



Deploy Nutanix with ONTAP storage

NetApp virtualization solutions

NetApp
October 28, 2026

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions-virtualization/nutanix/nutanix-connectivity.html> on October 28, 2026. Always check docs.netapp.com for the latest.

Table of Contents

- Deploy Nutanix with ONTAP storage 1
 - Prepare to deploy Nutanix Cloud Platform with ONTAP storage 1
 - Prerequisites 1
 - Network architecture 2
 - High-level deployment steps 3
 - Deploy a Nutanix compute cluster with ONTAP storage 4
 - Configure ONTAP volumes, export policies, and permissions for Nutanix 7
 - Create ONTAP FlexVol volumes 7
 - Configure ONTAP export policies 8
 - Configure ONTAP roles and permissions 9

Deploy Nutanix with ONTAP storage

Prepare to deploy Nutanix Cloud Platform with ONTAP storage

Review the prerequisites and the recommended network architecture for connecting Nutanix AHV compute-only hosts to ONTAP storage. This design lets you expand storage capacity and performance independently of compute, eliminating the need to add Nutanix nodes solely for storage growth.

The design uses dedicated storage networking between Nutanix AHV compute-only hosts and ONTAP storage controllers. Storage traffic is isolated from management and application traffic through a dedicated virtual switch (vswitch1) and external storage VLAN. ONTAP provides NFSv3 storage services through dedicated SVM data LIFs, while SVM management LIFs are used with the REST APIs for storage administration and integration.

For resiliency and performance, Nutanix compute-only hosts and ONTAP controllers use LACP (active/active) across redundant network paths. If LACP is unavailable, active/active with MAC pinning provides load balancing at the virtual switch layer. Storage traffic should reside on a dedicated non-routed VLAN, while management, live migration, disaster recovery replication, and application traffic continue to use the standard routed network.

Prerequisites

Before you integrate ONTAP storage with Nutanix Cloud Infrastructure, ensure that the following requirements are met.

Nutanix cluster

A Nutanix cluster running AHV is deployed and operational, and meets the following requirements:

- A minimum of three nodes.
- Compute nodes meet the Nutanix minimum requirements for CPU, memory, networking, and boot devices. For detailed information, see [Minimum Compute Requirements](#).
- Hardware and software are listed in the applicable Nutanix compatibility matrices. See [Compatibility and Interoperability Matrix for Compute Platforms](#).

NetApp ONTAP storage

NetApp ONTAP storage is deployed and configured with NFS services enabled, and meets the following requirements:

- Supported ONTAP platforms: AFF A-Series (all-flash), AFF C-Series (all-flash), and FAS (hybrid flash).
- ONTAP runs a supported release: 9.15.1P18 or later, 9.16.1P16 or later, 9.17.1P8 or later, 9.18.1P4 or later, or 9.19.1P2 or later.
- ONTAP One licensing.
- An ONTAP storage virtual machine (SVM) is configured to serve storage to the Nutanix compute cluster.
- One or more FlexVol volumes are exported as NFS shares. The Nutanix cluster mounts the NFS exports and presents them as shared storage for workloads.

- NetApp strongly recommends using an interface group as the home port for the NFS LIF. For more information, see [Combine physical ports to create ONTAP interface groups](#).

