

ERNW Newsletter 20 / Oktober 2007

Liebe Partner, liebe Kollegen,

willkommen zur 20. Ausgabe des ERNW-Newsletters mit dem Thema:

SNMP Version 3 in der Praxis

Ein Anwendungsbeispiel mit CiscoWorks LMS 3.0

von Peter Fiers

24.09.2007

Einführung

Das ‚Simple Network Management Protocol‘ in der Version 3 wird von Netzwerkadministratoren trotz seiner Vorteile gegenüber seinen Vorgängern stiefmütterlich behandelt. Dieses Dokument versucht es, sowohl die Vorteile als auch die Gründe für die Benachteiligung auf den Punkt zu bringen und an einem praktischen Beispiel zu zeigen, dass SNMPv3 durchaus für den Betrieb interessant sein kann.

SNMP-Versionen und die Datensicherheit

Welches Tool auch immer im Bereich Netzwerkmanagementsysteme (NMS) eingesetzt wird, es wird kaum ohne das ‚Simple Network Management Protocol‘ (SNMP) auskommen.

Definition – Umsetzung – Kontrolle

1



SNMP ist ein altgedienter und bewährter Standard. Veröffentlicht im Jahre 1988, erlebte es mittlerweile mehrere Aktualisierungen. Die jeweiligen Veränderungen / Ergänzungen waren unterschiedlicher Natur. Die zweite SNMP-Version brachte einen erweiterten Funktionsumfang gegenüber der Ersten mit (u.a. 'bulk retrieval' und erweiterte Fehlercodes). Außerdem wurde die community-basierte Authentifizierung der ersten Version auf die Zweite übertragen. Diese Variante der zweiten Version ist unter der Bezeichnung '2c' bekannt. Die dritte SNMP-Version verbesserte die Sicherheit der SNMP-Kommunikation mittels kryptographischer Mechanismen. In der NMS-Landschaft spielen heute die Versionen 2c und 3 (im Folgenden 'SNMPv2c' bzw. 'SNMPv3') eine Rolle, aber die meisten Implementierungen verwenden wohl SNMPv2c.

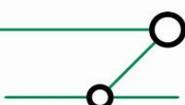
Wieso eigentlich nicht SNMPv3, wenn diese eine Verbesserung gegenüber SNMPv2c darstellt? Welcher sicherheitsbewusste und verantwortlich denkende Admin will seine Daten in Zeiten wachsender Bedrohung nicht durch kryptographische Lösungen schützen? Der Authentifizierungsmechanismus von SNMPv2c öffnet definitiv eine Sicherheitslücke. SNMPv2c verwendet bei Requests den 'Community-String', eine Art Kennwort, das unverschlüsselt zum abgefragten Gerät übertragen wird, um das NMS zu authentifizieren¹. Die Folgen einer möglichen Kompromittierung des Community-Strings fallen besonders gravierend aus, wenn der für den Schreibzugriff zuständige Community-String betroffen ist. Welches Sicherheitsrisiko die wohlbekannten Default-Communities in sich bergen, bedarf gar nicht der Erwähnung. Im Sicherheitsmodell von SNMPv3 sind dagegen sowohl eine Hash-Authentifizierung des NMS mit Benutzername und Kennwort als auch die Verschlüsselung von SNMP-Daten vorgesehen.

Warum also nicht SNMPv3 verwenden? Nun ja, wer will schon ein bewährtes System aufgeben, die Last der Umstellung auf sich nehmen? SNMPv3 ist außerdem aufwändiger in der Konfiguration und ihre Unterstützung durch die Hersteller von Managementsystemen ist mangelhaft. Mangelhaft bedeutet allerdings nicht "gar nicht vorhanden" und auch der Aufwand hält sich bei näherem Besehen in Grenzen. Im Folgenden soll gezeigt werden, wie eine Managementanwendung, die lange ohne SNMPv3 auskommen musste, mit einem verschwindend geringen Mehraufwand auch für die Verwendung von SNMPv3 konfiguriert werden kann.

User Tracking mit SNMPv2c

Das Tool 'User Tracking' (UT) aus Ciscos Produktfamilie CiscoWorks dient zur Ortung dem Netzwerk angeschlossener Endgeräte. Es wird von der CiscoWorks-Komponente 'Campus Manager' aus bedient. Der 'Campus Manager' liegt aktuell in der Version 5.0.1 vor. UT sammelt Layer-2-Informationen von den von CiscoWorks verwalteten Switchen im LAN und erstellt eine Tabelle, in der die Zuordnung zwischen MAC-Adressen und Switchports für

