Microsoft Server를 사용하여 Secure Web Appliance에서 SCP 푸시 로그 구성

목차

소개

이 문서에서는 SWA(Secure Web Appliance)의 로그를 다른 서버에 자동으로 복사하도록 SCP(Secure Copy)를 구성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SCP 작동 방식
- SWA 관리.
- Microsoft Windows 또는 Linux 운영 체제의 관리.

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.

- 라이센스가 활성화되었거나 설치되었습니다.
- 설치 마법사가 완료되었습니다.

- SWA GUI(Graphical User Interface)에 대한 관리 액세스
- Microsoft Windows(최소 Windows Server 2019 또는 Windows 10(빌드 1809)) 또는 Linux 시스템 설치됨

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

SCP

SCP(Secure Copy)의 동작은 RCP(Remote Copy)와 유사합니다. RCP는 Berkeley r-tools 제품군(Berkeley 대학교 자체 네트워킹 애플리케이션 세트)에서 제공되지만, SCP는 보안을 위해 SSH(Secure Shell)를 사용한다는 점이 다릅니다. 또한 SCP에서는 디바이스에서 사용자에게 올바른 권한 레벨이 있는지 확인할 수 있도록 AAA(Authentication, Authorization, and Accounting) 권한 부여를 구성해야 합니다

원격 서버의 SCP 방법(SCP 푸시와 동일)은 보안 복사 프로토콜에 의해 로그 파일을 원격 SCP 서버로 주기적으로 푸시합니다. 이 방법을 사용하려면 SSH2 프로토콜을 사용하는 원격 컴퓨터에 SSH SCP 서버가 있어야 합니다. 서브스크립션에는 원격 컴퓨터의 사용자 이름, SSH 키 및 대상 디렉토리가 필요합니다. 로그 파일은 사용자가 설정한 롤오버 일정을 기반으로 전송됩니다.

SWA 로그 서브스크립션

각 로그 파일 유형에 대해 여러 로그 서브스크립션을 생성할 수 있습니다. 서브스크립션에는 다음과 같은 아카이빙 및 스토리지 구성 세부 정보가 포함됩니다.

- 로그 파일이 아카이브되는 시기를 결정하는 롤오버 설정
- 아카이브된 로그에 대한 압축 설정
- 로그가 원격 서버에 아카이브되는지 아니면 어플라이언스에 저장되는지를 지정하는 아카이브된 로그에 대한 검색 설정입니다.

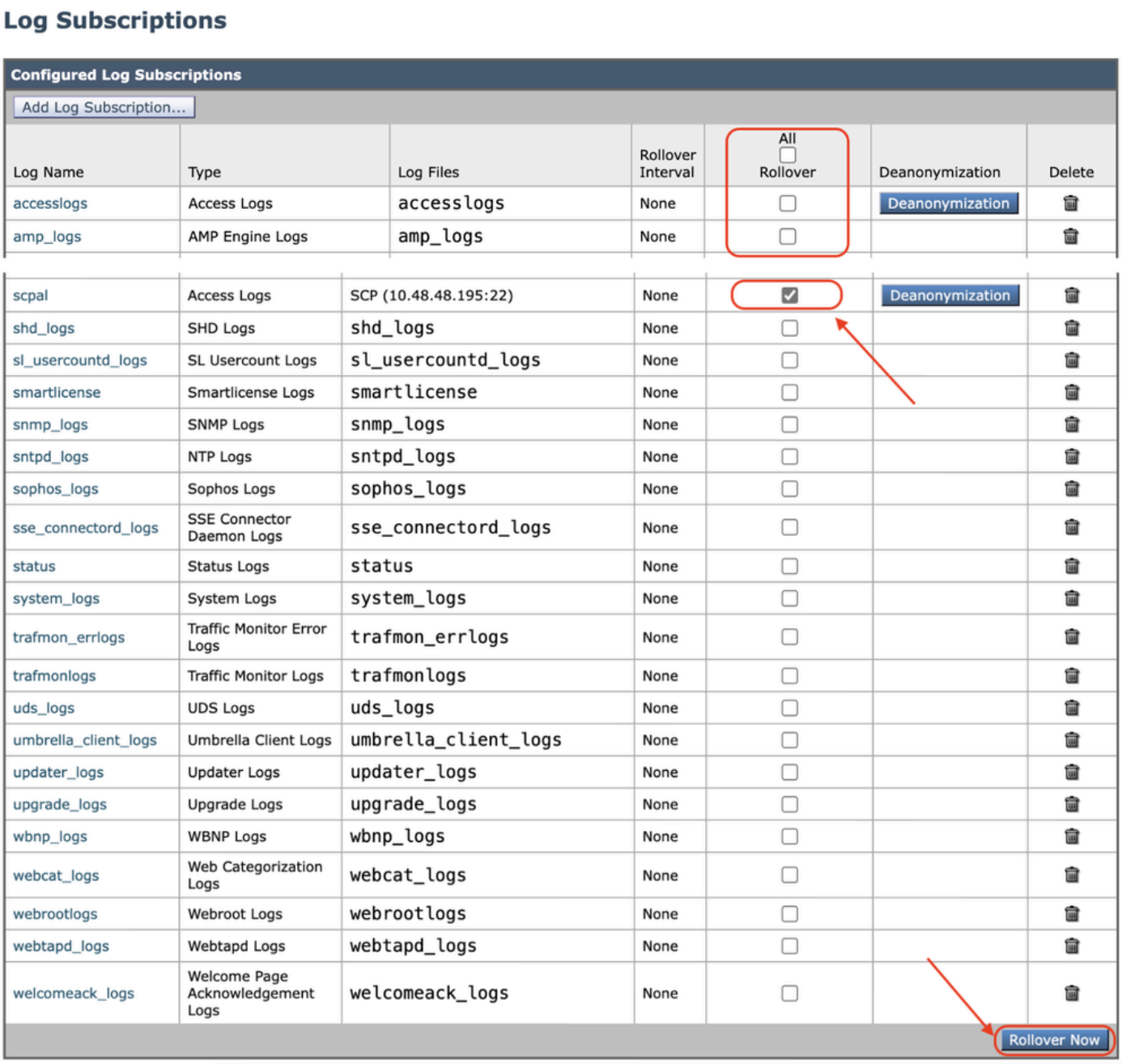
로그 파일 보관

AsyncOS는 현재 로그 파일이 사용자가 지정한 최대 파일 크기 또는 마지막 롤오버 이후 최대 시간 제한에 도달하면 로그 서브스크립션을 아카이브(롤오버)합니다.

