Nutanix, Inc.

Nutanix Cloud Platform

v6.8

Guidance Documentation Supplement

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.11

Prepared for:

NUTANIX™

Prepared by:

Corsec

Nutanix, Inc.
1740 Technology Drive
Suite 400
San Jose, CA 95110
United States of America

Phone: +1 855 688 2649
www.nutanix.com

Corsec Security, Inc.
12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2023-07-20	Ryan Butler	Initial draft.
0.2	2024-04-18	Ryan Butler	Observation responses.
0.3	2024-06-28	Iain Holness	Updates due to ORs
0.4	2024-08-27	Iain Holness	Updates due to ORs
0.5	2024-10-18	Ryan Butler	Updates due to ORs
0.6	2024-12-06	Iain Holness	Updates due to Ors
0.7	2025-01-31	Ryan Butler	• Corrected AOS naming scheme • Removed nCLI from scope and removed all references • Corrected Prism Admin role in Table 3 • Added clarification to Section 3.1.6 Nutanix Security Guide
0.8	2025-03-21	Ryan Butler	• Corrected SHA256 hash values in Table 1 • Added AGD to Table 1 • Added clarification regarding verification of AGD
0.9	2025-05-05	Ryan Butler	• Updated Prism Central version number and associated guidance documents
0.10	2025-06-10	Ryan Butler	• Updated Self-Service version number
0.11	2025.07-14	Ryan Butler	• Updated Files version number

©2025 Nutanix, Inc. – Confidential and Proprietary

Table of Contents

List of Tables

List of Figures

 ©2025 Nutanix, Inc. – Confidential and Proprietary

1. Introduction

The Target of Evaluation (TOE) is the Nutanix, Inc. (Nutanix) Nutanix Cloud Platform. The TOE is comprised of:

- Acropolis Operating System (AOS) v6.8
- Acropolis Hypervisor (AHV) v20230302.100173
- Prism Central (PC) pc.2024.2.0.6
- Flow Virtual Networking (FVN) v4.0.0
- Flow Network Security (FNS) v4.1.0
- Self-Service v3.8.1.1
- Files v5.0.0.1
- Objects v5.0
- Nutanix Database (NDB) v2.5.5

These are collectively referred to as the Nutanix Cloud Platform or NCP and will hereafter be referred to as the TOE throughout this document. A minimum of three hosts (either nodes or servers) that contain a copy of the TOE are combined to provide a High Availability (HA) cluster. This allows the TOE to be a unified solution for guest Virtual Machine (VM) management while eliminating administration overhead by removing the need for a separate storage network.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria Evaluation Assurance Level 2+ Evaluated Configuration. This document provides clarifications and changes to the Nutanix documentation and should be used as the guiding document for the installation and administration of the TOE in the Common Criteria-evaluated configuration. The official Nutanix documentation should be referred to and followed only as directed within this document. All Nutanix documentation listed in Table 1 is publicly available for download from the Nutanix Website at https://www.nutanix.com/trust/compliance-and-certifications/common-criteria-auditorevaluation.

Table 1 lists the guidance documents relevant to the installation and configuration of the TOE.

Table 1 – TOE Guidance Documents

Short Reference	Document Name / SHA256 Hash	Description
[AAAG]	*Nutanix Acropolis Advanced Administration Guide AOS 6.8 May 20, 2024* **SHA256:** ccff0ab60d8b6a8e61851a485c3a7e0c5521853db6f69ea9e837a77629ef6a7e	Contains information on how to maintain and configure the TOE.
[AHV_GUIDE]	*AHV Administration Guide AHV 6.8 May 21, 2024* **SHA256:** 86cf8b6db175b5ff0e3217129a685e9ca60661be8660f62e60c026c510b229da	
[SEC_GUIDE]	*Security Guide AOS Security 6.8 May 17, 2024* **SHA256:** 36251e3a58ae3e86d4feaf1cf45581f7be4c269c6ad67b918f39c003d53b26d4	Contains information on securing the TOE.
[PC_ADMIN]	*Prism Central Admin Center Guide Prism pc.2024.2 April 29, 2025* **SHA256:** a9d6cbb266f593f2b0712d92fc07b13aab473c4ead8d74c8b957a5629fc1122f	Contains information on how to use the web console.
[PC_INFRA]	*Prism Central Infrastructure Guide Prism pc.2024.2 April 17, 2025* **SHA256:** 830a770cbe108bab033dbd0be5eb1f00b0d40757bf99324f0f173d007811e1ee	Contains information on how to use the web console.
[API_REF_v1]	*Acropolis v1 API[1] Reference AOS 6.8 May 20, 2024* **SHA256:** 2fcdcfb758bb9b38406fa4e8d9ab5953ae60bfb99c4561a3a98925e1ccbbdab1	Contains information on the v1 and v2 REST[2] API interface.

