Desencadenado de Copias del Archivo de Configuración a un Servidor TFTP a través de SNMP

Objetivo

El objetivo de este artículo es describir los pasos para activar la copia de archivos de configuración desde un switch Cisco Business a través del protocolo simple de administración de red (SNMP).

Dispositivos aplicables

- Catalyst 1200 Series
- Catalyst 1300 Series
- Serie CBS250
- Serie CBS350

Introducción

Los archivos de configuración suelen copiarse de un switch mediante la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI). Un método más inusual es activar la tarea de copia a través de SNMP.

Gestión de datos confidenciales

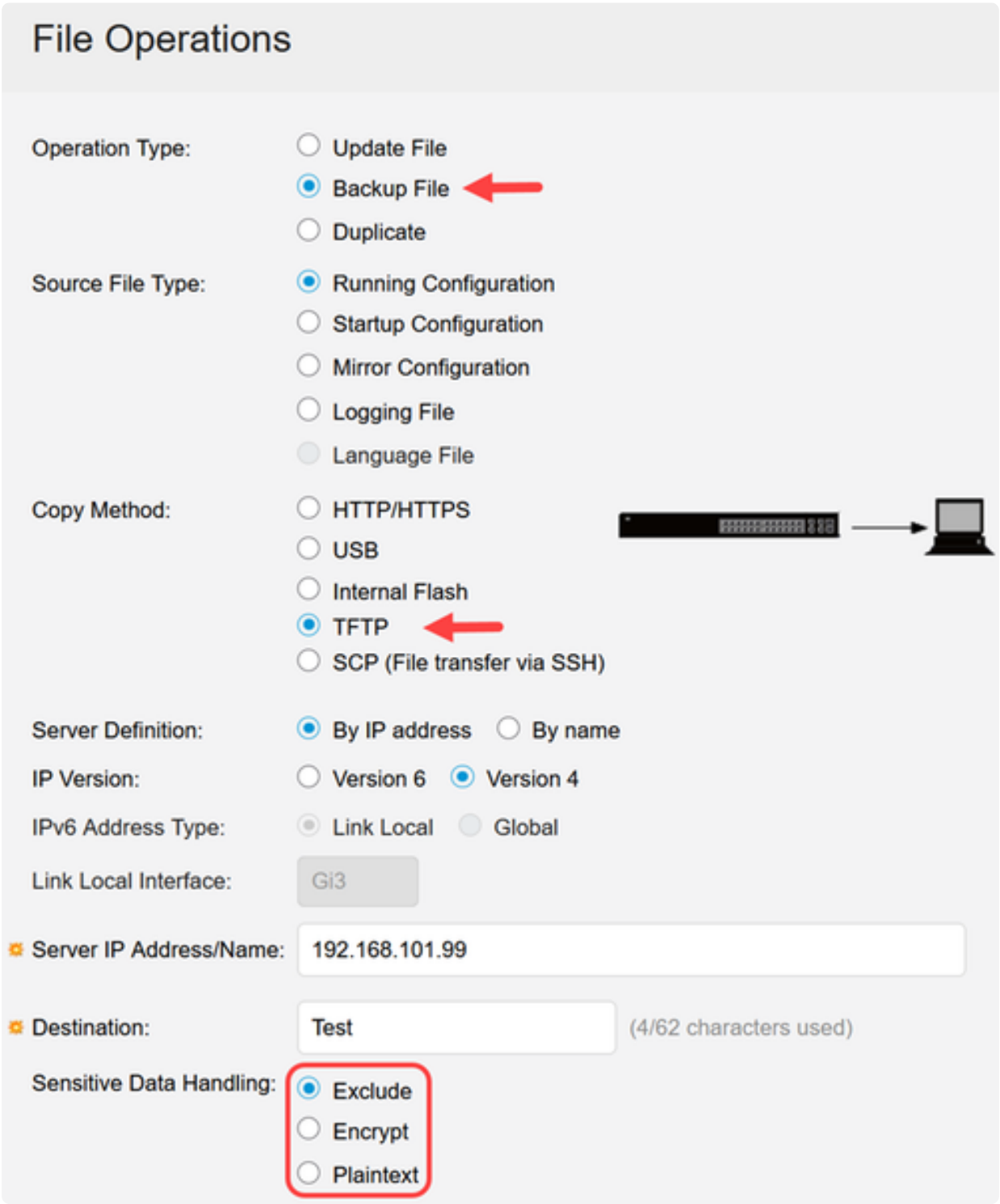
Al copiar un archivo de configuración que contiene datos confidenciales, la tarea de copia puede excluir datos confidenciales, incluirlos en formato cifrado, incluirlos como texto sin formato o utilizar un método predeterminado. La especificación de la gestión de datos confidenciales es opcional y, si no se especifica, se utilizará el valor predeterminado.

GUI

Para acceder al menú de gestión de datos confidenciales mediante la GUI, vaya al menú Administration > File Operations > File Management.

- Excluir: para excluir datos confidenciales.
- Cifrar: para cifrar datos confidenciales.

- Texto sin formato: para mostrar datos confidenciales en texto sin formato.



Note:

La opción Sensitive Data Handling solo aparece en el modo de archivo de respaldo para TFTP o SCP.

CLI

Desde la línea de comandos, se puede utilizar el comando copy:

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

Por ejemplo:

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

El valor predeterminado es el que se establezca en el modo de lectura de sesión de datos confidenciales seguros (SSD). Para ver el modo actual, ingrese show ssd session, o ingrese show running-config y busque el indicador SSD del archivo. Con la configuración predeterminada de fábrica, el modo de lectura de sesión SSD esperado se cifra.

```
show ssd session
```

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

Si se ingresó el comando copy sin especificar ninguna opción, se copiaría como si se hubiera elegido "include-encryption".

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

Sin embargo, el valor de lectura de la sesión se puede cambiar:

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

Este comando afecta el resultado de show running-config y show startup-config, además de actuar como el valor predeterminado para el tratamiento de datos confidenciales del comando copy.

Por ejemplo:

```
ssd session read plaintext

exit
```

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

El archivo resultante incluirá datos confidenciales en texto simple, al igual que la salida de "show running-config" y "show startup-config", por lo que se debe tener cuidado con el modo de lectura de la sesión SSD. Lo más seguro es dejarlo en el valor predeterminado.

> **Note:**
> Si el resultado de show running-config o show startup-config no muestra todo lo que se espera, por ejemplo, usuarios SNMP v3 con credenciales cifradas que son visibles en la GUI, asegúrese de que el valor de lectura de la sesión SSD no esté configurado en "exclude".

SNMP (Protocolo de administración de red simple)

Los switches de las series Catalyst 1200/Catalyst 1300/CBSx50 utilizan el identificador de objeto SNMP (OID) denominado rlCopyOptionsRequestedSsdAccess para controlar la opción de datos confidenciales. El objeto es un entero y, a primera vista, los valores que acepta son equivalentes a los del comando copy:

- 1: excluir
- 2: con cifrado incluido
- 3: include-decrypted (igual que "include-plaintext" en la línea de comandos)
- 4: predeterminado

La opción 3, que copia los datos confidenciales en texto sin formato, no se puede utilizar con SNMP v2c en absoluto, ni se puede utilizar con SNMP v3 a menos que se utilicen la autenticación y la privacidad (authPriv).

> **Note:**
> Establecer la opción de texto sin formato para copiar el archivo usando un protocolo inseguro como TFTP no es una buena idea.

SNMP v3 con authPriv sólo se utiliza para activar la copia, por lo que sus parámetros de privacidad no son útiles para proteger el archivo de configuración durante la transferencia. La copia con el protocolo de copia segura (SCP), por ejemplo, sería más segura.

La opción 4, la opción "predeterminada", no se comporta como cabría esperar. No actúa como el comando copy, y el valor de la sesión de lectura de SSD no influye en

absoluto en el resultado de la copia cuando se utiliza SNMP. En su lugar, la opción 4 es la misma que la opción 1 (excluir), con una excepción: Si utiliza SNMP v3 con authPriv, la opción 4 es la misma que la opción 3 (texto sin formato).

El comportamiento se resume en la siguiente tabla:

	1 (excluido)	2 (cifrado)	3 (texto sin formato)	predeterminado
copia de CLI	excluido	cifrados	texto simple	Valor de SSD
SNMP v2c	excluido	cifrados	falla	excluido
SNMP v3 authPriv	excluido	cifrados	texto simple	texto simple
SNMP v3 authNoPriv	excluido	cifrados	falla	excluido
SNMP v3 noAuthNoPriv	excluido	cifrados	falla	excluido

Configuración del switch para SNMP v3

SNMP v3 con authPriv no se requiere específicamente para accionar la tarea de copia, pero dado que proporciona mayor flexibilidad y seguridad, se recomienda sobre las

otras variantes SNMP y será el que se utilice para los siguientes ejemplos.

