Docusnap®

Inventarisierung und Analyse

Inventarisierung von SNMP Systemen

TITEL	Inventarisierung und Analyse
AUTOR	Docusnap Consulting
DATUM	10.10.2023
VERSION	3.1 | gültig ab 06.10.2023

INHALTSVERZEICHNIS

1. Einleitung

Aktive Netzwerkkomponenten wie z. B. Switche, Router und Drucker können mit Hilfe der SNMP-Inventarisierung mit Docusnap erfasst werden.

Die SNMP-Inventarisierung in Docusnap unterstützt die Versionen v1, v2c und v3. Dabei werden diverse vordefinierte Management Information Bases (MIB) abgefragt, wie z. B. die Printer-MIB oder die RFC1213-MIB.

Die gesammelten Daten können im Anschluss in Form von Berichten (Textform), oder Plänen (grafische Aufbereitungen wie z. B. Topologie und VLAN Pläne) dargestellt werden.

Für folgende Einsatzzwecke können Sie die SNMP Inventarisierung verwenden:

- Inventarisierung und Dokumentation der Netzwerkkomponenten
- Auswertung welche Systeme an welchem Switch, Port und VLAN zu finden sind

2. Voraussetzungen

2.1 Allgemeine Voraussetzungen

Um eine erfolgreiche SNMP-Inventarisierung eines Systems durchführen zu können, müssen folgende Voraussetzungen erfüllt sein.

- SNMP v1, v2c oder v3 muss aktiviert sein
  - Bei **v1 oder v2c** muss ein Read Community String verwendet werden
  - Bei **v3** müssen entsprechende Authentifizierungsdaten verwendet werden
- Die SNMP Systeme müssen vom Docusnap Server / Discovery Service System erreichbar sein (Firewall?)
- Eine vollständige Darstellung der Topologie setzt die folgenden Protokolle auf Switche, Router und Firewalls voraus:
  - Cisco Discovery Protocol (CDP)
  - Link Layer Discovery Protocol (LLDP)

Sollten trotz der oben beschriebenen Voraussetzungen nicht alle Systeme inventarisiert werden können, muss folgendes geprüft werden:

- Werden die Anfragen durch das Monitoring, Firewall oder andere Sicherheitslösungen blockiert?
  - Flooding Protection (ICMP, UDP)
  - Intrusion Protection
- IP-adressbasierte Access-Listen überprüfen
  - Welche IP Adressen dürfen per SNMP auf die Systeme zugreifen?
- Richtigkeit des Community Strings, bzw. der SNMPv3 Authentifizierungsdaten?
- Aktualität der Firmware der SNMP-Systeme?
- Bei fehlenden Topologie Informationen bzw. keine Verbindungen im Topologieplan die Aktivierung der Nachbarschaftsprotokolle über CLI oder Web prüfen (LLDP, CDP)
  - Z. B. show lldp neighbors / show lldp interface

Die Namen der inventarisierten SNMP-Systeme werden vom Systemnamen der Geräte abgeleitet, sofern dieser auf den Systemen gepflegt und vorhanden ist (OID: 1.3.6.1.2.1.1.5).

Alternativ kann in den Inventarisierungs-Optionen aktiviert werden, dass nicht der Systemname, sondern der DNS-Name verwendet wird.

Ist der Systemname nicht gepflegt, wird die IP-Adresse als Name verwendet. Aus diesem Grund empfiehlt es sich, die Systemnamen der SNMP-Systeme entsprechend zu pflegen, da die Darstellung mit der IP-Adresse oder auch den Standard SNMP Namen der Systeme unter Umständen nicht sehr aussagekräftig ist.

Wir empfehlen die Verwendung des Systemnamens anstatt des DNS-Namen.

2.2 Voraussetzungen CISCO SNMPv3

Bei Cisco Geräten bedarf es weiteren Voraussetzungen, wenn diese per SNMPv3 inventarisiert werden. Werden diese Voraussetzungen nicht durchgeführt, kann es dazu kommen, dass **gelernte MAC-Adressen** und **VLAN Zuordnungen** nicht, oder nur teilweise ausgelesen werden können. Dies wiederrum hat Auswirkungen auf die korrekte Darstellung des Topologie- und VLAN-Plans.

Auf den folgenden Seiten finden Sie entsprechende Informationen:

- https://community.cisco.com/t5/network-management/vlan-bridge-mib-and-snmpv3-contexts/td-p/1589698
- https://www.netnea.com/cms/2015/01/09/netdisco-with-snmp-v3-and-cisco/
- https://community.cisco.com/t5/network-management/bridge-mib-with-snmp-v3/td-p/1179194

Wir übernehmen keine Gewähr auf die Richtigkeit für die Inhalte auf den zuvor verlinkten Webseiten.

3. SNMP Inventarisierung

Docusnap unterstützt die SNMP Version v1, v2c und v3. Die Versionen v1 und v2c sind im SNMP-Inventarisierungsassistenten in einem Schritt zusammengefasst, v3 wird in einem weiteren Schritt konfiguriert.

