



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER
TO:

Joint Interoperability Test Command (JTE)

5 Oct 12

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the NetApp FAS3170 with DATA ONTAP Software Release (SR) 7.3.6

References:

- (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
- (b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
- (c) through (e), see Enclosure 1

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The NetApp FAS3170 with DATA ONTAP with SR 7.3.6, hereinafter referred to as the System Under Test (SUT), meets all the critical interoperability requirements for a Data Storage Controller and is certified for joint use within the Defense Information System Network (DISN). The certification status of the SUT will be verified during operational deployment. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of Defense Information Systems Agency (DISA) via a vendor Plan of Action and Milestones which addresses all new critical Test Discrepancy Reports within 120 days of identification. Testing was conducted using product requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and test procedures, Reference (d). No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect interoperability, but no later than three years from the date of the Unified Capabilities Approved Products List memorandum.

3. This finding is based on interoperability testing conducted by Telecommunication Systems Security Assessment Program (TSSAP), review of the vendor's Letters of Compliance (LoC), and TSSAP Information Assurance (IA) Certification Authority (CA) approval of the IA configuration. Interoperability testing was conducted by TSSAP, from 8 November 2011 to 11 November 2011, 29 November 2011 to 2 December 2011, and 12 December 2011 to 16 December 2011. Review of the vendor's LoC was completed on 7 January 2012. The DISA CA has reviewed the IA Assessment Report for the SUT, Reference (e), and based on the findings in the report has provided a positive recommendation. The acquiring agency or site will be responsible for the DoD Information Assurance Certification and Accreditation Process (DIACAP) accreditation. The JITC certifies the SUT as meeting the UCR for requirements for

Data Storage Controller. Enclosure 2 documents the test results and describes the tested network and system configurations including specified patch releases.

4. The interface, Capability Requirements (CR) and Functional Requirements (FR), and component status of the SUT are listed in Table 1. The threshold CR/FRs for security devices are established by Section 5.10 of Reference (c) and were used to evaluate the interoperability of the SUT.

Table 1. SUT Interface Interoperability Status

Interface	Critical	UCR Reference	Threshold CR/FR ¹	Status	Remarks																								
Network Attached Storage (NAS)																													
10Base-X	Yes	5.10.4.3	1-11	Certified	The SUT met all critical CRs and FRs for the interface.																								
100Base-X	Yes	5.10.4.3	1-11	Certified	The SUT met all critical CRs and FRs for the interface.																								
Gigabit Ethernet (GbE)	Yes	5.10.4.1	1-11	Certified	The SUT met all critical CRs and FRs for the interface.																								
10 GbE	Yes	5.10.4.1	1-11	Certified	The SUT met all critical CRs and FRs for the interface.																								
Storage Array Network (SAN)																													
Fibre Channel (FC)	No	5.10.5.1	1-11	Not Tested ²	This interface is supported by the SUT but was not tested and is not certified for use.																								
FC Protocol (FCP)	No	5.10.5.1	1-11	Not Tested ²	This interface is supported by the SUT but was not tested and is not certified for use.																								
Converged Network Adapter (CNA)																													
10 GbE	No	5.10.6.1	1-11	Not Tested	Not applicable.																								
<p>NOTES:</p> <p>1. CR/FR requirements are contained in Table 2. CR/FR numbers represent a roll-up of UCR requirements</p> <p>2. The requirement is not critical, was not tested, and therefore is not certified for use.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">CNA</td> <td style="width: 50%;">Converged Network Adaptor</td> <td>ID</td> <td>Identification</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>NAS</td> <td>Network Attached Storage</td> </tr> <tr> <td>FC</td> <td>Fibre Channel</td> <td>SAN</td> <td>Storage Array Network</td> </tr> <tr> <td>FCP</td> <td>FC Protocol</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>GbE</td> <td>Gigabit Ethernet</td> <td></td> <td></td> </tr> </table>						CNA	Converged Network Adaptor	ID	Identification	CR	Capability Requirement	NAS	Network Attached Storage	FC	Fibre Channel	SAN	Storage Array Network	FCP	FC Protocol	SUT	System Under Test	FR	Functional Requirement	UCR	Unified Capabilities Requirements	GbE	Gigabit Ethernet		
CNA	Converged Network Adaptor	ID	Identification																										
CR	Capability Requirement	NAS	Network Attached Storage																										
FC	Fibre Channel	SAN	Storage Array Network																										
FCP	FC Protocol	SUT	System Under Test																										
FR	Functional Requirement	UCR	Unified Capabilities Requirements																										
GbE	Gigabit Ethernet																												

Table 2. SUT CRs and FRs Status

CR/FR ID	Capability/Function	Applicability	UCR References	Status	Remarks
1	Storage System Requirements				
	Redundant Array of Independent Disks (RAID)	Required	5.10.2.1	Met	
	Availability	Required	5.10.2.2	Met ¹	
	Management Control	Required	5.10.2.3	Met	
	Data Storage Replication	Required	5.10.2.4	Met	
	Data Storage Backup	Required	5.10.2.4.1	Met	
	Replication	Required	5.10.2.4.2	Met	
	Disaster Recovery (DR)	Required	5.10.2.4.3	Met	
	Configuration Modes	Conditional	5.10.2.5	Met	
2	Storage Protocol Requirements				
	Network File System (NFSv3)	Required	5.10.3.1	Met	
	Network File System (NFSv4)	Conditional	5.10.3.2	Met	
	Network File System (NFSv4.1)	Conditional	5.10.3.3	Not Tested	
	Common Internet File System (CIFSv1.0)	Required	5.10.3.4	Met	
	Common Internet File System (CIFSv2.0)	Conditional	5.10.3.5	Met	
	Internet Small Computer System Interface (iSCSI)	Conditional	5.10.3.6	Met	
	Fibre Channel (FC) Protocol	Conditional	5.10.3.7	Not Tested ²	
	Fibre Channel over Ethernet (FCoE)	Conditional	5.10.3.8	Not Tested ²	
	HTTPS Server	Conditional	5.10.3.9	Not Tested ³	
	SSHv2 or SSL Implementation	Required	5.10.3.10	Met	
	Web-based Distributed Authoring and Versioning (WebDAV)	Conditional	5.10.3.11	Not Tested ³	
	Representational State Transfer (REST)	Conditional	5.10.3.12	Not Tested ⁴	
	Cloud Data Management Interface (CDMI)	Conditional	5.10.3.13	Not Tested ⁴	
Global Name Space (GNS) functionality	Required	5.10.3.14	Not Met ⁵		
3	Network Attached Storage (NAS) Interface Requirements				
	Gigabit Ethernet (GbE) and 10 GbE Services	Required	5.10.4.1	Met	
	Provision, Monitor and Detect Faults, and Restore Ethernet	Required	5.10.4.2	Met	
	SSHv2, SSL, HTTPS, and SNMPv3 Protocols	Required	5.10.4.3	Met	
	Auto-sensing, Auto-detecting and Auto-configuring	Required	5.10.4.4	Met	
	Ethernet Services and Logical Link IWF	Required	5.10.4.5	Met ¹	
	Ethernet Service Requirements	Required	5.10.4.6	Met	
	VLAN Requirements	Required	5.10.4.7	Met	
	Link Aggregation	Required	5.10.4.8	Met	
	Link Layer Discovery Protocol (LLDP)	Required	5.10.4.9	Partially Met ⁶	
4	Storage Array Network (SAN) Interface Requirements				
	Fiber Channel (FC) Physical Interfaces	Conditional	5.10.5.1	Not Tested ²	

