

通過CLI配置交換機上的SNMP組

目標

簡單網路管理協定(SNMP)是一種網路管理協定，有助於記錄、儲存和共用有關網路中裝置的資訊。這有助於管理員解決網路問題。SNMP使用管理資訊庫(MIB)以分層方式儲存可用資訊。SNMP組用於根據MIB中不同SNMP檢視的訪問許可權和授權來組合SNMP使用者。每個SNMP組由組名和安全級別組合唯一標識。

本文說明如何使用交換器的指令行介面建立和設定SNMP群組。假設已為該裝置配置了SNMP檢視。

也可通過交換機的基於Web的實用程式配置SNMP組。如需說明，請參閱[在交換器上設定簡易網路管理通訊協定\(SNMP\)群組](#)。

適用裝置

- Sx350系列
- SG350X系列
- Sx500系列
- Sx550X系列

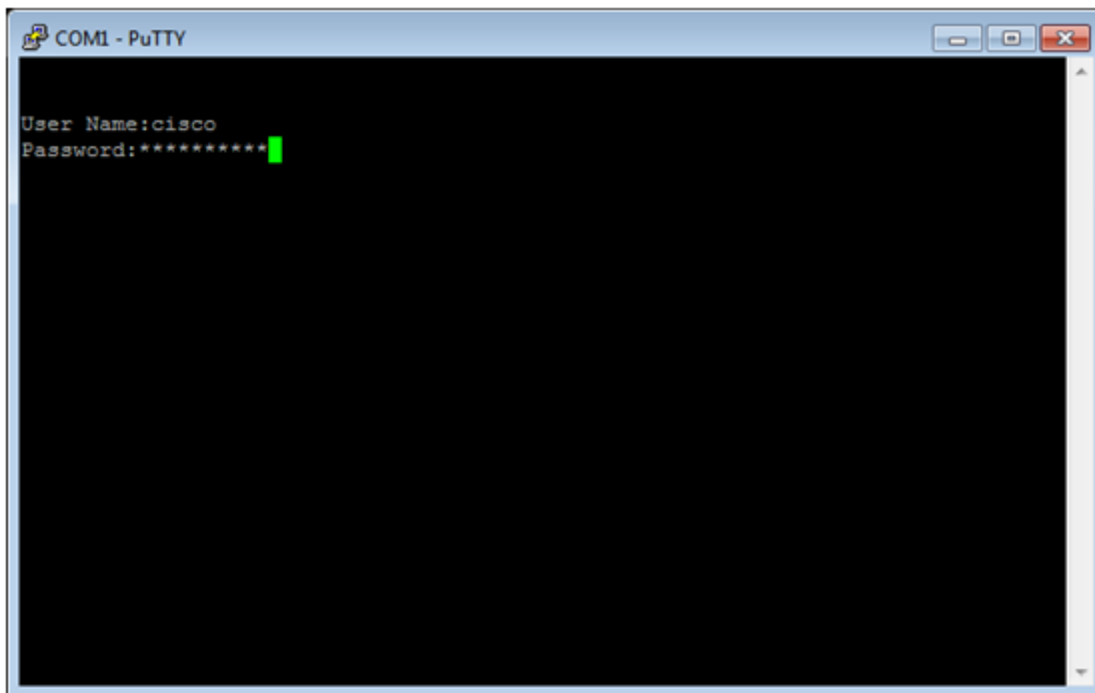
軟體版本

- 1.4.7.05 - Sx300、Sx500
- 2.2.8.04 - Sx250、Sx350、SG350X、Sx550X

在交換機上配置SNMP組

步驟1

存取交換器的CLI。



在本示例中，PuTTY是用於訪問交換機CLI的應用程式。預設使用者名稱和密碼為cisco/cisco。如果您已自定義您的憑據，請使用使用者名稱和密碼。

步驟2

通過輸入以下命令切換到全域性配置模式：

```
Switch350X#configure terminal
```

步驟3

使用以下語法建立SNMP組：

```
snmp-server group groupname{v1/v2/v3 {{noauth/auth/priv}}[notify notifyview]][read readview]  
[write writeview]。
```

其中：

- group *groupname* — 您可以在此處指定組的名稱。組名稱的長度可以是1到30個字元。
- v1 — 此選項使用SNMP版本1安全模型。
- v2 — 此選項使用SNMP版本2安全模型
- v3 — 此選項使用SNMP第3版安全模型。
- noauth — 此選項指定將不執行封包驗證。此選項僅適用於SNMPv3安全模型。
- auth — 此選項指定將執行不加密的資料包身份驗證。此選項僅適用於SNMPv3安全模型。
- priv — 此選項指定將執行加密資料包身份驗證。此選項僅適用於SNMPv3安全模型。
- notify *notifyview* — （可選）此選項指定用於生成通知或陷阱的檢視名稱。通知是需要確認的陷阱。此選項僅在SNMPv3安全模型上可用。
- read *readview* — （可選）此選項指定僅允許檢視的檢視名稱。檢視名稱的長度可在1到30個字元之間。
- write *writeview* — （可選）此選項指定用於配置代理的檢視名稱。檢視名稱可以是1到30個字元。

```
Switch350X#snmp-server group CiscoTestUsers v3 auth notify Cisco1234$ read
```

在本示例中，輸入了snmp-server group CiscoTestUsers v3 auth notify Cisco1234\$ read。

步驟4

使用以下命令驗證SNMP組：

```
Switch350X#show snmp groups
```

現在，您應該已經通過交換機的CLI配置了SNMP組設定。