ivanti

Neurons for Service Mapping-Discovery Requirements

Ver. 3.8

Technical Document

Table of Contents

Introduction

About This Document

This document provides the information required to scope and size a **Ivanti Neurons for Service Mapping Discovery application (DA)** deployment.

It also provides a checklist of the system requirements to run the Discovery Application on customer-hosted servers, the firewall rules to allow communication between the DA and Ivanti Neurons for Service Mapping cloud instance, and the credential requirements for accurate asset discovery, configuration collection, application dependencies and inter-relationships.

This document is not a how-to-guide for implementing, configuring or troubleshooting Ivanti Neurons for Service Mapping Discovery Application installations.

About Ivanti Neurons for Service Mapping

Ivanti Neurons for Service Mapping provides automatic inventory and configuration cataloging of computers, networks and storage assets – both on premise and on the cloud. The discovery process identifies physical and logical dependencies between applications and their host systems.

From there, enterprise services are easily mapped across all supporting infrastructure components and are viewable in the Ivanti Neurons for Service Mapping CMDB.

Ivanti Neurons for Service Mapping offers the ease of SaaS deployment and accessibility combined with the security and performance of on-premise discovery. The Discovery Application currently supports more than 140 agentless and extendable probes.

Summary of Changes

This section records the history of significant changes to this document. Only the most significant changes are described here.

Table 1

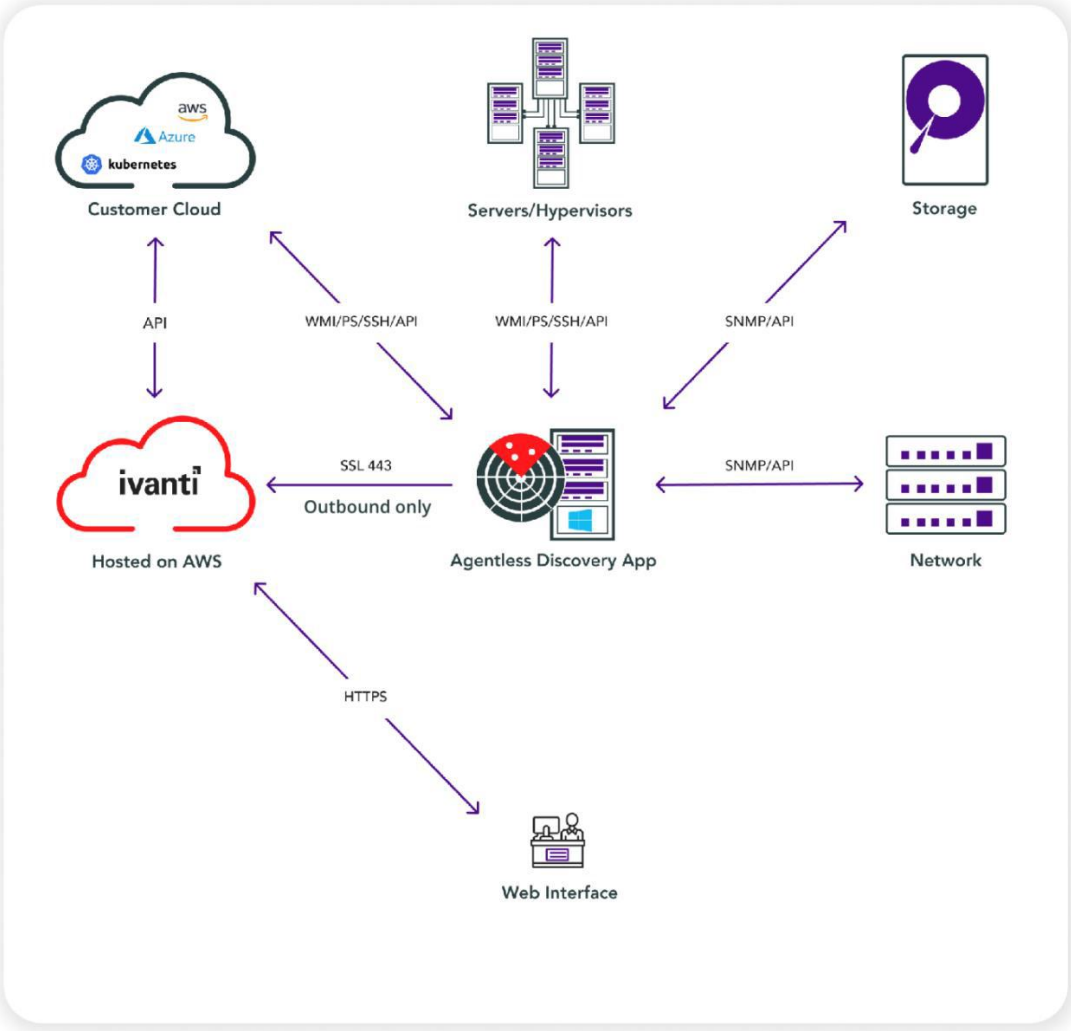
Version	Date	Description of Change
3.2.0	05-08-24	Added architecture diagram, agent requirements, and subnet details
3.21	06-28-24	Added proxy support configurations
3.3	09-23-24	Added additional credential types and details
3.4	01-27-24	Fixed inaccurate references
3.5	02-12-25	Added SUDO notes to Unix, Linux, Mac, and Solaris
3.6	02-24-25	Added MySQL requirements
3.7	11-24-2025	Version 6.1 updates