Networking

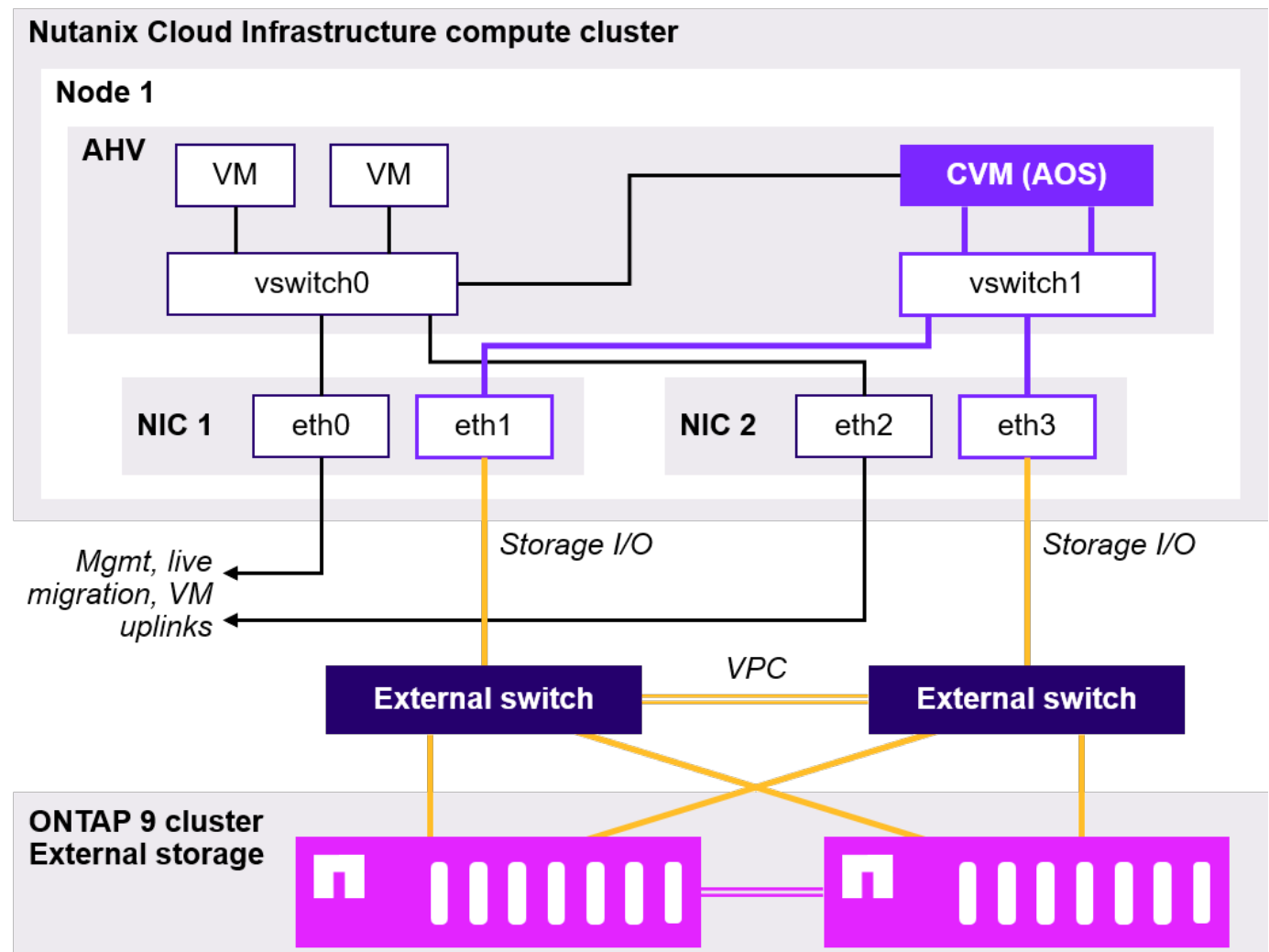
- Dedicated storage networking is available with a minimum of 10 GbE. 25 GbE or higher is recommended.
- Separate interfaces are available for storage traffic.
- Jumbo frames (MTU 9000) are configured consistently across the storage network where supported.



- Use a dedicated virtual switch for ONTAP storage traffic and configure an MTU of 9000 bytes (jumbo frames).
- After network segmentation is enabled for ONTAP private networking, it cannot be disabled. Disabling network segmentation makes the storage private IP unreachable and can result in critical cluster service failures.

Network architecture

The following diagram shows the connectivity between a Nutanix AHV node and an ONTAP cluster.



The following table describes each network component, its configuration, and its purpose.

Component	Configuration	Purpose
Nutanix compute nodes	Bonded NICs for the management and user VM network (routed VLAN) and the storage network (non-routed VLAN). If bonded NICs are not possible, use active/active uplinks for the virtual switches.	Provides network redundancy while isolating management, VM, and storage traffic.
ONTAP storage controllers	SVM management LIF and SVM data LIFs. Use interface groups for fault tolerance and load balancing whenever possible.	Management LIFs are used for ONTAP administration. Data LIFs provide NFSv3 storage access to the Nutanix cluster.
Management and user VM network (routed VLAN)	Prism management, CVM traffic, live migration, and replication traffic	Carries cluster management and virtual machine traffic.
Internal storage network (non-routed)	CVM-to-CVM communication, AHV services, cluster internode traffic	Dedicated network for storage and cluster services. Isolated from user traffic.
External storage network (non-routed VLAN)	NFSv3 storage traffic between AHV/CVMs and ONTAP	Provides low-latency, high-performance access to ONTAP storage.
vswitch0	Nutanix management, application traffic, live migration, and replication	Primary virtual switch for management and VM networking.
vswitch1	Dedicated NFSv3 storage traffic. Minimum of two physical uplinks. LACP (active/active) recommended. MTU 9000.	Dedicated storage switch that provides optimal performance, resiliency, and traffic isolation for ONTAP connectivity.

