Configuración de registros de inserción de SCP en un dispositivo web seguro con Microsoft Server

Contenido

Introducción

Este documento describe los pasos para configurar Secure Copy (SCP) para copiar automáticamente los registros en Secure Web Appliance (SWA) a otro servidor.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo funciona SCP.
- administración SWA.
- Administración del sistema operativo Microsoft Windows o Linux.

Cisco recomienda que tenga:

- SWA físico o virtual instalado.
- Licencia activada o instalada.
- El asistente de configuración ha finalizado.

- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA.
- Microsoft Windows (al menos Windows Server 2019 o Windows 10 (versión 1809).) o sistema Linux instalado.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

SCP

El comportamiento de Secure Copy (SCP) es similar al de la copia remota (RCP), que proviene del conjunto de herramientas R de Berkeley (propio conjunto de aplicaciones de red de la universidad de Berkeley), excepto en que SCP depende de Secure Shell (SSH) para la seguridad. Además, SCP requiere que se configure la autorización de autenticación, autorización y contabilidad (AAA) para que el dispositivo pueda determinar si el usuario tiene el nivel de privilegio correcto

El método SCP on Remote Server (equivalente a SCP Push) envía periódicamente archivos de registro mediante el protocolo de copia segura a un servidor SCP remoto. Este método requiere un servidor SSH SCP en un equipo remoto con el protocolo SSH2. La suscripción requiere un nombre de usuario, clave SSH y directorio de destino en el equipo remoto. Los archivos de registro se transfieren en función de una programación de renovación establecida por el usuario.

Suscripción a registro SWA

Puede crear varias suscripciones a registros para cada tipo de archivo de registro. Las suscripciones incluyen detalles de configuración para archivado y almacenamiento, entre los que se incluyen los siguientes:

- Configuración de reversión, que determina cuándo se archivan los archivos de registro.
- Configuración de compresión para los registros archivados.
- Configuración de recuperación para los archive logs, que especifica si los logs se archivan en un servidor remoto o se almacenan en el dispositivo.

Archivando archivos de registro

AsyncOS archiva (revierte) las suscripciones de registro cuando un archivo de registro actual alcanza un límite especificado por el usuario de tamaño máximo de archivo o tiempo máximo desde la última reversión.

Esta configuración de archivo se incluye en las suscripciones a registros:

- Renovación por tamaño de archivo
- Reversión por tiempo
- Compresión de registros
- Método de recuperación

También puede archivar manualmente los archivos de registro (rollover).
Paso 1. Elija Administración del sistema > Suscripciones de registro.
Paso 2. Marque la casilla de verificación de la columna Renovación de las suscripciones de registro que desea archivar o marque la casilla de verificación Todos para seleccionar todas las suscripciones.
Paso 3 .Haga clic en Rollover Now para archivar los registros seleccionados.

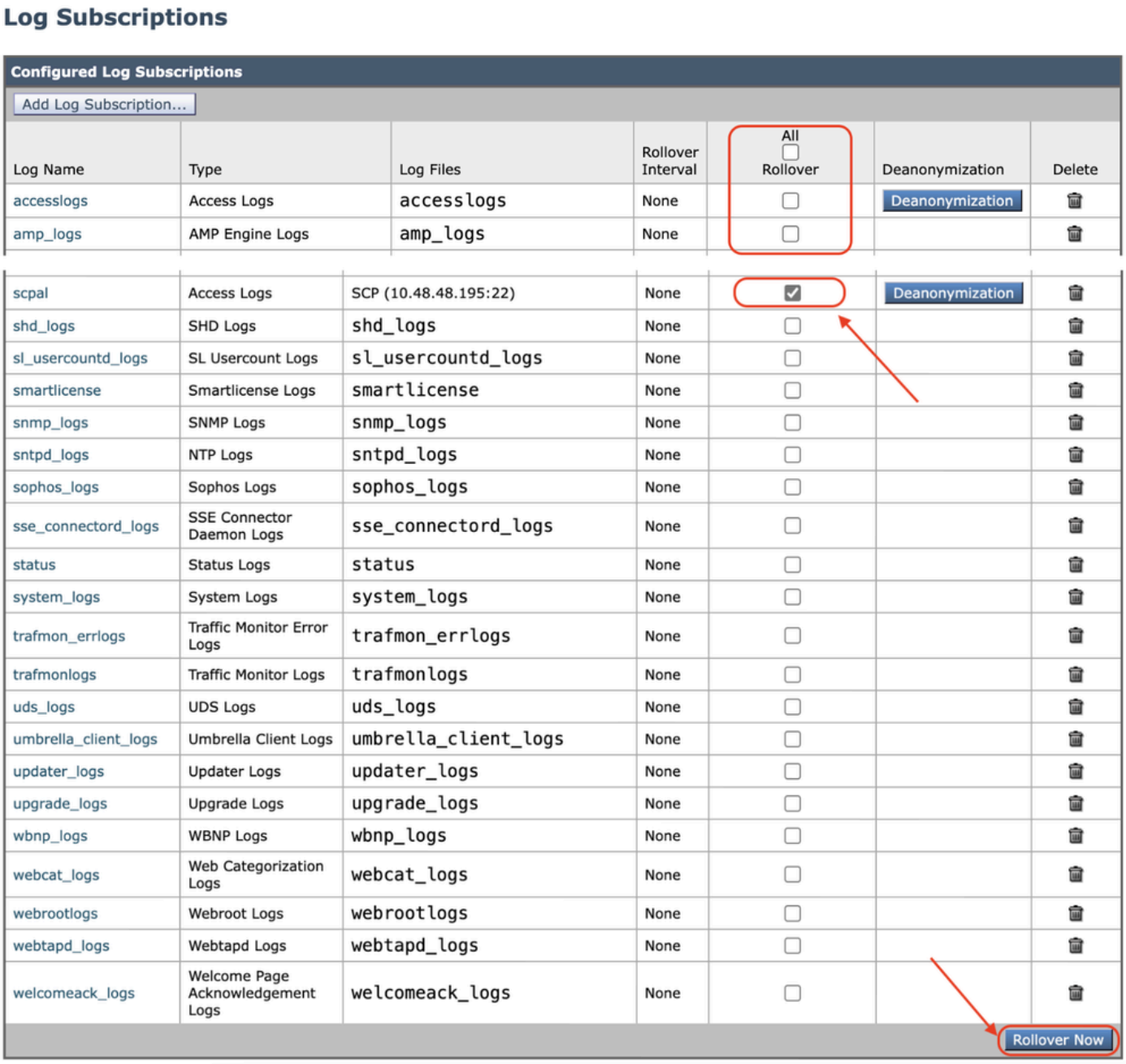


Imagen - Renovar ahora GUI

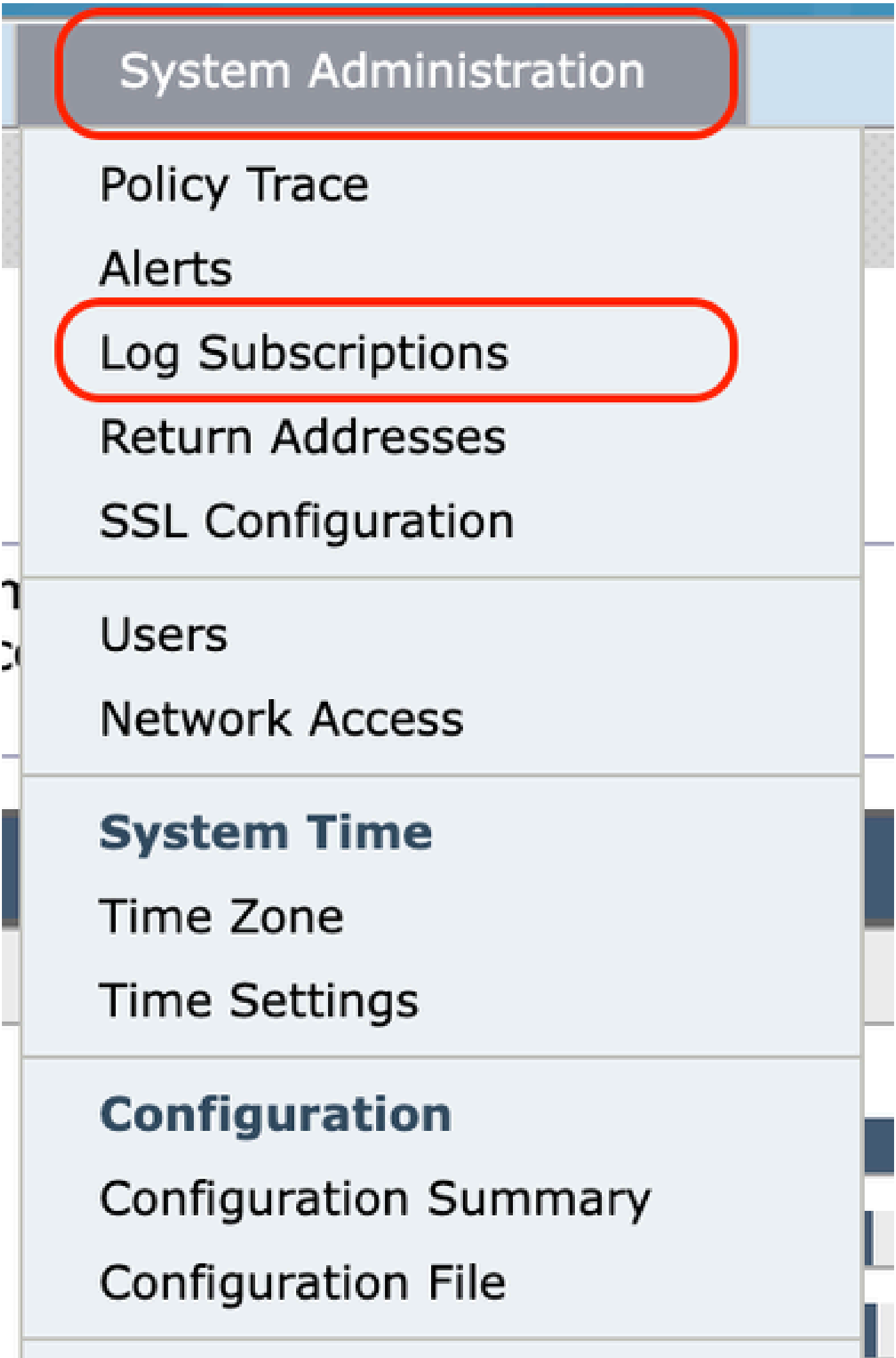
Configuración de la recuperación de registros mediante SCP en el servidor remoto

