Military Unique Deployment Guide

Data Storage Controller (DSC)

ONTAP version 9.1 (Clustered)

NetApp, Inc.
September 2017

Draft

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TABLE OF EXAMPLES

Change Control History

Submit recommended comments / changes to this document to ng-prodops-security@netapp.com.

Table 1) Version History

Version	Date	Comments
0.1	30 Apr 2017	Initial draft
1.0	15 Sep 2017	Updated to reflect final tested config as of IO V&V (8/30/17)

About This Guide

Items in **Shaded Highlight** denote example values which must be changed to conform to those values specific to the site in which the storage arrays are located (JITC test site, for example).

Items prefaced with **Important!**, whether as notes or other text, are of extreme importance. They convey important information which may be of a critical nature. Please take notice.

```
Items within gray shaded boxes depict either storage array console output or cli commands which
must be executed as part of the configuration process.
```

Notes to technican performing setup

Note: The configuration steps, outlined in this guide, should be performed in the sequence as presented. Many of these steps are prerequisite to those that follow.

Important! Use the cluster built-in, default 'admin' user account to perform the setup of one or more Data ONTAP cluster(s). Upon setup completion, the final procedure will disable the 'admin' account, and no further access via that account will be enabled.

Glossary of Terms

Table 2) Glossary

Term	Definition
CS	Cybersecurity
DSC	Data Storage Controller
FAS	Fabric Attached Storage – A family of hardware data storage controllers (DSCs) running NetApp's Data ONTAP software
HA pair	HA pairs provide hardware redundancy that is required for nondisruptive operations and fault tolerance and give each node in the pair the software functionality to take over its partner's storage and subsequently give back the storage
Data ONTAP Cluster	A group of DSCs (up to 12 HA pairs) functioning as one (1) homogenous data storage array
Service Processor (SP)	Integral embedded processor, in each DSC, used for hardware monitoring and basic maintenance/diagnostic access
SVM	Storage Virtual Machine – A virtual instance, running within the cluster, which performs specific storage array functions within its own context. Such functions include cluster management, individual node management, and data service.
NAS	Network Attached Storage (i.e.: CIFS and NFS)
SAN	Storage Area Network (i.e.: FC, FCoE, and iSCSI)

Term	Definition
LIF	Logical interface instance assigned to an SVM and attached to a physical network interface. This logical interface has a specific Firewall Policy assigned and operates within the constraints of that policy
Firewall Policy	A policy definition of which protocols may or may not traverse LIFs on which the policy is attached. This policy may also limit in scope the networks or hosts allowed to access the interface
UC	Defense Unified Capabilities
DISA	Defense Information Systems Agency
DoD	U.S. Department of Defense
JITC	Joint Interoperability Test Command
STIG	Security and Technical Implementation Guidance
RAE	Required Ancillary Equipment

1 Conditions of Fielding

When the system is deployed in an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the site's Designated Approving Authority:

a. The system must be integrated into the site's AD environment for authentication and authorization requirements. If AD is not incorporated, the following findings will be included in the site's architecture:

Network Device Management SRG:

- SRG-APP-000023-NDM-000205, Category (CAT) II (x2), NetApp FAS8040 (x2)
- SRG-APP-000024-NDM-000206, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000025-NDM-000207, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000026-NDM-000208, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000027-NDM-000209, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000028-NDM-000210, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000029-NDM-000211, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000033-NDM-000212, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000038-NDM-000213, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000148-NDM-000246, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000153-NDM-000249, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000156-NDM-000250, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000291-NDM-000275, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000292-NDM-000276, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000293-NDM-000277, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000294-NDM-000278, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000317-NDM-000282, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000319-NDM-000283, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000320-NDM-000284, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000329-NDM-000287, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000396-NDM-000311, CAT II (x2), NetApp FAS8040 (x2)

- SRG-APP-000170-NDM-000329, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000516-NDM-000336, CAT II (x2), NetApp FAS8040 (x2)

b. The site must use a Syslog device for auditing purposes. If Syslog is not incorporated, the following findings will be included in the site's architecture:

Storage Area Network:

- SRG-APP-000108-NDM-000232, CAT II (x2), NetApp FAS8040 (x2)
- SRG-APP-000125-NDM-000241, CAT II (x2), NetApp FAS8040 (x2)
- SAN04.020.00, CAT II (x2), NetApp FAS8040 (x2)

c. The site must use role-based security for user access and management of the vendor's device.

d. The site must disable all local user accounts on the device after initial setup/configuration with the exception of one emergency administrative account.

e. The site must ensure that the emergency administrative account's userid and password are locked up in separate safes, both of which are not accessible by any one individual, and procedures are implemented to log all access and usage.

f. The site must ensure that the emergency administrative account meets all DoD userid and password complexity requirements.

g. The site must ensure all unused ports are closed.

h. The site must use a STIG-compliant CAC-enabled workstation for management of the solution.

i. The configuration must be in compliance with the NetApp Inc. ONTAP military-unique features deployment guide.

j. The site must disable HTTPS and SNMP.

k. The site must register the system in the Systems Networks Approval Process Database <https://snap.dod.mil/index.cfm> as directed by the DoD Security Accreditation Working Group and Program Management Office.

2 Overview

The NetApp family of ONTAP 9.1 supported Data Storage Controllers (DSCs) includes the 17 models listed in table 3.