Ejemplo de configuración:

```
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 configuración anterior permite que el usuario llamado sbscadmin envíe comandos SNMP v3 al switch para activar la copia del archivo. El usuario sbscadmin es miembro del grupo snmpAdmin, al que se le han otorgado privilegios de escritura SNMP v3 completos en el switch.

Tenga en cuenta que el usuario tiene una contraseña de autenticación (auth) y una contraseña de privacidad (priv), es decir, authPriv, y el grupo snmpAdmin tiene el conjunto "priv" (que también incluye autenticación ya que la privacidad no se puede utilizar sin ella).

Desencadenado de la tarea de copia

A continuación se muestra un ejemplo del comando snmpset que desencadena la tarea de copia. Es tan largo como debe establecer varios valores de objeto. El comando se introduce todo en una línea, pero se puede utilizar una barra invertida como carácter de escape para separar cada elemento en su propia línea si así se desea. Esto se hizo a continuación para mejorar la legibilidad. La entrada se muestra en azul y la salida en blanco.

```
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
```

- Cada OID tiene ".1" anexado, que representa la fila de la tabla que se está utilizando para la tarea.
- "rlCopyRowStatus.1" se utiliza para insertar la entrada en rlCopyTable. Se establece en "createAndGo", es decir, crea la fila y la establece en activa para que pueda ser utilizada por el switch.
- El valor de acceso a SSD se establece en "include-encryption" (solo para esta copia).
- El archivo running-config se copia en el servidor TFTP en 192.168.111.18 con el nombre de archivo de destino "v3-2.txt".

Una vez ejecutada la tarea de copia, el valor de rlCopyOptionsRequestedSsdAccess vuelve a ser 4 (valor predeterminado).

> **Note:**
> El uso de nombres simbólicos para los objetos y sus valores es posible gracias a CISCOSB-COPY-MIB, que se describe en detalle en el archivo "CISCOSB-copy.mib", incluido con los archivos MIB en la página de descarga para el switch.

La siguiente tabla hace coincidir el nombre simbólico de cada objeto con su OID.

Nombre simbólico	Identificador de objeto (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

Si no se utilizan archivos MIB, la copia del archivo se puede activar utilizando los OID en lugar de los nombres simbólicos, aunque la entrada y la salida son menos intuitivas.

```
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
```

No se utilizó un simple símbolo "=" para establecer los valores porque, sin la MIB, el comando debe establecer explícitamente cada tipo de objeto ("i" para el entero, "a" para la dirección y "s" para la cadena). Los nombres de los valores ("local", "runningConfig", etc.) tampoco se pueden utilizar, ya que están definidos por la MIB, por lo que los enteros que representan esas opciones deben establecerse directamente.

Archivos Net-SNMP y Switch MIB

Las herramientas de administración SNMP pueden ser útiles para pruebas y resolución de problemas. Este artículo utiliza el comando snmpset incluido con Net-SNMP, un conjunto de herramientas SNMP libres y de código abierto.

Para utilizar los archivos MIB del switch con Net-SNMP, primero asegúrese de que los propios archivos MIB de Net-SNMP se coloquen en una ubicación donde Net-SNMP los busque, por ejemplo, $HOME/.snmp/mibs. Sin los propios archivos MIB de Net-SNMP instalados, los MIB del switch no funcionarán correctamente.

Los archivos MIB del switch se pueden descomprimir y ubicar en la misma ubicación que los archivos MIB de Net-SNMP, pero para evitar problemas de compatibilidad, no sobrescriba las versiones Net-SNMP de cualquier archivo que se superponga entre los dos conjuntos.

Una vez que todos los archivos MIB están en una ubicación apropiada, se puede llamar a las MIB relevantes usando el argumento "-m" con el comando deseado.

Por ejemplo:

```
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" es el nombre de la MIB en sí y no el archivo que la describe, que es CISCOSB-copy.mib.

Para obtener más información sobre cómo utilizar las herramientas Net-SNMP, vea la documentación y los tutoriales disponibles en el sitio Web de Net-SNMP.

Conclusión

Ahora ya sabe todos los pasos para activar la copia de archivos de configuración de un switch Cisco Business a un servidor TFTP a través de SNMP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).