Table 2. SUT CRs and FRs Status (continued)

CR/FR ID	Capability/Function	Applicability	UCR Reference ¹	Status	Remarks
5	Converged Network Adapter (CAN) Interface Requirements				
	FCoE Services	Conditional	5.10.6.1	Not Tested ²	
	Data Center Bridging (DCB) Table 5.10.6-1	Conditional	5.10.6.2	Not Tested ²	
6	IP Networking Requirements				
	IPv6 Requirements as defined in Section 5.3.5.5	Required	5.10.7.1	Met ^{1,7}	
	Replication (mirroring) Session Traffic Per Table 5.10.7-1	Required	5.10.7.3	Met ¹	
	Congestion Control	Required	5.10.7.4	Met ¹	
7	Name Services Requirements				
	Lightweight Directory Access Protocol (LDAP)	Required	5.10.8.1	Met ⁷	
	Kerberos Authentication	Required	5.10.8.2	Met	
	Domain Name System (DNS) Functionality	Required	5.10.8.3	Met	
	DNS Load Balancing	Required	5.10.8.4	Met	
	Network Information Service (NIS) Functionality	Required	5.10.8.5	Met ⁷	
	NIS Netgroups Functionality	Required	5.10.8.6	Met ⁷	
	NetBIOS over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS)	Conditional	5.10.8.7	Met	
	Internet Storage Name Service (iSNS) Functionality	Required	5.10.8.8	Met ¹	
FC Name and Zone Service	Required	5.10.8.9	Not Tested ⁸		
8	Security Services Requirements				
	IPSec	Conditional	5.10.9.1	Met ¹	
	Encapsulating Security Payload (ESP)	Conditional	5.10.9.2	Met ¹	
	Internet Key Exchange version 2 (IKEv2)	Conditional	5.10.9.3	Met ¹	
	The Packet Filter Service	Conditional	5.10.9.4	Not Tested ²	
	DoD Host-Based Security System (HBSS) Software	Conditional	5.10.9.5	Not Tested ²	
	Data Encryption	Required	5.10.9.6	Met ⁷	
STIGs Compliance	Required	5.10.9.7	Met ⁷		
9	Interoperability Requirements				
	IP ASLAN and DISN WAN Networks	Required	5.10.10.1	Met	
	Application Programming Interface (API)	Required	5.10.10.2	Met	
10	Class of Service (CoS) and Quality of Service (QoS) Requirements				
	Layer 2 CoS and QoS Markings	Required	5.10.11.1	Not Met ⁹	
	Layer 3 CoS and QoS Markings	Required	5.10.11.2	Met	
11	Virtualization Requirements				
	Virtualized Data Storage Controller (vDSC) Functionality	Conditional	5.10.12.1	Not Tested	
	Private Networking Domains (PNDs)	Conditional	5.10.12.2	Not Tested	
	Individual Command Line Interface (CLI)	Conditional	5.10.12.3	Not Tested	
	API Commands	Conditional	5.10.12.4	Not Tested	

Table 2. SUT CRs and FRs Status (continued)

	GNS	Conditional	5.10.12.5	Not Tested	
NOTES:					
<p>1. This UCR Requirement is met by vendor letter of compliance (LoC).</p> <p>2. This requirement is conditional, was not tested, and therefore is not certified for use.</p> <p>3. The SUT has no WEB Server functionality in the tested configuration and therefore is not certified for WebDAV.</p> <p>4. Representational State Transfer (REST) for distributed hypermedia systems and Cloud-Based functionalities are not included in this SUT and therefore the SUT is not certified for REST or CDMI.</p> <p>5. Global Name Space is not natively supported on the Data ONTAP filer for Version 7.3.6. On 4 May 2012, DISA adjudicated this as minor with a condition of field (COF) and POA&M. The COF is that a secondary component like a load balancer with global load balancing capability may be used. The POA&M is the software release of Data ONTAP version 8.2, which is projected to occur in third quarter 2013, with Global Name Space functionality included.</p> <p>6. The Ethernet services of the SUT only provide LLDP via the Cisco Discovery Protocol (CDP) In lieu of LLDP, which was adjudicated as a minor issue. On 28 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from “required” to “conditional” in a future version of the UCR and also because the implementation of discovery protocol (LLDP or CDP) is dependent upon the infrastructure that the DSC connects to. Therefore, the procurement requirements for DSC should specify the needed discovery protocol.</p> <p>7. The test results for this requirement were published in a separate report. See reference (E).</p> <p>8. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from “required” to “conditional” to be consistent with all other fiber channel requirements for a DSC. This requirement will change to condition in UCR 2013.</p> <p>9. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from “required” to “conditional” to align on layer 3 queuing for QoS and no longer requiring layer 2 CoS marking. This requirement will change to condition in UCR 2013.</p>					
LEGEND:					
ASLAN	Assured Service Local Area Network	IP	Internet Protocol		
API	Application Programming Interface	IPSEC	Internet Protocol Security		
CDMI	Cloud Data Management Interface	IPv6	Internet Protocol Version 6		
CDP	Cisco Discovery Protocol	iSCSI	Internet Small Computer System Interface		
CLI	Individual Command Line Interface	iSNS	Internet Storage Name Service		
CNA	Converged Network Adaptor	IWF	Interworking Function		
CoS	Class Of Service	LDAP	Lightweight Directory Access Protocol		
CR	Capability Requirement	LLDP	Link Layer Discovery Protocol		
DCB	Data Center Bridging	NAS	Network Attached Storage		
DISN	Defense Information Systems Network	NBT	NetBIOS Over TCP/IP		
DNS	Domain Name System	NIS	Network Information Service		
DoD	Department Of Defense	PND	Private Networking Domains		
DR	Disaster Recovery	QoS	Quality Of Service		
DSC	Data Storage Controller	RAID	Redundant Array Of Independent Disks		
ESP	Encapsulating Security Payload	REST	Representational State Transfer		
FC	Fibre Channel	SAN	Storage Array Network		
FCP	FC Protocol	SNMPv3	Simple Network Management Protocol Version 3		
FCoE	FC Over Ethernet	SSHv2	Secure Shell Version 2		
FC	Fibre Channel	SSL	Secure Socket Layer		
FCP	FC Protocol	STIG	Security Technical Implementation Guide		
FR	Functional Requirement	TCP/IP	Transmission Control Protocol/Internet Protocol		
GbE	Gigabit Ethernet	UCR	Unified Capabilities Requirements		
GNS	Global Name Space	vDSC	Virtualized Data Storage Controller		
HBSS	Host-Based Security System	VLAN	Virtual Local Area Network		
HTTPS	Hypertext Transport Protocol Secure	WAN	Wide Area Network		
ID	Identification	WebDAV	Web-Based Distributed Authoring And Versioning		
IKEv2	Internet Key Exchange Version 2	WINS	Windows Internet Name Service		

5. No detailed test report was developed in accordance with the Program Manager’s request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at

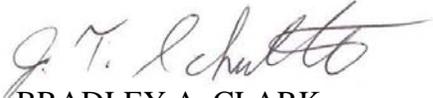
JITC Memo, JTE, Special Interoperability Test Certification of the NetApp FAS3170 with DATA ONTAP Software Release (SR) 7.3.6

<https://aplits.disa.mil>.

