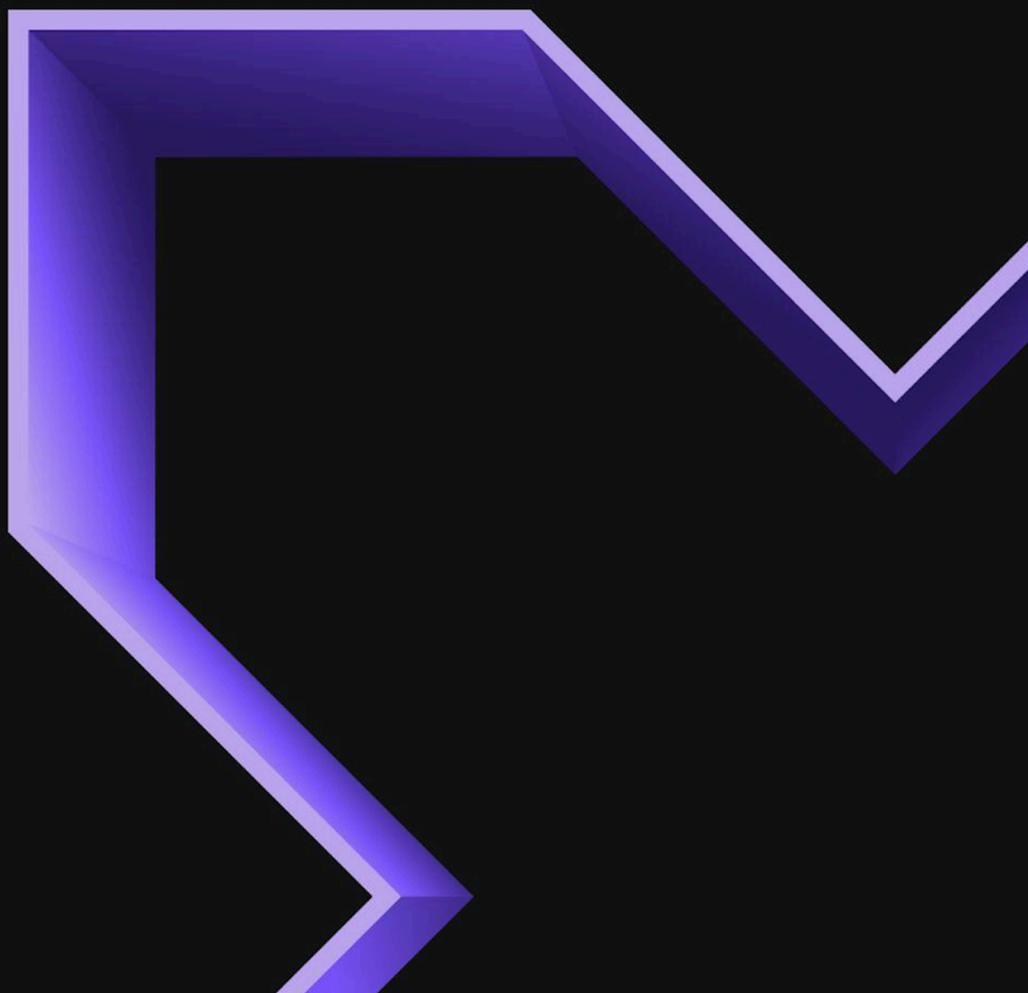
v5.9 | June 2024 | BP-2005

SOLUTIONS DOCUMENT

Data Protection and Disaster Recovery Best Practices



NUTANIX

Legal

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary

The Nutanix Cloud Platform can deliver storage, compute, and virtualization services for any application. Designed for supporting multiple virtualized environments, including Nutanix AHV, VMware ESXi, and Microsoft Hyper-V, Nutanix invisible infrastructure provides many ways to achieve your recovery point objectives (RPOs).

Enterprises are increasingly vulnerable to data loss and downtime during disasters, as they rely on virtualized applications and infrastructure that their legacy data protection and disaster recovery solutions can no longer adequately support. This best practice guide provides the optimal configuration for achieving data protection using the native Nutanix disaster recovery capabilities and the disaster recovery orchestration features available both on-premises, in Nutanix DRaaS, and in public cloud providers like Amazon Web Services (AWS).

Whatever your use case, you can protect your applications with ease. Nutanix Prism facilitates management to configure the shortest recovery time objectives (RTOs) possible, so that you can build complex disaster recovery workflows at a moment's notice. With Prism Central, you can apply protection policies across all your managed clusters. Based on your RPO, you can activate recovery plans to validate, test, migrate, and fail over seamlessly. Recovery plans can protect availability zones both on-premises and hosted in Nutanix DRaaS.

As application requirements change and grow, Nutanix can adapt to business needs. Nutanix is uniquely positioned to protect and operate in environments with minimal administrative effort because of its web-scale architecture and commitment to enterprise cloud operations.

This document provides best practice guidance for implementing data protection solutions on Nutanix servers running AOS 6.5 and covers the following topics:

- Scalable metadata
- Backup
- Crash-consistent versus application-consistent snapshots

- Protection domains
- Protection policies
- Recovery plans
- Scheduling snapshots and asynchronous replication
- Sizing disk space for local snapshots and replication
- Scheduling lightweight snapshots (LWS) and NearSync replication
- Sizing disk space for LWS and NearSync replication
- Determining bandwidth requirements
- File-level restore

Document Version History

Version Number	Published	Notes
1.0	December 2014	Original publication.
2.0	March 2016	Updated best practices throughout.
2.1	June 2016	Updated the Backup and Disaster Recovery on Remote Sites section.
2.2	July 2016	Updated bandwidth sizing information.
2.3	December 2016	Updated for AOS 5.0.
2.4	May 2017	Updated information on sizing SSD space on a remote cluster.
3.0	December 2017	Updated for AOS 5.5.
3.1	September 2018	Updated the Nutanix overview and the Remote Site Setup section.

Version Number	Published	Notes
4.0	December 2018	Updated for AOS 5.10 and Xi Leap.
4.1	February 2019	Updated the Sizing Space section and Leap product details.
4.2	August 2019	Updated for AOS 5.11.
4.3	October 2019	Updated for AOS 5.11.1 and Nutanix Files support for NearSync replication.
5.0	May 2020	Updated for AOS 5.17.
5.1	September 2020	Updated for AOS 5.18.
5.2	December 2020	Updated for AOS 5.19 and Leap multisite replication.
5.3	March 2021	Refreshed content.
5.4	February 2022	Updated the Third-Party Backup Products section.
5.5	May 2022	Updated product names and references to configuration maximums throughout.
5.6	August 2022	Updated the Third-Party Backup Products section.
5.7	October 2023	Removed the PowerShell Scripts section.
5.8	May 2024	Updated the Executive Summary section.
5.9	June 2024	Updated the Disaster Recovery Orchestration and Nutanix VSS Support with Nutanix Guest Tools sections.

2. Web-Scale Data Protection

One of the key architectural differentiators for Nutanix is the ability to scale. Nutanix isn't bound by the same limitations as dual-controller architectures or federations relying on special hardware like NVRAM or custom ASICs for performance. When it comes to snapshots and disaster recovery, scaling metadata is a key part of delivering performance while ensuring availability and reliability. Each Nutanix node is responsible for a subset of the overall platform's metadata. All nodes in the cluster serve and manipulate metadata entirely through software, eliminating traditional bottlenecks.

Because each node has its own virtual storage controller and access to local metadata, replication scales with the system. Every node participates in replication to reduce hotspots throughout the cluster.

Nutanix uses two different forms of snapshots: full snapshots for asynchronous replication (when the RPO is 60 minutes or greater) and lightweight snapshots (LWS) for NearSync replication (when the RPO is between 1 minute and 15 minutes). Full snapshots keep system resource usage low when you use many snapshots over an extended period. The LWS feature reduces metadata management overhead and increases storage performance by decreasing the high number of storage I/O operations that long snapshot chains can cause.

