلطتي .SSH2 لوكوتوربب دوزم ديعب رتويبمك ىلع SSH SCP مداخ ىلإ ادانتسا لجسلا تافلم لقن متي .ديعبلا رتويبمكلا ىلع ةهجو ليلدو SSH حاتفمو .كلبق نم هنييعت مت هيجوت ةداعإ لودج

# SWA لجس يف كارتشالا

نمضتت .لجسلا تافلم نم عون لكل لجسلا تاكارتشا نم ديدعلا ءاشنإ كنكمي يلي ام كلذ يف امب ،نيزختلاو ةفشرألل نيوكتلا ليصافت تاكارتشالا:

- لجسلا تافلم ةفشرأ متت ىتم ددحت يتلاو ،يقوفلا رورملا تادادعا.
- اەتڧشٍرأ تمت يتلا تالجسلل طغضلا تادادعا •
- دق تالجسلا تناك اذا ام ددحت يتلاو ،اهتفشرأ تمت يتلا تالجسّلل دادرتّسالا تادادعًا زاهجلا ىلع اهنيزخت مت مأ ديعب مداخ ىلع اهتفشرأ تمت.

# لجسلا تافلم ةفشرأ

تافيشرأ موقت AsyncOS (قوف رورملا) لىجستب (قوف رورملا) حافيشرأ موقت تقولل ىصقألا دحلا وأ فلملا مجحل ىصقألا دحلل مدختسملا لبق نم نيعم دح ىلإ يلاحلا .ميجوت ةداعإ رخآ ذنم لجسلا تاكارتشا يف هذه فيشرألا تادادعإ نيمضت متي:

- فلملا مجح بسح ريرمتلا
- تقولا بسح بالقنا •
- لجسلا طغض •
- دادرتسالا ةقيرط •

.ايودي (يقوفلا رورملا) لجسلا تافلم ةفشرأ اضيأ كنكمي

.تاكارتشالا ليجست < ماظنلا ةرادإ رتخأ .1 ةوطخلا

ةناخ ددح وأ ،اەتڧشرأل لجسلا تاكارتشاب صاخلا رورملا دومع يڧ رايتخالا ةناخ ددح .2 ةوطخلا تاكارتشالا عيمج ديدحتل لكلا رايتخالا.

ةددحملا تالجسلا ةفشرأل نآلا هيجوت ةداعإ قوف رقنا. 3 ةوطخلا.

### 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	Ŵ	
amp_logs	AMP Engine Logs		amp_logs	None			Ŵ	
1	1							
scpal	Access Logs	SCP (	10.48.48.195:22)	None		Deanonymization	Ì	
shd_logs	SHD Logs	shd_	logs	None			ŵ	
sl_usercountd_logs	SL Usercount Logs	sl_u	usercountd_logs	None			ŵ	
smartlicense	Smartlicense Logs	smar	rtlicense	None		$\mathbf{i}$	ŵ	
snmp_logs	SNMP Logs	snmp	o_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	tem_logs	None			ŵ	
trafmon_errlogs	Traffic Monitor Error Logs	trafmon_errlogs		None			ŵ	
trafmonlogs	Traffic Monitor Logs	traf	fmonlogs	None			Ē	
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	o_logs	None			ŵ	
webcat_logs	Web Categorization Logs	webo	cat_logs	None			ŵ	
webrootlogs	Webroot Logs	webr	rootlogs	None			<u>ت</u>	
webtapd_logs	Webtapd Logs	webt	tapd_logs	None			Ŵ	
welcomeack_logs	Welcome Page Acknowledgement Logs	weld	comeack_logs	None			Ì	
						Rol	lover Now	

### ديعبلا مداخلا ىلع SCP ربع لجسلا دادرتسإ نيوكت

:SWA نم SCP مادختساب ديعب مداخ ىلإ لجسلا دادرتسإ نيكمتل ناتيسيئر ناتوطخ كانه

.تالجسلا عفدل SWA نيوكتب مق .1

2. تالجسلا يقلتل ديعبلا مداخلا نيوكتب مق.