[1] API – Application Programming Interface
[2] REST – Representational State Transfer

©2025 Nutanix, Inc. – Confidential and Proprietary

Short Reference	Document Name / SHA256 Hash	Description
[FVN_GUIDE]	*Flow Virtual Networking Guide Flow Virtual Networking pc.2024.2 April 21, 2025* **SHA256:** 60e3f462d5ab1e21c48e043e44ace4e399049e82ff735a10a355834f45e1efe2	Contains usage information for the Flow Virtual Networking TOE component
[FNS_GUIDE]	*Flow Network Security Next-Gen Release version 4.1.x May 17, 2024* **SHA256:** d7abc459ce84617d600173db2dc2e091b6d9e8b29bd119ceec6398f81298ebdb	Contains usage information for the Flow Network Security TOE component
[SS_GUIDE]	*Self-Service Administration and Operations Guide Self-Service 3.8.1.1 May 26, 2025* **SHA256:** 88cd484c5382848e639176d7e2abb1c784adbee8382dfb50ceec21740a86282a	Contains usage information for the Self-Service TOE component
[FILES_GUIDE]	*Nutanix Files User Guide Files 5.0 May 20, 2024* **SHA256:** 6D2A7B075851244FCEFF3E41CD21ABE0DDD7CE1FA5CB48D1F51B649E8552FD90	Contains usage information for the Nutanix Files TOE component
[OBJECTS_GUIDE]	*Objects User Guide Objects 5.0 May 20, 2024* **SHA256:** 1D9EFF1FD4FCFCDE51F8ABE9050F1DDDED228492FB86F806216D28D732E08D73	Contains usage information for the Nutanix Objects TOE component
[NDB_GUIDE]	*Nutanix Database Service Administration Guide Nutanix Database Service (formerly Era) 2.5 March 15, 2024* **SHA256:** C194DFE9EA3C51FC03AD89AF332CB1E5F971B8790AED187CD56262A1E210EE16	Contains usage information for the Nutanix Database Service TOE component
[REST_3]	*Nutanix v3 API Reference* **SHA256**: 887F680909DA631ABCE82B6945797662BBCE64B92F70383CCA3D77CA3882E793	Contains information on the v3 REST API interface.
[REST_4]	*Nutanix REST API v4 Document* **SHA256**: 327F488F65D08A73291B90B85FE6D8ABE6BE5CAB59611B9967D610C87AB64053	Contains information on the v4 REST API interface.
[PRISM_WEB]	*Prism Element Web Console Guide, Prism 6.8, May 20, 2024* **SHA256**: 27267712112F9223A77716D343C96138931FB93D01CC7D3857C085141E43A753	Contains usage information for the Prism Element interface
[AGD]	*Nutanix Guidance Documentation Supplement v0.11, June 10, 2025* **SHA256: See published hash on Nutanix Website**	Common Criteria Administrative Guidance Supplement

Note: This document, the Nutanix Guidance Documentation Supplement v0.11, July 14, 2025, is also considered required reading and is part of the TOE. This document can be downloaded from the Nutanix website (https://www.nutanix.com/trust/compliance-and-certifications/common-criteria-auditorevaluation), and verified with the provided SHA256 hash on the downloads page. If you obtained this document from another source, please visit the link provided and verify the hash.

1.2 Target Audience

The audience for this document consists of the end-user, the Nutanix development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

©2025 Nutanix, Inc. – Confidential and Proprietary

1.3 Evaluated TOE Configuration

Figure 1 depicts the evaluation configuration of the TOE. The following acronyms are used in Figure 1 and are previously undefined:

