DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTB)

25 November 2025

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Nutanix Cloud Infrastructure (NCI) and Nutanix Unified Storage (NUS) with Software Release Versions Acropolis Hypervisor (AHV) 10.3, Acropolis Operating System (AOS) 7.3, and Files 5.2

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Change 2," September 2017
(c) through (d), see Enclosure 1

1. **Certification Authority.** Reference establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Department of Defense Information Network (DoDIN) products, Reference (b).

2. **Conditions of Certification.** The Nutanix Cloud Infrastructure (NCI) and Nutanix Unified Storage (NUS) with Software Release Versions Acropolis Hypervisor (AHV) 10.3, Acropolis Operating System (AOS) 7.3, and Files 5.2, hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (b), as a Data Storage Controller (DSC) and is certified for joint use with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than the expiration date listed in the DoDIN Approved Products List (APL) memorandum.

Table 1. Conditions

Description		**Operational Impact**	**Remarks**
UCR Waivers			
None			
TDR#	**Conditions of Fielding**		
	None		
TDR#	**Open Test Discrepancies**		
NA-1844-001	DAT-000010: Per the Vendor's LoC, the SUT does not support RAID as a fault tolerance measure. The SUT implements Erasure Coding to prevent data loss in the event of disk failures.	None UCR Change Requirement	(See note.)

(Table continues next page.)

Table 1. Conditions (continued)

Description		Operational Impact	Remarks
TDR#	**Open Test Discrepancies** (continued)		
NA-1844-002	DAT-000120: Per the Vendor's LoC, the SUT does not support SMB1. The SUT does support 3.0 CIFS.	None UCR Change Requirement	(See note.)
NA-1844-003	DAT-000420: Per the Vendor's LoC, NIS not supported.	None UCR Change Requirement	(See note.)
NA-1844-004	DAT-000430: Per the Vendor's LoC, NIS Netgroups not supported.	None UCR Change Requirement	(See note.)
NA-1844-005	DAT-000450: Per the Vendor's LoC, iSNS is not supported.	None UCR Change Requirement	(See note.)

NOTE(S): On 22 September 2025, DISA adjudicated interoperability test discrepancies documented in the following TDRs as UCR Change Requirements:

- NA-1844-001 – update to allow method equivalent to RAID.
- NA-1844-002 – modernize outdated SMB1 requirement.
- NA-1844-003 through -005 – change from Required to Conditional.

LEGEND:

CIFS	Common Internet File System	NIS	Network Information Service
DAT	UCR Data Storage Controller requirement	RAID	Redundant Array of Independent Disks
DISA	Defense Information Systems Agency	SMB	Server Message Block
iSNS	internet Storage Name Service	SUT	System Under Test
LoC	Letter of Compliance	TDR	Test Discrepancy Report
NA	Nutanix	UCR	Unified Capabilities Requirements

3. Interoperability Status. Table 2 provides the SUT Interface Status, Table 3 provides the Capability Requirements and Functional Requirements Status, and Table 4 provides a DoDIN APL Product Summary, to include subsequent Desktop Review (DTR) updates.

Table 2. SUT Interface Status

Interface (See note 1.)	**Applicability R/O/C**	**Status**	**Remarks**
Network Attached Storage Interfaces			
IEEE 802.3ab (1000BaseT UTP)	C	Met	
IEEE 802.3ae (10GBaseX)	C	Met	
Storage Array Network Interfaces			
8 Gbps FC	O	Not Tested	See note 2.
16 Gbps FC	O	Not Tested	See note 2.
32 Gbps FC	O	Not Tested	See note 2.
FC physical interfaces and FCP interfaces IAW ANSI X3.230, X3.297, and X3.303	C	Not Tested	See note 2.
Out-of-band Management Interfaces			
10 Mbps Ethernet	C	Met	See note 3.
100 Mbps Ethernet	C	Met	See note 3.
1 Gbps Ethernet	C	Met	

(Table continues next page.)

Table 2. SUT Interface Status (continued)

Interface (See note 1.)	**Applicability R/O/C**	**Status**	**Remarks**
Converged Network Adapter Interfaces			
FCoE services over a 10 GbE physical interface IAW ANSI T11 FC-BB-5 standard for FCoE with a CNA	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qbb for Priority-Based Flow Control	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qaz for Enhanced Transmission Selection	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qaz for Data Center Bridging Exchange Protocol	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qau for Congestion Notification	O	Not Tested	See note 2.

NOTE(S):

1. Table 3 depicts the SUT high-level requirements. Enclosure 3 provides a detailed list of requirements.
2. The SUT does not support this conditional or optional Interface
3. Testing was conducted on the higher data rate interfaces (1 and 10 GbE). JITC analysis determined the lower interface rates are low risk for certification based on the Vendor's LoC with the IEEE 802.3i and 802.3u standards and the test data collected at all other data rates.

LEGEND:

802.3i	10BaseT Mbps Ethernet over Twisted Pair	Gbps	Gigabits per second
802.3u	100BaseT Fast Ethernet, Copper and Fiber	GbE	Gigabit Ethernet
ANSI	American National Standards Institute	IAW	In Accordance With
BaseT	Megabit (Baseband Operation, Twisted Pair) Ethernet	IEEE	Institute of Electrical and Electronics Engineers
BaseX	Megabit Ethernet over Fiber or Copper	JITC	Joint Interoperability Test Command
BB	Backbone	LoC	Letters of Compliance
C	Conditional	Mbps	Megabits per second
CNA	Converged Network Adapter	O	Optional
FC	Fibre Channel	R	Required
FCoE	FC over Ethernet	SUT	System Under Test
FCP	FC Protocol	UTP	Unshielded Twisted Pair
GBaseX	Gigabit Ethernet over Fiber or Copper		

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	**UCR Requirement (High-Level)** (See note 1.)	**UCR 2013 Reference**	**Status**
1	Cybersecurity Requirements (R)	Section 4	Met (See note 2)
2	Data Storage Controller (R)	Section 14	Partially Met (See note 3).
3	IPv6 (R)	Section 5	Met

NOTE(S):

1. The annotation of 'required' refers to a high-level requirement category. Enclosure 3 provides the applicability of each sub-requirement.
2. An NIWC-led CS test team conducted CS testing and published the results in a separate report, Reference (c).
3. The SUT met the requirements with the exceptions noted in Table 1.

