White Paper Docusnap Inventory

Technical overview and suggested solutions to inventory problems

TITLE	White Paper Docusnap Inventory
AUTHOR	Docusnap Consulting
DATE	08/22/2019
VERSION	1.1 | valid from 08/22/2019

TABLE OF CONTENTS

1. Introduction

Often problems occur during the initial inventory due to missing permissions of a user or blocked ports of a firewall. In order to help you solve these problems, the necessary prerequisites are explained in more detail in the following chapters using ports, rights and an FAQ part.

The document is divided into a tabular overview and a detailed description of the individual inventories.

Further information and HowTos can be found in our Docusnap Knowledge Base. These can be found at www.docusnap.com/en/ in the Support tab.

All information in this White Paper is updated regularly. They may be incomplete.

2. Tabular overview

INVENTORY	PROTOCOL	PORT	TRANSPORT LAYER
WINDOWS - WMI	NetBIOS Name Service, NetBIOS Datagram Service - only for WMI	137, 138	UDP
	NetBIOS Session Service, Microsoft DS Active Directory, Windows Shares (CIFS)	139, 445	TCP
	dynamic High Range Port - WMI only	1024 - 65535	TCP/UDP
	LDAP - Lightweight Directory Access Protocol - only for Winodws (AD)	389	TCP/UDP
WINDOWS PSEXEC	DCE endpoint solution for PsExec, Microsoft-DS Active Directory, Windows shares (CIFS)	135, 445	TCP
	LDAP - Lightweight Directory Access Protocol - Windows only (AD)	389	TCP/UDP
SNMP SYSTEMS	SNMP - Simple Network Management Protocol	161	UDP
CIFS SYSTEMS	SNMP - Simple Network Management Protocol	161	UDP
	Microsoft DS Active Directory - Windows Shares (CIFS)	445	TCP
LINUX SYSTEMS	Secure Shell (SSH)	22	TCP/UDP
	SSH File Transfer Protocol (SFTP)	115	TCP
MAC SYSTEMS	Secure Shell (SSH)	22	TCP/UDP
VMWARE	https - Hypertext Transfer Protocol Secure	443	TCP
HP-UX	Secure Shell (SSH)	22	TCP/UDP
HYPER-V / IIS SERVER	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	DCE Endpoint Solution, NetBIOS Session Service, Microsoft-DS Active Directory, Windows Shares (CIFS)	135, 139, 445	TCP
	dynamic High Range Port	1024 - 65535	TCP/UDP
XENCENTER	https - Hypertext Transfer Protocol Secure	Port can be customized	TCP

IGEL SYSTEMS	SQL DATABASE - MSSQL (MICROSOFT SQL SERVER)	1433	TCP
	SQL Database - MSSQL (Microsoft SQL Server) Monitor	1434	TCP/UDP
	dynamic High Range Port	1024 - 65535	TCP/UDP
SHAREPOINT	DCE Endpoint Solution, Windows Shares (CIFS)	135, 445	TCP
EXCHANGE	NetBIOS Name Service, NetBIOS Datagram Service	137, 138	UDP
	DCE Endpoint Solution, NetBIOS Session Service, Microsoft-DS Active Directory, Windows Shares (CIFS)	135, 139, 445	TCP
	dynamic High Range Port - WMI	1024 - 65535	TCP/UDP
SQL SERVER / VEEAM / BACKUP EXEC	SQL Database - MSSQL (Microsoft SQL Server)	1433	TCP
	SQL Database - MSSQL (Microsoft SQL Server) Monitor	1434	TCP/UDP
	dynamic High Range Port	1024 - 65535	TCP/UDP
ORACLE DATABASE	Oracle SQL Net Listener and Data Guard	1521	TCP
DELL EMC² ISILON	http - Hypertext Transfer Protocol	8080	TCP
ACTIVE DIRECTORY / ADS SYNCHRONIZATION	LDAP - Lightweight Directory Access Protocol	389	TCP/UDP
	DCE Endpoint Solution, Microsoft DS Active Directory, Windows Shares (CIFS) - Group Policy only	135, 445	TCP
DFS	NetBIOS Name Service, NETBIOS Datagram Service	137, 138	UDP
	NetBIOS Session Service, Microsoft DS Active Directory - Windows Shares (CIFS)	139, 445	TCP
	dynamic High Range Port	1024 - 65535	TCP/UDP
	LDAP - Lightweight Directory Access Protocol	389	TCP/UDP
DNS / DHCP	DCE Endpoint Solution, Microsoft DS Active Directory, Windows Shares (CIFS)	135, 445	TCP
AZURE / OFFICE 365	https - Hypertext Transfer Protocol Secure	443	TCP

