

Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[SCP](#)

[Inscrição de log SWA](#)

[Arquivando Arquivos de Log](#)

[Configurar LogRetrieval via SCP no Servidor Remoto](#)

[Configurar o SWA para enviar os logs para o servidor remoto SCP a partir da GUI](#)

[Configurar o Microsoft Windows como Servidor Remoto SCP](#)

[Enviar Logs SCP por Push para um Drive Diferente](#)

[Solucionar problemas de envio de log SCP](#)

[Exibir Logs em SWA](#)

[Exibir logs no servidor SCP](#)

[Falha na verificação da chave de host](#)

[Permissão negada \(chave pública, senha, teclado interativo\)](#)

[Falha do SCP ao transferir](#)

[Referências](#)

Introdução

Este documento descreve as etapas para configurar o Secure Copy (SCP) para copiar automaticamente logs no Secure Web Appliance (SWA) para outro servidor.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como a SCP funciona.
- Administração SWA.
- Administração do sistema operacional Microsoft Windows ou Linux.

A Cisco recomenda que você:

- SWA físico ou virtual instalado.

- Licença ativada ou instalada.
- O assistente de instalação foi concluído.

- Acesso administrativo à interface gráfica do usuário (GUI) do SWA.
- Microsoft Windows (no mínimo Windows Server 2019 ou Windows 10 (build 1809).) ou sistema Linux instalado.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

SCP

O comportamento do Secure Copy (SCP) é semelhante ao do Remote Copy (RCP), que vem do conjunto de ferramentas `r` de Berkeley (conjunto próprio de aplicativos de rede da universidade de Berkeley), exceto que o SCP depende do Secure Shell (SSH) para segurança. Além disso, o SCP exige que a autorização de autenticação, autorização e contabilização (AAA) seja configurada para que o dispositivo possa determinar se o usuário tem o nível de privilégio correto

O método SCP no servidor remoto (equivalente ao SCP Push) envia periodicamente arquivos de log pelo protocolo de cópia segura para um servidor SCP remoto. Este método requer um servidor SSH SCP em um computador remoto com o protocolo SSH2. A assinatura requer um nome de usuário, uma chave SSH e um diretório de destino no computador remoto. Os arquivos de log são transferidos com base em uma programação de transferência definida por você.

Inscrição de log SWA

Você pode criar várias inscrições de log para cada tipo de arquivo de log. As assinaturas incluem detalhes de configuração para arquivamento e armazenamento, incluindo:

- Configurações de sobreposição, que determinam quando os arquivos de log são arquivados.
- Configurações de compactação para logs arquivados.
- Configurações de recuperação para logs arquivados, que especificam se os logs são arquivados em um servidor remoto ou armazenados no equipamento.

Arquivando Arquivos de Log

O AsyncOS arquiva (faz rollover) assinaturas de log quando um arquivo de log atual atinge um limite especificado pelo usuário de tamanho máximo de arquivo ou tempo máximo desde a última rollover.

Estas configurações de arquivamento estão incluídas nas inscrições de log:

- Sobreposição por tamanho de arquivo
- Sobreposição por Tempo
- Compactação de log
- Método de Recuperação

Você também pode arquivar manualmente (rolover) arquivos de log.

Etapa 1. Escolha System Administration > Log Subscriptions.

Etapa 2. Marque a caixa de seleção na coluna Sobreposição das assinaturas de log para arquivamento ou marque a caixa de seleção Todas para selecionar todas as assinaturas.

Etapa 3 .Clique em Rollover Now para arquivar os logs selecionados.

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](#)

Configurar recuperação de log via SCP no servidor remoto

Há duas etapas principais para a recuperação de logs em um servidor remoto com SCP do SWA:

1. Configure o SWA para enviar os logs.
2. Configure o servidor remoto para receber os logs.

Configurar o SWA para enviar os logs para o servidor remoto SCP a partir da GUI

Etapa 1. Faça login no SWA e, em Administração do sistema, escolha Inscrições de log.

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

System Time

Time Zone

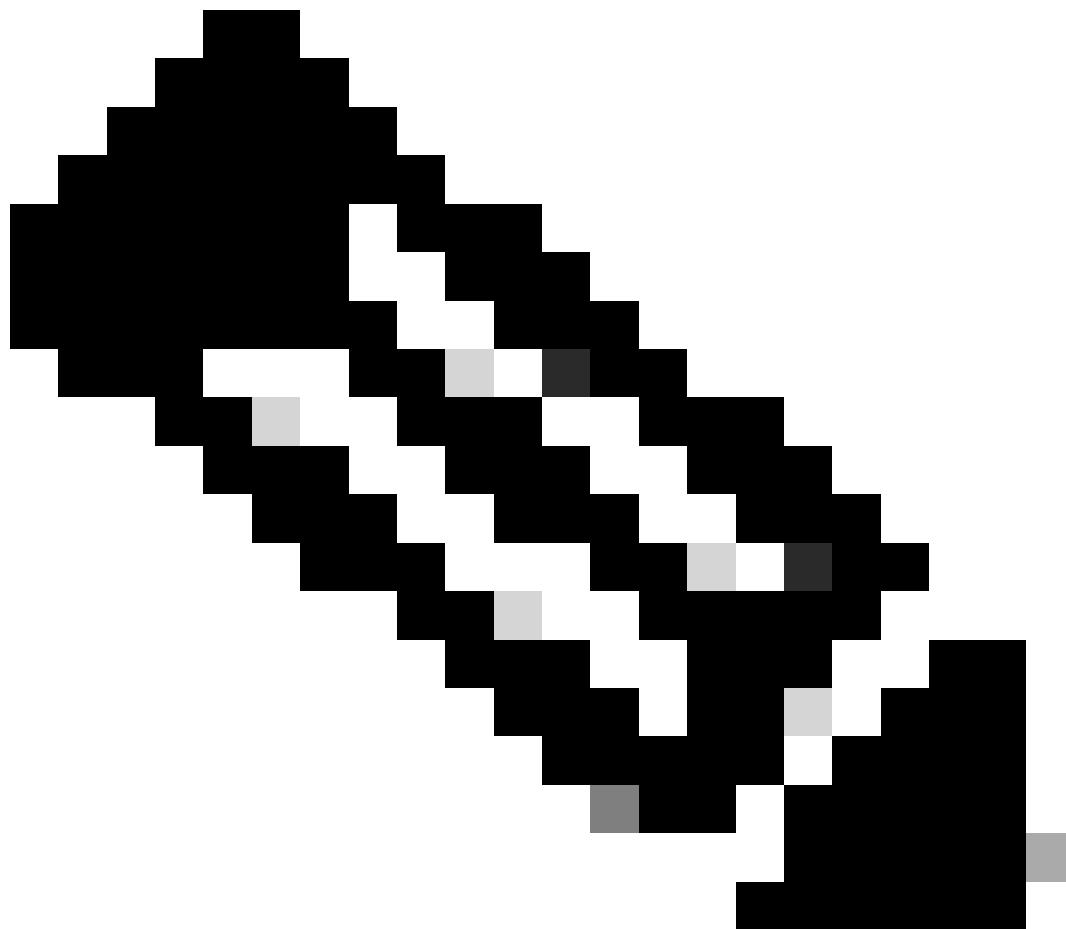
Time Settings

Configuration

Configuration Summary

Configuration File

Salve a chave SSH em um arquivo de texto para uso posterior na seção de configuração do servidor SCP remoto.