- NTP – Network Time Protocol

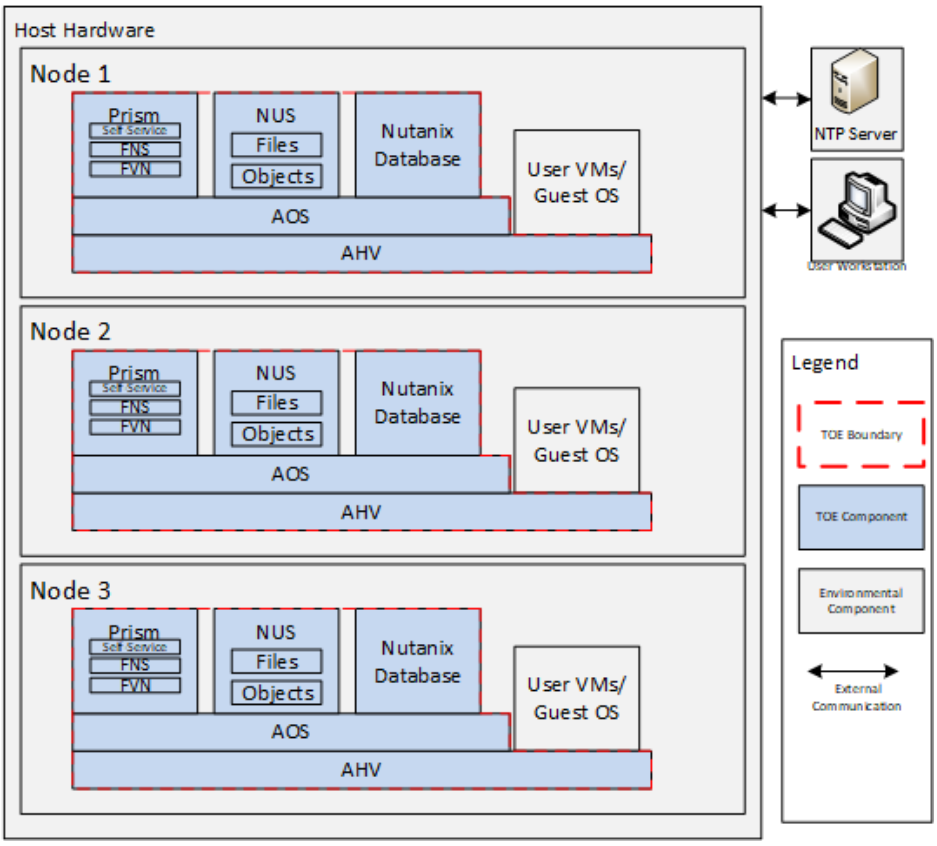

Figure 1 – Deployment Configuration of the TOE

As shown in Figure 1, the TOE comprises the following components of Nutanix Cloud Platform: AOS v6.8 and AHV v20230302.100173, as well as the Prism Central, Flow Network Security, Flow Virtual Networking, Self-Service, Files, Objects, and Nutanix Database services which run on AOS. Refer to the *Nutanix Cloud Platform v6.8 Security Target* for a complete description of these components.

The TOE is designed to run and store multiple guest VMs that offer virtualized services to end users. These VMs and the host hardware are considered to be environmental components. At least one guest VM must be running to make use to make use of the storage functionality provided by the TOE. Three hosts are required for the evaluated configuration.

1.4 Assumptions

The writers of this document assume the following:

- It is assumed that the TOE environment will be configured in such a way as to allow administrative users to access the information stored on the TOE.
- The network that the TOE uses for storage transfer is intended to be an internal private network that is protected from access by entities outside of the organization. External access to storage services are blocked by the TOE environment.

©2025 Nutanix, Inc. – Confidential and Proprietary

- It is assumed that administrative users accessing the storage on the TOE reside on the internal network and are not careless, negligent, or willfully hostile with regard to their access of the TOE.
- It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrative users only.
- It is assumed that the administrative users who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
- It is assumed that the administrators of the TOE's operating environment conduct proactive checking of all systems and media traversed by the communication between administrative systems and the TOE.
- It is assumed that the TOE environment will provide the time for the TOE from a reliable source.

©2025 Nutanix, Inc. – Confidential and Proprietary

2. Installation Procedure

This section describes the installation procedure notes and changes. As the installation is performed on the customer's premises by Nutanix Systems Engineers (SEs), this section describes only the procedures relevant to the following activities that the customer is expected to perform: confirm delivery of the TOE components, prepare the operational environment, verify the operational TOE, and complete any additional steps required to bring the TOE to its evaluated configuration.

2.1 Introduction

This section provides guidance for how to properly step through the installation instructions documented in the *[AHV_GUIDE]*, along with additions and changes to the instructions contained therein, in order to allow the installer to properly install the evaluated configuration of the TOE.

