Configuration des journaux de transmission SCP dans SWA avec Microsoft Server

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

SCP

Abonnement au journal SWA

Archivage des fichiers journaux

Configurer la récupération du journal via SCP sur le serveur distant

- Configurer SWA pour envoyer les journaux au serveur distant SCP à partir de l'interface utilisateur graphique
- Configurer Microsoft Windows en tant que serveur distant SCP

Diffuser les journaux SCP vers un autre lecteur

Dépannage de la poussée du journal SCP

- Afficher les journaux dans SWA
- Afficher les journaux dans le serveur SCP

Autres informations utiles

Introduction

Ce document décrit les étapes de configuration de Secure Copy (SCP) pour copier automatiquement les journaux dans Secure Web Appliance (SWA) vers un autre serveur.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fonctionnement de la SCP
- administration SWA
- Administration du système d'exploitation Microsoft Windows ou Linux

Cisco vous recommande d'avoir :

- SWA physique ou virtuel installé.
- Licence activée ou installée.
- L'Assistant de configuration est terminé.

- Accès administratif à l'interface utilisateur graphique (GUI) de SWA.
- Microsoft Windows (au moins Windows Server 2019 ou Windows 10 (build 1809).) ou Linux System Installed.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

SCP

Le comportement de Secure Copy (SCP) est similaire à celui de Remote Copy (RCP), qui provient de la suite Berkeley r-tools (propre ensemble d'applications réseau de l'université Berkeley), à ceci près que SCP s'appuie sur Secure Shell (SSH) pour la sécurité. En outre, la SCP exige que l'authentification, l'autorisation et la comptabilisation (AAA) d'autorisation soient configurées afin que le périphérique puisse déterminer si l'utilisateur a le niveau de privilège correct

La méthode SCP sur serveur distant (équivalente à SCP Push) copie périodiquement les fichiers journaux sur un serveur distant en utilisant SCP sur un serveur SCP distant. Cette méthode nécessite un serveur SSH SCP sur un ordinateur distant avec le protocole SSH2. L'abonnement nécessite un nom d'utilisateur, une clé SSH et un répertoire de destination sur l'ordinateur distant. Les fichiers journaux sont transférés en fonction d'un calendrier de transfert que vous avez défini.

Abonnement au journal SWA

Vous pouvez créer plusieurs abonnements au journal pour chaque type de fichier journal. Les abonnements incluent les détails de configuration pour l'archivage et le stockage, notamment :

- Paramètres de substitution, qui déterminent le moment où les fichiers journaux sont

archivés.
- Paramètres de compression des journaux archivés.
- Paramètres de récupération des journaux archivés, qui spécifient si les journaux sont archivés sur un serveur distant ou stockés sur l'appliance.

Archivage des fichiers journaux

Archive (transfert) AsyncOS des abonnements aux journaux lorsqu'un fichier journal en cours atteint une limite spécifiée par l'utilisateur de taille de fichier maximale ou de temps maximal depuis la dernière substitution.

Ces paramètres d'archivage sont inclus dans les abonnements aux journaux :

- Survol par taille de fichier
- Défilement par heure
- Compression du journal
- Méthode De Récupération

Vous pouvez également archiver manuellement les fichiers journaux (de substitution).
Étape 1. Choisissez System Administration > Log Subscriptions.
Étape 2. Cochez la case dans la colonne Rollover du journal des abonnements à archiver ou cochez la case All pour sélectionner tous les abonnements.
Étape 3. Cliquez sur Rollover Now pour archiver les journaux sélectionnés.

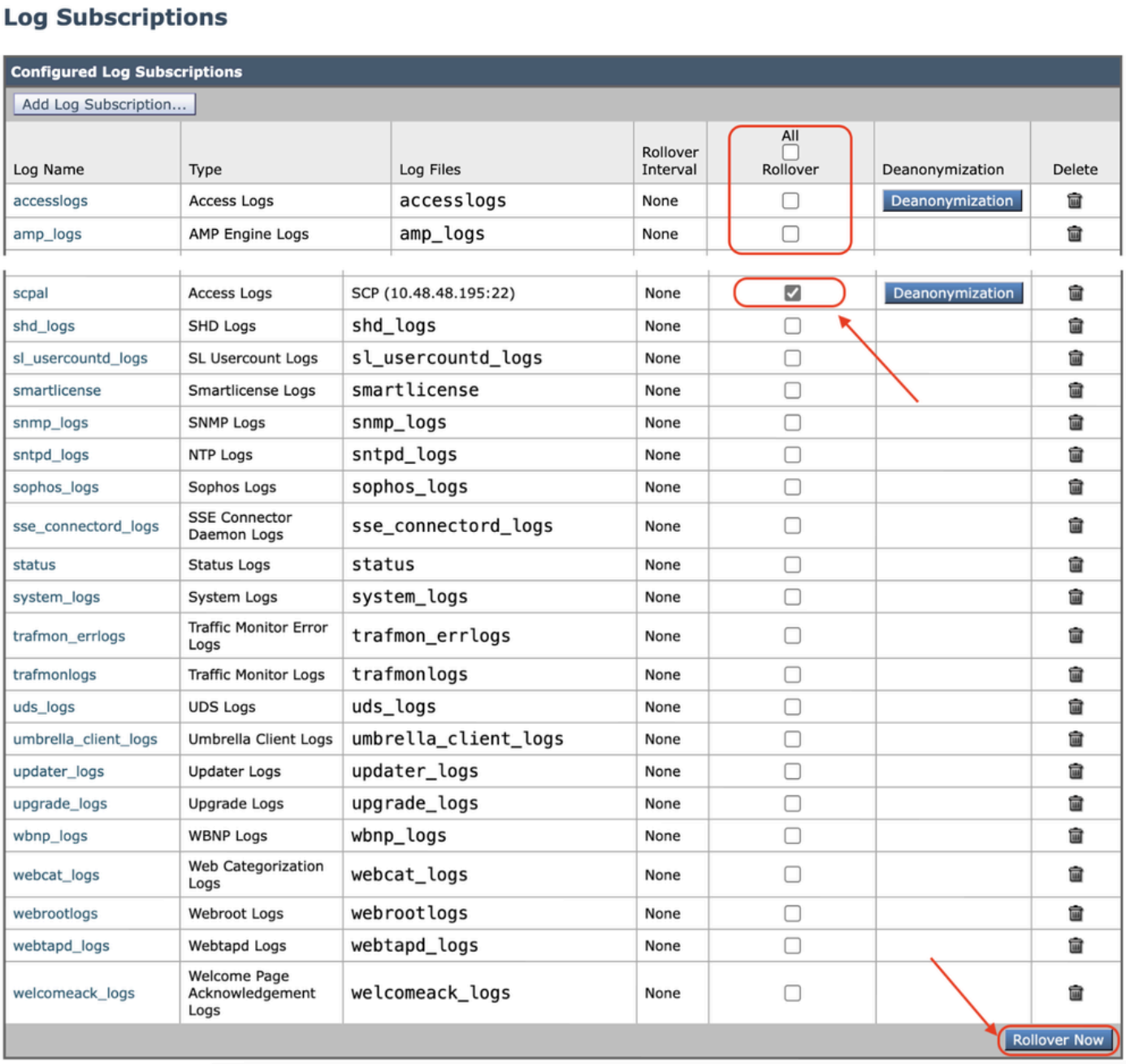


Image - Interface utilisateur graphique de survol

Configurer la récupération du journal via SCP sur le serveur distant

Il existe deux étapes principales pour que la récupération du journal sur un serveur distant avec SCP à partir de SWA :

1. Configurez SWA pour pousser les journaux.
2. Configurez le serveur distant pour recevoir les journaux.

Configurer SWA pour envoyer les journaux au serveur distant SCP à partir de l'interface utilisateur graphique

Étape 1. Connectez-vous à SWA et, dans Administration système, choisissez Log Subscriptions.