Discovery Architecture Overview

Discovery Architecture

The graphic below provides a visual representation of the methods Ivanti Neurons for Service Mapping employs to perform asset, configuration, software and relationship/dependency discovery. The two discovery methods are:

- **Agentless discovery** initiated from a local Discovery App server(s) deployed within the corporate network or cloud environment.
- **Discovery Agents** that communicate with a local Discovery App server.



Discovery App Sizing Considerations

The number and locations of DA's depend on several factors, including:

- The size of the network to scan
- Number of discoverable assets
- Time required to complete all scans
- Number of logically or physically separated networks

Key questions to consider:

- How many data centres or cloud environments will be scanned?
- What connectivity/bandwidth exists between each data centre?

- Do firewall rules/router settings prevent scanning between data centers? (see *Authentication Requirements* for ports/protocols)
- How many IP subnets per DC/Cloud environment?
- What is the approximate number of devices/virtual servers per subnet?
- What is the desired scan frequency?

Discovery App Scan Capabilities

Each Discovery App is capable of simultaneously scanning subnets of four /24, two /23 or one /22. Scan times can vary based on the number and types of connected devices. Generally, a scan of a /24 subnet with the maximum number of 256 devices will take 20-40 minutes to complete. This means four /24 subnets can be simultaneously scanned in an average time of 30 minutes. Table 2 shows the estimated scan times for various amounts of /24 subnets and Discovery Apps.

Table 2: Discovery App Scan Capabilities

Number of Subnets	Number of IPs	Number of Discovery Apps	Hours to complete scan*
4	1,024	1	.5
25	6,400	1	3
100	25,600	1	13
200	52,200	2	13
400	102,400	4	13

A single Discovery App can easily scan over 20,000 IPs per day. If daily scans for each IP are not required, subnet scans can be configured to run on alternating days to increase the IP scanning capacity from a single DA. Otherwise, multiple DA's may be required.

Discovery App Server Requirements

The Discovery App must be installed on a Windows Server (see Table 3 for recommended specs) regardless of the types of devices or operating systems to be discovered. The Windows Server must be located within the domain to be discovered or trust across domains must be enabled. The Discovery App Windows Server must also have a persistent outbound connection to the URLs shown in Table 4.

The Discovery App will be downloaded from a link inside the Ivanti Neurons for Service Mapping UI that points to an AWS S3 bucket. Please have the Chrome browser installed and download ability from an AWS S3 bucket on the Discovery App server or be able to download and copy the installer to the Discovery App server.

Table 3: Discovery App System Requirements

Operating System	Server Type	CPU	RAM	HD	Browser
Windows Server 2012 or newer	Dedicate Physical or Virtual	High performance (12-16 cores)	16 GB	50 GB	Chrome

Firewall Rules

Discovery is performed when the Discovery App retrieves commands from the Ivanti Neurons for Service Mapping cloud and launches selective probes per the defined schedule to the target systems. The data returned by the probes is then securely transmitted from the DA to the Ivanti Neurons for Service Mapping cloud for processing into the CMDB. Table 4 shows the necessary communications to allow the scans to run and have the data sent to the Ivanti Neurons for Service Mapping cloud. These firewall requirements are in addition to authentication and port requirements shown in the following section.

