Qualys Cloud Platform (VM, PC) v10.x

Release Notes

Version 10.8

February 22, 2021

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

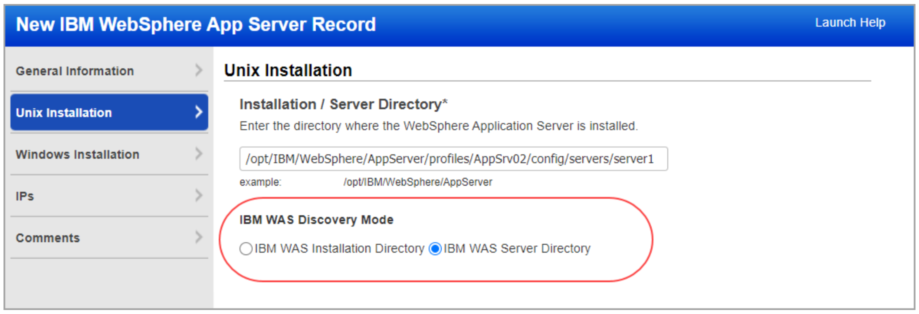
Qualys 10.8 brings you more improvements and updates! Learn more

Qualys Policy Compliance (PC/SCAP/SCA)

New IBM WAS Discovery Mode Option

When creating and updating IBM WebSphere App Server authentication records, you can now select the IBM WAS discovery mode (installation directory or server directory) for Unix installations. This lets you create custom authentication records for instances at the installation directory level or the server directory level, similar to system-created authentication records for IBM WebSphere App Server.

The new **IBM WAS Discovery Mode** option appears on the **Unix Installation** tab in the IBM WebSphere App Server authentication record. If you enter the installation directory path, then you'll want to select **IBM WAS Installation Directory**. If you enter the server directory path, then you'll want to select **IBM WAS Server Directory**. (Note that this option only applies to Unix. For Windows, the installation directory is supported.)



Unix Installation

Installation / Server Directory*
Enter the directory where the WebSphere Application Server is installed.
/opt/IBM/WebSphere/AppServer/profiles/AppSrv02/config/servers/server1
example: /opt/IBM/WebSphere/AppServer

IBM WAS Discovery Mode
○ IBM WAS Installation Directory ● IBM WAS Server Directory

Introducing SAP Hana Authentication

We now support SAP Hana authentication for compliance scans using Qualys PC or SCA. Simply create a SAP Hana authentication record with account login credentials, database information and target IPs.

Which technologies are supported?

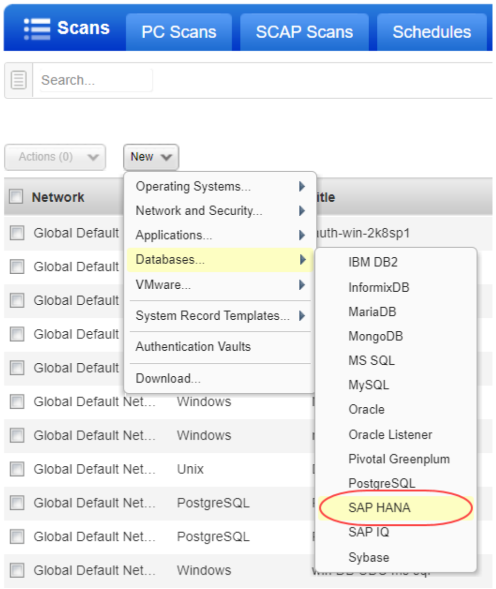
SAP Hana 2.x

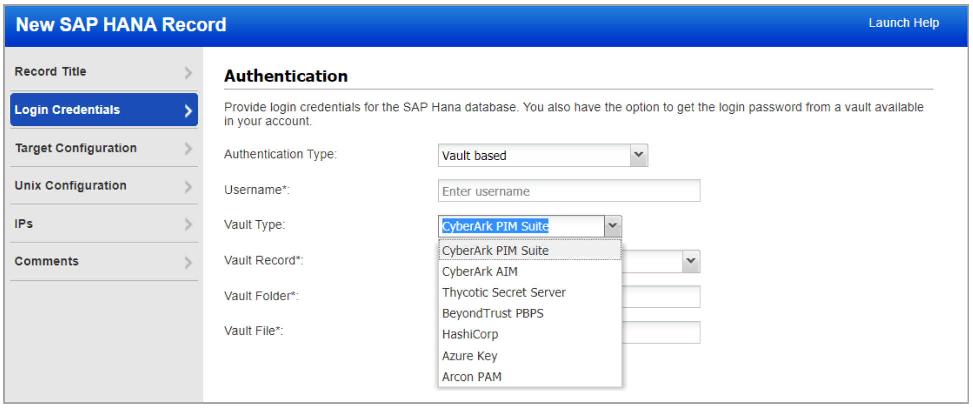
How do I get started?

Go to **Scans** > **Authentication**, and then go to **New** > **Databases** > **SAP HANA**.

Your SAP HANA Record

On the **Login Credentials** tab, enter the username and password (or select a password vault) for authenticating to the SAP Hana database.





Authentication

Provide login credentials for the SAP Hana database. You also have the option to get the login password from a vault available in your account.

