Managed Cisco Catalyst Center

(part two: automated operations)

Part two of this white paper covers the role of Managed Cisco Catalyst Center* in automated operations and how we use it in Managed Campus Networks.

In part one of this white paper, we set out how network technology is becoming much more software-defined and controller-driven, creating the ideal environment for Cisco's Catalyst Center to manage network operations in an efficient, automated and centralized way.

NTT's Managed Campus Networks platform then integrates these evolving, cloud-native network technologies to offer an improved managed service offering, including our Managed Cisco Catalyst Center service.

Alongside the monitoring-related benefits of this service, covered in part one, organizations can benefit from greater automation, and this is what we discuss here.

*Catalyst centre is formerly known as DNA Centre (DNAC)

Contents

Introduction 01

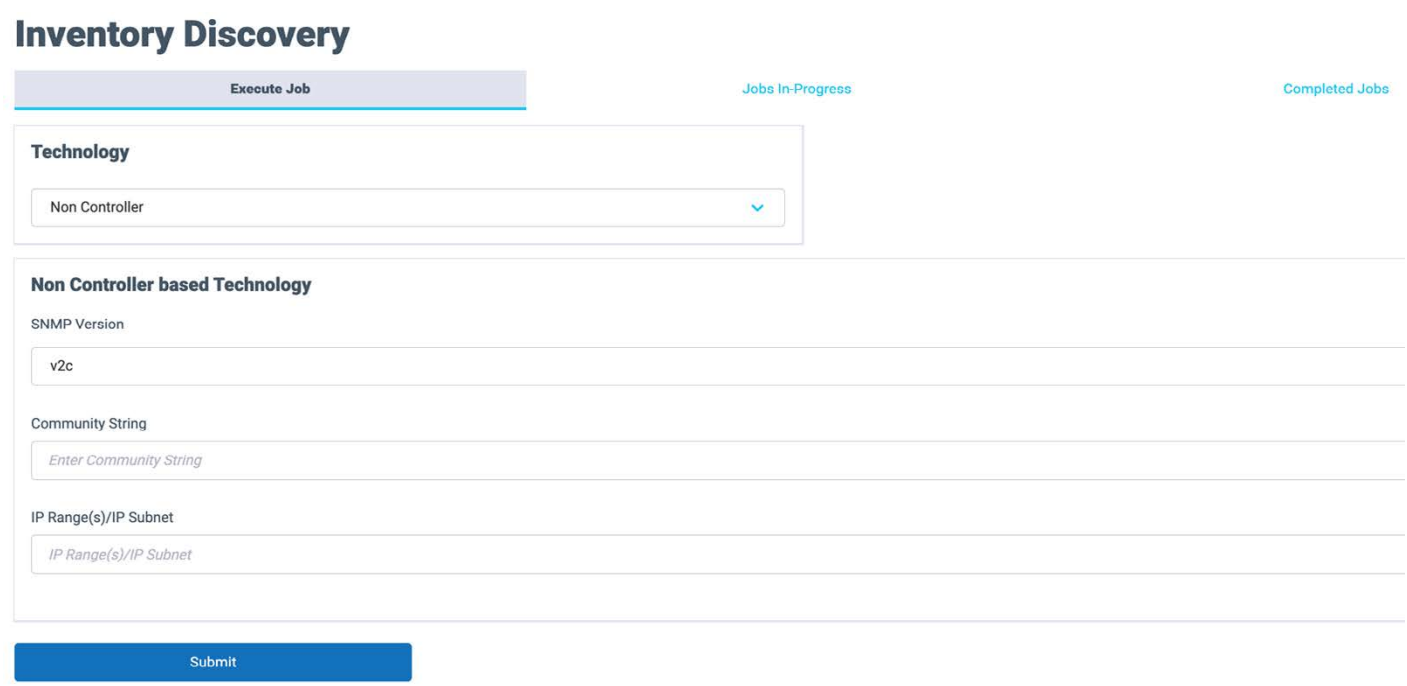
Automated Operations 03

Managed Cisco Catalyst Center: SWIM 07

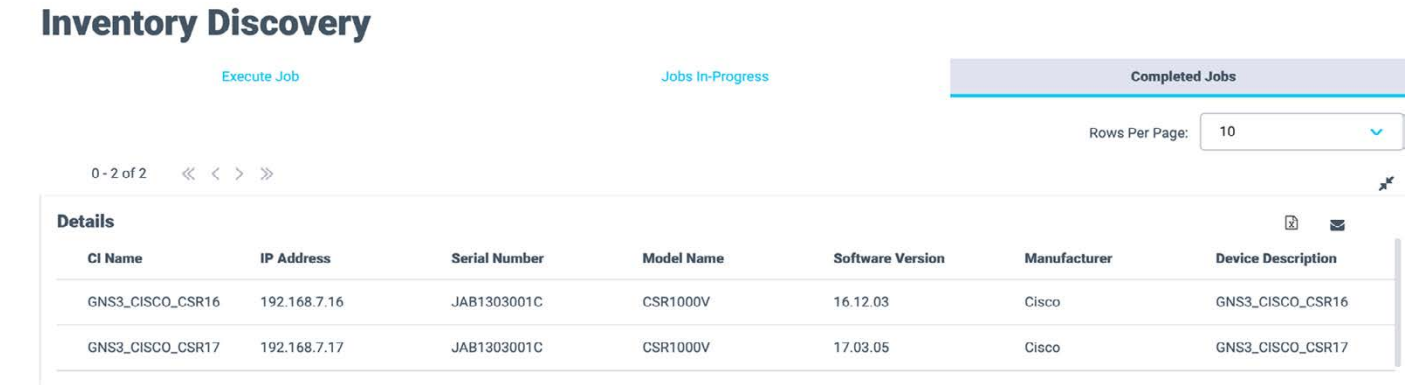
