IP-Scan

Inventarisierung von IP-Systemen

TITEL	IP-Scan
AUTOR	Docusnap Consulting
DATUM	19.09.2025
VERSION	4.2 | gültig ab 15.05.2025

INHALTSVERZEICHNIS

1. Einleitung

Der IP-Scan in Docusnap liefert Ihnen die Möglichkeit, Ihr Netzwerk oder das eines Kunden umfangreich nach aktiven Systemen zu durchsuchen. Alles, was Sie für diesen ersten Überblick, oder der Überprüfung auf eine vollständige Inventarisierung benötigen, sind die relevanten IP-Adressbereiche. Für den IP-Scan werden keinerlei Anmeldeinformationen oder Community Strings verwendet. Auf diesem Weg können Sie ein neues Netzwerk sehr schnell und einfach inventarisieren und sich dabei einen Überblick verschaffen.

In Ihrem eigenen Netzwerk können Sie auf diesem Weg jene aktiven Komponenten erfassen, die Sie mit einem detaillierteren Scan noch nicht erfasst haben. Gründe hierfür können u.a. sein, dass das System nicht bekannt ist oder die nötigen Anmeldeinformationen fehlen.

Docusnap unterscheidet zwischen einem normalen und dem erweiterten IP-Scan. Beide IP-Scans funktionieren auf Basis von **NMAP (Network Mapper)**. Der normale IP-Scan verwendet Funktionen wie SYN-ACK, ARP-Request, ICMP Anfragen und eine Namensauflösung. Antwortende Systeme werden mit rudimentären Netzwerkinformationen erfasst.

Durch die Verwendung spezieller NMAP-Parameter ist es dem erweiterten IP-Scan möglich zusätzliche Informationen, wie z. B. das Betriebssystem, zu erkennen.

Voraussetzung für den erweiterten IP-Scan ist die Installation des **NPCAP Treibers** auf dem inventarisierenden System.

2. Voraussetzungen

Ein erfolgreicher IP-Scan setzt im ersten Schritt nur die Bekanntheit der zu inventarisierenden IP-Adressbereiche voraus.

Wie bereits angesprochen, wird zwischen dem einfachen und dem erweiterten IP-Scan unterschieden. Für den erweiterten IP-Scan wird der NPCAP Treiber vorausgesetzt. Der NPCAP Treiber wird jeweils auf dem System benötigt, von dem aus der IP-Scan durchgeführt wird. Dies kann den Docusnap Server, Docusnap Client und die Docusnap Discovery Systeme betreffen.

Die Installation des NPCAP Treibers wird Ihnen im Zuge der Docusnap Installation angeboten und ist standardmäßig aktiv.

Eine nachträgliche Installation können Sie über das mitgebrachte Setup durchführen:

- %Docusnap-Installationsverzeichnis%\MSI\npcap-oem.exe
- %Docusnap-Discovery-Installationsverzeichnis%\MSI\npcap-oem.exe

2.1 Gefahren und Schwierigkeiten

Voraussetzung für die Installation des NPCAP Treibers sind lokale Administrator Rechte.

Bei der Installation des NPCAP Treibers ist zu beachten, dass dieser in den Netzwerk-Bereich eingreift. Speziell bei Systemen wie z. B. einem Domänen Controller, Exchange-Server oder ähnlichem sollte eine Installation nicht leichtfertig durchgeführt werden.

Ebenfalls gilt zu beachten, dass eine Installation des NPCAP Treibers in Konkurrenz zu ähnlichen Netzwerktreibern stehen kann. Dies kann auch andere Versionen des NPCAP Treibers betreffen. So wird bei einer Wireshark oder PRTG Installation ebenfalls ein NPCAP, oder ehemalig WINPCAP, Treiber installiert. Da es möglich ist, dass bei Wireshark oder PRTG andere Installationsoptionen gesetzt sind, können sowohl bei Wireshark als auch Docusnap fehlerhafte Resultate das Ergebnis sein.

Weitere Informationen zu den Voraussetzungen und Problematiken bei z. B. Firewall und Monitoring finden Sie in unserem **Whitepaper Docusnap Inventarisierung** im Kapitel IP-Scan.

3. IP-Scan

3.1 IP-Scan-Assistent

Der IP-Scan ist ein eigenständiger Inventarisierungsassistent in Docusnap. Unterschieden wird zwischen dem **Einfachen IP-Scan** und dem **Erweiterten IP-Scan**. Die Auswahl kann im Verlauf des Assistenten mittels einer Checkbox getroffen werden.

Den Assistenten für den IP-Scan finden Sie hier:

- Discovery – Alle Assistenten – IP Scan
- Inventar – Alle Assistenten – IP Scan
- Alle Aufträge – Alle Assistenten – IP Scan

IP-Scan

Der IP-Scan prüft mittels ICMP Anfragen die Adressen. Antwortet das angefragte System wird es als IP-System erfasst und mit zusätzlichen Informationen in der Datenbank gespeichert (Scandatum, IP-Adresse und Subnetzmaske). Zusätzlich versucht der IP-Scan den zugehörigen DNS-Namen aufzulösen. Ist dies erfolgreich, wird das System mit dem DNS-Namen erfasst.

