Advanced Load Balancing for VMware Cloud Foundation

Modified on 24 AUG 2021

VMware Cloud Foundation

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Advanced Load Balancing for VMware Cloud Foundation

1

The Advanced Load Balancing for VMware Cloud Foundation validated solution provides information on the use of NSX Advanced Load Balancer as a load balancing solution for VMware Cloud Foundation.

A VMware Validated Solution is a technical validated implementation that is built and tested by VMware and VMware partners to help customers resolve common business use cases. VMware Validated Solutions are operationally and cost-effective, performant, reliable and secure. Each solution contains a detailed design, implementation, and operational guidance.

Intended Audience

The Advanced Load Balancing for VMware Cloud Foundation documentation is intended for cloud architects, and administrators who are familiar with and want to use NSX Advanced Load Balancer for load balancing in the VMware Cloud Foundation.

Support Matrix

The Advanced Load Balancing for VMware Cloud Foundation validated solution is compatible with certain versions of the VMware products that are used for implementing the solution.

Note

1. Ensure that both the VCF BoM and the NSX Advanced Load Balancer release version are under support.
2. For more information on End of General Support and End of Technical Guidance dates, plase visit lifecycle.vmware.com.

Software Components in Advanced Load Balancing for VMware Cloud Foundation:

VMware Cloud Foundation Version	Product Group	Component Versions
5.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.1 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 30.1.1 or later ■ 22.1.2 or later

VMware Cloud Foundation Version	Product Group	Component Versions
5.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 5.0 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 30.1.1 or later ■ 22.1.2 or later
4.5.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.5.1 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 22.1.2 or later ■ 21.1.1 or later ■ 20.1.6 or later
4.5	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.5 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 22.1.2 or later ■ 21.1.1 or later ■ 20.1.6 or later
4.4	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.4 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 21.1.1 or later ■ 20.1.6 or later
4.3.1	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.3.1 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 21.1.1 or later ■ 20.1.6 or later
4.3.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.3 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 21.1.1 or later ■ 20.1.6 or later
4.2.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.2 Release Notes

VMware Cloud Foundation Version	Product Group	Component Versions
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 21.1.1 or later ■ 20.1.6 or later
4.1.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.1 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 21.1.1 or later ■ 20.1.6 or later
4.0	Products part of VMware Cloud Foundation	See VMware Cloud Foundation 4.0 Release Notes
	Solution-added Products	NSX Advanced Load Balancer. The following versions are supported: ■ 21.1.1 or later ■ 20.1.6 or later

Before You Apply This Guidance

To design and implement the Advanced Load Balancing for VMware Cloud Foundation validated solution, your environment must have a certain configuration.

Supported VMware Cloud Foundation Deployment

Workload Domain	Deployment Details
Management domain	Automated deployment of vCenter Server and NSX Manager cluster by using VMware Cloud Builder. Refer the following VMware Cloud Foundation documentation: ■ For information on deploying the management domain, refer to VMware Cloud Foundation Getting Started Guide and VMware Cloud Foundation Deployment Guide. ■ For information on designing the management domain, refer to VMware Cloud Foundation Design Guide for the Management Domain.
(Optional) One or more virtual infrastructure workload domains	Automated deployment of vCenter Server and NSX-T Manager cluster by using SDDC Manager. Refer the following VMware Cloud Foundation documentation: ■ For information on deploying the VI workload domain, refer to VMware Cloud Foundation Getting Started Guide and VMware Cloud Foundation Operations and Administration Guide. ■ For information on designing the VI workload domain, refer to VMware Cloud Foundation Design Guide for a Virtual Infrastructure Workload Domain.

Note Advanced Load Balancing for VMware Cloud Foundation solution currently does not support VCF Workload Domains which require load balancing on federated networks configured using NSX Federation.

Overview of Advanced Load Balancing for VMware Cloud Foundation

By applying the Advanced Load Balancing for VMware Cloud Foundation validated solution, you implement centralized load balancing (LB) for your application workloads within VMware Cloud Foundation and can configure enterprise grade load-balancing, global server load balancing, application security, and container ingress services.

Note NSX Advanced Load Balancer was formerly known as Avi. These represent the same product and are used interchangeably in this document.

Implementation Overview of Advanced Load Balancing for VMware Cloud Foundation

Stage	Steps
Implementation Overview of Advanced Load Balancing for VMware Cloud Foundation	Work with the technology team of your organization on configuring the network in the data center. Collect the environment details and write them down in the Chapter 4 Planning and Preparation of Advanced Load Balancing for VMware Cloud Foundationworkbook.
Deploy and configure Avi Control plane	1 Deploy NSX Advanced Load Balancer Controller VMs for central management of load balancing services. 2 Configure NSX Advanced Load Balancer Controller cluster.
Configure infrastructure on the NSX Advanced Load Balancer Controller to enable fully automated load balancing	1 Configure NSX-T Cloud on the NSX Advanced Load Balancer Controller. 2 Configure NSX Advanced Load Balancer Service Engine Groups for application isolation. 3 Configure a reference load-balanced application.

Update History

This Advanced Load Balancing for VMware Cloud Foundation is updated when necessary.

Revision	Description
20 Mar 2023	The validated solution now supports VMware Cloud Foundation 5.0.
30 October 2023	The validated solution now supports VMware Cloud Foundation 5.0.
11 October 2023	The validated solution now supports VMware Cloud Foundation 4.5.0, 4.5.1.
22 February 2022	The validated solution now supports VMware Cloud Foundation 4.4.0. This validated solution now supports registering NSX Advanced Load Balancer with Cloud Services to consume NSX Advanced Load Balancer with Cloud Services SaaS Subscriptions.
05 October 2021	The validated solution now supports VMware Cloud Foundation 4.3.1.
24 August 2021	Initial draft

Design Objectives of Advanced Load Balancing for VMware Cloud Foundation

2

The Advanced Load Balancing for VMware Cloud Foundation validated solution has objectives to deliver prescriptive content about the solution so that its fast to deploy and is suitable for use in production environments.

Objective	Description
Main Objective	Provide centralized enterprise grade load balancing services for VMware Cloud Foundation through the NSX Advanced Load Balancer.
Scope of guidance	■ Implementation ■ Configuration ■ Operational guidance ■ Solution interoperability ■ Deployment and initial configuration of NSX Advanced Load Balancer for workload domains ■ Operations for the NSX Advanced Load Balancer components such as monitoring and alerting, backup and restore, post-maintenance validation, and upgrade.

Scope of implementation	■ Configuration of load balancing with Advanced Load Balancing for VMware Cloud Foundation.
	■ Ecosystem integration configuration for automated load balancing with:
	  ■ NSX Manager
	  ■ vCenter Server
	■ Guidance for automated Load Balancing consumption on NSX Managed
	  ■ Overlay -backed segments and/ or
	  ■ VLAN-backed segments
	Note Scope of this guidance will not replace LB for the vRealize suite in the management workload domain.

Supported VMware Cloud Foundation architecture models	■ Standard ■ Consolidated
Supported workload domain	■ Consolidated management and workload domain ■ Virtual Infrastructure workload domain
Load-balanced application scale	Load-balanced application scale
Load Balancer scale	NSX Advanced Load Balancer Service Engines up to 400 per NSX Advanced Load Balancer Controller

Objective	Description
Cloud type	Private cloud
Availability	99%
Certificate signing	Certificates are signed by a certificate authority (CA) that consists of a root and intermediate certificate authority layers.

Detailed Design of Advanced Load Balancing for VMware Cloud Foundation

3

The design considers the components of the Advanced Load Balancing for VMware Cloud Foundation validated solution. It includes numbered design decisions, and the justification and implications of each decision.

Read the following topics next:

- Logical Design of Advanced Load Balancing for VMware Cloud Foundation
- Deployment Specification of Advanced Load Balancing for VMware Cloud Foundation
- Easy Deployment of NSX Advanced Load Balancer Integration with VMware Cloud Foundation
- Network Design for Advanced Load Balancing for VMware Cloud Foundation
- Lifecycle Management for Advanced Load Balancing for VMware Cloud Foundation
- Information Security and Access of Advanced Load Balancing for VMware Cloud Foundation

Logical Design of Advanced Load Balancing for VMware Cloud Foundation

The logical design provides a high-level overview of the solution design.

NSX Advanced Load Balancer (Formerly known as Avi Networks) provides multi-cloud load balancing, web application firewall, application analytics and container ingress services from the data center to the cloud. It is built on software-defined principles which separate the data plane from the control plane. The platform provides a centrally managed, dynamic pool of load balancing resources on commodity x86 servers, VMs or containers, to deliver granular services close to individual applications. This allows network services to scale near infinitely without the added complexity of managing hundreds of disparate appliances.

NSX Advanced Load Balancer can be configured in the following editions:

- NSX Advanced Load Balancer Enterprise with Cloud Services Edition, which provides all features that NSX Advanced Load Balancer has to offer along with value added SaaS delivered Cloud Services (Available from NSX Advanced Load Balancer v21.1.3 or later).

- NSX Advanced Load Balancer Enterprise Edition, which provides enterprise feature set that VMware NSX Advanced Load Balancer has to offer including load balancer, GSLB, WAF, Container Ingress and more.
- NSX Advanced Load Balancer Basic Edition, which is a replacement edition for NSX LB with restricted features equivalent to NSX Advanced Load Balancer.

The platform is comprised of the following components:

NSX Advanced Load Balancer Controller

The NSX Advanced Load Balancer Controller, as its name implies, implements the control plane for the NSX Advanced Load Balancer. It is the single point of management and control that serves as the 'brain' for the solution and for high availability is typically deployed as a three-node cluster. In a VMware Cloud Foundation, NSX Advanced Load Balancer Controllers run as VMs in the management VI workload domain.

VMware NSX Advanced Load Balancer Cloud Services

VMware *NSX Advanced Load Balancer* Cloud Services enables value added operational capabilities to the VMware *NSX Advanced Load Balancer* deployments delivered through the Cloud Services Portal including Central Licensing, Live Security Threat Intelligence, Proactive Support and more.

Note This is available for VMware *NSX Advanced Load Balancer* deployments running v21.1.3 or later.

NSX Advanced Load Balancer Service Engine

NSX Advanced Load Balancer Service Engine implements the data plane for the NSX Advanced Load Balancer. The NSX Advanced Load Balancer SEs perform load balancing for the configured applications.

NSX Advanced Load Balancer Admin Console

The NSX Advanced Load Balancer Admin Console is a modern web-based user interface that provides role-based access to control, manage and monitor applications. Its capabilities are likewise available via the NSX Advanced Load Balancer CLI. All services provided by the platform are available as REST API calls to enable IT automation, developer self-service, and a variety of third-party integrations. The NSX Advanced Load Balancer Admin Console is hosted by default on the Controller and can be accessed via the NSX Advanced Load Balancer Controller cluster FQDN/IP address.

Cloud Connectors

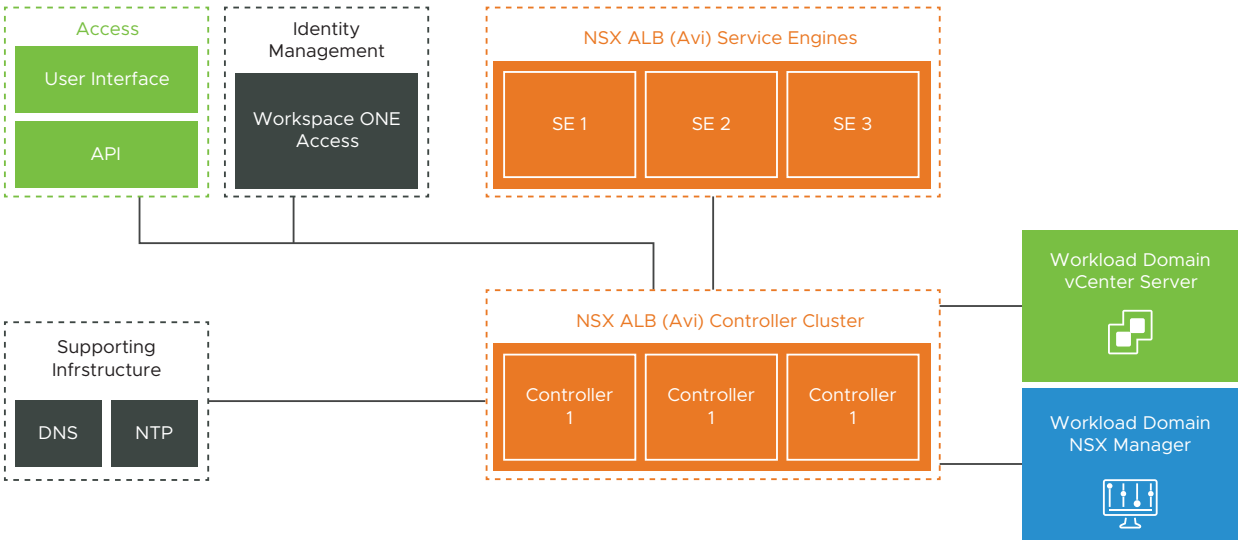
Cloud Connectors provide ecosystem integrations to enable automated life-cycle-management of the Service Engines and load-balanced applications that are configured on the NSX Advanced Load Balancer Controllers. Automation includes deploying, configuring and scaling NSX Advanced Load Balancer Service Engines, placing load-balanced applications on the right set of the Service Engines and much more.

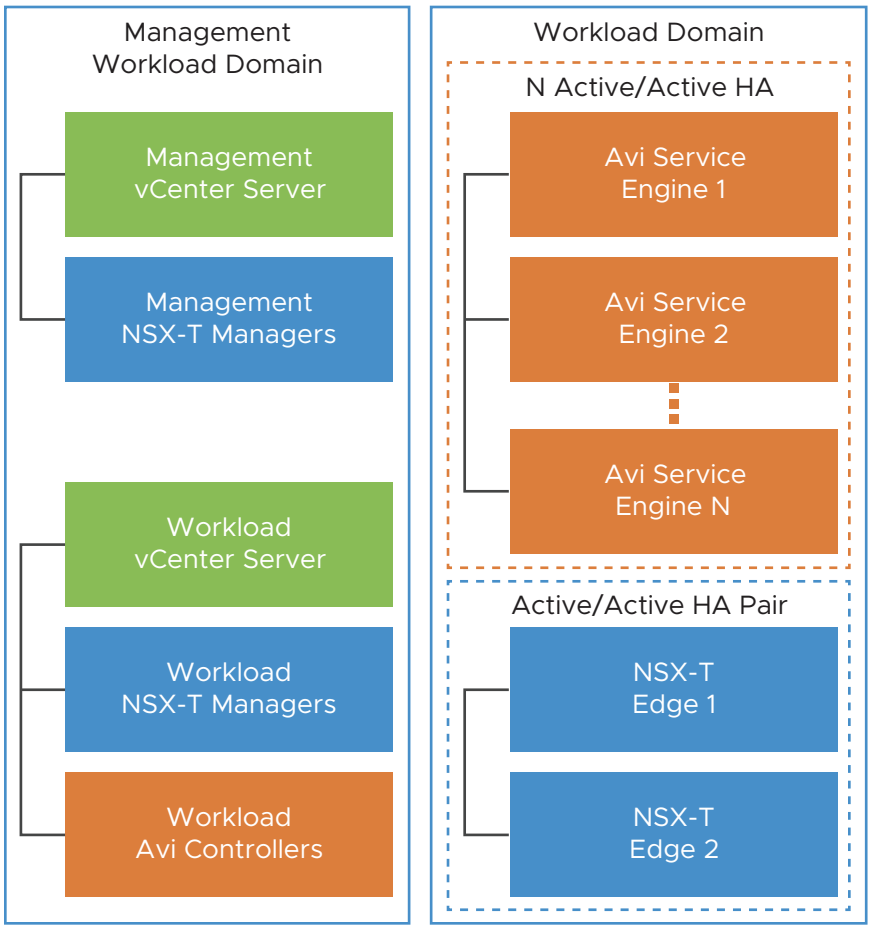
Advanced Load Balancing for VMware Cloud Foundation solution will provide guidance to implement NSX-T Cloud Connector integration, which will enable automated life-cycle-management for load-balanced applications that will be deployed on the NSX Advanced Load Balancer in the VMware Cloud Foundation on NSX-T managed networks.

Load Balancing Architecture for VMware Cloud Foundation

NSX Advanced Load Balancer will leverage the NSX-T Cloud Connector integration to provide fully automated load-balancing for VMware Cloud Foundation. NSX Advanced Load Balancer components are mapped to the specific workload domains.

Each NSX-T Data Center deployment managing virtual infrastructure (VI) workload domains will require an independent NSX Advanced Load Balancer Controller cluster to be deployed. The NSX Advanced Load Balancer Controller cluster will manage the Service Engines which will be deployed in the VI workload domains that the NSX-T Data Center manages and will provide load balancing services. Multiple NSX Advanced Load Balancer Controller clusters within a single VMware Cloud Foundation stack might be created in case of multiple NSX-T Data Center instances are used to manage the VI workload domains.





Deployment Specification of Advanced Load Balancing for VMware Cloud Foundation

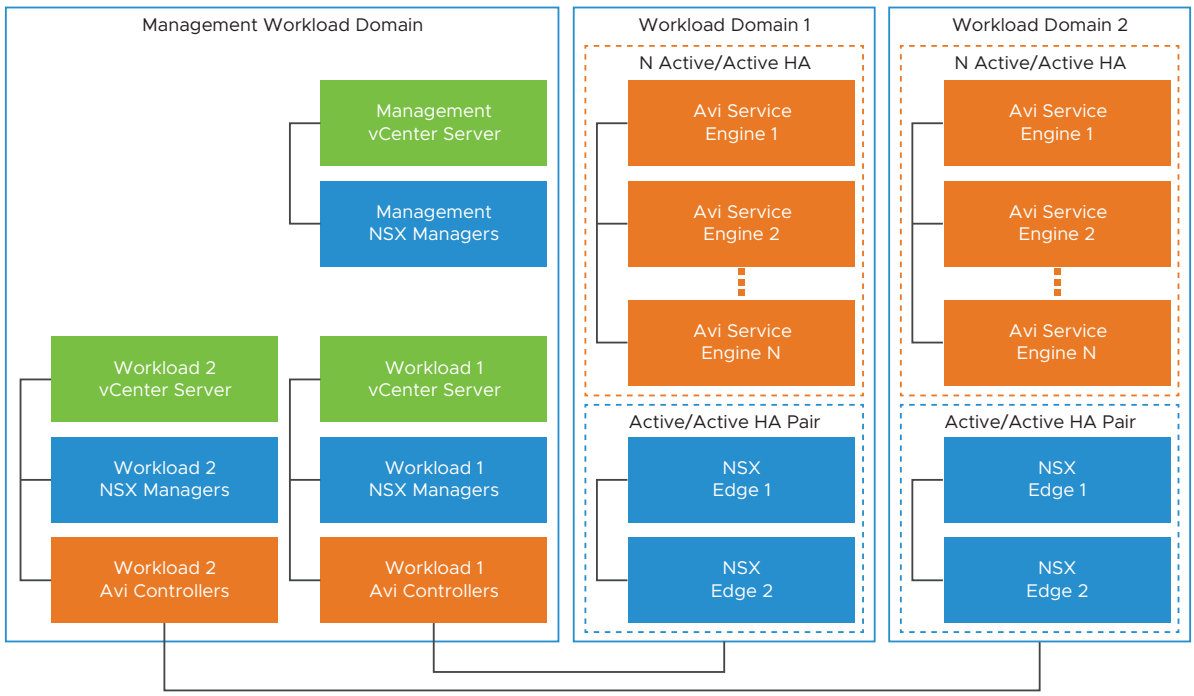
The deployment specification details the design decisions covering physical design, virtual design, and sizing for the NSX Advanced Load Balancer.

Deployment Model for Advanced Load Balancing for VMware Cloud Foundation

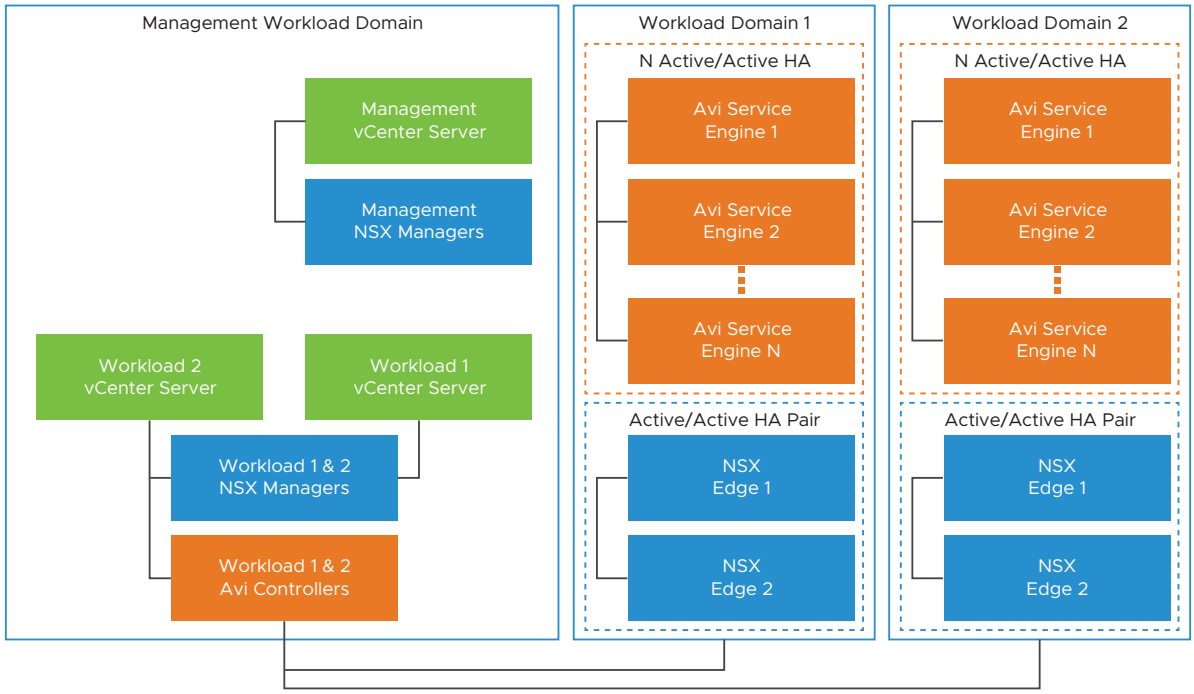
Deployment model of the NSX Advanced Load Balancer validated solution for VMware Cloud Foundation will follow these rules:

1 A unique NSX Advanced Load Balancer deployment needs to be created for every unique NSX-T Data Center deployment in the VMware Cloud Foundation. This NSX Advanced Load Balancer deployment will be associated with the corresponding NSX-T Data Center deployment.

2 Multiple NSX Advanced Load Balancer deployments could be created if multiple NSX-T Data Center deployments exist within the VMware Cloud Foundation. Refer to the following image which shows that one NSX Advanced Load Balancer Controller cluster is managing one workload domain. Each deployment of NSX Advanced Load Balancer is mapped to each deplyment of a NSX, here each NSX manages a single workload domain.



3 A single NSX Advanced Load Balancer deployment will provide load balancing services to all the VI workload domains that are serviced by the associated NSX-T Data Center deployment. Refer to the following image which shows one NSX Advanced Load Balancer Controller cluster managing multiple workload Domains. Each deployment of NSX Advanced Load Balancer is mapped to each deplyment of a NSX, here each NSX manages a multiple workload domains.



4 NSX Advanced Load Balancer Controllers will be deployed in the management domain

5 The Service Engines are deployed in the VI workload domain in which the NSX Advanced Load Balancer is providing load balancing services.

6 All SEs deployed in a VI workload domain are managed by the Controller that is part of the NSX Advanced Load Balancer deployment that is associated with the corresponding NSX-T Data Center managing the VI workload domain.

Advanced Load Balancing for VMware Cloud Foundation will utilize the NSX-T Cloud Connector integration. NSX-T Cloud Connector integration is an abstraction for an NSX transport zone. Each NSX-T Cloud Connector created on the NSX Advanced Load Balancer Controller provides load balancing services for all VI workload domains, i.e. vCenter Server(s) that share an NSX transport zone. You can create a new NSX-T Cloud Connector for each new NSX transport zone.

Note

- Multiple NSX-T Cloud Connectors can be configured on the same NSX Advanced Load Balancer Controller, i.e the same NSX Advanced Load Balancer deployment
- Multiple NSX-T Cloud Connectors configured on the same NSX Advanced Load Balancer Controller can point to the same NSX Manager cluster, provided there is a unique transport zone.
- Each NSX-T Cloud Connector can manage multiple vCenters Servers, i.e. can span multiple VI workload domains.

Table 3-1. *Design Decisions for Deploying the Controller for the VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-001	Initial setup should be done only on one NSX Advanced Load Balancer Controller VM out of the three deployed to create an NSX Advanced Load Balancer Controller cluster.	NSX Advanced Load Balancer Controller cluster is created from an initialized NSX Advanced Load Balancer Controller which becomes the cluster leader. Follower NSX Advanced Load Balancer Controller nodes need to be uninitialized to join the cluster.	NSX Advanced Load Balancer Controller cluster creation will fail if more than one NSX Advanced Load Balancer Controller is initialized.
AVI-CTLR-002	Apply vSphere DRS anti-affinity rules for the NSX Advanced Load Balancer Controller cluster nodes. **Note** For a default management vSphere cluster that consists of four ESXi hosts, you can put in maintenance mode only a single ESXi host at a time.	Ensure that NSX Advanced Load Balancer Controller VMs are distributed across ESXi hosts .	You must perform additional configuration to set up an anti-affinity rule.
AVI-CTLR-003	Protect NSX Advanced Load Balancer Controller cluster nodes using vSphere High Availability.	Supports the availability objectives for the NSX Advanced Load Balancer Controller cluster without requiring manual intervention during an ESXi host failure event.	None

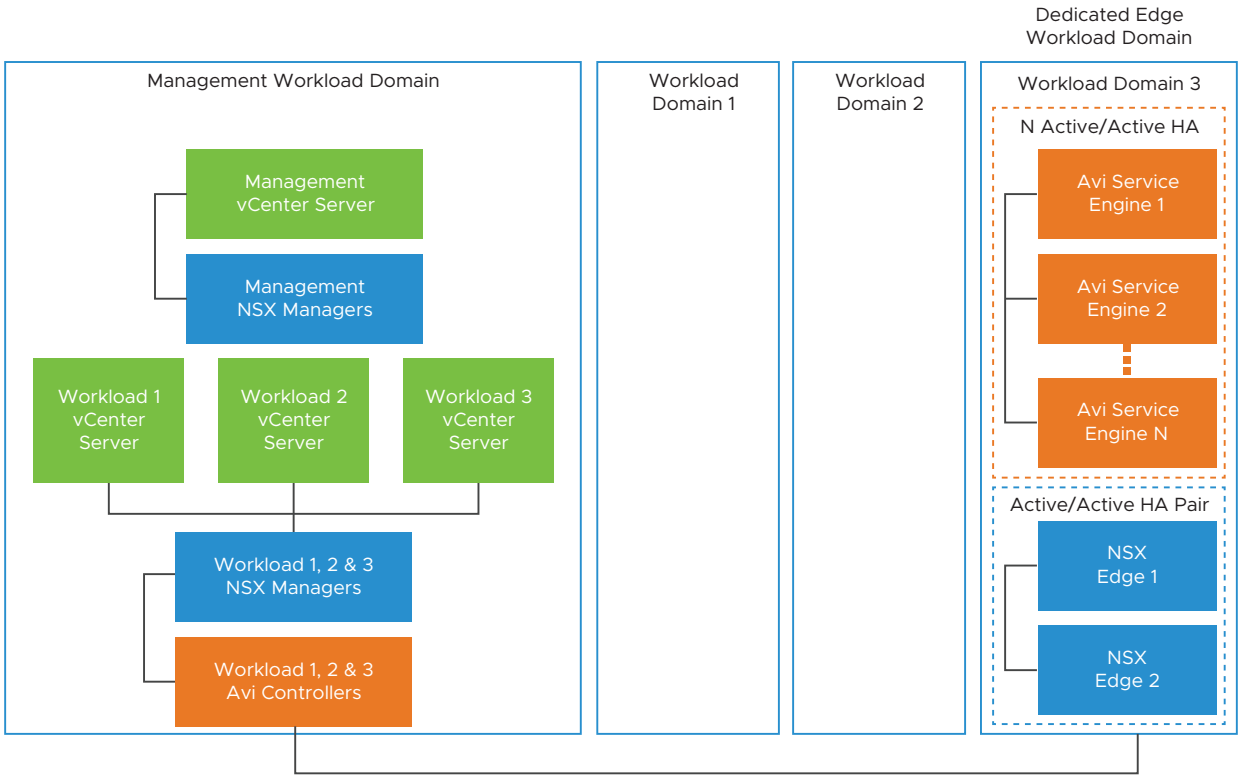
Table 3-2. *Design Decisions for deploying Service Engines for the VMware NSX Advanced Load Balancer*

Decision ID	Decision Design	Design Justification	Design Implication
AVI-CTLR-004	Create an NSX-T Cloud Connector on NSX Advanced Load Balancer Controller for each NSX transport zone requiring load balancing.	A NSX-T Cloud Connector configured on the NSX Advanced Load Balancer Controller will provide load balancing for workloads belonging to a Transport Zone on NSX-T. **Note** 1. A NSX Transport Zone can be unique to a vCenter cluster, a VI Workload Domain or can be shared across VI workload domains. 2. Multiple NSX-T Cloud connectors can be configured on the NSX Advanced Load Balancer Controller if load balancing is required across multiple Transport Zones configured on NSX-T.	None

Dedicated Edge VI Workload Domain

A dedicated edge VI workload domain is a workload domain created solely for the use of edge services. This is an optional deployment decision that customer could take to host networking services such as load balancing centrally when multiple VI workload domains share an NSX instance.

If the dedicated edge VI workload domain is large enough to support the capacity needs for hosting all the required Service Engines across all the VI workload domains managed by its NSX-T Data Center instance, then the Service Engines could be centrally deployed in this edge VI workload domain.



Note Workload Domain 3 is the dedicated edge VI workload domain.

Table 3-3. *Design Decisions for deploying Service Engines on a Dedicated Edge VI Workload Domain for NSX Advanced Load Balancer Platform*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-005	Choose to deploy the Service Engines on a dedicated edge VI workload domain.	Allows for centralized placement of the Service Engines.	Capacity growth might be a challenge. Might not work in all cases due to scale restrictions of the edge VI workload domain.
AVI-CTLR-006	Create separate Service Engine Groups to host Virtual Services from different VI workload domains.	Allows for application isolation.	Might require additional Service Engine resources.

Deployment of NSX Advanced Load Balancer Controller for Multiple Availability Zones

In an environment with multiple availability zones, the NSX Advanced Load Balancer Controller nodes run in the first availability zone. If a failure occurs in the first availability zone, the NSX Advanced Load Balancer Controller nodes are failed over to the second availability zone.

NSX Advanced Load Balancer Controller

NSX Advanced Load Balancer Controller cluster requires two out of three nodes to be up, for the control plane to continue regular function. It is recommended that all three nodes of the NSX Advanced Load Balancer Controller cluster are deployed on ESXi hosts residing in the first availability zone.

Note

- vSphere HA will recover the NSX Advanced Load Balancer control plane upon a fault domain failure event.
- vSphere DRS will re-balance the NSX Advanced Load Balancer Controller placement onto the ESXi hosts in the first availability zone.
- NSX Advanced Load Balancer Controller deployment should follow the requirements of a single availability zone design.

Table 3-4. *Design Decisions on Deployment of NSX Advanced Load Balancer Controllers in Multiple Availability Zones*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-VC-001	When using two availability zones, add the NSX Advanced Load Balancer Controller cluster nodes to the first availability zone VM group.	Ensures that, by default, the NSX Advanced Load Balancer Controller cluster nodes are powered on in the primary availability zone hosts group.	After the implementation of the second availability zone for the management domain, you must update the VM group for the primary availability zone virtual machines to include the NSX Advanced Load Balancer Controller cluster nodes.

NSX Advanced Load Balancer Service Engine

Applications requiring load balancing, might intend to use High-Availability between the two stretched locations. In such a situation care must be taken to place NSX Advanced Load Balancer SEs between the two physical locations and to carefully place load-balanced applications on these NSX Advanced Load Balancer SEs.

Table 3-5. *Design Decisions for placing applications on NSX Advanced Load Balancer Service Engines in a Multi Availability Zone environment*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-VC-002	Create a VM groups for the NSX Advanced Load Balancer SE VMs.	Ensures that the NSX Advanced Load Balancer SE VMs can be managed as a group and added to VM/ Host rules.	User must add each NSX Advanced Load Balancer SE VM to the primary availability zone.
AVI-VI-VC-003	Create a should-run VM-Host affinity rule to run all NSX Advanced Load Balancer SEs on the group of hosts in the first availability zone.	Ensures that all NSX Advanced Load Balancer SE VMs are in the first availability zone.	During normal operation, there would not be any NSX Advanced Load Balancer SEs running in the second availability zone. Therefore all apps would be active in the first availability zone.

Integration Design of Advanced Load Balancing for VMware Cloud Foundation

NSX Advanced Load Balancer integrates with vCenter and NSX to provide a fully automated lifecycle management for load balanced applications and offers flexibility to isolate applications to cater to any business need.

NSX-T Cloud Connector Integration

The NSX-T Cloud Connector integration will be utilized on the Advanced Load Balancing for VMware Cloud Foundation. NSX-T Cloud Connector integration provides automated life cycle management for load-balanced applications and the Service Engines. The Service Engines and load-balanced applications are assigned to a Cloud.

Life cycle management includes operations like Service Engine image upload, VM creation and deletion, network placement and programming, IP address assignment, NSGroup and NSService creation on NSX-T Data Center and much more.

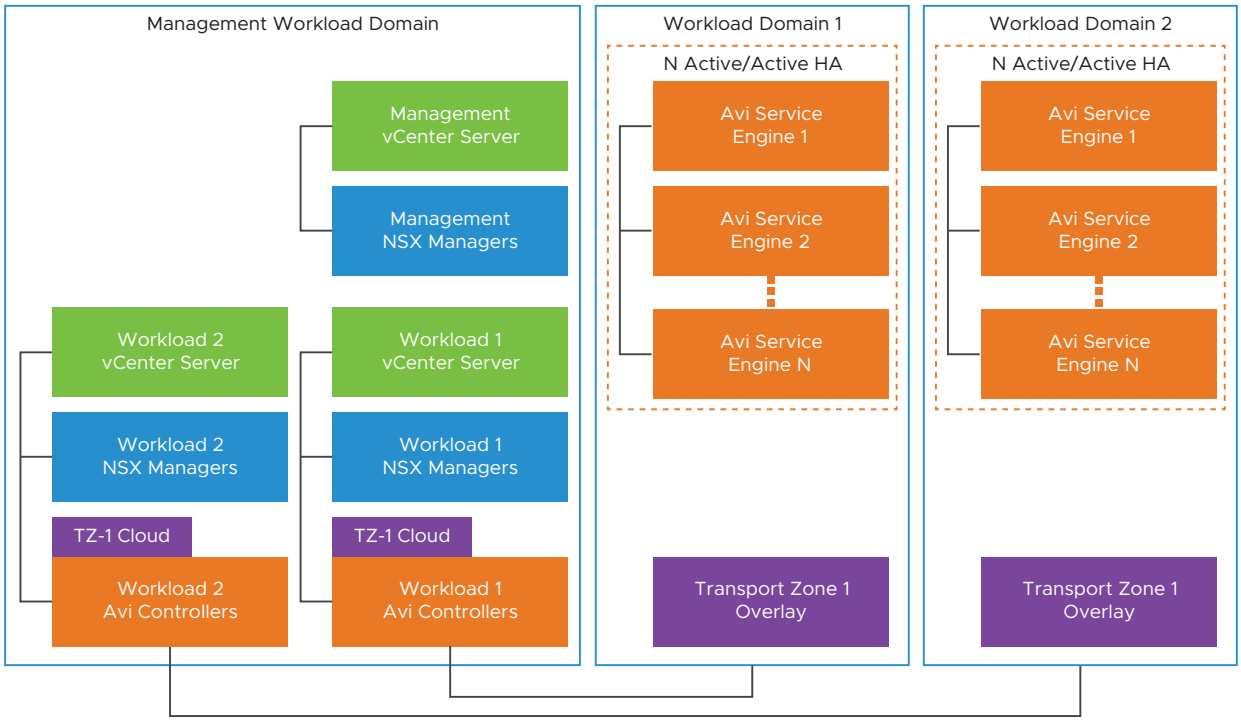
NSX Advanced Load Balancer provides two types of NSX-T Cloud connector integrations:

1. Overlay: Provide load balancing for applications deployed on overlay transport zones. Data networks for the Service Engines are attached to logical segments connected to Tier-1 routers. The Controller automatically inject a static route for the VIP into the Tier-1 router for connectivity.
2. VLAN: Provide load balancing for applications deployed on VLAN transport zones. Data networks for the Service Engines are attached to VLAN segments. The Service Engines will Address Resolution Protocol (ARP) for the VIP for connectivity.

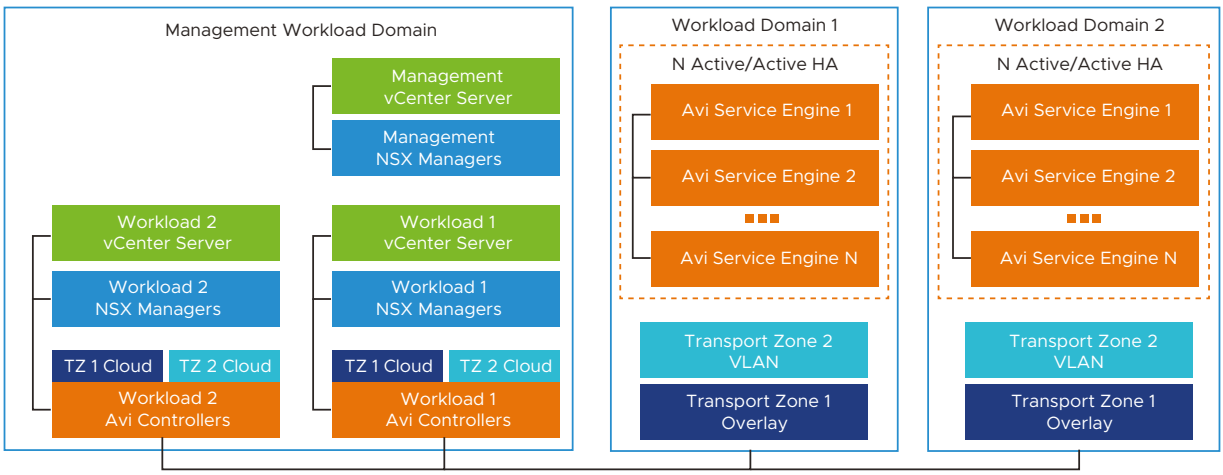
NSX-T Cloud Connector Configuration Models

An NSX-T Cloud connector are scoped to an NSX Manager cluster endpoint and a NSX transport zone. Therefore, for every new combination of NSX Manager cluster, NSX transport zone, a new NSX-T Cloud connector will be created on the Controller. The following models demonstrate typical configurations for VMware Cloud Foundation:

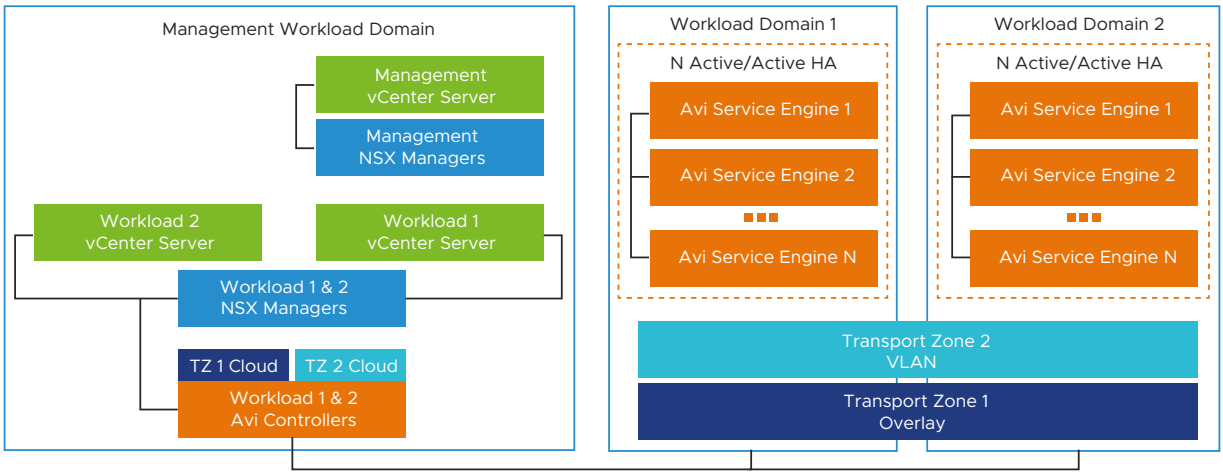
Dedicated NSX Manager cluster for each VI workload domain. Each NSX-T Data Center instance is configured with a single transport zone. You need to create a single NSX-T Cloud connector on the Controller for this transport zone.



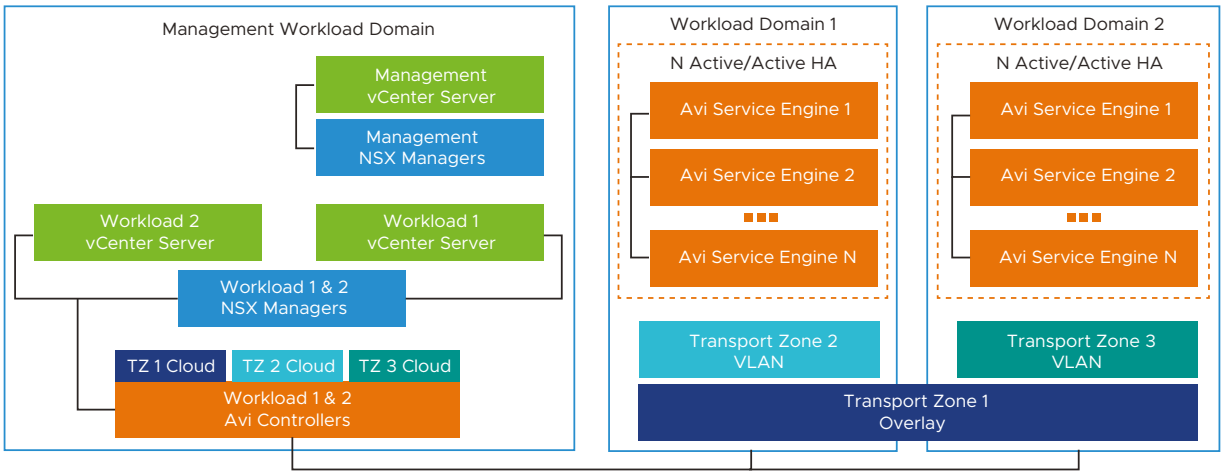
Dedicated NSX Manager cluster for each VI workload domain. Each NSX-T Data Center instance is configured with two transport zones. You need to create a unique NSX-T Cloud connector on the Controller for each of these transport zones.



Shared NSX Manager cluster between multiple VI workload domains. The NSX-T Data center instance is configured with two transport zones. Transport zones are stretched across VI Workload Domains. You need to create a unique NSX-T Cloud connector on the Controller for each of these transport zones.



Shared NSX Manager cluster between multiple VI workload domains. NSX-T Data Center instance is configured with three transport zones. One transport zones is stretched across VI Workload Domains. You need to create a unique NSX-T Cloud connector on the Controller for each of these transport zones.



Note NSX Edges have been omitted from the above figures depicting the NSX-T Cloud models.

Table 3-6. *Design Decisions for creating an NSX-T Cloud on the Controller for the VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-007	Create one NSX-T Cloud connector object on the Controller per transport zone configured on the NSX manager cluster that requires Load Balancing services. **Note** Transport zone could be dedicated to a VI workload domain or shared across VI workload domains.	Provides automated deployment of load-balanced applications through NSX-T Cloud integration. Allows for maximum flexibility, control, and isolation in terms of application deployment.	None
AVI-CTLR-008	Provide either a overlay-backed NSX segment connected to a Tier-1 logical router or a VLAN-backed NSX segment for the Service Engine management for the NSX-T Cloud of overlay type.	This network is used for the Controller to the Service Engine connectivity.	None
AVI-CTLR-009	Provide one or more NSX managed VLAN segments as data networks for the NSX-T Cloud connector of VLAN type. **Note** A single NSX-T Cloud connector of VLAN type can contain multiple data networks. Each data network should belong to a unique NSX managed VLAN segment.	The Service Engines are placed on NSX managed VLAN segments.	None

Table 3-6. *Design Decisions for creating an NSX-T Cloud on the Controller for the VMware Cloud Foundation* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-010	Provide a Tier-1 router and a connected overlay-backed NSX segment as data network for the NSX-T Cloud of overlay type. **Note** A single NSX-T Cloud connector of overlay type can contain multiple data networks. Each data network must belong to a unique Tier-1 router.	The Service Engines are placed on Overlay Segments created on these Tier-1 logical router(s).	None
AVI-CTLR-011	Provide an object name prefix when creating the NSX-T Cloud Connector on the NSX Advanced Load Balancer Controller.	Used for uniquely identifying NSX-T Cloud Connector created resources on NSX Manager cluster and vCenter Server.	None

Isolation Model for Load-Balanced Applications

NSX Advanced Load Balancer provides two ways of isolating load-balanced applications and the Service Engines.

1 Tenancy: Used for configuration isolation and optionally NSX Advanced Load Balancer Service Engine isolation.

2 Service Engine Groups: Used for NSX Advanced Load Balancer Service Engine isolation.

Tenancy Configuration

Admins can choose to deploy NSX Advanced Load Balancer in one of three levels of isolation modes with respect to tenancy.

- Provider/ Admin Tenant mode: All the Service Engines and configurations will reside in the ‘admin’ tenant. Provides least isolation.
- Config isolation Tenant mode: All the Service Engines will reside in the ‘admin’ tenant and are shared across the configured Tenants. Configurations will be scoped under each configured Tenant
- Config and Data isolation Tenant mode: The Service Engines as well as configuration will be scoped under each configured Tenant. Provides most isolation.

Reference examples of providing isolation through tenancy is to create a unique tenant for:

1 Each VI workload domain that the NSX Advanced Load Balancer provides load balancing services for.

2 Each line of business that the NSX Advanced Load Balancer provides load balancing services for.

3 Each of development, testing, production areas where the NSX Advanced Load Balancer provides load balancing services for.

Table 3-7. *Design Decisions for creating a Tenants for isolation on the VMware NSX Advanced Load Balancer for the VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-012	Create tenants to provide desired level of isolation for the VMware Cloud Foundation. **Note** NSX Advanced Load Balancer - Basic Edition does not provide tenant isolation.	Provides required level of configuration and data plane isolation for workloads.	Additional Service Engine resources might be required.

Service Engine Group Configuration

The Service Engine Groups provide the Service Engine isolation and thereby provide load-balanced application isolation within a tenant configured on the NSX Advanced Load Balancer.

The NSX Advanced Load Balancer Service Engine are created within a Service Engine Group, which contains the definition of how the Service Engines should be sized, placed, and made highly available. Each NSX-T Cloud connector will have at least one Service Engine Group. The Service Engines may only exist within one group and are never shared between the Service Engine Groups. Load-balanced applications are scoped to a Service Engine Group.

Note

- The Service Engine Group objects are scoped under the NSX-T Cloud connector objects only.
- Only Active/ Standby HA Mode is supported for the Basic license tier.

Table 3-8. *Design Decisions for Service Engine Group Design for VMware NSX Advanced Load Balancer for the VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-013	Create multiple Service Engine Groups as desired to isolate applications. **Note** Some of the criteria for grouping applications in different Service Engine Group(s) could be based on: ■ Multiple line of business ■ Prod v/s non-Prod ■ Different scale and performance requirements	Allows efficient isolation of applications and allows for better capacity planning. Allows flexibility of life-cycle-management.	None
AVI-CTLR-014	Create separate set of Service Engine Groups for each VI workload domain and scope the Service Engine Group to the VI workload domain vCenter server. **Note** ■ Applicable where a single Controller cluster serving multiple VI workload domains. ■ If applications need to be shared across VI workload domains, then the Service Engine Group could be scoped to multiple vCenter Servers.	Allows isolation of the Service Engines across VI workload domains. Enables per VI workload domain life-cycle-management.	None
AVI-CTLR-015	Configure Service Engine Group for Active/ Active HA mode. **Note** Legacy Active/ Standby HA mode might be required for certain applications.	Provides optimum resiliency, performance, and utilization.	Certain applications might not work in Active/ Active mode. For instance, applications that require preserving client IP. In such cases, use the Legacy Active/ Standby HA mode.

Table 3-8. *Design Decisions for Service Engine Group Design for VMware NSX Advanced Load Balancer for the VMware Cloud Foundation* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-016	Enable 'Dedicated dispatcher CPU' on Service Engine Groups that contain the Service Engine VMs of 4 or more vCPUs. **Note** This setting should be enabled on SE Groups that are servicing applications that have high network requirement.	This will enable a dedicated core for packet processing enabling high packet pipeline on the Service Engine VMs. **Note** By default, the packet processing core also processes load balancing flows.	None .
AVI-CTLR-017	Set 'Placement across the Service Engines' setting to 'distributed'.	This allows for maximum fault tolerance and even utilization of capacity.	Might require more Service Engine VMs as compared to 'compact' placement mode.
AVI-CTLR-018	Enable CPU and Memory reservation on the Service Engine Group. .	The Service Engines are a critical infrastructure component providing load-balancing services to mission critical applications.	None
AVI-CTLR-019	Configure a consistent Service Engine Name Prefix that indicates the Service Engine VM for instance, 'avise-xxxx'. **Note** Where ‘xxxx’ could be used as an arbitrary identifier.	This allows efficient grouping and filtering.	None
AVI-CTLR-020	Choose the Service Engine Group mode as Legacy HA Active/ Standby if the Controller is set to use basic edition. .	NSX Advanced Load Balancer Controller in Basic Edition only supports Legacy HA Active/ Standby mode.	Applications will not be deployed in an Active/ Active fashion, thereby losing out on elastic capacity management. NSX Advanced Load Balancer Enterprise Edition will allow Active/ Active as well as Legacy Active/ Standby deployments.

Physical Design of the Advanced Load Balancing for VMware Cloud Foundation

These design decisions are recommendations for the optimum functioning of the NSX Advanced Load Balancer.

Table 3-9. *Design Decisions for Physical Design of ESXi Hosts to support the VMware NSX Advanced Load Balancer*

Decision ID	Design Description	Design Justification	Design Implication
AVI-PHY-001	Provide high performance disks (SSD/ Flash) to hosts that run the Controller VMs.	The Controllers need high performance disks to process the analytics pipeline.	None
AVI-PHY-002	Enable AES-NI instructions setting in the BIOS for ESXi hosts.	AES-NI instruction set provides efficiency in SSL performance.	Most modern machines have AES-NI enabled by default, if not enabled by default, you need to reboot ESXi hosts to enable this setting.
AVI-PHY-003	Disable C-State and P-State settings in BiOS on the ESXi hosts. **Note** This is an optional design decision.	Provides maximum performance.	This might require a reboot and reconfigure of the BIOS causing an outage for each ESXi host.

vCenter Server Design of the Advanced Load Balancing for VMware Cloud Foundation

vCenter Server design of the Advanced Load Balancing for VMware Cloud Foundation.

Table 3-10. *Design Decisions for the Virtual Infrastructure to support the VMware NSX Advanced Load Balancer*

Decision ID	Design Description	Design Justification	Design Implication
AVI-VI-VC-004	Create anti-affinity 'VM/ Host' rule that prevents collocation of the Controller VMs.	vSphere will take care of placing the Controller VMs in a way that always ensures maximum HA for the Controller cluster.	None
AVI-VI-VC-005	Create a virtual machine group for the Controller VMs.	Ensures that the Controller VMs can be managed as a group.	You must add virtual machines to the allocated groups manually.
AVI-VI-VC-006	In vSphere HA, for each Controller and Service Engine VMs, set the restart priority policy to high and host isolation response to disabled.	This ensures fast recovery for the NSX Advanced Load Balancer.	None

Table 3-10. *Design Decisions for the Virtual Infrastructure to support the VMware NSX Advanced Load Balancer* (continued)

Decision ID	Design Description	Design Justification	Design Implication
AVI-VI-VC-007	Create one Content Library on the management domain to store Controller OVA.	Deploying OVA from the Content Library will be operationally easy to do.	Might not be necessary if deploying Controller VMs using automation tools such as vRO, Ansible, etc.
AVI-VI-VC-008	Create one Content Library on each of the VI workload domain to store Service Engine OVA.	The Controller's NSX-T Cloud Connector requires a Content Library configured to create the Service Engines.	None

Users and Roles required by the Advanced Load Balancing for VMware Cloud Foundation

The Controller(s) interacts with vCenter Server and NSX-T Managers clusters to provide full lifecycle management of the Service Engines. This requires users in vCenter Server and NSX-T Manager cluster with specific roles and permissions to exist or be created.

vCenter Server Access Control for NSX Advanced Load Balancer Controller

Create a vCenter Server Service Account (user) with a role having the following permissions. This user can be used by the NSX Advanced Load Balancer Controller to interact with the vCenter Server and provide lifecycle management for the Service Engines.

The NSX-T cloud connector interacts with vCenter for Service Engine (SE) lifecycle management, and with NSX-T manager to sync and create objects for networking and security. For this, the admin needs to configure vCenter and NSX-T user credentials which have required permissions for NSX Advanced Load Balancer to be able to perform these operations.

Category	Privilege	Sub-Privilege
Content Library	■ Add library item ■ Delete library item ■ Update files ■ Update library item	
Date Store	■ Allocate space ■ Remove file	
Folder	Create Folder	
Network	■ Assign network ■ Remove	
Resource	Assign virtual machine to resource pool	
Tasks	■ Create task ■ Update task	

Category	Privilege	Sub-Privilege
vApp	■ Add virtual machine ■ Assign resource pool ■ Assign vApp ■ Create ■ Delete ■ Export ■ Import ■ Power off ■ Power on ■ vApp application configuration ■ vApp instance configuration	
Virtual machine	Change configuration	■ Add existing disk ■ Add new disk ■ Add or remove device ■ Advanced configuration ■ Change CPU count ■ Change Memory ■ Change Settings ■ Change resource ■ Display connection settings ■ Extend virtual disk ■ Remove disk
	Edit inventory	■ Create new ■ Remove inventory
	Interaction	■ Connect devices ■ Install VMware Tools ■ Power off ■ Power on
	Provisioning	■ Allow disk access ■ Allow file access ■ Allow read-only disk access ■ Deploy template ■ Mark as virtual machine

Note **Propagate to children** checkbox must be checked for vCenter user having global permissions.

AviRole - Global

Category	Privilege	Sub-Privilege
Content Library	■ Add library item ■ Delete library item ■ Update files ■ Update library item	
Date Store	■ Allocate space ■ Remove file	
Folder	Create Folder	
Network	■ Assign network ■ Remove	
Resource	Assign virtual machine to resource pool	
Tasks	■ Create task ■ Update task	
vApp	■ Add virtual machine ■ Assign resource pool ■ Assign vApp ■ Create ■ Delete ■ Export ■ Import ■ Power off ■ Power on ■ vApp application configuration ■ vApp instance configuration	
Virtual machine	Change configuration	■ Add existing disk ■ Add new disk ■ Add or remove device ■ Advanced configuration ■ Change CPU count ■ Change Memory ■ Change Settings ■ Change resource ■ Display connection settings ■ Extend virtual disk ■ Remove disk
	Edit inventory	■ Create new ■ Remove inventory

Category	Privilege	Sub-Privilege
	Interaction	■ Connect devices ■ Install VMware Tools ■ Power off ■ Power on
	Provisioning	■ Allow disk access ■ Allow file access ■ Allow read-only disk access ■ Deploy template ■ Mark as virtual machine

Note **Propagate to children** checkbox must be selected for vCenter user having global permissions.

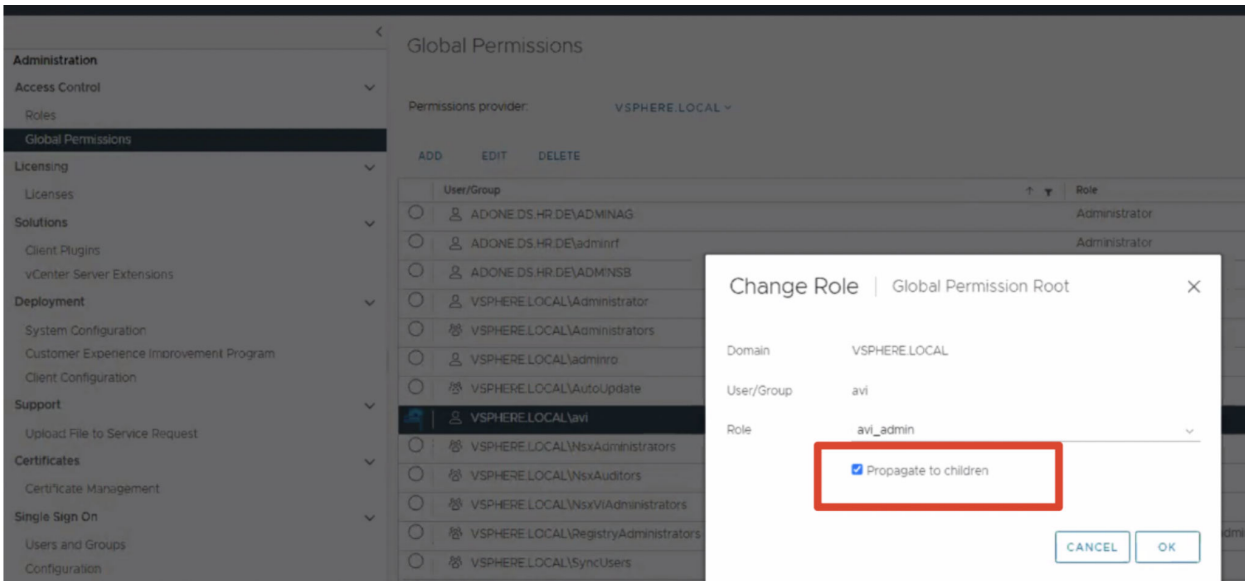


Table 3-11. *Design Decisions for vCenter Server Access Control for NSX Advanced Load Balancer Controller*

Decision ID	Design Description	Design Justification	Design Implication
AVI-VI-VC-009	Create or use a vCenter Server User/ Role with the described privileges. **Note** Do not use the local administrator or root user of vCenter Server for this purpose.	Required for NSX Advanced Load Balancer Controller to perform lifecycle management of the Service Engines. **Note** Update the vCenter User credential on the Controller when password for this user account is rotated.	None

NSX-T Data Center Design of the Advanced Load Balancing for VMware Cloud Foundation

NSX-T Data Center Access Control for NSX Advanced Load Balancer Controller

Use the 'Network Engineer' role and create a Service Account user . This user is used by the Controller to interact with NSX Manager cluster and provide lifecycle management for the Service Engines.

Table 3-12. *Design Decisions for NSX-T Data Center Access Control for NSX Advanced Load Balancer Controller*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-NSX-001	Create or use an NSX-T Manager cluster User/ Role with password with the described privileges. **Note** It is recommended not to use the local 'admin' user of NSX-T Data Center.	Required for the Controller to perform lifecycle management of the Service Engines. **Note** Update the NSX-T User Credential on the Controller when password for this user account is rotated.	None

NSX-T Data Center Distributed Firewall Rule Configuration

This section describes how to configure distributed firewall (DFW) rules on NSX-T Data Center for securing the load-balanced applications configured on the NSX Advanced Load Balancer.

Note The Controller's NSX-T Cloud Connector will create NSX-T Data Center inventory resources (Services and Groups) with the configured 'Object Name Prefix' in the Cloud configuration on the Controller.

During the NSX-T Cloud Connector creation on the Controller the following NSGroup(s)/ NSService(s) are created by the Controller:

Object	Naming Convention	Description
Group	<prefix>-ControllerCluster	Contains all the NSX Advanced Load Balancer Controller Management IPs
Group	<prefix>-ServiceEngineMgmtIPs	Contains all the Service Engine IPs
Group	<prefix>-ServiceEngines	Contains all the Service Engines as VMs
Service	<prefix>-ControllerCluster	Contains protocols/ports for the Controller. Allows TCP ports 22, 8443 and UDP 123

During load-balanced application creation on the Controller, the following NSGroup(s)/ NSService(s) are created by the Controller:

Object	Naming Convention	Description
Group	<prefix>-<VS-Name>	Contains all the data vNIC IPs of all the Service Engines Engines servicing traffic for this load-balanced application (VS)
Group	<prefix>-<VS-Name>VsServiceEngines	Contains all the Service Engine VMs servicing traffic for this load-balanced application (VS)
Service	<prefix>-<VS-Name>	Contains protocols/ports for the load-balanced application (VS)
Service	<prefix>-<Pool-Name>	Contains protocols/ports for the backend servers (Pool)

Table 3-13. *Design Decisions for the NSX-T Data Center Distributed Firewall Rules*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-NSX-002	Create necessary NSX DFW and/ or Gateway Firewall rules for the NSX Advanced Load Balancer control plane as described to ensure connectivity from: ■ Admin to the Controllers ■ The Controllers to the Controllers ■ The Controllers to Service Engines	These firewall rules are needed to allow required communication for the NSX Advanced Load Balancer control plane. **Note** If DFW is enabled and these rules are not configured, this might result in NSX Advanced Load Balancer control plane not functioning as expected.	None
AVI-NSX-003	Create necessary NSX DFW and/ or Gateway Firewall rules for the configured load-balanced applications as described to ensure connectivity from: ■ Client to VIPs ■ Service Enginess to Backend Pool Servers	These firewall rules are needed to allow required communication for the configured load-balanced applications. **Note** If DFW is enabled and these rules are not configured, this might result in the configured load-balanced applications not functioning as expected.	None

Control Plane Distributed Firewall Rule Configuration

When a new NSX-T Cloud Connector is created on NSX Advanced Load Balancer Controller, create these rules if DFW is enabled. These rules need to be created only once per-NSX-T Cloud connecter.

Rule	Source	Destination	Service	Apply to	Action
The Controller UI Access **Note** Required only if the Controller is connected to an NSX network segment.	Any Can be changed to restrict UI/ API/ CLI access	The Controller management IPs and the Cluster IP (if configured) Use the auto created `ControllerCluster` NSGroup	TCP (22, 80, 443)	DFW	Allow
The Controller cluster communication **Note** Required only if the Controller is connected to an NSX-network segment.	The Controller management IPs Use the NSX-T Cloud Connector created `ControllerCluster` specific NSGroup	The Controller Management IPs Use the auto created `ControllerCluster` NSGroup	TCP (22, 8443) Use the auto created `ControllerCluster` Service	DFW	Allow
The Service Engines to the Controller Secure Channel. **Note** The Service Engines initiates TCP connection for the secure channel to the Controllers.	The Service Engine management IPs Use the auto created `ServiceEngineMgmtIPs` NSGroup	The Controller Management IPs Use the auto created `ControllerCluster` NSGroup	TCP (22, 8443) and UDP (123) Use the auto created `ControllerCluster` Service	The Service Engine Virtual Machines Use the auto created `<prefix>-ServiceEngines` NSGroup	Allow

When a new NSX-T Cloud Connector is created on the Controller, create these rules if Gateway Firewall is enabled. These rules need to be created only once per-Cloud.

Rule	Source	Destination	Destination Port	Apply To	Action
The Service Engines to the Controller Secure Channel **Note** The Service Engines initiates TCP connection for the secure channel to the Controllers	The Service Engine management IPs Use the auto created `ServiceEngineMgmtIPs` NSGroup	The Controller management IPs and the Cluster IP (if configured) Use the auto created ControllerCluster NSGroup	TCP (22, 8443) and UDP (123) Use the auto created ControllerCluster Service	Tier-0 connected to the Service Engine Management Tier-1	Allow

Data Plane Distributed Firewall Rule Configuration

When a new load-balanced application is created on the Controller, create these rules if DFW is enabled. These rules need to be created for every new load-balanced application.

Rule	Source	Destination	Service	Apply to	Action
External Client to load-balanced application (VS)	External clients	VIP of the load-balanced application	VS ports Use the auto created `<prefix>-<VS-Name>` Service	Clients and Service Engine VMs servicing the load-balanced application Use the auto created `<prefix>-<VS-Name>VsServiceEngines` NSGroup	Allow
The Service Engines to Backend members (Pool)	The Service Engine Data IPs Use the auto created `<prefix>-<VS-Name>` NSGroup	Backend server IPs Recommended to create a NSGroup for backend servers	Backend pool ports Use the auto created `<prefix>-<Pool-Name>` Service	Backend Servers and Service Engine VMs servicing the load-balanced application Use the auto created `<prefix>-<VS-Name>VsServiceEngines` NSGroup	Allow
Inter Service Engine communication	The Service Engine Data IPs Use the auto created `<prefix>-<VS-Name>`NSGroup	The Service Engine Data IPs Use the auto created `<prefix>-<VS-Name>` NSGroup	Any	The Service Engine VMs servicing the load-balanced application. Use the auto created `<prefix>-<VS-Name>VsServiceEngines` NSGroup	Allow

When a new load-balanced application is created on the Controller, create these rules if Gateway Firewall is enabled. These rules need to be created for every new load--alanced application.

Rule	Source	Destination	Destination Port	Destination Port	Action
External Client to load-balanced application (VS)	External clients	VIP of the load-balanced application	VS ports Use the auto created <prefix>-<VS-Name> Service	Tier-0 connected to the Service Engine data Tier-1	Allow
East/ West traffic across Tier-1 routers	Application clients	VIP of the load-balanced application	VS ports Use the auto created <prefix>-<VS-Name> Service	Tier-1 routers connected to the Service Engine data and Client(s)	Allow
Backend pool member traffic across Tier-1 routers	The Service Engine Data IPs Use the auto created <prefix>-<VS-Name> NSGroup	Backend server IPs Recommended to create a NSGroup for backend servers	Backend pool ports Use the auto created <prefix>-<Pool-Name> Service	Tier-1 routers connected to the Service Engine data and backend server(s)	Allow

Load-Balanced Application Connectivity to External Clients

When using overlay networks with NSX-T, to enable north-south connectivity for load-balanced applications (VS), configure the following on the NSX Manager:

- Tier 1 to advertise static routes to Tier 0.
- Tier 0 to re-distribute Tier 1 advertised static routes to external peer.

This way whenever a new VIP is created on the Controller, it will be automatically advertised to the external peer.

Licensing VMware NSX Advanced Load Balancer for VMware Cloud Foundation

NSX Advanced Load Balancer is available in three editions:

- NSX Advanced Load Balancer Enterprise with Cloud Services edition, which provides all features that VMware NSX Advanced Load Balancer has to offer along with value added SaaS delivered Cloud Services (Available from NSX Advanced Load Balancer v21.1.3 or later).
- NSX Advanced Load Balancer Enterprise edition, which provides full enterprise grade load balancing including multi-cloud integration, active-active high availability, Global Server Load Balancing (GSLB), Web Application Firewall (WAF), and so on.
- NSX Advanced Load Balancer Basic edition, which provides equivalent functionality to the native NSX-T Load Balancer available in NSX-T Data Center

Note VMware recommends the customers who have purchased NSX-T Data Center licenses which have Load Balancing capability to deploy the NSX Advanced Load Balancer in the Basic edition as an alternative to the existing NSX-T Data Center Load Balancer.

Table 3-14. *Design Decisions for Licensing VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-021	Choose the VMware NSX Advanced Load Balancer Enterprise with Cloud Services licensing tier. **Note** 1. New VMware NSX Advanced Load Balancer deployments running v21.1.3 or later will be setup by default in Enterprise with Cloud Services licensing tier. 2. If running v21.1.2 or earlier, choose the VMware NSX Advanced Load Balancer Enterprise licensing tier.	Provides full-featured access to the NSX Advanced Load Balancer platform. **Note** If running v21.1.3 or later, alternative is to either use: i) Enterprise edition licensing tier. This provides a full-featured enterprise feature set but does not give access to Cloud Services and advanced App Security features. ii) Basic edition licensing tier. This provides equivalent functionality of NSX-T Data Center native Load Balancer. If running v21.1.2 or earlier, alternative is to use the Basic edition licensing tier. This provides equivalent functionality of NSX-T Data Center native Load Balancer.	None

Sizing Compute and Storage Resources of Advanced Load Balancing for VMware Cloud Foundation

Sizing Compute and Storage Resources for NSX Advanced Load Balancer Controller(s)

A three-node Controller cluster deployment is a requirement for optimum operation of the NSX Advanced Load Balancer.

NSX Advanced Load Balancer Controller Sizing Guidelines for CPU and Memory

The amount of CPU/memory capacity to allocate to the Controller is calculated based on the following parameters:

- The number of virtual services to support
- The number of Service Engines to support
- Analytics thresholds

For more details on Controller sizing, see Controller Sizing guide.

NSX Advanced Load Balancer Controller Sizing Guidelines for Disk

The amount of disk capacity to allocate to the Controller is calculated based on the following parameters:

- The amount of disk capacity required by analytics components
- The number of virtual services to support

For more details on Controller sizing, see Controller Sizing guide.

Table 3-15. *Design Decisions for sizing the Controllers for the NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-022	Deploy one Controller cluster for each NSX Manager cluster for configuring and managing load balancing services.	Required to form a highly available Controller cluster.	None
AVI-CTLR-023	Deploy each node in the Controller cluster with a minimum of 8 vCPUs, 32 GB memory and 216 GB of disk space.	Support up to 200 virtual services. Support up to 100 NSX Advanced Load Balancer Service Engines. Can scale-up with expansion of the Controller sizes anytime. **Note** Under sizing, the Controllers can lead to unstable control plane functionality.	None

Sizing Compute and Storage Resources for NSX Advanced Load Balancer Service Engine(s)

NSX Advanced Load Balancer publishes minimum and recommended resource requirements for new Service Engines. However, network and application traffic may vary. This section provides guidance on sizing.

The Service Engines can be configured with a minimum of 1 vCPU core and 1 GB RAM up to a maximum of 64 vCPU cores and 256 GB RAM. In write access mode, the Service Engine resources for newly created Service Engines can be configured within the Service Engine Group properties from the Controller.

CPU

CPU scales very linearly as more cores are added. CPU is a primary factor in SSL handshakes (TPS), throughput, compression, and WAF inspection. For NSX-T Clouds, the default is 1 vCPU cores, not reserved. However, vCPU reservation is highly recommended.

Memory

Memory scales near linearly. It is used for concurrent connections and HTTP caching. Doubling the memory will double the ability of the Service Engine to perform these tasks. For NSX-T Clouds, the default is 2 GB memory, reserved within the hypervisor for NSX-T Clouds.

Packets Per Second (PPS)

For throughput-related metrics, the hypervisor is likely going to be the bottleneck and provides limited PPS for a virtual machine such as Service Engine.

HTTP Requests Per Second (RPS)

HTTP RPS is dependent on the CPU or the PPS limits. It indicates the performance of the CPU and the limit of PPS that the Service Engine can push. On vSphere, the Service Engine can provide approximately 40k RPS per core running on Intel v3 servers. Maximum RPS on the Service Engine virtual machine running on ESXi will be approximately 160k.

Disk

The Service Engines may store logs locally before they are sent to the Controllers for indexing. Increasing the disk will increase the log retention on the Service Engine. SSDs are highly recommended, as they can write the log data faster. The recommended minimum size for storage is 10 GB, ((2 * RAM) + 5 GB) or 15 GB, whichever is greater. 15 GB is the default for Service Engines deployed in VMware clouds.

NSX Advanced Load Balancer Service Engine Performance Guidelines

The following table provides guidance to size an NSX Advanced Load Balancer Service Engine virtual machine with regards to performance:

vCenter Cloud	1 Core/ 2 GB RAM	2 Core/ 2 GB RAM	4 Core/ 4 GB RAM	6 Core/ 6 GB
SSL Transactions per sec (ECC)	2900	5800	8700	12000
SSL Transactions per sec (RSA)	950	1800	2600	4000
L7 Requests per sec	58000	80000	150000	185000
L4 Connections per sec (TCP)	42000	54000	100000	132000
L4 Open Connections*	40000	80000	160000	320000
L4 Throughput**	6 Gbps	6 Gbps	9.5 Gbps	13 Gbps
L7 Throughput	5 Gbps	5.6 Gbps	11 Gbps	12 Gbps
L7 SSL Throughput	2.6 Gbps	3.8 Gbps	7.2 Gbps	10 Gbps
SE CPU Cores	1	2	4	6

SE Memory	2 GB	2 GB	4 GB	6 GB
SE Disk	15 GB	20 GB	30 GB	40 GB

Note

1. Tested on Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz, supermicro, 32 CPUs x 2.4 GHz, 256 GB memory with NSX Advanced Load Balancer 20.1.6.
2. The Service Engines were deployed on VMware vCenter, using Avi's VMware Cloud Connector and Write Access automation.
3. Core = Service Engine VM Core (Service Cores)
4. Throughput measurements are virtual service throughput, calculated by aggregating the client-facing traffic only. Total throughput on the Service Engine is approximately double.
5. SSL Tests were performed with:
    a. EC (SECP2 56R1) and RSA (2048 Bits)
    b. Cipher used:
        1. EC — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        2. RSA — TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    c. PFS enabled, TLS version 1.2
6. The above data is per Service Engine VM. Avi's L3-based Active-Active scaling capability allows customers to scale out based on application requirements on-demand.
7. The performed tests are done with CPU limit set to 'unlimited' for Service Engine VM. This is the default setting for bringing up the Service Engine VM.
8. *Open Connections capacity (also known as Concurrent Connections) can be increased by adding more memory to the Service Engine.
9. **L4 Throughput on SEs with 4 core or more tested with 2 dispatcher cores.
10. SE dispatcher/ proxy cores configuration:
    - 1 Core and 2 Core SE — Dedicated dispatcher set to False
    - 4 Core and 6 Core SE — Dedicated dispatcher set to True
    - 4 Core SE — 1 dispatcher core, 3 proxy cores
        - 2 Dispatcher and 2 proxy cores for L4-throughput tests
    - 6 Core SE— 2 Dispatcher cores, 4 proxy cores

Easy Deployment of NSX Advanced Load Balancer Integration with VMware Cloud Foundation

To deploy Advanced Load Balancing for VMware Cloud Foundation, first you need to deploy and configure the Controller cluster based on the Deployment Model for the VMware NSX Advanced Load Balancer for the VMware Cloud Foundation. VMware provides an automated process through the VMware Flings Application Easy Deploy.

Prerequisites

- Administrative Credentials for SDDC Manager.
- Reserve four IPs in the management network to be assigned to the Controllers which will be used for management communication.
- Functioning DNS servers.

Deploying Easy Deploy Appliance

You can deploy the automation appliance virtual machine in the management domain. This appliance will provide a web interface to run the orchestration workflows.

Deployment Process

1 Download the Easy Deploy OVA from flings.vmware.com portal.

2 Upload the **Controller OVA** to the **Content Library**.

   a In a web browser, log in to the management domain vCenter Server by using the vSphere Client (https://vcenter_server_fqdn/ui).

   b Navigate to **Menu > Content Libraries** and click **sfo-m01-avic**.

   c In the **Templates** section, click **ACTIONS** and select **Import Item**.

   d Select the **Source > Source File** from **Local** file and click **UPLOAD FILE**.

   e Select the **Easy Deploy OVA** and click **Open**.

   f Specify the **Destination > Item Name** as **Avi-Easy-Deploy.ova**.

   g Click **IMPORT**.

3 Deploy Easy Deploy virtual machine.

   a In a web browser, log in to the management vCenter Server by using the vSphere Client (https://vcenter_server_fqdn/ui).

   b Navigate to one of the ESXi hosts in the **Management** domain and click **Summary**. Click **Hardware** and record the CPU {base clock speed}, this is used to reserve CPU for the Controller virtual machines.

   c Navigate to **Menu > Content Libraries** and click **sfo-m01-avic**.

   d Navigate to **Templates**.

e Right click on **Avi-Easy-Deploy.ova** and select **New VM from this Template**.

f Give a name **sfo-m01-easydeploy** to the virtual machine and select the datacenter in the **Select a location for the virtual machine** menu and click **NEXT**.

g Choose one of the hosts within the **Management Domain** to host the Controller virtual machine and click **NEXT**.

h Review details and click **NEXT**.

i Specify the following in the **Select Storage** section:

Setting	Value
Virtual Machine Storage Policy	vSAN default storage policy
Select virtual disk format	As defined in the virtual machine storage policy
Datastore	Storage compatible vSAN datastore

j Click **Next**.

k Choose a port group for **Destination Network** in **Network Mapping**. This port group is the management network for the Controller and will be used for all management communication.

l Click **Next**.

m Specify the following in the **Customize template** section:

Setting	Value
Hostname	Hostname of system
IP Address	IP Address of the system (Leave blank, if DHCP)
Network Prefix	CIDR notation (For instance, 24 for 255.255.255.0) - Ignored, if DHCP
Gateway	Gateway of the system (Leave blank, if DHCP)
DNS	DNS Server (Leave blank, if DHCP)
DNS Domain	DNS Domain (Leave blank, if DHCP)
Root Password	Root SSH Password

n Click **Next**.

o Review details and click **FINISH**.

Uploading Image to Easy Deploy Appliance

Upload the Advanced Load Balancer *ova* image to the Easy Deploy Appliance. This image will be used during the automated Controller virtual machine deployments.

Image Upload Process

1 In a web browser, navigate to the **Easy Deploy Menu** (https://easy_deploy_ip/menu)

2 Under **Actions**, click **DOWNLOAD/MANAGE** on the **Image Upload** panel.

3 On the **Image Upload** screen, click **ADD IMAGE**.

4 Specify the following in the **Image Selection** pop-up window.

a Download through **Customer Connect**:

Setting	Value
Want to download image using customer connect?	TRUE
Version	Select image version to download.
Username	Provide your **MyVMware** username.
Password	Provide your **MyVMware** password.

1 Click **NEXT**.

2 Click the **I AGREE TO THIS LICENSE AGREEMENT** checkbox on the **EULA**.

3 Click **SUBMIT**.

b Manually upload the NSX Advanced Load Balancer OVA:

Setting	Value
Want to download image using customer connect?	FALSE
Select File	Click the BROWSE button, in the File Explorer window select a valid ova image file. (For instance, `controller_sha1-22.1.3-9096.ova`)

c Click **Upload**.

Registering VCF Environment

Register the VCF environment with the Easy Deploy Appliance. This process runs a discovery process against the SDDC manager to collect information on the management and VI domains.

Registration Process

1 In a web browser, navigate to the Easy Deploy Menu (https://easy_deploy_ip/menu).

2 Under **Ecosystem**, click **OPEN** on the **VMware Cloud Foundation** panel.

3 On the **VMware Cloud Foundation Integration** screen, click **Register/ Refresh**.

a Specify the following in the **Register VCF Installation** pop-up window:

Setting	Value
Type of Registration	"Register VCF Installation"
SDDC Manager FQDN	Provide your SDDC Manager FQDN of your VCF installation.
Username	Provide your SDDC Manager username information.
Password	Provide your SDDC Manager password information.

4 Click **Register**.

5 Once registration is completed, a **Unlock Passphrase** pop-up window will appear. The passphrase provided can be used to unlock the encrypted data of the VCF registration. This can also be used by other users when accessing the tool through another browser. **Keep in a save location**.

6 Click **Close**.

Deploying Advanced Load Balancing for VMware Cloud Foundation

Run the Easy Deploy orchestration workflow agains the VCF domain to deploy and configure NSX Advanced Load Balancer Controller cluster.

The flow of actions for the automation process are:

1 Create NSX Advanced Load Balancer virtual machine folder.

2 Create deployment VM Tags, used by the Easy Deploy Appliance for registration and association. The tags created are as follows:

   a `AVI_CONTROLLER_WORKLOAD-DOMAIN`

   b `WORKLOAD-DOMAIN_DOMAIN_NAME`

   c `SDDC_MANAGER`

   d `WORKLOAD-DOMAIN-vCenter_Server`

   e `WORKLOAD-DOMAIN_NSXT-Server`

3 Create **Content Library**, if required.

4 Deploy Controller Node(s). Deploy 3 Controller Nodes, if Cluster is defined.

5 Wait for Controller Node(s) to deploy and services to start.

6 Configure initial system settings on **Leader Node**.

7 Configure Controller Cluster.

8 Wait for Controller Cluster configuration to complete.

Deployment Process

The following is the procedure to deploy Advanced Load Balancing for VMware Cloud Foundation:

1 In a web browser, navigate to the **Easy Deploy Menu** (https://easy_deploy_ip/menu)

2 Under **Ecosystem**, click **OPEN** on the VMware Cloud Foundation panel.

3 If the **VMware Cloud Foundation Integration** screen is empty, click **Register/ Refresh**.

4 Specify the following in the **Register VCF Installation** pop-up window:

a If you have an **Unlock Passphrase**:

Setting	Value
Type of Registration	"Unlock VCF Installation"
Unlock Passphrase	Provide your unlock passphrase.

1 Click **UNLOCK**.

b If you do not have an **Unlock Passphrase**:

Setting	Value
Type of Registration	Register VCF Installation
SDDC Manager FQDN	Provide your SDDC Manager FQDN of your VCF installation.
Username	Provide your SDDC Manager username information.
Password	Provide your SDDC Manager password information.

1 Click **Register**.

5 For the **WLD** that you would like to deploy Advanced Load Balancing on, click the associated **Actions** button.

6 Click **INITIALIZE**.

7 In the **Deployment** pop-up window, specify the following in the **Deployment Details** section:

Setting	Value
Available Images	Select a NSX Advanced Load Balancer deployment image version.
Deployment Size	Select the NSX Advanced Load Balancer controller deployment size. See Sizing Guidelines.

8 Click **NEXT**.

9 Specify the following in the **vSphere Details** section:

Setting	Value
Datacenter	Select a datacenter for deployment.
Cluster	Select a cluster for deployment.
Datastore	Select a datastore for deployment.
Do you want to create a new content library?	If you want to use an **EXISTING** Content Library then select a Content Library for deployment. If you want to use a **NEW** Content Library then provide a name for the new Content Library.

10 Click **NEXT**.

11 Specify the following in the **Controller Setup** section:

Setting	Value
Controller Credentials	You have the option to configure a password for the NSX Advanced Load Balancer Controller. If **Password** and **Confirm Password** is left blank, a strong password will be generated.
Cluster	Enable to create 3-Node Cluster.
Cluster IP	Enable to configure Cluster IP.
DNS Server	At least one DNS entry is required. By default, a DNS server is pulled from the vCenter configuration.
DHCP	Enable to utilize DHCP for Controller Management Network.
Network Port group	Select a port group for Management Network.
Network/CIDR	Provide a network subnet for management. (Hidden, if DHCP)
Gateway	Provide gateway address for management. (Hidden, if DHCP)

12 Click **NEXT**.

13 Specify the following in the **Controller IP Configuration** section:

Setting	Value
Controller IP 1	Provide IP address for Controller 1
Controller IP 2	Provide IP address for Controller 2
Controller IP 3	Provide IP address for Controller 3
Cluster IP	Provide IP address for Controller Cluster. (Hidden if Cluster IP not selected)

14 Click **NEXT**.

15 Review details and click **DEPLOY**.

16 On the **VMware Cloud Foundation Integration** screen, the **WLD** configured and any **WLD** that shares the underlying NSX-T Manager Status will change from **NOT INITIALIZED** to **DEPLOYING %**.

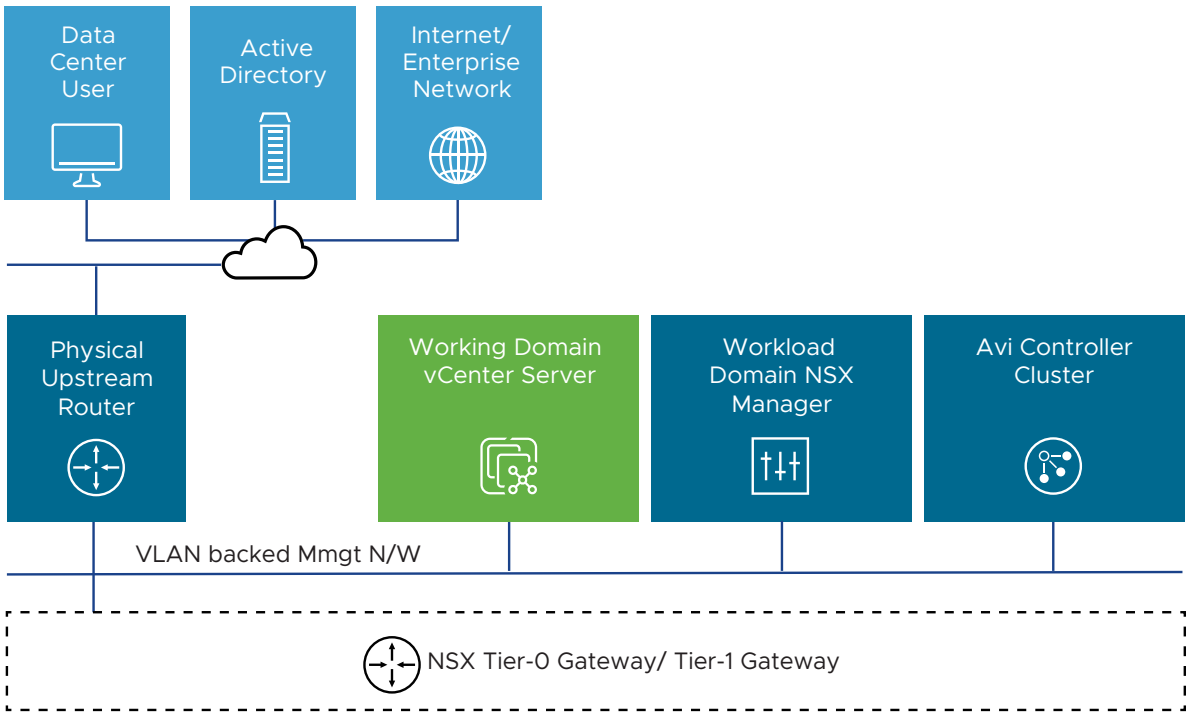
17 Click the **Expand** button beside the configured **WLD** to view the **Deployment Status**. This process can take up to one hour to complete. If the deployment fails, you will be presented with the error output and the option to roll back and destroy the deployed elements.

Network Design for Advanced Load Balancing for VMware Cloud Foundation

Network Segment

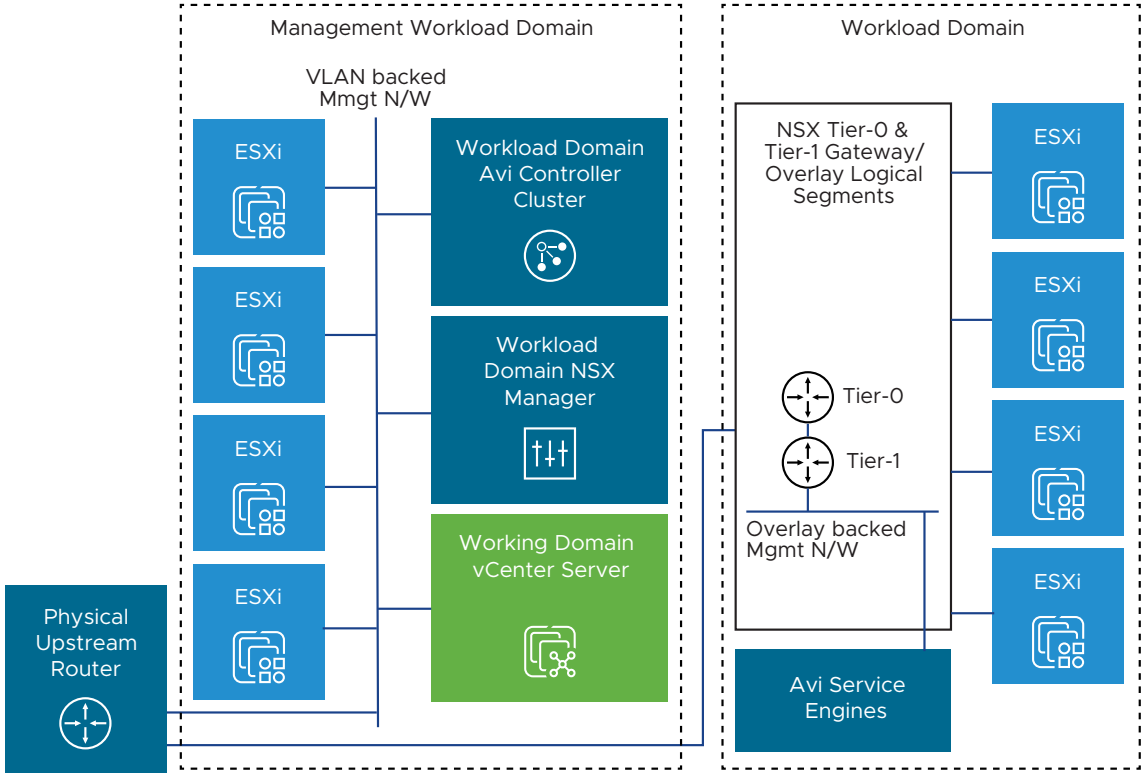
In the network design for the NSX Advanced Load Balancer users are required to provide three types of connectivity:

1 Management connectivity for the Controllers.

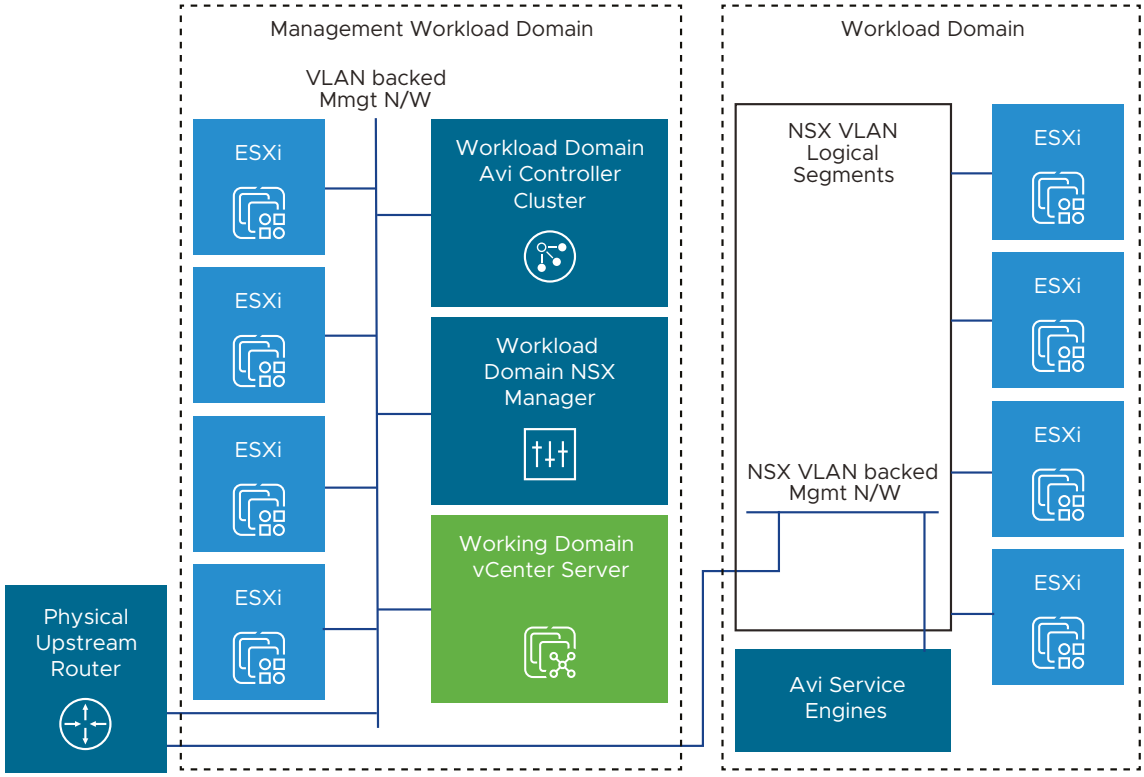


2 Management connectivity between the Controllers and the Service Engines and:

a NSX Advanced Load Balancer Service Engines connected to an NSX-T Managed Overlay network.



b NSX Advanced Load Balancer Service Engines connected to an VLAN-backed NSX segments.



3 Data connectivity to service load-balanced application traffic for the Service Engines.

Table 3-16. *Design Decisions for the Networking Design for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-VC-010	Deploy the Controller cluster nodes on the VMware Cloud Foundation management network.	Allows for ease of management for the Controllers. Allows for configuring a floating cluster VIP; a single IP address that will be assigned to the cluster leader. Administrative tasks, connectivity to the Service Engines and connectivity to network services will all use this network.	None
AVI-NSX-004	Configure a management network to deploy the Service Engines. Management network needs to be NSX segment and could be either of: 1 VLAN-backed NSX segment 2 Overlay-backed NSX segment connected to a Tier-1 router **Note** This network should have connectivity to the IP addresses of each of the Controllers.	This is required to configure the Controller NSX-T Cloud Connector.	None
AVI-NSX-005	Configure one or more data network(s) for the Service Engines to service load-balanced applications. Data networks need to be NSX-T managed and could be either of: 1 VLAN-backed NSX segment, or, 2 Overlay-backed NSX segment connected to a Tier-1 router **Note** For overlay-backed NSX segments, one logical segment is required per Tier-1 router.	The Service Engines require data networks to provide access for load-balanced applications.	None

Table 3-16. *Design Decisions for the Networking Design for VMware NSX Advanced Load Balancer* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-024	Latency between the Controllers must be <10ms.	The Controller quorum is latency sensitive. **Note** The Control plane might go down if latency is high.	None
AVI-CTLR-025	Latency between the Controllers and the Service Engines should be <75ms.	Required for correct operation of the Service Engines. **Note** May lead to issues with heartbeats and data synchronization between the Controller and the Service Engines.	None

IP Addressing Scheme

You can assign an IP address to Avi using static or dynamic allocation based on the network configuration of your environment. It is recommended to reserve an IP address from the selected local network segment and statically assign it to the corresponding Controller instance.

Table 3-17. *Design Decisions for the IP Addressing Scheme for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-026	Use static IPs or DHCP with reservation ensuring a permananet lease for the Controllers.	The Controller cluster uses management IPs to form and maintain quorum for the control plane. **Note** The Controller control plane might go down if the management IPs of the Controller change.	None
AVI-VI-001	Reserve an IP in the management subnet to be used as the cluster IP for the Controller cluster.	A floating IP that will always be accessible regardless of a specific individual Avi cluster node.	None
AVI-NSX-006	Configure DHCP on the networks/ logical segments used for data traffic.	Having DHCP enabled for data networks makes the Service Engine configuration simple. **Note** Alternatively, operators could use static IPs, but can have to program IP pools for the data networks to be used by the Service Engines and also add a static route for the data network's gateway on the Controller .	None

Name Resolution

Name resolution provides the translation between an IP address and a fully qualified domain name (FQDN), this makes it easier to remember and connect to components across the SDDC. Each IP address assigned to the Controller instance must have valid DNS forward (A) and reverse (PTR) records.

Table 3-18. *Design Decisions for the Name Resolution for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-002	Configure DNS A records for the three Controllers and cluster VIP.	The Controllers are accessible by an easy to remember FQDN as well as directly by IP address.	Assumes DNS infrastructure is available .

Time Synchronization

Time synchronization provided by the Network Time Protocol (NTP) is important to ensure that all components within the Software-Defined Data Center are synchronized to the same time source.

Table 3-19. *Design Decisions for the Time Synchronization for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-003	Configure time synchronization by using an NTP time for the Controller. **Note** Recommendation is to use the same source as SDDC Manager, vCenter Server and NSX Manager cluster.	Prevents from time synchronization issues. Not required to provide connectivity to an external NTP server.	An operational NTP service must be available in the environment. Ensure that NTP traffic between the Controllers, the Service Engines and the NTP servers is allowed on the required network ports and not firewalled.

Ports Requirements for the VMware NSX Advanced Load Balancer

Port	Protocol	Source	Destination	Description
The Controller to the Controller Access				
22	TCP	The Controller cluster Nodes	The Controller cluster Nodes	Secure channel over SSH
443	TCP	The Controller cluster Nodes	The Controller cluster Nodes	Access to portal over HTTPS (UI)
8443	TCP	The Controller cluster Nodes	The Controller cluster Nodes	Secure key exchange portal over HTTPS
The Service Engine to the Controller cluster Node Access				
22	TCP	The Service Engine management IPs	The Controller cluster Nodes	Secure channel over SSH
8443	TCP	The Service Engine management IPs	The Controller cluster Nodes	Secure key exchange over HTTPS
123	UDP	The Service Engine management IPs	The Controller cluster Nodes	NTP time synchronization
Administration Access				
22	TCP	Admin User IPs	The Controller cluster Nodes	SSH access to the Controller cluster shell/ CLI

Port	Protocol	Source	Destination	Description
443	TCP	Admin User IPs	The Controller cluster Nodes	HTTPS access to the Controller cluster system portal (UI/ SDK)
161	UDP	Admin User IPs	The Controller cluster Nodes	SNMP Poll
5054	TCP	Admin User IPs	The Controller cluster Nodes	(Optional) The Controller CLI through remote shell
The Controller cluster Nodes to External Services				
25	TCP	The Controller cluster Nodes	SMTP Servers	SMTP Notifications
49	TCP	The Controller cluster Nodes	TACACS Servers	TACACS+
53	UDP	The Controller cluster Nodes	DNS Servers	DNS
123	UDP	The Controller cluster Nodes	NTP Servers	NTP
389	TCP/UDP	The Controller cluster Nodes	LDAP Servers	LDAP
636	TCP/UDP	The Controller cluster Nodes	LDAP Servers	LDAPs
162	UDP	The Controller cluster Nodes	SNMP Trap Collectors	SNMP Traps
514	UDP	The Controller cluster Nodes	Syslog Servers	Syslog Notifications
Application Connectivity				
*	*	Application Clients	The Service Engines	Open up the required TCP/UDP ports for the clients to communicate with the application.
*	*	The Service Engines	Application Servers	Open up the required TCP/UDP ports for the Service Engines to communicate with the backend application servers.

Lifecycle Management for Advanced Load Balancing for VMware Cloud Foundation

Lifecycle management design details the design decisions covering the lifecycle management of the Advanced Load Balancing for VMware Cloud Foundation validated solution.

When performing lifecycle management of the NSX Advanced Load Balancer you should consider the amount of time and effort taken to perform a patch, update, or upgrade operation, and the impact these operations may have on the configured load-balanced applications.

You perform lifecycle management of the NSX Advanced Load Balancer using the Controller upgrade workflow. The Controllers will upgrade all the NSX Advanced Load Balancer components including the Controllers and the associated Service Engines.

NSX Advanced Load Balancer supports two methods of updating the system:

1 Upgrade: Used for regular upgrades

2 Patch: Used for hot fixes

Customers can choose to apply the following methodology while updating the NSX Advanced Load Balancer:

1 Full System Update: The Controllers and all the associated Service Engines are updated together in a single maintenance window.

   a Allowed in both basic and enterprise license tiers.

   b All associated Service Engines are updated along with the Controllers.

2 Separate Control and Data Plane Update: The Controllers and all the associated Service Engines can be updated separately in multiple maintenance windows.

   a Only allowed in the Enterprise License Tier.

   b The Controllers (Control Plane Only) must be updated first.

   c All associated Service Engines need to be updated to complete the upgrade sequence.

   d The Service Engine updated can be done on a per Service Engine Group basis.

Rollbacks with NSX Advanced Load Balancer

- Rollback is automatically triggered if there is a failure during the control plane upgrade.
- Customers can choose to rollback the system at will if desired for reasons that are outside the scope of this guidance.
- Before executing a rollback, you need to delete all the Service Engine Groups that were created after upgrade (in the current release).
- Only a single step rollback is possible, current release to previous release.

Table 3-20. *Design Decisions for Lifecycle Management of the VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-027	Use the Controller to performance lifecycle management of the NSX Advanced Load Balancer.	■ Lifecycle of NSX Advanced Load Balancer is not managed by SDDC Manager. ■ The Controller manages lifecycle for all NSX Advanced Load Balancer components including the Controllers and all the associated Service Engines.	Deployment, patching, updates, and upgrades of NSX Advanced Load Balancer are performed without native SDDC automation.
AVI-CTLR-028	When a VI workload domain is upgraded, upgrade NSX Advanced Load Balancer before upgrading NSX-T Data Center based on the compatibility matrix with vCenter Server and NSX-T Data Center. **Note** Check the version compatibility matrix in the Advanced Load Balancing for VMware Cloud Foundation validated solution document before upgrading.	Ensures NSX Advanced Load Balancer cloud integration with NSX-T Data Center and vCenter Server continues to function as expected. **Note** Upgrading vCenter Server and/ or NSX-T Data Center before NSX Advanced Load Balancer might lead to issues with the NSX-T Cloud Connector integration on the Controller due to version incompatibility.	None
AVI-CTLR-029	If the Controller is providing services to multiple VI workload domains, choose to upgrade the Controller and only the Service Engine Groups that are associated with the VI workload domain that is being upgraded. **Note** This is optional. Alternatively, choose to upgrade the entire Controller cluster, which will upgrade the Controllers and all the Service Engines.	■ Allows isolated upgrade for the VI workload domain ■ Upgrade only the Service Engines that reside on the VI workload domain that is being upgraded ■ VI workload domain that is currently not being upgraded, but shares the same Controller is left untouched.	None

Information Security and Access of Advanced Load Balancing for VMware Cloud Foundation

Information security and access design details the design decisions covering authentication and access controls for the NSX Advanced Load Balancer.

Table 3-21. *Design Decisions for Information Security and Access of the VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-030	Create a strong password for the local admin account on NSX Advanced Load Balancer: ■ Minimum 8 char long ■ Contains at least one char in each of 3/4 of the following categories: ■ Uppercase letters ■ Lowercase letters ■ Digits ■ Special characters	This reduces the risk of the account being compromised. This is a requirement to setup user accounts, including the admin account.	None.
AVI-CTLR-031	Rotate passwords at least every 3 months.	Ensures security of the user accounts.	None
AVI-CTLR-032	Limit the use of the local accounts for both interactive or API access and solution integration.	Local accounts are not specific to user identity and do not offer complete auditing from an endpoint back to the user identity.	You must define and manage service accounts, security groups, group membership, and security controls in Active Directory.
AVI-CTLR-033	Create user accounts with desired Roles on the Controller to limit the scope and privileges for accounts used for both interactive or API access and solution integrations. **Note** A custom 'Role' might be created if a user account needs to have specific permissions that are not available out of the box on the Controllers.	The principle of least privilege is a critical aspect of access management and should be part of a comprehensive defense-in-depth security strategy.	You may need to define and manage custom roles and security controls to limit the scope and privileges used for interactive access or solution integration.

Planning and Preparation of Advanced Load Balancing for VMware Cloud Foundation

4

Before you start implementing the components of the Advanced Load Balancing for VMware Cloud Foundation validated solution, you must set up an environment that has a specific compute, storage, and network configuration, and that provides external services to the components of the solution.

You need to review the Planning and Preparation of Advanced Load Balancing for VMware Cloud Foundation documentation ahead of deployment of NSX Advanced Load Balancer to avoid costly rework and delays.

Hardware Requirements

To implement the NSX Advanced Load Balancer from this design, your hardware must meet certain requirements.

Component	Requirement per Region
Servers	BIOS Configuration ■ Advanced Encryption Standard-New Instructions (AES-NI) Enabled
Network Interfaces	Minimum of 10GB

Software Requirements

To implement the VMware NSX Advanced Load Balancer from this design, your software must have the requirements specified in the Solution Interoperability of Advanced Load Balancing for VMware Cloud Foundation section.

SCP Backup Target

You can choose to setup a Secure Copy Protocol (SCP) service for remote backups of NSX Advanced Load Balancer before you deploy the components of this design.

Dedicate space on a remote server to save data backups for NSX Advanced Load Balancer over SCP.

Requirement	Description
Backup Target	A backup target for the Controller VMs in the SDDC. The server must support SCP connections.

VLANs and IP Subnets

This validated solution requires that you allocate certain VLAN IDs and IP subnets for the traffic types in the SDDC.

For the Controllers, it is recommended to share the port-group used for core VMware Cloud Foundation management services. This means that Controller VMs should use the same port-group as used by vCenter Server(s) and NSX Manager(s).

For the Service Engines, an VLAN-backed NSX segment(s) can be used for:

- The management network for the Service Engines for both types of NSX-T Cloud Connector integrations i.e. overlay-backed and VLAN-backed on the NSX Advanced Load Balancer.
- The data network(s) for the Service Engines for NSX-T Cloud Connector integration of type VLAN on the NSX Advanced Load Balancer.

Overlay-backed NSX Segments and IP Subnets

If an overlay-backed NSX segment is being used in the VI workload domains, this design requires that you allocate certain overlay-backed NSX segments connected to a Tier-1 logical router and IP subnets for the Service Engine(s) to service traffic.

Cluster	Overlay-backed NSX Segment Function	Logical Segment Name	Subnet
VI workload domain	Management network for the Service Engines.	sfo-w01-cl01-vds01-pg-avimgmt	
VI workload domain	Data Network for the Service Engines. **Note** More can be added as required.	sfo-w01-cl01-vds01-pg-avidata01	

Note Alternatively, a NSX VLAN segment could be used as the management network for the Service Engines.

Host Names and IP Addresses

Before you deploy the NSX Advanced Load Balancer by following this design, you must define the host names and IP addresses for the Controller VMs and configure them in DNS with fully qualified domain names (FQDN) that map the host names to their IP addresses.

Table 4-1. Example

Component	Host Name	DNS Zone	IP Address	Description
The Controller cluster VIP			10.10.10.100	The Controller cluster VIP Interface
The Controller instances			10.10.10.101	The Controller instances for the management cluster
			10.10.10.102	
			10.10.10.103	

Workload Footprint

Before you deploy the NSX Advanced Load Balancer, you must provide sufficient compute and storage resources to meet the footprint requirements of the Controller cluster and the Service Engines.

Note It is required that the Controller VMs are created in the management workload domain of the VMware Cloud Foundation.

Workload Footprint for Management Domain

Workload	vCPUs	vRAM (GB)	Storage (GB)
NSX Advanced Load Balancer Controller cluster			
Total			
Total with 30% free storage capacity			

Workload Footprint for VI Workload Domain

Workload	vCPUs	vRAM (GB)	Storage (GB)
Service Engines			
Total			
Total with 30% free storage capacity			

Implementation of Advanced Load Balancing for VMware Cloud Foundation

5

Implementing the Advanced Load Balancing for VMware Cloud Foundation validated solution includes enabling NSX Advanced Load Balancer in your SDDC by deploying the Controller cluster with three nodes and configuring a NSX-T Cloud Connector to provide automated load balancing.

For information on the Advanced Load Balancing design, refer to Chapter 3 Detailed Design of Advanced Load Balancing for VMware Cloud Foundation section.

Note NSX Advanced Load Balancer version 20.1.6 will be used as a place holder release. Any NSX Advanced Load Balancer release beginning v20.1.6 is qualified to be used with this validated solution.

VMware provides automation for various workflows described in this solution. Automation is provided using vRealize Orchestrator workflows and Ansible playbooks. Clone the GitHub repository for this solution. See https://github.com/vmware-samples/validated-solutions-for-cloud-foundation.

For instance, if you are using Git on Windows, run the following commands:

```
mkdir vvs
cd vvs
git clone https://github.com/vmware-samples/validated-solution-for-cloud-foundation.git
cd validated-solutions-for-cloud-foundation/alb
dir
```

The repository layout consists of two parts for easy navigation:

1 Folder for each automation tool - Pick the tool of choice for automation.

2 Folder for each automated workflow - Contains detailed information on how to execute the workflow.

Prerequisites

Verify that your environment is configured according to Before You Apply This Guidance and the Chapter 4 Planning and Preparation of Advanced Load Balancing for VMware Cloud Foundation section.

Procedure

Day 0 Workflows – One-time workflows to setup the NSX Advanced Load Balancer

1 Deploy Advanced Load Balancing for VMware Cloud Foundation

2 Automate Application Orchestration for Advanced Load Balancing for VMware Cloud Foundation

Read the following topics next:

- Deploy Advanced Load Balancing for VMware Cloud Foundation
- Automate Application Orchestration for Advanced Load Balancing for VMware Cloud Foundation

Deploy Advanced Load Balancing for VMware Cloud Foundation

To deploy Advanced Load Balancing for VMware Cloud Foundation, first you need to deploy and configure the Controller cluster based on the Deployment Model for Advanced Load Balancing for VMware Cloud Foundation.

Prerequisites

1 Create a Content Library on the management domain vCenter Server to host NSX Advanced Load Balancer images.

   a Create a dedicated Content Library for hosting the Controller Images. Content Library name used in this documentation is ‘avicsfo-m01-’.

   b Create a dedicated Content Library for hosting the Service Engine images.

2 For Stretched Cluster deployments,

   a Create a VM Group for NSX Advanced Load Balancer Controller VMs.

   b Create Host Groups for ESXi hosts in each AZ.

   c Create a ‘should’ anti-affinity rule between the Controller VM Group and ESXi Host Group.

Procedure

- Deploy NSX Advanced Load Balancer Controller VMs in the Management Domain
- Create an NSX Advanced Load Balancer Controller Cluster
- Setup Licensing for the VMware NSX Advanced Load Balancer
- Setup Alerting for the VMware NSX Advanced Load Balancer
- Create Tenants on the NSX Advanced Load Balancer Controller Cluster

Deploy NSX Advanced Load Balancer Controller VMs in the Management Domain

Deploy three Controller VMs in the management domain. These will form a highly available control plane for the NSX Advanced Load Balancer.

Note

- Deploy all the Controller VMs in the first availability zone if using a Stretched cluster.
- Refer to Sizing Compute and Storage Resources for NSX Advanced Load Balancer Controller(s) section to size the Controller cluster appropriately. A 'small' sized Controller cluster deployment is demonstrated here.

Prerequisites

- Reserve four IPs in the management network to be assigned to the Controllers which will be used for management communication.
- Create a Content Library to host the Controller OVAs on the management domain vCenter Server.

Procedure

- Download the Controller OVA from my.vmware.com portal. Follow this KB article to download the Controller OVA image.
- Upload the Controller OVA to the Content Library.
  a In a web browser, log in to the management domain vCenter Server by using the vSphere Client (https://vcenter_server_fqdn/ui).
  b Navigate to **Menu > Content Libraries** and click on **sfo-m01-avic**.
  c In the **Templates** section, click on **ACTIONS** and select **Import Item**.
  d Select the **Source > Source File** from **Local file** and click on **UPLOAD FILE**.
  e Select the **Avi Controller OVA** and click on **Open**.
  f Specify the **Destination > Item Name** as **Avi-Controller-v20.1.6.ova**.
  g Click on **IMPORT**.

Deploy NSX Advanced Load Balancer Controller VM.

- In a web browser, log in to the management vCenter Server by using the vSphere Client (https://vcenter_server_fqdn/ui).
- Navigate to one of the ESXi hosts in the Management domain and click on **Summary**, click on **Hardware**, and record the CPU {base clock speed}, this is used to reserve CPU for the Controller VMs.
- Navigate to **Menu > Content Libraries** and click on **sfo-m01-avic**.
- Navigate to **Templates**.

- Right click on **Avi-Controller-v20.1.6.ova** and select **New VM from this Template**.
- Give a name **sfo-m01-avic01a** to the Controller VM and select the datacenter in the **Select a location for the virtual machine** menu and click on **NEXT**.
- Choose one of the hosts within the Management Domain to host the Controller VM and click on **NEXT**.
- Review details and click on **NEXT**.
- Specify the following in the **Select Storage** section:

Setting	Value
VM Storage Policy	vSAN Default Storage Policy
Select virtual disk format	As defined in the VM storage policy
Datastore	Storage compatible vSAN datastore

- Click on **NEXT**.
- Choose a port group for Destination Network in **Network Mapping**. This port group is the management network for the Controller and will be used for all management communication.
- Click on **NEXT**.
  - Specify the following properties and click on **NEXT**.

    Note The '`sysadmin login authentication`' key is used to specify an SSH public key and is NOT required.

Setting	Value
Management Interface IP Address	IP address for the management interface. Leave blank if using DHCP. For instance, 192.168.10.4
Management Interface Subnet Mask	Subnet mask for the management interface. Leave blank if using DHCP. For instance, 24 or 255.255.255.0
Default Gateway	Optional default gateway for the management network. Leave blank if using DHCP.
Management Interface IPv6 Address	IP address for the management interface. Leave blank if using DHCP.
Management Interface Subnet Mask	IPv6 Subnet mask for the management interface. Leave blank if using DHCP.
Default v6 Gateway	Optional default gateway for the management network. Leave blank if using DHCP.
Sysadmin login authentication key	Sysadmin login authentication key

- Validate and click on **NEXT**.

Navigate to the **Avi Controller VM**, click on **Actions > Edit Settings**, and adjust the following Controller VM settings, click on *OK*.

Note Select the size of the Controller VMs depending on the requirement.

Setting	Value
CPU	8 vCPU; set reservation to 8*{base clock speed} for the host from earlier
Memory	24 GB; set reservation to 24 GB
Hard disk 1	208 GB

Note This documentation assumes that the VMware NSX Advanced Load Balancer belongs to the **sfo.rainpole.io** domain.

Having FQDNs registered for NSX Advanced Load Balancer Controller with DNS is not a requirement.

For ease of use, FQDNs for NSX Advanced Load Balancer Controller can be configured locally on the workstation from which NSX Advanced Load Balancer Controller UI is launched, for instance, in /etc/hosts file if using MacOS.

Having a FQDN entry for the NSX Advanced Load Balancer Controller is a requirement when registering with Cloud Services.

Sample Naming Convention for the NSX Advanced Load Balancer Controllers:

- `sfo-m01-avic01a`
- `sfo-m01-avic01b`
- `sfo-m01-avic01c`

- Repeat 'Deploy the Controller VM' steps to create two additional Controllers to be used to form a three-node Controller cluster which will form the control plane for the NSX Advanced Load Balancer.
- Create an anti-affinity 'VM/Host' rule to make sure Controller VMs are placed on separate hosts.
  a Navigate to the vSphere cluster where the Controller VMs are deployed and click on **Configure**.
  b Create an anti-affinity 'VM/Host Rules' rule by clicking on **Add**.
  c Create the rule by filling in the following details and click on **OK**.

Setting	Value
Name	avi-ctrl-anti-affinity-rule
Enable rule	Check box
Add VMs	Add the three Controller VMs

- Power on Controller VMs.
  a Navigate to each of the three Controller VMs and power them on.

Create an NSX Advanced Load Balancer Controller Cluster

Configure NSX Advanced Load Balancer Controller cluster to provide a highly available control plane for the NSX Advanced Load Balancer.

Prerequisites

1 Deploy three Controller VMs in the management domain.

2 Reserve one IP in the management network to be assigned as the Controller cluster VIP which will be used as a single end point to manage NSX Advanced Load Balancer.

3 To guarantee priority recovery of the Controller VMs, configure VM Override rules with the following properties:
  a Set VM Restart Policy to ‘Medium’.
  b Set Host Isolation Response to ‘Disable’.

Procedure

1 Initialize the first NSX Advanced Load Balancer Controller VM
  a In a web browser, log in to the first Controller by using https://sfo-m01-avic01a.sfo.rainpole.io/.

  Note While the system is booting up, a blank web page or a 503-status code may appear. Wait for about 5 to 10 minutes and then follow the instructions below for the setup wizard.

  b Once the NSX Advanced Load Balancer welcome screen appears, create an 'admin' account by specifying the following information and click on **Create Account**:

Setting	Value
username	admin
Password	<COMPLEX_PASSWORD>
Confirm Password	<COMPLEX_PASSWORD>
Email Address	Specify the administrator email address

  c Specify the DNS and NTP information and click on **Next**.

d Setup SMTP source as 'Local Host' with From Address as **admin@avicontroller.net** and click on**Next**.

e Under **Tenant Settings** select **Share IP route doman across tenets**.

f Under **Service Engines are managed within the** select **Provider**.

g Under **Tenet Access to Service Engine** select **Read Access**.

h Click **Save.**

The UI will log into the NSX Advanced Load Balancer Controller dashboard.

2 Configure an NSX Advanced Load Balancer Controller cluster.

a Navigate to **Administration > Controller** and select Edit.

b Specify the 'Name' of the cluster as **sfo-m01-avic**.

c Specify the 'Controller Cluster IP' that had been reserved.

d Add the following details for each of the three NSX Advanced Load Balancer Controller nodes.

Setting	Value
IP	<CONTROLLER_IP_ADDRESS>
Name	sfo-m01-avic01a (sfo-m01-avic01b and sfo-m01-avic01c)
Password	Leave blank
Public IP	Leave blank

e Click on **Save**. It will take a few minutes for the services to restart and the Controller cluster to be up.

1 In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

2 Navigate to **Administration > Controller** and ensure all the Controllers show ‘State’ as ‘Active’ which represents a healthy Controller cluster.

3 Setup the Controller cluster Portal Certificate. By default, the Controller cluster Portal will be setup with a self-signed certificate. It is recommended to setup a trusted CA signed certificate for the Controller cluster Portal.

Note Steps to sign a CSR by a Trusted CA are not covered in this document.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Templates > Security > SSL/TLS Certificates** and click on **CREATE** and select on **Controller Certificate**.

c Select Type as 'CSR' and specify the following information:

Setting	Value
Name	sfo-m01-avic01-portal-certificate
Common Name	sfo-m01-avic01.sfo.rainpole.io

d Click on **SAVE** to generate a **Certificate Signing Request**.

e Click on **Edit** (pencil icon) on the **sfo-m01-avic01-portal-certificate** and copy the CSR.

f Take the copied CSR and get it signed from a trusted CA. This will generate a signed Certificate. Copy the signed Certificate to be used for the Controller cluster portal.

g Click on **Paste text** and paste the copied signed certificate.

h Click on **SAVE**.

i Navigate to **Administration > Settings > Access Settings** and edit **System Access Settings**.

j Remove the pre-existing **SSL/TLS Certificate** entries (these are the self-signed Controller cluster portal certificates) and select the **sfo-m01-avic01-portal-certificate** certificate from the drop-down.

k Click on **SAVE**.

l Refresh the browser to re-negotiate TLS with the Controller cluster portal. The signed Certificate should be presented by the Controller cluster portal.

4 Setup the Controller Cluster Secure Channel Certificate. By default, the Controller cluster will be setup with a self-signed certificate to be used for communication between the Controllers and the Service Engines. It is recommended to setup a trusted CA signed certificate for the Controller cluster Secure Channel.

Note Steps to sign a CSR by a Trusted CA are not covered in this document.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Templates > Security > SSL/TLS Certificates** and click on **CREATE** and select **Controller Certificate**.

c Select Type as 'CSR' and specify the following information:

Setting	Value
Name	sfo-m01-avic01-secure-channel-certificate
Common Name	sfo-m01-avic01.sfo.rainpole.io

d Click **SAVE** to generate a **Certificate Signing Request**.

e Click on **Edit** (pencil icon) on the **sfo-m01-avic01-secure-channel-certificate** and copy the CSR.

f Take the copied CSR and get it signed from a trusted CA. This will generate a signed Certificate. Copy the complete signed Certificate bundle to be used for the Controller cluster portal.

g Click on **Paste text** and paste the copied complete signed Certificate bundle.

h Click on **SAVE**

i Navigate to **Administration > Settings > Access Settings** and edit **System Access Settings**.

j Remove the pre-existing **Secure Channel SSL/TLS Certificate** entry (this is the self-signed Controller cluster secure channel certificates) and select the **sfo-m01-avic01-secure-channel-certificate** Certificate from the drop-down.

k Click on **SAVE**.

5 All Service Engines that will be created will use this certificate to authenticate the Controller cluster.

Setup Licensing for the VMware NSX Advanced Load Balancer

Configure NSX Advanced Load Balancer in the desired licensing tier and import required licenses.

By default,

1 NSX Advanced Load Balancer deploymets running v21.1.3 or later will be setup in the Enterprise with Cloud Services licensing tier. This is the recommended licensing tier which allows customers access to complete feature set along with Cloud Services. Customers can optionally choose to setup NSX Advanced Load Balancer in the Enterprise or Basic licensing tier.

2 NSX Advanced Load Balancer deploymets running v21.1.2 or earlier will be setup in the Enterprise licensing tier. Customers can optionally choose to setup NSX Advanced Load Balancer in the Basic licensing tier.

Prerequisites

- Verify that the Controller cluster is deployed and operational, refer to Create an NSX Advanced Load Balancer Controller Cluster section.
- If you are using Enterprise with Cloud Services tier, verify that you have obtained a valid NSX Advanced Load Balancer with Cloud Services Subscription. Verify the following prerequisites are met before registering your Controller with Cloud Services.
- If you are using Enterprise or Basic licensing tier, verify that you have obtained a valid license key.

Procedure

Follow this guide to register your Controller cluster with Cloud Services and use it in the Enterprise with Cloud Services licensing tier.

Note Enterprise with Cloud Services is available with NSX Advanced Load Balancer v21.1.3 or later.

- (Optional) Switch the licensing tier on the Controller cluster.
  a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.
  b Navigate to **Administration > Settings > Licensing** and click the gear icon beside **Licensing** and select the licensing tier required.
  c Click on **SAVE**.

  Note This step is optional and should only be performed if required.

  Basic license tier provides NSX-T Data Center Load Balancing equivalent feature set only.

  Customers can follow the same workflow and setup the Controller cluster back in the Enterprise with Cloud Services or Enterprise license tier.

- If the Controller cluster is running either in Enterprise or Basic licensing tiers, apply licenses on the Controller cluster by following these steps:
  a Copy NSX Advanced Load Balancer license keys from customerconnect.vmware.com portal.
    1 If you are using Basic licensing tier, existing NSX-T Data Center licenses can be used.
  b In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.
  c Navigate to **Administration > Settings > Licensing** and click on **KeyApply**.

Setting	Value
License Key	Paste the copied license keys

  d Click **Apply Key**.
  e Multiple license keys can be imported on the Controller cluster.

Setup Alerting for the VMware NSX Advanced Load Balancer

Setup alert destinations for the NSX Advanced Load Balancer Alerts. A combination of Syslog, Email, SNMP and Control Script can be chosen to notify an alert.

Prerequisites

- Verify that the Controller cluster is deployed and operational, refer to Create an NSX Advanced Load Balancer Controller Cluster section.
- Verify that vRealize Log Insight is deployed and operational if you plan to enable syslog notifications.

Note

- You can choose to apply one or many mechanisms for notifications.
- Control Scripts are not allowed if the Controller cluster is setup in the basic license tier. For Control Scripts, the Controller cluster must be setup in the enterprise license tier.
- You can create custom 'Alert Config' based on custom thresholds and KPIs on the Controller cluster. These KPIs can be based on numerous Infrastructure and Application parameters that the Controller cluster gathers.

Procedure

1 Create a Syslog notification object.

Note You can configure vRealize Log Insight as a syslog endpoint and can use the content pack for NSX Advanced Load Balancer which is available here.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Operations > Notifications > Syslog**, and click on **Create**.

c Specify **avisyslog** as the Name for the syslog notification config.

d Click on **Add Syslog Server**.

e Specify syslog server details.

Setting	Value
Syslog server	IP of the syslog server
Port	Default port used is 514. User can override this setting

f Repeat to add more syslog servers if required.

g Click on **Save**.

2 Create an Email notification object.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Operations > Notifications > Email**, and click on **Create**.

c Specify **aviemail** as the Name for the email notification config.

d Fill out the destination emails in the following fields:

Setting	Value
To Address	Email of the primary recipient
CC Address	Comma separated email addresses of secondary recipients

e Click on **Save**

3 Create a SNMP notification object.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Operations > Notifications > SNMP Trap** , and click on **Create**.

c Specify **avisnmp** as the Name for the **snmp notification config**.

d Specify SNMP server details.

Setting	Value
Trap Server IP Address	IP of the SNMP trap receiver
SNMP Version	SNMP_VER2
SNMP Community	Trap server community string

e Click on **Add SNMP Server** to add more SNMP servers.

f Click on **Save**

4 Create a Control Script object.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Templates > Scripts > ControlScripts** , and click on **Create**.

c Specify any desired name for the ControlScript.

d Type the script in the **Enter your ControlScript Here** box.

e Click on **Save**.

5 Attach the Syslog, Email and/or SNMP notification objects to Alerts.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Operations > Alerts > Alert Actions**.

c Edit the **System-Alert-Level-High** action.

d (Optional) From the **Syslog** drop-down, choose **avisyslog** which was created previously.

e (Optional) From the **Email** drop-down, choose **aviemail** which was created previously.

f (Optional) From the **SNMP Trap** drop-down, choose **avisnmp** which was created previously.

g (Optional) From the **ControlScript** drop-down, choose the desired ControlScript.

h Click on **Save**.

6 Repeat for **System-Alert-Level-Medium** and **System-Alert-Level-Low**.

Create Tenants on the NSX Advanced Load Balancer Controller Cluster

A tenant can be configured to isolate load-balanced application configurations on the NSX Advanced Load Balancer. This is an optional configuration which should be chosen depending on the business requirements.

Please refer to the Isolation Model for Load-Balanced Applications before deciding.

Note

- The NSX Advanced Load Balancer will have the 'admin'/ provider tenant configured by default.
- This workflow is optional and is intended to be used only if implementing tenancy on the NSX Advanced Load Balancer.

Prerequisites

Verify that the Controller cluster is deployed and operational, refer to Create an NSX Advanced Load Balancer Controller Cluster section.

Procedure

1 (Option 1) Create a Tenant with 'config isolation only'.

a In a Linux shell, SSH to the Controller cluster VIP by using admin@sfo-m01-avic01.sfo.rainpole.io.

b Specify the NSX Advanced Load Balancer CLI by executing '`shell -user admin -password <ENTER_PASSWORD>`'.

c Create a Tenant by executing the following CLI commands:

```
configure tenant <TENANT_NAME>
config_settings
se_in_provider_context
tenant_access_to_provider_se
no tenant_vrf
save
save
```

2 (Option 2) Create a Tenant with 'config + data isolation'.

a In a Linux shell, SSH to the Controller cluster VIP by using `admin@sfo-m01-avic01.sfo.rainpole.io`

b Specify the NSX Advanced Load Balancer CLI by executing '`shell -user admin -password <ENTER_PASSWORD>`'

c Create a Tenant by executing the following CLI commands:

```
configure tenant <TENANT_NAME>
config_settings

no se_in_provider_context
no tenant_access_to_provider_se

no tenant_vrf
save

save
```

Automate Application Orchestration for Advanced Load Balancing for VMware Cloud Foundation

After you deploy Advanced Load Balancing for VMware Cloud Foundation, you need to setup the necessary Cloud Connector configuration on the Controller based on Cloud Connector Integration in the Advanced Load Balancing for VMware Cloud Foundation. This provides automated orchestration for load-balanced applications.

Note Every Controller cluster can be configured with one or more Cloud Connectors depending on the requirements.

Prerequisites

- Verify that the Controller cluster is deployed and operational, refer to Create an NSX Advanced Load Balancer Controller Cluster section.
- Verify that a VI workload domain is deployed and operational in VMware Cloud Foundation.
- Verify a content library has been created within the VI workload domain vCenter Server to store the Service Engine OVAs.

Procedure

- Create Credential Objects on VMware NSX Advanced Load Balancer
- Create Cloud Connector for Automated Orchestration of Applications on VMware NSX Advanced Load Balancer
- Create Service Engine Groups for Data Plane Isolation of Applications on VMware NSX Advanced Load Balancer
- Create a Sample Load-Balanced Application on VMware NSX Advanced Load Balancer

Create Credential Objects on VMware NSX Advanced Load Balancer

You can create credential objects on the NSX Advanced Load Balancer to interact with NSX-T Data Center and vCenter Server.

For access control refer to the following design sections:

- NSX-T Data Center Access Control for NSX Advanced Load Balancer Controller
- vCenter Server Design of the Advanced Load Balancing for VMware Cloud Foundation

Prerequisites

- Verify that the NSX Advanced Load Balancer Controller cluster has network connectivity to the VI workload domain vCenter Server and and NSX Manager cluster.
- Verify that the vCenter Server service account has created and assigned appropriate access.
- Verify that the NSX Manager cluster service account has been created and assigned appropriate access.

Procedure

1 Create vCenter Server User Credential object on the Controller cluster.

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Administration > User Credentials**.

   c Click on **Create**.

   d Specify the following information to create a vCenter Server user credential object:

Setting	Value
Name	vCenter-<ID> Recommendation: Use VI workload domain name as the <ID>
Credential Type	vCenter
User	<username>
Password	<password>

   e Click on **Save**

   f Repeat for each vCenter Server that will be serviced by this Controller cluster.

2 Create NSX Manager User Credential object on the Controller cluster.

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Administration > User Credentials**.

   c Click on **Create**.

d Specify the following information to create a NSX-T Data Center user credential object:

Setting	Value
Name	vCenter-<ID> Recommendation: Use VI workload domain name as the <ID> Use the VI workload domain name if NSX-T Data Center manages VI workload domains
Credential Type	NSX-T
User	<username>
Password	<password>

e Click on **Save**.

Create Cloud Connector for Automated Orchestration of Applications on VMware NSX Advanced Load Balancer

Create NSX-T Cloud Connector object on the NSX Advanced Load Balancer Controller cluster. Choose the Cloud Connector model based on the Models for configuring an NSX-T Cloud Connector on the Advanced Load Balancing for VMware Cloud Foundation section.

Prerequisites

- Create User Credential objects for NSX-T Data Center and vCenter Server on the Controller cluster.
- Create a content library for hosting the Service Engine images on each of the vCenter Server(s) that are managed by NSX-T Data Center.
- If using overlay-backed NSX segments for load balancing, create a Tier-1 router and dedicated a Tier-1 connected Logical Segment for the Service Engine data networks (vNICS).
- If using an overlay-backed NSX segments for Service Engine management, create at least one overlay-backed NSX segments connected to a Tier-1 router (Applicable to NSX-T Cloud Connector of type overlay).
- If using a VLAN network for the Service Engine management, create at least one VLAN-backed NSX segments (Applicable to NSX-T Cloud Connector of type overlay and/or VLAN).
- If using VLAN networks for load balancing, create at least one VLAN-backed NSX segments for the Service Engine data networks (vNICS).

Procedure

1 Create a new NSX-T Cloud Connector on the Controller cluster.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Infrastructure > Clouds**.

c Click on **CREATE** and select **NSX-T Cloud**.

d To configure the Cloud, specify the following general settings:

Setting	Value
Name	NSX-T-<ID> Recommendation: Use VI workload domain name as the <ID>. Use the VI workload domain name if NSX-T Data Center manages VI workload domains.
DHCP	Select (If using DHCP for the Service Engine data networks).
Object Name Prefix	<prefix> This prefix will be used for all objects created by this NSX-T Cloud Connector. Recommendation: Use an easy identifier like 'avise-<ID>', where <ID> is the same ID used for the cloud name.

2 Attach the Cloud Connector to an NSX Manager cluster.

a Click **CHANGE CREDENTIALS** under NSX-T credentials and specify the following information:

Setting	Value
NSX-T Manager Address	FQDN of the NSX Manager cluster that is managing this VI workload domain.
NSX-T Manager Credentials	NSX-T-<ID> Name of the NSX-T Data Center user credential object that was configured on the Controller cluster.

b Click on **CONNECT**.

3 Configure the management network for the Service Engines.

a Under the **Management Network** section, select a **Transport Zone**.

b If a VLAN Transport Zone is selected, select a **VLAN Segment**.

c If an overlay Transport Zone is selected, select a **Tier1 Logical Router** and then an **Overlay Segment**.

4 Configure the data network(s) for the Service Engines.

a Under the **Data Networks** section, select a **Transport Zone**.

b If a VLAN Transport Zone is selected, select a **VLAN Segment**.

c If an overlay Transport Zone is selected, select a **Tier1 Logical Router** and then an **Overlay Segment**.

d Repeat to add multiple data networks as required.

Note 1. All data networks should belong to the same Transport Zone. Therefore all data networks are either VLAN-backed NSX segments or Tier-1 router attached overlay-backed NSX segments.

2. Only one overlay-backed NSX segment can be added per Tier-1 router.

3. Each Tier-1 router requiring load balancing services will be added as a new data network in the Cloud Connector configuration.

5 Configure the vCenter Server(s).

a Click on **ADD** to add a new vCenter Server and specify the following information:

Setting	Value
Name	<name> Recommendation: Use VI workload domain name as an easy identifier
Credentials	
vCenter Address	Specify The vCenter Server FQDN/IP
vCenter Credentials	vCenter-<ID> Name of the vCenter Server user credential object that was configured on the Controller cluster.

b Click on **CONNECT**.

c From the **Content Library** drop-down, select the content library configured to host the Service Engine images.

d Click on **DONE**.

e Repeat to add multiple vCenter Server(s) as required.

f Click on **SAVE**.

Create Service Engine Groups for Data Plane Isolation of Applications on VMware NSX Advanced Load Balancer

Choose to isolate load-balanced applications based on the Service Engine Group Configuration in the NSX Advanced Load Balancer section.

Prerequisites

Create required NSX-T Cloud Connector objects on the Controller cluster.

Procedure

1 Create a new Service Engine Group on the Controller cluster.

a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

b Navigate to **Infrastructure > Cloud ResourcesService Engine Group**.

c Select the configured **NSX-T-<ID>** cloud from the **Select Cloud** drop-down.

d Click on **CREATE**.

2 Configure basic settings for the Service Engine Group.

a Specify the following to configure the **Basic Settings** of the Service Engine Group:

Setting	Value
Name	<name> Recommendation: Consider the use-case and location while naming
High Availability Mode	HA Mode Recommendation: Use Active/ Active HA Mode
VS Placement across the Service Enginess	Distributed

b Real Time Metrics table:

Setting	Value
Maximum Number of Service Engines	Adjust according to scale requirements
Memory per Service Engine	Adjust according to scale requirements
vCPU per Service Engine	Adjust according to scale requirements
Disk per Service Engine	3x the Memory per the Service Engine (minimum 15GB)
Memory Reserve	Select
CPU Reserve	Select
Real Time Metrics	Checked and set time to 0 minimum

c Configure the appropriate **Service Engine Capacity and Limit Settings** based on 'Sizing Compute and Storage Resources for NSX Advanced Load Balancer Service Engine(s)'.

3 Configure advanced settings for the SE Group.

a Click on **Advanced** and specify the following information:

Setting	Value
SE Name Prefix	<prefix> Recommendation: string that will help identify VMs as the Service Engines. Additionally, use a prefix that helps identify the workloads that these Service Engines will be servicing, if applicable.
Buffer SEs	Change as required Minimum: 1, Maximum: 128

Setting	Value
Scale Per Virtual Service (Minimum)	Change as required Minimum: 1, Maximum: 128
Scale Per Virtual Service (Maximum)	Change as required Minimum: 1, Maximum: 128
Dedicated Dispatcher CPU	Select if configured vCPU per Service Engine >= 4

4 Configure scoping for the Service Engines for the Service Engine Group.

a Click on **+ Add vCenter** to scope the Service Engine Group to a vCenter Server.

b Select the**vCenter** from the drop-down. All vCenter Server(s) configured in the Cloud Connector should be listed. This is a good way to isolate the Service Engines between VI workload domains.

c Configure the **Placement Scope** settings.

Setting	Value
Service Engine Folder	vCenter VM Folder Recommendation: Select a vCenter folder to place all the Service Engines created by this SE Group.
Host Scope Service Engine within	Optional setting to include/ exclude ESXi Hosts on which Service Engines will be spawned.
Data Store Scope for Service Engine Virtual Machine	Select Shared → Include the shared storage configured for the VI workload domain.

d Click on **Save**.

Create a Sample Load-Balanced Application on VMware NSX Advanced Load Balancer

This section will showcase how to create a load-balanced web application. This section should be used as a template.

The following are the resources created on the Controller cluster:

1 Pool

2 Virtual Service

Note This reference application will be configured on an NSX-T Cloud Connector using overlay-backed NSX segment as the Service Engine data networks.

Prerequisites

- NSX-T Cloud Connector for VI workload domain has been setup.
- The Service Engine Group to host the application and Service Engines has been setup.

- DHCP on NSX-T Data Center as been enabled for the Service Engine data networks (Recommended, not a requirement).
- Create workload VMs in vCenter Server that are run a web server.
- Configure a NSGroup in NSX Manager cluster for these web server VMs (Recommended, not a requirement).

Procedure

1 Create a Pool object on the Controller cluster.

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Applications > Pools** and click on **CREATE POOL**.

   c Select the appropriate NSX-T Cloud Connector from **Select Cloud** and click on **Next**.

   d Specify the **Name** for the Pool, for instance, Sample-WebPool.

   e Select the **Tier1 Logical Router** from the drop-down.

   f Click on **Add Active Monitor** and select **System-HTTP** Health Monitor from the **Select a Health Monitor** drop-down.

   g Select **Enable real time metrics**.

   Note **Enable real time metrics** is not available in basic license tier.

   h Click on **Next** to add backend (upstream) servers.

   i Option 1: Specify the range or list of IP Addresses of the web servers and click on **Add Server**.

   j Option 2: Click on **Security Groups** and from the **NSX Security Groups** drop-down, select the configured NSGroup in NSX Manager cluster for the web server VMs.

   k Click on **Next**.

   l Set **Connection Ramp** to 0.

   m Click on **Next**.

   n Click on **Save**.

2 Create a VirtualService object on the Controller cluster.

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Applications > Virtual Services** and click on **CREATE VIRTRUAL SERVICE** and select **Advanced Setup**.

   c Select the appropriate NSX-T Cloud Connector from **Select Cloud** and click on **Next**.

   d Specify the **Name** for the Virtual Service, for instance, Sample-WebVS.

e Specify the VIP IP in the **FQDN or IPv4 Address** box.

f Select the **Tier1 Logical Router** from the drop-down.

Note This should match what was selected for the 'Sample-WebPool'.

g Specify the following in the **Services** section (Click on **Add Port** to add the 2nd service):

Setting	Value
Service 1 (HTTP)	Port: 80 SSL: Unselected HTTP2: Unselected
Service 2 (HTTPs)	Port: 443 SSL: Selected HTTP2: Unselected

h Select **System-Secure-HTTP** from the **Application Profile** drop-down.

i Select the created **Sample-WebPool** from the **Pool** drop-down.

j Select **System-Default-Cert** and**System-Default-Cert-EC** to the **SSL Certificate**.

k Click on **Next**.

l Click on **Next**.

m Select **Real time metrics** and set it to **0**.

n Select **Log all headers**.

o Set **Non-significant log duration** to **0**.

Note 'real time metrics', 'log all headers' and, 'non-significant logs' are not available in Basic License Tier.

p Click on **Next**.

q Select a **SE Group** from the drop-down.

r Click on **Save**.

Operational Guidance of Advanced Load Balancing for VMware Cloud Foundation

6

After you complete the implementation of the Advanced Load Balancing for VMware Cloud Foundation validated solution, you perform common operations on the environment, such as examining the operational state of the components added to the environment during the implementation and updating the certificates and account passwords for these components.

For operational guidance on the components that are deployed automatically in Advanced Load Balancing for VMware Cloud Foundation or complement the basic Advanced Load Balancing for VMware Cloud Foundation configuration, refer to VMware Cloud Foundation Operations and Administration Guide in the VMware Cloud Foundation documentation.

- Example Personas in Advanced Load Balancing for VMware Cloud Foundation
- Operational Verification of Advanced Load Balancing for VMware Cloud Foundation
- Operational Verification of the NSX-T Cloud Connector
- Certificate Management for Advanced Load Balancing for VMware Cloud Foundation
- Password Management for Advanced Load Balancing for VMware Cloud Foundation

Read the following topics next:

- Example Personas in Advanced Load Balancing for VMware Cloud Foundation
- Operational Verification of Advanced Load Balancing for VMware Cloud Foundation
- Operational Verification of the NSX-T Cloud Connector
- Certificate Management for Advanced Load Balancing for VMware Cloud Foundation
- Password Management for Advanced Load Balancing for VMware Cloud Foundation
- Rotate Passwords for Advanced Load Balancing for VMware Cloud Foundation
- Rotate Service Account Passwords for Advanced Load Balancing for VMware Cloud Foundation

Example Personas in Advanced Load Balancing for VMware Cloud Foundation

Personas are a method to design for an ideal target and help you define a baseline for identity and access management. Personas allow you to use a common language and make when defining access based on specific responsibilities and organizational structures.

Personas describe ideal or conceptual targets, but these personas are typically aligned with real people and their job responsibilities. Each organization defines the roles and responsibilities for a persona. The following is an example of baseline personas defined by Advanced Load Balancing for VMware Cloud Foundation validated solution and their equivalent access. This can be used as the basis for building your own delegation of roles.

Example Persona	Component Role or Group
Application Admin	Application Administrator
Application Operator	Operator, Viewer
Security Admin	Security Engineer
WAF Admin	Security Engineer
Tenant Admin	Enterprise Administrator
System Admin	Enterprise Administrator

Operational Verification of Advanced Load Balancing for VMware Cloud Foundation

After you add a NSX Advanced Load Balancer in your VMware Cloud Foundation environment using the implementation of the Advanced Load Balancing for VMware Cloud Foundation validated solution, verify that the newly implemented components are operational and functioning within expected parameters.

Operational Verification of NSX Advanced Load Balancer Controller

Validate the operational state of the Controller cluster by performing the operational verification steps on the Controller cluster VIP.

Procedure

1 In a web browser, log in as ‘admin’ to the Controller cluster VIP by using the user interface (https://<avi_controller_cluster_vip_fqdn>/).

2 Navigate to **Administration > Controller > Nodes** in the user interface.

3 Verify all nodes report **Active**.

Operational Verification of the NSX-T Cloud Connector

Validate the operational state of the NSX-T Cloud Connector created on the Controller cluster by performing the operational verification steps on the Controller cluster VIP.

Procedure

1 In a web browser, log in as 'admin' to the Controller cluster VIP by using the user interface (https://<avi_controller_cluster_vip_fqdn>/).

2 Navigate to **Infrastructure > Clouds** in the user interface.

3 Verify NSX-T Cloud **Status** reports **Green**.

Certificate Management for Advanced Load Balancing for VMware Cloud Foundation

After the implementation of the Advanced Load Balancing for VMware Cloud Foundation validated solution, consider replacing the portal certificate of the NSX Advanced Load Balancer i.e., the Controller portal certificate. It is recommended to rotate the Controller cluster Portal Certificate and the Controller cluster Secure Channel Certificate every 90 days at a minimum.

Note

- Steps to sign a CSR by a Trusted CA are not covered in this document.
- It is required to upload the complete certificate bundle after the CSR is signed by the trusted CA.
- Certificate rotatation on NSX or vCenter does not impact NSX Advanced Load Balancer.

Prerequisites

Deploy the NSX Advanced Load Balancer on the Advanced Load Balancing for VMware Cloud Foundation.

The security of the environment depends on the validity and trust of the management components certificates. As a best practice, you replace certificates in the following cases:

1 Before certificates expire

2 When a certificate is compromised

3 When the attributes related to a certificate change, for instance, the host name or the organization name

The certificate replacement for the NSX Advanced Load Balancer consists of the following phases:

1 Generate a Certificate Signing Request (CSR) for the NSX Advanced Load Balancer portal certificate from the Controller.

2 Provide the generated CSR to the CA and request to sign the CSR.

3 Update the CSR on the Controller with the signed certificate.

4 Update the system configuration on the Controller with the updated certificate.

Procedure

1 Rotate the Controller cluster portal certificate

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Templates > Security > SSL/TLS Certificates** and click on the Pencil Icon to edit the '`sfo-m01-avic01-portal-certificate`' Controller Certificate object.

   c Select **Copy to clipboard** in the **Certificate Signing Request** that was previously generated.

   d Take the copied CSR and get it signed from a trusted CA. This will generate a new signed certificate bundle.

   e Navigate to **Templates > Security > SSL/TLS Certificates** and click the Pencil icon to edit the `sfo-m01-avic01-portal-certificate` Controller certificate object.

   f Click on `Paste text` and paste the newly generated signed certificate bundle.

   g Click on **SAVE.**

   h Refresh the browser to re-negotiate TLS with the Controller cluster portal. The new signed Certificate should be presented by the Controller cluster portal.

2 Rotate the Controller cluster secure Cchannel certificate

   a **Note** It is required to upload the complete certificate bundle on the Controller for the secure channel certificate.

   b In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   c Navigate to **Templates > Security > SSL/TLS Certificates** and click the Pencil icon to edit the `sfo-m01-avic01-secure-channel-certificate` Controller certificate object.

   d Select **Copy to clipboard** in the **Certificate Signing Request** that was previously generated.

   e Take the copied CSR and get it signed from a trusted CA. This will generate a new signed Certificate bundle.

   f Navigate to **Templates > Security > SSL/TLS Certificates** and click the Pencil icon to edit the '`sfo-m01-avic01-secure-channel-certificate`' Controller certificate object.

   g Click on **Paste text** and paste the newly generated signed certificate bundle.

   h Click on **SAVE**.

Password Management for Advanced Load Balancing for VMware Cloud Foundation

Manage the account passwords of NSX Advanced Load Balancer in your VMware Cloud Foundation environment according to the design objectives and design guidance for Advanced Load Balancing for VMware Cloud Foundation validated solution.

After NSX Advanced Load Balancer is deployed on the Advanced Load Balancing for VMware Cloud Foundation, it is recommended to rotate the password every 90 days at a minimum for the local admin user account configured on the Controller cluster.

Prerequisites

Deploy the NSX Advanced Load Balancer on the Advanced Load Balancing for VMware Cloud Foundation.

Procedure

1 Rotate the local admin user password for the Controller cluster.

2 In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

3 Login as the local admin user.

4 Click on the **Avi Logo** on the top right corner of the browser and click on **My Account**.

5 Specify the following information to rotate the local admin user password click on **Save**.

Setting	Value
Old Password	Enter the password that was used for login
New Password	Enter a new complex password
Confirm New Password	Re-enter the new complex password

Rotate Passwords for Advanced Load Balancing for VMware Cloud Foundation

After NSX Advanced Load Balancer is deployed on the Advanced Load Balancing for VMware Cloud Foundation. It is recommended to rotate the password every 90 days at a minimum for the local admin user account configured on the Controller cluster.

Prerequisites

Deploy the NSX Advanced Load Balancer on the Advanced Load Balancing for VMware Cloud Foundation.

Procedure

1 Rotate the local admin user password for the Controller cluster.

2 In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

3 Login as the local admin user.

4 Click on the **Avi Logo** on the top right corner of the browser and click on **My Account**.

5 Specify the following information to rotate the local admin user password click on **Save**.

Setting	Value
Old Password	Enter the password that was used for login
New Password	Enter a new complex password
Confirm New Password	Re-enter the new complex password

Rotate Service Account Passwords for Advanced Load Balancing for VMware Cloud Foundation

It is recommended to rotate the NSX and vCenter Service Account passwords used every 90 days at a minimum. Admins must update the respective user credential object on the Controller when these Service Account passwords are rotated.

Prerequisites

User credential objects should be created on the Controller (Refer to Create Credential Objects on VMware NSX Advanced Load Balancer section).

Procedure

1 Rotate the vCenter service account password used for the Controller cluster.

2 In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

3 Login as the local admin user.

4 Navigate to **Administration > User Credentials**, select the vCenter user credential and click on **Edit**.

5 Update the **Password** and click on **Save**.

6 Rotate the NSX-T Manager service aAccount password used for Create Tenants on the NSX Advanced Load Balancer Controller Cluster Controler cluster.

7 In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/. Login as the local admin user.

8 Navigate to **Administration > User Credentials**, select the NSX-T User Credential and click on **Edit**.

9 Update the **Password** and click on **Save**.

Solution Interoperability of Advanced Load Balancing for VMware Cloud Foundation

7

Integrate the Advanced Load Balancing for VMware Cloud Foundation validated solution with components added to your VMware Cloud Foundation environment by other validated solutions for operations management and business continuity. You can use such validated solutions for monitoring and alerting, logging, backup and restore, disaster recovery, and life cycle management with certain considerations.

Performing the deployments and configurations that are part of validated solutions for operations management and business continuity, are out of scope of the Advanced Load Balancing for VMware Cloud Foundation validated solution. However, the solution provides either design or implementation guidance to enable the integration with such solutions.

- Monitoring and Alerting of Advanced Load Balancing for VMware Cloud Foundation
- Logging of Advanced Load Balancing for VMware Cloud Foundation
- Data Protection of Advanced Load Balancing for VMware Cloud Foundation
- Disaster Recovery of Advanced Load Balancing for VMware Cloud Foundation
- Life Cycle Management of Advanced Load Balancing for VMware Cloud Foundation

Read the following topics next:

- Monitoring and Alerting of Advanced Load Balancing for VMware Cloud Foundation
- Logging of Advanced Load Balancing for VMware Cloud Foundation
- Data Protection of Advanced Load Balancing for VMware Cloud Foundation
- Disaster Recovery of Advanced Load Balancing for VMware Cloud Foundation
- Life Cycle Management of Advanced Load Balancing for VMware Cloud Foundation

Monitoring and Alerting of Advanced Load Balancing for VMware Cloud Foundation

After you implement the Advanced Load Balancing for VMware Cloud Foundation validated solution, by using VMware or third-party components, monitor the parameters of the components that are newly added to or re-configured in your VMware Cloud Foundation environment.

For validated monitoring solutions, refer to VMware Cloud Foundation Validated Solutions main page.

NSX Advanced Load Balancer can send system and user defined alerts via one or more of the following mechanisms:

- Syslog
- Email
- SNMP
- Control script

Table 7-1. *Design Decisions for Monitoring and Alerting for Advanced Load Balancing for VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-035	Choose one or more types of notification of choice for monitoring/ alerting. It is recommended to enable alerts on the following pre-defined `System` alerts: ■ System-VS-Alert ■ System-SSL-Alert ■ System-SE-Alert ■ System-Controller-Alert ■ System-CC-Alert	Ensure good health through proactive alerting of the NSX Advanced Load Balancer cluster.	None

Logging of Advanced Load Balancing for VMware Cloud Foundation

After you implement the Advanced Load Balancing for VMware Cloud Foundation validated solution, by using VMware or third-party components, collect log data in a central place from the components that are newly added to or re-configured in your VMware Cloud Foundation environment.

For validated logging solutions, refer to VMware Cloud Foundation Validated Solutions main page.

If your environment is running vRealize Log Insight, you can connect vRealize Log Insight to the NSX Advanced Load Balancer over syslog as documented in the Syslog notification section. Content pack for NSX Advanced Load Balancer is available here.

Data Protection of Advanced Load Balancing for VMware Cloud Foundation

After you implement the Advanced Load Balancing for VMware Cloud Foundationvalidated solution, backing up the newly added components ensures that you can keep your environment operational if a data loss or failure occurs.

Note Only the Controller cluster configuration is required to be backed up.

For validated data protection solutions, refer to VMware Cloud Foundation Validated Solutions main page.

Prerequisites

- Verify that you implemented a backup solution to take configuration backups for the Controllers to a target in a separate fault domain.
- Verify that the backup target has sufficient disk space to store the backups.
- Deploy the NSX Advanced Load Balancer on the Advanced Load Balancer for VMware Cloud Foundation.
- Setup a remote backup server with SCP enabled for transport.
- The Controller cluster will utilize SCP protocol to transfer backups.
- Create a directory on the remote backup server to host backups.

Note

- Remote backup of the NSX Advanced Load Balancer is currently supported over the SCP protocol.
- Only the Controller configuration needs to be backed up.
- VM based backups for the NSX Advanced Load Balancer solution are not required.

You implement backups to prepare for:

- A critical failure of the Controllers
- An upgrade of the NSX Advanced Load Balancer solution
- A certificate update of the Controller clusters portal

You take the following backup types:

- Scheduled backups, which ensure that at any given point in time, you can restore from a recent backup.
- Manual backups before a system update, which ensure that if the operation is unsuccessful, you can restore to a point in time immediately before the operation.
- Manual backups after a recovery of a failed part of the system.

To back up NSX Advanced Load Balancer, you create configuration backups of the Controller by using your backup solution which supports SCP based transfers.

- Log in to the Controller and setup the SCP-compatible backup solution endpoint.
- On the Controller create a backup schedule take periodic backups daily.

Procedure

1 Setup remote backup user credentials on the Controller cluster.

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Administration > User Credentials** and click on **CREATE**.

   c Specify the following information to create a SSH user and click on **GENERATE & SAVE**.

Setting	Value
Name	SSH Username (Set this up on the Backup Server as well)
Credential Type	SSH
Authentication	SSH Key
Keys	Generate SSH Key Value Pair

2 Setup the remote backup server to use the created backup user credentials.

   a Run `curl -ks https://sfo-m01-avic01.sfo.rainpole.io/api/linux_host_install?username=<SSH USERNAME> | sudo bash` on the Backup server.

      1 A Linux user will be created if it does not exist on the Backup server.

3 Configure backups schedule on the Controller cluster.

4 In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

5 Navigate to **Administration > System > Configuration Backup** and click on the pencil icon.

6 Specify the following information and click on **Save**.

Setting	Value
Enable Configuration Backup	selected
Frequency	1
Frequency Unit	Day(s)
Backup Passphrase	<COMPLEX_PASSWORD>
Remote Server	selected
Server Address	Remote backup server FQDN or IP address
Directory	Directory on remote backup server to store backup
User Credentials	Previously created user credentials

Table 7-2. *Design Decisions for Data Protection of Advanced Load Balancing for VMware Cloud Foundation*

Design ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-036	Create a backup schedule to take periodic backups at least every 24 hours.	Backed up configuration will aid in rebuilding and recovering the NSX Advanced Load Balancerconfiguration from catastrophic failires.	Backup server should support SCP as the transport protocol.

Disaster Recovery of Advanced Load Balancing for VMware Cloud Foundation

After you implement the Advanced Load Balancing for VMware Cloud Foundation validated solution, by using VMware or third-party components, enable planned migration and disaster recover for the newly added components in your VMware Cloud Foundation environment.

For validated site protection and recovery solutions, refer to VMware Cloud Foundation Validated Solutions main page.

When failure of a host or availability zone occurs, recovery for the Controller VMs will be enabled by vSphere HA. The Service Engine recovery will be automatically handled by the Controllers.

When a data-center wider disaster event occurs, recovery could be enabled by restoring the latest backed up NSX Advanced Load Balancer configuration to a Controller cluster that is setup in the backup data center. The Service Engine recovery will be automatically handled once the Controllers are functional.

Load-balanced applications that span across VMware Cloud Foundations are recommended to use Global Server Load Balancing (GSLB) for disaster recovery. NSX Advanced Load Balancer will be configured in each VMware Cloud Foundation and can participate in the GSLB federation. For more details, refere to the VMware NSX Advanced Load Balancer GSLB product documentation.

Life Cycle Management of Advanced Load Balancing for VMware Cloud Foundation

After you implement the Advanced Load Balancing for VMware Cloud Foundation validated solution, by using VMware or third-party components, enable upgrade and patching of the components that have been added to your VMware Cloud Foundation environment.

For information on the impact of performing life cycle management of the products in this validated solution on VMware Cloud Foundation and other validated solutions that might be deployed in your environment, refer to Performing Life Cycle Management Across Validated Solutions.

Upgrade Advanced Load Balancing for VMware Cloud Foundation

All upgrade related activity is managed and administered through the Controller cluster endpoint. Software update for NSX Advanced Load Balancer is handled through a single image file for both the Controllers and the Service Engines.

Note Only system upgrades allowed if the NSX Advanced Load Balancer is setup in the basic license tier. For flexible upgrades, enterprise license tier is required.

Prerequisites

- Deploy the VMware NSX Advanced Load Balancer on the Advanced Load Balancing for VMware Cloud Foundation.
- Have a my.vmware.com customer portal account. This is used to access NSX Advanced Load Balancer upgrade and patch images.

Procedure

1 Take a local backup of the configuration before upgrading or patching.

   a In a Linux shell, SSH to the Controller cluster VIP by using admin@sfo-m01-avic01.sfo.rainpole.io.

   b Specify the NSX Advanced Load Balancer CLI by executing `shell –user admin –password <ENTER_PASSWORD>`.

   c Create a configuration backup by executing the following CLI commands:

```
export configuration file /tmp/upgrade_backup.json full_system
Please enter the passphrase to encrypt configuration: <ENTER A PASSPHRASE>
Retype passphrase: <RE-ENTER THE PASSPHRASE>
```

   A full system configuration backup is be available at the specified location, i.e. '`/tmp/upgrade_backup.json`'.

2 Download the required upgrade or patch image from my.vmware.com customer portal.

   a Follow this KB article to access NSX Advanced Load Balancer images.

   Note The steps mentioned in the KB article are valid for upgrade and patch images as well. The KB article describes steps for downloading the install image.

   b Click on the specific version to be downloaded.

   Note Patch releases are suffixed by the patch release number, for instance, 20.1.4-2p5 where 2p5 is the patch.

   c For upgrade images navigate to the **Upgrade** section and under **VMware / OpenStack / AWS / KVM / CSP**.

      1 Click on the download icon.

2. Accept the EULA and click **CONTINUE** to start download of the upgrade image.

d. For patch images navigate to the 'system' section.

1. Click the download icon.
2. Accept the EULA and click on **CONTINUE** to start download of the patch image.

3. Upload the required upgrade or patch image to the Controller cluster.
   a. In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/
   b. Navigate to **Administration > Controller > Software** and click on **Upload From Computer**.
   c. Select the upgrade or patch image file that was download and click on **Open**.
   d. Wait until the image upload is complete.
4. Perform a **Full System** update for the NSX Advanced Load Balancer.
   a. In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.
   b. Navigate to **Administration > Controller > System Update**.
   c. Choose the uploaded file and click on **UPGRADE**.
   d. Select **Upgrade All Service Engine Groups**.
   e. Select **Suspend** for **ACTION TO TAKE ON SEG UPDATE FAILURE**.
   f. Click on **Continue** and then click on **Confirm**.
   g. Progress can be tracked via the **In Progress** section in the **Administration > Controller > System Update** page.
   h. Wait until the upgrade or patch is complete.
5. Perform a **Separate Control and Data Plane** update for the NSX Advanced Load Balancer – Part I (the Controllers Only).
   a. In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.
   b. Navigate to **Administration > Controller > System Update**.
   c. Choose the uploaded file and click on **UPGRADE**.
   d. Un-select on **Upgrade All Service Engine Groups**.
   e. Click on **Continue** and then click on **Confirm**.
   f. Progress can be tracked via the **In Progress** section in the **Administration > Controller > System Update** page.
   g. Wait until the upgrade or patch is complete.

6 Perform a **Separate Control and Data Plane** update for the NSX Advanced Load Balancer – Part II (The Srtvice Engines Only).

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Administration > Controller > SEG Update**.

   c Select the Service Engine Groups to be upgraded or patched and click on .**UPGRADE**.

   d Select the **System** or **Patch** check box as appropriate and click on **Next**.

   e Select **Suspend** for **ACTION TO TAKE ON SEG UPDATE FAILURE**.

   f Click on **Continue** and then click on **Confirm**.

   g Progress can be tracked via the **In Progress** section in the **Administration > Controller > SEG Update** page.

   h Wait until the upgrade or patch is complete.

7 Perform a **Rollback** for the NSX Advanced Load Balancer.

   a In a web browser, log in to the Controller cluster VIP by using https://sfo-m01-avic01.sfo.rainpole.io/.

   b Navigate to **Administration > Controller > System Update**.

   c Select **ROLLBACK** and click on the previous version.

   d Select **Rollback All Service Engine Groups**.

   e Click on **Continue** and then click on **Confirm**.

   f Progress can be tracked via the **In Progress** section in the **Administration > Controller > System Update** page.

   g Wait until the rollback is complete.

Design Decisions of Advanced Load Balancing for VMware Cloud Foundation

8

This section explains the design decisions of Advanced Load Balancing for VMware Cloud Foundation.

Deployment Model for the Advanced Load Balancing for VMware Cloud Foundation

Table 8-1. *Design Decisions for Deploying the Controller for the VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-001	Initial setup should be done only on one NSX Advanced Load Balancer Controller VM out of the three deployed to create an NSX Advanced Load Balancer Controller cluster.	NSX Advanced Load Balancer Controller cluster is created from an initialized NSX Advanced Load Balancer Controller which becomes the cluster leader. Follower NSX Advanced Load Balancer Controller nodes need to be uninitialized to join the cluster.	NSX Advanced Load Balancer Controller cluster creation will fail if more than one NSX Advanced Load Balancer Controller is initialized.
AVI-CTLR-002	Apply vSphere DRS anti-affinity rules for the NSX Advanced Load Balancer Controller cluster nodes. **Note** For a default management vSphere cluster that consists of four ESXi hosts, you can put in maintenance mode only a single ESXi host at a time.	Ensure that NSX Advanced Load Balancer Controller VMs are distributed across ESXi hosts .	You must perform additional configuration to set up an anti-affinity rule.
AVI-CTLR-003	Protect NSX Advanced Load Balancer Controller cluster nodes using vSphere High Availability.	Supports the availability objectives for the NSX Advanced Load Balancer Controller cluster without requiring manual intervention during an ESXi host failure event.	None

Table 8-2. *Design Decisions for deploying Service Engines for the VMware NSX Advanced Load Balancer*

Decision ID	Decision Design	Design Justification	Design Implication
AVI-CTLR-004	Create an NSX-T Cloud Connector on NSX Advanced Load Balancer Controller for each NSX transport zone requiring load balancing.	A NSX-T Cloud Connector configured on the NSX Advanced Load Balancer Controller will provide load balancing for workloads belonging to a Transport Zone on NSX-T. **Note** 1. A NSX Transport Zone can be unique to a vCenter cluster, a VI Workload Domain or can be shared across VI workload domains. 2. Multiple NSX-T Cloud connectors can be configured on the NSX Advanced Load Balancer Controller if load balancing is required across multiple Transport Zones configured on NSX-T.	None

Table 8-3. *Design Decisions for deploying Service Engines on a Dedicated Edge VI Workload Domain for NSX Advanced Load Balancer Platform*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-005	Choose to deploy the Service Engines on a dedicated edge VI workload domain.	Allows for centralized placement of the Service Engines.	Capacity growth might be a challenge. Might not work in all cases due to scale restrictions of the edge VI workload domain.
AVI-CTLR-006	Create separate Service Engine Groups to host Virtual Services from different VI workload domains.	Allows for application isolation.	Might require additional Service Engine resources.

Table 8-4. *Design Decisions on Deployment of NSX Advanced Load Balancer Controllers in Multiple Availability Zones*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-VC-001	When using two availability zones, add the NSX Advanced Load Balancer Controller cluster nodes to the first availability zone VM group.	Ensures that, by default, the NSX Advanced Load Balancer Controller cluster nodes are powered on in the primary availability zone hosts group.	After the implementation of the second availability zone for the management domain, you must update the VM group for the primary availability zone virtual machines to include the NSX Advanced Load Balancer Controller cluster nodes.

Table 8-5. *Design Decisions for placing applications on NSX Advanced Load Balancer Service Engines in a Multi Availability Zone environment*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-VC-002	Create a VM groups for the NSX Advanced Load Balancer SE VMs.	Ensures that the NSX Advanced Load Balancer SE VMs can be managed as a group and added to VM/Host rules.	User must add each NSX Advanced Load Balancer SE VM to the primary availability zone.
AVI-VI-VC-003	Create a should-run VM-Host affinity rule to run all NSX Advanced Load Balancer SEs on the group of hosts in the first availability zone.	Ensures that all NSX Advanced Load Balancer SE VMs are in the first availability zone.	During normal operation, there would not be any NSX Advanced Load Balancer SEs running in the second availability zone. Therefore all apps would be active in the first availability zone.

Integration of the Advanced Load Balancing for VMware Cloud Foundation

Table 8-6. *Design Decisions for creating an NSX-T Cloud on the Controller for the VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-007	Create one NSX-T Cloud connector object on the Controller per transport zone configured on the NSX manager cluster that requires Load Balancing services. **Note** Transport zone could be dedicated to a VI workload domain or shared across VI workload domains.	Provides automated deployment of load-balanced applications through NSX-T Cloud integration. Allows for maximum flexibility, control, and isolation in terms of application deployment.	None
AVI-CTLR-008	Provide either a overlay-backed NSX segment connected to a Tier-1 logical router or a VLAN-backed NSX segment for the Service Engine management for the NSX-T Cloud of overlay type.	This network is used for the Controller to the Service Engine connectivity.	None
AVI-CTLR-009	Provide one or more NSX managed VLAN segments as data networks for the NSX-T Cloud connector of VLAN type. **Note** A single NSX-T Cloud connector of VLAN type can contain multiple data networks. Each data network should belong to a unique NSX managed VLAN segment.	The Service Engines are placed on NSX managed VLAN segments.	None

Table 8-6. *Design Decisions for creating an NSX-T Cloud on the Controller for the VMware Cloud Foundation* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-010	Provide a Tier-1 router and a connected overlay-backed NSX segment as data network for the NSX-T Cloud of overlay type. **Note** A single NSX-T Cloud connector of overlay type can contain multiple data networks. Each data network must belong to a unique Tier-1 router.	The Service Engines are placed on Overlay Segments created on these Tier-1 logical router(s).	None
AVI-CTLR-011	Provide an object name prefix when creating the NSX-T Cloud Connector on the NSX Advanced Load Balancer Controller.	Used for uniquely identifying NSX-T Cloud Connector created resources on NSX Manager cluster and vCenter Server.	None

Isolation Model for Load-Balanced Applications in Advanced Load Balancing for VMware Cloud Foundation

Table 8-7. *Design Decisions for creating a Tenants for isolation on the VMware NSX Advanced Load Balancer for the VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-012	Create tenants to provide desired level of isolation for the VMware Cloud Foundation. **Note** NSX Advanced Load Balancer - Basic Edition does not provide tenant isolation.	Provides required level of configuration and data plane isolation for workloads.	Additional Service Engine resources might be required.

Table 8-8. *Design Decisions for Service Engine Group Design for VMware NSX Advanced Load Balancer for the VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-013	Create multiple Service Engine Groups as desired to isolate applications. **Note** Some of the criteria for grouping applications in different Service Engine Group(s) could be based on: ■ Multiple line of business ■ Prod v/s non-Prod ■ Different scale and performance requirements	Allows efficient isolation of applications and allows for better capacity planning. Allows flexibility of life-cycle-management.	None
AVI-CTLR-014	Create separate set of Service Engine Groups for each VI workload domain and scope the Service Engine Group to the VI workload domain vCenter server. **Note** ■ Applicable where a single Controller cluster serving multiple VI workload domains. ■ If applications need to be shared across VI workload domains, then the Service Engine Group could be scoped to multiple vCenter Servers.	Allows isolation of the Service Engines across VI workload domains. Enables per VI workload domain life-cycle-management.	None
AVI-CTLR-015	Configure Service Engine Group for Active/ Active HA mode. **Note** Legacy Active/ Standby HA mode might be required for certain applications.	Provides optimum resiliency, performance, and utilization.	Certain applications might not work in Active/ Active mode. For instance, applications that require preserving client IP. In such cases, use the Legacy Active/ Standby HA mode.

Table 8-8. *Design Decisions for Service Engine Group Design for VMware NSX Advanced Load Balancer for the VMware Cloud Foundation* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-016	Enable 'Dedicated dispatcher CPU' on Service Engine Groups that contain the Service Engine VMs of 4 or more vCPUs. **Note** This setting should be enabled on SE Groups that are servicing applications that have high network requirement.	This will enable a dedicated core for packet processing enabling high packet pipeline on the Service Engine VMs. **Note** By default, the packet processing core also processes load balancing flows.	None .
AVI-CTLR-017	Set 'Placement across the Service Engines' setting to 'distributed'.	This allows for maximum fault tolerance and even utilization of capacity.	Might require more Service Engine VMs as compared to 'compact' placement mode.
AVI-CTLR-018	Enable CPU and Memory reservation on the Service Engine Group. .	The Service Engines are a critical infrastructure component providing load-balancing services to mission critical applications.	None
AVI-CTLR-019	Configure a consistent Service Engine Name Prefix that indicates the Service Engine VM for instance, 'avise-xxxx'. **Note** Where ‘xxxx’ could be used as an arbitrary identifier.	This allows efficient grouping and filtering.	None
AVI-CTLR-020	Choose the Service Engine Group mode as Legacy HA Active/ Standby if the Controller is set to use basic edition. .	NSX Advanced Load Balancer Controller in Basic Edition only supports Legacy HA Active/ Standby mode.	Applications will not be deployed in an Active/ Active fashion, thereby losing out on elastic capacity management. NSX Advanced Load Balancer Enterprise Edition will allow Active/ Active as well as Legacy Active/ Standby deployments.

Physical Design of the Advanced Load Balancing for VMware Cloud Foundation

Table 8-9. *Design Decisions for Physical Design of ESXi Hosts to support the VMware NSX Advanced Load Balancer*

Decision ID	Design Description	Design Justification	Design Implication
AVI-PHY-001	Provide high performance disks (SSD/ Flash) to hosts that run the Controller VMs.	The Controllers need high performance disks to process the analytics pipeline.	None
AVI-PHY-002	Enable AES-NI instructions setting in the BIOS for ESXi hosts.	AES-NI instruction set provides efficiency in SSL performance.	Most modern machines have AES-NI enabled by default, if not enabled by default, you need to reboot ESXi hosts to enable this setting.
AVI-PHY-003	Disable C-State and P-State settings in BiOS on the ESXi hosts. **Note** This is an optional design decision.	Provides maximum performance.	This might require a reboot and reconfigure of the BIOS causing an outage for each ESXi host.

vCenter Design of the Advanced Load Balancing for VMware Cloud Foundation

Table 8-10. *Design Decisions for the Virtual Infrastructure to support the VMware NSX Advanced Load Balancer*

Decision ID	Design Description	Design Justification	Design Implication
AVI-VI-VC-004	Create anti-affinity 'VM/ Host' rule that prevents collocation of the Controller VMs.	vSphere will take care of placing the Controller VMs in a way that always ensures maximum HA for the Controller cluster.	None
AVI-VI-VC-005	Create a virtual machine group for the Controller VMs.	Ensures that the Controller VMs can be managed as a group.	You must add virtual machines to the allocated groups manually.
AVI-VI-VC-006	In vSphere HA, for each Controller and Service Engine VMs, set the restart priority policy to high and host isolation response to disabled.	This ensures fast recovery for the NSX Advanced Load Balancer.	None

Table 8-10. *Design Decisions for the Virtual Infrastructure to support the VMware NSX Advanced Load Balancer* (continued)

Decision ID	Design Description	Design Justification	Design Implication
AVI-VI-VC-007	Create one Content Library on the management domain to store Controller OVA.	Deploying OVA from the Content Library will be operationally easy to do.	Might not be necessary if deploying Controller VMs using automation tools such as vRO, Ansible, etc.
AVI-VI-VC-008	Create one Content Library on each of the VI workload domain to store Service Engine OVA.	The Controller's NSX-T Cloud Connector requires a Content Library configured to create the Service Engines.	None

VCenter Server Design of the Advanced Load Balancing for VMware Cloud Foundation

NSX-T Data Center Design of the Advanced Load Balancing for VMware Cloud Foundation

Table 8-11. *Design Decisions for NSX-T Data Center Access Control for NSX Advanced Load Balancer Controller*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-NSX-001	Create or use an NSX-T Manager cluster User/ Role with password with the described privileges. **Note** It is recommended not to use the local 'admin' user of NSX-T Data Center.	Required for the Controller to perform lifecycle management of the Service Engines. **Note** Update the NSX-T User Credential on the Controller when password for this user account is rotated.	None

Table 8-12. *Design Decisions for the NSX-T Data Center Distributed Firewall Rules*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-NSX-002	Create necessary NSX DFW and/ or Gateway Firewall rules for the NSX Advanced Load Balancer control plane as described to ensure connectivity from: ■ Admin to the Controllers ■ The Controllers to the Controllers ■ The Controllers to Service Engines	These firewall rules are needed to allow required communication for the NSX Advanced Load Balancer control plane. **Note** If DFW is enabled and these rules are not configured, this might result in NSX Advanced Load Balancer control plane not functioning as expected.	None
AVI-NSX-003	Create necessary NSX DFW and/ or Gateway Firewall rules for the configured load-balanced applications as described to ensure connectivity from: ■ Client to VIPs ■ Service Enginess to Backend Pool Servers	These firewall rules are needed to allow required communication for the configured load-balanced applications. **Note** If DFW is enabled and these rules are not configured, this might result in the configured load-balanced applications not functioning as expected.	None

Licensing VMware Advanced Load Balancing for VMware Cloud Foundation

Table 8-13. *Design Decisions for Licensing VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-021	Choose the VMware NSX Advanced Load Balancer Enterprise with Cloud Services licensing tier. **Note** 1. New VMware NSX Advanced Load Balancer deployments running v21.1.3 or later will be setup by default in Enterprise with Cloud Services licensing tier. 2. If running v21.1.2 or earlier, choose the VMware NSX Advanced Load Balancer Enterprise licensing tier.	Provides full-featured access to the NSX Advanced Load Balancer platform. **Note** If running v21.1.3 or later, alternative is to either use: i) Enterprise edition licensing tier. This provides a full-featured enterprise feature set but does not give access to Cloud Services and advanced App Security features. ii) Basic edition licensing tier. This provides equivalent functionality of NSX-T Data Center native Load Balancer. If running v21.1.2 or earlier, alternative is to use the Basic edition licensing tier. This provides equivalent functionality of NSX-T Data Center native Load Balancer.	None

How to size Advanced Load Balancing for VMware Cloud Foundation

Table 8-14. *Design Decisions for sizing the Controllers for the NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-022	Deploy one Controller cluster for each NSX Manager cluster for configuring and managing load balancing services.	Required to form a highly available Controller cluster.	None
AVI-CTLR-023	Deploy each node in the Controller cluster with a minimum of 8 vCPUs, 32 GB memory and 216 GB of disk space.	Support up to 200 virtual services. Support up to 100 NSX Advanced Load Balancer Service Engines. Can scale-up with expansion of the Controller sizes anytime. **Note** Under sizing, the Controllers can lead to unstable control plane functionality.	None

Network Design for Advanced Load Balancing for VMware Cloud Foundation

Table 8-15. *Design Decisions for the Networking Design for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-VC-010	Deploy the Controller cluster nodes on the VMware Cloud Foundation management network.	Allows for ease of management for the Controllers. Allows for configuring a floating cluster VIP; a single IP address that will be assigned to the cluster leader. Administrative tasks, connectivity to the Service Engines and connectivity to network services will all use this network.	None
AVI-NSX-004	Configure a management network to deploy the Service Engines. Management network needs to be NSX segment and could be either of: 1 VLAN-backed NSX segment 2 Overlay-backed NSX segment connected to a Tier-1 router **Note** This network should have connectivity to the IP addresses of each of the Controllers.	This is required to configure the Controller NSX-T Cloud Connector.	None

Table 8-15. *Design Decisions for the Networking Design for VMware NSX Advanced Load Balancer* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-NSX-005	Configure one or more data network(s) for the Service Engines to service load-balanced applications. Data networks need to be NSX-T managed and could be either of: 1 VLAN-backed NSX segment, or, 2 Overlay-backed NSX segment connected to a Tier-1 router **Note** For overlay-backed NSX segments, one logical segment is required per Tier-1 router.	The Service Engines require data networks to provide access for load-balanced applications.	None
AVI-CTLR-024	Latency between the Controllers must be <10ms.	The Controller quorum is latency sensitive. **Note** The Control plane might go down if latency is high.	None
AVI-CTLR-025	Latency between the Controllers and the Service Engines should be <75ms.	Required for correct operation of the Service Engines. **Note** May lead to issues with heartbeats and data synchronization between the Controller and the Service Engines.	None

Table 8-16. *Design Decisions for the IP Addressing Scheme for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-026	Use static IPs or DHCP with reservation ensuring a permananet lease for the Controllers.	The Controller cluster uses management IPs to form and maintain quorum for the control plane. **Note** The Controller control plane might go down if the management IPs of the Controller change.	None
AVI-VI-001	Reserve an IP in the management subnet to be used as the cluster IP for the Controller cluster.	A floating IP that will always be accessible regardless of a specific individual Avi cluster node.	None
AVI-NSX-006	Configure DHCP on the networks/ logical segments used for data traffic.	Having DHCP enabled for data networks makes the Service Engine configuration simple. **Note** Alternatively, operators could use static IPs, but can have to program IP pools for the data networks to be used by the Service Engines and also add a static route for the data network's gateway on the Controller .	None

Table 8-17. *Design Decisions for the IP Addressing Scheme for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-026	Use static IPs or DHCP with reservation ensuring a permananet lease for the Controllers.	The Controller cluster uses management IPs to form and maintain quorum for the control plane. **Note** The Controller control plane might go down if the management IPs of the Controller change.	None
AVI-VI-001	Reserve an IP in the management subnet to be used as the cluster IP for the Controller cluster.	A floating IP that will always be accessible regardless of a specific individual Avi cluster node.	None
AVI-NSX-006	Configure DHCP on the networks/ logical segments used for data traffic.	Having DHCP enabled for data networks makes the Service Engine configuration simple. **Note** Alternatively, operators could use static IPs, but can have to program IP pools for the data networks to be used by the Service Engines and also add a static route for the data network's gateway on the Controller .	None

Table 8-18. *Design Decisions for the Time Synchronization for VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-VI-003	Configure time synchronization by using an NTP time for the Controller. **Note** Recommendation is to use the same source as SDDC Manager, vCenter Server and NSX Manager cluster.	Prevents from time synchronization issues. Not required to provide connectivity to an external NTP server.	An operational NTP service must be available in the environment. Ensure that NTP traffic between the Controllers, the Service Engines and the NTP servers is allowed on the required network ports and not firewalled.

Lifecycle Management for Advanced Load Balancing for VMware Cloud Foundation

Table 8-19. *Design Decisions for Lifecycle Management of the VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-027	Use the Controller to performance lifecycle management of the NSX Advanced Load Balancer.	■ Lifecycle of NSX Advanced Load Balancer is not managed by SDDC Manager. ■ The Controller manages lifecycle for all NSX Advanced Load Balancer components including the Controllers and all the associated Service Engines.	Deployment, patching, updates, and upgrades of NSX Advanced Load Balancer are performed without native SDDC automation.
AVI-CTLR-028	When a VI workload domain is upgraded, upgrade NSX Advanced Load Balancer before upgrading NSX-T Data Center based on the compatibility matrix with vCenter Server and NSX-T Data Center. **Note** Check the version compatibility matrix in the Advanced Load Balancing for VMware Cloud Foundation validated solution document before upgrading.	Ensures NSX Advanced Load Balancer cloud integration with NSX-T Data Center and vCenter Server continues to function as expected. **Note** Upgrading vCenter Server and/ or NSX-T Data Center before NSX Advanced Load Balancer might lead to issues with the NSX-T Cloud Connector integration on the Controller due to version incompatibility.	None
AVI-CTLR-029	If the Controller is providing services to multiple VI workload domains, choose to upgrade the Controller and only the Service	■ Allows isolated upgrade for the VI workload domain ■ Upgrade only the Service Engines that reside on the VI workload domain that is being upgraded ■ VI workload domain that is currently not being upgraded, but shares the same Controller is left untouched.	None

Table 8-19. *Design Decisions for Lifecycle Management of the VMware NSX Advanced Load Balancer* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
	Engine Groups that are associated with the VI workload domain that is being upgraded. **Note** This is optional. Alternatively, choose to upgrade the entire Controller cluster, which will upgrade the Controllers and all the Service Engines.		

Information Security and Access of Advanced Load Balancing for VMware Cloud Foundation

Table 8-20. *Design Decisions for Information Security and Access of the VMware NSX Advanced Load Balancer*

Decision ID	Design Decision	Design Justification	Design Implication

AVI-CTLR-030	Create a strong password for the local admin account on NSX Advanced Load Balancer:
	■ Minimum 8 char long
	■ Contains at least one char in each of 3/4 of the following categories:
	  ■ Uppercase letters
	  ■ Lowercase letters
	  ■ Digits
	  ■ Special characters
		This reduces the risk of the account being compromised.
		This is a requirement to setup user accounts, including the admin account.
			None.

AVI-CTLR-031	Rotate passwords at least every 3 months.	Ensures security of the user accounts.	None

Table 8-20. *Design Decisions for Information Security and Access of the VMware NSX Advanced Load Balancer* (continued)

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-032	Limit the use of the local accounts for both interactive or API access and solution integration.	Local accounts are not specific to user identity and do not offer complete auditing from an endpoint back to the user identity.	You must define and manage service accounts, security groups, group membership, and security controls in Active Directory.
AVI-CTLR-033	Create user accounts with desired Roles on the Controller to limit the scope and privileges for accounts used for both interactive or API access and solution integrations. **Note** A custom 'Role' might be created if a user account needs to have specific permissions that are not available out of the box on the Controllers.	The principle of least privilege is a critical aspect of access management and should be part of a comprehensive defense-in-depth security strategy.	You may need to define and manage custom roles and security controls to limit the scope and privileges used for interactive access or solution integration.

Monitoring and Alerting of Advanced Load Balancing for VMware Cloud Foundation

Table 8-21. *Design Decisions for Monitoring and Alerting for Advanced Load Balancing for VMware Cloud Foundation*

Decision ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-035	Choose one or more types of notification of choice for monitoring/ alerting. It is recommended to enable alerts on the following pre-defined `System` alerts: ■ System-VS-Alert ■ System-SSL-Alert ■ System-SE-Alert ■ System-Controller-Alert ■ System-CC-Alert	Ensure good health through proactive alerting of the NSX Advanced Load Balancer cluster.	None

Data Protection of Advanced Load Balancing for VMware Cloud Foundation

Table 8-22. *Design Decisions for Data Protection of Advanced Load Balancing for VMware Cloud Foundation*

Design ID	Design Decision	Design Justification	Design Implication
AVI-CTLR-036	Create a backup schedule to take periodic backups at least every 24 hours.	Backed up configuration will aid in rebuilding and recovering the NSX Advanced Load Balancerconfiguration from catastrophic failires.	Backup server should support SCP as the transport protocol.