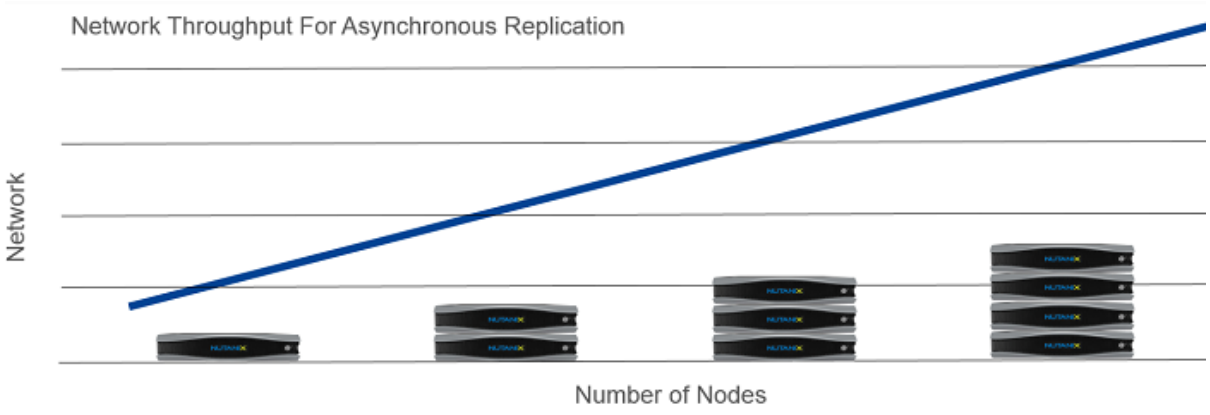


Figure 1: Scalable Replication

In asynchronous replication, every node can replicate four files, up to an aggregate of 100 MBps at one time. Thus, in a four-node configuration, the cluster can replicate 400 MBps or 3.2 Gbps. As you grow the cluster, the virtual storage controllers keep replication traffic distributed. In many-to-one deployments, as when remote branch offices communicate with a main datacenter, the main datacenter can use all its available resources to handle the increased replication load from the branch offices. When the main site is scalable and reliable, administrators don't have multiple replication targets to maintain, monitor, and manage. You can protect both VMs and volume groups with asynchronous replication.

NearSync offers unbound throughput. All writes go to SSD, so to avoid filling the performance tier, AOS automatically allocates 7 percent of it for NearSync. NearSync, which covers both VMs and volume groups, is supported for bidirectional replication between two clusters.

Nutanix also provides cross-hypervisor disaster recovery natively with asynchronous replication. Existing vSphere clusters can target AHV-based clusters as their disaster recovery and backup targets. With VM mobility, you can place your workloads on the platform that best meets their needs.

3. Deployment Overview

Nutanix meets real-world requirements with native backup and replication infrastructure and management features that support a wide variety of enterprise topologies.

Native Nutanix Snapshots

Per-VM or per-volume group snapshots enable instant recovery. Depending on the workload and associated SLAs, you can tune the snapshot schedule and retention periods to meet RPOs. With the intuitive snapshot browser, you can perform restore and cloning operations instantly on the local cluster.

Two-Way Mirroring

The ability to mirror VM and volume group replication between multiple sites is necessary in environments where all sites must support active traffic. Consider a two-site example. Site B is the data protection target for selected workloads running on site A. At the same time, site A serves as the target for designated workloads running on site B. While asynchronous replication is supported for all workflows listed in this section, two-way mirroring is the only supported topology for NearSync.

Figure 2: Two-Way Mirroring

Many-to-One

In many-to-one or hub-and-spoke architectures, you can replicate workloads running on sites A and B to a central site C. Centralizing replication to a single site can improve operational efficiency for geographically dispersed environments. Remote and branch office (ROBO) use cases are a classic many-to-one architecture.

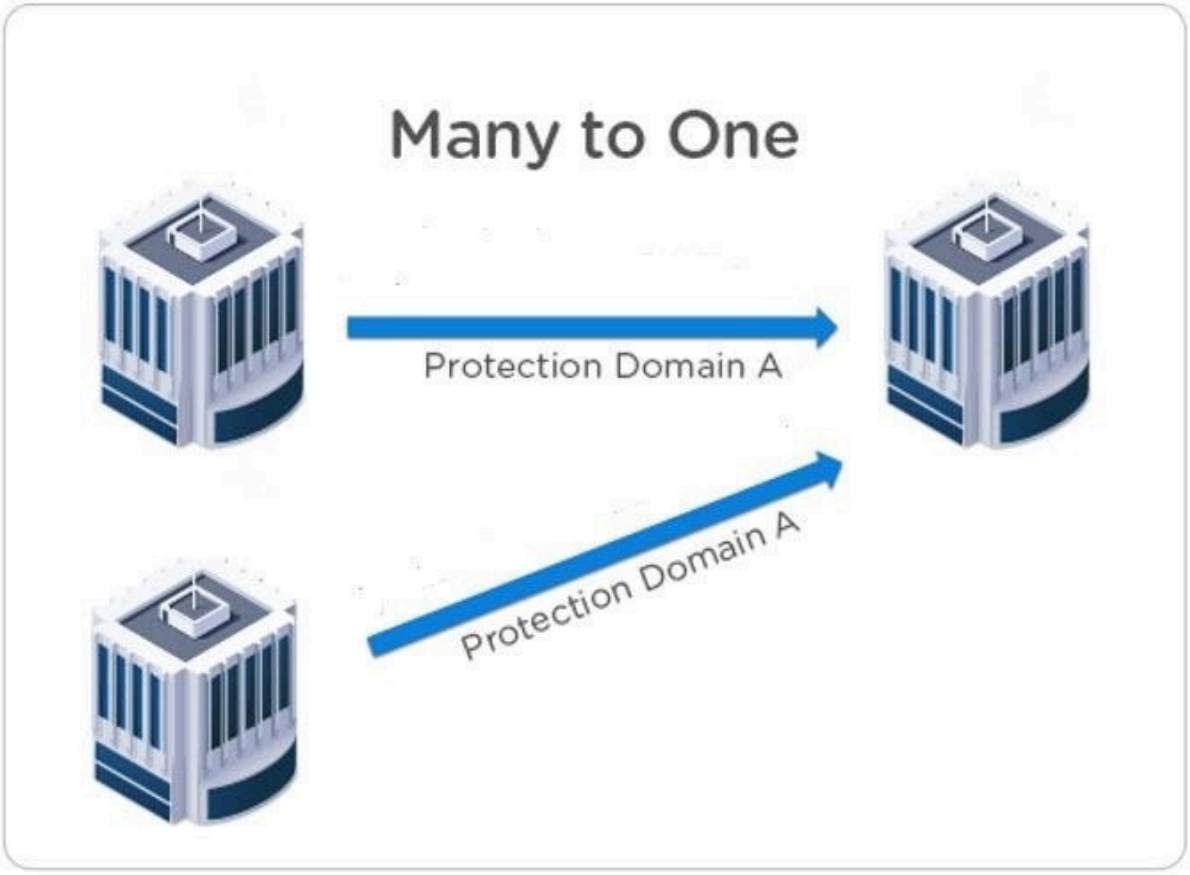


Figure 3: Many-to-One Architecture

To the Cloud

With Cloud Connect, you can use the public cloud as a destination for backing up your on-cluster VMs and volume groups. Currently, Nutanix supports Amazon Web Services (AWS) as the cloud destination. This option is particularly suitable if you don't have an offsite location for backups or are currently relying on tapes for storing backups offsite. Cloud Connect provides you with backup options for both Hyper-V and ESXi using Nutanix Prism. You can also deploy a Nutanix cluster in a public cloud provider like AWS, setting up protection domains and employing the same workflows you use with on-premises clusters.

Figure 4: Public Cloud as a Backup Destination

Single-Node Backup

Nutanix has added support for single-node backup as a cost-efficient solution for providing full native backups. Using the same underlying disaster recovery technology, the single node can be either on-site or remote. Nutanix protects data on the node from single drive failure and provides native backup end to end. Single-node systems can also run VMs for testing or remote branch offices.

Disaster Recovery Orchestration

With Prism Central, you can monitor and manage multiple clusters. Supported AOS versions provide protection policies and recovery plans in Prism Central, offering a way to orchestrate operations around migrations and unplanned failures. You can apply orchestration policies for ESXi and AHV from a central location, ensuring consistency across all your sites and clusters.

