Attivazione delle copie dei file di configurazione su un server TFTP tramite SNMP

Obiettivo

L'obiettivo di questo articolo è delineare i passaggi per attivare la copia dei file di configurazione da uno switch Cisco Business tramite il protocollo SNMP (Simple Network Management Protocol).

Dispositivi interessati

- Catalyst serie 1200
- Catalyst serie 1300
- Serie CBS250
- Serie CBS350

Introduzione

I file di configurazione vengono in genere copiati da uno switch utilizzando l'interfaccia utente grafica (GUI) o l'interfaccia della riga di comando (CLI). Un metodo più insolito consiste nell'attivare l'operazione di copia tramite SNMP.

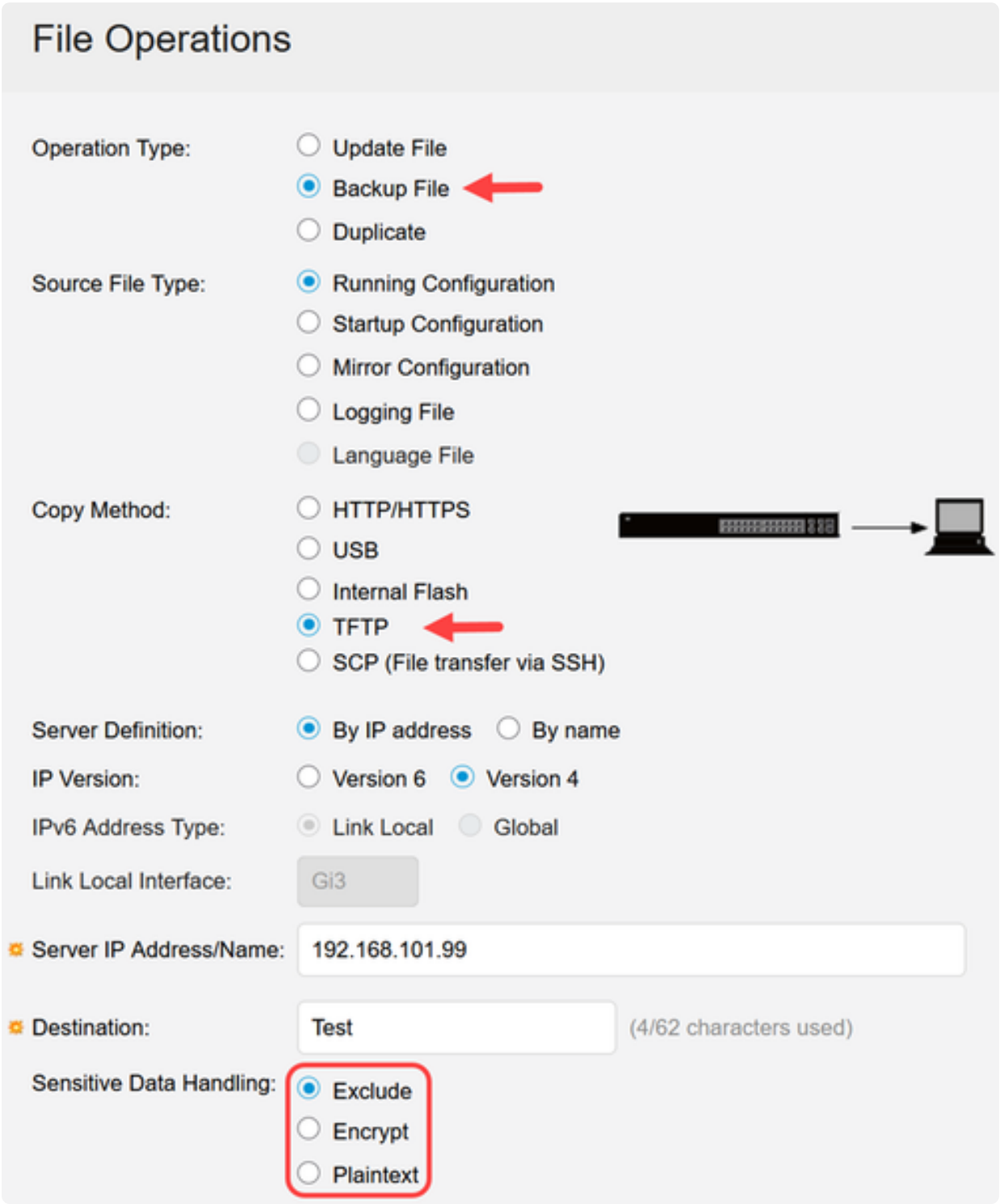
Gestione dei dati sensibili

Quando si copia un file di configurazione contenente dati riservati, l'operazione di copia può escludere i dati riservati, includerli in forma crittografata, includerli come testo normale o utilizzare un metodo predefinito. L'impostazione della gestione dei dati sensibili è facoltativa e, se non è specificata, verrà utilizzata l'impostazione predefinita.