Für die SNMP Inventarisierung starten Sie den entsprechenden Assistenten:

- Discovery – Alle Assistenten – SNMP
- Inventar – Alle Assistenten – SNMP
- Alle Aufträge – Alle Assistenten – SNMP

In **Schritt 1** wählen Sie Ihre Firma oder die Firma Ihres Kunden aus.

In **Schritt 2** wählen Sie den Discovery Service aus, über den Sie die Inventarisierung durchführen möchten.

Für eine zeitgesteuerte Inventarisierung wählen Sie hier den Docusnap Server Discovery oder einen von Ihnen konfigurierten Discovery Service.

Weiterhin wählen oder geben Sie eine / die Domäne an, unterhalb derer die zu inventarisierenden Systeme einsortiert werden sollen.

3.1 SNMP V1 / V2

In **Schritt 3** werden nun ALLE IP-Adressbereiche benötigt, die Sie im Einsatz haben.

Weiterhin hinterlegen Sie die lesende Community.

Befinden sich in dem IP-Bereich Geräte mit unterschiedlichen Community Strings, können Sie die Community Strings kommasepariert eintragen

Die IP-Adressbereiche können Sie auch in einer CSV-Datei vorbereiten und importieren. Der folgende Aufbau wird vorausgesetzt:

IP von	IP bis	Community	Timeout
192.168.0.1	192.168.255.255	public, MyCommunity	2500
10.0.0.1	10.0.0.255	public, MyCommunity	2500

Es ist nicht zu empfehlen, an den folgenden Einstellungen eine Änderung vorzunehmen:

- Gerätedaten für einzelne v1 und v2 Systeme inventarisieren (Aktiv)
- Topologie Informationen für v1 und v2 Systeme inventarisieren (Aktiv)
- Inventarisierung auf minimale Datenmenge reduzieren (Inaktiv)

Parallel ausgeführte Pings während der Inventarisierung

- Reduzieren Sie diesen Wert, wenn Sie feststellen, dass einzelne Systeme im Zuge der Inventarisierung nicht inventarisiert werden oder Ihre Monitor- / Sicherheitslösung anschlägt.

Systemerreichbarkeit per Ping prüfen

- Im ersten Schritt werden die SNMP Systeme angepingt – ist kein Ping möglich, findet keine Inventarisierung statt
- Ist aus Sicherheitsgründen der Ping deaktiviert, deaktivieren Sie auch diese Option

Weiterhin sollten die Timeout-Einstellungen beachtet werden, wenn Cisco Geräte im Einsatz sind. Sollten Sie hier nicht alle Systeme erreichen können, empfiehlt sich eine Erhöhung des Timeouts. Dies ist notwendig, da Cisco Geräte teilweise erst später auf Anfragen reagieren.

3.2 SNMP V3

In **Schritt 4** hinterlegen Sie die zu inventarisierenden SNMPv3 Systeme über den Button **+ Neu**

Sie können ein spezifisches System oder einen IP-Bereich hinterlegen.

Daraufhin müssen die entsprechenden SNMPv3 Anmeldedaten eingegeben werden.

Die Anmeldedaten können auch von einem bereits hinterlegten System übernommen werden.

Anmeldedaten für alle Systeme übernehmen

In diesem Fall werden die hinterlegten Anmeldedaten auf alle vorhandenen und zukünftig eingetragenen SNMPv3 Systeme angewendet

Bei einer Vielzahl von SNMPv3 Systemen / IP-Bereichen empfiehlt es sich diese per **Liste Laden** zu importieren. In dieser CSV Datei, kann nicht nur der Hostname bzw. die IP-Adresse übergeben werden, sondern auch die notwendigen Anmeldedaten. Die CSV Datei muss den folgenden Aufbau besitzen – **für den Import entfernen Sie die Zeile mit den Überschriften!**

Name / IP	Benutzer	Auth Alg.	Auth. Pwd.	Privacy Alg.	Privacy Pwd.	Kontextname	Timeout
192.168.100.1-192.168.100.100	Docusnap	SHA384	Password	AES256	Password	Kontext	2600
192.168.101.1-192.168.101.100							
192.168.100.101	Docusnap	SHA512	Password	AES128	Password	Kontext	2600
192.168.100.102	Docusnap	SHA256	Password	AES	Password	Kontext	2600

Wenn die Systeme / IP-Bereiche über die gleichen Anmeldedaten verfügen, reicht es aus, diese für das erste System zu hinterlegen.

Sollte die Sicherheitsstufe **Auth_NoPriv** ausgewählt sein, dann lassen Sie die Felder für **Privacy Algorithmus** und **Privacy Password** leer. Auch den Kontextnamen können Sie leer lassen, wenn keiner konfiguriert wurde.