Existen dos pasos principales para la recuperación de registros en un servidor remoto con SCP desde SWA:

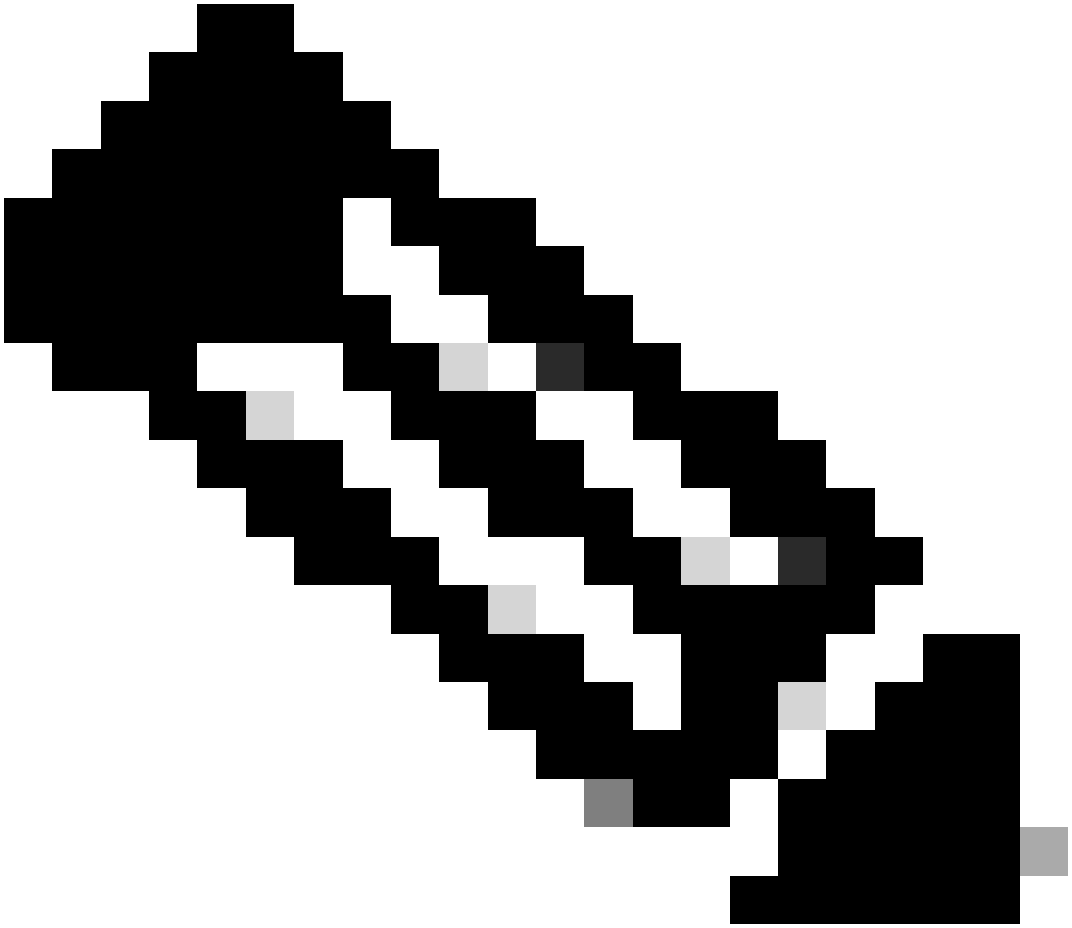
1. Configure SWA para enviar los registros.
2. Configure el servidor remoto para recibir los registros.

Configuración de SWA para enviar los registros al servidor remoto de SCP desde la GUI

Paso 1. Inicie sesión en SWA y, en Administración del sistema, seleccione Registrar suscripciones.


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

Guarde la clave SSH en un archivo de texto para su uso posterior en la sección de configuración del servidor SCP remoto.



Nota: Debe copiar ambas líneas que comienzan con ssh- y terminan con root@<nombre de host SWA> .

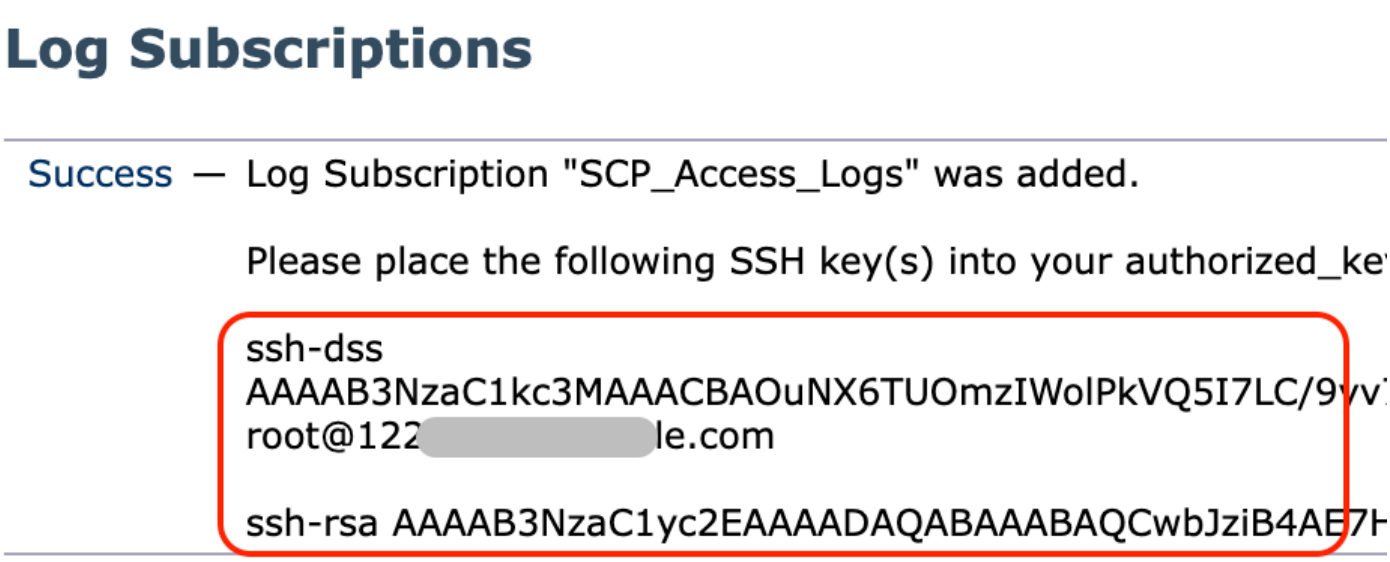
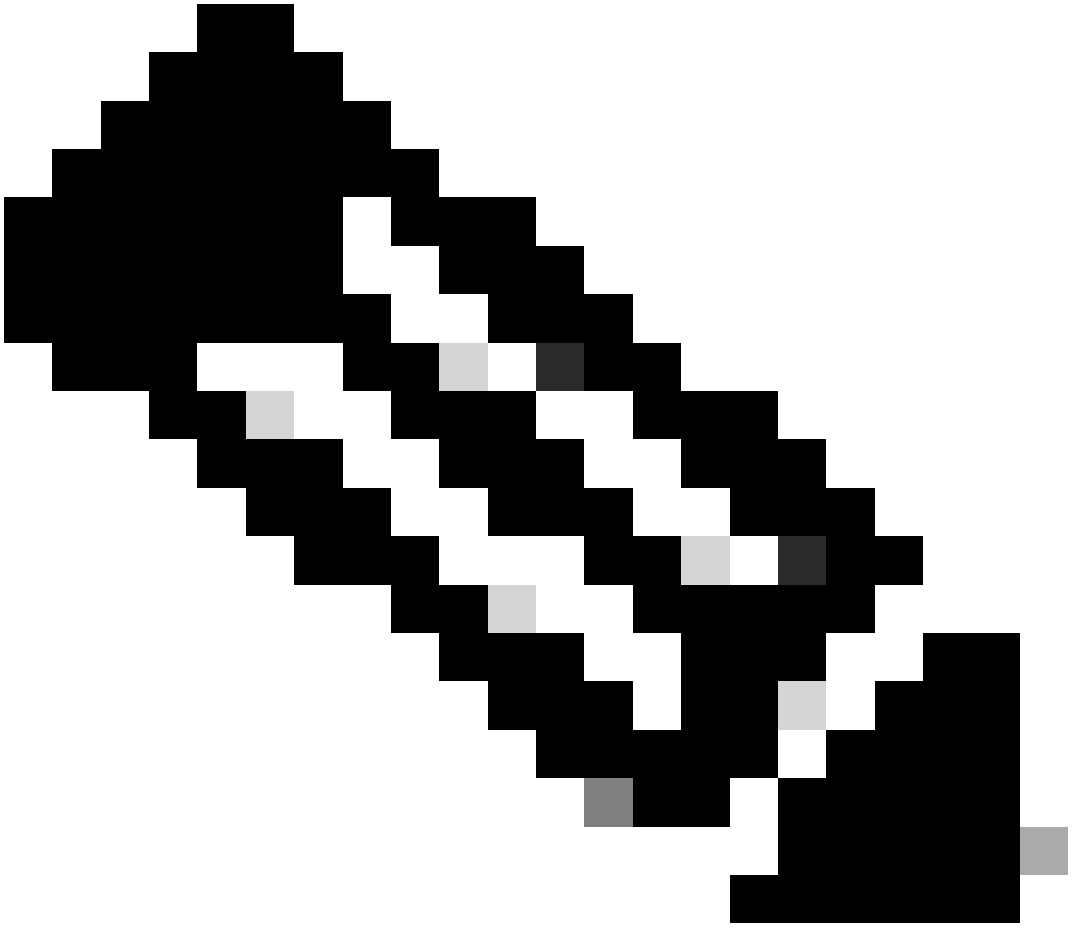


Imagen: guarde la clave SSH para utilizarla más adelante.

Paso 10. Registrar cambios.

Configuración de Microsoft Windows como servidor remoto de SCP

Paso 10. Para crear un usuario para el servicio SCP, acceda a Administración de equipos:



Nota: si ya dispone de un usuario para SCP, vaya directamente al paso 16.

Paso 11. Seleccione Usuarios locales y grupo y elija Usuarios en el panel izquierdo.