Authentication Type: Vault based

Username*: Enter username

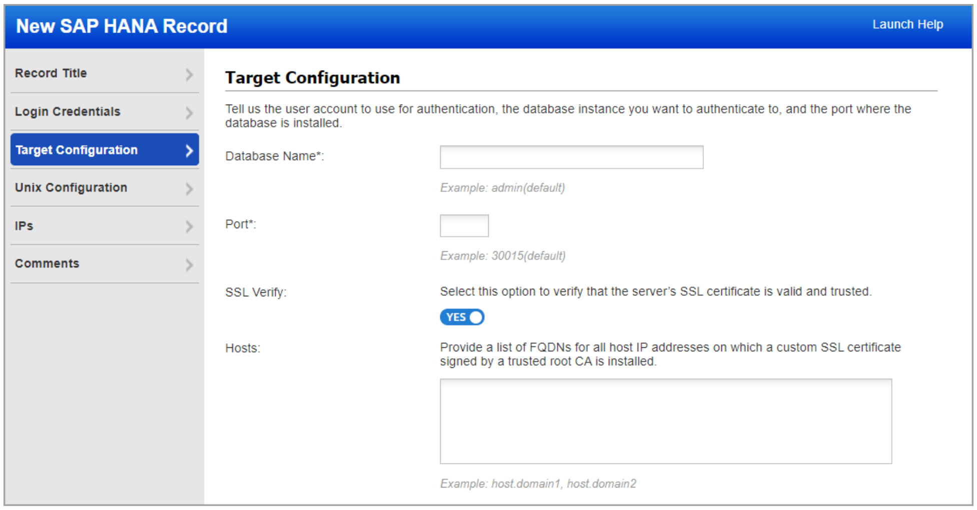
Vault Type: CyberArk PIM Suite

Vault Record*:

Vault Folder*:

Vault File*:

On the **Target Configuration** tab, tell us the database name to authenticate to and the port the database is running on. You'll also choose whether to perform a complete SSL certificate validation. This option is only valid for servers that support SSL.



Target Configuration

Tell us the user account to use for authentication, the database instance you want to authenticate to, and the port where the database is installed.

Database Name*:

Example: admin(default)

Port*:

Example: 30015(default)

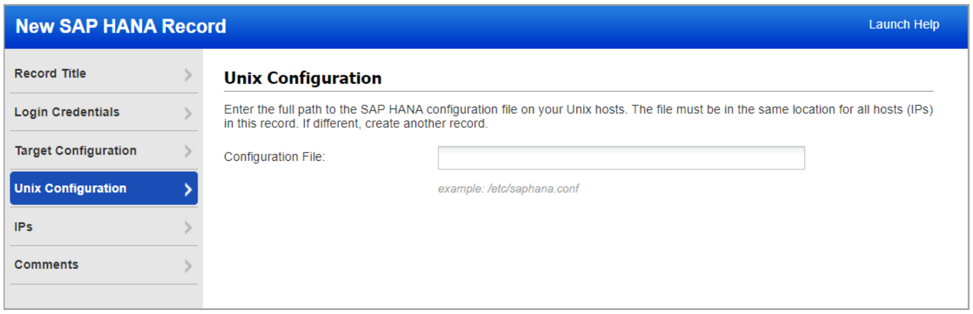
SSL Verify: Select this option to verify that the server's SSL certificate is valid and trusted.

YES

Hosts: Provide a list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.

Example: host.domain1, host.domain2

On the **Unix Configuration** tab, enter the full path to the SAP Hana configuration files on your Unix hosts. These files are accessed to run certain checks. Ensure that files are in the same location for all the hosts that you want scan.



Unix Configuration

Enter the full path to the SAP HANA configuration file on your Unix hosts. The file must be in the same location for all hosts (IPs) in this record. If different, create another record.

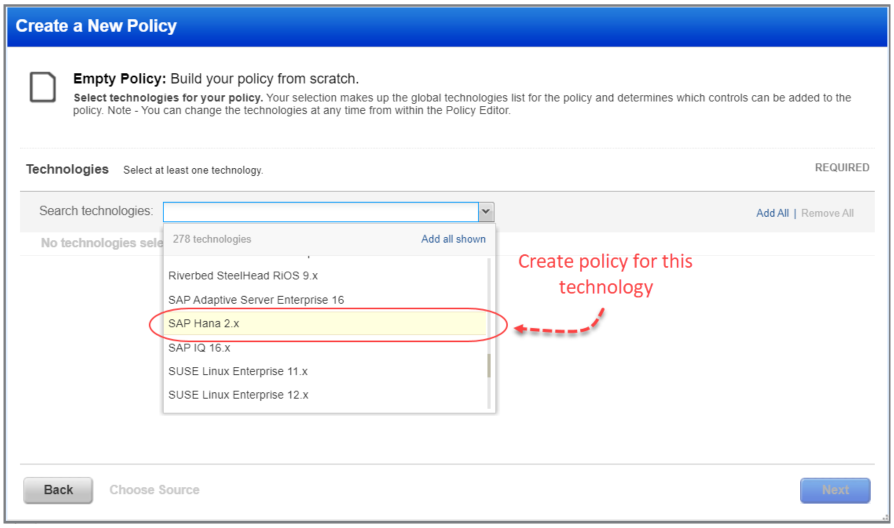
Configuration File:

example: /etc/saphana.conf

On the **IPs** tab, enter the IP addresses for the SAP Hana databases that the scanning engine should log into using the specified credentials.

Creating Policies

You'll see the SAP Hana 2.x technology listed when creating new policies.