Automated operations

Our Managed Campus Networks platform provides a suite of process and runbook automation capabilities used in service delivery. The automated operations available on the platform include:

1. **Automated inventory discovery:** This feature allows engineers to discover devices in the network and easily add them to the service. It supports the discovery of both controller devices (such as on-premises controllers like Catalyst Center or cloud-based controllers like Cisco Meraki) and noncontroller devices. It uses Simple Network Management Protocol (SNMP) to cover devices within a specific IP range as well as application programming interface (API) calls to a controller to discover the devices it manages.

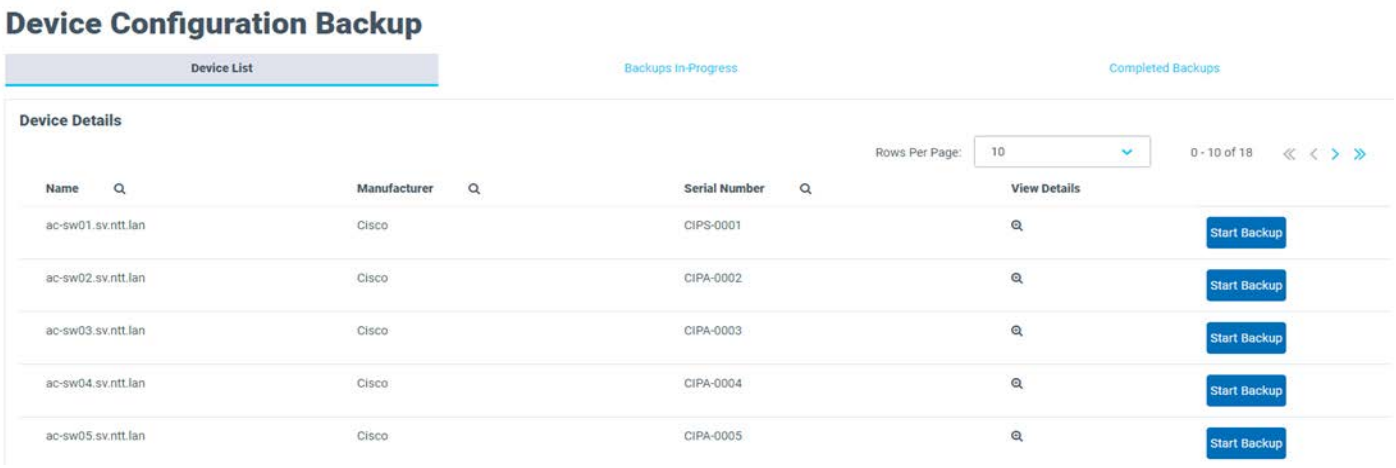


The client portal displays a list of discovered devices, their model details and other information such as the device name, its IP address, its serial number and the operating-system version. The platform will maintain a record of past discoveries on a particular network.



