Software Defined Access (SDA) Provisioning Best Practice Guide

Contents

Introduction

This article lists the various pre-checks, dos & dont's the user can folllow to avoid the pitfalls while provisioning Software Defined Access (SDA) Fabric through Cisco DNA Center. Here is the list of provisioning use cases and check list.

1. Device Provisioning:

1. Make sure the device is reachable and in Managed state in Cisco DNA Center inventory Application.
2. Check the network design page and make sure the corresponding site level settings (credentials, AAA server) are preserved.
3. Check if there is any Fabric level provisioning operation is on going on the Fabric site where the device is attached to.
4. Make sure Cisco ISE(Identity Service Engine) integration is active and there is aNetwork Access Device (NAD) created for this device in Identity Services Engine (ISE).
5. Check and make sure the provisioning status is not in "Configuring" State.
6. If you want to change the management IP address of the device, change it first on the Cisco DNA Center Inventory page. Then, change it on the device. To avoid any IP address conflicts, resynchronize the Inventory page (**Inventory > Resync Device**).
7. Confirm that the devices in the fabric are not sending traps, such as LINK_UP or LINK_DOWN.
8. Before performing any provisioning or fabric operation, review the scale limits in the [Cisco DNA Center Data Sheet](#).

2. SDA Fabric devices Add/Remove/Edit Provisioning

1. Make sure the device which you need add/remove is reachable and in Managed state in Cisco DNA Center's inventory app.
2. Make sure the device is still part of the network before you remove the device from the Fabric.

3. Check if there is any Fabric level provisioning operation is on going on the Fabric site where the device is attached to.
4. In case of a border/Control plance devices removal, replacement, make sure all the edge devices were reachable and Managed state in DNA Center inventory application.
5. If there is any previous Fabric wide provisioning failure in few of the devices, reprovision those devices so that the latest fabric configuration will be pushed to all the devices.
6. Please do not try to remove the device from the Cisco DNA Center's inventory app until the device got removed from the Fabric. Do not use the inventory API to remove the device from the inventory. Inventory APIs will not clean up the Fabric data from the switch as well as Cisco DNA Center's DB(DataBase).
7. As of 1.3.3.x, there is no support for Fabric device Return Merchandise Authorization (RMA) in Cisco DNA Center. The best way to RMA a border or edge node is to remove it from the fabric and use the RMA work flow to replace the device and add it back to the Fabric.
8. Do not include unreachable devices as part of the fabric.
9. Before adding a device to the fabric, confirm that the device or interface does not have a fabric-related configuration, including a switch port configuration.
10. Clear the device config manually before you add the device to the fabric. If you remove an unreachable device from the fabric, the configuration is retained on the device.
11. Confirm that any user-defined template configuration does not interfere with the fabric configuration.
12. Removing a device from the inventory does not clear any configuration provisioned via a template.
13. To prevent provisioning latency or failure, do not use a command-level authorization configuration in fabric devices in a scaled environment.
14. Do not reprovision a device while a fabric-wide provision operation is in progress.
15. Do not configure any fabric-related manual configuration on a device.

3. VitualNetwork - IP pool provisioning

a. Check the Design page and make sure the IP pool reservation is getting displayed in the UI and make sure the used percentage value is correct.

b. If VirtualNetwork-IP pool association provisioning operation Failed for any device in the Fabric, check for the reason and try to reprovision those failed switches before moving to the next provisioning.

c. If any IP pool is not getting listed when you add a segment, check the design Ip pool reservation page and make sure it is not 100% used.

d. Do not add/remove/edit Fabric border/edge devices while VN IP pool provisioning is in progress in the particular Fabric.

e. Before removing any SGT (Scalable Group Tag) from the VN page, check whether it is getting used in any of the existing VN-IP pool association.

e. Before removing any IP pool, check and make sure it is not getting used in any of the static port assignment.

4. Host onboarding - Port Assignment

a. Check and make sure all the access ports are getting displayed for the device. Otherwise, we need to check the switch or Cisco DNA Center inventory app.

b. If few of the interfaces are not getting displayed, check the SDA compatibility matrix and make sure the device is supported (SDA Compatibility Matrix).

c. If you see any discrepancy on the port assignment in the Fabric compliance page, reprovision the port(clear and configure) from Cisco DNA Center during a Maintenance Window and re-check the compliance.

5. LAN Automation

1. Before starting LAN automation, follow the steps in the Cisco DNA Center SD-Access LAN Automation Deployment Guide.
2. If a LAN automated device is deleted from Cisco DNA Center, add it back via LAN automation. Do not add it back via the Inventory or Discovery pages.
3. Do not modify the LAN automated interface configuration in the device manually, including Loopback0 or Loopback60000.
4. Do not move the LAN automated L3 interface configuration from one interface to another interface or from one device to another device manually.
5. Do not use an IP address from the underlay pool for any other purpose in the network. Use a dedicated pool for the underlay
6. Confirm that the PnP agent serial number does not already exist in the ISE NAD and in the PnP page.