To manage these protection policies and recovery plans, Nutanix uses a construct called availability zones. When on-premises, an availability zone includes all the Nutanix clusters managed by one Prism Central instance. An availability zone can also represent a region in Nutanix DRaaS. For disaster recovery, availability zones exist in pairs—either on-premises to on-premises, on-premises to cloud using Nutanix Cloud Clusters, or on-premises to Nutanix DRaaS. Multiple Nutanix DRaaS subscription plans are available, so you don't have to pay the full cost of buying a secondary cluster up front, and you save the time it takes to manage and operate the infrastructure.

4. Local Backup with Snapshots

Nutanix native snapshots provide production-level data protection without sacrificing performance. Nutanix uses a redirect-on-write algorithm to dramatically improve system efficiency for snapshots. Native snapshots operate at the VM level, and our crash-consistent snapshot implementation is the same across hypervisors. Implementation varies for application-consistent snapshots because of differences in the hypervisor layer. Nutanix can create local backups and recover data instantly to meet a wide range of data protection requirements.

Best practices:

- All VM files should sit on Nutanix storage. If you make non-Nutanix storage available to store files (VMDKs), the storage must have the same file path on both the source and destination clusters.
- Remove all external devices, including ISOs and floppy devices.

Crash-Consistent vs. Application-Consistent Snapshots

VM snapshots are by default crash-consistent, which means that the vDisks captured are consistent with a single point in time. The snapshot represents the on-disk data as if the VM crashed or the power cord was pulled from the server—it doesn't include anything that was in memory when the snapshot was taken. Today, most applications can recover well using crash-consistent snapshots.

Application-consistent snapshots capture the same data as crash-consistent snapshots, with the addition of all data in memory and all transactions in process. Because of their extra content, application-consistent snapshots are the most involved and take the longest to perform.

While most organizations find crash-consistent snapshots to be sufficient, Nutanix also supports application-consistent snapshots. The Nutanix application-consistent snapshot uses the Nutanix Volume Shadow Copy Service (VSS) to quiesce the file system for ESXi and AHV before taking the snapshot. You can configure which type of snapshot each protection domain maintains.

Nutanix VSS Support with Nutanix Guest Tools

Nutanix Guest Tools (NGT) plays an important role in application-consistent snapshots. ESXi and AHV-based snapshots call the Nutanix VSS provider from the Nutanix Guest Agent, which is one component of NGT. VMware Tools talk to the guest VM's Nutanix VSS writers. Application-consistent snapshots quiesce all I/O, complete all open transactions, and flush the caches. Nutanix VSS freezes write I/O while the native Nutanix snapshot takes place so that all data and metadata are written consistently. After the snapshot takes place, Nutanix VSS resumes the system and allows queued writes to proceed. Application-consistent snapshots don't snapshot the OS memory during this process.

Requirements for Nutanix VSS snapshots:

- You must have NGT installed.
- An external cluster IP address must be configured.
- Guest VMs must be able to reach the external cluster IP on port 2074.
- The TCP port 23578 in the guest VM must be accessible if you want to use the Nutanix VSS service.
- Guest VMs must have an empty IDE CD-ROM for installing and configuring NGT.
- Guest VMs must use ESXi or AHV.
- Virtual disks must use the SCSI bus type.
- For NearSync support, you must have NGT version 1.3 installed.
- Nutanix VSS isn't supported with NearSync or if the VM has any delta disks (hypervisor snapshots).

- Nutanix VSS snapshots are only available for these supported versions:
  - Windows 7 and later
  - Windows Server 2008 R2 and later
  - CentOS 6.5 and 7.0
  - Red Hat Enterprise Linux (RHEL) 6.5 and 7.0
  - Oracle Linux 6.5 and 7.0
  - SUSE Linux Enterprise Server (SLES) 11 SP4 and 12
- Microsoft VSS must be running on the guest VM (Windows).
- The guest VM must support the use of Nutanix VSS writers.
- Nutanix VSS isn't supported for volume groups.
- You can't include volume groups in a protection domain configured for Metro Availability.
- You can't include volume groups in a protected VStore.
- You can't use Nutanix native snapshots to protect VMs that have VMware fault tolerance enabled.

For ESXi, if NGT isn't installed, the process fails back using VMware Tools. Because the VMware Tools method creates and deletes an ESXi-based snapshot whenever it creates a native Nutanix snapshot, it generates more I/O stress. To eliminate this stress, we strongly recommend installing NGT.

Best practices:

- Schedule application-consistent snapshots during off-peak hours. NGT takes less time to quiesce applications than VMware Tools, but application-consistent snapshots still take longer than crash-consistent snapshots.
- Increase cluster heartbeat settings when using Windows Server Failover Cluster (WSFC).

- To avoid accidental cluster failover when you perform a vMotion, follow VMware best practices to increase heartbeat probes:
  - Change the tolerance of missed heartbeats from the default of 5 to 10. Increase the number to 20 if your servers are on different subnets.
  - If you run Windows Server 2012, adjust the RouteHistoryLength to double the CrossSubnetThreshold value.

Microsoft failover settings adjusted for using Nutanix VSS:

```
(get-cluster).SameSubnetThreshold = 10
(get-cluster).CrossSubnetThreshold = 20
(get-cluster).RouteHistoryLength = 40
```

VSS on Hyper-V

Hyper-V on Nutanix supports VSS only through third-party backup applications, not snapshots. Because the Microsoft VSS framework requires a full share backup for every virtual disk in the share, Nutanix recommends limiting the number of VMs on any container using VSS backup.

Best practices:

- Create different containers for VMs that need VSS backup support. Don't exceed 50 VMs on each container.
- Create a separate large container for crash-consistent VMs.

5. Protection Domains

A protection domain is a group of VMs or volume groups that you can either snapshot locally or replicate to one or more clusters when a remote site is configured. Prism Element uses protection domains when replicating between remote sites.

Best practices:

- Protection domain names must be unique across sites.
- VMware Site Recovery Manager and Metro Availability protection domains are limited to 3,200 files.
- No more than 10 VMs per protection domain with LWS.
- Group VMs with similar RPO requirements.
- NearSync can only have one schedule, so place NearSync VMs in their own protection domain.

For more information on protection domain limits, see the Nutanix Configuration Maximums page.

Consistency Groups

Administrators can create a consistency group for VMs and volume groups that are part of a protection domain and need to be snapshotted in a crash-consistent manner.

Best practices:

- Keep consistency groups as small as possible. Collect dependent applications or service VMs into a consistency group to ensure that they're recovered in a consistent state (for example, put a web server and database in the same consistency group).
- For all hypervisors, try to limit consistency groups to fewer than 10 VMs following these best practices. Although we tested consistency groups with up to 50 VMs, it's more efficient to have smaller consistency groups.

- Each consistency group using application-consistent snapshots can contain only one VM.
- When you provide disaster recovery for VDI using VMware View Composer or Machine Creation Services (MCS), place each protected VM in its own consistency group (including the gold image) inside a single protection domain.

6. Backup and Disaster Recovery on Remote Sites

With Nutanix you can set up remote sites, and you can choose to use those remote sites either for simple backup or for both backup and disaster recovery.

Remote sites are a logical construct. You must configure any AOS cluster—either physical or based in the cloud—as a remote site from the perspective of the source cluster before you use it as the destination for storing snapshots. Similarly, on this secondary cluster, you must configure the primary cluster as a remote site before snapshots from the secondary cluster start replicating to it.

Configuring the backup option on Nutanix allows you to use its remote site as a replication target. This option means you can back up data to this site and retrieve snapshots from it to restore locally, but failover protection (that is, running failover VMs directly from the remote site) isn't enabled. Backup supports using multiple hypervisors; as an example, an enterprise might have ESXi in the main datacenter but use Hyper-V at a remote location. With the backup option configured, the Hyper-V cluster could use storage on the ESXi cluster for backup. Using this method, Nutanix can also back up to AWS from Hyper-V or ESXi.