Auch bei SNMPv3 ist es nicht zu empfehlen, an den folgenden Einstellungen eine Änderung vorzunehmen:

- Gerätedaten für einzelne v1 und v2 Systeme inventarisieren (Aktiv)
- Topologie Informationen für v1 und v2 Systeme inventarisieren (Aktiv)
- Inventarisierung auf minimale Datenmenge reduzieren (Inaktiv)

4. Analyse

4.1 SNMP Systeme

Die inventarisierten Daten der SNMP Systeme können wie gewohnt über die Baumstruktur betrachtet werden

- Ihre Firma – Infrastruktur – Ihre Domäne – SNMP-Systeme

Die inventarisierten SNMP Systeme werden nun nach deren Gerätetyp aufgelistet. Wie Sie diese Zuordnungen anpassen und erweitern können, wird in Kapitel SNMP Typen automatisch zuordnen / SNMP Typen manuell zuordnen beschrieben.

4.2 Topologieplan

Docusnap kann die Topologie von entsprechenden Netzwerkgeräten (Switche, Router etc.) inventarisieren. Dies bedeutet, dass die direkten Verbindungen von Netzwerkgeräten ausgelesen und im Topologie Plan angezeigt werden.

Darüber hinaus wird anhand der gelernten MAC-Adressen ein Portbelegungsplan von Switchen erstellt und im Topologie Plan angezeigt. Diese Informationen finden Sie im Detailplan eines Switches.

Der Detailplan eines Switches löst die gelernten MAC-Adressen des Switches auf, sofern das entsprechende Gerät inventarisiert wurde und damit in Docusnap bekannt ist. Ist das Gerät noch nicht bekannt, wird an dem Port nur eine MAC-Adresse und der Hersteller angezeigt - dies wird über den Hersteller Teil der MAC-Adresse durchgeführt. Auch IT-Assets und manuell erstellte Systeme, die Sie mit Netzwerkinformationen (speziell die MAC-Adresse) dokumentiert haben, werden im Topologie Plan dargestellt.

Dabei ist es wichtig zu beachten, dass der Topologieplan nur die Daten der letzten Inventarisierung heranzieht. Weiterhin sind die gelernten MAC-Adressen der Switche flüchtig. Dies bedeutet, dass Ports gelernte MAC-Adressen wieder vergessen, wenn die angeschlossenen Systeme längere Zeit inaktiv sind. Von daher sollte die Inventarisierung von SNMP-Systemen, speziell der Switche, zu „Stoßzeiten" erfolgen.

Folgend finden Sie eine Auflistung, welche Systeme etc. im Topologie Plan aufgelistet werden

- SNMP-Geräte vom Typ Switch
- SNMP-Geräte mit Topologie Informationen (CDP, LLDP) – z. B. Access Points
- IP-Systeme und MAC-Adressen, die über LLDP und CDP-Informationen von Switchen erkannt werden
- Generell Geräte welche redundant auf mehr als einem Switch gesteckt sind
- Router

Der Topologieplan kann Ad-Hoc, über die Baumstruktur erstellt und exportiert werden. Zusätzlich kann der Plan auch automatisiert und zeitgesteuert exportiert werden (PNG, HTML, VDX, SVG).

Über die Baumstruktur finden Sie den Topologieplan an folgenden Stellen und in folgenden Ausführungen:

Ihre Firma – Infrastruktur – Standardpläne – Topologieplan

- Firmenweit werden Geräte für den Topologie Plan herangezogen – Domänenübergreifend.

Ihre Firma – Infrastruktur – Ihre Domäne – Standardpläne – Topologieplan

- Nur die Geräte der Domäne werden herangezogen.

Ihre Firma – Assets – Systemgruppen – Ihre Domäne – Systemgruppe – Standardpläne – Topologieplan

- Nur die Geräte der ausgewählten Systemgruppe werden herangezogen

Ihre Firma – Standorte – Standort – Dokumentation – Topologieplan

- Nur die Geräte des ausgewählten und der untergeordneten Standorte werden herangezogen.

Ihre Firma – Infrastruktur – Ihre Domäne – Systeme (Server, Linux,…) – Dokumentation – Topologieplan

- Es wird, in einer einfachen grafischen Darstellung, dargelegt, an welchem Switch sowie Port das angewählte System angesteckt ist

Ihre Firma – Infrastruktur – Ihre Domäne – SNMP Systeme – Switch – Dokumentation – Topologieplan

- Es wird der Detailplan dieses Switches ausgegeben

Ihre Firma – Infrastruktur – Ihre Domäne – System (Windows, Linux, Mac etc.) – Dokumentation – Topologieplan

- Topologie des Systems – Switche, an denen das System anegschlossen ist

4.2.1 Topologieplan - Optionen

Nachdem Sie den Topologie Plan geöffnet haben, steht im Aktionsmenü ein eigener Bereich mit Optionen zur Verfügung. Beispielsweise können Sie den Plan exportieren. Weiterhin haben Sie die folgenden Optionen zur Verfügung, die eine direkte Auswirkung auf den Plan besitzen.

In den Optionen von Docusnap können Sie für die folgenden Einstellungen auch Voreinstellungen treffen:

- Optionen (Titelleiste – Zahnrad) – Dokumentation – Pläne – Einstellungen Topologiepläne und VLAN Visualisierung

Spezial

Potenzielle Access Points anzeigen

- Zeigt potenzielle Access Points im Übersichtsplan an. Potenzielle Access Points werden anhand von CDP- bzw. LLDP-Einträgen der Switche erkannt, die aber nicht in der Docusnap Datenbank vorhanden sind.