LEGEND:

CR	Capability Requirement	NIWC	Naval Information Warfare Center
CS	Cybersecurity	R	Required
FR	Functional Requirement	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements
IPv6	Internet Protocol version 6		

Table 4. DoDIN APL Product Summary

Product Identification			
Product Name	Nutanix Cloud Infrastructure (NCI) and Nutanix Unified Storage (NUS)		
Software Release Version(s)	Acropolis Hypervisor (AHV) 10.3, Acropolis Operating System (AOS) 7.3, and Files 5.2		
UCR Product Type(s)	Data Storage Controller (DSC)		
Product Description	The SUT consists of the Nutanix NX-3060-G9 running NCI with AHV and AOS, and NUS with Files software versions AHV 10.3, AOS 7.3, and Files 5.2, and includes two individual hardware components, a Nutanix NX-3060-G9 appliance serving as the primary cluster and a Nutanix NX-3060-G9 appliance serving as the disaster recovery cluster. Both hardware platforms run identical software versions. The NCI provides enterprise-grade VM-centric storage for virtualized applications and includes the AHV and AOS products. The NUS provides highly available NFS and SMB version 3.0 storage services with the Files product.		
Product Components	**Component Name** (See note.)	**Tested Version**	**Remarks**
NCI and NUS	**NX-3060-G9 Primary Cluster** NX-1065-G9 NX-1175S-G9 NX-3035-G9 NX-3060-G9 NX-3155-G9 NX-8155-G9 NX-8155A-G9 NX-8170-G9 NX-9151-G9	NA	Hardware appliance hosting software
	NX-3060-G9 DR Cluster NX-1065-G9 NX-1175S-G9 NX-3035-G9 NX-3060-G9 NX-3155-G9 NX-8155-G9 NX-8155A-G9 NX-8170-G9 NX-9151-G9	NA	Hardware appliance hosting software.
	AHV	**10.3**	Hypervisor on Rocky Linux 8
	AOS	**7.3**	OS on VM
	Files	**5.2**	File server on VM

NOTE(S): NIWC tested the bolded and underlined components. The other components in the product series were not tested; however, JITC certified the other components for joint use because they utilize the same software and similar hardware as tested and certified components and analysis determined they were functionally identical for interoperability certification purposes.

LEGEND:

AHV	Acropolis Hypervisor	NFS	Network File System
AOS	Acropolis Operating System	NIWC	Naval Information Warfare Center
APL	Approved Products List	NUS	Nutanix Unified Storage
DoDIN	Department of Defense Information Network	OS	Operating System
DR	Disaster Recovery	SMB	Server Message Block
DSC	Data Storage Controller	SUT	System Under Test
JITC	Joint Interoperability Test Command	UCR	Unified Capabilities Requirements
NA	Not Applicable	VM	Virtual Machine
NCI	Nutanix Cloud Infrastructure		

4. **Test Details.** This certification is based on interoperability (IO) testing, review of the Vendor’s Letter of Compliance (LoC), DISA adjudication of open test discrepancy reports (TDRs), and the DISA Certifying Authority Recommendation for inclusion on the DoDIN APL. The test team at the Assured Real-Time Communications Lab at the Naval Information Warfare Center (NIWC), Norfolk, Virginia completed review of the Vendor’s LoC on 2 September 2025 and conducted IO testing from 8 September to 12 September 2025, using test procedures derived

from Reference (d). DISA adjudicated outstanding TDRs on 22 September 2025. A NIWC-led Cybersecurity (CS) test team conducted CS testing and published the results in a separate report, Reference (c). Enclosure 2 documents the test results and describes the test network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Sensitive but Unclassified Internet Protocol Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.jitc.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Industry Toolkit (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the CS Assessment Package that contains the approved configuration and deployment guide must be requested directly from the Approved Products Certification Office (APCO) via e-mail: disa.meade.peo-transport.list.approved-products-certification-of@mail.mil. All associated information is available on the DISA APCO website located at https://aplits.disa.mil/.

6. Point of Contact (POC). NIWC testing POC: Mrs. Alexandra Helfrich; Phone: (757) 675-5180; E-mail: alexandra.e.helfrich.civ@us.navy.mil. JITC certification POC: Mr. Edward Mellon; Phone: (667) 890-5056; E-mail: edward.a.mellon.civ@mail.mil; Mailing Address: Joint Interoperability Test Command, ATTN: JTB - Mr. Edward Mellon, 6910 Cooper Avenue, Fort Meade, MD 20755-7085. The APCO tracking number for the SUT is 2429001.

FOR THE COMMANDER:

DORN.LAWRENCE.T.1168371930
Digitally signed by DORN.LAWRENCE.T.1168371930
Date: 2025.11.25 09:53:03 -07'00'

3 Enclosures a/s

LAWRENCE T. DORN
Chief
Force Support and Logistics Division

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
ISG Secretariat, DISA, JT
U.S. Strategic Command, J66
USSOCOM J65
USTRANSCOM J6
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6, SAIS-CBC
US Air Force, SAF/A6SA
US Marine Corps, MARCORSYSCOM, SEAL, CERT Division
US Coast Guard, CG-64
DISA/ISG REP
OUSD Intel, IS&A/Enterprise Programs of Record
DLA, Test Directorate, J621C
NSA/DT
NGA, Compliance and Assessment Team
DOT&E
Medical Health Systems, JMIS PEO T&IVV
HQUSAISEC, AMSEL-IE-ME
APCO

ADDITIONAL REFERENCES

(c) Naval Information Warfare Center, "Cybersecurity Assessment Report for Nutanix Cloud Infrastructure (NCI) and Nutanix Unified Storage (NUS), Software Release AHV: 10.3, AOS: 7.3, Files: 5.2, Tracking Number (TN) 2429001," October 2025

(d) JITC, "Data Storage Controller (DSC) Test Procedures Version 1.2 For Unified Capabilities Requirements (UCR) 2013 Change 2," April 2022 (Draft)

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Nutanix Cloud Infrastructure (NCI) and Nutanix Unified Storage (NUS) with Software Release Versions Acropolis Hypervisor (AHV) 10.3, Acropolis Operating System (AOS) 7.3, and Files 5.2 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	None
Sponsor Point of Contact	None
Vendor Point of Contact	TJ Dehaven, Email: tjdehaven@tachyondynamics.com; Phone: 757-477-4064
System Name	Nutanix Cloud Infrastructure and Nutanix Unified Storage
Software Release Version(s)	AHV 10.3, AOS 7.3, and Files 5.2
Product Category	Data Storage Controller
System Background	
Previous certifications	1833801
Tracking	
APCO Tracking Number	2429001
System Tracking Program ID	System 8467
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Change 2, Sections 5 and 14
Remarks	None
Test Organization(s)	Naval Information Warfare Center, Norfolk, Virginia

LEGEND:

AHV	Acropolis Hypervisor	APCO	Approved Products Certification Office
AOS	Acropolis Operating System	ID	Identification

2. SYSTEM DESCRIPTION. A Data Storage Controller (DSC) is a specialized multiprotocol computer system with an attached disk array that serves in the role of a disk array controller and end node in Base/Post/Camp/Station (B/P/C/S) networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services Local Area Network (ASLAN); however, the DSC is not considered part of the ASLAN.