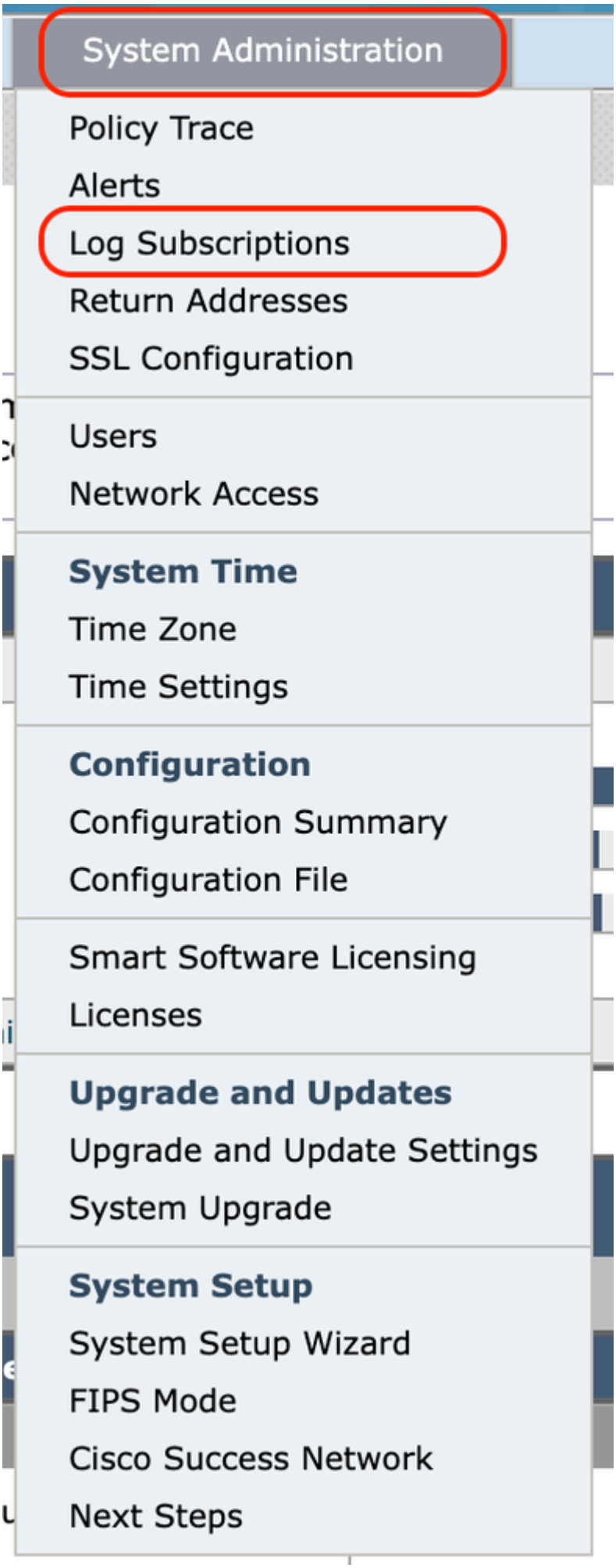

System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary
Configuration File
Smart Software Licensing
Licenses
Upgrade and Updates
Upgrade and Update Settings
System Upgrade
System Setup
System Setup Wizard
FIPS Mode
Cisco Success Network
Next Steps

Image - Choisir les abonnements au journal

Étape 2. Sur la page Inscriptions au journal, choisissez Ajouter une inscription au journal :



Image - Sélectionnez Ajouter un abonnement au journal

Étape 3. Sélectionnez le type de journal. Dans cet exemple, le journal d'accès a été sélectionné.

Étape 4. Entrez un nom pour votre inscription au journal .

Étape 5. (Facultatif) Vous pouvez modifier la substitution par taille de fichier.

Étape 6. Dans la méthode Retrieval, choisissez SCP on Remote Server.

Étape 7. Entrez ces informations pour vos serveurs distants :

- Nom d'hôte ou adresse IP SCP
- Numéro de port d'écoute sur le serveur distant écoutant SSH (TCP/22 par défaut)
- Nom du répertoire
- Nom d'utilisateur pour la connexion au serveur distant

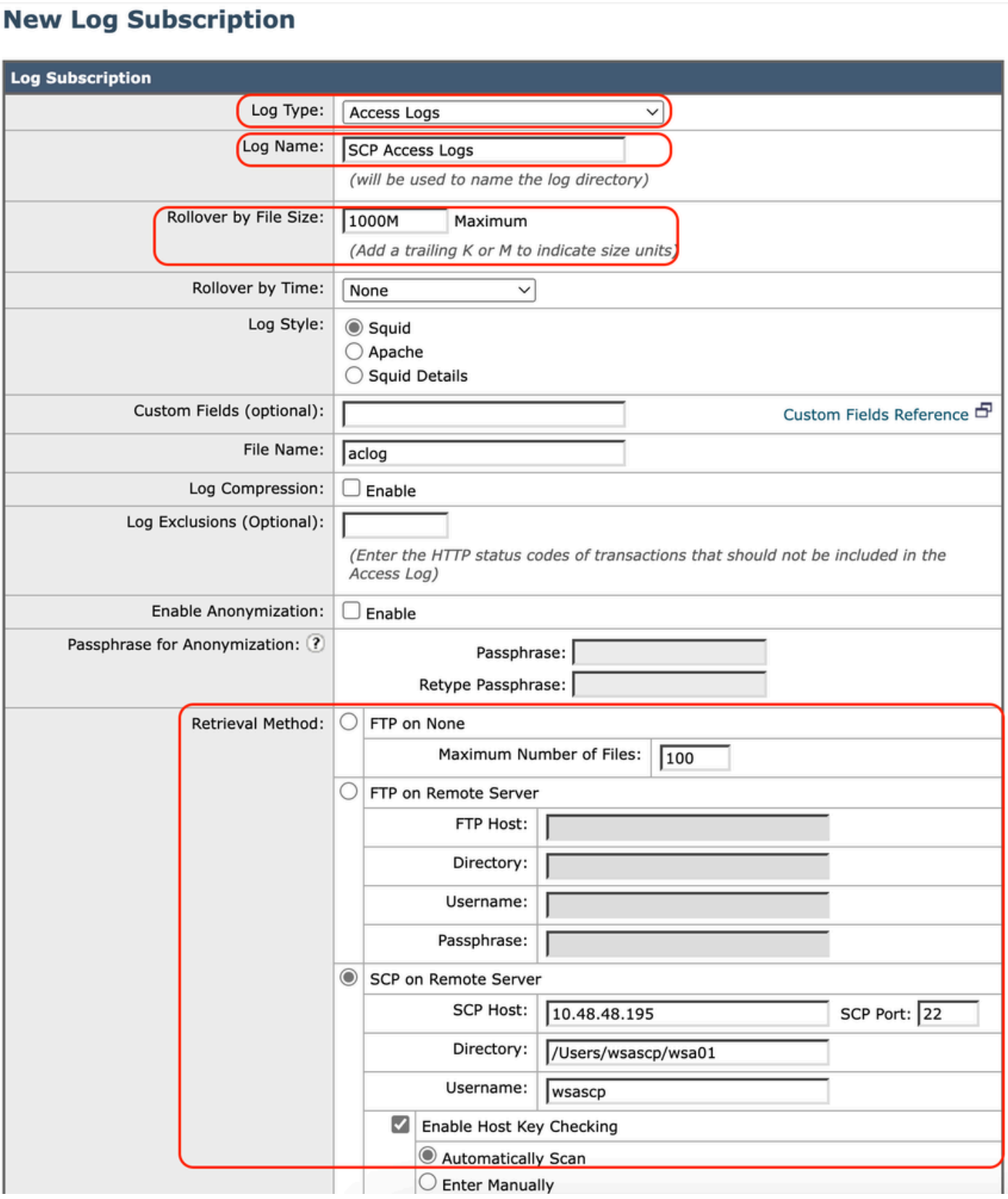


Image - Configuration des paramètres du journal

Remarque : Dans cet exemple, le nom d'utilisateur est wsascp et le serveur distant est le système d'exploitation Microsoft Windows. Un dossier wsa01 a été créé dans le dossier c:\users\wccpscp (qui est le dossier du profil utilisateur dans Microsoft).