Layer3 Elemente anzeigen

- Layer 3 Systeme z. B. Router werden im Übersichtsplan eingeblendet.

Tunnelverbindungen anzeigen

- Ist via LLDP oder CDP eine Tunnelverbindung bekannt, wird die Verbindung durch diese Option angezeigt.

VLAN

VLAN-Tabellen anzeigen

- Durch diese Option werden für Switche die jeweiligen VLANS als Tabelle angezeigt.
- VLAN-Tabellen mit gleichem Inhalt werden gleich eingefärbt.

Ports mit VLAN-Informationen anzeigen

- Durch diese Option werden bei den Detailplänen für die Switche die **tagged** und **untagged** Informationen bei den Ports angezeigt.

Filtern auf relevante VLANs

- Nur relevante VLANs werden angezeigt. VLANs die auf Switchen aktiv sind, dieses jedoch auf keinem Port anliegt, werden ignoriert.

Details

Details anzeigen

- Switch Details, Kabelbandbreite und Portbezeichnung können eingeblendet werden.

Virtuell

Virtuelle Strukturen ausblenden

- Blendet die virtuellen Switche im Übersichtsplan aus.

Virtuelle Switche

- Detailpläne der virtuellen Switche werden nicht erstellt.

Visualisierung

Kabelbandbreite visualisieren

- Durch diese Option werden die Linien einer Verbindung, je nach Geschwindigkeit, unterschiedlich eingefärbt.
- Bei höherer Geschwindigkeit wird eine dickere Linie verwendet.
- Übersteigt die Geschwindigkeit 10 Gbit/s wird die Linie blau dargestellt.
- Unterschreitet die Geschwindigkeit 1 Gbit/s wird sie rot dargestellt.
- In den anderen Fällen wird die Linie in grüner Farbe gezeichnet.

Fehlende Daten hervorheben

- Durch diese Option werden Switche markiert, bei denen keine LLDP oder CDP Informationen verfügbar sind.
- Weiterhin werden Geräte markiert, wenn keine gelernten MAC-Adressen verfügbar sind oder die Interface Stackdaten fehlen.
- Durch Rechtsklick auf das hervorgehobene Objekt - **Daten anzeigen**, wird in einem zusätzlichen Dialog die Fehlermeldung ausgegeben.

4.3 VLAN Plan

In erster Ausprägung werden Sie feststellen, dass der VLAN-Plan die gleichen Informationen ausgibt, die Sie auch innerhalb des Topologie Plans mit der Option **VLAN Tabellen** erhalten.

Im Übersichtsplan werden die Verbindungen der Switche untereinander mit den zum Switch gehörenden VLAN Tabellen angezeigt.

Darüber hinaus können Sie auch einen VLAN-Detailplan erstellen. Bei diesem Detailplan wählen Sie ein VLAN aus. Daraufhin erhalten Sie alle Switche des VLANs. Auch die auf den Switchen und im ausgewählten VLAN gesteckten Systeme werden angezeigt.

4.4 Berichte

Neben dem Topologie- und VLAN-Plan gibt es auch Berichte, mit denen Sie diese Informationen der SNMP Systeme analysieren können. Diese Berichte sind wie folgt zu finden:

- Ihre Firma – Infrastruktur – Ihre Domäne – Berichte – Infrastruktur Netz

Netzwerkgeräte

- Der Bericht listet alle SNMP Systeme, mit den im Standard inventarisierten Informationen auf – u. a.
  - Allgemeine Informationen, Netzwerkinformationen, Schnittstellen

Drucker

- Alle Drucker mit den druckerspezifischen Informationen
  - Druckerinformationen, Toner

Switches

- Dieser Bericht gibt Ihnen Detailinformationen bezüglich der Switche aus – u. a.
  - VLAN-Informationen und deren Portzuordnung
  - Auflistung der Ports und der dort gesteckten Systeme

VLAN

- Bei der Erstellung des Berichts können Sie zunächst ein oder mehrere VLANs auswählen
- Daraufhin bekommen Sie, gruppiert nach den ausgewählten VLANs, alle zugehörigen Systeme aufgelistet

VLAN Übersicht Switch

- Auch hier wählen Sie zunächst ein oder mehrere VLANs aus
- Daraufhin wird erneut nach den ausgewählten VLANs gruppiert
- Zusätzlich wird nun auch nach Switchen gruppiert, auf denen die zugehörigen Systeme gesteckt sind – mit Angabe des Systemtyps, MAC- und IP-Adresse und Port

4.5 Topologie Liste

- Ihre Firma – Infrastruktur – Ihre Domäne – Zusammenfassung – Topologie

Diese Ansicht gibt Ihnen Informationen bezüglich der verwendeten Switch-Ports aus. Es kann beispielsweise nach einer MAC-Adresse oder Systemname gefiltert werden, um so schnell herauszufinden, an welchem Switch-Port das Gerät angeschlossen ist.