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: Add All | Remove All

No technologies sele

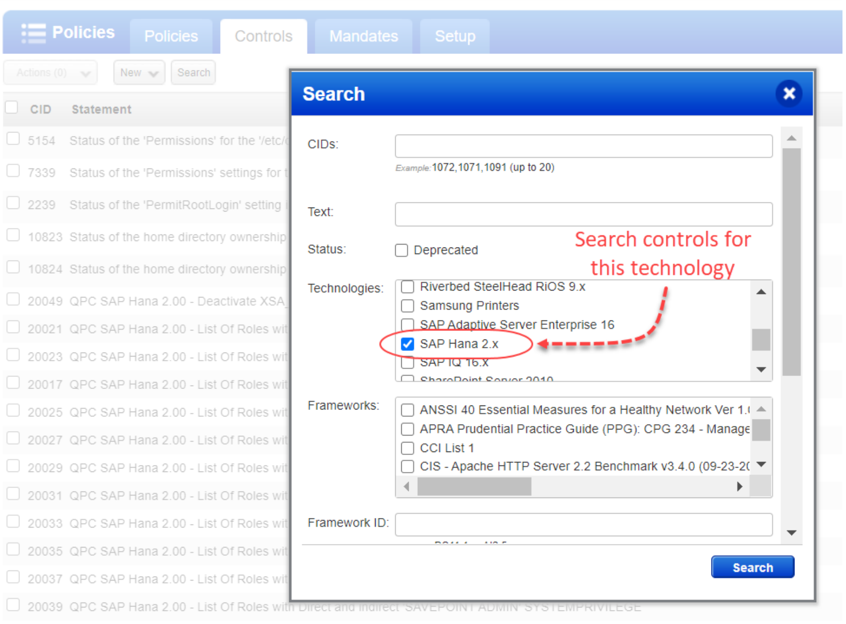
278 technologies Add all shown

- Riverbed SteelHead RiOS 9.x
- SAP Adaptive Server Enterprise 16
- SAP Hana 2.x
- SAP IQ 16.x
- SUSE Linux Enterprise 11.x
- SUSE Linux Enterprise 12.x

Create policy for this technology

Searching Controls

You'll also see SAP Hana 2.x when searching controls by technologies.



CID	Statement
5154	Status of the 'Permissions' for the '/etc/
7339	Status of the 'Permissions' settings for t
2239	Status of the 'PermitRootLogin' setting
10823	Status of the home directory ownership
10824	Status of the home directory ownership
20049	QPC SAP Hana 2.00 - Deactivate XSA_
20021	QPC SAP Hana 2.00 - List Of Roles wit
20023	QPC SAP Hana 2.00 - List Of Roles wit
20017	QPC SAP Hana 2.00 - List Of Roles wit
20025	QPC SAP Hana 2.00 - List Of Roles wit
20027	QPC SAP Hana 2.00 - List Of Roles wit
20029	QPC SAP Hana 2.00 - List Of Roles wit
20031	QPC SAP Hana 2.00 - List Of Roles wit
20033	QPC SAP Hana 2.00 - List Of Roles wit
20035	QPC SAP Hana 2.00 - List Of Roles wit
20037	QPC SAP Hana 2.00 - List Of Roles wit
20039	QPC SAP Hana 2.00 - List Of Roles with Direct and Indirect 'SAVEPOINT ADMIN' SYSTEMPRIVILEGE

Search

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

Text:

Status: □ Deprecated

Technologies:
- □ Riverbed SteelHead RiOS 9.x
- □ Samsung Printers
- □ SAP Adaptive Server Enterprise 16
- ☑ SAP Hana 2.x
- □ SAP IQ 16.x
- □ SharePoint Server 2010

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 v3.4.0 (09-23-2(

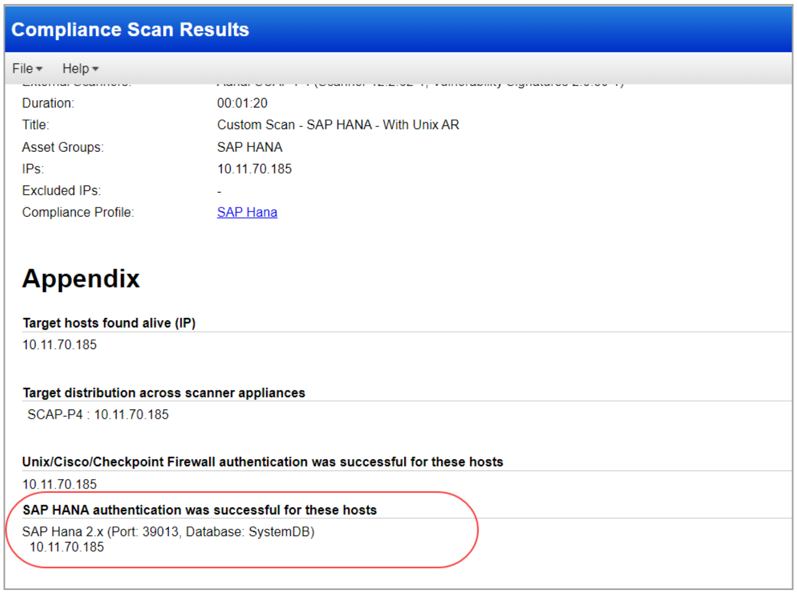
Framework ID:

Search controls for this technology

Sample Reports

The SAP HANA 2.x technology will appear in scan results and reports with instance information.