The SUT is a DSC. The SUT consists of the Nutanix NX-3060-G9 running NCI with AHV and AOS, and NUS with Files, software versions AHV 10.3, AOS 7.3, and Files 5.2. The SUT includes two individual hardware components, a Nutanix NX-3060-G9 appliance serving as the primary cluster and a Nutanix NX-3060-G9 appliance serving as the disaster recovery (DR) cluster. Both hardware platforms run identical software versions.

Nutanix NX-3060-G9 Primary Cluster. Hardware appliance hosting software, serving as the primary cluster.

Nutanix NX 3060-G9 DR Cluster. Hardware appliance hosting software, serving as the DR cluster.

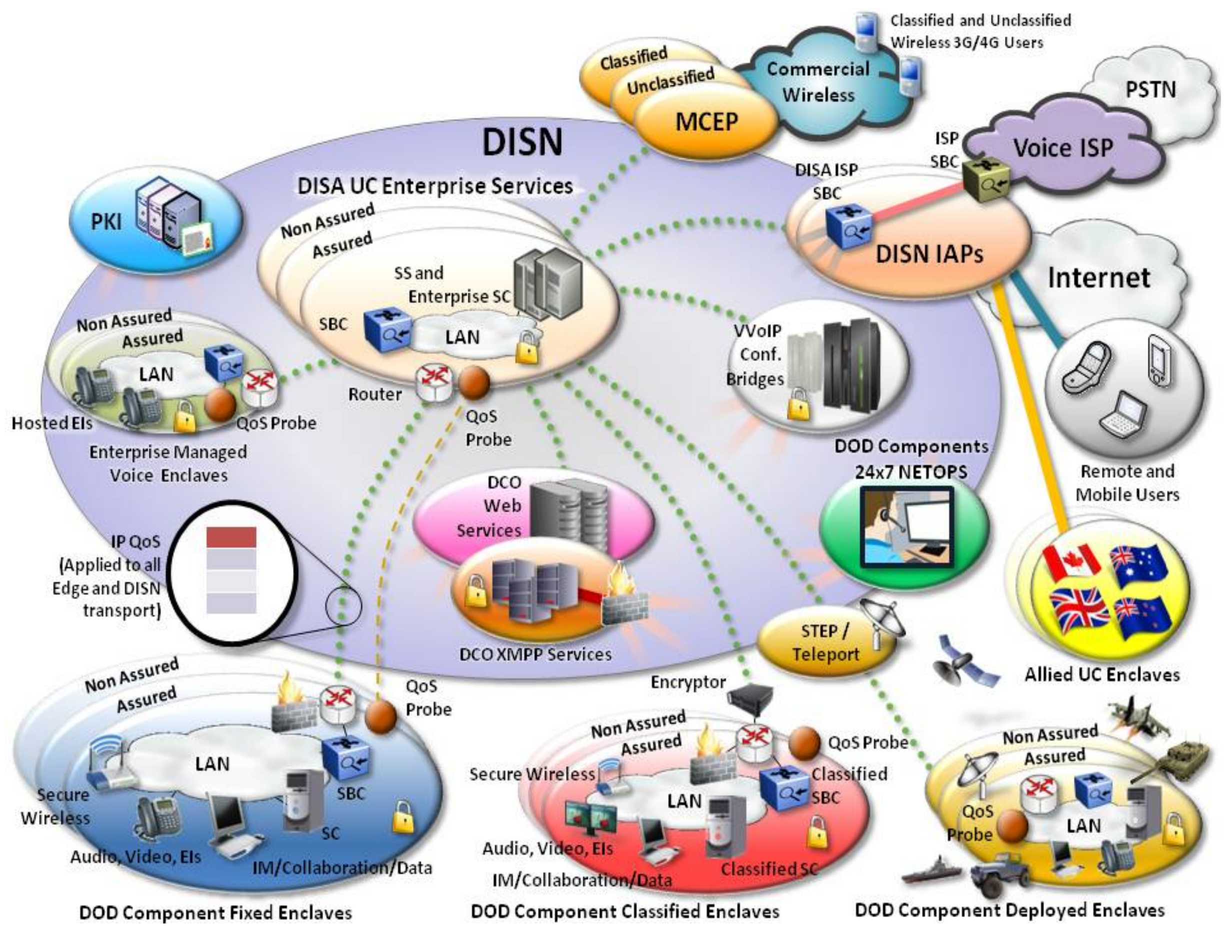
Nutanix AHV. The Nutanix AHV is a modern and secure virtualization platform that powers virtual machines (VMs) and containers for applications and cloud-native workloads on-premises and in public clouds. The AHV runs as hypervisor installed directly on bare metal.

Nutanix AOS. The Nutanix AOS provides the core functionality leveraged by workloads and services running on the platform. The AOS is a back-end service that allows for workload and resource management, provisioning, and operations. Its goal is to abstract the facilitating resource (e.g., hypervisor, on-premises, cloud, etc.) from the workloads running, while providing a single "platform" to operate. This gives workloads the ability to seamlessly move between hypervisors, cloud providers, and platforms. The AOS runs as a VM referred to as the Controller Virtual Machine (CVM), on top of the AHV hypervisor.

