



CONTINUITY



StorageGuard



# STORAGEGUARD SUPPORT MATRIX

SAN Arrays	File Storage & NAS	Storage Virtualization	Storage Management
<ul style="list-style-type: none"> <li>Dell EMC Symmetrix • VMAX • PowerMAX</li> <li>Dell EMC XtremIO • PowerStore* • IDPA</li> <li>Dell EMC VNX • VNX2 • Unity</li> <li>NetApp FAS/AFF • cDOT • 7-mode • filer</li> <li>Hitachi VSP/USP • AMS • HUS • G-Series</li> <li>IBM DS • XIV • IBM SVC • V7000/5000 • Storwize • A9000/R • V9000 • FlashSystem • Spectrum Virtualize • Spectrum Accelerate • N-Series</li> <li>HPE XP • 3PAR • Nimble*</li> <li>Infinidat InfiniBox</li> <li>Pure*</li> </ul>	<ul style="list-style-type: none"> <li>NetApp FAS/AFF • cDOT • 7-mode</li> <li>Dell EMC Isilon • PowerScale • VNX/2 • Unity</li> <li>IBM N-Series • Hitachi NAS* • HPE StoreEasy* • Infinibox</li> </ul>	<ul style="list-style-type: none"> <li>Dell EMC VPLEX</li> <li>IBM SAN Volume Controller • Spectrum Virtualize</li> <li>NetApp FlexArray*</li> </ul>	
Server-based SAN & HCI	Object Storage	Data Protection	
<ul style="list-style-type: none"> <li>Dell EMC PowerFlex (ScaleIO / vxflex OS)</li> <li>VMware VSAN*</li> <li>Nutanix*</li> </ul>	<ul style="list-style-type: none"> <li>Hitachi Content Platform (HCP)</li> <li>Dell EMC Elastic Cloud Storage (ECS)</li> <li>IBM Object Storage* • NetApp StorageGRID*</li> </ul>	<ul style="list-style-type: none"> <li>Dell EMC RecoverPoint • Dell EMC Data Domain • Dell EMC PowerProtect DD • Dell EMC Avamar</li> <li>NetBackup • Commvault* • HP StoreOnce • Veeam* • Cohesity* • Rubrik*</li> <li>IBM Spectrum Protect (Tivoli Storage Manager)*</li> </ul>	
	Storage Network	Cloud Storage*	
	<ul style="list-style-type: none"> <li>Brocade directors / switches • OEM versions</li> <li>Cisco MDS • Nexus • OEM versions</li> <li>HP VirtualConnect / FlexFabric</li> </ul>	<ul style="list-style-type: none"> <li>Amazon Elastic Block Storage • S3 • Glacier</li> <li>Azure Blob / Disk Storage</li> <li>Nasuni • Zadara</li> <li>NetApp Cloud Volumes ONTAP</li> </ul>	
	Storage Appliance		
	<ul style="list-style-type: none"> <li>IBM Spectrum Scale* • Hadoop Appliance*</li> <li>Oracle ZFS* • Oracle Exadata storage*</li> </ul>		

(\*) roadmap items



## Viewing Results and Status

Date

from Nov-16-20

to Nov-22-20

## System types

- ☐ Cisco
- ☐ Isilon
- ☐ NetApp Vserver
- ☐ NetApp cluster
- ☐ NetApp filer
- ☐ NetApp vFiler
- ☐ Symmetrix
- ☐ Windows

## Risks during a selected period

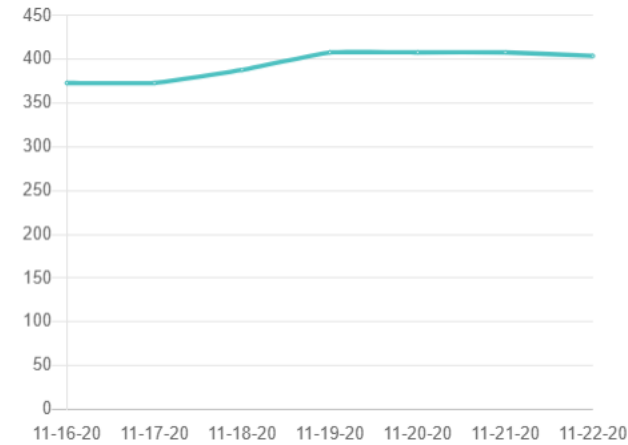
Total open risks  
**404** +8%

Average open risks per system  
**18** +8%

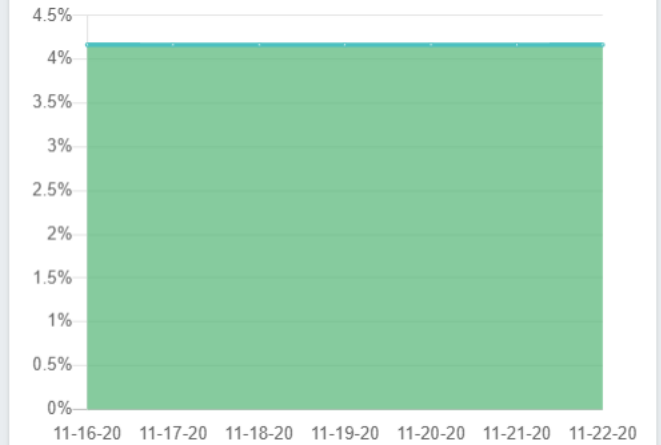
Max open risks per system  
**29** +11%

Scan Coverage  
**92%**

## New risks



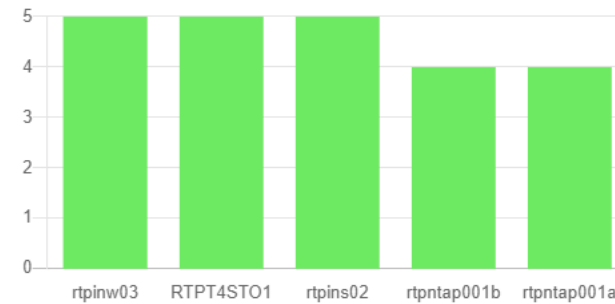
## Systems health



## Scan Coverage

System Type	Discovered	In Scope	Scanned
Cisco	6	6	6
Isilon	4	4	2
NetApp Vserve	8	8	8
NetApp cluster	1	1	1
NetApp filer	2	2	2
NetApp vFiler	4	0	0
Symmetrix	2	2	2
Windows	1	1	1

## Highest-risk system



Rule name | [DSA-CVEs]: NetApp 7-Mode vulnerability analysis: NTAP-20140924-0001: ...

Send feedback

NetApp filer      \* \* \* \*      vulnerability identified (NTAP-20140924-0001)

SuppressMark complete

#1848    Aug-04-21

Medium Urgency	Warning Severity	Open Status	Storage Domain
-------------------	---------------------	----------------	-------------------

Description

+

CVE-2014-6271

CVE-2014-6277

CVE-2014-6278

CVE-2014-7169

CVE-2014-7186

+2

NTAP-20140924-0001: A vulnerability present in the GNU Bash implementation known as Shellshock may affect multiple NetApp products and the impact is under investigation. Successful exploitation of this vulnerability may result in execution of arbitrary code via a crafted environment variable. Certain products ship with an affected version of the Bash shell.

link: <https://security.netapp.com/advisory/ntap-20140924-0001/>  
CVSS Score: 10.0

Vulnerable version

- 8.1.3P3

Impact

Exploitation of this vulnerability may lead to unauthorized disclosure of information, unauthorized modification, and/or disruption of service.

Activity log

Notes

Add a note

Resolution

update to version 8.1.4.P6 or higher.

Check name | Access Control (Authentication): Uncontrolled Local Users [Suppress check](#)

HP 3PAR TXDC3PAR0001 has uncontrolled local users with admin rights

Send feedback

Suppress

Mark as complete

#1 Dec-05-18

High

Urgency

Error

Severity

Open

Status

Baseline Violation

Impact

Payments app

Business impact

Storage Array (Block)

Resource

US East

Region

× Baseline

× Password Control

× NIST 800-53

× CIS

× PCI DSS

+

Description

HP 3PAR TXDC3PAR0001 at site **Rochester** has local users with unlimited rights that are not controlled through an account vault solution. Authentication control does not meet the required standard (see Impact).

The following table shows the uncontrolled local users:

User	Role	Default
lorap	super	No
steve_old	super	No
admgrp1	super	No
anadin	super	No
jacob	Edit	No

Impact

The HP 3PAR OS does not implement a strict password policy. Thus, a password policy is not used for local storage administration user accounts. **Password complexity, password expiration, password length and similar security requirements are not enforced.**

Impacted business entities

- Payments app

Notes

Anadin is our emergency local account, rest of the users should be deleted

Cancel

Post

Resolution

1. Prefer use of AD/LDAP user accounts over local user accounts and delete unnecessary local users.  
To delete a local 3PAR user, use the following command: ***removeuser username***
2. Keep use of local users to a minimum (for emergency scenarios).
3. When choosing to use local users, ensure password policy is enforced using a password vault solution.

Activity log



[Send feedback](#)

**Suppress**

Mark complete

High   
Urgency

**Error**  
Severity

**Open**  
Status

## Storage Domain

11

+7

that i

large

✓

**Add a note**

9

11

```
fpolicy policy event create -vsrv {param1} -event-name ransomware_EVENT -
protocol cifs -file-operations create rename
fpolicy policy create -vsrv {param1} -policy-name ransomware_POLICY -events
ransomware_EVENT
fpolicy policy scope create -vsrv {param1} -policy-name ransomware_POLICY -
shares-to-include * -file-extensions-to-include {param2}
fpolicy enable -vsrv {param1} -policy-name ransomware_POLICY -sequence-number
2
# param1 vsrv name
# param2 list of known ransomware file extensions to block
```

Check name | [DSA-Data Domain]: K010CI0MP145: External log host status ...

Send feedback

DataDomain

\* \* \* \*

Remote audit logging is disabled


Suppress


Mark complete


#14 Mar-18-20


Medium Urgency	Error Severity	Open Status	Audit Impact	Storage Domain
-------------------	-------------------	----------------	-----------------	-------------------


+

CIS Contro... 

CIS Control 6.5 

Community 

ISO 

ISO/IEC 27001 

+8

Description

Remote audit logging is disabled on the EMC Data Domain system. Security events are not sent to external syslog servers.

Remote logging

- Disabled

Impact

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files. By writing logs to central log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

By writing logs to central and hardened log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Without central log servers, an organization may fail to meet audit log retention and accuracy requirements.

Activity log

▼

Notes

Add a note

Resolution

The following command can be used to enable logging:

```
log host enable
log host add {param1}
# param1 syslog server
```



Rule name | [DSA-CVEs]: NetApp 7-Mode vulnerability analysis: NTAP-20140924-0001: ...

Send feedback

NetApp filer

\* \* \* \*

vulnerability identified (NTAP-20140924-0001)

SuppessMark complete

#1848Aug-04-21

Medium Urgency

Warning Severity

Open Status

Storage Domain

Description

+ CVE-2014-6271 CVE-2014-6277 CVE-2014-6278 CVE-2014-7169 CVE-2014-7186 +2

NTAP-20140924-0001: A vulnerability present in the GNU Bash implementation known as Shellshock may affect multiple NetApp products and the impact is under investigation. Successful exploitation of this vulnerability may result in execution of arbitrary code via a crafted environment variable. Certain products ship with an affected version of the Bash shell.

link: <https://security.netapp.com/advisory/ntap-20140924-0001/>  
CVSS Score: 10.0

Vulnerable version

- 8.1.3P3

Impact

Exploitation of this vulnerability may lead to unauthorized disclosure of information, unauthorized modification, and/or disruption of service.

Activity log

Notes

Add a note

Resolution

update to version 8.1.4.P6 or higher.

Rule name | [DSA-NetApp]: K0102I0MP100: Centralized log server (cDOT): ...

Send feedback

NetApp cluster \* \* \* \* External syslog servers are not configured

Suppress

Mark complete

#588 Nov-15-20

High Urgency

▼

Error Severity

Open Status

Storage Domain

Description

⛶

+

Sample2 ×

CIS Control 🔒

CIS Control 6.5 🔒

Community 🔒

ISO 🔒

+9

A NetApp system is not configured to send audit log messages to external logging (syslog) servers.

Syslog servers

- none

Impact

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files. By writing logs to central log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

By writing logs to central and hardened log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Without central log servers, an organization may fail to meet audit log retention and accuracy requirements.

Notes

Add a note

Resolution

Use the following command to configure syslog destinations:

```
cluster log-forwarding create -destination {param1} -port 514 -facility {param2} -protocol tcp-encrypted
# param1 name or ip of destination
# param2 syslog facility
```

Activity log

▼

Rule name | [DSA-CVEs]: NetApp cDOT vulnerability analysis: NTAP-20190719-0002: ...

Send feedback

NetApp cluster \* \* \* \* vulnerability identified (NTAP-20190719-0002)

SupressMark complete

#573 Nov-15-20

Medium Urgency

Warning Severity

Open Status

Storage Domain

Description

+

Sample2 ×

CVE-2019-9924 🔒

NetApp

NTAP-20190719-0002: Multiple NetApp products incorporate libxml2  
Versions of libxml2 through 2.9.8 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS)  
link: <https://security.netapp.com/advisory/ntap-20190719-0002/>  
CVSS Score: 6.5

Unsecured Version

- 9.5P6

⌵

Impact

Successful exploitation of this vulnerability could lead to Denial of Service (DoS).

Activity log

▼

Notes

Add a note

Resolution

update to version 9.5P10 or higher

Check name | Ransomware: Protection Best Practices [Suppress check](#)

[Send feedback](#)

NetApp cluster \* \* \* \* at site **Rochester** is not enabled with ransomware protection features

Suppress

Mark as complete

#6 Jan-07-19

High Urgency	Error Severity	Open Status	Best Practice Impact	Gen-PROD Business impact	Storage System (NAS) Resource	US East Region
-----------------	-------------------	----------------	-------------------------	-----------------------------	----------------------------------	-------------------

× NetApp

× AVScan

× PCI DSS

+

Description

Ransomware protection features on NetApp cluster tlddr1010 at site Rochester are not configured correctly:

1. Each vservers must be configured with a scanner pool such that Mandatory **Antivirus** scan is set to on.
2. An FPolicy for **blocking common ransomware file extensions** should be configured.

The following table shows the status of ransomware protection features:

Feature	Status
Antivirus	off
FPolicy	Not configured

Notes

Add a note

Resolution

1. Configure the NetApp system such that an **active scanner pool** is defined for each vservers.
2. Use the *fpolicy* command to create a policy for blocking ransomware suspected traffic.

Impact

Where supported by the storage system, **on-access antivirus protection** must be used to provide **real-time identification of malware** located on non-administrative CIFS/SMB file shares. Failing to meet this practice may lead to virus infections.

The NetApp FPolicy solution allows organizations to **block traffic based on common ransomware file extensions and file metadata** such as .micro .encrypted .locked .crypto .crypt .crinf .r5a, .XRNT .XTBL .R16M01D05 .pzdc .good .LOL! .OMG!, .RDM .RRK .encryptedRS .crjoker .EnCIPhErEd and .LeChiffre. Not using the fpolicy capability increases the risk of a successful ransomware attack.

Impacted business entities

- Gen-PROD

Activity log



List



Rule name

| [DSA-CVEs]: Hitachi vulnerability analysis: hitachi-sec-2020-111: ...

Send feedback

HDS 58182: vulnerability identified

Suppress

Mark complete

#14 Mar-22-21

Medium

Urgency

Warning

Severity

Open

Status

Storage

Domain

Description



CVE-2020-2754

CVE-2020-2755

CVE-2020-2756

CVE-2020-2757

CVE-2020-2767

+9

hitachi-sec-2020-111: Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE.

link: <http://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2020-111/index.html>  
CVSS Score: 3.0

Vulnerable version

- v8.6.2

Impact

Unauthorized ability to cause a partial denial of service (partial DOS) of Java SE and Unauthorized update insert or delete access to some of Java SE accessible data.  
in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data.

Activity log



Notes

Add a note

Resolution

update to version 8.7.4 or higher.

Rule name | [DSA-CVEs]: Hitachi vulnerability analysis: hitachi-sec-2020-118: ...

Send feedback

HDS 91240336: vulnerability identified

SuppressMark complete

#2093May-06-21

Medium  
Urgency

Warning  
Severity

Open  
Status

Storage  
Domain

Description

⊕HDS hitachi-sec-2020-118 hitachi-sec-2020-118: Hitachi Device Manager contains a vulnerability to Denial of Service (DoS) attacks.  
link: https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2020-118/index.html  
CVSS Score: 3.0  
Vulnerable version

- v8.6.2

Impact

The process of the database built in to the Hitachi Command Suite products could stop, even the service itself, which can cause malfunction of the Hitachi Device Manager server and the other Hitachi Command Suite products that are installed on the same machine.

Activity log

Notes

Add a note

Resolution

update to version 8.7.3 or higher.

← List



Rule name | [DSA-HiCommand]: K0110I0MP0419: Logical Unit Port Security: ...

Send feedback

HDS 58577: LUN security not enabled on ports

Suppress

Mark complete

#5 Mar-22-21

High Urgency	Error Severity	Open Status	Storage Domain
-----------------	-------------------	----------------	-------------------

Description



+ CIS Control CIS Control 4.1 Community HDS ISO/IEC 27040 +6

The storage systems has ports for which lun security has not been enabled.

Violated Ports:

- PORT.R800.58577.244, PORT.R800.58577.188, PORT.R800.58577.243, PORT.R800.58577.187, PORT.R800.58577.242, PORT.R800.58577.186, PORT.R800.58577.241, PORT.R800.58577.247, PORT.R800.58577.246, PORT.R800.58577.245 (34 more...)

Customizable parameters for this check:

- Scope (Regex): N/A
- logical unit security status: enable

Impact

To protect mission-critical data in your storage system from illegal access, apply security policies to logical volumes. Use LUN Manager to enable LUN security on ports to safeguard LUs from illegal access. If LUN security is enabled on ports, host groups affect which host can access which LUs. Hosts can access only the LUs associated with the host group to which the hosts belong. Hosts cannot access LUs associated with other host groups.

Activity log



Notes

Add a note

Resolution

The following command can be used to secure lun port:

In the Storage Navigator:

- Click Storage Systems, and then expand the Storage Systems tree.
- Click Ports/Host Groups/iSCSI Targets.
- In the Ports/Host Groups/iSCSI Targets window, click the Ports tab.
- Select the desired port, and then click Edit Ports.
- Select the Port Security check box, and then select Enable.
- Click Finish.



List



Rule name | [DSA-HiCommand]: K0110I0MP0438: Logical device encryption: ...

[Send feedback](#)

## HDS 58130: Unencrypted logical devices

Suppress

Mark complete

#303 Mar-22-21

High  
Urgency

Error  
Severity

Open  
Status

Storage  
Domain

### Description



+ CIS Control CIS Control 14.8 HDS HIPAA ISO/IEC 27040 +7

The storage system has logical devices that store unencrypted data.

Violated LDEVs:

- LDEV.R800.58130.64769, LDEV.R800.58130.64768, LDEV.R800.58130.64767, LDEV.R800.58130.64766, LDEV.R800.58130.64765, LDEV.R800.58130.64764, LDEV.R800.58130.64763, LDEV.R800.58130.1133, LDEV.R800.58130.5975, LDEV.R800.58130.64762 (2941 more...)

Customizable parameters for this check:

- Scope (Regex): N/A
- logical device encrypted status: enable

### Impact

- Data at-rest encryption protects against unauthorized access in the event of drive loss, incorrect assignment or theft.
- Data at-rest encryption helps with compliance and regulations (FIPS 140-2, HIPAA, PCI, SOX and more).

### Activity log



### Notes

Add a note

### Resolution

The following command can be used to encrypt a logical device:



[List](#)

Rule name | [DSA-HiCommand]: K0810I00P183: Protected recovery copies: ...

[Send feedback](#)

# HDS 58577: Snapshot retention lock not enabled

[Suppress](#)[Mark complete](#)

#48 Mar-22-21

High Urgency	Error Severity	Open Status	Storage Domain
-----------------	-------------------	----------------	-------------------

## Description



+ FFIEC HDS Hitachi Vantara ISO/IEC 27040 NIST SP800-209 +1

The system does not protect data copies from being overwritten or erased.

Violated LDEVs:

- LDEV.R800.58577.8475, LDEV.R800.58577.8474, LDEV.R800.58577.7145, LDEV.R800.58577.8477, LDEV.R800.58577.7146, LDEV.R800.58577.8476, LDEV.R800.58577.6058, LDEV.R800.58577.7147, LDEV.R800.58577.8479, LDEV.R800.58577.7148 (1471 more...)

Customizable parameters for this check:

- Scope (Regex): N/A
- guardmode status: Protect

## Impact

An attacker obtaining administrative access could delete backup copies and make recovery of data impossible. Recovery from a ransomware attack may not be possible due to having encrypted production and snapshot volumes.

## Activity log



## Notes

[Add a note](#)

## Resolution

The following command can be used to enable data retention lock features:

```
raidvchkset -g {@param1} -vg {param2} {param3}
# param1 group name
# param2 guard type. inv: The target volumes are concealed from SCSI Inquiry command by responding 'unpopulated volume'. sz0: The target volumes replies with 'SIZE 0' through SCSI Read capacity command. rwd: The target volumes are prohibited from reading and writing. wtd: The target volumes are prohibited from writing. svd: If the target volume is SMPL, it is protected from paircreate (from becoming an S-VOL). If the target volume is P-VOL, it is protected from pairresync restore or pairresync swaps(p). If the target volume is SVOL_PSUS(SSUS), it is protected from pairresync synchronous copy
# param3 retention period (days)
```

Rule name | [DSA--XtremIO]: K070E00M0851: SNMP community default string: ...

Send feedback

XtremIOCluster | \* \* \* \* at site New York: Unsecure SNMP community settings

SuppressMark complete

#325Jul-30-20

High  
Urgency

Error  
Severity

Open  
Status

Storage  
Domain

Description

+

Sample ×

CIS Control

CIS Control 4.2

Community

FFIEC

ISO/IEC 27040

NIST

NIST SP800-53

NIST SP800-53 IA-5

PCI DSS

PCI DSS 2.1

XtremIOCluster

—

An EMC XtremIO storage system is configured with the default (known) community string: public.

Violation:  
{ "community": "public" }

Impact

The SNMP Community String is like a user id or password that is sent along with each SNMP Get-Request and allows (or denies) access to a device. If the community string is correct, the device responds with the requested information. Most network vendors ship their equipment with a default password of "public". Whether SNMP is active or not, it is recommended to change the community string to keep intruders from getting information about the network setup.

Activity log

Notes

Add a note

Resolution

The following command can be used to change the community name:

```
modify-snmp-notifier community={param1}  
# param1 community name
```

Rule name | [DSA-Data Domain]: K050CI0MP610: NTP servers redundancy: ...

Send feedback

DataDomain      \* \* \* \*      at site **New York**: Insufficient NTP server redundancy

#155   Jul-08-20

Suppress   Mark complete

Medium Urgency

Warning Severity

Open Status

Storage Domain

Description

+

Sample ×

Sample2 ×

CIS Control 🔒

CIS Control 6 🔒

CIS Control 6.1 🔒

+13

An EMC Data Domain system is not configured with sufficient number of NTP servers (for redundancy). The NTP service is used for time synchronization.

Actual Level of Redundancy

- 1

Customizable parameters for this check:

- Minimum number of NTP servers: 2

Impact

NTP service is critical for time synchronization. Thus, the best practice and industry guideline it to use multiple NTP servers and to avoid an NTP single point of failure. For example, CIS Control recommends to use at least three synchronized time sources.

In the event the NTP server becomes unavailable, dependent systems may suffer from the following issues:

- Inaccurate timestamp for log messages, events and alerts
- Inconsistent time across different devices
- Failure to perform log analysis, correlation, anomaly detection or forensics
- Non-compliance

More on the importance of time synchronization:

- When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.
- Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Activity log

▼

Notes

Add a note

Resolution

The following command can be used to add an NTP server:

```
ntp add timeserver {param1}
# param1 server-name
```

Check name | [DSA-Data Domain]: K010CI0MP145: External log host status ...

Send feedback

DataDomain

\* \* \* \*

Remote audit logging is disabled


Suppress


Mark complete


#14 Mar-18-20


Medium Urgency	Error Severity	Open Status	Audit Impact	Storage Domain
-------------------	-------------------	----------------	-----------------	-------------------


+

CIS Contro... 

CIS Control 6.5 

Community 

ISO 

ISO/IEC 27001 

+8

Description

Remote audit logging is disabled on the EMC Data Domain system. Security events are not sent to external syslog servers.

Remote logging

- Disabled

Impact

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, and they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files. By writing logs to central log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.

Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

By writing logs to central and hardened log servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Without central log servers, an organization may fail to meet audit log retention and accuracy requirements.

Activity log

▼

Notes

Add a note

Resolution

The following command can be used to enable logging:

```
log host enable
log host add {param1}
# param1 syslog server
```

Rule name | [DSA--Data Domain]: K060CI0MP700: http service status: ...

Send feedback

DataDomain

\* \* \* \*

at site New York: Unsecure clear-text HTTP connections are enabled

Supress

Mark complete

#483 Aug-13-20

High Urgency	Error Severity	Open Status	Storage Domain
-----------------	-------------------	----------------	-------------------

Description

⛶

+

Sample2 ×

CIS Control 🔒

CIS Control 4.5 🔒

CIS Control 12.4 🔒

CIS Control 16.5 🔒

+12

An EMC Data Domain system is enabled with unsecure HTTP connections. Only secure protocols should be used for administrative access.

Violation:  
http yes -

Impact

If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. Clear text protocols are vulnerable to sniffing, interception and other attacks.

Activity log

▼

Notes

Add a note

Resolution

The following commands can be used to disable HTTP:

adminaccess disable http

Rule name | [DSA-XtremIO]: K010EI00P891: TLS level: ...

Send feedback

XtremIOCluster \* \* \* \* at site New York: Incorrect TLS level configured

SuppressMark complete

#348 Jul-30-20

High Urgency	Error Severity	Open Status	Storage Domain
-----------------	-------------------	----------------	-------------------

Description

+

● Sample ×

○ EMC Security Guide 🔒

● PCI DSS 🔒

● SWIFT 🔒

○ XtremIOCluster

EMC XtremIO storage system is configured with incorrect TLS level for client connections. Leading information security standards require that at minimum TLS 1.1 will be used and preferably TLS 1.2.

min-tls-version

- 1

Customizable parameters for this check:

- Required TLS version: 1.2

Impact

TLS 1.0 includes a means by which a TLS implementation can downgrade the connection to SSL 3.0, thus weakening security and exposing it to the POODLE vulnerability.

Activity log

▼

Notes

Add a note

Resolution

The following command can be used to set the TLS level:

```
modify-xms-parameters min-tls-version="{param1}"  
# param1 required TLS version
```

Filters

Reset

594 Risks

- 🕒 Date

All
- 🔍 Urgency

▼
- 📊 High

281
- 📊 Medium

304
- 📊 Low

9
- ⚠️ Severity

▼
- 📊 Error

281
- 📊 Warning

304
- 📊 Info

9
- 🔍 Impact

▼
- 📊 Audit

92
- 📊 Authentication

165
- 📊 Authorization

85
- 📊 Configuration Man...

20
- 📊 Encryption

24
- 📊 Information Security

129
- 📊 Malware Protection

2
- 📊 Services and Protoc...

16
- 📊 Vulnerabilities (CVE)

61
- 🔒 Security labels

^
- 🏷️ Labels

^
- 📁 Status

^
- ✅ Open

594
- ✅ Reopened

Sort by: Urgency

Group by: Check

Search

>	<input type="checkbox"/>	[DSA-Data Domain]: K130C000P725: ddbost file replication encryption	2 Risks	2 New	2 Opened	2	0	0	...
>	<input type="checkbox"/>	[DSA-Cisco]: K0419I0MP400: user role association	3 Risks	3 New	3 Opened	3	0	0	...
▼	<input type="checkbox"/>	[DSA-Navicli]: K101100MP285: IPFilter status	1 Risks	1 New	1 Opened	1	0	0	...
	<input type="checkbox"/>	CLARiiON MEXVNX7879: IP Filtering is disabled	High Urgency	Open Status	Error Severity	Information Security Impact			Apr-23-20 #300
>	<input type="checkbox"/>	[DSA-Data Domain]: K030CI0MP295: Disable of expired users	2 Risks	2 New	2 Opened	2	0	0	...
>	<input type="checkbox"/>	[DSA-Data Domain]: K130C00MP730: ddbost encryption enforcement	2 Risks	2 New	2 Opened	2	0	0	...
>	<input type="checkbox"/>	[DSA-Data Domain]: K020CI0MP295: Initial password change	2 Risks	2 New	2 Opened	2	0	0	...
>	<input type="checkbox"/>	[DSA-Navicli]: K010EI00P891: TLS level	1 Risks	1 New	1 Opened	1	0	0	...
>	<input type="checkbox"/>	[DSA-Data Domain]: K020CI0MP295: Maximum password age	2 Risks	2 New	2 Opened	2	0	0	...
>	<input type="checkbox"/>	[DSA-Data Domain]: K020CI0MP295: Maximum number of repeated password characters	2 Risks	2 New	2 Opened	2	0	0	...
>	<input type="checkbox"/>	[DSA-NetApp]: K0303I0MP295: Minimum password lowercase characters (7-Mode)	3 Risks	3 New	3 Opened	0	3	0	...

Check name

[DSA-Navicli]: K101100MP285: IPFilter status

CLARiiON

\*\*\*\*

IP Filtering is disabled

#300

Apr-23-20

High Urgency

Error Severity

Open Status

Information Security Impact

Storage Domain

+ CIS Control

+ CIS Control 9.4

CLARiiON

Description

An EMC VNX is not configured with IP filtering for management hosts. Administrative access is not restricted to a list of trusted storage management clients.









Current IP Filtering State

disabled

Impact

Attackers search for remotely accessible network services that are vulnerable to exploitation. Any host installed with EMC management software would be able to remotely run commands, API calls, etc.

View more

- Scheduling
- Catalog
- Findings Summary  
- Findings Summary  
- Findings Summary  
- Findings Summary  

# Reports Catalog

Administration

Scan Status

Scan History

System Event Log

Data Collection Expansion Package Summary

Data Collectors Summary

License Usage

Scan Troubleshooting

Business Entity Scan Coverage

Activity Report

Inventory

Installed Software

SAN Switch Version

SAN Zone Details

Security Configuration Change Log

Findings

Executive HealthCheck

Findings Summary

Analysis Summary

General

Database Views Schema Documentation

Custom Reports

Results - Data Protection Systems: Summary

Results - NAS Arrays: Summary

Results - SAN Arrays: Summary

Results - Storage Network: Summary

Results - Storage Virtualization: Summary

cyberSummary - cyberSummary



# Analysis Summary

Systems Cluster95

Generate

## Report Preview

☐ Landscape

### DETAILED ANALYSIS

The following table presents the types of risks checked during the scan, and the status of the check

Category	Principle	Classification	Check	NetApp cluster Cluster95
Access Control	Authorized logging servers are used	DSA-NetApp	K0102i0MP102: Approved syslog servers (cDOT)	PASS
Access Control	Firewall / IPfilter is enabled	DSA-NetApp	K100200MP285: Firewall status (cDOT)	PASS
Access Control	Idle sessions are terminated	DSA-NetApp	K1102i00P690: Session timeout (cDOT)	FAIL
Access Control	System use notification is presented	DSA-NetApp	K1102i00P110: banner status (cDOT)	FAIL
Access Control	System use notification is presented	DSA-NetApp	K1102i00P110: mold status (cDOT)	FAIL
Audit	Audit logging is enabled	DSA-NetApp	K01020000145: Security audit logging - read-only (cDOT)	FAIL
Audit	External (central) log servers are configured	DSA-NetApp	K0102i0MP100: Centralized log server (cDOT)	FAIL
Audit	External (central) log servers are configured	DSA-NetApp	K0102i0MP104: Required External (central) log servers (cDOT)	PASS
Audit	Logging server redundancy	DSA-NetApp	K0102i0MP100: Centralized log server redundancy (cDOT)	PASS
Audit	Synchronization with authoritative time source is enabled	DSA-NetApp	K0502i0MP600: NTP servers (cDOT)	PASS
Authentication	Account lockout duration	DSA-NetApp	K0202i0MP295: Minimum account lockout duration (cDOT)	PASS
Authentication	Account lockout threshold	DSA-NetApp	K0202i0MP295: Account lockout threshold (cDOT)	FAIL
Authentication	Central authentication is used	DSA-NetApp	K140200M0525: Central authentication for file share access (cDOT)	N/A
Authentication	Initial password change required	DSA-NetApp	K0202i0MP295: Initial password change (cDOT)	FAIL
Authentication	Local user accounts should not be used	DSA-NetApp	K1002i0MP120: Non-default local users (cDOT)	FAIL
Authentication	Maximum password lifetime is restricted	DSA-NetApp	K0202i0MP295: Maximum password age (cDOT)	FAIL
Authentication	Minimum password length is enforced	DSA-NetApp	K0202i0MP295: Minimum password length (cDOT)	PASS
Authentication	Minimum password lifetime is restricted	DSA-NetApp	K0202i0MP295: Minimum password age (cDOT)	FAIL
Authentication	Password reuse is limited	DSA-NetApp	K0202i0MP295: Number of disallowed past passwords (cDOT)	PASS
Authentication	Use of digits in passwords	DSA-NetApp	K0202i0MP295: Minimum password digits (cDOT)	FAIL
Authentication	Use of lowercase characters in passwords	DSA-NetApp	K0202i0MP295: Minimum password lowercase characters (cDOT)	FAIL
Authentication	Use of special characters in passwords	DSA-NetApp	K0202i0MP295: Minimum password special characters (cDOT)	FAIL
Authentication	Use of uppercase characters in passwords	DSA-NetApp	K0202i0MP295: Minimum password uppercase characters (cDOT)	FAIL
Authorization	Access rights granted to authorized users/hosts only	DSA-NetApp	K0202000P950 - Multifactor authentication status (cDOT)	FAIL
Authorization	Access rights granted to authorized users/hosts only	DSA-NetApp	K06020000960 - Password hash strength (cDOT)	PASS
Authorization	Access rights granted to authorized users/hosts only	DSA-NetApp	K140200M0345: File share client access list (cDOT)	N/A
Authorization	Least privilege	DSA-NetApp	K140200M0560: share access rights (cDOT)	N/A
Configuration Management	Name service is enabled	DSA-NetApp	K03020000150: DNS service status (cDOT)	PASS
Encryption	Weak SSH MAC algorithms are disabled	DSA-NetApp	K0602i0M0806: SSH MAC strength (cDOT)	FAIL

- EXCEL
- PDF
- RTF
- WORD

- Scheduling
- Catalog
- Security Configurati...
- Security Configurati...
- Findings Summary
- Analysis Summary
- Analysis Summary
- Analysis Summary
- Analysis Summary

# Security Configuration Change Log

From date 2020-11-15 to ☐ From last full scan

Scope:

- ☐ Cluster
- ☐ Database
- ☐ Host
- ☒ Storage

Change Type:

- ☒ Changed
- ☐ New
- ☐ Removed

Generate

## Report Preview

☐ Landscape



## INFRASTRUCTURE CHANGE LOG

Report generation time: Jan 19, 2021 5:26:55 AM

Date	Type	Context	System	Changed Attribute	Old Value	New Value
Nov 15, 2020 3:43:30 AM	Changed	Storage	* * * *	Audit Configuration - cli-get	false	true
Nov 15, 2020 3:43:30 AM	Changed	Storage	* * * *	System Timeout	CLI session timeout: 30 minutes	CLI session timeout: 1440 minutes
Nov 15, 2020 6:21:38 AM	Changed	Storage	* * * *	Cifs Options	All Options: Option Value ----- domain-account-mmc-share-management enabled (*) idle-timeout 1800 (*) idmap-type rid (*) loglevel 1 (*) max-global-open-files 10000 (*) max-mpx-count 50 (*) max-tcp-connections 150 (*) organizational-unit Computers (*) restrict-anonymous disabled (*) server-signing disabled (*) tcp-window-size 1048576 (*) ----- (*) default value	All Options: Option Value ----- restrict-anonymous enabled domain-account-mmc-share-management enabled (*) idle-timeout 1800 (*) idmap-type rid (*) loglevel 1 (*) max-global-open-files 10000 (*) max-mpx-count 50 (*) max-tcp-connections 150 (*) organizational-unit Computers (*) server-signing disabled (*) tcp-window-size 1048576 (*) ----- (*) default value
Nov 15, 2020 6:21:38 AM	Changed	Storage	* * * *	FTPS Option: session-timeout	default (infinite)	90
Nov 15, 2020 6:21:38 AM	Changed	Storage	* * * *	Ftps options	N/A session-timeout default (infinite)	N/A session-timeout 90
Nov 15, 2020 6:21:38 AM	Changed	Storage	* * * *	Ntp Config	NTP is currently disabled. ----- No NTP servers configured; using multicast	NTP is currently enabled. # Server ----- 1 ntp-d.nist.gov

- ☒ Brocade
- ☒ Cisco
- ☒ DataDomain
- ☒ Isilon
- ☐ Linux
- ☒ NetApp cluster
- ☐ Symmetrix
- ☐ VPLEX cluster
- ☐ Windows
- ☐ Xtrem IO cluster

Check Name	Pass	Fail	Insufficient Info	Labels
[DSA-Data Domain]: K020CI0MP295: Minimum password special characters	0	4	0	NIST NIST SP800-53 NIST SP800-53 IA-5
[DSA-Data Domain]: K050CI0MP605: Required NTP servers	1	3	0	CIS Control CIS Control 6 NIST NIST SP800-53 NIST SP800-53 AU-4
[DSA-Cisco]: K12190000630: Idle session timeout	8	0	0	CIS Control CIS Control 16 NIST NIST SP800-53 NIST SP800-53 AC-11 NIST SP800-53 AC-12
[DSA-Brocade]: K0104I0MP145: Audit logging status	3	0	2	CIS Control CIS Control 6 NIST NIST SP800-53 NIST SP800-53 AU-2
[DSA-Data Domain]: K020CI0MP295: Minimum password age	0	4	0	CIS Windows Server Benchmark CIS Windows Server Benchmark CCE-37073-4 NIST NIST SP800-171 NIST SP800-171 3.5.8 NIST SP800-53 NIST SP800-53 IA-5
[DSA-Brocade]: K0304000P160: DNS server redundancy	3	0	2	NIST NIST SP800-53 NIST SP800-53 SC-22
[DSA--Cisco]: K0319I0MP295: Maximum password age	0	8	0	CIS Control CIS Control 4 NIST NIST SP800-53 NIST SP800-53 IA-5
[DSA-Brocade]: K010400M0160: Approved syslog servers	3	0	2	CIS Control CIS Control 6 NIST NIST SP800-53 NIST SP800-53 AU-4
[DSA-Brocade]: K0204I00P210: Authentication server redundancy	3	0	2	CIS Control NIST NIST SP800-53 NIST SP800-63B
[DSA-Cisco]: K011900M0160: Required syslog servers	8	0	0	CIS Control CIS Control 6 NIST NIST SP800-53 NIST SP800-53 AU-4
[DSA--Data Domain]: K010C00M0125: External syslog server redundancy	3	1	0	NIST NIST SP800-53 NIST SP800-53 AU-4
[DSA-Data Domain]: K020CI0MP295: Maximum number of repeated password characters	0	4	0	NIST NIST SP800-63B
[DSA-NetApp]: K0202I0MP295: Account lockout threshold (cDOT)	0	1	0	NIST NIST SP800-53 NIST SP800-53 AC-7
[DSA-Data Domain]: K030CI0MP295: password hash strength	2	2	0	NIST NIST SP800-107
[DSA-Isilon]: K140D00M0370: nobody user status	0	1	0	CIS Windows Server Benchmark
[DSA-Isilon]: K170D00M0230: Antivirus server configuration	0	1	0	CIS Control CIS Control 8.1 NIST NIST SP800-53 NIST SP800-53 SI-3
[DSA-Isilon]: K020DI0MP120: Non-default local users	0	1	0	NIST NIST SP800-53 NIST SP800-53 AC-2 NIST SP800-53 IA-2
[DSA-Isilon]: K030DI0MP295: Password complexity	0	1	0	CIS Control CIS Control 4 NIST NIST SP800-53 NIST SP800-53 IA-5
[DSA-NetApp]: K1102I00P690: Session timeout (cDOT)	0	1	0	CIS Control CIS Control 16 NIST NIST SP800-53 NIST SP800-53 AC-11 NIST SP800-53 AC-12
[DSA-Isilon]: K050DI0MP600: NTP server configuration	1	0	0	CIS Control CIS Control 6.1 NIST NIST SP800-53 NIST SP800-53 AU-8
[DSA-Isilon]: K030DI0MP295: Password history	0	1	0	NIST NIST SP800-171 NIST SP800-171 3.5.8 NIST SP800-53 NIST SP800-53 IA-5
[DSA-Brocade]: K05040000665: NTP server redundancy	0	3	2	CIS Control CIS Control 6 CIS Control 6.1 NIST NIST SP800-53 NIST SP800-53 AU-4 NIST SP800-53 AU-8
[DSA-Cisco]: K0219I0MP120: Non-default local users	0	8	0	NIST NIST SP800-53 NIST SP800-53 AC-2 NIST SP800-53 IA-2
[DSA-Brocade]: K0104I0MP100: Centralized log server redundancy	3	0	2	NIST NIST SP800-53 NIST SP800-53 AU-4



## Configuring, Tuning and Customizing



Scan



Associations



Admin



Schedule



Troubleshooting

Data Security  
Advisor

Authentication

Servers

Storage

Proxies

Arrays

SAN

Scan &gt; Storage &gt; Arrays

Storage arrays | Troubleshooting

Search...

Group By: None



Type	Name	IP Address	Site	Policy	Proxy	Verify	Verify Date	Scan	Scan Date	Note	Enabled
EMC Symmetrix	000297801226		Unknown Site	Inherited from SymmCLI (Dat...	SymmCLI		Dec-27-20		Dec-27-20		<input checked="" type="checkbox"/>
EMC Symmetrix	000297801225		Unknown Site	Inherited from SymmCLI (Dat...	SymmCLI		Dec-27-20		Dec-27-20		<input checked="" type="checkbox"/>
EMC Symmetrix	000295701062		Unknown Site	Inherited from SymmCLI (Dat...	SymmCLI		Dec-27-20		Dec-27-20		<input checked="" type="checkbox"/>

- Delete
- Assign proxy
- Disable
- Enable
- Verify
- Scan
- Scan Custom Collection
- Scan and Execute Risk Detection
- View Custom Collection
- View Built-in Collection

On-demand scan and  
analysis

Show

50



1

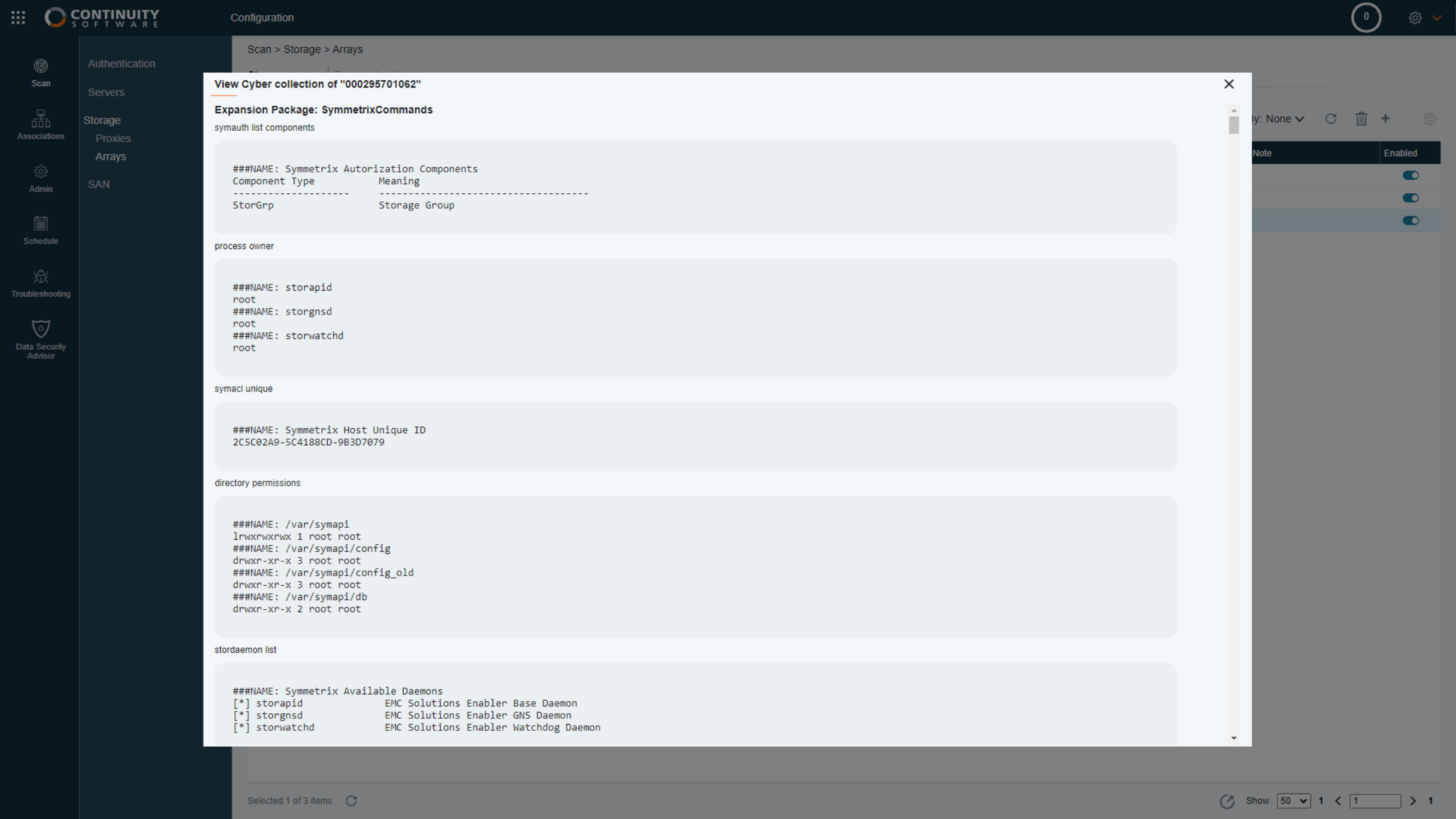


1



&gt;

1



### View Cyber collection of "000295701062"

#### Expansion Package: SymmetrixCommands

symauth list components

```
###NAME: Symmetrix Authorization Components
Component Type      Meaning
-----
StorGrp              Storage Group
```

process owner

```
###NAME: storapid
root
###NAME: storgnsd
root
###NAME: storwatchd
root
```

symacl unique

```
###NAME: Symmetrix Host Unique ID
2C5C02A9-5C4188CD-9B3D7079
```

directory permissions

```
###NAME: /var/symapi
lrwxrwxrwx 1 root root
###NAME: /var/symapi/config
drwxr-xr-x 3 root root
###NAME: /var/symapi/config_old
drwxr-xr-x 3 root root
###NAME: /var/symapi/db
drwxr-xr-x 2 root root
```





stordaemon list

```
###NAME: Symmetrix Available Daemons
[*] storapid      EMC Solutions Enabler Base Daemon
[*] storgnsd      EMC Solutions Enabler GNS Daemon
[*] storwatchd    EMC Solutions Enabler Watchdog Daemon
```

&gt;

Done     

Site	Scan ...	Scan Date	Enabled
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Oct-26-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Nov-02-20	<input checked="" type="checkbox"/>
0		Nov-02-20	<input checked="" type="checkbox"/>
0		Nov-02-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>
0		Nov-02-20	<input checked="" type="checkbox"/>
0		Oct-19-20	<input checked="" type="checkbox"/>


 Show 50 
 1  1  1

Data Security Advisor > Manage principles

Search...

Group By: None

	Name	Category	Labels
<input type="checkbox"/> 799	Audit log configuration (Log content)	Audit	PCI DSS PCI DSS 10 ISO ISO/IEC 27001 ISO/IEC 27001 A.12.4.1 ISO/IEC 27040 CIS Control CIS Control 6 NIST NIST SP800-53
<input type="checkbox"/> 842	Audit logging is enabled	Audit	PCI DSS PCI DSS 10 ISO ISO/IEC 27001 ISO/IEC 27001 A.12.4.3 ISO/IEC 27040 CIS Control CIS Control 6 NIST NIST SP800-53
<input type="checkbox"/> 889	Authorized (secure) time source servers are used	Audit	PCI DSS PCI DSS 10.5 ISO ISO/IEC 27001 ISO/IEC 27001 A.12.4.3 CIS Control CIS Control 6 NIST NIST SP800-53 NIST SP800-53
<input type="checkbox"/> 953	Authorized antivirus servers are used	Malware Protection	PCI DSS PCI DSS 5.1 ISO/IEC 27001 ISO/IEC 27001 A.12.2.1 CIS Control CIS Control 8.1 NIST NIST SP800-53 NIST SP800-53
<input type="checkbox"/> 790	Authorized authentication servers are used	Authentication	PCI DSS ISO ISO/IEC 27001 ISO/IEC 27040 CIS Control CIS Control 16.2 NIST SP800-53 NIST SP800-63B
<input type="checkbox"/> 852	Authorized logging servers are used	Access Control	PCI DSS PCI DSS 10.5 ISO ISO/IEC 27001 ISO/IEC 27001 A.12.4.3 CIS Control CIS Control 6 NIST NIST SP800-53 NIST SP800-53
<input type="checkbox"/> 806	Authorized name servers are used	Configuration Management	SANS NIST NIST SP800-53 NIST SP800-53 SC-22 NIST SP800-81-2
<input type="checkbox"/> 841	Central authentication is used	Authentication	PCI DSS ISO ISO/IEC 27001 ISO/IEC 27040 CIS Control NIST NIST SP800-53 NIST SP800-63B
<input type="checkbox"/> 830	Central authentication server redundancy	Authentication	PCI DSS ISO ISO/IEC 27001 CIS Control NIST NIST SP800-53 NIST SP800-63B
<input type="checkbox"/> 884	Clear-text protocols are disabled	Encryption	FFIEC PCI DSS PCI DSS 2.3 Community ISO/IEC 27040 CIS Control CIS Control 12.4 CIS Control 16.5 CIS Control 4.5 NIST
<input type="checkbox"/> 980	Client certification verification is mandatory	Authentication	EMC Security Guide
<input type="checkbox"/> 984	Credentials caching should be limited	Authentication	NIST SP800-53 IA-5 DoD
<input type="checkbox"/> 976	Data at-rest is encrypted	Encryption	PCI DSS PCI DSS 3.4 PCI DSS 8.2.1 HIPAA ISO/IEC 27040 SANS CIS Control CIS Control 14.8 NIST NIST SP800-53 NIST SP800-53
<input type="checkbox"/> 900	External (central) log servers are configured	Audit	PCI DSS PCI DSS 10.5 ISO ISO/IEC 27001 ISO/IEC 27001 A.16.1.7 Community ISO/IEC 27040 CIS Control CIS Control 6.5 NIST
<input type="checkbox"/> 916	FIPS compliance features are enabled	Encryption	FIPS
<input type="checkbox"/> 855	Fabric access is restricted	Access Control	Brocade Fibre Channel Security Best Practices ISO/IEC 27040
<input type="checkbox"/> 966	Firewall / IPfilter is enabled	Access Control	CIS Control CIS Control 9.4
<input type="checkbox"/> 946	Guest/Anonymous user access is limited	Authorization	CIS Windows Server Benchmark ISO/IEC 27040 SANS
<input type="checkbox"/> 985	Hardening (STIG)	Information Security	Defense Information Systems Agency (DISA) DoD
<input type="checkbox"/> 862	Idle sessions are terminated	Access Control	PCI DSS PCI DSS 12.3.8 CIS Control CIS Control 16 NIST NIST SP800-53 NIST SP800-53 AC-11 NIST SP800-53 AC-12
<input type="checkbox"/> 986	Immutable data copies	Malware Protection	FFIEC ISO/IEC 27040 SEC Rule 17a-4
<input type="checkbox"/> 942	In-flight data (client-server) is encrypted	Encryption	ISO/IEC 27040 NIST NIST SP800-53 NIST SP800-53 SC-8
<input type="checkbox"/> 932	Inactive user accounts are disabled	Authentication	PCI DSS PCI DSS 8.1.4 CIS Control CIS Control 16.10
<input type="checkbox"/> 940	Initial password change required	Authentication	PCI DSS PCI DSS 8.2.3 SWIFT ISO/IEC 27001 ISO/IEC 27001 A.9.4.3 Community ISO/IEC 27040 CIS Control CIS Control 4.4 NIST

195 items



Scan

Associations

Admin

Schedule

Troubleshooting

AvailabilityGuard

Data Security Advisor

Policies

Principles

Labels

Checks

Custom checks

Data Security Advisor > Manage checks

Search...

Group By: None

	Active	Principle	Check		Category	Associated Policies	Labels	Severity
	⚠	Clear-text protocols are disabled	[DSA--Brocade] LDAP SSL	↑	Encryption	All Checks, CIS, Community BP, ISO/IE	FFIEC PCI DSS PCI DSS 2.3 Community ISO/IEC 27040	WARNING
	✓	Maximum password lifetime is restricted	[DSA--Cisco] K0319I0MP295: Maximum password age		Authentication	All Checks, CIS, Community BP, ISO/IE	PCI DSS PCI DSS 8.2.4 SWIFT SWIFT CSP 4.1 ISO ISO/IEC	WARNING
	✓	Strong password hashing algorithm used	[DSA--Cisco] K0319I0MP296: Strong password encryption		Authentication	All Checks, My Policy, NIST	NIST NIST SP800-107	WARNING
	✓	Fabric access is restricted	[DSA--Cisco] K0519I0M0707: Watch-for-login-attacks feature		Access Control	All Checks, ISO/IEC, Vendor BP	Brocade Fibre Channel Security Best Practices ISO/IEC 27040	WARNING
	✓	Sensitive information is not transmitted as cleartext	[DSA--Cisco] K071900M0806: SNMP message privacy enforcement		Encryption	All Checks, CIS, My Policy, NIST, PCI D:	PCI DSS PCI DSS 3.4 CIS Control CIS Control 16.5 CIS Con	WARNING
	✓	Secure SNMP versions used (SNMPv3 or its successors)	[DSA--Cisco] K071900M0810: SNMP versions enabled		Services and Protoc...	All Checks, CIS, Vendor BP	CISA CISA Alert TA17-156 Cisco Implementation Guide	WARNING
	✓	Only enable SNMP if absolutely necessary	[DSA--Cisco] K071900M0851: SNMP status		Services and Protoc...	All Checks	Defense Information Systems Agency (DISA) The Center for Int	WARNING
	✓	Vendor-supplied default passwords are not used	[DSA--Cisco] K071900M0852: SNMP community default string		Access Control	All Checks, CIS, Community BP, ISO/IE	FFIEC PCI DSS PCI DSS 2.1 Community ISO/IEC 27040	WARNING
	✓	Logging server redundancy	[DSA--Data Domain] K010C00M0125: External syslog server redund...		Audit	All Checks, ISO/IEC, My Policy, NIST, P	PCI DSS PCI DSS 10.5 ISO ISO/IEC 27001 ISO/IEC 27001 A	WARNING
	✓	Remove or disable all default (factory) user accounts	[DSA--Data Domain] K020C00P110: Default users used		Authentication	All Checks, Community BP, ISO/IEC, M	FFIEC PCI DSS PCI DSS 8.1.1 ISO ISO/IEC 27001 ISO/IEC	WARNING
	✓	Access rights granted to authorized users/hosts only	[DSA--Data Domain] K020CI0M0584: Client authentication enforce...		Authorization	All Checks, CIS, Community BP, ISO/IE	PCI DSS PCI DSS 7.1 Community ISO/IEC 27040 CIS Conu	WARNING
	✓	Anonymous user access is limited	[DSA--Data Domain] K030CI000377: Root squash is enforced		Authorization	All Checks, CIS, ISO/IEC, Vendor BP	CIS Windows Server Benchmark ISO/IEC 27040 SANS	WARNING
	✓	certification verification is mandatory	[DSA--Data Domain] K040CI00P462: SMB digital signing		Authentication	All Checks, Vendor BP	EMC Security Guide	INFO
	✓	Clear-text protocols are disabled	[DSA--Data Domain] K060CI0MP700: ftp service status		Encryption	All Checks, CIS, Community BP, ISO/IE	FFIEC PCI DSS PCI DSS 2.3 Community ISO/IEC 27040	ERROR
	✓	Clear-text protocols are disabled	[DSA--Data Domain] K060CI0MP700: http service status		Encryption	All Checks, CIS, Community BP, ISO/IE	FFIEC PCI DSS PCI DSS 2.3 Community ISO/IEC 27040	ERROR
	✓	SNMP authentication required	[DSA--Data Domain] K070C00M0800: SNMP user authentication		Services and Protoc...	All Checks, CIS, Community BP, My Pc	PCI DSS PCI DSS 8 Cisco Security Baseline Community	WARNING
	✓	Strong encryption used	[DSA--Data Domain] K070C00M0806: SNMP message privacy algori...		Encryption	All Checks, PCI DSS, Vendor BP	PCI DSS SWIFT EMC Security Guide	WARNING
	✓	Sensitive information is not transmitted as cleartext	[DSA--Data Domain] K070C00M0807: SNMP message privacy		Encryption	All Checks, CIS, My Policy, NIST, PCI D:	PCI DSS PCI DSS 3.4 CIS Control CIS Control 16.5 CIS Con	WARNING
	✓	Secure SNMP versions used (SNMPv3 or its successors)	[DSA--Data Domain] K070C00M0810: SNMPv1 / SNMPv2 status		Services and Protoc...	All Checks, CIS, Vendor BP	CISA CISA Alert TA17-156 Cisco Implementation Guide	WARNING
	✓	Vendor-supplied default passwords are not used	[DSA--Data Domain] K070C00M0852: SNMP community default stri...		Access Control	All Checks, CIS, Community BP, ISO/IE	FFIEC PCI DSS PCI DSS 2.1 Community ISO/IEC 27040	ERROR
	✓	Immutable data copies	[DSA--Data Domain] K080CI00P183: Protected recovery copies		Malware Protection	All Checks, ISO/IEC	FFIEC ISO/IEC 27040 SEC Rule 17a-4	WARNING
	✓	Idle sessions are terminated	[DSA--Data Domain] K110CI00P690: Session timeout		Access Control	All Checks, CIS, My Policy, NIST, PCI D:	PCI DSS PCI DSS 12.3.8 CIS Control CIS Control 16 NIST	WARNING
	✓	FIPS compliance features are enabled	[DSA--Data Domain] K150C00P100: FIPS mode status		Encryption	All Checks	FIPS	WARNING
	✓	Vulnerability identification	[DSA--Isilon] Isilon vulnerability analysis: DSA-2020-039		Vulnerabilities (CVE)	All Checks, CVE	CVE-2019-9924	WARNING
	✓	Vulnerability identification	[DSA--Isilon] Isilon vulnerability analysis: DSA-2020-096		Vulnerabilities (CVE)	All Checks, CVE	CVE-2019-9924	WARNING
	✓	Vulnerability identification	[DSA--Isilon] Isilon vulnerability analysis: DSA-2020-124		Vulnerabilities (CVE)	All Checks, CVE	CVE-2019-9924	WARNING
	✓	Vulnerability identification	[DSA--Isilon] Isilon vulnerability analysis: DSA-2020-155		Vulnerabilities (CVE)	All Checks, CVE	CVE-2019-9924	WARNING
	✓	Vulnerability identification	[DSA--Isilon] Isilon vulnerability analysis: DSA-2020-164		Vulnerabilities (CVE)	All Checks, CVE	CVE-2019-9924	WARNING

Selected 1 of 451 items

⌂

Show 50 1 < 1 > 10

Scan

Associations

Admin

Schedule

Troubleshooting

Data Security Advisor

Policies

Principles

Labels

Checks

Custom checks

Data Security Advisor > Security policies

Search...

Group By: None

	Name	Description	Labels	Number Of Princ...	Enabled
5	CIS	All checks associated with CIS Controls will be executed	CIS Windows Server Benchmark, CIS Windows Server Benchmark CCE-37073-4, CISA, CISA Alert Tr	40	<input checked="" type="checkbox"/>
6	CVE	DSA searches for known storage vulnerabilities and exp...	CVE-1999-0511, CVE-2007-6750, CVE-2013-5211, CVE-2013-6449, CVE-2014-8964, CVE-2015-02	1	<input checked="" type="checkbox"/>
7	Community BP	Checks based on expert forums and user feedback	Community	32	<input checked="" type="checkbox"/>
3	ISO/IEC	All checks associated with ISO standards will be executed	ISO, ISO/IEC 17799, ISO/IEC 17799 11.5.1, ISO/IEC 17799 15.1.5, ISO/IEC 27001, ISO/IEC 27001	44	<input checked="" type="checkbox"/>
1	My Checks	My DSA checks will be executed	Brocade Fibre Channel Security Best Practices, FFIEC, PCI DSS, PCI DSS 10, PCI DSS 10.4, PCI D	78	<input checked="" type="checkbox"/>
2	NIST	All checks associated with NIST guides will be executed	NIST SP 800-131A, NIST, NIST IR 7966, NIST SP800-107, NIST SP800-123, NIST SP800-171, NIS	55	<input checked="" type="checkbox"/>
4	PCI DS	All checks associated with PCI DSS will be executed	PCI DSS, PCI DSS 10, PCI DSS 10.4, PCI DSS 10.5, PCI DSS 10.7, PCI DSS 12.3.8, PCI DSS 2.1	45	<input checked="" type="checkbox"/>
8	Vendor	All checks associated with vendor security guides or artic...	Brocade Fibre Channel Security Best Practices, CIS Windows Server Benchmark, CIS Windows Serve	13	<input checked="" type="checkbox"/>

- Add

Edit

Delete

Disable

Edit customizable parameters

View related principles

Assign additional items

Scan

Associations

Admin

Schedule

Troubleshooting

Data Security Advisor

Policies

Principles

Labels

Checks

Custom d

Data Security Advisor > Security policies

Parameters for policy "NIST"

Search...

Group By: None

	Principle	Package	Check name	Parameter	Value
	Account lockout duration	DSA-Brocade	K030DI0MP295: Minimum account lockout dur...	Account lockout duration	Number: 2
	Account lockout duration	DSA-Isilon	K030DI0MP295: Minimum account lockout dur...	Lockout duration (Isilon time)	String: 15m
	Account lockout duration	DSA-Cisco	K0319I0MP295: Minimum account lockout dur...	Account lockout duration	Positive Number: 13
	Account lockout enforcement for admin	DSA-Brocade	K0304I0MP295: Lockout enforcement for admin	Enable admin lockout	Number: 1
	Account lockout threshold	DSA-NetApp	K0202I0MP295: Account lockout threshold (7-...	Maximum failed login	Number: 3
	Account lockout threshold	DSA-NetApp	K0202I0MP295: Account lockout threshold (cD...	Maximum failed login	Number: 3
	Account lockout threshold	DSA-Brocade	K0304I0MP295: Account lockout threshold	Account lockout threshold	Number: 2
	Account lockout threshold	DSA-Isilon	K030DI0MP295: Account lockout threshold	Max login attempts	Number: 3
	Account lockout threshold	DSA-Hitachi	K0310I0MP295: Account lockout threshold	Max login attempts	Number: 3
	Account lockout threshold	DSA-Cisco	K0319I0MP295: Account lockout threshold	Lockout threshold	Positive Number: 2
	Antivirus server redundancy	DSA-NetApp	K170300M0230: Antivirus server redundancy (...)	Minimum number of vscan servers	Number: 2
	Antivirus server redundancy	DSA-Isilon	K170D00M0230: Antivirus server redundancy	Minimum number of ICAP servers	Number: 2
	Approved OS release	DSA-Isilon	K090D00MP150: OS version check	Approved version	String: N/A
	Audit log configuration (Log content)	DSA-Brocade	K0104I00P160: Event types enabled for audit l...	Required filters (event classes)	String: ZONE,SECURITY,CONFIGURATION,FIRMI
	Audit log configuration (Log content)	DSA-Cisco	K0119I00P165: Event types enabled for audit l...	Required Logger Types	String: console,monitor,linecard,loopback,logfl.
	Audit logging is enabled	DSA-NetApp	K01020000144: Audit logging status (7-Mode)	Enable audit logging	String: on
	Audit logging is enabled	DSA-NetApp	K01020000145: Security audit logging - read-o...	Audit read-only API	String: on
	Audit logging is enabled	DSA-NetApp	K01020000145: Security audit logging - read-o...	GET Audit logging required for interfaces	String: CLI,ONTAPI,HTTP,SNMP
	Authorized (secure) time source servers are us...	DSA-Brocade	K05040000660: Approved NTP Servers	Approved NTP Servers	10.92.4.55
	Authorized (secure) time source servers are us...	DSA-Data Domain	K050C10MP605: Required NTP servers	Required NTP servers	String: N/A

Selected 1 of 215 items

Show

50

1 <

1

>

5

Apply

Number Of Princ...

Enabled

13

45

56

44

32

132

40

210

Selected 1 of 8 items

Show

50

1 <

1

>

1



Scan



Associations



Admin



Schedule



Troubleshooting

Data Security  
Advisor

Policies

Principles

Labels

Checks

Custom checks

Data Security Ad

Search...

8

4

2

3

7

6

5

1

## Add Security policies



## Name

My Custom Policy - Only Checks labeled CIS

## Description

## Include labels (RegExp)

CIS

## Exclude labels (RegExp)

## Labels (0)

CIS Windows Server Benchmark CIS Windows Server Benchmark CCE-37073-4 CISA CISA Alert TA17-156 Cisco Implementation Guide Cisco MDS 9000 Series Fabric Configuration Guide  
Cisco MDS 9000 Series Security Configuration Guide Cisco Security Baseline The Center for Internet Security (CIS) CIS Control CIS Control 11.5 CIS Control 12.4 CIS Control 14.4  
CIS Control 14.8 CIS Control 16 CIS Control 16.10 CIS Control 16.2 CIS Control 16.5 CIS Control 18.3 CIS Control 4 CIS Control 4.1 CIS Control 4.2 CIS Control 4.4 CIS Control 4.5  
CIS Control 6 CIS Control 6.1 CIS Control 6.5 CIS Control 8.1 CIS Control 9.4

## Scope rules (automatic assigned)

☐ Fetch only systems in scan scope

System types

Symmetrix x

Isilon x



Sites Select...

Name (RegExp)



## Additional items (directly assigned)

Cancel

Save

Group By: None v



Number Of Princ...

Enabled

CIS Windows Server Benchmark	CIS Windows Server	13	<input checked="" type="checkbox"/>
DSS 10.5 PCI DSS 10.7 PCI DSS 12.3.3 PCI DSS 2.1 PCI		45	<input checked="" type="checkbox"/>
NIST SP800-107 NIST SP800-123 NIST SP800-171 NIST		56	<input checked="" type="checkbox"/>
ISO/IEC 17799 15.1.5 ISO/IEC 27001 ISO/IEC 27001 A		44	<input checked="" type="checkbox"/>
3-5211 CVE-2013-6449 CVE-2014-8964 CVE-2014-9935		32	<input checked="" type="checkbox"/>
13-5211 CVE-2013-6449 CVE-2014-8964 CVE-2014-9935		132	<input checked="" type="checkbox"/>
Windows Server Benchmark CCE-37073-4 CISA CISA Alert TA1		40	<input checked="" type="checkbox"/>
85 FFIEC PCI DSS PCI DSS 10 PCI DSS 10.4 PCI DSS		210	<input checked="" type="checkbox"/>

8 items



Show

50 v

1 &lt;

1

&gt; 1