Paso 12. Haga clic con el botón derecho del ratón en la página principal y seleccione nuevo usuario.

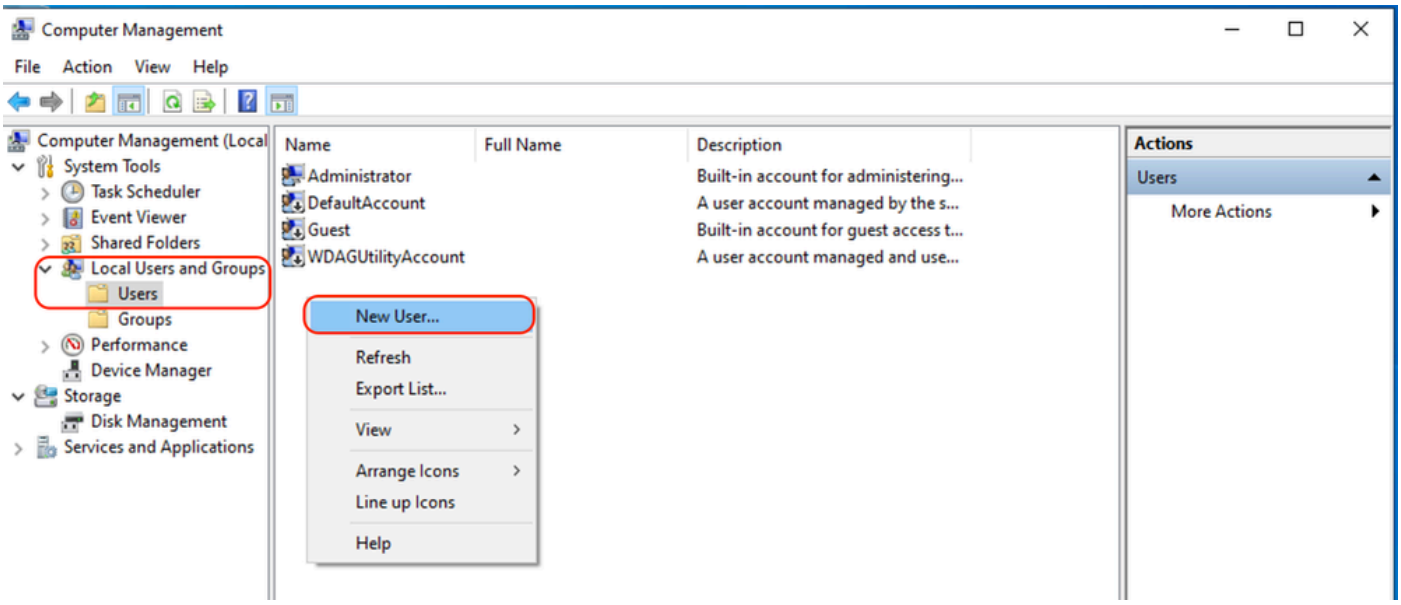


Imagen: creación de un usuario para el servicio SCP.

Paso 13. Introduzca el nombre de usuario y la contraseña deseada.

Paso 14. Elija Password Never Expired.

Paso 15. Haga clic en Create y, a continuación, cierre la ventana.

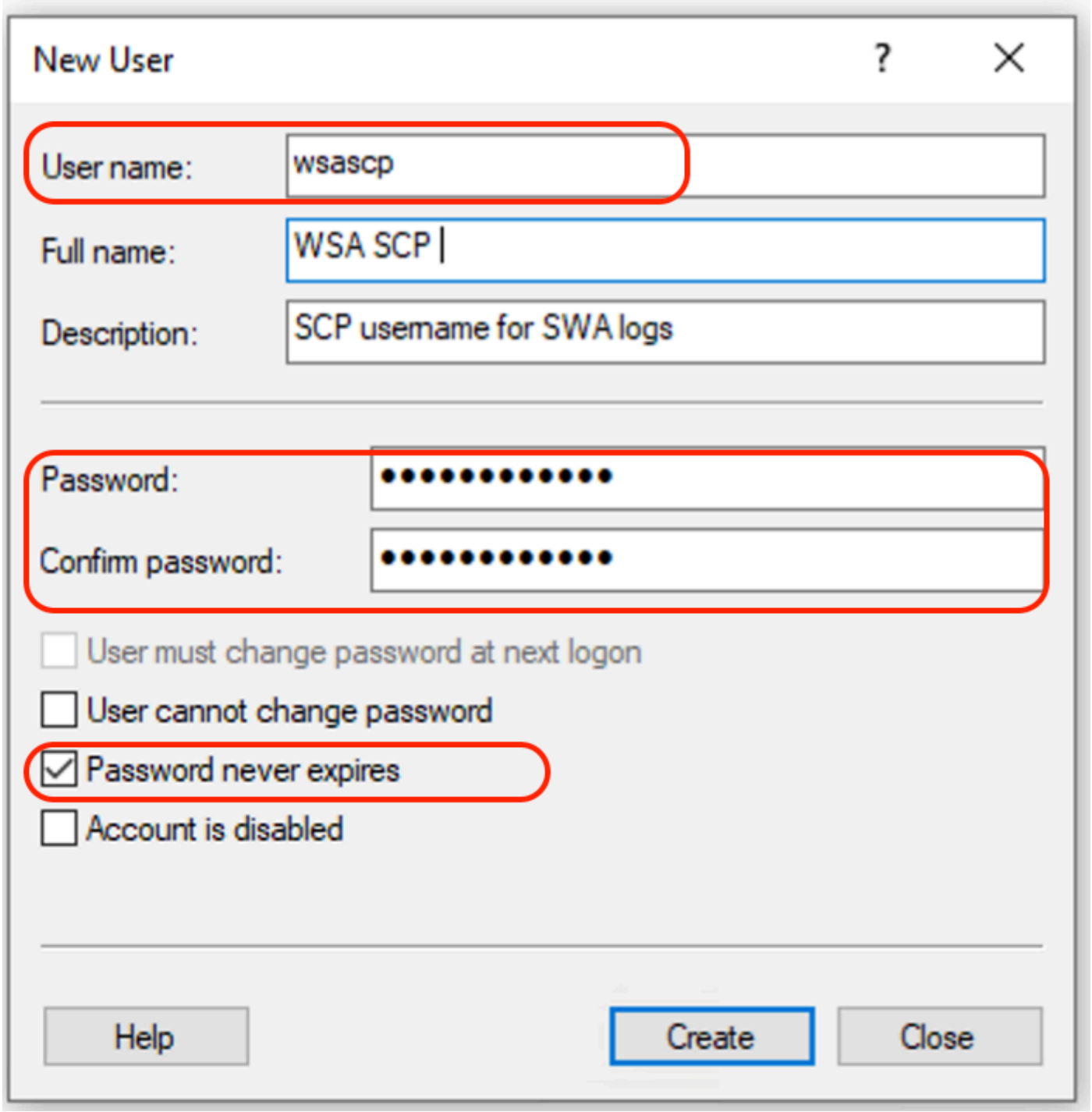
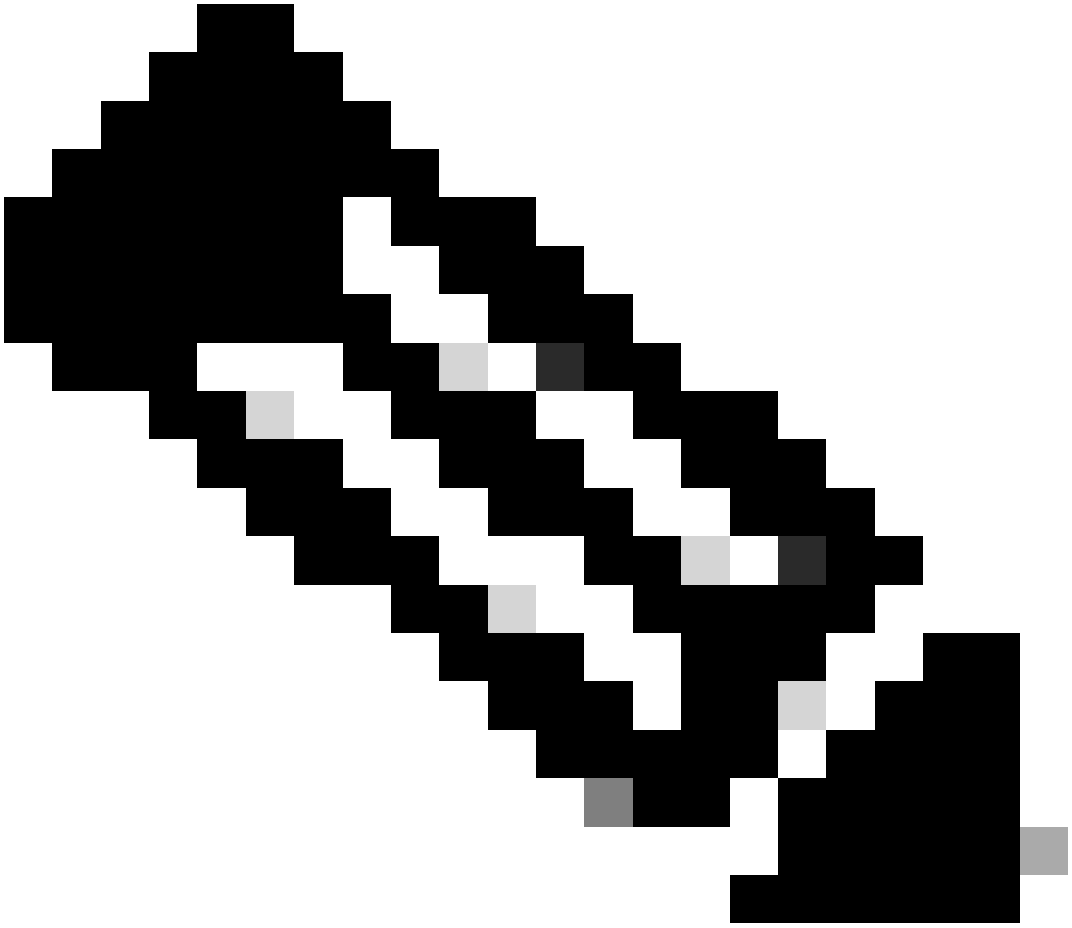


Imagen: introduzca la información del nuevo usuario.

Paso 16. Inicie sesión en el servidor SCP remoto con el usuario recién creado para crear el directorio de perfiles.