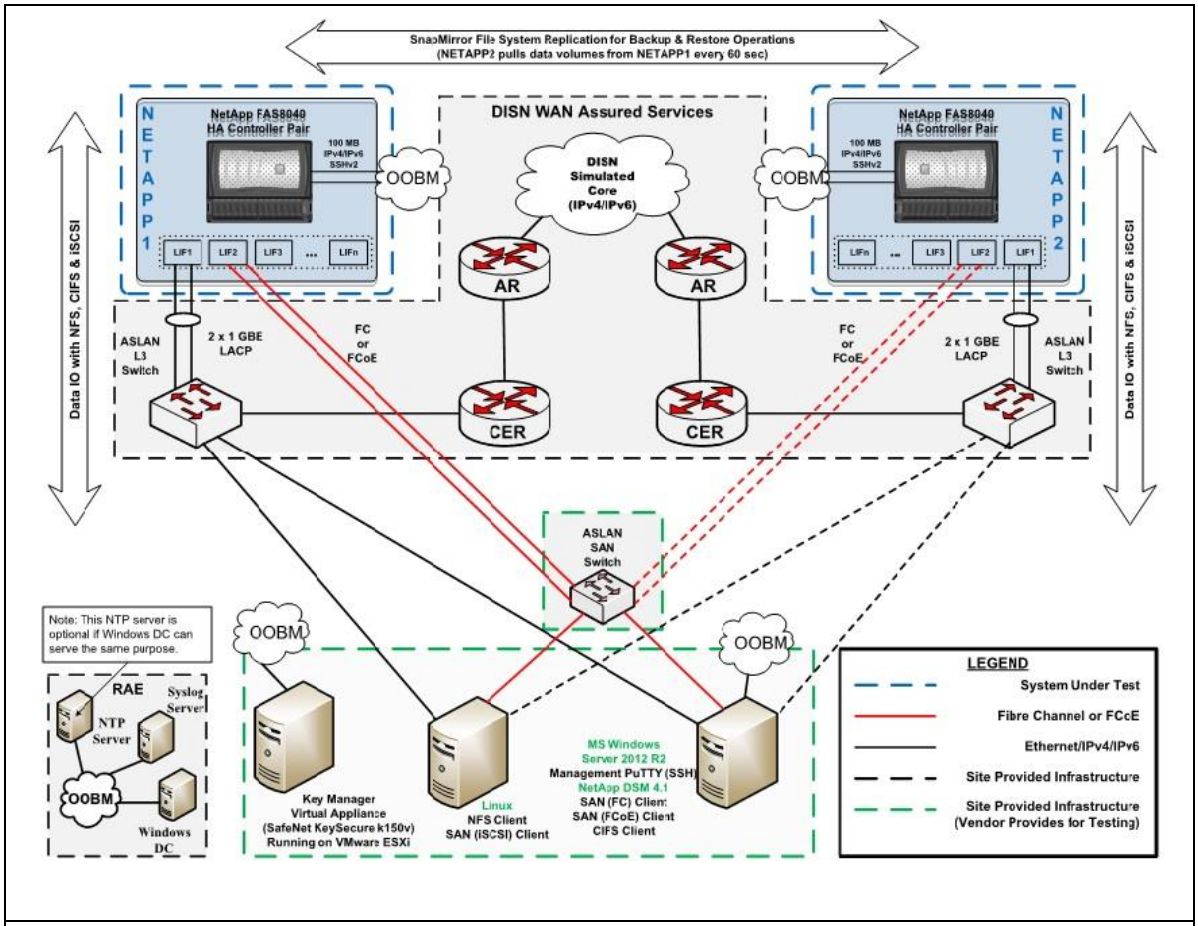
Table 3) ONTAP 9.1 Supported Platforms

Fabric Attached Storage (FAS) Models	All Flash FAS (AFF) Models
FAS2520	AFF A200
FAS2552	AFF A300
FAS2554	AFF A700
FAS2620	AFF A700s
FAS2650	AFF8040
FAS8020	AFF8080 EX
FAS8040	
FAS8060	
FAS8080 EX	
FAS8200	
FAS9000	

The DoD Unified Capabilities (UC) testing program - run by the Joint Interoperability Test Command (JITC) and the DoD Information Systems Agency (DISA) – require the distribution of a Deployment Guide. This Deployment Guide annotates the various conditions of fielding, specific configuration for hardening and Information Assurance (IA) in concert with the DISA Security and Technical Implementation Guidance (STIG), and DoD-site specific Required Ancillary Equipment (RAE) needed for full compliance.

3 Test Configuration

Figure 1) Test configuration, components, and connectivity schemes



Legend:

AR	Access Router	IP	Internet Protocol
ASLAN	Assured Service Local Area Network	L	Layer
CER	Customer Edge Router	LACP	Link Aggregation Control Protocol
CIFS	Common Internet File System	LF	Line Feed
DISA	Defense Information Systems Agency	OOBM	Out of Band Management
FAS	Fabric Attached Storage	NFS	Network File System
FC	Fibre Channel	NTP	Network Time Protocol
FCoE	Fibre Channel over Ethernet	RAE	Required Ancillary Equipment
GBE	Gigabit Ethernet	SAN	Storage Area Network
IO	Input Output	WAN	Wide Area Network
ISCSI	Internet Small Computer Interface		

4 Pre-Hardening Deployment Requirements

Complete the following prior to the detailed configuration procedures in section 5:

1. Complete the physical install and cabling of the Data Storage Controllers (DSCs)
2. Complete the initial setup of the clustered DSCs using the Data ONTAP 'cluster setup' software wizard. Refer to the ONTAP9 Software Setup Guide for cluster configuration (https://library.netapp.com/ecm/ecm_download_file/ECMLP2492611).