مدختسملا المحاوية العام ديعبل المداخ المحالي المرال SWA تي وكت (GUI) المحافي (GUI) مداخ المحافي (GUI) المحافي (GUI) المحافي المحافي (GUI) المحافي المحافي المحافي المحافي المح

لجسلا تاكارتشا رتخأ ،ماظنلا ةرادإ نمو ،SWA ىلٍ لوخدلا ليجستب مق .1 ةوطخلا.

	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

تابلطتملا نم ققحتلل رمألا اذه ليغشتب مقو ( لوؤسمك ليغشت ) لوؤسملا تازايتماب ةيساسألا:

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

،Microsoft معد قيرف عم ققحت ،الإو .ةعباتملا كنكمي ،احيحص جارخإلا ناك اذإ

الوؤسمك ليغشت ) لوؤسملا زايتماب PowerShell مادختساب OpenSSH تيبثتل .18 ةوطخلا )، ليغشتب مق )،

# 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

قحجانلا جئاتنلا نم ةنيع يلي اميف:

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

PowerShell يف OpenSSH تيبثت -PowerShell



. Windows ليغشت ةداعإ ىجريف ،"باوص" ىلإ RestartNeeded نييعت مت اذإ :ريذحت

لضفت ،Microsoft Windows نم ىرخألاا تارادصإلاا ىلع تيبثتلاا لوح تامولعملاا نم ديزمل OpenSSH لنم ديزرل م<u>ادختسا عدب</u> :طابترالاا اذه قرايزب

ة العام الم جوز عاشنإب مقو (ةعوفرم ريغ) ةيداع PowerShell تسلج حتفا .19 قوطخلا RSA حيتافم نم جوز عاشنإب مقو (تعوفرم ريغ) الماج عيتافم نم جوز عاشنا

ssh-keygen -t RSA

.كب صاخلا مدختسملا فيرعت فلم ليلد أشنأ دق ssh. دلجم ىرت نأ كنكمي ،رمألا ءاهتنا دعب



RSA حاتفم ءاشنإ - ةروصلا

.( لوؤسمك ليغشت ) لوؤسملا زايتما مادختساب PowerShell نم SSH ةمدخ أدبا. 20 ةوطخلا

#### Start-Service sshd

،"يئاقلت" ىلإ ةمدخلا ليغشت ءدب عون رييغتب مق (ەب ىصوم نكلو يرايتخإ) .21 ةوطخلا، لوؤسمك ليغشت) لوؤسملا زايتما مادختساب.

Set-Service -Name sshd -StartupType 'Automatic'

### مت يذلا 22 TCP ذفنم ىلإ لوصولاب حامسلل ةيامحلا رادج ةدعاق ديكأتب مق .22 ةوطخلا مۇاشنا.

- 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 "
- Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and exists."
- }

يف programDataː\ssh\sshd\_config : يف دوجوملا SSH نيوكت فلم ريرحتب مق 23. ةوطخلا و RSA و RSA ل # ةلازاو ةركفملا

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

ناونع ،لاثملا اذه يف .programDataː\ssh\sshd\_config يف لاصتالا طورش ريرحت .24 ةوطخلا كميمصتل ارظن اهصيصخت كنكمي .تاهجاولا ناونع لكل وه ءاغصإلا.

Port 22 #AddressFamily any ListenAddress 0.0.0.0

```
فلملا ةياهن يف نيدنبلا نيذه ىلع ةمالع عضوب مق .25 ةوطخلا
:رطس لك ةيادب يف # ةفاضإب programData/\ssh\sshd_config/
```

# Match Group administrators
# AuthorizedKeysFile \_\_PROGRAMDATA\_\_/ssh/administrators\_authorized\_keys

يف ةمراصلا عاضوألا ريرحتب مق (يرايتخإ).26 ةوطخلا programData:/\ssh\sshd\_config، اذإ SSH حيتافم ىلإ ةدنتسملا ةقداصملا عنمو عضولا اذه نيكمت متي ،يضارتفا لكشب حيحص لكشب ةيمحم ةماعلاو ةصاخلا حيتافملا نكت مل.

