

SNMPによるTFTPサーバへの設定ファイルコピーのトリガー

目的

この記事の目的は、Simple Network Management Protocol(SNMP)を介してCisco Businessスイッチからコンフィギュレーションファイルのコピーをトリガーする手順を説明することです。

適用可能なデバイス

- Catalyst 1200 シリーズ
- Catalyst 1300 シリーズ
- CBS250シリーズ
- CBS350シリーズ

はじめに

コンフィギュレーションファイルは通常、Graphical User Interface (GUI ; グラフィカルユーザインターフェイス) またはCommand Line Interface (CLI ; コマンドラインインターフェイス) を使用してスイッチからコピーされます。さらに珍しい方法として、SNMP経由でコピータスクをトリガーする方法があります。

機密データの処理

機密データを含む構成ファイルをコピーする場合、コピータスクでは、機密データの除外、暗号化形式での挿入、プレーンテキストでの挿入、または既定の方法を使用できます。機密データの処理の指定はオプションで、指定しない場合は既定が使用されます。

GUI

GUIを使用して機密データ処理メニューにアクセスするには、Administration > File Operations > File Managementメニューの順に選択します。

- Exclude : 機密データを除外します。
- Encrypt : 機密データを暗号化します。
- プレーンテキスト : 機密データをプレーンテキストで表示します。

File Operations

Operation Type:

☐ Update File

☒ Backup File 

☐ Duplicate

Source File Type:

☒ Running Configuration

☐ Startup Configuration

☐ Mirror Configuration

☐ Logging File

☐ Language File

Copy Method:

☐ HTTP/HTTPS

☐ USB

☐ Internal Flash

☒ TFTP 

☐ SCP (File transfer via SSH)

Server Definition:

☒ By IP address ☐ By name

IP Version:

☐ Version 6 ☒ Version 4

IPv6 Address Type:

☒ Link Local ☐ Global

Link Local Interface:

Gi3

Server IP Address/Name: 192.168.101.99

Destination: Test (4/62 characters used)

Sensitive Data Handling:

☒ Exclude

☐ Encrypt

☐ Plaintext



Note:

機密データ処理オプションは、TFTPまたはSCPのバックアップファイルモードでのみ表示されます。

CLI を使う場合：

コマンドラインからは、copyコマンドを使用できます。

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

例：

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

デフォルトは、Secure Sensitive Data(SSD)セッションの読み取りモードが設定されているものです。現在のモードを表示するには、show ssd sessionと入力するか、show running-configと入力してファイルSSDインジケータを探します。工場出荷時のデフォルト設定では、予想されるSSDセッションの読み取りモードは暗号化されます。

```
show ssd session
```

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

オプションを指定せずにcopyコマンドを入力すると、「include-encrypted」が選択されたかのようにコピーされます。

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

ただし、セッションの読み取り値は変更できます。

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

このコマンドは、show running-configおよびshow startup-configの出力に影響を与え、copyコマンドで機密データを処理する際のデフォルト値として機能します。

例：

```
ssd session read plaintext
```

```
exit
```

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

この結果のファイルには、show running-configおよびshow startup-configの出力と同様、機密データがプレーンテキストで含まれるため、SSDセッションの読み取りモードに注意する必要があります。デフォルトのままにしておくのが最も安全です。

Note:

show running-configまたはshow startup-configの出力が、たとえばGUIで表示できる暗号化クレデンシャルを持つSNMP v3ユーザなど、予想されるすべてを表示しない場合、SSDセッションの読み取り値が「exclude」に設定されていないことを確認します。

SNMP

Catalyst 1200/Catalyst 1300/CBSx50シリーズスイッチでは、rICopyOptionsRequestedSsdAccessと呼ばれるSNMPオブジェクト識別子(OID)を使用して機密データオプションを制御します。オブジェクトは整数であり、受け取る値は一見するとcopyコマンドの値と同等になります。

- 1: 除外
- 2: 暗号化を含む
- 3: include-decrypted (コマンドラインの"include-plaintext"と同じ)
- 4: デフォルト

オプション3 (機密データをプレーンテキストでコピー) は、認証とプライバシー(authPriv)の両方を使用しない限り、SNMP v2cでは使用できず、SNMP v3でも使用できません。

Note:

プレーンテキストオプションを設定して、TFTPなどの安全でないプロトコルを使用してファイルをコピーするのは得策ではありません。

authPrivを使用するSNMP v3はコピーのトリガーにのみ使用されるため、そのプライバシー設定は転送中のコンフィギュレーションファイル自体の保護には役立ちません。たとえば、Secure Copy Protocol(SCP)を使用したコピーの方がより安全です。

オプション4 (「デフォルト」オプション) は、期待どおりに動作しません。このコマンドはcopyコマンドとは異なる動作をし、SNMPを使用する場合のコピー結果ではSSDの読み取りセッションの値は一切関係ありません。ただし、オプション4はオプション1 (除外) と同じですが、異なる点が1つあります。authPrivでSNMP v3を使用している場合、オプション4はオプション3 (プレーンテキスト) と同じです。

動作の概要を次の表に示します。

	1 (除外)	2 (暗号化)	3 (プレーンテキスト)	デフォルト
CLIコピー	除外	暗号化	プレーンテキスト	SSD値
SNMP v2c	除外	暗号化	失敗	除外
SNMP v3 authPriv	除外	暗号化	プレーンテキスト	プレーンテキスト
SNMP v3 authNoPriv	除外	暗号化	失敗	除外
SNMP v3 noAuthNoPriv	除外	暗号化	失敗	除外