Note: The cluster setup wizard must be run on the initial node on which the cluster will be created. Once created, the additional nodes should be "joined" using the cluster setup wizard and the "join" option.

3. Run `cluster image show` command to verify that the DSC system is running ONTAP version 9.1.

Note: As part of the DoD hardening guidance the use of NSE drives is recommended using an external Key management solution such as Gemalto. Detailed NSE configuration should reference the NetApp Storage Encryption: Preinstallation Requirements and Procedures for SafeNet KeySecure Guide. https://safenet.gemalto.com/resources/integration-guide/data-protection/NetApp_Storage_Encryption__Preinstallation_Requirements_and_Procedures_for_SafeNet_KeySecure/.

5 Detailed Configuration Procedures

5.1 Verify / Enable Support for IPv6

IPv6 is a requirement for DoD approved systems and is disabled by default IPv6 in ONTAP 9.1.

Verify that IPv6 support has been enabled for the cluster:

```
Ntap-ontap91::> network options ipv6 show
IPv6 Enabled: true
Ntap-ontap91::>
```

If IPv6 enabled is `false`, then enable IPv6:

```
Ntap-ontap91::> network options ipv6 modify -enabled true
```

Once IPv6 is enabled, configure the required interfaces with the respective IPv6 addresses.

Important! Once IPv6 support is enabled for the cluster, the cluster setup wizard will no longer function, as it does not support IPv6.

5.2 Secure the Cluster Node(s) Service Processors (SPs)

Access the SP CLI (command line interface) using one of following methods:

- Connection to the controller serial interface
- SSH to the SP (via the cluster node e0M interface) (see note)

Note: A second IP address defined for the eoM interface is required for SSH access to the SP. Do not confuse this with the IP address assigned for normal network access.

For each node in the cluster, secure the SP using the commands in example 1.

Example 1) Commands to Secure the DSC's SP

```
Ntap-ontap91::> system service-processor network modify -node stl-IAC-cDOT-1-01 -address-family
IPv6 -enable false -dhcp none -ip-address 0::0 -prefix-length 64
Ntap-ontap91::> system service-processor network modify -node stl-IAC-cDOT-1-02 -address-family
IPv6 -enable false -dhcp none -ip-address 0::0 -prefix-length 64
```

Note: The commands shown above are too long to display in this document. Enter the entire command before hitting the return key.

Note: Only the emergency (serial console access) local administrative account will be granted the capability of “login-sp”, allowing login access to the SP.

5.3 Disable Autosupport “Call Home”

NetApp Autosupport is disabled by default in ONTAP 9.1. This function exists on each member node.

1. Use `autosupport show` command to verify the current state (enabled or disabled) as follows:

```
Ntap-ontap91::> system node autosupport show
Node                State     From          To            Mail Hosts
------------------- --------- ------------- ------------- ----------
Ntap-ontap91-01     enable    Postmaster    -             mailhost
Ntap-ontap91-02     enable    Postmaster    -             mailhost
2 entries were displayed.
```

2. If Autosupport enabled, disable Autosupport for each member node per example 2.

Example 2) Disable Autosupport

```
Ntap-ontap91-01::> system node autosupport modify -node Ntap-ontap91-01 -state disable
Ntap-ontap91-02::> system node autosupport modify -node Ntap-ontap91-02 -state disable
```

3. Run `autosupport show` command again to verify that Autosupport is disabled.

5.4 Cluster Default SVMs

A cluster contains three types of SVMs: Admin, Node, and Data.

- **Admin SVM**: The cluster setup process automatically creates the admin SVM for the cluster. The admin SVM represents the cluster.
- **Node SVM**: A node SVM is created when the node joins the cluster, and the node SVM represents the individual nodes of the cluster.
- **Data SVM**: A data SVM represents the data serving SVMs.

After cluster setup, the cluster administrator must manually create:

- One SVM to run the CIFS service that provides access to a Microsoft Active Directory Domain for storage administrator authentication.
- One or more SVMs as required to serve data and add volumes to these SVMs to enable data access from the cluster.

Note: A cluster must have at least one data SVM to serve data to its clients.

5.5 Setup SSH Encryption Ciphers and Key Exchange Algorithms

ONTAP supports multiple SSH encryption ciphers and key exchange algorithms that can be modified / restricted as required to comply with organizational security policy.

Note: DISA prohibits Cipher-Block Chaining (CBC) mode of operation (see example 3 ciphers in red).

Table 4) Installed Encryption Ciphers and Key Exchange Algorithms

Encryption Cipher	Key Exchange Algorithm	MAC Algorithms
aes256-ctr	diffie-hellman-group-exchange-sha256	hmac-sha1
aes192-ctr	diffie-hellman-group-exchange-sha1	hmac-sha1-96
aes128-ctr	diffie-hellman-group14-sha1	hmac-sha2-256
aes256-cbc	ecdh-sha2-nistp256	hmac-sha2-512

Encryption Cipher	Key Exchange Algorithm	MAC Algorithms
aes192-cbc	ecdh-sha2-nistp384	hmac-sha1-etm
aes128-cbc	ecdh-sha2-nistp521	hmac-sha1-96-etm
3des-cbc	ecdh	hmac-sha2-256-etm
aes128-gcm		hmac-sha2-512-etm
aes256-gcm		

1. Apply SSH ciphers and algorithms to each SVM where SSH access is possible (Cluster and Data).
2. Run `security ssh show` command to display ciphers and algorithms in use cluster-wide per example 3.