6. The testing point of contact is Ryan Bradshaw, TSSAP, commercial (210) 925-6900 or DSN 945-6900; e-mail address is ryan.bradshaw.3@us.af.mil. The JITC certification point of contact is Anita Mananquil, commercial (520) 538-5164 or DSN (312) 879-5164; e-mail address is anita.mananquil.civ@mail.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-1298. The Unified Capabilities Connection Office tracking number is 1111701.

FOR THE COMMANDER:

2 Enclosures a/s


for BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DoD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

ADDITIONAL REFERENCES

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 3," September 2011
- (d) Joint Interoperability Test Command, "Storage Device Test Plan," Draft.
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of NetApp, FAS3170 Data Storage Controller with Rel. 7.3.6 (TN 1111701)," 12 March 2012.

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. The NetApp, FAS3170, Data Storage Controller with SR 7.3.6, hereinafter referred to the System Under Test (SUT)

2. SPONSOR. DISA, ATTN: Catrena Gainer,
Address, Phone, e-mail: 6919 Cooper Ave. Ft. Meade, MD 20755, (703) 882-0454,
catrena.gainer@disa.mil.

3. SYSTEM POC. Tachyon Dynamics, ATTN: Jeremy Duncan,
Address, Phone, e-mail: 9936 Wood Wren Court, Fairfax, Virginia, (703)259-8550,
jduncan@tachyondynamics.com.

4. TESTER. Telecommunication Systems Security Assessment Program (TSSAP),
Lackland AFB, TX

5. SYSTEM DESCRIPTION. The NetApp FAS3170 DATA ONTAP with SR 7.3.6 is NetApp's Fabric-Attached Storage. The NetApp FAS3170 DATA ONTAP with SR 7.3.6 functions in an enterprise-class Storage Area Network (SAN), as well as a networked storage appliance. It can serve storage over a network using file-based as well as block-based protocols. NetApp Fabric Attached Storage systems implement their physical storage in large disk arrays. The SUT supports the following features which were met through testing or vendor submission of Letters of Compliance (LoC).

- Network Interfaces: 10/100 Megabits per second (Mbps), GE and 10GbE network interface card.
- File-Based Protocols: NFSv3, NFSv4, CIFSv1.0, CIFSv2.0. The SUT supports FTP, TFTP and HTTP; however these protocols were not tested, therefore, are not certified.
- Block-Based Protocols: Small Computer System Interface (iSCSI). The SUT supports Fibre Channel Protocol, Fibre Channel over Ethernet; however, these features were not tested, therefore, are not certified.
- RAID-DP® High Performance RAID-6.
- Mirroring: Asynchronous Replication.

6. OPERATIONAL ARCHITECTURE. Figure 2-1 depicts a notional operational Unified Capabilities (UC) end-to-end architecture that the SUT may be used in.

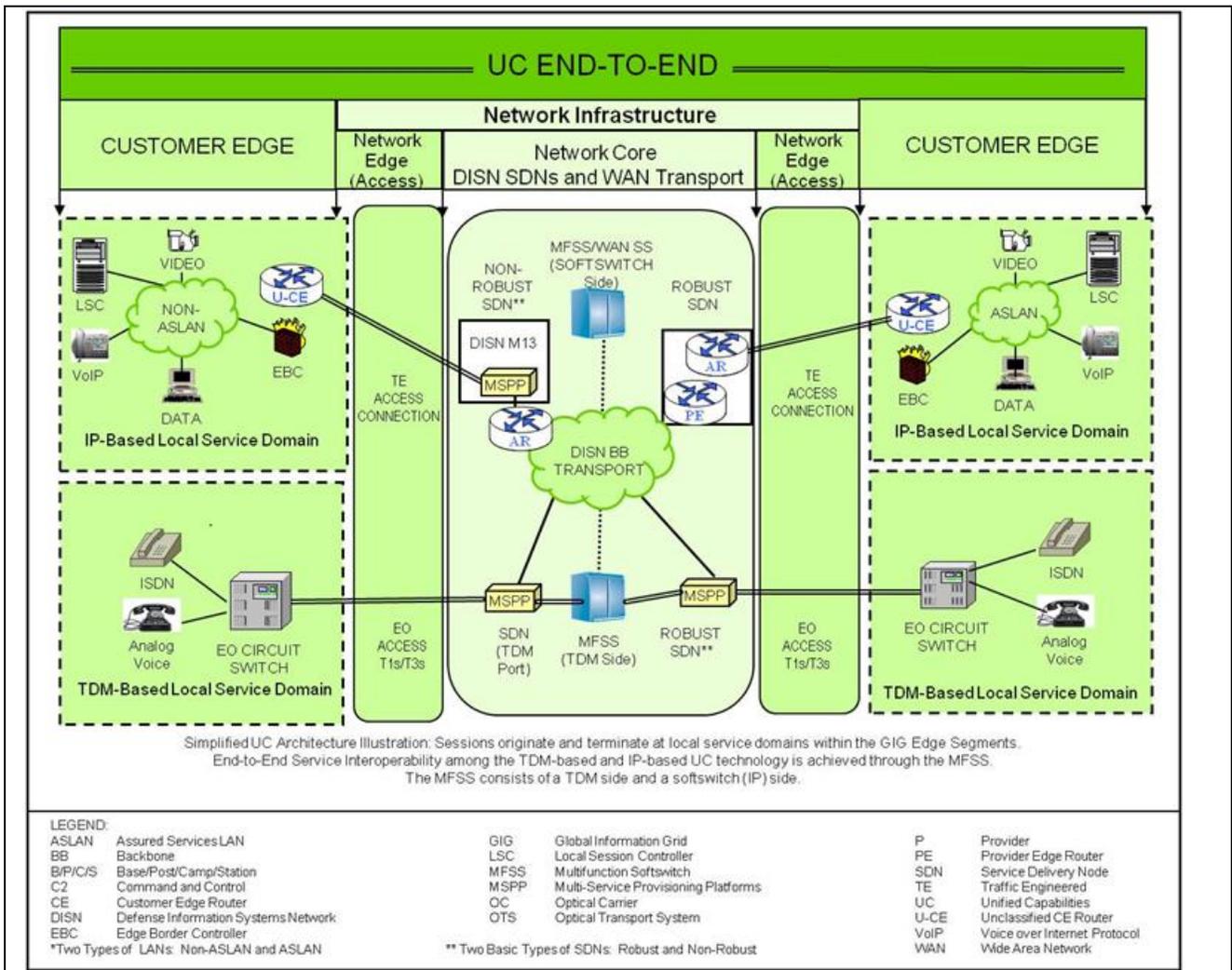


Figure 2-1. Notional UC End-to-End Architecture

7. REQUIRED SYSTEM INTERFACES. Requirements specific to the SUT and interoperability results are listed in Table 2-1. These requirements are derived from Reference (c) and verified through the test procedures listed in Reference (d).