이러한 아카이브 설정은 로그 서브스크립션에 포함됩니다.

- 파일 크기별 롤오버
- 시간별 롤오버
- 로그 압축
- 검색 방법

로그 파일을 수동으로 보관(롤오버)할 수도 있습니다.
1단계. System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션)를 선택합니다.
2단계. 아카이브할 로그 서브스크립션의 Rollover(롤오버) 열에서 확인란을 선택하거나 All(모두) 확인란을 선택하여 모든 서브스크립션을 선택합니다.
3단계.Rollover Now(지금 롤오버)를 클릭하여 선택한 로그를 보관합니다.



이미지 - 지금 롤오버 GUI

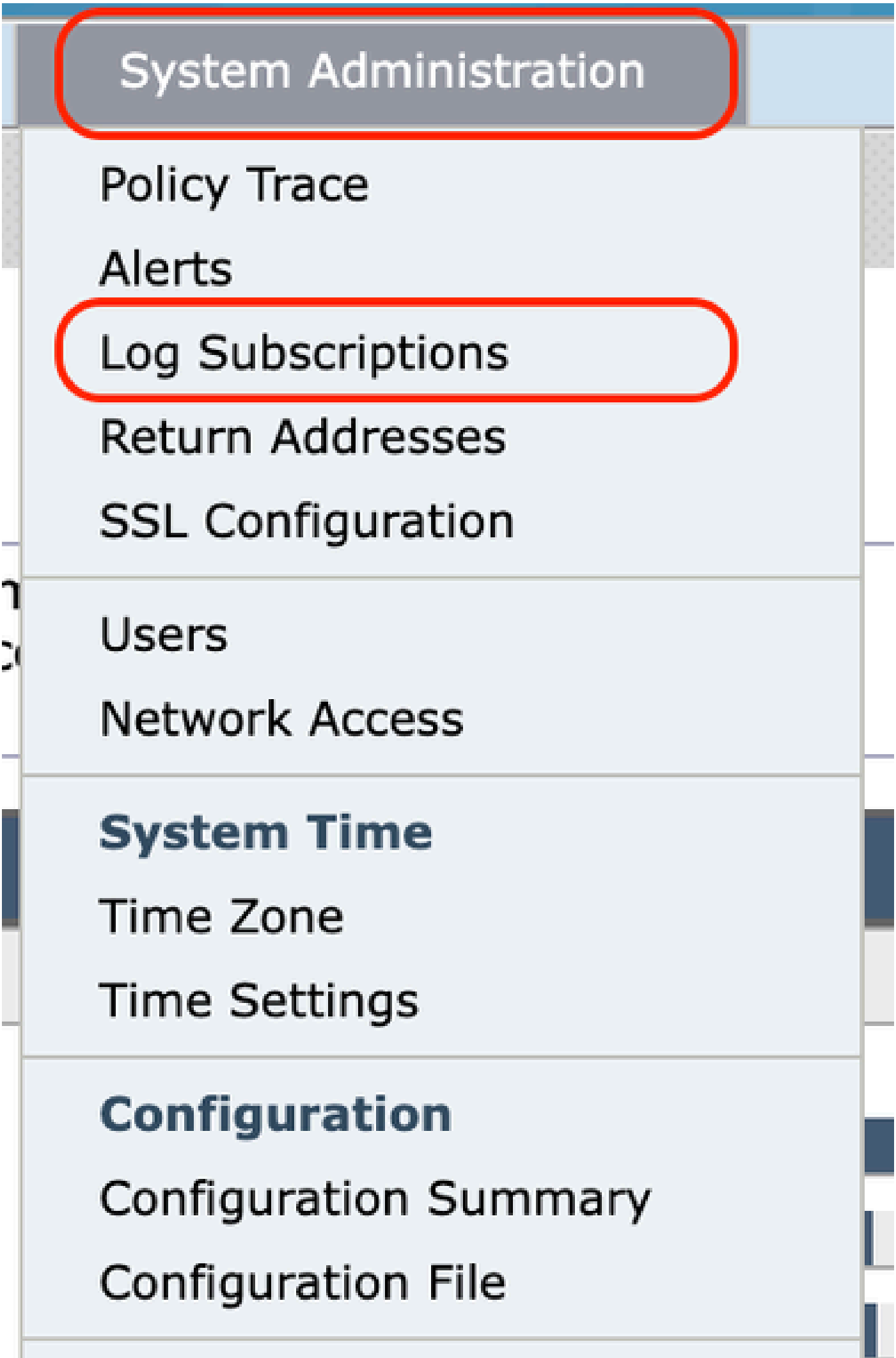
원격 서버의 SCP를 통한 로그 검색 구성

SWA에서 SCP를 사용하여 원격 서버에 로그를 검색하는 두 가지 주요 단계는 다음과 같습니다.

1. 로그를 푸시하도록 SWA를 구성합니다.
2. 로그를 수신하도록 원격 서버를 구성합니다.

GUI에서 SCP 원격 서버로 로그를 전송하도록 SWA 구성

1단계. SWA에 로그인하고 System Administration(시스템 관리)에서 Log Subscriptions(로그 서브스크립션)를 선택합니다.


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

. 이 예에서 수신 주소는 모든 인터페이스 주소에 사용됩니다. 디자인으로 인해 맞춤 제작이 가능합니다.

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

25단계. 각 줄의 시작 부분에 #을 추가하여 %programdata%\ssh\sshd_config 파일 끝에 다음 두 줄을 표시합니다.

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

26단계(선택 사항)%programdata%\ssh\sshd_config에서 Strict Mode를 편집합니다. 기본적으로 이 모드는 활성화되어 있으며 개인 키와 공개 키가 제대로 보호되지 않는 경우 SSH 키 기반 인증을 차단합니다.

