

Managed Cisco Application Centric Infrastructure Technology Service Description

Overview

Cisco Application Centric Infrastructure (ACI) devices managed under the Managed Campus Network offering will be supported in accordance with the NTT processes described in the *MCN Statement of Work*. Technology specific tasks associated with the Cisco ACI technology stack are described in this document and includes the following:

- Cisco APIC controllers
- Cisco 9K Spine Switches
- Cisco 9K Leaf Switches
- ACI software

Further detail on these Service offers can be found in their specific sub-sections.

Client Responsibilities and Prerequisites

In addition to the pre-requisites documented in the MCN Statement of Work, the following technology specific pre-requisites are applicable.

The Client is responsible for the following and must ensure that these pre-requisites are met as part of the MCN offering:

Technology Specific Operations

Monitors

Monitoring will be performed in accordance with the process described in the Event Management section of the *MCN Statement of Work*. The monitoring will be for the network infrastructure and not of the fabric overlay workload with the exception of the APIC hypervisor which is monitored as defined in the table below. This is because the APIC appliance is an all-in-one solution that includes the hardware, the hypervisor and the operating software.

The following monitors can be configured by default for Managed Cisco ACI:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Fabric Node Health	15 min fabric node health measurement	✔	Obtains information about fabric node health	Engineering Teams will troubleshoot and solve the issue	600
Fabric Pod Health	15 min fabric pod health measurement	✔	Obtains information about fabric pod health	Engineering Teams will troubleshoot and solve the issue	600
Leaf/Spine Device Availability	Up / down status of the device	✔	Obtains information about the device availability.	Engineering Teams will troubleshoot and solve the issue	600

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Cisco APIC Hypervisor	Status information for compute hypervisor within the fabric	✓	Status information for compute hypervisor deployed within the fabric.	Engineering Teams will troubleshoot and solve the issue	600
Cisco APIC Interfaces	Interface performance measurements	✓	Obtains information about interface performance.	Engineering Teams will troubleshoot and solve the issue	60
Cisco APIC CPU	System CPU usage from the APICs	✓	Obtains system CPU information.	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.	600
Cisco APIC Memory	System memory measurements	✓	Obtains system memory information.	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.	600
Cisco APIC Storage	Storage measurements via the APIC API	✓	Obtains storage information.	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if storage is provided by Client.	600
Cisco APIC Virtual Machines	Measures status of the VMs deployed within the fabric	✗	N/A	N/A	N/A

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description.

Cisco ACI supports traditional external storage options via a physical server or virtual machine (VM) on private or public cloud. All the changes to the configuration can be checked using the configuration audit menu from within the Cisco ACI portal. THE ACI Change Log allows checking of all changes executed and can be helpful for basic troubleshooting and manual changes on individual Client requests.

A weekly backup can be scheduled to export the entire Fabric configuration to a remote location (i.e., external server) using SCP, FTP, or SFTP for which an external local storage location (client provided) is required for this functionality. The ACI backup policy will be configured using the APIC backup and restore engine and should therefore be reviewed during the initial transition.

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- Only vendor validated platforms and configurations as defined in the [ACI Virtualization Compatibility Matrix](#) are supported under the offering.

- The Managed Cisco ACI Service will utilize the Cisco ACI GUI for remote administration and operational insights. The GUI provides a management interface enabling the following Service functions (Client read-only access is available for Client-approved individuals):
- System to collect and display a summary of the overall system health, its history, and a table of system-level faults:
 - Overview of system health
 - Configuration of global system policies
 - View of licenses status
 - View of active user sessions
- Tenants to manage the configuration of tenants. Default tenants include:
 - Common Tenant: Manages policies that are common to all tenants in the fabric.
 - Infra Tenant: Manages the configuration of the fabric infrastructure.
 - Management Tenant (preconfigured for in-band and out-of-band connectivity configurations of hosts and fabric nodes i.e. leafs, spines, and controllers).
 - Additional tenants (supported as part of the Client specific design).
- Fabric for the configuration of the fabric and is supported as part of the Managed Cisco ACI Service. This includes:
 - Inventory of the individual components of the fabric
 - Monitoring and troubleshooting of fabric policies and fabric protocol settings or fabric maximum transmission unit (MTU) settings.
 - Access Policies displaying the access policies that apply to the edge ports of the system. These ports are on the leaf switches that communicate externally.
- Layer 4 – 7 Services
 - Inventory of L4 – L7 devices (such as firewalls, SSL offloads, load balancers, SSI termination devices, or intrusion prevention systems (IPS)).
 - Import L4 - L7 device packages to implement, configure, and monitor a network service device that are prescribed by the client.
- The Managed Cisco ACI offering includes platform specific administrative functions such as:
 - the configuration of authentication, authorization, and accounting (as applicable per design)
 - scheduling policies
 - retaining and purging records
 - controlling features such as syslog, Call Home, and SNMP.

Limitations

- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual ACI appliances.

Service Requests

A list of service requests available for this technology can be found in the MCN Request Catalogue.

Below is a non-exhaustive list of change requests that have been deemed complex and therefore specifically excluded the list of service requests:

- L4 – L7 Service integration
- Service Graph design and implementation.
- VMM or container domain integration
- inter-pod network (ipn) connectivity re-design
- ACI AppCenter testing and app deployment.
- northbound communications from APIC to operation support systems (oss), automation systems and programmatic platforms for data extraction

Technology Transition Tasks

In addition to the standard transition tasks described in the MCN Statement of Work, the following technology specific transition tasks are included:

- Design verification of the ACI environment (required prior to transition to Day 2 management). This will enable knowledge transfer of the existing environment and provide a detailed review of tenants, EPGs, bridge domains, naming conventions, addressing, VRFs, and VLANs.
- Initial configuration of a Cisco ACI on-premise backup strategy

Note:

Any tasks not explicitly described under the Technology Transition Tasks are implicitly excluded from transition.