Erweiterter IP-Scan

Mit Hilfe des Erweiterten Modus werden zusätzlich MAC-Vendor, Informationen zum Betriebssystem, Betriebszeit und der letzte Systemstart erfasst. Eine Genauigkeitsangabe der erfassten Informationen wird in Prozent angegeben. Dies kommt daher, dass NMAP das Betriebssystem etc. nicht immer zu 100% bestimmen kann. Anhand der Reaktion auf abgesetzte Anfragen schätzt NMAP diese Informationen ab.

Wird der Erweiterte IP-Scan aktiviert, so sucht Docusnap nach dem benötigten NPCAP Treiber. Ist dieser nicht vorhanden, kann der Erweiterte IP-Scan nicht verwendet werden.

Möchten Sie mehrere Netze zur Inventarisierung angeben empfiehlt sich die Verwendung des CSV Imports. Diesen können Sie über **Liste laden** aufrufen. Nachfolgend wird der Aufbau der CSV Datei beschrieben:

IP VON; IP Bis
192.168.0.1;192.168.0.254
192.168.10.1;192.168.10.254
192.168.100.1;192.168.103.254

Die maximale Größe eines Netzsegments ist auf **Class B** beschränkt.

3.2 Analyse und Ergebnis

Die Ergebnisse Ihres IP-Scans finden Sie im Datenbaum von Docusnap unter

- Firma – Infrastruktur – Domäne – IP Systeme

Überblick der Informationen die erfasst werden können:

- Name: Name des Systems. Wenn ein DNS-Eintrag vorhanden ist, wird dieser als Name verwendet, ansonsten die IP-Adresse.
- Scandatum: Zeitpunkt, wann das System das letzte Mal per IP-Scan erfasst wurde
- IP-Adresse: IP-Adresse des Systems
- Subnetzmaske: Subnetzmaske des Systems
- MAC Adresse: MAC Adresse des Systems. **Hinweis: Die MAC-Adresse ist nur vorhanden, wenn sich das Inventarisierte IP-System im gleichen Netzwerk wie der inventarisierende Part (Docusnap Server, Client, Discovery Service) befindet.**
- MAC-Vendor: Hersteller – Ergibt sich aus der erfassten MAC Adresse
- Betriebssystem: Information zu dem verwendeten Betriebssystem
- Hersteller: Hersteller des Betriebssystems
- Version: Versionsnummer des Betriebssystems
- Systemfamilie: Familie, z. B. Windows oder Linux
- Betriebszeit: Zeitangabe in Stunden
- Letzter Systemstart: Datum, wann das System das letzte Mal neu gestartet wurde
- Genauigkeit: Angabe zur Genauigkeit der erweiterten Informationen in Prozent

Mit Hilfe der erweiterten Informationen wie z. B. dem MAC-Vendor und Informationen zum Betriebssystem kann sich ein allgemeiner Überblick über das Netzwerk verschafft werden. Anschließend können die Systeme einem Assistenten für die weitere Inventarisierung zugeordnet werden.

IP-Systeme werden sowohl in Berichten als auch im Netzwerk- und Topologie Plan berücksichtigt.

3.3 MAC-Filter für IP-Systeme

Manche Systeme können nur via IP-Scan erfasst werden, da keine andere Standard Schnittstelle, z. B. SNMP unterstützt wird. Damit diese Systeme im Topologie Plan als z. B. Telefone dargestellt werden können, steht Ihnen ein MAC Filter zur Verfügung. Dadurch wird Ihnen die Unterscheidung der IP-Systeme im Topologie Plan erleichtert.

Vorgehensweise:

- Identifizieren sie den kleinsten gemeinsamen Nenner bei der MAC Adresse. Bei zwei IP-Telefonen mit jeweils einer MAC Adressen **00-1A-E8-EC-CA-70** und **00-1A-E8-EC-E9-DC** wäre der kleinste gemeinsame Nenner **00-1A-E8- (= Hersteller)**.
- Wechseln Sie in die Docusnap **Administration** – **Inventar** – **MAC Filter**
- Hinterlegen Sie dort die MAC Adresse – **00-1A-E8-**
- Unterstützte Wildcard Zeichen sind ***** um mehrere beliebige Zeichen und **?** um genau ein beliebiges Zeichen anzugeben.

MAC Adressen vom Typ Ignorieren und Virtuell werden im Topologie Plan anschließend nicht mehr dargestellt.

Weitere Informationen zum MAC Filter finden Sie im Docusnap Handbuch im Bereich MAC Filter. (F1 Taste im entsprechenden Bereich innerhalb der Docusnap Administration) oder im HowTo **Inventarisierung und Auswertung von SNMP** in der **Docusnap Knowledge Base**.