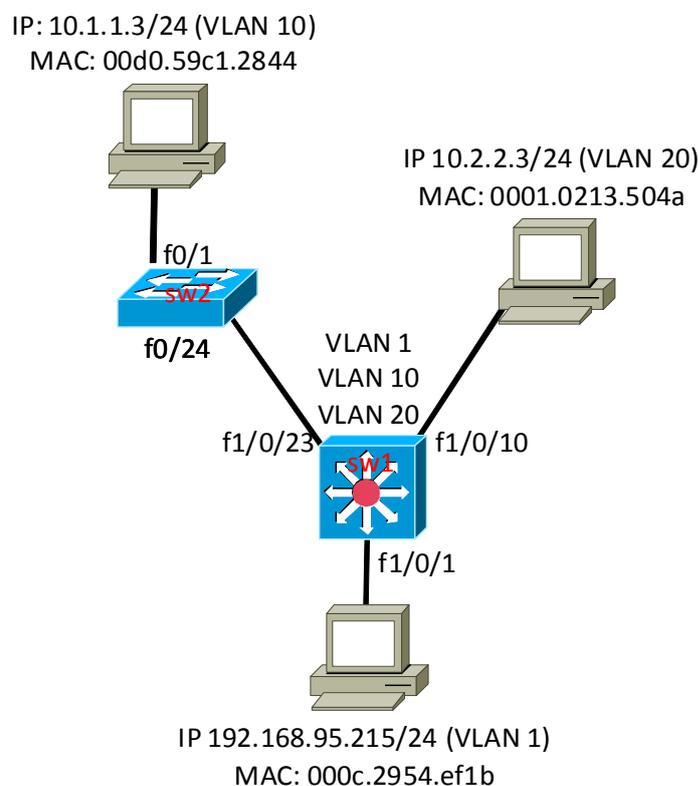
¹ Bei den nachstehend beschriebenen Tests arbeiten wir nur mit SNMP-Requests. SNMP-Notifications, bei denen die Authentifizierung anders verläuft, werden bewusst und grundsätzlich ausgeklammert.



jedes VLAN festgehalten wird². Um an die benötigten Informationen zu kommen, liest UT den Inhalt der sogenannten BRIDGE-MIB mittels SNMP aus. Es existieren allerdings mehrere Instanzen dieser MIB auf einem Gerät, wenn das Gerät mehrere VLANs konfiguriert hat: eine Instanz pro VLAN. Um an die vollständigen Daten heranzukommen, muss UT alle Instanzen der MIB auslesen.

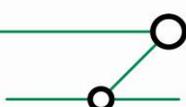
Zur Adressierung einzelner Instanzen einer MIB wird von SNMPv2c das sogenannte 'community indexing' eingesetzt. Dabei wird einer SNMP-Abfrage nicht einfach nur der Community-String übergeben, sondern dieser wird auch mit einem Index versehen, der auf die MIB-Instanz hinweist, an welcher das abfragende System interessiert ist. Die MIB-Instanz wird mit der VLAN-ID referenziert. Das Konstrukt hat dementsprechend folgendes Format: *community-string@vlan-id*.

Um es gleich konkret zu machen, betrachten wir folgendes Szenario:



Der Switch sw1 (ein Catalyst 3750) hat drei VLANs konfiguriert: 1, 10 und 20. Die Ports f1/0/1 und f1/0/10 sind Access-Ports in VLAN 1 bzw. VLAN 20. Über diese Ports sind zwei PCs mit dem Switch verbunden. Ein dritter PC hängt an einem anderen Switch in VLAN 10

² Die UT-Datenbank kann auch andere Informationen (IP-Adressen, Benutzernamen) enthalten, diese Dinge gehören aber nicht zu unserem Thema.



und ist über den Trunk-Port f1/0/23 von sw1 aus zu erreichen. Dieser kommuniziert mit den Hosts in den VLANs über SVIs. Als Management-VLAN wird VLAN 1 benutzt. Hier hat sw1 die IP-Adresse 192.168.95.240. Er kommt mit einer denkbar einfachen SNMP-Konfiguration aus, um UT zu unterstützen. Es müssen die Community-Strings für den Lese- und den Schreibzugriff konfiguriert sein³:

```
sw1#sh run | incl snmp
snmp-server community public RO
snmp-server community private RW4
```

Es soll jetzt am Beispiel der Auslesung von MAC-Adressen gezeigt werden, wie 'community indexing' funktioniert⁵. Analog dazu geht es auch mit anderen Object-IDs, die von UT abgefragt werden. Zunächst wollen wir aber auf dem herkömmlichen Weg Informationen sammeln, um die Richtigkeit der Angaben in der Grafik zu bestätigen und um zu sehen, über welche Informationen der Switch verfügt. Der Inhalt des ARP-Caches zeigt die Zuordnung von MAC-Adressen zu IP-Adressen:

```
sw1#sh arp
Protocol  Address                Age (min)  Hardware Addr  Type
Interface
Internet  10.2.2.3                0          0001.0213.504a  ARPA          Vlan20
Internet  10.1.1.3                0          00d0.59c1.2844  ARPA          Vlan10
Internet  192.168.95.215         0          000c.2954.ef1b  ARPA          Vlan1
...
```

Möglicherweise müssen die PCs zuerst angepingt werden, damit die einschlägigen Tabellen mit Einträgen gefüllt werden. Die MAC-Adress-Tabelle gibt Auskunft darüber, welche MAC-Adresse über welchen Switchport zu erreichen ist. Die VLAN-Zugehörigkeit der MAC-Adressen wird mit ausgegeben:

```
sw1#sh mac-address-table
          Mac Address Table
-----
Vlan    Mac Address             Type           Ports
----    -
1       000c.2954.ef1b         DYNAMIC       Fa1/0/1
```

³ Es tut sich eine weitere Sicherheitslücke auf: Die Community-Strings werden im Klartext in der Konfig aufbewahrt.