Conseil : Vous pouvez simplement taper le nom du dossier ; dans cet exemple, il s'agit de wsa01.

Étape 8. Soumettre les modifications

Étape 9. Enregistrez la clé SSH dans un fichier texte pour une utilisation ultérieure dans la section de configuration du serveur SCP distant.

Remarque : Vous devez copier les deux lignes commençant par ssh- et se terminant par root@<SWA hostname> .

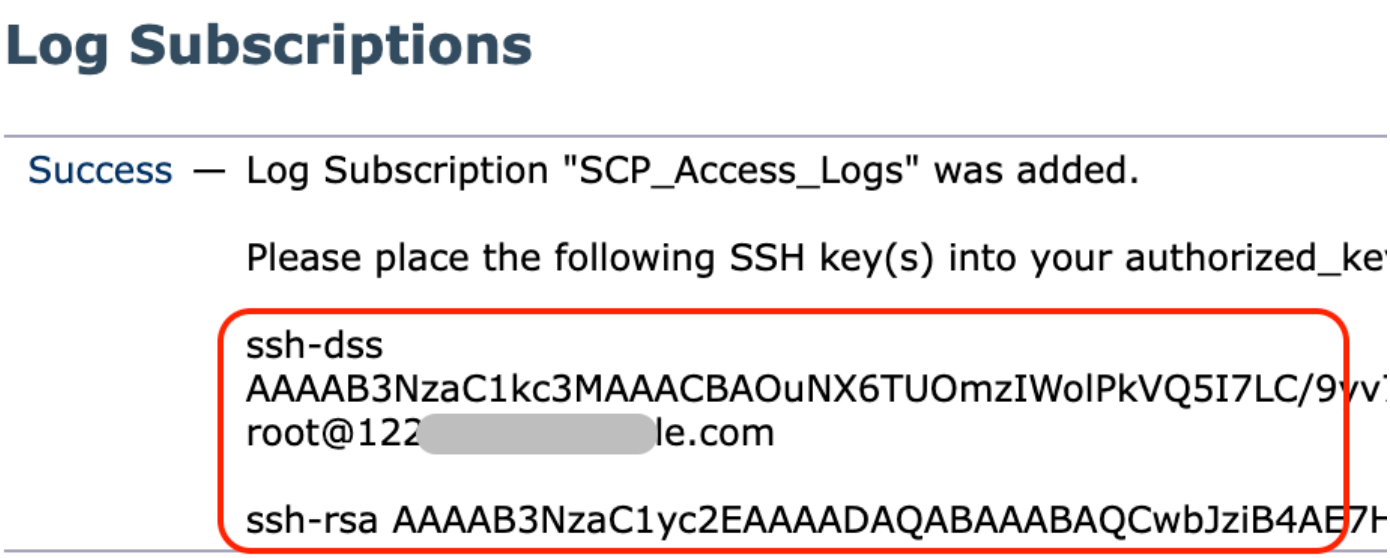


Image : enregistrez la clé SSH pour une utilisation ultérieure.

Étape 10. Validez les modifications.

Configurer Microsoft Windows en tant que serveur distant SCP

Étape 11. Pour créer un utilisateur pour votre service SCP, accédez à Computer Management :

Remarque : Si vous avez déjà un utilisateur pour SCP, passez à l'étape 16.

Étape 12. Sélectionnez Utilisateurs et groupes locaux, puis choisissez Utilisateurs dans le volet de

gauche.

Étape 13. Cliquez avec le bouton droit sur la page principale et sélectionnez nouvel utilisateur.

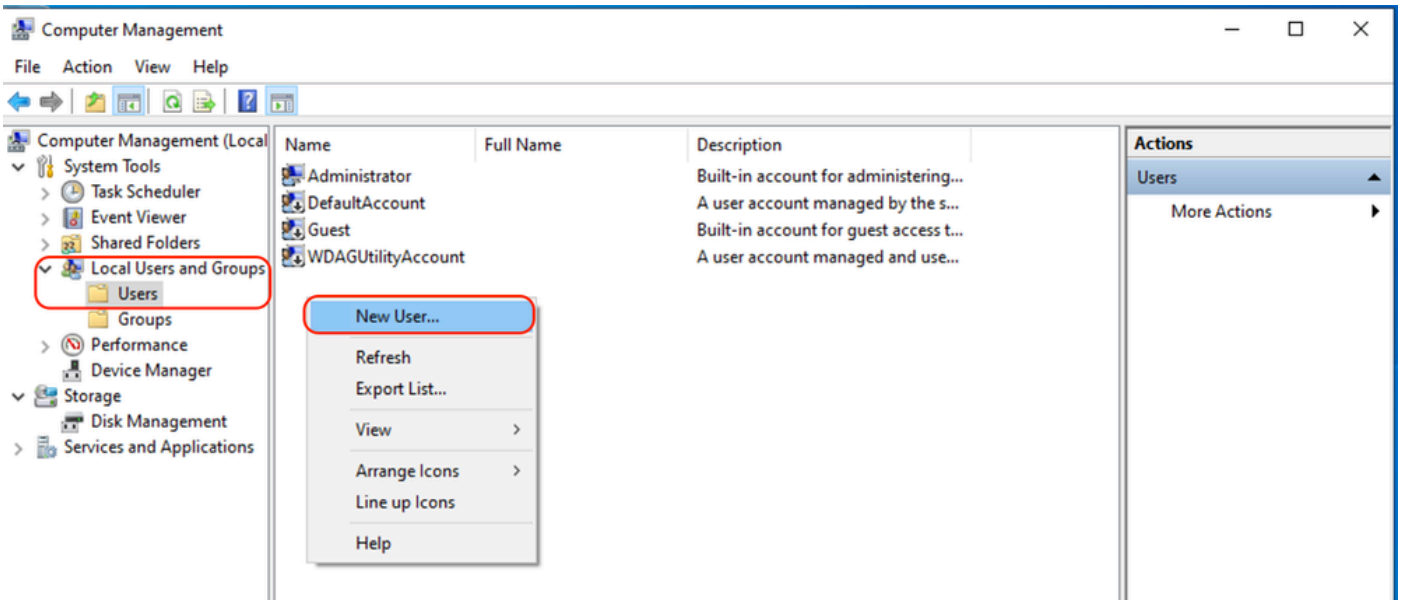


Image - Créer un utilisateur pour le service SCP.

Étape 14. Entrez le nom d’utilisateur et le mot de passe souhaité.

Étape 15. Choisissez Password Never Expires.

Étape 16. Cliquez sur Create, puis fermez la fenêtre.

