

ASML - ACI Nexus Dashboard (ND) - SDD

January 26, 2024

Version 0.2

Cisco Systems, Inc.

Corporate Headquarters

170 West Tasman Drive

San Jose, CA 95134-1706 USA

Phone: +1 408-526-4000

Toll Free: +1 800-553-NETS (6387)

Fax: +1 408-526-4100

**Document Classification**

**Cisco Highly Confidential**

Contents

[Contents 2](#_Toc256000070)

[List of Figures and Tables 4](#_Toc256000071)

[About This Document 5](#_Toc256000072)

[History 5](#_Toc256000073)

[Review 5](#_Toc256000074)

[Document Conventions 5](#_Toc256000075)

[1 Introduction 7](#_Toc256000076)

[1.1 Preface 7](#_Toc256000077)

[1.2 Audience 7](#_Toc256000078)

[1.3 Scope 7](#_Toc256000079)

[1.4 Assumptions 7](#_Toc256000080)

[1.5 Related Documents 8](#_Toc256000081)

[2 ASML Network Overview 9](#_Toc256000082)

[3 Nexus Dashboard Overview 10](#_Toc256000083)

[3.1 Nexus Dashboard Form Factors 10](#_Toc256000084)

[3.2 Cluster sizing 11](#_Toc256000085)

[3.3 Site Management 11](#_Toc256000086)

[3.4 Cluster Connectivity 11](#_Toc256000087)

[3.4.1 ND connectivity to ACI via L2 connection 11](#_Toc256000088)

[3.4.2 ND connectivity to ACI via L3Out 12](#_Toc256000089)

[3.4.3 Communication Considerations 14](#_Toc256000090)

[3.4.4 Communication to Cisco Intersight 15](#_Toc256000091)

[4 Nexus Dashboard Applications 16](#_Toc256000092)

[4.1 Nexus Dashboard Insights 16](#_Toc256000093)

[4.1.1 NDI Overview 16](#_Toc256000094)

[4.1.2 Nexus Insights Flow Collection 17](#_Toc256000095)

[4.1.3 Nexus Dashboard Insights Telemetry Collection Capabilities 18](#_Toc256000096)

[5 ASML Nexus Dashboard Deployment Information 20](#_Toc256000097)

[5.1 Nexus Dashboard prerequisites in ACI 20](#_Toc256000098)

[5.1.1 ACI in-band management IP addresses 20](#_Toc256000099)

[5.1.2 In-band management VRF L3out 21](#_Toc256000100)

[5.1.3 Precision Time Protocol 21](#_Toc256000101)

[5.1.4 DOM and Feature selection 21](#_Toc256000102)

[5.2 Cluster Details 23](#_Toc256000103)

[5.2.1 Software 25](#_Toc256000104)

[5.2.2 VM deployment 25](#_Toc256000105)

[5.3 Nexus Dashboard cluster configuration 26](#_Toc256000106)

[5.4 Connecting Nexus Dashboard to Cisco Intersight 27](#_Toc256000107)

[5.5 User authentication 29](#_Toc256000108)

[5.6 Onboard sites 29](#_Toc256000109)

[5.7 Scaling and Compatibility References 30](#_Toc256000110)

[6 Installing and configuring NDI 31](#_Toc256000111)

[Trademarks and Disclaimers 32](#_Toc256000112)

[Document Acceptance 33](#_Toc256000113)

List of Figures and Tables

[Figure 1 ASML ACI Physical Design 9](#_Toc256000114)

[Figure 2 Nexus Dashboard Applications 10](#_Toc256000115)

[Figure 3 Nexus Dashboard Connectivity to ACI via EPG 12](#_Toc256000116)

[Figure 4 Nexus Dashboard Connectivity to ACI via L3out 13](#_Toc256000117)

[Figure 5 APIC Connectivity Preferences 20](#_Toc256000118)

[Figure 6 Precision Time Protocol 21](#_Toc256000119)

[Figure 7 Fabric Node Controls 22](#_Toc256000120)

[Figure 8 Create Leaf Switch Policy Group 22](#_Toc256000121)

[Figure 9 Leaf Switch Profile 23](#_Toc256000122)

[Figure 10 ND System Settings 27](#_Toc256000123)

[Figure 11 Connection to Intersight 28](#_Toc256000124)

[Table 1 ASML Site Locations 7](#_Toc256000125)

[Table 2 Assumptions 7](#_Toc256000126)

[Table 3 Related Documents 8](#_Toc256000127)

[Table 4 Nexus Dashboard RTT Requirements 14](#_Toc256000128)

[Table 5 Nexus Dashboard Communication Ports 14](#_Toc256000129)

[Table 6 NI Flow Collection Rules 18](#_Toc256000130)

[Table 7 ACI <fabricName> in-band management IP Addresses 20](#_Toc256000131)

[Table 8 Nexus Dashboard Clusters Summary 24](#_Toc256000132)

[Table 9 Nexus Dashboard Cluster Parameters 25](#_Toc256000133)

[Table 10 Recommended versions 25](#_Toc256000134)

[Table 11 VM requirements 25](#_Toc256000135)

[Table 12 Virtual ND sizing chart 26](#_Toc256000136)

[Table 13 Network Scale 26](#_Toc256000137)

[Table 14 Static routes 27](#_Toc256000138)

[Table 15 Intersight Device Connector Parameters 29](#_Toc256000139)

**No table of figures entries found.**

About This Document

|  |  |
| --- | --- |
| Rendered by | Michael Van Kleij (mvanklei@cisco.com) |
| Change Authority | Cisco Systems |
| DCP Reference | 1782432 |
| Project ID | A99178 |

History

Manually maintained document history:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | Reason for Change |
| 0.1 | 26-01-2024 | Draft | Work in progress |
| 0.2 | 26-01-2024 | Draft | Modifications after internal review |
|  |  |  |  |

Automated and very detailed change history is accessible via following Cisco internal URL:

<https://scdp.cisco.com/conf/pages/viewpreviousversions.action?pageId=287657187>

Review

Manually maintained review history:

|  |  |  |
| --- | --- | --- |
| Version | Reviewer's Detail | Review Date |
| 0.1 | Marcel van Rijswijk | 26-01-2024 |

Automated review history is accessible via following Cisco internal URL:

<https://scdp.cisco.com/conf/pages/viewpageactivity.action?pageId=287657187>

Document Conventions

|  |
| --- |
| **Tip**  Time saver. Expedite the task by following the recommendation being described. |

|  |
| --- |
| **Info**  Alerts reader that the information will help them solve a problem or better understand the subject being described. |

|  |
| --- |
| **Note**  Alerts readers to be careful. You might do something that could negatively impact a solution, project, equipment, or the quality of the work being described. |

|  |
| --- |
| **Warning**  Alerts readers of a situation that could cause injury or severely impact a solution, project, equipment, or the quality of the work being described. |

# Introduction

## Preface

This document provides the Nexus Dashboard Solution Design and Implementation plan a Proof of Value implementation for ASML. The POV Nexus Dashboard cluster for ASML will be based on virtual appliances deployed on ESXi servers in NRW. The deployment will be based on Nexus Dashboard version 3.0(1i). On top of the Nexus Dashboard cluster the Nexus Dashboard Insights (NDI) application will be hosted.

Part of the implementation will entail changes in the current ACI fabric of ASML. These will be described in this document.

ASML is aware that the scale deployed in this POV is insufficient to use NDI for their entire environment.

This document was developed in collaboration with the following teams and organizations through a series of workshops and meetings:

* ASML Team
* NTT
* Cisco CX Team

## Audience

This document is intended for the following team:

* ASML Team
* NTT
* Cisco CX Team

## Scope

The scope of this document is limited to the following:

* The Nexus Dashboard platform design with Day-2 applications for the sites listed below:

Table 1 ASML Site Locations

|  |  |
| --- | --- |
| No. | Site Name |
| 1 | Norwalk |
| 2 |  |
| 3 |  |

## Assumptions

The following assumptions have been made during the development of this document.

Table 2 Assumptions

|  |  |  |
| --- | --- | --- |
| No. | Assumption | Validated |
| 1 | Only NDI will be hosted on top of the ND cluster | **yes** |
| 2 | There will be overall 3 virtual nodes hosted on ESXi. | **Yes** |
| 3 | There will be no more than 50ms in round trip time between Nexus Dashboard nodes and the APIC cluster(s) | **Yes** |

Related Documents

The following documents have been used as an input or reference for this document.

