Déclenchement de copies de fichiers de configuration sur un serveur TFTP via SNMP

Objectif

L'objectif de cet article est de décrire les étapes permettant de déclencher la copie des fichiers de configuration à partir d'un commutateur Cisco Business via le protocole SNMP (Simple Network Management Protocol).

Périphériques pertinents

- Gamme Catalyst 1200
- Gamme Catalyst 1300
- Gamme CBS250
- Gamme CBS350

Introduction

Les fichiers de configuration sont généralement copiés à partir d'un commutateur à l'aide de l'interface graphique utilisateur (GUI) ou de l'interface de ligne de commande (CLI). Une méthode plus inhabituelle consiste à déclencher la tâche de copie via SNMP.

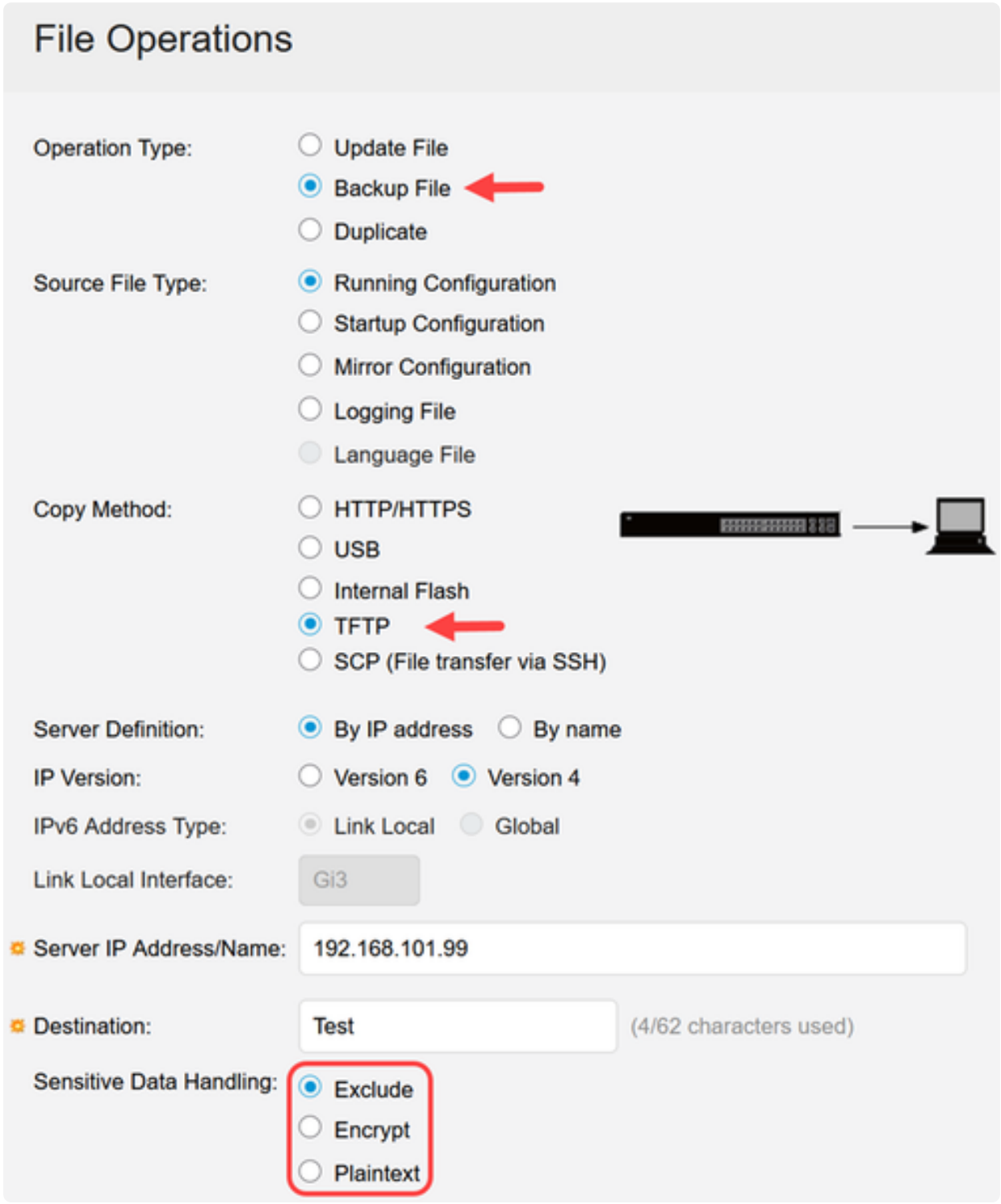
Traitement des données sensibles

Lors de la copie d'un fichier de configuration contenant des données sensibles, la tâche de copie peut exclure les données sensibles, les inclure sous forme chiffrée, les inclure en texte clair ou utiliser une méthode par défaut. La spécification du traitement des données sensibles est facultative et la valeur par défaut sera utilisée si elle n'est pas spécifiée.

IUG

Pour accéder au menu de gestion des données sensibles à l'aide de l'interface graphique utilisateur, accédez au menu Administration > File Operations > File Management.

- Exclure - pour exclure les données sensibles
- Chiffrer : pour chiffrer les données sensibles.
- Texte clair : pour afficher les données sensibles en texte clair.



Note:

L'option Sensitive Data Handling apparaît uniquement en mode de fichier de sauvegarde pour TFTP ou SCP.

CLI

À partir de la ligne de commande, la commande copy peut être utilisée :

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

Exemple :

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

La valeur par défaut est le mode de lecture de session SSD (Secure Sensitive Data) défini sur. Pour afficher le mode actuel, entrez show ssd session, ou entrez show running-config et recherchez l'indicateur de fichier SSD. Avec les paramètres d'usine par défaut, le mode de lecture de session SSD attendu est chiffré.

```
show ssd session
```

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

Si la commande copy a été entrée sans aucune option spécifiée, la copie est effectuée comme si l'option « include-encryption » avait été sélectionnée.

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

Cependant, la valeur de lecture de session peut être modifiée :

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

Cette commande a un impact sur le résultat de show running-config et show startup-config, ainsi qu'en agissant comme valeur par défaut pour le traitement des données sensibles par la commande copy.

Exemple :

```
ssd session read plaintext

exit

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

Le fichier résultant inclura des données sensibles en texte clair, tout comme le résultat de "show running-config" et "show startup-config", donc il faut faire attention avec le mode de lecture de session SSD. Laisser la valeur par défaut est plus sûr.

> **Note:**
> Si la sortie de show running-config ou de show startup-config n'affiche pas tout ce qui est attendu, par exemple, les utilisateurs SNMP v3 avec des informations d'identification chiffrées qui sont visibles dans l'interface graphique utilisateur, assurez-vous que la valeur de lecture de la session SSD n'est pas définie sur « exclude ».

SNMP

Les commutateurs de la gamme Catalyst 1200/Catalyst 1300/CBSx50 utilisent l'identificateur d'objet (OID) SNMP appelé rlCopyOptionsRequestedSsdAccess pour contrôler l'option de données sensibles. L'objet est un entier et à première vue, les valeurs qu'il accepte semblent équivalentes à celles de la commande copy :

- 1: laisser à l'écart
- 2: include-encrypted
- 3: include-decrypted (comme "include-plaintext" sur la ligne de commande)
- 4: manquer à ses obligations

L'option 3, qui copie les données sensibles en texte clair, ne peut pas être utilisée avec SNMP v2c, ni avec SNMP v3, à moins que l'authentification et la confidentialité (authPriv) ne soient utilisées.

> **Note:**
> Définir l'option de texte clair pour copier le fichier en utilisant un protocole non sécurisé comme TFTP n'est pas une bonne idée.

SNMP v3 avec authPriv est uniquement utilisé pour déclencher la copie, de sorte que ses paramètres de confidentialité ne sont pas utiles pour la protection du fichier de configuration lui-même pendant le transfert. La copie à l'aide du protocole Secure Copy Protocol (SCP), par exemple, serait plus sécurisée.

L'option 4, l'option par défaut, ne se comporte pas comme on pourrait s'y attendre. Il n'agit pas comme la commande copy, et la valeur de session de lecture SSD n'a aucune influence sur le résultat de copie lors de l'utilisation de SNMP. L'option 4 est identique à l'option 1 (exclure), à une exception près : Si vous utilisez SNMP v3 avec authPriv, l'option 4 est identique à l'option 3 (texte clair).

Le comportement est résumé dans le tableau ci-dessous :

	1 (exclure)	2 (crypté)	3 (texte clair)	manquer à ses obligations
copie CLI	exclus	chiffré	texte brut	Valeur SSD
SNMP v2c	exclus	chiffré	échoue	exclus
SNMP v3 authPriv	exclus	chiffré	texte brut	texte brut
SNMP v3 authNoPriv	exclus	chiffré	échoue	exclus
SNMP v3 noAuthNoPriv	exclus	chiffré	échoue	exclus

Configuration du commutateur pour SNMP v3

SNMP v3 avec authPriv n'est pas spécifiquement requis pour déclencher la tâche de copie, mais comme il offre une plus grande flexibilité et sécurité, il est recommandé par rapport aux autres variantes SNMP et sera celui utilisé pour les exemples suivants.

Exemple de configuration :

```
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 configuration ci-dessus permet à l'utilisateur nommé sbscadmin d'envoyer des commandes SNMP v3 au commutateur pour déclencher la copie du fichier. L'utilisateur sbscadmin est membre du groupe snmpAdmin, qui a reçu des privilèges d'écriture SNMP v3 complets sur le commutateur.