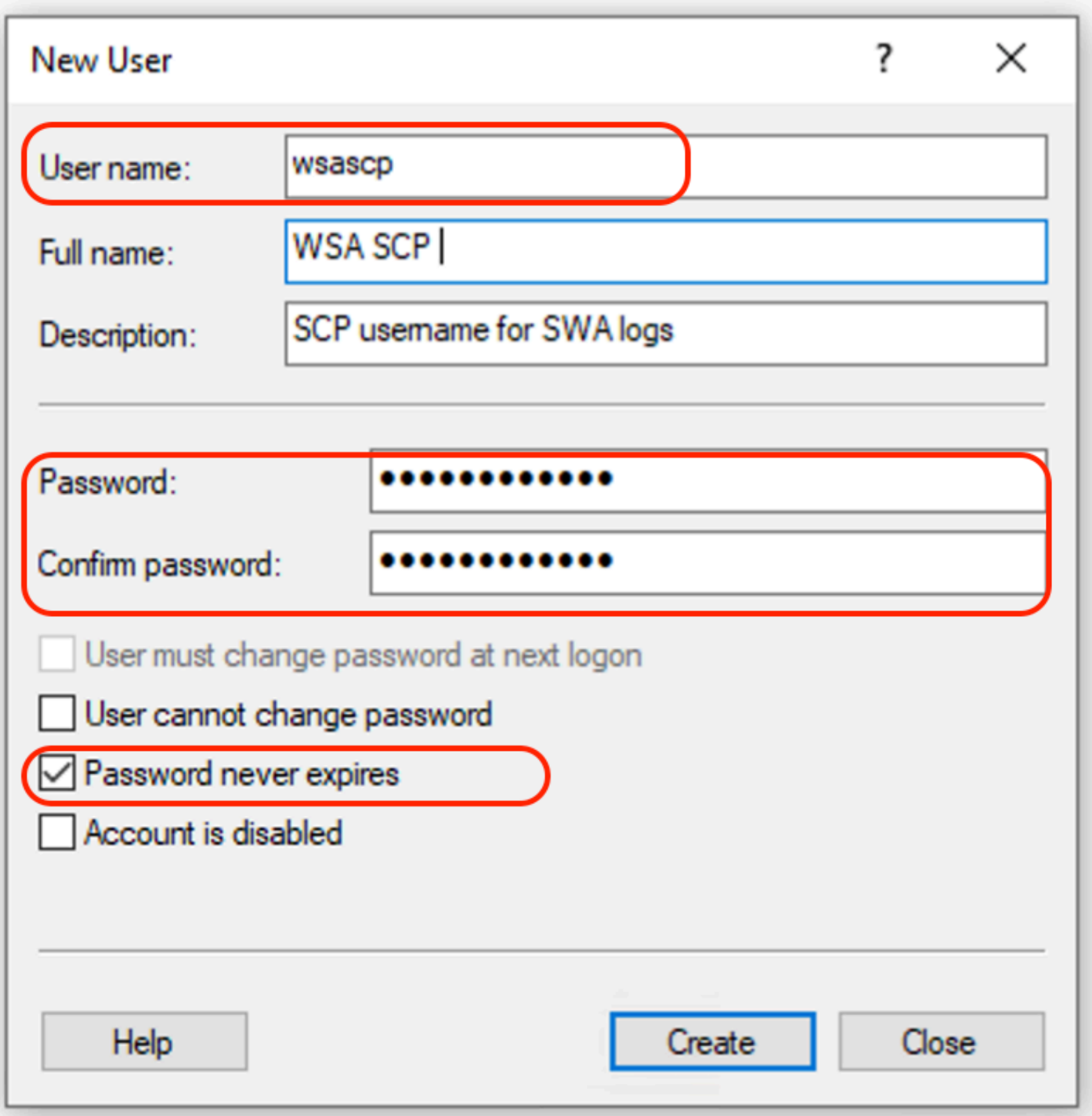


Image : saisissez les informations relatives au nouvel utilisateur.

Étape 17. Connectez-vous au serveur SCP distant avec le nouvel utilisateur pour créer le répertoire de profil.

Remarque : Si OpenSSL est installé sur votre serveur Remote SCP, passez à l'étape 19.

Étape 18. Ouvrez PowerShell avec des privilèges d'administrateur (Exécuter en tant qu'administrateur) et exécutez cette commande pour vérifier les conditions requises :

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

Si la sortie est True, vous pouvez continuer. Sinon, consultez l'équipe d'assistance Microsoft,

Étape 19.Pour installer OpenSSH à l'aide de PowerShell avec le privilège Administrateur (Exécuter en tant qu'administrateur), exécutez :

```
# 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
```

Voici un exemple de résultats positifs :

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

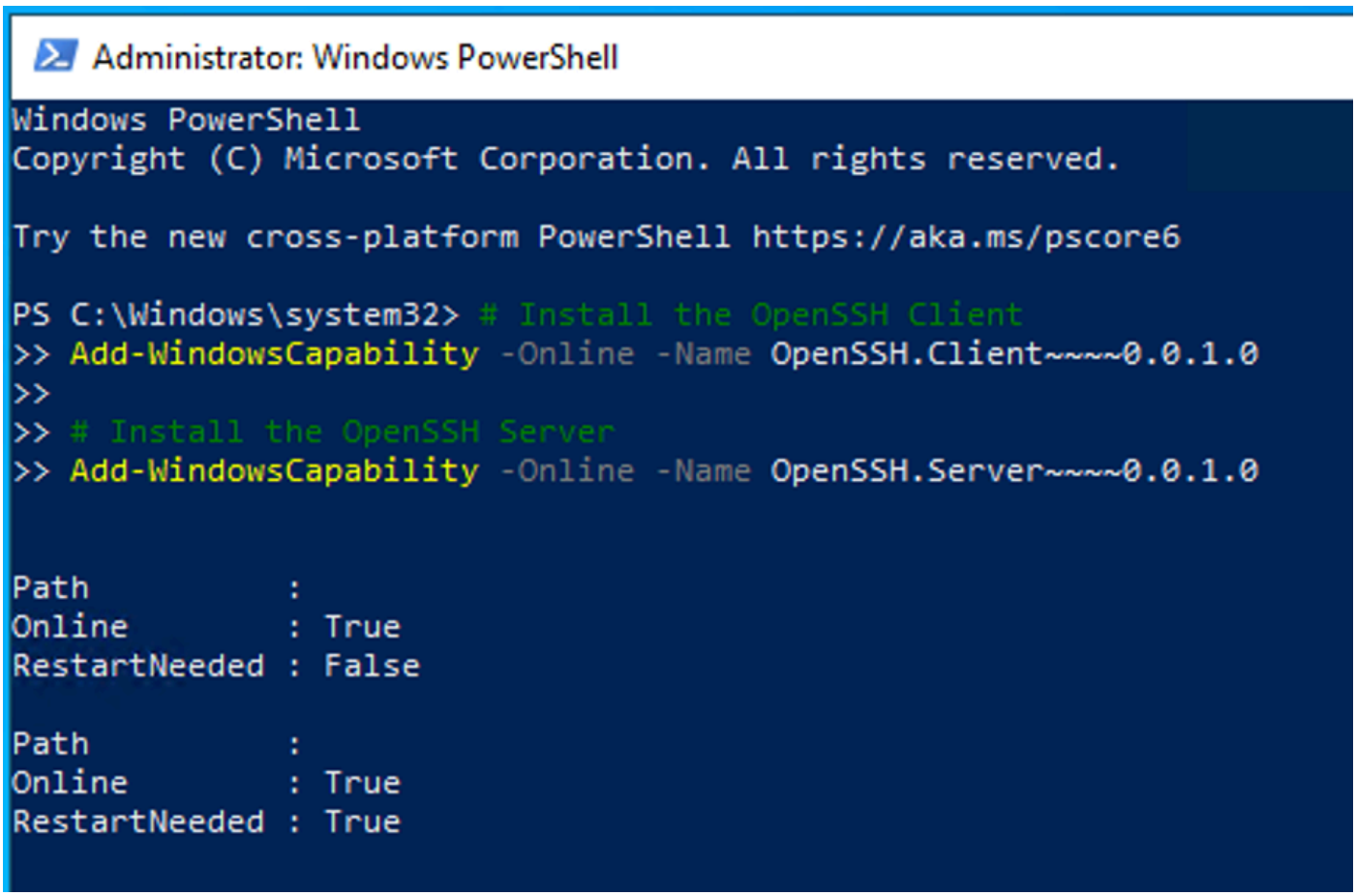


Image - Installer OpenSSH dans PowerShell

⚠ Mise en garde : Si RestartNeeded est défini sur True, veuillez redémarrer Windows.