3. Inventories

In the following chapters the different inventories are described.

3.1 Windows - WMI / PsExec (fallback method)

3.1.1 Protocols and Authorizations

Protocols used Windows WMI:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE - ONLY AT WMI	137, 138	UDP
NETBIOS SESSION SERVICE, MICROSOFT DS ACTIVE DIRECTORY, WINDOWS SHARES (CIFS)	139, 445	TCP
DYNAMIC HIGH RANGE PORT - WMI ONLY	1024 – 65535	TCP/UDP
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL - ONLY FOR WINODWS (AD)	389	TCP/UDP

Protocols used Windows - PsExec:

DESIGNATION	PORT	TRANSPORT
DCE ENDPOINT-SOLUTION, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS SHARES (CIFS)	135, 445	TCP
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL - ONLY FOR WINODWS (AD)	389	TCP/UDP

Required rights Windows general:

- Domain administrator
  - NetBIOS notation
  - UPN notation
- Alternatively, a domain user with local administrator rights is possible for clients and servers.
- When using local administrator rights with Windows (IP), observe UAC. See FAQ for more information.
  - For single registration computer name\user
  - For collective inventory .\user

Additional rights - WMI:

- Active WMI services on the target system
  - Windows Management Instrumentation
  - Remote Procedure Call (RPC)

Additional rights - PsExec:

- Execution of PsExec.exe (Microsoft Sysinternals Tool) possible
  - Test of the execution:
    - C:\Program Files\Docusnap X\bin\PsExec.exe \\Hostname/IP-address -u domain\user cmd
  - PsExec can be blocked by the virus scanner:
    - C:\Windows\PSEXESVC.EXE - release on target system
    - C:\Program Files\Docusnap X\bin\PsExec.exe - release on source system

3.1.2 Network requirements

- Windows system is member of Active Directory (Windows (AD) only)
- Unique name resolution must be given (Forward Lookup & Reverse Lookup)
- Transparent firewall configuration
- System must be reachable via ping
- When using the fallback method, execution of PsExec must be allowed.

3.1.3 FAQs

Q1 Despite authentication with a sufficiently authorized user, the error message "Connection could not be established" appears. What's the problem?

A1 When authenticating against the domain, please use a user specification with domain suffix.

- *User principal name* *UserName@Example.intern*
- *Down-level logon name* *Example\UserName*

Q2 Despite using a user with local administrator membership, the "Access denied" error message occurs.

A2 *The reason for the problem is the User Account Control (UAC). The user connects with "normal permissions" and the so-called auto-elevation mechanism, which should increase permissions if necessary, does not work with remote access. With the following command a corresponding registry entry can be set which solves the problem.*

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Q3 Where can further information on inventory be found?

A3 *For more information about Windows inventory, see the Docusnap Knowledge Base.*

- *WMI Access Problems*
- *Windows Firewall Exceptions*

Q4 Is it possible to inventory Windows systems via script?

A4 *Yes, you can find more detailed information about the inventory using a script in the corresponding HowTo in the Docusnap Knowledge Base.*

- *Docusnap Script Windows*

Q5 Some systems are connected via a slow line. An inventory results in a timeout error. How can it be fixed?

A5 *You can increase the timeout in the inventory options. Navigate to the menu Docusnap - Inventory - General*

Q6 Why is PsExec classified as threatening by a virus scanner?