Compliance scan results



Duration:	00:01:20
Title:	Custom Scan - SAP HANA - With Unix AR
Asset Groups:	SAP HANA
IPs:	10.11.70.185
Excluded IPs:	-
Compliance Profile:	SAP Hana

Appendix

Target hosts found alive (IP)

10.11.70.185

Target distribution across scanner appliances

SCAP-P4 : 10.11.70.185

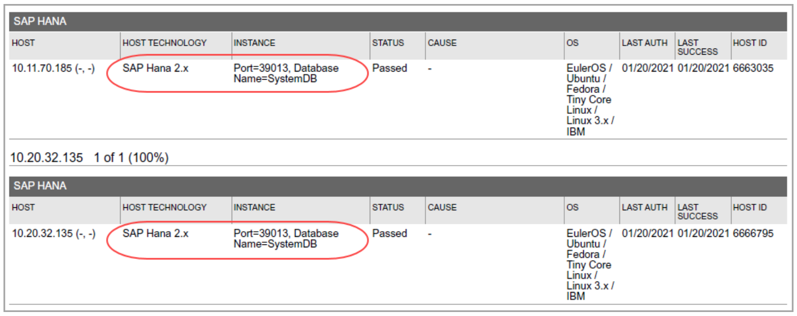
Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts

10.11.70.185

SAP HANA authentication was successful for these hosts

SAP Hana 2.x (Port: 39013, Database: SystemDB)
10.11.70.185

Authentication Report



SAP HANA

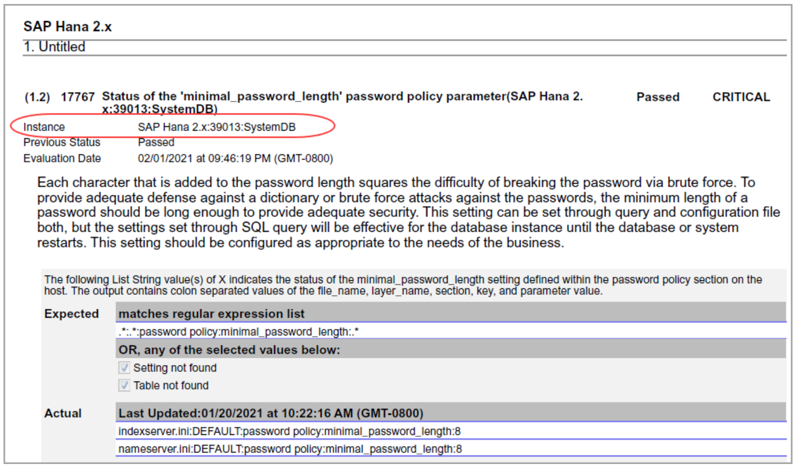
HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID
10.11.70.185 (-, -)	SAP Hana 2.x	Port=39013, Database Name=SystemDB	Passed	-	EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux 3.x / IBM	01/20/2021	01/20/2021	6663035

10.20.32.135 1 of 1 (100%)

SAP HANA

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS	HOST ID
10.20.32.135 (-, -)	SAP Hana 2.x	Port=39013, Database Name=SystemDB	Passed	-	EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux 3.x / IBM	01/20/2021	01/20/2021	6666795

Policy Report



SAP Hana 2.x

1. Untitled

(1.2) 17767 Status of the 'minimal_password_length' password policy parameter(SAP Hana 2.x:39013:SystemDB) Passed CRITICAL

Instance	SAP Hana 2.x:39013:SystemDB
Previous Status	Passed
Evaluation Date	02/01/2021 at 09:46:19 PM (GMT-0800)

Each character that is added to the password length squares the difficulty of breaking the password via brute force. To provide adequate defense against a dictionary or brute force attacks against the passwords, the minimum length of a password should be long enough to provide adequate security. This setting can be set through query and configuration file both, but the settings set through SQL query will be effective for the database instance until the database or system restarts. This setting should be configured as appropriate to the needs of the business.

The following List String value(s) of X indicates the status of the minimal_password_length setting defined within the password policy section on the host. The output contains colon separated values of the file_name, layer_name, section, key, and parameter value.

Expected **matches regular expression list**

.*:.*:password policy:minimal_password_length:.*

OR, any of the selected values below:

☑ Setting not found
☑ Table not found

Actual **Last Updated:01/20/2021 at 10:22:16 AM (GMT-0800)**

indexserver.ini:DEFAULT:password policy:minimal_password_length:8
nameserver.ini:DEFAULT:password policy:minimal_password_length:8