⁴ Verwenden Sie für Ihre Geräte im Produktivbetrieb niemals die hier genannten Community-Strings „public“ und „private“.

⁵ Dafür allein würde übrigens auch die Konfiguration des Community-Strings für den Lesezugriff reichen.



```
10    00d0.59c1.2844    DYNAMIC    Fa1/0/23
20    0001.0213.504a    DYNAMIC    Fa1/0/10
```

...

Diese Informationen müssen auch per SNMP zu beziehen sein, damit UT erfolgreich arbeiten kann. Ein Schritt ist die Besorgung der MAC-Adressen. Die OID für das Herunterziehen der MAC-Adress-Tabelle heißt *dot1dTpFdbAddress* (.1.3.6.1.2.1.17.4.3.1.1). Wenn man ein *snmpwalk*⁶ ohne 'community indexing' durchführt, bekommt man allerdings nur ein Teil der dem Switch bekannten MAC-Adressen. Dann wird nämlich nur die MIB-Instanz des VLAN 1 (Default-VLAN) ausgelesen:

```
gipszjakab@pal:/home/gipszjakab> snmpwalk -v 2c -c public 192.168.95.240 \
.1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.212.0 = Hex-STRING: 00 08 21 23 D4 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.212.24 = Hex-STRING: 00 08 21 23 D4 18
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.221.0 = Hex-STRING: 00 08 21 23 DD 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.221.24 = Hex-STRING: 00 08 21 23 DD 18
SNMPv2-SMI::mib-2.17.4.3.1.1.0.9.232.151.10.194 = Hex-STRING: 00 09 E8 97 0A C2
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.12.4.116 = Hex-STRING: 00 0C 29 0C 04 74
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.84.239.27 = Hex-STRING: 00 0C 29 54 EF 1B
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.170.109.246 = Hex-STRING: 00 0C 29 AA 6D F6
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.232.214.231 = Hex-STRING: 00 0C 29 E8 D6 E7
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.240.108.202 = Hex-STRING: 00 0C 29 F0 6C CA
SNMPv2-SMI::mib-2.17.4.3.1.1.0.19.169.201.161.20 = Hex-STRING: 00 13 A9 C9 A1 14
SNMPv2-SMI::mib-2.17.4.3.1.1.0.20.242.155.247.196 = Hex-STRING: 00 14 F2 9B F7 C4
SNMPv2-SMI::mib-2.17.4.3.1.1.0.26.146.79.6.219 = Hex-STRING: 00 1A 92 4F 06 DB
SNMPv2-SMI::mib-2.17.4.3.1.1.0.96.8.78.32.34 = Hex-STRING: 00 60 08 4E 20 22
```

Um auch die anderen MIB-Instanzen auslesen zu können, müssen wir den passenden Index dranhängen:

```
gipszjakab@pal:/home/gipszjakab> snmpwalk -v 2c -c public@10 192.168.95.240
.1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.208.89.193.40.68 = Hex-STRING: 00 D0 59 C1 28 44
gipszjakab@pal:/home/gipszjakab> snmpwalk -v 2c -c public@20 192.168.95.240
.1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.1.2.19.80.74 = Hex-STRING: 00 01 02 13 50 4A
```