Table 3 Related Documents

|  |  |  |
| --- | --- | --- |
| No. | Document Title | Document URL/Version (If Any) |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |

# ASML Network Overview

The next-generation Data Center network is based upon the Cisco Application Centric Infrastructure (ACI) solution, consisting of the physical switching fabric (built upon Nexus 9000 series switches in a spine/leaf topology) and the Application Policy Infrastructure Controller (APIC). The APIC is a clustered network policy and control engine, responsible for fabric bring-up, fabric management, policy configuration and more. The switches in the ACI fabric form a fat-tree topology, where each leaf node is connected to each spine node, with no connections across the same layer (i.e. no leaf-leaf or spine-spine links).

The ACI fabric Day-2 operations will be supported with Cisco tools for ACI fabric monitoring and assurance. This is Nexus Dashboard Insights (NDI). This application is running hosted on Nexus Dashboard (ND).

Cisco Nexus Dashboard (ND) is a platform that is designed to host multiple insights and operations applications. Customers now can provision one appliance cluster to run various applications simultaneously instead of having to manage independent appliance clusters. ND is a purpose-built appliance that can host containerized applications on a common platform based on Kubernetes. K8s orchestration is used for lifecycle management of the applications running on the Cisco Nexus Dashboard.

Cisco Nexus Dashboard Insights (NDI) is an application to provide pro-active assurance on the network-wide state of configuration, policy model, resource utilization and Cisco Advisories. It helps to transform Data Center operations from a reactive model to a fundamentally more proactive one. With the usage of mathematical modeling, it gives confidence to NetOps teams that their network policy is always consistent with the intent.

This document will cover the design of Day-2 operations POV for ASML ACI fabric.

Figure 1 ASML ACI Physical Design

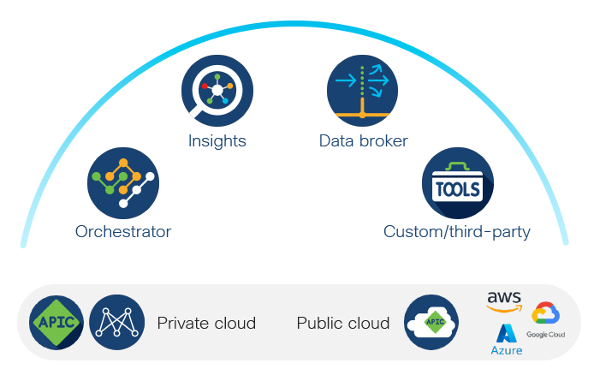


# Nexus Dashboard Overview

Nexus Dashboard is a single-pane-of-glass console that offers a centralized management console, allowing network operators to easily access the applications needed to perform the lifecycle management of their fabric from provisioning, troubleshooting, or simply get deeper visibility into their network.

Cisco Nexus Dashboard provides a common platform for deploying Cisco Data Center applications like Insights or Orchestrator.

Figure 2 Nexus Dashboard Applications



## Nexus Dashboard Form Factors

Cisco Nexus Dashboard can be deployed using a number of different form factors, depending on scale and requirements. Supported form factors are:

* Physical Appliance
* Virtual Appliance: VMware ESX
* Virtual Appliance: KVM
* Cloud Appliance: (AWS / Azure)
* Linux (RHEL)

The POV for ASML will be based on:

* Virtual Appliance: VMware ESX

|  |
| --- |
| **Note**  The same form factor must be used for all nodes as mixing different form factors within the same cluster is not supported. |

## Cluster sizing

The size of the cluster is dependent on the scale of the fabric(s) which need to be managed and the applications used. To ensure the right number of Nexus Dashboard nodes the cluster sizing tool can be used: <https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html>.

## Site Management

Nexus Dashboard and NDI support the management of multiple sites. To manage multiple sites the scaling needs to be taken into account. Also ensure that Service Compatibility is satisfied: <https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/dcn-apps/index.html>.

For the ASML POV only a single site will be onboarded.

## Cluster Connectivity

Each Nexus Dashboard node is connected to two networks: Data network and Management network.

The management network is used for:

* Accessing the Cisco Application Services Engine GUI
* Accessing the CLI over SSH
* DNS and NTP
* Firmware uploads
* Cisco Intersight device connector

The data network is used for:

* Cisco Application Services Engine Clustering
* App to app communication
* Access the Management network of the Cisco ACI fabric
* All app to ACI fabric communications

These interfaces are configured as Linux bonds. Interfaces on the connected switch need to be set up as individual host interfaces as “switchport mode access” if VLAN is not configured on Nexus Dashboard interface. Otherwise, the interfaces will need to be set up as trunk.

Two design options are supported to connect Nexus Dashboard to ACI fabric:

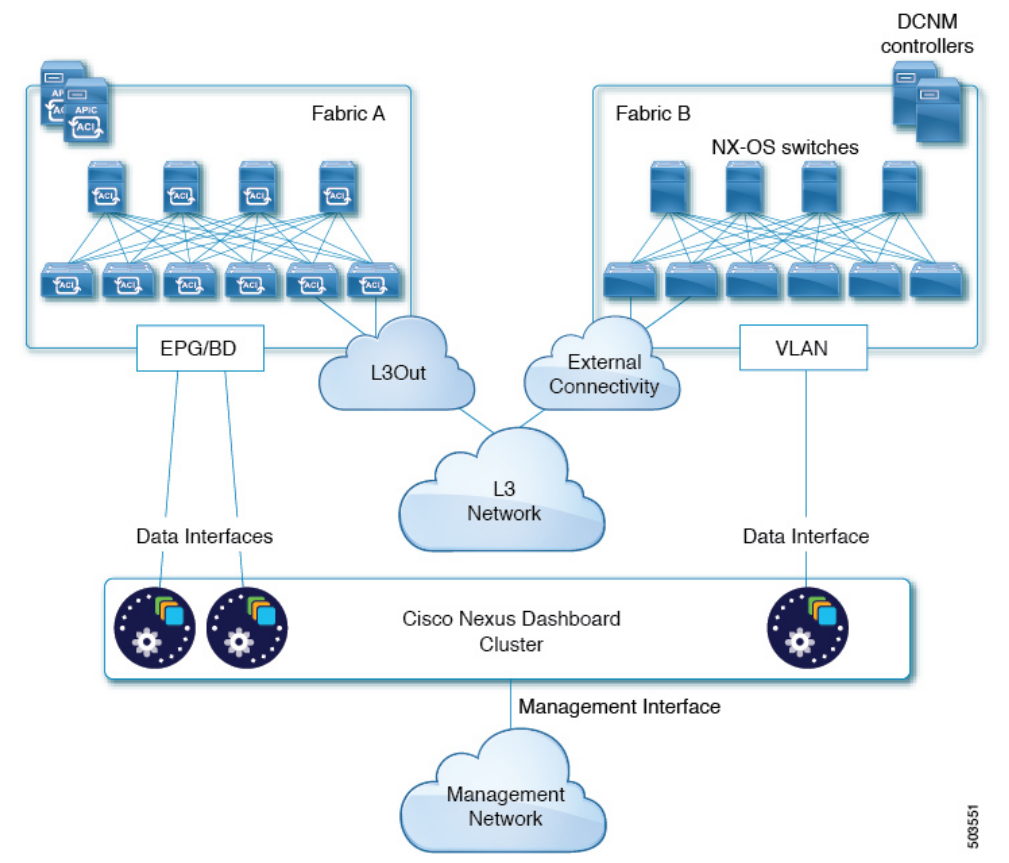
* ND connectivity to ACI via L2 connection
* ND connectivity to ACI via L3Out

### ND connectivity to ACI via L2 connection

With this model, the Nexus Dashboard server Data Interface is connected to ACI leaf switches and the applications on the Nexus Dashboard talk to the in-band Management network in the ACI mgmt tenant via the Data Interface.

The Data Interface IP Subnet is an EPG/BD in ACI fabric. This EPG must have a contract to talk to the ACI Inband EPG in mgmt tenant. It is recommended to put this EPG directly in mgmt tenant and VRF INB (in-band). The ND Data Subnet has to be different from the ACI in-band.