Pour plus d'informations sur l'installation sur d'autres versions de Microsoft Windows, visitez [Get started with OpenSSH for Windows | Microsoft Learn.]

Étape 20. Ouvrez une session PowerShell normale (sans élévation de privilèges) et générez une paire de clés RSA à l'aide de la commande :

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

Une fois la commande terminée, vous pouvez voir que le dossier .ssh a créé votre répertoire de profil utilisateur.

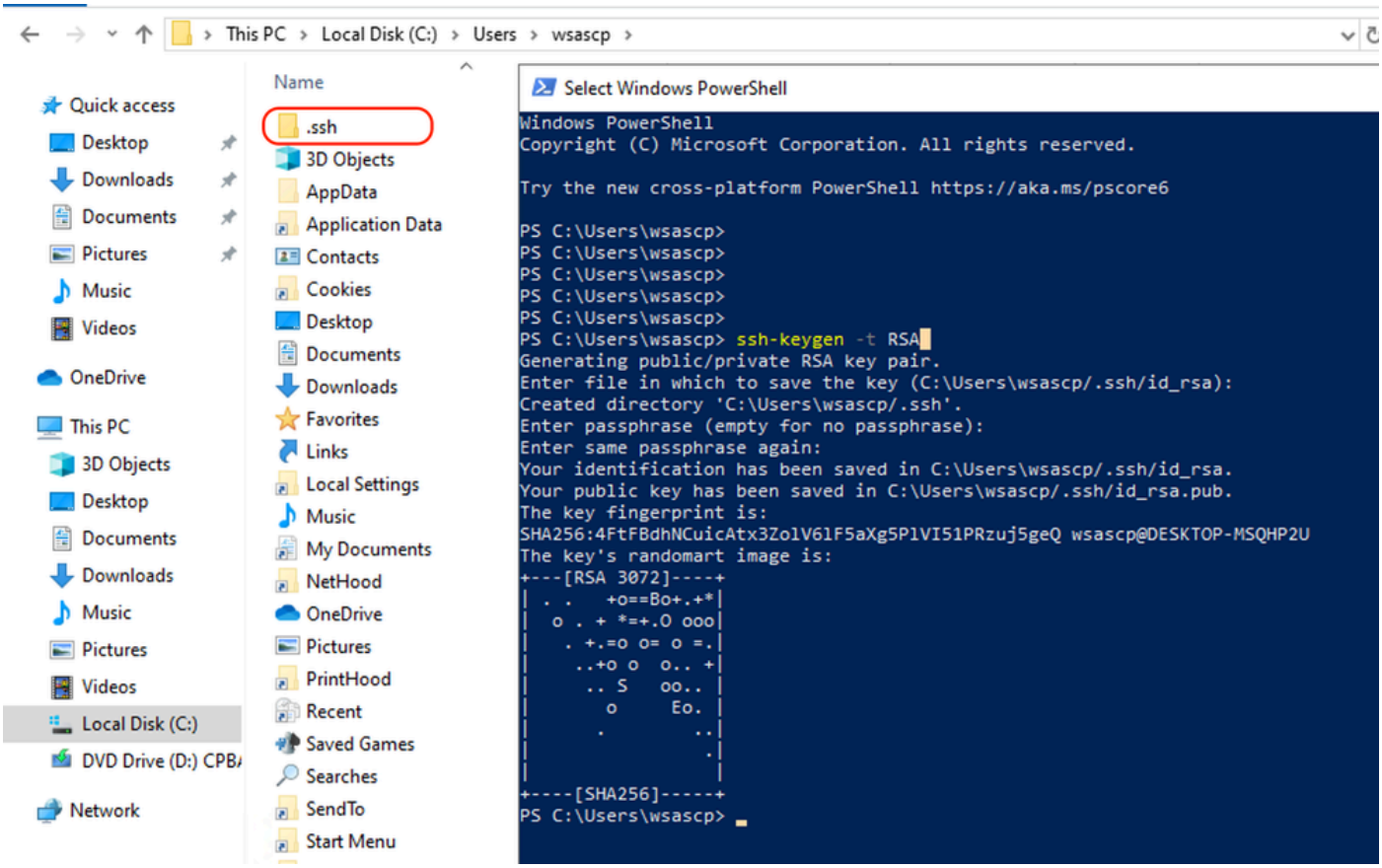


Image - Générer la clé RSA

Étape 21. Démarrez le service SSH à partir de PowerShell avec le privilège Administrateur

(Exécuter en tant qu'administrateur).

```
Start-Service sshd
```

Étape 22. (Facultatif mais recommandé) Remplacez le type de démarrage du service par Automatique, avec le privilège Administrateur (Exécuter en tant qu'administrateur).

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

Étape 23. Confirmez que la règle de pare-feu autorisant l'accès au port TCP 22 a été créée.

```
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction SilentlyContinue | Select-Object Na
    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."
}
```

Étape 24. Modifiez le fichier de configuration SSH situé dans : %programdata%\ssh\sshd_config dans le Bloc-notes, en supprimant le # pour RSA et 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
```

Étape 25. Modifier les conditions de connexion dans %programdata%\ssh\sshd_config. Dans cet exemple, l'adresse d'écoute est pour toutes les adresses d'interface. Vous pouvez personnaliser ce paramètre en fonction de votre conception de déploiement.

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

Étape 26. Marquez ces deux lignes à la fin du fichier %programdata%\ssh\sshd_config en ajoutant # au début de chaque ligne :

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

Étape 27. (Facultatif) Modifiez les modes Strict Modes dans %programdata%\ssh\sshd_config. Par défaut, ce mode est activé et empêche l'authentification SSH basée sur des clés si les clés privées et publiques ne sont pas correctement protégées.

Décommentez la ligne #StrictModes yes et changez-la en StrictModes no :

```
StrictModes No
```

Étape 28. Supprimez le # de cette ligne dans %programdata%\ssh\sshd_config pour autoriser l'authentification par clé publique