Configuring the disaster recovery option allows you to use the remote site both as a backup target and as a source for dynamic recovery. In this arrangement, failover VMs can run directly from the remote site. Nutanix provides cross-hypervisor disaster recovery between ESXi and AHV clusters. Currently, Hyper-V clusters can only provide disaster recovery to other Hyper-V-based clusters.

For data replication to succeed, configure forward (DNS A) and reverse (DNS PTR) DNS entries for each ESXi management host on the DNS servers used by the Nutanix cluster.

Remote Site Setup

You can customize several options when you set up a remote site. Protection domains inherit all remote site properties during replication.

Address

Use the external cluster IP as the address for the remote site. The external cluster IP is highly available, as it creates a virtual IP address for all the virtual storage controllers. You can configure the external cluster IP in Nutanix Prism under cluster details.

Other recommendations:

- Try to keep both sites at the same AOS version. If both sites require compression, both must have the compression feature licensed and enabled.
- Open the following ports between both sides:
  - 2009 TCP
  - 2020 TCP
  - 9440 TCP
  - 53 UDP
- If you use the SSH tunnel, also open 22.
- Use the external cluster IP address for the source and destination. Cloud Connect uses a port between 3000—3099, but that setup occurs automatically.
- You must allow all CVM IPs to pass replication traffic between sites with the ports listed previously. To simplify firewall rules, you can use the proxy described in the following section.

Enable Proxy

The enable proxy option redirects all egress remote replication traffic through one node. This remote site proxy is different from the Prism proxy. When you enable the proxy, replication traffic goes to the remote site proxy, which then forwards it to other nodes in the cluster. This arrangement significantly reduces the number of firewall rules you need to set up and maintain.

Best practice: Use the proxy in conjunction with the external address

SSH Tunnel

An SSH tunnel is a point-to-point connection—one node in the primary cluster connects to a node in the remote cluster. By enabling proxy, we force replication traffic to go over

this node pair. You can use the SSH tunnel between Cloud Connect and physical Nutanix clusters when you can't set up a virtual private network (VPN) between the two clusters. We recommend using an SSH tunnel as a fail-back option rather than a VPN.

Best practices:

- To use an SSH tunnel, enable the proxy.
- Open port 22 between external cluster IPs.
- Only use SSH tunnel for testing—not production. Use a VPN between remote sites or a Virtual Private Cloud (VPC) with AWS.

Capabilities

The disaster recovery option requires that both sites either support cross-hypervisor disaster recovery or have the same hypervisor. Today, Nutanix supports only ESXi and AHV for cross-hypervisor disaster recovery with full snapshots. When using the backup option, the sites can use different hypervisors, but you can't restore VMs on the remote side. You also use the backup option when you back up to AWS and Azure.

Bandwidth Throttling

Max bandwidth is set to throttle traffic between sites when no network device can limit replication traffic. With the max bandwidth option, you can set different settings throughout the day and assign a max bandwidth policy when your sites are busy with production data. You can also disable the policy when they aren't as busy. Max bandwidth doesn't imply a maximum observed throughput.

When you talk with your networking teams, note that this setting is in megabytes per second, not megabits per second. NearSync doesn't currently honor maximum bandwidth thresholds.

Remote Container

VStore name mapping identifies the container on the remote cluster used as the replication target. When you establish the VStore mapping, we recommend that you create a new, separate remote container with no VMs running on it on the remote side. This configuration helps the hypervisor administrator recognize the failed-over VMs quickly and apply policies on the remote side easily in case of a failover.

Best practices:

- Create a new remote container as the target for the VStore mapping.
- If you're backing up many clusters to one destination cluster and the source containers have similar advanced settings, use only one destination container.
- Enable MapReduce compression if licensing permits.
- If you use vCenter Server to manage both the primary and remote sites, don't have storage containers with the same name on both sites.

If the aggregate incoming bandwidth required to maintain the current change rate is less than 500 Mbps, we recommend skipping the performance tier. This setting saves your flash for other workloads while also saving on SSD write endurance. To skip the performance tier, use the following command from the nCLI:

```
ncli ctr edit sequential-io-priority-order=DAS-SATA,SSD-SATA,SSD-PCIe
 name=<container-name>
```

You can reverse this command at any time.

Network Mapping

AOS supports network mapping for disaster recovery migrations moving to and from AHV. Whenever you delete or change the network attached to a VM specified in the network map, modify the network map accordingly.

Scheduling Full Snapshots and Asynchronous Replication

Set the snapshot schedule to be equal to your desired RPO. In practical terms, your RPO determines how much data you can afford to lose in the event of a failure. The failure might be due to a hardware malfunction, human error, or environmental issues. Taking a snapshot every 60 minutes for a server that changes infrequently or when you don't need a low RPO takes resources from more critical services.

You set your RPO from the local site. If you set a schedule to take a snapshot every hour, bandwidth and available space at the remote site determine if you can achieve the RPO. In constrained environments, limited bandwidth might cause the replication to take longer than the one-hour RPO, increasing the RPO. This document lists guidelines for sizing bandwidth and capacity to avoid this scenario.

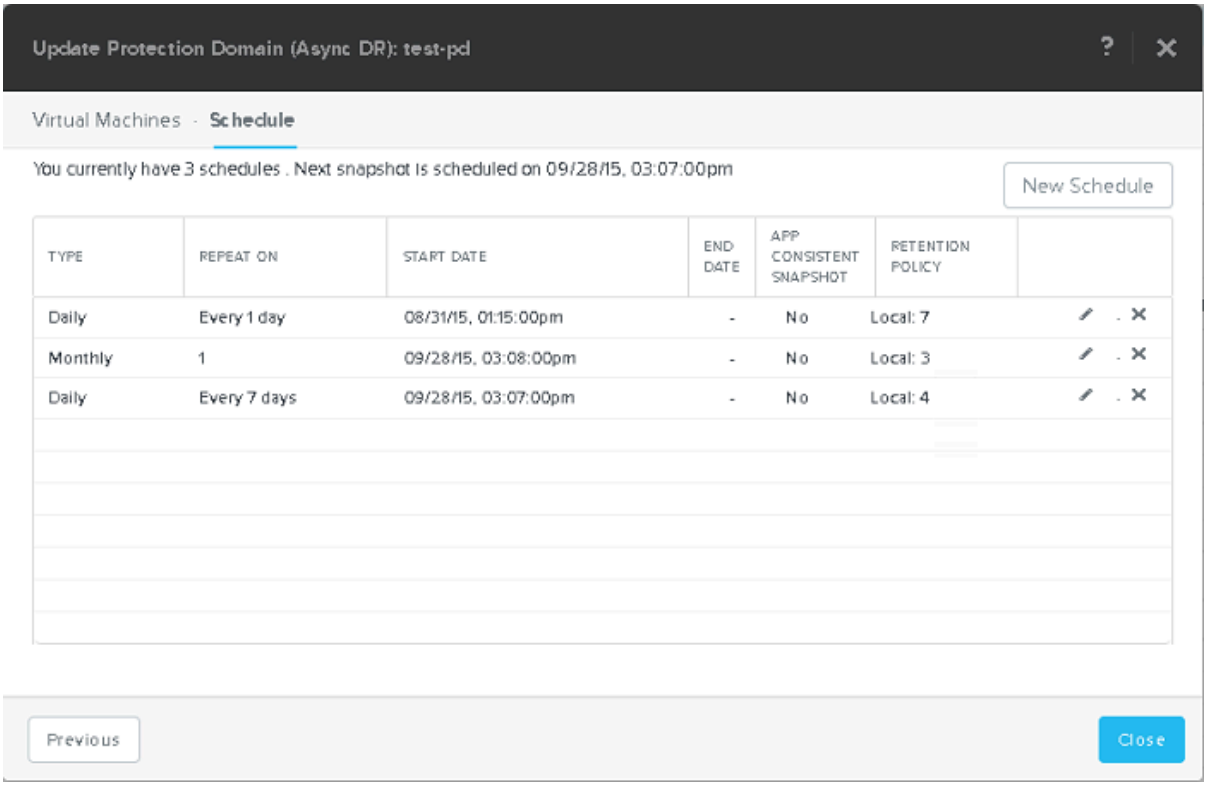


Figure 5: Multiple Schedules for a Production Domain

You can create multiple schedules for a protection domain using full snapshots, and you can have multiple protection domains. The previous figure shows seven daily snapshots, four weekly snapshots, and three monthly snapshots to cover a three-month retention policy. This policy manages metadata on the cluster more efficiently than a daily snapshot with a 180-day retention policy.