Figure 3 Nexus Dashboard Connectivity to ACI via EPG



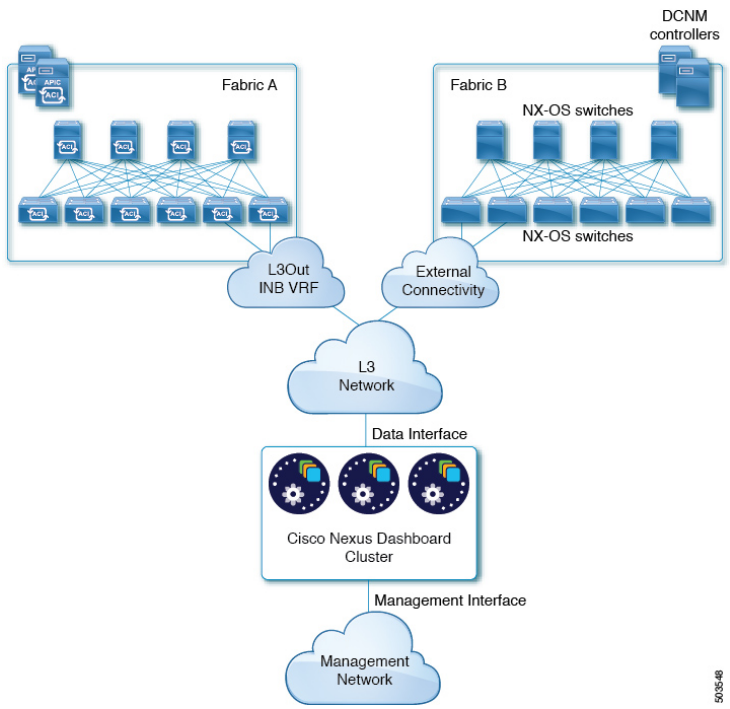
In a Multi-Fabric deployment, IP reachability to other fabrics needs to be established via the tenant mgmt L3Out associated with VRF INB.

### ND connectivity to ACI via L3Out

With this model, the Nexus Dashboard server Data Interface is connected to an L3 Network where also the Fabric Inband Management network in INB VRF L3out is connected.

In a Multi-Fabric deployment, IP reachability to other fabrics is established the same way.

Figure 4 Nexus Dashboard Connectivity to ACI via L3out



It is not supported to have Nexus Dashboard Data network and Management network in the same subnet. To add to this, ND subnets must not overlap with infrastructure in-band subnet. In addition, each network interface across different nodes in the cluster can also be in different subnets under the condition that any ND node can reach any other ND node.

The Data network must provide IP reachability to the fabrics' in-band IPs for Day-2 operations apps. The Data network interface uses MTU of 1500 by default but supports higher MTU as well.

For communication between the containers used by the Nexus Dashboard, the following two internal networks are required:

* **Application overlay** – Used for applications internally within Nexus Dashboard. It must be a /16 network and a default value is prepopulated during deployment.
* **Service overlay** – Used internally by the Nexus Dashboard. It must be a /16 network and a default value is prepopulated during deployment.

|  |
| --- |
| **Note**  Application and Service Overlay network addresses are never exposed outside and any traffic on these networks is routed internally. Communications between containers deployed in different Nexus Dashboard nodes are VXLAN-encapsulated and use the data interfaces' IP addresses as source and destination. |

### Communication Considerations

Cisco Nexus Dashboard is deployed with the concept of Multi-Fabric. Type of sites that can be onboarded to Nexus Dashboard are:

* ACI (fabric on-prem): APIC
* Cloud ACI: cAPIC
* DCNM (collections of VXLAN EVPN fabrics managed by DCNM): DCNM server

When Nexus Dashboard is running in Multi-Fabric environment, it is recommended not to connect the cluster nodes to the ACI fabric to prevent fate sharing.

Evaluate the use of more than one cluster in case of conflicting requirements. The Data network must have IP reachability to the fabrics' in-band IPs for Day-2 operations apps.

|  |
| --- |
| **Note**  The Data network uses MTU of 1500 by default but supports higher MTU as well. |

The following table gives the Round-Trip Time requirements:

Table 4 Nexus Dashboard RTT Requirements

|  |  |  |
| --- | --- | --- |
| Application | Connectivity | Maximum RTT |
| **Nexus Dashboard Cluster** | Between Nodes | 150 ms |
| **Nexus Dashboard Insights (NDI)** | Between Nodes | 50 ms |
| To Sites | 50 ms |

For more information, refer to Fabric Connectivity chapter in User Guide:

<https://www.cisco.com/c/dam/en/us/td/docs/dcn/nd/3x/nd-overview/nexus-dashboard-overview.pdf>

Furthermore, the following ports are required by the Nexus Dashboard cluster and its applications:

Table 5 Nexus Dashboard Communication Ports

|  |  |  |
| --- | --- | --- |
| Purpose | Port Number | Port Type |
| Management Interface | --- | ICMP |
| 22 | TCP |
| 67 | UDP |
| 69 | UDP |
| 80 | TCP |
| 443 | TCP |
| 5555 | TCP |
| 9880 | TCP |
| 30012 | TCP |
| 30021 | TCP |
| 30500-30600 | TCP/UDP |
| Data Interface (between ND nodes) | 53 | TCP/UDP |
| 443 | TCP |
| 3379 | TCP |
| 3380 | TCP |
| 4789 | UDP |
| 9969 | TCP |
| 9979 | TCP |
| 9989 | TCP |
| 15223 | TCP |
| 30002-30006 | TCP |
| 30009-30010 | TCP |
| 30012 | TCP |
| 30015-30019 | TCP |
| 30017 | UDP |
| 30025 | TCP |
| 30500-30600 | TCP/UDP |
| Data Interface (ND - APIC) | 22 | TCP |
| 443 | TCP |
| Data Interface (ND - ACI fabric) | 443 | TCP |
| 2022 | TCP |
| 5640-5671 | UDP |
| 5965 | UDP |
| 8884 | TCP |
| 9989 | TCP |
| 30000-30001 | TCP |

### Communication to Cisco Intersight

Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure management platform that provides global management and augmented intelligence to many platforms, including Cisco Nexus Dashboard.

For Data Center apps, such as Cisco Nexus Insights, connect to the Cisco Intersight portal through a Device Connector, which provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection. Nexus Insights uses Intersight to update Bug/PSIRT/recommendations.

|  |
| --- |
| **Note**  Please refer to [Connecting Nexus Dashboard to Cisco Intersight](#scroll-bookmark-36) section for Intersight Device Connector parameters used in deployment. |

# Nexus Dashboard Applications

In ASML ACI network, Nexus Dashboard will serve the function of a platform to host the following applications:

* Nexus Dashboard Insights (NDI)

## Nexus Dashboard Insights

### NDI Overview

Cisco Nexus Insights (NDI) application provides a way to gather information through data collection to get an overview of available resources and their active processes and configurations across the entire Application Policy Infrastructure Controller (APIC).

The application monitors a Data Center network and pinpoints issues that can be addressed to maintain availability and reduce surprise outages. Cisco NDI’s understanding of your network allows it to provide proactive advice with a focus on maintaining availability and alerting customers about potential issues that can impact uptime.

The Cisco NDI app provides log collection functionalities that are useful when working with Cisco TAC. It provides a way for Cisco customers to collect tech support across multiple devices and upload that tech support to Cisco Intersight Cloud. Additionally, it enables the capability for Cisco TAC teams to collect technical support on demand for a particular device.

Cisco NDI app consists of the following components:

* **Data Management** – settings to configure flows and schedule jobs to collect Software Telemetry and Flow Telemetry data.
* Flow Configuration – manage flow configuration rules on the site enabled on Cisco NI app.
* Collection Status – displays the node capabilities and collection status of the nodes for the features that are supported and not supported.
* Bug Scan – provides access to configure, schedule, on-demand bug scan that runs for a selected site. Bug scan generates system anomalies and alerts that are critical for a particular node on the site.
* Third-Party Integrations – provides access to onboard an AppDynamics Controller onto the Cisco NI app.
* Export Data – streams the data collected from Cisco NI app through a Kafka exporter to send the summary of data in Cisco NI app email.
* **Devices** – provides various ways of viewing the behavior of the nodes based on Resource Utilization, Environmental, Statistics, End Point Analytics, and Flow Analytics.
* **Analyze Alerts** – access to total advisories, notices, PSIRTs, hardware, software, and hardening check advisories applicable to your network.
* **Advisories**
* Field Notices – notices such as end-of-life notices for switch hardware and software.
* PSIRTs – Product Security Incident Response Team notices that display three levels of advisory severity for switch hardware and software in your network.
* Best Practices – provides access to configure and schedule a compliance job that runs for a selected site.
* Firmware Upgrade Path and Upgrade Impact – to upgrade to a recommended software version, Cisco NI app suggests an upgrade path and determines the potential impact of the upgrade to the first-hop.
* **Anomalies**
* Bug Scan – provides access to configure and schedule bug scan that runs for a selected site.
* **Log Collection** – Collect and upload the logs for devices in your network to Cisco Intersight Cloud. Enables Cisco TAC to trigger on-demand collection of logs for user devices on the site and pull the logs from Cisco Intersight Cloud.
* **Data Collection** – The streaming of telemetry data is done by the Operating Systems on the site nodes. As each data source is different and the format in which data is streamed is different, there are corresponding collectors running analytics that translate the telemetry events from the nodes into data records to be stored in the data lake. The data stored in the data lake is a format that the analytics pipeline can understand and work upon.