Wird ein Port aufgelistet, der nur eine Mac Adresse nicht aber ein verbundenes System anzeigt, dass ist das System mit dieser Mac Adresse noch nicht in Docusnap inventarisiert. Mit dem **Filterausdruck \NULL** in der Spalte **Verbundenes System**, könne Sie so nach allen noch unbekannten Systemen filtern.

Auch IT-Assets und manuell erstellte Systeme, die Sie mit Netzwerkinformationen (speziell die MAC-Adresse) dokumentiert haben, werden aufgelistet.

4.6 VLAN Übersicht

- Ihre Firma – Infrastruktur – VLAN Übersicht – VLAN Gesamtübersicht

In dieser Ansicht können die verwendeten VLANs und die darin befindlichen Systeme aufgelistet werden

5. Anpassungen

5.1 Switch bearbeiten – manuelle Verbindungen konfigurieren

Es wurde zuvor beschrieben, dass die Daten aus dem Switch Detailplan durch das Auslesen der gelernten MAC-Adressen bereitgestellt werden, und dass diese wiederrum flüchtig sind. Für eine vollständige Dokumentation können Sie dem Switch-Port auch manuell eine MAC-Adresse zuweisen und dauerhaft dokumentieren. Diese manuell durchgeführten Anpassungen bleiben auch nach einer neuen Inventarisierung bestehen!

Die manuelle Zuweisung findet in der Docusnap Administration statt:

- Administration – Inventar – SNMP – Switch bearbeiten
- Wählen Sie die Firma, die Domäne und anschließend den Switch aus
- Wählen Sie nun den anzupassenden Port aus und fügen die MAC-Adresse hinzu

5.2 Mac Filter

Es kommt vor, dass manche Systeme nicht korrekt / vollständig inventarisiert werden können. Im Zuge dessen sind im Topologie Detailplan nur die MAC-Adressen zu finden. Ein Beispiel hierfür sind IP-Telefone.

Mit Hilfe des Mac Filters können Sie nun einen für die Geräte übereinstimmenden Teil der Mac Adresse hinterlegen und auswählen, ob diese nun als Gerät, als Telefon oder nicht im Topologieplan gezeigt werden sollen. Die Mac Adressen können Sie in der Docusnap Administration hinterlegen.

- Administration – Inventar – SNMP – Mac Filter

Tragen Sie einen entsprechenden MAC Filter ein – * kann als Platzhalter verwenden werden.

6. SNMP Geräte typisieren

Die SNMP Systeme werden in der Baumstruktur nach Ihrem Typ gruppiert angezeigt. Hierbei kann es vorkommen, dass keine Zuordnung stattgefunden hat (Typ Allgemein) oder, dass Sie eine vorhandene Zuordnung anpassen möchten.

Die Zuordnung der Geräte zu Ihrem Typ erhöht die Qualität der in Docusnap befindlichen Daten. Sie können auf diesem Weg viel schneller herausfinden, wie viele Drucker, Switche, Router, USV, Webcams etc. im Einsatz sind. Auch in den verfügbaren Plänen werden die SNMP Systeme mit aussagekräftigen Icons dargestellt.

Die Zuordnung kann automatisch, anhand Suchwörter stattfinden, oder manuell.

Die vordefinierten SNMP Typen können um eigene Typen erweitert werden.

6.1 SNMP Typen automatisch zuordnen

Die automatische Zuordnung findet anhand von definierten Suchwörtern innerhalb der Geräte-Beschreibung eines SNMP Systems statt. Das Beschreibungsfeld finden Sie wie folgt:

- Ihre Firma – Infrastruktur – Ihre Domäne – SNMP Systeme – SNMP Systemtyp
  - SNMP System – Inventarisierungsdatum – Allgemein – Beschreibung

Wenn Sie nun ein nicht zugeordnetes System zuordnen möchten, suchen Sie aus dem Beschreibungsfeld ein oder mehrere zusammenhängende Wörter – z. B.

Beschreibungstext	Suchwort
HPE StoreOnce 2700 Backup	%Backup%
HP ETHERNET MULTI-ENVIRONMENT,ROM none,JETDIRECT,JD149	%JETDIRECT%
HP Onboard Administrator	HP Onboard Administrator
Integrated Lights-Out 4 2.62 Jan 09 2019	%Integrated Lights-Out%
HP P2000 G3 FC	%P2000%
HPE_3PAR 7200, ID: 53216, Serial number....	%3PAR%
HP J4813A ProCurve Switch 2524, revision F.05.80, ROM F.02.01	%J4813A% oder %ProCurve% oder %Switch%

Die neuen Suchwörter hinterlegen Sie in der Docusnap Administration

- Administration – Inventar – SNMP – SNMP Typen
  - Neu
    Tragen Sie das Suchwort ein und wählen Sie den passenden Typ
    %.....% dient hierbei als Platzhalter

6.2 SNMP Typen manuell zuordnen

Die manuelle Zuordnung kann notwendig sein, wenn ein SNMP-System keine Beschreibung liefert, oder diese nicht für eine eindeutige Zuordnung genutzt werden kann.