Nota: Si tiene OpenSSL instalado en el servidor SCP remoto, vaya directamente al paso 19.

Paso 17. Abra PowerShell con privilegios de administrador (Ejecutar como administrador) y ejecute este comando para comprobar los requisitos previos:

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

Si el resultado es True, puede continuar. De lo contrario, consulte al equipo de soporte técnico de Microsoft,

Paso 18. Para instalar OpenSSH mediante PowerShell con privilegios de administrador (Ejecutar como administrador), ejecute :

```
# 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
```

A continuación se muestra una muestra de resultados satisfactorios:

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

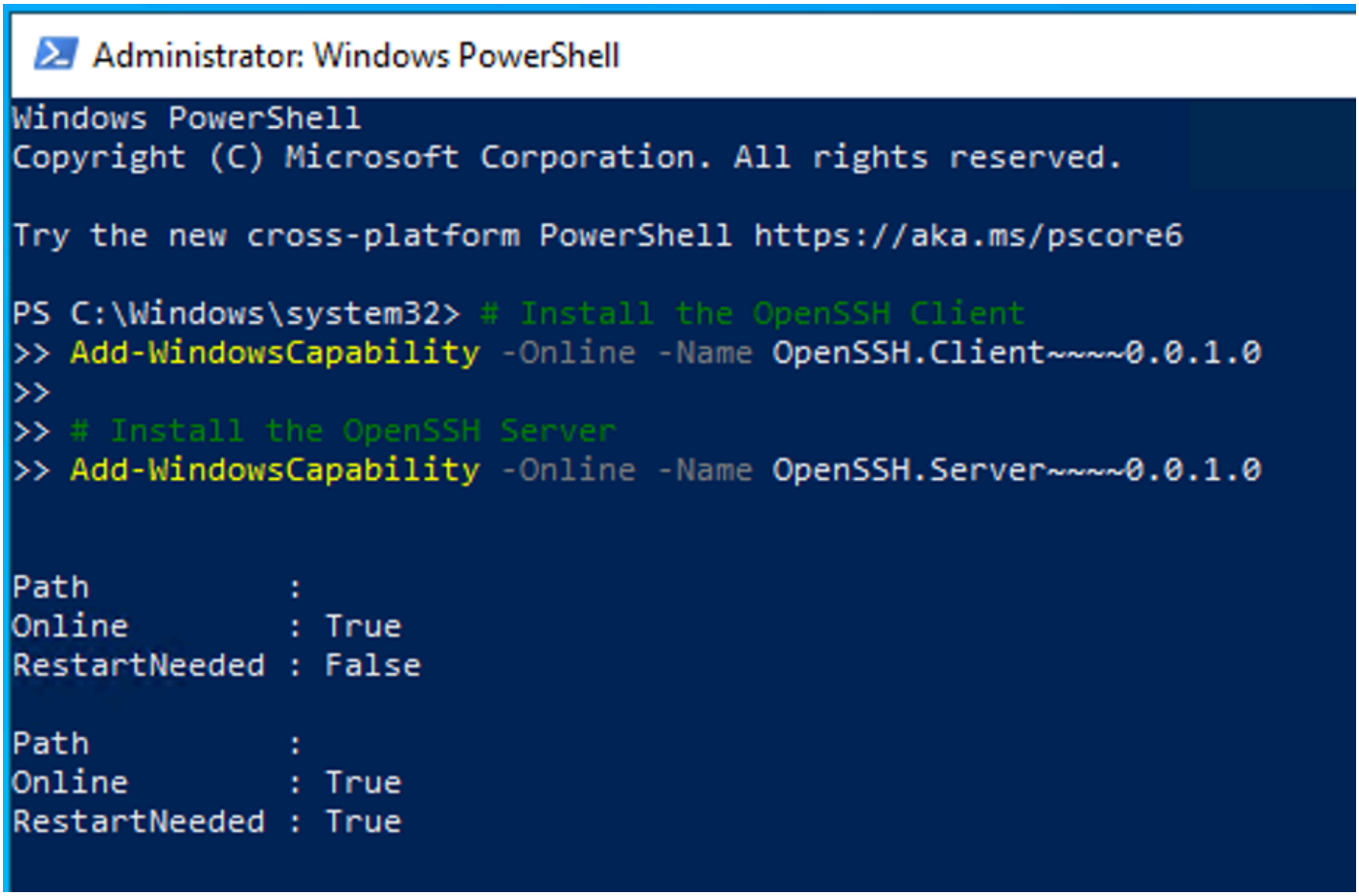
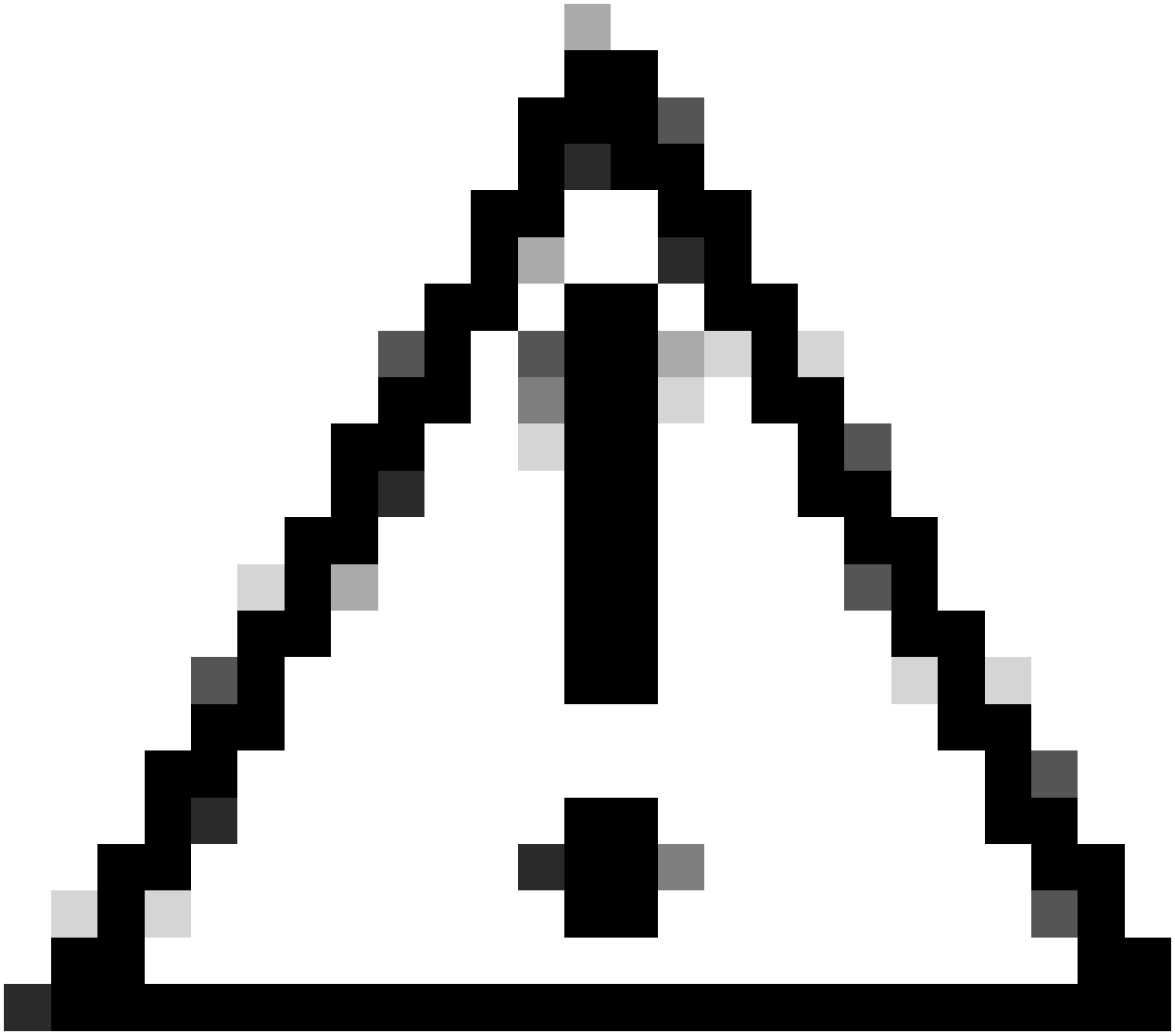


Imagen- Instalar OpenSSH en PowerShell



Precaución: si RestartNeeded se establece en True, reinicie Windows .

Para obtener más información sobre la instalación en otras versiones de Microsoft Windows, visite este enlace: Introducción a OpenSSH para Windows | Microsoft Learn

Paso 19.Abra una sesión normal (no elevada) de PowerShell y genere un par de claves RSA mediante el comando:

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

Una vez finalizado el comando, puede ver que la carpeta .ssh ha creado su directorio de perfil de usuario.