Example 3) SSH ciphers and algorithms in use cluster-wide

```
Vserver         Ciphers           Key Exchange Algorithms     MAC Algorithms
--------------- ----------------  --------------------------  --------------
Ntap-ontap91    aes256-ctr,       diffie-hellman-group-       hmac-sha1,
                aes192-ctr,       exchange-sha256,            hmac-sha1-96,
                aes128-ctr,       diffie-hellman-group-       hmac-sha2-256,
                aes256-cbc,       exchange-sha1,              hmac-sha2-512,
                aes192-cbc,       diffie-hellman-group14-     hmac-sha1-etm,
                aes128-cbc,       sha1, ecdh-sha2-nistp256,   hmac-sha1-96-etm,
                3des-cbc,         ecdh-sha2-nistp384,
                aes128-gcm,       ecdh-sha2-nistp521,         hmac-sha2-256--etm,
                aes256-gcm        curve25519-sha256           hmac-sha2-512-etm
```

3. Remove or restore SSH ciphers and algorithms as needed using the `security ssh modify` command.

Note: Modifying ciphers / algorithms with the `security ssh modify` command per example 4 updates the default list of ciphers / algorithms available to the Cluster SVM and newly created SVMs.

Example 4) Setting the Default Encryption Ciphers and Key Exchange Algorithms

```
Ntap-ontap91::> security ssh modify -vserver Ntap-ontap91 -key-exchange-algorithms diffie-
hellman-group-exchange-sha256 -ciphers aes256-ctr,aes192-ctr,aes128-ctr,aes128-gcm,aes256-gcm
Warning: You have updated the SSH configuration settings for admin Vserver "Ntap-ontap91". All
newly created data Vserver will inherit this new setting. To modify an individual data
Vserver's configuration, login as the Vserver admin user and use the "security ssh" commands.
```

4. Run `security ssh show` command again to verify list of available ciphers per example 5.

Example 5) Restricted list of SSH Ciphers and Key Exchange Algorithms

```
Vserver         Ciphers           Key Exchange Algorithms     MAC Algorithms
--------------- ----------------  --------------------------  --------------
Ntap-ontap91    aes256-ctr,       diffie-hellman-group-       hmac-sha1,
                aes192-ctr,       exchange-sha256             hmac-sha1-96,
                aes128-ctr,                                   hmac-sha2-256,
                aes128-gcm,                                   hmac-sha2-512,
                aes256-gcm                                    hmac-sha1-etm,
                                                              hmac-sha1-96-etm,
                                                              hmac-sha2-256-etm,
                                                              hmac-sha2-512-etm
```

5.6 Setup Secure Firewall Policies for the Administrative Access Interfaces

About Firewall Policies

Access to cluster network logical interfaces (LIFs) is controlled by firewall policies. Table 5 describes the four built-in policies created when Clustered Data ONTAP is installed.

Table 5) Built-In Firewall Policies

Policy	Description
cluster	This policy governs protocol access used for intracluster communications between the cluster nodes (apply to all intracluster LIFs)
data	This policy governs protocol access used by consumers of storage data (i.e.: clients) This policy should not be used directly on data interfaces (LIFs), but should be cloned and the clones modified for specific access needs (you may also create the policy from scratch)
intercluster	This policy governs protocol access when Data ONTAP cluster peering is in use
mgmt	This policy governs protocol access used on cluster management interfaces This policy should not be used directly on management interfaces (LIFs), but should be cloned and the clones modified for specific access needs (you may also create the policy from scratch)

Each policy is comprised of one or more protocol specifications specifying access lists of addresses allowed or denied access to that specific protocol. The supported protocols are: dns, http, https, ndmp, ntp, rsh, snmp, ssh, and telnet.

1. For **intracluster connections**, (i.e.: through the intracluster switches or for a switchless two-node cluster), NetApp recommends using the built-in cluster policy.
2. For **data and management connections**, NetApp recommends using the built-in data and mgmt policies as policy templates.
   a. Clone the policy templates into new policies
   b. Modify the new policies as required to meet the organization's security needs
   c. Replace the built-in policies with the new ones as appropriate on existing LIFs

Note: An administrator may optionally create new policies from scratch

Important! The built-in firewall policies cannot be deleted from the cluster. However, if not attached to any interfaces, they pose no security risk.

Firewall Policy Protocols

Firewall policy entries are comprised of a protocol type, a firewall action, and an address list to which the action applies.

The following network protocols may be managed by a firewall policy:

Table 6) Firewall Policy Protocols

Protocol	Actions	Address List Members
dns	Allow and/or deny	List of IPv4 and IPv6 addresses
http	Allow and/or deny	List of IPv4 and IPv6 addresses
https	Allow and/or deny	List of IPv4 and IPv6 addresses
ndmp	Allow and/or deny	List of IPv4 and IPv6 addresses
ntp	Allow and/or deny	List of IPv4 and IPv6 addresses
rsh	Allow and/or deny	List of IPv4 and IPv6 addresses
snmp	Allow and/or deny	List of IPv4 and IPv6 addresses
ssh	Allow and/or deny	List of IPv4 and IPv6 addresses
telnet	Allow and/or deny	List of IPv4 and IPv6 addresses

The address list for each policy entry is an access list of IPv4 and IPv6 networks and/or individual addresses associated with the policy. The IPv4 address 0.0.0.0/0 is a generic entry meaning all IPv4

networks and the addresses contained, therein. The IPv6 address ::/0 is a generic entry meaning all IPv6 networks and its related addresses.

