

SNMP를 통해 TFTP 서버에 대한 컨피그레이션 파일 복사 트리거

목표

이 문서의 목적은 SNMP(Simple Network Management Protocol)를 통해 Cisco Business 스위치에서 컨피그레이션 파일 복사를 시작하는 단계를 설명하는 것입니다.

적용 가능한 디바이스

- Catalyst 1200 시리즈
- Catalyst 1300 시리즈
- CBS250 시리즈
- CBS350 시리즈

소개

일반적으로 구성 파일은 GUI(그래픽 사용자 인터페이스) 또는 CLI(명령줄 인터페이스)를 사용하여 스위치에서 복사됩니다. 더 특이한 방법은 SNMP를 통해 복사 작업을 트리거하는 것입니다.

민감한 데이터 처리

중요한 데이터가 포함된 구성 파일을 복사할 때 복사 작업은 중요한 데이터를 제외하거나, 암호화된 형식으로 포함하거나, 일반 텍스트로 포함하거나, 기본 메서드를 사용할 수 있습니다. 민감한 데이터 처리를 지정하는 것은 선택 사항이며 지정하지 않을 경우 기본값이 사용됩니다.

GUI

GUI를 사용하여 민감한 데이터 처리 메뉴에 액세스하려면 Administration(관리) > File Operations(파일 작업) > File Management(파일 관리) 메뉴로 이동합니다.

- 제외 - 민감한 데이터를 제외합니다.
- 암호화 - 민감한 데이터를 암호화합니다.
- 일반 텍스트 - 민감한 데이터를 일반 텍스트로 표시합니다.

File Operations

Operation Type:

☐ Update File

☒ Backup File 

☐ Duplicate

Source File Type:

☒ Running Configuration

☐ Startup Configuration

☐ Mirror Configuration

☐ Logging File

☐ Language File

Copy Method:

☐ HTTP/HTTPS

☐ USB

☐ Internal Flash

☒ TFTP 

☐ SCP (File transfer via SSH)

Server Definition:

☒ By IP address ☐ By name

IP Version:

☐ Version 6 ☒ Version 4

IPv6 Address Type:

☒ Link Local ☐ Global

Link Local Interface:

Gi3

⚠ Server IP Address/Name: 192.168.101.99

⚠ Destination: Test (4/62 characters used)

Sensitive Data Handling:

☒ Exclude

☐ Encrypt

☐ Plaintext



Note:

민감한 데이터 처리 옵션은 TFTP 또는 SCP의 백업 파일 모드에 표시됩니다.

CLI

명령줄에서 copy 명령을 사용할 수 있습니다.

```
copy {running-config | startup-config} dst-url [exclude | include-encrypted | include-plaintext]
```

예를 들면 다음과 같습니다.

```
copy running-config tftp://192.168.101.99/destination-file.txt exclude
```

기본값은 SSD(Secure Sensitive Data) 세션 읽기 모드가 설정된 것입니다. 현재 모드를 보려면 show ssd session을 입력하거나 show running-config를 입력하고 파일 SSD 표시기를 찾습니다. 공장 기본 설정에서는 예상 SSD 세션 읽기 모드가 암호화됩니다.

```
show ssd session
```

```
show running-config | include SSD
```

copy 명령이 아무 옵션도 지정하지 않고 입력된 경우 "include-encrypted"가 선택된 것처럼 복사됩니다.

```
copy running-config tftp://192.168.101.99/destination-file.txt
```

그러나 세션 읽기 값은 다음과 같이 변경할 수 있습니다.

```
ssd session read {exclude | encrypted | plaintext}
```

이 명령은 show running-config 및 show startup-config의 출력에 영향을 줄 뿐만 아니라 copy 명령의 민감한 데이터 처리에 대한 기본값 역할도 합니다.

예를 들면 다음과 같습니다.

```
ssd session read plaintext
```

```
exit
```

```
copy running-config tftp://192.168.101.99/destination-file.txt
```

결과 파일에는 "show running-config" 및 "show startup-config"의 출력과 마찬가지로 민감한 데이터가 일반 텍스트에 포함됩니다. 따라서 SSD 세션 읽기 모드에 주의해야 합니다. 기본값으로 두는 것이 가장 안전합니다.

Note:

show running-config 또는 show startup-config의 출력에 필요한 모든 내용이 표시되지 않는 경우(예: GUI에 표시되는 암호화된 자격 증명을 사용하는 SNMP v3 사용자) SSD 세션 읽기 값이 "exclude"로 설정되지 않았는지 확인합니다.

SNMP

Catalyst 1200/Catalyst 1300/CBSx50 시리즈 스위치는 rCopyOptionsRequestedSsdAccess라는 SNMP OID(object identifier)를 사용하여 민감한 데이터 옵션을 제어합니다. 객체는 정수이며, 기본적으로 이 객체가 받아들이는 값은 copy 명령의 값과 동일하게 표시됩니다.