Eine manuelle Zuordnung wird nicht durch die Verwendung von Suchwörtern überschrieben!

Die manuelle Zuordnung kann im Datenbereich oder im Kontextmenü durchgeführt werden.

Datenbereich

Im Datenbereich können mehrere Geräte mit Hilfe der Checkboxen einem SNMP Typ zugewiesen werden. Nach der Auswahl der Geräte können Sie diese einem **SNMP Typ zuweisen**. Sie können auch die **Manuelle Zuweisung entfernen.**

Die Spalte **Fixer SNMP Typ** gibt Auskunft darüber, ob dieses Gerät über einen Automatismus, oder per manueller Zuweisung dem SNMP Typ zugeordnet wurde.

Kontextmenu

Aus dem Kontextmenu (Rechtsklick in der Baumstruktur auf das System) heraus kann ein spezifisches System manuell einem SNMP Typ zugeordnet werden.

6.3 Eigene SNMP Typen definieren

Sie haben auch die Möglichkeit, eigene SNMP Typen zu erstellen - falls die vordefinierten SNMP Typen nicht ausreichen.

Eigene SNMP Typen werden in der Administration erstellt und verwaltet:

- Administration - Inventar - SNMP - SNMP Basis Typen
- Neu
  - *Name*
  - *Wert* – Empfehlung: beginnend ab 1000
  - *Text Deutsch*
  - *Text Englisch*

Diesen eigenen SNMP Typen können Sie auch passende Icons hinterlegen.

- Administration – Customizing – Icons – Icons
- Neu
  - *Gruppe* – SNMP
  - *Wert* – Wert des zuvor erstellten SNMP Typen
    Kann auch über *Referenzwert* ausgewählt werden
  - Standard Icon – 16x16, png Format
  - Vorschau Icon – 100x100, png Format

Das Docusnap Icon Pack finden Sie zum Download in unserer Community, im Bereich Benefits, **Customizing - Docusnap Icon Pack**

7. Herstellerspezifische MIBs

Die SNMP Inventarisierung kann durch die Einbindung von herstellerspezifischen MIBs erweitert werden. Dadurch werden zusätzliche OIDs bei der Inventarisierung ausgelesen. Es ist zu beachten, dass diese zusätzlichen Informationen entsprechend aufbereitet (SQL-View, Bericht) werden müssen, da diese im Standard nur im SNMP Explorer ersichtlich sind und ansonsten keine weitere Verarbeitung erfolgt.

Herstellerspezifische MIBs können dafür sorgen, dass weitaus mehr Informationen inventarisiert werden. Aus diesem Grund kann das Einbinden die Inventarisierungsdauer um ein vielfaches verlängern.

Es wird nicht empfohlen, herstellerspezifische MIBs „einfach so" zu importieren, der richtige Ansatz ist:

- Verschaffen Sie sich eine Übersicht darüber, welche Informationen mit den herstellerspezifischen MIBs von Nutzen sind
    - Am besten über Herstellerinformationen der SNMP Geräte
- Unterhalb welcher OIDs sind diese Informationen zu finden
- Importierten Sie die MIB
    - Ordnen Sie die MIB dem SNMP System Typ zu
    - Aktivieren Sie nur die relevanten OIDs

7.1 Herstellerspezifische MIB einbinden

Herstellerspezifische MIBs werden in der Administration von Docusnap importiert:

- Administration – Inventar – SNMP – SNMP MIBs – Import

WICHTIG!
MIBs weisen Abhängigkeiten zu anderen MIBs auf. Wenn Sie eine MIB importieren, kann es zu einer Fehlermeldung kommen, wenn die Abhängigkeit nicht aufgelöst werden konnte.

In diesem Fall sammeln Sie die in der Meldung angegebenen MIBs in einem Ordner und führen den Import daraufhin nochmals durch.

Nach dem erfolgreichen Import wählen Sie im nächsten Schritt den dazugehörigen **SNMP System Typ** aus. Dies gibt an, dass die MIB beispielsweise auf USV oder Firewalls ausgeführt werden soll.

Im nächsten Schritt können Sie die zu inventarisierenden Informationen im Bereich **MIBs durchsuchen** anpassen. Beispielsweise wird es immer empfohlen, TRAPS abzuwählen. Da die Abfrage dieser bei einigen Systemen zu Problemen führen kann.

7.2 Daten auswerten

Die zusätzlichen Informationen, die durch den MIB Import ausgelesen werden, sind zunächst im SNMP Explorer zu finden.

- Ihre Firma – Infrastruktur – Ihre Domäne – SNMP Systeme – SNMP Systemtyp
  - SNMP System – Inventarisierungsdatum – SNMP Explorer – SNMPv2-SMI
    - org – dod – internet – private – enterprises

Im Anschluss folgt die Struktur der importierten MIB. Z. B. bei der Sophos MIB

- sophos – xg-firewall – sfosSystem – sysInstall – applianceModel
  OID: 1.3.6.1.4.1.21067.2.1.1.2.0

Diese Informationen können auch in einer View, bzw. in einem neuen Knoten in der Baumstruktur aufgelistet werden.