A6 *Some antivirus scanners report that one or more of the tools are infected with a remote admin virus. PsTools do not contain viruses, but they have been used by viruses. For this reason, a virus message may appear and PsExec must be released from quarantine.*

Q7 How can an inventory be activated via PsExec connection (fallback method)?

A7 *You will find the option under Docusnap - Inventory - Inventory tab. Then activate the checkbox "Fallback Method for Windows Inventory" and confirm your change with "OK". You have then successfully activated the inventory using PsExec.*

3.2 IP Scan

3.2.1 Protocols and Authorizations

A detailed overview of the ports used during the IP Scan cannot be given. Depending on how the IP Scan is configured, different ports are scanned. A distinction can be made between individual ports up to a complete range. In theory, it is possible for the IP Scan to check all possible ports.

Note: Due to a high number of ICMP requests, an IP Scan can cause the network monitoring to generate warning messages. Monitoring tools can also issue a warning message that invalid packets are being sent. This behavior is normal for an IP Scan. These packets are sent so that, for example, the operating system can be recognized.

Required rights:

- Enable the call of Nmap. In some cases, antivirus vendors block Nmap from being called from another software.
- Local administrator rights to install the WinPcap driver. This is required for an "extended IP Scan".
- If the "extended IP Scan" is not used, no WinPcap driver is required. Additional functions such as operating system recognition are therefore not possible.

3.2.2 Network requirements

- Installation of the current WinPcap driver on the running system. Can be selected in the setup routine or installed subsequently.
- Various third-party software can influence the execution of the IP Scan; e.g. Wireshark.

3.2.3 FAQs

Q1 If a complete IP range is specified, not all systems in this range will be found. However, it is possible to scan the systems individually. What's the mistake?

A1 *If the systems are found individually during the scan, a scan should also be possible by specifying an IP range. If necessary, please check your firewall settings with regard to ICMP Flooding Protection.*

Q2 How do I know if the current WinPcap driver is installed?

A2 *As soon as the extended mode is activated in the wizard, Docusnap checks if the additional network driver is available. If this is not installed, the extended mode is not possible.*

3.3 SNMP systems

3.3.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL	161	UDP

Note: Due to a high number of ICMP requests, an SNMP inventory can cause the network monitoring system to generate warning messages.

Required rights:

- Read community string - in standard public
- Authentication credentials for SNMP v3
- SNMP manager (querying system, e.g. Docusnap Server) must be authorized for SNMP polling on the SNMP agent (**whitelisting**).

3.3.2 Network requirements

- SNMP protocol is enabled. V1, V2 or V3
- Transparent firewall configuration

3.3.3 FAQs

Q1 If a complete IP range is specified, not all systems in this range are found. However, an inventory of the systems is possible individually. What's the mistake?

A1 *If the systems are inventoried individually, an inventory should also be possible by specifying an IP range. If necessary, please check your firewall settings with regard to ICMP Flooding Protection.*

3.4 CIFS Systems

With the help of the CIFS inventory, releases of systems (e.g. NAS, etc.) can be recorded. Thus the CIFS inventory forms the basis for an authorization analysis in Docusnap.

The system to be inventoried via CIFS must not already be registered via Linux or Windows wizards.

3.4.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SNMP - SIMPLE NETWORK MANAGEMENT PROTOCOL	161	UDP
MICROSOFT DS ACTIVE DIRECTORY - WINDOWS SHARES (CIFS)	445	TCP

Required rights:

- Read community string
- Domain administrator or comparable - depending on system
- Authorization to start SNMP queries on the target system

3.4.2 Network requirements

- Transparent firewall configuration
- If a user other than the currently logged in user is used for the CIFS inventory, the currently logged in user must not establish a connection to the CIFS system (e.g. connection via a network drive).
    - These can be checked using the *net use* command.
- Special case: NAS system groups have to be considered (readout of SMB permissions)

3.5 Linux Systems

3.5.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SECURE SHELL (SSH)	22	TCP/UDP
SSH FILE TRANSFER PROTOCOL (SFTP)	115	TCP

Required rights:

- root user
- remote login as root allowed

3.5.2 Network requirements

- Transparent firewall configuration
- supported Linux derivative
    - An overview of the supported derivatives can be found in the Docusnap system requirements.