The following telemetry information is collected from various nodes on the site to achieve the goal:

* **Resources Analytics** – This includes monitoring software and hardware resources of site nodes on the Cisco APIC.
* **Environmental** – This includes monitoring environmental statistics of hardware resources such as fan, CPU, memory, and power of the site nodes.
* **Statistics Analytics** – This includes monitoring of nodes, interfaces, and protocols on the Cisco APIC and site nodes.
* **Flow Analytics** – This includes monitoring of flows on the Cisco site nodes, detecting average latency, packet drop indication, and flow move indication across the entire Cisco ACI.
* **Endpoint Analytics** – This includes monitoring endpoints on the Cisco site nodes for rapid endpoint moves and endpoints that do not get learned back after a reboot across the entire Cisco ACI.
* **Event Analytics** – This includes monitoring of events, faults and configuration changes.
* **Resource Utilization and Environmental Statistics** – Resource analytics supports configuration, operational, and hardware resources. Environmental covers CPU, memory, temperature, fan utilization, power, and storage related to the leaf nodes, spine nodes, and Cisco APIC. System analytics also covers anomalies, the trending information of each resource, and graphing of parameters, which help network operators debug nodes over periods of time.
* **Predictive Analytics and Correlation** – The value-add of this platform is predicting failures in the site and correlating internal site failures to the user-visible or interesting failures.
* **Anomaly Detection** – Involves understanding the behavior of each component using different machine learning algorithms and raising anomalies when the resource behavior deviates from the expected pattern. Anomaly detector applications use different supervised and unsupervised learning algorithms to detect the anomalies in the resources and they log the anomalies in an anomaly database.

### Nexus Insights Flow Collection

Once Nexus Dashboard Insights Application is installed and enabled, you can configure flow collections in the Data Management menu. The flow configuration can be enabled as a rule for flow data collection within tenant and VRF, subnet filter can be added for more granular control of collected flow data.

The table below gives the flow rules configuration for ASML ACI fabrics:

Table 6 NI Flow Collection Rules

|  |  |  |  |
| --- | --- | --- | --- |
| Rule Name | Tenant | VRF | Subnet |
|  |  |  |  |

|  |
| --- |
| **Note**  The prerequisites for functional flow collection are:   * **ACI Fabric Node Controls** policy must be set to Telemetry Priority. * **Precision Time Protocol (PTP)** must be enabled in the ACI fabric. Best practice is to use IPN/ISN node as PTP grandmaster when running ND in Multi-Fabric environment. * **DOM** must be enabled from APIC to populate DOM info for interfaces in Nexus Insights.   Furthermore, Nexus Insights leverages Intersight connectivity to fetch the Cisco information base for issues relevant to the ACI environment, therefore Nexus Dashboard Intersight connectivity must be functional. Please refer to section [Communication to Cisco Intersight](#scroll-bookmark-34). |

### Nexus Dashboard Insights Telemetry Collection Capabilities

Software Telemetry provides visibility to control-plane protocol state, environmental info, and counters, such as:

* Utilization of Operational (MAC address, unicast/multicast routing/IPv4/IPV6 tables, TCAM)
* Configuration (VLANs, VRFs, EPGs, BD, LPM)
* Hardware resources (Ports in admin UP state, switch bandwidth)
* Switch Environmentals (CPU, memory, temperature, power, fan speed)
* Interface statistics (Rate, counters, CRC errors, LLDP flaps, routing layer errors)

Hardware Telemetry is provided by hardware ASIC. It can be divided in:

* Data plane flow
* ASIC state data

Source of Hardware Telemetry are:

* FT – Flow Telemetry
* FTE – Flow Telemetry Events
* SSX – Streaming Statistics eXport

Flow Telemetry captures full data-plane packet flow information and uses the flow records stored in the flow table. A flow record consists of the following:

* 5-tuple flow information
* Interface/queue information
* Flow start/stop time
* Flow latency

Flow Telemetry Events triggers notifications or events when certain conditions are detected in the packets of a flow. These detected events are first collected in a first-in, first-out (FIFO) method within the flow table. Once a predetermined threshold is reached, these events are exported.

An event packet typically includes information such as the following about the flow:

* Flow tuple
* Event reason
* Drop info (for example: acl\_drop, policer\_drop, policy\_drop, buffer\_drop, ids\_drop, forward\_drop)
* TCP-related fields (for example flags, seq/ack num, and so on)
* Interface info (for example srcid, oport, oclass, and so on)
* L2 or L4 payload length

Streaming Statistics Export (SSX) module streams ASIC statistics based on user configuration. It can read a register or (directly accessible) memory of the switch. SSX supports many opcodes and general-purpose registers to host many applications. SSX is a hardware-assisted export of various ASIC counters, like interface counters, drop counters and so forth, that can be captured very frequently, without involving a switch CPU. Examples of these hardware-assisted captures are:

* Interface counters (packets/bytes/drops)
* Ingress/Egress queue depth
* Ingress/Egress queue drops
* Egress queue microbursts
* Buffer depth
* User-defined streaming parameters

# ASML Nexus Dashboard Deployment Information

## Nexus Dashboard prerequisites in ACI

The paragraphs below describe the changes which need to be done in ACI to be able to utilise NDI. This includes configuring the in-band management IP addresses, the L3out and changes in the configuration of the fabric. None of these changes should have impact on the traffic flow within the fabric, though it is recommended to perform the changes during a change window.

### ACI in-band management IP addresses

To be able to run NDI for an ACI fabric some modifications need to be made on the ACI fabric of ASML. First the APICs, Leaf and Spine switches need to be provisioned with an inband management IP address. The table below shows the IP addresses which will be configured on each device.

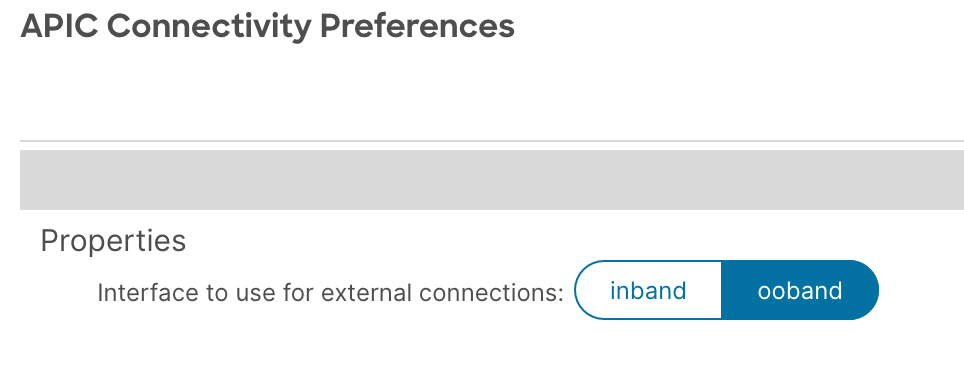
This configuration can be found at: *tenant* ***mgmt*** *> Node Management Addresses > Static Node Management Addresses*

Table 7 ACI APICNRW in-band management IP Addresses

|  |  |  |  |
| --- | --- | --- | --- |
| Node Name | IP address | Gateway | inb management EPG |
| apicnrw01 | 172.23.132.154 | 172.23.132.129 | ndi\_inband |
| apicnrw02 | 172.23.132.155 | 172.23.132.129 | ndi\_inband |
| apicnrw03 | 172.23.132.156 | 172.23.132.129 | ndi\_inband |
| swnrwle101 | 172.23.132.132 | 172.23.132.129 | ndi\_inband |
| swnrwle102 | 172.23.132.133 | 172.23.132.129 | ndi\_inband |
| swnrwle103 | 172.23.132.134 | 172.23.132.129 | ndi\_inband |
| swnrwle104 | 172.23.132.135 | 172.23.132.129 | ndi\_inband |
| swnrwle105 | 172.23.132.136 | 172.23.132.129 | ndi\_inband |
| swnrwle106 | 172.23.132.137 | 172.23.132.129 | ndi\_inband |
| swnrwle107 | 172.23.132.138 | 172.23.132.129 | ndi\_inband |
| swnrwle108 | 172.23.132.139 | 172.23.132.129 | ndi\_inband |
| swnrwle109 | 172.23.132.140 | 172.23.132.129 | ndi\_inband |
| swnrwle110 | 172.23.132.141 | 172.23.132.129 | ndi\_inband |
| swnrwle111 | 172.23.132.142 | 172.23.132.129 | ndi\_inband |
| swnrwle112 | 172.23.132.143 | 172.23.132.129 | ndi\_inband |
| swnrwle113 | 172.23.132.144 | 172.23.132.129 | ndi\_inband |
| swnrwle114 | 172.23.132.145 | 172.23.132.129 | ndi\_inband |
| swnrwle115 | 172.23.132.146 | 172.23.132.129 | ndi\_inband |
| swnrwle116 | 172.23.132.147 | 172.23.132.129 | ndi\_inband |
| swnrwle117 | 172.23.132.148 | 172.23.132.129 | ndi\_inband |
| swnrwle118 | 172.23.132.149 | 172.23.132.129 | ndi\_inband |
| swnrwle119 | 172.23.132.150 | 172.23.132.129 | ndi\_inband |
| swnrwle120 | 172.23.132.151 | 172.23.132.129 | ndi\_inband |
| swnrwsp1101 | 172.23.132.152 | 172.23.132.129 | ndi\_inband |
|  |  |  |  |
| swnrwsp1102 | 172.23.132.153 | 172.23.132.129 | ndi\_inband |