Nutanix Files. The Nutanix Files is a software-defined, scale-out file storage solution that provides a repository for unstructured data, such as home directories, user profiles, departmental shares, application logs, backups, and archives. Unlike standalone Network Attached Storage (NAS) appliances, the Files solution consolidates VM and file storage, eliminating the need to create an infrastructure silo. Integration with Active Directory enables support for quotas and access-based enumeration (ABE), as well as self-service restores with the Windows previous version feature. The Nutanix Files also supports native remote replication and file server cloning, which allows back up Files off-site and runs antivirus scans and machine learning without affecting production. The Files runs as a set of three VMs referred to as File Server Virtual Machines (FSVM), on top of the AHV hypervisor.

3. OPERATIONAL ARCHITECTURE. The Department of Defense (DoD) Information Network (DoDIN) architecture is a two- level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The DoD Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine the type of switch allowable at a particular location. The DoDIN architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational DoDIN architecture in which the SUT may be used. Figure 2-2 depicts the DSC functional model.

4. TEST CONFIGURATION. The Naval Information Warfare Center (NIWC) test team tested the SUT at the Assured Real-Time Communications Lab at the NIWC, Norfolk, Virginia, in a manner and configuration similar to that of the notional operational environment depicted in Figure 2-1. The test team tested the SUT's required functions and features using the test configuration depicted in Figure 2-2. Cybersecurity (CS) testing used the same configuration.

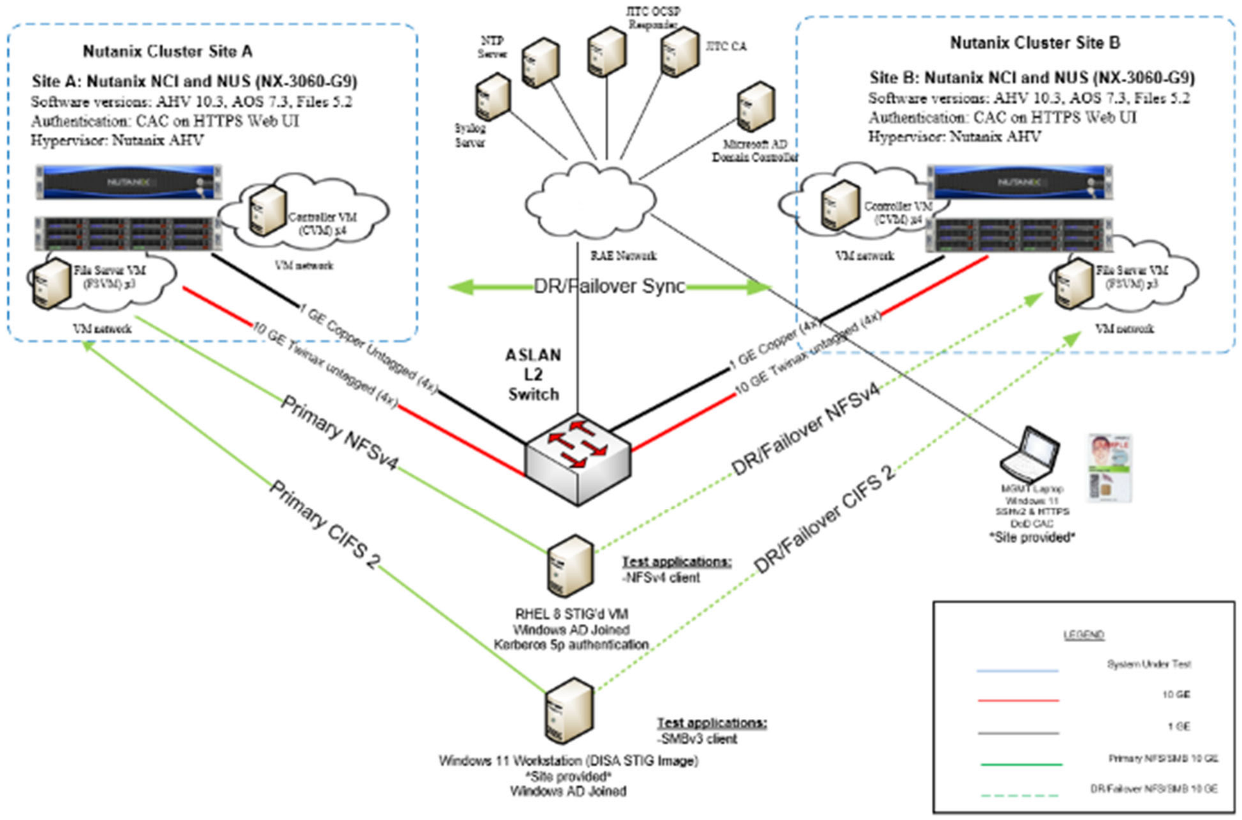


LEGEND:

ASLAN	Assured Services Local Area Network
AS-SIP	Assured Services Session Initiation Protocol
DCO	Defense Connection Online
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	Department of Defense Information Technology Standards Registry
EBC	Edge Boundary Controller
EI	End Instrument
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
LSC	Local Session Controller
MFSS	Multifunction Softswitch
NETOPS	Network Operations
PKI	Public Key Infrastructure
QoS	Quality of Service
SBC	Session Border Controller
SRTP	Secure Real-Time Transport Protocol
SS	Softswitch
SSL	Secure Socket Layer
TLS	Transport Layer Security
UC	Unified Capabilities
VLAN	Virtual Local Area Network
VVoIP	Voice and Video over IP
XMPP	Extensible Messaging and Presence Protocol

Figure 2-1. Notional DoDIN Network Architecture

Nutanix Cloud Infrastructure (NCI) with Acropolis Hypervisor (AHV) and Acropolis Operating System (AOS), and Nutanix Unified Storage (NUS) with Files
Data Storage Controller (DSC), Version AHV 10.3, AOS 7.3, Files 5.2



LEGEND:

AD	Active Directory	MGMT	Management
AHV	Acropolis Hypervisor	NCI	Nutanix Cloud Infrastructure
AOS	Acropolis Operating System	NFS	Network File System
ASLAN	Assured Services Local Area Network	NTP	Network Time Protocol
CA	Certifying Authority	NUS	Nutanix Unified Storage
CAC	Common Access Card	OCSP	Online Certificate Status Protocol
CIFS	Common Internet File System	RAE	Required Ancillary Equipment
CVM	Controller Virtual Machine	RHEL	Red Hat Enterprise Linux
DISA	Defense Information Systems Agency	SMB	Server Message Block
DR	Disaster Recovery	STIG	Security Technical Implementation Guide
DSC	Data Storage Controller	SSH	Secure Shell version 2
FSVM	File Server Virtual Machine	Syslog	System Log
GE	Gigabit Ethernet	UI	User Interface
HTTPS	Hypertext Transfer Protocol Secure	v	Version
JITC	Joint Interoperability Test Command	VM	Virtual Machine
L2	Layer 2		

Figure 2-2. SUT Test Configuration

5. METHODOLOGY. NIWC conducted testing of the SUT in accordance with (IAW) DSC requirements derived from the Unified Capabilities Requirements (UCR) 2013, Change 2, Reference (b), and using DSC test procedures derived from Reference (d). Any discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor Plan of Action and Milestones (POA&M), which will address all new critical Test Discrepancy Reports (TDRs) within 120 days of identification.