Note: Firewall policies may contain a single action entry for allow, deny, or one of each type.

Note: Firewall policies for cluster and intercluster logical interfaces support IPv4 addresses only.

5.7 Creating the Management Access and Domain Access Firewall Policies

Create and enforce one management access policy on all management network logical interfaces. Multiple, unique, data policies may be created to fit the needs of the various data interfaces within the cluster. One of these data policies should be tailored specifically for Microsoft Active Directory Domain access (using CIFS) and used only for that purpose.

Management Access Policy

1. Define a secure firewall policy for management interfaces with `system services firewall policy create` command per example 6.

Example 6) Create Firewall Policy Entry

```
Ntap-ontap91::> system services firewall policy create -policy <policy-name> -service
<protocol_name> -action <allow | deny> -ip-list <IPv4 and/or IPv6 address list>
```

Note: The first command reference to a new policy will create the policy. Subsequent references will add additional entries to that policy.

The following table lists the desired entries for the secured management firewall policy `secure_mgmt`:

Table 7) Secure Management Firewall Policy Entry Settings

Protocol	Action	Access List	Net Effect
dns	allow	IP address list for allowed DNS servers	Allow DNS access to list
dns	deny	0.0.0.0/0, ::/0	Deny all except above allow list
http	deny	0.0.0.0/0, ::/0	Deny all
https	deny	0.0.0.0/0, ::/0	Deny all
ndmp	deny	0.0.0.0/0, ::/0	Deny all
ntp	allow	IP address list for allowed NTP servers	Allow NTP access to list
ntp	deny	0.0.0.0/0, ::/0	Deny all except above allow list
rsh	deny	0.0.0.0/0, ::/0	Deny all
snmp	deny	0.0.0.0/0, ::/0	Deny all
ssh	allow	IP address list for allowed SSH clients	Allow SSH access from list
ssh	deny	0.0.0.0/0, ::/0	Deny all except above allow list
telnet	deny	0.0.0.0/0, ::/0	Deny all

For this cluster, the following commands are used to create a policy named `secure_mgmt`:

Example 7) Create Firewall Policy 'secure_mgmt'

```
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service dns -action
allow -ip-list 10.63.165.0/24, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service dns -action
deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service http -action
deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service https -
action deny -ip-list 0.0.0.0/0, ::/0
```

```
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service ndmp -action
deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service ntp -action
allow -ip-list 10.63.165.0/24, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service ntp -action
deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service rsh -action
deny  -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service snmp -action
deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service ssh -action
allow -ip-list 10.63.165.0/24, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service ssh -action
deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy secure_mgmt -service telnet -
action deny -ip-list 0.0.0.0/0, ::/0
```

Note: The examples above are too long to display as a single command lines in this document. Do not press 'enter' until the entire command line has been entered.

2. Verify the policy action entries using the command in example 8.

Example 8) Show Firewall Policy `secure_mgmt`

```
Ntap-ontap91::> system services firewall policy> show -policy secure_mgmt
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
secure_mgmt
                 dns        allow  10.63.165.0/24, ::/0
                 dns        deny   0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       deny   0.0.0.0/0, ::/0
                 ntp        allow  10.63.165.0/24, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
                 snmp       deny   0.0.0.0/0, ::/0
                 ssh        allow  10.63.165.0/24, ::/0
                 ssh        deny   0.0.0.0/0, ::/0
                 telnet     deny   0.0.0.0/0, ::/0
12 entries were displayed.
```

Apply the Secure Management Policy to the 'eoM' Interface

This step applies the firewall policy for secure management in example 7 to the LIFs on the cluster and node management interfaces (e0M). Perform this step for the 'cluster' SVM and each 'cluster node' SVM:

For the cluster SVM use:

```
Ntap-ontap91::> network interface modify -vserver Ntap-ontap91-01 -lif cluster_mgmt -firewall-
policy secure_mgmt
```

For the node SVMs use:

```
Ntap-ontap91::> network interface modify -vserver Ntap-ontap91-01 -lif mgmt1 -firewall-policy
secure_mgmt
Ntap-ontap91::> network interface modify -vserver Ntap-ontap91-02 -lif mgmt1 -firewall-policy
secure_mgmt
```

The Microsoft Active Directory Domain Access Policy

Create a policy specifically for the SVM running CIFS protocol granting access to the Microsoft Active Directory Domain. The policy should have the following entries:

Table 8) Domain Access Firewall Policy Entry Settings

Protocol	Action	Access List	Net Effect
dns	allow	IP address list for allowed DNS servers	Allow DNS access to list
dns	deny	0.0.0.0/0, ::/0	Deny all except above allow list
http	Deny	0.0.0.0/0, ::/0	Deny all
https	deny	0.0.0.0/0, ::/0	Deny all
ndmp	deny	0.0.0.0/0, ::/0	Deny all
ntp	allow	IP address list for allowed NTP servers	Allow NTP access to list
ntp	deny	0.0.0.0/0, ::/0	Deny all except above allow list
rsh	deny	0.0.0.0/0, ::/0	Deny all
snmp	deny	0.0.0.0/0, ::/0	Deny all
ssh	deny	0.0.0.0/0, ::/0	Deny all
telnet	deny	0.0.0.0/0, ::/0	Deny all

For this cluster, use the following commands to create a policy named `domain_access`:

Example 9) Create Domain Access Firewall Policy

```
Ntap-ontap91::> system services firewall policy create -policy domain_access -service dns -
action allow -ip-list 192.168.0.0/24, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service dns -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service http -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service https -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service ndmp -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service ntp -
action allow -ip-list 192.168.0.0/24, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service ntp -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service rsh -
action deny  -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service snmp -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service ssh -
action deny -ip-list 0.0.0.0/0, ::/0
Ntap-ontap91::> system services firewall policy create -policy domain_access -service telnet -
action deny -ip-list 0.0.0.0/0, ::/0
```

Once the policy is created, verify the policy action entries using the command in example 10.