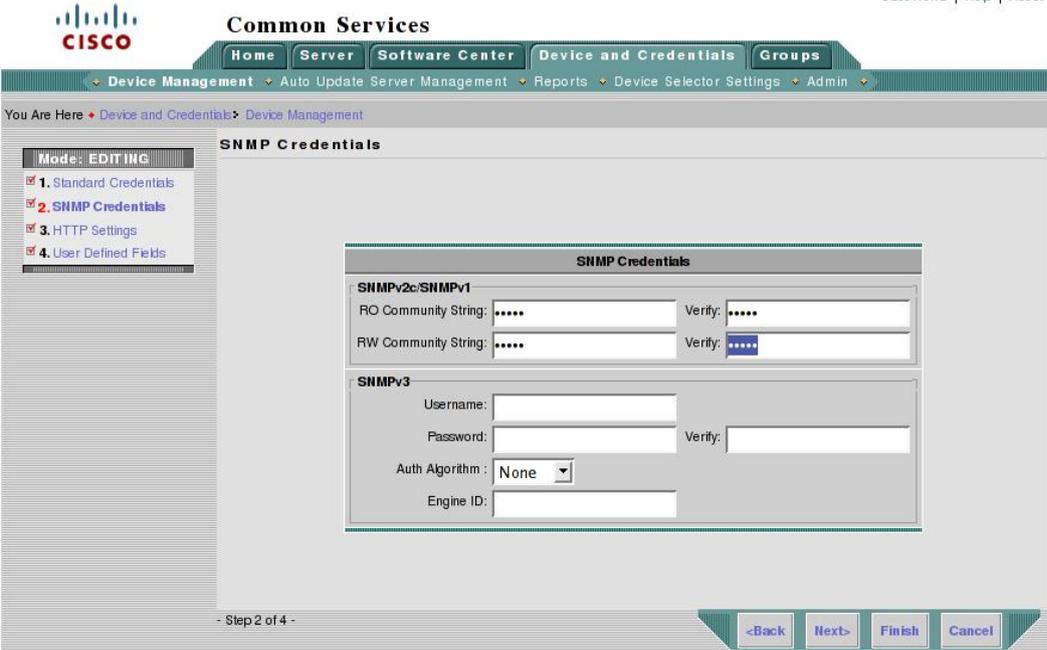
Dem Einsatz von UT steht nichts im Wege. UT macht die nötigen Abfragen, ohne dass man am NMS etwas anderes konfigurieren muss als die passenden Community-Strings. Um es geräte- oder gerätegruppenweise zu erledigen, sucht man **Common Services > Device and Credentials > Device Management** auf, wählt das/die zu bearbeitende/n Gerät/e im Fenster **Device Summary** aus und klickt auf die Schaltfläche **Edit Credentials**. Es erscheint eine neue Seite, dort klickt man **SNMP Credentials** in der Linkliste an der linken Seite an. In der daraufhin angezeigten Maske füllt man dann die entsprechenden Felder sinngemäß aus:

⁶ Snmpwalk ist ein Tool aus der Softwarefamilie Net-SNMP (<http://net-snmp.sourceforge.net/>)





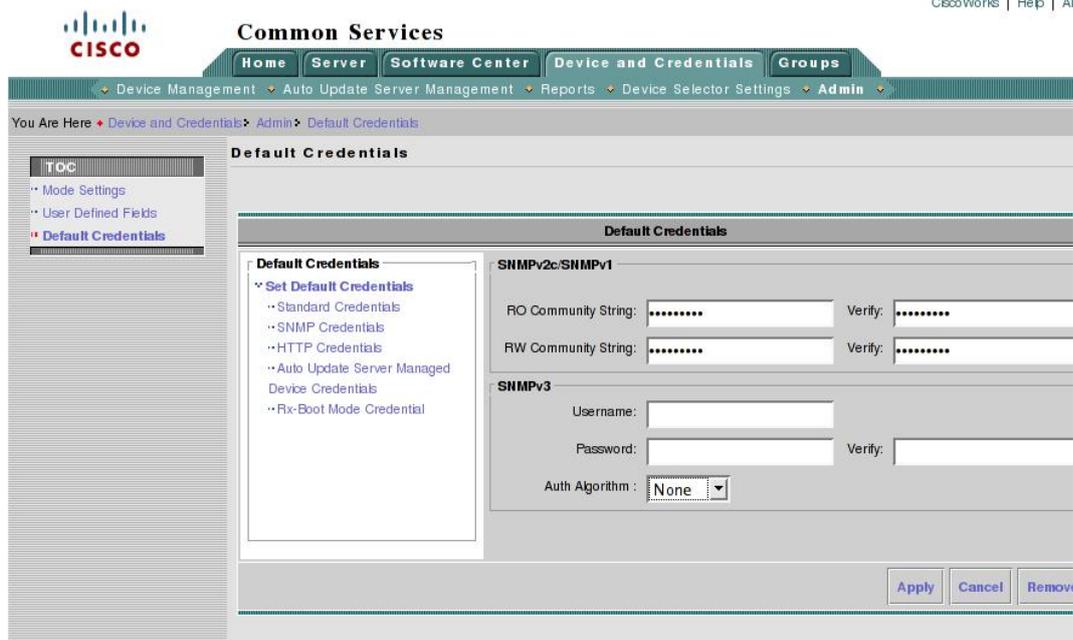
The screenshot shows the 'Common Services' interface with the 'Device Management' section active. The breadcrumb trail is: Home > Server > Software Center > Device and Credentials > Groups > Device Management > Auto Update > Server Management > Reports > Device Selector Settings > Admin. The main content area is titled 'Device Management' and contains a 'Device Summary' window. This window has a search bar and a table with columns 'All', 'Search Results', and 'Selection'. Under 'All Devices', three IP addresses are listed: 192.168.95.240 (checked), 192.168.95.241, and 192.168.95.242. Below the table are buttons for 'Edit Identity', 'Edit Credentials', 'Delete', 'View', 'Add', 'Bulk Import', 'Export', and 'Exclude'. A status bar at the bottom indicates '1 devices (n) selected'.