Table 2-1. Data Storage Controller Interface Requirements

Interface (See note)	UCR Ref	NAS	SAN	Converged Network	Criteria	Remarks
10Base-X	5.10.4.3	R	C	C	Support minimum threshold CRs/FRs 1-11 and 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 5.4, Information Assurance Requirements.	
100Base-X	5.10.4.3	R	C	C	Support minimum threshold CRs/FRs 1-11 and 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 5.4, information assurance requirements.	
Gigabit Ethernet (GbE)	5.10.4.1	R	C	C	Support minimum threshold CRs/FRs 1-11 and the interfaces shall be autosensing, auto-detecting and auto-configuring with incoming and corresponding Ethernet link negotiation signals	
10 GbE	5.10.4.1	R	C	C	Support minimum threshold CRs/FRs 1-11 and the interfaces shall be autosensing, auto-detecting and auto-configuring with incoming and corresponding Ethernet link negotiation signals	
Fibre Channel (FC)	5.10.5.1	R	C	C	Support minimum threshold CRs/FRs 1-11 and the system shall provide FC physical interfaces and services as per ANSI x3.230, x3.297, and x3.303	
FC Protocol (FCP)	5.10.5.1	R	C	C	Support minimum threshold CRs/FRs 1-11 and the system shall provide FC physical interfaces, FCP interfaces and services as per ANSI x3.230, x3.297, and x3.303	

Table 2-1. Data Storage Controller Interface Requirements (continued)

NOTE:
CR/FR requirements are contained in Table 2-2. CR/FR numbers represent a roll-up of UCR requirements.

LEGEND:

ANSI	American National Standards Institute	R	Required
C	Conditional	Ref	Reference
CR	Capability Requirement	SAN	Storage Array Network
EIA	Electronic Industries Alliance	SNMPV3	Simple Network Management Protocol Version 3
FC	Fibre Channel	SSHV2	Secure Shell Version 2
FCP	FC Protocol	SSL	Secure Socket Layer
FR	Functional Requirement	SUT	System Under Test
GbE	Gigabit Ethernet	TIA	Telecommunications Industry Association
HTTPS	HyperText Transfer Protocol Secure	UCR	Unified capabilities Requirements
NAS	Network Attached Storage	VPN	Virtual Private network
R	Required		

8. TEST NETWORK DESCRIPTION. The SUT was tested at Telecommunication Systems Security Assessment Program in a manner and configuration similar to that of a notional operational environment. Testing the system’s required functions and features was conducted using the test configuration depicted in Figure 2-2.

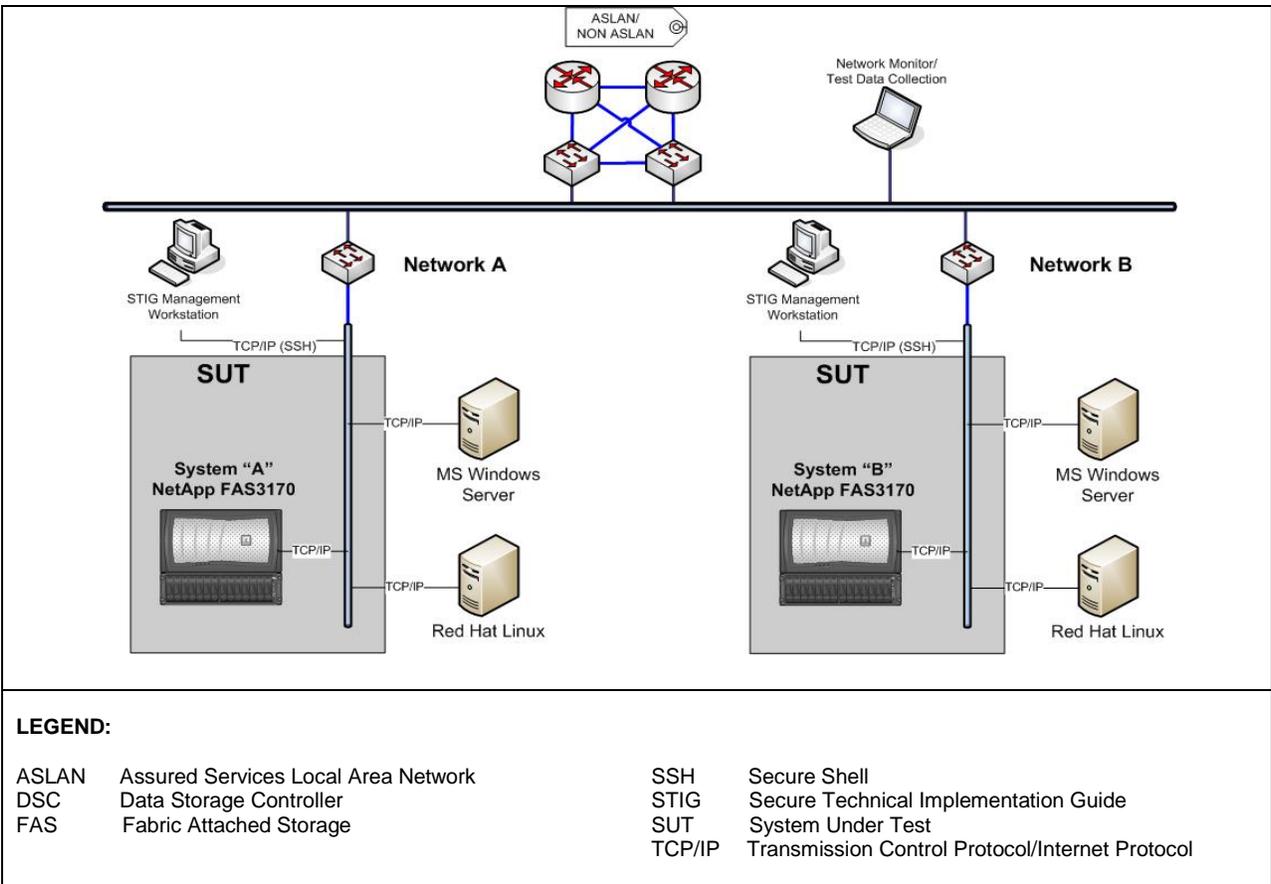


Figure 2-2. SUT Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-3 provides the system configurations, hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic.