Observação: você precisa copiar as duas linhas, começando com ssh- e terminando com 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:

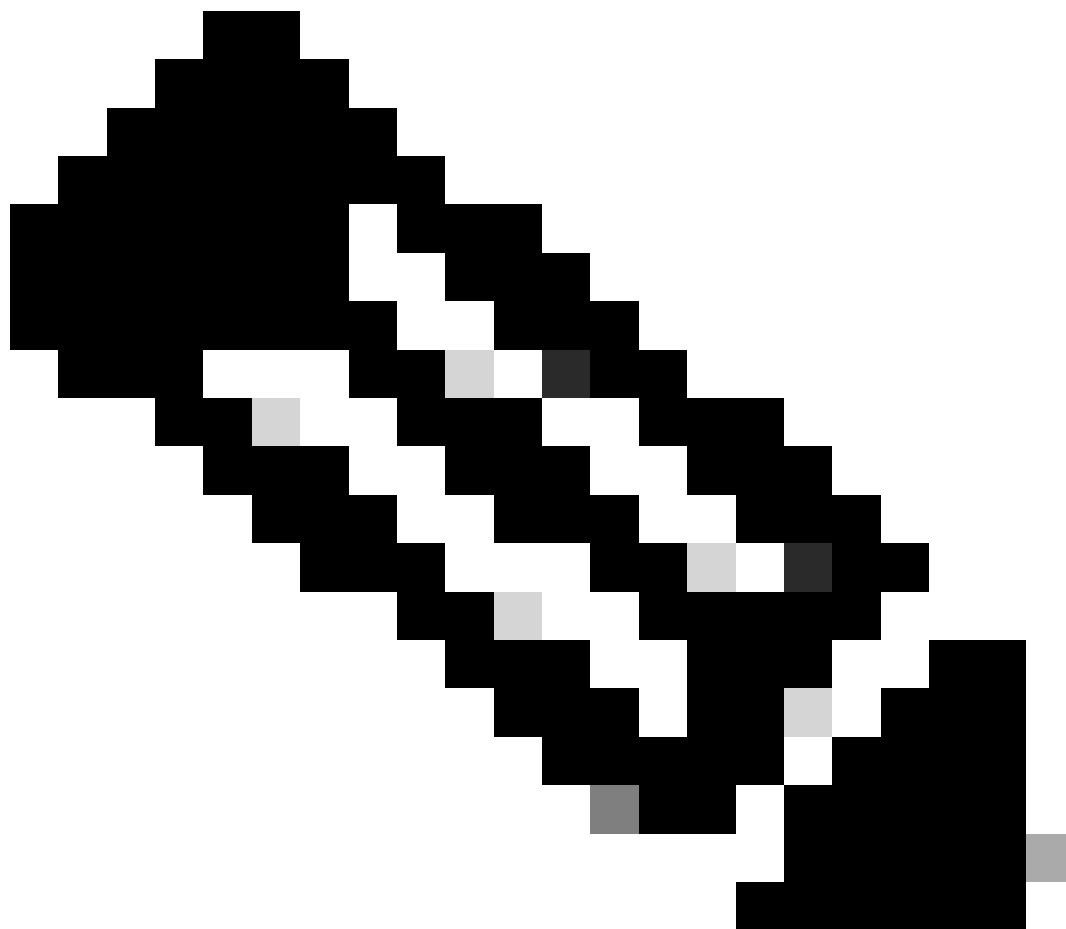
```
ssh-dss  
AAAAB3NzaC1kc3MAAACBAOuNX6TUOmzIWolPkVQ5I7LC/9yv:  
root@122[REDACTED]le.com  
  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACwbJziB4AE7H
```

Imagem - Salve a chave SSH para uso posterior.

Etapa 10. Confirmar alterações.

Configurar o Microsoft Windows como Servidor Remoto SCP

Etapa 10. Para criar um usuário para o serviço SCP, vá até Gerenciamento do Computador:



Observação: se você já tiver um usuário para SCP, vá para a Etapa 16.

Etapa 11. Selecione Usuários locais e grupo e escolha Usuários no painel esquerdo.

Etapa 12. Clique com o botão direito do mouse na página principal e escolha novo usuário.

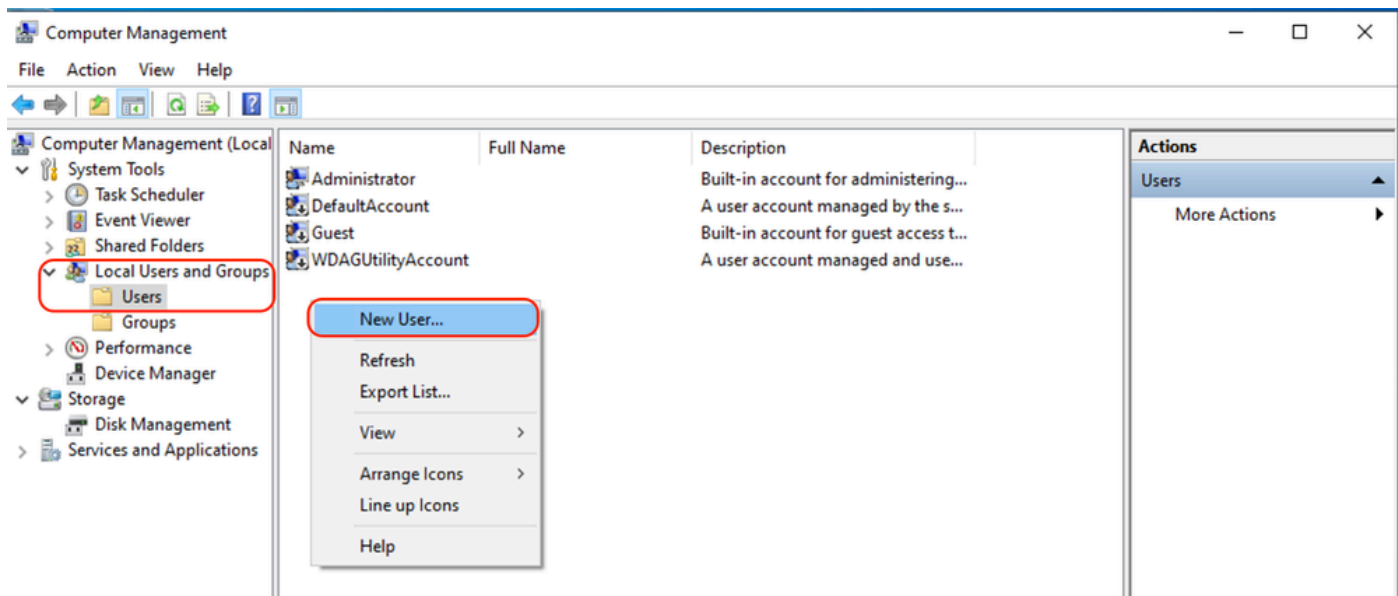


Imagem - Criar um usuário para o serviço SCP.

Etapa 13. Digite o nome de usuário e a senha desejada.

Etapa 14. Escolha Password Never Expired.

Etapa 15. Clique em Criar e feche a janela.

New User

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

Imagem - Insira as informações do novo usuário.

Etapa 16. Faça login no servidor SCP Remoto com o usuário recém-criado para que o diretório de perfil seja criado.



Observação: se você tiver o OpenSSL instalado em seu servidor SCP Remoto, vá para a etapa 19.