2.2 Secure Installation

Note: Throughout this section, the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the *[AHV_GUIDE]*

2.2.1 Phase 1 – Initial Preparation

To prepare the operational environment, the following items will be needed and must be acquired before the Nutanix SE arrives on site for the installation:

- A general-purpose computer (GPC) used to access the TOE's storage and services. The workstation provides access to the TOE's Prism Central and Prism Element web consoles, REST API, and other management interfaces via an HTTPS[3] connection. It should be running the following:
  - The latest version of a modern web browser such as:
    - Mozilla Firefox
    - Google Chrome
    - Apple Safari
    - Microsoft Edge
    - Microsoft Internet Explorer 11
  - A REST API client (such as Postman or Insomnia)
- Network infrastructure providing connectivity to the TOE (refer to the "Host Network Management" section of [AHV_GUIDE]).
- An NTP server that will provide a reliable time to the TOE.
- Confirmed delivery of the host hardware by verifying the shipment against the "Installed Configured Options" section on the shipping label of the package. The evaluated configuration of the TOE was tested on the three-node NX-3060N-G8[4] hardware platform, however, the following host hardware models are considered to be equivalent, and are allowed in the evaluated configuration:
  - NX-1065-G8

[3] HTTPS – Secure Hypertext Transfer Protocol

[4] also referred to as the NX-3360N-G8, where the "3" in the place of the "0" denotes the three nodes of the platform

 ©2025 Nutanix, Inc. – Confidential and Proprietary

- NX-1065-G9
- NX-1065N-G8
- NX-1175S-G8
- NX-1175S-G9
- NX-3035-G9
- NX-3060-G8
- NX-3060-G9
- NX-3155G-G8
- NX-3155GN-G8
- NX-3155-G9
- NX-3170-G8
- NX-3170N-G8
- NX-8035-G8
- NX-8035N-G8
- NX-8150-G8
- NX-8150-G9
- NX-8150N-G8
- NX-8155-G8
- NX-8155N-G8
- NX-8155-G9
- NX-8155A-G9
- NX-8170-G8
- NX-8170N-G8
- NX-8170-G9

The *Nutanix AOS ANY Getting Started Guide NX Series* is delivered alongside the TOE hardware or can be downloaded from the Nutanix Portal. When setting up the 2U 3 node (2U3N) hardware for the TOE, the information about the 2U4N chassis in this document is used. This is because the same chassis is used for both setups except the 2U3N will not have the 4th node slot populated.

If a customer prefers to do the installation themselves, then they can proceed with the installation steps below after verifying receipt of the components listed above. If performing the host installation without the Nutanix SE, refer to the *Nutanix Foundation 5.4.x Field Installation Guide May 3, 2023*.

2.2.2 Phase 2 – Downloading and Installing the Software

2.2.2.1 TOE Component Version Checking

The TOE is delivered with the base AHV and AOS software pre-installed on the host hardware. Additional components are installed onsite by the Nutanix Support Engineer. The host hardware could be delivered with a version of AHV and AOS that is not the evaluated version. After the Nutanix Support Engineer concludes the installation of the TOE and its components, each of the components of Nutanix Cloud Platform (AOS, AHV, Prism Central, Flow Virtual Networking, Flow Network Security, Self-Service, Files, Objects, and Nutanix Database Service) must be inspected by the customer to determine that the correct, evaluated version of the software is

©2025 Nutanix, Inc. – Confidential and Proprietary

installed. The version numbers for each component must match exactly with the version numbers listed in Section 1.

For Prism Central, AOS, Self-Service, Files, Objects, Flow Network Security, and Flow Virtual Networking, currently installed version numbers can be viewed in Prism Central by navigating to **Admin Center -> LCM -> Inventory.** If necessary, click **Perform Inventory** and wait for the operation to finish. Version numbers for Self-Service are listed under the "Calm" component name. Version numbers for Flow Virtual Networking are listed under the "Network Controller" component name.

The version number for AHV can be viewed by logging into Prism Element, selecting **LCM** from the dropdown menu, then selecting **Inventory** from the navigation bar. If necessary, click **Perform Inventory** and wait for the operation to finish. Once the operation is completed, the AHV version number is listed under the **AHV hypervisor** column.

The version number for NDB can be viewed at the top right of the dashboard in the NDB GUI.

If the components' versions are correct, the upgrade steps in the next section can be skipped.