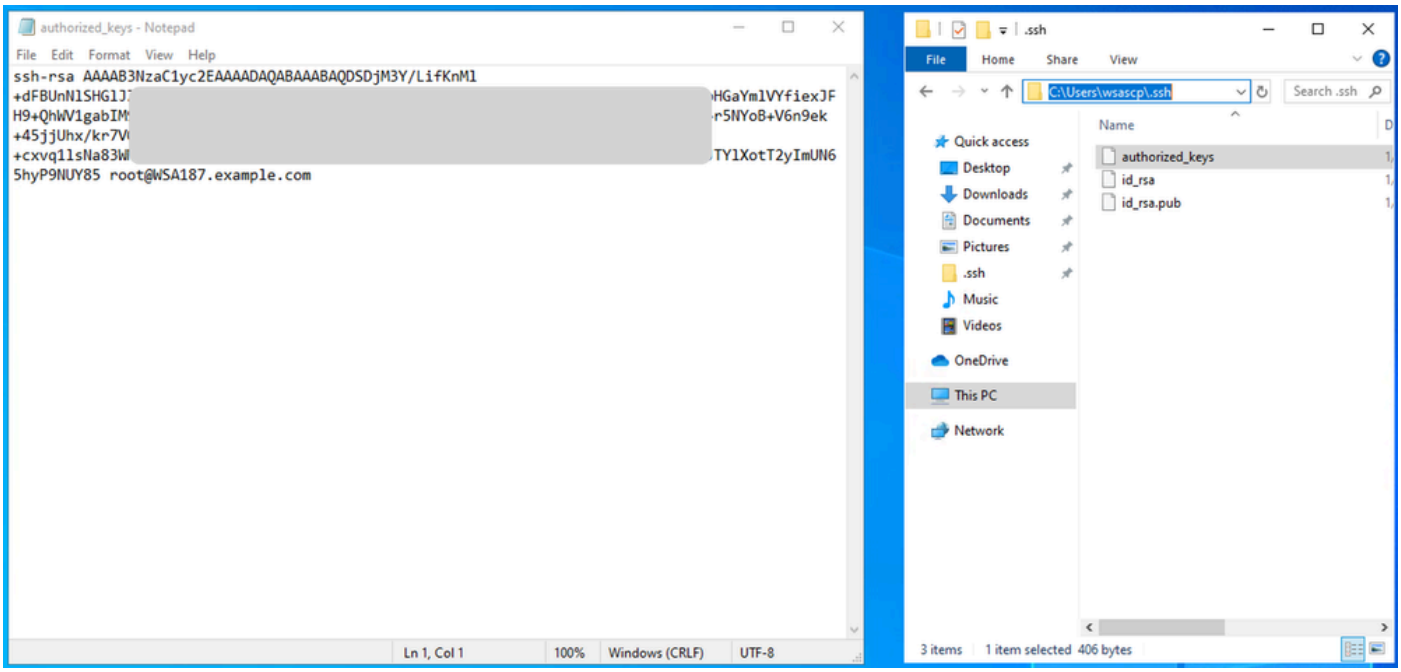
yes 행 주석#StrictModes 제거하고 StrictModes no로 변경합니다.

```
StrictModes No
```

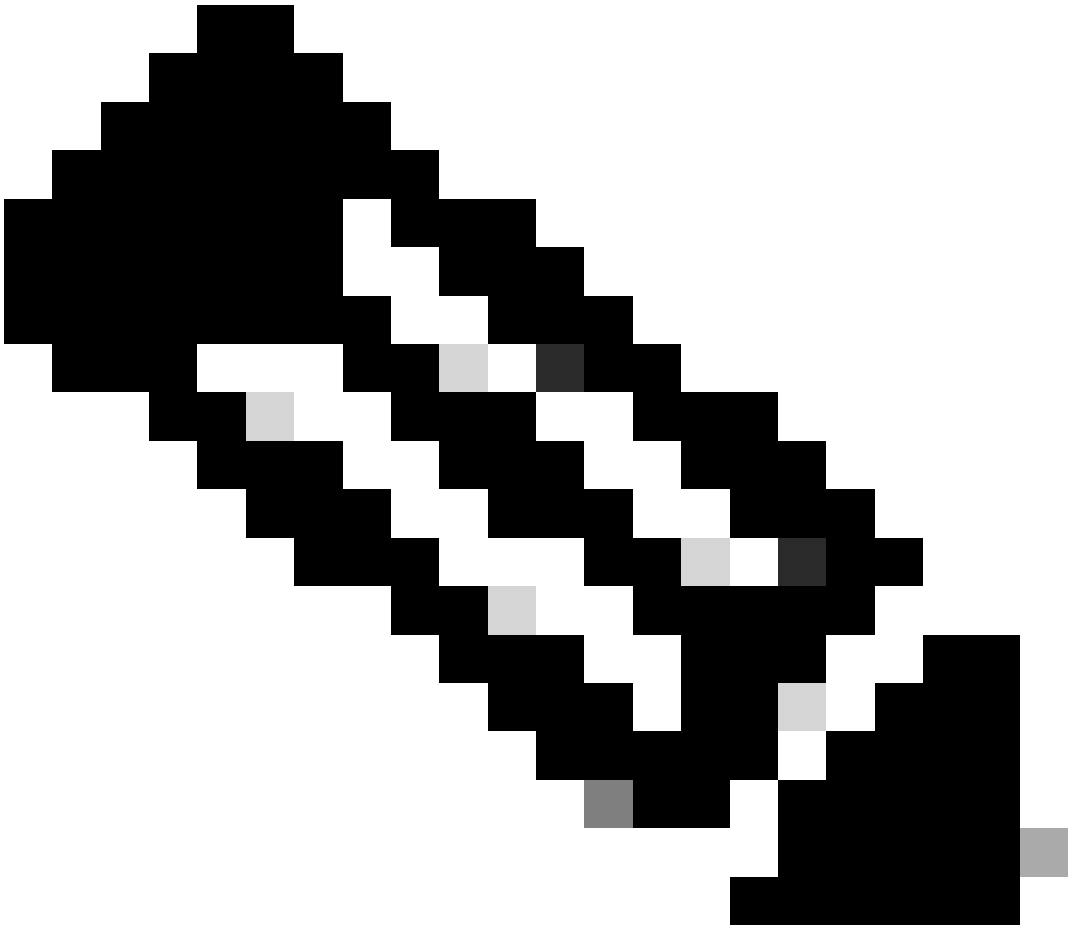
27단계. 공개 키 인증을 허용하려면 이 줄에서 %programdata%\ssh\sshd_config를 제거하십시오.

```
PubkeyAuthentication yes
```