Example 10) Show Firewall Policy 'domain_access'

```
Ntap-ontap91::> system services firewall policy show -policy domain_access
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
domain_access
                 dns        allow  192.168.0.0/0, ::/0
                 dns        deny   0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       deny   0.0.0.0/0, ::/0
                 ntp        allow  192.168.0.0/0, ::/0
                 ntp        allow  0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
                 snmp       deny   0.0.0.0/0, ::/0
                 ssh        deny   0.0.0.0/0, ::/0
                 telnet     deny   0.0.0.0/0, ::/0
```

```
11 entries were displayed.
```

5.8 Create a CIFS SVM for Domain Access (Admin User Authentication)

About SVMs

ONTAP uses SVMs (Storage Virtual Machines) for several purposes. SVM functions are unique to the type of SVM.

Table 9) SVM Types

SVM Type	Purpose
Admin	• Cluster management • Does not run data access protocol services • Managed only by Cluster administrators • Automatically created at Cluster initialization
Node	• Individual member node management • Does not run data access protocol services • Managed only by Cluster administrators • Automatically created when member node joins the Cluster

Data	• Runs data access protocol services
	  ○ NAS (CIFS, NFS)
	  ○ SAN (iSCSI, FC, FCoE)
	• May be managed by Cluster administrators or designated SVM administrators
	• Created by Cluster administrators

An SVM must be created to run the CIFS protocol, allowing the cluster to authenticate management users against a Microsoft Active Directory Domain. This SVM can also be used to service data consumers (clients) using CIFS as the connection protocol. Once created and joined to a domain, the cluster management SVM can access the domain connection (via an internal tunnel) for management user account authorization. As Clustered Data ONTAP can allow multiple SVMs running CIFS services to multiple domains, it is important to select the correct SVM for use by the Cluster Domain-Tunnel.

This setup is a multi-step process as outlined in the sub-sections below:

Create the Domain Access SVM

```
Ntap-ontap91::> vserver create -vserver domain_access -rootvolume da_root -aggregate aggr1 -
rootvolume-security-style mixed
```

Create Network Interface Failover Group for Use by Network LIF (Domain Access)

Execute the following commands (one for each cluster node):

```
Ntap-ontap91::> network interface failover-groups create -failover-group da_fail_grp1 -node Ntap-
ontap91-01  -port e1b
Ntap-ontap91::> network interface failover-groups create -failover-group da_fail_grp1 -node Ntap-
ontap91-02 -port e1b
```

Create a Network LIF for Use by the SVM

```
Ntap-ontap91::> network interface create -vserver domain_access -lif lif_domain_access -role data
-data-protocol cifs -home-node Ntap-ontap91-01 -home-port e1b -address 192.168.1.81 -netmask
255.255.255.0 -status-admin up -firewall-policy domain_access -auto-revert true -failover-group
da_fail_grp1

Info: Your interface was created successfully; the routing group d192.168.1.0/24 was created
```

Create a Route Definition for Use by the LIF (if needed)

```
Ntap-ontap91::> network routing-groups route create -vserver domain_access -routing-group
d192.168.1.0/24 -destination 192.168.0.0/24 -gateway 192.168.1.1 -metric 20
```

Setup DNS for the SVM

```
Ntap-ontap91::> vserver services dns create -vserver domain_access -domains
iacerts.stl.netapp.com    -state enabled -timeout 2 -attempts 1 -name-servers 192.168.0.20
```

Create a CIFS Service on the SVM

```
Ntap-ontap91::> vserver cifs create -cifs-server DOMAIN_ACCESS_S -domain
iacerts.stl.netapp.com -ou CN=Computers -default-site "" -status-admin up -vserver
domain_access

In order to create an Active Directory machine account for the CIFS server, you must supply the
name and password of a Windows account with sufficient privileges to add computers to the
"CN=Computers" container within the "IACERTS.STL.NETAPP.COM" domain.

Enter the user name: Administrator

Enter the password: XXXXXXXXXXXXXX
```

Link the Cluster Management SVM to the Domain via a Domain-Tunnel

```
Ntap-ontap91::> security login domain-tunnel create -vserver domain_access
```

5.9 Network Time Protocol (NTP) Configuration

Per the DISA STIGs, NTP must use more than one server. It is assumed that the NTP servers will be on the same network sub-net as the Microsoft Active Directory Domain used for administrative user access. However, that is not a requirement. The only requirement is that the servers be reachable from logical interfaces which have a policy allowing the NTP protocol.

Use the `system services ntp server create` command to create NTP server references. You can use the `system services ntp server modify` command to modify existing server records. You must do this for each member node in the cluster.

To designate a particular NTP server as preferred, elevate your session privilege to “advanced”.

