通过SNMP触发配置文件复制到TFTP服务器

目标

本文的目的是概述通过简单网络管理协议(SNMP)触发从Cisco业务交换机复制配置文件的步骤。

适用设备

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

简介

配置文件通常使用图形用户界面(GUI)或命令行界面(CLI)从交换机进行复制。比较不寻常的方法是通过SNMP触发复制任务。

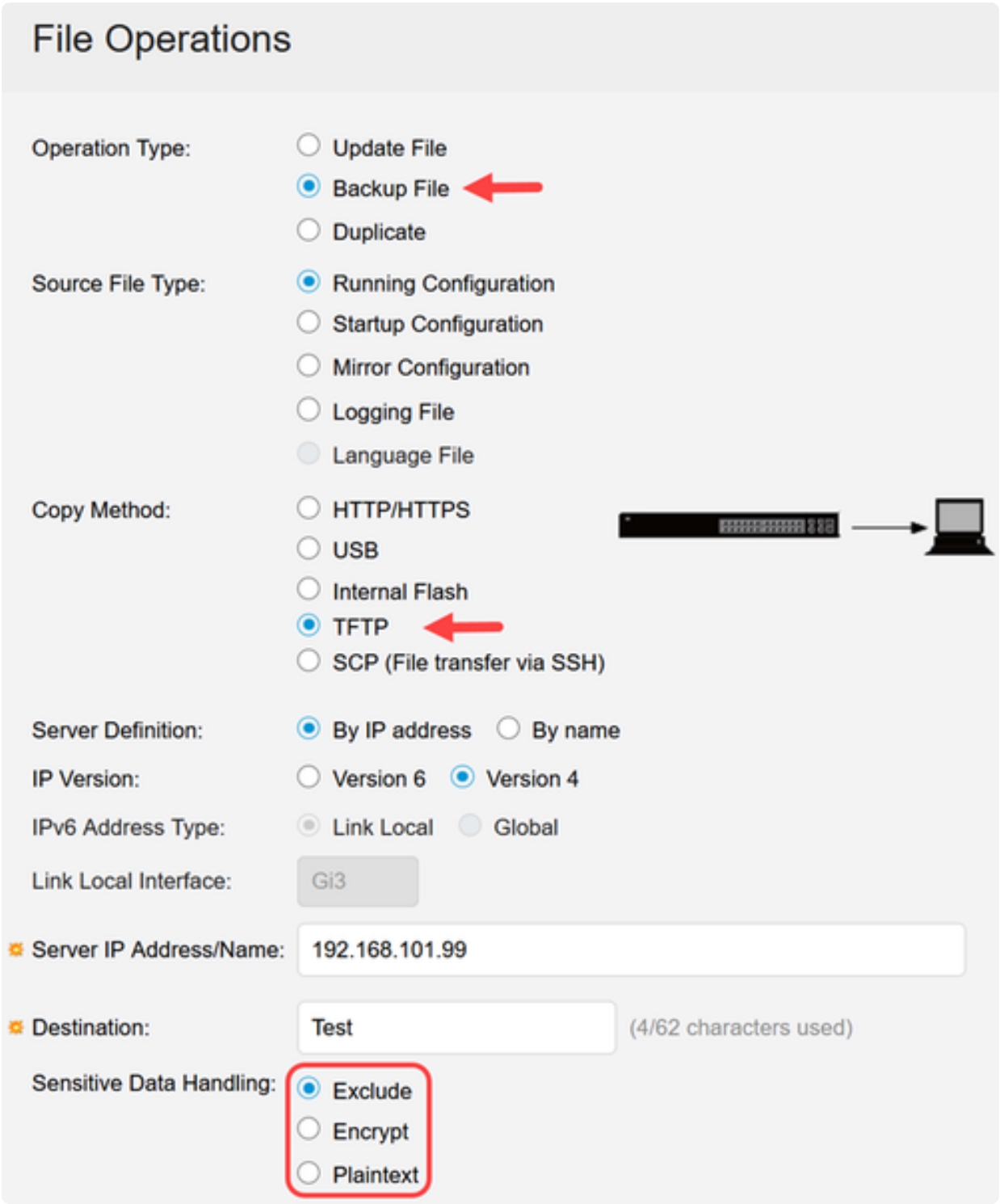
敏感数据处理

复制包含敏感数据的配置文件时，复制任务可以排除敏感数据、以加密形式包含敏感数据、以明文形式包含敏感数据或使用默认方法。指定敏感数据处理是可选的，如果未指定，将使用默认值。

GUI

要使用GUI访问敏感数据处理菜单，请导航到管理>文件操作>文件管理菜单。

- 排除 — 排除敏感数据
- 加密 — 加密敏感数据
- 明文 — 以明文显示敏感数据。



Note:
敏感数据处理选项仅在TFTP或SCP的备份文件模式下显示。

CLI

在命令行中，可以使用copy命令：

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

例如：

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

默认设置是安全敏感数据(SSD)会话读取模式设置为的任何值。要查看当前模式，请输入show ssd session，或输入show running-config，然后查找文件SSD指示灯。使用出厂默认设置，预期的SSD会话读取模式将被加密。

```
show ssd session
```