To prevent a change in behavior when configuring the fabric with in-band management IP addresses we need to change the management interface preference in ACI. This controls whether the in-band or the out-of-band interface is used to reach services like NTP and DNS. Since ASML currently doesn't use the in-band management addresses we want to keep the behavior the same. The default configuration however, is that ACI uses the in-band interfaces if configured. To ensure the out-of-band interface will be used configure the APIC connectivity preferences to be **ooband** at *System > System Settings > APIC Connectivity Preferences*

Figure 5 APIC Connectivity Preferences



### In-band management VRF L3out

ASML has chosen to deploy NDI in NRW and connect the NDI cluster via L3 to the ACI fabric. This deployment model requires the creation of a L3out in the **inb** VRF, which is part of the **mgmt** tenant. The VRF is a default part of ACI and can't be renamed.

*L3out: l3out-ospf\_mgmt\_inband*

*Node profile: np-mgmt\_inband*

*Node ID: 101 & 102*

*Transit Network: 172.23.132.72/29*

*swnrwle101-vrf-inb-l3out.asml.com   172.23.132.75*

*swnrwle102-vrf-inb-l3out.asml.com   172.23.132.76*

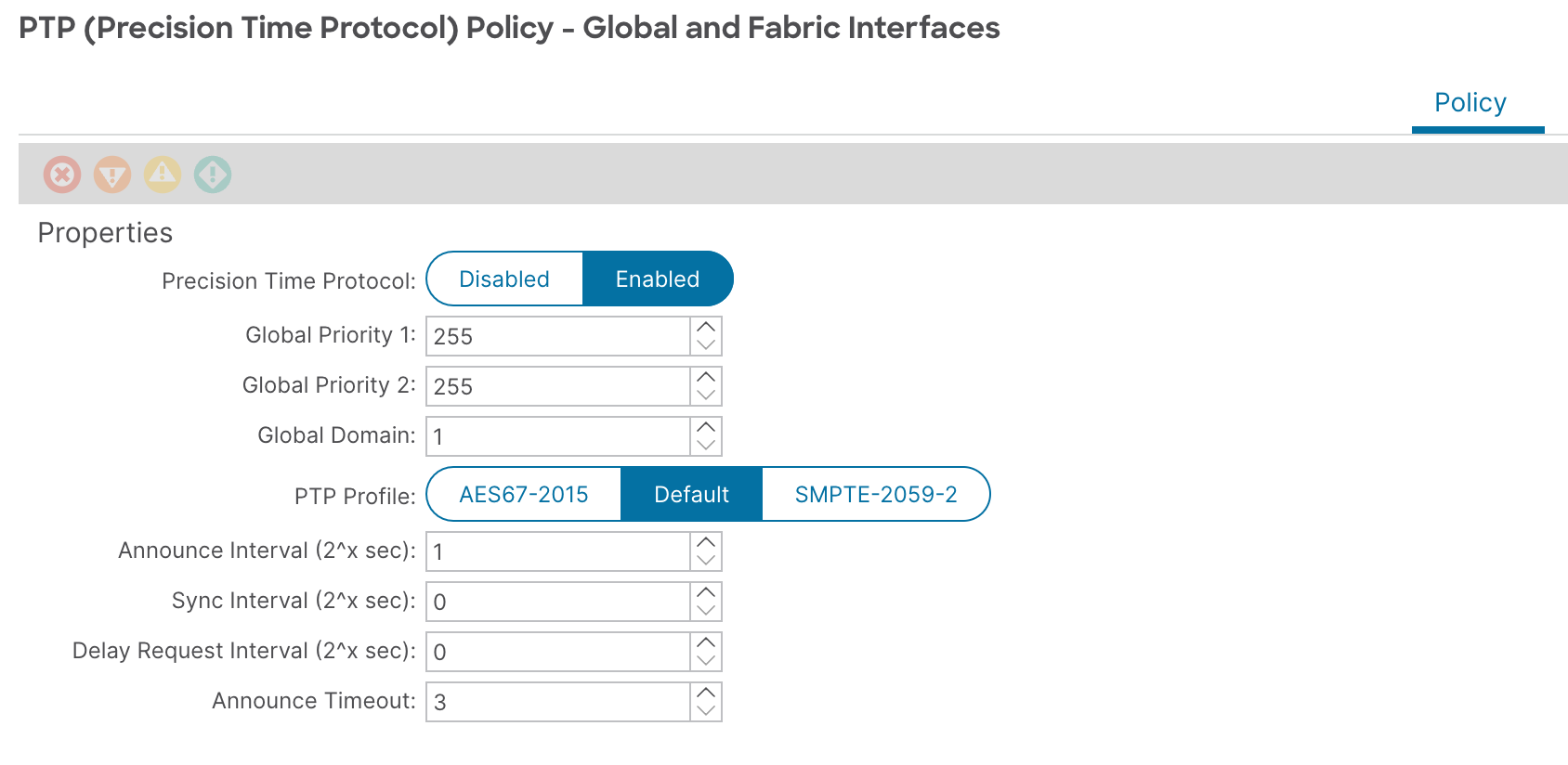
*Interface profile: intprof-rtnrwf62\_inband*

### Precision Time Protocol

To be able to perform flow telemetry, the ACI fabric must be enabled for Precision Time Protocol (PTP). Within a single fabric enabling PTP is simple. In multi-pod or multi-site fabrics the process is a bit more involved as the configuration requires an external grand master clock. For the POV this is not necessary as it will be deployed in a single site fabric. The production deployment will have need for an external grand master clock.

Enable PTP by navigating to *System > System settings > PTP and Latency Measurement*. Ensure that Precision Time Protocol is set to **Enabled.**