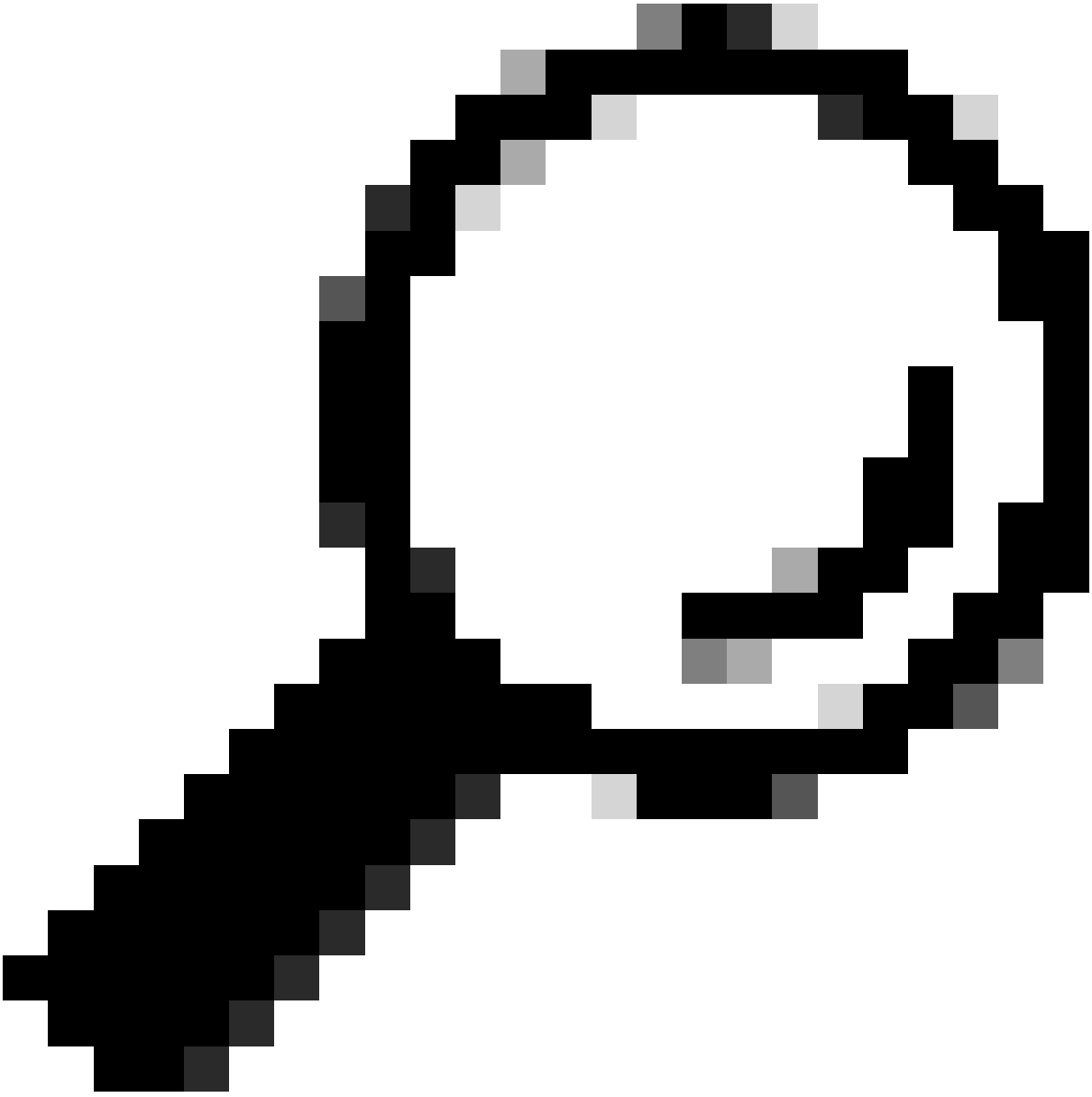
28단계. .ssh 폴더에 텍스트 파일 "authorized_keys"를 만들고 SWA 공용 RSA 키(9단계에서 수집됨)를 붙여넣습니다.


authorized_keys - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSDjM3Y/LifKnMl
5hyP9NUY85 root@WSA187.example.com
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
.ssh
File Home Share View
C:\Users\wsascp\.ssh
Search .ssh
Quick access
Desktop
Downloads
Documents
Pictures
.ssh
Music
Videos
OneDrive
This PC
Network
Name
authorized_keys
id_rsa
id_rsa.pub
3 items
1 item selected 406 bytes

이미지 - SWA 공개 키



참고: ssh-rsa로 시작하고 root@<your_SWA_hostname>으로 끝나는 전체 행을 복사합니다.



팁: RSA가 SCP 서버에 설치되어 있으므로 ssh-dss 키를 붙여 넣을 필요가 없습니다

29단계. 관리자 권한(관리자로 실행)으로 PowerShell에서 "OpenSSH Authentication Agent"를 활성화합니다.

```
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>
```

이미지 - Enable Open SSH Authentication Agent

30단계(선택 사항)키 유형을 허용하려면 %programdata%\ssh\sshd_config에 이 행을 추가합니다.

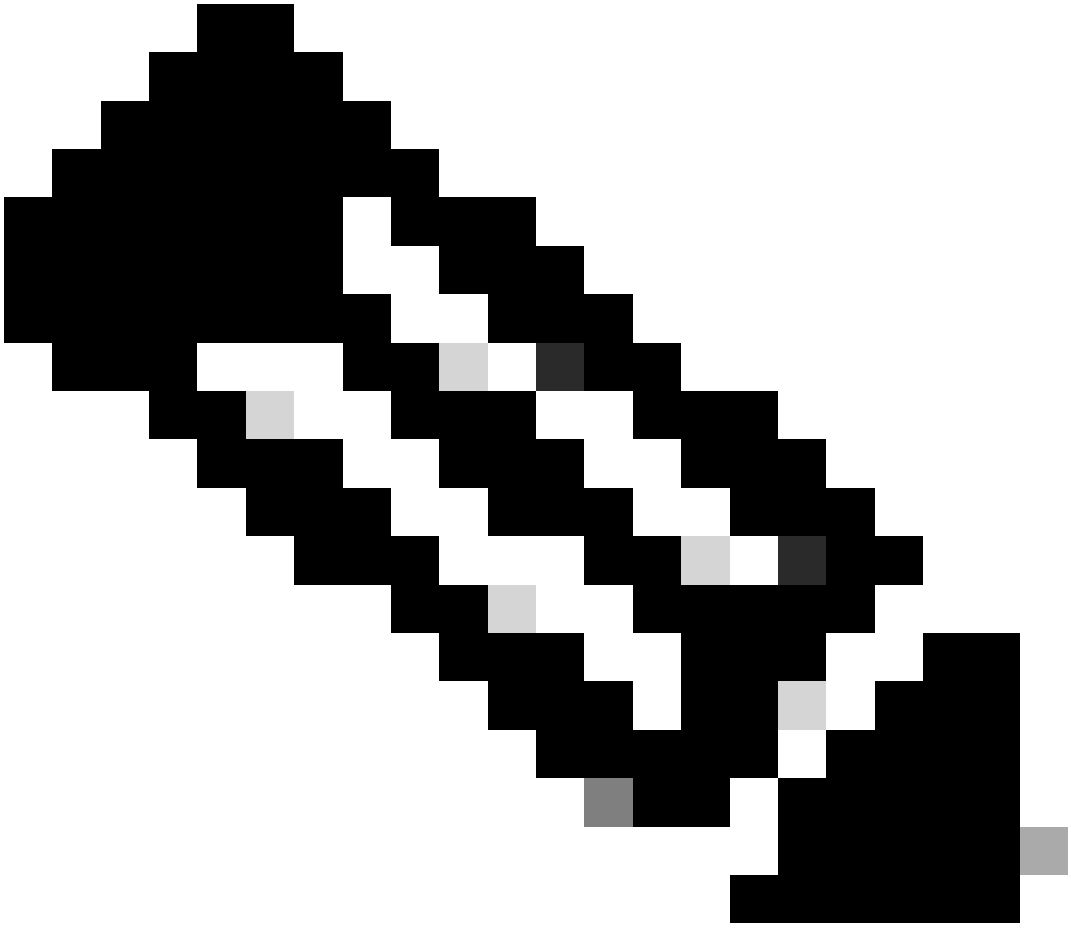
```
PubkeyAcceptedKeyTypes ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-ed25519,ssh-rs
```

