IP-Scan

Inventory of IP Systems

TITLE	IP-Scan
AUTHOR	Docusnap Consulting
DATE	11/27/2024
VERSION	4.2 | valid from May 15, 2025

TABLE OF CONTENTS

1. Introduction

The IP-Scan in Docusnap gives you the possibility to search your network or that of a customer extensively for active systems. All you need for this initial overview, or to check for a complete inventory, are the relevant IP address ranges. No login information or community strings are used for the IP Scan. This way you can quickly and easily inventory a new network and get an overview.

In your own network, you can use this method to capture active components that you have not yet captured with a more detailed scan. Reasons for this could be, for example, that the system is not known, or the necessary logon information is missing.

Docusnap distinguishes between a normal and an extended IP Scan. Both IP Scans are based on **NMAP (Network Mapper)**. The normal IP Scan uses functions like SYN-ACK, ARP-Request, ICMP requests and name resolution. Responding systems are captured with rudimentary network information.

By using special NMAP parameters, the extended IP Scan can detect additional information such as the operating system.

Prerequisite for the extended IP Scan is the installation of the **NPCAP driver** on the inventorying system.

2. Prerequisites

In the first step, a successful IP scan only requires the IP address ranges to be inventoried to be known.

As already mentioned, a distinction is made between the simple and the extended IP scan. The NPCAP driver is required for the extended IP scan. The NPCAP driver is required on the system from which the IP scan is performed. This can be the Docusnap Server, Docusnap Client and the Docusnap Discovery systems.

The installation of the NPCAP driver is offered to you in the course of the Docusnap installation and is active by default.

You can perform a subsequent installation using the setup provided:

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

2.1 Risks and Difficulties

Prerequisite for the installation of the NPCAP driver are local administrator rights.

When installing the NPCAP driver, please note that it interferes with the network area. Especially with systems such as a domain controller, Exchange server or similar, an installation should not be carried out lightly.

Also note that installing the NPCAP driver may be in competition with similar network drivers. This may also affect other versions of the NPCAP driver. For example, a Wireshark or PRTG installation will also install a NPCAP, or former WINPCAP, driver. Since it is possible that Wireshark or PRTG has different installation options, both Wireshark and Docusnap may produce incorrect results.

You can find further information on the requirements and problems with e.g. firewalls and monitoring in our White Paper Docusnap Inventory in the IP Scan chapter.

3. IP-Scan

3.1 IP-Scan Wizard

The IP-Scan is a standalone inventory wizard in Docusnap. A distinction is made between the **Simple IP-Scan** and the **Advanced IP-Scan**. The selection can be made during the wizard using a checkbox.

The IP-Scan Wizard can be found here:

- Discovery – All Wizards – IP Scan
- Inventar – All Wizards – IP Scan
- Alle Aufträge – All Wizards – IP Scan

IP Scan

The IP Scan checks the addresses using ICMP requests. If the requested system responds, it is recorded as an IP system and stored in the database with additional information (scan date, IP address and subnet mask). In addition, the IP Scan attempts to resolve the associated DNS name. If this is successful, the system is registered with the DNS name.

Advanced IP Scan

With the help of the extended mode, MAC vendor, information on the operating system, operating time and the last system start are also recorded. The accuracy of the information collected is expressed as a percentage. This is because NMAP cannot always determine the operating system etc. one hundred percent. NMAP estimates this information based on the response to requests sent.

If the Extended IP Scan is activated, Docusnap searches for the required NPCAP driver. If this is not available, the extended IP Scan cannot be used.

If you want to specify several networks for inventory it is recommended to use the CSV import. You can call this up by choosing **Load list**.

IP FROM; IP TO
192.168.0.1;192.168.0.254
192.168.10.1;192.168.10.254
192.168.100.1;192.168.103.254

The maximum size of a network segment is limited to **Class B.**

3.2 Analysis and Result

You can find the results of your IP Scan in the Docusnap data tree under

- Company - Infrastructure - Domain - IP Systems.

Overview of the information that can be captured:

- Name: Name of the system. If a DNS entry exists, this DNS entry will be used as the name, otherwise the IP address.
- Scan Date: Time at which the system was last captured by IP Scan
- IP Address: IP address of the system
- Subnet Mask: Subnet mask of the system
- MAC Address: MAC address of the system. Note: The MAC address is only available if the inventoried IP system is on the same network as the inventorying part (Docusnap Server, Client, Discovery Service)
- MAC Vendor: Vendor - Based on the MAC address entered
- Operating System: Information on the operating system used
- Vendor: Vendor of the operating system
- Version: Version number of the operating system
- System Family: Family, e.g. Windows or Linux
- Operating Time: Time in hours
- Last Boot Start: Date on which the system was last booted
- Accuracy: Indication of the accuracy of the extended information in percent

With the help of advanced information such as the MAC vendor and information on the operating system, a general overview of the network can be obtained. The systems can then be assigned to an assistant for further inventory.