Use the following commands to set the configuration. Repeat for each member node:

Example 11) Setup NTP Server References

```
Ntap-ontap91::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when directed to do so
by NetApp personnel.
Do you want to continue? {y|n}: y
Ntap-ontap91::*> system services ntp server create -node Ntap-ontap91-01 -server 10.57.157.104
-version max -preferred true
Ntap-ontap91::*> system services ntp server create -node Ntap-ontap91-01 -server 10.57.158.104
-version max -preferred false
Ntap-ontap91::*> system services ntp server create -node Ntap-ontap91-02 -server 10.57.157.104
-version max -preferred true
Ntap-ontap91::*> system services ntp server create -node Ntap-ontap91-02 -server 10.57.158.104
-version max -preferred false
Ntap-ontap91::*> set -privilege admin
```

Note: The commands shown above are too long for the display in this document. Enter the entire command before hitting the return key. Substitute the appropriate IP address for the referenced NTP server.

5.10 Secure Shell (SSH) Configuration

There are several configuration categories related to SSH use. These are:

- Access lists
- Encryption ciphers and Key Exchange algorithms
- Session timeout

SSH access lists

Individual Hosts or sub-net IP addresses allowed to make SSH connections are controlled by the Firewall Policies applied to network interfaces (LIFs) where such connections occur.

SSH Encryption Ciphers and Key Exchange Algorithms

See section 5.5 Setup SSH Encryption Ciphers and Key Exchange Algorithms

Session Timeout

Enter the following command to view the current cli session timeout value (in minutes):

```
Ntap-ontap91::> system timeout show
CLI session timeout: 30 minutes
```

Set time value to 10 minutes (or a value specific to current security policy) using the following command:

```
Ntap-ontap91::> system timeout modify -timeout 10
```

Note: This session timeout also applies to console sessions.

5.11 Required Ancillary Equipment (RAE)

Many items in the DISA STIGs are met by using an RAE device. The specific RAE devices required by testing are:

- User authentication functions over LDAP (i.e.: Microsoft Windows Server 2008 R2, Active Directory)
- An external syslog server like RSYSLOG, Solarwinds, Kiwi Syslog Server, or Splunk.

MS AD Authentication Configuration

Using non-local user accounts (Microsoft Active Directory) for administrative access has several pre-requisites:

- The storage array must have a valid CIFS license installed.
- The CIFS service must be setup and be in a “running” state.
- The Active Directory User Accounts for the storage administrators must already exist
  - See Create Administrative User Accounts Authenticated by the Microsoft Active Directory Domain

Logging to an External SYSLOG Server

DISA STIGs require the ability to export (send) event messaging to an external Syslog server.

This is accomplished by assigning a Syslog server IP address to an “Event Destination” entry and then routing all event log messages to that event destination.

The following example shows the “built-in” event destinations provided by Clustered Data ONTAP:

```
Ntap-ontap91::event destination> show
                                                                    Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.       Params
---------------- ----------------- ------------------ ------------------ ------
```

```
allevents        -                -                -                false
asup             -                -                -                false
criticals        -                -                -                false
pager            -                -                -                false
traphost         -                -                -                false
5 entries were displayed.
```

The event destination “allevents” will be used and configured to point to an external Syslog server.

The following command will set an IP address for an external Syslog server (multiple addresses may be given, separated by commas):

Example 12) Setting IP Address for an External Syslog Server

```
Ntap-ontap91::> event destination modify -name allevents -syslog 10.63.165.225
```

The output below show the result of the above command.

```
Ntap-ontap91::> event destination show
                                                                    Hide
Name             Mail Dest.       SNMP Dest.       Syslog Dest.     Params
---------------- ---------------- ---------------- ---------------- ------
allevents        -                -                10.63.165.225    false
asup             -                -                -                false
criticals        -                -                -                false
pager            -                -                -                false
traphost         -                -                -                false
5 entries were displayed.
```

Event messages are routed to the “allevents” Syslog server at the designated IP address. As there are over 7000 different event messages currently defined for Clustered Data ONTAP, care should be taken in which messages to select. For this purpose, all messages will be selected. Unwanted messages or message families can be removed, if necessary.

Enter the following command to route these messages to the “allevents” destination:

```
Ntap-ontap91::event route> add-destinations -messagename * -destinations allevents
7009 entries were acted on.
```

After setting these configurations, there may be some lag time before messages are posted to the external server(s).

5.12 Create Administrative User Accounts and Account Access Roles

Administrative User accounts are defined by applying specific attributes to an identifying Username.

The attributes are:

Attribute	Description
SVM affiliation	Either the Cluster SVM or a Data SVM
Login method	Method used to login (i.e.: console, http, ontapi, rsh, snmp, service-processor, ssh, and telnet)
Authentication method	Determines how the account is authenticated at login.
Access role	A definition of which CLI commands are accessible by the account as well as other attributes, such as password security profile, password history limit, etc…
Accompanying comment	Optional comment text (128 characters, max.)

Note: The same user name may be affiliated with multiple SVMs, however, the user account must be explicitly created (use the security login create command) for each SVM.

Note: To meet DISA requirements for account access, only ssh and console logins will be allowed. The console (emergency) login account will also have SP login access.

Important! Per DISA requirements, all administrative user accounts (with the exception of the emergency console login account) will be authenticated by a Microsoft Active Directory Domain and not locally on the DSC.