Etapa 17. Abra o PowerShell com privilégios de Administrador (Executar como Administrador) e execute este comando para verificar os pré-requisitos:

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

Se a saída for True, você poderá continuar. Caso contrário, verifique com a equipe de suporte da Microsoft,

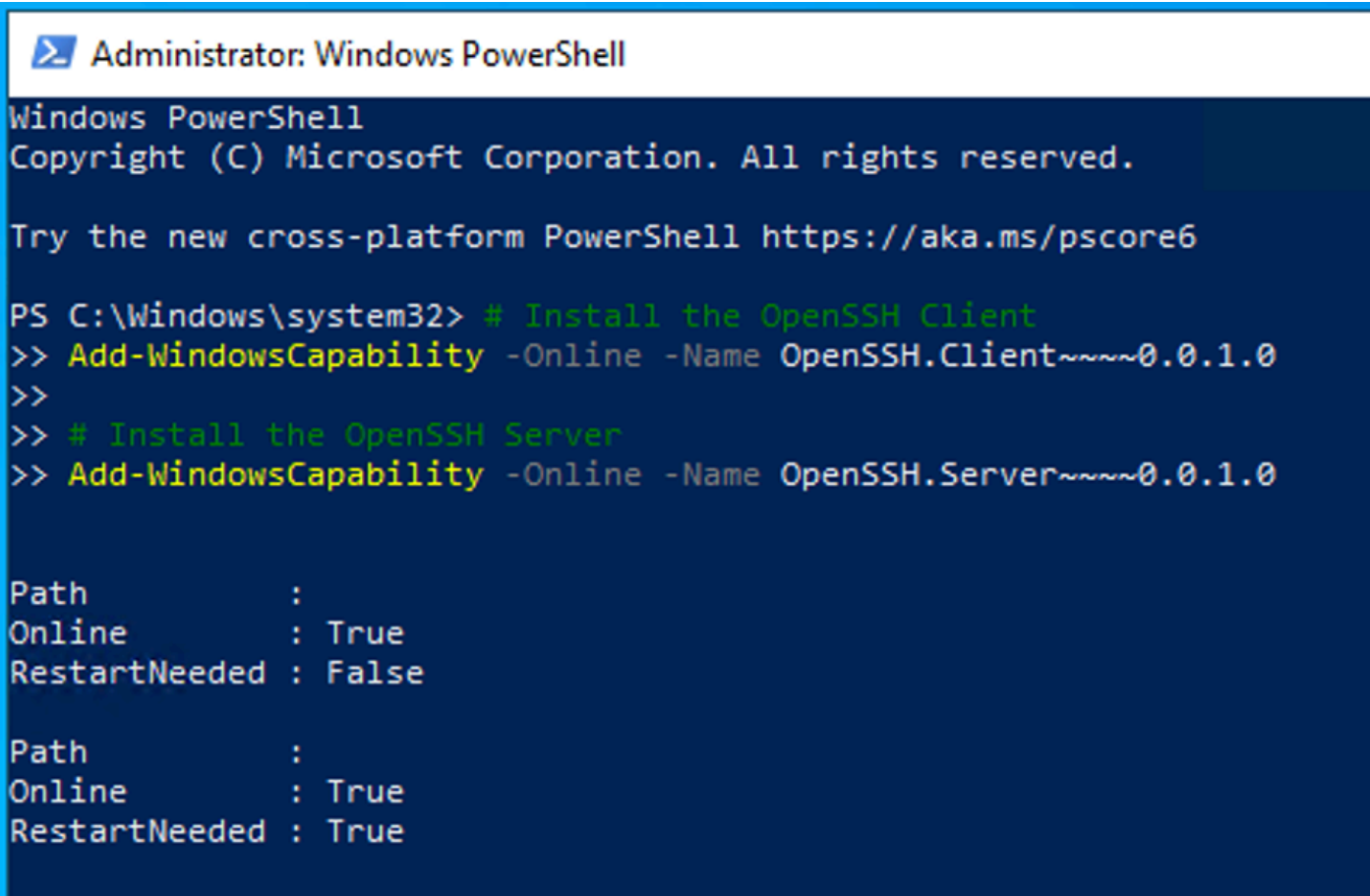
Etapa 18. Para instalar o OpenSSH usando o PowerShell com privilégio de Administrador (Executar como Administrador), execute :

```
# 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
```

Aqui está um exemplo de resultados bem-sucedidos:

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

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of two commands to install OpenSSH capabilities. The first command, `Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0`, is followed by a prompt for the output: `Path : Online : True RestartNeeded : False`. The second command, `Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0`, is followed by a prompt for the output: `Path : Online : True RestartNeeded : True`. The terminal background is dark blue with white text, and the command text is highlighted in green and yellow.

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

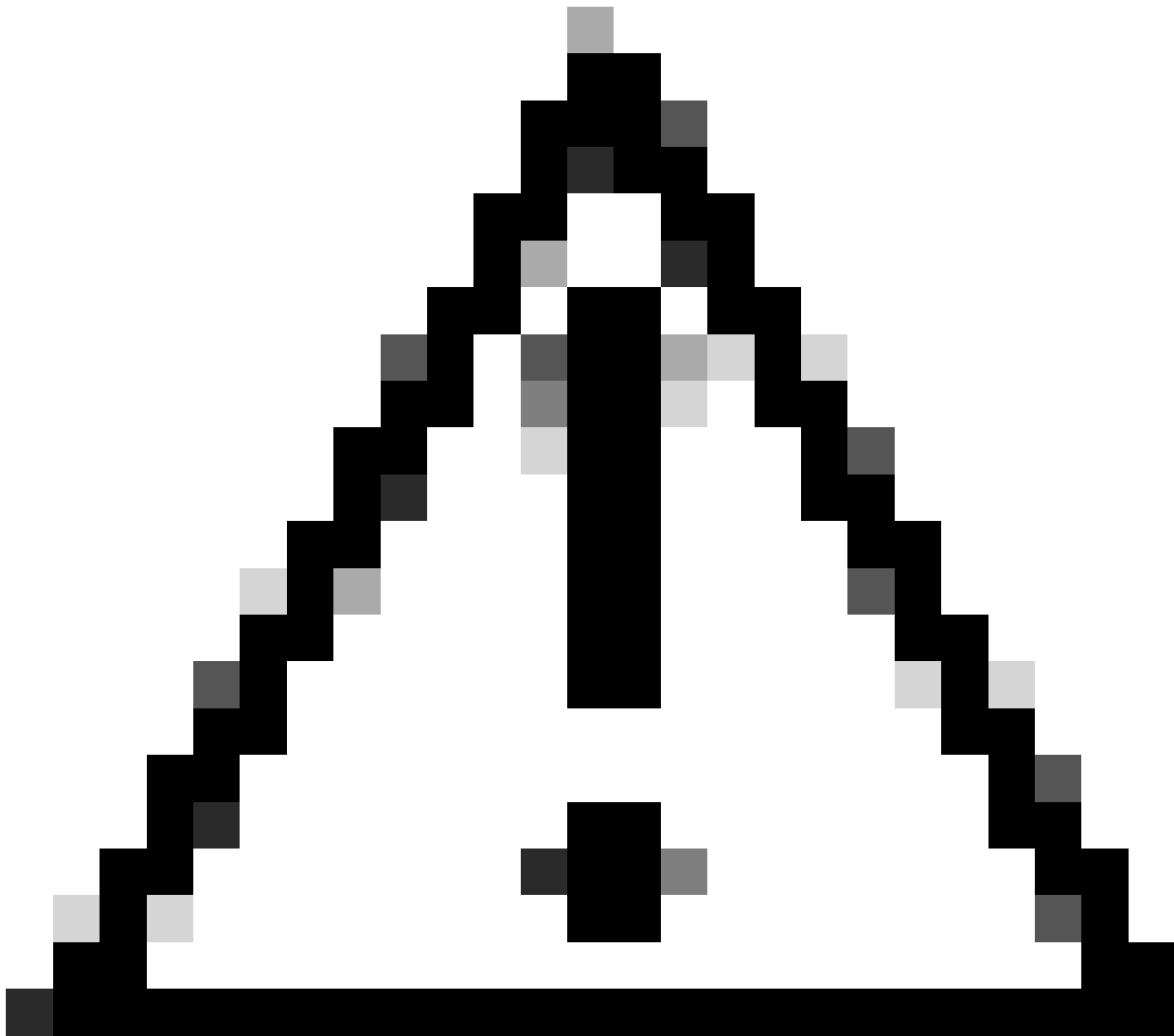
Try the new cross-platform PowerShell https://aka.ms/pscore6