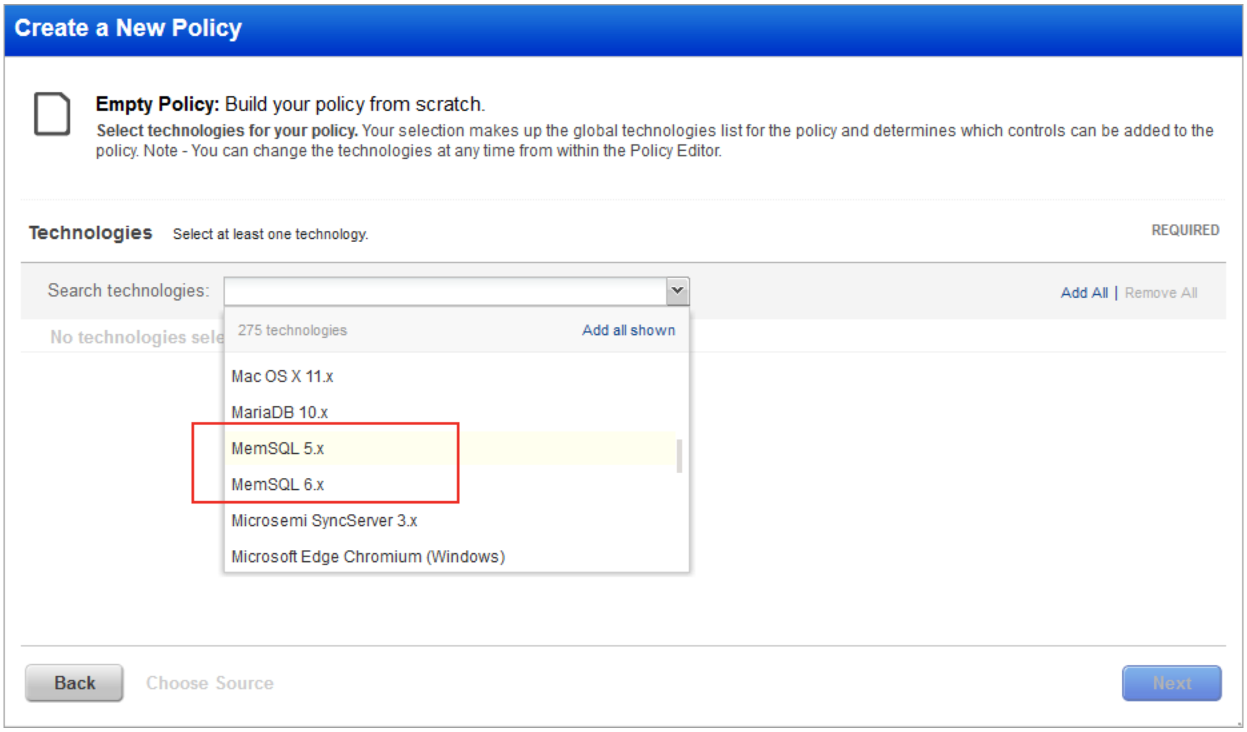
Support for OS Authentication-based Technology MemSQL (SingleStore) 5.x and MemSQL(SingleStore) 6.x

We've extended our support of OS authentication-based technologies to include MemSQL 5.x and MemSQL 6.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 for the hosts running MemSQL 5.x or MemSQL 6.x instances.

You can now include the MemSQL technology in your compliance policies and when searching controls. You'll also see MemSQL host instance information in Policy Compliance authentication reports, scan results, and policy reports.

Policy Editor

When you create or edit a compliance policy, MemSQL 5.x and MemSQL 6.x are now available in the list of supported technologies.



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: Add All | Remove All

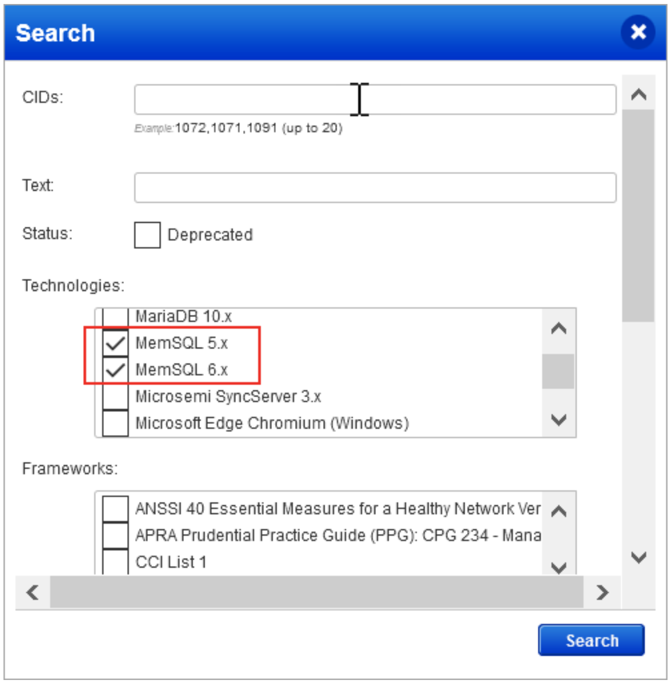
No technologies sele

275 technologies Add all shown

- Mac OS X 11.x
- MariaDB 10.x
- MemSQL 5.x
- MemSQL 6.x
- Microsemi SyncServer 3.x
- Microsoft Edge Chromium (Windows)

Search Controls

When you search controls, now you see MemSQL 5.x and MemSQL 6.x in the list of technologies. Go to Policies > Controls > Search, and select MemSQL 5.x and MemSQL 6.x in the list.



Search

CIDs:

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

Text:

Status: □ Deprecated

Technologies:

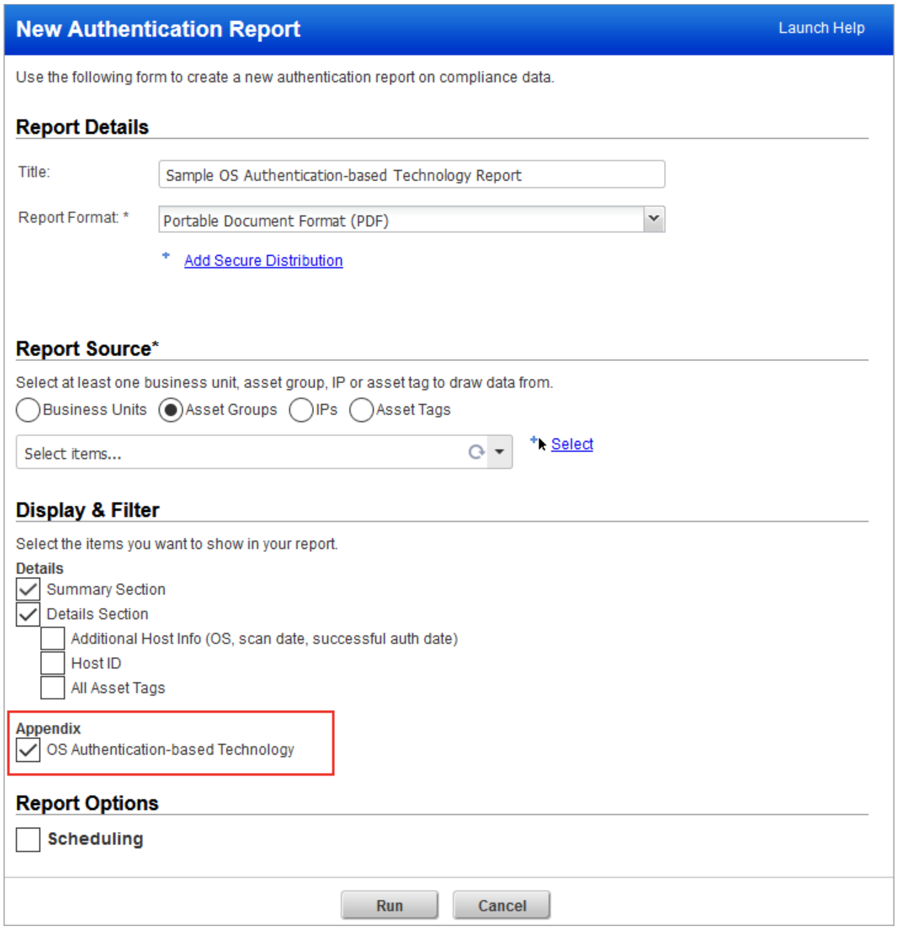
- □ MariaDB 10.x
- ☑ MemSQL 5.x
- ☑ MemSQL 6.x
- □ Microsemi SyncServer 3.x
- □ Microsoft Edge Chromium (Windows)

Frameworks:

- □ ANSSI 40 Essential Measures for a Healthy Network Ver
- □ APRA Prudential Practice Guide (PPG): CPG 234 - Mana
- □ CCI List 1

Authentication Reports

To display all OS auth-based instance technologies per host in your authentication report, go to Reports > Compliance Report > Authentication Report, and enable the OS Authentication-based Technology option under the Appendix.



New Authentication Report Launch Help

Use the following form to create a new authentication report on compliance data.

Report Details

Title:	Sample OS Authentication-based Technology Report
Report Format: *	Portable Document Format (PDF)

+ Add Secure Distribution

Report Source*

Select at least one business unit, asset group, IP or asset tag to draw data from.

○ Business Units ● Asset Groups ○ IPs ○ Asset Tags

Select items... Select

Display & Filter

Select the items you want to show in your report.

Details

- ☑ Summary Section
- ☑ Details Section
  - □ Additional Host Info (OS, scan date, successful auth date)
  - □ Host ID
  - □ All Asset Tags

Appendix

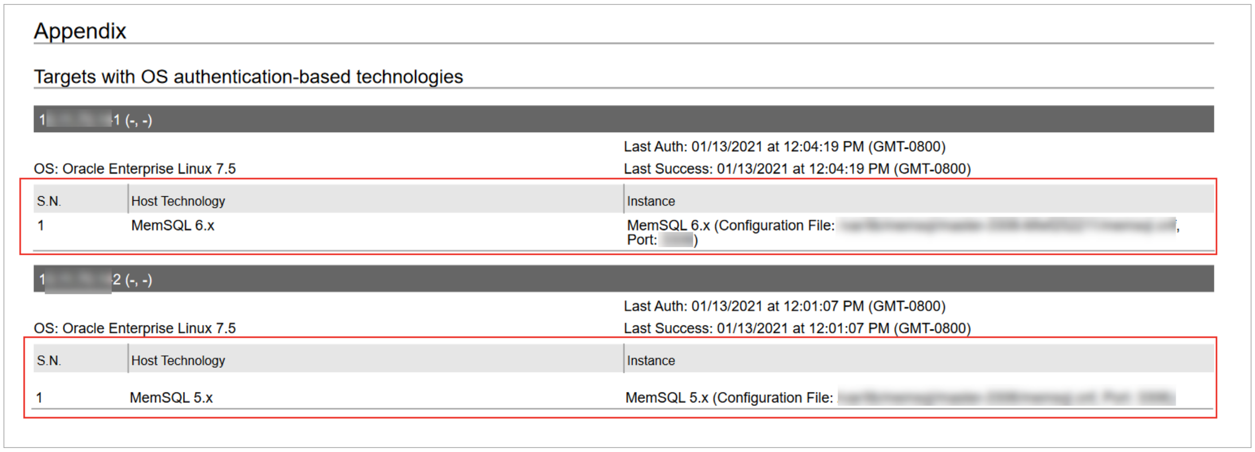
☑ OS Authentication-based Technology

Report Options

□ Scheduling

Run Cancel

Scroll down to the **Appendix** section of your authentication report to see **Targets with OS authentication-based technologies**.