High-level deployment steps

Complete the following high-level steps to prepare ONTAP, configure storage networking, and connect the Nutanix hosts to ONTAP storage.

1. Deploy and configure ONTAP.
 - a. See [Quick start for ONTAP](#).
 - b. Create interface groups whenever possible. See [Combine physical ports to create ONTAP interface groups](#).
 - c. Create SVMs for the ONTAP network. See [Create SVMs for the ONTAP network](#).
 - d. Create ONTAP LIFs for management and NFS data. See [Create ONTAP LIFs](#).
 - e. Add a volume with ONTAP System Manager. The volume must use the UNIX security style to serve NFSv3 data. See [Add a volume with ONTAP System Manager](#) and [Create ONTAP NAS volumes with specified junction points](#).
 - f. Configure export policies to allow access from the Nutanix compute-only hosts. See [How export policies control client access to ONTAP NFS volumes or qtrees](#).
2. Configure storage networking.
 - a. Create a dedicated non-routed VLAN for NFS storage traffic. See [Create a dedicated non-routed VLAN](#).

- b. Configure a redundant switching infrastructure.
 - c. Enable jumbo frames (MTU 9000) end to end. For ONTAP, see [Change the MTU value for ports in an ONTAP broadcast domain](#).
3. Provision and connect Nutanix hosts to ONTAP.
 - a. Validate connectivity to the ONTAP NFS data LIFs.
 - b. Verify load balancing and path redundancy.
4. Create a dedicated storage virtual switch.
 - a. Create vswitch1 on Nutanix AHV.
 - b. Assign at least two dedicated physical NICs.
 - c. Configure LACP (active/active) where supported.
5. Validate resiliency.
 - a. Test storage path failover.
 - b. Confirm that AHV automatically reroutes storage traffic during link or switch failures without impacting running VMs.

This architecture provides a high-performance, highly available storage fabric for Nutanix environments while allowing compute and storage resources to scale independently. Storage growth can be accommodated through ONTAP expansion without requiring additional Nutanix compute-only nodes, reducing infrastructure costs while maintaining enterprise-class performance and availability.

Deploy a Nutanix compute cluster with ONTAP storage

Deploy a Nutanix compute cluster that consumes storage from NetApp ONTAP. You download the AOS and AHV installation packages, set up Foundation Central, image and onboard the compute nodes, create the cluster, and then connect ONTAP storage to it.

Steps

1. Download the AOS and AHV installation packages.

For more information, see [Downloading the AOS and AHV Installation Packages](#).

2. Set up Foundation Central.

Nutanix Foundation Central (FCA) is the recommended deployment tool for imaging the supported OEM servers and creating the Nutanix compute cluster.

- a. Download the Foundation installer bundle and deploy the Foundation VM.
- b. Complete the [Foundation Central setup](#).
- c. Update the management IP address and network settings as required.
- d. Access the Foundation Central web UI using the configured IP address.



If the Foundation Central deployment fails, log in to the FCA VM, run `k3d cluster delete fccluster`, and then rerun the setup process.

For more information, see [Installing the Foundation VM](#).

3. Upload the AOS and AHV installation images.

Use Foundation Central image management to do the following:

- a. Upload the AOS and AHV images into Foundation Central.
- b. Verify that the images are available for deployment.

4. Discover and image the compute nodes.

Choose one of the following options.

Option A: Hardware provider (recommended)

Use a [hardware provider](#) to automate node imaging and onboarding.

- a. Configure a hardware provider connection using HPE iLO or Dell iDRAC.
- b. Discover the target servers automatically.
- c. Select the uploaded AOS and AHV images.
- d. Image the nodes directly from Foundation Central.

Option B: Manual imaging

If hardware provider discovery is unavailable, use [manual imaging](#).