Best practices:

- Stagger replication schedules across protection domains. If you have a protection domain starting at the top of the hour, stagger the protection domains by half of the most common RPO. The goal is to spread out replication impact on performance and bandwidth.
- Configure snapshot schedules to retain the lowest number of snapshots while still meeting the retention policy, as shown in the previous figure.

Remote snapshots implicitly expire based on how many snapshots exist and how frequently they are taken. For example, if you take daily snapshots and keep a maximum of five, the first snapshot expires on the sixth day. At that point, you can't recover from the first snapshot because the system deletes it automatically.

In case of a prolonged network outage, Nutanix always retains the last snapshot to ensure that you don't ever lose all the snapshots. You can modify the retention schedule from the nCLI by changing the `min-snap-retention-count` parameter. This value specifies the number of snapshots to retain, even if all the snapshots reach the expiry time. This setting works at the protection-domain level.

Scheduling Lightweight Snapshots and NearSync

Nutanix offers NearSync replication with a telescopic schedule (time-based retention). When you set the RPO between 1 and 15 minutes, you can save your snapshots for n number of weeks or months. Once you select NearSync, you can't add any more schedules.

The following table presents the default telescopic schedule to save recovery points for one month.

Table: Default Telescopic Schedule for One Month

Type	Frequency	Retention
Minute increments	Every minute	15 minutes
Hourly	Every hour	6 hours
Daily	Every 24 hours	7 days
Weekly	Every week	4 weeks
Monthly	Every month	1 month

For more information on the latest requirements and limitations, see Requirements of Data Protection with NearSync Replication.

Limit the number of VMs to 10 or fewer per protection domain. If you can, maintain one VM per protection domain to help you transition back to NearSync if you run out of lightweight snapshots (LWS) reserve storage.

Cross-Hypervisor Disaster Recovery

Nutanix provides cross-hypervisor disaster recovery for migrating between ESXi and AHV clusters. The migration works with one click and uses the Prism data protection workflow. Once you've installed the mobility drivers through NGT, VMs can move freely between the hypervisors.

Best practices:

- Configure the CVM external IP address.
- Obtain the mobility driver from NGT.
- Don't migrate VMs:
  - With delta disks (hypervisor-based snapshots)
  - Using SATA disks
- Ensure that protected VMs have an empty IDE CD-ROM attached.
- Ensure that network mapping is complete.

Single-Node Backup Target

Nutanix offers the ability to use an NX-1155 or NX-1175 appliance as a single-node backup target for an existing Nutanix cluster. Because this target has different resources than the original cluster, its primary use case is to provide backup for a small set of VMs. This utility gives a fully integrated backup option to small and midsize businesses for remote and branch office (ROBO) protection.

Best practices:

- Limit all protection domains combined to fewer than 30 VMs.
- Limit backup retention to a three-month policy. We recommend a policy that includes seven daily, four weekly, and three monthly backups.
- Only map an NX-1155 or NX-1175 to one physical cluster.
- Set the snapshot schedule to at least six hours.
- Turn off deduplication.

Cloud Connect

The CVM running in AWS and Azure has limited SSD space, so we recommend following these best practices when you size:

- Try to limit each protection domain to one VM to speed restore operations. This approach also saves money, as it limits the amount of data going across the WAN.
- The RPO must not be lower than four hours.
- Turn off deduplication.
- Try to use Cloud Connect to protect workloads that have an average change rate of less than 0.5 percent.

7. Disaster Recovery Orchestration

The following best practices for disaster recovery orchestration cover both on-premises environments and Nutanix DRaaS. We've noted any differences between the two.

Required Infrastructure for Disaster Recovery Orchestration

- Deploy Prism Central.
  - › For on-premises environments, deploy two Prism Central instances or one Prism Central instance at a separate site for high availability.
  - › Nutanix Disaster Recovery for ROBO sites only requires one Prism Central, at the main site. When you replicate between two clusters managed from the same Prism Central instance, the minimum RPO is one hour or more and cross-hypervisor disaster recovery isn't supported.
- Deploy Prism Central on a subnet that doesn't fail over.
- Place the CVM and hypervisor IPs on a separate subnet from those used by VMs.
- The test network for on-premises disaster recovery orchestration requires a nonroutable VLAN.

Availability Zones

Paired availability zones synchronize the following disaster recovery configuration entities:

- Protection policies
- Recovery plans
- Categories used in protection policies and recovery plans

Issues (like network connectivity loss between paired availability zones) or user actions (such as unpairing availability zones, and then pairing those availability zones again) can

affect entity synchronization. Pairing previously unpaired availability zones triggers an automatic synchronization event.

If you don't update entities before you resolve a connectivity issue or pair the availability zones again, the synchronization behavior resumes. If you update entities in either or both availability zones before you resolve such issues or pair unpaired availability zones again, you can't synchronize the entities. In such a scenario, you can force the entities in one availability zone to synchronize with the paired availability zone. This forced synchronization overwrites entities at the paired availability zone.

Observe the following recommendations to avoid inconsistencies and the resulting synchronization issues:

- During network connectivity issues, don't update an entity at both availability zones in a pair. You can safely make updates at any one location. After the connectivity issue is resolved, force synchronization from the updated availability zone. Failure to adhere to this recommendation results in synchronization failures.
- You can safely create new entities in either or both availability zones if you don't assign the same name to entities in both availability zones. After you resolve the connectivity issue, force synchronization from the availability zone where you created the entities.
- If one of the availability zones becomes unavailable or if a service in the paired availability zone is down, force synchronization from the paired availability zone after you resolve the issue.

Protection Policies

A protection policy automates the creation and replication of snapshots. When you configure a protection policy for creating local snapshots, you specify the RPO, retention policy, and the entities to protect. To automate snapshot replication to a remote location, you can also specify the remote location. Nutanix Disaster Recovery uses entity-centric disaster recovery.

Requirements for using protection policies:

- A VM can only belong to a protection domain or a protection policy, not both.

- If you don't use Nutanix AHV IPAM and need to retain your IP addresses, you must install NGT on the VMs you want protected.
- You can associate a VM with a maximum of two protection policies.
- When you protect a VM with more than one protection policy, only one of those policies can use NearSync or have Nutanix DRaaS as the target.

Best practices for using protection policies:

- Apply protection policies using categories.
- For VMs that haven't been replicated before, create a container with the same name on both sides. If the VM was in a protection domain before, it continues to use the same container.
- All protection policies that use NearSync must have fewer than 200 VMs.

Cross-Hypervisor Disaster Recovery

AOS supports cross-hypervisor disaster recovery for Nutanix DRaaS for ESXi on-premises. (Because Nutanix DRaaS already runs AHV, AHV on-premises just works.) Cross-hypervisor disaster recovery preserves the following elements of the ESXi configuration on failback when your on-premises environment is healthy again:

- Port group (based on network mapping)
- Virtual hardware version
- Network adapter types
- Disk adapter type
- VMware Tools state
- Amount of vCPU
- Number of cores per vCPU
- Static MAC address
- Disk provisioning (thick or thin)
- OS type

Cross-hypervisor disaster recovery has the following limitations:

- Doesn't preserve SCSI controllers (Nutanix uses LSI logic on failback)
- No support for UEFI boot
- Doesn't preserve vSphere High Availability (HA) and Distributed Resource Scheduler (DRS) settings
- No support for hypervisor-based snapshots, VMware VSS, or linked clones

Recovery Plans

A recovery plan orchestrates restoring protected VMs at a backup location. Recovery plans can either recover all specified VMs at once or, using what is essentially a runbook functionality, use power-on sequences with optionally configurable interstage delays to recover applications gracefully and in the required order. Recovery plans that restore applications in Nutanix DRaaS can also create the required networks during failover and can assign public-facing IP addresses to VMs.

The requirements for recovery plans are as follows:

- To enable disaster recovery orchestration, you must set up a Prism Element external data services IP.
- Prism Central must run on a Nutanix cluster with the external data services IP.