2.2.2.2 Upgrading/Downgrading the TOE

In order to upgrade or downgrade the version currently running on the host, perform the following steps:

1. Run the Nutanix Cluster Checks (NCC) inside Prism Element by clicking on the dropdown list in the top left and selecting **Health**.
2. Click on the **Actions** dropdown list in the top right and select **Run NCC Checks**.
3. Select **All Checks** and click on the **Run** button.
4. If any of the checks report failed, warning, or error, resolve the reported issues before proceeding. If you are unable to resolve the issues, contact Nutanix support for assistance.
5. Once everything has passed, log into the Nutanix Support Portal at `http://portal.nutanix.com`, click on the menu bar in the top left, hover over the **Downloads** link, and choose **AOS**.
6. Click on the link to download the AOS v6.8 tar.gz and metadata files to a workstation.
7. Once the files have been downloaded, verify the SHA[5]256 hash of the tar.gz file against the SHA256 value listed at the end of the metadata file.
8. If the hashes match, log into Prism at `https://<IP_Address>:9440/console` to do the upload. If the hashes do not match, contact Nutanix support and report the issue.
9. Click the gear icon in the top right to go to the **Settings** page.
10. Click on **Upgrade Software**.
11. On the AOS page, click on the link to upload a software binary.
12. Click **Choose File** under **AOS BASE SOFTWARE METADATA FILE** and select the metadata file downloaded from the Support Portal.
13. Click **Choose File** under **AOS BASE SOFTWARE BINARY FILE** and select the tar.gz file downloaded from the Support Portal.
14. Make sure the option to overwrite the existing AOS base software binary file is unchecked. Click **Upload Now** to begin the upload.
15. When the upload process is completed, click on **Upgrade**, **Upgrade Now**, and then **Continue**.
16. Click on the **Yes** button when it asks to refresh the page.

[5] SHA – Secure Hash Algorithm

17. Once the page has refreshed, click on the Hypervisor tab to upgrade AHV. Note that the files were uploaded as part of the AOS upload.
18. Click on **Upgrade**, **Upgrade Now**, and then **Yes**.
19. The process will be complete once the status reads "Successfully Upgraded Hypervisor 100%".

Note that by uploading the AOS files, the required AHV files are also uploaded and AHV is upgraded during the AOS upgrade. If there are any errors in the upgrade process, contact Nutanix support to help correct the errors. After the upload is complete, repeat the first set of steps to check the "CURRENT VERSION" for both components.

Once the software is on the correct version and the Nutanix SE has completed their duties, the password for the *admin* account must be changed. Preform the following steps to change a password:

1. Log into Prism at `https://<IP_Address>:9440/console`.
2. Click on the user menu in the top right and click on **Change Password**.
3. The password complexity requirements are displayed and can be referenced in Section 3.1.1.
4. Click on the **Save** button to set the new password.

Additionally, the AHV password should be changed from its default value. Refer to the "Changing the Root User Password" section of the [AHV_GUIDE] for steps on changing the password.

2.2.2.3 TOE Component Software Verification

Customers wishing to perform the setup of the TOE themselves must verify the validity of the TOE software before installation. Nutanix provides published MD5 hashes on their downloads site for each file. Table 2 below lists the filename and hash for each component:

Table 2 – TOE Component Software

Component	Filename	Hashes
AHV	**ISO:** `AHV-DVD-x86_64-el8.nutanix.20230302.100173.iso`	**SHA256:** `05f392a5e02ddcac9b84d010715f4d2d993b87b1430643e09524295e3a8282ff`
	LCM[6]: `lcm_ahv_el8.nutanix.20230302.100173.tar.gz`	**SHA256:** `0e41e56a772570c5bc50a4db393c479e7787cfa51fb5e52495813cfaff5f1315`
AOS	**Upgrade:** `nutanix_installer_package-release-fraser-6.8-stable-9b27c8bcb5fcaac58016f3bed74009655a157049-x86_64.tar.gz`	**SHA256:** `f8192c654ac45a714dc56d0532595c9dfa18bdc9183122d53b79b1daefa242db`
	LCM: `lcm_nos_6.8.tar.gz`	**SHA256:** `b7b850d5fb8e90399b464b3422cb562720e686195cd4a37c8edb977b4714fa36`
Prism Central	**Upgrade:** `pc.2024.2.0.6-e7141238ee6a3838cb87a1467496b119224bb219-x86_64.tar.gz`	**SHA256:** `b2731240c1d33b071c08b3d2699367cd71f8d7ab1610e1c4bf5036c22bb2edc1`
	LCM: `lcm_pc_pc.2024.2.0.6.tar.gz`	**SHA256:** `bac961593477e6dcc8fcee00ebab59620340132657c58cd0f25004133aa30d22`
Flow Network Security	**LCM:** `lcm_flow_pc_4.1.0.tar.gz`	**SHA256:** `565e17a2d1335c2c61e7093d1e14954b077ab4a323b40b1af537a551f20871d2`
Flow Virtual Networking	**LCM:** `4.0.0.tar.gz`	**SHA256:** `14ebfe2139807a070b0ef4f04b7c0ab6cb2d534609a1d267a609b0d9e6d11970`
Files	**Upgrade:** `nutanix-afs-el8.5-release-afs-5.0.0.1-stable-8da0965291d7453229238d58dc1abc3f09f4031d.qcow2`	**SHA256:** `86635e87ef0313606c1dcee5c9451a11a4a6182cf8619e878544774f9bc140f7`
	LCM: `lcm_file_server_5.0.0.1.tar.gz`	**SHA256:** `72a4bbc00a17098c229a7fa794028cf736e7a1588e9b12a705953a84e8ab438a`
Objects	**LCM:** `objects-5.0.tar.gz`	**SHA256:** `f6d8384aab4800a92c0b9fe9eda2ed87b2368d5e2b88aff17e32dc633d1bc62b`