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
```

Imagem - Instalar o OpenSSH no PowerShell



Cuidado: se RestartNeeded estiver definido como True, reinicialize o Windows .

Para obter mais informações sobre a instalação em outras versões do Microsoft Windows, visite este link: [Introdução ao OpenSSH para Windows | Aprender da Microsoft](#)

Etapa 19. Abra uma sessão normal (não elevada) do PowerShell e gere um par de chaves RSA usando o comando:

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

Após a conclusão do comando, você poderá ver que a pasta `.ssh` criou seu diretório de perfil de usuário.

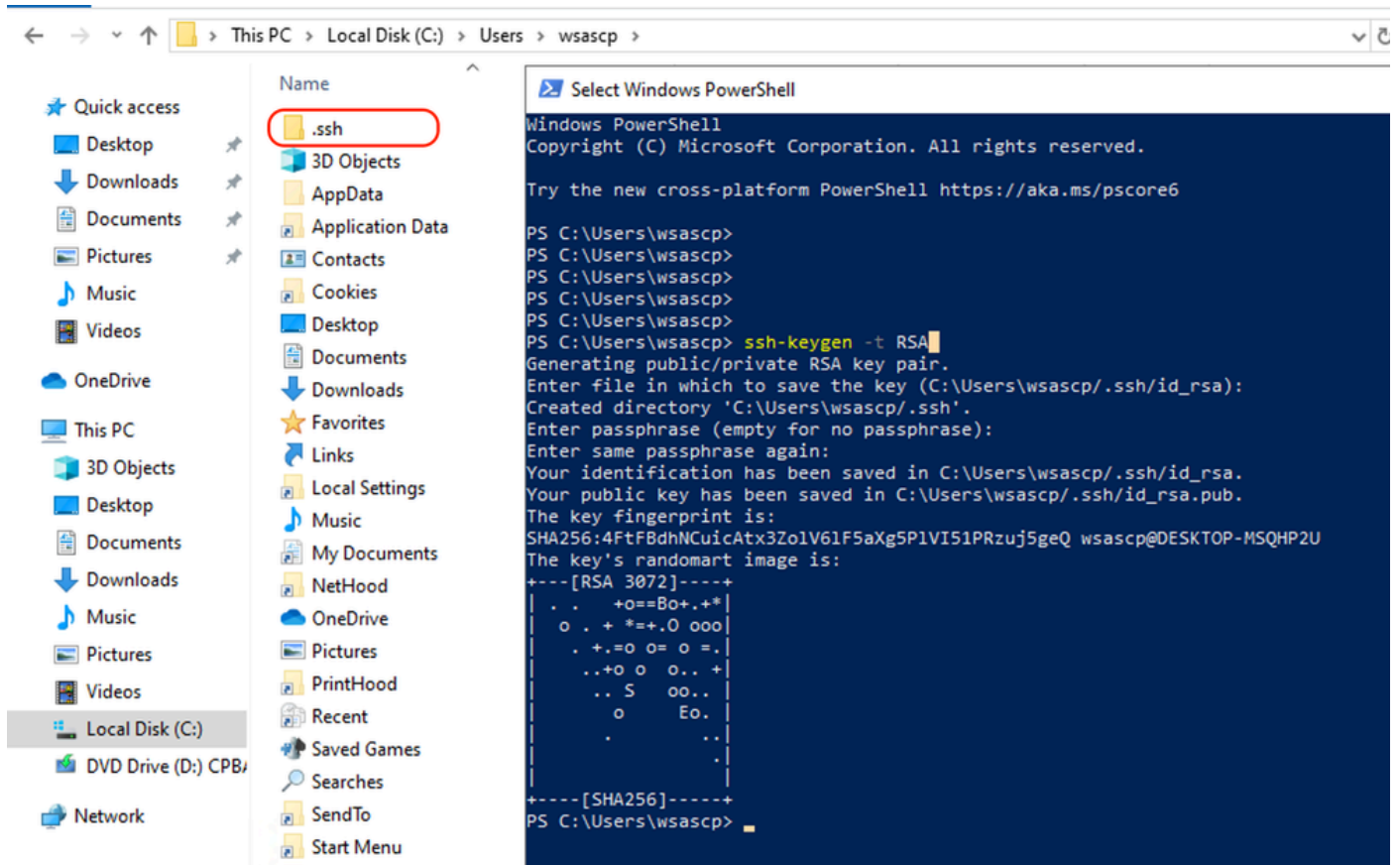


Imagem - Gerar chave RSA

Etapa 20. Inicie o serviço SSH do PowerShell com privilégio de Administrador (Executar como Administrador).

```
Start-Service sshd
```

Etapa 21. (Opcional, mas recomendado) Alterar o tipo de inicialização do serviço para Automático, com privilégio de Administrador (Executar como Administrador).

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

Etapa 22. Confirme se a regra de firewall para permitir o acesso à porta TCP 22 foi criada.

```
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."
}
```

Etapa 23. Edite o arquivo de configuração SSH localizado em : %programdata%\ssh\sshd_config no bloco de notas e remova o # para RSA e DSA.

```
HostKey __PROGRAMDATA__/ssh/ssh_host_rsa_key
HostKey __PROGRAMDATA__/ssh/ssh_host_dsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ecdsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ed25519_key
```

Etapa 24. Edite as condições de conexão em %programdata%\ssh\sshd_config. Neste exemplo, o endereço de escuta é para todos os endereços de interfaces. Você pode personalizá-lo devido ao seu design.

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

Etapa 25. Marque essas duas linhas no final do %programdata%\ssh\sshd_config adicionando # no início de cada linha:

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

Etapa 26.(Opcional) Edite os Modos Estritos em %programdata%\ssh\sshd_config. Por padrão, esse modo está habilitado e impede a autenticação baseada em chave SSH se as chaves privadas e públicas não estiverem adequadamente protegidas.

Descomente a linha #StrictModes sim e altere-a para StrictModes no:

```
StrictModes No
```

Etapa 27. Remova o #desta linha para %programdata%\ssh\sshd_config para permitir a autenticação de chave pública