Notez que l'utilisateur dispose à la fois d'un mot de passe d'authentification (auth) et d'un mot de passe de confidentialité (priv), c'est-à-dire authPriv, et que le groupe snmpAdmin a un jeu de mots de passe "priv" (qui inclut également l'authentification puisque la confidentialité ne peut pas être utilisée sans elle).

Déclenchement de la tâche de copie

L'exemple suivant est un exemple de commande snmpset qui déclenche la tâche de copie. Il est long tant qu'il doit définir plusieurs valeurs d'objet. La commande est entrée sur une seule ligne, mais une barre oblique inverse peut être utilisée comme caractère d'échappement pour séparer chaque élément sur sa propre ligne si nécessaire. Ceci a été fait ci-dessous pour améliorer la lisibilité. L'entrée est affichée en bleu et la sortie en blanc.

```
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
```

- À chaque OID est ajouté ".1", qui représente la ligne de la table utilisée pour la tâche.
- "rlCopyRowStatus.1" est utilisé pour insérer l'entrée dans rlCopyTable. Il est défini sur "createAndGo", c'est-à-dire, créer la ligne et la définir sur active afin qu'elle puisse être utilisée par le commutateur.
- La valeur d'accès SSD est définie sur "include-encryption" (pour cette copie uniquement).
- Le fichier running-config est copié sur le serveur TFTP à l'adresse 192.168.111.18 avec le nom de fichier de destination "v3-2.txt".

Une fois la tâche de copie exécutée, la valeur de rlCopyOptionsRequestedSsdAccess revient à 4 (valeur par défaut).

> **Note:**
> L'utilisation de noms symboliques pour les objets et leurs valeurs est rendue possible par CISCOSB-COPY-MIB, qui est décrit en détail dans le fichier "CISCOSB-copy.mib", inclus avec les fichiers MIB sur la page de téléchargement pour le commutateur.

Le tableau suivant fait correspondre le nom symbolique de chaque objet à son OID.

Nom symbolique	Identificateur d'objet (OID)
TableauOptionsCopieURL	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
TableCopieRL	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
AdresseIpSourceCopieRl	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
TypeFichierSourceCopieRL	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
AdresseIpDestinationCopieURL	1.3.6.1.4.1.9.6.1.101.87.2.1.9
NomFichierDestinationCopieURL	1.3.6.1.4.1.9.6.1.101.87.2.1.11

TypeFichierDestinationCopieURL	1.3.6.1.4.1.9.6.1.101.87.2.1.12

Si les fichiers MIB ne sont pas utilisés, la copie de fichier peut être déclenchée à l'aide des OID au lieu des noms symboliques, bien que l'entrée et la sortie soient moins intuitives.

```
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
```

Un simple "=" symbole n'a pas été utilisé pour définir les valeurs car, sans la MIB, la commande doit explicitement définir chaque type d'objet ("i" pour entier, "a" pour adresse et "s" pour chaîne). Les noms des valeurs ("local", "runningConfig", etc.) ne peuvent pas non plus être utilisés car ils sont définis par la MIB, de sorte que les entiers représentant ces options doivent être définis directement.

Fichiers MIB de Net-SNMP et de commutateur

Les outils de gestion SNMP peuvent être utiles à des fins de test et de dépannage. Cet article utilise la commande snmpset incluse avec Net-SNMP, une suite d'outils SNMP libres et open-source.

Afin d'utiliser les fichiers MIB du commutateur avec Net-SNMP, assurez-vous d'abord que les propres fichiers MIB de Net-SNMP sont placés dans un emplacement où Net-SNMP les recherchera, par exemple, $HOME/.snmp/mibs. Si les fichiers MIB de Net-SNMP ne sont pas installés, les MIB du commutateur ne fonctionneront pas correctement.

Les fichiers MIB du commutateur peuvent être décompressés et placés au même emplacement que les fichiers MIB de Net-SNMP, mais pour éviter les problèmes de compatibilité, n'écrasez pas les versions Net-SNMP des fichiers qui se chevauchent entre les deux ensembles.

Une fois que tous les fichiers MIB se trouvent dans un emplacement approprié, les MIB appropriées peuvent être appelées à l'aide de l'argument "-m" avec la commande souhaitée.

Exemple :

```
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" est le nom de la MIB elle-même et non le fichier qui la décrit, qui est CISCOSB-copy.mib.

Pour plus d'informations sur l'utilisation des outils Net-SNMP, consultez la documentation et les didacticiels disponibles sur le site Web Net-SNMP.

Conclusion

Vous connaissez maintenant toutes les étapes à suivre pour déclencher la copie des fichiers de configuration d'un commutateur Cisco Business vers un serveur TFTP via SNMP.

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.