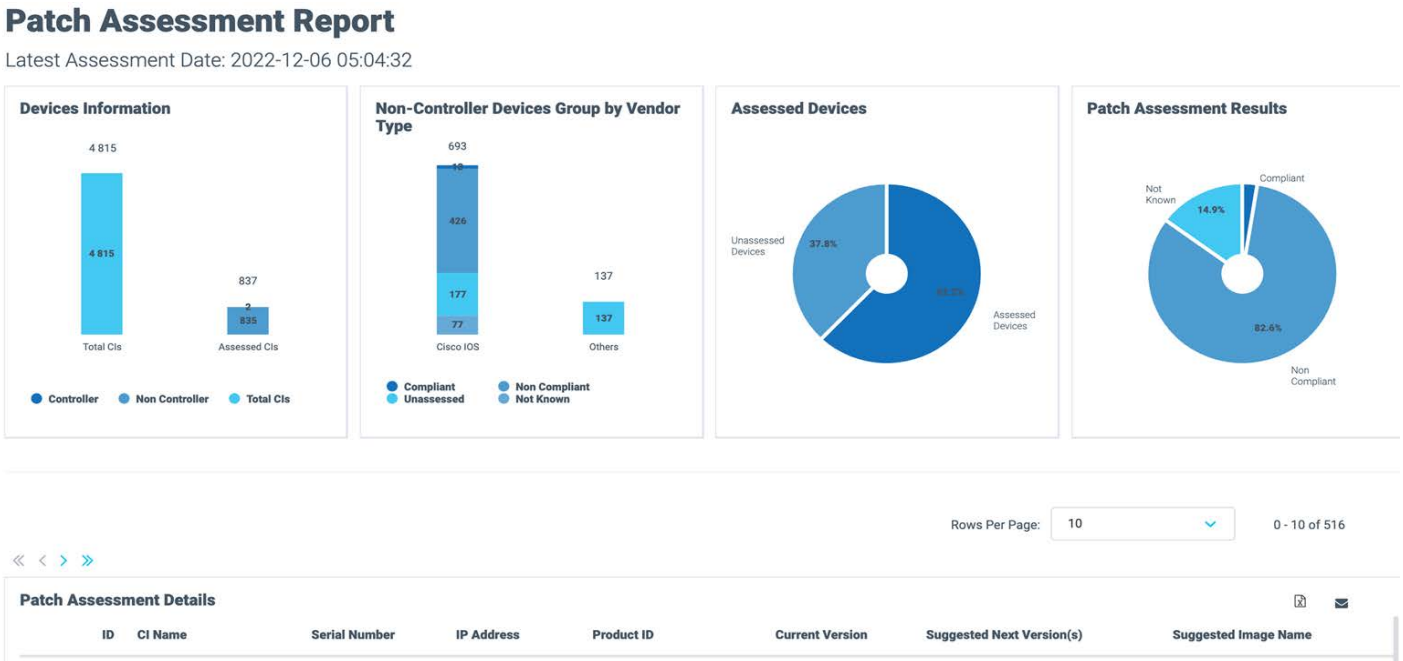
2. **Automated backup:** This capability automates the on-demand backup of devices and generates an event in case of device backup failure during periodic or on-demand backup operations. Automating configuration-backup failure detection is critical for service continuity, as it ensures that the latest device configuration is available in case of unexpected failures. Failure of the configuration backup will generate an incident for the operations team to handle.

The portal also supports executing on-demand backup, which the operations team can action before performing any changes to the system configuration.



Device configurations are backed up on NTT's cloud-based managed services platform, in client-provided storage or in an edge backup repository, depending on the device type and backup option that was selected. On completion of the backup, the portal will display the status of the backup. It also gives an option to view the differences between backup versions, in the case of text-based configuration.