```
PubkeyAuthentication yes
```

Etapa 28. Crie um arquivo de texto "authorized_keys" na pasta .ssh e cole a chave RSA pública

do SWA (que foi coletada na etapa 9)

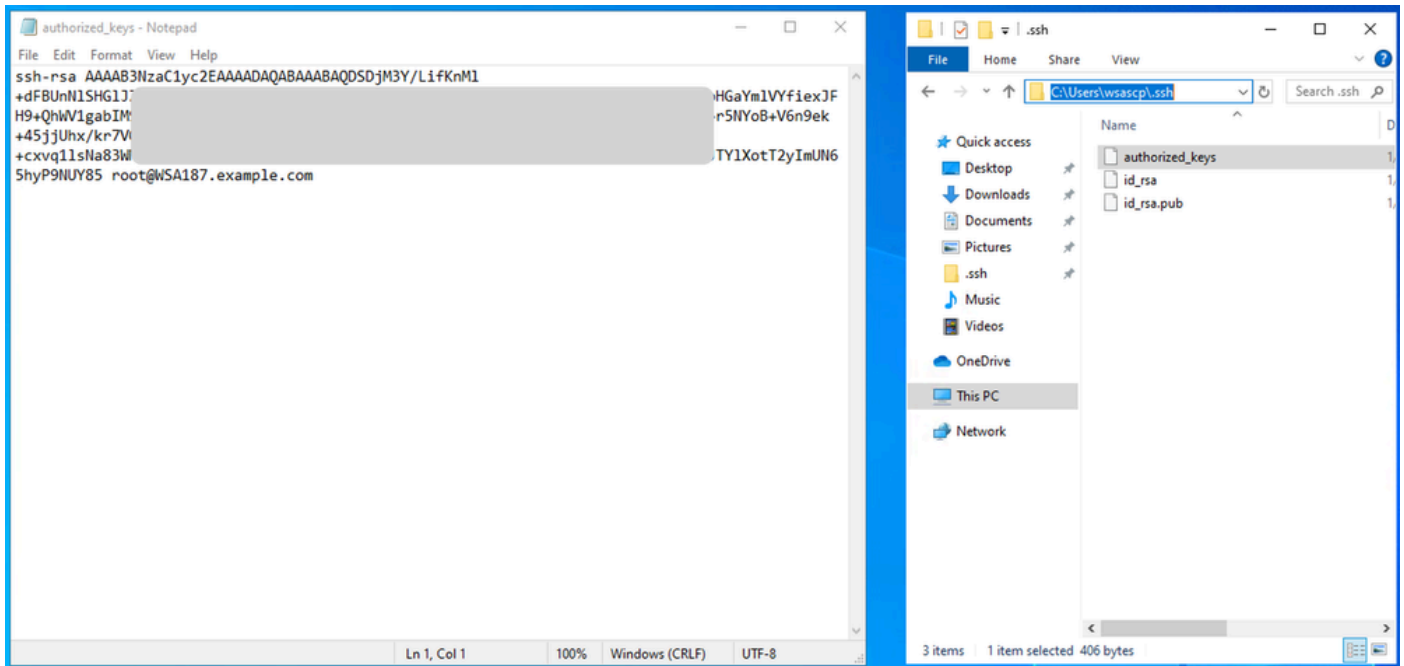
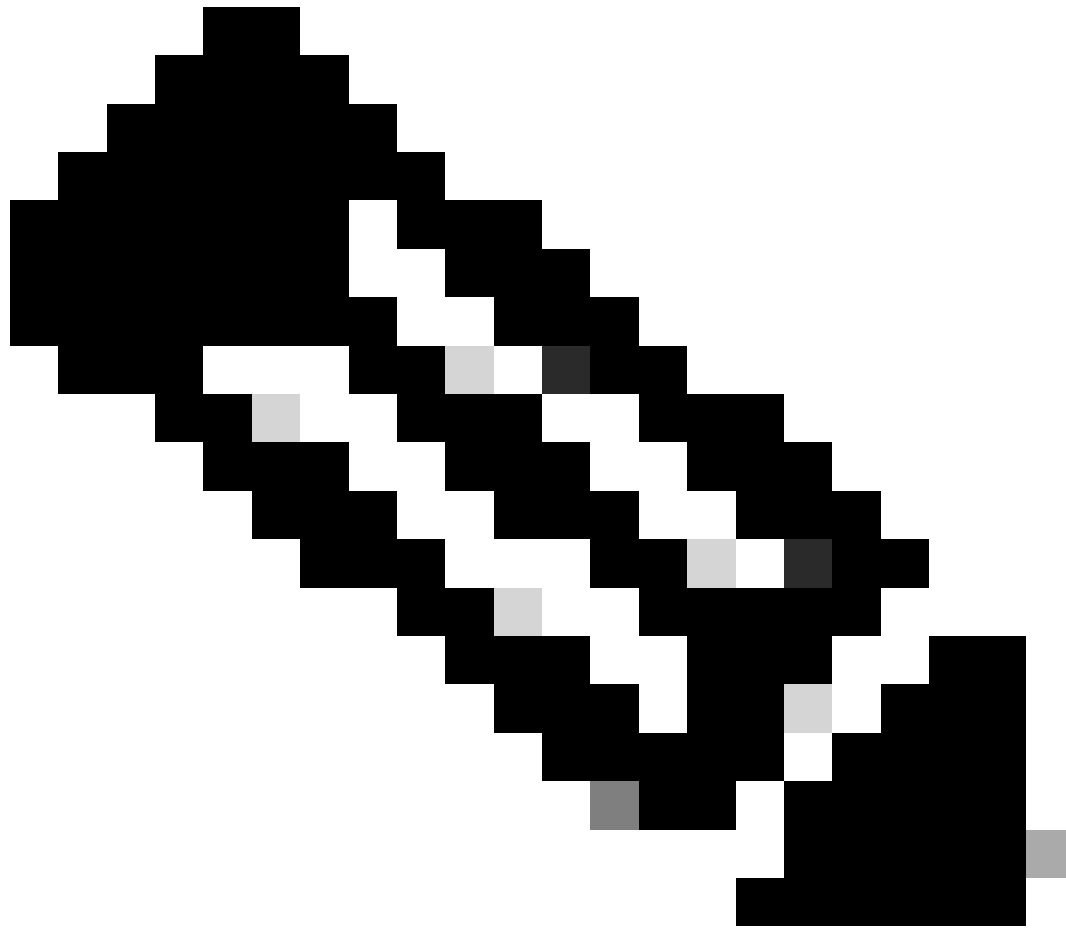
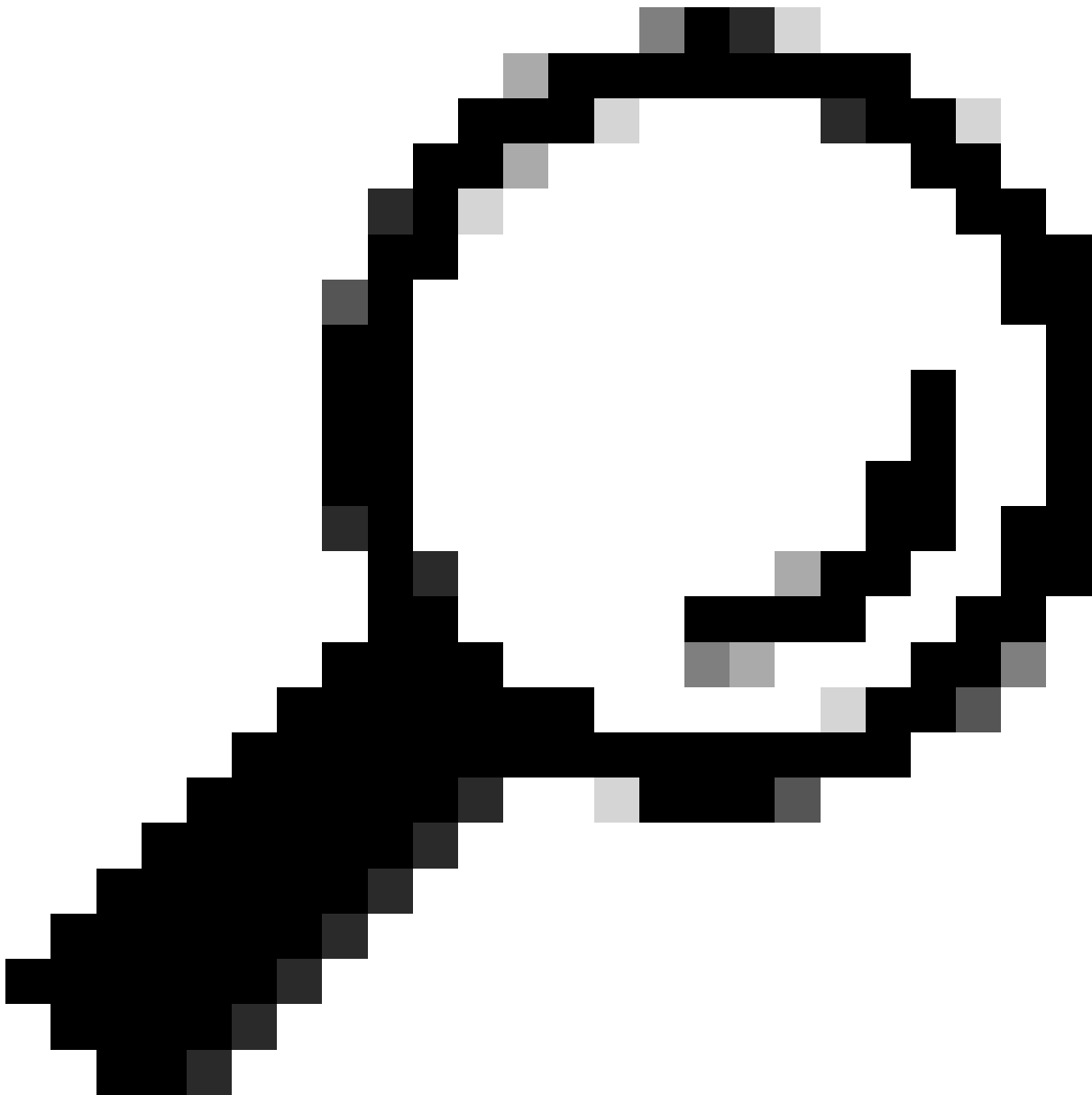


Imagem - Chave pública SWA



Observação: copie a linha inteira começando com ssh-rsa e terminando com root@<your_SWA_hostname>



Dica: como o RSA está instalado no servidor SCP, não há necessidade de colar a chave ssh-dss

Etapa 29. Habilite o "OpenSSH Authentication Agent" no PowerShell com privilégio de Administrador (Executar como Administrador).

