通過SNMP觸發配置檔案複製到TFTP伺服器

目標

本文的目的是概述通過簡單網路管理協定(SNMP)觸發從思科業務交換機複製配置檔案的步驟。

適用裝置

- Catalyst 1200 系列
- Catalyst 1300 系列
- CBS250系列
- CBS350系列

簡介

配置檔案通常使用圖形使用者介面(graphical user interface， GUI)或命令列介面(command line interface， CLI)從交換機複製。比較不尋常的方法是通過SNMP觸發複製任務。

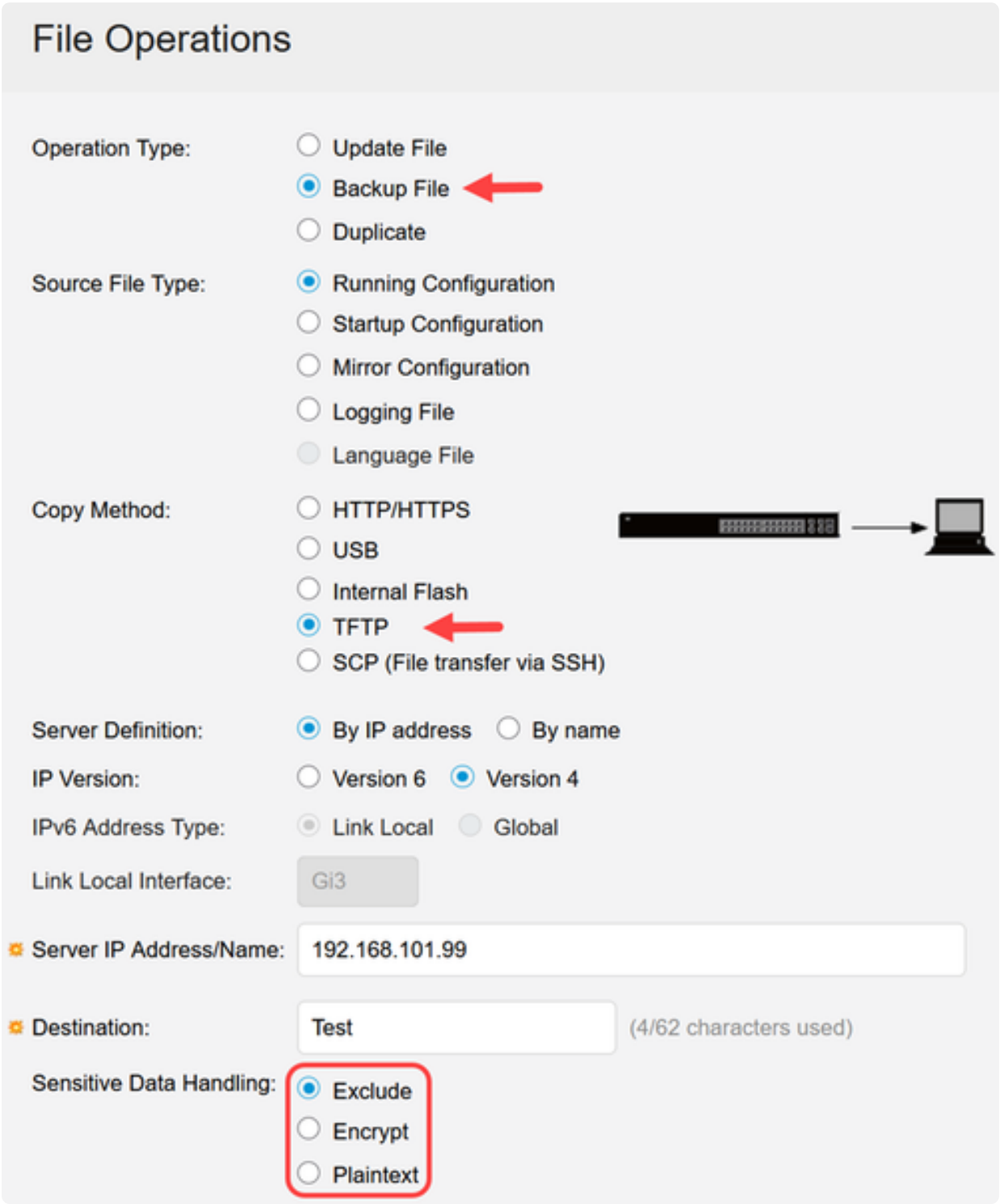
敏感資料處理

複製包含敏感資料的配置檔案時，複製任務可以排除敏感資料、以加密形式包含它、以明文形式包含它，或使用預設方法。指定敏感資料處理是可選的，如果未指定，將使用預設值。

GUI

要使用GUI訪問敏感資料處理選單，請導航到管理>檔案操作>檔案管理選單。

- 排除 — 排除敏感資料
- Encrypt — 加密敏感資料
- 明文 — 以明文形式顯示敏感資料。



Note:
「敏感資料處理」選項僅在TFTP或SCP的備份檔案模式下顯示。

CLI

在命令列中，可以使用copy命令：

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

舉例來說：

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

預設設定是安全敏感資料(SSD)會話讀取模式設定為的任何值。要檢視當前模式，請輸入show ssd session，或輸入show running-config，然後查詢文件SSD指示燈。使用出廠預設設定時，預期的SSD會話讀取模式將被加密。

```
show ssd session
```

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

如果在輸入沒有指定選項的情況下輸入copy命令，則其複製方式與選擇「include-encrypted」一樣。

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

但是，可以更改會話讀取值：

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

此命令會影響show running-config和show startup-config的輸出，以及充當copy命令處理敏感資料的預設值。

舉例來說：

```
ssd session read plaintext

exit

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

產生的檔案將包含明文形式的敏感資料，show running-config和「show startup-config」的輸出亦然，因此應注意SSD會話讀取模式。讓其處於預設狀態是最安全的。

> Note:
> 如果show running-config或show startup-config的輸出未顯示預期的所有內容，例如在GUI中顯示具有加密憑據的SNMP v3使用者，請確保SSD會話讀取值未設定為「排除」。

SNMP

Catalyst 1200/Catalyst 1300/CBSx50系列交換器使用名為rlCopyOptionsRequestedSsdAccess的SNMP物件識別碼(OID)控制敏感資料選項。對象為整數，乍看之下，它接受的值與copy命令的值相同：

- 1:排除
- 2:include-encrypt
- 3:include-decrypted（與命令列中的「include-plaintext」相同）
- 4:預設

選項3（複製明文形式的敏感資料）根本不能與SNMP v2c一起使用，除非同時使用身份驗證和隱私(authPriv)，否則它也不能與SNMP v3一起使用。

> Note:
> 設定純文字檔案選項以使用不安全協定（如TFTP）複製檔案不是好主意。

具有authPriv的SNMP v3僅用於觸發複製，因此其隱私設定對於傳輸期間保護配置檔案本身沒有幫助。例如，使用安全複製協定(SCP)進行複製會更安全。

選項4（「default」選項）的表現與預期不符。它不像copy命令那樣工作，在使用SNMP時，SSD讀取會話值對複製結果沒有任何影響。相反，選項4與選項1（排除）相同，只有一個例外：如果將SNMP v3與authPriv一起使用，選項4與選項3（純文字檔案）相同。

該行為總結在下表中：

	1（排除）	2（已加密）	3（純文字檔案）	預設
CLI副本	已排除	已加密	明文	SSD價值

SNMP v2c	已排除	已加密	失敗	已排除
SNMP v3 authPriv	已排除	已加密	明文	明文
SNMP v3 authNoPriv	已排除	已加密	失敗	已排除
SNMP v3 noAuthNoPriv	已排除	已加密	失敗	已排除

SNMP v3的交換機配置

觸發複製任務時並非特別要求使用authPriv的SNMP v3，但由於它提供了更大的靈活性和安全性，因此建議使用其他SNMP變體，並且將用於以下示例。

配置示例：

```
snmp-server server

snmp-server engineID local 8000000903f01d2da99341

snmp-server group snmpAdmin v3 priv write Default

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

上述配置允許名為sbscadmin的使用者向交換機傳送SNMP v3命令以觸發檔案複製。使用者sbscadmin是snmpAdmin組的成員，該組在交換機上被授予完全的SNMP v3 write許可權。

請注意，使用者具有驗證(auth)密碼和私密性(priv)密碼（即authPriv），而snmpAdmin群組已設定「priv」（這也包括驗證，因為如果沒有該密碼，私密性就無法使用）。