Table 2-3. Tested System Configurations

System Name	Equipment
Required Ancillary Equipment	Active Directory (Microsoft Windows Server 2008)
	SysLog Server(Kiwi SysLog Server 9.2)
Additional Equipment Needed	Management Workstation
	LDAP Server (Microsoft Windows Server 2008)
System Name	Equipment
NetApp FAS3170	Software/Firmware
	Data ONTAP Release 7.3.6
LEGEND:	
FAS	Fabric Attached Storage
LDAP	Lightweight Directory Access Protocol

10. TESTING LIMITATIONS. None.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for Data Storage Controllers in accordance with Section 5.10 of the Unified Capabilities Requirements (UCR) 2008 Change 3 and is certified for joint use with other network infrastructure products listed on the Approved Products List (APL). Additional discussion regarding specific testing results is located in subsequent paragraphs.

11.1 Interfaces. The interface status of the SUT is provided in Table 2-4.

Table 2-4. Data Storage Controller Interface Requirements Status

Interface	Critical ¹	UCR Reference	Threshold CR/FR ¹	Status	Remarks																				
Network Attached Storage (NAS)																									
10Base-X	Yes	5.10.4.3	1-11	Met																					
100Base-X	Yes	5.10.4.3	1-11	Met																					
Gigabit Ethernet (GbE)	Yes	5.10.4.1	1-11	Met																					
10 GbE	Yes	5.10.4.1	1-11	Met																					
Storage Array Network (SAN)																									
Fibre Channel (FC)	No	5.10.5.1	1-11	Not Tested ²																					
FC Protocol (FCP)	No	5.10.5.1	1-11	Not Tested ²																					
Converged Network																									
10 GbE	No	5.10.6.1	1-11	Not Tested ²																					
<p>NOTES:</p> <p>1. CR/FR requirements are contained in Table 2. CR/FR numbers represent a roll-up of UCR requirements</p> <p>2. This requirement is conditional, was not tested, and therefore is not certified for use.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td>CR</td> <td>Capability Requirement</td> <td>NAS</td> <td>Network Attached Storage</td> </tr> <tr> <td>FC</td> <td>Fibre Channel</td> <td>SAN</td> <td>Storage Array Network</td> </tr> <tr> <td>FCP</td> <td>FC Protocol</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>GbE</td> <td>Gigabit Ethernet</td> <td></td> <td></td> </tr> </table>						CR	Capability Requirement	NAS	Network Attached Storage	FC	Fibre Channel	SAN	Storage Array Network	FCP	FC Protocol	SUT	System Under Test	FR	Functional Requirement	UCR	Unified Capabilities Requirements	GbE	Gigabit Ethernet		
CR	Capability Requirement	NAS	Network Attached Storage																						
FC	Fibre Channel	SAN	Storage Array Network																						
FCP	FC Protocol	SUT	System Under Test																						
FR	Functional Requirement	UCR	Unified Capabilities Requirements																						
GbE	Gigabit Ethernet																								

11.2 Capability Requirements (CR) and Functional Requirements (FR). The Data Storage Controller Products have required and conditional features and capabilities that are established by Section 5.10 of the Unified Capabilities Requirements (UCR). The System Under Test (SUT) does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements. The detailed Functional Requirements (FR) and Capability Requirements (CR) for Security Device products are listed in Table 2-5.

Table 2-5. Data Storage Controller CRs and FRs Status

CR/FR ID	Capability/Function	Applicability	UCR References	Status	Remarks
1	Storage System Requirements				
	Redundant Array of Independent Disks (RAID)	Required	5.10.2.1	Met	
	Availability	Required	5.10.2.2	Met ¹	
	Management Control	Required	5.10.2.3	Met	
	Data Storage Replication	Required	5.10.2.4	Met	
	Data Storage Backup	Required	5.10.2.4.1	Met	
	Replication	Required	5.10.2.4.2	Met	
	Disaster Recovery (DR)	Required	5.10.2.4.3	Met	
	Configuration Modes	Conditional	5.10.2.5	Met	
2	Storage Protocol Requirements				
	Network File System (NFSv3)	Required	5.10.3.1	Met	
	Network File System (NFSv4)	Conditional	5.10.3.2	Met	
	Network File System (NFSv4.1)	Conditional	5.10.3.3	Not Tested	
	Common Internet File System (CIFSv1.0)	Required	5.10.3.4	Met	
	Common Internet File System (CIFSv2.0)	Conditional	5.10.3.5	Met	
	Internet Small Computer System Interface (iSCSI)	Conditional	5.10.3.6	Met	
	Fibre Channel (FC) Protocol	Conditional	5.10.3.7	Not Tested ²	
	Fibre Channel over Ethernet (FCoE)	Conditional	5.10.3.8	Not Tested ²	
	HTTPS Server	Conditional	5.10.3.9	Not Tested ³	
	SSHv2 or SSL Implementation	Required	5.10.3.10	Met	
	Web-based Distributed Authoring and Versioning (WebDAV)	Conditional	5.10.3.11	Not Tested ³	
	Representational State Transfer (REST)	Conditional	5.10.3.12	Not Tested ⁴	
Cloud Data Management Interface (CDMI)	Conditional	5.10.3.13	Not Tested ⁴		
	Global Name Space (GNS) functionality	Required	5.10.3.14	Not Met ⁵	
3	Network Attached Storage (NAS) Interface Requirements				
	Gigabit Ethernet (GbE) and 10 GbE Services	Required	5.10.4.1	Met	
	Provision, Monitor and Detect Faults, and Restore Ethernet	Required	5.10.4.2	Met	
	SSHv2, SSL,HTTPS, and SNMPv3 Protocols	Required	5.10.4.3	Met	
	Auto-sensing, Auto-detecting and Auto-configuring	Required	5.10.4.4	Met	
	Ethernet Services and Logical Link IWF	Required	5.10.4.5	Met ¹	
	Ethernet Service Requirements	Required	5.10.4.6	Met	
	VLAN Requirements	Required	5.10.4.7	Met	
	Link Aggregation	Required	5.10.4.8	Met	
	Link Layer Discovery Protocol (LLDP)	Required	5.10.4.9	Partially Met ⁶	
4	Storage Array Network (SAN) Interface Requirements				
	Fiber Channel (FC) Physical Interfaces	Conditional	5.10.5.1	Not Tested ²	

Table 2-5. Data Storage Controller CRs and FRs Status (continued)