StrictMode no: ىلإ ەرييغتو معن StrictMode# رطسلا ىلع قىلعتلا ءاغلإ

StrictModes No

ة قوطخلاا عام ب حامس ل programDataː\ssh\sshd\_config ي ا رطس ا اذه نم # قلاز إب مق 27. قوطخلا ماع ل ا حات ف مل

PubkeyAuthentication yes

يصن فلم ءاشنإ .28 ةوطخلا SWA ل ماعلا RSA حاتفم قصلو .ssh دلجم يف "RSA ل ماعل SWA ل ماعل (9 ةوطخلا يف معيمجت مت يذلا)

authorized_keys - Notepad		– 🗆 🛛		≂ i.ssh		-	пx
File Edit Format View Help			File H	lome Shar	e View		~ 🕐
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSDjM3Y/LifKnM1		^	4		lease \users and ach	~ 7.	Search reh 0
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSDjM3Y/LifKnM1 +dFBUnNISHGlJI H9+QhWV1gabIM +45jjUhx/kr7Vi +cxvq1lsNa83Wl ShyP9NUY85 root@WSA187.example.com		HGaYmlVYfiexJF r5NYoB+V6n9ek TYlXotT2yImUN6	<ul> <li>← → ~</li> <li>✓ Quick</li> <li>■ Desi</li> <li>↓ Dow</li> <li>☆ Doc</li> <li>○ Pict</li> <li>… ssh</li> <li>♪ Mus</li> <li> Vide</li> <li>● OneD</li> <li> This P</li> <li>→ Network</li> </ul>	top # mloads # uments # uments # ic os rive C	Isers/wsascp)ssh Name authorized_keys id_rsa id_rsa.pub	~ ð	Search .ssh $ ho$ D 1, 1, 1,
In 1 Cal 1	100% Windows (CPLE)	UTE-9	3 items	l item selected	406 bytes		) 
Ln I, Col I	100% windows (CRLF)	011-0	Sitems	inchi selecteu	to offer		Been of the

ماعلا SWA حاتفم - ةروصلا



ب ءاەتناو ssh-rsa نم اءدب ەلمكأب رطسلا خسنا :ةظحالم root@<your\_SWA\_hostname>



SSH-dss حاتفم قصل ىلإ ةجاح دجوت ال ،SCP مداخ ىلع RSA تيبثت ذنم :حيملت

لوؤسملا زايتما عم PowerShell يف "OpenSSH ةقداصم ليمع" نيكمتب مق 29. ةوطخلا (لوؤسمك ليغشت).

