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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) 11 May 2023

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Dell PowerScale OneFS with Software Release 9.5

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 (a) 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 Dell PowerScale OneFS with Software Release 9.5, hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements, Reference (b), is certified for joint use as a Data Storage Controller (DSC) with the condition described in Table 1. The PowerScale F200 Cluster was the tested model. The additional PowerScale F600 and PowerScale F900 models listed in Table 4 were not tested but JITC also certified the additional models because they utilize the same software and similar hardware as the PowerScale F200 model and JITC analysis determined they were functionally identical for interoperability certification purposes.

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		

(Table continues next page.)

Table 1. Conditions (continued)

Description		Operational Impact	Remarks
TDR#	**Open Test Discrepancies**		
DEL-0809-002	UCR 2013 Change 2, Section 14.8, DAT-000450: SUT does not provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171.	Minor	See note.

NOTE(S): DEL-0809-002 - DISA adjudicated this discrepancy as having a minor operational impact with no POA&M. The SUT does not support discovery via the iSNS. iSNS is a protocol used for name discovery by block storage devices; however, PowerScale does not provide block storage, it provides unstructured file storage, and the clusters are discoverable via the Domain Name Service.

LEGEND:

DISA	Defense Information Systems Agency	RFC	Request for Comment
IETF	Internet Engineering Task Force	SUT	System Under Test
iSNS	Internet Storage Name Service	TDR	Test Discrepancy Report
POA&M	Plan of Action and Milestones	UCR	Unified Capabilities Requirements

3. Interoperability Status. Table 2 provides the SUT interface interoperability status, Table 3 provides the Capability Requirements and Functional Requirements status, and Table 4 provides the 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			
1 GbE IAW IEEE 802.3ab	C	Met	
10 GbE IAW IEEE 802.3ae	C	Met	
Storage Array Network Interface			
FC physical interfaces and FCP interfaces IAW ANSI X3.230, X3.297, and X3.303	C	Not Tested	The SUT does not support Storage Array Network.
Out-of-band Management Interfaces			
10 Mbps Ethernet	C	Met	
100 Mbps Ethernet	C	Met	
1 GbE 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	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qbb for Priority-Based Flow Control	O	Not Tested	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qaz for Enhanced Transmission Selection	O	Not Tested	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qaz Data Center Bridging Exchange Protocol	O	Not Tested	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qau for Congestion Notification	O	Not Tested	The SUT does not support FCoE.

(Table continues next page.)

Table 2. SUT Interface Status (continued)

LEGEND:			
ANSI	American National Standards Institute	GbE	Gigabit Ethernet
BB	Backbone	IAW	In Accordance With
C	Conditional	IEEE	Institute of Electrical and Electronics Engineers
CNA	Converged Network Adapter	Mbps	Megabits per second
FC	Fibre Channel	O	Optional
FCoE	Fibre Channel over Ethernet	R	Required
FCP	Fibre Channel Protocol	SUT	System Under Test

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Data Storage Controller (DSC) (R)	Section 14	Partially Met (See note 2.)
2	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. The SUT met the requirements with the exception noted in Table 1.

LEGEND:

CR	Capability Requirement	IPv6	Internet Protocol version 6
DSC	Data Storage Controller	R	Required
FR	Functional Requirement	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements

Table 4. DoDIN APL Product Summary

Product Identification			
Product Name	Dell PowerScale OneFS		
Software Release	9.5		
UCR Product Type(s)	Data Storage Controller		
Product Description	The PowerScale is deployed with an additional PowerScale cluster to provide redundancy and high availability functions. To meet this requirement the SUT was tested with an additional PowerScale OneFS F200 3-node cluster.		
Product Components (See note 1.)	**Component Name** (See note 2.)	**Version**	**Remarks**
PowerScale OneFS F200 Cluster	**PowerScale F200**, PowerScale F600, PowerScale F900	OneFS 9.5.0 0	DSC
		Apache 2.4.54	
	Admin Workstation (Site Provided)	Windows 11 Enterprise	SUT Management
		ActivClient 6.2.0.50	
		Axway Desktop Validator SE 4.11.2.753	

NOTE(S):
1. Table 3-3 in Enclosure 3 of Reference (c) provides the detailed descriptions on the initially tested components and sub-components.
2. Components bolded and underlined were tested by JITC. 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:

APL	Approved Products List	SE	Standard Edition
DoDIN	Department of Defense Information Network	SUT	System Under Test
FS	File System	UCR	Unified Capabilities Requirements
JITC	Joint Interoperability Test Command		

4. Test Details. This certification is based on interoperability (IO) testing, review of the Vendor's Letter of Compliance (LoC), Defense Information Systems Agency (DISA) adjudication of open Test Discrepancy Reports (TDRs), and the DISA Certifying Authority Recommendation for inclusion on the DoDIN APL. JITC completed review of the Vendor's LoC on 13 March 2023 and conducted IO testing at the JITC Global Network Test Facility at Fort Huachuca, Arizona from 27 March through 31 March 2023, using test procedures derived from Reference (c). DISA adjudicated one IO test discrepancy, as noted in Table 1. A JITC-led Cybersecurity (CS) test team conducted CS testing and published the results in a separate report, Reference (d). 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.ie.list.approved-products-certification-office@mail.mil. All associated information is available on the DISA APCO website located at https://aplits.disa.mil/.

6. Point of Contact (POC). JITC POC: Ms. Lorraine Gardner; commercial telephone (520) 538-5221, DSN telephone (312) 879-5221, FAX DSN (312) 879-4347; e-mail address: lorraine.gardner.civ@mail.mil; mailing address: Joint Interoperability Test Command, ATTN: JTE2 (Ms. Lorraine Gardner), P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The APCO tracking number for the SUT is 2223601.

FOR THE COMMANDER:

DORN.LAWRENCE.T.1168371930
Digitally signed by DORN.LAWRENCE.T.1168371930
Date: 2023.05.11 13:50:36 -07'00'

3 Enclosures a/s

LAWRENCE T. DORN
Chief
Specialized Test Division

JITC Memo, JTE, Joint Interoperability Certification of the Dell PowerScale OneFS with Software Release 9.5

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) Joint Interoperability Test Command (JITC), "Data Storage Controller (DSC) Test Procedures Version 1.2 for Unified Capabilities Requirements (UCR) 2013 Change 2," April 2022 (Draft)
(d) JITC, "Cybersecurity Assessment Report for Dell PowerScale OneFS, Software Release 9.5, Tracking Number (TN) 2223601," March 2023

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Dell PowerScale OneFS with Software Release 9.5 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	Legacy
Sponsor Point of Contact	None
Vendor Point of Contact	Derrick Howard, 520-456-4160, E-mail: derrick.howard@dell.com
System Name	Dell PowerScale OneFS
Increment and/or Version	9.5
Product Category	Data Storage Controller
System Background	
Previous certifications	None
Tracking	
APCO ID	2223601
System Tracking Program ID	10632
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Change 2, Sections 5 and 14
Remarks	None
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND: APCO Approved Products Certification Office 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 a PowerScale OneFS F200 3-node cluster. The PowerScale architecture has four layers supporting a variety of data flow:

- Client/Application layer, which Windows, Linux, Apple, and UNIX clients.
- Front-end Ethernet layer.
- Storage layer, which hosts file data and cluster/node configuration data.
- Cluster communication layer, which supports inter-node communication for continuous and scaled cluster operation.

The PowerScale is deployed with an additional PowerScale cluster to provide redundancy and high availability functions. To meet this requirement the SUT was tested with an additional PowerScale OneFS F200 3-node cluster.

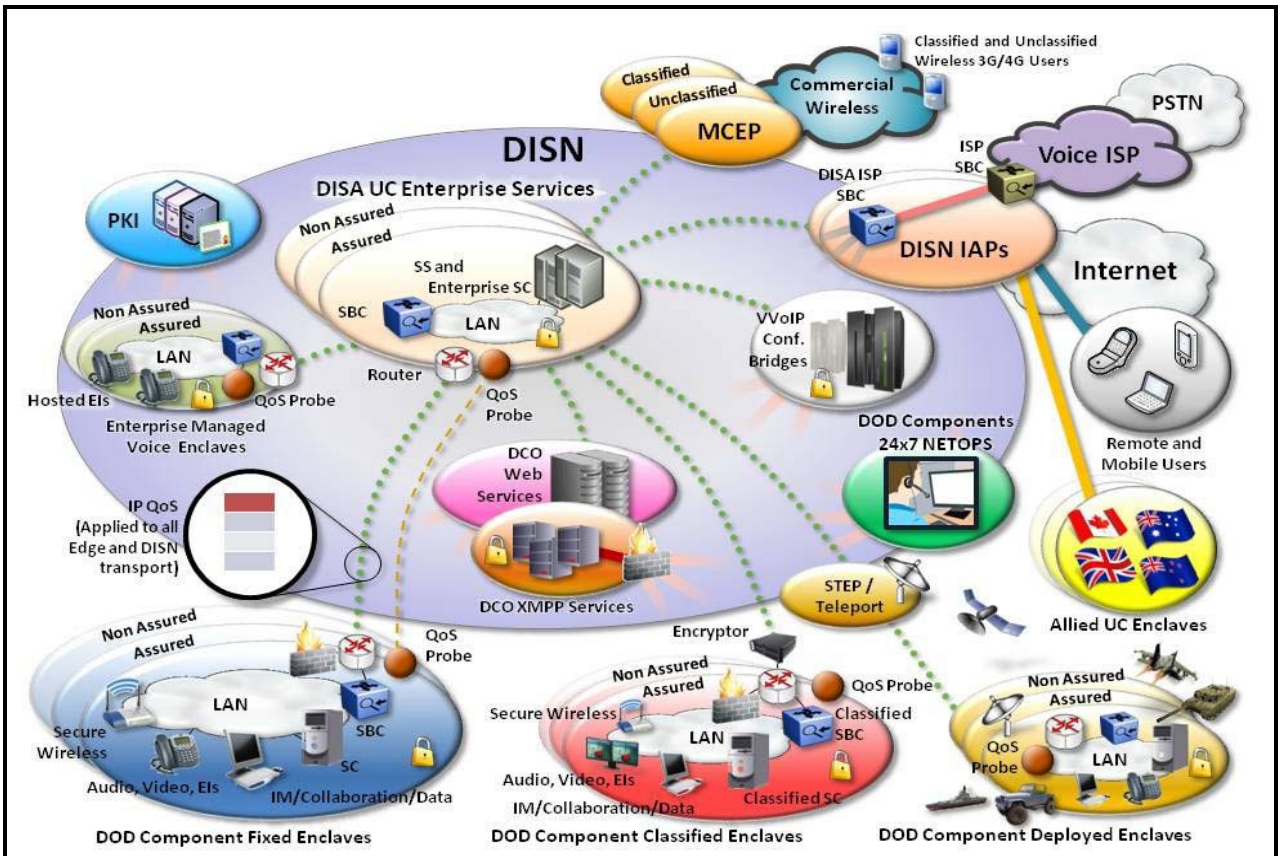
There are no non-privileged system clients. The PowerScale uses a unified permission model that spans disparate clients and is access protocol independent.

Management Description. The SUT's remote management access is provided by the administration workstation via a web-based Universal Indicator via Hypertext Transport Protocol-Secure (HTTPS) or command line via Secure Shell version 2 (SSHv2); by default, only the account of last resort has SSHv2 access after setup. Each method supports multi-factor authentication with Common Access Card (CAC)/Personal Identification Verification (PIV) (SecureCRT) or username and password. Login privileges span System, Security, Configuration, File Access, and Namespace privileges. Microsoft users authenticate with Active Directory, while Linux users authenticate with Lightweight Directory Access Protocol (LDAP). A central Identity Access Management platform allows the creation of custom management and access profiles for role-based-access control (RBAC). Password-based management access is provided using either a provided web-based UI via https, or command-line access. Each supports multi-factor authentication with CAC/PIV. The system can report to external syslog services, using TLS 1.2 where encryption is needed.

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 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.

4. TEST CONFIGURATION. The Joint Interoperability Test Command (JITC) test team tested the SUT at the JITC Global Network Test Facility (GNTF) at Fort Huachuca, Arizona, 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 interoperability functions and features using the test configuration depicted in Figure 2-2. Cybersecurity (CS) testing used the same configuration.

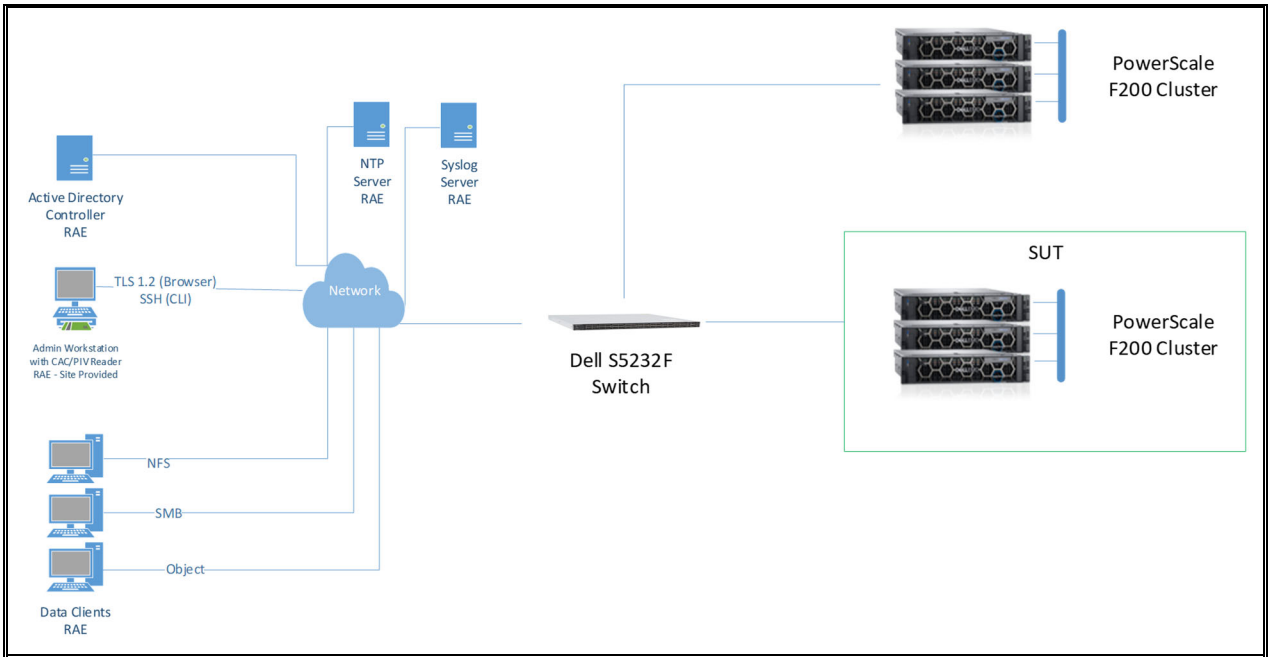
5. METHODOLOGY. The JITC GNTF conducted testing using DSC requirements derived from the Unified Capabilities Requirements (UCR) 2013, Change 2, Reference (c), and the DSC test procedures derived from Reference (c). In addition to testing, an analysis of the Vendor's Letters of Compliance (LoC) verified the SUT met letter "R" requirements. Test Discrepancy Reports (TDRs) document any noted discrepancies. The Vendor submitted Plan of Action and Milestones (POA&M) as required. The Defense Information Systems Agency (DISA) adjudicated the TDR as minor, as noted in Table 1. DISA will evaluate any new discrepancy noted in the operational environment for impact on the existing certification. DISA will adjudicate these discrepancies via a vendor POA&M, which must address all new critical TDRs within 120 days of identification.



LEGEND:

DCO	Defense Connection Online	NETOPS	Network Operations
DISA	Defense Information Systems Agency	PKI	Public Key Infrastructure
DISN	Defense Information Systems Network	PSTN	Public Switched Telephone Network
DoD	Department of Defense	QoS	Quality of Service
EI	End Instrument	SBC	Session Border Controller
IAP	Internet Access Point	SC	Session Controller
IM	Instant Messaging	SS	Softswitch
IP	Internet Protocol	STEP	Standardized Tactical Entry Point
ISP	Internet Service Provider	UC	Unified Capabilities
LAN	Local Area Network	VVoIP	Voice and Video over IP
MCEP	Multi Carrier Entry Point	XMPP	Extensible Messaging and Presence Protocol

Figure 2-1. Notional DoDIN Network Architecture



LEGEND:

CAC	Common Access Card	SMB	Server Message Block
CLI	Command Line Interface	SSH	Secure Shell
NFS	Network File System	SUT	System Under Test
NTP	Network Timing Protocol	Syslog	System Log
PIV	Personal Identity Verification	TLS	Transport Layer Security
RAE	Required Ancillary Equipment		

Figure 2-2. SUT Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS.

The UCR 2013, Change 2, Section 14 establishes the interface, Capability Requirements (CRs), Functional Requirements (FRs), CS, and other requirements for the DoDIN DSCs. Table 3-1 provides the SUT interface interoperability status and Table 3-2 provides the CR and FR status. Testing details and results are provided in the following sub-paragraphs. Optional and/or conditional requirements are not included in the test results unless otherwise noted.

a. Interface Status. The DSC shall provide physical interfaces for, at a minimum, 1 Gigabit Ethernet (GbE) and 10GbE in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet Local Area Network (LAN) interfaces. The SUT met the (1) GbE 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: SSHv2, Transport Layer Security (TLS), HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Cybersecurity. The SUT met the interface requirements with testing. The system may optionally provide 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 met this optional requirement with testing. The system may optionally 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 FCoE and therefore does not support this optional requirement.

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 drives and RAID-5 for Serial Attached SCSI and FC drives, although stronger RAID levels are acceptable. The SUT utilizes dual parity Server Attached Storage (SAS) drives, which are equivalent to dual parity RAID-6 drives. The SUT met this requirement with testing. Testing included removing one of the RAID-5 drives while writing data to the Common Internet File System (CIFS) share using the 1GbE interface. The degraded drive status was displayed in the system status.

b) The system shall be capable of 99.9 percent availability. The SUT met this requirement with the Vendor's LoC, redundant equipment (including but not limited to power supplies, DSCs, dual parity SAS drives), and Vendor product availability documentation.

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 as well as the 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 testing. Testing included powering off one of the two power supplies. The SUT displayed the correct status and continued working. The system's health status was reviewed prior to and after the drive was removed.

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. Testing included data backup, replication, system replication and migration, and data recovery operations.

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 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. Data storage and configuration information was replicated onto a standby DSC using regularly scheduled backup operation using asynchronous replication mode.

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. Testing included backing up and replicating data storage and configuration information onto a standby DSC. The data on the standby DSC was accessible for DR/COOP.

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 in both synchronous and asynchronous modes.

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

a) The system shall provide a NFS version 3 (NFSv3) server for file systems data input/output (I/O). The SUT met this requirement with testing.

b) The system shall provide a NFS version 4 (NFSv4) server for file systems data input/output (I/O). The SUT met this requirement with testing.

c) The system shall provide a NFS version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O. This SUT does not support this optional 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 CIFSv1.0. CIFSv1.0 is no longer used due to associated security risks.

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 using a Windows-based client. Wireshark captures showed protocol features.

f) The system shall provide iSCSI server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators). The SUT does not provide block storage and therefore does not support this optional requirement.

g) The system shall provide FCP server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT does not provide block storage and therefore does not support this optional 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 the 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 Secure Socket Layer (SSL) or 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 testing.

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. SSHv2 was used for management access to the storage controller operating system.

k) The system shall provide Web-based Distributed Authoring and Versioning, per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures. The SUT met this requirement with the Vendor's LoC.

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

m) The system shall implement the Storage Networking Industry Association Cloud Data Management Interface (CDMI) standard. The SUT does not implement CDMI and therefore does not support this optional 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 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 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 10GbE services in conformance with IEEE 802.3 for Ethernet LAN interfaces. The SUT met this requirement with testing for the 10 GbE interface. Wireshark captures showed no anomalies during the test with the 1 and 10 GbE interfaces.

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 requirement with the Vendor's LoC, system logs, and system monitoring tool.

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 requirement with testing the remote access using SSHv2, SSL, HTTPS, and SNMPv3. A JITC-led CS test team conducted CS testing and published the results published in a separate report, Reference (d).

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 requirement with testing and the Vendor's LoC.

e) Ethernet services of the system and the Logical Link Interworking Function 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 requirement with testing and 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 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 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 requirement with testing. Testing included assigning a unique Ethernet MAC address to the Ethernet interface associated with a VLAN.

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 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 does not provide LLDP and therefore does not support this optional requirement.

4) The UCR 2013, Section 14.5, Storage Array Network (SAN) Interface, states the system shall provide FC physical interfaces and FCP interfaces and services as per ANSI X3.230, X3.297, and X3.303. The SUT does not support this conditional SAN 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 CNA. The SUT does not support optional FCoE requirement.

b) The system shall provide physical interfaces for Data Center Bridging (also known as Converged Enhanced Ethernet) features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging. The SUT does not accommodate Data Center Bridging and therefore does not support this optional 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 Unified Capabilities Profile Categories, for a simple server/network appliance. The SUT met the IPv6 requirements with testing and 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 end-to-end path bandwidth, Maximum Segment Size, Round Trip Time, and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 Kilobyte (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 testing and 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 testing and 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 directory services per IETF RFC 4510. The SUT met this requirement with the Vendor's LoC.

b) The system shall provide Kerberos authentication service per IETF RFC 4120. The SUT met this requirement with 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. Wireshark was used to capture the results.

e) The system shall provide Network Information Service (NIS) client directory service functionality. Although the SUT provides support for an NIS server, this requirement was not tested because an NIS server was not available for test. There is no operational impact since the SUT uses DNS and CISCO's native discovery protocol for client-server directory services.

f) The system shall provide NIS Netgroups client directory service functionality. Although the SUT provides support for an NIS server, this requirement was not tested because an NIS server was not available for test. There is no operational impact since the SUT provides DNS and CISCO's native discovery protocol for client-server directory services.

g) The system shall provide Network Basic Input/Output System over TCP/IP Name Resolution and Windows Internet Name Service. The SUT does not support this optional requirement.

h) The system shall provide Internet Storage Name Service client functionality per IETF RFC 4171. The SUT does not support discovery via the iSNS. iSNS is a protocol used for name discovery by block storage devices; however, PowerScale does not provide block storage; PowerScale provides unstructured file storage. PowerScale clusters are discoverable via the Domain Name Service. DISA adjudicated this discrepancy as having a minor operational impact with no POA&M, as noted in Table 1.

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

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

a) The system shall provide IP Security per RFC 4301. The SUT does not support IPSec and therefore does not meet this optional requirement.

b) The system shall provide Encapsulating Security Payload per RFC 4303. The SUT does not support RFC 4303 and therefore does not meet this optional requirement.

c) The system shall provide Internet Key Exchange (IKE) version 2 per RFC 4306. The SUT does not provide IKE and therefore does not meet this optional requirement.

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. The Packet Filter service shall provide a configuration policy for

defining combinations of multiple packet match rules and processing actions. The SUT met this requirement with the Vendor's LoC.

e) The system shall provide encryption of data at rest at a minimum of Advanced Encryption Standard (AES)-256 in accordance with Federal Information Processing Standard 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. The SUT met this requirement with the Vendor's LoC.

2. Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place. The SUT met this requirement with the Vendor's LoC.

f) The system shall comply with all appropriate Security Technical Implementation Guides to include the Database Security Technical Implementation Guide. A JITC-led CS test team conducted CS testing and published the results in a separate report, Reference (d).

9) The UCR 2013, Section 14.10, Interoperability, 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) 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, VLAN 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 met this requirement with testing and the Vendor's LoC.

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 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 testing and the Vendor's LoC.

11) The UCR 2013, Section 14.12 includes the Virtualization requirements in the subparagraphs below. The SUT does not support the optional virtualized DSC (vDSC) requirements; therefore, the requirements in the subparagraphs below do not apply.

a) The system shall provide 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.

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 per vDSC.

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.

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.

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.

7. HARDWARE/SOFTWARE/FIRMWARE VERSION IDENTIFICATION. Table 3-3 provides the SUT components' hardware, software, and firmware tested. The JITC 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 in accordance with the UCR 2013, Change 2, and is certified for joint 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			
1 GbE IAW IEEE 802.3ab	C	Met	
10 GbE IAW IEEE 802.3ae	C	Met	
Storage Array Network Interface			
FC physical interfaces and FCP interfaces IAW ANSI X3.230, X3.297, and X3.303	C	Not Tested	The SUT does not support Storage Array Network.
Out-of-band Management Interfaces			
10 Mbps Ethernet	C	Met	
100 Mbps Ethernet	C	Met	
1 GbE 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	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qbb for Priority-Based Flow Control	O	Not Tested	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qaz for Enhanced Transmission Selection	O	Not Tested	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qaz Data Center Bridging Exchange Protocol	O	Not Tested	The SUT does not support FCoE.
Data Center Bridging also known as Converged Enhanced Ethernet features IAW IEEE 802.1Qau for Congestion Notification	O	Not Tested	The SUT does not support FCoE.

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over Twisted Pair	FCP	Fibre Channel Protocol
802.3ae	10 Gbps Ethernet over Fiber	GbE	Gigabit Ethernet
ANSI	American National Standards Institute	Gbps	Gigabits per second
BaseT	Megabit (Baseband Operation, Twisted Pair) Ethernet	IAW	In Accordance With
		IEEE	Institute of Electrical and Electronics Engineers
BB	Backbone	Mbps	Megabits per second
C	Conditional	O	Optional
CNA	Converged Network Adapter	R	Required
FC	Fibre Channel	SUT	System Under Test
FCoE	Fibre Channel over Ethernet		

Table 3-2. Capability and Functional Requirements and Status

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

NOTE(S):
1. The annotation of 'required' refers to a high-level requirement category.
2. The SUT does not support the conditional Storage Array Network requirement.
3. The SUT does not support FCoE nor accommodate Data Center Bridging and therefore does not support these optional requirements.
4. The SUT met the Name Services requirements with the following exceptions:
   - Although the SUT provides support for an NIS server, this requirement was not tested because an NIS server was not available for test. There is no operational impact since the SUT uses the Domain Name System and CISCO's native discovery protocol for client-server directory services.
   - The SUT does not provide iSNS client functionality per IETF RFC 4171. DISA adjudicated this discrepancy as having a minor operational impact with no POA&M. The SUT does not support discovery via the iSNS. iSNS is a protocol used for name discovery by block storage devices; however, PowerScale does not provide block storage. PowerScale provides unstructured file storage. PowerScale clusters are discoverable via the Domain Name Service.
5. A JITC-led Cybersecurity test team conducted Cybersecurity testing and published the results published in a separate report, Reference(d).
6. The SUT does not support the virtualized DSC requirements and therefore does not support this optional requirement.

LEGEND:

CR	Capability Requirement	JITC	Joint Interoperability Test Command
DISA	Defense Information Systems Agency	NIS	Network Information Service
DSC	Data Storage Controller	O	Optional
FCoE	Fibre Channel over Ethernet	POA&M	Plan of Action and Milestones
FR	Functional Requirement	R	Required
ID	Identification	RFC	Request for Comment
IETF	Internet Engineering Task Force	SUT	System under Test
iSNS	Internet Storage Name Service	UCR	Unified Capabilities Requirements

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

Components (See note.)	Release	Sub-component	Function
PowerScale F200 PowerScale F600 PowerScale F900	OneFS 9.5.0 0	NA	DSC
	Apache 2.4.54		
Admin Workstation (Site Provided)	Windows 11 Enterprise		SUT Management
	ActivClient 6.2.0.50		
	Axway Desktop Validator SE 4.11.2.753		

NOTE(S): Components bolded and underlined were tested by JITC. 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:

DSC	Data Storage Controller	NA	Not Applicable
FS	File System	SE	Standard Edition
JITC	Joint Interoperability Test Command	SUT	System Under Test

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

System Name	Software Release	Function
Required Ancillary Equipment (Site Provided)		
Active Directory	v10.0.1	Active Directory/Domain Controller
Domain Controller	Windows 2016 V1607 OS Build 14393-4350	
NTP	CISCO 4451 17.6.3a	Network Timing Protocol
PKI	Windows 2016 V1607 OS Build 14393-4350	Revocation Server
SNMP	SolarWinds Orion 2020.2.6	Network Management
Syslog Server	Kiwi v1.6.1	Logging
Test Network Component		
Workstation (Site Provided)	Windows 11 22H2	Admin Workstation
	ActivClient 6.2.0.50	
	Axway Desktop Validator SE 4.11.2.753	

LEGEND:

IP	Internet Protocol	SE	Standard Edition
NTP	Network Time Protocol	SNMP	Simple Network Management Protocol
OS	Operating System	Syslog	System Log
PKI	Public Key Infrastructure	V/v	Version
RADIUS	Remote Authentication Dial-In User Service		