Before you begin, ensure that the following prerequisites are met:

- UEFI boot mode is enabled.
- Secure Boot is disabled.
- The out-of-band (OOB) and data networks are reachable.
- There is no time skew between the hosts and Foundation Central.
- One AHV IP address is available for each host.



Do not assign IP addresses from a subnet that overlaps with the 192.168.5.0/24 address space on the default VLAN.

- e. Create secure claim tokens.
- f. Mount the AHV installation ISO on each compute node.
- g. Boot and install AHV manually.

5. Onboard the nodes.

Onboarding registers the discovered servers with the Foundation Central Appliance and prepares them for imaging or cluster creation workflows.

- a. Select the discovered AHV hosts.
- b. Begin the onboarding process.
- c. Verify that all nodes appear under the nodes inventory.

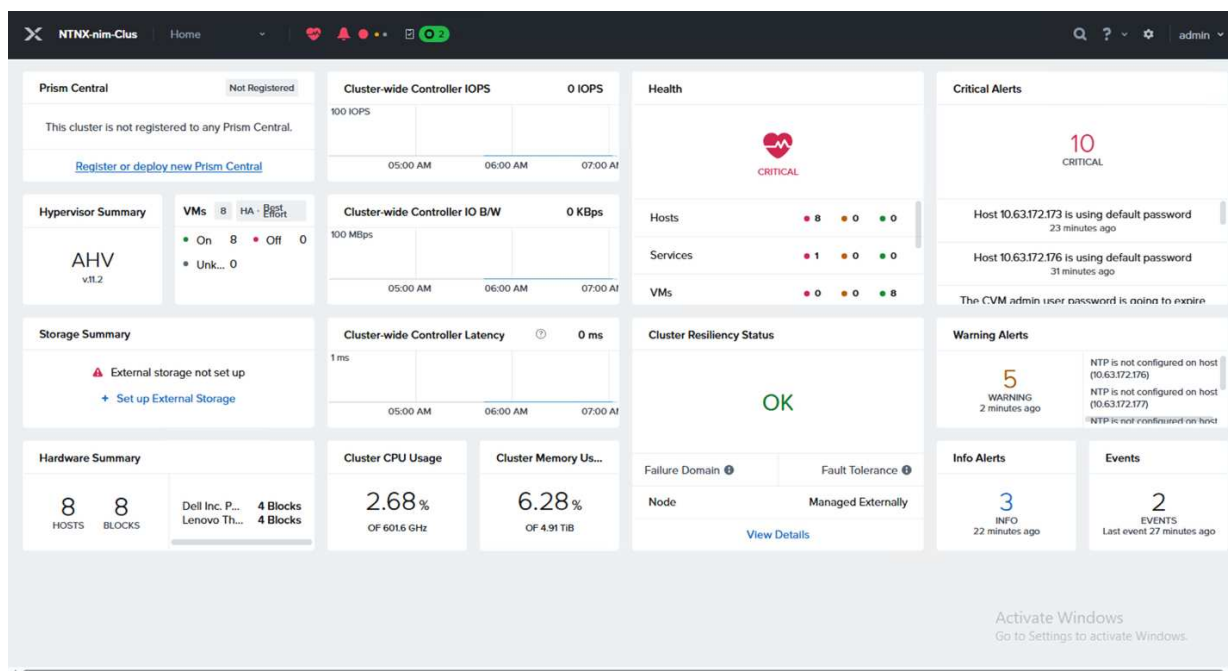
After onboarding is complete, the hosts are ready for cluster creation.

6. Create the Nutanix cluster.

- Select the onboarded nodes.
- Click **Create Cluster**.
- Provide the cluster configuration information.
- Enter the Controller VM (CVM) IP addresses when prompted.

The cluster creation workflow does the following:

- Deploys the CVMs.
- Installs AOS.
- Configures cluster services.
- Performs validation checks.



Ensure that there is no time skew between nodes. Clock synchronization failures can cause cluster deployment to fail, requiring the process to be restarted.

7. Connect ONTAP storage to the Nutanix compute cluster.

After the Nutanix cluster is operational, do the following:

- Verify connectivity between all AHV hosts and the ONTAP NFS data LIFs.
- Add the ONTAP NFS exports to the Nutanix cluster.
- Mount the exported FlexVol NFS shares.
- Validate read/write access.
- Confirm datastore visibility and availability.