3.5.3 FAQs

Q1 The system was successfully inventoried, but only part of the information is visible.

A1 To ensure that the collected information is complete, you must use the root user. A complete inventory is only possible with the root user.

Q2 Is it possible to inventory Linux systems via script?

A2 Yes, you can find more detailed information about the inventory using a script in the corresponding HowTo in the Docusnap Knowledge Base.

- *Docusnap Script Linux*

Q3 Is authentication via RSA key possible?

A3 Yes, you can find more detailed information about the inventory by RSA key in the corresponding HowTo in the Docusnap Knowledge Base.

- *Linux Inventory Using RSA Key Authentication*

3.6 Mac Systems

3.6.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SECURE SHELL (SSH)	22	TCP/UDP

Required rights:

- remote login with a password-protected user
- Activate the "Remote login" service for the user used.

3.6.2 Network requirements

- Transparent firewall configuration

3.6.3 FAQs

Q1 Is it possible to inventory Mac systems via script?

A1 Yes, the corresponding script file can be found in the installation directory of Docusnap, subfolder "Bin".

3.7 VMware

3.7.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Required rights:

- Root user or AD user with continuous administrator rights
- Alternatively it is possible to create a "Read Only" user. This has read-only permissions for the entire environment.

3.7.2 Network requirements

- Transparent firewall configuration
- Set proxy exceptions if necessary

3.7.3 FAQs

Q1 You cannot connect to the ESXi Host or vCenter in the Inventory Wizard.

A1 Please perform a connection test of the Web API and activate it or set proxy exceptions if necessary.

➔ *https://hostname-vCenter/mob*

3.8 HP-UX

3.8.1 Protocols and Authorizations

Protocols used in the standard system:

DESIGNATION	PORT	TRANSPORT
SECURE SHELL (SSH)	22	TCP/UDP

Required rights:

- Users with administrative authorizations on the HP-UX Server

Required commands / tools:

- bdf - Free Memory Information
- cprop - System Information: Disk/Memory/Network Information/Processors/Firmware/System Summary
- cstm - Can execute scripts
- swlist - Software Information
- grep - Used to parse log files
- uname - Operating system/kernel info
- machinfo - Additional system information

3.8.2 Network requirements

- Transparent firewall configuration

3.9 Hyper-V / IIS Server

3.9.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
DCE ENDPOINT-SOLUTION, NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS SHARES (CIFS)	135, 139, 445	TCP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP

Required rights:

- Local administrator or domain administrator
  - NetBIOS notation
  - UPN notation
- Administration rights Hyper-V manager
- SharePoint Farmadmin permissions on a SharePoint IIS
  - Enter the authentication with NetBIOS name

3.9.2 Network requirements

- Transparent firewall configuration
- Unique name resolution must be given (forward lookup & reverse lookup).

3.9.3 FAQs

Q1 I own a Hyper-V environment / IIS server, but no domain. Nevertheless, an authentication against the domain is assumed in the inventory dialog.

A1 *In the Docusnap menu - Inventory - Inventory tab – section Other a domain authentication for the Hyper-V and IIS wizard can be deactivated. Authentication with a local user is then possible.*

3.10 XenCenter

3.10.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	Port can be customized	TCP

Required rights:

- Administrator rights on Xen Server

3.10.2 Network requirements

- Transparent firewall configuration
- Set proxy exceptions if necessary

3.11 Igel Systems

3.11.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SQL DATABASE - MSSQL (MICROSOFT SQL SERVER)	1433	TCP
SQL DATABASE - MSSQL (MICROSOFT SQL SERVER) MONITOR	1434	TCP/UDP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP

Required rights:

- Users with at least read permissions on the Igel database (db_reader).

3.11.2 Network requirements

- Transparent firewall configuration
- Database and server must allow remote connections

3.11.3 FAQs

Q1 There is only an Igel embedded Database available. How can Docusnap connect to it?