GUI

Per accedere al menu di gestione dei dati sensibili dalla GUI, selezionare Amministrazione > Operazioni file > Menu Gestione file.

- Escludi - per escludere i dati sensibili
- Crittografa - per crittografare i dati sensibili
- Testo normale: per visualizzare i dati riservati in testo normale.



Note:

L'opzione Gestione dati sensibili viene visualizzata solo in modalità file di backup per TFTP o SCP.

CLI

Dalla riga di comando, è possibile utilizzare il comando copy:

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

Ad esempio:

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

Il valore predefinito è quello impostato per la modalità di lettura della sessione SSD. Per visualizzare la modalità corrente, immettere show ssd session o show running-config e cercare l'indicatore SSD del file. Con le impostazioni predefinite di fabbrica, la modalità di lettura prevista per la sessione SSD è crittografata.

```
show ssd session
```

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

Se il comando copy è stato immesso senza specificare alcuna opzione, verrà copiato come se fosse stato scelto "include-encrypted".

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

Tuttavia, il valore di lettura della sessione può essere modificato:

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

Questo comando influisce sull'output di show running-config e show startup-config, nonché sul valore predefinito per il trattamento dei dati riservati da parte del comando copy.

Ad esempio:

```
ssd session read plaintext

exit

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

Il file risultante includerà dati sensibili in testo normale, come l'output di "show running-config" e "show startup-config", quindi è necessario prestare attenzione alla modalità di lettura della sessione SSD. Lasciarlo al valore predefinito è il modo più sicuro.

> **Note:**
> Se l'output di show running-config o show startup-config non visualizza tutto il previsto, ad esempio gli utenti SNMP v3 con credenziali crittografate visibili nella GUI, verificare che il valore di lettura della sessione SSD non sia impostato su "exclude".

SNMP

Gli switch Catalyst serie 1200/Catalyst 1300/CBSx50 usano l'identificatore di oggetto SNMP (OID) chiamato rlCopyOptionsRequestedSsdAccess per controllare l'opzione dei dati sensibili. L'oggetto è un numero intero e a prima vista i valori accettati sono equivalenti a quelli del comando copy:

- 1: escludere
- 2: include-encrypted
- 3: include-decrypted (uguale a "include-plaintext" sulla riga di comando)
- 4: predefinito

L'opzione 3, che copia i dati sensibili in testo non crittografato, non può essere utilizzata con SNMP v2c, né con SNMP v3 a meno che non si utilizzino sia l'autenticazione che la privacy (authPriv).

> **Note:**
> Non è consigliabile impostare l'opzione Testo normale per copiare il file utilizzando un protocollo non protetto come TFTP.

SNMP v3 con authPriv viene utilizzato solo per attivare la copia, quindi le relative impostazioni di privacy non sono utili per la protezione del file di configurazione stesso durante il trasferimento. Ad esempio, la copia con il protocollo SCP (Secure Copy Protocol) sarebbe più sicura.

L'opzione 4 (predefinita) non funziona come previsto. Non funziona come il comando copy e il valore della sessione di lettura SSD non ha alcun effetto sul risultato della copia quando si utilizza SNMP. L'opzione 4 equivale all'opzione 1 (esclusa), con una sola eccezione: Se si utilizza SNMP v3 con authPriv, l'opzione 4 è uguale all'opzione 3 (testo normale).

Il comportamento è riassunto nella tabella seguente:

	1 (escludi)	2 (crittografato)	3 (testo normale)	predefinito
Copia CLI	escluso	crittografia	testo normale	Valore SSD
SNMP v2c	escluso	crittografia	non riuscito	escluso
AuthPriv SNMP v3	escluso	crittografia	testo normale	testo normale
AuthNoPriv SNMP v3	escluso	crittografia	non riuscito	escluso
SNMP v3 noAuthNoPriv	escluso	crittografia	non riuscito	escluso

Configurazione switch per SNMP v3

SNMP v3 con authPriv non è richiesto specificamente per attivare l'attività di copia, ma poiché fornisce maggiore flessibilità e sicurezza, è consigliato rispetto alle altre varianti SNMP e sarà quello utilizzato per gli esempi seguenti.

Esempio di configurazione:

```
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]
```

La configurazione precedente consente all'utente sbscadmin di inviare comandi SNMP v3 allo switch per attivare la copia dei file. L'utente sbscadmin è un membro del gruppo snmpAdmin, a cui sono stati concessi privilegi di scrittura SNMP v3 completi sullo switch.

Si noti che l'utente dispone sia di una password di autenticazione (auth) sia di una password per la privacy (priv), ad esempio authPriv, e che per il gruppo snmpAdmin è impostata l'opzione "priv" (che include anche l'autenticazione, in quanto la privacy non può essere utilizzata senza di essa).

Attivazione dell'attività di copia

Di seguito è riportato un esempio di comando snmpset che attiva l'attività di copia. È sufficiente impostare diversi valori dell'oggetto. Il comando viene immesso in un'unica riga, ma è possibile utilizzare una barra rovesciata come carattere di escape per separare ogni elemento sulla propria riga, se lo si desidera. Questa operazione è stata eseguita di seguito per migliorare la leggibilità. L'ingresso viene visualizzato in blu e l'output in bianco.

