

Konfigurieren der PnP-Einstellungen auf einem Switch über die CLI

Ziel

Die Installation neuer Netzwerkgeräte oder der Austausch von Geräten kann bei manueller Ausführung teuer, zeitaufwendig und fehleranfällig sein. In der Regel werden neue Geräte zuerst an eine zentrale Staging-Einrichtung gesendet, wo die Geräte nicht im Boxed-Zustand sind, mit einem Staging-Netzwerk verbunden sind, mit den richtigen Lizenzen, Konfigurationen und Images aktualisiert werden und dann verpackt und an den eigentlichen Installationsstandort geliefert werden. Nach Abschluss dieser Prozesse müssen die Experten zu den Installationsstandorten reisen, um die Installation durchzuführen. Selbst in Szenarien, in denen die Geräte im NOC (No Objection Certificate) oder im Rechenzentrum selbst installiert sind, gibt es möglicherweise nicht genügend Experten für die schiere Anzahl von Geräten. All diese Probleme führen zu Verzögerungen bei der Bereitstellung und verursachen zusätzliche Betriebskosten.

Die Cisco Plug-in-Play-Lösung senkt die Kosten für die Bereitstellung und Installation von Netzwerkgeräten, beschleunigt die Installation und reduziert die Komplexität der Bereitstellung, ohne die Sicherheit zu gefährden. Mit der Cisco Plug-in-Play-Lösung können Sie Zero-Touch-Installationen der Switches in verschiedenen Bereitstellungsszenarien und Bereitstellungsstandorten durchführen.

Dieser Artikel enthält Anweisungen zur Konfiguration der PnP-Einstellungen auf Ihrem Switch über die Befehlszeilenschnittstelle (CLI).

Unterstützte Geräte

- Sx350-Serie
- SG350X-Serie
- Sx550X-Serie

Software-Version

- 2.3.5.63

PNP-Einstellungen konfigurieren

Schritt 1: Melden Sie sich bei der Switch-Konsole an. Der Standardbenutzername und das Standardkennwort lauten "cisco". Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, müssen Sie an dieser Stelle diese neuen Anmeldeinformationen eingeben.

Anmerkung: Um zu erfahren, wie Sie über SSH oder Telnet auf eine SMB-Switch-CLI zugreifen, klicken Sie [hier](#).

```
[User Name:cisco  
[Password:*****
```

Anmerkung: Die Befehle können je nach genauem Switch-Modell variieren. In diesem Beispiel wird über Telnet auf einen SG350X-Switch zugegriffen.

Schritt 2: Geben Sie im privilegierten EXEC-Modus des Switch den nachfolgenden Befehl ein, um in den globalen Konfigurationsmodus zu wechseln.

```
CBS350X#configure
```

Schritt 3: Um PnP auf Ihrem Switch global zu aktivieren, geben Sie Folgendes ein:

```
SG350X(config)#pnp enable
```

```
[SG350X#configure  
[SG350X(config)#pnp enable  
SG350X(config)#
```

Schritt 4: Geben Sie das Protokoll und den PnP-Servernamen oder die IP-Adresse ein, um Konfigurationsinformationen zu finden:

```
SG350X(config)#pnp transport [protocol] {{server [name] [ip address]}}
```

Anmerkung: Das Standard-Transportprotokoll ist HTTP, und der PnP-Servername ist **pnpserver**.

```
[SG350X#configure  
[SG350X(config)#pnp enable  
[SG350X(config)#pnp transport http 192.168.100.112  
SG350X(config)#
```

Anmerkung: In diesem Beispiel wird HTTP als PnP-Transportprotokoll verwendet, und die IP-Adresse des Servers wird 192.168.100.112 eingegeben.

Schritt 5: Um den Benutzernamen und das Kennwort für die Eingabe in PnP-Paketen zu konfigurieren, geben Sie Folgendes ein:

```
SG350X(config)#pnp device username [username] password [password]
```

```
[SG350X#configure  
[SG350X(config)#pnp enable  
[SG350X(config)#pnp transport http 192.168.100.112  
[SG350X(config)#pnp device username cisco password Cisc01234$  
SG350X(config)#
```

Anmerkung: In diesem Beispiel lautet der Benutzername cisco und das Kennwort Cisco01234\$.

Schritt 6: Um das Wiederherstellungsintervall in Sekunden zu konfigurieren, bevor Sie versuchen, die Sitzung nach dem Verbindungsverlust erneut zu verbinden, geben Sie Folgendes ein:

```
SG350X(config)#pnp reconnect interval [seconds]
```

```
SG350X#configure
SG350X(config)#pnp enable
SG350X(config)#pnp transport http 192.168.100.112
SG350X(config)#pnp device username cisco password Cisco01234$
SG350X(config)#pnp reconnect interval 30
SG350X(config)#
```

Anmerkung: In diesem Beispiel wird "Use Default" (Standard verwenden) ausgewählt, der den Standardwert von 30 Sekunden hat.