A1 *Docusnap only supports Microsoft SQL databases when inventorying Linux systems using the Igel wizard. An Igel embedded database is not supported. However, this can be migrated to a Microsoft SQL environment. The exact procedure is described in the Igel manual.*

Q2 Is it possible to inventory the Igel thin clients using a script?

A2 *Yes, you can inventory Igel thin clients with a Linux operating system using the Linux script. The corresponding script file can be found in the installation directory of Docusnap, in the subfolder "Bin". A possible method of automated execution of the script is to use the Igel UMS.*

Note: The thin client is stored in the database as a Linux system and not as a thin client.

3.12 SharePoint

3.12.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
DCE ENDPOINT-SOLUTION, WINDOWS SHARES (CIFS)	135, 445	TCP

Required rights:

- Full access to the SharePoint system. Corresponds to the FarmAdmin used during the installation. It is necessary to add the domain suffix to the user name.
  - NetBIOS notation
  - UPN notation
- Db_owner rights in every SharePoint database
- Administration rights for all website collections
- Starting with Windows Server 2008 R2 and the separation of SharePoint and SQL Server, authentication problems may occur due to "multi-hop".
  - In this case, the inventory user must be included in the group of local administrators on the SharePoint server.
  - FarmAdmin must be stored in the authentication dialog. No user may be stored for server authentication.

3.12.2 Network requirements

- Transparent firewall configuration
- Execution of PsExec.exe (Microsoft Sysinternals Tool) possible
- PsExec can be blocked by virus scanner

3.12.3 FAQs

Q1 Despite the use of the specified FarmAdmin, the inventory is erroneous or incomplete.

A1 *If, for example, a domain administrator is used during the SharePoint installation, this is the "real" FarmAdmin. Check an inventory with this user.*

Q2 Is it possible to inventory via script?

A2 *Yes. In the Docusnap installation directory, subfolder "Bin" you will find a DocusnapSP** script. Select the appropriate script for your SharePoint version. You can start the script on the SharePoint Server via CMD or Power Shell. The results are packed into a Zip archive. You can then import this into Docusnap using the Script Import.*

3.13 Exchange

3.13.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
DCE ENDPOINT-SOLUTION, NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS SHARES (CIFS)	135, 139, 445	TCP
DYNAMIC HIGH RANGE PORT - WMI CONNECTION	1024 - 65535	TCP/UDP

Required rights:

- Domain administrator and membership in the Exchange Organization Administrators (Organization Management) group. It is necessary to add the domain suffix to the user name.
    - NetBIOS notation
    - UPN notation

3.13.2 Network requirements

- Transparent firewall configuration
- Execution of PsExec.exe (Microsoft Sysinternals Tool) possible
- PsExec can be blocked by virus scanner

3.13.3 FAQs

Q1 An inventory was successful, but no mailboxes were evaluated.

A1 Please check if the inventory user is a member of the Exchange Organization Administrators.

Q2 Is it possible to inventory via script?

A2 Yes, you can inventory Exchange data via script.

3.14 SQL Server / Veeam / BackupExec

3.14.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
SQL DATABASE - MSSQL (MICROSOFT SQL SERVER)	1433	TCP
SQL DATABASE - MSSQL (MICROSOFT SQL SERVER) MONITOR	1434	TCP/UDP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP

Required rights:

- SysAdmin authorization for SQL Server inventory
- If a user without SysAdmin role is used, a "limited inventory" is possible. Only parts of the SQL Server or the instance are inventoried.
- For Veeam and BackupExec inventory a user with read permissions on the Veeam or BackupExec database is required (db_reader).
- SQL user or Domain user
    - Domain user is integrated in the inventory dialog. This cannot be changed. The session user or the deposited user account of the Docusnap Server service is used.
    - SQL user can be stored separately for each instance found

3.14.2 Network requirements

- Transparent firewall configuration
- Database and server must allow remote connections
- TCP/IP protocol activated for SQL server or instance.

3.14.3 FAQs

Q1 In an automatic SQL server search, not all SQL servers are found.

A1 Please check whether the SQL server browser is active on the SQL server to be inventoried. This is necessary for automatic determination. SQL server instances are determined using broadcast. No systems are found across a router (broadcast domain).