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> _
```

حوتفملا SSH ةقداصم ليكو نيكمت - ةروصلا

عاونأب حامسلل programDataː/\ssh\sshd\_config٪ ىلإ رطسلا اذه فضأ (يرايتخإ).30 ةوطخلا حيتافملا:

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

مادختساب PowerShell نم رمألا اذه مادختسإ كنكمي .SSH ةمدخ ليغشت ةداعإب مق .31 ةوطخلا ( لوؤسمك ليغشت ) لوؤسملا زايتما

restart-Service -Name sshd

تالجسلا ەيجوت ةداعإب مق ،حيحص لكشب ەنيوكت مت SCP عفد ناك اذإ ام رابتخال .32 ةوطخلا ةەجاو وأ (GUI) ةيموسرلا مدختسملا ةەجاو نم لك نم كلذب مايقلا كنكمي ،اەنيوكت مت يتلا رماوألا رطس

WSA\_CLI> rollovernow scpal



.scpal" وه لجسلا مسا ،لاثملا اذه يف :ةظحالم

لاثملا اذه يف ناك يذلاو ،فرعملا دلجملا ىلإ تالجسلا خسن ديكأت كنكمي c:/users/wsascp/wsa01

# فلتخم صارقأ كرحم ىلإ SCP تالجس عفد

دلجم نم طابترا ءاشناب مق ،:C ريغ رخآ صارقاً كرحم ىلإ تالجسلا عفد ىلإ ةجاحلا ةلاح يف ىلإ تالجسلا عفد متي ،لاثملا اذه يف .بوغرملا صارقالا كرحم ىلإ مدختسملا فيرعت فلم D:\WSA\_Logs\WSA01 .

- لاثملا اذه يف ،بوغرملا صارقألا كرحم يف تادلجملا ءاشنإب مق .1 ةوطخلا
- ( لوؤسمك ليغشت ) لوؤسملا زايتماب رماوأ هجوم حتف .2 ةوطخلا
- :طابترالا ءاشنإل رمألا اذه ليغشتب مق .3 ةوطخلا

#### mklink /d c:\users\wsascp\wsa01 D:\WSA\_Logs\WSA01

Select Administrator: Command Prompt	_		×	📙   🕑 📙 🖛   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 Shar	re View		~ <b>(</b> )
C:\>dir c:\Users\wsascp Volume in drive C has no label. Volume Cricit Newton in Data data				← → * ↑	NSA_Logs\WSA01 0	Search WSA01 Date modified	,0 Туре
Directory of c:\Users\wsascp				<ul> <li>OneDrive</li> </ul>	aclog.@20240103T111359.1.s	1/3/2024 10:52 AM	S File
01/03/2024 10:49 AM <0TR> . 01/03/2024 10:49 AM <0TR> 01/03/2024 10:07 AM <0TR> 01/03/2024 09:55 AM <0TR> 01/03/2024 09:55 AM <0TR> Contacts 01/03/2024 09:55 AM <0TR> Desktop 01/03/2024 09:55 AM <0TR> Documents 01/03/2024 09:55 AM <0TR> Documents 01/03/2024 09:55 AM <0TR> Downloads 01/03/2024 09:55 AM <0TR> Elinks 01/03/2024 09:55 AM <0TR> Links 01/03/2024 09:55 AM <0TR> Music 01/03/2024 09:55 AM <0TR> Music 01/03/2024 09:55 AM <0TR> Music 01/03/2024 09:55 AM <0TR> Music 01/03/2024 09:55 AM <0TR> Saved Games 01/03/2024 09:55 AM <0TR> Saved Games 01/03/2024 09:55 AM <0TR> Saved Games 01/03/2024 09:55 AM <0TR> Videos 01/03/2024 10:35 AM <0TR> Saved Games 01/03/2024 10:35 AM <0TR> Sav				This PC  3 D Objects Desktop Documents Documents Downloads Music Pictures Videos Local Disk (C:) New Volume (D:) WSA_Logs WSA01 DVD Drive (E:) CPB:	À		
C:\>			v	Network 1 item	¢		>

SYM طابترإ ءاشنإ - ةروص



يف WSA01 دلجم ىلإ تالجسلا عفدل SWA نيوكت متي ،لاثملا اذه يف :ةظحالم C:\Users\wsascp ، ىل يزمر طابتراك WSA01 دلجملا D:\WSA\_Logs\WSA01

<u>mklink | Microsoft Learn</u> : عقوملا ةرايز ىجري ،Microsoft Symbol Link لوح تامولعملا نم ديزملل

### اهحالصإو SCP لجس عفد ءاطخأ فاشكتسأ

### SWA يف تالجسلا ضرع

:يف ءاطخألا نم قرقحت ،امحالصإو SCP لجس عفد ةيلمع ءاطخأ فاشكتسال

1. CLI (رماوألا رطس ةەجاو) > Displayalerts

2. System\_log



مقرلا رايتخاو ،CLI يف GREP رمأ مادختسإ كنكمي ،system\_log ةءارقل :ةظحالم جلاعملا يف لاؤسلا ىلع ةباجإلاو system\_log ب طبترملا.

### SCP مداخ يف تالجسلا ضرع

< تامدخلاو تاقيبطتلا تالجس يف Microsoft ثادحأ ضراع يف SCP مداخ تالجس ةءارق كنكمي OpenSSH ليغشتلا ديق < OpenSSH