31단계. SSH 서비스를 다시 시작합니다. PowerShell에서 관리자 권한(관리자로 실행)으로 이 명령을 사용할 수 있습니다

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

32단계. SCP 푸시가 올바르게 구성되었는지 테스트하려면 구성된 로그를 롤오버합니다. GUI 또는 CLI(rollovernow 명령)에서 롤오버할 수 있습니다.

```
WSA_CLI> rollovernow scpal
```



참고: 이 예에서 로그 이름은 "scpal"입니다.

로그가 정의된 폴더(이 예에서는 c:/Users/wsascp/wsa01)에 복사되었는지 확인할 수 있습니다

다른 드라이브에 SCP 로그 푸시

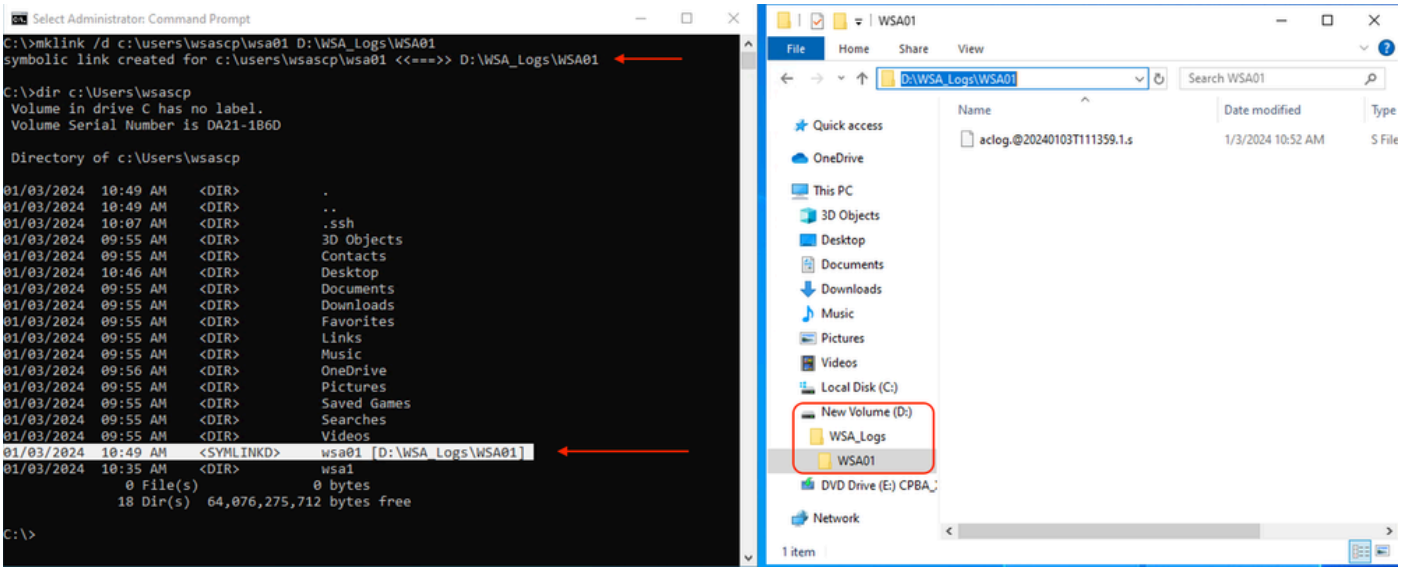
C:가 아닌 다른 드라이브로 로그를 푸시해야 하는 경우 사용자 프로필 폴더에서 원하는 드라이브로 링크를 생성합니다. 이 예에서는 로그가 D:\WSA_Logs\WSA01에 푸시됩니다.