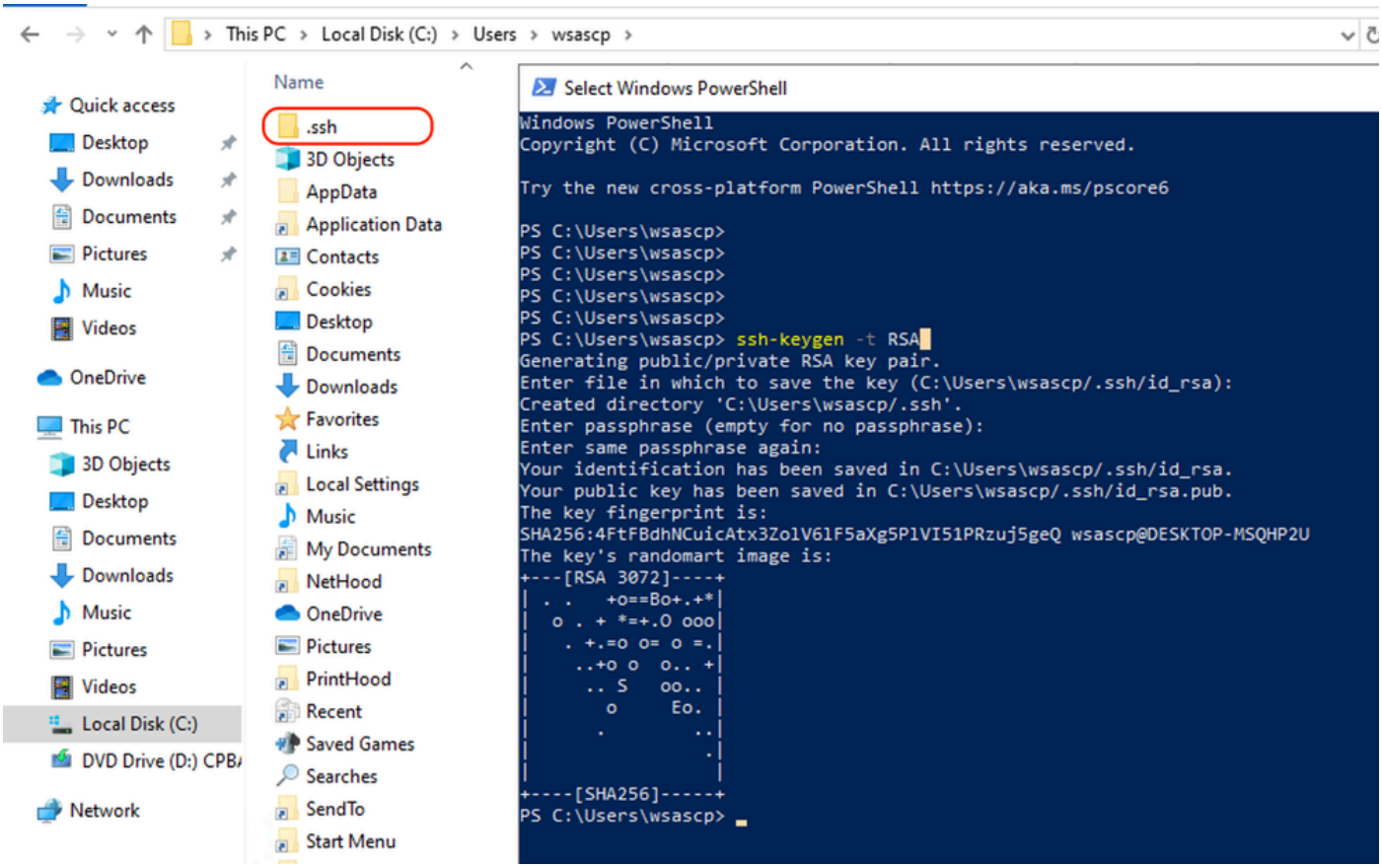


Imagen - Generar clave RSA

Paso 20. Inicie el servicio SSH desde PowerShell con el privilegio de administrador (Ejecutar como administrador).

```
Start-Service sshd
```

Paso 21. (Opcional pero recomendado) Cambie el tipo de inicio del servicio a Automático, con privilegios de administrador (Ejecutar como administrador).

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

Paso 22. Confirme que se ha creado la regla de firewall para permitir el acceso al puerto TCP 22.

```
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."
}
```

Paso 23. Edite el archivo de configuración SSH ubicado en : %programdata%\ssh\sshd_config en el bloc de notas y quite el número para RSA y 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
```

Paso 24. Edite las condiciones de conexión en %programdata%\ssh\sshd_config. En este ejemplo, la dirección de escucha es para la dirección de todas las interfaces. Puede personalizarlo gracias a su diseño.

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

Paso 25. Marque estas dos líneas al final del archivo %programdata%\ssh\sshd_config agregando # al principio de cada línea:

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

Paso 26.(Opcional) Edite los Modos Estrictos en %programdata%\ssh\sshd_config, De forma predeterminada, este modo está habilitado y evita la autenticación basada en claves SSH si las claves privada y pública no están protegidas correctamente.

Anule los comentarios de la línea #StrictModes sí y cámbiela a StrictModes no:

```
StrictModes No
```

Paso 27. Quite el # de esta línea a %programdata%\ssh\sshd_config para permitir la autenticación de clave pública

```
PubkeyAuthentication yes
```

Paso 28. Cree un archivo de texto "authorized_keys" en la carpeta .ssh y pegue la clave RSA

pública SWA (recopilada en el paso 9)

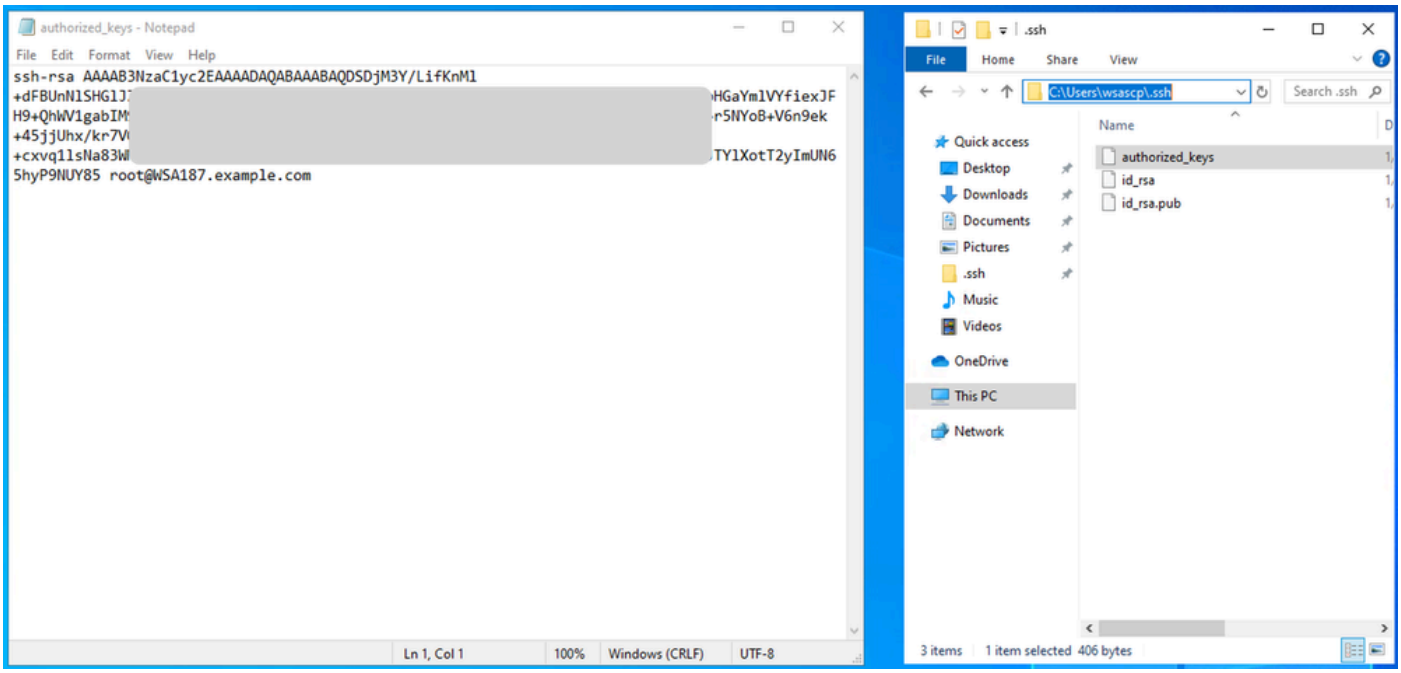
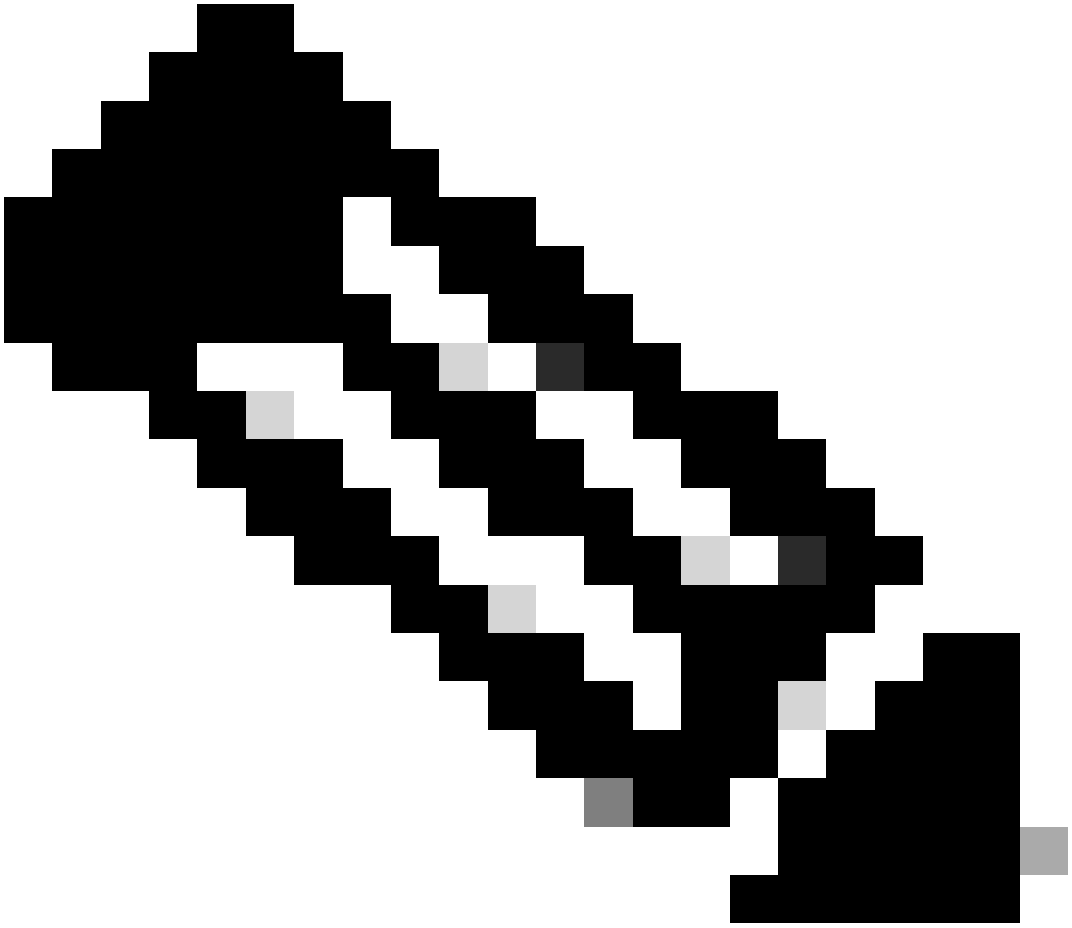
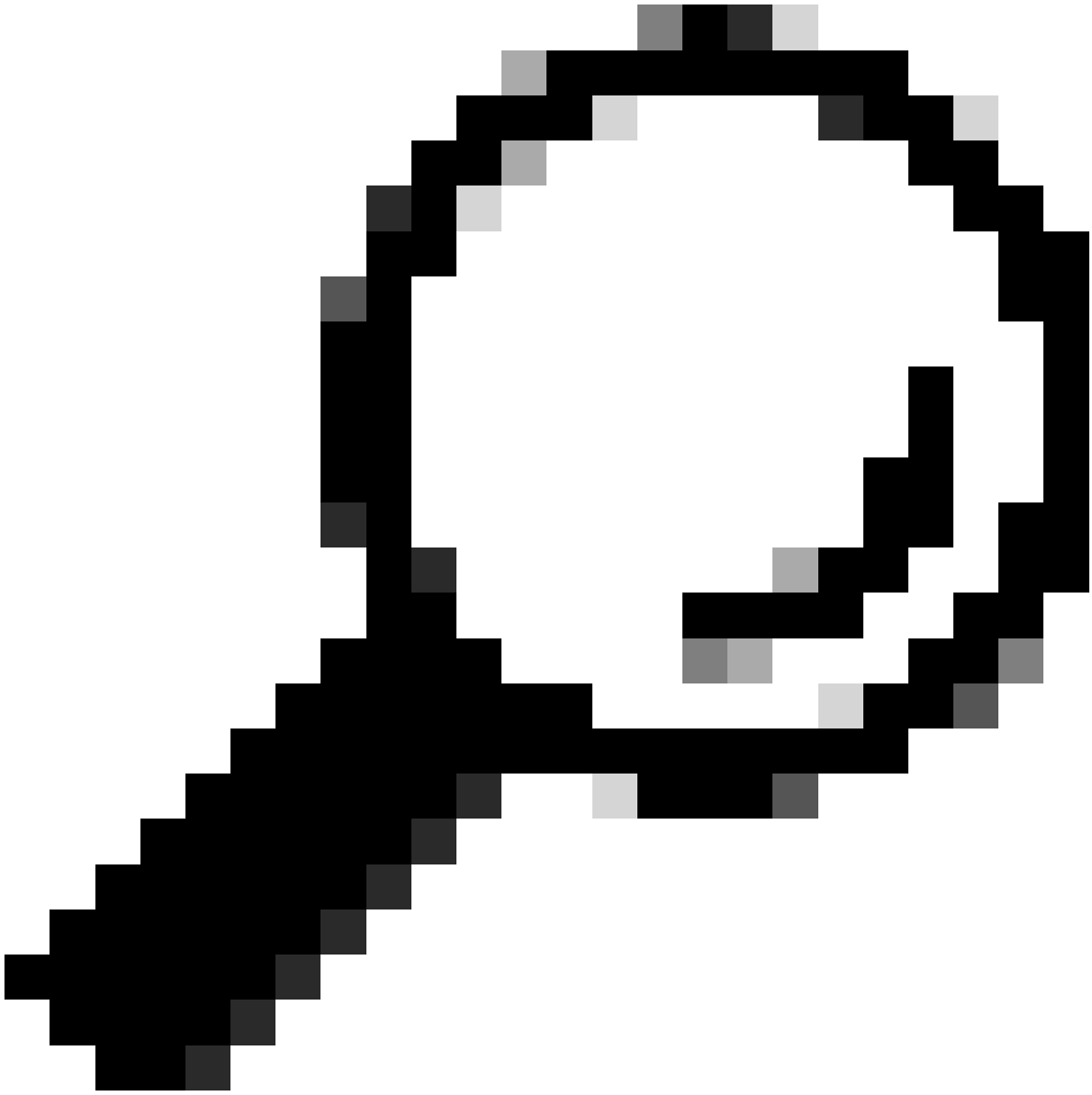


Imagen: clave pública SWA



Nota: copie la línea completa comenzando con ssh-rsa y terminando con root@<your_SWA_hostname>



Sugerencia: Dado que RSA está instalado en el servidor SCP, no es necesario pegar la clave ssh-dss

---

Paso 29. Habilite "Agente de autenticación OpenSSH" en PowerShell con privilegios de administrador (Ejecutar 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>
```