觸發複製任務

以下是snmpset命令觸發複製任務的示例。它必須設定多個對象值。該命令全部在一行中輸入，但反斜線可以用作跳脫字元，根據需要將每個專案分隔到自己的行中。這是為了提高可讀性。輸入顯示為藍色，輸出顯示為白色。

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

-a SHA -A [authentication_password] \

-x AES -X [privacy_password] -m +CISCOSB-COPY-MIB 192.168.111.253 \

rlCopyOptionsRequestedSsdAccess.1 = include-encrypted \

rlCopyRowStatus.1 = createAndGo \

rlCopySourceLocation.1 = local \

rlCopySourceIpAddress.1 = 0.0.0.0 \

rlCopySourceUnitNumber.1 = 1 \

rlCopySourceFileType.1 = runningConfig \

rlCopyDestinationLocation.1 = tftp \

rlCopyDestinationIpAddress.1 = 192.168.111.18 \

rlCopyDestinationFileName.1 = v3-2.txt \

rlCopyDestinationFileType.1 = backupConfig
```

- 每個OID都附加了「.1」，表示表中用於任務的行。
- 「rlCopyRowStatus.1」用於將條目插入rlCopyTable。它設定為「createAndGo」，即建立行並將其設定為活動，以便交換機可以使用它。
- SSD訪問值設定為「include-encrypted」（僅用於此副本）。
- 將運行配置檔案複製到目標檔名為「v3-2.txt」的TFTP伺服器192.168.111.18。

執行複製任務後，rlCopyOptionsRequestedSsdAccess的值將恢復為4（預設值）。

> **Note:**
> CISCOSB-COPY-MIB允許對對象及其值使用符號名稱，在交換機下載頁面上的MIB檔案隨附的「CISCOSB-copy.mib」檔案中對此進行了詳細描述。

下表將每個對象的符號名稱與其OID相匹配。

符號名稱	對象識別符號(OID)
rlCopyOptionsTable	1.3.6.1.4.1.9.6.1.101.87.12
rlCopyOptionsRequestedSsdAccess	1.3.6.1.4.1.9.6.1.101.87.12.1.2
rlCopyTable	1.3.6.1.4.1.9.6.1.101.87.2
rlCopyRowStatus	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
rlCopyDestinationIpAddress	1.3.6.1.4.1.9.6.1.101.87.2.1.9
rlCopyDestinationFileName	1.3.6.1.4.1.9.6.1.101.87.2.1.11
rlCopyDestinationFileType	1.3.6.1.4.1.9.6.1.101.87.2.1.12

如果不使用MIB檔案，可以使用OID而不是符號名稱來觸發檔案副本，但輸入和輸出並不直觀。

```
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
```

沒有使用簡單的「=」符號來設定值，因為如果不使用MIB，命令必須顯式設定每個對象型別(整數為「i」，地址為「a」，字串為「s」)。 這些值的名稱(「local」、「runningConfig」等)也無法使用，因為它們是由MIB定義的，因此必須直接設定表示這些選項的整數。

Net-SNMP和交換機MIB檔案

SNMP管理工具對於測試和故障排除很有幫助。本文使用隨Net-SNMP（一組自由且開源的SNMP工具）提供的snmpset命令。

為了將交換器MIB檔案與Net-SNMP搭配使用，首先請確保Net-SNMP自己的MIB檔案放在Net-SNMP會尋找的位置，例如$HOME/.snmp/mib。如果不安裝Net-SNMP自己的MIB檔案，交換機MIB將無法正常工作。

交換機MIB檔案可以解壓縮並放置在Net-SNMP的MIB檔案所在的同一位置，但是為了

避免相容性問題，請不要覆蓋兩個集之間重疊的任何Net-SNMP版本。

一旦所有MIB檔案都位於適當的位置，就可以使用「 — m」引數結合所需的命令來呼叫相關MIB。

舉例來說：

```
snmpget -v 3 -u snmpuser -l authPriv \

-a SHA -A [authentication_password] \

-x AES -X [privacy_password] \

                192.168.111.253 rlCopyOptionsRequestedSsdAccess.1
```

> Note:
> 「CISCOSB-COPY-MIB」是MIB本身的名稱，而不是描述它的檔案，即CISCOSB-copy.mib。

有關如何使用Net-SNMP工具的更多資訊，請參閱Net-SNMP網站上的文檔和教程。

結論

現在您已瞭解通過SNMP觸發將配置檔案從Cisco Business交換機複製到TFTP伺服器的所有步驟。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。