Figure 6 Precision Time Protocol

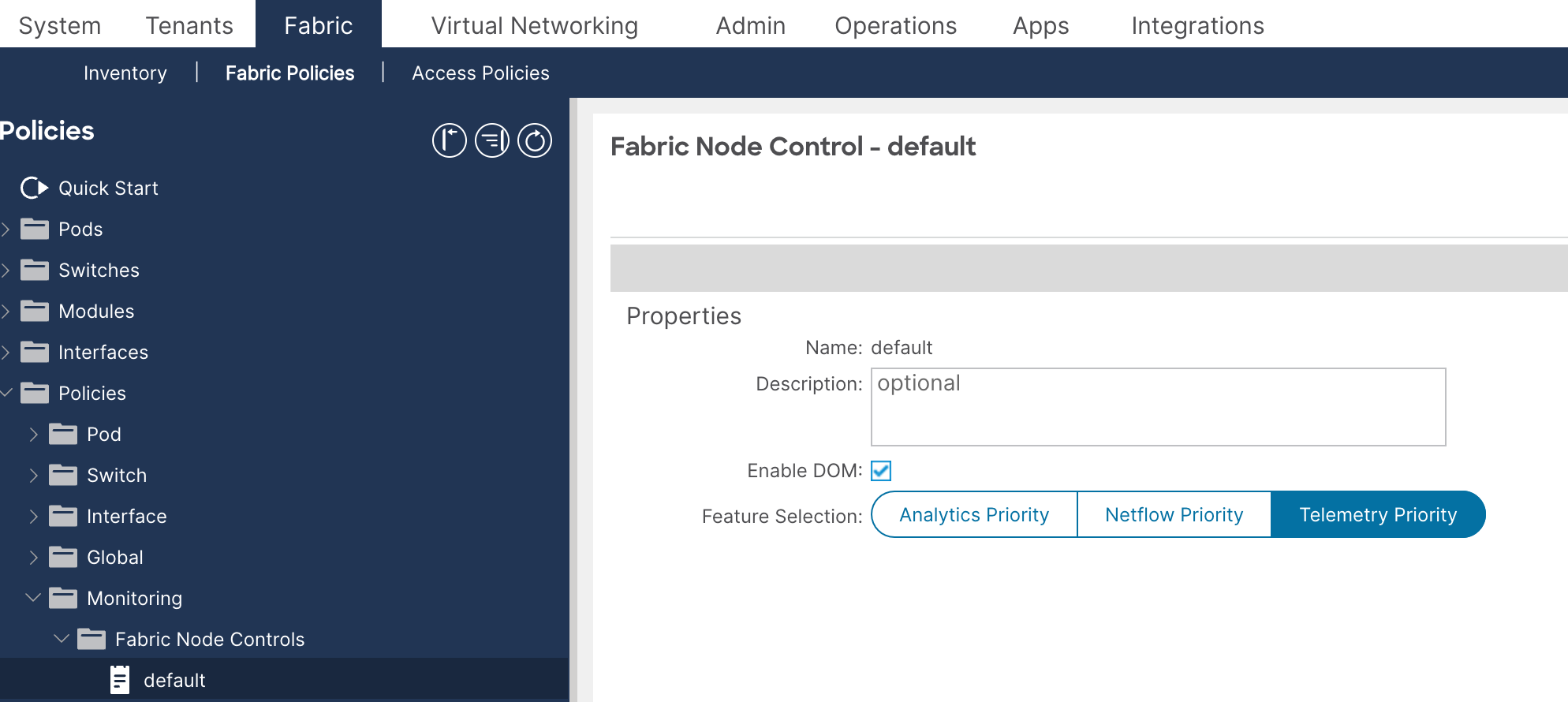


### DOM and Feature selection

Digital Optics Monitoring is another feature which needs to be enabled for NDI to function properly. It can simply be enabled by modifying the default monitoring policy at *Fabric > Fabric Policies > Policies > Monitoring > Fabric Node Controls > default*.

On the same page the feature selection needs to be configured as **Telemetry Priority**. This should be the default.

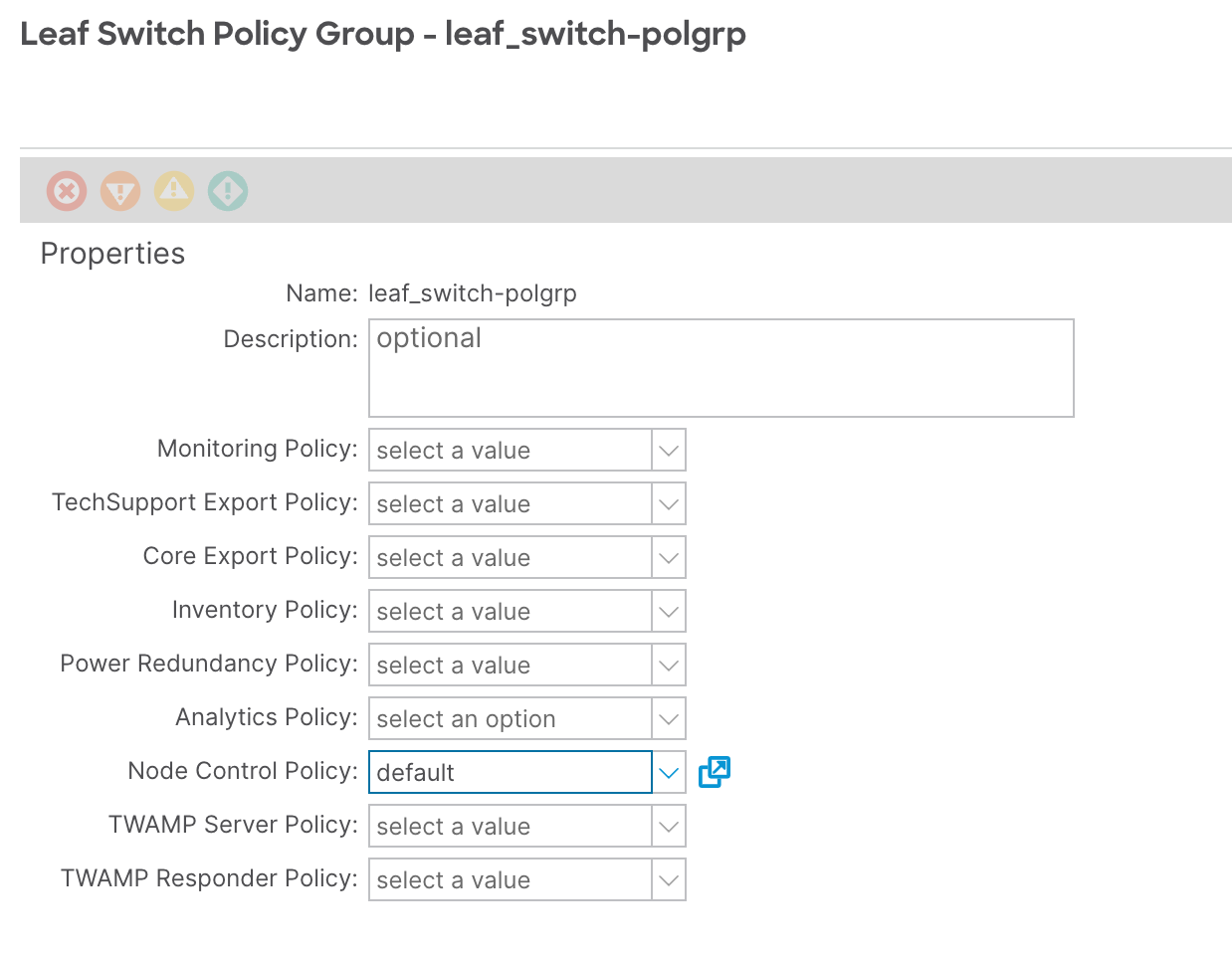
Figure 7 Fabric Node Controls



|  |
| --- |
| **Note**  This configuration assumes that the default policy, or no policy, is used in the ASML fabric. If another policy is used that can also be modified. |

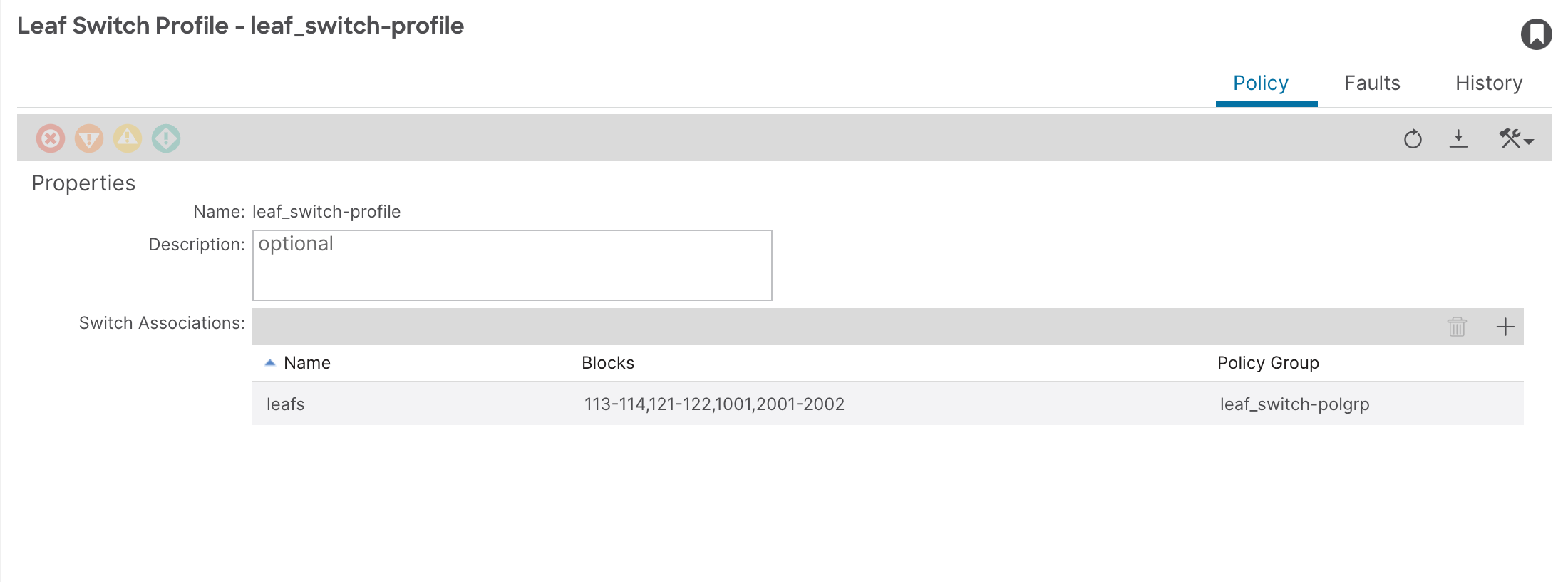
Once the profile has been created it must be applied to the switches. For this Leaf and Spine Policy Groups need to be created and applied to the switches. This can be done under *Fabric > Fabric Policies > Switches > Leaf Switches (and Spine Switches) > Policy Groups*. The Policy Group needs to refer to the Node Control Policy created earlier.

