Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.16

December 10, 2021 (Updated December 13, 2021)

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Cloud Platform

Qualys Policy Compliance (PC/SCAP/SCA)

Qualys Vulnerability Management (VM)

Qualys 10.16 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

Invalid EC2 Instance IDs Skipped at Scan Launch

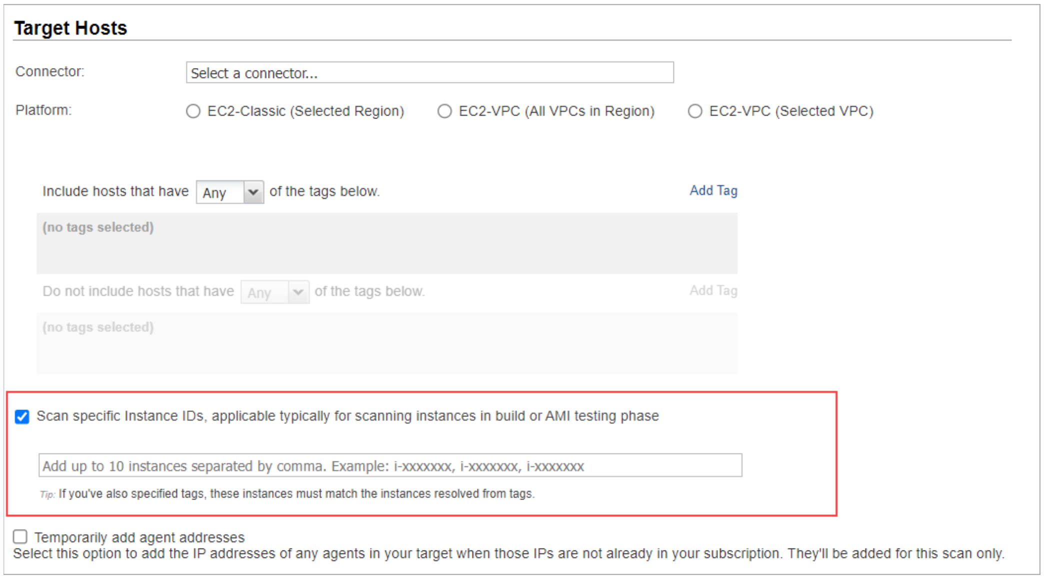
When you launch an EC2 scan and specify EC2 instance IDs as part of the scan target, we will identify and skip any invalid instances and continue the scan on the valid instances. Previously, the entire scan would have been blocked if an instance ID specified as part of the scan target was considered invalid. In addition, we have provided a more detailed notification/error message to the user when detecting an invalid manual ec2 instance id(s) in the scan request.

A specified EC2 instance ID could be considered invalid for these reasons:

- The instance does not belong to the EC2 environment being scanned.
- The instance does not match EC2 hosts resolved from asset tags specified as part of the scan target. Applicable only when asset tags are also specified for the scan.
- The instance has not been activated for the current module (VM, PC/SCA, CertView). For example, you're launching a vulnerability scan but the EC2 host is not activated for VM.
- The Unit Manager launching the scan does not have permission to scan the EC2 host.

Specifying instance IDs

These changes only apply when the scan target includes specific EC2 instance IDs. Not sure where to specify instance IDs? When configuring an EC2 scan, go to the **Target Hosts** section and select the check box "**Scan specific instance IDs, applicable typically for scanning instances in build or AMI testing phase**" and then enter the instance IDs in the field provided.



Target Hosts

Connector: Select a connector...

Platform: ○ EC2-Classic (Selected Region) ○ EC2-VPC (All VPCs in Region) ○ EC2-VPC (Selected VPC)

Include hosts that have Any of the tags below.

(no tags selected)

Do not include hosts that have Any of the tags below.

(no tags selected)

☑ Scan specific Instance IDs, applicable typically for scanning instances in build or AMI testing phase

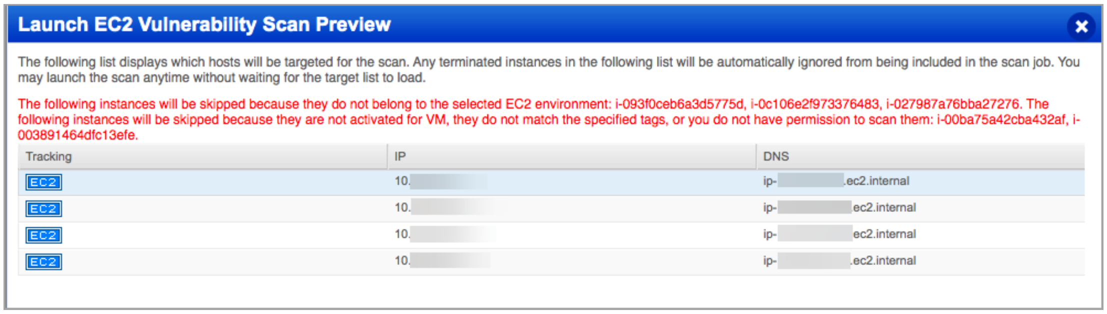
Add up to 10 instances separated by comma. Example: i-xxxxxxx, i-xxxxxxx, i-xxxxxxx

Tip: If you've also specified tags, these instances must match the instances resolved from tags.

☐ Temporarily add agent addresses
Select this option to add the IP addresses of any agents in your target when those IPs are not already in your subscription. They'll be added for this scan only.

When some instances are valid and some are invalid

When EC2 instance IDs are specified, and at least one of the instance IDs is valid, and at least one is invalid, you'll see a message on the Launch EC2 Scan Preview page with the invalid instance IDs listed and the reasons they are invalid (in red). See example below.



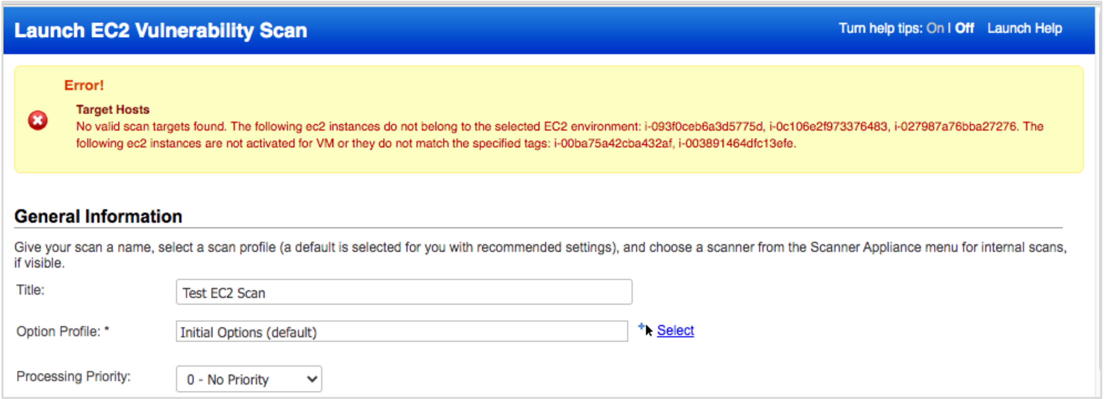
The following list displays which hosts will be targeted for the scan. Any terminated instances in the following list will be automatically ignored from being included in the scan job. You may launch the scan anytime without waiting for the target list to load.

The following instances will be skipped because they do not belong to the selected EC2 environment: i-093f0ceb6a3d5775d, i-0c106e2f973376483, i-027987a76bba27276. The following instances will be skipped because they are not activated for VM, they do not match the specified tags, or you do not have permission to scan them: i-00ba75a42cba432af, i-003891464dfc13efe.