```
PubkeyAuthentication yes
```

Étape 29. Créez un fichier texte authorized_keys dans le dossier .ssh et collez la clé RSA publique SWA (qui a été collectée à l'étape 9) :

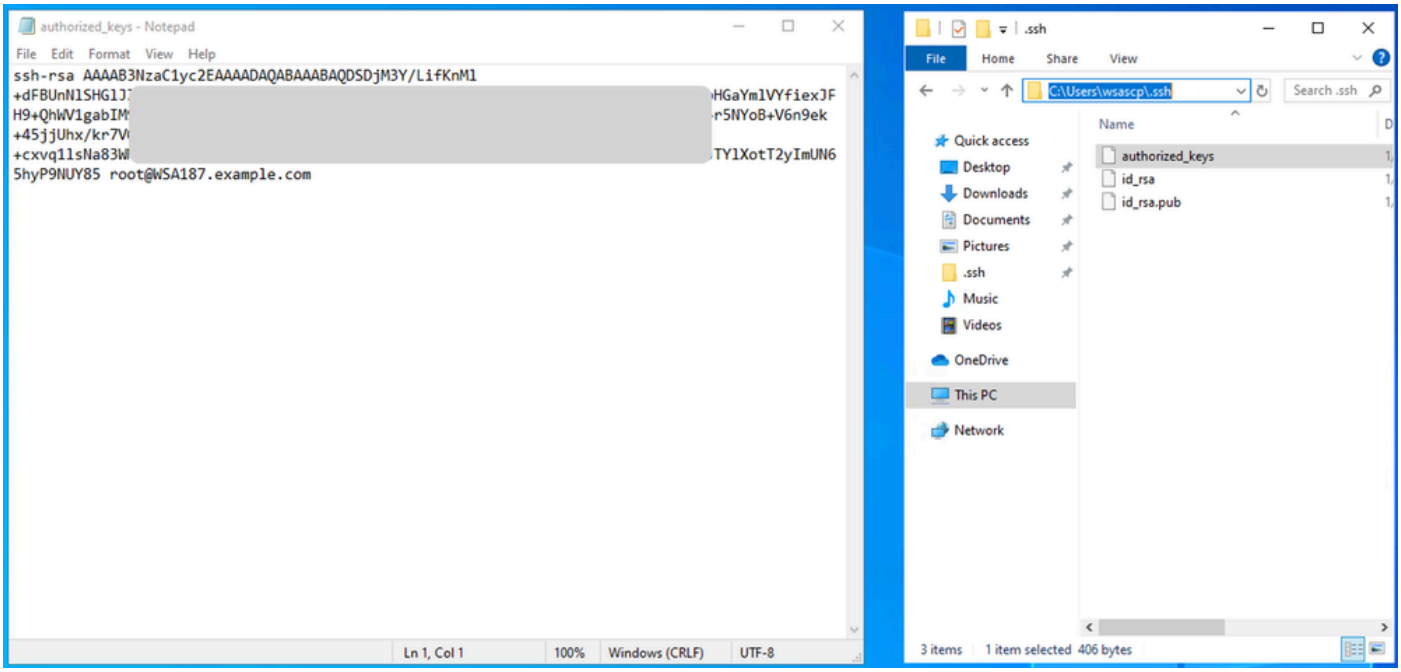


Image - Clé publique SWA

Remarque : copiez la ligne entière, en commençant par ssh-rsa et en terminant par root@<your_SWA_hostname>.

Conseil : Étant donné que RSA est installé sur le serveur SCP, il n'est pas nécessaire de coller la clé ssh-dss.

Étape 30. Activer l'agent d'authentification OpenSSH dans PowerShell avec le privilège Administrateur (Exécuter en tant qu'administrateur).

```
Set-Service -Name ssh-agent -StartupType 'Automatic'
Start-Service ssh-agent
```

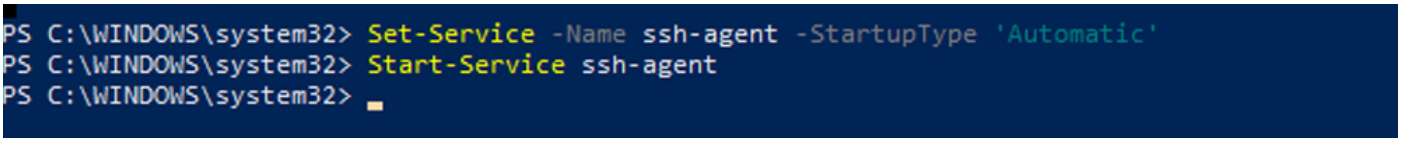


Image - Activer l'agent d'authentification SSH ouvert

Étape 31. (Facultatif) Ajoutez cette ligne à %programdata%\ssh\sshd_config pour autoriser les types de clés :

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

Étape 32. Redémarrez le service SSH. Vous pouvez utiliser cette commande à partir de PowerShell avec le privilège Administrateur (Exécuter en tant qu'administrateur).

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

Étape 33. Pour tester si la transmission SCP est correctement configurée, placez le pointeur sur les journaux configurés, vous pouvez le faire à partir de l'interface graphique utilisateur ou de l'interface de ligne de commande (commande rollovernow) :