CR/FR ID	Capability/Function	Applicability	UCR Reference ¹	Status	Remarks
5	Converged Network Adapter (CAN) Interface Requirements				
	FCoE Services	Conditional	5.10.6.1	Not Tested ²	
	Data Center Bridging (DCB) Table 5.10.6-1	Conditional	5.10.6.2	Not Tested ²	
6	IP Networking Requirements				
	IPv6 Requirements as defined in Section 5.3.5.5	Required	5.10.7.1	Met ^{1,7}	
	Replication (mirroring) Session Traffic Per Table 5.10.7-1	Required	5.10.7.3	Met ¹	
	Congestion Control	Required	5.10.7.4	Met ¹	
7	Name Services Requirements				
	Lightweight Directory Access Protocol (LDAP)	Required	5.10.8.1	Met ⁷	
	Kerberos Authentication	Required	5.10.8.2	Met	
	Domain Name System (DNS) Functionality	Required	5.10.8.3	Met	
	DNS Load Balancing	Required	5.10.8.4	Met	
	Network Information Service (NIS) Functionality	Required	5.10.8.5	Met ⁷	
	NIS Netgroups Functionality	Required	5.10.8.6	Met ⁷	
	NetBIOS over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS)	Conditional	5.10.8.7	Met	
	Internet Storage Name Service (iSNS) Functionality	Required	5.10.8.8	Met ¹	
FC Name and Zone Service	Required	5.10.8.9	Not Tested ⁸		
8	Security Services Requirements				
	IPSec	Conditional	5.10.9.1	Met ¹	
	Encapsulating Security Payload (ESP)	Conditional	5.10.9.2	Met ¹	
	Internet Key Exchange version 2 (IKEv2)	Conditional	5.10.9.3	Met ¹	
	The Packet Filter Service	Conditional	5.10.9.4	Not Tested ²	
	DoD Host-Based Security System (HBSS) Software	Conditional	5.10.9.5	Not Tested ²	
	Data Encryption	Required	5.10.9.6	Met ⁷	
STIGs Compliance	Required	5.10.9.7	Met ⁷		
9	Interoperability Requirements				
	IP ASLAN and DISN WAN Networks	Required	5.10.10.1	Met	
	Application Programming Interface (API)	Required	5.10.10.2	Met	
10	Class of Service (CoS) and Quality of Service (QoS) Requirements				
	Layer 2 CoS and QoS Markings	Required	5.10.11.1	Not Met ⁹	
	Layer 3 CoS and QoS Markings	Required	5.10.11.2	Met	
11	Virtualization Requirements				
	Virtualized Data Storage Controller (vDSC) Functionality	Conditional	5.10.12.1	Not Tested	
	Private Networking Domains (PNDs)	Conditional	5.10.12.2	Not Tested	
	Individual Command Line Interface (CLI)	Conditional	5.10.12.3	Not Tested	

Table 2-5. Data Storage Controller CRs and FRs Status (continued)

	API Commands	Conditional	5.10.12.4	Not Tested	
	GNS	Conditional	5.10.12.5	Not Tested	
NOTES:					
<p>1. This UCR Requirement is met by vendor letter of compliance (LoC).</p> <p>2. This requirement is conditional, was not tested, and therefore is not certified for use.</p> <p>3. The SUT has no WEB Server functionality in the tested configuration and therefore is not certified for WebDAV.</p> <p>4. Representational State Transfer (REST) for distributed hypermedia systems and Cloud-Based functionalities are not included in this SUT and therefore the SUT is not certified for REST or CDMI.</p> <p>5. Global Name Space is not natively supported on the Data ONTAP filer for Version 7.3.6. On 4 May 2012, DISA adjudicated this as minor with a condition of field (COF) and POA&M. The COF is that a secondary component like a load balancer with global load balancing capability may be used. The POA&M is the software release of Data ONTAP version 8.2, which is projected to occur in third quarter 2013, with Global Name Space functionality included.</p> <p>6. The Ethernet services of the SUT only provide LLDP via the Cisco Discovery Protocol (CDP) In lieu of LLDP, which was adjudicated as a minor issue. On 28 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from “required” to “conditional” in a future version of the UCR and also because the implementation of discovery protocol (LLDP or CDP) is dependent upon the infrastructure that the DSC connects to. Therefore, the procurement requirements for DSC should specify the needed discovery protocol.</p> <p>7. The test results for this requirement were published in a separate report. See reference (E).</p> <p>8. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from “required” to “conditional” to be consistent with all other fiber channel requirements for a DSC. This requirement will change to condition in UCR 2013.</p> <p>9. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from “required” to “conditional” to align on layer 3 queuing for QoS and no longer requiring layer 2 CoS marking. This requirement will change to condition in UCR 2013.</p>					
LEGEND:					
ASLAN	Assured Service Local Area Network	IP	Internet Protocol		
API	Application Programming Interface	IPSEC	Internet Protocol Security		
CDMI	Cloud Data Management Interface	IPv6	Internet Protocol Version 6		
CDP	Cisco Discovery Protocol	iSCSI	Internet Small Computer System Interface		
CLI	Individual Command Line Interface	iSNS	Internet Storage Name Service		
CNA	Converged Network Adaptor	IWF	Interworking Function		
CoS	Class Of Service	LDAP	Lightweight Directory Access Protocol		
CR	Capability Requirement	LLDP	Link Layer Discovery Protocol		
DCB	Data Center Bridging	NAS	Network Attached Storage		
DISN	Defense Information Systems Network	NBT	NetBIOS Over TCP/IP		
DNS	Domain Name System	NIS	Network Information Service		
DoD	Department Of Defense	PND	Private Networking Domains		
DR	Disaster Recovery	QoS	Quality Of Service		
DSC	Data Storage Controller	RAID	Redundant Array Of Independent Disks		
ESP	Encapsulating Security Payload	REST	Representational State Transfer		
FC	Fibre Channel	SAN	Storage Array Network		
FCP	FC Protocol	SNMPv3	Simple Network Management Protocol Version 3		
FCoE	FC Over Ethernet	SSHv2	Secure Shell Version 2		
FC	Fibre Channel	SSL	Secure Socket Layer		
FCP	FC Protocol	STIG	Security Technical Implementation Guide		
FR	Functional Requirement	TCP/IP	Transmission Control Protocol/Internet Protocol		
GbE	Gigabit Ethernet	UCR	Unified Capabilities Requirements		
GNS	Global Name Space	vDSC	Virtualized Data Storage Controller		
HBSS	Host-Based Security System	VLAN	Virtual Local Area Network		
HTTPS	Hypertext Transport Protocol Secure	WAN	Wide Area Network		
ID	Identification	WebDAV	Web-Based Distributed Authoring And Versioning		
IKEv2	Internet Key Exchange Version 2	WINS	Windows Internet Name Service		

a. Storage System Requirements.

(1) UCR reference 5.10.2.1, Redundant Array of Independent Disks (RAID).

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 (SAS) and FC drives, although stronger RAID levels are acceptable. The SUT met this requirement with both testing and the vendor's LoC.

(2) UCR reference 5.10.2.1, 5.10.2.2, High Availability. The system shall be capable of 99.9 percent availability in High Availability (HA) mode. The SUT met this requirement with the vendor's LoC.

(3) UCR reference 5.10.2.3, Management Control. 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 also 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 testing.

(4) UCR reference 5.10.2.4, Data Storage Replication. The system shall provide data storage replication (e.g., mirroring) services (IPv4 and 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 planning (COOP). The SUT met this requirement with testing.

(5) UCR reference 5.10.2.4.1, Data Storage Backup. 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.