[6] LCM – Nutanix Lifecycle Manager

©2025 Nutanix, Inc. – Confidential and Proprietary

Component	Filename	Hashes
Self-Service	`Epsilon-3.8.1.1.zip`	**SHA256:** `f05b8af12c56daeeb7d2913417e8d90d76d5859cdecaba5368397d37714c5c78`
Nutanix Database	**Install:** `NDB-Server-build-2.5.5-e6a22438d6f5bdbda5f6c72e910e113d22655c6d.qcow2`	**SHA256:** `0b83d4c5b7b02e568b37d2a19470b039336c33f9c7f023005131003e7ce3ef5e`
	Upgrade: `era_upgrade_bundle-2.5.5-e6a22438d6f5bdbda5f6c72e910e113d22655c6d.zip`	**SHA256:** `84fdca9a59319e9bfeff2540f8e045c2cbe916269cfe16bca6548d9c63be7ea1`

If the TOE is set up by a Nutanix Support Engineer, it is the responsibility of that engineer to verify the software according to Nutanix internal procedures before installation, and the customer can trust that the software is valid.

2.2.3 Phase 3 – Configuring the Software

2.2.3.1 Disabling IPMI[7]

In the evaluated configuration, IPMI is disabled. Record the original IP address used for IPMI as it will be needed later. Disable IPMI by setting its IP address to a non-routable one. This can be accomplished from the AHV SSH connection with the following command:

```
ipmitool lan set 1 ipsrc static
ipmitool lan set 1 ipaddr 0.0.0.0
ipmitool lan set 1 netmask 0.0.0.0
ipmitool lan set 1 defgw ipaddr 127.0.0.1
ipmitool lan set 1 bakgw ipaddr 127.0.0.1
ipmitool lan set 1 access off
```

Once these commands have been run, an administrative user can run the `ipmitool lan print` command to verify the settings and attempt to ping the original IPMI IP address to confirm that it is disabled. Repeat the commands on each instance of AHV in the cluster.

2.2.3.2 Configuring NTP Servers

An NTP server is used to provide reliable timestamps for audit logging, by performing the following steps:

1. Log into Prism at `https://<IP_Address>:9440/console`.
2. Click the gear icon in the top right to go to the Settings page.
3. Click on **NTP Server** in the **Settings** sidebar.
4. In the **NTP Server** textbox, type the name or IP address of the server and click the **Add** button.
5. Remove any other NTP servers by clicking the **x** icon next to their names.

[7] IPMI – Intelligent Platform Management Interface

©2025 Nutanix, Inc. – Confidential and Proprietary

2.2.3.3 Disable SNMP[8]

SNMP is disabled in the evaluated configuration by performing the following steps:

1. Log into Prism at `https://<IP_Address>:9440/console`.
2. Click the gear icon in the top right to go to the Settings page.
3. Click on **SNMP** in the **Settings** sidebar.
4. Uncheck the **Enable for Nutanix objects** checkbox and Prism should automatically save the changes.

2.2.3.4 Disabling Remote SSH[9]

The *Prism Web Console Guide* describes a feature that allows Nutanix remote support to SSH into the system to fix issues that might occur. The following steps disable this feature.