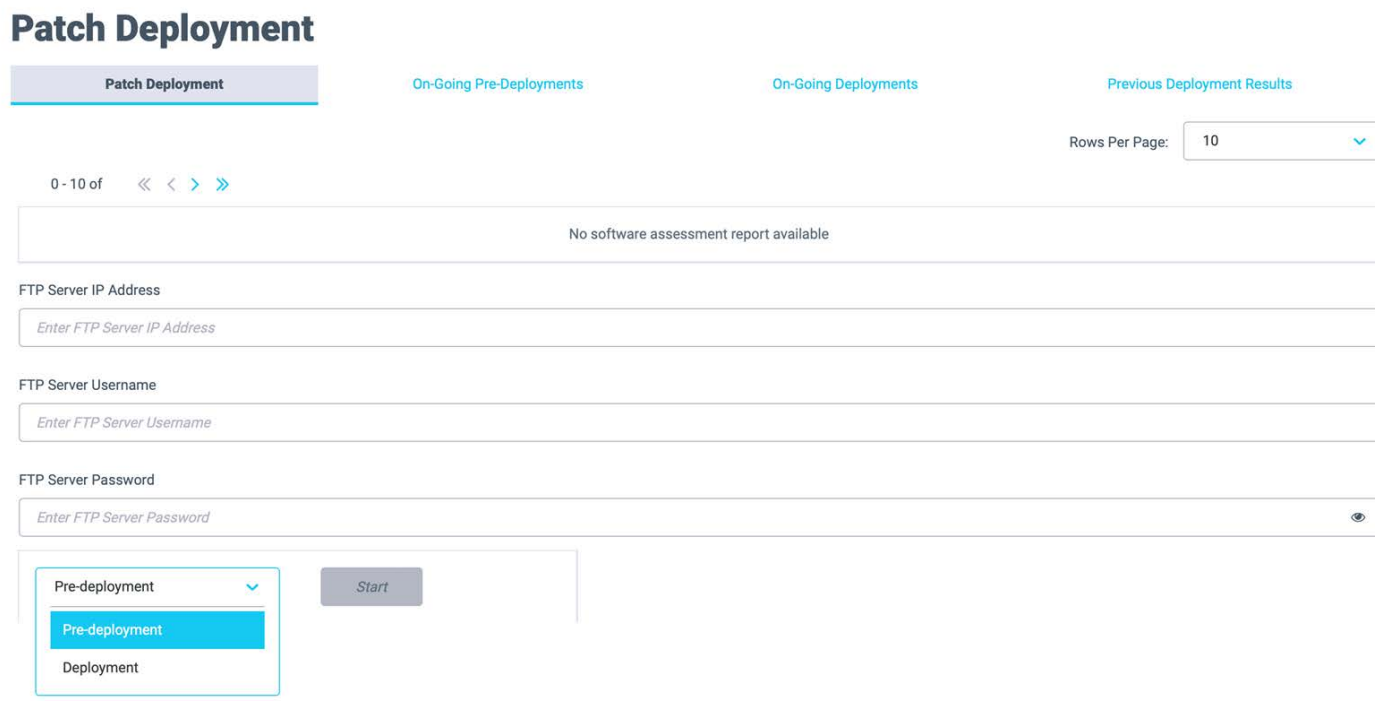
3. **Automated lifecycle management (patch assessment and deployment):** Our platform allows clients to automate the assessment of their devices and software. By performing regular software assessments, the platform can discover and list the software version running on each device, and make recommendations on which software is available for an upgrade.



 © Copyright NTT Ltd.