```
WSA_CLI> rollovernow scpal
```

Remarque : Dans cet exemple, le nom du journal est scpal.

Vous pouvez confirmer que les journaux sont copiés dans le dossier défini, qui dans cet exemple était c:/Users/wsascp/wsa01.

Diffuser les journaux SCP vers un autre lecteur

Si vous devez pousser les journaux vers un lecteur différent de C, créez un lien du dossier de profil utilisateur vers le lecteur souhaité. Dans cet exemple, les journaux sont envoyés à D:\WSA_Logs\WSA01.

Étape 1. Créez les dossiers dans le lecteur souhaité.

Étape 2. Ouvrez l'invite de commandes avec le privilège Administrateur (Exécuter en tant qu'administrateur).

Étape 3. Exécutez cette commande pour créer le lien :

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

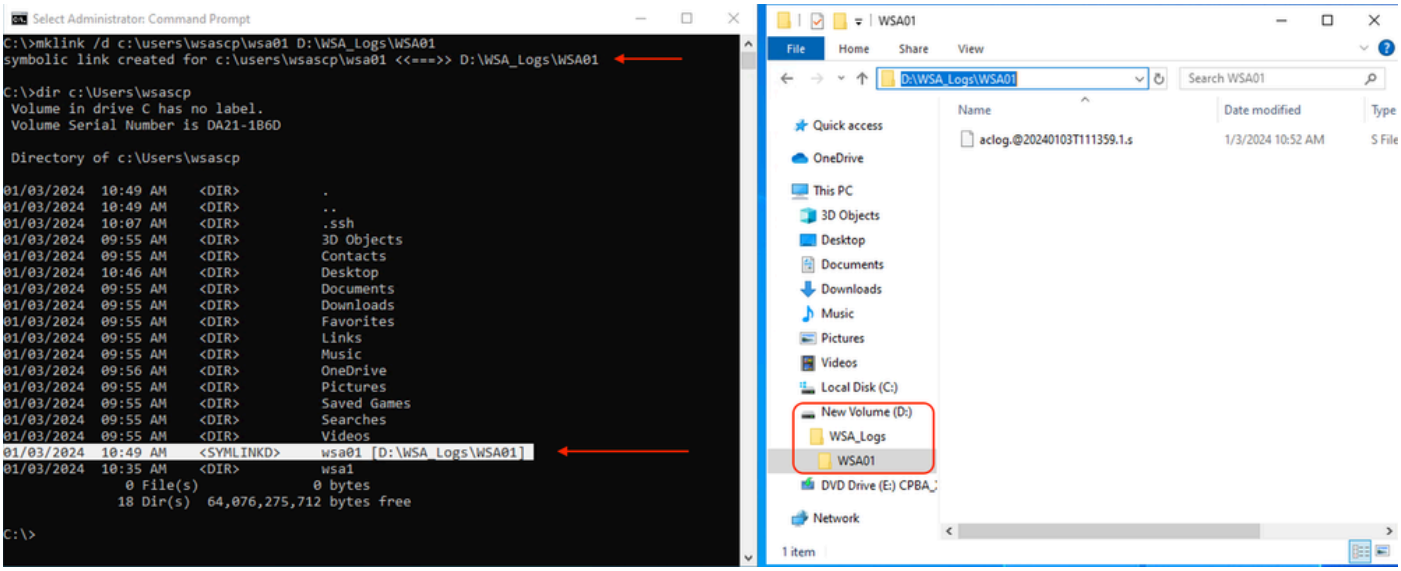


Image - Créer un lien SYM

Remarque : Dans cet exemple, SWA est configuré pour pousser les journaux vers le dossier WSA01 dans C:\Users\wsascp , et le serveur SCP a le dossier WSA01 comme lien symbolique vers D:\WSA_Logs\WSA01 .

Pour plus d'informations sur Microsoft Symbol Link, visitez : mklink | Microsoft Learn

Dépannage de la poussée du journal SCP

Afficher les journaux dans SWA

Pour dépanner la transmission du journal SCP, vérifiez les erreurs dans :

1. CLI > afficher les alertes

2. Journaux_système

Remarque : Pour lire system_logs, vous pouvez utiliser la commande grep dans la CLI . Choisissez le numéro associé à system_logs et répondez à la question dans l'assistant.

Afficher les journaux dans le serveur SCP

Vous pouvez lire les journaux du serveur SCP dans Microsoft Event Viewer, dans Applications and Services Logs > OpenSSH > Operational :

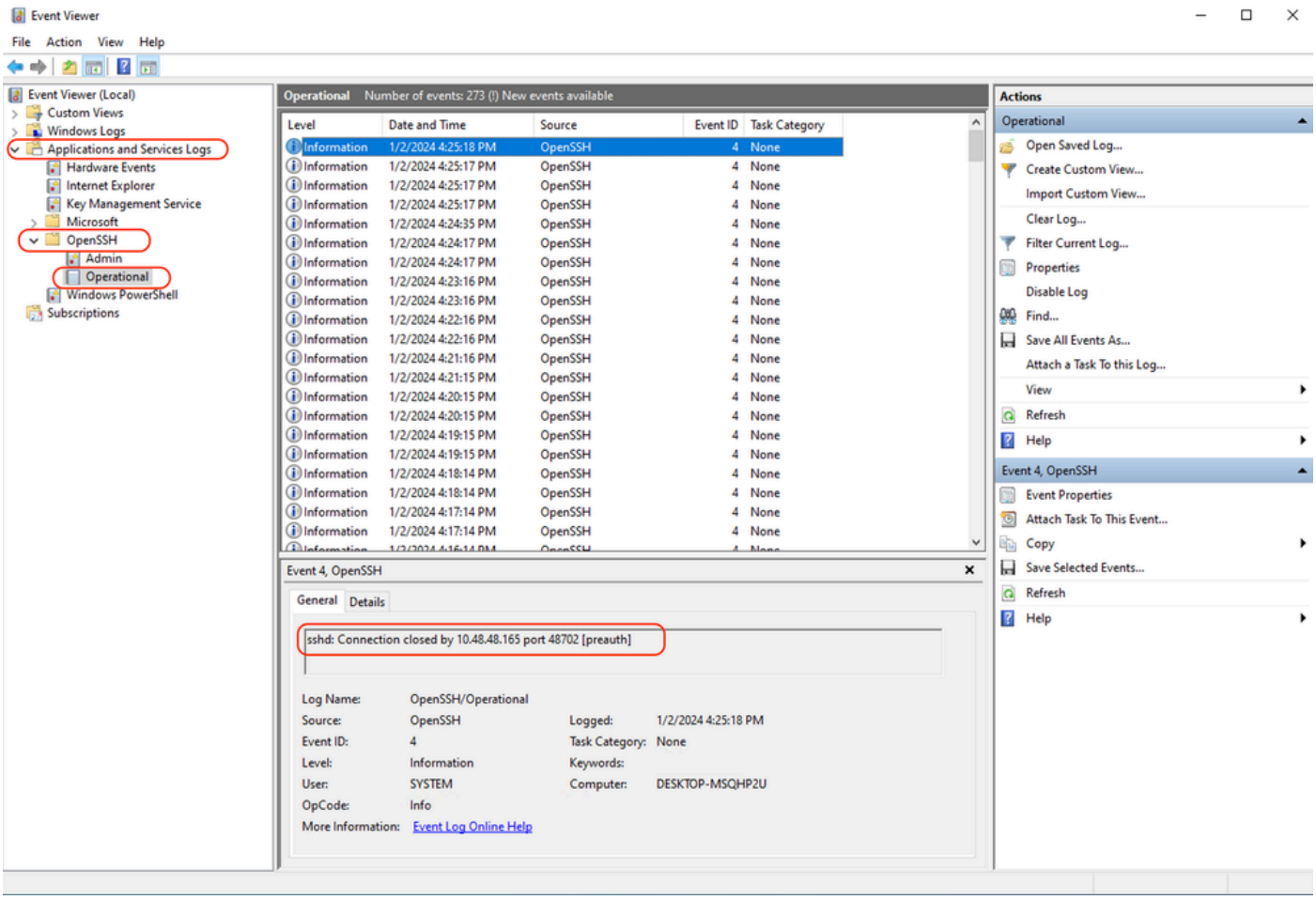


Image - Échec de PreAuth

"Échec de la vérification de la clé hôte."

Cette erreur indique que la clé publique du serveur SCP stockée dans SWA n'est pas valide.

Voici un exemple d'erreur provenant du résultat de la commande displayalerts dans 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.
```

Voici quelques exemples de l'erreur dans 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
```

Pour résoudre ce problème, vous pouvez copier l'hôte à partir du serveur SCP et le coller dans la page d'abonnement aux journaux SCP. Référez-vous à l'étape 7 dans Configurer SWA pour envoyer les journaux au serveur distant SCP à partir de l'interface graphique utilisateur ou vous pouvez contacter Cisco TAC pour supprimer la clé d'hôte du serveur principal.

"Autorisation refusée (clé publique, mot de passe, clavier interactif)."

Cette erreur indique généralement que le nom d'utilisateur fourni dans SWA n'est pas valide.

Voici un exemple de journal d'erreurs dans 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
```

Voici un exemple d'erreur du serveur SCP : "Utilisateur SCP non valide à partir du port <SWA_IP address> <TCP port SWA se connecte au serveur SCP>".