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The UCR 2013, Change 2, Sections 5 and 14 establish the interface, Capability Requirements (CRs) and Functional Requirements (FRs), CS, and other requirements for DSCs. Table 3-1 provides the SUT interface interoperability status, and Table 3-2 provides the CR and FR status. The subparagraphs below provide the testing details and results. Optional and/or conditional requirements are not included in the test results unless otherwise noted.

a. Interface Status. The NIWC testing interface status of the SUT is provided in Table 3-1. The DSC shall provide physical interfaces for, at a minimum, 1 Gigabit Ethernet (GbE) and 10 GbE in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet Local Area Network (LAN) interfaces. The SUT met the 1GbE and 10 GbE Ethernet LAN interface requirements with testing. The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Megabit per second (Mbps) Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), Hyper Text Transfer Protocol Secure (HTTPS), and Simple Network Management Protocol (SNMP) version 3; and the protocols shall be secured in accordance with Section 4, Information Assurance. The SUT met the OOBM interface requirements with testing. The system may optionally provide Fiber Channel (FC) physical interfaces and FC Protocol (FCP) interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT does not support the optional FC physical and FCP interface requirements. The system may optionally provide physical interfaces for FC over Ethernet (FCoE) services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT does not support the optional CNA interface requirements.

b. Capability and Functional Requirements and Status.

1) The UCR 2013, Section 14.2 includes the Storage System requirements in the subparagraphs below.

a) The system shall provide a Redundant Array of Independent Disks (RAID) for multiple disk drives. The system shall provide a configuration option to select the specific RAID level to be provisioned in the disk array. The RAID levels available for use shall be subject to the specific vendor implementation. At a minimum, the RAID level shall be dual parity RAID-6 for Serial Advanced Technology Attachment (SATA) drives and RAID-5 for Serial Attached Small Computer Systems Interface (SCSI) and FC drives, although stronger RAID levels are acceptable. The SUT does not support RAID as a fault tolerance measure. The SUT implements

Erasure Coding to prevent data loss in the event of disk failures. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-001).

b) The system shall be capable of 99.9 percent availability. The SUT met this requirement with the Vendor's LoC.

c) The system shall provide a management control function for low-level system monitoring and control functions, interface functions, and remote management. The management control function shall provide an Ethernet physical interface(s) for connection to the owner's (i.e., MILDEP) management network/LAN and provide status. The monitoring shall include an initial system check, system cooling fans, temperatures, power supplies, voltages, and system power state tracking and logging. The SUT met this requirement with the Vendor's LoC.

d) The system shall provide data storage replication (e.g., mirroring) services [Internet protocol (IP) version 4 (IPv4) and version 6 (IPv6)] between systems that are configured as source and destination replication pairs. The replication operations shall provide capabilities for data backup replication, system replication and migration, and system disaster recovery (DR) services in support of continuity of operations (COOP) planning. The SUT met this requirement with testing and the Vendor's LoC.

e) When the system interfaces to an Integrated Data Protection (IDP) service and the IDP makes copies of data storage information on to another DSC for periodic data storage backup, DR/COOP, migration, and data archiving operation, the system replication service shall complete the replication regardless of the host connection protocols used between the application servers and the DSC. The SUT met this requirement with testing and the Vendor's LoC.

f) The system replication and migration services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for migrating data storage information. The SUT met this requirement with testing and the Vendor's LoC.

g) The system DR services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for DR/COOP. The SUT met this requirement with testing and the Vendor's LoC.

h) The system shall provide configurable modes for replication (mirroring) operations between the source DSC and the destination DSC. During replication, both the source and the destination must be in a known good state. The configurable modes shall be Asynchronous or Synchronous and are depicted in UCR 2013, Change 1, Table 14.2-1, Replication Operation Modes. The SUT met this requirement with testing and the Vendor's LoC.

2) The UCR 2013, Section 14.3 includes the Storage Protocol requirements in the subparagraphs below.

a) The system shall provide a Network File System version 3 (NFSv3) server for file systems data input/output (I/O). The SUT met this requirement with testing and the Vendor's LoC.

b) The system shall provide a NFS version 4 (NFSv4) server for file systems data I/O. The SUT met this requirement with testing and the Vendor's LoC.

c) The system shall provide a NFS version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O. The SUT does not support this optional NFSv4.1 requirement.

d) The system shall provide a CIFS version 1.0 (CIFSv1.0) server for file systems data I/O. The SUT does not support CIFS/SMB1. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-002).

e) The system shall provide a CIFS version 2.0 (CIFSv2.0) server for file systems data I/O. The SUT met this requirement with testing and the Vendor's LoC.

f) The system shall provide Internet Small Computer Systems Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators). The SUT met this optional requirement with testing and the Vendor's LoC.

g) The system shall provide FCP server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT does not support this optional FCP requirement.

h) The system shall provide FCoE server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT does not support this optional FCoE requirement.

i) The system shall provide a HTTPS server for file system data I/O and management access to the storage controller operating system. The session shall be secured with SSL or Transport Layer Security (TLS), per Internet Engineering Task Force (IETF) Request for Comment (RFC) 5246, and shall comply with Section 4, Cybersecurity, for that protocol. The SUT met this requirement with the Vendor's LoC.

j) The system shall provide SSHv2 or TLS for management access to the storage controller operating system. The SSHv2 or TLS implementation shall comply with Section 4, Cybersecurity, for that protocol. The SUT met this requirement with testing and the Vendor's LoC.

k) The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures. The SUT does not support this optional WebDAV requirement.

l) The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures. The SUT met this optional requirement with testing and the Vendor's LoC.

m) The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard. The SUT does not support this optional SNIA/CDMI requirement.

n) The system shall provide Global Name Space (GNS) or single name space functionality. The GNS functionality shall provide the capability to aggregate disparate and remote network-based file systems to provide a consolidated view to reduce complexities of localized file management and administration. The GNS functionality shall provide large (i.e., 14 Petabyte [PB] or greater) working pools of disks, transparent data migration, and it shall serve to reduce the number of storage mount points and shares. Each system shall have a dedicated and unique GNS. The SUT met this requirement with testing and the Vendor's LoC.

