NTT DATA

Inventory Discovery Technical Service Description

Overview of Service

Inventory discovery is an initial step during Consulting Engagements and Managed Service Offerings, which will help to baseline and document the client network inventory. The discovered inventory will be an important input for designing the new proposals and services to the client.

The service is designed to connect to client estate remotely and auto discover the multi-vendor network equipment within the client's estate, replacing the slow and error-prone manual process of gathering the inventory details from the client. Getting an up to inventory of client estate has been a challenge most times and this service can provide an accurate and up to date device inventory report within a short time.

Scope of Service

Description: Inventory Discovery Service scans the client network remotely to create a detailed report of the client network inventory.

Details:
- Cloud-based discovery portal controlled by role-based access to remotely initiate Inventory Discovery
- Supports multi-vendor inventory discovery and discovers devices managed by the following technology types:
  - Non-controller Devices
  - On-premises Controller
  - SaaS Controller

Outcome:
- Detailed report of the up-to-date inventory list of client estate for the following technology types:
  - Non-controller Devices
  - On-premises Controller
  - SaaS Controller

Benefits (to client):
- Automated process to discover devices on the organization's network
- Improve time taken to collect inventory details during pre-sales and transition phase.
- Faster onboarding of devices to Managed Campus Platform.
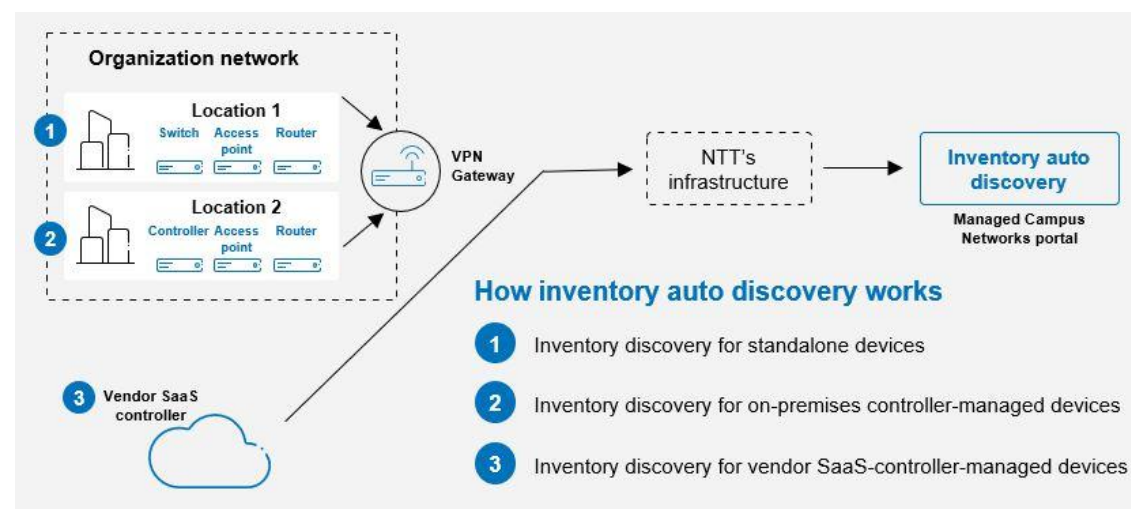
Client Responsibilities and Prerequisites

NTT requires the following in order to deliver the service.
- Active service contract with NTT for the Campus Network environment
- Remote Access - OpenVPN connectivity to client estate to execute the discovery job from MCN portal. This is a pre-requisite for non-controller and on-premises controller managed devices.
- Simple Network Management Protocol (SNMP) must be enabled and configured for devices to be discovered
- Additional Information required from client depends on the technology used by client and this is captured in the Statement of Work
- Additional information required includes IP address, SNMP credential for non-controller devices to controller access credentials for on-premises and SaaS controller

Service Requests

As part of the Service, the fulfilment of the tasks listed in the table below are included.

Inventory Discovery Service Requests

Task	Description	Included
Not Applicable	None defined.	❌

Supported Technologies

The scope of this service includes support for the following technologies

1. Non-Controller Technology
   - o Standalone devices not managed by controller
   - o Discovery Mechanism: ICMP and SNMP Walk
   - o Supported Devices: Routers, Switches, AP, WLC, Firewall
2. On-Premises Controller
   - o Devices managed by Controller deployed on customer premises
   - o Discovery Mechanism: API call
   - o Supported Controllers: Cisco DNAC
3. SaaS Controller
   - o Devices managed by cloud controllers
   - o Discovery Mechanism: API call
   - o Supported SaaS controllers: Juniper Mist

Tasks Associated with Service

The following tasks are included in the service fee.
- Readiness assessment, gathering of Client environment information
- Verify the remote connectivity to client environment using the VPN profile file provided by client
- Initiate remote discovery of devices in client estate

The following tasks are excluded from the service fee.
- Any local installation of inventory discovery tool
- Any associated hardware or software licensing
- Any activity on the device, outside of tasks defined in the run book

Service Exclusions

For the avoidance of doubt, the following tasks and deliverables are not included as part of the MCN Inventory Discovery services.
- Any advanced reporting services including patch and vulnerability assessment, configuration compliance.