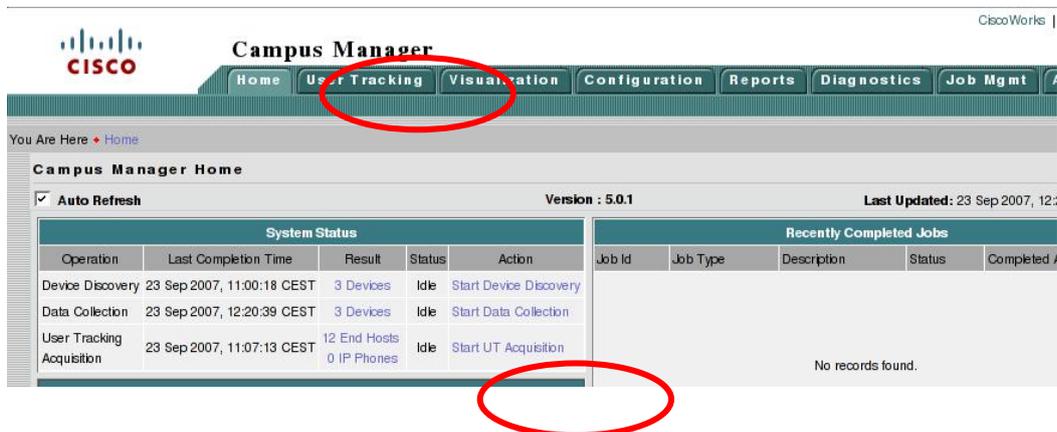
The screenshot shows the 'SNMP Credentials' configuration page in 'Mode: EDITING'. The breadcrumb trail is: Home > Server > Software Center > Device and Credentials > Groups > Device Management > Auto Update > Server Management > Reports > Device Selector Settings > Admin. On the left, a sidebar lists four steps: 1. Standard Credentials, 2. SNMP Credentials (selected), 3. HTTP Settings, and 4. User Defined Fields. The main form is titled 'SNMP Credentials' and is divided into two sections: 'SNMPv2c/SNMPv1' and 'SNMPv3'. The 'SNMPv2c/SNMPv1' section has fields for 'RO Community String' and 'RW Community String', each with a 'Verify' field. The 'SNMPv3' section has fields for 'Username', 'Password', 'Auth Algorithm' (set to 'None'), and 'Engine ID', along with a 'Verify' field. At the bottom, there are navigation buttons: '<Back', 'Next>', 'Finish', and 'Cancel'. A status bar at the bottom left indicates '- Step 2 of 4 -'.

Man kann die Zugangsdaten auch auf der Common-Services-Seite unter **Common Services > Device and Credentials > Admin > Default Credentials** eintragen, dann hätte man sie auch für Geräte parat, für die keine eigenen Zugangsdaten explizit in der Datenbank vorhanden sind:



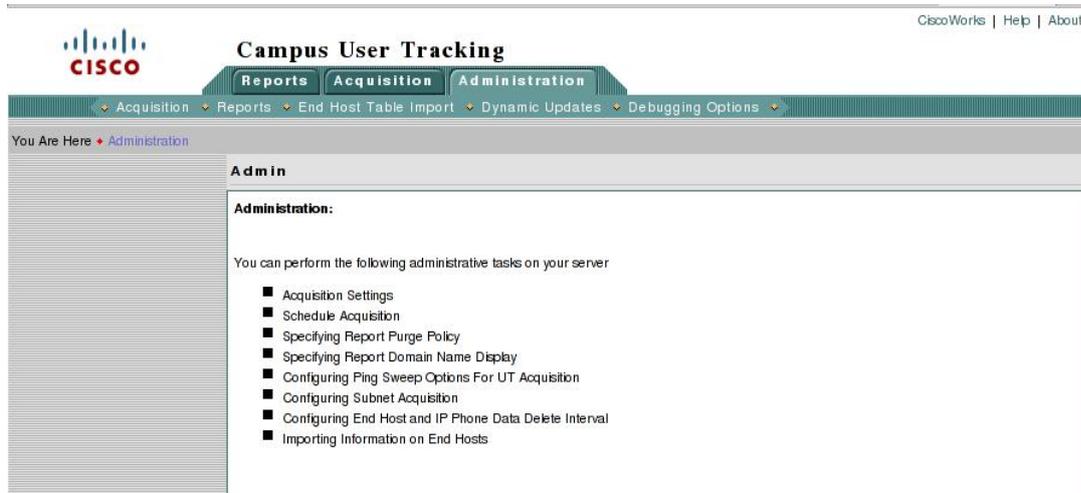


Die Bedienung von UT selbst erfolgt in einem gesonderten Bereich des 'Campus Manager' und eine Anleitung dazu würde ein eigenes Kapitel füllen. Im nachstehenden Screenshot sieht man den für die Seite 'User Tracking' zuständigen Reiter. Außerdem hat man hier auf der Anfangsseite vom 'Campus Manager' die Möglichkeit eine sog. UT-Acquisition (Informationssammlung) mit den aktuellen Einstellungen anzustoßen.