3) The UCR 2013, Section 14.4 includes the Network Attached Storage Interface requirements in the subparagraphs below.

a) The system shall provide physical interfaces for GbE and 10 GbE services in conformance with IEEE 802.3 for Ethernet LAN interfaces. The SUT met this conditional requirement with testing and the Vendor's LoC.

b) The system shall be able to provision, monitor, and detect faults, and to restore Ethernet services in an automated fashion. The SUT met this conditional requirement with the Vendor's LoC.

c) The system shall provide physical interfaces for OOBM access and services with 10/100 Mbps Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, SSL, HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Cybersecurity. The SUT met this conditional requirement with testing and the Vendor's LoC. A NIWC-led CS test team conducted CS testing and published the results in a separate report, Reference (c).

d) When the system uses Ethernet, Fast Ethernet, GbE, and 10GbE interfaces, the interfaces shall be autosensing, auto-detecting, and auto-configuring with incoming and corresponding Ethernet link negotiation signals. Autosensing, auto-detecting, and auto-configuring only applies to interfaces below 10GbE interfaces. The SUT met this conditional requirement with the Vendor's LoC.

e) Ethernet services of the system and the Logical Link Interworking Function (IWF) of the system shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEEE 802.3. The SUT met this conditional requirement with the Vendor's LoC.

f) Ethernet services of the system shall support jumbo frames with a configurable Maximum Transmission Unit (MTU) of 9000 bytes or greater, excluding Ethernet encapsulation. When Ethernet encapsulation is included in the frame size calculation, an additional 22 bytes must be included for the MAC header (14 bytes), the Virtual LAN (VLAN) tag (4 bytes), and the Cyclical Redundancy Check (CRC) Checksum (4 bytes) fields in the Ethernet frame, resulting in a maximum of 9022 bytes or greater. The system shall also support a configurable MTU between 1280 bytes and 1540 bytes to ensure packets can transit type 1 encryptors. The system default MTU shall be 1540 bytes. The SUT met this conditional requirement with the Vendor's LoC.

g) Ethernet services of the system shall allocate a unique Ethernet MAC address to each Ethernet interface associated with a VLAN, as per IEEE 802.1Q. The SUT met this conditional requirement with the Vendor's LoC.

h) Ethernet services of the system shall support "Link Aggregation," as per IEEE 802.3ad or IEEE 802.1AX-2008 and use with the Link Aggregation Control Protocol. The SUT met this conditional requirement with the Vendor's LoC.

i) Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB. The SUT met this optional requirement with the Vendor's LoC.

4) The UCR 2013, Section 14.5, states the system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT does not support this optional FC physical and FCP interface requirement.

5) The UCR 2013, Section 14.6 includes the Converged Network Adapter Interface requirements in the subparagraphs below.

a) The system shall provide physical interfaces for FCoE services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT does not support this optional FCoE requirement.

b) The system shall provide physical interfaces for Data Center Bridging [DCB, also known as Converged Enhanced Ethernet (CEE)] features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging. The SUT does not support this optional DCB requirement.

6) The UCR 2013, Section 14.7 includes the IP Networking requirements in the subparagraphs below.

a) The system shall meet the IPv6 requirements defined in Section 5.2.2, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance. The SUT met this requirement with the Vendor's LoC.

b) The system shall provide statically provisioned, or dynamically adjusted large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. The receive buffers may be statically provisioned or the operating system of the system may dynamically self-adjust the packet receive buffer size based on measurements of the E2E path bandwidth, Maximum Segment Size (MSS), Round Trip Time (RTT), and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 KB per replication (mirroring) session. The system shall provide a statically provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8192 KB per replication (mirroring) session. The SUT met this requirement with the Vendor's LoC.

c) The system shall provide an optimized congestion control (congestion avoidance) algorithm in Transmission Control Protocol (TCP) for avoidance of traffic loss on communications paths in high-speed networks with high latency or large bandwidth-delay products. The SUT met this requirement with the Vendor's LoC.

7) The UCR 2013, Section 14.8 includes the Name Services requirements in the subparagraphs below.

a) The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510. The SUT met this requirement with testing and the Vendor's LoC.

b) The system shall provide Kerberos authentication service per IETF RFC 4120. The SUT met this requirement with testing and the Vendor's LoC.

c) The system shall provide Domain Name System (DNS) client functionality. The SUT met this requirement with testing and the Vendor's LoC.

d) The system shall provide DNS client-side Load Balancing. The SUT met this requirement with testing and the Vendor's LoC.

e) The system shall provide Network Information Service (NIS) client directory service functionality. The SUT does not support NIS. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-003).

f) The system shall provide NIS Netgroups client directory service functionality. The SUT does not support NIS Netgroups. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-004).

g) The system shall provide Network Basic Input/Output System The over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS). The SUT met this optional requirement with the Vendor's LoC.

h) The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171. The SUT does not support external iSCSI capabilities, and thus does not support iSNS client. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-005).

i) If the system has a FC interface, then the system shall provide FC Name and Zone Service. The SUT does not support this conditional FC interface requirement.

8) The UCR 2013, Section 14.9 includes the Security Services requirements in the subparagraphs below.

A NIWC-led CS test team conducted CS testing for the Security Services requirements listed below and published the results in a separate report, Reference (c).

a) The system shall provide IPSec per RFC 4301.

b) The system shall provide Encapsulating Security Payload (ESP) per RFC 4303.

c) The system shall provide Internet Key Exchange version 2 (IKEv2) per RFC 4306.

d) The system shall provide a configurable Packet Filter (Firewall) service to block unauthorized access (for intrusion prevention) while permitting authorized communications. The Packet Filter service shall use a "stateless" design that does not degrade performance and shall filter all packets received based on interface, source IP address, protocol, port, Type of Service (TOS), or Time To Live (TTL). The Packet Filter service shall provide a configuration policy for defining combinations of multiple packet match rules and processing actions.

e) The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with Federal Information Processing Standard (FIPS) 140-2 level 1 or higher to provide the following capabilities:

1. Rapid crypto shredding (destruction) of data, in accordance with National Institute of Standards and Technology 800-88, for tactical systems that operate in harm's way and may fall into enemy hands.

2. Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place.

f) The system shall comply with all appropriate STIGs to include the Database Security Technical Implementation Guide.

9) The UCR 2013, Section 14.10, states the system shall provide an Application Programming Interface (API) to enable interaction with other software and systems. The interactions shall include routines, data structures, object classes, and protocols used to communicate between the consumer and implementer of the API. The API protocol and message format (e.g., Extensible Markup Language [XML]) shall be subject to the specific vendor system operating system implementation. The SUT met this requirement with the Vendor's LoC.

10) The UCR 2013, Section 14.11 includes the Class of Service and Quality of Service requirements in the subparagraphs below.

a) The system shall provide Class of Service (CoS) and Quality of Service (QoS) marking on egress traffic at layer 2 per IEEE 802.1p and, Section 7.2.1.3, Class of Service Markings, and Section 7.2.1.4, Virtual LAN Capabilities. Traffic classification and marking must occur before the egress transmission of the Ethernet frame with a rule or policy engine that matches on various storage and management protocol types as offered by the system. The SUT does not support this optional COS at layer 2 requirement.

b) The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 6, Network Infrastructure End-to-End Performance. Traffic classification and marking must occur before the egress transmission of the IP packet with a rule or policy engine that matches on various storage and management protocols that occur within the system, such as those listed in Table 14.11-1. The IP packets are marked in the TOS field of the IPv6 packet header with Differentiated Services Code Point (DSCP) values from 0 and 63, inclusive. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements. The SUT met this requirement with the Vendor's LoC.

11) The UCR 2013, Section 14.12 includes the Virtualization requirements in the subparagraphs below.

a) The system shall provide virtualized Data Storage Controller (vDSC) functionality and individual protocol server processes. The vDSC shall meet all the requirements of a DSC with minor exceptions that are related to design and technical limitations associated with the complete virtualization of an operating system, which include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations. The SUT does not support this optional vDSC requirement.

b) The vDSC capability within the system shall provide secure, Private Networking Domains (PNDs) for Ethernet, VLANs, and IP that isolate the network domains of system units. The PND shall support the use of duplicate IP addresses and IP subnet address ranges among those of any other configured vDSC in the system. The PND shall provide a dedicated IP Forwarding Information Base (FIB) per vDSC. The SUT does not support this optional vDSC requirement.

c) The vDSC shall provide an individual Command Line Interface (CLI) context with the full command set of the system, with the scope of the commands limited to the individual vDSC CLI context. The SUT does not support this optional vDSC requirement.

d) The vDSC shall provide a programmatic API with the full command set of the system with the scope of the API commands limited to the individual vDSC context. The SUT does not support this optional vDSC requirement.

e) The vDSC capability within the system shall provide an individual GNS unique from the system or shall provide a single name space that provides the capability to aggregate disparate hardware and storage architectures into a single file system. The GNS shall provide the capability to aggregate disparate and remote network-based file systems, providing a consolidated view to reduce complexities of localized file management and administration. The GNS shall provide large working pools of disks and transparent data migration and shall serve to reduce the number of storage mount points and shares. The single name space shall be spread across multiple physical network access server heads all representing the same file system without replication. The single name space shall include the ability to tier data automatically within the same file system. The SUT does not support this optional vDSC requirement.

7. HARDWARE/SOFTWARE/FIRMWARE VERSION IDENTIFICATION. Table 3-3 provides the SUT components' hardware, software, and firmware tested. NIWC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

8. TESTING LIMITATIONS. None

9. CONCLUSION(S). The SUT meets the critical interoperability requirements for a DSC IAW the UCR, Reference (b), and is certified for joint use with other products listed on the DoDIN Approved Products List (APL). The SUT is certified for use with the interfaces listed in Table 3-1.

DATA TABLES

Table 3-1. SUT Interface Status

Interface (See note 1.)	**Applicability** **R/O/C**	**Status**	**Remarks**
Network Attached Storage Interfaces			
IEEE 802.3ab (1000BaseT UTP)	C	Met	
IEEE 802.3ae (10GBaseX)	C	Met	
Storage Array Network Interfaces			
8 Gbps FC	O	Not Tested	See note 2.
16 Gbps FC	O	Not Tested	See note 2.
32 Gbps FC	O	Not Tested	See note 2.
FC physical interfaces and FCP interfaces IAW ANSI X3.230, X3.297, and X3.303	C	Not Tested	See note 2.
Out-of-band Management Interfaces			
10 Mbps Ethernet	C	Met	See note 3.
100 Mbps Ethernet	C	Met	See note 3.
1 Gbps Ethernet	C	Met	
Converged Network Adapter Interfaces			
FCoE services over a 10 GbE physical interface IAW ANSI T11 FC-BB-5 standard for FCoE with a CNA	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qbb for Priority-Based Flow Control	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qaz for Enhanced Transmission Selection	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qaz for Data Center Bridging Exchange Protocol	O	Not Tested	See note 2.
Data Center Bridging, also known as Converged Enhanced Ethernet, features IAW IEEE 802.1Qau for Congestion Notification	O	Not Tested	See note 2.

NOTE(S):

1. Table 3 depicts the SUT high-level requirements. Enclosure 3 provides a detailed list of requirements.
2. The SUT does not support this conditional or optional Interface
3. Testing was conducted on the higher data rate interfaces (1 and 10 GbE). JITC analysis determined the lower interface rates are low risk for certification based on the Vendor's LoC with the IEEE 802.3i and 802.3u standards and the test data collected at all other data rates.

LEGEND:

802.3i	10BaseT Mbps Ethernet over Twisted Pair	Gbps	Gigabits per second
802.3u	100BaseT Fast Ethernet, Copper and Fiber	GbE	Gigabit Ethernet
ANSI	American National Standards Institute	IAW	In Accordance With
BaseT	Megabit (Baseband Operation, Twisted Pair) Ethernet	IEEE	Institute of Electrical and Electronics Engineers
BB	Backbone	JITC	Joint Interoperability Test Command
C	Conditional	LoC	Letters of Compliance
CNA	Converged Network Adapter	Mbps	Megabits per second
FC	Fibre Channel	O	Optional
FCoE	FC over Ethernet	R	Required
FCP	FC Protocol	SUT	System Under Test
GBaseX	Gigabit Ethernet over Fiber or Copper	UTP	Unshielded Twisted Pair

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Change 2 Reference	Status
1	**Cybersecurity (CS) (R)**	4	See note 2.
2	**Data Storage Controller (DSC) (R)**		
	Storage System (R)	14.2	Partially Met (See note 3.)
	Storage Protocol (R)	14.3	Partially Met (See note 4.)
	Network Attached Storage Interface (R)	14.4	Met
	Storage Array Network Interface (O)	14.5	Not Tested (See note 5.)
	Converged Network Adapter Interface (O)	14.6	Not Tested (See note 5.)
	IP Networking (R)	14.7	Met
	Name Services (R)	14.8	Partially Met (See note 6.)
	Security Services (R)	14.9	Met (See note 2.)
	Interoperability (R)	14.10	Met
	Class of Service and Quality of Service (R)	14.11	Met
	Virtualization (O)	14.12	Not Tested (See note 7.)
3	Internet Protocol version 6 (IPv6) (R)	5	Met

NOTE(S):

1. The annotation of ‘required’ refers to a high-level requirement category. The UCR 2013, Change 2, Reference (b), provides additional information on the applicability of each sub-requirement.
2. A NIWC-led CS test team conducted CS testing and published the results in a separate report, Reference (c).
3. The SUT met the Storage System requirements with the following exception: The SUT does not support RAID as a fault tolerance measure. The SUT implements Erasure Coding to prevent data loss in the event of disk failures. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-001).
4. The SUT met the Storage Protocol requirements with the following exception: The SUT does not support CIFS/SMB1. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-002).
5. The SUT does not support this optional requirement.
6. The SUT met the Name Services requirements with the following exceptions:
   - The SUT does not support NIS. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-003).
   - The SUT does not support NIS Netgroups. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-004).
   - The SUT does not support external iSCSI capabilities and thus does not support iSNS client. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 (TDR NA-1844-005).
7. The SUT does not support the optional vDSC requirement.

LEGEND:

CIFS	Common Internet File System	NIWC	Naval Information Warfare Center
CR	Capability Requirement	O	Optional
CS	Cybersecurity	R	Required
DISA	Defense Information Systems Agency	RAID	Redundant Array of Independent Disks
FR	Functional Requirement	SMB	Server Message Block
ID	Identification	SUT	System Under Test
IP	Internet Protocol	TDR	Test Discrepancy Report
iSCSI	Internet Small Computer Systems Interface	UCR	Unified Capabilities Requirements
iSNS	Internet Storage Name Service	v	version
NA	TDR acronym for Nutanix	vDSC	virtualized Data Storage Controller
NIS	Network Information Service		

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Component (See note.)	Release	Sub-component	Function
NX-3060-G9 Primary Cluster NX-1065-G9 NX-1175S-G9 NX-3035-G9 NX-3060-G9 NX-3155-G9 NX-8155-G9 NX-8155A-G9 NX-8170-G9 NX-9151-G9	NA	NA	Hardware appliance hosting software serving as the primary cluster.
NX-3060-G9 DR Cluster NX-1065-G9 NX-1175S-G9 NX-3035-G9 NX-3060-G9 NX-3155-G9 NX-8155-G9 NX-8155A-G9 NX-8170-G9 NX-9151-G9			Hardware appliance hosting software serving as the disaster recovery cluster.
AHV	**10.3**		Modern and secure virtualization platform that powers VMs and containers for applications and cloud-native workloads on-premises and in public clouds. The AHV runs as hypervisor installed directly on bare metal
AOS	**7.3**		Provides the core functionality leveraged by workloads and services running on the platform. The AOS is a back-end service that allows for workload and resource management, provisioning, and operations. Its goal is to abstract the facilitating resource (e.g., hypervisor, on-premises, cloud, etc.) from the workloads running, while providing a single “platform” to operate. This gives workloads the ability to seamlessly move between hypervisors, cloud providers, and platforms. The AOS runs as a VM referred to as the Controller Virtual Machine (CVM), on top of the AHV hypervisor
Files	**5.2**		Software-defined, scale-out file storage solution that provides a repository for unstructured data, such as home directories, user profiles, departmental shares, application logs, backups, and archives. Unlike standalone NAS appliances, the Files solution consolidates VM and file storage, eliminating the need to create an infrastructure silo. Integration with AD enables support for quotas and ABE, as well as self-service restores with the Windows previous version feature. The Nutanix Files also supports native remote replication and file server cloning, which allows back up Files off-site and runs antivirus scans and machine learning without affecting production. The Files runs as a set of three VMs (referred to as FSVMs), on top of the AHV hypervisor.

NOTE(S): NIWC tested the components bolded and underlined. The other components in the family series were not tested; however, JITC certified the other components for joint use because they utilize the same software and similar hardware as tested components and analysis determined they were functionally identical for interoperability certification purposes.

LEGEND:

ABE	Access-based Enumeration	FSVM	Files Server Virtual Machine
AD	Active Directory	JITC	Joint Interoperability Test Command
AHV	Acropolis Hypervisor	NAS	Network Attached Storage
AOS	Acropolis Operating System	NIWC	Naval Information Warfare Center
CVM	Controller Virtual Machine	SUT	System Under Test
DR	Disaster Recovery	VM	Virtual Machine

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

System Name	Software Release	Function
Required Ancillary Equipment		
JITC CA		
JITC OCSP Responder		
Syslog Server		
NTP Server		
ADDS		
SSH Client		
Test Network Components		
Management Laptop (site-provided)	Windows 11	Domain Joined workstation for SMB testing.
Server	RHEL 8	Domain Joined server for NFS testing.
Cisco 9300 (ASLAN Switch)	IOS XE 16.09.06	Maintains data traffic between devices.

LEGEND:

ADDS	Active Directory Domain Services
ASLAN	Assured Services Local Area Network
CA	Certifying Authority
JITC	Joint Interoperability Test Command
NFS	Network File System
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
RHEL	Red Hat Enterprise Linux
SMB	Server Message Block
SSH	Secure Shell
Syslog	System Log