Table 4: Discovery App Firewall Rules

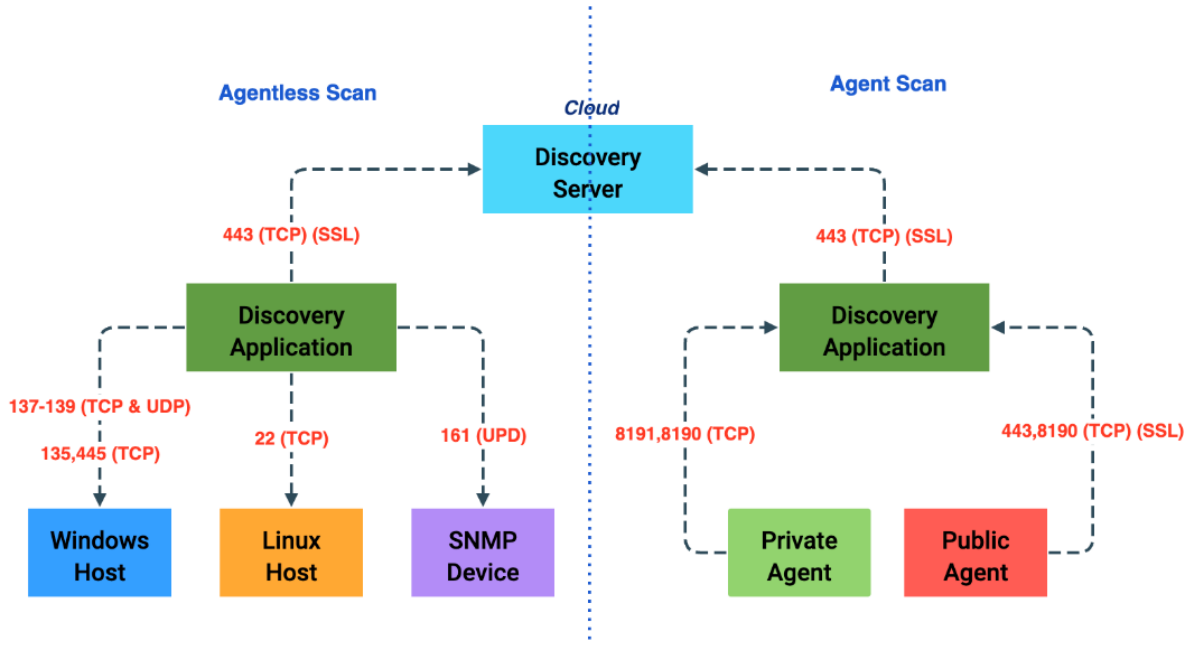
<table>
<tr><th colspan="2">Outbound (Discovery App to Ivanti cloud)</th></tr>
<tr><th colspan="2">SSL Port 443 to the following URL's (Geo dependent)</th></tr>
<tr><td>U.S. Hosting
https://discoveryselector-usw2.ivanticloud.com
https://discoveryserver1-usw2.ivanticloud.com
https://servicemapping-usw2.ivanticloud.com</td><td>EU (Frankfurt) Hosting
https://discoveryserver1-euc1.ivanticloud.com
https://discoveryselector-euc1.ivanticloud.com</td></tr>
<tr><td>Australia Hosting
https://discoveryserver1-apse2.ivanticloud.com/
https://discoveryselector-apse2.ivanticloud.com/</td><td></td></tr>
</table>

Proxy Server
Proxy server is supported* for outbound communication from Discovery App to INSM cloud with the following properties in Discovery Application common.properties file: #ProxyHost= #ProxyPort= #ProxyUserName= #ProxyPassWord= *Currently a proxy server cannot be used in conjunction with CyberArk PAM integration
Allow Persistent Connection
Firewall rules must allow for a persistent connection between the Discovery Application and Ivanti Neurons for Service Mapping cloud. Same is true for connections between Discovery Agents and the Discovery Application.
ICMP Ping or NMAP
As of version 6.1 both ICMP Ping and NMAP to check for hosts have been deprecated. Host checks are now done via port checks (ports 22, 135, 161)

Port Requirements

The figure below details the ports required for the Discovery App to conduct agentless scanning, receive data from the Windows agents, and transfer the discovery data to the Ivanti Neurons for Service Mapping cloud (depicted as “Discovery Server”).