Von der UT-Seite aus kann UT mit verschiedenen Einstellungen konfiguriert werden, Acquisitions über bestimmte Gerätegruppen lassen sich anstoßen und Berichte können generiert werden:





User Tracking mit SNMPv3

Wenn man das oben Beschriebene mit SNMPv3 machen will, muss man in erster Linie den Geräten ein Plus an Aufmerksamkeit widmen. CiscoWorks und User Tracking brauchen keine besondere Konfiguration, davon einmal abgesehen, dass man als SNMP-Zugangsdaten nicht die Community-Strings eingibt, sondern einen Benutzernamen und ein Kennwort. Die Abfragen werden von UT automatisch angepasst. Um die Switchkonfiguration manuell zu testen, braucht man allerdings schon andere snmpwalk-Befehle als mit SNMPv2c. Aber das Testen lohnt sich, denn wenn die manuelle Abfrage zum Erfolg führt, hat man gute Chancen, dass auch UT funktioniert. Zunächst sollen einige für die Konfiguration relevante Dinge angesprochen werden.

Mit SNMPv3 wurde, wie bereits erwähnt, ein neues Sicherheitsmodell eingeführt. Dieses Modell bietet drei Sicherheitsstufen:

- Authentifizierung lediglich durch einen Benutzernamen – vergleichbar der Lösung mit dem Community-String (noAuthNoPriv).
- Hash-Authentifizierung mit den Algorithmen MD5 oder SHA (authNoPriv)
- Hash-Authentifizierung und DES-Verschlüsselung der übertragenen Daten (authPriv)

Ferner darf nicht jeder – zumindest bei der Cisco-Implementierung von SNMPv3 –, der SNMP-Zugriff auf ein Gerät hat, von vornherein alles, sondern man kann das Wirkungsfeld eines authentifizierten Benutzers mit sog. Views einschränken. Dazu werden auf den Geräten Gruppen erstellt, die Gruppen bekommen Rechte an bestimmten Views und die Benutzer werden der passenden Gruppe bei dem Anlegen zugewiesen. Zuletzt darf nicht vergessen werden, dass einzelne Instanzen von MIBs bei einer Abfrage nach wie vor gesondert adressiert werden müssen. Da hier aber nicht mit 'community indexing' gearbeitet



werden kann, weil es ja keine Communities mehr in SNMPv3 gibt, stehen dafür sog. Kontexte zur Verfügung.

Wie müssen wir also unseren Switch sw1 umkonfigurieren? Zunächst löschen wir die beiden Community-Strings. An dieser Stelle soll eine Warnung an diejenigen ergehen, die denken, sie könnten sowohl SNMPv2c als auch SNMPv3 auf ihren Geräten und in CiscoWorks konfigurieren, "die Anwendung wird schon die Version auswählen und verwenden, mit der sie arbeiten kann": Wenn Zugangsdaten für beide Versionen in der Credentials-Datenbank von CiscoWorks enthalten sind, benutzt der Server nur die SNMPv3-Zugangsdaten.

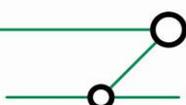
Noch ein Hinweis: Wenn das IOS-Image keine VLAN-basierten Kontexte unterstützt, können einzelne Instanzen einer MIB nicht abgefragt werden, somit kann auch UT nicht funktionieren. Ob und welche Kontexte vorhanden sind, lässt sich mit dem Befehl 'sh snmp context' ermitteln. Ist der Befehl nicht verfügbar, fehlt auch die Unterstützung für die Kontexte. Die Möglichkeit dessen, dass UT SNMPv3-Abfragen erfolgreich durchführt, ist somit stark auf bestimmte Modelle und neuere IOS-Versionen eingeschränkt. Cisco nennt in den Release Notes zum Campus Manager 5.0 die IOS-Version 12.2(25)SEE und die Modelle Cisco Catalyst 2900XL, Cisco Catalyst 3500XL, Cisco Catalyst 3750, Cisco Catalyst 4000 und Cisco Catalyst 6000. Die Praxis bestätigt diese Information: 3750-er unterstützen Kontexte, 2950-er dagegen nicht. Das neueste Image für einen 2950-er hat derzeit auch die Version 12.1(22)EA10a. Alles in allem kann man wohl davon ausgehen, dass alle neueren Modelle mit einer höheren IOS-Version diese Voraussetzung erfüllen.

Die komplette SNMP-Konfiguration eines Gerätes sieht folgendermaßen aus:

```
fig)#snmp-server group snmpadmins v3 auth write v1default
fig)#snmp-server group snmpadmins v3 auth context vlan-1
fig)#snmp-server group snmpadmins v3 auth context vlan-10
fig)#snmp-server group snmpadmins v3 auth context vlan-20
fig)#snmp-server user snmpadmin01 snmpadmins v3 auth md5 cisco123
```

1. Der erste Befehl erstellt die Gruppe *snmpadmins*. Die Gruppe benutzt das Sicherheitsmodell von SNMPv3 mit der Sicherheitsstufe 'authNoPriv' (Hash-Authentifizierung, aber keine Verschlüsselung). Die Gruppe bekommt Schreibberechtigung auf die View *v1default*. Leseberechtigung auf dieselbe View ist im Befehl implizit enthalten.
2. Die Befehle 2-4 weisen der Gruppe *snmpadmins* die Views der Kontexte *vlan-1*, *vlan-10* und *vlan-20* zu.
3. Mit dem letzten Befehl wird der Benutzer *snmpadmin01* angelegt, in die Gruppe *snmpadmins* aufgenommen (erbt also deren Rechte), er benutzt das Sicherheitsmodell und die Sicherheitsstufe der Gruppe mit dem Hash-Algorithmus MD5 und muss sich mit dem Kennwort *cisco123* authentifizieren.