Event Viewer (Local) Operational Number of events: 273 (!) New events available Actions
Custom Views
Applications and Service Log.   Open Saved Log.  Open Sav
Create Custom View     Create Custom View
internet Explorer III Information 1/2/2024 4:25:17 PM OpenSSH 4 None
Key Management Service
Microsoft [] Information 1/2/2024 4:24:35 PM OpenSSH 4 None Clear Log
(v ≧ OpenSSH         4 None         ▼ Filter Current Log
Admin I/2/2024 4:24:17 PM OpenSSH 4 None Properties
Operational     Operation     Operation     Operational     Operational     Operational
windows Powersneii Uinformation 1/2/2024 4:23:16 PM OpenSSH 4 None On the Cog
The subscriptions 1/2/2024 4:22:16 PM OpenSSH 4 None Find
Dinformation 1/2/2024 4:22:16 PM OpenSSH 4 None Save All Events As
Unformation 1/2/2024 4:21:16 PM OpenSSH 4 None Attach a Task To this Log
Unformation 1/2/2024 4:21:15 PM OpenSSH 4 None View
Unformation 1/2/2024 4:20:15 PM OpenSSH 4 None
Unformation 1/2/2024 42:0:15 PM OpenSSH 4 None G Kerresh
Uniformation 1/2/2024 419:15 PM OpenSSH 4 None 2 Help
Uniformation 1/2/2024 419:15 PM OpenSSH 4 None Event 4 OpenSSH
Uniformation 1/2/2024 416:14 PM OpenSSH 4 None
Uniformation 1/2/2024 41/214 PM OpenSSH 4 None E EVENt Properties
Continuation 1/2/2004 41714 PM OpenSSH 4 None
Copy
Event 4 OpenSSH 🗙 🕞 Save Selected Events
Reference State St
General Details
I Help
sshd: Connection closed by 10.48.48.165 port 48702 [preauth]
Log Name: OpenSSH/Operational
Source: OpenSSH Logged: 1/2/2024 4:25:18 PM
Event ID: 4 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-MSQHP2U
OpCode: Info
More Information: Event Log Online Help

PreAuth لشف - ةروصلا

### فيضملا حاتفم نم ققحتلا لشف

.حلاص ريغ SWA يف نزخملا SCP مداخل ماعلا حاتفملا نأ ىلٍ أطخلا اذه ريشي

DisplayAlerts جارخإ نم أطخلا نم ةنيع انه CLI: يف

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 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 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.

: system\_log يف أطخلا نم ةنيع يلي اميف

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

يف كارتشالاا ةحفص يف ەقصلو SCP مداخ نم فيضملا خسن كنكمي ،ةلكشملا ەذە لحل تالجس SCP.

اعيطتسي تنأ وأ GUI نم ديعب لدان SCP ىل log لا لسري نأ SWA لكشي يف 7 ةوطخ تلحأ فلخلا نم حاتفم فيضملا ليزي نأ cisco TAC تلصتا.

(حيتافملا ةحول عم publicKey،password،password،interactive) نذإلا ضفر مت

.حلاص ريغ SWA يف رفوتملا مدختسملا مسا نأ ىلإ ةداع أطخلا اذه ريشي.

: system\_log يف ءاطخاُلا ليجست نم ةنيع يلي اميف

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

نم أطخلاا نم ةنيع انه SCP ءانيم <swa\_ip address> نم SCP حلاص ريغ مدختسم :لدان SCP نم أطخلاا نم ةنيع انه حلدان SVA يلإ طبري SVA ءانيم

Event Viewer							-	
File Action View Help								
🔶 🔿 🚾 🖬 🖬								
Event Viewer (Local)	Operational Numb	er of events: 212 (!) New ever	nts available			/	Actions	
> Gustom Views	Level D	ate and Time So	ource	Event ID	Task Category	~	Operational	
> Windows Logs	(i)Information 1	/2/2024 7-41-13 PM	nenSSH	4	None		Open Saved Log	
Hardware Events	Information 1	/2/2024 7:41:13 PM O	nenSSH	4	None		Contra Contem Minu	
Internet Explorer	Information 1	/2/2024 7:41:13 PM O	penSSH	4	None		Create Custom view	