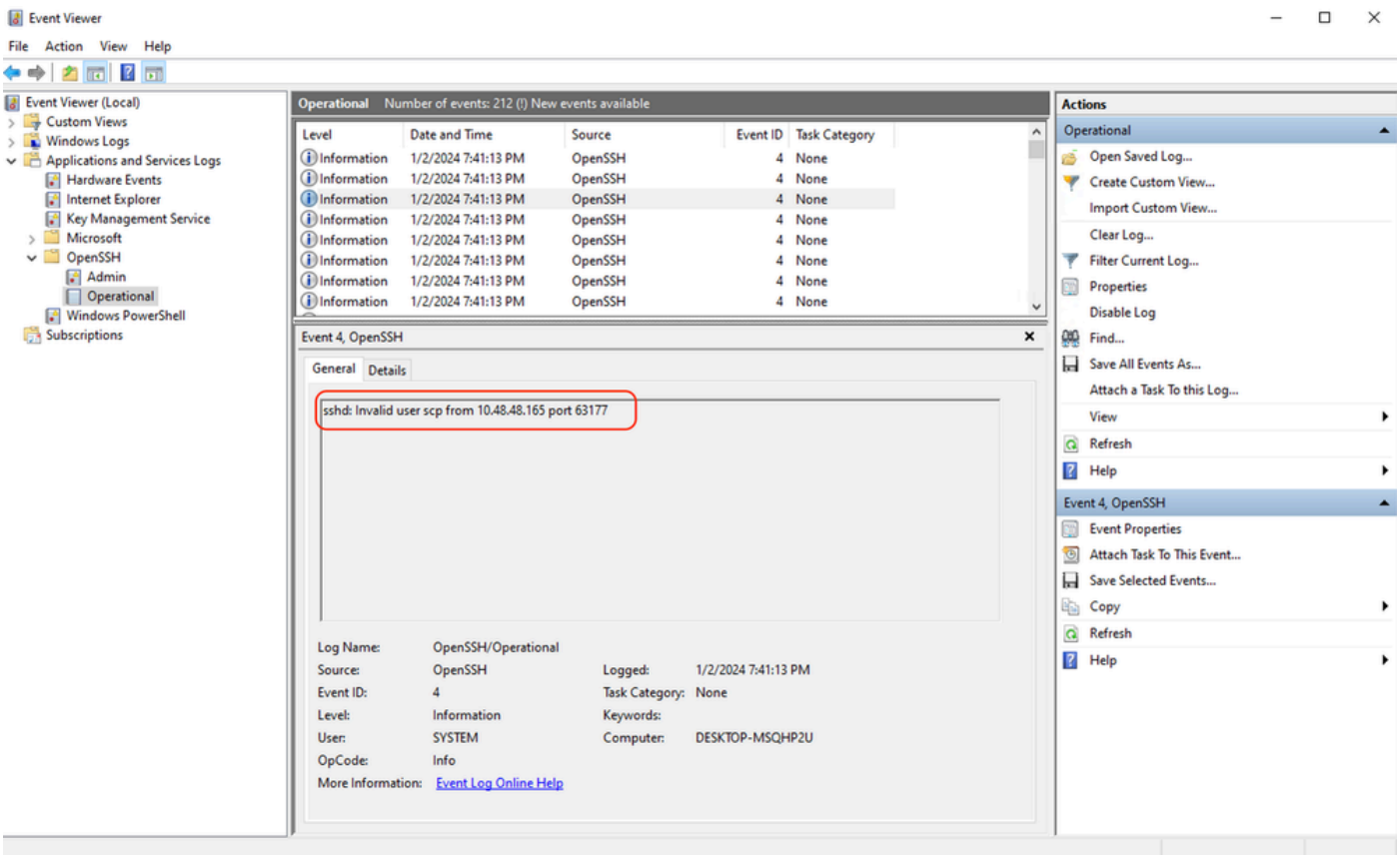


Image - Utilisateur non valide

Pour résoudre cette erreur, vérifiez l'orthographe et assurez-vous que l'utilisateur (configuré dans SWA pour pousser les journaux) est activé dans le serveur SCP.

"Aucun fichier ou répertoire de ce type."

Cette erreur indique que le chemin d'accès fourni dans la section d'abonnement aux journaux SWA n'est pas valide,

Voici un exemple d'erreur 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
```

Pour résoudre ce problème, vérifiez l'orthographe et assurez-vous que le chemin est correct et valide dans le serveur SCP.

"Échec du transfert de SCP."

Cette erreur peut être un indicateur d'une erreur de communication. Voici un exemple d'erreur :

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

Pour dépanner la connectivité, utilisez la commande telnet dans l'interface de ligne de commande 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...
```

Dans cet exemple, la connexion n'est pas établie. La connexion réussie est la suivante :

```
SWA_CLI> telnet

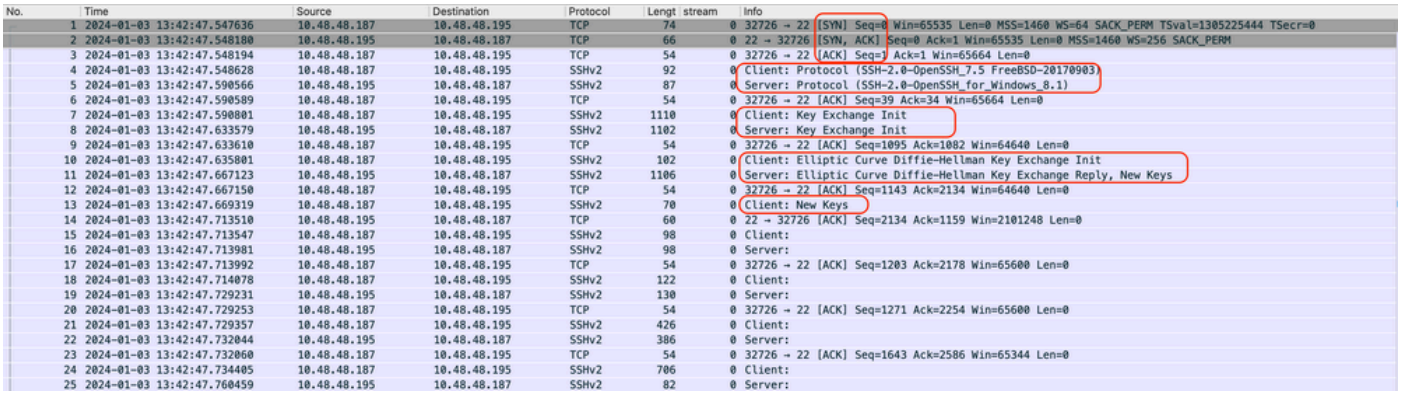
Please select which interface you want to telnet from.
1. Auto
2. Management (10.48.48.187/24: rishi2Man.calo.lab)
[1]> 2
Enter the remote hostname or IP address.
[]> 10.48.48.195
Enter the remote port.
[23]> 22

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

Si la connexion Telnet n'est pas établie :

1. Vérifiez si le pare-feu du serveur SCP bloque l'accès.
2. Vérifiez si des pare-feu bloquent l'accès sur le chemin entre SWA et le serveur SCP.
3. Vérifiez si le port TCP 22 est en état d'écoute sur le serveur SCP.
4. Exécutez la capture de paquets dans les serveurs SWA et SCP pour une analyse plus approfondie.

Voici un exemple de capture de paquets d'une connexion réussie :



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:

Image - Capture de paquets de connexion réussie

"Aucun type de clé d'hôte correspondant trouvé"

Cette erreur indique que les algorithmes de clé d'hôte, fournis par SWA dans la phase d'échange de clé client, ne correspondent pas dans le serveur SCP.

```
Wed Feb 12 20:21:40 2025 Critical: Log Error: Push error for subscription al: SCP failed to transfer to
Wed Feb 12 20:21:40 2025 Critical: Log Error: Push error for subscription al: SCP failed to transfer to
Wed Feb 12 20:21:40 2025 Critical: Log Error: Push error for subscription al: SCP failed to transfer to
```

Pour résoudre ce problème, procédez comme suit :

Étape 1 : lancement d’une capture de paquets dans SWA et filtrage de l’adresse IP du serveur SCP.

Étape 2. Placez le pointeur sur le fichier journal pour vous assurer que SWA envoie les fichiers au serveur SCP.

Étape 3. Arrêtez la capture de paquets et ouvrez le fichier.

Étape 4. Dans le fichier de capture, recherchez un paquet avec Client : Init d'échange de clés dans la section Info.

Étape 5. Développez le protocole SSH et accédez à la section Algorithms.

Étape 6. Vérifiez la chaîne server_host_key_algorithms (par exemple : server_host_key_algorithms chaîne : ssh-rsa)

Étape 7. Accédez au serveur SCP et modifiez le fichier sshd_config.

Étape 8. Recherchez une ligne qui commence par HostKeyAlgorithms et ajoutez la clé d'hôte prise en charge mentionnée à l'étape 6 au fichier. (Dans cet exemple : HostKeyAlgorithms (ssh-rsa)

Remarque : Si aucune ligne n'a démarré avec HostKeyAlgorithms, vous pouvez ajouter la ligne à la fin du fichier.

Étape 9. Enregistrez les modifications et redémarrez le service SSHD.

Autres informations utiles

- Recommandations relatives aux meilleures pratiques des dispositifs de sécurité Web Cisco
- BRKSEC-3303 (ciscolive)
- Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance - GD (General Deployment) - Connect, Install, and Configure [Cisco Secure Web Appliance]
- Premiers pas avec OpenSSH pour Windows | Microsoft Learn
- Configuration de l'authentification de clé publique SSH sous Windows | Concentrateur de système d'exploitation Windows (woshub.com)
- Authentification par clé dans OpenSSH pour Windows | Microsoft Learn

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.