You can use the mounted NFS storage for the following:

- Virtual machine workloads
- Image repositories
- Templates
- Application data

For the detailed procedure, see [Attach ONTAP NFS storage to a Nutanix compute cluster](#).

Configure ONTAP volumes, export policies, and permissions for Nutanix

Create and configure ONTAP storage volumes, configure export policies, and define the SVM role and service account that Nutanix uses to manage ONTAP storage. After you complete these tasks, you can attach the FlexVol exports to the Nutanix cluster as shared storage for virtual machine workloads.

The process starts by creating ONTAP FlexVol volumes and configuring NFS export policies. You then define the required SVM role and REST API permissions, and finally attach the ONTAP storage to the Nutanix compute cluster.

Create ONTAP FlexVol volumes

Create the required FlexVol volumes and apply the recommended ONTAP settings to optimize capacity utilization, storage efficiency, and performance for Nutanix workloads.

Steps

1. Create the FlexVol volumes with the following settings:

Setting	Configuration
Volume guarantee	None (thin provisioned)
<code>fractional_reserve</code>	0%
<code>snap_reserve</code>	0%
Autosize	On
Storage efficiency	Enabled
Autodelete	<code>volume / oldest_first</code>
Volume tiering policy	Snapshot only
<code>try_first</code>	Autogrow
Snapshot policy	None



- Provision multiple FlexVol volumes and add them as storage containers.
- Create a minimum of 4 to 8 NFSv3 volumes to host the virtual machine data.
- Use a dedicated volume for the Nutanix service or metadata volume. While service data can share a data volume, a dedicated volume is recommended.
- Use FlexVol export paths by default. If qtrees are used, specify the qtree export path when

you attach the storage container.

- Distribute volumes evenly across ONTAP nodes, placing volumes on an alternating-node basis to balance workload placement and resource utilization across the cluster.

Calculate the service volume size

Calculate the size of the metadata (service) volume by allocating a minimum of 1 TiB per cluster node ($N \times 1$ TiB). For example, an 8-node cluster requires at least 8 TiB of available capacity.



- Create a single thin-provisioned FlexVol volume for Nutanix metadata.
- If a dedicated export path is not specified for the service volume, the system automatically uses the first export path configured for the cluster services (metadata) volume and applies the **Cluster Services** tag to that path.
- Do not rename the selected FlexVol volumes or their associated export paths after deployment. Renaming can disrupt virtual machine I/O operations and impact workload accessibility.
- The FlexVol volume used for the service volume can be configured using thin provisioning.

Calculate the data volume size

Data volume sizing is similar to datastore sizing. Size storage container volumes based on the expected number of virtual machines, their capacity requirements, and projected growth. Plan sufficient free space to accommodate VM provisioning, snapshots, and operational overhead while distributing workloads across multiple volumes to support scalability and balanced resource utilization.

Configure ONTAP export policies

Configure export policies so that only the Nutanix CVMs can access the NFS volumes.

Data volumes

1. Create a volume-level export policy that allows the CVM IP addresses or subnet range.
2. Set the following rules:
 - a. Read-only rule (`rorule`): `sys`
 - b. Read-write rule (`rwrule`): `sys`
 - c. Superuser: `sys`
3. If qtrees are used, create a dedicated export policy rule per qtree with the same permissions.

Service or metadata volume

1. Create a volume-level export policy that allows the CVM IP addresses or subnet range.
2. Set the following rules:
 - a. Read-only rule (`rorule`): `sys`
 - b. Read-write rule (`rwrule`): `sys`
 - c. Superuser: `sys`



- All ONTAP NFS exports should allow access only from the Nutanix CVM IP addresses or the designated CVM subnet.
- Use the Prism API or `nccli` to find the list of the CVM host IP addresses to update the export policy.

Configure ONTAP roles and permissions

To connect ONTAP storage to a Nutanix compute cluster, Nutanix uses the ONTAP REST API for control plane operations (VM provisioning, cloning, snapshots, and storage management) and NFSv3 for the data path.

Create an ONTAP role with minimum privileges so that you do not need to use the ONTAP `admin` role to perform operations in the Nutanix compute-only cluster. These minimum roles are required at the SVM level on the ONTAP storage side.



- Use the default ONTAP NFS configuration settings.
- You can also use the `vsadmin` role.