Mit dieser Konfiguration bekommt ein authentifizierter User faktisch alle Rechte auf dem Gerät, sie ist also gleichwertig mit der Konfiguration einer Lese- und einer Schreib-Community. Die hier verwendete Sicherheitsstufe spiegelt die Möglichkeiten, die CiscoWorks bietet, wieder: Man kann die Hash-Authentifizierung, jedoch keine Verschlüsselung verwenden. Alternativ zu MD5 steht allerdings auch SHA zur Verfügung. Achtung! Der Befehl, mit dem man den Benutzer angelegt hat, erscheint in der *running-*



`config` nicht. Dagegen kann man die Einstellungen mit den Befehlen `'sh snmp user'` und `'sh snmp group'` verifizieren:

```
sw1#sh snmp user

User name: snmpadmin01
Engine ID: 80000009030000137FDB5103
storage-type: nonvolatile          active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: snmpadmins
```

```
sw1#sh snmp group | beg snmpadmins
groupname: snmpadmins                security model:v3 auth
readview : vldefault                 writeview: vldefault
notifyview: <no notifyview specified>
row status: active
```

Die Ausgabe des zweiten Befehls, wie sie hier dargestellt wird, wiederholt sich sozusagen für jeden Kontext.

Mit dieser Konfiguration ausgerüstet, können wir unsere Tests mit `snmpwalk` machen.

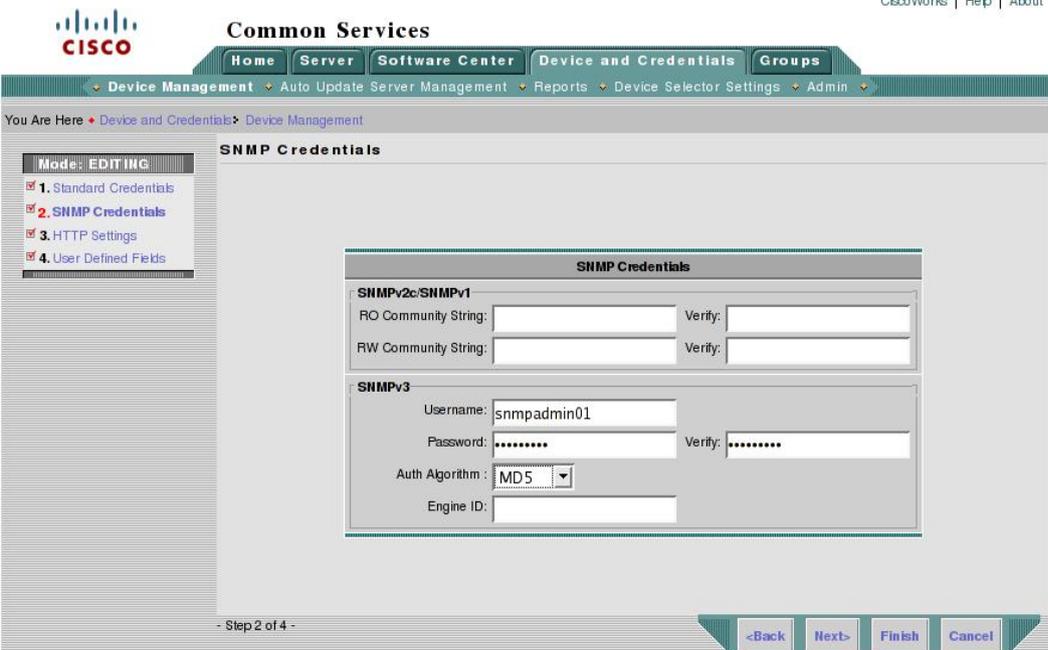
```
gipszjakab@pal:/home/gipszjakab> snmpwalk -v 3 -a MD5 -A 'cisco123' -l authNoPriv \
-u snmpadmin01 192.168.95.240 .1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.212.0 = Hex-STRING: 00 08 21 23 D4 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.212.24 = Hex-STRING: 00 08 21 23 D4 18
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.221.0 = Hex-STRING: 00 08 21 23 DD 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.221.23 = Hex-STRING: 00 08 21 23 DD 17
SNMPv2-SMI::mib-2.17.4.3.1.1.0.8.33.35.221.24 = Hex-STRING: 00 08 21 23 DD 18
SNMPv2-SMI::mib-2.17.4.3.1.1.0.9.232.151.10.194 = Hex-STRING: 00 09 E8 97 0A C2
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.12.4.116 = Hex-STRING: 00 0C 29 0C 04 74
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.84.239.27 = Hex-STRING: 00 0C 29 54 EF 1B
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.225.159.164 = Hex-STRING: 00 0C 29 E1 9F A4
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.226.105.229 = Hex-STRING: 00 0C 29 E2 69 E5
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.232.214.231 = Hex-STRING: 00 0C 29 E8 D6 E7
SNMPv2-SMI::mib-2.17.4.3.1.1.0.12.41.240.108.202 = Hex-STRING: 00 0C 29 F0 6C CA
SNMPv2-SMI::mib-2.17.4.3.1.1.0.20.242.155.247.150 = Hex-STRING: 00 14 F2 9B F7 96
SNMPv2-SMI::mib-2.17.4.3.1.1.0.20.242.155.247.196 = Hex-STRING: 00 14 F2 9B F7 C4
SNMPv2-SMI::mib-2.17.4.3.1.1.0.96.8.78.32.34 = Hex-STRING: 00 60 08 4E 20 22
```