Nutanix DRaaS doesn't allow you to create a recovery plan if you meet either of the following conditions:

- The recovery network that you specify exists with the same name on multiple clusters.
- The networks have the same name but different IP address spaces.

> **Note:** If you add a VM to multiple recovery plans and perform failover simultaneously on those recovery plans, each recovery plan creates an instance of the VM at the recovery location. You must manually clean up the additional instances.

Create your recovery plans based on the following best practices:

- For on-premises availability zones, create a nonroutable network for testing failovers.
- Run the Validate workflow after you make changes to recovery plans.

- After you run the Test workflow, run the Clean-Up workflow instead of manually deleting VMs.
- Keep asynchronous or NearSync replication VMs in separate recovery plans from synchronous replication VMs. Synchronous recovery plans don't support planned failover.

For more information on the configuration maximums for Nutanix Disaster Recovery in multiple scenarios, see Nutanix Configuration Maximums.

Virtual Networks in On-Premises Clusters

Virtual networks in on-premises Nutanix clusters are virtual subnets bound to a single VLAN. At physical locations, including the recovery location, administrators must create these virtual subnets manually, with separate virtual subnets created for production and test purposes. You must create these virtual subnets before you configure recovery plans.

When you configure a recovery plan, map the virtual subnets at the source location to the virtual subnets at the recovery location.

Virtual Networks in Nutanix DRaaS

Nutanix DRaaS features two built-in virtual networks: Production and Test. These virtual networks aren't analogous to the virtual subnets used in on-premises Nutanix clusters; they only provide two separate IP address spaces for production and testing so that activities performed in one do not affect the other. These separate Production and Test IP address spaces contain virtual subnets that are analogous to the virtual subnets in on-premises Nutanix clusters.

The Production virtual network contains subnets used for production workloads. These production workloads can be either workloads created and maintained in Nutanix DRaaS or workloads that have failed over from a paired physical location.

The Test virtual network contains the subnets to recover VMs to when you test failover from the virtual subnets at a paired physical location. When you configure a recovery plan, map the virtual subnets on your on-premises clusters to virtual subnets in the Production and Test networks in Nutanix DRaaS.

Best practices:

- Set up administrative distances on VLANs for subnets that completely fail over. If you don't set up administrative distances, shut down the VLAN on the source side after failover if the VPN connection is maintained between the two sites. If you're failing over to a new subnet, set up the subnet beforehand so that you can test the routing.
- The prefix length for network mappings must be the same at the source and the destination.
- If you don't use Nutanix IPAM, you must install NGT to maintain a static address.
- To maintain a static address for Linux VMs that don't use Nutanix IPAM, the VMs must have the NetworkManager command-line tool (nmcli) version 0.9.10.0 or later installed. Additionally, you must use NetworkManager to manage the network for the Linux VMs. To enable NetworkManager on a Linux VM, set the value of the `NM_CONTROLLED` field to `yes` in the interface configuration file (for example, in CentOS, the file is `/etc/sysconfig/network-scripts/ifcfg-eth0`). After you set this field, restart the network service on the VM.

For networking best practices specific to Nutanix DRaaS, see the Nutanix DRaaS Connectivity Tech Note.

Nutanix DRaaS Hypervisor Support

Nutanix DRaaS supports clusters running AHV or ESXi as the source.

Nutanix DRaaS VM Configuration Limitations

VMs with the following configurations can't start:

- VMs configured with a GPU resource.
- VMs configured with four vNUMA sockets.

8. Sizing Space

This section provides storage sizing guidance for the following snapshot configurations:

- Full local snapshots
- Asynchonous replication
- Lightweight snapshots (LWS)
- NearSync replication

Full Local Snapshots

To size space for local snapshots, you need to account for the rate of change in your environment and how long you plan to keep your snapshots on the cluster. Reduced snapshot frequency might increase the rate of change because common blocks are more likely to change before the next snapshot.

As you lower the RPO for asynchronous replication, you might need to account for an increased rate of transformed garbage, which is space that was allocated for I/O optimization or space that was assigned but the metadata no longer refers to.

To find the space needed to meet your RPO, you can use the following formula:

```
snapshot reserve = (frequency of snapshots × change rate per frequency) +
(change rate per frequency × # of snapshots in a full curator scan × 0.1)
```

A full curator scan runs every six hours. You can compare the incremental differences between your backups to find the change rate. You can also take a conservative approach and start with a low snapshot frequency and a short expiry policy, then gauge the size difference between backups before consuming too much space.

To demonstrate using the local snapshot reserve formula, we assume that the change rate is 35 GB of data every six hours and that we keep ten snapshots:

```
snapshot reserve = (frequency of snapshots × change rate per frequency) +
(change rate per frequency × # of snapshots in a full curator scan × 0.1)
= (10 × 35,980 MiB) + (35,980 MiB × 1 × 0.1)
= 359,800 + (35,980 × 1 × 0.1)
= 359,800 + 3,598
= 363,398 MiB
```



```
= 363 GiB
```

Asynchronous Replication

Asynchronous replication uses the same process, but you must include the first full copy of the protection domain plus delta changes based on the set schedule.

Remote snapshot reserve formula:

```
snapshot reserve = (frequency of snapshots × change rate per frequency) +
(change rate per frequency × # of snapshots in a full curator scan × 0.2)
+ total size of the source protection domain
```

For the minimum amount of space needed at the remote side, 130 percent of the protection domain is a good average to work from.

If the remote target also runs a workload, incoming replication uses the performance tier. If you use a hybrid cluster, size for the additional hot data. You can also skip the performance tier by creating a separate container for incoming replication and following the steps in the Remote Container section.

Lightweight Snapshots

Sizing for LWS is similar to sizing for full snapshots in that you must account for change rate and retention time. During the LWS retention time, you don't have to size for transformed garbage space, but LWS does use additional SSD space that you must size for. By default, 7 percent of each node's SSD space forms the LWS reserve, which is an additional factor.

Duplicating the workload from the full snapshot example, let's change the RPO to one minute. LWS data exists for 75 minutes plus one extra snapshot based on the RPO value. Because the frequency rate in this scenario is high, it's very important to account for overwrites in the change rate. Because all data goes through the oplog, it's compressed; the type and amount of compression varies by workload. Using inline compression, we typically see a 2:1 compression rate.

Example Using 35 GB Change Rate Over Six Hours

If your change rate is 35 GB of data every six hours, add 5 GB to account for overwrites. 40 GB every six hours has a change rate of approximately 114 MB per minute. If the cluster is running with replication factor 2, you must account for the total physical space.

LWS reserve:

```
= (frequency of snapshots × change rate per frequency) × oplog compression ×
 replication factor
= (75 × 114 MB per minute) × 0.50 × 2
= 8,550 MB
= 8.6 GB
```

If you run a 3460 hybrid system with two 1.9 TB SSDs, the following calculation shows your cluster LWS reserve:

```
= ((total SSD capacity per node – (CVM + metadata + oplog + cache overhead))
 × number of nodes) × LWS reserve percentage
= (3,539 GiB – (120 GiB + 30 GiB + 200 GiB + 40 GiB)) × 4 × 0.07
= 3,149 GB × 4 × 0.07
= 881.72 GiB
= ~945 GB
```

Apply the 7 percent of the SSD space used by the extent store after you account for the rest of the system. Because the LWS cluster reserve is 945 GB, this system has room for the workload and additional business-critical applications.

As mentioned in the Scheduling Lightweight Snapshots and NearSync section, a telescopic schedule has a total of six hourly, seven daily, four weekly, and one monthly snapshots. You only need to account for additional garbage space for the daily snapshots because of the higher frequency. Using the change rate above, you can calculate each separate schedule and add them all together. Because full snapshots occur less often than LWS, you don't have to be concerned with overwrites and can use the original 35 GB change rate for every six hours.