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

如果在未指定选项的情况下输入copy命令，则复制将如同选择“include-encrypted”一样。

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

但是，可以更改会话读取值：

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

此命令会影响show running-config和show startup-config的输出，并充当copy命令处理敏感数据的默认值。

例如：

```
ssd session read plaintext

exit

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

产生的文件将包含明文形式的敏感数据，以及“show running-config”和“show startup-config”的输出，因此应注意SSD会话读取模式。将其保留为默认值是最安全的。

> **Note:**
> 如果show running-config或show startup-config的输出未显示预期的所有内容，例如在GUI中可见的具有加密凭据的SNMP v3用户，请确保SSD会话读取值未设置为“exclude”。

SNMP

Catalyst 1200/Catalyst 1300/CBSx50系列交换机使用名为rlCopyOptionsRequestedSsdAccess的SNMP对象标识符(OID)来控制敏感数据选项。对象是一个整数，乍看之下，它接受的值与copy命令的值相同：

- 1:排除
- 2:include-encrypted
- 3:include-decrypted（与命令行中的“include-plaintext”相同）
- 4:默认

选项3（以明文形式复制敏感数据）根本不能与SNMP v2c一起使用，除非同时使用身份验证和隐私(authPriv)，否则也不能与SNMP v3一起使用。

> **Note:**
> 设置纯文本选项以使用不安全的协议（如TFTP）复制文件是不明智的。

带authPriv的SNMP v3仅用于触发复制，因此其隐私设置对于传输期间保护配置文件本身没有帮助。例如，使用安全复制协议(SCP)进行复制会更加安全。

选项4“default”选项未按预期运行。它不像copy命令那样工作，并且使用SNMP时，SSD读取会话值对复制结果没有任何影响。相反，选项4与选项1（排除）相同，但有一个例外：如果将SNMP v3与authPriv一起使用，则选项4与选项3（明文）相同。

该行为在下表中进行了总结：

	1（排除）	2（已加密）	3（明文）	默认
CLI副本	已排除	已加密	明文	SSD值

SNMP v2c	已排除	已加密	失败	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	失败	已排除
SNMP v3 noAuthNoPriv	已排除	已加密	失败	已排除

SNMP v3的交换机配置

带authPriv的SNMP v3不是触发复制任务的特定要求，但是由于它提供了更大的灵活性和安全性，因此建议使用其他SNMP变体，并用作以下示例的变体。

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]
```

上述配置允许名为sbscadmin的用户向交换机发送SNMP v3命令以触发文件复制。用户sbscadmin是snmpAdmin组的成员，该组在交换机上已被授予完全SNMP v3写权限。

请注意，用户同时具有身份验证(auth)密码和隐私(priv)密码（即authPriv），并且

snmpAdmin组已设置“priv”（也包含身份验证，因为如果没有密码，隐私将无法使用）。

触发复制任务

以下是触发copy任务的snmpset命令的示例。只要它必须设置几个对象值即可。该命令全部在一行中输入，但反斜杠可以用作转义字符，根据需要将每个项目分隔到自己的行中。这是为了提高可读性，在下面完成的。输入显示为蓝色，输出显示为白色。

```
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
```

- 每个OID都附加“。1”，表示表中用于该任务的行。
- rlCopyRowStatus.1用于将条目插入rlCopyTable。它设置为“createAndGo”，即创建行并将其设置为活动状态，以便交换机可以使用它。
- SSD访问值设置为“include-encrypted”（仅用于此副本）。
- running-config文件复制到目标文件名为“v3-2.txt”的TFTP服务器192.168.111.18。

执行复制任务后，rlCopyOptionsRequestedSsdAccess的值将恢复为4（默认值）。

> Note:
> CISCOSB-COPY-MIB允许对对象及其值使用符号名称，在文件“CISCOSB-copy.mib”中有详细描述，该文件包含在交换机的下载页面上的MIB文件中。

下表将每个对象的符号名称与其OID进行匹配。

符号名称	对象标识符(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

如果未使用MIB文件，则可能会使用OID而不是符号名称来触发文件副本，但输入和输出并不直观。

```
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
```

没有使用简单的“=”符号来设置值，因为如果不使用MIB，命令必须显式设置每个对象类型(“i”表示整数，“a”表示地址，而“s”表示字符串)。 这些值的名称(“local”、“runningConfig”等)也无法使用，因为它们由MIB定义，因此必须直接设置代表这些选项的整数。

Net-SNMP和交换机MIB文件

SNMP管理工具有助于进行测试和故障排除。本文使用Net-SNMP（一套免费和开放源代码SNMP工具）附带的snmpset命令。

为了将交换机MIB文件与Net-SNMP一起使用，首先确保Net-SNMP自己的MIB文件放在Net-SNMP将查找它们的位置，例如$HOME/.snmp/mibs。如果不安装Net-SNMP自己的MIB文件，交换机MIB将无法正常工作。

交换机MIB文件可以解压缩并放置在Net-SNMP的MIB文件的相同位置，但是为了避免兼容性问题，请不要覆盖两个集之间重叠的任何Net-SNMP版本。

当所有MIB文件都位于适当的位置后，可以使用带有所需命令的“-m”参数来调用相关

MIB。

例如：

```
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本身的名称，而不是描述它的文件，即CISCOSB-copy.mib。

有关如何使用Net-SNMP工具的更多信息，请参阅Net-SNMP网站上提供的文档和教程。

结论

现在您已了解通过SNMP触发将配置文件从Cisco Business交换机复制到TFTP服务器的所有步骤。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。