```
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> █
```

Imagem - Habilitar o Open SSH Authentication Agent

Etapa 30.(Opcional) Adicione esta linha a %programdata%\ssh\sshd_config para permitir tipos de chave:

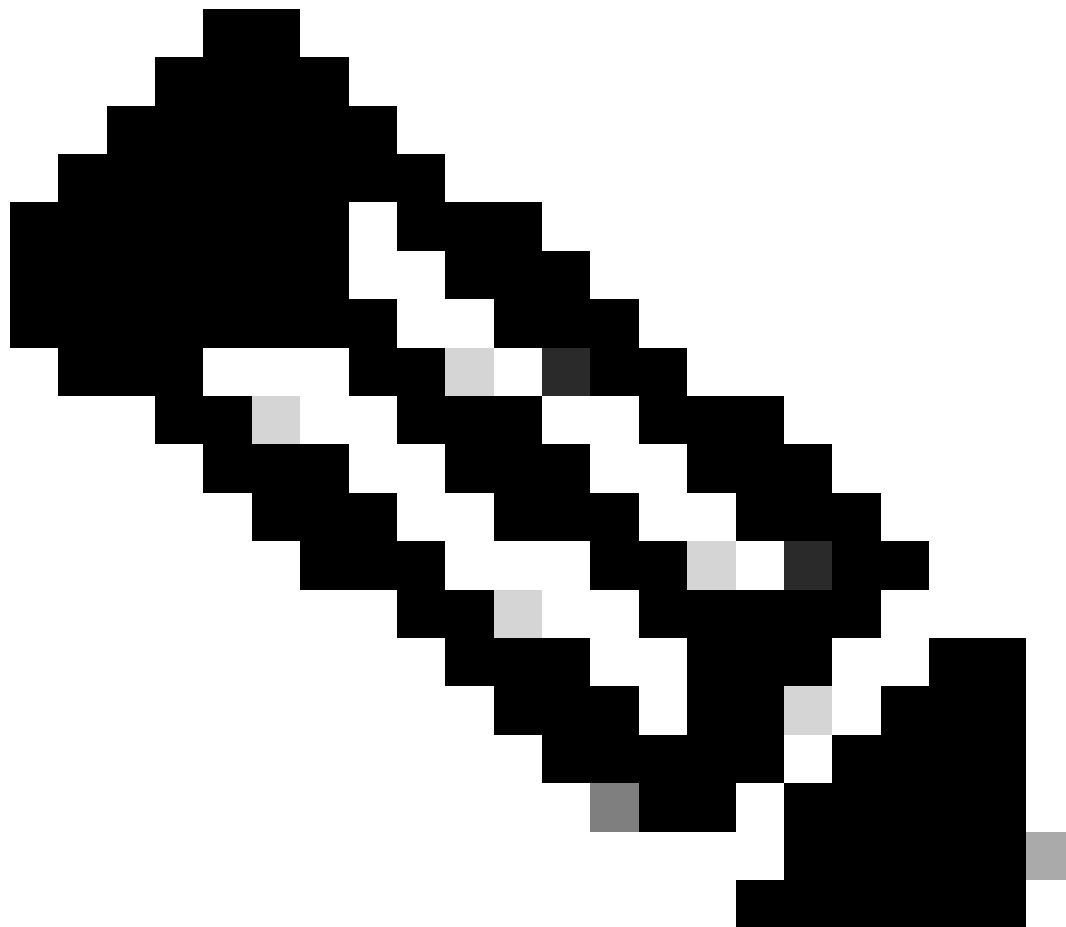
```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rsa
```

Etapa 31. Reinicie o serviço SSH. Você pode usar este comando do PowerShell com privilégio de Administrador (Executar como Administrador)

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

Etapa 32. Para testar se o envio de SCP está configurado corretamente, role os logs configurados, você pode fazer isso a partir da GUI ou da CLI (comando rollovernow):