Imagen - Habilitar Agente de autenticación SSH abierto

Paso 30.(Opcional) Agregue esta línea a %programdata%\ssh\sshd_config para permitir tipos de clave:

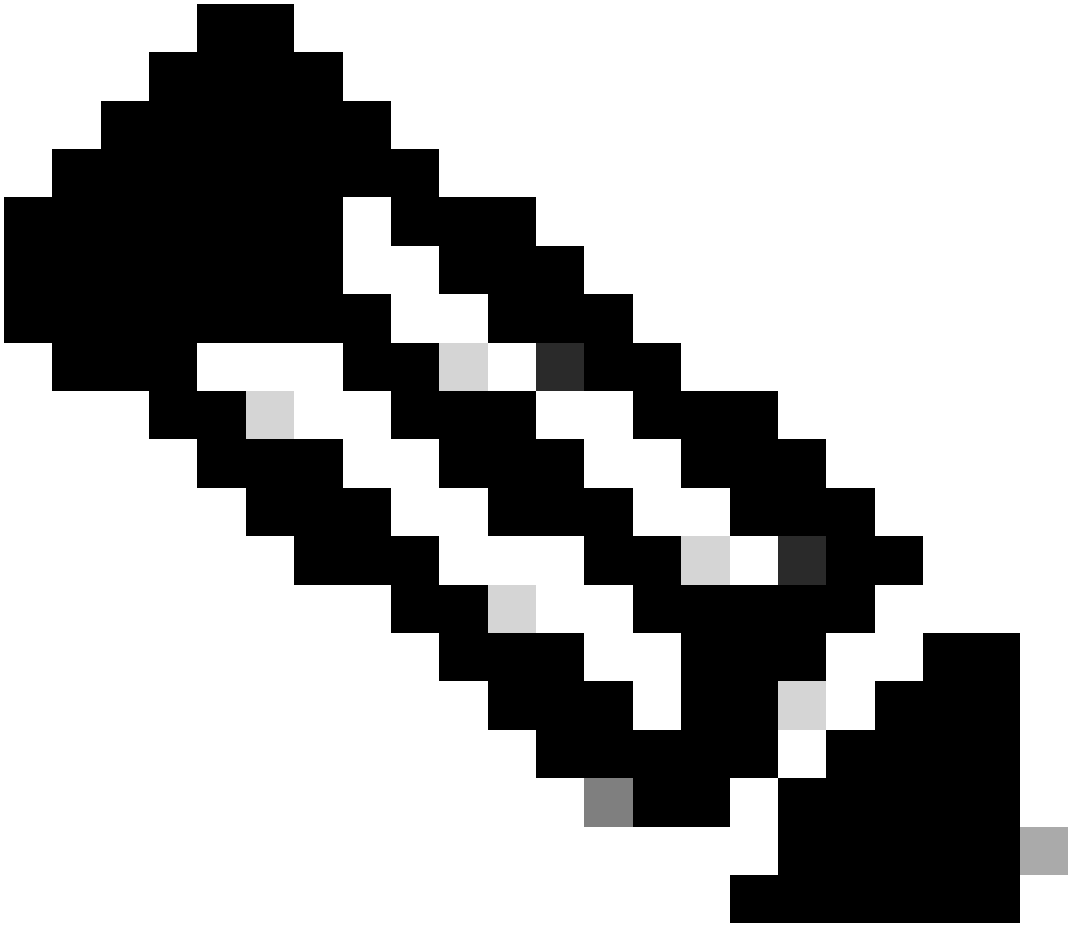
```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rsa
```

Paso 31. Reinicie el servicio SSH. Puede utilizar este comando desde PowerShell con privilegios de administrador (Ejecutar como administrador)

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

Paso 32. Para probar si la inserción de SCP está configurada correctamente, traspase los registros configurados, puede hacerlo desde la GUI o la CLI (comando rollovernow):

```
WSA_CLI> rollovernow scpal
```



Nota: En este ejemplo, el nombre del registro es "scpal".

Puede confirmar que los registros se copian en la carpeta definida, que en este ejemplo era c:/Users/wsascp/wsa01

Inserción de registros de SCP en una unidad diferente

en caso de que necesite enviar los registros a una unidad diferente que no sea C:, cree un vínculo desde la carpeta de perfil de usuario a la unidad deseada. En este ejemplo, los registros se envían a D:\WSA_Logs\WSA01 .

Paso 1. cree las carpetas en la unidad deseada, en este ejemplo

Paso 2. Abrir el símbolo del sistema con privilegios de administrador (Ejecutar como administrador)

Paso 3. Ejecute este comando para crear el link:

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

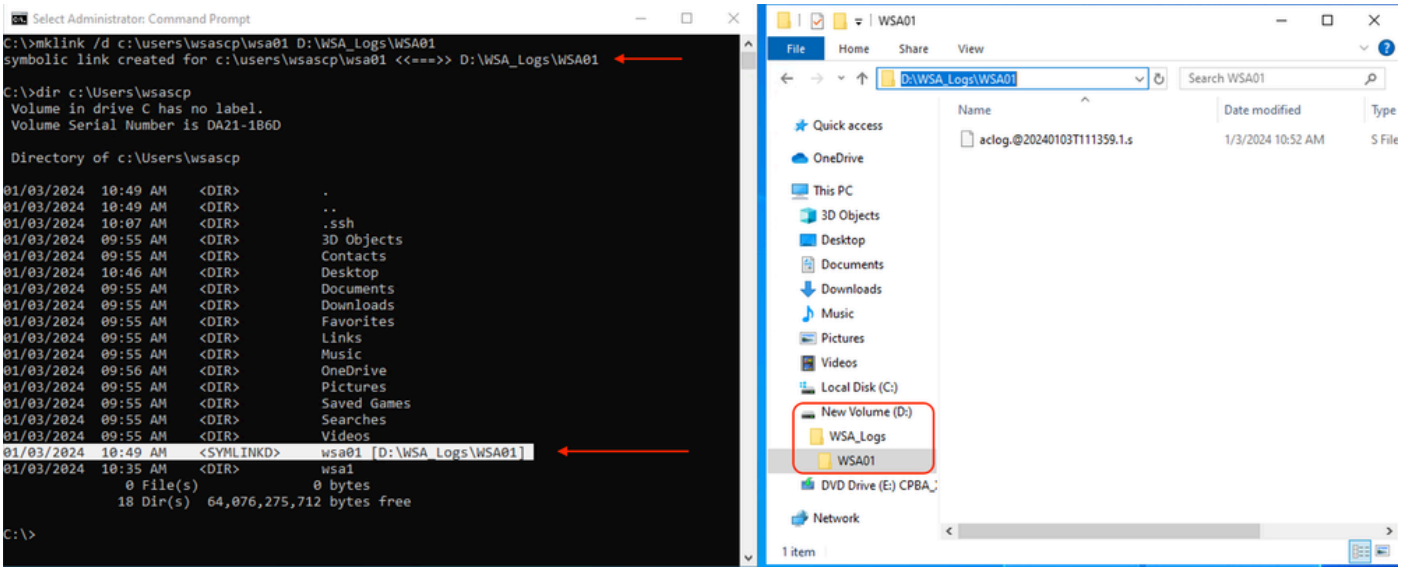
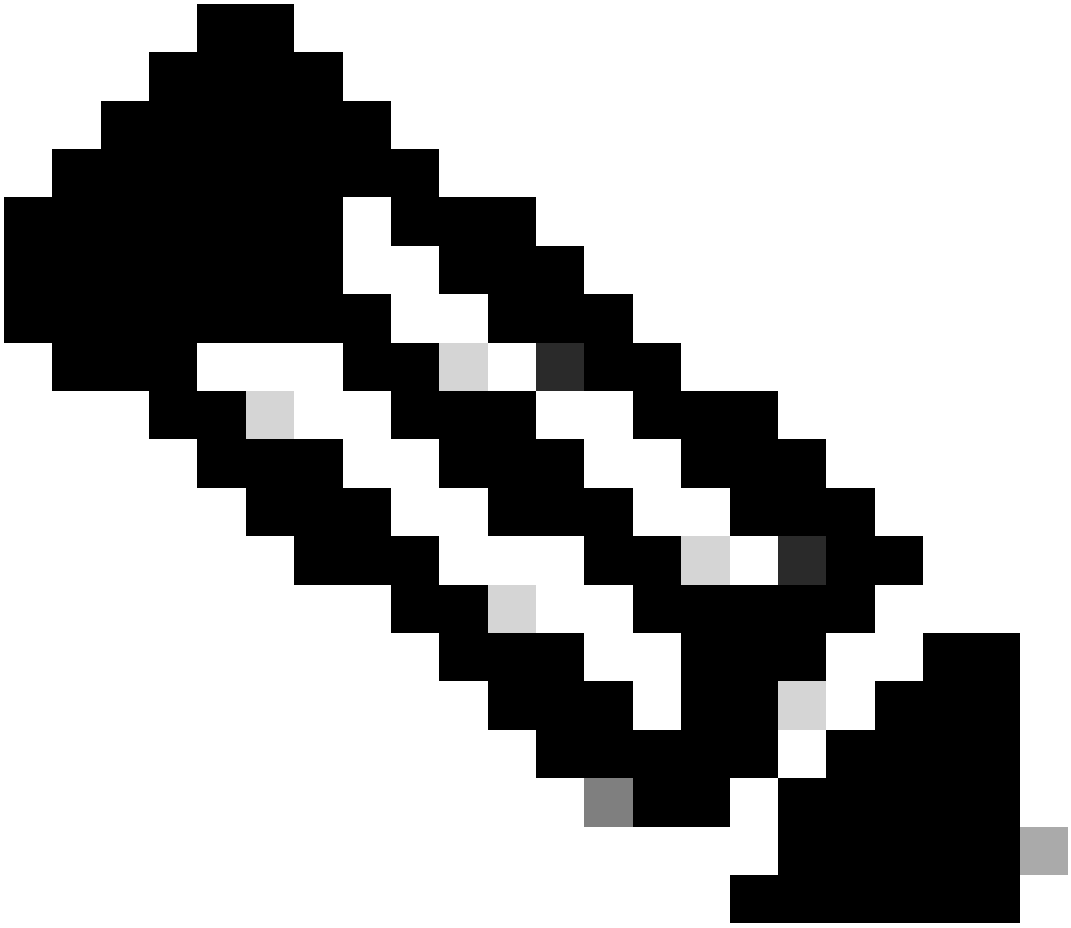


Imagen: enlace Crear SYM



Nota: En este ejemplo, SWA está configurado para enviar los registros a la carpeta WSA01 en C:\Users\wsascp y el servidor SCP tiene la carpeta WSA01 como enlace simbólico a D:\WSA_Logs\WSA01

Para obtener más información sobre Microsoft Symbol Link, visite: mklink | Microsoft Learn

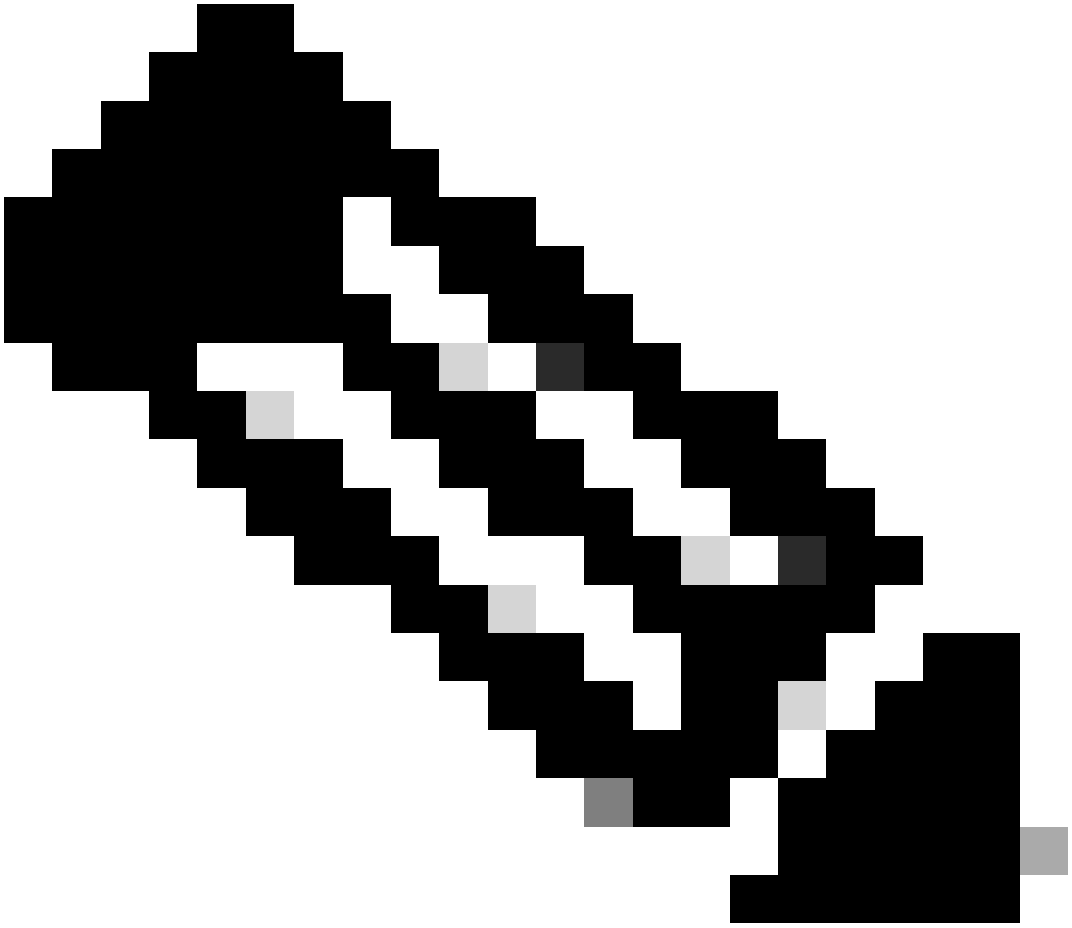
Troubleshooting de SCP Log Push

Ver registros en SWA

Para resolver problemas de la inserción de registro de SCP, verifique los errores en:

1. CLI > mostraralertas

2. Registros_del_sistema



Nota: Para leer system_logs, puede utilizar el comando grep en CLI , elija el número asociado con system_logs y responda a la pregunta en el asistente.

Ver registros en el servidor SCP

Puede leer los registros del servidor SCP en el Visor de eventos de Microsoft, en Registros de aplicaciones y servicios > OpenSSH > Operativo