Example of a Telescopic NearSync Snapshot Schedule

```
Hourly change rate: 5,833 MB
Daily change rate: 140,000 MB
Weekly change rate: 980,000 MB
Monthly change rate: 3,920,000 MB

snapshot overall capacity reserve = (hourly schedule + daily schedule +
 weekly schedule + monthly schedule)

For the hourly schedule:
(frequency of snapshots × change rate per frequency) + (change rate per
 frequency × # of snapshots in a full curator scan × 0.1)

The remaining schedules:
= (frequency of snapshots × change rate per frequency)
snapshot overall capacity reserve = ((6 × 5,833)+(5,833 × 6 × 0.1)) + (7 ×
 140,000) + (4 × 980,000) + (2 × 3,920,000)
= 34,998 + 3,500 + 980,000 + 3,920,000 + 8,257,538
= 13,196,036 MB
= ~13 TB
```


For most small and medium businesses, a daily change of 140 GB is considered high. This NearSync example highlights the difference between keeping a lot of snapshots around and keeping only the 10 snapshots in the full snapshot example.

NearSync

NearSync uses the same process as the snapshot process outlined previously, but you must include the first full copy of the protection domain and delta changes based on the set schedule.

For the minimum amount of space needed at the remote site, start with 130 percent of the protection domain plus the required LWS reserve space.

Best practices:

- Use drives with the same or greater capacity at the remote site compared to those in your primary cluster to ensure enough LWS reserve space.
- Don't enable deduplication on the source container for NearSync.

9. Bandwidth

You must have enough available bandwidth to keep up with the replication schedule. If you're still replicating when the next snapshot is scheduled, the current replication job finishes first. The newest outstanding snapshot then starts to get the newest data to the remote side first. To help replication run faster when you have limited bandwidth, you can seed data on a secondary cluster at the primary site before shipping that cluster to the remote site.

Seeding

To seed data for a new site:

1. Set up a secondary cluster with local IPs at the primary site.
2. Enable compression on the remote site in the production domain.
3. Set the initial retention time to 3 months.
4. Reconfigure the secondary cluster with remote IPs.
5. Turn off the secondary cluster.
6. Ship the secondary cluster to the remote site.
7. Turn on the remote cluster.
8. Update the remote site on the primary cluster to the new IP.

If you can't seed the protection domain at the local site, you can create the remote cluster as a normal install and turn on compression over the wire. Manually create a one-time replication with retention time set to three months. We recommend this retention time setting because of the extra time it takes to replicate the first data set across the wire.

To figure out how much throughput you need, you must know your RPO. If you set the RPO to one hour, you must be able to replicate the changes within that time.

Assuming you know your change rate based on incremental backups or local snapshots, you can calculate the bandwidth needed. The next example uses a change rate of 15 GB and an RPO of one hour. We don't use deduplication in the calculation, partly so the dedupe savings can serve as a buffer in the overall calculation and because the one-time cost for deduped data going over the wire has less impact once the data is present at the

remote site. We assume an average of 30 percent bandwidth savings for compression on the wire.

Bandwidth sizing:

```
Bandwidth needed = (RPO change rate × (1 – compression on wire savings %)) /
 RPO

Example:
(15 GB × (1 - 0.3)) / 3,600 sec
(15 GB × 0.7) / 3,600 sec
10.5 GB / 3,600 sec
(10.5 × 1,000 MB) / 3,600 sec (changing to MBps)
(10,500 MB) / 3,600 sec
10,500 MB / 3,600 = 2.92 MBps
Bandwidth needed = 23.33 Mbps
```

If you keep missing your replication schedule, either increase your bandwidth or your RPO. For more RPO flexibility, you can run different schedules on the same production domain; for example, have one daily replication schedule and create a separate schedule to take local snapshots every two hours.

10. Failover: Migrate vs. Activate

Nutanix offers two options for handling VMs and volume groups during failover: migrate and activate.

Use the migrate option when you know that both the production site and the remote site are healthy. This option is only available on the active production site. Migrate shuts down the VM or volume group, takes another snapshot, and replicates the VM or volume group to the selected remote site.

The activate option for restoring a VM is only available on the remote site. When you select activate, the system uses the last snapshot on the remote side to bring up the VM, regardless of whether the active production site is healthy. You can't sync any outstanding changes to the VM from the production site.

If you activate a protection domain because the primary site is down but the primary site comes back up after the failover, you can have a split-brain scenario. To resolve this situation, deactivate the protection domain on the former primary site. The following command is hidden from the nCLI because it deletes the VMs, but it resolves the split while keeping the existing snapshots:

```
ncli> pd deactivate_and_destroy_vms name=<protection_Domain_Name>
```

You can test a VM at the remote site without breaking replication using the restore or clone functionality.

Use the local snapshot browser on the inactive production domain at the remote site, and choose the restore option to clone a VM to the datastore. Add a prefix to the VM's path.

Best practices:

- When you activate protection domains on the remote site, use intelligent placement for Hyper-V and DRS for ESXi clusters. Intelligent placement evenly spreads out the VMs on startup during a failover. AOS powers on VMs uniformly at start time.
- Install NGT on machines using volume groups.
- Configure the data services cluster IP on the remote cluster.

Protection Domain Cleanup

Because inactive protection domains still consume space in existing snapshots, you should remove any unused protection domains to reclaim that space.

To remove a protection domain from a cluster, follow these steps:

1. Remove existing schedules.
2. Remove both local and remote snapshots.
3. Remove the VMs from the active protection domain.
4. Delete the protection domain.

11. Self-Service File Restore

Self-service file restore is available for ESXi and AHV. The goal is to offer self-service file-level restore with minimal support from infrastructure administrators. Once you install NGT, you can open a web browser and go to `http://localhost:5000` to browse snapshots sorted by today, last week, last month, and user-defined criteria. Self-service works with both protection domains and Nutanix Disaster Recovery.

- Guest VMs must use:
  - Windows 2008, Windows 7, or later
  - Centos 6.5 or later and 7.0 or later
  - Red Hat 6.5 or later and 7.0 or later
  - OEL 6.5 or later
  - SLES 11 or later
- Install VMware Tools.
- Remove JRE 1.8 or later if installed with a previous release.
- Configure a cluster external IP address.
- Add the VM to a protection domain.
- Use the default disk.EnableUUID = true for the VM in advanced settings for ESXi.
- The VM must have an IDE-based CD-ROM configured for installation. On newer versions of ESXi, a SATA-based CD-ROM is added by default.
- Detach the mounted disk after you restore your files.

Limitation: For Linux VMs, logical volumes spanning multiple disks aren't supported.

12. Third-Party Backup Products

Nutanix provides its own hypervisor-agnostic, changed-region tracking API that vendors can access using a REST API. Currently, Cohesity, Commvault, Druva, HYCU, and Rubrik provide backup support specifically for AHV. Nutanix systems can integrate with any backup vendor that supports vStorage APIs for Data Protection for ESXi. Nutanix also offers a VSS provider for Hyper-V backup software vendors. For more information on certified third-party solutions, see the Nutanix Elevate Technology Alliance Partner Program page.

Backups with Replication

Hypervisor-based snapshots left on the VM when you take a hardware-based snapshot might cause the recovery to fail. You must manually turn on the VM. For more information, see VMware KB 1025279.

Backup software interacting with AHV uses scoped production domains, also known as backup snapshots. When the backup software requests a snapshot of a VM that isn't protected under any user-created production domain, temporarily protect the VM by placing it in a scoped production domain. Issue a snapshot of this production domain, then remove the VM from the production domain. With backup snapshots, you can also back up VMs and use disaster recovery orchestration. The only possible issue is that while the snapshot operation on the scoped production domain is in progress, the user-initiated VM protection might fail in the regular production domain.

Best practices:

- Avoid using hypervisor-based snapshots.
- Try to schedule hypervisor snapshots or user-created, hardware-based snapshots at times outside of the backup window.

For optimization and scaling recommendations for third-party backup solutions, see the best practice guides on an enhanced disk-to-disk backup architecture on the Nutanix Support Portal.

13. Conclusion

Nutanix offers granular data protection based on your required recovery point objectives across many different deployment models. As your application requirements change and your cluster grows, you can add and remove VMs from protection domains. Sizing capacity and bandwidth are key to achieving optimal data protection and maintaining cluster health. Snapshot frequency and the daily change rate affect the capacity and bandwidth needed between sites to meet the needs of the business.