(6) UCR reference 5.10.2.4.2, Replication. 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.

(7) UCR reference 5.10.2.4.3, Disaster Recovery (DR). 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.

(8) UCR reference 5.10.2.5, Configuration Modes. 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 Table 5.10.2-1, Replication Operation Modes. The SUT met this requirement with testing.

b. Storage Protocol Requirements.

(1) UCR reference 5.10.3.1, Network File System (NFSv3). The system shall provide a Network File System version 3 (NFSv3) server for file systems data I/O. The SUT met this requirement with testing.

(2) UCR reference 5.10.3.2, Network File System (NFSv4). The system shall provide a Network File System version 4 (NFSv4) server for file systems data I/O. The SUT met this requirement with testing.

(3) UCR reference 5.10.3.3, Network File System (NFSv4.1) The system shall provide a Network File System version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O. This requirement is conditional, was not tested, and therefore is not certified for use.

(4) UCR reference 5.10.3.4, Common Internet File System (CIFSv1.0). The system shall provide a Common Internet File System version 1.0 (CIFSv1.0) server for file systems data I/O. The SUT met this requirement with testing.

(5) UCR reference 5.10.3.5, Common Internet File System (CIFSv2.0). The system shall provide a Common Internet File System version 2.0 (CIFSv2.0) server for file systems data I/O. The SUT met this requirement with testing.

(6) UCR reference 5.10.3.6, Internet Small computer system Interface (iSCSI). The system shall provide Internet Small Computer System Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators). The SUT met this requirement with vendor's LoC.

(7) UCR reference 5.10.3.7, Fibre Channel (FC) Protocol. The system shall provide Fibre Channel Protocol (FCP) server (target) operations for data I/O of FCP LUNs to clients (initiators). This requirement is conditional, was not tested, and therefore is not certified for use.

(8) UCR reference 5.10.3.8, Fibre Channel over Ethernet (FCoE). The system shall provide Fibre Channel over Ethernet (FCoE) server (target) operations for data I/O of FCP LUNs to clients (initiators).). This requirement is conditional, was not tested, and therefore is not certified for use.

(9) UCR reference 5.10.3.9, HTTPS Server. The system shall provide a HyperText Transport Protocol Secure (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 Transport Layer Security (TLS), per IETF RFC 5246, and shall comply with Section 5.4, Information Assurance Requirements, for that protocol. This requirement is conditional, was not tested, and therefore is not certified for use.

(10) UCR reference, 5.10.3.10, SSHv2 or SSL Implementation. The system shall provide Secure Shell version 2 (SSHv2) or SSL for management access to the storage controller operating system. The SSHv2 or SSL implementation shall comply with Section 5.4, Information Assurance Requirements, for that protocol. The SUT met this requirement with testing.

(11) UCR reference 5.10.3.11, Web-based Distributed Authoring and Versioning (WebDAV). The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures. This requirement is conditional, was not tested, and therefore is not certified for use.

(12) UCR reference 5.10.3.12, Representational State Transfer (REST). The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures. This requirement is conditional, was not tested, and therefore is not certified for use.

(13) UCR reference 5.10.3.13, Cloud Data Management Interface (CDMI). The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard. This requirement is conditional, was not tested, and therefore is not certified for use.

(14) UCR reference 5.10.3.14, Global Name Space (GNS) functionality. 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 SUT did not meet this requirement. Global name space is not natively supported on the DATA ONTAP filer for version 7.3.6. On 4 May 2012, DISA adjudicated this as minor with a Condition of Fielding (COF) and POA&M. The COF is that a secondary component like a load balancer with global load balancing capability may be used. The POA&M is the release of DATA ONTAP version 8.2 projected to occur in third quarter 2013.

c. Network Attached Storage (NAS) Interface Requirements.

(1) UCR reference 5.10.4.1, Gigabit Ethernet (GbE) and 10 GbE Services. The system shall provide physical interfaces for Gigabit Ethernet (GE) and 10 Gigabit Ethernet (10 GbE) services in conformance with IEEE 802.3 for Ethernet LAN interfaces. The SUT met this requirement with testing.

(2) UCR reference 5.10.4.2, Provision, Monitor and Detect Faults, and Restore Ethernet. 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 testing.

(3) UCR reference 5.10.4.3, SSHv2, SSL, HTTPS, and SNMPV3 Protocols. The system shall provide physical interfaces for out-of-band management (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 5.4, Information Assurance Requirements. The SUT met this requirement with testing.

(4) UCR reference 5.10.4.4, Auto-sensing, Auto-detecting, and Auto-configuring. When the system uses Ethernet, Fast Ethernet, GE, and 10 GbE interfaces, the interfaces shall be auto-sensing, auto-detecting and auto-configuring with incoming and corresponding Ethernet link negotiation signals. The SUT met this requirement with testing.

(5) UCR reference 5.10.4.5, Ethernet Services and Logical Link IWF. Ethernet services of the system and the Logical Link IWF of the system shall terminate the MAC layer of Ethernet as described in Ethernet Standard IEEE 802.3. The SUT met this requirement with vendor's LoC.

(6) UCR reference 5.10.4.6, Ethernet Service Requirements. 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 VLAN tag (4 bytes), and the 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 requirement with testing.

(7) UCR reference 5.10.4.7, VLAN Requirements. Ethernet services of the system shall provide VLANs, as per IEEE 802.1Q, and shall allocate a unique Ethernet MAC address to each VLAN. The SUT met this requirement with testing.

(8) UCR reference 5.10.4.8, Link Aggregation. 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 testing.

(9) UCR reference 5.10.4.9, Link Layer Discovery Protocol (LLDP). Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB. The SUT partially met this requirement with testing. The SUT only provides Cisco Discovery Protocol (CDP). On 28 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from "required" to "conditional" in a future version of the UCR and also because the implementation of discovery protocol (LLDP or CDP) is dependent upon the infrastructure that the DSC connects to. Therefore, the procurement requirements for DSC should specify the needed discovery protocol.

d. Storage Array Network (SAN) Interface Requirements.

(1) UCR reference 5.10.5.1, Fiber Channel (FC) Physical Interfaces. The system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per ANSI X3.230, X3.297, and X3.303. This requirement is conditional, was not tested, therefore, is not certified for use.

e. Converged Network Adapter (CNA) Interface Requirements.

(1) UCR reference 5.10.6.1, FCoE Services. The system shall provide physical interfaces for FCoE services over a 10 GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). This requirement is conditional, was not tested, therefore, is not certified for use.

(2) UCR reference 5.10.6.2, Data Center Bridging (DCB) Table 5.10.6-1. 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 5.10.6-1, Physical Interfaces for Data Center Bridging. This requirement is conditional, was not tested, therefore, is not certified for use.

f. Internet Protocol (IP) Networking Requirements.

(1) UCR reference 5.10.7.1, IPv6 Requirements as defined in Section 5.3.5.5. The system shall meet the IPv6 requirements defined in Section 5.3.5.5, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance. The IPv6 test results were published in a separate report. See reference (e).

