

Kopieën van configuratiebestanden naar een TFTP-server via SNMP activeren

Doel

Het doel van dit artikel is om de stappen te beschrijven om het kopiëren van configuratiebestanden van een Cisco Business switch via Simple Network Management Protocol (SNMP) te activeren.

Toepasselijke apparaten

- Catalyst 1200 Series software
- Catalyst 1300 Series switches
- CBS250 Series
- CBS350 Series

Inleiding

Configuratiebestanden worden doorgaans gekopieerd van een switch met behulp van de grafische gebruikersinterface (GUI) of de opdrachtregelinterface (CLI). Een meer ongebruikelijke methode is om de kopieertaak via SNMP te activeren.

Gevoelige gegevensverwerking

Wanneer u een configuratiebestand met gevoelige gegevens kopieert, kan de kopieertaak gevoelige gegevens uitsluiten, in versleuteld formulier opnemen, het als onbewerkte tekst opnemen of een standaardmethode gebruiken. Het specificeren van gevoelige gegevensverwerking is facultatief en de standaardinstelling wordt gebruikt als deze niet is gespecificeerd.

GUI

Om toegang te krijgen tot het menu voor gevoelige gegevensverwerking met de GUI, navigeer naar **Beheer > Bestandsbewerkingen > Het menu Bestandsbeheer**.

- Uitsluiten - om gevoelige gegevens uit te sluiten
- Versleutelen - voor het versleutelen van gevoelige gegevens
- Platte tekst - voor het weergeven van gevoelige gegevens in platte tekst.

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:

De optie Sensitive Data Handling verschijnt alleen in de back-upbestandsmodus voor TFTP of SCP.

Vanaf de opdrachtregel kan de opdracht Copy worden gebruikt:

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

Voorbeeld:

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

De standaardinstelling is de modus voor het lezen van beveiligde gevoelige gegevens (SSD)-sessies die is ingesteld op. Om de huidige modus te zien, toont `ssd sessie`, of ga tonen in werking stelt -in werking stellen-config en zoek de bestand SSD indicator. Met fabrieksinstellingen wordt de verwachte leesmodus voor SSD-sessies versleuteld.

```
show ssd session
```

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

Als het exemplaarbevel zonder gespecificeerde optie was ingevoerd, zou het kopiëren alsof "omvatten-gecodeerd" werd gekozen.

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

De waarde voor het lezen van de sessie kan echter worden gewijzigd:

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

Deze opdracht heeft invloed op de output van `show in werking stellen-config` en tonen `startup-config`, evenals het handelen als de standaardwaarde voor de behandeling van gevoelige gegevens van het kopieerbevel.

Voorbeeld:

```
ssd session read plaintext
```

```
exit
```

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

Het resulterende bestand zal gevoelige gegevens in plaintext, evenals de output van "show running-config" en "show startup-config", dus zorg moet worden genomen met de SSD sessie gelezenodus. Het is het veiligst om de standaardinstelling te handhaven.

Note:

Als de output van show in werking stellen-config of tonen startup-config niet alles toont wat wordt verwacht, bijvoorbeeld, SNMP v3 gebruikers met versleutelde referenties die zichtbaar zijn in de GUI, zorg er dan voor dat de SSD sessie gelezen waarde niet is ingesteld om uit te sluiten.

SNMP

Catalyst 1200/Catalyst 1300/CBSx50 Series switches gebruiken de SNMP-objectidentificer (OID) genaamd rIcopyOptionsRequestedSSDAccess om de optie voor gevoelige gegevens te besturen. Het object is een geheel getal en op het eerste gezicht lijken de door het object aanvaarde waarden gelijkwaardig aan die van de opdracht Copy:

- 1: uitsluiten
- 2: opgenomen-versleuteld
- 3: include-decrypted (hetzelfde als "include-plaintext" op de opdrachtregel).
- 4: standaard

Optie 3, die de gevoelige gegevens in plaintext kopieert, kan niet met SNMP v2c worden gebruikt, noch kan het met SNMP v3 worden gebruikt tenzij zowel de authenticatie als privacy (authPriv) worden gebruikt.

Note:

Het is geen goed idee om de platte optie in te stellen om het bestand te kopiëren met een onveilig protocol zoals TFTP.

SNMP v3 met authPriv wordt alleen gebruikt om de kopie te activeren, zodat de privacy-instellingen niet nuttig zijn voor de bescherming van het configuratiebestand zelf tijdens de overdracht. Het kopiëren met Secure Copy Protocol (SCP) zou bijvoorbeeld veiliger zijn.

Optie 4, de "standaard" optie, gedraagt zich niet zoals zou kunnen worden verwacht. Het gedraagt zich niet als de kopieer opdracht, en de SSD lees sessie waarde heeft geen enkele invloed op het kopieer resultaat bij het gebruik van SNMP. In plaats

daarvan is optie 4 hetzelfde als optie 1 (uitsluiten), met één uitzondering: Als u SNMP v3 met authPriv gebruikt, is optie 4 hetzelfde als optie 3 (plaintext).

Het gedrag is samengevat in de onderstaande tabel:

	1 (niet inbegrepen)	2 (versleuteld)	3 (onbewerkte tekst)	standaard
CLI-kopie	uitgesloten	versleuteld	platte tekst	SSD-waarde
SNMP v2c	uitgesloten	versleuteld	faalt	uitgesloten
SNMP v3 authPriv	uitgesloten	versleuteld	platte tekst	platte tekst
SNMP v3 authNoPriv	uitgesloten	versleuteld	faalt	uitgesloten
SNMP v3 zonder toestemming	uitgesloten	versleuteld	faalt	uitgesloten

Switch Configuration voor SNMP v3

SNMP v3 met authPriv is niet specifiek vereist om de kopieertaak te activeren, maar

aangezien het grotere flexibiliteit en veiligheid biedt, wordt het aanbevolen over de andere SNMP-varianten en zal worden gebruikt voor de volgende voorbeelden.

Voorbeeldconfiguratie:

```
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]
```

Door de bovenstaande configuratie kan de gebruiker met de naam sbscadmin SNMP v3-opdrachten naar de switch sturen om het bestandsexemplaar te activeren. Gebruiker sbscadmin is lid van de snmpAdmin groep, die volledige SNMP v3 schrijfrechten op de switch heeft gekregen.

Merk op dat de gebruiker zowel een authenticatie (auth) wachtwoord en een privacy (priv) wachtwoord heeft, d.w.z. authPriv, en de snmpAdmin groep heeft "priv" ingesteld (wat ook verificatie omvat omdat privacy niet zonder kan worden gebruikt).

De kopieertaak activeren

Het volgende is een voorbeeld van [snmpset](#)-opdracht die de kopieertaak activeert. Het is lang als het verschillende objectwaarden moet instellen. Het commando wordt in één regel ingevoerd, maar een backslash kan worden gebruikt als een escape-teken om elk item desgewenst op de eigen regel te scheiden. Dit werd hieronder gedaan om de leesbaarheid te verbeteren. De invoer wordt in blauw weergegeven en de uitvoer in wit.

```
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 \  
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
```

- Elke OID heeft ".1" toegevoegd, die de rij in de tabel vertegenwoordigt die voor de taak wordt gebruikt.
- "rlCopyRowStatus.1" wordt gebruikt om het item in te voegen in rlCopyTable. De instelling is "creerAndGo", d.w.z. maak de rij en stel deze in op actief zodat hij door de switch kan worden gebruikt.
- De toegangswaarde van de SSD is ingesteld op "include-encrypted" (alleen voor dit exemplaar).
- Het in werking stelt -in werking stellen-configuratiedossier wordt gekopieerd aan de server van TFTP in 192.168.111.18 met een bestemmingsdossier - naam van "v3-2.txt".

Nadat de kopieertaak is uitgevoerd, keert de waarde van rlCopyOptionsRequestedSSDAccess terug naar 4 (standaard).

Note:

Het gebruik van symbolische namen voor de objecten en hun waarden wordt mogelijk gemaakt door CISCOSB-COPY-MIB, die in detail wordt beschreven in het bestand "CISCOSB-copy.mib", inclusief de MIB-bestanden op de downloadpagina voor de switch.

In de volgende tabel wordt de symbolische naam van elk object aan de OID gekoppeld.

Symbolische naam	Objectidentificatiecode (OID)
rlKopie-optiesTabel	1.3.6.1.4.1.9.6.1.101.87.12
rlKopieeroptiesAangevraagdeSSD access	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
rlCopyRow-status	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
rlCopySourceIP-adres	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
rlCopyBestemmingslocatie	1.3.6.1.4.1.9.6.1.101.87.2.1.8
rlCopyBestemmingIP-adres	1.3.6.1.4.1.9.6.1.101.87.2.1.9

rlCopyBestemmingBestandsnaam	1.3.6.1.4.1.9.6.1.101.87.2.1.11
rlCopyBestemmingBestandstype	1.3.6.1.4.1.9.6.1.101.87.2.1.12

Als MIB-bestanden niet worden gebruikt, kan het kopiëren van bestanden worden geactiveerd met de OID's in plaats van de symbolische namen, hoewel de invoer en uitvoer minder intuïtief zijn.

```
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
```

Een simpel "=" symbool werd niet gebruikt om de waarden in te stellen omdat, zonder de MIB, de opdracht expliciet elk objecttype moet instellen ("i" voor integer, "a" voor address, en "s" voor string). De namen voor de waarden ("lokaal", "runningConfig", enzovoort) kunnen ook niet worden gebruikt, omdat ze worden gedefinieerd door de MIB, zodat de gehele getallen die deze opties vertegenwoordigen rechtstreeks moeten worden ingesteld.

Net-SNMP- en Switch MIB-bestanden

SNMP-beheertools kunnen nuttig zijn voor test- en probleemoplossingsdoeleinden. In dit artikel wordt de snmpset-opdracht gebruikt die bij [Net-SNMP is](#) inbegrepen, een reeks gratis en opensource SNMP-tools.

Om de switch MIB-bestanden met Net-SNMP te kunnen gebruiken, moet u er eerst voor zorgen dat de eigen MIB-bestanden van Net-SNMP op een locatie worden geplaatst waar Net-SNMP ernaar zal zoeken, bijvoorbeeld \$HOME/.snmp/mibs. Zonder de eigen MIB-bestanden van Net-SNMP zullen de switch MIBs niet goed werken.

De switch MIB-bestanden kunnen worden uitgepakt en op dezelfde locatie geplaatst als de MIB-bestanden van Net-SNMP, maar om compatibiliteitsproblemen te voorkomen, moet u de Net-SNMP-versies van alle versies die de twee sets overlappen niet overschrijven.

Zodra alle MIB-bestanden op een geschikte locatie zijn geïnstalleerd, kunnen de relevante MIB(s) worden aangeroepen met behulp van het "-m" argument met de gewenste opdracht.

Voorbeeld:

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

```

192.168.111.253 rlCopyOptionsRequestedSsdAccess.1

Note:

"CISCOB-COPY-MIB" is de naam van de MIB zelf en niet het bestand dat het beschrijft, namelijk CISCOSB-copy.mib.

Zie de documentatie en zelfstudies op de [Net-SNMP-website voor](#) meer informatie over het gebruik van de Net-SNMP_tools.

Conclusie

Nu kent u alle stappen om het kopiëren van configuratiebestanden van een Cisco Business switch naar een TFTP-server via SNMP te activeren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.