Schritt 7: Um die Zeitüberschreitungseinstellungen für die Erkennung zu konfigurieren, geben Sie Folgendes ein:

```
SG350X(config)#pnp discovery timeout [seconds] [exponential factor] [timeout value]
```

```
SG350X#configure
SG350X(config)#pnp enable
SG350X(config)#pnp transport http 192.168.100.112
SG350X(config)#pnp device username cisco password Cisco01234$
SG350X(config)#pnp reconnect interval 30
SG350X(config)#pnp discovery timeout 60 3 540
SG350X(config)#
```

Folgende Optionen sind verfügbar:

- timeout seconds (Timeout-Sekunden) - Die Zeit, die in Sekunden gewartet wird, bevor erneut versucht wird, eine Erkennung durchzuführen, nachdem eine Erkennung des PnP-Servers fehlgeschlagen ist. Der Standardwert ist 60 Sekunden.
- exponentieller Faktor - Der Wert, der den Erkennungsversuch exponentiell auslöst, indem der vorherige Timeout-Wert mit einem exponentiellen Wert multipliziert und das Ergebnis als Timeout angewendet wird (wenn der Wert kleiner als der maximale Timeout-Wert ist). In diesem Beispiel wird der Standardwert 3 verwendet.
- max timeout value - Der maximale Wert von Timeout in discovery. Der Wert muss größer als der Wert für das Discovery-Timeout sein.

Schritt 8: Um das Überwachungs-Timeout zu konfigurieren, geben Sie Folgendes ein:

```
SG350X(config)#pnp watchdog timeout [seconds]
```

- seconds (Sekunden) - das Zeitintervall, in dem gewartet wird, bis eine Antwort von einem PnP oder einem Dateiserver während einer aktiven PnP-Sitzung, z. B. während eines Datei-Download-Prozesses, eingeht. In diesem Beispiel werden 60 Sekunden verwendet.

```
SG350X#configure
SG350X(config)#pnp enable
SG350X(config)#pnp transport http 192.168.100.112
SG350X(config)#pnp device username cisco password Cisc01234$
SG350X(config)#pnp reconnect interval 30
SG350X(config)#pnp discovery timeout 60 3 540
SG350X(config)#pnp watchdog timeout 60
SG350X(config)#
```

Schritt 9: Geben Sie den Befehl **exit** ein, um zum privilegierten EXEC-Modus zurückzukehren:

```
SG350X#configure
SG350X(config)#pnp enable
SG350X(config)#pnp transport http 192.168.100.112
SG350X(config)#pnp device username cisco password Cisc01234$
SG350X(config)#pnp reconnect interval 30
SG350X(config)#pnp discovery timeout 60 3 540
SG350X(config)#pnp watchdog timeout 60
SG350X(config)#exit
SG350X#
```

Schritt 10: (Optional) Geben Sie Folgendes ein, um die PnP-Einstellungen auf Ihrem Switch anzuzeigen:

CBS350X#show pnp

```
SG350X(confia)#exit
SG350X#show pnp
Administrative status: enabled
Operational status: ready
PnP Agent state: discoveryWait
Transport protocol: http
Server IP address: 192.168.100.112
TCP port: 80
Username: cisco
(Encrypted>Password: R0Z8xIG/Z6y1iBQgm0IjzCChWoNV3LiNH3gwByD4V0k=
Discovery Timeout: 60 seconds
Discovery Exponential Factor: 3
Discovery Maximum Timeout: 540 seconds
PnP Session Interval Timeout: 30 seconds
PnP Watchdog Timeout: 60 seconds
Timer Remainder: 211 seconds
SG350X#
```

Schritt 11: (Optional) Speichern Sie im privilegierten EXEC-Modus des Switches die konfigurierten Einstellungen in der Startkonfigurationsdatei, indem Sie Folgendes eingeben:

CBS350X#copy running-config startup-config

```
SG550XG# copy running-config startup-config  
Overwrite file [startup-config]... (Y/N)[N] ?
```

Schritt 12: (Optional) Drücken Sie Y für Yes (Ja) oder N für No (Nein) auf Ihrer Tastatur, sobald die Überschreibdatei [startup-config].... wird angezeigt.

```
SG350X# copy running-config startup-config  
Overwrite file [startup-config]... (Y/N)[N] ?Y  
22-Sep-2017 04:09:18 %COPY-I-FILECPY: Files Copy - source URL running-config des  
tination URL flash://system/configuration/startup-config  
22-Sep-2017 04:09:20 %COPY-N-TRAP: The copy operation was completed successfully  
SG350X#
```

Sie sollten jetzt die PnP-Einstellungen auf Ihrem Switch erfolgreich über die CLI konfiguriert haben.