Figure 8 Create Leaf Switch Policy Group



Next the policy group needs to be applied to the switches. This is done using a Switch Profile. Again this has to be done for both the Leaf and Spine switches. The Switch Profiles can be created at *Fabric > Fabric Policies > Switches > Leaf Switches (and Spine Switches) > Profiles.* Ensure that the selector selects all switches.

Figure 9 Leaf Switch Profile



## Cluster Details

In ASML ACI fabric, Nexus Dashboard cluster will be deployed at NRW. The tables below summarize ND clusters design:

Table 8 Nexus Dashboard Clusters Summary

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cluster Name | Node Name | Role | ESXi Server | Data Interface EPG | Data Interface IP | Data Gateway IP | Mgmt Interface EPG | Mgmt Interface IP | Mgmt Gateway IP |
| usnrwndi | usnrwndi01 | App | NRW | epg-2118 | 172.23.194.16 | 172.23.194.1 | epg-2015 | 172.23.170.88 | 172.23.170.1 |
| usnrwndi02 | App | NRW | epg-2118 | 172.23.194.17 | 172.23.194.1 | epg-2015 | 172.23.170.89 | 172.23.170.1 |
| usnrwndi03 | App | NRW | epg-2118 | 172.23.194.18 | 172.23.194.1 | epg-2015 | 172.23.170.90 | 172.23.170.1 |

Table 9 Nexus Dashboard Cluster Parameters

|  |  |
| --- | --- |
| Parameter | Value |
| Cluster Name | usnrwndi |
| NTP Server | 146.106.15.34, 146.106.15.35, 146.106.15.37 |
| NTP authentication key (if required) | Not applicable |
| DNS Provider | 146.106.15.32, 146.106.15.33 |
| Proxy Server | Not applicable |
| DNS Search Domain | asml.com sn-eu.asml.com eu.asml.com us.asml.com sn-us.asml.com as.asml.com |
| App Network | 172.17.0.1/16 |
| Service Network | 100.80.0.0/16 |

|  |
| --- |
| **Note**  Nexus Dashboard needs Internet access for various features. The proxy server needs to allow access to the following URLs:   * dcappcenter.cisco.com * svc.intersight.com * svc.ucs-connect.com * svc-static1.intersight.com * svc-static1.ucs-connect.com |

### Software

For the ASML POV deployment the ND and NDI cluster will be running the software versions as listed in the table below. Currently this version does not support the co-hosting of multiple applications on a ND cluster. This means that this ND cluster can only be used for NDI.

Table 10 Recommended versions

|  |  |
| --- | --- |
| Software | Version |
| Nexus Dashboard | 3.0(1i) |
| Nexus Dashboard Insights | 6.3.1.40 |

When considering different software versions it is recommended to verify the software versions using the [Application Compatibility Matrix](https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/dcn-apps/index.html).

### VM deployment

For the POV, ASML will deploy Nexus Dashboard as a virtual appliance. The table below shows the requirements for these virtual machines.

Table 11 VM requirements

|  |  |
| --- | --- |
| Data Node requirements | App Node requirements |
| * VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3 * VMware vCenter 7.0.1, 7.0.2, 7.0.3 if deploying using vCenter * Each VM requires the following: * 32 vCPUs with physical reservation of at least 2.2GHz * 128GB of RAM with physical reservation * 3TB SSD storage for the data volume and an additional 50GB for the system volume   Data nodes must be deployed on storage with the following minimum performance requirements:   * The SSD must be attached to the data store directly or in JBOD mode if using a RAID Host Bus Adapter (HBA) * The SSDs must be optimized for Mixed Use/Application (not Read-Optimized) * 4K Random Read IOPS: 93000 * 4K Random Write IOPS: 31000 | * VMware ESXi 7.0, 7.0.1, 7.0.2, 7.0.3 * VMware vCenter 7.0.1, 7.0.2, 7.0.3 if deploying using vCenter * Each VM requires the following: * 16 vCPUs with physical reservation of at least 2.2GHz * 64GB of RAM with physical reservation * 1536GB SSD/NVMe storage for the data volume and an additional 50GB for the system volume   Some services require App nodes to be deployed on faster SSD storage while other services support HDD. Check the [Nexus Dashboard Capacity Planning](https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html) tool to ensure that you use the correct type of storage. |

|  |
| --- |
| **Note**  We recommend that each Nexus Dashboard node is deployed in a different ESXi server |

The size of the ND cluster is dependent on the number of switches being managed.

Table 12 Virtual ND sizing chart

|  |  |  |
| --- | --- | --- |
| Number of Leaf switches | Number of App nodes | Number of Data nodes |
| 1 - 50 | 3 | 0 |
| 51 - 200 | 6 | 3 |
| > 200 | Not supported | Not supported |

More detail can be found using the  [Nexus Dashboard Capacity Planning](https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html) tool.

Ensure that the IP connectivity for the Management and Data interfaces is prepared, the follow the steps listed in the [install guide](https://www.cisco.com/c/en/us/td/docs/dcn/nd/3x/deployment/cisco-nexus-dashboard-deployment-guide-301/nd-deploy-esx-30x.html). Use the information provided at the beginning of this chapter.

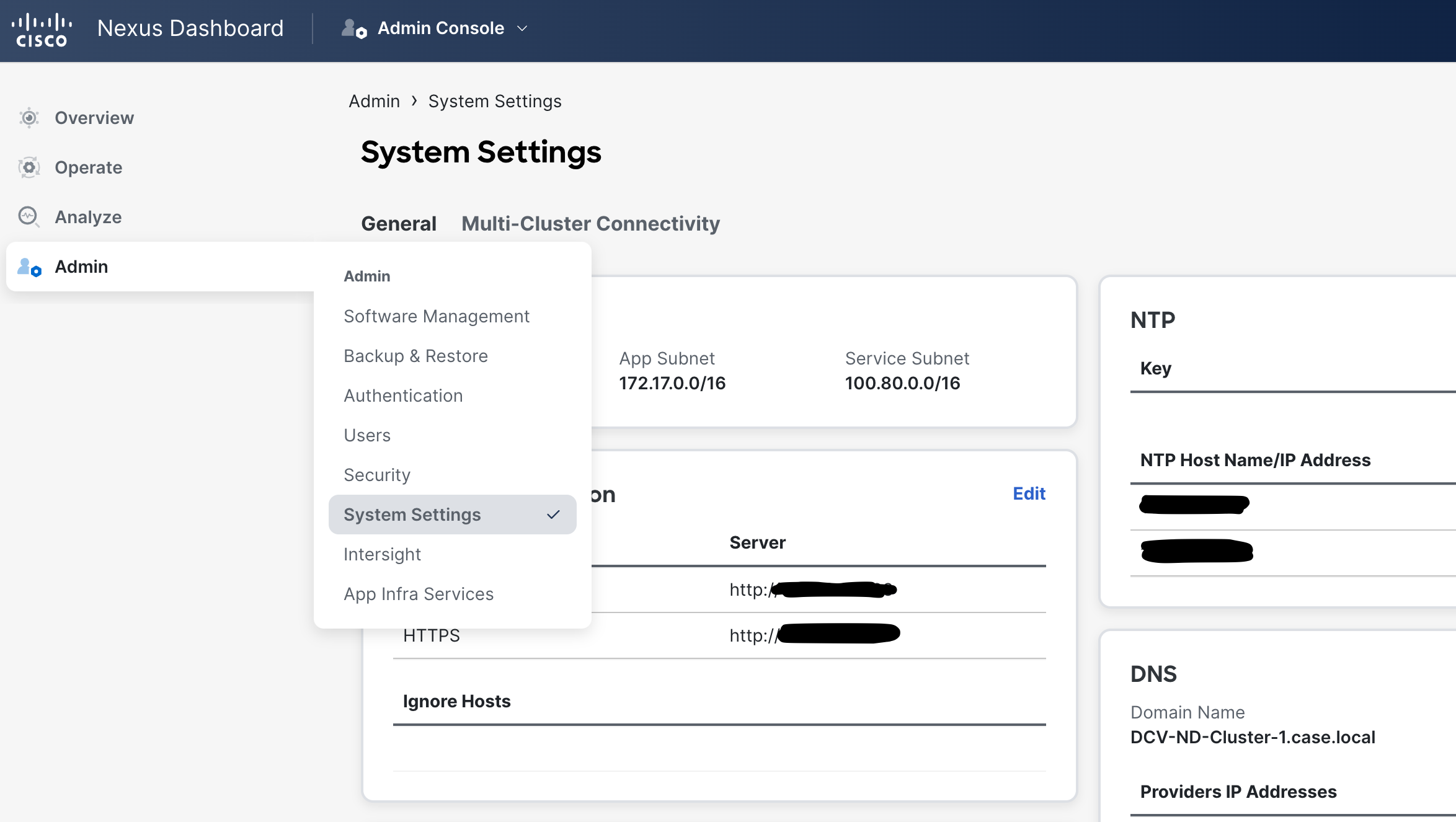
## Nexus Dashboard cluster configuration