Key Management Service	(i) Information 1	/2/2024 7:41:13 PM O	penSSH	4	None		Import Custom View	
> 🧮 Microsoft	(i) Information 1	/2/2024 7:41:13 PM O	penSSH	4	None		Clear Log	
✓ ☐ OpenSSH	Information 1	/2/2024 7:41:13 PM O	penSSH	4	None		Filter Current Log	
Admin Admin	(i) Information 1	/2/2024 7:41:13 PM O	penSSH	4	None	1	Properties	
Operational	(i) Information 1	/2/2024 7:41:13 PM O	penSSH	4	None	v   6	Properties	
Windows PowerShell							Disable Log	
5 Subscriptions	Event 4, OpenSSH					(	Find	
	General Details					1	Save All Events As	
	Cetons						Attach a Task To this Log	
Isshd: Invalid user scp from 10.48.48.165 port 63177							Man	
							View	,
							Q Refresh	
							Help	•
							Event 4, OpenSSH	-
						1	Event Properties	
						1	Attach Task To This Event	
							Save Selected Events	
							a save selected Events	
							🚡 Сору	,
	Les Neuer	0				1	G Refresh	
	Log Name:	OpenSSH/Operational					7 Help	•
	Source:	OpenSSH	Logged:	1/2/2024 /:41:13	PM			
	Event ID:	4	Task Category:	None				
	Level:	Information	Keywords:					
	User:	SYSTEM	Computer:	DESKTOP-MSQH	IP2U			
	OpCode:	Info						
	More Information	Event Log Online Help						
	-							

حلاص ريغ مدختسم -ةروص

مت يذلا) مدختسملا نيكمت نم ققحتلاو ءالمإلا ةحص نم ققحتلا ءاجرلا ،أطخلا اذه لحل يف هنيوكت SCP. مداخ يف (تالجسلا ىلع طغضلل SWA يف هنيوكت

ليلدلا وأ فلملا اذه لثم دجوي ال

،حلاص ريغ SWA تالجس كارتشا مسق يف رفوتملا راسملا نأ ىلإ أطخلا اذه ريشي.

system\_log: نم أطخلا نم ةنيع يلي اميف

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

. SCP مداخ يف ەتيحالصو راسملا ةحص نم دكأتو ءالمإلا ةحص نم ققحت ،ةلكشملا ەذە لحل

SCP لقن لشف

:أطخلا لاثم انه .لاصتالا يف أطخل ارشؤم أطخلا اذه نوكي دق

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

ل (CLI) رماوألا رطس ةهجاو يف telnet رمألا مدختسأ ،اهحالصإو لااصتالا ءاطخأ فاشكتسال 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...

لثم جراخ حجانلاا لاصتالا. لاصتالا ءاشنا متي مل ،لاثملا اذه يف:

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

الصتم Telnet جمانرب نكي مل اذإ:

لوصولا عنمي SCP مداخ ةيامح رادج ناك اذإ امم قرقحت [1].

.لوصولا عنمي يذلا SCP مداخ ىلإ SWA نم راسملا يف ةيامح ناردج يأ دوجو نم ققحت [2]

. SCP مداخ يف عامتسإ ةلاح يف TCP 22 ذفنم ناك اذإ امم قرقحت [3]

.ليلحتلا نم ديزم ىلع لوصحلل SWA SCP مداخ نم لك يف ةمزحلا طاقتلا ليغشتب مق [4]

حجانلا لاصتالا ةمزح طاقتلا نم ةنيع يلي اميف:

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] Seg=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] Seg=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] Seg=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:

حاجنب لاصتالا ةمزح طاقتلا - ةروصلا

# عجارملا

<u>Cisco - Cisco نم بيول نامأ ةزهجأ تاسرامم لضفأ تاداشرا</u>

BRKSEC-3303 (ciscolive)

<u>- (ماعلا رشنال) AsyncOS 14.5 U Cisco Secure Web Appliance - GD (ماعلا رشنال) - (ماعلا رشنال) (Cisco Secure Web Appliance] - Cisco</u>

<u>OpenSSH ل Windows | Microsoft Learn مادختس| ءدب</u>

<u>كاتفم ققداصم نيوكت SSH ليغشتلا ماظن لصو قحول Windows يلع ماعل SSH حاتفم ققداصم نيوكت (woshub.com</u>

<u>OpenSSH ل Windows | Microsoft Learn يف حيتافملا ىل قدنتسملا ةقداصملا</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما