Disparando cópias do arquivo de configuração para um servidor TFTP via SNMP

Objetivo

O objetivo deste artigo é descrever as etapas para ativar a cópia de arquivos de configuração de um switch Cisco Business através do SNMP (Simple Network Management Protocol).

Dispositivos aplicáveis

- Catalyst 1200 Series
- Catalyst 1300 Series
- Série CBS250
- Série CBS350

Introdução

Os arquivos de configuração são normalmente copiados de um switch usando a interface gráfica do usuário (GUI) ou a interface de linha de comando (CLI). Um método mais incomum é disparar a tarefa de cópia via SNMP.

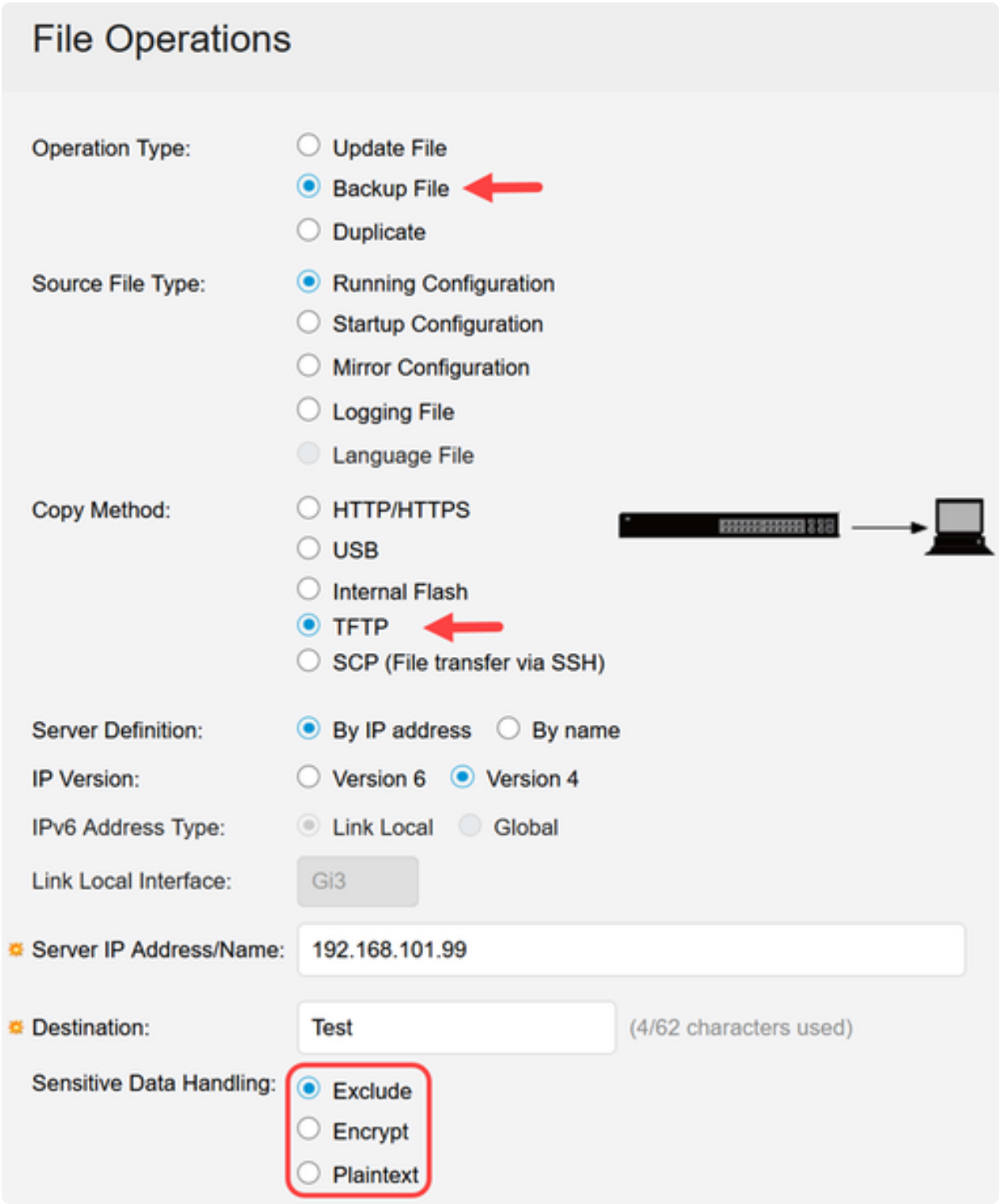
Tratamento de dados confidenciais

Ao copiar um arquivo de configuração que contém dados confidenciais, a tarefa de cópia pode excluir dados confidenciais, incluí-los no formato criptografado, incluí-los como texto sem formatação ou usar um método padrão. A especificação do tratamento de dados confidenciais é opcional e o padrão será usado se não for especificado.