- 1: 제외
- 2: 암호화 포함
- 3: include-decrypt(명령줄에서 "include-plaintext"와 동일)
- 4: 기본값

민감한 데이터를 일반 텍스트로 복사하는 옵션 3은 SNMP v2c와 함께 사용할 수 없으며, 인증 및 프라이버시(authPriv)를 모두 사용하지 않는 한 SNMP v3와 함께 사용할 수도 없습니다.

Note:

TFTP와 같은 안전하지 않은 프로토콜을 사용하여 파일을 복사하도록 일반 텍스트 옵션을 설정하는 것은 좋은 생각이 아닙니다.

authPriv가 있는 SNMP v3는 사본을 트리거하는 데만 사용되므로 전송 중에 컨피그레이션 파일 자체를 보호하는 데 프라이버시 설정이 도움이 되지 않습니다. 예를 들어 SCP(Secure Copy Protocol)를 사용하여 복사하는 것이 더 안전합니다.

옵션 4, "기본" 옵션은 예상대로 작동하지 않습니다. SNMP를 사용할 때 copy 명령처럼 동작하지 않으며 SSD 읽기 세션 값이 복사 결과에 전혀 영향을 주지 않습니다. 대신, 옵션 4는 옵션 1(제외)과 동일하며, 한 가지 예외가 있습니다. authPriv와 함께 SNMP v3를 사용하는 경우 옵션 4는 옵션 3(일반 텍스트)과 동일합니다.

동작은 아래 표에 요약되어 있습니다.

	1(제외)	2(암호화)	3(일반)	기본값

		됨)	텍스트)	
CLI 사본	제외됨	암호화	평문	SSD 값
SNMP v2c	제외됨	암호화	실패	제외됨
SNMP v3 authPriv	제외됨	암호화	평문	평문
SNMP v3 authNoPriv	제외됨	암호화	실패	제외됨
SNMP v3 noAuthNoPriv	제외됨	암호화	실패	제외됨

SNMP v3에 대한 스위치 컨피그레이션

authPriv가 있는 SNMP v3는 복사 작업을 트리거하는 데 특별히 필요하지 않지만, 더 큰 유연성과 보안을 제공하기 때문에 다른 SNMP 변형보다 권장되며 다음 예에 사용됩니다.

컨피그레이션 예:

```
snmp-server server
```

```
snmp-server engineID local 80000000903f01d2da99341
```

```
snmp-server group snmpAdmin v3 priv write Default
```

```
encrypted snmp-server user sbscadmin snmpAdmin v3 auth sha
[authentication_password] priv [privacy_password]
```

위의 컨피그레이션에서는 sbscadmin이라는 사용자가 스위치에 SNMP v3 명령을 보내 파일 복사를 트리거할 수 있습니다. 사용자 sbscadmin은 스위치에 대해 전체 SNMP v3 쓰기 권한이 부여된 snmpAdmin 그룹의 멤버입니다.

사용자에게 인증(auth) 비밀번호와 프라이버시(priv) 비밀번호(즉, authPriv)가 있으며, snmpAdmin 그룹에는 "priv" 집합(이를 사용하지 않으면 프라이버시를 사용할 수 없으므로 인증도 포함)이 있습니다.

복사 작업 트리거

다음은 복사 작업을 트리거하는 snmpset 명령의 예입니다. 몇 가지 개체 값을 설정해야 하는 경우 이 명령은 한 줄에 모두 입력되지만, 원하는 경우 백슬래시를 이스케이프 문자로 사용하여 각 항목을 해당 줄로 분리할 수 있습니다. 이 작업은 가독성을 높이기 위해 아래와 같이 수행되었습니다. 입력은 파란색으로 표시되고 출력은 흰색으로 표시됩니다.

```
blake@MintBD:~$ snmpset -v 3 -u snmpuser -l authPriv \
-a SHA -A [authentication_password] \
-x AES -X [privacy_password] -m +CISCO-SB-COPY-MIB 192.168.111.253 \
r1CopyOptionsRequestedSsdAccess.1 = include-encrypted \
r1CopyRowStatus.1 = createAndGo \
r1CopySourceLocation.1 = local \
r1CopySourceIpAddress.1 = 0.0.0.0 \
r1CopySourceUnitNumber.1 = 1 \
r1CopySourceFileType.1 = runningConfig \
r1CopyDestinationLocation.1 = tftp \
r1CopyDestinationIpAddress.1 = 192.168.111.18 \
r1CopyDestinationFileName.1 = v3-2.txt \
r1CopyDestinationFileType.1 = backupConfig
```

- 각 OID에는 ".1"이 추가되어 작업에 사용되는 테이블의 행을 나타냅니다.
- "rICopyRowStatus.1"은 항목을 rICopyTable에 삽입하는 데 사용됩니다. "createAndGo"로 설정됩니다. 즉, 행을 생성하고 스위치에서 사용할 수 있도록 활성화로 설정합니다.
- SSD 액세스 값은 "include-encrypted"로 설정됩니다(이 사본에만 해당).
- running-config 파일은 192.168.111.18의 TFTP 서버에 대상 파일 이름 "v3-2.txt"로 복사됩니다.

