NUTANIX ACROPOLIS
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

26 January 2026

Developed by Nutanix and DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Nutanix Acropolis STIG provides technical security configuration and assessment controls for the Nutanix hyper-converged infrastructure (HCI) platform and components.

The Nutanix platform is designed to simplify and modernize data center operations. It integrates compute, storage, and networking into a single software-defined solution, eliminating the need for traditional infrastructure. Nutanix clusters consist of multiple nodes, each containing compute, storage, and networking resources. These nodes work together to form a unified pool of resources. This architecture is designed to support hybrid cloud environments, enabling seamless integration with public cloud services while maintaining on-premises control.

Key components of the architecture include:

- The **Acropolis Operating System (AOS)** provides a distributed storage fabric, application mobility, and virtualization capabilities.
- The **Controller Virtual Machine (CVM)** is a virtual storage appliance. CVM holds all Controller VMs and interfaces (i.e., Prism Element web console, nCLI, and SSH). The CVM is responsible for ensuring the efficient operation of the cluster by handling tasks such as resource allocation, data replication, and cluster-wide communication. It operates as a virtual machine on each node within a Nutanix cluster and serves as the control plane for managing and orchestrating the cluster's resources, including storage, compute, and networking.
- **Acropolis Hypervisor (AHV)** is a built-in hypervisor that simplifies virtualization management for enterprise applications. While AHV focuses on virtualization, CVM handles the management and coordination of workloads.
- **Prism Element** is a user interface tool for CVM, providing a configuration interface for management of a single cluster.
- **Prism Central** provides a centralized management interface for monitoring and managing the entire infrastructure, including multiple Nutanix clusters from a single interface. Prism Central does not require a license for basic functionality, but advanced features (e.g., Prism Pro) may require additional licensing.
- **Nutanix Files** is included in the scope of the current STIG but is not a required component for DOD implementation. Files is a software-defined file storage solution that allows the sharing of files in a centralized and protected location to eliminate the requirement for a third-party file server. Files offerings also include File Analytics for statistics and monitoring of file servers, and the Files Manager for a unified control plane of all file servers and the deployment of file servers in Prism Central.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security

requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made based on the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Input into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.

2. ASSESSMENT CONSIDERATIONS

The Nutanix AOS license model can vary based on the needs of the organization. The Nutanix Acropolis STIG assumes the use of AOS, AHV, and Prism Central as components of the base configuration. The assessment must consist of the Nutanix Acropolis Operating System (OS) STIG and the Nutanix Acropolis Application Server (AS) STIG as a minimum security assessment baseline for each Nutanix cluster. Sites with multiple clusters must apply the STIG package and all requirements to each cluster separately.

DOD requires using centralized configuration, monitoring, and management. Prism Central is fully integrated and provides the best management, particularly where multiple clusters are used or in larger, complex enclaves. If Prism Central is not used for this function, the product that provides this function must be included in the security assessment using the applicable STIG, and the Prism Central requirements are not applicable.

The Files server application is included in the scope of this STIG package but is not required. If this application is not used, the Files requirements are not applicable.

Table 2-1: Security Assessment Based on Component

Component	Nutanix Acropolis OS STIG	Nutanix Acropolis AS STIG
AOS	Required	
AHV	Required	Required
Prism Element		Required
Prism Central	Required	Required
Files	Required	Required