Port Requirements



Authentication Requirements

As part of the Discovery App installation, customers enter the appropriate credentials for the types of systems to be scanned. These credentials are stored and encrypted locally within the DA Windows Server and never go to the cloud. Table 6 lists the most common types of credentials and communication methods required for the probes to successfully scan each asset type. Note, the list may not be inclusive of requirements and is subject to change.

Unless specifically referenced below, do not assume a specific asset or hardware type is discoverable with out-of-box-probes. Always confirm with Ivanti prior to purchase that something is supported or Ivanti is committed to add. Otherwise, Ivanti assumes no responsibility or obligation to discover unsupported asset types.

Table 6: Discovery Credential and Port Requirements

Asset Type	Method	Port/Protocol	Authentication Method	Notes
Windows (Batch method) *see note above)	Batch scripts with WMI commands and PAExec from Disc. App.	TCP: 135, 139 (WMI) and 445 (File and Print sharing) UDP: 137,138	Windows admin credentials with elevated privileges	Elevated privileges required for relationship discovery WMI and PAExec is required to push Windows Discovery Agents via the Discovery App.
Windows (PS remoting method)	PowerShell from Disc. App.	Port 5985	Windows username/password	PS-Remoting must be enabled on target hosts and Discovery App
Unix, Linux, Mac, Solaris	SSH from Disc. App.	22 (SSH)	SSH username/ password or private keys	Update the sudoers file to not require TTY. Requires SUDO on netstat or SS command to fetch IP connections. SUDO dmidecode required to fetch serial number. SNMP will not discover relationships
Network Infrastructure (via SSH)	SSH (Cisco CDP) from Disc. App.	22 (SSH)	SSH User ID/password	SSH required to discover relationships.

Asset Type	Method	Port/Protocol	Authentication Method	Notes
SNMP(Network Infrastructure, Windows, Linux, misc. edge devices)	SNMP from Disc. App.	161 (SNMP)	Community String (v1, v2) or User ID/password (v3)	SNMP does not provide sufficient capability to discover relationships for any device type so other methods are preferred.
AWS resources	API from cloud UI	443/80	Account ID, AWS access key, secret key, account ID	See *AWS IAM Policy* below, EC2 OS details require server discovery scan
Azure resources	API from cloud UI	443/80	Account ID, client ID, tenant ID, secret key	See *Azure Role Setup* below, Virtual machine details require server discovery scan
VMware vCenter	API from Disc. App.	443/80	VCenter SSO User ID and password	This will discover ESXi hosts managed by vCenter
ESXi Hosts	SSH from Disc. App.	22 (SSH)	SSH Host Credentials	For standalone ESXi host discovery
Active Directory	WMI/API	135, 88	AD host, Domain, Base DN, Bind DN, Password	Domain admin required
MS SQL Database	WMI from Disc. App.	1433, 1434	Windows or SQL Server account	Requires SQL server credential profile with user read rights on the sys.databases table
MySQL	SSH from Disc. App.	22	MySQL User with SHOW DATABASES Privilege	Allow remote MySQL access. Ensure firewall rules allow MySQL traffic.
MMC Certificates	WMI and PowerShell from Disc. App.	135, 137, 138, 139 (WMI) and 445 (file/print sharing)	Windows admin credentials with elevated privileges	Requires enabling PowerShell scripting
TLS/SSL Certificates	WMI from Disc. App.	443	Windows admin credentials with elevated privileges	Certs that reside on a server can be discovered. E.g. if port 443 is open on a server, it is assumed it contains an SSL cert which Ivanti Neurons for Service Mapping tries to retrieve from the port query
IIS Websites	WMI from Disc. App.	135, 137, 138, 139 (WMI) and	Webserver credentials	Requires IIS Management Tools installed with IIS Management Scripts and Tools selected