Tracking	IP	DNS
EC2	10.[redacted]	ip-[redacted].ec2.internal
EC2	10.[redacted]	ip-[redacted]ec2.internal
EC2	10.[redacted]	ip-[redacted]ec2.internal
EC2	10.[redacted]	ip-[redacted].ec2.internal

When no valid scan targets are found

When EC2 instance IDs are specified, but there are no valid scan targets, you'll see an Error on the Scan Launch page with the invalid instance IDs listed and the reasons they are invalid.



Error!

Target Hosts

No valid scan targets found. The following ec2 instances do not belong to the selected EC2 environment: i-093f0ceb6a3d5775d, i-0c106e2f973376483, i-027987a76bba27276. The following ec2 instances are not activated for VM or they do not match the specified tags: i-00ba75a42cba432af, i-003891464dfc13efe.

General Information

Give your scan a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title: Test EC2 Scan

Option Profile: * Initial Options (default) Select

Processing Priority: 0 - No Priority

Sample Messages

You may see a single message or a combination of messages when instance IDs are invalid for different reasons. For the sample messages below, please note:

<module> is the module for the EC2 scan type. You'll see one of these values: VM, PC/SCA, CertView.

<EC2 instance IDs> is a comma-separated list of invalid EC2 instance IDs.

Sample Messages on Launch EC2 Scan Preview Page

Here are sample messages that could appear on the Launch EC2 Scan Preview page when there are invalid instance IDs that are being skipped.

Manager:

The following instances will be skipped because they do not belong to the selected EC2 environment: <EC2 instance IDs>

The following instances will be skipped because they do not belong to the selected EC2 environment and tags: <EC2 instance IDs>

The following instances will be skipped because they are not activated for <module>: <EC2 instance IDs>

The following instances will be skipped because they are not activated for <module> or they do not match the specified tags: <EC2 instance IDs>

Unit Manager:

The following instances will be skipped because they are not activated for <module>, or you do not have permission to scan them: <EC2 instance IDs>

The following instances will be skipped because they are not activated for <module>, they do not match the specified tags, or you do not have permission to scan them: <EC2 instance IDs>

Sample Messages on Scan Launch Page

Here are sample messages that could appear on the Launch Scan page when there are no valid scan targets found.

Manager:

No valid scan targets found. The following instances are not activated for <module>: <EC2 instance IDs>

No valid scan targets found. The following instances are not activated for <module> or they do not match the specified tags: <EC2 instance IDs>

No valid scan targets found. The following instances do not belong to the selected EC2 environment: <EC2 instance IDs>. The following instances are not activated for <module>: <EC2 instance IDs>

Unit Manager:

No valid scan targets found. The following instances are not activated for <module> or you do not have permission to scan them: <EC2 instance IDs>

No valid scan targets found. The following instances are not activated for <module>, they do not match the specified tags, or you do not have permission to scan them: <EC2 instance IDs>

No valid scan targets found. The following instances do not belong to the selected EC2 environment: <EC2 instance IDs>. The following instances are not activated for <module> or you do not have per-mission to scan them: <EC2 instance IDs>

API Vault Support added for IBM DB2 Authentication Records

We already support vaults for IBM DB2 authentication records from the UI. Starting in this release, we'll also support vaults for IBM DB2 authentication records from the API. This means that you can specify a vault when creating/updating a IBM DB2 authentication record using the API, and you'll see vault information when listing records using the API.

Please refer to the Qualys Cloud Platform 10.16 API Release Notes for API samples.

Qualys Policy Compliance (PC/SCAP/SCA)

New Option to Scan Disconnected ESXi Hosts via vCenter

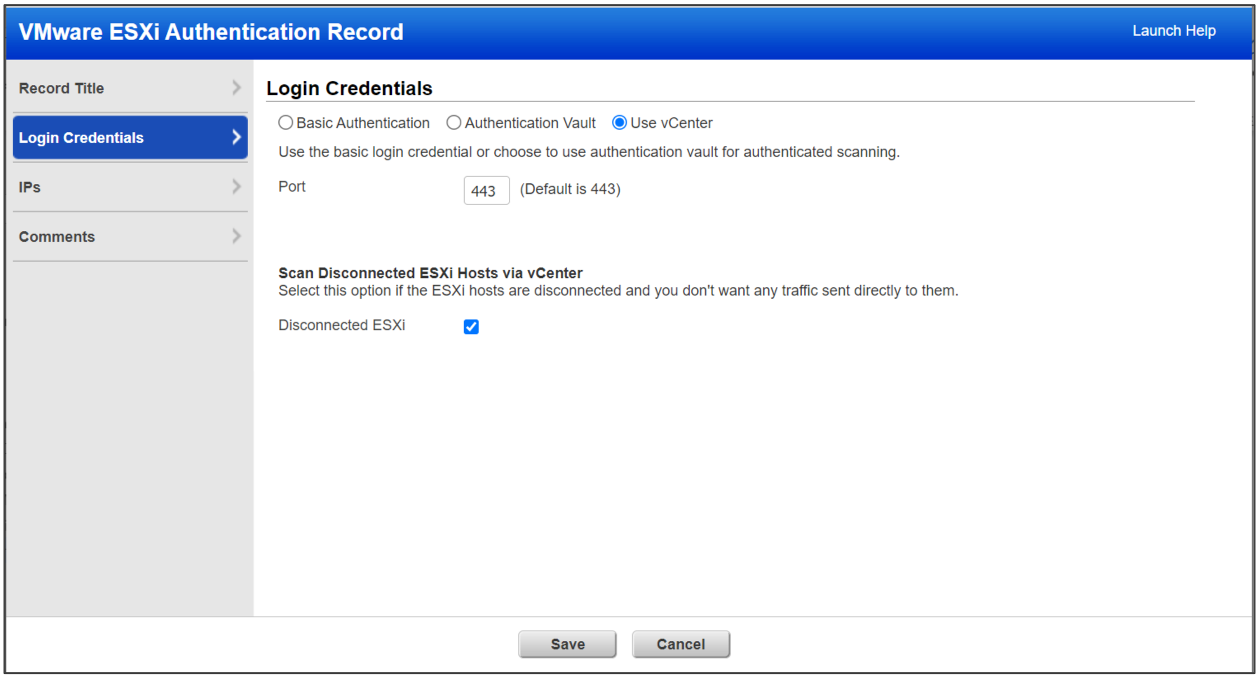
We have now introduced a new option to scan disconnected ESXi hosts. Use this option to scan ESXi hosts without sending any data to the host. In this case, on scanning, Qualys gets the required information from vCenter without sending any network traffic to the host.

Good to Know

- The Disconnected ESXi option is only supported when scanning ESXi hosts through vCenter.
- This feature is only supported for compliance scans.
- Scanning disconnected ESXi hosts is not supported for IPv6 scans.

How do I enable this option?

- Go to **Scans** > **Authentication** > **New** > **VMware** > **VMware ESXi**, and click **Login Credentials** in the VMware ESXi Authentication Record page.
- Select the **Use vCenter** option under Login Credentials section.
- Select the **Disconnected ESXi** option in the **Scan Disconnected ESXi Hosts via vCenter** section. By default, this option is clear (un-selected).



VMware ESXi Authentication Record

Login Credentials

○ Basic Authentication ○ Authentication Vault ● Use vCenter

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Port 443 (Default is 443)

Scan Disconnected ESXi Hosts via vCenter
Select this option if the ESXi hosts are disconnected and you don't want any traffic sent directly to them.

Disconnected ESXi ☑

Addition of STIG ID in DISA STIG Report

Now when you run the Compliance STIG Based Report from the UI, you'll see STIG IDs in the CSV report output. This allows you to sort STIG requirements by STIG ID. There is a one-to-one mapping between a STIG ID and a STIG Rule/Rule ID. This notification is intended to inform you of new CSV columns in the report, so you can make any changes necessary to correctly parse the report data.

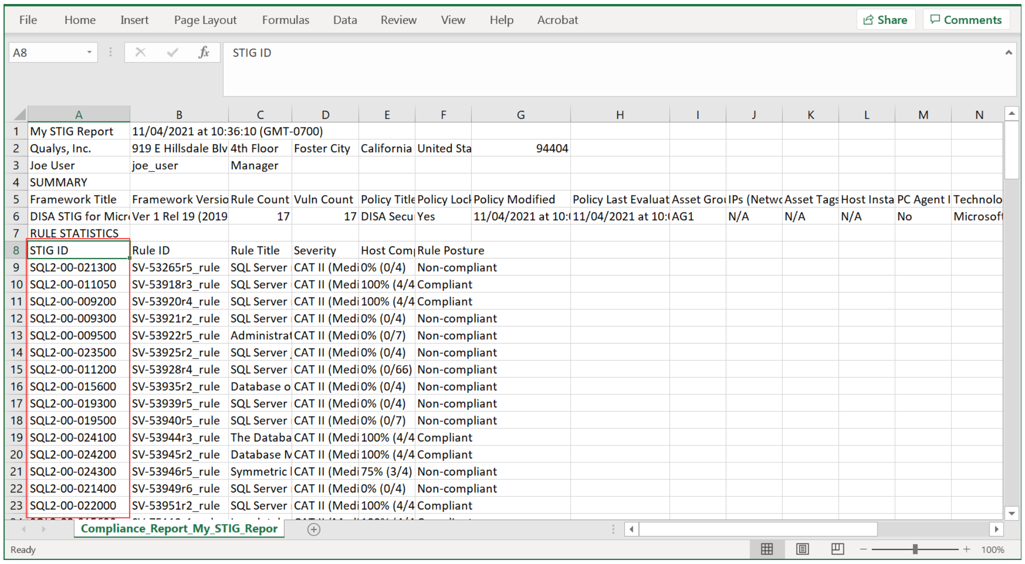
In the CSV report, you'll see a new STIG ID column in the following sections:

- STIG ID appears as the first column in the RULE STATISTICS section
- STIG ID appears before Rule ID in the RESULTS section
- STIG ID appears before Rule in the APPENDIX section (part of STIG Framework details)

Sample STIG Based Report

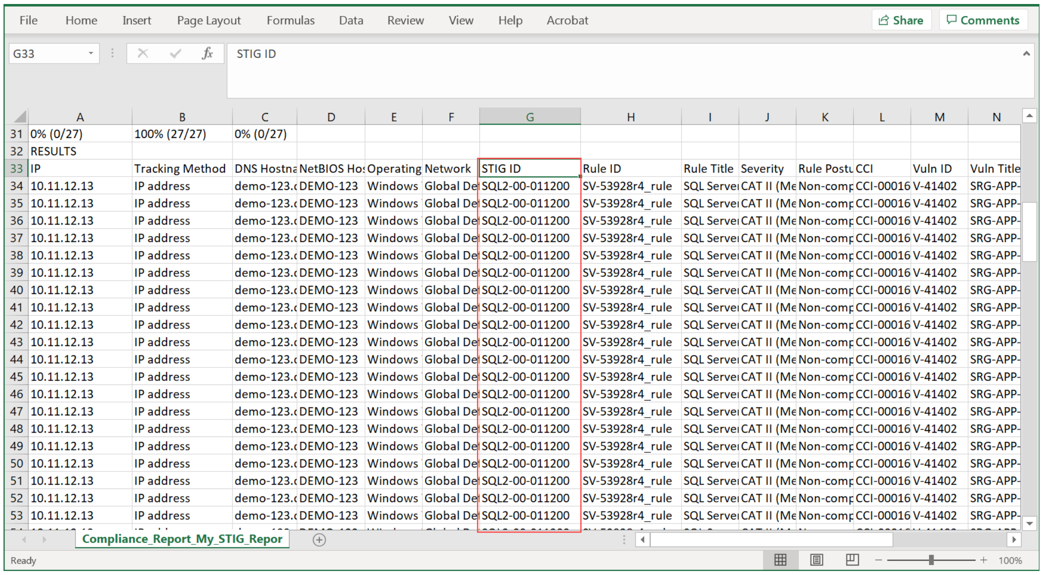
Here are clips from a sample STIG Based Report in CSV format, showing the new STIG ID columns. Run your own report to see all the columns in the CSV report output.

RULE STATISTICS section



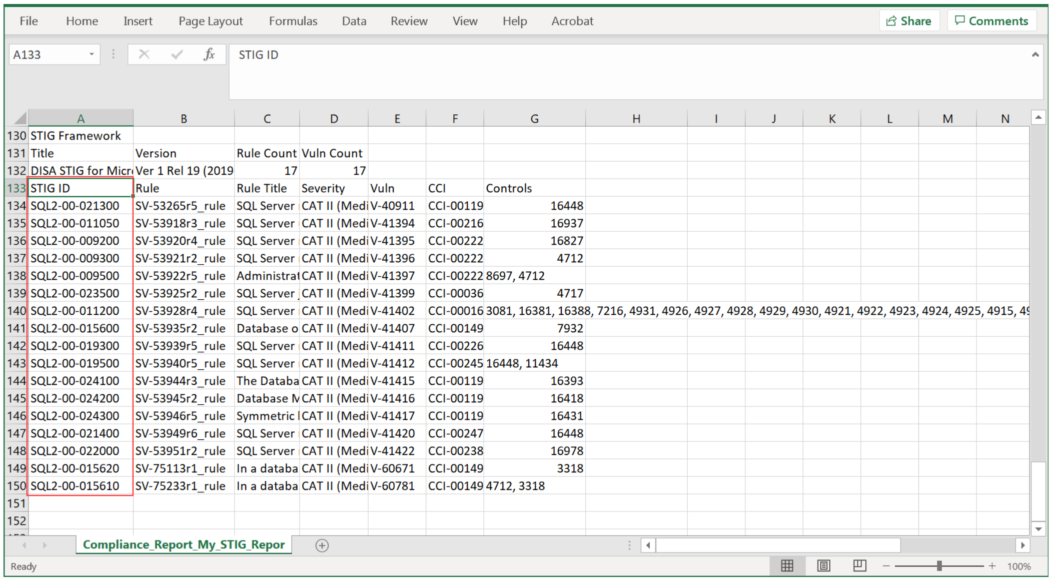
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	My STIG Report	11/04/2021 at 10:36:10 (GMT-0700)												
2	Qualys, Inc.	919 E Hillsdale Blv	4th Floor	Foster City	California	United Sta	94404							
3	Joe User	joe_user	Manager											
4	SUMMARY													
5	Framework Title	Framework Versio	Rule Count	Vuln Count	Policy Title	Policy Lock	Policy Modified	Policy Last Evaluat	Asset Grou	IPs (Netwo	Asset Tags	Host Insta	PC Agent I	Technolo
6	DISA STIG for Micr	Ver 1 Rel 19 (2019	17	17	DISA Secu	Yes	11/04/2021 at 10:(	11/04/2021 at 10:(	AG1	N/A	N/A	N/A	No	Microsoft
7	RULE STATISTICS													
8	STIG ID	Rule ID	Rule Title	Severity	Host Com	Rule Posture								
9	SQL2-00-021300	SV-53265r5_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
10	SQL2-00-011050	SV-53918r3_rule	SQL Server	CAT II (Medi	100% (4/4	Compliant								
11	SQL2-00-009200	SV-53920r4_rule	SQL Server	CAT II (Medi	100% (4/4	Compliant								
12	SQL2-00-009300	SV-53921r2_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
13	SQL2-00-009500	SV-53922r5_rule	Administrat	CAT II (Medi	0% (0/7)	Non-compliant								
14	SQL2-00-023500	SV-53925r2_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
15	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Medi	0% (0/66)	Non-compliant								
16	SQL2-00-015600	SV-53935r2_rule	Database o	CAT II (Medi	0% (0/4)	Non-compliant								
17	SQL2-00-019300	SV-53939r5_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
18	SQL2-00-019500	SV-53940r5_rule	SQL Server	CAT II (Medi	0% (0/7)	Non-compliant								
19	SQL2-00-024100	SV-53944r3_rule	The Databa	CAT II (Medi	100% (4/4	Compliant								
20	SQL2-00-024200	SV-53945r2_rule	Database M	CAT II (Medi	100% (4/4	Compliant								
21	SQL2-00-024300	SV-53946r5_rule	Symmetric I	CAT II (Medi	75% (3/4)	Non-compliant								
22	SQL2-00-021400	SV-53949r6_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
23	SQL2-00-022000	SV-53951r2_rule	SQL Server	CAT II (Medi	100% (4/4	Compliant								

RESULTS section



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
31	0% (0/27)	100% (27/27)	0% (0/27)											
32	RESULTS													
33	IP	Tracking Method	DNS Hostna	NetBIOS Ho:	Operating	Network	STIG ID	Rule ID	Rule Title	Severity	Rule Postu	CCI	Vuln ID	Vuln Title
34	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
35	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
36	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
37	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
38	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
39	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
40	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
41	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
42	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
43	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
44	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
45	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
46	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
47	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
48	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
49	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
50	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
51	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
52	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
53	10.11.12.13	IP address	demo-123.c	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Serve	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-

APPENDIX section

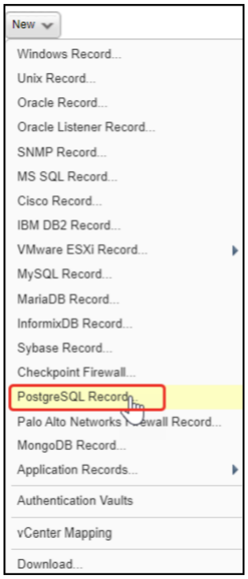


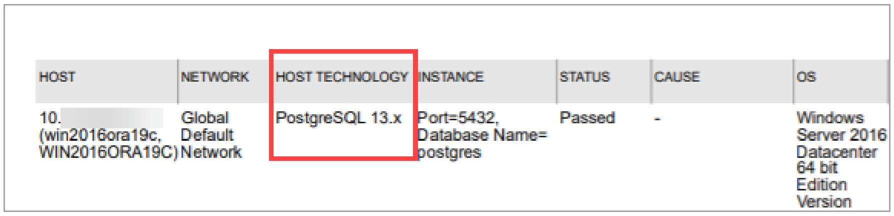
	A	B	C	D	E	F	G
130	STIG Framework						
131	Title	Version	Rule Count	Vuln Count			
132	DISA STIG for Micr	Ver 1 Rel 19 (2019	17	17			
133	STIG ID	Rule	Rule Title	Severity	Vuln	CCI	Controls
134	SQL2-00-021300	SV-53265r5_rule	SQL Server	CAT II (Medi	V-40911	CCI-00119	16448
135	SQL2-00-011050	SV-53918r3_rule	SQL Server	CAT II (Medi	V-41394	CCI-00216	16937
136	SQL2-00-009200	SV-53920r4_rule	SQL Server	CAT II (Medi	V-41395	CCI-00222	16827
137	SQL2-00-009300	SV-53921r2_rule	SQL Server	CAT II (Medi	V-41396	CCI-00222	4712
138	SQL2-00-009500	SV-53922r5_rule	Administrat	CAT II (Medi	V-41397	CCI-00222	8697, 4712
139	SQL2-00-023500	SV-53925r2_rule	SQL Server	CAT II (Medi	V-41399	CCI-00036	4717
140	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Medi	V-41402	CCI-00016	3081, 16381, 16388, 7216, 4931, 4926, 4927, 4928, 4929, 4930, 4921, 4922, 4923, 4924, 4925, 4915, 49
141	SQL2-00-015600	SV-53935r2_rule	Database o	CAT II (Medi	V-41407	CCI-00149	7932
142	SQL2-00-019300	SV-53939r5_rule	SQL Server	CAT II (Medi	V-41411	CCI-00226	16448
143	SQL2-00-019500	SV-53940r5_rule	SQL Server	CAT II (Medi	V-41412	CCI-00245	16448, 11434
144	SQL2-00-024100	SV-53944r3_rule	The Databa	CAT II (Medi	V-41415	CCI-00119	16393
145	SQL2-00-024200	SV-53945r2_rule	Database M	CAT II (Medi	V-41416	CCI-00119	16418
146	SQL2-00-024300	SV-53946r5_rule	Symmetric I	CAT II (Medi	V-41417	CCI-00119	16431
147	SQL2-00-021400	SV-53949r6_rule	SQL Server	CAT II (Medi	V-41420	CCI-00247	16448
148	SQL2-00-022000	SV-53951r2_rule	SQL Server	CAT II (Medi	V-41422	CCI-00238	16978
149	SQL2-00-015620	SV-75113r1_rule	In a databa	CAT II (Medi	V-60671	CCI-00149	3318
150	SQL2-00-015610	SV-75233r1_rule	In a databa	CAT II (Medi	V-60781	CCI-00149	4712, 3318
151							
152							

Support New Technology: PostgreSQL 13.x

We've extended our support for PostgreSQL authentication to include PostgreSQL 13.x. We already support PostgreSQL 9.x, 10.x, 11.x and 12.x.

You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a host and scan it for compliance. You'll also need a Unix/Windows record for the host running the database. This record type is only available in accounts with PC or SCA and is only supported for compliance scans.





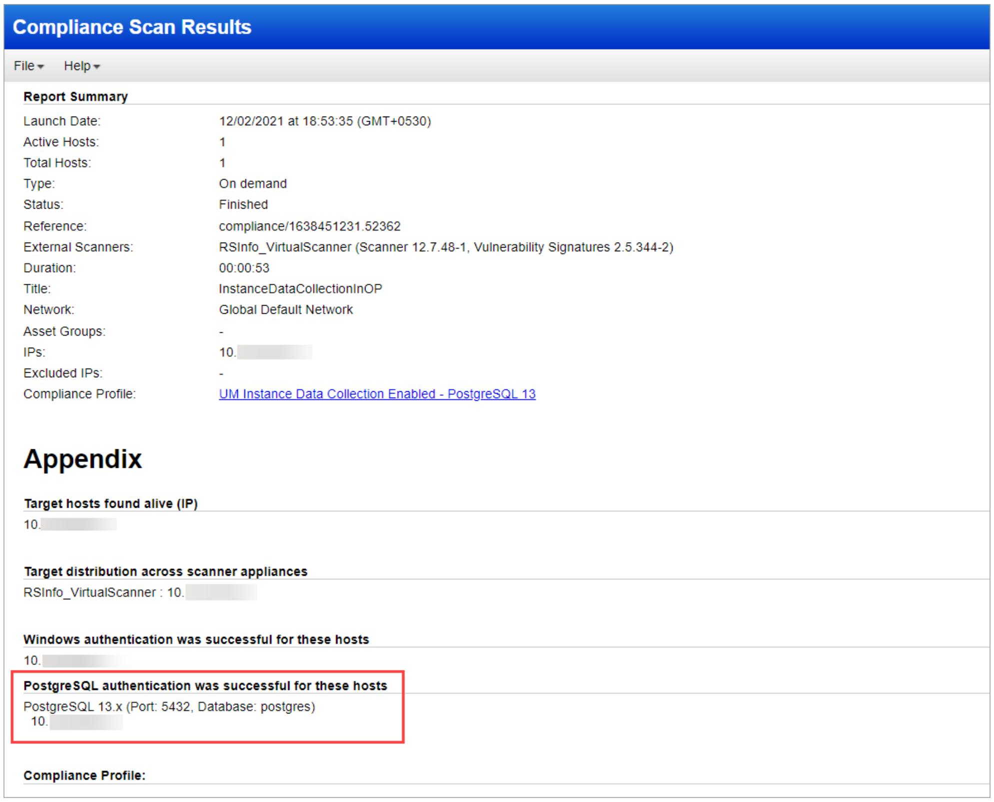
HOST	NETWORK	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS
10.[redacted] (win2016ora19c, WIN2016ORA19C)	Global Default Network	PostgreSQL 13.x	Port=5432, Database Name= postgres	Passed	-	Windows Server 2016 Datacenter 64 bit Edition Version

How do I get started?

- Go to **Scans** > **Authentication**.
- Check that you have a Unix/Windows record already defined for the host running the database.
- Create a PostgreSQL record for the same host. Go to **New** > **PostgreSQL Record**.

Sample Reports

You'll see the PostgreSQL 13.x technology in compliance reports and in compliance scan results.



Compliance Scan Results

File ▾ Help ▾

Report Summary

Launch Date:	12/02/2021 at 18:53:35 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	compliance/1638451231.52362
External Scanners:	RSInfo_VirtualScanner (Scanner 12.7.48-1, Vulnerability Signatures 2.5.344-2)
Duration:	00:00:53
Title:	InstanceDataCollectionInOP
Network:	Global Default Network
Asset Groups:	-
IPs:	10.[redacted]
Excluded IPs:	-
Compliance Profile:	UM Instance Data Collection Enabled - PostgreSQL 13

Appendix

Target hosts found alive (IP)

10.[redacted]

Target distribution across scanner appliances

RSInfo_VirtualScanner : 10.[redacted]

Windows authentication was successful for these hosts

10.[redacted]

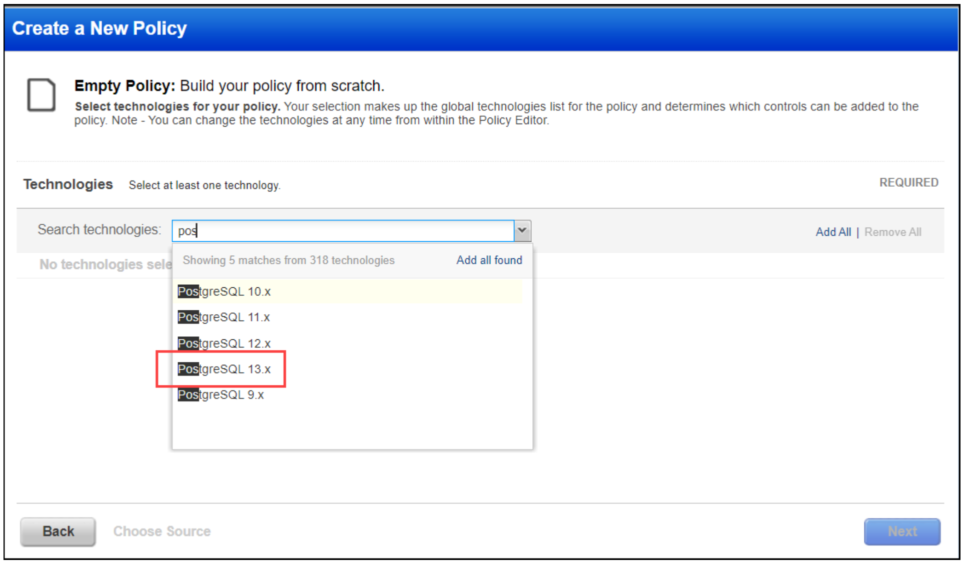
PostgreSQL authentication was successful for these hosts

PostgreSQL 13.x (Port: 5432, Database: postgres)
10.[redacted]

Compliance Profile:

Policies and Controls

You’ll see PostgreSQL 13.x in the technologies list when creating a new policy.



Create a New Policy

Empty Policy: Build your policy from scratch.

Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

Technologies Select at least one technology. REQUIRED

Search technologies: pos

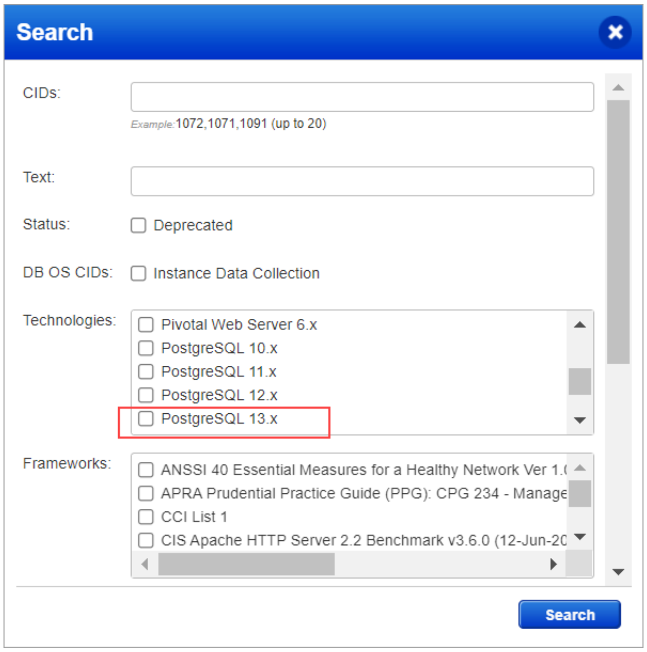
Add All | Remove All

No technologies sele

Showing 5 matches from 318 technologies Add all found

PostgreSQL 10.x
PostgreSQL 11.x
PostgreSQL 12.x
PostgreSQL 13.x
PostgreSQL 9.x

You’ll also see it when searching controls.



Search

CIDs:

Example: 1072,1071,1091 (up to 20)

Text:

Status: □ Deprecated

DB OS CIDs: □ Instance Data Collection

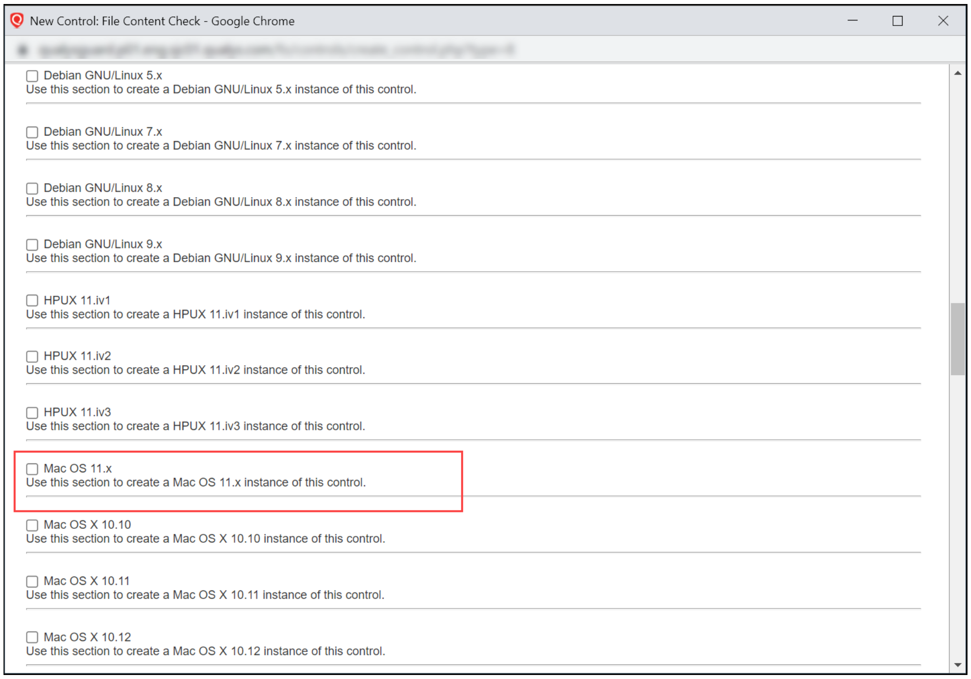
Technologies:
□ Pivotal Web Server 6.x
□ PostgreSQL 10.x
□ PostgreSQL 11.x
□ PostgreSQL 12.x
□ PostgreSQL 13.x

Frameworks:
□ ANSSI 40 Essential Measures for a Healthy Network Ver 1.(
□ APRA Prudential Practice Guide (PPG): CPG 234 - Manage
□ CCI List 1
□ CIS Apache HTTP Server 2.2 Benchmark v3.6.0 (12-Jun-20

Support for UDCs on MAC OS 11.x

We have extended the User Defined Control (UDC) support for MAC OS 11.x.
Note: MAC OS 11.x is supported for scanner only.

Want to create a UDC for MAC OS 11.x? Go to **Policies** > **Controls** > **New** > **Control** > **Unix Control Types** and select the required control type from the list. Scroll to the **Control Technologies** section to provide a rationale statement and expected value for each technology.



New Control: File Content Check - Google Chrome

□ Debian GNU/Linux 5.x
Use this section to create a Debian GNU/Linux 5.x instance of this control.

□ Debian GNU/Linux 7.x
Use this section to create a Debian GNU/Linux 7.x instance of this control.

□ Debian GNU/Linux 8.x
Use this section to create a Debian GNU/Linux 8.x instance of this control.

□ Debian GNU/Linux 9.x
Use this section to create a Debian GNU/Linux 9.x instance of this control.

□ HPUX 11.iv1
Use this section to create a HPUX 11.iv1 instance of this control.

□ HPUX 11.iv2
Use this section to create a HPUX 11.iv2 instance of this control.

□ HPUX 11.iv3
Use this section to create a HPUX 11.iv3 instance of this control.

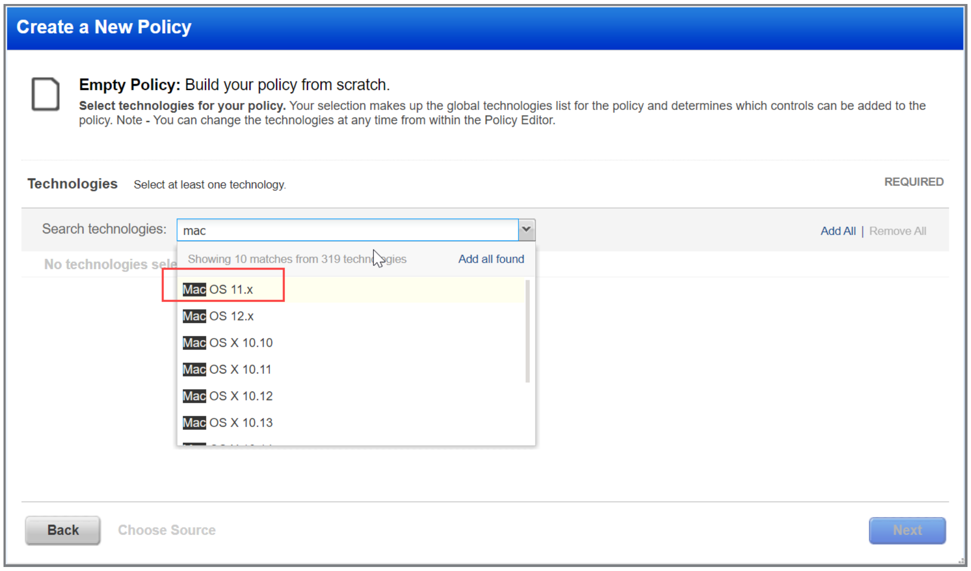
□ Mac OS 11.x
Use this section to create a Mac OS 11.x instance of this control.

□ Mac OS X 10.10
Use this section to create a Mac OS X 10.10 instance of this control.

□ Mac OS X 10.11
Use this section to create a Mac OS X 10.11 instance of this control.

□ Mac OS X 10.12
Use this section to create a Mac OS X 10.12 instance of this control.

While creating a new policy, select **MAC OS 11.x** from the **Technologies** list.



Create a New Policy

Empty Policy: Build your policy from scratch.
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

Technologies Select at least one technology. REQUIRED

Search technologies: mac

Showing 10 matches from 319 technologies

New Authentication Technology Support

We've added additional technology support for different authentication record types since the last Qualys Cloud Platform release. The following technologies are now supported.

Windows Authentication:
Windows 2022 Server
NetApp Data ONTAP 7.x, 8.x

Unix Authentication:
Cisco NX-OS ACI Mode
CentOS Stream 8.x
Red Hat Enterprise Linux CoreOS 4.x
A10 Advanced Core OS 4.x
Huawei VRP 5.x
NetApp Ontap 9.x

Cisco Authentication:
Cisco IOS XR 6.x, 7.x

IBM DB2 Authentication:
IBM DB2 z/OS
IBM DB2 z/OS 1

VMware vCenter Authentication:
VMware vCenter Server 5.x-6.x (Windows)
VMware vCenter Server Appliance 5.x-7.x (Windows and Unix)

Support for OS Authentication-Based Instance Technologies

We've expanded our support of OS authentication-based technologies to include the following:

Jenkins 2.x
Redis 3.x
Redis 5.x
Redis 6.x
IBM Sterling Connect:Direct 6.x
Apple Safari 14.x
Apache Hadoop 2.x
FreeBSD 13.x

You can collect data for these technology versions by using the underlying UNIX technology instance without the need to create authentication records. You must have a Unix authentication record with 'Sudo' as root delegation. You can include these technologies in your compliance policies and when searching controls. You'll also see host instance information in Policy Compliance authentication reports, scan results, and policy reports.

Support for New OCA Technologies

We now support the following new technologies on assets for which data is collected using Out-of-Band Configuration Assessment (OCA) tracking.

Data Domain OS 5.x
Data Domain OS 6.x

Using the OCA module, upload the corresponding configuration or command output for the assets. Then navigate to Policy Compliance > Reports tab to run the Policy Compliance Report for these technologies to view the compliance posture.

Qualys Vulnerability Management (VM)

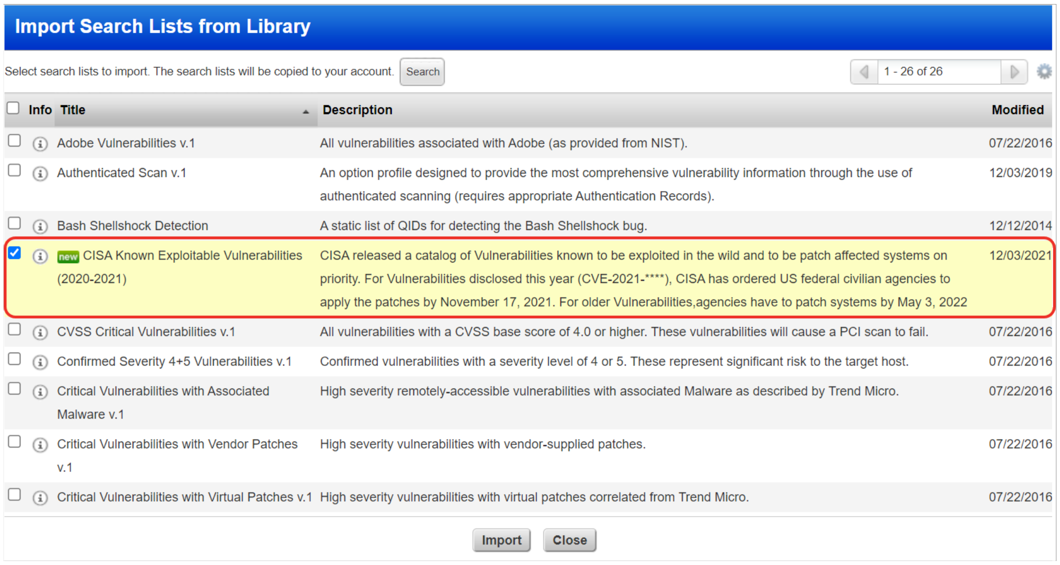
New CISA Known Exploitable Vulnerabilities Search List Available in Library

Now, you can import the new "CISA Known Exploitable Vulnerabilities" search list from the Library. This search list includes vulnerabilities known to be exploited in the wild and affected systems need to be patched on priority.

Note: You can use the "CISA Known Exploitable Vulnerabilities" search list from the library only to create a static search list.

How to import search lists

Go to the **Search Lists** tab (under Scans, Reports or KnowledgeBase) and pick **New** > **Import** from Library. Select the new search list and click **Import** again.



Select search lists to import. The search lists will be copied to your account.

☐	Info	Title	Description	Modified
☐	ⓘ	Adobe Vulnerabilities v.1	All vulnerabilities associated with Adobe (as provided from NIST).	07/22/2016
☐	ⓘ	Authenticated Scan v.1	An option profile designed to provide the most comprehensive vulnerability information through the use of authenticated scanning (requires appropriate Authentication Records).	12/03/2019
☐	ⓘ	Bash Shellshock Detection	A static list of QIDs for detecting the Bash Shellshock bug.	12/12/2014
☑	ⓘ	new CISA Known Exploitable Vulnerabilities (2020-2021)	CISA released a catalog of Vulnerabilities known to be exploited in the wild and to be patch affected systems on priority. For Vulnerabilities disclosed this year (CVE-2021-****), CISA has ordered US federal civilian agencies to apply the patches by November 17, 2021. For older Vulnerabilities,agencies have to patch systems by May 3, 2022	12/03/2021
☐	ⓘ	CVSS Critical Vulnerabilities v.1	All vulnerabilities with a CVSS base score of 4.0 or higher. These vulnerabilities will cause a PCI scan to fail.	07/22/2016
☐	ⓘ	Confirmed Severity 4+5 Vulnerabilities v.1	Confirmed vulnerabilities with a severity level of 4 or 5. These represent significant risk to the target host.	07/22/2016
☐	ⓘ	Critical Vulnerabilities with Associated Malware v.1	High severity remotely-accessible vulnerabilities with associated Malware as described by Trend Micro.	07/22/2016
☐	ⓘ	Critical Vulnerabilities with Vendor Patches v.1	High severity vulnerabilities with vendor-supplied patches.	07/22/2016
☐	ⓘ	Critical Vulnerabilities with Virtual Patches v.1	High severity vulnerabilities with virtual patches correlated from Trend Micro.	07/22/2016

Updates to Cloud Asset Metadata Fields in Host-Based Scan Reports

With this release, we've provided the option to include GCP Cloud Provider Metadata in the host-based scan report. We've also made a couple of enhancements to the host-based scan report.

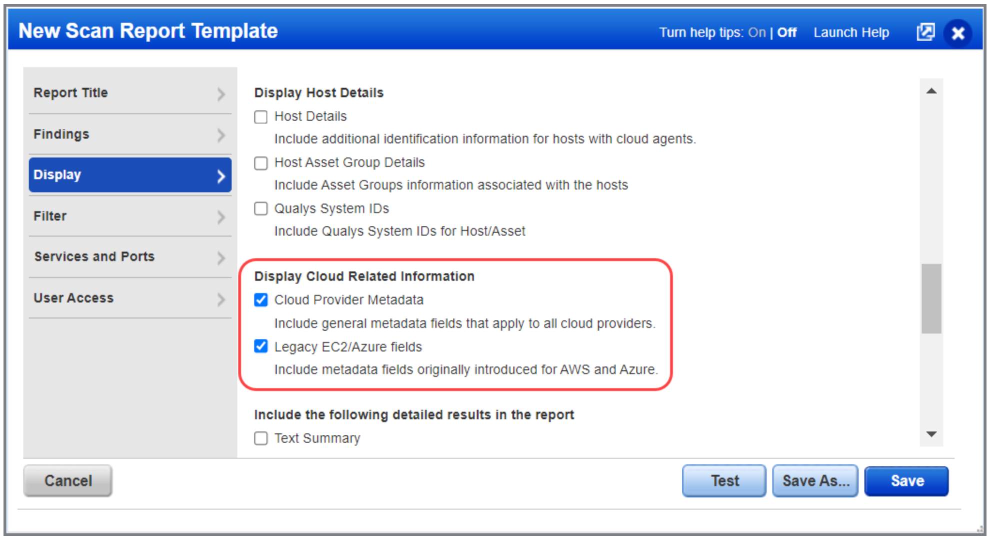
For this, we've done a couple of changes in the Scan Report Template and Scan Report:

- Removed 'Cloud Related Information' checkbox from the Display Host Details section of the Display tab from the Scan Report Template
- Added new section as 'Display Cloud Related Information' in the Display tab in the Scan Report Template and included two options under it:
  - Cloud Provider Metadata: This option allows you to include general fields that apply to all cloud providers, including AWS, Azure, GCP, and future support to your report.
  - Legacy EC2/Azure fields: This option allows you to include cloud provider-specific metadata fields originally introduced for AWS and Azure.

- We'll automatically update your existing scan report templates to use the new options. If you had the "Cloud Related Information" template option selected prior to this release, then we'll select the "Legacy EC2/Azure fields" option. If your subscription had the "Cloud Perimeter Azure VM Scan" feature enabled, then we will also select the "Cloud Provider Metadata Fields" option.
- We added the new field Cloud Provider Service. This will appear when "Cloud Provider Metadata" is selected in the template. It will also appear in XML reports for AWS and Azure assets when "Legacy EC2/Azure fields" is selected. The Cloud Provider Service field will replace the existing Cloud Service field in a future release. For AWS, you'll see "EC2" for Cloud Provider Service/Cloud Service. For Azure, you'll see "VM" for Cloud Provider Service/Cloud Service. For GCP, you'll see "Compute Engine" for Cloud Provider Service and "VM Instance" for Cloud Service.
- We added the fields Cloud Resource Type and Cloud Image ID. These fields will only appear when "Cloud Provider Metadata" is selected in the template.
- In CSV output, we changed the order of the columns. When all fields are included in the report, the Cloud Resource Metadata column is no longer the last column in the report. It appears before the Legacy EC2/Azure fields.
- We dropped certain requirements for displaying cloud related information in reports. Users no longer need the "EC2 Scanning" feature enabled for their subscription in order to include cloud related information in Host Based Scan Reports. Additionally, users no longer need the "Cloud Perimeter Azure VM Scan" feature enabled for their subscription in order to display the general cloud provider metadata fields in the CSV format of the report.

Update to Scan Report Template

Go to **Reports** > **Templates** > **New** > **Scan Template...**



Display Host Details

☐ Host Details
Include additional identification information for hosts with cloud agents.

☐ Host Asset Group Details
Include Asset Groups information associated with the hosts

☐ Qualys System IDs
Include Qualys System IDs for Host/Asset

Display Cloud Related Information

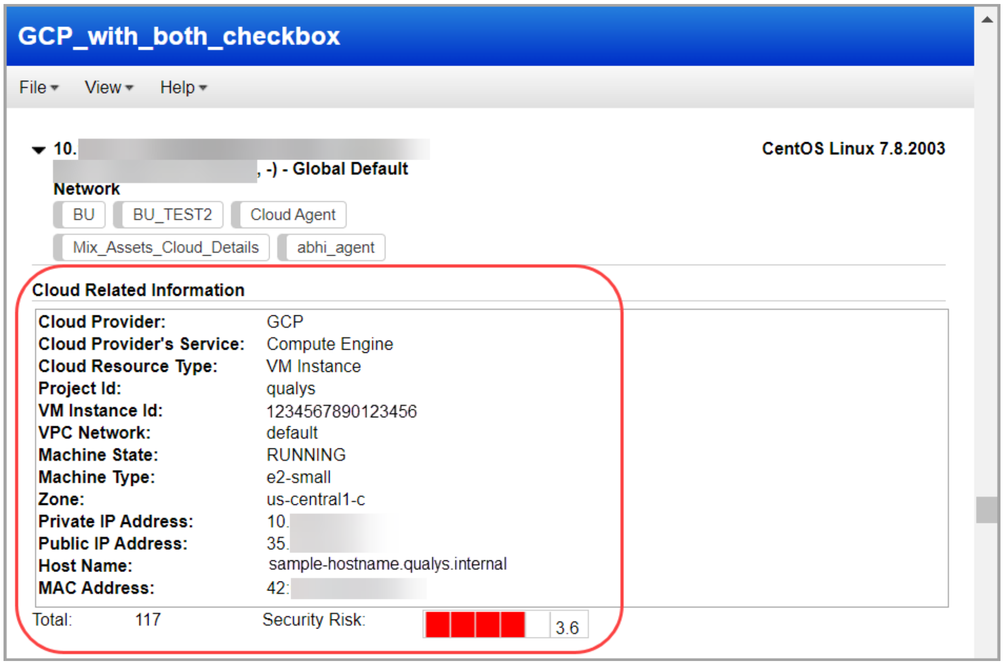
☑ Cloud Provider Metadata
Include general metadata fields that apply to all cloud providers.

☑ Legacy EC2/Azure fields
Include metadata fields originally introduced for AWS and Azure.

Include the following detailed results in the report

☐ Text Summary

Sample Scan Report



GCP_with_both_checkbox

10.[redacted]
[redacted], -) - Global Default Network

CentOS Linux 7.8.2003

BU | BU_TEST2 | Cloud Agent | Mix_Assets_Cloud_Details | abhi_agent

Cloud Related Information

Cloud Provider:	GCP
Cloud Provider's Service:	Compute Engine
Cloud Resource Type:	VM Instance
Project Id:	qualys
VM Instance Id:	1234567890123456
VPC Network:	default
Machine State:	RUNNING
Machine Type:	e2-small
Zone:	us-central1-c
Private IP Address:	10.[redacted]
Public IP Address:	35.[redacted]
Host Name:	sample-hostname.qualys.internal
MAC Address:	42:[redacted]

Total: 117 Security Risk: 🟥🟥🟥🟥 3.6

Issues Addressed

- We made a fix to improve performance when collecting evidence information in the Compliance Posture Information API request.
- We fixed an issue where an IP-tracked asset was not migrated to DNS-tracked after getting a valid DNS Host Name in QID 6 and DNS tracking being enabled. Now, the IP-tracked asset migrates without any issue to DNS-tracked asset when getting valid DNS Host Name in QID 6 and DNS tracking being enabled.
- We fixed an issue in the Policy Editor where users got an error while saving a policy that included deleted asset groups.
- Scanner users are now able to save new option profiles and should not see "invalid user" error.
- We fixed the error message that appears when launching an SCA scan with an option profile that does not contain CIS policies.
- We fixed an issue where some customers with VMDR enabled for their subscription did not see the VMDR Dashboard after they logged in to the UI.
- Now, the Last Compliance Scan date in Asset Search Reports will show the correct date for SCA assets. The "Last Scan Date (PC)" filter returns only PC assets, whereas the "Last Scan Date (SCA)" filter returns only SCA assets.
- We fixed an issue for AGMS-enabled subscriptions where users could not launch Map Reports on valid domain names. Users can now launch map reports with valid domain names for AGMS-enabled accounts. Changes are done to validate specific domain names and return the result if the domain is present in the subscription.
- We fixed a UI issue on the Authentication tab where the authentication records list was not visible when the graph was displayed and the user zoomed in on the page. Now, users can view the authentication record list without hiding graphs on the authentication record page.
- We fixed an issue where Map Reports showed asset groups from different networks. Now, users will only see asset groups for the selected network in their Map Reports.
- We fixed an issue in VM Scan Results and Reports where when the View option was used to load a select IP range, the entire list of IPs was shown instead of the selected range.
- We fixed an issue where the Hosts Scanned count was incorrect in VM Scorecard Reports when the "Hosts with Cloud Agents" options were used, also fixed the Host Type Filter values included Agent Data and Scan Data to run the report in all formats.
- Now, users with a Remediation User role will no longer see a link to view the Host Information page for IPs on the Remediation > Tickets list since these users do not have permission to view the Host Information page.
- We fixed an issue where VM scan-based reports failed to finish when report data was sorted by OS and there was an empty OS value for some hosts. Now the OS value will be shown as Unknown.
- Now, the activity log will display the removed schedule scan due to the user role being demoted to Reader.
- We fixed an issue where scheduled scans failed to launch when some IPs were removed from the subscription. Now, the scheduled scan will launch as expected even when some IPs are removed.
- We fixed an issue where the "Exclude non-running kernels" and "Exclude non-running services" options were not working properly for VM Scorecard Reports when enabled together.

- We fixed an issue where there was a host filter count mismatch between CSV and XML formats of a report in the Report Information page.
- We fixed an issue so the Scanner users can now create Patch Report Templates using the API with asset_group ALL.
- We fixed an issue where SAML integration with certificates was not working properly. After the user logged in using SAML login, the final redirect URL was going to the standard login URL instead of the Certs login URL.
- For Host List Detection API, we fixed the list of supported values for output_format to include "CSV_NO_METADATA_MS_EXCEL" and "CSV_MS_EXCEL" and fixed the API documentation.
- We fixed the error message that appears when adding IPs in CIDR format ending with /32.
- We fixed an issue where a Warning appeared when adding IPs to the account as a subnet but the duplicate IPs were not listed.
- Fixed an issue where users got an error when creating asset tags from the Asset Search Report because of timeout request.
- When you view details for a Cisco or Checkpoint Firewall authentication record from the Authentication tab, the Record Type displayed in the UI was Unix. Now we'll show the record type as Cisco or Checkpoint Firewall instead of Unix.
- Now, the previously detected Information Gathered QIDs will not be removed as the result of a Host Alive scan.
- When configuring static routes for a scanner appliance, the target network mask must have values between 8 and 31 inclusive, but the error message had a typo as 0 to 31 inclusive, which caused confusion. This is now fixed.
- When activating PCI Compliance Service, the City and State values for the user's account are required and cannot be left empty.
- We fixed an issue with the Vulnerability Scorecard Report where customers saw different report data when they used the default scorecard report template vs. a copy of the template.
- Fixed an issue where some customers saw duplicate entries of IP 128.0.0.0 in VM reports for hosts that don't have a valid IP address. These will no longer appear.