Im ersten Schritt werden dafür werden die entsprechenden OIDs benötigt – z. B. folgende, aus der Sophos MIB

- 1.3.6.1.4.1.21067.2.1.1.1.0 - ApplianceKey
- 1.3.6.1.4.1.21067.2.1.1.2.0 - ApplianceModel
- 1.3.6.1.4.1.21067.2.1.1.3.0 – xg-firewallVersion – wird als Firmware bezeichnet

Im zweiten Schritt wird eine neue View in der Docusnap Administration angelegt:

- Administration – Customizing – Tabellen verwalten
- +Neu
  - *Tabellentyp* – Sicht
  - *Tabellenname – xv* – SophosMib – SophosMibView
    - xv ist von Docusnap vordefiniert
    - *SophosMib* ist der Name des Namespaces für das Customizing
    - *SophosMibView* ist der eigentliche Name der View
      Die View heißt daraufhin *xvSophosMIBSophosMibView*
  - *Name Deutsch*
  - *Name Englisch*
  - *SQL Statement (ohne Zeilenumbruch)* [1]
    SNMP-Single:(1.3.6.1.4.1.21067.2.1.1.1.0,ApplianceKey;1.3.6.1.4.1.21067.2.1.1.2.0,ApplianceModel;1.3.6.1.4.1.21067.2.1.1.3.0,Firmware)

[1] Um Werte auszugeben, die für jedes SNMP-Gerät nur einmal vorkommen, z. B. die Seriennummer, wird das Statement mit *SNMP-Single* begonnen.
Wird eine Tabelle ausgegeben, dann wird das Statement mit *SNMP* begonnen. Beispielsweise die IP-Adressen eines Systems.

Im nächsten Schritt werden die Felder der View angelegt – **Felder bearbeiten**:

Feldname	Datentyp	Name Deutsch	Name Englisch
ApplianceKey	String	Appliance Key	Appliance Key
ApplianceModel	String	Appliance Modell	Appliance Model
Firmware	String	Firmware	Firmware
ValueID	BigInt	ValueID	ValueID

Die ValueID dient als Primärschlüssel. Bei diesem Feld können Sie die Option **Feld in Listen anzeigen** deaktivieren.

Wählen Sie nun noch den Primärschlüssel und das Anzeigefeld.

Nun wird die neue Sicht in den Datenbaum integriert.

- Administration – Customizing – Objekte verwalten

Wählen Sie in der Objekthierarchie:

- Account – NetworkEnvironment – Domain – SNMP Systems
  - SNMPTypes_Data - SNMP_Data - SNMPDocu_Data

Erstellen Sie zwei neue Objekte - **+Neu**

Objektname	Kategorie	Namespace	Text Deutsch	Text Englisch	Standard Icon	Vorschau Icon
SophosMibView	Überschrift	SophosMIB	SophosMibView	SophosMibView	16x16, png	100x100, png

Objektname	Kategorie	Tabelle	Text Deutsch	Text Englisch	Icons
SophosMibView_Data	Daten	xvSophosMIBSophosMibView	SophosMibView_Data	SophosMibView_Data	Siehe oben

Nun werden die Daten in der Baumstruktur angezeigt.

Weitere Informationen zur Erstellung und Einbindung von Views finden Sie im HowTo: Customizing – Datensicht (View) erstellen in der Knowldge Base.

8. SNMP Troubleshooting

Oft treten bei der SNMP-Inventarisierung dieselben Fehler auf. Um Ihnen außerhalb des klassischen Supports eine Möglichkeit zur schnellen Analyse und Problembehebung zu bieten, stehen Ihnen zwei Checklisten zur SNMP Inventarisierung zur Verfügung. Der Docusnap Support prüft bei einem SNMP Problem zuerst dieselben Punkte.

Die erste Prüfliste behandelt die Problemlösung bei der SNMP Inventarisierung an sich. In der zweiten Checkliste wird das Troubleshooting bei fehlenden Topologie Informationen behandelt.

In den Prüflisten wird von SNMP-Agenten und SNMP-Manager gesprochen. Diese beiden Begriffe beschreiben im Wesentlichen die Funktion des jeweiligen Systems.

SNMP-Manager

Abfragendes System. z.B. Docusnap Server oder Docusnap Client.

SNMP-Agent

Das abgefragte (zu inventarisierende) System. Z.B. Drucker, Switch, Router oder andere SNMP fähige Netzwerkgeräte.