After the initial setup the rest of the cluster needs to be configured. In the Admin Console, open *Admin > System Settings*. Here NTP, DNS and Proxy configuration can be edited if required. Additional configuration parameters can also be found here. One of the things which need to be configured here is the **Network Scale.**This defines the number of sites, Switches and Flows to expect.

Table 13 Network Scale

|  |  |  |
| --- | --- | --- |
| Number of Sites | Number of Switches | Flows per Second |
| 1 | 22 | <2500|5000> |

Figure 10 ND System Settings



Additionally static routes can be configured here. For the PoV a single static route needs to be defined.

Table 14 Static routes

|  |  |
| --- | --- |
| Subnet | Interface |
| 172.23.132.128/25 | Data Network |
|  |  |
|  |  |

## Connecting Nexus Dashboard to Cisco Intersight

To be able to use all NDI features you need to have integration with Intersight. Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure Management Platform that provides global management and augmented intelligence to many platforms, including Cisco Nexus Dashboard.

Data Center applications, such as Cisco Nexus Insights, connect to the Cisco Intersight portal through a Device Connector that provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal using a secure internet connection. Nexus Insights uses Intersight to update Bug/PSIRT/Recommendations.

To setup Device Connector, select *Admin > Intersight* and follow these steps:

**Step 1:** At the top right of the main pane, click "Settings".

**Step 2:** Click the "General" tab to configure basic options.

1. Use the Device Connector knob to enable or disable the Device Connector. This enables you to claim the device and leverage the capabilities of Intersight. If it is disabled, no communication is allowed to Cisco Intersight.
2. In the Access Mode area, choose whether to allow Intersight the capability to make changes to this device.
3. **Allow Control** (Default)—Enables you to perform full read or write operations from the cloud based on the features available in Cisco Intersight.
4. **Read-only**—Ensures that no changes are made to this device from Cisco Intersight. For example, actions such as upgrading firmware, or a profile deployment will not be allowed in read-only mode. However, the actions depend on the features available for a particular system.
5. Use the Auto Update knob to enable automatic Device Connector updates. It is recommended that you enable automatic updates. When enabled, the Device Connector will automatically upgrade its image whenever there is any upgrade push from Intersight. If you disable the automatic updates, you will be asked to manually update the software when new releases become available.

**Step 3:** Click "Save" to save the changes.

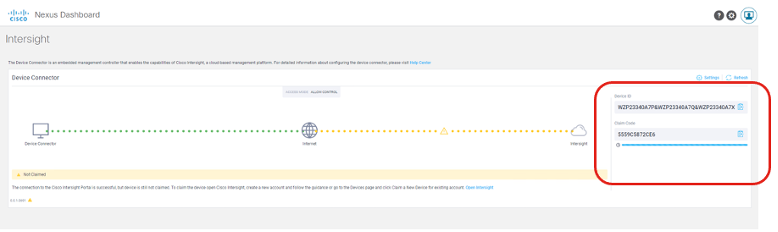
**Step 4:** Click the Certificate Manager tab if you want to import additional certificates. By default, the device connector trusts only the built-in certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device. You can choose to upload additional certificates by clicking the "Import" button on this screen.

The imported certificates must be in the .pem (base64 encoded) format. After a certificate is successfully imported, it is listed in the list of Trusted Certificates and if the certificate is correct, it is shown in the In-Use column. You can click the "View" icon at the end of the certificate row to view its details such as Name, Issue, and Expiration Dates.

To establish communication, Cisco Intersight must Claim the device. It is assumed that you have an account already created on <https://www.intersight.com>.

**Step 5:** Go back to **Admin** > **Intersight** menu, you will see a screen similar to the image below.

Figure 11 Connection to Intersight



If you see a red dotted line connecting to the Internet on the Device Connector page, you must configure a proxy for your Nexus Dashboard cluster to be able to access the Internet.

If you see a yellow dotted line and a caution icon while connecting the Internet to Intersight in the Device Connector page and the text "Not Claimed", then your Intersight Device Connector is not yet configured and connected to the Intersight service, and the device is not yet claimed.

In this case, copy the Device ID and the Claim Code you find on the right.

**Step 6:** Log in to the Cisco Intersight cloud site at <https://www.intersight.com> and:

* Click "Devices" tab and then click "Claim a New Device".
* Provide the Device ID and the Claim Code you have obtained earlier and click "Claim".

The message "Your device has been successfully claimed" should be displayed on the "Claim a New Device" page.

**Step 7:** Going back to Nexus Dashboard; at the *Admin > Intersight* menu, you should see a green dotted line connecting the Internet to Intersight in the Device Connector page and the text "Claimed".

The table below lists Intersight connection parameters used in Nexus Dashboard deployment.

Table 15 Intersight Device Connector Parameters

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Connector | Update | Proxy IP | Proxy Port | Proxy User | Proxy Password |
| Allow Control | Auto Update |  |  |  |  |

## User authentication

Nexus Dashboard can authenticate users via various authentication providers. The following providers are supported:

* Local
* LDAP
* RADIUS
* TACACS+
* OIDC

For the PoV only local users will be created. For a production deployment we do recommend using an external authentication provider like TACACS+ or RADIUS.

## Onboard sites

Nexus Dashboard uses the concept of sites to be able to manage multiple fabrics. To onboard a fabric into ND it needs to be added.

**Step 1:**On the ND dashboard go to *Operate > Sites.* Click on "Add site".

**Step 2:** Fill the form with the correct information and click on "Next".

|  |  |
| --- | --- |
| Parameter | Value |
| Hostname / IP address | APICNRW01, APICNRW02, APICNRW03 |
| Username | <username> |
| Password | Documented in secure location |
| Login Domain | <domain> |

**Step 3:**Give the site a name and place the site on a location. The location itself is an approximation.

**Step 4:** Finish the wizard.

## Scaling and Compatibility References

To correctly size a Nexus Dashboard Cluster, please refer to the following tool on CCO: <https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/nd-sizing/index.html>.

For compatibility information, please refer to the following tool on CCO: <https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/dcn-apps/index.html>.

# Installing and configuring NDI

Once Nexus Dashboard has been installed and configured it is possible to install additional services on top. To install NDI we need to go to *Operate > Services > App Store*. Here Nexus Dashboard Insights is listed. Click on "Install" to install the app. Once installed the app can be started using the "Start" button at *Operate > Services > Installed Services.*

Once NDI has been installed it can be accessed via the dropdown menu at the top, which currently should state **Admin Console**. Here **Insights** can be selected. NDI will open on its main page.

When opening the *Operate > Sites* page you will be greeted with a message that no sites have been configured. When Clicking **Add Site**, the Add site wizard will start. NDI will collect the sites from Nexus Dashboard and will show the option to add that site to NDI too.

Trademarks and Disclaimers

IF THIS DOCUMENT IS PROVIDED AS A DELIVERABLE IN ACCORDANCE WITH THE CISCO TERMS AND CONDITIONS ASSOCIATED WITH A PURCHASED CISCO SERVICE (“TERMS”) THEN THIS DOCUMENT IS PRESENTED SUBJECT TO THOSE TERMS. IN ALL OTHER EVENTS, THIS DOCUMENT IS PROVIDED “AS-IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2023 Cisco and/or its affiliates. All rights reserved.

Document Acceptance

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |