Best Practices for Virtualization and Clustering of NativeEdge Endpoints

White Paper

H04556.1

Abstract

This paper presents best practices for clustering Dell NativeEdge endpoints, addressing hardware, networking, storage, VM operations, scaling, and lifecycle management in distributed compute environments.

November 2025

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Best Practices for Virtualization and Clustering of NativeEdge Endpoints

Introduction

Dell NativeEdge, as enabled in the Dell Automation Platform, is a full-stack, end-to-end edge solution that handles both infrastructure management and application orchestration. With Dell NativeEdge, you can simplify edge operations, optimize for AI at the edge, and protect your edge estate.

Revision history

The following table lists the revision history of this document.

Table 1. Revision history

Revision	Date	Change description
H04556.1	Nov 2025	● Updated Hardware considerations. ● Updated Network considerations. ● Updated Cluster quorum. ● Updated Adding or removing nodes.
H04556	Aug 2025	Initial release.

Terminology

The following table provides definition for some of the terms that are used in this document, Dell Automation Platform concepts, and Dell NativeEdge concepts.

Table 2. Terminology

Term	Definition
Blueprint	A YAML file with definitions of resources and connections between them (based on the TOSCA specification), that is used to templatize application deployment.
Cluster	A group of interconnected, identical endpoints working together to improve performance, scalability, and fault tolerance in a network environment.
Deployments	Applications or solutions that are deployed from blueprints.
FIDO Device Onboard (FDO)	The primary technology used to provide Secure Device Onboarding with FDO. For more information, see FIDO Device Onboard Specification 1.1.
Catalog	A collection of applications for a specifc independent software vendors (ISVs) or utilities, including the necessary configurations and application metadata.
NativeEdge endpoint	Select Dell hardware optimized for the platform with the NativeEdge OS for secure device onboarding, providing a secure and scalable operating environment to run edge applications as VMs.
Dell Automation Platform orchestrator	A management component built into the edge platform that provides hierarchical security, orchestration, and lifecycle management of vertical solutions distributed across the edge, core, and edge local deployments.
NativeEdge OS	A combination of a Linux-based operating system, KVM hypervisor, and an orchestrator agent that enables NativeEdge infrastructure to work within the Dell Automation Platform.
Onboarding service	A support service for FDO protocols to bind the endpoint to the Dell Automation Platform orchestrator and allow the orchestrator to provision the device.
Rendezvous service	A networking service that run within the Dell Automation Platform orchestrator that determines how the newly powered-on NativeEdge endpoint connects to the Dell Automation Platform orchestrator.

Product overview

Dell NativeEdge is a secure, scalable edge operations software solution that is designed to simplify and accelerate the deployment, management, and security of edge infrastructure and applications. Built to address the complexities of operating at the edge, NativeEdge enables zero-touch provisioning, centralized orchestration, and policy-based automation across geographically distributed locations. It supports a wide range of workloads—from AI inference to industrial control—on diverse hardware form factors, including servers, desktop workstations, and gateways. With integrated security features such as role-based access control, encrypted communications, and device attestation, NativeEdge helps IT and OT teams ensure consistent, compliant deployments. Its open architecture and integration with popular tools like Ansible, Kubernetes, and ServiceNow make it a flexible choice for organizations scaling their digital transformation to the edge.

Dell Automation Platform orchestrator

The Dell Automation Platform orchestrator is the centralized engine behind Dell NativeEdge, providing a single-pane-of-glass interface to remotely deploy, configure, monitor, and update edge infrastructure at scale. It enables zero-touch provisioning, templated deployments, and policy-driven governance to ensure consistent, secure, and repeatable operations across distributed environments.

NativeEdge endpoints

NativeEdge endpoints—such as servers and PC workstations—are managed through the orchestrator and designed for diverse, often remote environments. These endpoints run critical workloads including AI, analytics, and control systems, and benefit from automated lifecycle management, integrated telemetry, and secure updates. Together, the orchestrator and endpoints form a resilient, scalable, and manageable edge solution for IT and OT teams.

Clustering NativeEdge endpoints

Clustering NativeEdge endpoints enables high availability, scalability, and workload distribution across multiple edge devices within a local environment. By grouping endpoints into a cluster, organizations can ensure that critical applications remain resilient to hardware failures and resource constraints. NativeEdge supports automated cluster formation and management, simplifying the deployment of virtual machine workloads with shared networking and shared storage. Clusters can be configured to support load balancing, failover, and data redundancy, making them ideal for edge use cases that demand uptime and performance. This approach not only enhances fault tolerance but also allows for more efficient use of compute resources across the edge footprint.

Hardware considerations

When deploying NativeEdge in a clustered configuration, you must give careful attention to hardware uniformity and compatibility to ensure optimal performance and reliability. NativeEdge supports both 3-node and 4-node cluster configurations, offering flexibility in scaling edge infrastructure based on workload demands. However, a critical requirement for clustering is that all participating endpoints must be identical in their hardware specifications. This uniformity is essential to maintain consistency in performance, simplify management, and avoid compatibility issues during orchestration and failover scenarios.

It is recommended to maintain uniformity across the nodes as well, as doing so not only streamlines the deployment process, but also enhances the resilience, performance, and manageability of the NativeEdge cluster.

Network considerations

A single network switch may suffice for basic NativeEdge setups, but clustered high-availability (HA) environments require a more robust and segmented network design to ensure performance, fault tolerance, and manageability.

Separate management switches are used for administrative access: one connects to NativeEdge onboarding interfaces using the host operating system, while the other provides true out-of-band (OOB) connectivity to integrated Dell Remote Access Controller (iDRAC) interfaces. Isolating management traffic from production workloads enhances security and simplifies troubleshooting. Static IP addressing or a dedicated DHCP scope should be used for management interfaces and access should be tightly controlled through VLAN segmentation.

The data plane is supported by two redundant switches that handle both virtual machine traffic and inter-node cluster communication. These switches should be deployed in a high-availability configuration—such as Multi-Chassis Link Aggregation (MLAG) or switch stacking—to eliminate single points of failure. Additionally, VLAN segmentation is recommended to logically separate VM and cluster traffic.

Port bonding adds another layer of redundancy. NativeEdge supports active-passive bonding, where one interface handles traffic and the other remains on standby. If a link fails, traffic automatically switches to the passive interface, ensuring continuous connectivity. This setup also simplifies network management by consolidating multiple physical interfaces into one logical connection.

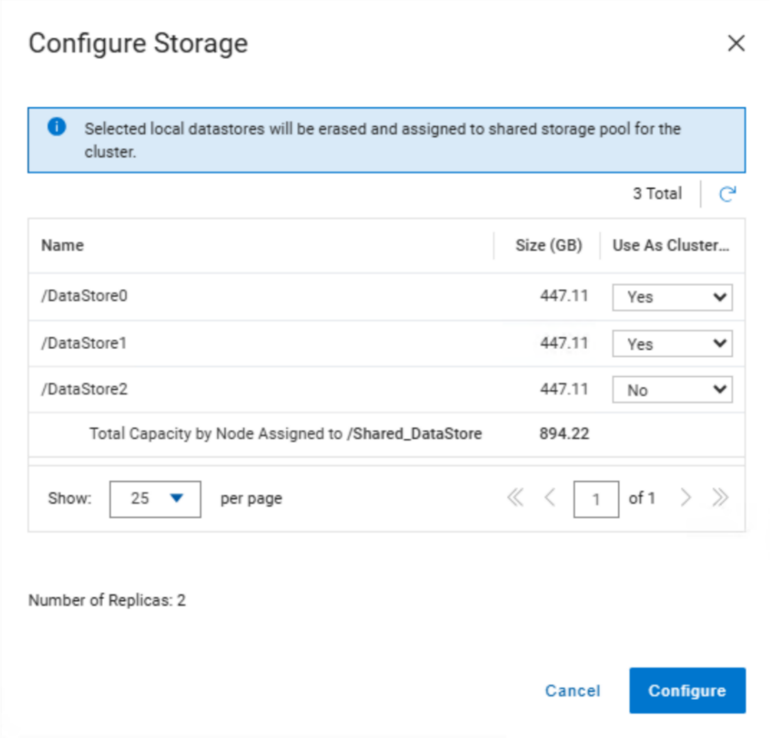
By following these best practices, organizations can build a scalable, resilient, and secure network foundation for NativeEdge deployments—whether in a single-node setup or a fully clustered HA environment.

Storage

In a NativeEdge cluster, the endpoints work together to form a software-defined storage (SDS) pool, enabling distributed, resilient storage across the entire cluster. This is achieved by selecting a specific datastore from each node to contribute to the shared storage pool. These selected datastores are then abstracted and managed collectively by the cluster software, allowing workloads to access a virtual datastore.

NativeEdge ensures data resiliency and high availability by maintaining two copies of each data block across different nodes in the cluster. This redundancy protects against node or hardware failures, ensuring that data and applications remains accessible even if one node becomes unavailable.

Additionally, the software-defined storage pool is dynamically scalable. Administrators can scale up the storage capacity by adding additional datastores—if available—on the NativeEdge endpoints. Conversely, the pool can be scaled down by removing datastores, provided that the cluster maintains the required redundancy and capacity thresholds. This flexibility allows organizations to adapt their storage infrastructure to evolving workload demands without disrupting operations.



Configure Storage

Selected local datastores will be erased and assigned to shared storage pool for the cluster.

3 Total

Name	Size (GB)	Use As Cluster...
/DataStore0	447.11	Yes
/DataStore1	447.11	Yes
/DataStore2	447.11	No
Total Capacity by Node Assigned to /Shared_DataStore	894.22	

Show: 25 per page 1 of 1

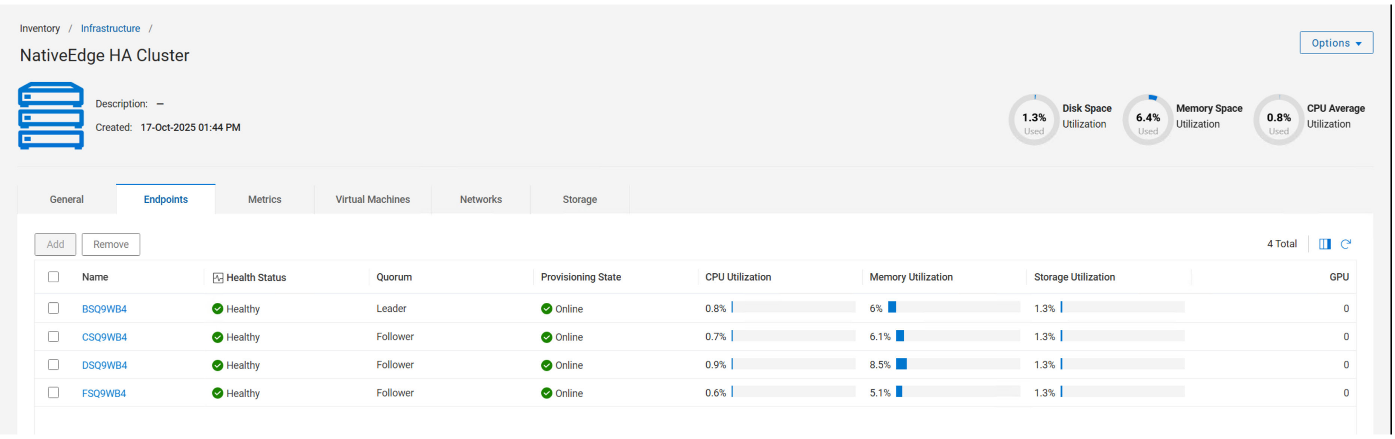
Number of Replicas: 2

Figure 1. Configure shared storage

Cluster quorum

In a clustered NativeEdge environment, quorum is a critical concept that ensures the cluster operates reliably and avoids “split-brain” scenarios—situations where disconnected nodes might act independently, leading to data inconsistencies or conflicting operations. Quorum refers to the minimum number of healthy, connected nodes required to make authoritative decisions and maintain cluster integrity.

NativeEdge uses a leader-follower architecture to manage quorum and ensure high availability. When a cluster is first formed, one node is designated as the leader, responsible for coordinating configuration changes, orchestrating operations, and maintaining a consistent state across all nodes. The remaining nodes join as followers, operating under the leader’s direction to stay synchronized.



NativeEdge HA Cluster

Description: –
Created: 17-Oct-2025 01:44 PM

1.3% Used Disk Space Utilization
6.4% Used Memory Space Utilization
0.8% Used CPU Average Utilization

4 Total

□	Name	Health Status	Quorum	Provisioning State	CPU Utilization	Memory Utilization	Storage Utilization	GPU
□	BSQ9WB4	✓ Healthy	Leader	✓ Online	0.8%	6%	1.3%	0
□	CSQ9WB4	✓ Healthy	Follower	✓ Online	0.7%	6.1%	1.3%	0
□	DSQ9WB4	✓ Healthy	Follower	✓ Online	0.9%	8.5%	1.3%	0
□	FSQ9WB4	✓ Healthy	Follower	✓ Online	0.6%	5.1%	1.3%	0

Figure 2. HA cluster

To maintain quorum, NativeEdge continuously monitors the health and connectivity of all nodes. If the leader becomes unavailable, the system automatically initiates a leader election among the followers. This process promotes a new leader without manual intervention, preserving decision-making authority and keeping the cluster operational.

By ensuring that only one active leader exists and that a sufficient number of nodes are connected, NativeEdge maintains a unified and resilient cluster state. This architecture supports seamless scalability, allowing new follower nodes to be added without disrupting governance or performance.

Adding or removing nodes

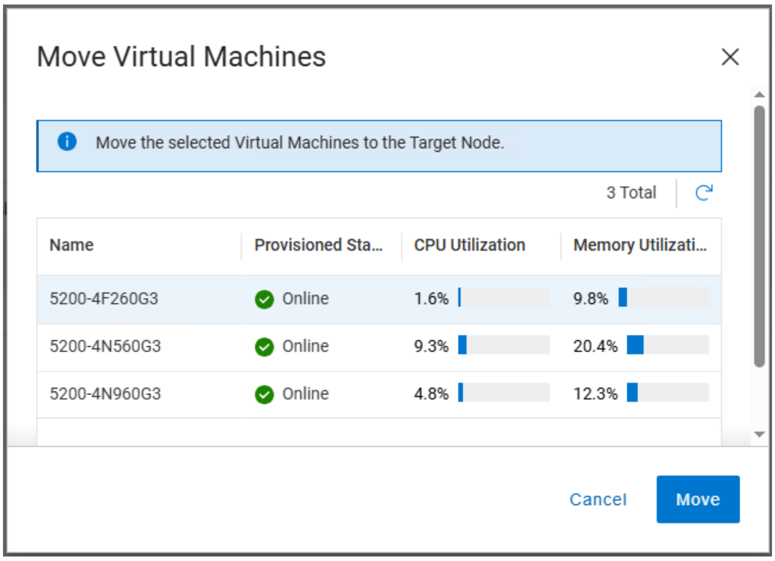
Adding and removing nodes in a cluster is a seamless and intuitive process, enabling administrators to scale or reconfigure their environments with minimal effort. When expanding a cluster, new nodes can be easily added and automatically integrated as followers under the direction of the existing leader, allowing them to quickly contribute to the cluster’s workload. It is important to ensure that all endpoints being added are configured with the same hardware model and configuration as existing nodes. The nodes also require the same virtual network segments, with the same names on all nodes. This consistency is critical for maintaining performance, compatibility, and reliability across the cluster. Removing nodes is also straightforward; however, any virtual machines running on a node must be migrated prior to its removal. This ensures that workloads remain uninterrupted and that the cluster maintains its operational integrity during the reconfiguration process.

This flexible node management approach offers several key benefits. It supports dynamic scaling to accommodate changing resource demands, simplifies maintenance and hardware lifecycle management, and enhances overall operational agility. Whether responding to growth, optimizing resource allocation, or performing infrastructure upgrades, NativeEdge makes it easy to maintain a resilient and efficient cluster environment—provided that all scaled endpoints match the configuration and hardware standards of the existing infrastructure.

VM mobility

VM migration types

NativeEdge supports several types of virtual machine (VM) migration—referred to as a 'move' within the platform—to ensure flexibility and resilience within a cluster. These include offline migration, online migration, and failover migration, each serving different operational needs.



Move Virtual Machines

Move the selected Virtual Machines to the Target Node.

3 Total

Name	Provisioned Sta...	CPU Utilization	Memory Utilizati...
5200-4F260G3	Online	1.6%	9.8%
5200-4N560G3	Online	9.3%	20.4%
5200-4N960G3	Online	4.8%	12.3%

Figure 3. Move Virtual Machines

Offline migration Involves shutting down a VM before moving it to another node. This method is typically used during planned maintenance or when live migration is not feasible due to hardware or configuration limitations. While it introduces temporary downtime, it ensures a clean and controlled transfer of the VM.

Online migration Often referred to as live migration, online migration allows a VM to move between nodes without any downtime. This is ideal for mission-critical workloads that require continuous availability. The process relies on compatible hardware and sufficient network bandwidth to transfer the VM's memory and state seamlessly while it continues to run.

Failover migration An automated process that is triggered when a node unexpectedly fails. In this scenario, the VM is restarted on another healthy node using the replicated data that are stored in the cluster's software-defined storage pool. This ensures high availability and minimizes service disruption, leveraging integrated monitoring and resiliency features.

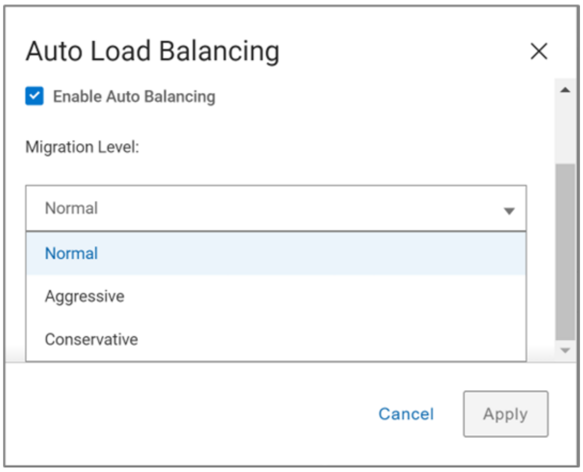
Together, these migration methods provide a robust framework for maintaining uptime, optimizing resource usage, and ensuring business continuity in edge environments.

Automatic load balancing

Dell NativeEdge supports automatic load balancing (ALB) to streamline resource distribution across clustered endpoints. This feature enables the system to autonomously migrate virtual machines between nodes based on real-time CPU utilization, eliminating the need for manual intervention.

When ALB is enabled, the Application Scheduler—running on the cluster's leader node—evaluates the CPU utilization of all nodes every 10 minutes. If the difference in CPU usage between nodes exceeds a configured threshold, the system initiates VM migrations to balance the load.

ALB supports three migration sensitivity levels—**Conservative** (40%), **Normal** (30%), and **Aggressive** (20%)—which define how much CPU utilization disparity is tolerated before triggering migrations. The default setting is **Normal**, but users can adjust the migration level or disable ALB entirely based on workload characteristics. Once enabled, the system automatically identifies overutilized nodes and redistributes VMs to underutilized ones, including those recently imported. This ensures consistent performance and resource efficiency without requiring manual VM placement or intervention and integrates seamlessly with the broader VM lifecycle management framework.



Auto Load Balancing

☑ Enable Auto Balancing

Migration Level: Normal

Figure 4. Auto Load Balancing window

In a NativeEdge high-availability (HA) cluster with three endpoints, each endpoint runs multiple VMs supporting a variety of workloads:

- Endpoint 1:
  - Web server VM (8 vCPUs, 32 GB RAM)
  - Logging VM (2 vCPUs, 8 GB RAM)
  - Monitoring agent VM (2 vCPUs, 4 GB RAM)
- Endpoint 2:
  - File server VM (4 vCPUs, 16 GB RAM)
  - Backup VM (2 vCPUs, 8 GB RAM)
  - Print service VM (2 vCPUs, 4 GB RAM)
- Endpoint 3:
  - Database server VM (6 vCPUs, 24 GB RAM)
  - Reporting VM (2 vCPUs, 8 GB RAM)
  - Cache VM (2 vCPUs, 4 GB RAM)

During a high-traffic eCommerce event, the web server VM on Endpoint 1 spikes to 85% CPU utilization. This heavy load begins to impact the performance of the other VMs on the same endpoints, particularly the logging and monitoring services.

NativeEdge's ALB, operating in fully automated mode, detects the resource contention on Endpoint 1. To alleviate pressure and maintain performance, ALB live-migrates the logging VM to Endpoint 2 and the monitoring agent VM to Endpoint 3. The web server VM remains on Endpoint 1, as it is the primary workload driving the CPU usage and benefits from local resource continuity. These migrations occur without downtime, ensuring uninterrupted service.

Post-migration resource distribution:

- Endpoint 1: Now focused solely on the web server VM, CPU usage stabilizes around 75%.
- Endpoint 2: Takes on the logging VM, rising to 60% CPU utilization.
- Endpoint 3: Endpoints the monitoring agent VM, increasing to 55% CPU utilization.

This scenario illustrates how NativeEdge's ALB intelligently balances workloads by offloading secondary services, ensuring critical applications like the web server continue to perform optimally under pressure.

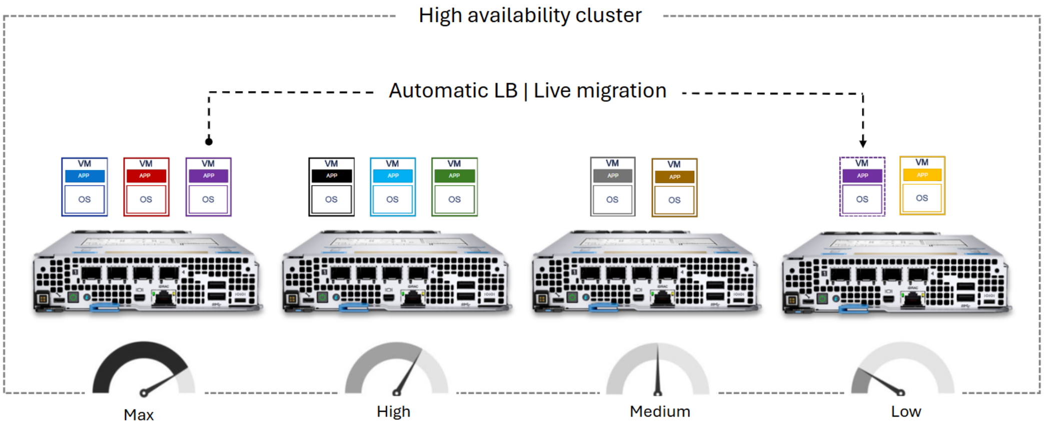


Figure 5. Automatic load balancing

HA groups

High Availability (HA) groups in Dell NativeEdge enable administrators to manage virtual machine placement and continuity across clustered nodes by defining node priorities.

HA groups in Dell NativeEdge provide a structured way to manage virtual machine placement and continuity across clustered nodes. These groups allow administrators to define node priorities, which influence where VMs are allowed—or preferred—to run. By assigning VMs to HA groups and configuring node preferences, organizations gain precise control over failover behavior, workload recovery, and operational alignment.

In a NativeEdge cluster with three nodes, an organization is running several critical workloads:

- Finance DB VM—a high-performance database supporting financial transactions.
- Analytics engine VM—a batch processing workload that generates real-time business insights.
- Reporting VM—a scheduled job that compiles daily operational reports.

Initially, all three VMs are running on Node 1, which has the most available resources and is optimized for performance. However, to ensure high availability and intelligent workload placement in the event of a failure or maintenance, the administrator creates an HA group named Mission Critical.

The Mission Critical HA group is configured with the following node priorities:

- Node 1—Priority 1 (preferred)
- Node 2—Priority 2 (fallback)

The three VMs are then assigned to this HA group. With this configuration in place, NativeEdge ensures that:

- Under normal conditions, the VMs run on Node 1.
- If Node 1 becomes unavailable (for example, due to maintenance or failure), the VMs are automatically restarted on Node 2.
- Once Node 1 is back online, NativeEdge live-migrates the VMs back to their preferred node, maintaining alignment with the HA group’s policy.

This setup guarantees that critical workloads always run on the most optimal infrastructure when available, while still ensuring uptime and continuity during disruptions.

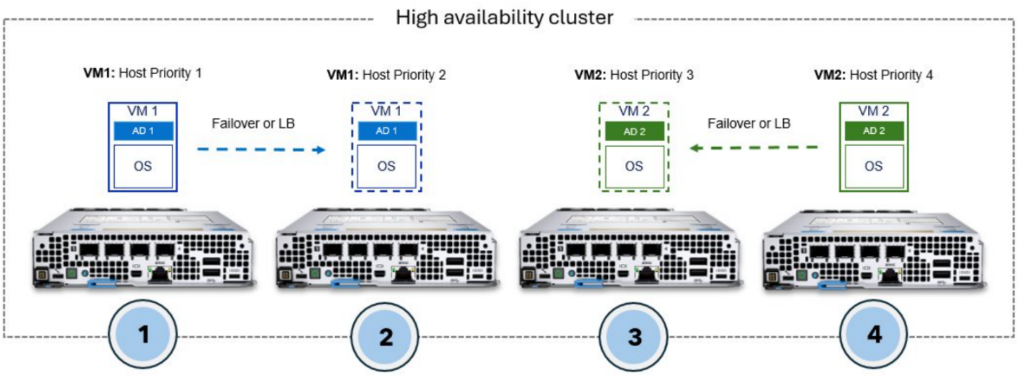


Figure 6. HA groups

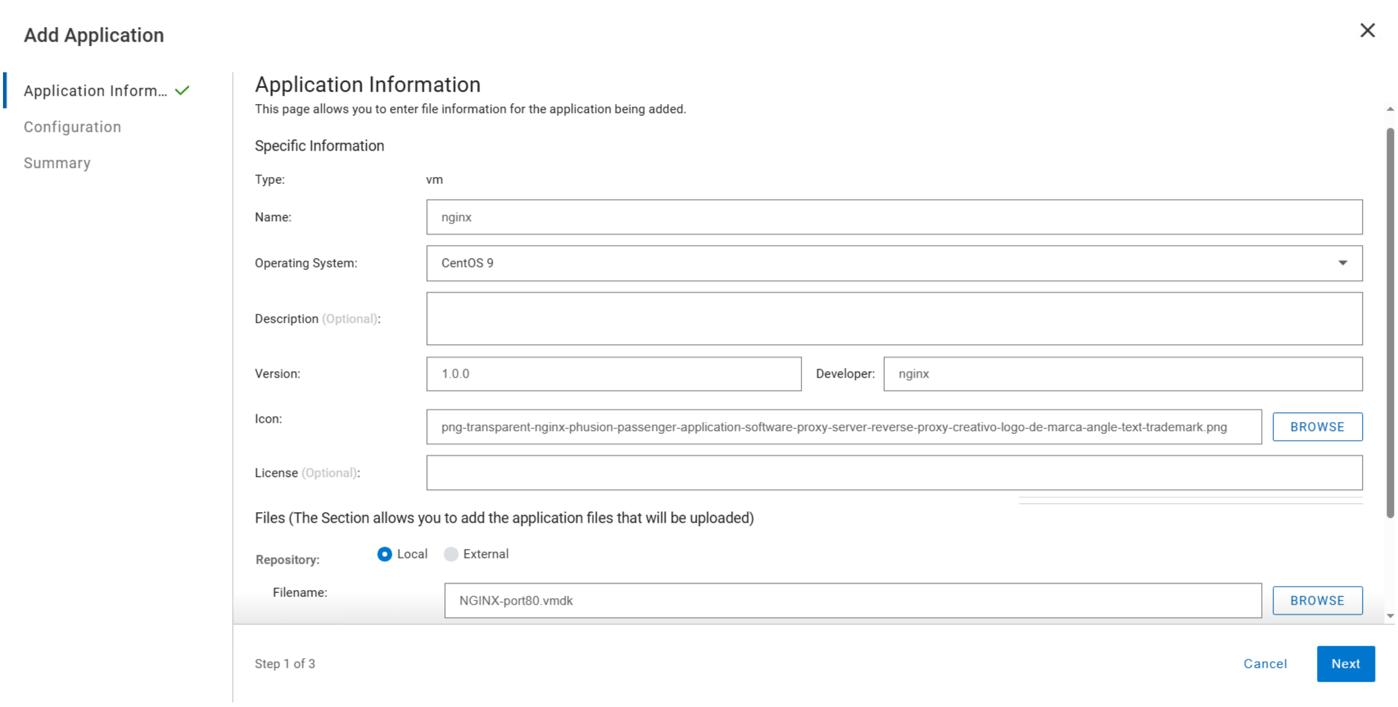
Importing VMs

When transitioning workloads from VMware environments to NativeEdge, Dell provides two streamlined methods to import VMs, each tailored to different use cases and operational scales.

Creating a VM blueprint

Users can import a VMDK file and define the VM's configuration parameters, such as CPU, memory, and networking, within a custom blueprint.

As shown in the following figure, the first method involves importing a VMDK file and using it to create a NativeEdge blueprint. This approach is ideal for single VM use cases, such as development, testing, or proof-of-concept scenarios. Users can export the VMDK from their VMware environment and then upload it into NativeEdge, where they can define the VM's configuration parameters—such as CPU, memory, and networking—within a custom blueprint. This method provides a simple and controlled way to bring individual workloads into the NativeEdge ecosystem.



Add Application

Application Information

This page allows you to enter file information for the application being added.

Specific Information

Type: vm

Name: nginx

Operating System: CentOS 9

Description (Optional):

Version: 1.0.0

Developer: nginx

Icon: png-transparent-nginx-phusion-passenger-application-software-proxy-server-reverse-proxy-creativo-logo-de-marca-angle-text-trademark.png

License (Optional):

Files (The Section allows you to add the application files that will be uploaded)

Repository: ● Local ○ External

Filename: NGINX-port80.vmdk

Step 1 of 3

Figure 7. Virtual machine blueprint

Automated import from vCenter

NativeEdge supports automated importing of VMs from VMware vCenter, allowing for seamless and efficient migration with minimal manual intervention.

About this task

For larger-scale environments, NativeEdge supports automated importing of VMs through integration between NativeEdge and VMware vCenter. By connecting to a vCenter Server, the orchestrator can automatically discover all VMs within the environment. Users can then select multiple VMs for import, specify the target NativeEdge endpoint, choose a datastore, and assign a virtual network segment. Once configured, the import process begins, enabling a seamless and efficient migration of multiple VMs from VMware to NativeEdge with minimal manual intervention.

The import process from VMware to NativeEdge is both flexible and efficient, accommodating a wide range of migration scenarios—from single VM transfers using VMDK files to large-scale, automated imports using vCenter integration. Whether modernizing legacy workloads or consolidating infrastructure, NativeEdge provides the tools and automation that is needed to simplify migration, reduce downtime, and ensure operational continuity. By leveraging the NativeEdge capabilities, organizations can confidently transition their virtual environments into a modern, edge-optimized platform—laying the foundation for improved performance, centralized management, and future scalability.

Consider the following example: An enterprise IT team is modernizing its infrastructure and needs to migrate several legacy Windows Server VMs from a VMware vCenter environment into Dell NativeEdge. These VMs support internal tools and services that are still critical to daily operations but are running on aging hardware and software stacks.

Source environment:

- VMware vCenter Server managing a cluster of ESXi hosts
- Legacy Windows VMs

Target environment:

- Dell Automation Platform orchestrator
- NativeEdge cluster with three endpoints
- Predefined datastores and virtual network segments

The import process is detailed in the following steps.

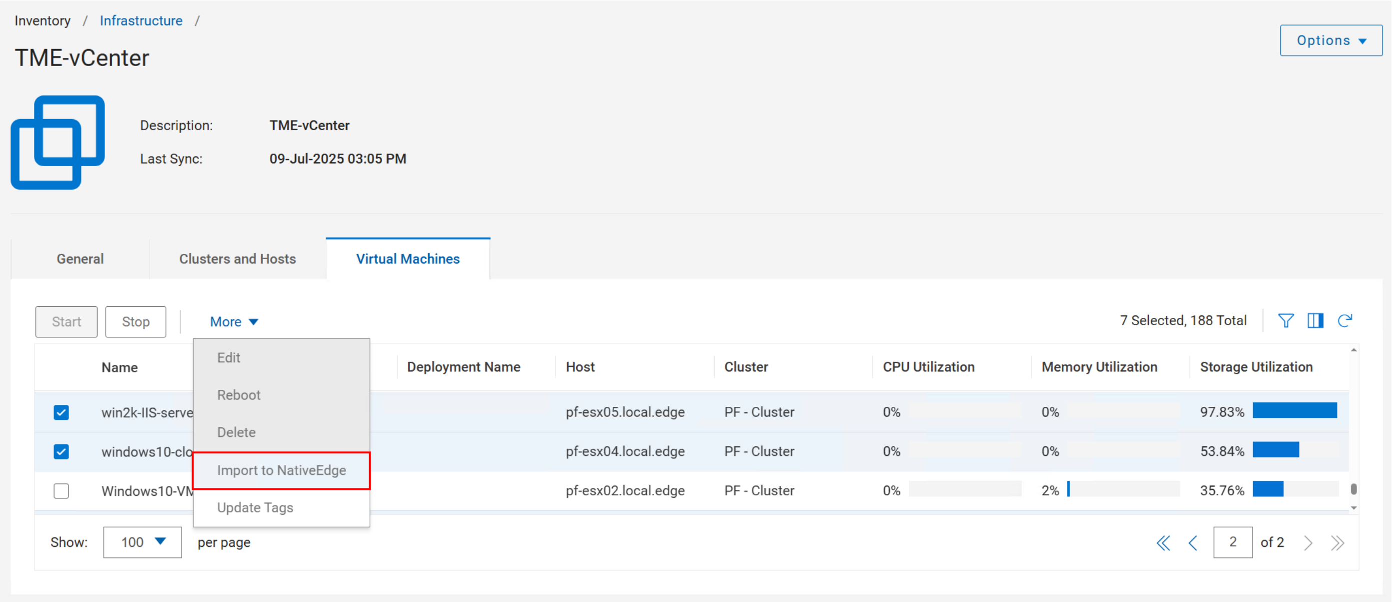
Steps

1. Connect to vCenter.

   The administrator uses the orchestrator to establish a secure connection to the vCenter Server. Once connected, the orchestrator automatically discovers all VMs in the environment.

2. Select VMs for import.

   From the orchestrator interface, the admin selects the three legacy Windows VMs for import.



Description: TME-vCenter

Last Sync: 09-Jul-2025 03:05 PM

	Name	Deployment Name	Host	Cluster	CPU Utilization	Memory Utilization	Storage Utilization
☑	win2k-IIS-serve		pf-esx05.local.edge	PF - Cluster	0%	0%	97.83%
☑	windows10-clo		pf-esx04.local.edge	PF - Cluster	0%	0%	53.84%
□	Windows10-VM		pf-esx02.local.edge	PF - Cluster	0%	2%	35.76%

Figure 8. NativeEdge and VMware vCenter integration

3. Define the import parameters.

   The admin specifies the following:

   - Target NativeEdge cluster or endpoint (based on available capacity)
   - Datastore for VM storage
   - Virtual network segment for connectivity

4. Initiate import.

   With a few clicks, the import process begins. The orchestrator handles the conversion and transfer of VM data, ensuring compatibility with NativeEdge's runtime environment.

5. Post-import validation.

   Once the VMs are imported, the admin verifies that:

   - All services are running as expected.
   - Network configurations are intact.
   - Performance baselines are met.

Upgrades

Cluster-level upgrades in NativeEdge provide a streamlined and resilient approach to updating all nodes or endpoints within a cluster. Rather than upgrading each node manually, the system performs a sequential upgrade, updating one node at a time. This ensures that the cluster remains operational throughout the process, minimizing disruption to workloads.

During the upgrade, each node is automatically placed into maintenance mode. This temporarily blocks new virtual machine deployments and lifecycle management (LCM) operations on that node, ensuring consistency and preventing conflicts during the update. While a node is being upgraded, NativeEdge performs automatic live migration of virtual machines to other healthy nodes in the cluster. This allows workloads to continue running without interruption, maintaining service availability and performance.

By orchestrating upgrades in this controlled and automated manner, NativeEdge ensures that infrastructure remains up to date while preserving uptime and operational continuity across the edge environment.