```
WSA_CLI> rollovernow scpall
```



Observação: neste exemplo, o nome do log é "scpal".

Você pode confirmar que os logs são copiados para a pasta definida, que neste exemplo era `c:/Users/wsascp/wsa01`

Enviar logs SCP para uma unidade diferente

caso seja necessário enviar os logs para uma unidade diferente de C:, crie um link da pasta de perfil do usuário para a unidade desejada. Neste exemplo, os logs são enviados para `D:\WSA_Logs\WSA01` .

Etapa 1. criar as pastas na unidade desejada, neste exemplo

Etapa 2. Abrir Prompt de Comando com privilégio de Administrador (Executar como Administrador)

Etapa 3. Execute este comando para criar o link:

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

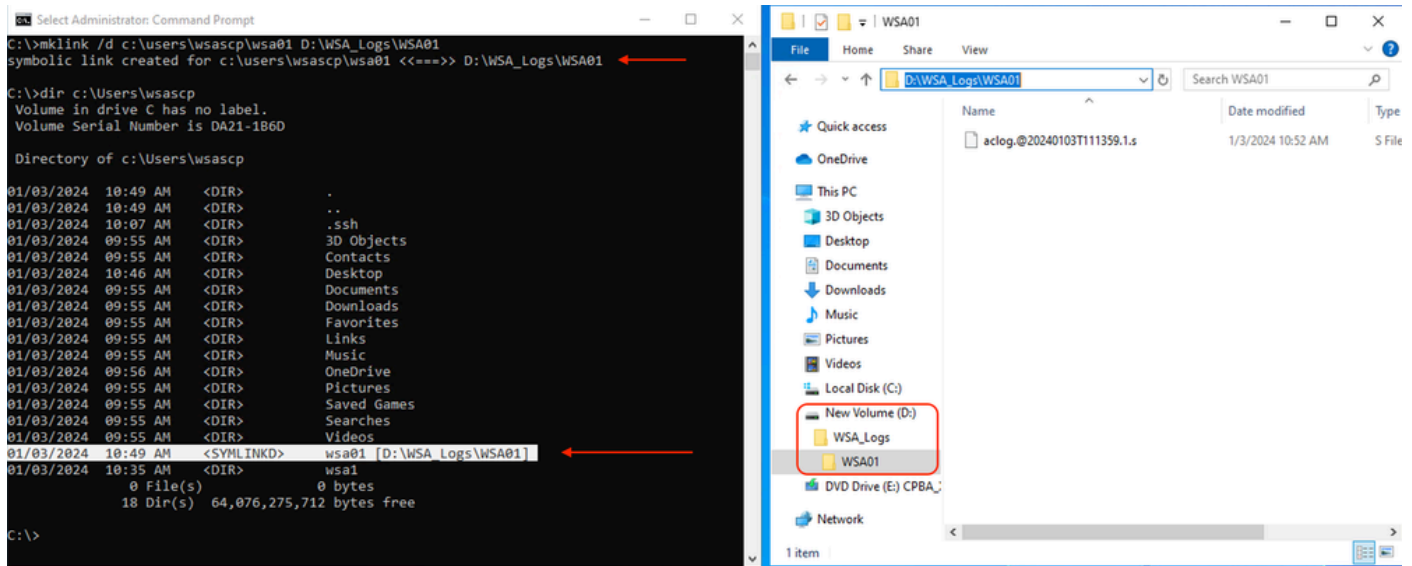


Imagem - Criar link SYM



Observação: neste exemplo, o SWA é configurado para enviar os logs para a pasta WSA01 em C:\Users\wsascp e o servidor SCP tem a pasta WSA01 como link simbólico para D:\WSA_Logs\WSA01

Para obter mais informações sobre o Microsoft Symbol Link, visite : [mklink | Aprender da Microsoft](#)

Solucionar problemas de envio de log SCP

Exibir Logs em SWA

Para solucionar problemas do envio de registro SCP, verifique os erros em:

1. CLI > exhibealertas
2. System_logs



Observação: para ler `system_logs`, você pode usar o comando `grep` na CLI , escolher o número associado a `system_logs` e responder à pergunta no assistente.

Exibir logs no servidor SCP

Você pode ler os logs do servidor SCP no Visualizador de Eventos da Microsoft, em Logs de Aplicativos e Serviços > OpenSSH > Operacional

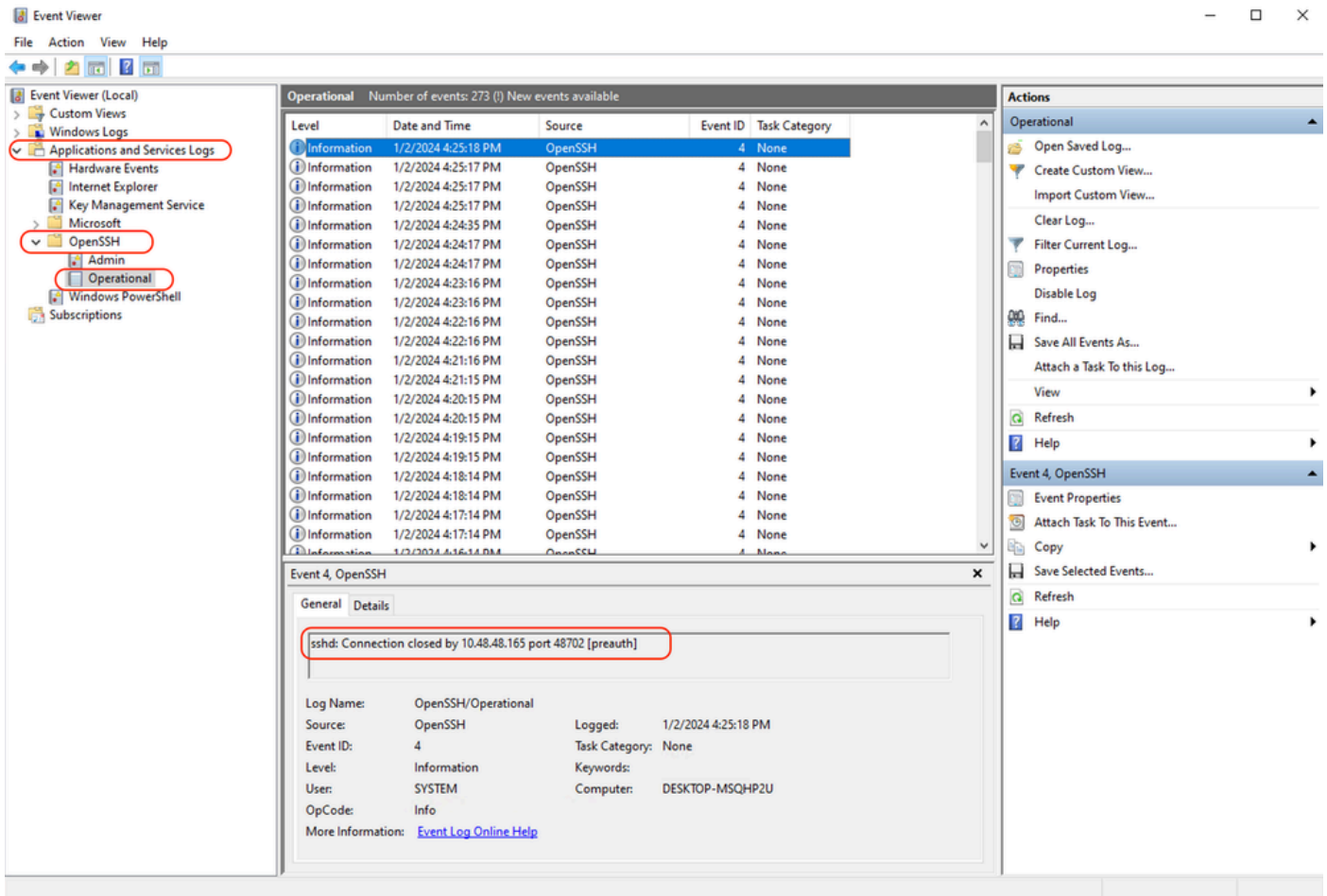


Imagem - Falha de PreAuth

Falha na verificação da chave de host

Este erro indica que a chave pública do servidor SCP armazenada em SWA é inválida.

Aqui está um exemplo de erro da saída displayalerts na CLI:

```
02 Jan 2024 16:52:35 +0100 Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: Host key verification failed. Last message occurred 68 times between Tue Jan 2 15:53:01 2024 and Tue Jan 2 16:52:31 2024.
```

```
Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: Host key verification failed. Last message occurred 46 times between Tue Jan 2 16:30:19 2024 and Tue Jan 2 16:52:31 2024.
```

```
Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: lost connection to host. Last message occurred 68 times between Tue Jan 2 15:53:01 2024 and Tue Jan 2 16:52:31 2024.
```

```
Log Error: Push error for subscription scpal: SCP failed to transfer to 10.48.48.195:22: ssh: connect to host 10.48.48.195 port 22: Connection refused. Last message occurred 22 times between Tue Jan 2 15:53:01 2024 and Tue Jan 2 16:29:18 2024.
```

Aqui estão alguns exemplos de erro em system_logs :

```
Tue Jan 2 19:49:50 2024 Critical: Log Error: Push error for subscription scp: SCP failed to transfer to 10.48.48.195:22: Host key verification failed.
```


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

Para resolver esse problema, você pode copiar o Host do servidor SCP e colá-lo na página de inscrição de logs SCP.

Consulte a etapa 7 em Configurar o SWA para Enviar os registros para o servidor remoto SCP da GUI ou entre em contato com o TAC da Cisco para remover a chave do host do back-end.

Permissão negada (chave pública, senha, teclado interativo)

Esse erro geralmente indica que o nome de usuário fornecido em SWA é inválido.

Aqui está um exemplo de log de erros em system_logs :

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

Aqui está um exemplo de erro do servidor SCP: SCP de usuário inválido da porta <SWA_IP address> <TCP port SWA conecta-se ao servidor SCP>

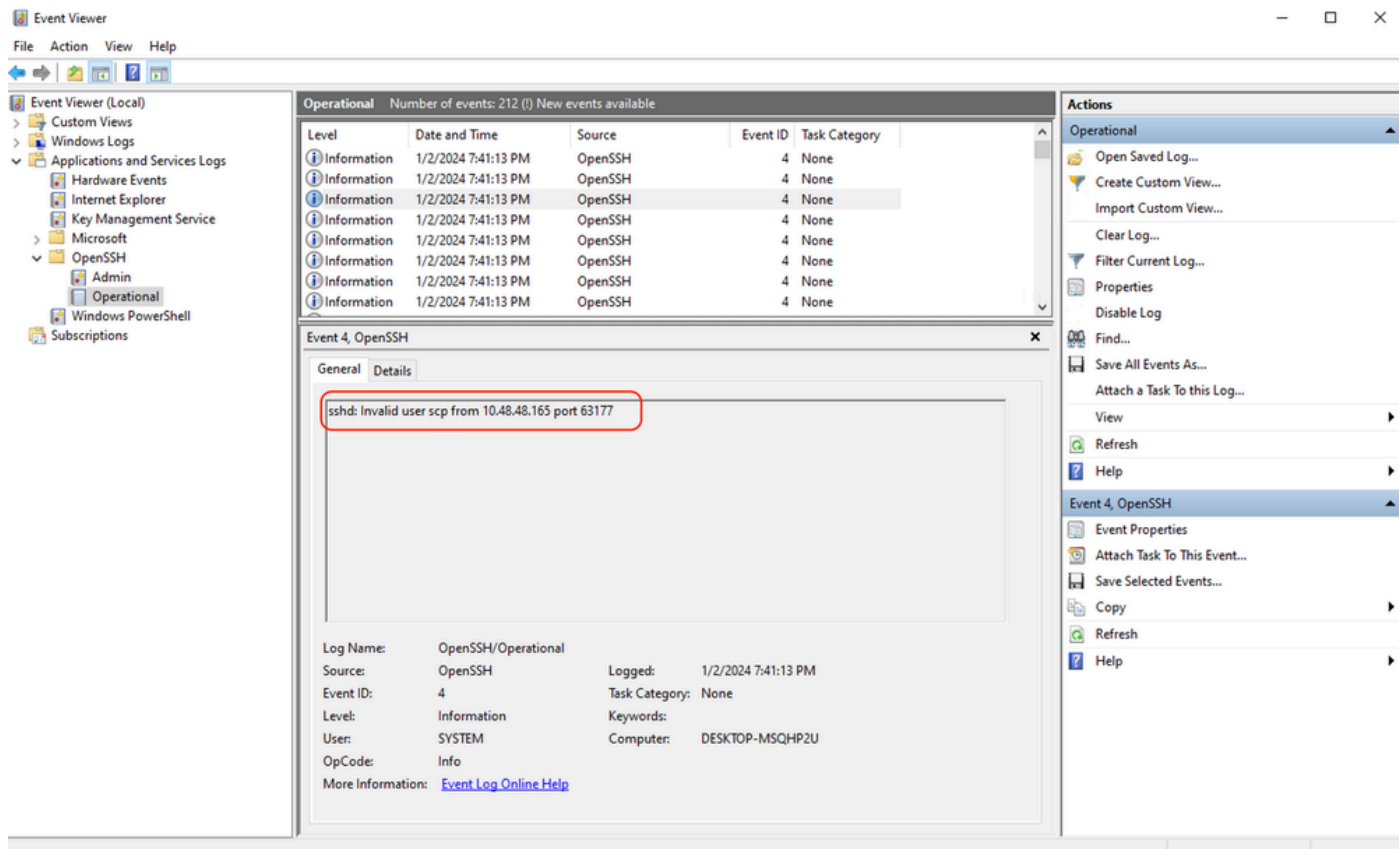


Imagem - Usuário inválido

Para resolver esse erro, verifique a ortografia e se o usuário (configurado no SWA para enviar os logs) está habilitado no servidor SCP.

O arquivo ou diretório não existe

Este erro indica que o caminho fornecido na seção de inscrição de logs SWA não é válido,

Aqui está um exemplo de erro de 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
```

Para resolver esse problema, verifique a ortografia e se o caminho está correto e válido no servidor SCP.

Falha do SCP ao transferir

esse erro pode ser um indicador de um erro de comunicação. Aqui está um exemplo de erro:

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

Para solucionar problemas de conectividade, use o comando telnet na CLI do 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.
[1]> 10.48.48.195

Enter the remote port.
[23]> 22

Trying 10.48.48.195...
```

Neste exemplo, a conexão não é estabelecida. A conexão de saída bem-sucedida é como:

```
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.
[1]> 10.48.48.195
Enter the remote port.
[23]> 22
```

```
Trying 10.48.48.195...
Connected to 10.48.48.195.
Escape character is '^]'.
SSH-2.0-OpenSSH_for_Windows_SCP
```

Se o telnet não estiver conectado:

- [1] Verifique se o firewall do servidor SCP está bloqueando o acesso.
- [2] Verifique se há algum firewall no caminho do SWA para o servidor SCP bloqueando o acesso.
- [3] Verifique se a porta TCP 22 está em um estado de escuta no servidor SCP.
- [4] Execute a captura de pacotes em ambos os servidores SWA e SCP para análise posterior.

Aqui está um exemplo de Captura de Pacotes de conexão bem-sucedida:

No.	Time	Source	Destination	Protocol	Length	Stream	Info
1	2024-01-03 13:42:47.547636	10.48.48.187	10.48.48.195	TCP	74	0	32726 → 22 [SYN] Seq= 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= 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:

Imagem - Captura de pacote de conexão bem-sucedida

Referências

[Diretrizes de práticas recomendadas do Cisco Web Security Appliance - Cisco](#)

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

[Manual do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD \(General Deployment\) - Conectar, Instalar e Configurar \[Cisco Secure Web Appliance\] - Cisco](#)

[Introdução ao OpenSSH para Windows | Aprender da Microsoft](#)

[Configurando a autenticação de chave pública SSH no Windows | Hub de SO Windows \(woshub.com\)](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.