8.1 Checkliste – SNMP Inventarisierung nicht möglich

1. ☐ Unterstützt das Zielsystem SNMP
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: Es ist keine SNMP Inventarisierung möglich, das Gerät muss manuell erfasst werden
2. ☐ Ist das SNMP Protokoll auf dem Agenten aktiviert?
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: SNMP aktivieren
3. ☐ Ist eine Kommunikation via Ping zwischen SNMP Agent und Manger möglich?
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: Netzwerkverbindung prüfen oder beim SNMPv1/v2c-Scan die Systemerreichbarkeit nicht überprüfen lassen
4. ☐ Verläuft die Kommunikation zwischen SNMP Agent und Manger über ein zusätzliches Netzwerkgerät, z.B. über eine Firewall?
    a. ☐ Nein: Weiter mit nächstem Schritt
    b. ☐ Ja: Log der Firewall prüfen, gegebenenfalls blockiert diese die Verbindung
5. ☐ Welche SNMP Version wird unterstützt?
    a. ☐ SNMP v1/ v2
        i. ☐ Wird der richtige Community String verwendet?
            1. ☐ Ja: Weiter mit nächstem Schritt
            2. ☐ Nein: Community String anpassen
    b. ☐ SNMP v3
        i. ☐ Authentifizierungsdaten richtig?
            1. ☐ Ja: Weiter mit nächstem Schritt
            2. ☐ Nein: Authentifizierungsdaten anpassen
6. ☐ Prüfen ob sich ein Backslash oder ein @ im Community String / Username / Passwort befindet
    a. ☐ Nein: Weiter mit nächstem Schritt
    b. ☐ Ja: Passwort ändern. Viele Systeme haben ein Problem mit Sonderzeichen
7. ☐ Ist der SNMP Manger (Abfragendes System, Docusnap Client bzw. Server) für SNMP Abfragen berechtigt?
    a. ☐ Nein: SNMP Manager auf SNMP Agent für SNMP Polling berechtigen.
    b. ☐ Ja
        i. ☐ Frägt der richtige SNMP Manager das richtige System ab?
            1. ☐ Ja: Weiter mit nächstem Schritt
            2. ☐ Nein: Richtigen SNMP Manager auswählen
8. ☐ Muss der konfigurierte Zugang eventuell noch auf den OID Baum berechtigt werden?
    a. ☐ Nein: Weiter mit nächstem Schritt
    b. ☐ Ja: Berechtigungen auf Community bzw. Gruppe zuteilen
9. ☐ Wird Abfrage ggf. durch (Monitoring) Firewall oder Sicherheitslösungen geblockt (Flooding Protection, Intrusion Protection)
    a. ☐ Nein: Weiter mit nächstem Schritt
    b. ☐ Ja: Entsprechende Ausnahmen konfigurieren
10. ☐ Prüfen ob Docusnap eine Inventarisierung durchführen kann.
    a. ☐ Ja: Prüfliste erfolgreich abgeschlossen
    b. ☐ Nein: Prüfen ob SNMP Agent Teil des konfigurierten IP-Segments ist
        i. ☐ Ja: weiter mit nächstem Schritt
        ii. ☐ Nein: IP-Segment ergänzen

11. ☐ Prüfen ob 3rd Party Tools, wie der Paessler SNMP Tester, die Daten lesen können (Uptime, Description,…)
    a. ☐ Nein: Weiter mit nächstem Schritt
    b. ☐ Ja: Kontaktaufnahme Docusnap Support
12. ☐ Ist die Firmware des SNMP Agenten auf dem aktuellen Stand?
    a. ☐ Ja: weiter mit nächstem Schritt
    b. ☐ Nein: Update auf aktuelle Version prüfen (keine Gewährleistung seitens Docusnap Support)
13. ☐ Kontaktaufnahme Docusnap Support

8.2 Checkliste – Fehlende Topologieinformationen

LLDP

Link Layer Discovery Protokoll

CDP

Cisco Discovery Protokoll

1. ☐ Unterstützt das SNMP System Nachbarschaftsprotokolle (CDP, LLDP)
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: Topologie nur über manuelle Konfiguration möglich
2. ☐ Ist LLDP bzw. CDP aktiviert
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: LLDP oder CDP aktivieren
3. ☐ Wird ein einheitliches Nachbarschaftsprotokoll verwendet?
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: Einheitliches Nachbarschaftsprotokoll konfigurieren (bevorzugt: LLDP)
4. ☐ Muss der konfigurierte Zugang noch auf den OID Baum berechtigt werden?
    a. ☐ Nein: Weiter mit nächstem Schritt
    b. ☐ Ja: Berechtigungen auf Community bzw. Gruppe zuteilen
5. ☐ Ist die Firmware auf aktuellem Stand
    a. ☐ Ja: Weiter mit nächstem Schritt
    b. ☐ Nein: Update auf aktuelle Version prüfen (keine Gewährleistung seitens Docusnap Support)
6. ☐ Kontaktaufnahme Docusnap Support

VERSIONSHISTORIE

Datum	Beschreibung
16.04.2019	Dokument erstellt
27.09.2019	Beschreibung Topologie Plan und VLAN Plan angepasst und erweitert
19.12.2019	Checkliste für SNMP Troubleshooting und SNMP Inventarisierung mit Docusnap hinzugefügt
06.05.2020	Version 2.0 – Überarbeitung des HowTos für Docusnap 11
03.06.2022	Kapitel 5.2 eingefügt - Eigene SNMP Typen definieren
04.01.2023	Version 3.0 – Überarbeitung des HowTos für Docusnap 12
06.10.2023	Version 3.1 – Kommaseparierte Eingabe von Community Strings / SNMPv3 IP-Bereiche verwenden