Minimum REST API permissions

Create a custom ONTAP SVM role with the minimum required REST API permissions to enable Nutanix storage discovery, provisioning, cloning, and management operations.

REST API endpoint	Access	Purpose
<code>/api/cluster</code>	Read only	Cluster authentication and version validation
<code>/api/cluster/jobs</code>	Read only	Monitor asynchronous storage operations
<code>/api/network/ip/interfaces</code>	Read only	Discover ONTAP data LIFs
<code>/api/storage/file/clone</code>	Read/Create	VM cloning, snapshot, and backup operations
<code>/api/storage/volumes</code>	Read only	Volume discovery and management
<code>/api/storage/volumes/*/files</code>	Full access	Create, modify, read, and delete Nutanix-managed files

Configure the service account

You can create the role and user with ONTAP System Manager or with the ONTAP CLI.

System Manager

Steps

1. Create a custom role at the SVM level.
 - a. Select **Storage > Storage VMs > *designated SVM* > Settings > Users and Roles**.
 - b. Select the arrow icon (→) next to **Users and Roles**.
 - c. Under **Roles**, select **+Add**.
 - d. Define the rules for the role and click **Save**.

Role attributes

REST API path i	Secondary path i	Access i	
/api/cluster/jobs	Enter secondary path	Read-only	
/api/network/ip/interfaces	Enter secondary path	Read-only	
/api/storage/file/clone	Enter secondary path	Read/create	
/api/storage/volumes	Enter secondary path	Read-only	
/api/storage/volumes	/* /files	Read/write	
/api/cluster	Enter secondary path	Read-only	

2. Map the role to the Nutanix admin user.

- On the **Users and Roles** page, under **Users**, select **+Add**.
- Select the required username, and then select the role that you created in the previous step from the **Role** drop-down menu.
- For user login methods, select **HTTP**.
- Click **Save**.

ntnx-svm Users and roles [All settings](#)

Users

+ Add

☐

User

Role

MFA for HTTP

Account locked

nim-NTNX

nim-ntnx-role

Disabled

No

Application
HTTP

Authentication
Password, MFA disabled

vsadmin

vsadmin

Disabled

No

Roles

+ Add

☐

Role

nim-ntnx-role

API

Access level

/api/cluster

Read-only

/api/cluster/jobs

Read-only

/api/network/ip/interfaces

Read-only

/api/storage/file/clone

Read/create

/api/storage/volumes

Read-only

/api/storage/volumes/*/files

Read/write

Users

+ Add

Search

Filter

Menu

	User	Role	MFA for HTTP	Account locked
^	nim-NTNX	nim-ntnx-role	Disabled	No
Application		Authentication		
HTTP		Password, MFA disabled		
ONTAPI		Password		
v	vsadmin	vsadmin	Disabled	No

Roles

+ Add

Search

Filter

Menu

	Role	
^	nim-ntnx-role	
API		Access level
/api/cluster		Read-only
/api/cluster/jobs		Read-only
/api/network/ip/interfaces		Read-only
/api/storage/file/clone		Read/create
/api/storage/volumes		Read-only
/api/storage/volumes/*/files		Read/write

CLI

Steps

1. Create the role by running the following commands. Replace `ntnx-svm` and `nim-ntnx-role` with your SVM and role names.

```
security login rest-role create -vserver ntnx-svm -role nim-ntnx-role -api "/api/cluster" -access readonly
security login rest-role create -vserver ntnx-svm -role nim-ntnx-role -api "/api/cluster/jobs" -access readonly
security login rest-role create -vserver ntnx-svm -role nim-ntnx-role -api "/api/network/ip/interfaces" -access readonly
security login rest-role create -vserver ntnx-svm -role nim-ntnx-role -api "/api/storage/file/clone" -access read_create
security login rest-role create -vserver ntnx-svm -role nim-ntnx-role -api "/api/storage/volumes" -access readonly
security login rest-role create -vserver ntnx-svm -role nim-ntnx-role -api "/api/storage/volumes/*/files" -access all
```

2. Create the user and map it to the role.

```
security login create -vserver ntnx-svm -user-or-group-name nim-ntnx-user -application http -authentication-method password -role nim-ntnx-role
```



The ONTAP service account username and password are required when you add the ONTAP array to the Nutanix cluster. Use this user when you configure the ONTAP storage SVM in Prism Element or Prism Central.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.