1단계. 이 예에서는 원하는 드라이브에 폴더를 만듭니다

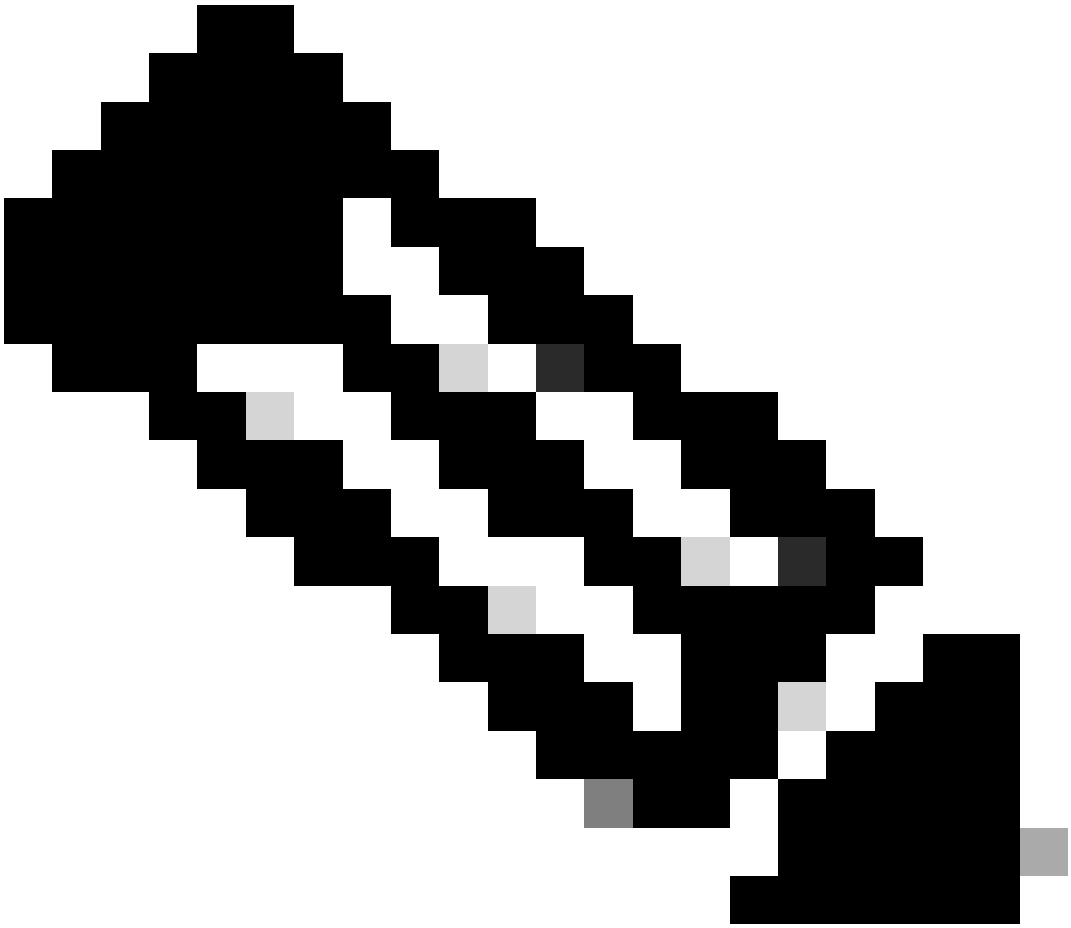
2단계. 관리자 권한으로 명령 프롬프트 열기(Run as Administrator)

3단계. 이 명령을 실행하여 링크를 생성합니다.

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



이미지 - SYM 링크 생성



참고: 이 예에서 SWA는 로그를 C:\Users\wsascp의 WSA01 폴더로 푸시하도록 구성되며,

SCP 서버는 WSA01 폴더를 D:\WSA_Logs\WSA01에 대한 심볼 링크로 가집니다

Microsoft Symbol Link에 대한 자세한 내용은 mklink를 참조하십시오. | Microsoft Learn

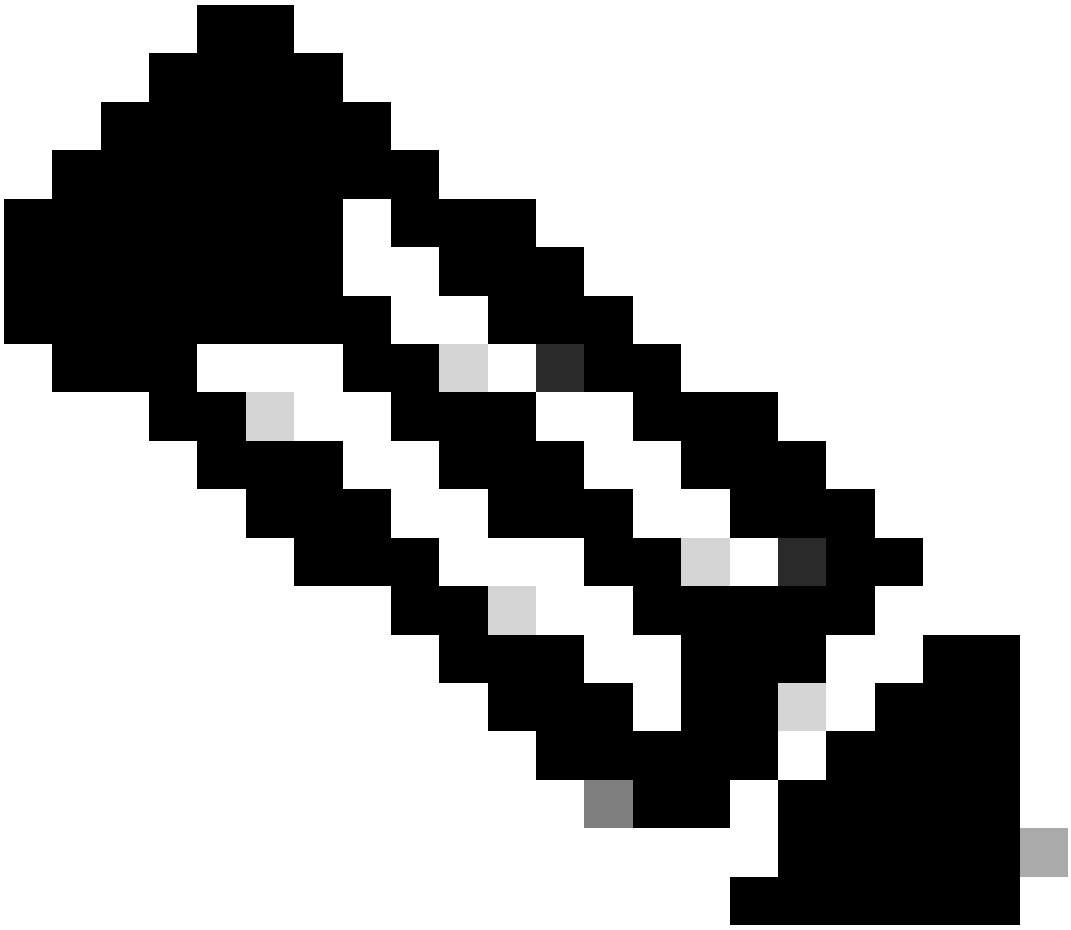
SCP 로그 푸시 문제 해결

SWA의 로그 보기

SCP 로그 푸시를 트러블슈팅하려면 다음 위치에서 오류를 확인하십시오.