Create Roles for Administrative Users

Clustered Data ONTAP creates several built-in roles which may be used in user account creation. These are: ***admin, autosupport, backup, none, readonly, vsadmin, and several other "vsadmin" related roles*.**

It is appropriate to assign the "***admin***" role to the emergency login account, as this account must have complete administrative capability on the cluster. The following modifications must be made to that role in order to comply with DISA STIGs. The values supplied should reflect the current Datacenter polices in effect at the installation site. The following command will effect these changes:

Example 13) Modify "admin" role configuration

```
Ntap-ontap91::> security login role config modify -role admin -vserver Ntap-ontap91-01 -username-
alphanum disabled -passwd-minlength 14 -passwd-alphanum enabled -passwd-min-special-chars 1 -
passwd-expiry-time 60 -require-initial-passwd-update enabled -max-failed-login-attempts 3 -
lockout-duration 60 -disallowed-reuse 24 -change-delay 1 -username-minlength 4

Warning: User accounts with this role exist. Modifications to the username/password restrictions
on this role could result in non-compliant user accounts.
Do you want to continue? {y|n}: y

This change won't affect expiry of existing user accounts or passwords if any, until next login
expirytime (time of day = 00:00:00)
```

A role ("***admin_ssh***") should be created for top-level administrative users who use SSH to login and are authenticated by the Microsoft Active Directory Domain. The role will be similar to the built-in "admin" role with the exception that the ability to access/manage the SP configuration settings will be removed. Use the following commands to create this rule and set its configuration:

Example 14) Create Role for Top-Level Administrative Users using SSH Access

```
Ntap-ontap91::> security login role create -role admin_ssh -cmddirname DEFAULT -access all -
vserver Ntap-ontap91-01
Ntap-ontap91::> security login role create -role admin_ssh -cmddirname "system node service-
processor" -access none -vserver Ntap-ontap91-01
Ntap-ontap91::> security login role config modify -role admin_ssh -vserver Ntap-ontap91-01 -
username-alphanum disabled -passwd-minlength 14 -passwd-alphanum enabled -passwd-min-special-
chars 1 -passwd-expiry-time 60 -require-initial-passwd-update enabled -max-failed-login-attempts
3 -lockout-duration 60 -disallowed-reuse 24 -change-delay 1 -username-minlength 4
```

Note: The values used in the configuration settings should mirror (as closely as possible) those used in the Microsoft Active Directory Domain used for login authentication.

Note: Other access roles may be defined and tailored to meet the specific need of lower-level administrators.

Create the Local Emergency Administrator Account

This defines the creation of an emergency administrative account to be used during network outages. This account has access via the controller serial console only. Authentication is by local password. Full cli and security capability roles are granted to this account by it being granted the "***admin***" role. This account will be defined twice. Once for serial console access, and once for SP login access.

To create this account, enter the following commands:

Example 15) Create Emergency Local Administator Account

```
Ntap-ontap91::> security login create -username E_User1 -application console -authmethod password
-role admin -vserver Ntap-ontap91-01 -comment "Emergency Console Admin"

Please enter a password for user 'E_User1': XXXXXXXXXXXXXX
Please enter it again: XXXXXXXXXXXXXX

Ntap-ontap91::> security login create -username E_User1 -application service-processor -
authmethod password -role admin -vserver Ntap-ontap91-01 -comment "Emergency SP Admin"
```

Important! You must now login as the emergency administrative user, from the DSC serial console, so that you can change the account password.

Create Administrative User Accounts Authenticated by the Microsoft Active Directory Domain

Administrative user accounts which are authenticated by the Microsoft Active Directory Domain require that the user account already exist on the domain. The command syntax for adding these users is as follows:

Example 16) Create a Domain Authenticated Administrative User Account

```
Ntap-ontap91::security login> create -username IACERTS\garrettc -application ssh -authmethod
domain -role admin_ssh -vserver Ntap-ontap91-01 -comment "Administrator (SSH)"
```

Note: The username is expressed as the domain's NETBIOS name followed by a backslash ("\") character and followed by the domain user's name. When logging into the cluster, the same syntax for the username must be used.

5.13 Disable External Web Access

This augments system Firewall Policies to prevent Web access (http/https) by clients external to Clustered Data ONTAP. Firewall policies should deny HTTP and HTTPS access.

Enter the following command to view the current cluster-level configuration of Web protocols:

```
Ntap-ontap91::> system services web show
External Web Services: true
              Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: true
        SSLv2 Enabled: false
```

If 'External Web Services' is true, then enter the following command to disable external access to the Web service:

```
Ntap-ontap91::> system services web modify -external false -sslv3-enabled false -sslv2-enabled
false

Warning: Modifying the cluster configuration will cause pending web service requests to be
interrupted as the web servers are restarted.
Do you want to continue? {y|n}: y
```

Re-executing the show command should indicate that external access is now false:

```
Ntap-ontap91::> system services web show
External Web Services: false
              Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
        TLSv1 Enabled: true
        SSLv3 Enabled: false
```

```
        SSLv2 Enabled: false
```

5.14 Disable Built-in ‘admin’ account

This is the final step in setting up the NetApp DSC. This step disables the built-in ‘admin’ account as per DISA STIG requirement. Enter the following command:

```
Ntap-ontap91::> security login lock -vserver Ntap-ontap91-01 -username admin
```

Attempt to logon using the ‘admin’ account to verify that it has been disabled.

The NetApp built-in ‘admin’ account will no longer be able to login to the data storage controller.

Important! If you have not created the emergency login (console) account or have not created Microsoft Active Directory domain authenticated accounts with sufficient privileges enabled, then you may no longer have the ability to properly administer this DSC.