For Prism Element:

1. Log into Prism Element at `https://<Prism Element_IP_Address>:9440/console`.
2. Click the gear icon in the top right to go to the Settings page.
3. Click on **Remote Support** in the **Settings** sidebar.
4. If the text does not read "Remote support is currently disabled", select the **Disable** radio button and click on the **Save** button.
5. Click on **Cluster Lockdown** in the **Settings** sidebar.
6. On the **Cluster Lockdown** page, Uncheck the **Enable Remote Login with Password** box.
7. Click on the **OK** button to disable remote login.
8. Remove any public keys that have been added to prevent key-based authentication by clicking the **x** icon next to their names.

For Prism Central:

1. Log into Prism Central at `https://<Prism_Central_IP _Address>:9440/console`.
2. Click on the drop-down menu in the top left corner. Select **Admin Center.**
3. Click the gear icon in the top right corner to go to the Settings page.
4. Click on **Cluster Lockdown** in the **Settings** sidebar.
5. On the **Cluster Lockdown** page, uncheck the

Ensure that no SSH keys are added while operating the TOE in the evaluated configuration.

2.2.3.5 Disabling SMTP[10]

The SMTP feature needs to be disabled in the evaluated configuration by performing the following steps:

1. Log into Prism at `https://<IP_Address>:9440/console`.
2. Click the gear icon in the top right to go to the Settings page.
3. Click on **SMTP Server** in the **Settings** sidebar.
4. If the fields are populated, click on the **Remove** button and then the **OK** button.
5. If the fields are not populated, leave them empty to keep SMTP disabled.

[8] SNMP – Simple Network Management Protocol
[9] SSH – Secure Shell
[10] SMTP – Simple Mail Transfer Protocol

©2025 Nutanix, Inc. – Confidential and Proprietary

3. Administrative Guidance

This section provides additional guidance not found in the guides listed in Table 1. Any clarifications, exclusions, or additions are detailed here to allow the TOE Administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should have successfully completed the installation procedures listed in section 2 before applying the guidance found in sections 3.1 and 3.2.

3.1 Clarifications

This section clarifies how to use the security-relevant functions and interfaces described in the operational user guidance. Please note that acronyms Service Virtual Machine (SVM) and Controller Virtual Machine (CVM) that appear throughout Nutanix guidance documentation are synonymous.

3.1.1 Password Complexity Requirements

The following complexity requirements must be used when setting a new password for any TOE account: at least eight characters must be used.

3.1.2 User Roles and Permissions

The TOE contains the following RBAC roles that can each access Prism Central management interface:

Table 3 – RBAC Roles

Role	Description
Super Admin	Highest-level admin with full infrastructure and tenant access. Manages a Nutanix deployment and can set up, configure, and make use of every feature in the platform.
Prism Admin	Day-to-day admin of a Nutanix deployment. Manages the infrastructure and platform, but cannot entitle other users to be admins.
Prism Viewer	View-only admin of a Nutanix deployment. Has access to all infrastructure and platform features, but cannot make any changes.
Self-Service Admin	Cloud admin for a Nutanix tenant. Manages virtual infrastructure, oversees self service, and can delegate end user management.
Consumer	Lifecycle manager for team applications. Launches blueprints and controls their lifecycle and actions.
Developer	Application developer within a team. Authors blueprints, tests deployments, and publishes applications for other project members.
Operator	Owner of team applications at runtime. Works on existing application deployments, exercises blueprint actions.
Project Admin	Team lead to whom cloud administration gets delegated in the context of a project. Manages end users within the project and has full access to their entities.
VPC Admin	VPC admin of a Nutanix deployment. Manages VPCs and related entities. Agnostic of the physical network/infrastructure.
Files Admin	Full access to Files operations.
Files Viewer	View access for Files operations.
Flow Admin	Full access to Flow operations.
Flow Viewer	View access for Flow operations.
Network Infra Admin	Network infrastructure admin of a Nutanix deployment. Manages the infrastructure and underlay networking.
Cluster Admin	Full access to Cluster operations.
Cluster Viewer	View access for Cluster operations.
Disaster Recovery Admin	Full access to Disaster recovery operations.
Disaster Recovery Viewer	View access for Disaster recovery operations.