IP systems are considered in reports as well as in the network and Topology Plan.

3.3 MAC Filters for IP Systems

Some systems can only be captured via IP Scan because no other standard interface, e.g. SNMP, is supported. A MAC filter is available so that these systems can be displayed in the Topology Plan as telephones, for example. This makes it easier for you to distinguish the IP systems in the Topology Plan.

Procedure:

- Identify the lowest common denominator at the MAC address. For two IP telephones, each with one MAC address **00-1A-E8-EC-CA-70** and **00-1A-E8-EC-E9-DC**, the lowest common denominator would be **00-1A-E8- (= Vendor).**
- Switch to Docusnap **Administration** - **Inventory** tab - **MAC filter**
- Put the MAC address there - **00-1A-E8-**
- Supported wildcard characters are ***** to specify multiple arbitrary characters and **?** to specify exactly one arbitrary character.

MAC addresses of the Ignore and Virtual type are no longer displayed in the Topology Plan.

Further information about the MAC Filter can be found in the Docusnap manual in the MAC Filter section. (F1 key in the corresponding area within the Docusnap Administration) or in the HowTo Inventory and Analysis of SNMP in the Docusnap Knowledge Base.

4. Application Cases and Practical Examples

4.1 Initial Inventory

A complete and detailed inventory of a network environment is only possible with sufficiently privileged users. Often the person taking the inventory has neither root access to Linux systems nor administrative access to Windows systems for a new customer. Nevertheless, the network needs a first overview.

The advanced IP Scan allows you to analyze the desired networks without the need for administrative rights. You can find out how many systems are available. With the help of the operating system information it is then possible to subdivide the data into corresponding categories.

- ➔ Number of Windows systems
- ➔ Number of Linux systems
- ➔ Number of possible SNMP systems
- ➔ Etc.

4.2 Increase data quality

A prerequisite for high-quality documentation is good data quality in Docusnap. Since there is often no overview of the existing systems, it is not possible to check the inventoried systems against each other. With the help of the IP Scan it is possible for you to create an overview with unknown systems and to capture them specifically.

Initial situation:
All the company's printers are in the XYZ network. This network is already regularly inventoried via SNMP. To make sure that all systems within the network are really captured, the IP Scan is also used regularly.

In this case, if devices are not yet included in Docusnap, they will now be added to the IP systems.

You should then check the IP systems that have been captured regarding the SNMP interface.

If these systems are recorded as SNMP systems in the future, the entry below the IP systems will be moved. However, a downgrade is not possible - e.g. SNMP to IP system.

4.3 Detect Security Vulnerabilities

Bring your own device, old network components and Internet of Things. These systems are often associated with security vulnerabilities. The following describes how you can detect, document, and react to security vulnerabilities using the Docusnap IP Scan.

Detect old network components:

In a growing network, more and more old systems may become available over time. Depending on the function, this can result in a security gap. If these systems do not support at least the SNMP protocol as an interface, it will be difficult to record, document and react accordingly.

The IP Scan allows you to perform a regular scan of your network. If, for example, an old switch is still in use, it is detected by the IP Scan. This will prevent your network from failing due to outdated hardware, for example.

Bring your own Device / Internet of Thins

The statement "Every new refrigerator has an IP address" does not quite correspond to reality but hits the nail on the head. Various systems are connected to the networks of a company. From workstations, servers, private mobile phones to everyday systems, everything is included. Due to the security of the network, these are often divided into different areas. Security gaps can occur if the coffee machine is suddenly available in the same VLAN as the switches.

To detect such a misconfiguration, the IP Scan is a good choice. Since all active systems are captured on the network, you can also find the everyday systems and other devices and check their network configuration.

VERSION HISTORY

Date	Description
October 7, 2019	Version 1.0 - Description of the IP Scan
April 22, 2020	Version 2.0 - Revision of the HowTo for Docusnap 11
August 01, 2022	Version 2.1 – Extension by the missing MAC addresses from other networks
January 10., 2023	Version 3.0 – Revision of the HowTo for Docusnap 12
November 28, 2023	Version 4.0 – Revision of the HowTo for Docusnap 13
November 27, 2024	Version 4.1 - CSV import adjustment
May 15, 2024	Version 4.2 - Default parameter Docusnap 14 adjusted
September 19, 20925	Version 4.3 - Chapter removed – Using the IP Scan Analysis Tool