1. CLI > displayalerts

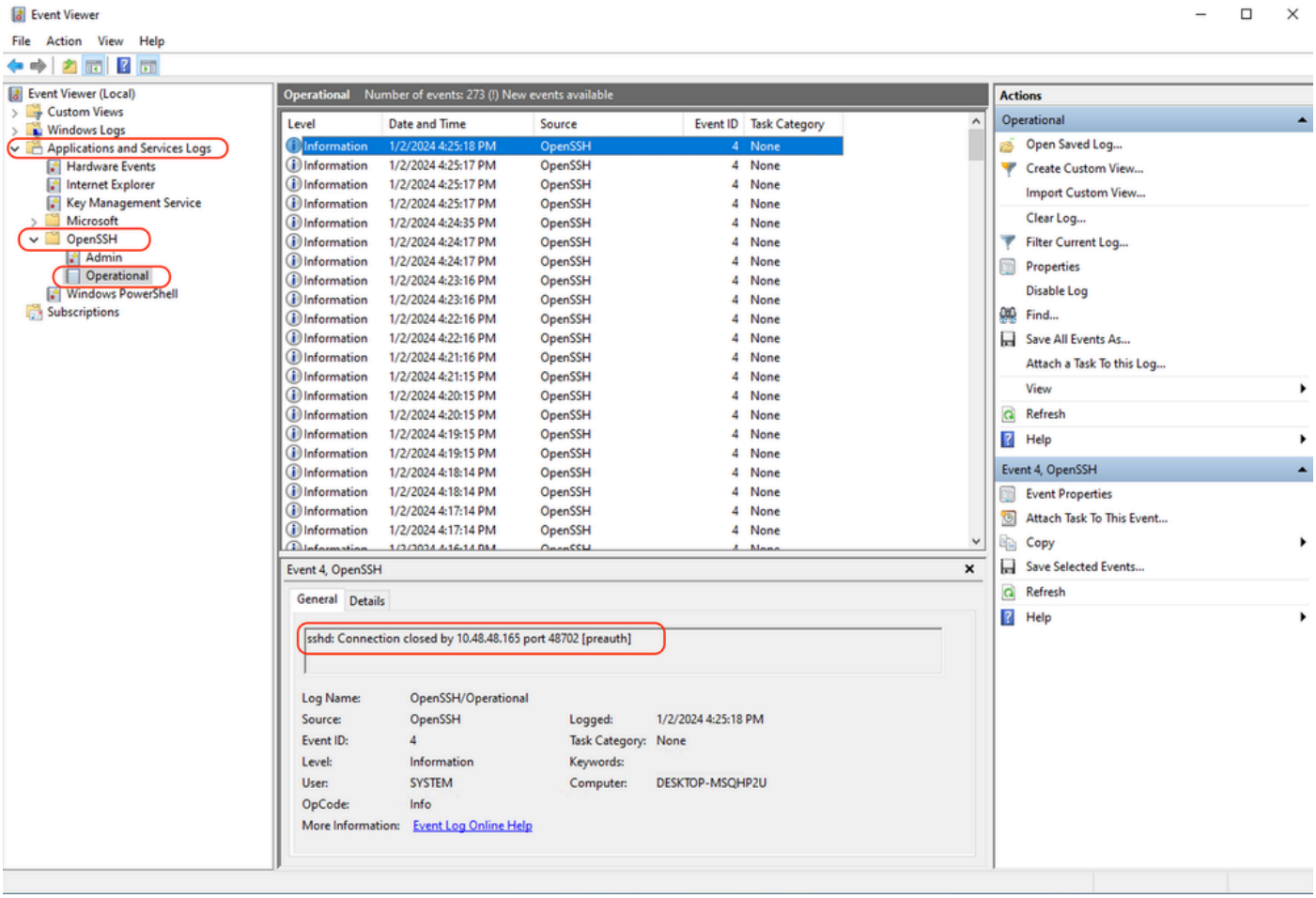
2. System_logs



참고: system_logs를 읽으려면 CLI에서 grep 명령을 사용하고 system_logs와 연결된 번호를 선택하고 마법사에서 질문에 답할 수 있습니다.

SCP 서버의 로그 보기

Microsoft Event Viewer의 Applications and Services Logs(애플리케이션 및 서비스 로그) > OpenSSH > Operational(운영)에서 SCP 서버 로그를 읽을 수 있습니다.



이미지 - 사전 인증 실패

호스트 키 확인 실패

이 오류는 SWA에 저장된 SCP 서버 공개 키가 잘못되었음을 나타냅니다.

다음은 CLI의 displayalerts 출력에서 발생하는 오류의 예입니다.

```
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.
```

다음은 system_logs의 오류 샘플입니다.

```
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
```

이 문제를 해결하려면 SCP 서버에서 호스트를 복사하고 SCP 로그 서브스크립션 페이지에 붙여넣을 수 있습니다.

GUI에서 SCP 원격 서버로 로그를 보내려면 SWA 구성의 7단계를 참조하거나 Cisco TAC에 문의하여 백엔드에서 호스트 키를 제거할 수 있습니다.