(2) UCR reference 5.10.7.3, Replication (mirroring) Session Traffic Per Table 5.10.7-1. The system shall provide statically provisioned or dynamically adjusted large IP packets 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 2,048 KB per replication (mirroring) session. The system shall provide a statically provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8,192 KB per replication (mirroring) session. These IP packets receive buffer size requirements are conceptually based on either the Satellite or Transoceanic and Terrestrial Fiber Optic Cable E2E IP transport path models as depicted in Table 5.10.7-1, IP End-to-End Transport Path Models. The SUT met this requirement with vendor's LoC.

(3) UCR reference 5.10.7.4, Congestion Control. The system shall provide an optimized congestion control (congestion avoidance) algorithm in 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 vendor's LoC.

g. Name Services Requirements.

(1) UCR reference 5.10.8.1, Lightweight Directory Access Protocol (LDAP). The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510. The LDAP test results were published in a separate report. See reference (e).

(2) UCR reference 5.10.8.2, Kerberos Authentication. The system shall provide Kerberos authentication service per IETF RFC 4120. The Kerberos test results were published in a separate report. See reference (e).

(3) UCR reference 5.10.8.3, Domain Name System (DNS) Functionality. The system shall provide Domain Name System (DNS) client functionality. The SUT met this requirement with testing.

(4) UCR reference 5.10.8.4, DNS Load Balancing. The system shall provide DNS client-side Load Balancing. The SUT met this requirement with testing.

(5) UCR reference 5.10.8.5, Network Information Service (NIS) Functionality. The system shall provide Network Information Service (NIS) client directory service functionality. The NIS test results were published in a separate report. See reference (e).

(6) UCR reference 5.10.8.6, NIS Netgroups Functionality. The system shall provide NIS Netgroups client directory service functionality. The NIS Netgroups test results were published in a separate report. See reference (e).

(7) UCR reference 5.10.8.7, NetBIOS over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS). The system shall provide NetBIOS over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS). The SUT met this requirement with testing.

(8) UCR reference 5.10.8.8, Internet Storage Name Service (iSNS) Functionality. The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171. The SUT met this requirement with a vendor's LoC.

UCR reference 5.10.8.9, FC Name and Zone Service. The system shall provide FC Name and Zone Service. The SUT was not tested for this requirement. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from "required" to "conditional" to be consistent with all other fiber channel requirements for a DSC. This requirement will change to condition in UCR 2013.

h. Security Services Requirements.

(1) UCR reference 5.10.9.1, IPsec. The system shall provide IPsec per RFC 4301. This requirement is conditional, was not tested, and therefore, not certified for use.

(2) UCR reference 5.10.9.2, Encapsulating Security Payload (ESP). The system shall provide Encapsulating Security Payload (ESP) per RFC 4303. This requirement is conditional, was not tested, and therefore, not certified for use.

(3) UCR reference 5.10.9.3, Internet Key Exchange version 2 (IKEv2). The system shall provide Internet Key Exchange Version 2 (IKEv2) per RFC 4306. This requirement is conditional, was not tested, and therefore, not certified for use.

(4) UCR reference 5.10.9.4, Packet Filter Service. 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 the 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. This requirement is conditional, was not tested, and therefore, not certified for use.

(5) UCR reference 5.10.9.5, DoD Host-Based Security System (HBSS) Software. The system shall provide work with the DoD Host-Based Security System (HBSS) software to protect data stored in the file systems in the attached disk array. This requirement is conditional, was not tested, and therefore, not certified for use.

(6) UCR reference 5.10.9.6, Data Encryption. The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with FIPS 140-2 level 1 or higher to provide the following capabilities:

- Rapid crypto-shredding (destruction) of data, in accordance with NIST 800-88, for tactical systems that operate in harm's way and may fall into enemy hands
- Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place

The test results for this requirement were published in a separate report, reference (e).

(7) UCR reference 5.10.9.7, STIGs Compliance. The system shall comply with all appropriate STIGs to include the "Database Security Technical Implementation Guide." The DISA STIGs test results were published in a separate report. See reference (e).

i. Interoperability Requirements.

(1) UCR reference 5.10.10.1, IP ASLAN and DISN WAN Networks. The system user interfaces, software, firmware, and hardware shall be compatible and interoperable with traffic transport and protection mechanisms of IP ASLAN and DISN WAN networks. The SUT met this requirement with testing.

(2) UCR reference 5.10.10.2, Application Programming Interface (API). 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., XML) shall be subject to the specific vendor system operating system implementation. The SUT met this requirement with testing.

j. Class of Service (CoS) and Quality of Service (QoS) Requirements.

(1) UCR reference 5.10.11.1, Layer 2 CoS and QoS Markings. 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 5.3.1.3.3, Class of Service Markings, and Section 5.3.1.3.4, 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, listed as follows and as offered by the system: NFSv3, NFSv4, NFSv4.1, CIFSv1.0, CIFSv2.0, iSCSI, FCoE, HTTP/HTTPS/REST, SFTP, FTPS, SSHv2, SNMPv2, SNMPv3, and user-defined protocols (e.g., proprietary system to system mirroring protocol). The marking is made in Ethernet VLAN tags by setting the priority value to between zero and seven, inclusive for various traffic classes. 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 did not meet the requirement. The SUT does not provide support for CoS/802.1p frame tagging. On 12 September 2012, DISA adjudicated this issue as minor because this requirement will be changed from "required" to "conditional" to align on layer 3 queuing for QoS and no longer requiring layer 2 CoS marking. This requirement will change to condition in UCR 2013.

(2) UCR reference 5.10.11.2, Layer 2 CoS and QoS Markings. The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 5.3.3, Network Infrastructure End-to-End Performance Requirements. 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 protocol types listed as follows: NFSv3, NFSv4, NFSv4.1, CIFSv1.0, CIFSv2.0, iSCSI, FCoE, HTTP/HTTPS/REST, FTPS, SFTP, SSHv2, SNMPv2, SNMPv3 User-defined protocols (e.g., proprietary system to system mirroring protocol). The IP packets are marked in the TOS field of the IPv6 packet header with 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 testing.

k. Virtualization Requirements.

(1) UCR reference 5.10.12.1, Virtualized Data Storage Controller (vDSC) Functionality. 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. Examples include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations. This requirement is conditional, was not tested, and therefore, not certified for use.

(2) UCR reference 5.10.12.2, Private Networking Domains (PNDs). 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. This requirement is conditional, was not tested, and therefore, not certified for use.

(3) UCR reference 5.10.12.3, Individual Command Line Interface (CLI). 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. This requirement is conditional, was not tested, and therefore, not certified for use.

(4) UCR reference 5.10.12.4, API Commands. 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. This requirement is conditional, was not tested, and therefore, not certified for use.

(5) UCR reference 5.10.12.5, GNS. 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 NAS 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. This requirement is conditional, was not tested, and therefore, not certified for use.

11.3 Information Assurance. The IA report is published in a separate report, Reference (e).

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System 2-7 Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.