©2025 Nutanix, Inc. – Confidential and Proprietary

Role	Description
Objects Admin	Full access to Object store operations.
Objects Viewer	View access for Object store operations.
File Server Security Admin	All File Server security related permissions
File Server Share Admin	All File Server security related permissions
Monitoring Admin	Full access to perform all Monitoring operations
Monitoring Viewer	View access to all API in Monitoring
Action Service User	Basic Playbook access for all users
Category Viewer	View access for category object
Category Admin	Full access for category object
CSI System	Full access for Kubernetes cluster infrastructure resources for CSI
Kubernetes Data Services System	Full access for Kubernetes cluster infrastructure resources for Kubernetes Data Services
Kubernetes Infrastructure Provision	Access for Kubernetes cluster infrastructure VMs resources
Storage Viewer	View access for Storage entities.
Storage Admin	Storage admin of a Nutanix deployment. This user can view and perform actions on Storage entities.
Objects Editor	Edit access to Object store operations.
Flow Policy Author	Full Access to flow operations, except categories provisioning
Virtual Machine Viewer	View access for Virtual Machines.
Virtual Machine Operator	Gives access for day-to-day activities on Virtual Machines.
Virtual Machine Admin	Full access to Virtual Machines.

Additionally, the TOE maintains the following roles for Prism Element accounts only: User Admin, Cluster Admin, Backup Admin, and Viewer. The Viewer role is assigned to all accounts by default; if a local account is not assigned to a role, it has only the Viewer role. The permissions of each role are as follows:

- **User Admin** allows the user to view information, perform any administrative task, and create or modify user accounts. (Checking this box automatically selects the Cluster Admin box to indicate that this user has full permissions. However, a user administrator has full permissions regardless of whether the Cluster Admin box is checked.)
- **Cluster Admin** allows the user to view information and perform any administrative task (but not create or modify user accounts).
- **Backup Admin** allows the user to perform backup-related administrative tasks. This role does not have permission to perform cluster or user administrative tasks.
- Leaving all the boxes unchecked assigns the **Viewer** role, which allows the user to view information, but it does not provide permission to perform cluster or user-administrative administrative tasks.

When assigning roles to Administrative users, note that multiple roles can be assigned to one account. Each TSFI in the TOE applies the same permissions that the above roles allow. If an Administrative user is allowed to change a setting through Prism Central, they are allowed to change the same setting through Prism Element and the REST API.

3.1.3 Default Accounts

The TOE has two local default accounts: admin and Nutanix. Both of these accounts possess the Super Admin role that give them management access to all of the TOE's SFR-related functionality. Either account can be used to configure the TOE since they both have the Super Admin role and can access the same areas of the TOE. The Nutanix account is only needed for legacy support with programs from the environment and must be disabled while in the evaluated configuration.

©2025 Nutanix, Inc. – Confidential and Proprietary

3.1.4 IPMI Usage

In the TOE's evaluated configuration, IPMI is disabled. Any references to enabling IPMI in the guidance documentation should be omitted. It is important to note that enabling IPMI will remove the TOE from the evaluated configuration and it will not be considered the CC certified product because it provides functionality that has not been tested.

3.1.5 Nutanix Cmdlets Client Usage

In the TOE's evaluated configuration, the Nutanix Cmdlets client, which is downloaded from either Prism Element or Prism Central, should not be used.

3.1.6 Nutanix Security Guide

In the *Security Guide AOS Security 6.8 May 17, 2024*, Table 1 references a command to enable Core with a note that recommends that Core should not be enabled. To clarify these instructions, Core should remain disabled while in the evaluated configuration. If it has been enabled, run the following command to disable it:

```
ncli cluster edit-hypervisor-securityparams enable-core=false
```

Additionally, the "Built-in Role Management" table on Page 25 contains duplicate entries for the "Storage Admin" and "Storage Viewer" roles. The permissions described are functionally equivalent, however, the permissions listed in Table 3 of this document should be considered the proper reference.

3.1.7 TOE Modes of Operation

The TOE has one mode of operation in the evaluated configuration.

3.2 Exclusions

Please refer to the *Nutanix, Inc. Nutanix Cloud Platform v6.8 Security Target* for a list of features and functionalities that have been scoped out of this Common Criteria evaluation.

©2025 Nutanix, Inc. – Confidential and Proprietary

4. Acronyms

Table 4 defines the acronyms used throughout this document.

Table 4 – Acronyms

Acronym	Definition
AHV	Acropolis Hypervisor
AOS	Acropolis Operating System
API	Application Programming Interface
CVM	Controller Virtual Machine
EAL	Evaluation Assurance Level
GCP	General Purpose Computer
HA	High Availability
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
nCLI	Nutanix Command Line Interface
NTP	Network Time Protocol
REST	Representational State Transfer
SE	System Engineer
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SVM	Service Virtual Machine
TOE	Target of Evaluation
VM	Virtual Machine

©2025 Nutanix, Inc. – Confidential and Proprietary

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com