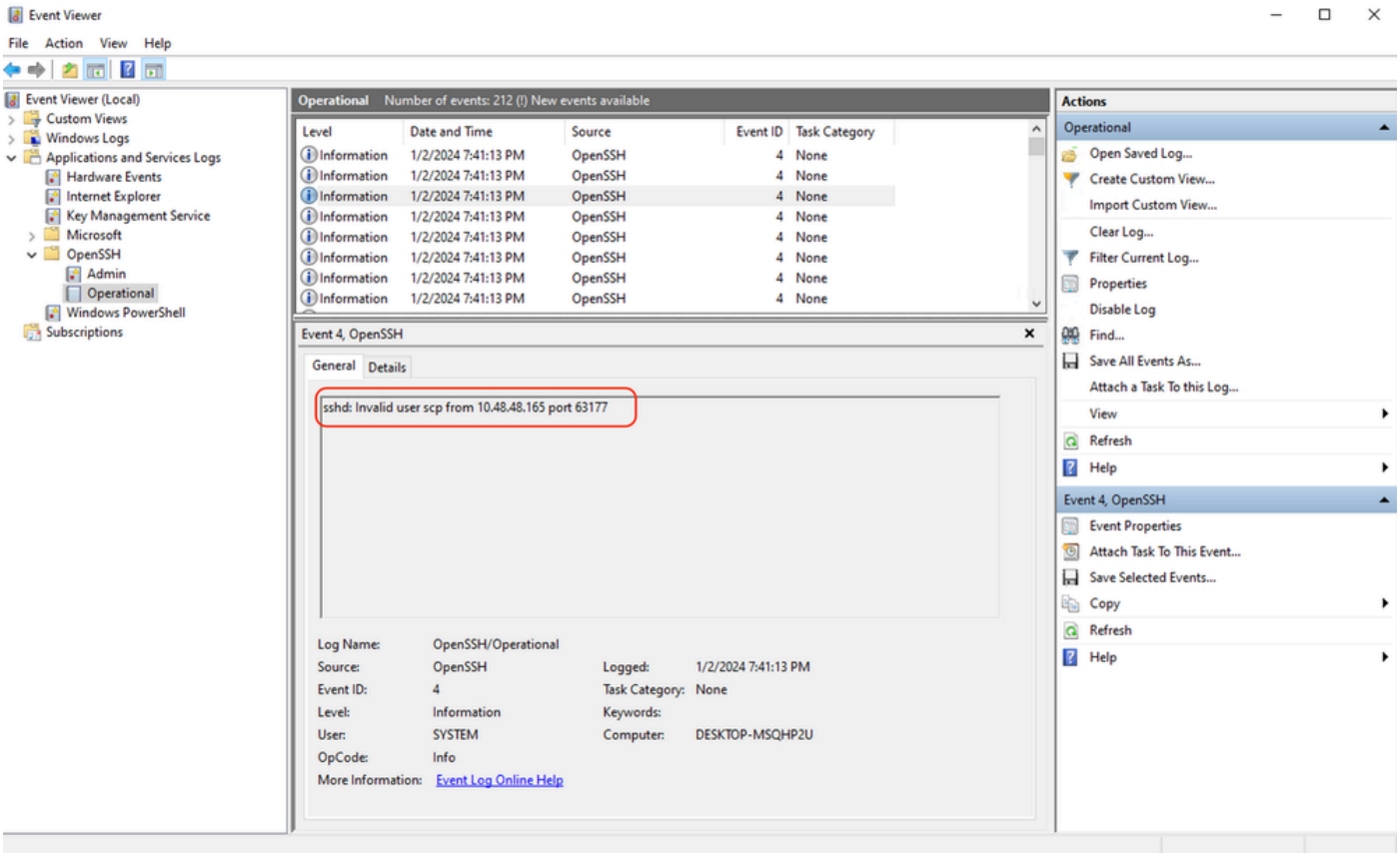
사용 권한 거부됨(publickey,password,keyboard-interactive)

이 오류는 일반적으로 SWA에 제공된 사용자 이름이 유효하지 않음을 나타냅니다.

다음은 system_logs의 오류 로그 샘플입니다.

```
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
```

다음은 SCP 서버의 오류 샘플입니다. <SWA_IP address> 포트 <TCP 포트 SWA가 SCP 서버에 연결하는 잘못된 사용자 SCP



이미지 - 잘못된 사용자

이 오류를 해결하려면 맞춤법을 검사하고 사용자(로그를 푸시하도록 SWA에서 구성됨)가 SCP 서버에서 활성화되었는지 확인하십시오.

해당 파일 또는 디렉토리가 없습니다.

이 오류는 SWA 로그 서브스크립션 섹션에 제공된 경로가 유효하지 않음을 나타냅니다.

다음은 system_logs의 오류 샘플입니다.

```
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
```

이 문제를 해결하려면 맞춤법을 확인하고 SCP 서버에서 경로가 올바르고 올바른지 확인하십시오.

SCP 전송 실패

이 오류는 통신 오류의 표시일 수 있습니다. 다음은 오류 샘플입니다.

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

연결 문제를 해결하려면 SWA CLI에서 telnet 명령을 사용합니다.

```
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...
```

이 예에서는 연결이 설정되지 않습니다. 성공적인 연결 종료는 다음과 같습니다.

```
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
```

텔넷이 연결되지 않은 경우:

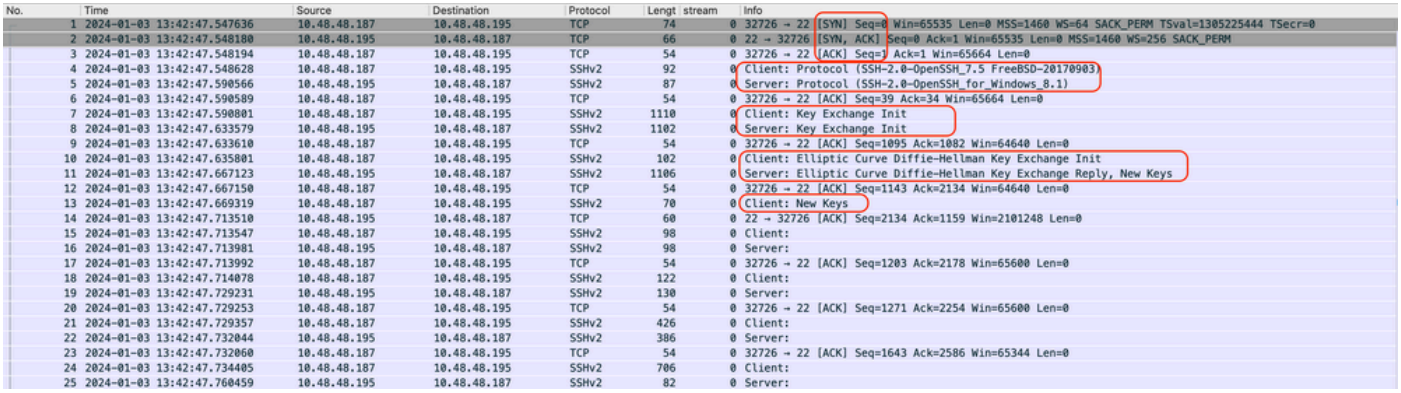
[1] SCP 서버 방화벽이 액세스를 차단하고 있는지 확인합니다.

[2] SWA에서 SCP 서버로의 경로에 방화벽이 있는지 확인하여 액세스를 차단합니다.

[3] SCP 서버에서 TCP 포트 22가 수신 대기 상태인지 확인합니다.

[4] 추가 분석을 위해 두 SWA ans SCP 서버에서 패킷 캡처를 실행합니다.

다음은 성공적인 연결의 패킷 캡처 샘플입니다.



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:

이미지 - 성공적인 연결 패킷 캡처

참조

Cisco Web Security Appliance 모범 사례 지침 - Cisco

BRKSEC-3303(ciscolive)

AsyncOS 14.5 for Cisco Secure Web Appliance - GD(General Deployment) - 연결, 설치 및 구성 [Cisco Secure Web Appliance] 사용 설명서 - Cisco

Windows용 OpenSSH 시작하기 | Microsoft Learn

Windows에서 SSH 공개 키 인증 구성 | Windows OS 허브(woshub.com)

Windows용 OpenSSH의 키 기반 인증 | Microsoft Learn

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.