Ohne Kontextangabe kommt auch hier erst einmal die Information über VLAN 1. Um die restlichen MAC-Adressen zu ermitteln, muss man `snmpwalk` den Kontextnamen mit dem Schalter `'-n'` übergeben:

```
gipszjakab@pal:/home/gipszjakab> snmpwalk -v 3 -a MD5 -A 'cisco123' -l authNoPriv \
-u snmpadmin01 -n vlan-10 192.168.95.240 .1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.208.89.193.40.68 = Hex-STRING: 00 D0 59 C1 28 44
gipszjakab@pal:/home/gipszjakab> snmpwalk -v 3 -a MD5 -A 'cisco123' -l authNoPriv \
-u snmpadmin01 -n vlan-20 192.168.95.240 .1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.1.2.19.80.74 = Hex-STRING: 00 01 02 13 50 4A
```



Wenn die Voraussetzungen auf diese Art und Weise geschaffen sind, können wir uns CiscoWorks zuwenden und die Zugangsdaten eintragen. Es wird an derselben Stelle gemacht wie bei der Konfiguration von SNMPv2c (**Common Services > Device and Credentials > Device Management > Edit Credentials > SNMP Credentials**), nur dass die Felder für v3 ausgefüllt werden:



Dasselbe gilt, wenn man die Zugangsdaten als 'Default Credentials' anlegen will. Hier noch einmal der Pfad zur einschlägigen Maske: **Common Services > Device and Credentials > Admin > Default Credentials**.

Zwei Dinge sollten noch erwähnt werden. (1) Das Tool utdebug, gedacht für die Fehlersuche bei UT-Problemen, konnte von uns bei einem funktionierenden UT nicht erfolgreich eingesetzt werden, wenn SNMPv3 im Spiel war. Utdebug scheint mit dieser SNMP-Version nicht kompatibel zu sein, was auch der von ihm ausgegebene Bericht unterstreicht: Dort wird der Benutzer aufgefordert, einen manuellen Check mit einem indizierten Community-String durchzuführen. (2) Damit UT auch Endgeräte erfasst, die sich hinter einem Trunkport befinden, muss die Acquisition dafür explizit konfiguriert sein. Das kann unter '**Campus Manager > User Tracking > Administration > Acquisition > Configure Trunk For End Hosts Discovery**' erledigt werden. Damit hat man eine Möglichkeit, die Einschränkung, die einem von den Geräten auferlegt wird, die SNMPv3 mit Kontexten nicht unterstützen, teilweise zu umgehen.

Fazit

Netzwerkmanagement ist durchaus praktikabel, auch wenn man auf die Sicherheit, die SNMPv3 bietet, nicht verzichten will, wenn man nur seine Geräte und seine Software auf dem neuesten Stand hält. Neuimplementierungen sollten den Vorteil von SNMPv3 auf jeden



Fall nutzen, aber auch ein Upgrade sollte dort problemlos verlaufen, wo es ein funktionierendes Konfigurationsmanagement gibt, z.B. mit CiscoWorks im Einsatz.

Literatur aus dem Cisco-Fundus

- Using SNMP to Find a Port Number from a MAC Address on a Catalyst Switch (www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801c9199.shtml)
- How To Get Dynamic CAM Entries (CAM Table) for Catalyst Switches Using SNMP (www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml)
- SNMP Community String Indexing (www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801576ff.shtml)
- SNMPv3 (IOS 12.0 T) - behandelt die Konfiguration von Kontexten nicht (www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a00800878fa.html)
- Catalyst 3750 Switch Software Configuration Guide, 12.2(37)SE - behandelt die Konfiguration von Kontexten nicht (www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_37_se/configuration/guide/scg.html)
- Release Notes for Campus Manager 5.0 on Windows (www.cisco.com/en/US/customer/products/sw/cscowork/ps563/prod_release_note09186a0080846c42.html)
- User Guide for Campus Manager 5.0 (www.cisco.com/en/US/products/sw/cscowork/ps563/products_user_guide_book09186a0080843fe3.html)

ERNW GmbH
Peter Fiers
Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 173 6745905
www.ernw.de
info@ernw.de