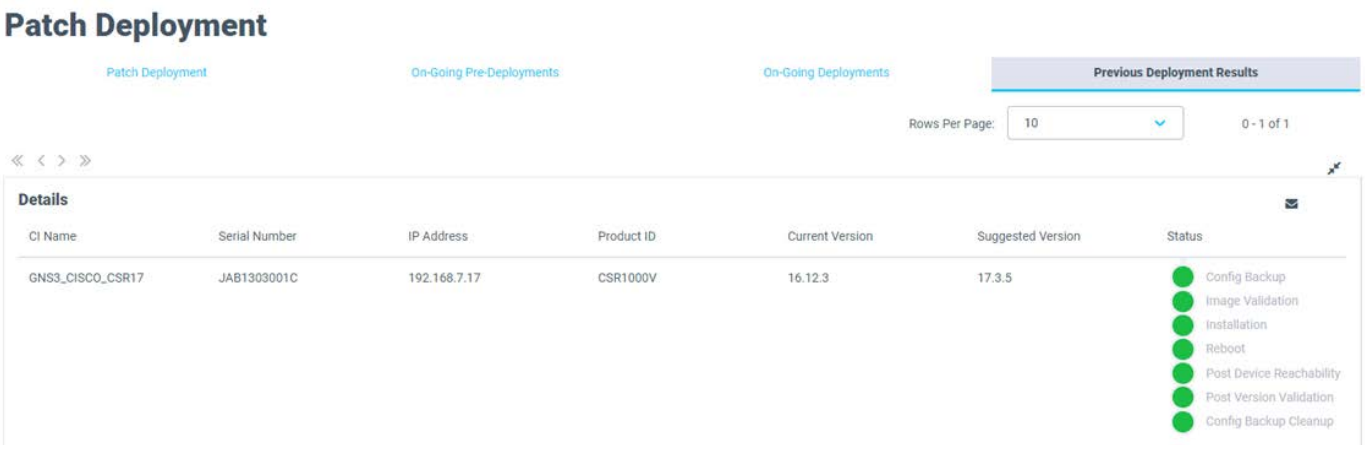
The patch-assessment feature provides a comprehensive assessment of the devices in the network and their software categories and installed versions. For each device, it provides the suggested version for an upgrade and the suggested image to use for the upgrade. It also gives a summary of the infrastructure readiness for these upgrades, in terms of the storage and memory required by each image, and whether a device meets these requirements.

Engineers can then use the automated patch-deployment feature to do prechecks before the patch upgrade.



The predeployment checks will scan for any issues that might derail software updates on a device. These checks include determining the device's health, whether it has the required amount of storage and memory, and whether there are any pending changes to be done on the device before the software update.

The platform then executes the patch upgrade on the target devices selected by the engineers, using the parameters provided by an engineer (target operating-system version, image to use and so forth). It concludes with a summary of the upgrade.



4. **Vulnerabilities assessment:** Another important area in automated operations is the ability to continually check the network for vulnerabilities and provide vendor advisories for any vulnerabilities found.

The platform will execute the assessment regularly (users can configure how often these assessments are run) and produce a report on the vulnerabilities it identifies, along with the advisories published by the technology vendors for each of these vulnerabilities.

The vulnerabilities will be categorized depending on their severity. Those with a critical severity will be automatically assigned in a ticket to the operational engineer, and the client will be notified. The client can then, with our assistance, decide how and when to mitigate these vulnerabilities.

Another important area in automated operations is the ability to continually check the **network for vulnerabilities and provide vendor advisories for any vulnerabilities found.**

 © Copyright NTT Ltd.

Managed Cisco Catalyst Center: SWIM

The Software Image Management (SWIM) module of the Cisco Catalyst Center platform allows network administrators to manage software images across their network devices.

So, they can automate the processes involved in upgrading, downgrading or installing new software images on network devices, thereby improving the network's performance with less danger of downtime.

Key features of Cisco Catalyst Center SWIM include:

1. **Centralization:** Network administrators can manage software images for multiple network devices centrally, making this a simpler task.
2. **Image compatibility checks:** Before deploying a new software image, SWIM checks for compatibility with network devices and current software images, to avoid possible network downtime.
3. **Image version control:** It tracks the version of software images installed on every network device, giving administrators a full view across the network.
4. **Rollback:** Administrators can easily roll back to a previous version of a software image should a compatibility issue or other problem arise.
5. **Scheduling:** Network administrators can schedule software image upgrades or downgrades. This means less hands-on intervention and makes it possible to deploy updates in off-peak periods.

Our Managed Campus Networks platform integrates with Catalyst Center and uses the SWIM features to provide a reliable way of managing the software lifecycle of Cisco devices under Catalyst Center management.

Using our platform along with Catalyst Center for automated operations will ensure that:

- Operational changes are aligned with the overall Information Technology Infrastructure Library (ITIL) processes and in line with client processes.
- There is integration with other tasks and changes in the network estate.
- Bulk operation executions are of high quality.
- Vulnerabilities and anomalies are automatically discovered and communicated to engineers who can take preventive action.

These are all powerful tools for any organization to use, and deliver speed, reliability and security in the network in support of business goals.

Network Assessment

Take our Network Assessment now to gain a deeper understanding of your network requirements and embark on your digital transformation journey.

 © Copyright NTT Ltd.


NTT