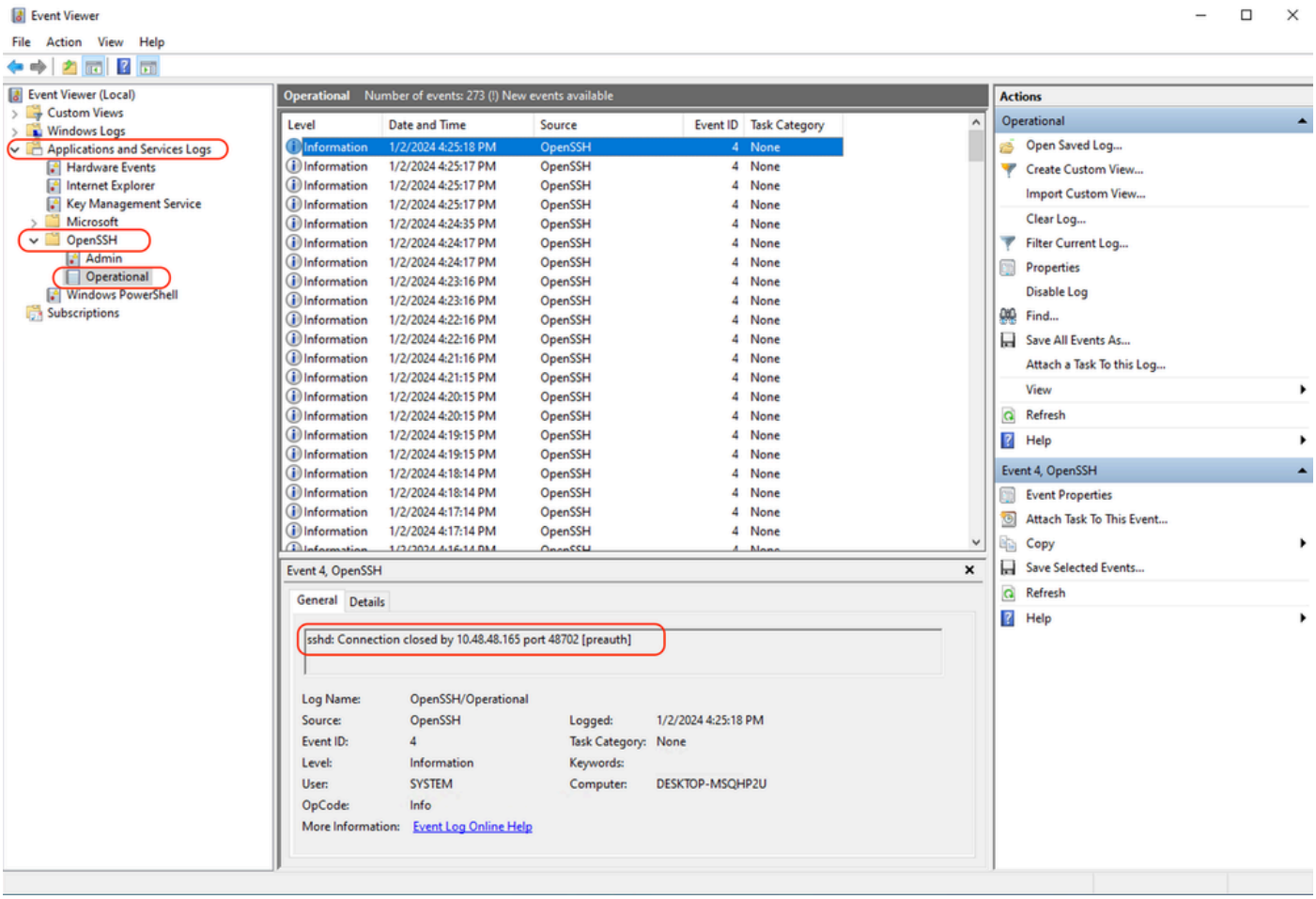


Imagen - PreAuth Failed

Error de verificación de clave de host

Este error indica que la clave pública del servidor SCP almacenada en SWA no es válida.

A continuación se muestra un ejemplo de error de la salida de displayAlerts en 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.
```

Aquí hay algunos ejemplos de Error en 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
```

Para resolver este problema, puede copiar el host del servidor SCP y pegarlo en la página de suscripción de registros SCP.

Consulte el paso 7 en Configure SWA para Enviar los Registros al Servidor Remoto SCP desde la GUI o puede comunicarse con el TAC de Cisco para quitar la Clave de Host del backend.

Permiso denegado (clave pública, contraseña, teclado interactivo)

Este error suele indicar que el nombre de usuario proporcionado en SWA no es válido.

Aquí hay un ejemplo de registro de errores en 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
```

Este es un ejemplo de error del servidor SCP: usuario no válido de SCP desde el puerto <SWA_IP address> <TCP port SWA connect to SCP server>

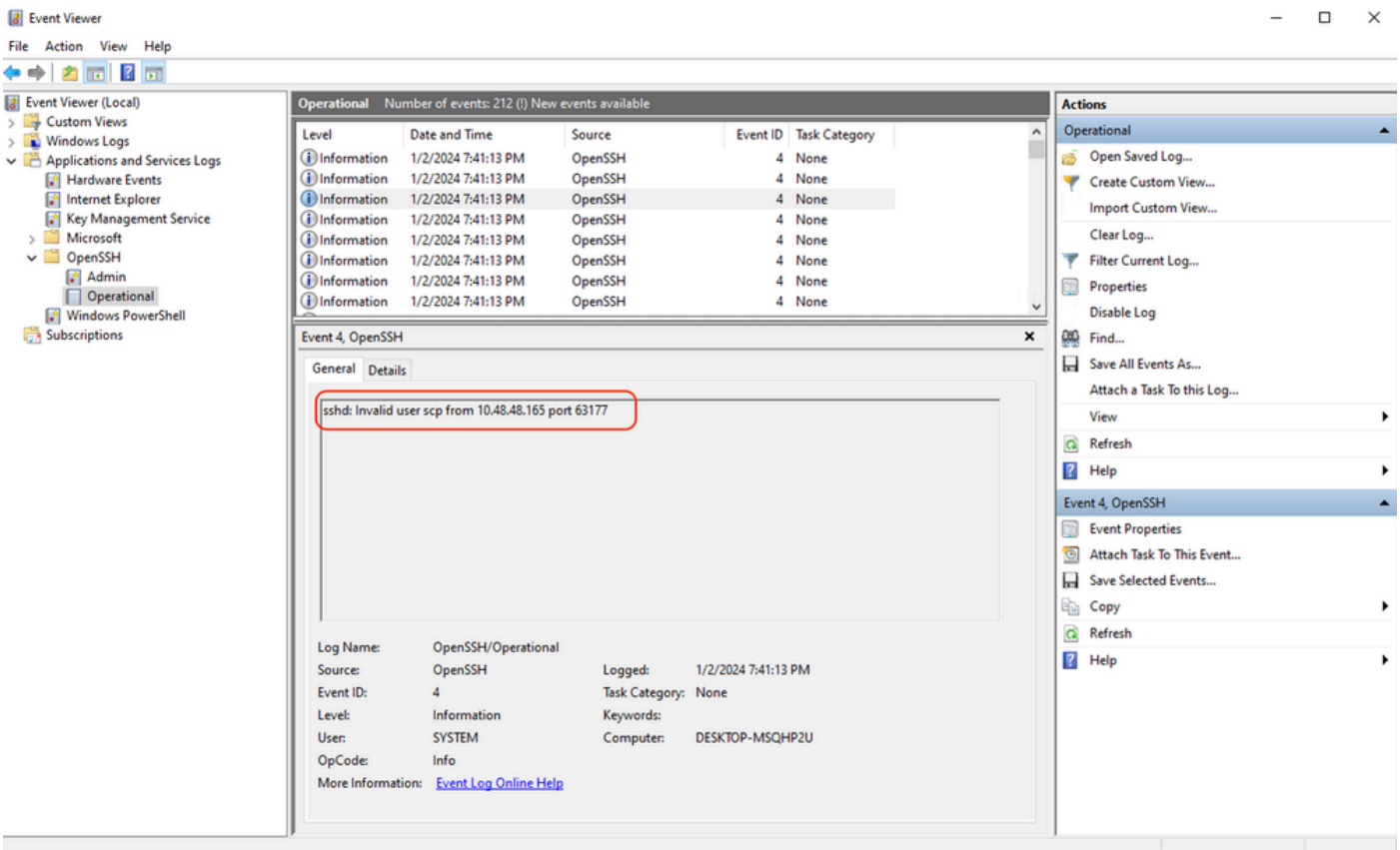


Imagen - Usuario no válido

Para solucionar este error, revise la ortografía y compruebe que el usuario (configurado en SWA para insertar los registros) está habilitado en el servidor SCP.

No existe tal archivo o directorio

Este error indica que la ruta proporcionada en la sección de suscripción de registros SWA no es válida.

A continuación se muestra un ejemplo de error de 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
```

Para resolver este problema, compruebe la ortografía y asegúrese de que la ruta de acceso es correcta y válida en el servidor SCP.

SCP no pudo transferir

este error podría ser un indicador de un error de comunicación. Este es el ejemplo de error:

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

Para solucionar problemas de conectividad, utilice el comando telnet en la CLI de 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...
```

En este ejemplo, la conexión no se ha establecido. La conexión exitosa es 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.
[]> 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
```

Si el telnet no está conectado:

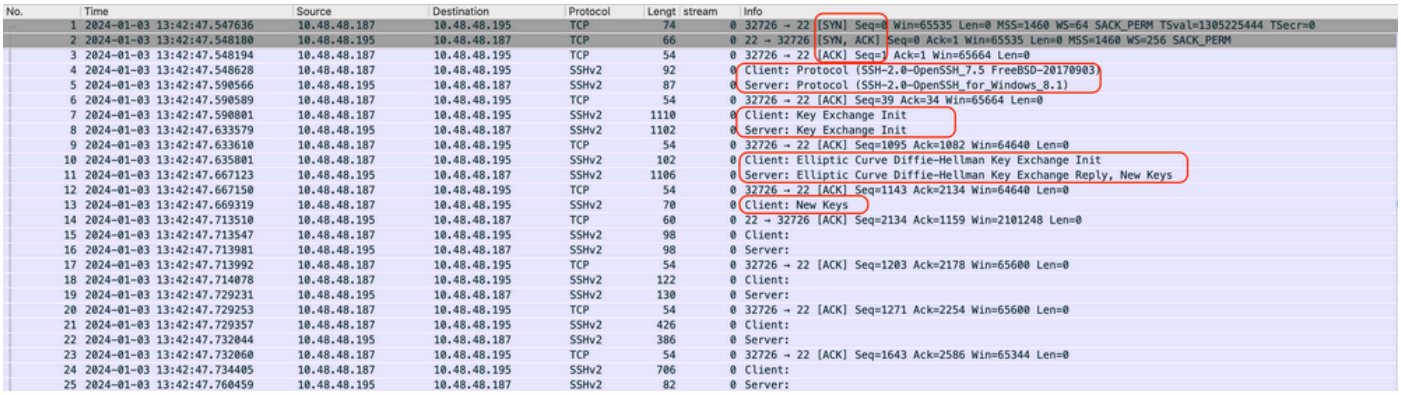
[1] Compruebe si el firewall del servidor SCP está bloqueando el acceso.

[2] Compruebe si hay algún firewall en la ruta desde SWA hasta el servidor SCP que bloquee el acceso.

[3] Verifique si el puerto TCP 22 está en estado de escucha en el servidor SCP .

[4] Ejecute la captura de paquetes en el servidor SWA y SCP para realizar un análisis más detallado.

A continuación se muestra un ejemplo de la captura de paquetes de una conexión exitosa:



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:

Imagen - Captura de paquetes de conexión correcta

Referencias

[Directrices sobre prácticas recomendadas de Cisco Web Security Appliance: Cisco]

[BRKSEC-3303 (CiscoLive)]

[Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance - GD (implementación general) - Conexión, instalación y configuración [Cisco Secure Web Appliance] - Cisco]

[Introducción a OpenSSH para Windows | Microsoft Learn]

Configuración de SSH Public Key Authentication en Windows | Concentrador del sistema operativo Windows (woshub.com)

Autenticación basada en claves en OpenSSH para Windows | Microsoft Learn

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).