Asset Type	Method	Port/Protocol	Authentication Method	Notes
		445 (file/print sharing)		
Cisco Meraki	API from cloud UI	443/80	API key	Requires Meraki Cloud Dashboard API access
Oracle DB	WMI/ PowerShell/SSH from Disc. App	Default Port: 1521 (TCP) and Configurable SSH (Linux) or WMI/WinRM (Windows)	Windows/ Linux Username, Password	Process access to list/read Oracle processes File read access to Oracle configuration files Command access to run sqlplus and lsnrctl.
NetApp Storage Server (Beta)	ONTAP REST API from Disc. App	443	Username, Password	Requires reachable API endpoints and valid credentials.
HP MSA Storage (Beta)	API from Disc. App	443	Username, Password	Ensure the HP MSA server and all required REST API v2 endpoints are reachable (online and responding) before initiating API-based discovery of HP MSA arrays.
Nutanix (Beta)	API, SSH from Disc. App	9440, 22	Username, Password	Requires reachable API endpoints and valid credentials if Scans via APIs Ensure port 22 is open and valid credentials are available if scans via SSH.
CCM	PowerShell Script	5985	Username, Password Site code	SCCM site server and SQL Server are installed, reachable, and healthy. Required ports are open between clients, site system roles, and SQL (per your topology). DNS/AD are configured properly; time sync is correct. Proper service accounts/permissions and valid client push/admin credentials are available. Boundary groups and networking (subnets/VPN) are defined for client assignment and content.
Intune	API from cloud UI	443/80	Client ID, tenant ID, secret key	See Microsoft Intune setup below
JAMF				

***Note on scanning Windows OS via Batch (WMI and PAExec):** The Discovery App will copy a few files to the Windows admin$ share and then launch a local service with the credentials provided. It will scan the system with all the probe details. Once the scan is complete, it will stop and remove the service and files from the admin$ share folder. For this to work, the account being used must have remote file access to the admin$ share, have admin rights on the box being scanned, and must have Log on as a service right on the local Windows machine.

AWS IAM Policy

To allow the importing of AWS objects into the CMDB the following must be done within the AWS account. Note: EC2 operating system discovery is performed via the Discovery App per the Windows/Linux/Unix methods listed in the Authentication Requirements Table above.


```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ecr:Describe*",
"ec2:Describe*",
"rds:Describe*",
"elasticloadbalancing:Describe*",
"autoscaling:Describe*",
"iam:GetUser",
"dynamodb:Describe*",
"s3:ListAllMyBuckets"
],
"Resource": "*"
}
]
}
```

Azure Role Setup

To allow the importing of Azure objects into the CMDB the following Azure Role Setup must be performed.

> ***Note:*** *Azure Virtual Machine operating system discovery is performed via the Discovery App per the Windows/Linux/Unix methods listed in the* Credential Requirements Table *above.*

Register an Application in Azure

1. Go to "***https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade"***.
2. Create a new app registration
3. From the **Overview** section, copy and save the following details:
    a. **Client ID** (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)
    b. **Tenant ID** (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)
    c. **Secret Key-Value** (Needs to be created from Certificates & Secrets) (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)

Assign a Role in Azure Subscription

1. Go to "***https://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade"***
2. Copy and save the **Subscription ID** (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)
3. Open the subscription details and navigate to **Access Control (IAM)**
4. Select **Add** and then click on **Add Role Assignment**
5. Select **Reader** as the role and click **Next**
6. Click **Select Members**, then search for the newly registered app. Select it and click **Select**
7. Review and assign the role

Microsoft Intune Setup (via Azure App Registration)

To import Microsoft Intune objects into the CMDB, the Intune discovery must be configured using an Azure App Registration with the required Microsoft Graph permissions.
Note: Azure VM operating system discovery is performed through the Discovery App using the standard Windows/Linux/Unix authentication methods listed in the Authentication Requirements table.

1. Go to https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade and create a new App Registration and note down the below details from Overview

- **Client ID** (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)
- **Tenant ID** (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)
- **Secret Key-Value** (Needs to be created from Certificates & Secrets) (Required in Ivanti Neurons for Service Mapping to add Azure Credentials)

2. Assign Microsoft Graph permissions for Intune
   - App registration → API permissions → Add a permission → Microsoft Graph
   - Add the required permission(s) to read Intune devices (e.g., Intune device read scope).
   - Click Grant admin consent after adding permissions

Additional Considerations

This document is intended to help ensure the proper scoping and sizing of Ivanti Neurons for Service Mapping Discovery applications. The information provided covers most customer environments and will help identify any possible exceptions that should be addressed early in the sales or professional services engagement.

Learn More


ivanti.com


1 801 308 8047 (Americas Support)


support@ivanti.com