복사 작업이 실행되면 rICopyOptionsRequestedSsdAccess 값이 4(기본값)로 되돌아갑니다.

Note:

CISCOB-COPY-MIB는 스위치의 다운로드 페이지에 있는 MIB 파일과 함께 "CISCOB-copy.mib" 파일에 자세히 설명되어 있습니다.

다음 표에서는 각 객체의 기호 이름을 해당 OID와 일치시킵니다.

기호 이름	OID(개체 식별자)
rICopy옵션 테이블	1.3.6.1.4.1.9.6.1.101.87.12
rICopyOptionsRequestedSsdAcce	1.3.6.1.4.1.9.6.1.101.87.12.1.2

ss	
rlCopy테이블	1.3.6.1.4.1.9.6.1.101.87.2
rlCopy행 상태	1.3.6.1.4.1.9.6.1.101.87.2.1.17
rlCopySourceLocation	1.3.6.1.4.1.9.6.1.101.87.2.1.3
rlCopySourceIpAddress	1.3.6.1.4.1.9.6.1.101.87.2.1.4
rlCopySourceUnitNumber	1.3.6.1.4.1.9.6.1.101.87.2.1.5
rlCopySourceFileType	1.3.6.1.4.1.9.6.1.101.87.2.1.7
rlCopyDestinationLocation	1.3.6.1.4.1.9.6.1.101.87.2.1.8
rlCopy대상Ip주소	1.3.6.1.4.1.9.6.1.101.87.2.1.9
rlCopy대상 파일 이름	1.3.6.1.4.1.9.6.1.101.87.2.1.11
rlCopy대상 파일 유형	1.3.6.1.4.1.9.6.1.101.87.2.1.12

MIB 파일을 사용하지 않을 경우, 입력 및 출력이 덜 직관적일지라도 기호 이름 대신 OID를 사용하여 파일 복사를 트리거할 수 있습니다.

```
blake@MintBD:~$ snmpset -v 3 -u sbscadmin -l authPriv \
```

```
-a SHA -A [authentication_password] \  
  
-x AES -X [privacy_password] 192.168.111.253 \  
  
1.3.6.1.4.1.9.6.1.101.87.12.1.2.1 i 1 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.17.1 i 4 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.3.1 i 1 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.4.1 a 0.0.0.0 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.5.1 i 1 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.7.1 i 2 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.8.1 i 3 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.9.1 a 192.168.111.18 \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.11.1 s destination-file.txt \  
  
1.3.6.1.4.1.9.6.1.101.87.2.1.12.1 i 4
```

MIB가 없으면 명령에서 각 개체 유형("i"(정수의 경우), "a"(주소) 및 "s"(문자열의 경우)을 명시적으로 설정해야 하므로 간단한 "=" 기호를 사용하여 값을 설정하지 않았습니다. 값 ("local", "runningConfig" 등)의 이름도 MIB에 의해 정의되므로 해당 옵션을 나타내는 정수를 직접 설정해야 합니다.

Net-SNMP 및 스위치 MIB 파일

SNMP 관리 툴은 테스트 및 문제 해결 목적으로 유용하게 사용할 수 있습니다. 이 문서에서는 무료 및 오픈 소스 SNMP 툴 [제품군인 Net-SNMP](#)에 포함된 snmpset 명령을 사용합니다.

Net-SNMP와 함께 스위치 MIB 파일을 사용하려면 먼저 Net-SNMP의 고유한 MIB 파일이 Net-SNMP에서 검색할 위치(예: \$HOME/.snmp/mib)에 배치되어야 합니다. Net-SNMP의 자체 MIB 파일이 설치되지 않으면 스위치 MIB가 제대로 작동하지 않습니다.

스위치 MIB 파일의 압축을 풀고 Net-SNMP의 MIB 파일과 같은 위치에 배치할 수 있지만 호환성 문제를 방지하려면 두 세트 간에 겹치는 Net-SNMP 버전을 덮어쓰지 마십시오.

모든 MIB 파일이 적절한 위치에 있으면 원하는 명령과 함께 "-m" 인수를 사용하여 관련 MIB를 호출할 수 있습니다.

예를 들면 다음과 같습니다.

```
snmpget -v 3 -u snmpuser -l authPriv \  
-a SHA -A [authentication_password] \  
-x AES -X [privacy_password] \  
192.168.111.253 r1CopyOptionsRequestedSsdAccess.1
```

Note:

"CISCOB-COPY-MIB"는 MIB 자체의 이름이며 이를 설명하는 파일이 아닙니다. CISCOB-copy.mib입니다.

Net-SNMP 툴 사용 방법에 대한 자세한 내용은 [Net-SNMP 웹 사이트](#)에서 사용 가능한 설명서 및 [자습서를 참조하십시오](#).

결론

이제 SNMP를 통해 Cisco Business 스위치에서 TFTP 서버로 컨피그레이션 파일의 복사를 시작하는 단계에 대해 모두 알 수 있습니다.

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.