GUI

Para acessar o menu de tratamento de dados confidenciais usando a GUI, navegue para o menu Administração > Operações de arquivo > Gerenciamento de arquivos.

- Excluir - para excluir dados confidenciais
- Criptografar - para criptografar dados confidenciais
- Texto simples - para exibir dados confidenciais em texto sem formatação.



Note:

A opção Tratamento de dados confidenciais aparece apenas no modo de arquivo Backup para TFTP ou SCP.

CLI

Na linha de comando, o comando copy pode ser usado:

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

Por exemplo:

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

O padrão é qualquer que seja o modo de leitura da sessão de Secure Sensitive Data (SSD) definido. Para ver o modo atual, digite show ssd session ou digite show running-config e procure o indicador de arquivo SSD. Com as configurações padrão de fábrica, o modo de leitura de sessão SSD esperado é criptografado.

```
show ssd session
```

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

Se o comando copy fosse inserido sem nenhuma opção especificada, ele copiaria como se "include-encrypted" tivesse sido escolhido.

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

No entanto, o valor de leitura da sessão pode ser alterado:

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

Esse comando afeta a saída de show running-config e show startup-config, bem como age como o valor padrão para o tratamento de dados confidenciais do comando copy.

Por exemplo:

```
ssd session read plaintext

exit

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

O arquivo resultante incluirá dados confidenciais em texto simples, assim como a

saída de "show running-config" e "show startup-config", portanto, deve-se tomar cuidado com o modo de leitura da sessão SSD. Deixá-lo como padrão é o mais seguro.

> **Note:**
> Se a saída de show running-config ou show startup-config não mostrar tudo o que é esperado, por exemplo, usuários SNMP v3 com credenciais criptografadas que são visíveis na GUI, certifique-se de que o valor de leitura da sessão SSD não esteja definido como "exclude".

SNMP

Os Catalyst 1200/Catalyst 1300/CBSx50 Series Switches usam o identificador de objeto (OID) SNMP chamado rlCopyOptionsRequestedSsdAccess para controlar a opção de dados confidenciais. O objeto é um número inteiro e, à primeira vista, os valores que ele aceita parecem equivalentes aos do comando copy:

- 1: excluir
- 2: include-encrypted
- 3: include-decrypted (o mesmo que "include-plaintext" na linha de comando)
- 4: padrão

A opção 3, que copia os dados confidenciais em texto simples, não pode ser usada com o SNMP v2c, nem com o SNMP v3, a menos que a autenticação e a privacidade (authPriv) sejam usadas.

> **Note:**
> Não é uma boa ideia configurar a opção de texto simples para copiar o arquivo usando um protocolo inseguro como o TFTP.

O SNMP v3 com authPriv é usado apenas para disparar a cópia, portanto, suas configurações de privacidade não são úteis para a proteção do próprio arquivo de configuração durante a transferência. Copiar com Secure Copy Protocol (SCP), por exemplo, seria mais seguro.

A opção 4, a opção "padrão", não se comporta como seria de esperar. Ele não age como o comando copy, e o valor da sessão de leitura SSD não tem nenhuma influência no resultado da cópia ao usar SNMP. Em vez disso, a opção 4 é a mesma que a opção 1 (excluir), com uma exceção: Se estiver usando SNMP v3 com authPriv, a opção 4 é igual à opção 3 (texto simples).

O comportamento está resumido na tabela abaixo:

	1 (excluir)	2 (criptografado)	3 (texto sem formatação)	padrão
cópia CLI	excluído	criptografado	texto simples	Valor SSD
SNMP v2c	excluído	criptografado	falha	excluído
SNMP v3 authPriv	excluído	criptografado	texto simples	texto simples
SNMP v3 authNoPriv	excluído	criptografado	falha	excluído
SNMP v3 noAuthNoPriv	excluído	criptografado	falha	excluído

Configuração do switch para SNMP v3

O SNMP v3 com authPriv não é especificamente necessário para disparar a tarefa de cópia, mas como ele fornece maior flexibilidade e segurança, é recomendado sobre as outras variantes de SNMP e será o usado para os exemplos a seguir.

Exemplo de configuração:

```
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]
```

A configuração acima permite que o usuário chamado sbscadmin envie comandos SNMP v3 ao switch para disparar a cópia do arquivo. O usuário sbscadmin é membro do grupo snmpAdmin, que recebeu privilégios totais de SNMP v3 write no switch.

Observe que o usuário tem uma senha de autenticação (auth) e uma senha de privacidade (priv), ou seja, authPriv, e o grupo snmpAdmin tem "priv" definido (o que também inclui a autenticação, já que a privacidade não pode ser usada sem ela).

Disparando a Tarefa de Cópia

Veja a seguir um exemplo do comando snmpset que dispara a tarefa de cópia. Ele tem de definir vários valores de objeto. O comando é inserido completamente em uma linha, mas uma barra invertida pode ser usada como um caractere de escape para separar cada item em sua própria linha, se desejado. Isso foi feito abaixo para melhorar a legibilidade. A entrada é mostrada em azul e a saída é em branco.

```
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 tem ".1" anexado, representando a linha na tabela que está sendo usada para a tarefa.
- "rlCopyRowStatus.1" é usado para inserir a entrada em rlCopyTable. Ele é definido como "createAndGo", ou seja, cria a linha e a define como ativa para que possa ser usada pelo switch.
- O valor de acesso à SSD é definido como "include-encrypted" (somente para esta cópia).
- O arquivo running-config é copiado para o servidor TFTP em 192.168.111.18 com um nome de arquivo de destino "v3-2.txt".

Quando a tarefa de cópia é executada, o valor de rlCopyOptionsRequestedSsdAccess é revertido para 4 (padrão).

> **Note:**
> O uso de nomes simbólicos para os objetos e seus valores é possibilitado pelo CISCOSB-COPY-MIB, que é descrito em detalhes no arquivo "CISCOSB-copy.mib", incluído com os arquivos MIB na página de download do switch.

A tabela a seguir corresponde o nome simbólico de cada objeto ao seu OID.

Nome 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

Se os arquivos MIB não forem usados, a cópia do arquivo poderá ser acionada usando os OIDs em vez dos nomes simbólicos, embora a entrada e a saída sejam 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
```

Um símbolo simples "=" não foi usado para definir os valores porque, sem o MIB, o comando deve definir explicitamente cada tipo de objeto ("i" para inteiro, "a" para endereço e "s" para cadeia de caracteres). Os nomes dos valores ("local", "runningConfig", etc.) também não podem ser usados, pois são definidos pela MIB, portanto, os inteiros que representam essas opções devem ser definidos diretamente.

Arquivos MIB Net-SNMP e Switch

As ferramentas de gerenciamento SNMP podem ser úteis para fins de teste e solução de problemas. Este artigo usa o comando snmpset incluído com Net-SNMP, um conjunto de ferramentas SNMP gratuitas e de código aberto.

Para usar os arquivos MIB do switch com o Net-SNMP, primeiro certifique-se de que os próprios arquivos MIB do Net-SNMP sejam colocados em um local onde o Net-SNMP irá procurá-los, por exemplo, $HOME/.snmp/mibs. Sem os próprios arquivos MIB do Net-SNMP instalados, os MIBs do switch não funcionarão corretamente.

Os arquivos MIB do switch podem ser descompactados e colocados no mesmo local que os arquivos MIB do Net-SNMP, mas para evitar problemas de compatibilidade, não substitua as versões do Net-SNMP de nenhum que se sobreponha entre os dois conjuntos.

Quando todos os arquivos MIB estiverem em um local apropriado, a(s) MIB(s) relevante(s) poderá(ão) ser chamada(s) usando o argumento "-m" com o comando desejado.

Por exemplo:

```
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" é o nome do próprio MIB e não o arquivo que o descreve, que é CISCOSB-copy.mib.

Para obter mais informações sobre como usar as ferramentas Net-SNMP, consulte a documentação e os tutoriais disponíveis no site Net-SNMP.

Conclusão

Agora você sabe tudo sobre as etapas para disparar a cópia de arquivos de configuração de um switch Cisco Business para um servidor TFTP via SNMP.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.