3.15 Oracle Database

3.15.1 Protocols and Authorizations

Protocols used in the standard system:

DESIGNATION	PORT	TRANSPORT
ORACLE SQL NET LISTENER AND DATA GUARD	1521	TCP

Required rights:

- Correspondingly authorized user (DBA). Inventory user can be created with the help of a script.
    - This can be found in the Docusnap manual in the chapter "Oracle" Inventory.
- Specify host name, service name, and port.
    - Data can be read out in the configuration
- Authorized user
    - Create session
    - Select any dictionary

3.15.2 Network requirements

- Transparent firewall configuration

3.16 Dell EMC² Isilon

3.16.1 Protocols and Authorizations

Protocols used in the standard system:

DESIGNATION	PORT	TRANSPORT
HTTP. HYPERTEXT TRANSFER PROTOCOL	8080	TCP

Required rights:

- Root rights in EMC² Isilon environment.

3.16.2 Network requirements

- Transparent firewall configuration
- If necessary, proxy exceptions must be set.
- Standard port may differ

3.17 Active Directory / ADS Synchronization

3.17.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL	389	TCP/UDP
DCE ENDPOINT-SOLUTION, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS SHARES (CIFS) - GROUP POLICY ONLY	135, 445	TCP

Required rights:

- A full ADS scan requires a domain administrator login.
    - Specification in NetBIOS or UPN notation
- As a domain user, a query is also possible - as long as the default configuration has not been changed.
    - It is not possible to read the configuration partition here.
- Optional GPO inventory requires access to the domain controller via PsExec.exe.

3.17.2 Network requirements

- Transparent firewall configuration
- PsExec can be blocked by virus scanner

3.17.3 FAQs

Q1 The Active Directory was successfully inventoried. However, no users and groups were read out.

A1 Please check whether your domain is stored in Docusnap with the FQDN; e.g. "docusnap.internal".

Q2 How can it be avoided that the ADS reconciliation deletes inventoried systems that are not members of the domain?

A2 Set the OU filter to the uppermost level during ADS adjustment. Subsequently, the wizard compares the workgroup domains to membership domains. Only systems that no longer exist and were part of the domain are now removed.

3.18 DFS

3.18.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
NETBIOS NAME SERVICE, NETBIOS DATAGRAM SERVICE	137, 138	UDP
NETBIOS SESSION SERVICE, MICROSOFT DS ACTIVE DIRECTORY - WINDOWS SHARES (CIFS)	139, 445	TCP
DYNAMIC HIGH RANGE PORT	1024 - 65535	TCP/UDP
LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL	389	TCP/UDP

Required rights:

- Domain administrator
  - NetBIOS notation
  - UPN notation

3.18.2 Network requirements

- Transparent firewall configuration
- DNS (resolution and recursive resolution)

3.19 DNS / DHCP

3.19.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
DCE ENDPOINT-SOLUTION, NETBIOS SESSION SERVICE, MICROSOFT-DS ACTIVE DIRECTORY, WINDOWS SHARES (CIFS)	135, 139, 445	TCP

Required rights:

- Domain administrator
  - NetBIOS notation
  - UPN notation

3.19.2 Network requirements

- Transparent firewall configuration
- Execution of PsExec.exe (Microsoft Sysinternals Tool) possible
- PsExec can be blocked by virus scanner

3.20 Azure / Office365

3.20.1 Protocols and Authorizations

Protocols used:

DESIGNATION	PORT	TRANSPORT
HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE	443	TCP

Required rights:

- A global administrator is required to create the necessary applications.
  - Azure: registered application with read access to Azure information
  - Office365: Registered application with read access to Office365 information

- A detailed description of the inventory can be found in the HowTos of the Docusnap Knowledge Base.
  - Inventorying Microsoft Azure
  - Inventorying Microsoft Office 365

3.20.2 Network requirements

- Transparent firewall configuration
- Discovery service must reach the Internet
- If necessary, set proxy exceptions.

VERSION HISTORY

Date	Description
03/20/2019	Documentation created
07/01/2019	IP Scan module was added