4. Anwendungsfälle und Praxisbeispiele

4.1 Erstinventarisierung

Eine vollständige und detaillierte Inventarisierung einer Netzwerkumgebung ist nur mit ausreichend privilegierten Benutzern möglich. Oftmals hat die inventarisierende Person bei einem neuen Kunden weder einen root Zugang zu Linux Systemen noch einen administrativen Zugang zu den Windows Systemen zur Verfügung. Trotzdem wird von dem Netzwerk ein erster Überblick benötigt.

Mit Hilfe des erweiterten IP-Scans können Sie die gewünschten Netzwerke analysieren, ohne dass administrative Rechte benötigt werden. Dabei können Sie herausfinden, wie viele Systeme vorhanden sind. Mit Hilfe der Betriebssysteminformationen ist anschließend eine Unterteilung in entsprechende Kategorien möglich.

- ➔ Anzahl der Windows Systeme
- ➔ Anzahl der Linux Systeme
- ➔ Anzahl der möglichen SNMP Systeme
- ➔ Etc.

4.2 Erhöhen der Datenqualität

Voraussetzung für eine qualitativ hochwertige Dokumentation ist eine gute Datenqualität in Docusnap. Da oftmals keine Übersicht der bestehenden Systeme vorhanden ist, ist ein Gegenprüfen der inventarisierten Systeme nicht möglich. Mit Hilfe des IP-Scans ist es Ihnen möglich eine Übersicht mit noch unbekannten Systemen zu erstellen und gezielt zu erfassen.

Ausgangssituation:
Alle Drucker des Unternehmens befinden sich im Netz XYZ. Dieses Netz wird bereits regelmäßig per SNMP inventarisiert. Um sicher zu gehen, dass wirklich alle Systeme innerhalb des Netzes erfasst werden, wird zusätzlich noch regelmäßig der IP-Scan eingesetzt.

Sind in diesem Fall Geräte noch nicht in Docusnap erfasst, werden diese nun zu den IP-Systemen hinzugefügt.

Anschließend sollten Sie die erfassten IP-Systeme bezüglich der SNMP Schnittstelle prüfen.

Werden diese Systeme zukünftig als SNMP Systeme erfasst, wird der Eintrag unterhalb der IP-Systeme verschoben. Eine Herabstufung hingegen ist nicht möglich – z. B. SNMP zu IP-System.

4.3 Sicherheitslücken erkennen

Bring your own Device, alte Netzwerkkomponenten und Internet of Things. Oftmals werden diese Systeme in Verbindung mit Sicherheitslücken gebracht. Nachfolgend wird Ihnen beschrieben, wie Sie mittels des Docusnap IP-Scans Sicherheitslücken erfassen, dokumentieren und darauf reagieren können.

Alte Netzwerkkomponenten erkennen:

In einem wachsenden Netzwerk kommt es im Laufe der Zeit vor, dass immer mehr alte Systeme vorhanden sind. Je nach Funktion kann dadurch eine Sicherheitslücke entstehen. Unterstützen diese Systeme als Schnittstelle nicht mindestens das SNMP Protokoll wird es schwierig diese zu erfassen, dokumentieren und entsprechend zu reagieren.

Mit Hilfe des IP-Scans können Sie einen regelmäßigen Scan Ihres Netzwerks durchführen. Ist z. B. noch ein alter Switch im Einsatz, wird dieser durch den IP-Scan erfasst. Dadurch vermeiden Sie z. B. den Ausfall Ihres Netzwerks aufgrund veralteter Hardware.

Bring your own Device / Internet of Thins

Die Aussage „Jeder neue Kühlschrank hat eine IP-Adresse“ entspricht nicht ganz der Realität, trifft den Nagel jedoch auf den Kopf. Mit den Netzwerken eines Unternehmens sind verschiedenste Systeme verbunden. Von Arbeitsplatzrechnern, Servern, privaten Mobiltelefonen bis hin zu Systemen des Alltags ist alles dabei. Aufgrund der Sicherheit des Netzes werden diese oftmals in verschiedene Bereiche eingeteilt. Zu Sicherheitslücken kann es kommen, wenn die Kaffeemaschine plötzlich im selben VLAN wie die Switche verfügbar ist.

Um eine solche Fehlkonfiguration zu erkennen, bietet sich der IP-Scan an. Da alle aktiven Systeme im Netzwerk erfasst werden, finden Sie auch die Systeme des Alltags sowie die sonstigen Geräte und können deren Netzwerkkonfiguration prüfen.

VERSIONSHISTORIE

Datum	Beschreibung
07.10.2019	Version 1.0 – Beschreibung des IP-Scans
22.04.2020	Version 2.0 - Überarbeitung des HowTos für Docusnap 11
01.08.2022	Version 2.1 – Erweiterung um die fehlenden MAC-Adressen aus anderen Netzwerken
10.01.2023	Version 3.0 – Überarbeitung des HowTos für Docusnap 12
28.11.2023	Version 4.0 – Überarbeitung des HowTos für Docusnap 13
27.11.2024	Version 4.1 – Anpassung CSV Import
15.05.2025	Version 4.2 – Standardparameter Docusnap 14 angepasst
19.09.2025	Version 4.3 – Kapitel entfernet – Nutzung des IP Scan Analyse Tool