Appendix

Targets with OS authentication-based technologies

1[redacted]1 (-, -)

OS: Oracle Enterprise Linux 7.5

Last Auth: 01/13/2021 at 12:04:19 PM (GMT-0800)
Last Success: 01/13/2021 at 12:04:19 PM (GMT-0800)

S.N.	Host Technology	Instance
1	MemSQL 6.x	MemSQL 6.x (Configuration File: [redacted], Port: [redacted])

1[redacted]2 (-, -)

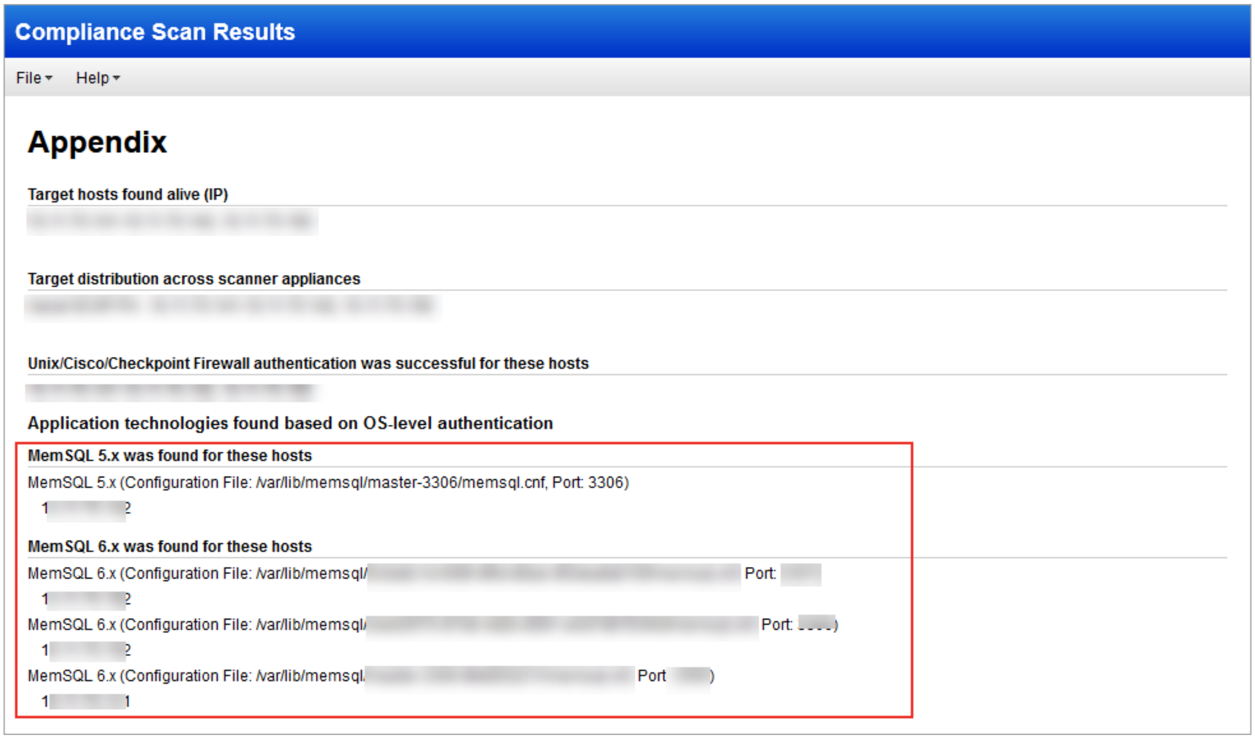
OS: Oracle Enterprise Linux 7.5

Last Auth: 01/13/2021 at 12:01:07 PM (GMT-0800)
Last Success: 01/13/2021 at 12:01:07 PM (GMT-0800)

S.N.	Host Technology	Instance
1	MemSQL 5.x	MemSQL 5.x (Configuration File: [redacted]

Scan Results

You see MemSQL 5.x and MemSQL 6.x listed under **Application technologies found based on OS-level authentication** in the **Appendix** section of a compliance scan result.



Appendix

Target hosts found alive (IP)

[redacted]

Target distribution across scanner appliances

[redacted]

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts

[redacted]

Application technologies found based on OS-level authentication

MemSQL 5.x was found for these hosts

MemSQL 5.x (Configuration File: /var/lib/memsql/master-3306/memsql.cnf, Port: 3306)

1[redacted]2

MemSQL 6.x was found for these hosts

MemSQL 6.x (Configuration File: /var/lib/memsql/[redacted] Port: [redacted]

1[redacted]2

MemSQL 6.x (Configuration File: /var/lib/memsql/[redacted] Port: [redacted])

1[redacted]2

MemSQL 6.x (Configuration File: /var/lib/memsql[redacted] Port [redacted])

1[redacted]1

Support for New OCA Technologies

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

- Arista 4.x
- Cisco IOS XR 6.x
- Cisco IOS XR 7.x
- Juniper JUNOS 15.x
- Juniper JUNOS 16.x
- Juniper JUNOS 17.x
- Juniper JUNOS 18.x
- Juniper JUNOS 19.x
- Juniper JUNOS 20.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 of the corresponding assets.

Qualys Cloud Platform

Deleting vCenter and ESXi Mapping Data

With this release, users can delete individual mapping records from the vCenter ESXi Mapping Data list. The existing ‘Purge’ feature allows users to delete all data while this new feature allows users to select the records they want to delete. This feature is applicable for VM and PC.