With data protection features that are purpose-built, fully integrated, and completely software-defined, Nutanix provides the adaptability and flexibility for meeting your enterprise's backup and recovery needs.

14. Appendix

The following sections provide high-level best practices for backup and disaster recovery on Nutanix.

General Best Practices

- Store all VM files on Nutanix storage. If non-Nutanix storage stores files externally, it should have the same file path on both sides.
- Remove all external devices, including ISOs or floppy devices.

Nutanix Native VSS Snapshots

- Configure an external cluster IP address.
- Guest VMs must be able to reach the external cluster IP on port 2074.
- Guest VMs must have an empty IDE CD-ROM for attaching NGT.
- Guest VMs must use ESXi or AHV.
- Virtual disks must use the SCSI bus type.
- VSS must be running in the guest VM.
- The guest VM needs to support the use of VSS writers.
- Schedule application-consistent snapshots during off-peak hours or ensure that additional I/O performance is available. If you take a VSS snapshot during peak usage, the delta disk from the hypervisor-based snapshot might become large. When you delete the hypervisor-based snapshot, collapsing it takes additional I/O; account for this additional I/O to avoid affecting performance.

Hyper-V VSS Provider

- VSS support is only for backup.

- Create different containers for VMs that need VSS backup support. Limit the number of VMs on each container to 50.
- Create a separate large container for crash-consistent VMs.

Protection Domains

- Protection domain names must be unique across sites.
- Group VMs with similar RPO requirements.
- For current limits, see the Nutanix Configuration Maximums page.
- VMware Site Recovery Manager and Metro Availability protection domains are limited to 50 VMs.
- Linked clone VMs (typically nonpersistent View desktops) aren't supported with NearSync.
- Remove unused protection domains to reclaim space.
- If you must activate a protection domain rather than migrate it, deactivate the old primary protection domain when the site comes back up.

Consistency Groups

- Keep consistency groups as small as possible. Keep dependent applications or service VMs in one consistency group to ensure that they are recovered in a consistent state (for example, App and DB).
- Each consistency group using application-consistent snapshots can contain only one VM.

Disaster Recovery and Backup

- Ensure that you configure forward (DNS A) and reverse (DNS PTR) DNS entries for each ESXi management host on the DNS servers used by the Nutanix cluster.

Remote Sites

- Use the external cluster IP as the address for the remote site.
- Use disaster recovery proxy to limit firewall rules.
- Use max bandwidth to limit replication traffic.
- When activating protection domains, use intelligent placement for Hyper-V and DRS for ESXi clusters on the remote site. Intelligent placement evenly spreads out the VMs at start time during a failover. AOS starts VMs uniformly at start time.
- If you use vCenter Server to manage both the primary and remote sites, don't use storage containers with the same name on both sites.

Remote Containers

- Create a new remote container as the target for the VStore mapping.
- When you back up many clusters to one destination cluster, use only one destination container if the source containers have similar advanced settings.
- Enable MapReduce compression if licensing permits.
- If the aggregate incoming bandwidth required to maintain the current change rate is less than 500 Mbps, we recommend skipping the performance tier to save flash capacity and increase device longevity.

Network Mapping

- Whenever you delete or change the network attached to a VM specified in the network map, modify the network map accordingly.

Scheduling

- To spread out replication impact on performance and bandwidth, stagger replication schedules across protection domains. If you have a protection domain starting at the top of the hour, stagger the protection domains by half of the most common RPO.

- Configure snapshot schedules to retain the smallest number of snapshots while still meeting the retention policy.
- Metro and SRM-protected containers aren't supported.
- Deduplication on the source container isn't currently supported for NearSync.

Cross-Hypervisor Disaster Recovery

- Configure the CVM external IP address.
- Obtain the mobility driver from NGT.
- Don't migrate VMs with delta disks (hypervisor-based snapshots), using SATA disks, or using volume groups.
- Ensure that protected VMs have an empty IDE CD-ROM attached.
- Ensure that network mapping is complete.

Disaster Recovery Orchestration

- Deploy Prism Central to each on-premises site.
- Deploy Prism Central on a subnet that doesn't fail over.
- Place CVM and hypervisor IPs on a separate subnet from the subnets used by VMs.
- On-premises disaster recovery orchestration requires a nonroutable VLAN for the test network.

Availability Zones

- If one of the availability zones becomes unavailable or if a service in the paired availability zone is down, resolve the issue and then force synchronization from the paired availability zone.

Protection Policies

- A VM can only belong to a protection domain or a protection policy, not both.

- If you don't use Nutanix AHV IPAM and need to retain your IP addresses, install NGT on the VMs to be protected.
- Use categories to apply protection policies.
- For Nutanix Disaster Recovery on-premises, create the same container name on both sides. If the container name doesn't match on both sides, data replicates by default to the SelfServiceContainer.

Cross-Hypervisor Support with ESXi for Protection Policies

- No support for UEFI boot
- Doesn't preserve vSphere HA and DRS settings
- No support for hypervisor-based snapshots, VMware VSS, or linked clones

Recovery Plans

- For on-premises availability zones, create a nonroutable network for testing failovers.
- Run the Validate workflow after making changes to recovery plans.
- After you run the Test workflow, run the Clean-Up workflow instead of manually deleting VMs.
- For the current limits, see Nutanix Configuration Maximums.

Network Mapping

- Set up administrative distances on VLANs for subnets that completely fail over. If you don't set up administrative distances, shut down the VLAN on the source side after failover if the VPN connection is maintained between the two sites. If you're failing over to a new subnet, set up the subnet beforehand so you can test the routing.
- The prefix length for network mappings at the source and the destination must be the same.
- If you don't use Nutanix IPAM, you must install the NGT software package to maintain a static address.

- To maintain a static address for Linux VMs that don't use Nutanix IPAM, the VMs must have the NetworkManager command-line tool (nmcli) version 0.9.10.0 or later installed. Additionally, you must use NetworkManager to manage the network for the Linux VMs. To enable NetworkManager on a Linux VM, set the value of the NM_CONTROLLED field to `yes` in the interface configuration file (for example, in CentOS, the file is `/etc/sysconfig/network-scripts/ifcfg-eth0`). After you set the field, restart the network service on the VM.

Nutanix DRaaS Hypervisor Support

- Nutanix DRaaS only supports clusters running AHV.

Nutanix DRaaS VM Configuration Restrictions

- Can't power on VMs configured with a GPU resource.
- Can't power on VMs configured with four vNUMA sockets.

Single-Node Backup

- Limit all protection domains combined to fewer than 30 VMs.
- Limit backup retention to a three-month policy. We recommended seven daily, four weekly, and three monthly backups.
- Only map an NX-1155 to one physical cluster.
- Snapshot schedule must be at least six hours.
- Turn off deduplication.

Cloud Connect

- Try to limit each protection domain to one VM to speed up restores. This approach also saves money, as it limits the amount of data going across the WAN.
- The RPO shouldn't be lower than four hours.
- Turn off deduplication.

- Try to use Cloud Connect to protect workloads that have an average change rate of less than 0.5 percent.

Sizing

- Size local and remote snapshot storage using the application's change rate.
- Remember to either size the performance tier for hybrid clusters to accommodate incoming data or bypass the performance tier and write directly to disk.

Bandwidth

- Seed locally for replication if WAN bandwidth is limited.
- Set a high initial retention time for the first replication when you seed.

File-Level Restore

- Guest VMs must use:
  - Windows 2008, Windows 7, or later
  - Centos 6.5 or later and 7.0 or later
  - Red Hat 6.5 or later and 7.0 or later
  - OEL 6.5 or later
  - SLES 11 or later
- Install VMware tools.
- Install JRE 1.8 or later.
- Configure a cluster external IP address.
- Add the VM to a protection domain.
- Use the default `disk.EnableUUID = true` for the VM in advanced settings.
- The VM must have a CD-ROM configured.

- Detach the mounted disk after restoring your files.

About Nutanix

Nutanix offers a single platform to run all your apps and data across multiple clouds while simplifying operations and reducing complexity. Trusted by companies worldwide, Nutanix powers hybrid multicloud environments efficiently and cost effectively. This enables companies to focus on successful business outcomes and new innovations. Learn more at Nutanix.com.

List of Figures