SNMP v3のスイッチ設定

authPrivを使用するSNMP v3は、特にコピータスクのトリガーとして必要というわけではありませんが、柔軟性とセキュリティが向上するため、他のSNMPバリエーションよりも推奨されます。以下の例では、このバージョンを使用します。

設定例：

```
snmp-server server
```

```
snmp-server engineID local 80000000903f01d2da99341
```

```
snmp-server group snmpAdmin v3 priv write Default
```

```
encrypted snmp-server user sbscadmin snmpAdmin v3 auth sha  
[authentication_password] priv [privacy_password]
```

上記の設定では、sbscadminという名前のユーザがスイッチにSNMP v3コマンドを送信してファイルのコピーをトリガーできます。ユーザsbscadminは、スイッチに対する完全なSNMP v3 write権限が付与されたsnmpAdminグループのメンバーです。

ユーザには認証(auth)パスワードとプライバシー(priv)パスワードの両方(authPriv)があり、snmpAdminグループには「priv」が設定されています(これなしではプライバシーは使用できないため、このグループには認証も含まれています)。

コピータスクのトリガー

次に、copyタスクをトリガーする[snmpset](#)コマンドの例を示します。複数のオブジェクト値を設定する必要がある限り有効です。このコマンドは1行で入力できますが、必要に応じてバックスラッシュをエスケープ文字として使用して、各項目を個別の行に区切ることができます。これは、読みやすさを向上させるために以下で行われました。入力は青色で表示され、出力は白色で表示されます。

```
blake@MintBD:~$ snmpset -v 3 -u snmpuser -l authPriv \  
  
-a SHA -A [authentication_password] \  
  
-x AES -X [privacy_password] -m +CISCO-SB-COPY-MIB 192.168.111.253 \  
  
r1CopyOptionsRequestedSsdAccess.1 = include-encrypted \  
  
r1CopyRowStatus.1 = createAndGo \  
  
r1CopySourceLocation.1 = local \  
  
r1CopySourceIpAddress.1 = 0.0.0.0 \  
  
r1CopySourceUnitNumber.1 = 1 \  
  
r1CopySourceFileType.1 = runningConfig \  
  
r1CopyDestinationLocation.1 = tftp \  
  
r1CopyDestinationIpAddress.1 = 192.168.111.18 \  
  
r1CopyDestinationFileName.1 = v3-2.txt \  

```

`rlCopyDestinationFileType.1 = backupConfig`

- 各OIDには、タスクに使用されるテーブルの行を表す「.1」が付加されています。
- 「rlCopyRowStatus.1」は、エントリをrlCopyTableに挿入するために使用されます。これは「createAndGo」に設定されています。つまり、行を作成してアクティブに設定し、スイッチで使用するようにします。
- SSDアクセスの値は「include-encrypted」（このコピーのみ）に設定されます。
- running-configファイルは、192.168.111.18のTFTPサーバにコピーされます。コピー先のファイル名は「v3-2.txt」です。

コピータスクが実行されると、rlCopyOptionsRequestedSsdAccessの値は4（デフォルト）に戻ります。

Note:

オブジェクトのシンボリック名とその値はCISCOSB-COPY-MIBによって使用できます。これについては、「CISCOSB-copy.mib」ファイルで詳しく説明されており、スイッチのダウンロードページにあるMIBファイルに含まれています。

次の表は、各オブジェクトのシンボリック名とそのOIDを一致させます。

シンボリック名	オブジェクト識別子(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
テーブルのコピー	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

MIBファイルを使用しない場合は、シンボリック名の代わりにOIDを使用してファイルのコピーがトリガーされる可能性があります、入出力の方が直感的ではありません。

```
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
```

MIBを使用しない場合、コマンドで各オブジェクトタイプを明示的に設定する必要があります。そのため、単純な「=」記号を使用して値を設定できませんでした(整数の場合は「i」、アドレスの場合は「a」、文字列の場合は「s」)。値の名前(「local」、「runningConfig」など)も使用できません。これらはMIBで定義されているためです。そのため、これらのオプションを表す整数は直接設定する必要があります。

Net-SNMPおよびスイッチMIBファイル

SNMP管理ツールは、テストとトラブルシューティングに役立ちます。この記事では、フリーでオープンソースのSNMPツールスイートであるNet-SNMPに含まれているsnmpsetコマンドを使用しています。

Net-SNMPでスイッチのMIBファイルを使用するには、まずNet-SNMP自身のMIBファイルが、Net-SNMPによって検索される場所(\$HOME/.snmp/mibsなど)に配置されていることを確認します。Net-SNMP独自のMIBファイルがインストールされていないと、スイッチのMIBが正しく動作しません。

スイッチのMIBファイルは解凍して、Net-SNMPのMIBファイルと同じ場所に配置できますが、互換性の問題を避けるため、2つのセット間でオーバーラップするNet-SNMPバージョンを上書きしないでください。

すべてのMIBファイルが適切な場所に配置されたら、適切なコマンドで引数「-m」を使用して関連MIBを呼び出すことができます。

例：

```
snmpget -v 3 -u snmpuser -l authPriv \  
  
-a SHA -A [authentication_password] \  
  
-x AES -X [privacy_password] \  
  
192.168.111.253 r1CopyOptionsRequestedSsdAccess.1
```

Note:

「CISCOSB-COPY-MIB」はMIB自体の名前であり、それを説明するファイルではない。これがCISCOSB-copy.mibである。

Net-SNMPツールの使用方法の詳細については、[Net-SNMP Webサイト](#)で入手できるドキュメントとチュートリアルを参照してください。

結論

これで、SNMPを使用してCisco BusinessスイッチからTFTPサーバへのコンフィギュレーションファイルのコピーをトリガーする手順がすべてわかりました。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。