To accommodate this new feature, we’ve added:

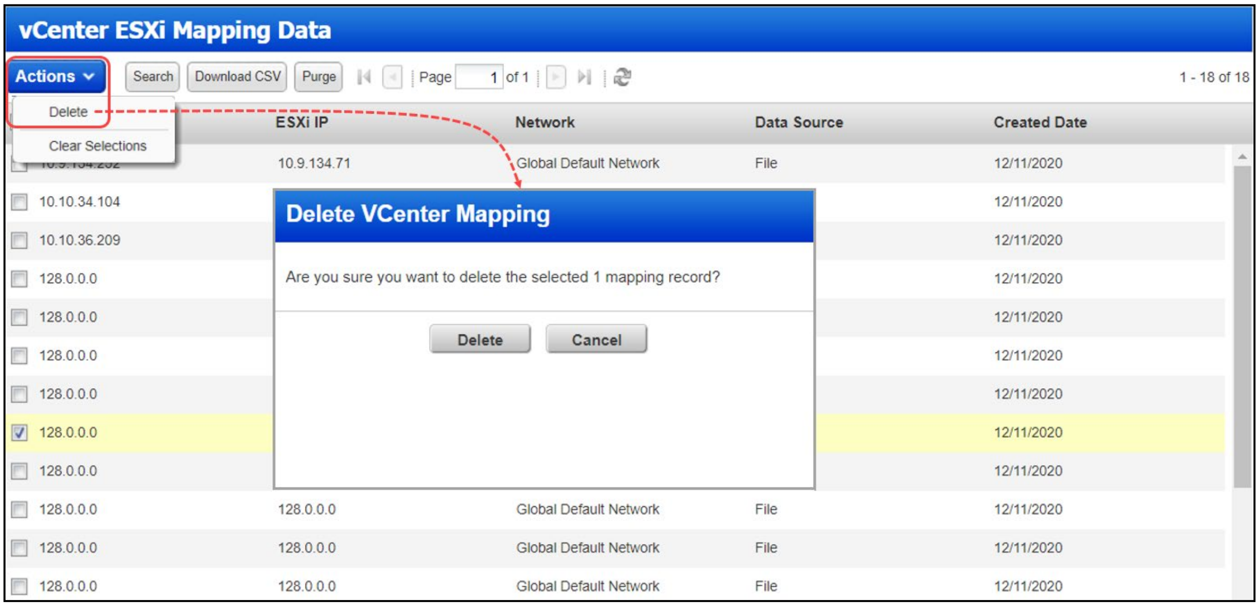
- **Actions** drop down with ‘Delete' and 'Clear' actions

- Check boxes are added to select the rows to be deleted

You can delete a maximum of 1000 records at a time.

What are the steps?

Go to **Scans** > **Authentication** > **New** > **VMware...** > **vCenter Mapping List**. Select the mapping records to be deleted, and choose **Delete** from **Actions** menu.



	ESXi IP	Network	Data Source	Created Date
□ [illegible]	10.9.134.71	Global Default Network	File	12/11/2020
□ 10.10.34.104				12/11/2020
□ 10.10.36.209				12/11/2020
□ 128.0.0.0				12/11/2020
□ 128.0.0.0				12/11/2020
□ 128.0.0.0				12/11/2020
□ 128.0.0.0				12/11/2020
☑ 128.0.0.0				12/11/2020
□ 128.0.0.0				12/11/2020
□ 128.0.0.0	128.0.0.0	Global Default Network	File	12/11/2020
□ 128.0.0.0	128.0.0.0	Global Default Network	File	12/11/2020
□ 128.0.0.0	128.0.0.0	Global Default Network	File	12/11/2020

Are you sure you want to delete the selected 1 mapping record?

Issues Addressed

- We fixed an issue where QIDs were getting fixed after launching a scan with the “Enable Host Alive Testing” option enabled in the option profile.
- We fixed an issue where the XML Patch Report was showing the incorrect VULN_TITLE for respective VULN_QID.
- Fixed an issue where /api/2.0/fo/scan/ API request was showing error code (999) with an improper error message. With this fix, you’ll see the proper error code and error message.
- We fixed an issue where while scanning any asset, if the user was specifying multiple FQDN values as targets with space, comma, or newline characters, then VM was skipping the FQDN values that were appearing after space, comma, or newline characters. Now after the fix, when the scan is launched on FQDN values, VM picks all the values that appear after space, comma, or newline characters.
- We fixed an issue where daily trouble ticket email notifications were displaying zero value for the total tickets owned by the user in some cases. Now, after the fix, the notifications are displaying the correct number of tickets for the total tickets owned by the user.
- We have fixed a typographical error in one of the options for the Status field in the Middleware search.
- The Unit Manager can now edit GUI and API values of his sub-users (depending on the Unit Manager’s own GUI and API permissions.)
- We have fixed an issue where the patch report generated using template for the combination of IP address and tags displayed blank. Now, the patch report is generated with correct data.
- We fixed an issue where the Help > About page was not showing the latest Vulnerability Signature Version in some cases.
- In Japanese locale, in the SCA and PC modules, English Help was launched instead of Japanese Help. We’ve fixed this localization issue.
- Updated User API documentation to remove the ui_interface_style input parameter which has been deprecated.
- We’ve added sample queries for Sybase and SAP IQ user-defined controls (UDCs) to the online help.
- For the Host List Detection API, we fixed the description for the output_format parameter by removing the CSV_MS_EXCEL_NO_METADATA value, which is not supported.
- We made improvements to the CyberArk AIM Integration document to clarify that only Allowed Machines authentication method is supported.
- We have rectified and updated description of “output_format” and “show_attributes” parameters for Asset Group List in VM/PC API User Guide and API online help.