```
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
```

- A ogni OID viene aggiunto ".1", che rappresenta la riga della tabella utilizzata per l'attività.
- "rlCopyRowStatus.1" viene utilizzato per inserire la voce in rlCopyTable. È impostata su "createAndGo", ovvero crea la riga e la imposta su attiva in modo che possa essere utilizzata dallo switch.
- Il valore di accesso SSD è impostato su "include-encrypted" (solo per questa copia).
- Il file running-config viene copiato sul server TFTP in 192.168.111.18 con il nome file di destinazione "v3-2.txt".

Una volta eseguita l'attività di copia, il valore di rlCopyOptionsRequestedSsdAccess torna a 4 (impostazione predefinita).

> **Note:**
> L'uso di nomi simbolici per gli oggetti e i loro valori è reso possibile da CISCOSB-COPY-MIB, che è descritto in dettaglio nel file "CISCOSB-copy.mib", incluso con i file MIB nella pagina di download dello switch.

Nella tabella seguente il nome simbolico di ogni oggetto viene associato al relativo OID.

Nome simbolico	OID (Object Identifier)
TabellaOpzioniCopiaRI	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
rlCopiaTabella	1.3.6.1.4.1.9.6.1.101.87.2
rlCopiaStatoRiga	1.3.6.1.4.1.9.6.1.101.87.2.1.17
rlCopiaPosizioneOrigine	1.3.6.1.4.1.9.6.1.101.87.2.1.3
IndirizzoIpOrigineRI	1.3.6.1.4.1.9.6.1.101.87.2.1.4
NumeroUnitàOrigineRI	1.3.6.1.4.1.9.6.1.101.87.2.1.5
rlCopiaTipoFileOrigine	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
rlCopyDestinationIndirizzoIp	1.3.6.1.4.1.9.6.1.101.87.2.1.9
rlCopyNomeFileDestinazione	1.3.6.1.4.1.9.6.1.101.87.2.1.11

TipoFileDestinazioneRI	1.3.6.1.4.1.9.6.1.101.87.2.1.12

Se non si utilizzano i file MIB, la copia dei file può essere attivata utilizzando gli OID anziché i nomi simbolici, anche se l'input e l'output sono meno intuitivi.

```
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
```

Per impostare i valori non è stato utilizzato un semplice simbolo "=" perché, senza MIB, il comando deve impostare esplicitamente ciascun tipo di oggetto ("i" per numero intero, "a" per indirizzo e "s" per stringa). I nomi per i valori ("local", "runningConfig", ecc.) non possono essere utilizzati poiché sono definiti dal MIB, quindi i numeri interi che rappresentano tali opzioni devono essere impostati direttamente.

File MIB di Net-SNMP e switch

Gli strumenti di gestione SNMP possono essere utili a scopo di test e risoluzione dei problemi. In questo articolo viene utilizzato il comando snmpset incluso in Net-SNMP, una suite di strumenti SNMP gratuiti e open-source.

Per utilizzare i file MIB dello switch con Net-SNMP, accertarsi innanzitutto che i file MIB di Net-SNMP siano posizionati in un punto in cui Net-SNMP li cercherà, ad esempio $HOME/.snmp/mibs. Senza i file MIB di Net-SNMP installati, i MIB dello switch non funzioneranno correttamente.

I file MIB dello switch possono essere decompressi e collocati nella stessa posizione dei file MIB di Net-SNMP; tuttavia, per evitare problemi di compatibilità, non sovrascrivere le versioni Net-SNMP di eventuali file che si sovrappongono tra i due set.

Una volta che tutti i file MIB si trovano nella posizione appropriata, i MIB rilevanti possono essere chiamati utilizzando l'argomento "-m" con il comando desiderato.

Ad esempio:

```
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" è il nome del MIB stesso e non il file che lo descrive, ovvero CISCOSB-copy.mib.

Per ulteriori informazioni su come utilizzare gli strumenti Net-SNMP, vedere la

documentazione e le esercitazioni disponibili sul sito Web Net-SNMP.

Conclusioni

A questo punto, è possibile conoscere tutte le procedure per attivare la copia dei file di configurazione da uno switch Cisco Business a un server TFTP tramite SNMP.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).