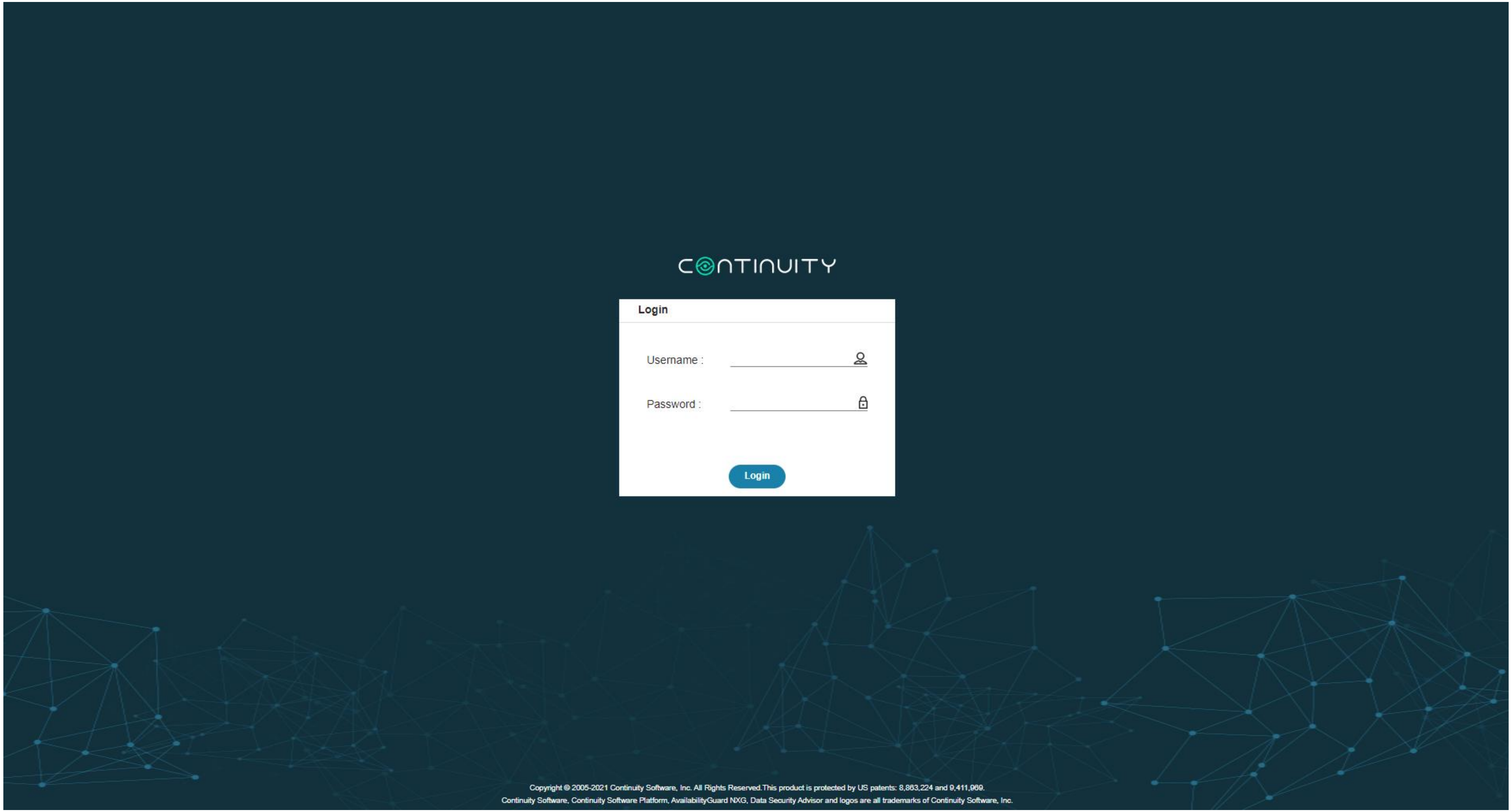
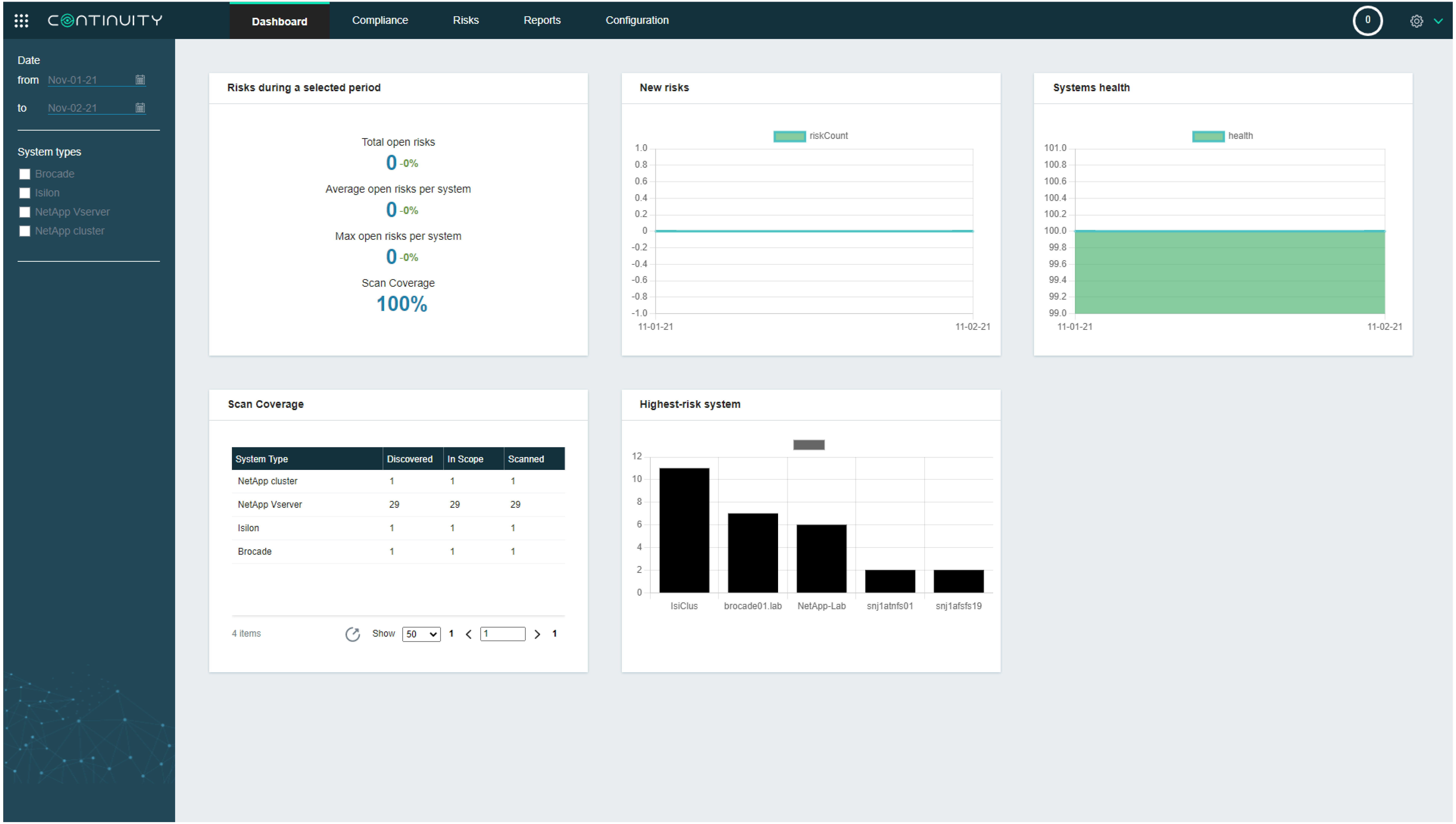
What we will do today

Step-by-Step Guided StorageGuard ™ POC, including:

Step I: Scan	Scan a sample Storage system in Continuity Labs
Step II: Detect	Run StorageGuard ™ Security Risk Analysis
Step III: Review	Review Sample Misconfigurations & Vulnerabilities detected by StorageGuard™
Step IV: Report	Generate the StorageGuard ™ Risk Assessment Report – Automatically!

Q&A


CONTINUITY
Login
Username :
Password :
Login



Date

from Nov-01-21

to Nov-02-21

System types

- □ Brocade
- □ Isilon
- □ NetApp Vserver
- □ NetApp cluster

Risks during a selected period

Total open risks

0 -0%

Average open risks per system

0 -0%

Max open risks per system

0 -0%

Scan Coverage

100%

New risks

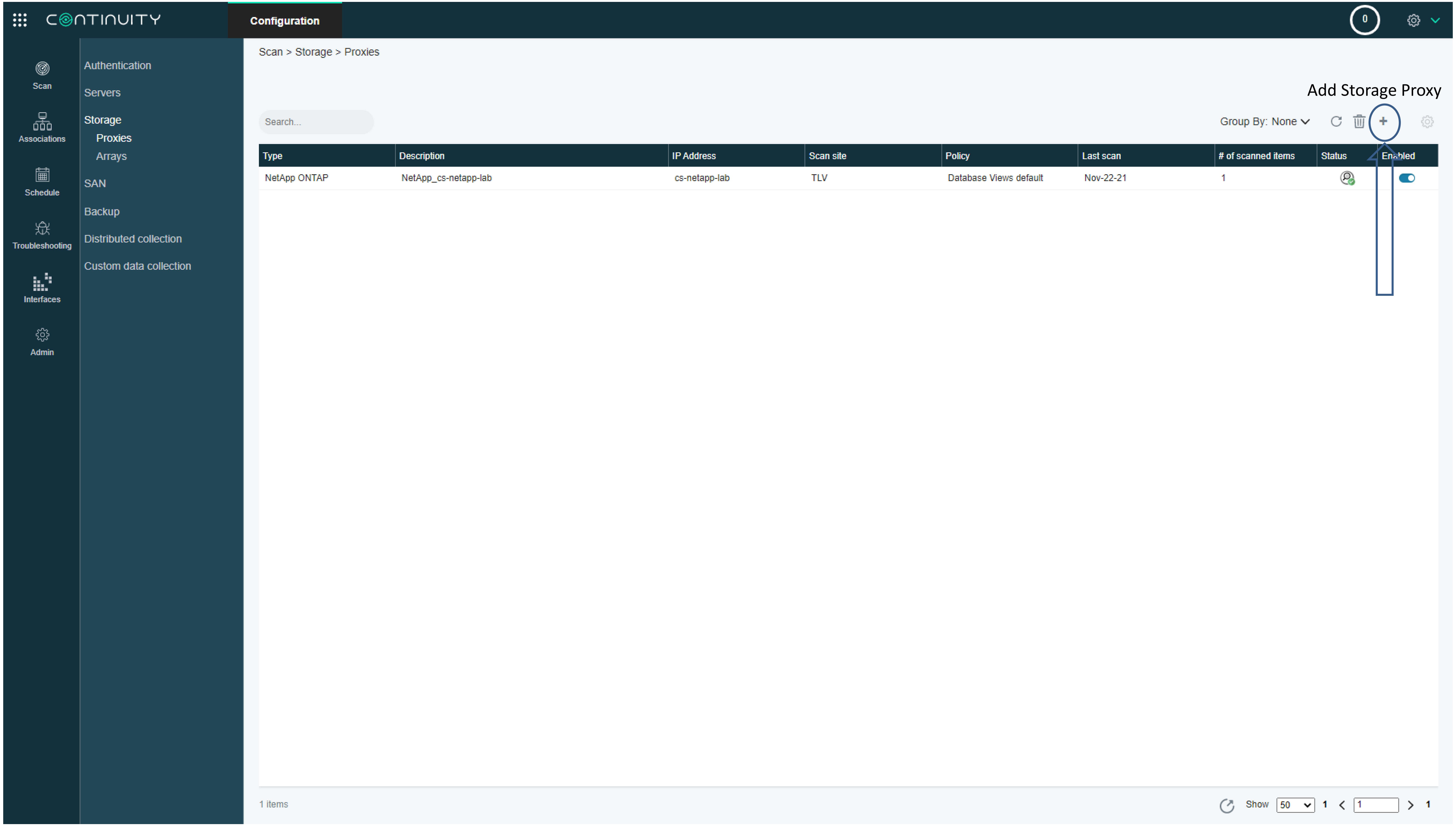
Systems health

Scan Coverage

System Type	Discovered	In Scope	Scanned
NetApp cluster	1	1	1
NetApp Vserver	29	29	29
Isilon	1	1	1
Brocade	1	1	1

4 items

Highest-risk system

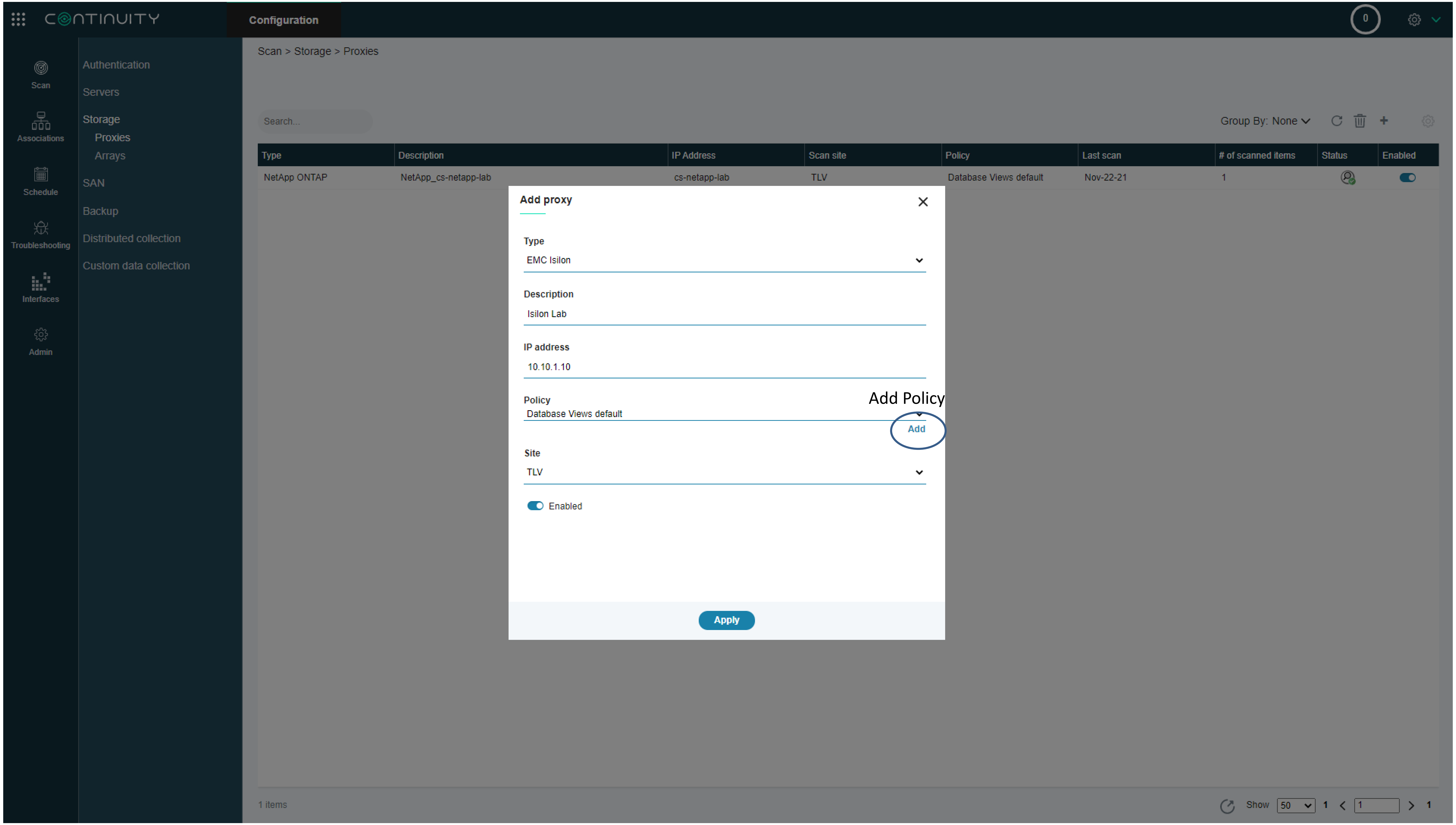


Scan > Storage > Proxies

Add Storage Proxy

Type	Description	IP Address	Scan site	Policy	Last scan	# of scanned items	Status	Enabled
NetApp ONTAP	NetApp_cs-netapp-lab	cs-netapp-lab	TLV	Database Views default	Nov-22-21	1		

1 items



Type	Description	IP Address	Scan site	Policy	Last scan	# of scanned items	Status	Enabled
NetApp ONTAP	NetApp_cs-netapp-lab	cs-netapp-lab	TLV	Database Views default	Nov-22-21	1		

Add proxy

Type: EMC Isilon

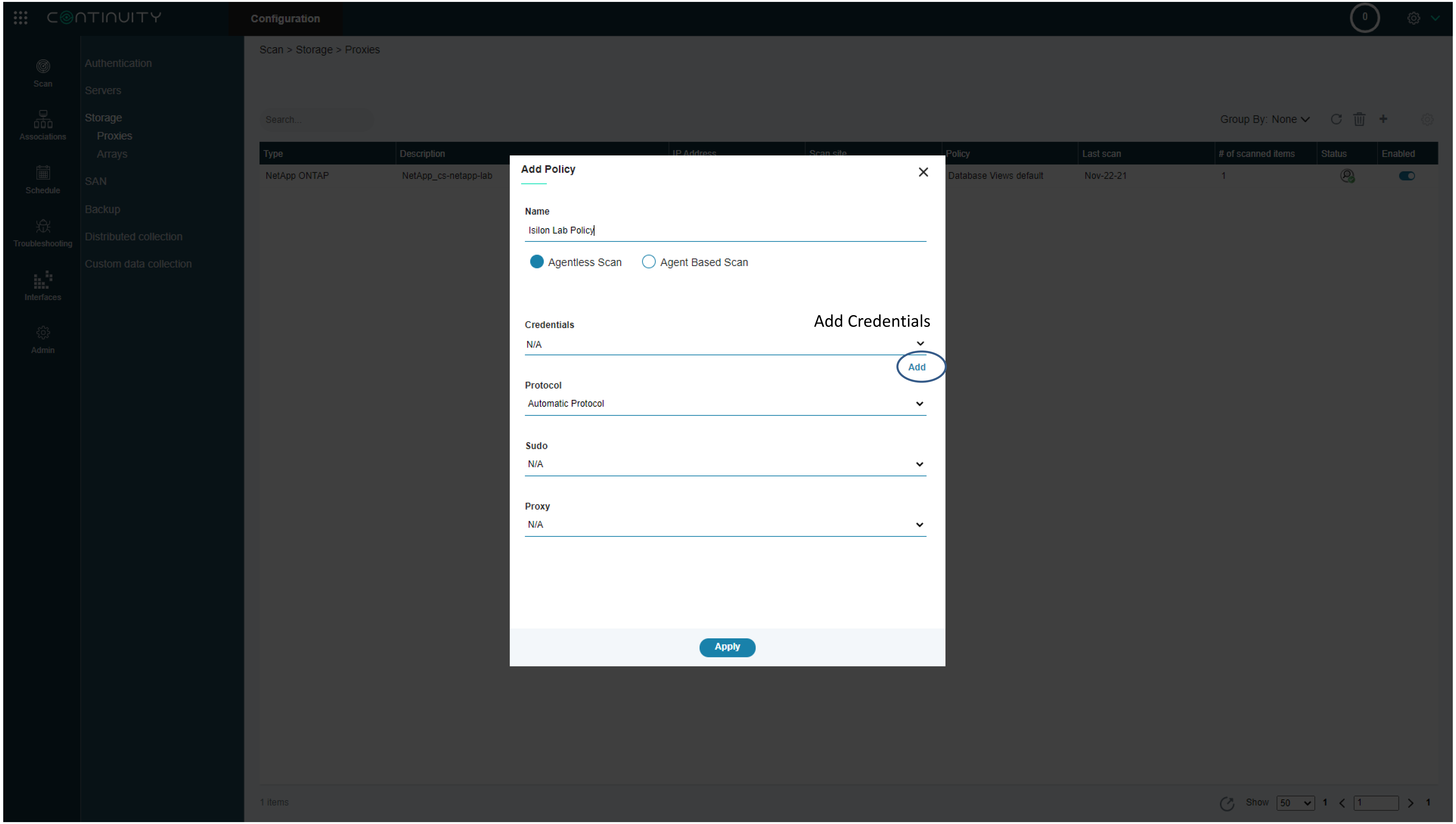
Description: Isilon Lab

IP address: 10.10.1.10

Policy: Database Views default

Site: TLV

Enabled



Type	Description	IP Address	Scan site	Policy	Last scan	# of scanned items	Status	Enabled
NetApp ONTAP	NetApp_cs-netapp-lab			Database Views default	Nov-22-21	1		

Add Policy

Name: Isilon Lab Policy

● Agentless Scan ○ Agent Based Scan

Add Credentials

Credentials: N/A

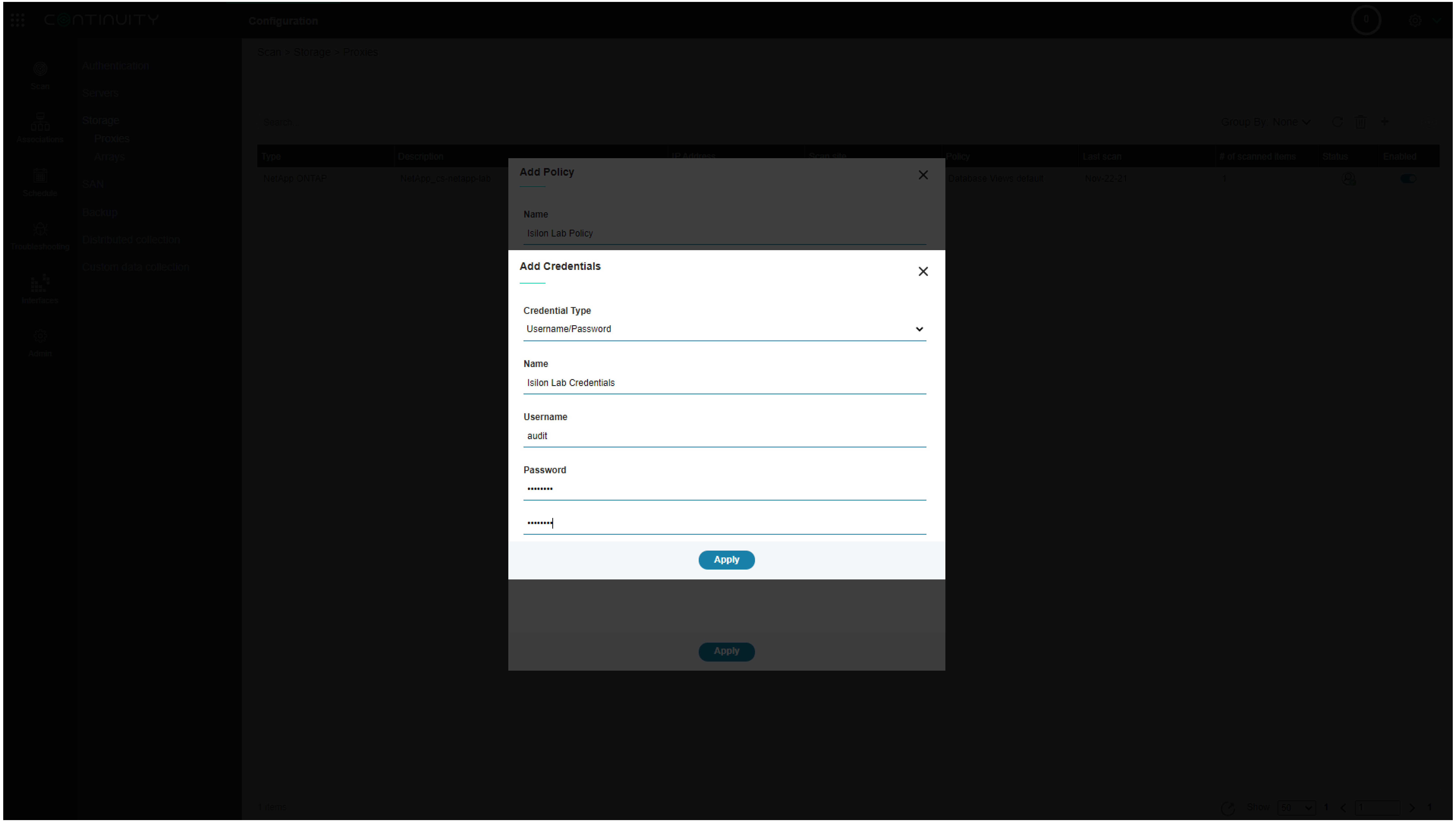
Add

Protocol: Automatic Protocol

Sudo: N/A

Proxy: N/A

Apply



Add Policy

Name

Isilon Lab Policy

Add Credentials

Credential Type

Username/Password

Name

Isilon Lab Credentials

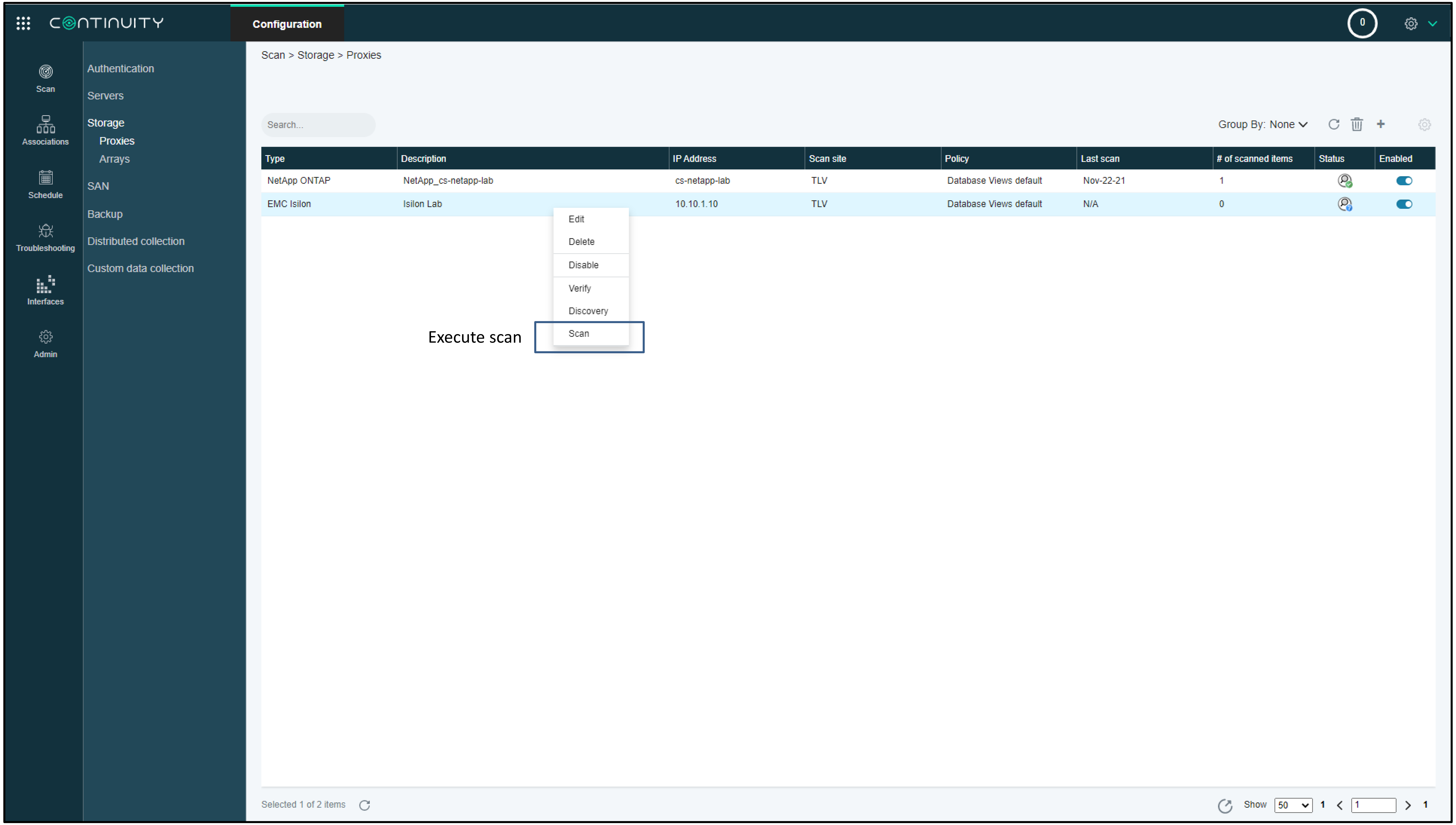
Username

audit

Password

••••••••

••••••••

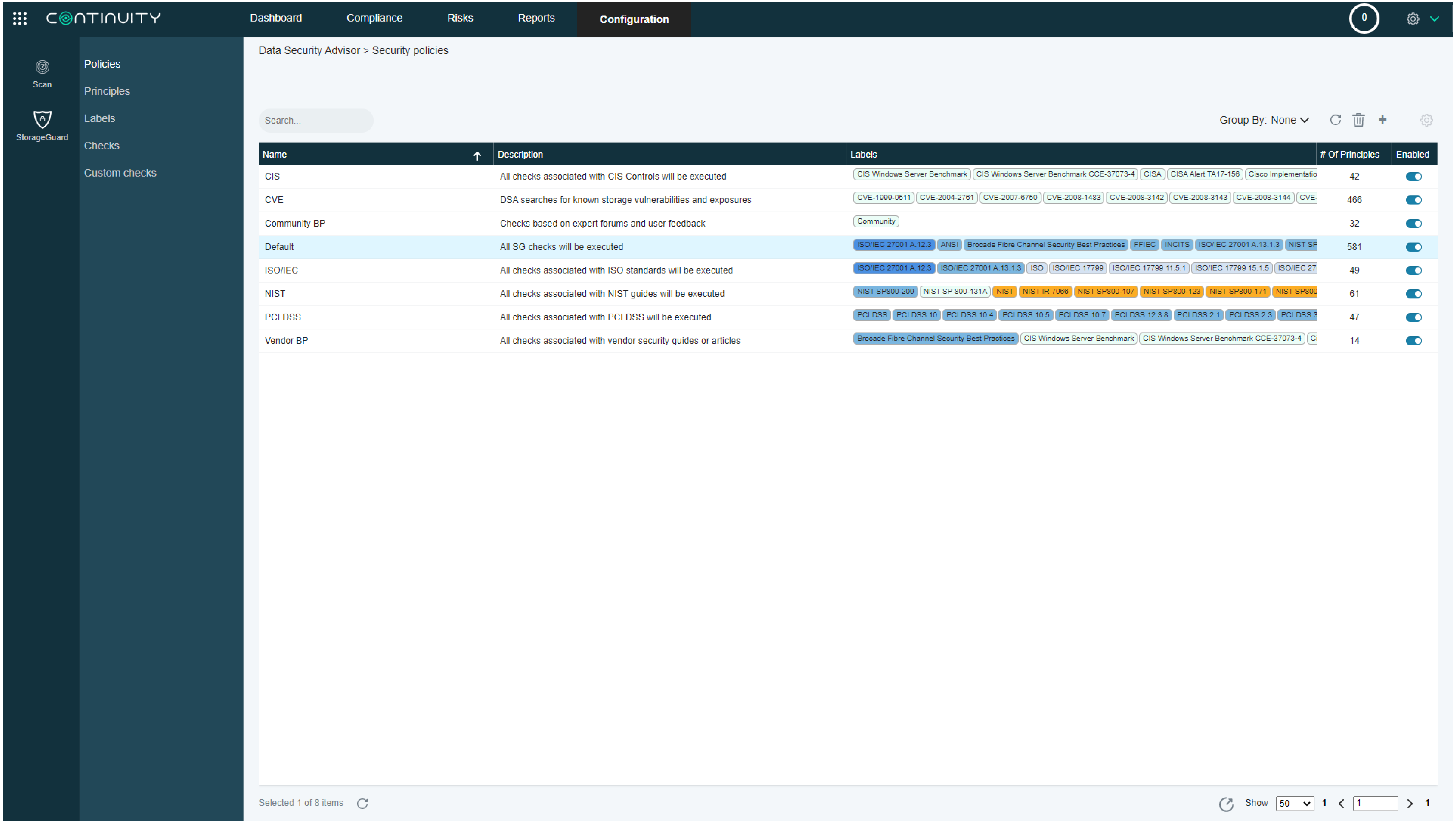


Scan > Storage > Proxies

Type	Description	IP Address	Scan site	Policy	Last scan	# of scanned items	Status	Enabled
NetApp ONTAP	NetApp_cs-netapp-lab	cs-netapp-lab	TLV	Database Views default	Nov-22-21	1		
EMC Isilon	Isilon Lab	10.10.1.10	TLV	Database Views default	N/A	0		

Execute scan

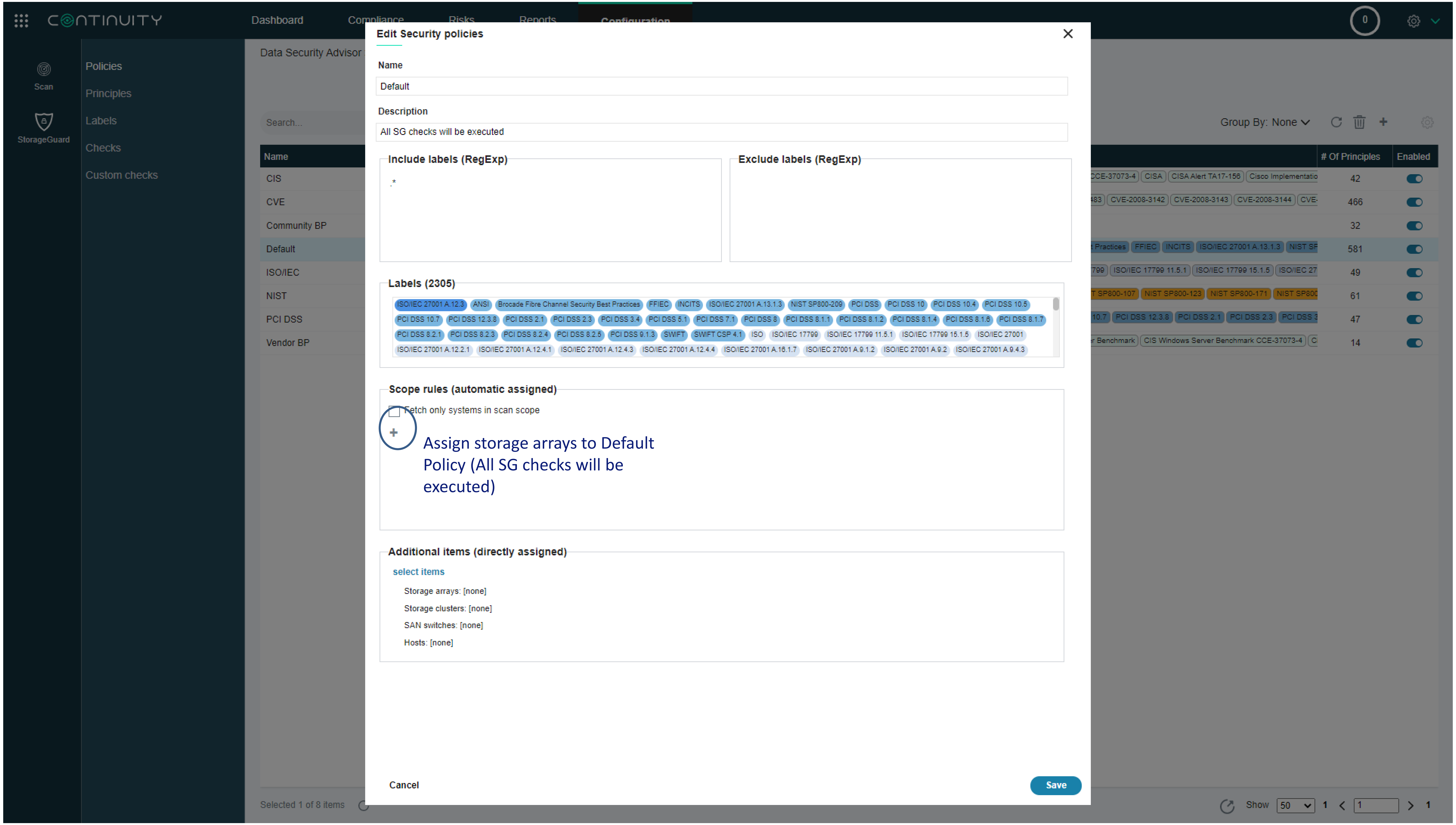
Selected 1 of 2 items



Data Security Advisor > Security policies

Name	Description	Labels	# Of Principles	Enabled
CIS	All checks associated with CIS Controls will be executed	CIS Windows Server Benchmark CIS Windows Server Benchmark CCE-37073-4 CISA CISA Alert TA17-156 Cisco Implementatio	42	●
CVE	DSA searches for known storage vulnerabilities and exposures	CVE-1999-0511 CVE-2004-2761 CVE-2007-6750 CVE-2008-1483 CVE-2008-3142 CVE-2008-3143 CVE-2008-3144 CVE-	466	●
Community BP	Checks based on expert forums and user feedback	Community	32	●
Default	All SG checks will be executed	ISO/IEC 27001 A.12.3 ANSI Brocade Fibre Channel Security Best Practices FFIEC INCITS ISO/IEC 27001 A.13.1.3 NIST SF	581	●
ISO/IEC	All checks associated with ISO standards will be executed	ISO/IEC 27001 A.12.3 ISO/IEC 27001 A.13.1.3 ISO ISO/IEC 17799 ISO/IEC 17799 11.5.1 ISO/IEC 17799 15.1.5 ISO/IEC 27	49	●
NIST	All checks associated with NIST guides will be executed	NIST SP800-209 NIST SP 800-131A NIST NIST IR 7966 NIST SP800-107 NIST SP800-123 NIST SP800-171 NIST SP800	61	●
PCI DSS	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 PCI DSS 2.3 PCI DSS 3	47	●
Vendor BP	All checks associated with vendor security guides or articles	Brocade Fibre Channel Security Best Practices CIS Windows Server Benchmark CIS Windows Server Benchmark CCE-37073-4 C	14	●

Selected 1 of 8 items



Name	# Of Principles	Enabled
CIS	42	●
CVE	466	●
Community BP	32	●
Default	581	●
ISO/IEC	49	●
NIST	61	●
PCI DSS	47	●
Vendor BP	14	●

Edit Security policies

Name

Default

Description

All SG checks will be executed

Include labels (RegExp)

.*

Exclude labels (RegExp)

Labels (2305)

ISO/IEC 27001 A.12.3 · ANSI · Brocade Fibre Channel Security Best Practices · FFIEC · INCITS · ISO/IEC 27001 A.13.1.3 · NIST SP800-209 · 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 · PCI DSS 2.3 · PCI DSS 3.4 · PCI DSS 5.1 · PCI DSS 7.1 · PCI DSS 8 · PCI DSS 8.1.1 · PCI DSS 8.1.2 · PCI DSS 8.1.4 · PCI DSS 8.1.6 · PCI DSS 8.1.7 · PCI DSS 8.2.1 · PCI DSS 8.2.3 · PCI DSS 8.2.4 · PCI DSS 8.2.5 · PCI DSS 9.1.3 · SWIFT · SWIFT CSP 4.1 · ISO · ISO/IEC 17799 · ISO/IEC 17799 11.5.1 · ISO/IEC 17799 15.1.5 · ISO/IEC 27001 · ISO/IEC 27001 A.12.2.1 · ISO/IEC 27001 A.12.4.1 · ISO/IEC 27001 A.12.4.3 · ISO/IEC 27001 A.12.4.4 · ISO/IEC 27001 A.16.1.7 · ISO/IEC 27001 A.9.1.2 · ISO/IEC 27001 A.9.2 · ISO/IEC 27001 A.9.4.3

Scope rules (automatic assigned)

□ Fetch only systems in scan scope

+

Assign storage arrays to Default Policy (All SG checks will be executed)

Additional items (directly assigned)

select items

Storage arrays: [none]

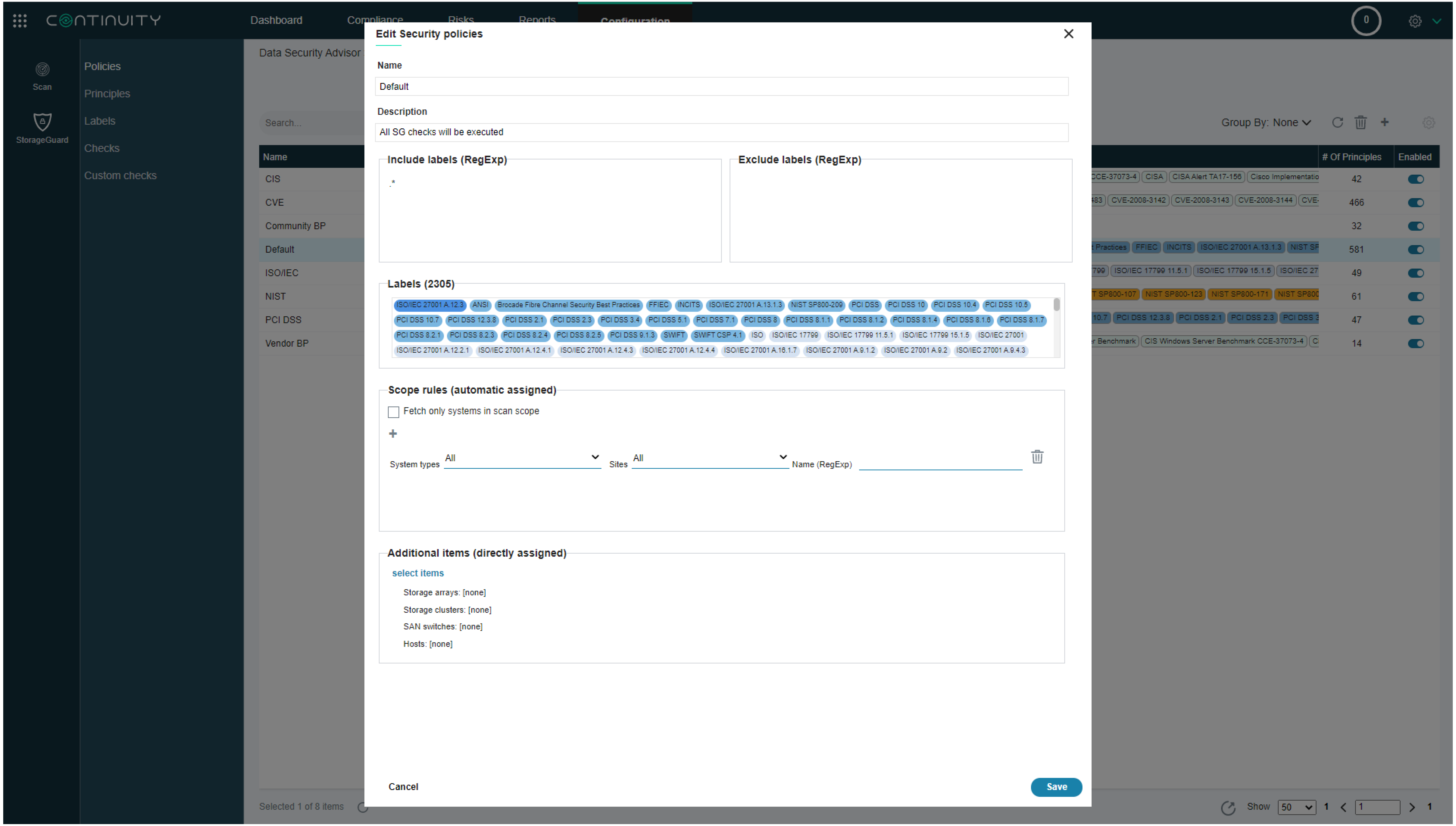
Storage clusters: [none]

SAN switches: [none]

Hosts: [none]

Cancel

Save



Name		# Of Principles	Enabled
CIS	CCE-37073-4 · CISA · CISA Alert TA17-156 · Cisco Implementatio	42	●
CVE	483 · CVE-2008-3142 · CVE-2008-3143 · CVE-2008-3144 · CVE-	466	●
Community BP		32	●
Default	t Practices · FFIEC · INCITS · ISO/IEC 27001 A.13.1.3 · NIST SF	581	●
ISO/IEC	799 · ISO/IEC 17799 11.5.1 · ISO/IEC 17799 15.1.5 · ISO/IEC 27	49	●
NIST	T SP800-107 · NIST SP800-123 · NIST SP800-171 · NIST SP800	61	●
PCI DSS	10.7 · PCI DSS 12.3.8 · PCI DSS 2.1 · PCI DSS 2.3 · PCI DSS 3	47	●
Vendor BP	r Benchmark · CIS Windows Server Benchmark CCE-37073-4 · C	14	●

Edit Security policies

Name

Default

Description

All SG checks will be executed

Include labels (RegExp)

.*

Exclude labels (RegExp)

Labels (2305)

ISO/IEC 27001 A.12.3 · ANSI · Brocade Fibre Channel Security Best Practices · FFIEC · INCITS · ISO/IEC 27001 A.13.1.3 · NIST SP800-209 · 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 · PCI DSS 2.3 · PCI DSS 3.4 · PCI DSS 5.1 · PCI DSS 7.1 · PCI DSS 8 · PCI DSS 8.1.1 · PCI DSS 8.1.2 · PCI DSS 8.1.4 · PCI DSS 8.1.6 · PCI DSS 8.1.7 · PCI DSS 8.2.1 · PCI DSS 8.2.3 · PCI DSS 8.2.4 · PCI DSS 8.2.5 · PCI DSS 9.1.3 · SWIFT · SWIFT CSP 4.1 · ISO · ISO/IEC 17799 · ISO/IEC 17799 11.5.1 · ISO/IEC 17799 15.1.5 · ISO/IEC 27001 · ISO/IEC 27001 A.12.2.1 · ISO/IEC 27001 A.12.4.1 · ISO/IEC 27001 A.12.4.3 · ISO/IEC 27001 A.12.4.4 · ISO/IEC 27001 A.16.1.7 · ISO/IEC 27001 A.9.1.2 · ISO/IEC 27001 A.9.2 · ISO/IEC 27001 A.9.4.3

Scope rules (automatic assigned)

☐ Fetch only systems in scan scope

+

System types: All · Sites: All · Name (RegExp):

Additional items (directly assigned)

select items

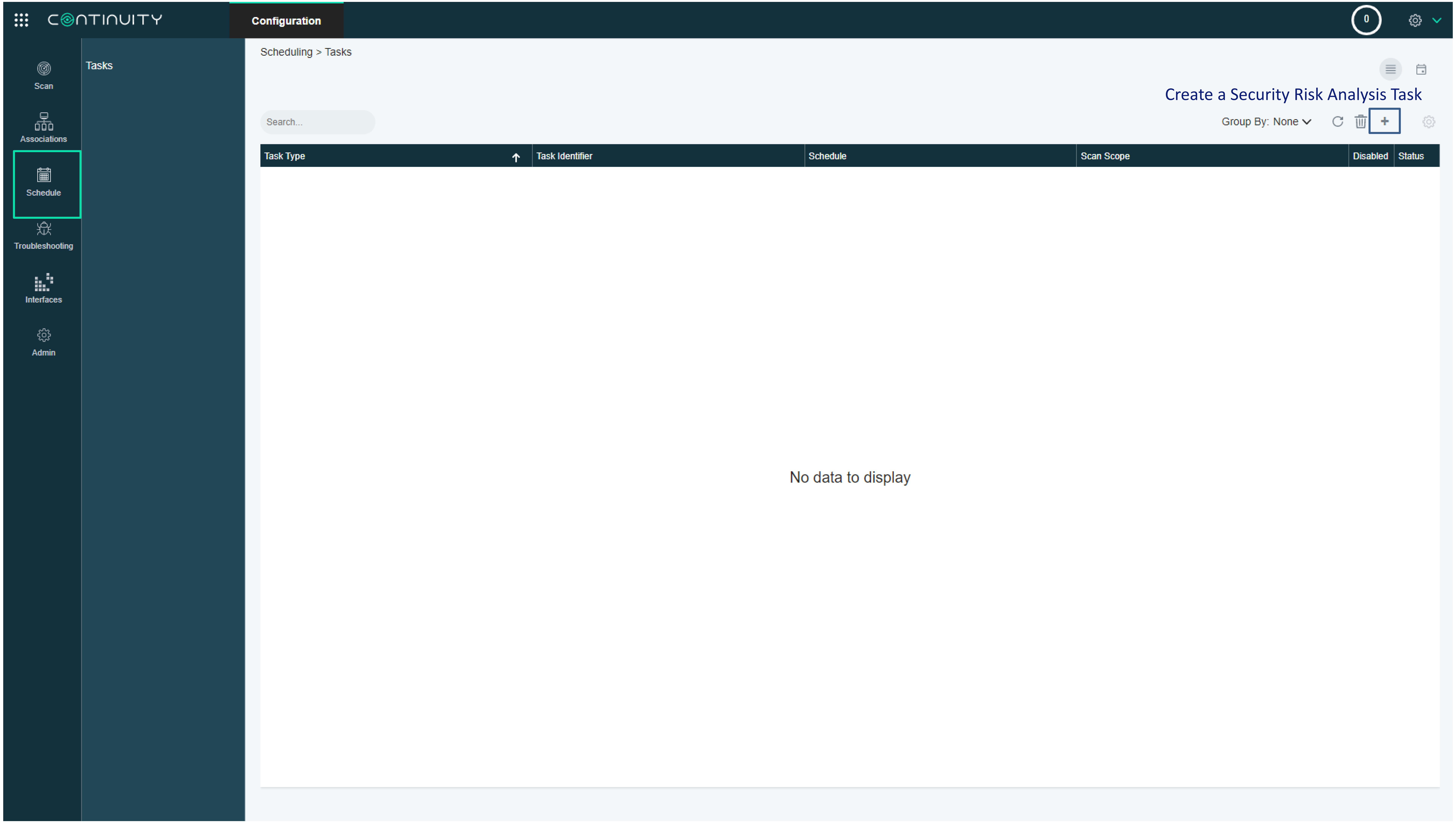
Storage arrays: [none]

Storage clusters: [none]

SAN switches: [none]

Hosts: [none]

Cancel · Save

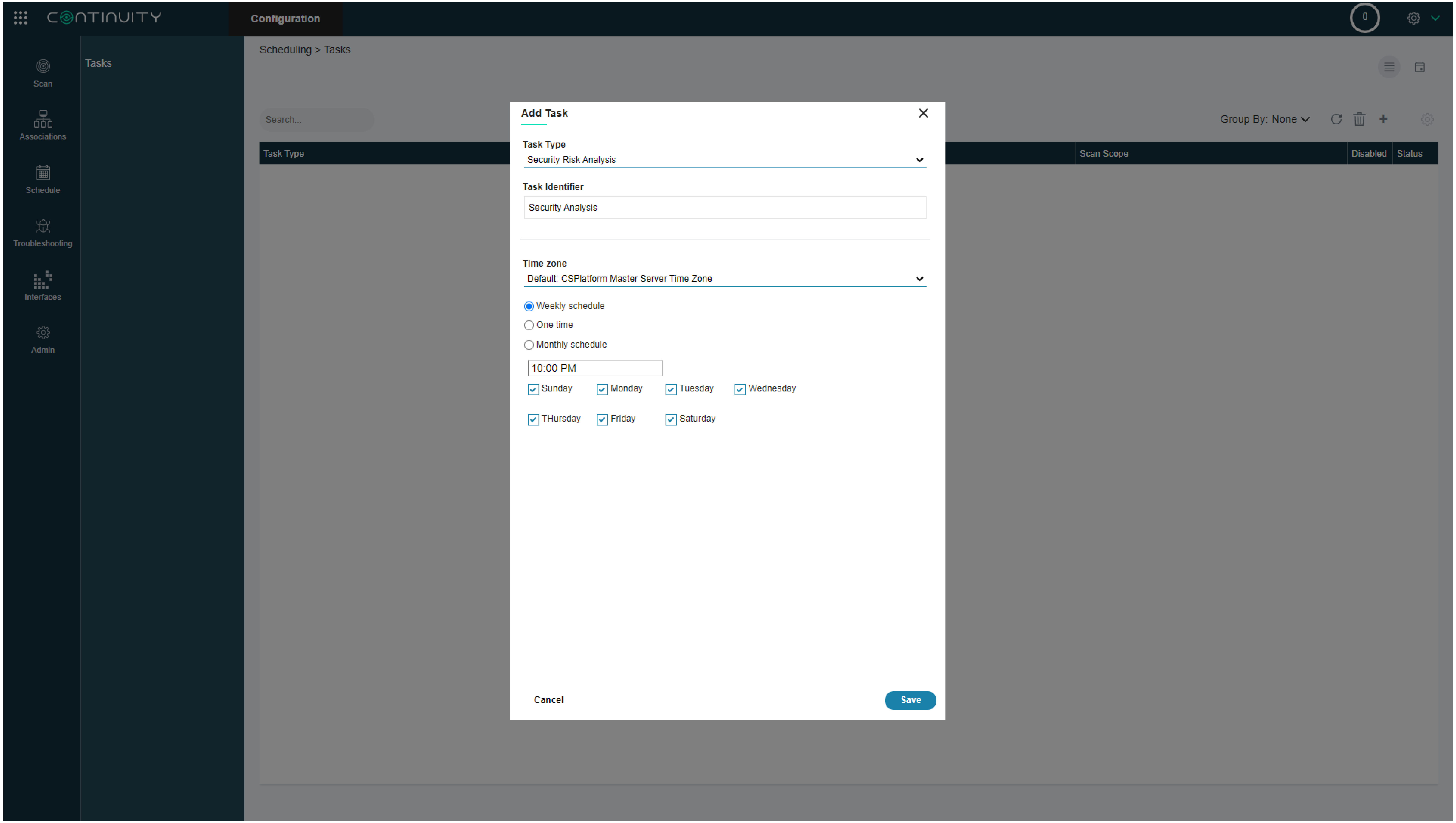


Create a Security Risk Analysis Task

Scheduling > Tasks

Task Type	Task Identifier	Schedule	Scan Scope	Disabled	Status

No data to display



Add Task

Task Type
Security Risk Analysis

Task Identifier
Security Analysis

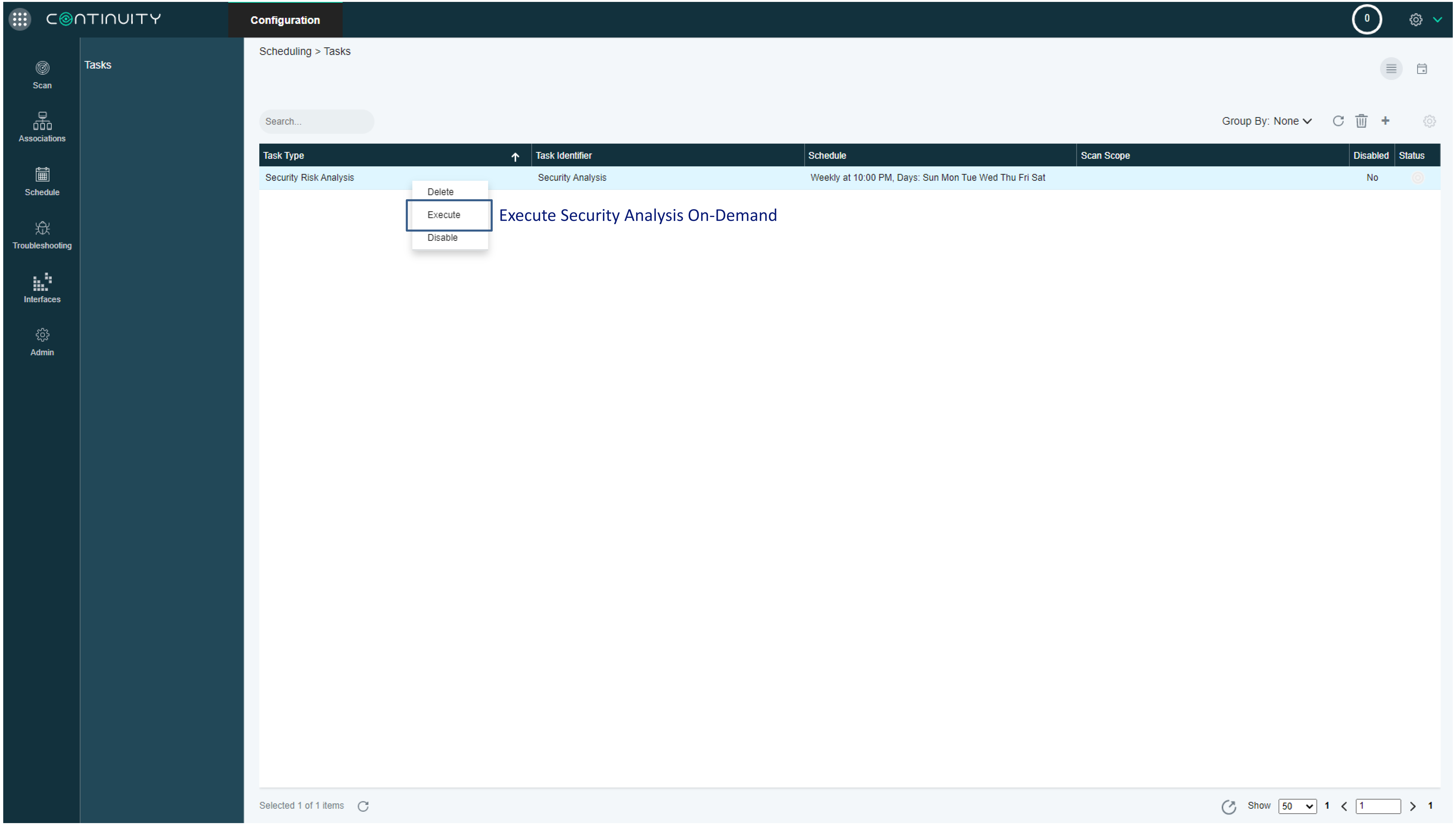
Time zone
Default: CSPlatform Master Server Time Zone

● Weekly schedule
○ One time
○ Monthly schedule

10:00 PM

☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday

☑ THursday ☑ Friday ☑ Saturday



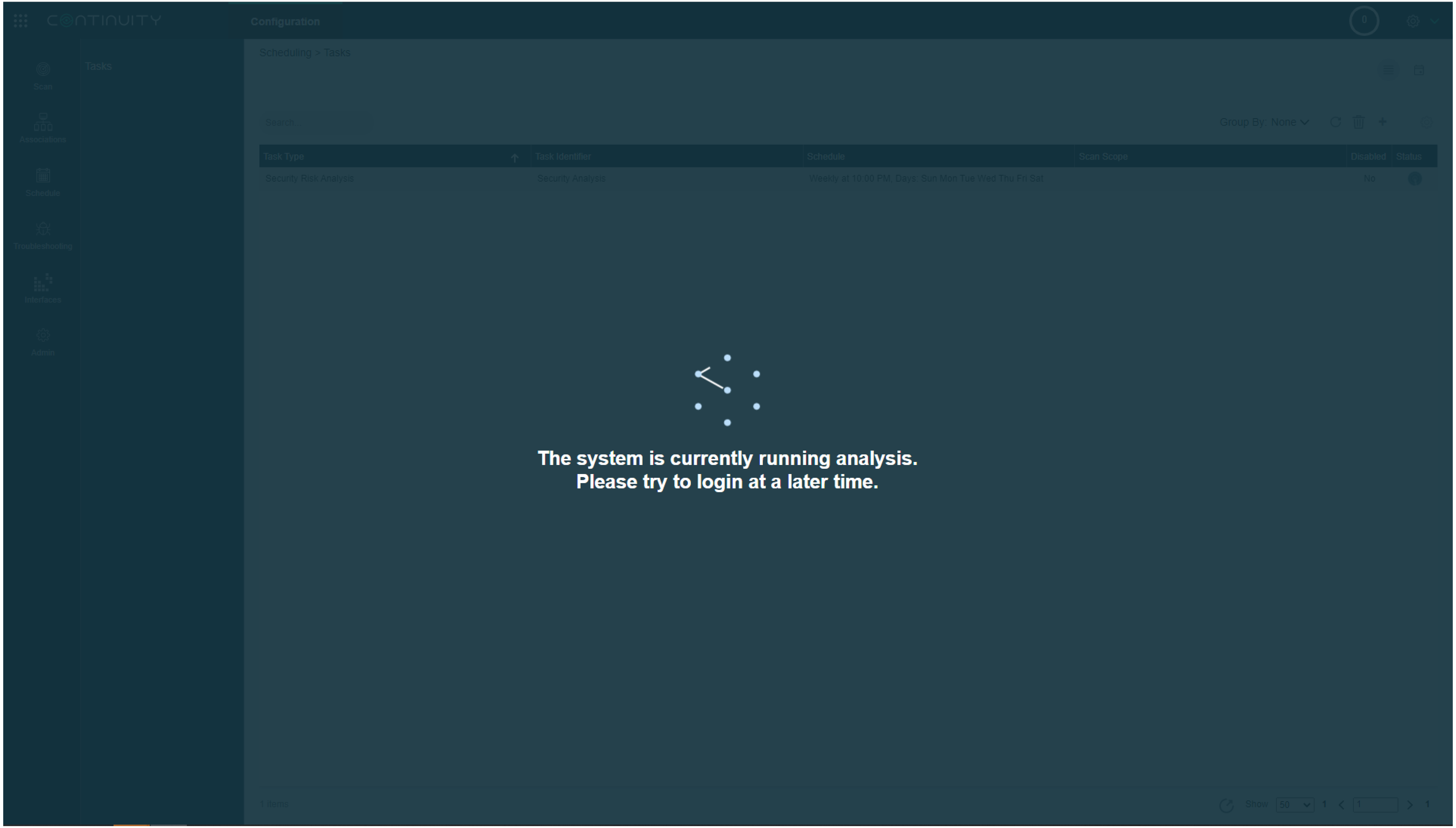
Scheduling > Tasks

Task Type	Task Identifier	Schedule	Scan Scope	Disabled	Status
Security Risk Analysis	Security Analysis	Weekly at 10:00 PM, Days: Sun Mon Tue Wed Thu Fri Sat		No	

Execute Security Analysis On-Demand

Selected 1 of 1 items

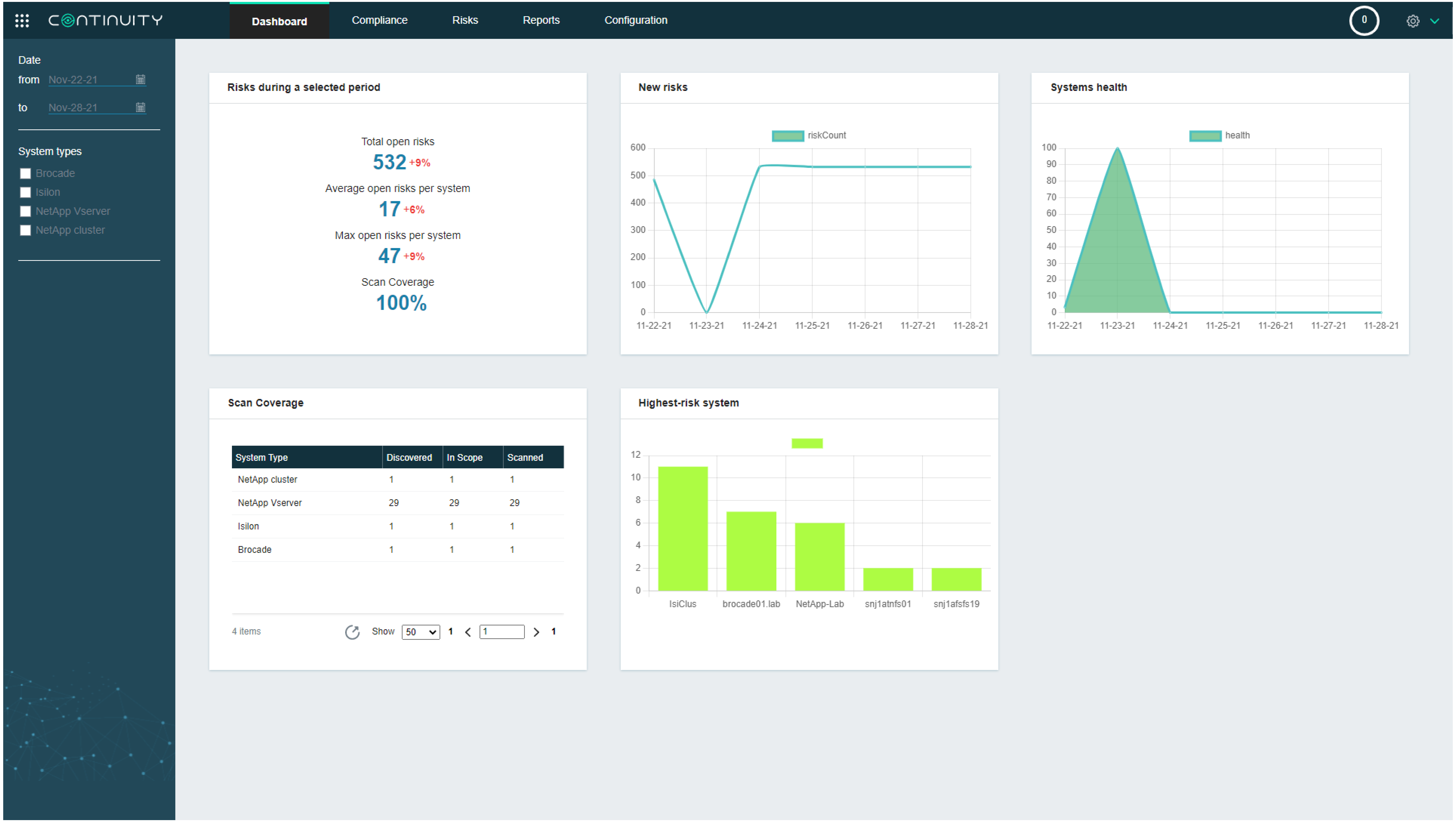
1 < 1 > 1



Task Type	Task Identifier	Schedule	Scan Scope	Disabled	Status
Security Risk Analysis	Security Analysis	Weekly at 10:00 PM, Days: Sun Mon Tue Wed Thu Fri Sat		No	●

1 items

**The system is currently running analysis.
Please try to login at a later time.**



Date
from Nov-22-21
to Nov-28-21

System types
□ Brocade
□ Isilon
□ NetApp Vserver
□ NetApp cluster

Risks during a selected period

Total open risks
532 +9%

Average open risks per system
17 +6%

Max open risks per system
47 +9%

Scan Coverage
100%

New risks

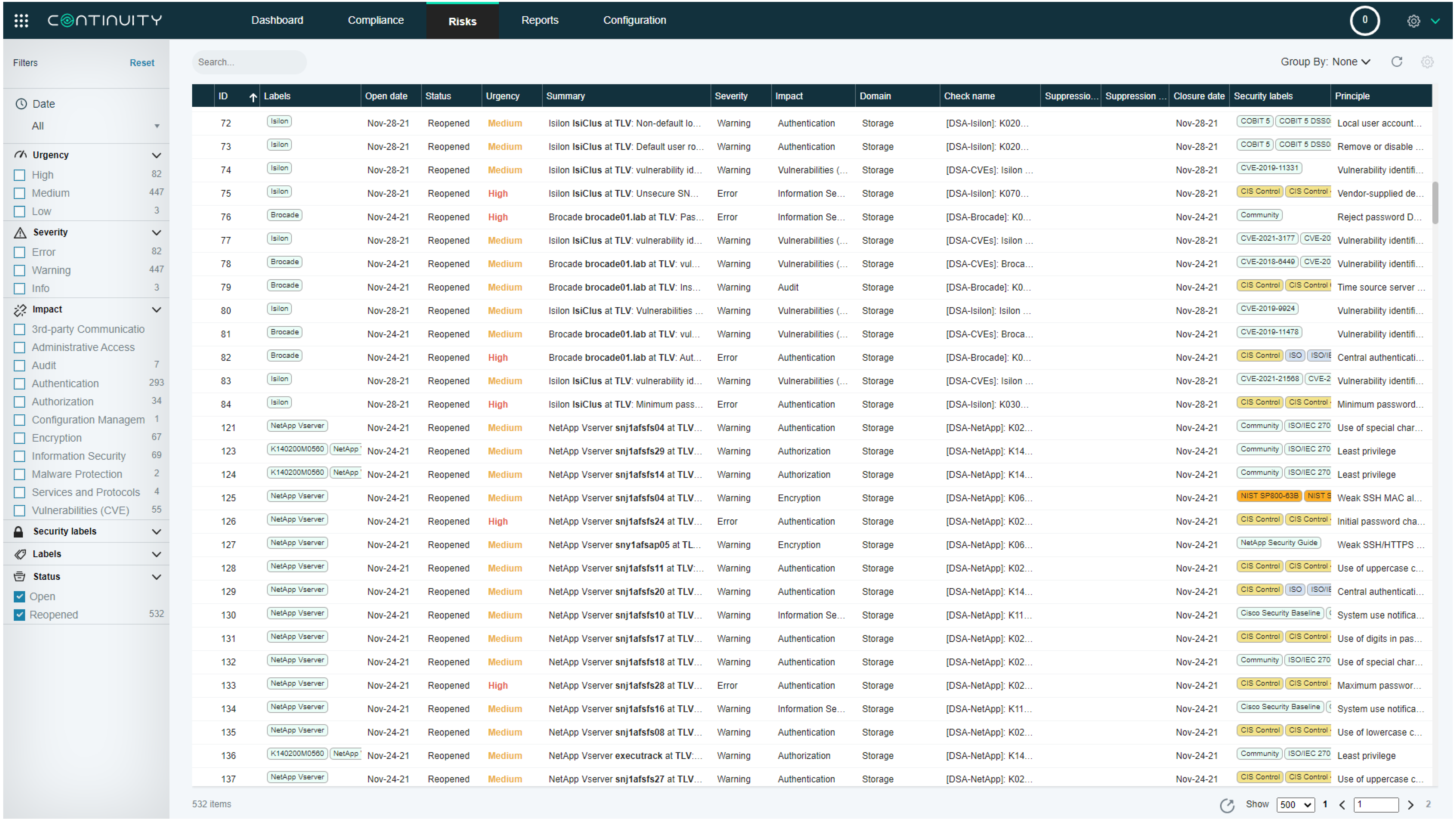
Systems health

Scan Coverage

System Type	Discovered	In Scope	Scanned
NetApp cluster	1	1	1
NetApp Vserver	29	29	29
Isilon	1	1	1
Brocade	1	1	1

4 items Show 50 1 < 1 > 1

Highest-risk system



Filters Reset

Date
All

Urgency
- □ High 82
- □ Medium 447
- □ Low 3

Severity
- □ Error 82
- □ Warning 447
- □ Info 3

Impact
- □ 3rd-party Communicatio
- □ Administrative Access
- □ Audit 7
- □ Authentication 293
- □ Authorization 34
- □ Configuration Managem 1
- □ Encryption 67
- □ Information Security 69
- □ Malware Protection 2
- □ Services and Protocols 4
- □ Vulnerabilities (CVE) 55

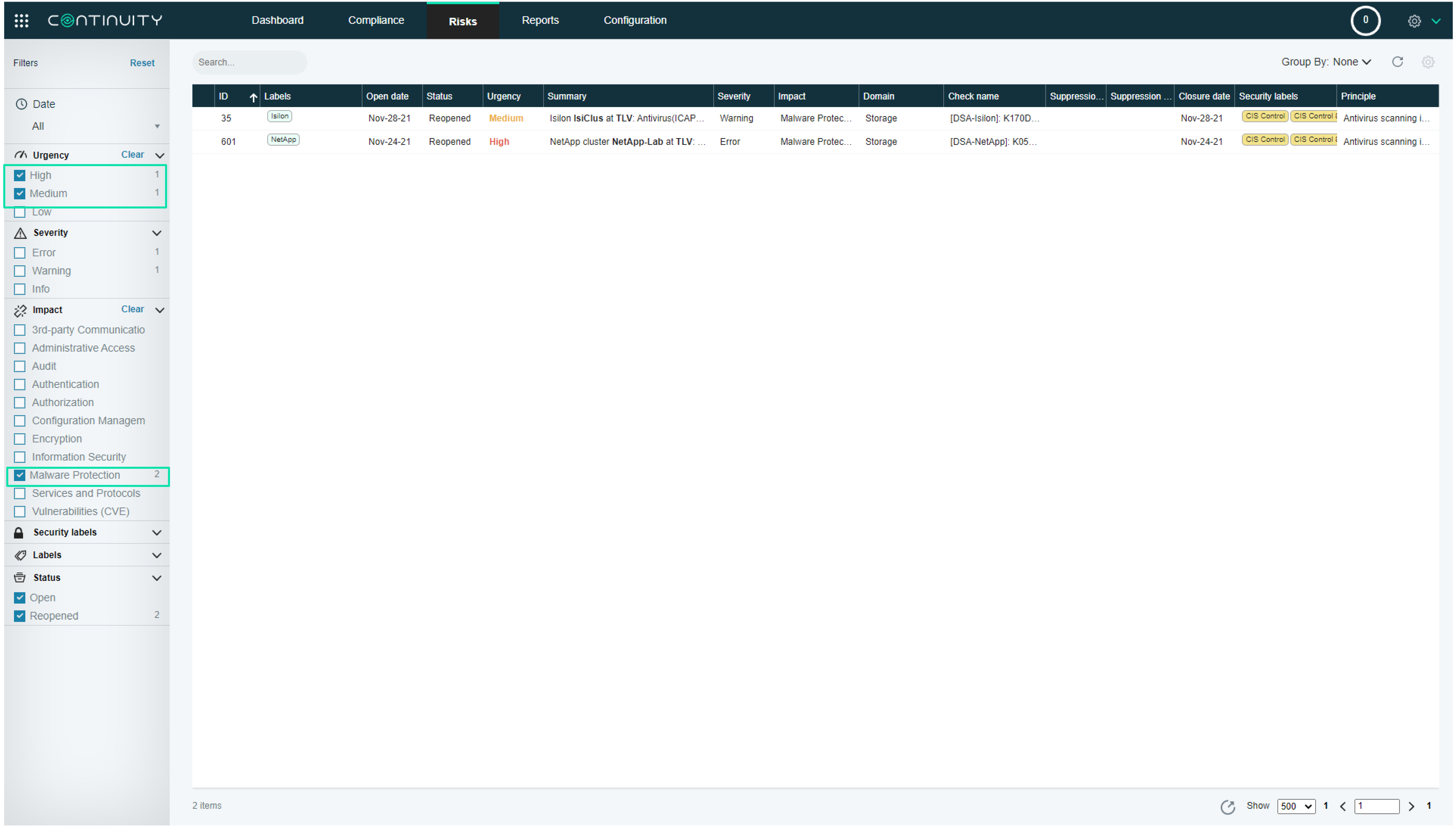
Security labels

Labels

Status
- ☑ Open
- ☑ Reopened 532

ID	Labels	Open date	Status	Urgency	Summary	Severity	Impact	Domain	Check name	Suppressio...	Suppression ...	Closure date	Security labels	Principle
72	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: Non-default lo...	Warning	Authentication	Storage	[DSA-Isilon]: K020...			Nov-28-21	COBIT 5 COBIT 5 DSS0	Local user account...
73	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: Default user ro...	Warning	Authentication	Storage	[DSA-Isilon]: K020...			Nov-28-21	COBIT 5 COBIT 5 DSS0	Remove or disable ...
74	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability id...	Warning	Vulnerabilities (...	Storage	[DSA-CVEs]: Isilon ...			Nov-28-21	CVE-2019-11331	Vulnerability identifi...
75	Isilon	Nov-28-21	Reopened	High	Isilon **IsiClus** at **TLV**: Unsecure SN...	Error	Information Se...	Storage	[DSA-Isilon]: K070...			Nov-28-21	CIS Control CIS Control	Vendor-supplied de...
76	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Pas...	Error	Information Se...	Storage	[DSA-Brocade]: K0...			Nov-24-21	Community	Reject password D...
77	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability id...	Warning	Vulnerabilities (...	Storage	[DSA-CVEs]: Isilon ...			Nov-28-21	CVE-2021-3177 CVE-20	Vulnerability identifi...
78	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vul...	Warning	Vulnerabilities (...	Storage	[DSA-CVEs]: Broca...			Nov-24-21	CVE-2018-6449 CVE-20	Vulnerability identifi...
79	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: Ins...	Warning	Audit	Storage	[DSA-Brocade]: K0...			Nov-24-21	CIS Control CIS Control	Time source server ...
80	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: Vulnerabilities ...	Warning	Vulnerabilities (...	Storage	[DSA-Isilon]: Isilon ...			Nov-28-21	CVE-2019-9924	Vulnerability identifi...
81	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vul...	Warning	Vulnerabilities (...	Storage	[DSA-CVEs]: Broca...			Nov-24-21	CVE-2019-11478	Vulnerability identifi...
82	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Aut...	Error	Authentication	Storage	[DSA-Brocade]: K0...			Nov-24-21	CIS Control ISO ISO/IE	Central authenticati...
83	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability id...	Warning	Vulnerabilities (...	Storage	[DSA-CVEs]: Isilon ...			Nov-28-21	CVE-2021-21568 CVE-2	Vulnerability identifi...
84	Isilon	Nov-28-21	Reopened	High	Isilon **IsiClus** at **TLV**: Minimum pass...	Error	Authentication	Storage	[DSA-Isilon]: K030...			Nov-28-21	CIS Control CIS Control	Minimum password...
121	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs04** at **TLV**...	Warning	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	Community ISO/IEC 270	Use of special char...
123	K140200M0560 NetApp	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs29** at **TLV**...	Warning	Authorization	Storage	[DSA-NetApp]: K14...			Nov-24-21	Community ISO/IEC 270	Least privilege
124	K140200M0560 NetApp	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs14** at **TLV**...	Warning	Authorization	Storage	[DSA-NetApp]: K14...			Nov-24-21	Community ISO/IEC 270	Least privilege
125	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs04** at **TLV**...	Warning	Encryption	Storage	[DSA-NetApp]: K06...			Nov-24-21	NIST SP800-63B NIST S	Weak SSH MAC al...
126	NetApp Vserver	Nov-24-21	Reopened	High	NetApp Vserver **snj1afsfs24** at **TLV**...	Error	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	CIS Control CIS Control	Initial password cha...
127	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **sny1afsap05** at **TL**...	Warning	Encryption	Storage	[DSA-NetApp]: K06...			Nov-24-21	NetApp Security Guide	Weak SSH/HTTPS ...
128	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs11** at **TLV**:...	Warning	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	CIS Control CIS Control	Use of uppercase c...
129	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs20** at **TLV**...	Warning	Authentication	Storage	[DSA-NetApp]: K14...			Nov-24-21	CIS Control ISO ISO/IE	Central authenticati...
130	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs10** at **TLV**...	Warning	Information Se...	Storage	[DSA-NetApp]: K11...			Nov-24-21	Cisco Security Baseline	System use notifica...
131	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs17** at **TLV**...	Warning	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	CIS Control CIS Control	Use of digits in pas...
132	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs18** at **TLV**...	Warning	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	Community ISO/IEC 270	Use of special char...
133	NetApp Vserver	Nov-24-21	Reopened	High	NetApp Vserver **snj1afsfs28** at **TLV**...	Error	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	CIS Control CIS Control	Maximum passwor...
134	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs16** at **TLV**...	Warning	Information Se...	Storage	[DSA-NetApp]: K11...			Nov-24-21	Cisco Security Baseline	System use notifica...
135	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs08** at **TLV**...	Warning	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	CIS Control CIS Control	Use of lowercase c...
136	K140200M0560 NetApp	Nov-24-21	Reopened	Medium	NetApp Vserver **executrack** at **TLV**:...	Warning	Authorization	Storage	[DSA-NetApp]: K14...			Nov-24-21	Community ISO/IEC 270	Least privilege
137	NetApp Vserver	Nov-24-21	Reopened	Medium	NetApp Vserver **snj1afsfs27** at **TLV**...	Warning	Authentication	Storage	[DSA-NetApp]: K02...			Nov-24-21	CIS Control CIS Control	Use of uppercase c...

532 items



Filters Reset

Date: All

Urgency Clear
- ☑ High 1
- ☑ Medium 1
- □ Low

Severity
- □ Error 1
- □ Warning 1
- □ Info

Impact Clear
- □ 3rd-party Communicatio
- □ Administrative Access
- □ Audit
- □ Authentication
- □ Authorization
- □ Configuration Managem
- □ Encryption
- □ Information Security
- ☑ Malware Protection 2
- □ Services and Protocols
- □ Vulnerabilities (CVE)

Security labels

Labels

Status
- ☑ Open
- ☑ Reopened 2

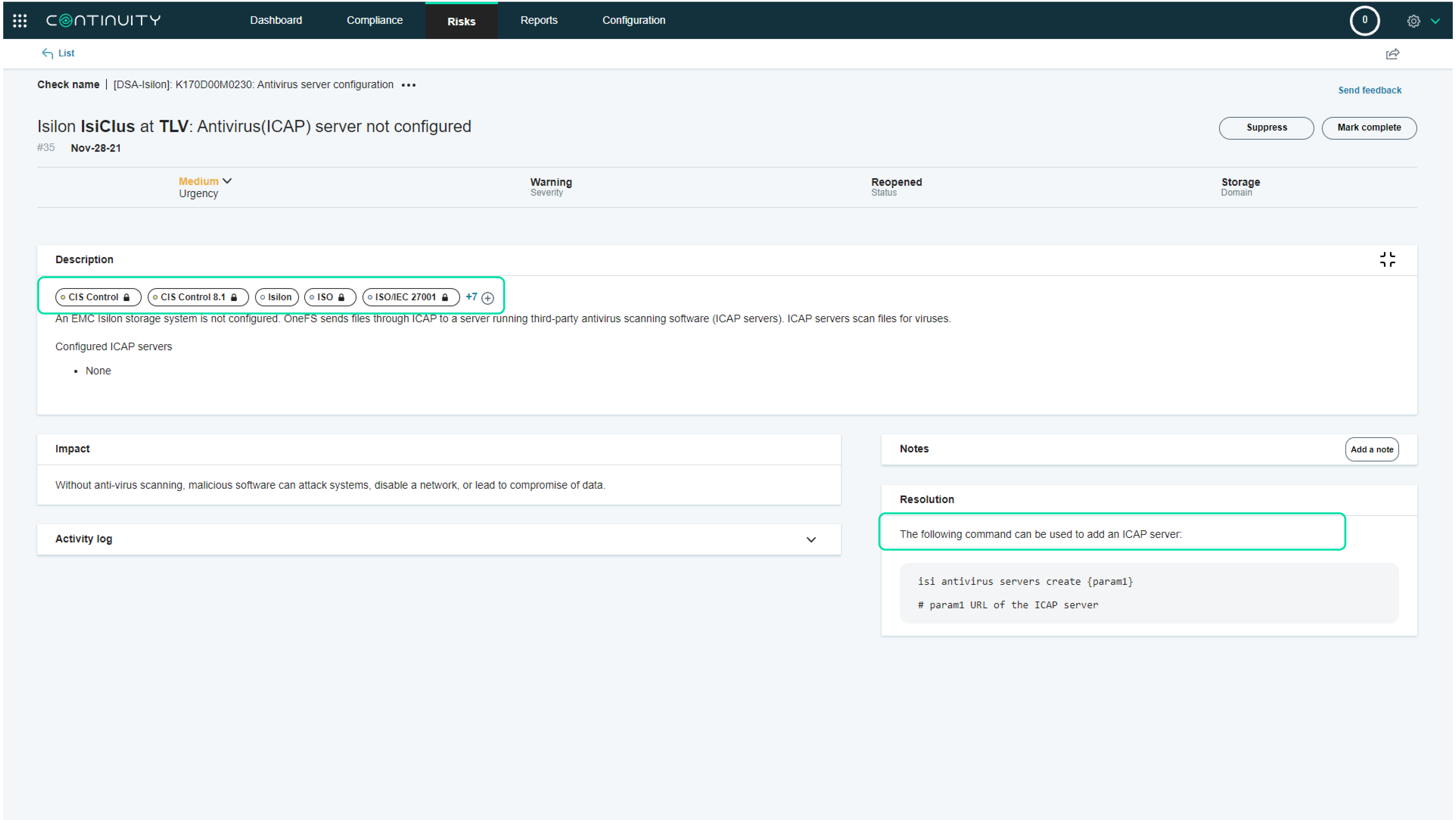
Search...

Group By: None

ID	Labels	Open date	Status	Urgency	Summary	Severity	Impact	Domain	Check name	Suppressio...	Suppression ...	Closure date	Security labels	Principle
35	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: Antivirus(ICAP...	Warning	Malware Protec...	Storage	[DSA-Isilon]: K170D...			Nov-28-21	CIS Control CIS Control 8	Antivirus scanning i...
601	NetApp	Nov-24-21	Reopened	High	NetApp cluster **NetApp-Lab** at **TLV**: ...	Error	Malware Protec...	Storage	[DSA-NetApp]: K05...			Nov-24-21	CIS Control CIS Control 8	Antivirus scanning i...

2 items

Show 500 1 < 1 > 1



Check name | [DSA-Isilon]: K170D00M0230: Antivirus server configuration •••

Isilon **IsiClus** at **TLV**: Antivirus(ICAP) server not configured

#35 **Nov-28-21**

Medium Urgency	Warning Severity	Reopened Status	Storage Domain

Description

CIS Control 🔒 | CIS Control 8.1 🔒 | Isilon | ISO 🔒 | ISO/IEC 27001 🔒 | +7 ⊕

An EMC Isilon storage system is not configured. OneFS sends files through ICAP to a server running third-party antivirus scanning software (ICAP servers). ICAP servers scan files for viruses.

Configured ICAP servers

- None

Impact

Without anti-virus scanning, malicious software can attack systems, disable a network, or lead to compromise of data.

Activity log

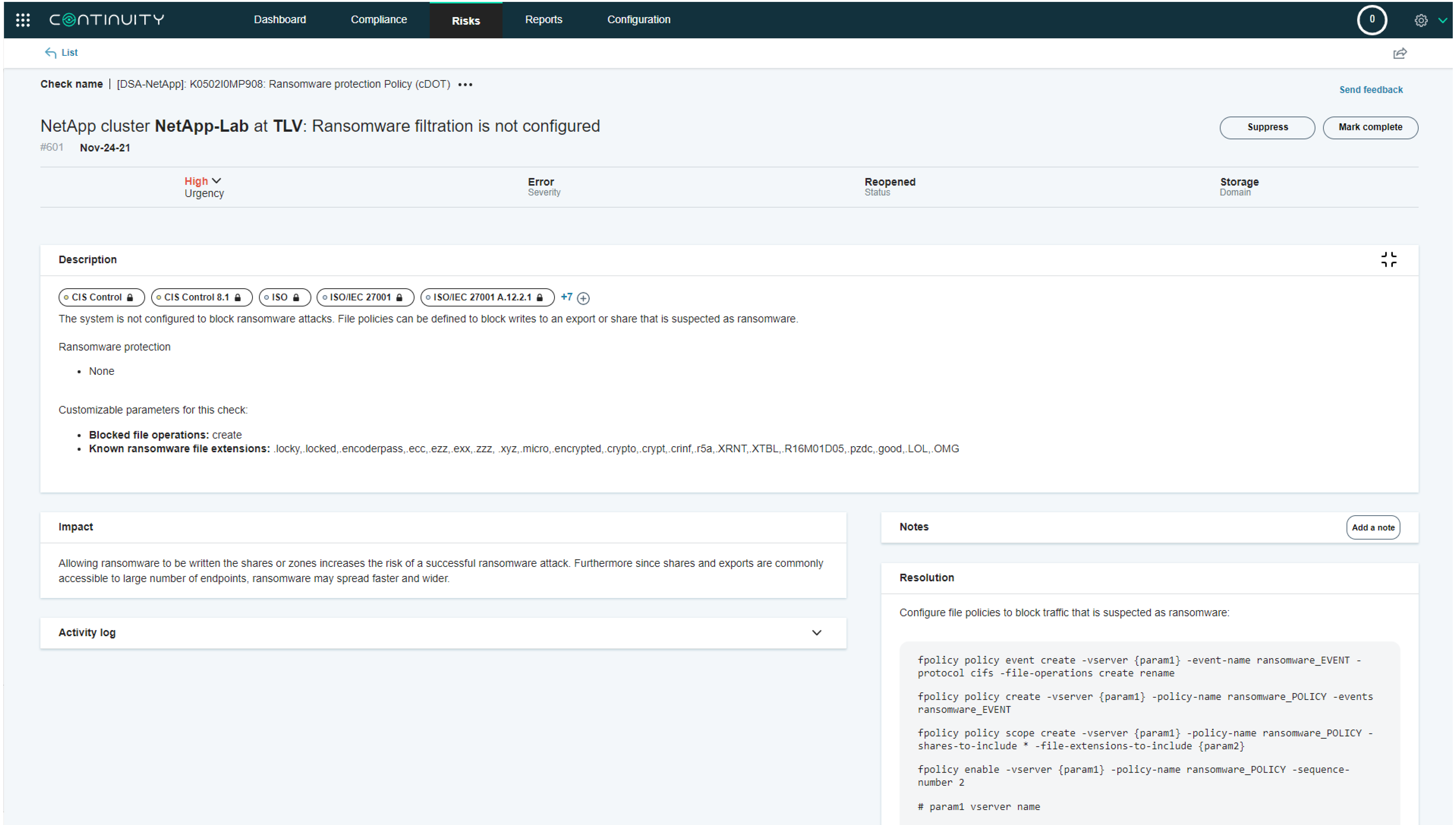
Notes

Resolution

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

```
isi antivirus servers create {param1}

# param1 URL of the ICAP server
```



Check name | [DSA-NetApp]: K0502I0MP908: Ransomware protection Policy (cDOT) •••

NetApp cluster **NetApp-Lab** at **TLV**: Ransomware filtration is not configured

#601 **Nov-24-21**

High Urgency	**Error** Severity	**Reopened** Status	**Storage** Domain

Description

CIS Control | CIS Control 8.1 | ISO | ISO/IEC 27001 | ISO/IEC 27001 A.12.2.1 | +7

The system is not configured to block ransomware attacks. File policies can be defined to block writes to an export or share that is suspected as ransomware.

Ransomware protection

- None

Customizable parameters for this check:

- **Blocked file operations:** create
- **Known ransomware file extensions:** .locky,.locked,.encoderpass,.ecc,.ezz,.exx,.zzz, .xyz,.micro,.encrypted,.crypto,.crypt,.crinf,.r5a,.XRNT,.XTBL,.R16M01D05,.pzdc,.good,.LOL,.OMG

Impact

Allowing ransomware to be written the shares or zones increases the risk of a successful ransomware attack. Furthermore since shares and exports are commonly accessible to large number of endpoints, ransomware may spread faster and wider.

Activity log

Notes

Resolution

Configure file policies to block traffic that is suspected as ransomware:

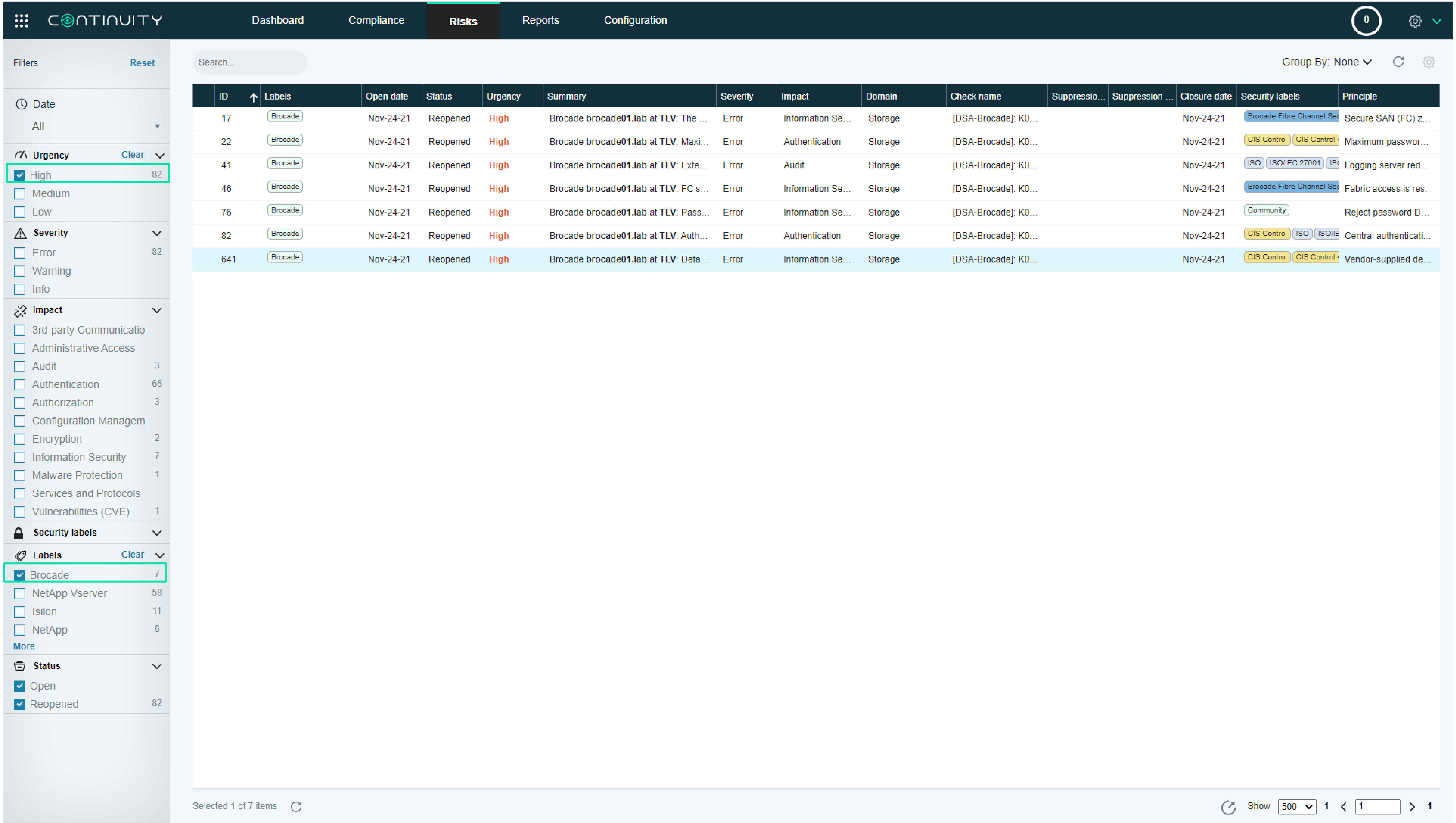
```
fpolicy policy event create -vserver {param1} -event-name ransomware_EVENT -
protocol cifs -file-operations create rename

fpolicy policy create -vserver {param1} -policy-name ransomware_POLICY -events
ransomware_EVENT

fpolicy policy scope create -vserver {param1} -policy-name ransomware_POLICY -
shares-to-include * -file-extensions-to-include {param2}

fpolicy enable -vserver {param1} -policy-name ransomware_POLICY -sequence-
number 2

# param1 vserver name
```



Filters Reset

Date
All

Urgency Clear
- ☑ High 82
- □ Medium
- □ Low

Severity
- □ Error 82
- □ Warning
- □ Info

Impact
- □ 3rd-party Communicatio
- □ Administrative Access
- □ Audit 3
- □ Authentication 65
- □ Authorization 3
- □ Configuration Managem
- □ Encryption 2
- □ Information Security 7
- □ Malware Protection 1
- □ Services and Protocols
- □ Vulnerabilities (CVE) 1

Security labels

Labels Clear
- ☑ Brocade 7
- □ NetApp Vserver 58
- □ Isilon 11
- □ NetApp 6

More

Status
- ☑ Open
- ☑ Reopened 82

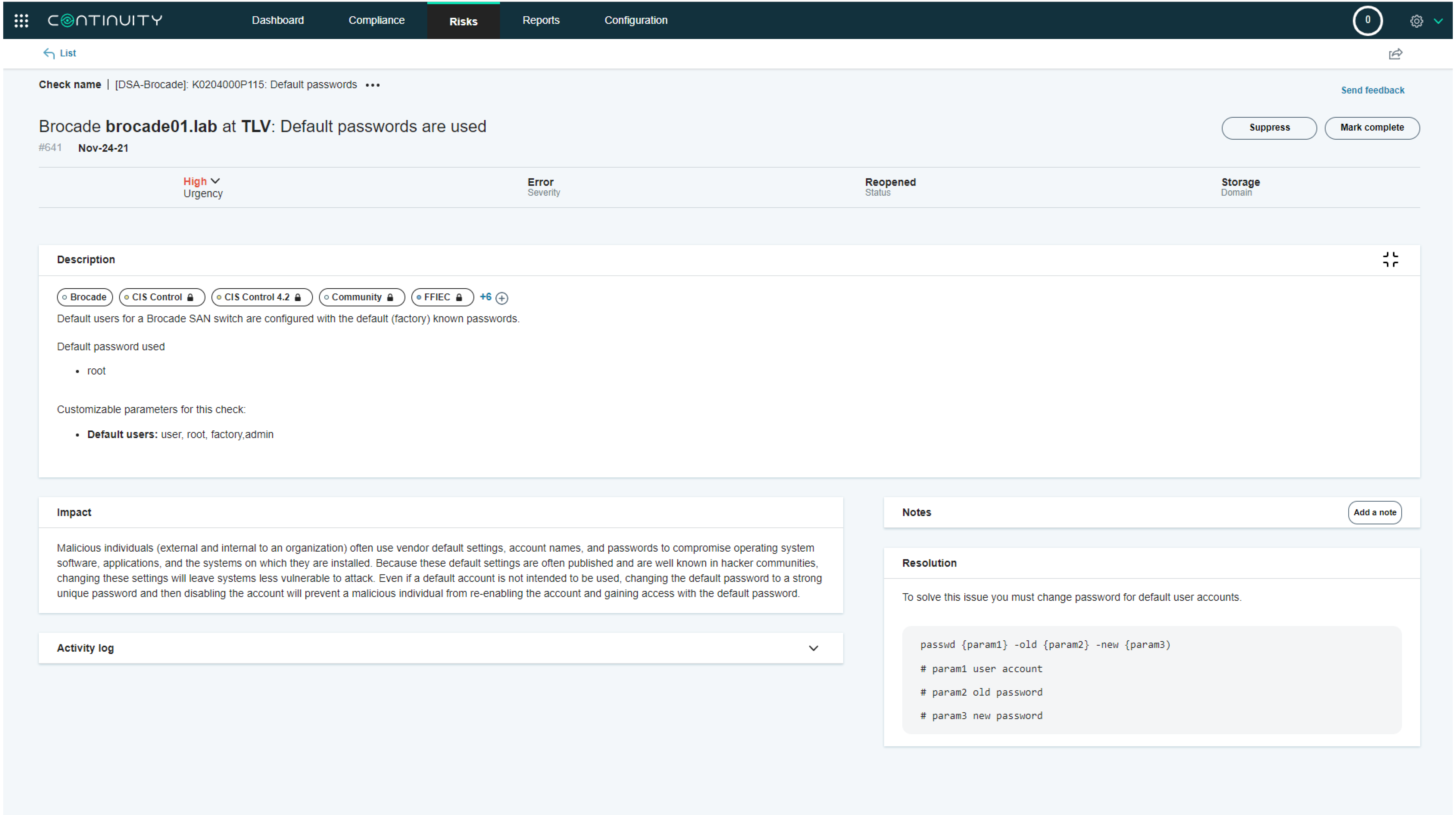
Search...

Group By: None

ID	Labels	Open date	Status	Urgency	Summary	Severity	Impact	Domain	Check name	Suppressio...	Suppression ...	Closure date	Security labels	Principle
17	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: The ...	Error	Information Se...	Storage	[DSA-Brocade]: K0...			Nov-24-21	Brocade Fibre Channel Sec	Secure SAN (FC) z...
22	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Maxi...	Error	Authentication	Storage	[DSA-Brocade]: K0...			Nov-24-21	CIS Control CIS Control	Maximum passwor...
41	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Exte...	Error	Audit	Storage	[DSA-Brocade]: K0...			Nov-24-21	ISO ISO/IEC 27001 IS	Logging server red...
46	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: FC s...	Error	Information Se...	Storage	[DSA-Brocade]: K0...			Nov-24-21	Brocade Fibre Channel Sec	Fabric access is res...
76	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Pass...	Error	Information Se...	Storage	[DSA-Brocade]: K0...			Nov-24-21	Community	Reject password D...
82	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Auth...	Error	Authentication	Storage	[DSA-Brocade]: K0...			Nov-24-21	CIS Control ISO ISO/IE	Central authenticati...
641	Brocade	Nov-24-21	Reopened	High	Brocade **brocade01.lab** at **TLV**: Defa...	Error	Information Se...	Storage	[DSA-Brocade]: K0...			Nov-24-21	CIS Control CIS Control	Vendor-supplied de...

Selected 1 of 7 items

Show 500 1 1 1



Check name | [DSA-Brocade]: K0204000P115: Default passwords •••

Brocade **brocade01.lab** at **TLV**: Default passwords are used

#641 **Nov-24-21**

High Urgency	**Error** Severity	**Reopened** Status	**Storage** Domain

Description

○ Brocade ○ CIS Control ○ CIS Control 4.2 ○ Community ○ FFIEC +6

Default users for a Brocade SAN switch are configured with the default (factory) known passwords.

Default password used

- root

Customizable parameters for this check:

- **Default users:** user, root, factory,admin

Impact

Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

Activity log

Notes

Resolution

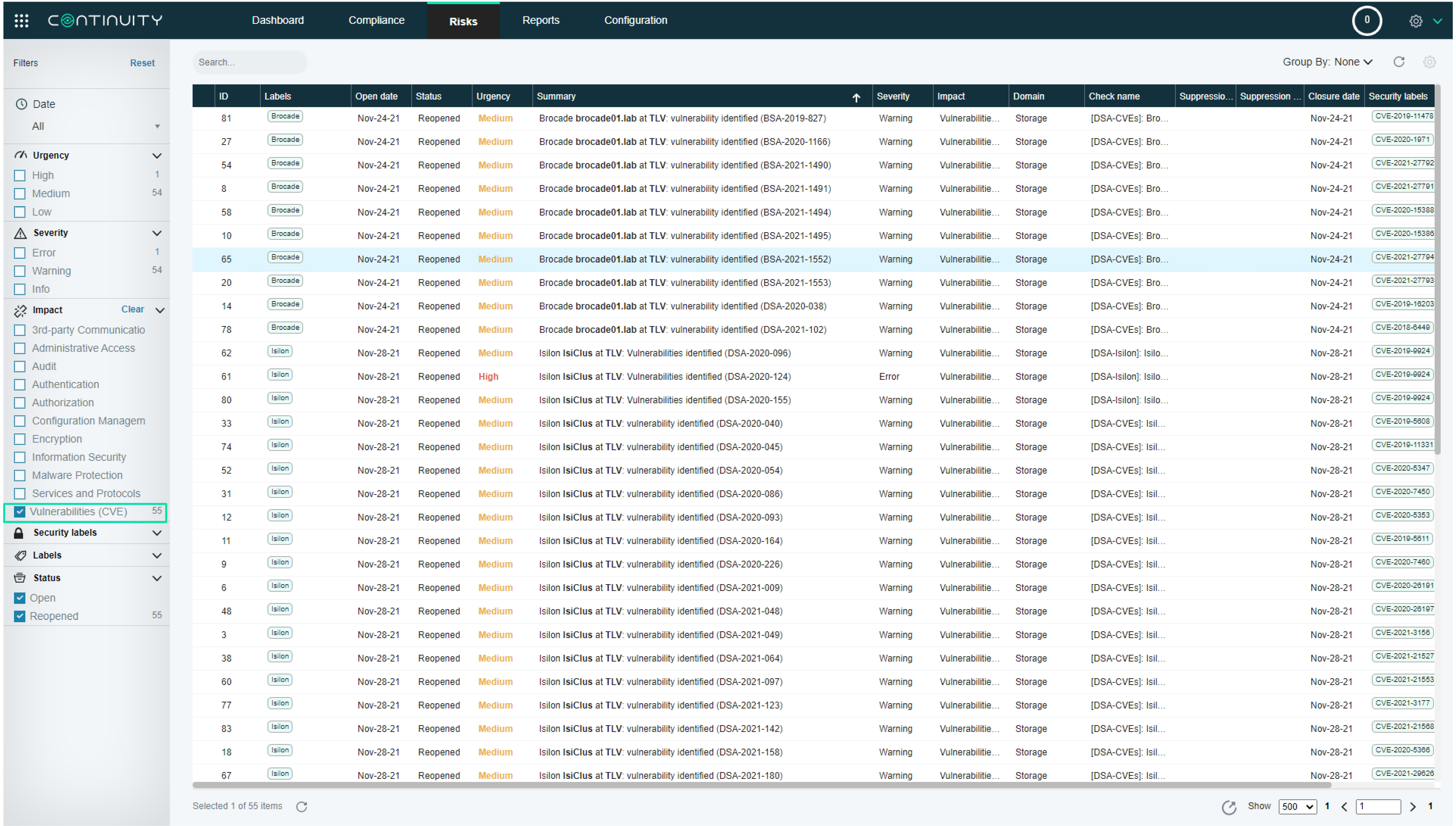
To solve this issue you must change password for default user accounts.

```
passwd {param1} -old {param2} -new {param3}

# param1 user account

# param2 old password

# param3 new password
```



Filters Reset

Date
All

Urgency
- □ High 1
- □ Medium 54
- □ Low

Severity
- □ Error 1
- □ Warning 54
- □ Info

Impact Clear
- □ 3rd-party Communicatio
- □ Administrative Access
- □ Audit
- □ Authentication
- □ Authorization
- □ Configuration Managem
- □ Encryption
- □ Information Security
- □ Malware Protection
- □ Services and Protocols
- ☑ Vulnerabilities (CVE) 55

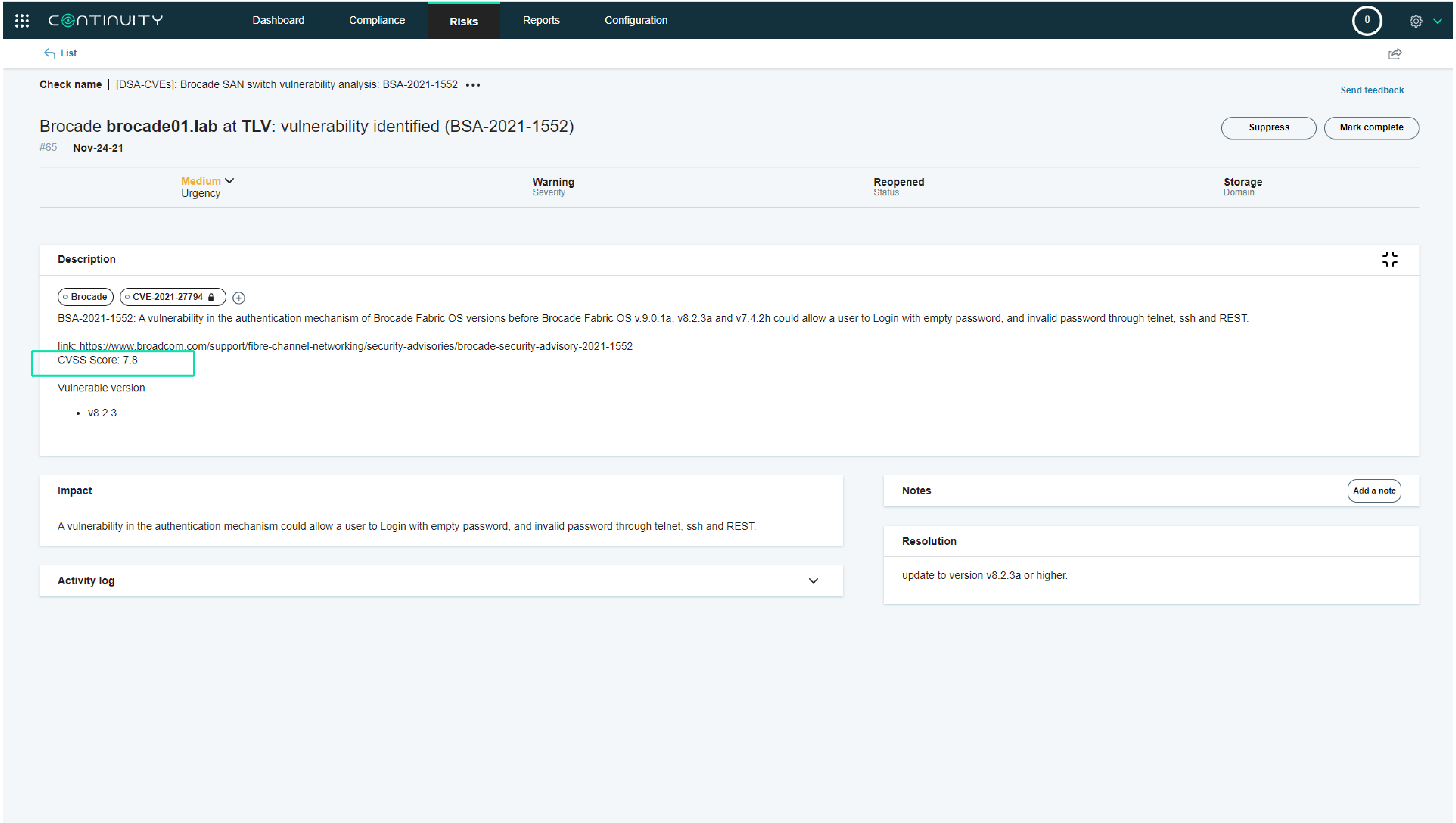
Security labels

Labels

Status
- ☑ Open
- ☑ Reopened 55

ID	Labels	Open date	Status	Urgency	Summary	Severity	Impact	Domain	Check name	Suppressio...	Suppression ...	Closure date	Security labels
81	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2019-827)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2019-11478
27	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2020-1166)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2020-1971
54	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1490)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2021-27792
8	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1491)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2021-27791
58	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1494)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2020-15388
10	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1495)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2020-15386
65	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1552)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2021-27794
20	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1553)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2021-27793
14	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (DSA-2020-038)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2019-16203
78	Brocade	Nov-24-21	Reopened	Medium	Brocade **brocade01.lab** at **TLV**: vulnerability identified (DSA-2021-102)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Bro...			Nov-24-21	CVE-2018-6449
62	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: Vulnerabilities identified (DSA-2020-096)	Warning	Vulnerabilitie...	Storage	[DSA-Isilon]: Isilo...			Nov-28-21	CVE-2019-9924
61	Isilon	Nov-28-21	Reopened	High	Isilon **IsiClus** at **TLV**: Vulnerabilities identified (DSA-2020-124)	Error	Vulnerabilitie...	Storage	[DSA-Isilon]: Isilo...			Nov-28-21	CVE-2019-9924
80	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: Vulnerabilities identified (DSA-2020-155)	Warning	Vulnerabilitie...	Storage	[DSA-Isilon]: Isilo...			Nov-28-21	CVE-2019-9924
33	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-040)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2019-5608
74	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-045)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2019-11331
52	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-054)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-5347
31	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-086)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-7450
12	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-093)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-5353
11	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-164)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2019-5611
9	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2020-226)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-7460
6	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-009)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-26191
48	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-048)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-26197
3	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-049)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2021-3156
38	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-064)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2021-21527
60	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-097)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2021-21553
77	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-123)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2021-3177
83	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-142)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2021-21568
18	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-158)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2020-5366
67	Isilon	Nov-28-21	Reopened	Medium	Isilon **IsiClus** at **TLV**: vulnerability identified (DSA-2021-180)	Warning	Vulnerabilitie...	Storage	[DSA-CVEs]: Isil...			Nov-28-21	CVE-2021-29626

Selected 1 of 55 items



Check name | [DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2021-1552 •••

Brocade **brocade01.lab** at **TLV**: vulnerability identified (BSA-2021-1552)

#65 **Nov-24-21**

Medium Urgency	**Warning** Severity	**Reopened** Status	**Storage** Domain

Description

○ Brocade ○ CVE-2021-27794

BSA-2021-1552: A vulnerability in the authentication mechanism of Brocade Fabric OS versions before Brocade Fabric OS v.9.0.1a, v8.2.3a and v7.4.2h could allow a user to Login with empty password, and invalid password through telnet, ssh and REST.

link: https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2021-1552
CVSS Score: 7.8

Vulnerable version

- v8.2.3

Impact

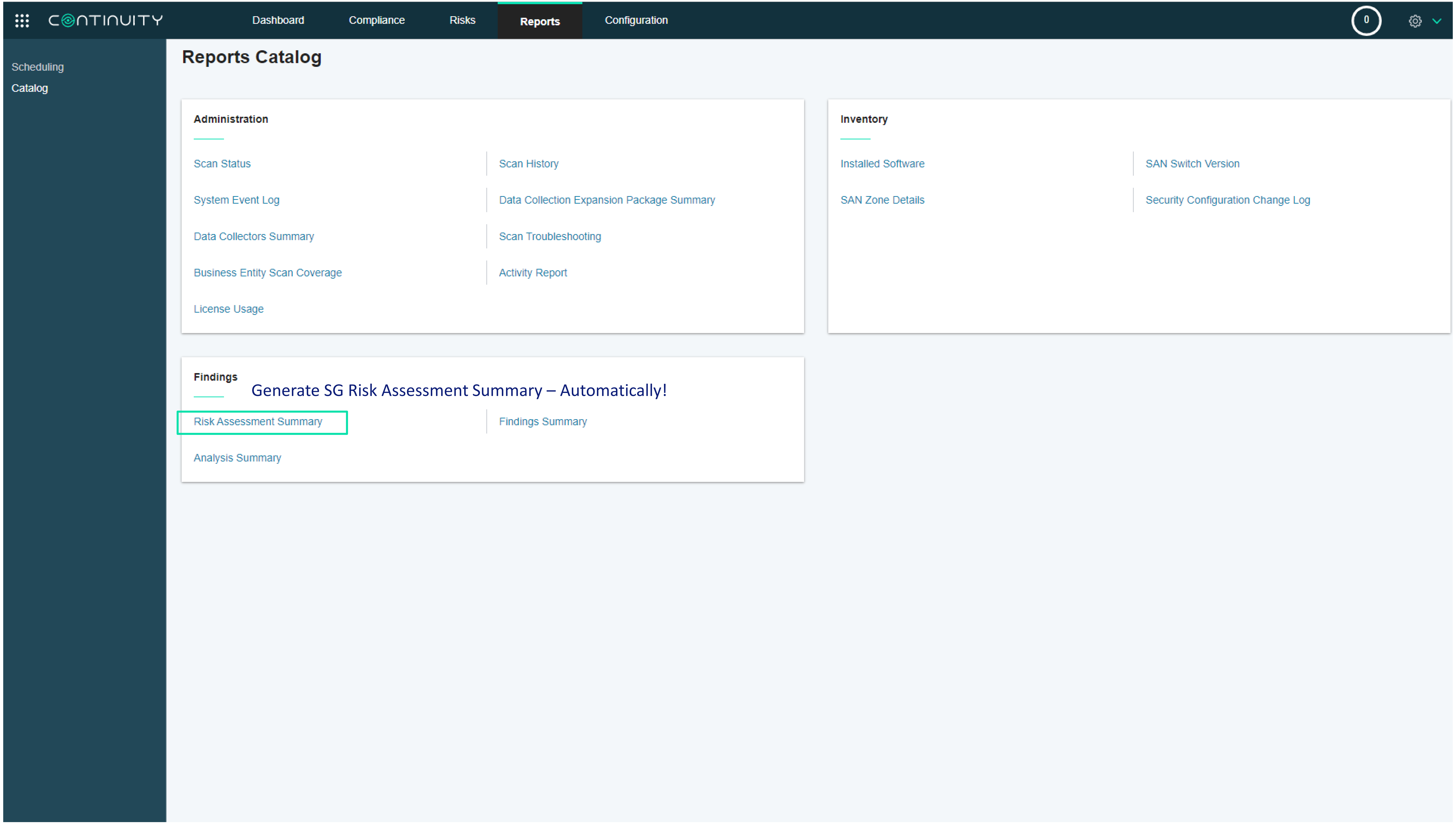
A vulnerability in the authentication mechanism could allow a user to Login with empty password, and invalid password through telnet, ssh and REST.

Activity log

Notes

Resolution

update to version v8.2.3a or higher.



Reports Catalog

Administration

Scan Status	Scan History
System Event Log	Data Collection Expansion Package Summary
Data Collectors Summary	Scan Troubleshooting
Business Entity Scan Coverage	Activity Report
License Usage	

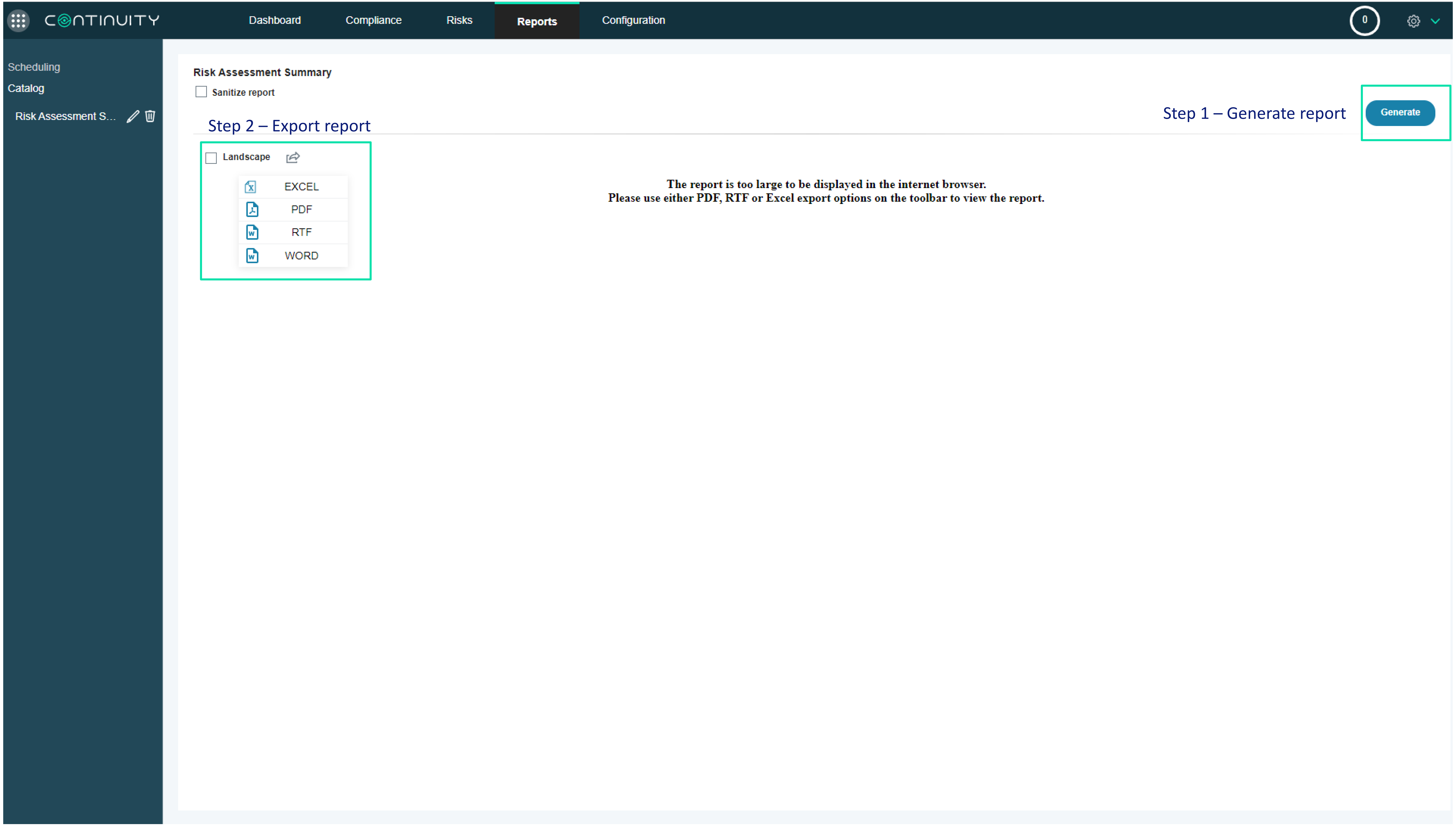
Inventory

Installed Software	SAN Switch Version
SAN Zone Details	Security Configuration Change Log

Findings

Generate SG Risk Assessment Summary – Automatically!

Risk Assessment Summary	Findings Summary
Analysis Summary	



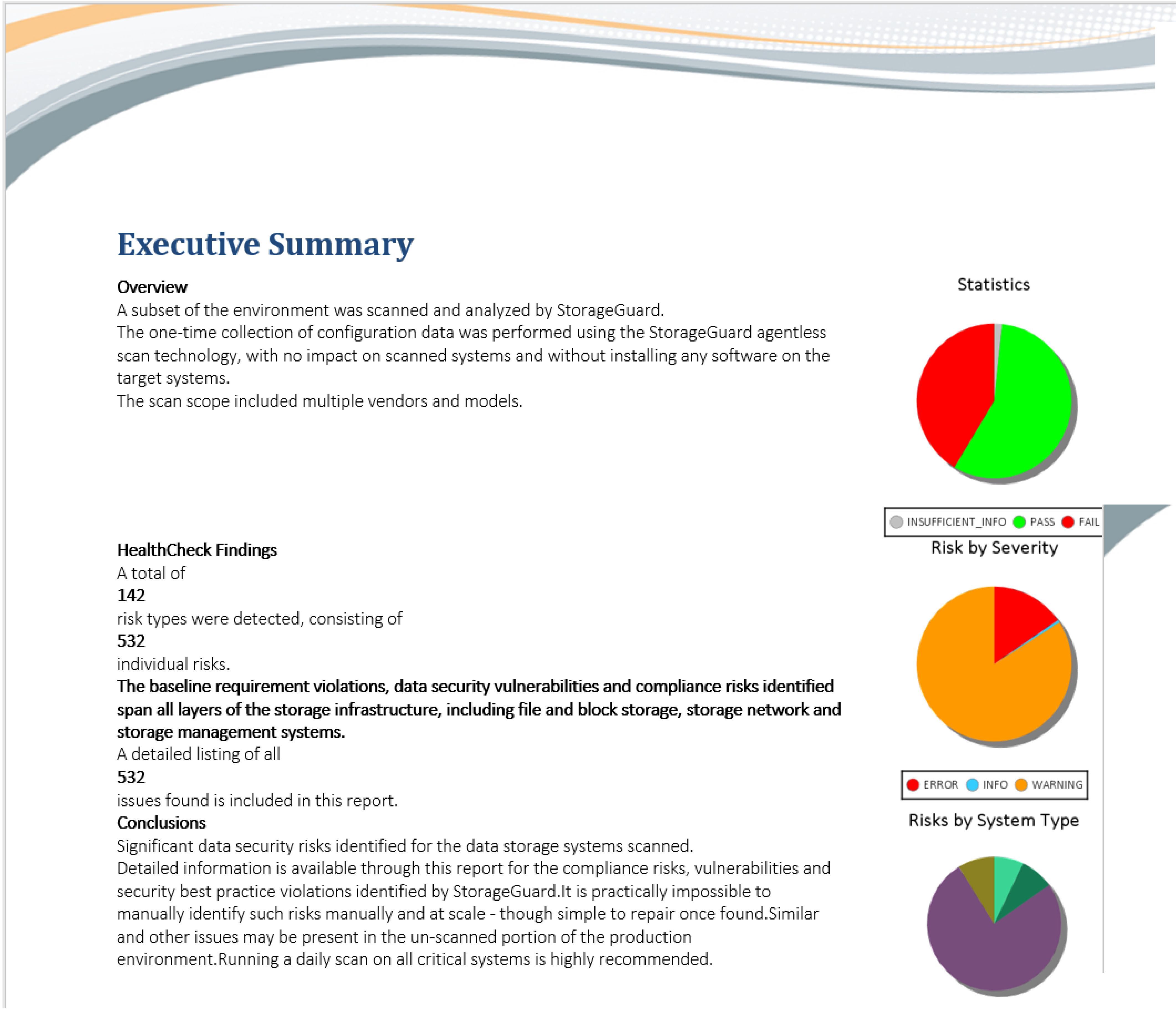
Risk Assessment Summary

□ Sanitize report

Step 1 – Generate report

Step 2 – Export report

The report is too large to be displayed in the internet browser.
Please use either PDF, RTF or Excel export options on the toolbar to view the report.



Executive Summary

Overview

A subset of the environment was scanned and analyzed by StorageGuard.

The one-time collection of configuration data was performed using the StorageGuard agentless scan technology, with no impact on scanned systems and without installing any software on the target systems.

The scan scope included multiple vendors and models.

HealthCheck Findings

A total of

142

risk types were detected, consisting of

532

individual risks.

The baseline requirement violations, data security vulnerabilities and compliance risks identified span all layers of the storage infrastructure, including file and block storage, storage network and storage management systems.

A detailed listing of all

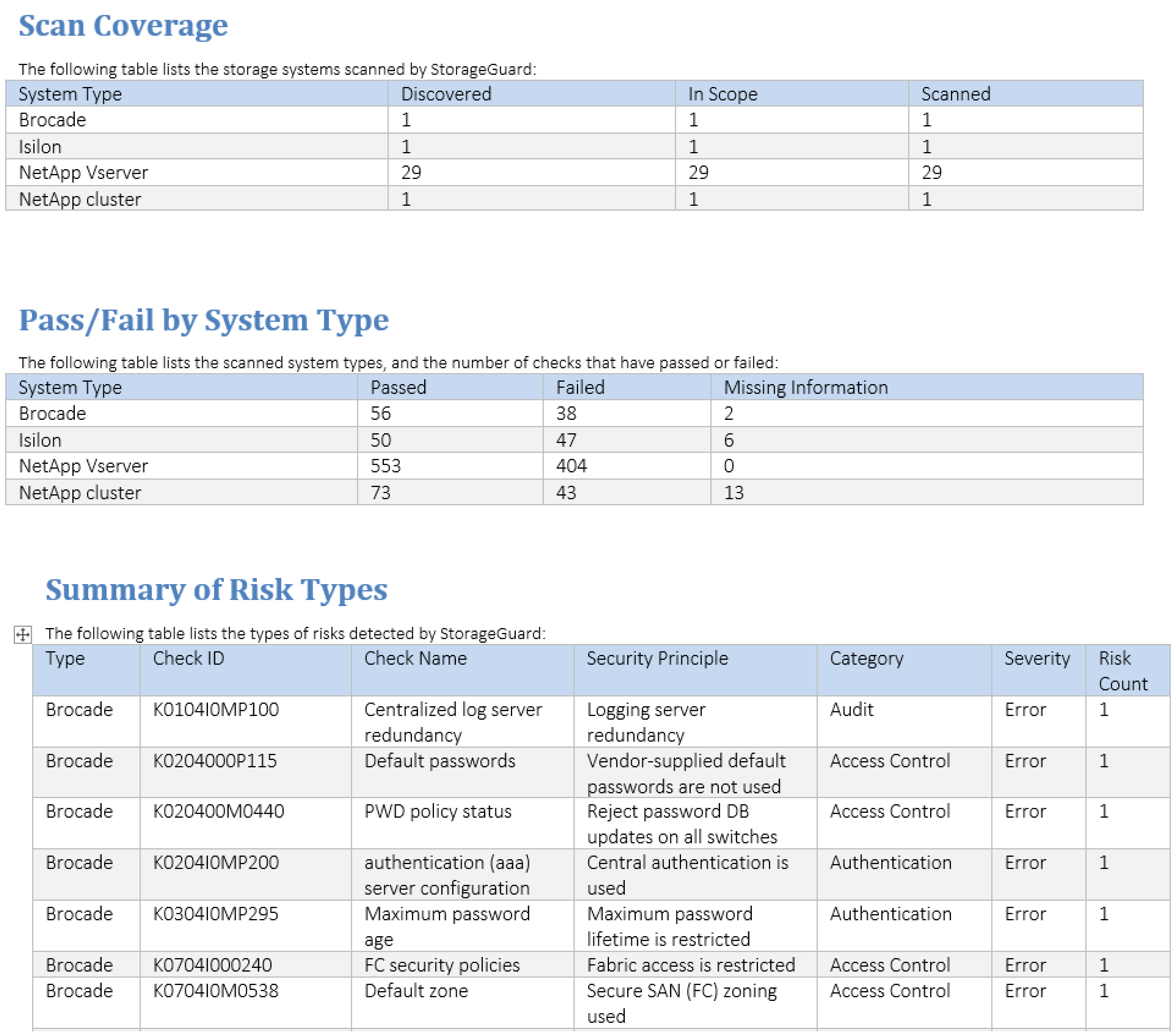
532

issues found is included in this report.

Conclusions

Significant data security risks identified for the data storage systems scanned.

Detailed information is available through this report for the compliance risks, vulnerabilities and security best practice violations identified by StorageGuard.It is practically impossible to manually identify such risks manually and at scale - though simple to repair once found.Similar and other issues may be present in the un-scanned portion of the production environment.Running a daily scan on all critical systems is highly recommended.



Scan Coverage

The following table lists the storage systems scanned by StorageGuard:

System Type	Discovered	In Scope	Scanned
Brocade	1	1	1
Isilon	1	1	1
NetApp Vserver	29	29	29
NetApp cluster	1	1	1

Pass/Fail by System Type

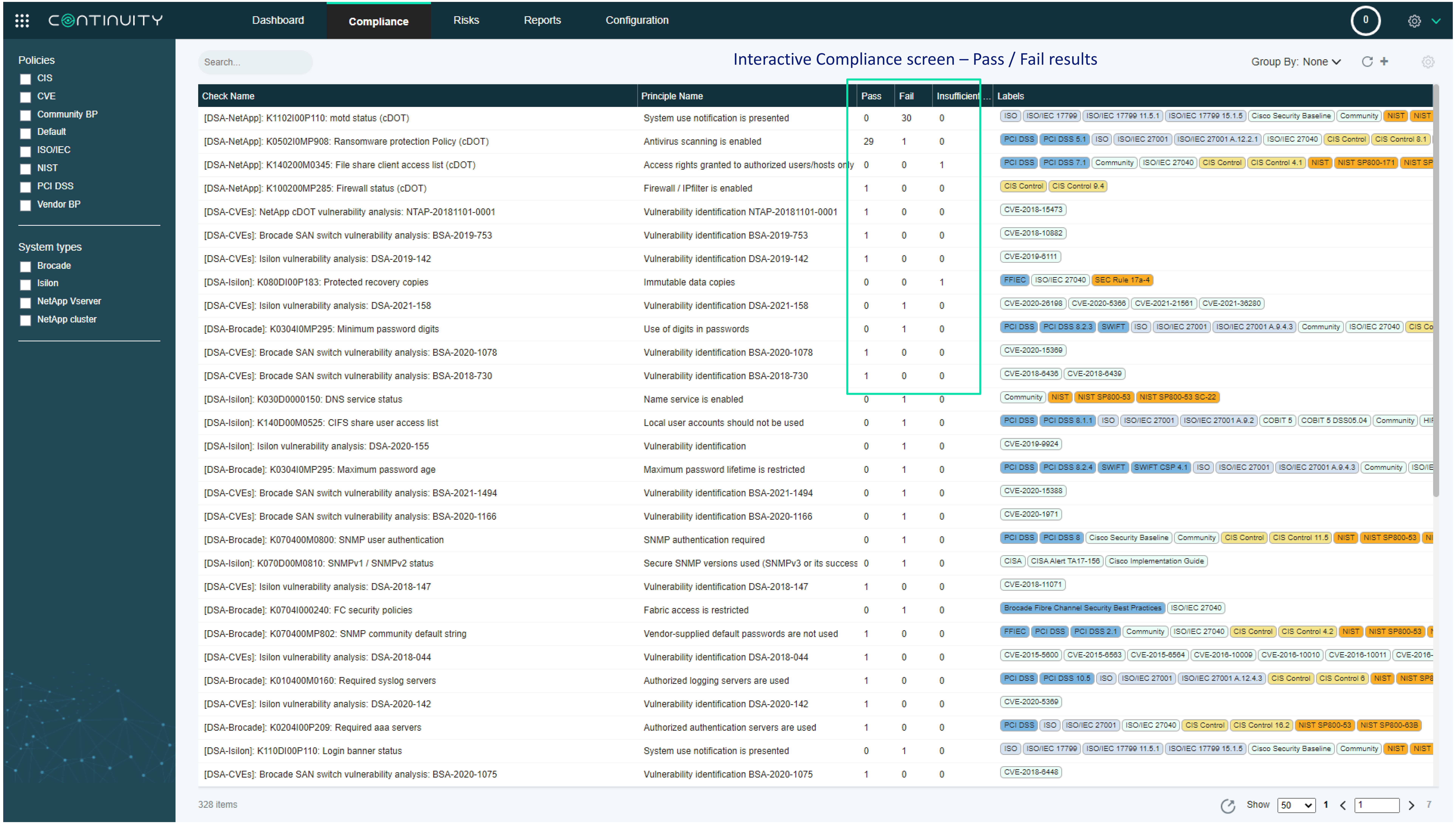
The following table lists the scanned system types, and the number of checks that have passed or failed:

System Type	Passed	Failed	Missing Information
Brocade	56	38	2
Isilon	50	47	6
NetApp Vserver	553	404	0
NetApp cluster	73	43	13

Summary of Risk Types

The following table lists the types of risks detected by StorageGuard:

Type	Check ID	Check Name	Security Principle	Category	Severity	Risk Count
Brocade	K0104I0MP100	Centralized log server redundancy	Logging server redundancy	Audit	Error	1
Brocade	K0204000P115	Default passwords	Vendor-supplied default passwords are not used	Access Control	Error	1
Brocade	K020400M0440	PWD policy status	Reject password DB updates on all switches	Access Control	Error	1
Brocade	K0204I0MP200	authentication (aaa) server configuration	Central authentication is used	Authentication	Error	1
Brocade	K0304I0MP295	Maximum password age	Maximum password lifetime is restricted	Authentication	Error	1
Brocade	K0704I000240	FC security policies	Fabric access is restricted	Access Control	Error	1
Brocade	K0704I0M0538	Default zone	Secure SAN (FC) zoning used	Access Control	Error	1



Policies

- □ CIS
- □ CVE
- □ Community BP
- □ Default
- □ ISO/IEC
- □ NIST
- □ PCI DSS
- □ Vendor BP

System types

- □ Brocade
- □ Isilon
- □ NetApp Vserver
- □ NetApp cluster

Search...

Interactive Compliance screen – Pass / Fail results

Group By: None

Check Name	Principle Name	Pass	Fail	Insufficient ...	Labels
[DSA-NetApp]: K1102I00P110: motd status (cDOT)	System use notification is presented	0	30	0	ISO, ISO/IEC 17799, ISO/IEC 17799 11.5.1, ISO/IEC 17799 15.1.5, Cisco Security Baseline, Community, NIST, NIST
[DSA-NetApp]: K0502I0MP908: Ransomware protection Policy (cDOT)	Antivirus scanning is enabled	29	1	0	PCI DSS, PCI DSS 5.1, ISO, ISO/IEC 27001, ISO/IEC 27001 A.12.2.1, ISO/IEC 27040, CIS Control, CIS Control 8.1
[DSA-NetApp]: K140200M0345: File share client access list (cDOT)	Access rights granted to authorized users/hosts only	0	0	1	PCI DSS, PCI DSS 7.1, Community, ISO/IEC 27040, CIS Control, CIS Control 4.1, NIST, NIST SP800-171, NIST SP
[DSA-NetApp]: K100200MP285: Firewall status (cDOT)	Firewall / IPfilter is enabled	1	0	0	CIS Control, CIS Control 9.4
[DSA-CVEs]: NetApp cDOT vulnerability analysis: NTAP-20181101-0001	Vulnerability identification NTAP-20181101-0001	1	0	0	CVE-2018-15473
[DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2019-753	Vulnerability identification BSA-2019-753	1	0	0	CVE-2018-10882
[DSA-CVEs]: Isilon vulnerability analysis: DSA-2019-142	Vulnerability identification DSA-2019-142	1	0	0	CVE-2019-6111
[DSA-Isilon]: K080DI00P183: Protected recovery copies	Immutable data copies	0	0	1	FFIEC, ISO/IEC 27040, SEC Rule 17a-4
[DSA-CVEs]: Isilon vulnerability analysis: DSA-2021-158	Vulnerability identification DSA-2021-158	0	1	0	CVE-2020-26198, CVE-2020-5366, CVE-2021-21561, CVE-2021-36280
[DSA-Brocade]: K0304I0MP295: Minimum password digits	Use of digits in passwords	0	1	0	PCI DSS, PCI DSS 8.2.3, SWIFT, ISO, ISO/IEC 27001, ISO/IEC 27001 A.9.4.3, Community, ISO/IEC 27040, CIS Co
[DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2020-1078	Vulnerability identification BSA-2020-1078	1	0	0	CVE-2020-15369
[DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2018-730	Vulnerability identification BSA-2018-730	1	0	0	CVE-2018-6436, CVE-2018-6439
[DSA-Isilon]: K030D0000150: DNS service status	Name service is enabled	0	1	0	Community, NIST, NIST SP800-53, NIST SP800-53 SC-22
[DSA-Isilon]: K140D00M0525: CIFS share user access list	Local user accounts should not be used	0	1	0	PCI DSS, PCI DSS 8.1.1, ISO, ISO/IEC 27001, ISO/IEC 27001 A.9.2, COBIT 5, COBIT 5 DSS05.04, Community, HI
[DSA-Isilon]: Isilon vulnerability analysis: DSA-2020-155	Vulnerability identification	0	1	0	CVE-2019-9924
[DSA-Brocade]: K0304I0MP295: Maximum password age	Maximum password lifetime is restricted	0	1	0	PCI DSS, PCI DSS 8.2.4, SWIFT, SWIFT CSP 4.1, ISO, ISO/IEC 27001, ISO/IEC 27001 A.9.4.3, Community, ISO/IE
[DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2021-1494	Vulnerability identification BSA-2021-1494	0	1	0	CVE-2020-15388
[DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2020-1166	Vulnerability identification BSA-2020-1166	0	1	0	CVE-2020-1971
[DSA-Brocade]: K070400M0800: SNMP user authentication	SNMP authentication required	0	1	0	PCI DSS, PCI DSS 8, Cisco Security Baseline, Community, CIS Control, CIS Control 11.5, NIST, NIST SP800-53, NI
[DSA-Isilon]: K070D00M0810: SNMPv1 / SNMPv2 status	Secure SNMP versions used (SNMPv3 or its success	0	1	0	CISA, CISA Alert TA17-156, Cisco Implementation Guide
[DSA-CVEs]: Isilon vulnerability analysis: DSA-2018-147	Vulnerability identification DSA-2018-147	1	0	0	CVE-2018-11071
[DSA-Brocade]: K0704I000240: FC security policies	Fabric access is restricted	0	1	0	Brocade Fibre Channel Security Best Practices, ISO/IEC 27040
[DSA-Brocade]: K070400MP802: SNMP community default string	Vendor-supplied default passwords are not used	1	0	0	FFIEC, PCI DSS, PCI DSS 2.1, Community, ISO/IEC 27040, CIS Control, CIS Control 4.2, NIST, NIST SP800-53
[DSA-CVEs]: Isilon vulnerability analysis: DSA-2018-044	Vulnerability identification DSA-2018-044	1	0	0	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-
[DSA-Brocade]: K010400M0160: Required syslog servers	Authorized logging servers are used	1	0	0	PCI DSS, PCI DSS 10.5, ISO, ISO/IEC 27001, ISO/IEC 27001 A.12.4.3, CIS Control, CIS Control 6, NIST, NIST SP8
[DSA-CVEs]: Isilon vulnerability analysis: DSA-2020-142	Vulnerability identification DSA-2020-142	1	0	0	CVE-2020-5369
[DSA-Brocade]: K0204I00P209: Required aaa servers	Authorized authentication servers are used	1	0	0	PCI DSS, ISO, ISO/IEC 27001, ISO/IEC 27040, CIS Control, CIS Control 16.2, NIST SP800-53, NIST SP800-63B
[DSA-Isilon]: K110DI00P110: Login banner status	System use notification is presented	0	1	0	ISO, ISO/IEC 17799, ISO/IEC 17799 11.5.1, ISO/IEC 17799 15.1.5, Cisco Security Baseline, Community, NIST, NIST
[DSA-CVEs]: Brocade SAN switch vulnerability analysis: BSA-2020-1075	Vulnerability identification BSA-2020-1075	1	0	0	CVE-2018-6448

328 items