Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.18

March 11, 2019

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

Qualys Vulnerability Management (VM)

Launch Cloud CertView Vulnerability Scan for EC2 Assets
Support for New Authentication Types to Filter Vulnerabilities

Qualys Policy Compliance (PC/SCA)

Support for InformixDB Authentication
IBM WebSphere Application Server 9.x Support
PostgreSQL 10.x Support

Qualys 8.18 brings you many more improvements and updates! **Learn more**

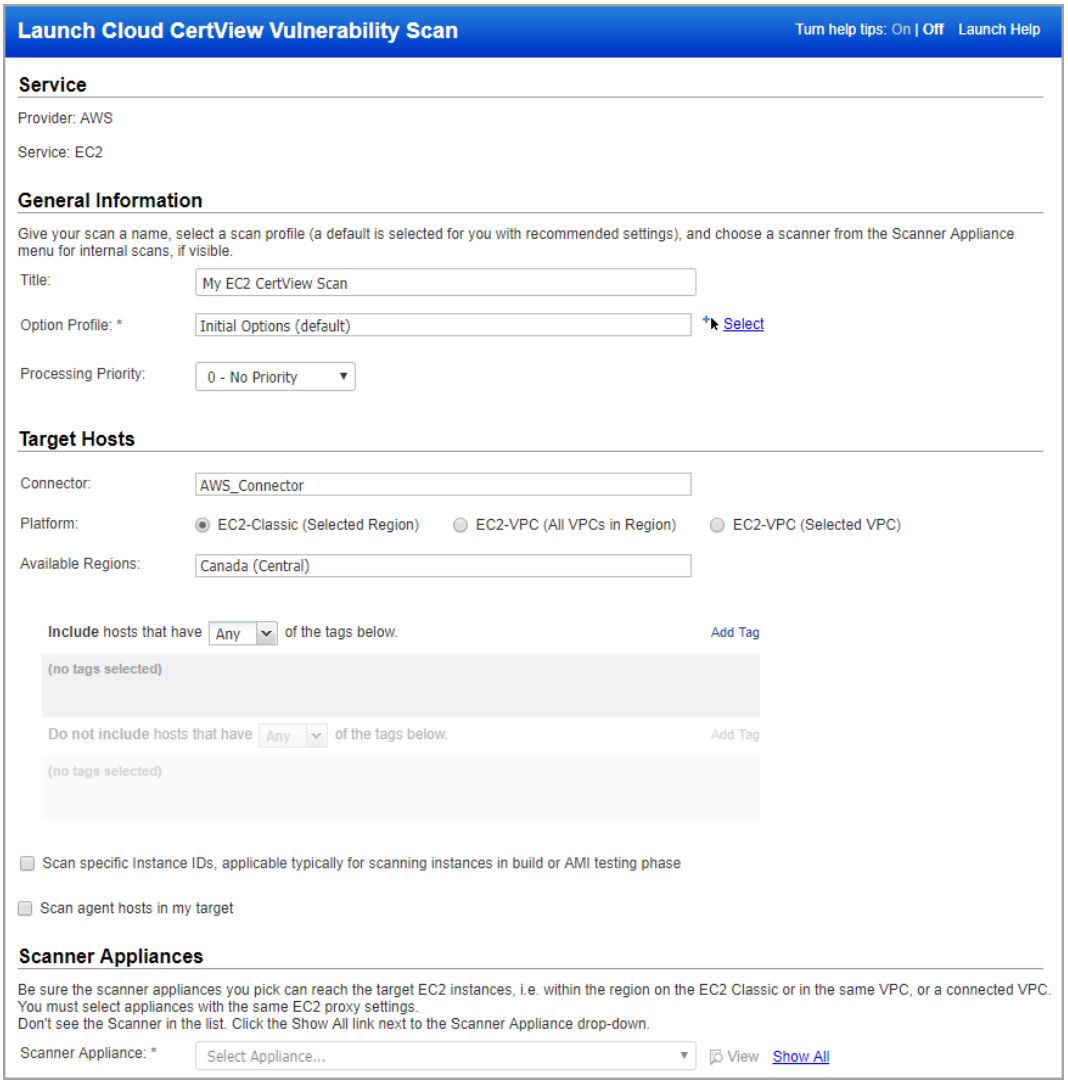
Qualys Vulnerability Management (VM)

Launch Cloud CertView Vulnerability Scan for EC2 Assets

You can now launch Cloud CertView scans and start getting up to date view on your certificates and security posture for your AWS EC2 hosts using Qualys Certificate View!

Before you launch Cloud CertView scans you must activate EC2 Assets for CertView Scanning. Once you create an EC2 connecter in AssetView, EC2 assets will be activated automatically to scan CertView Scanning application.

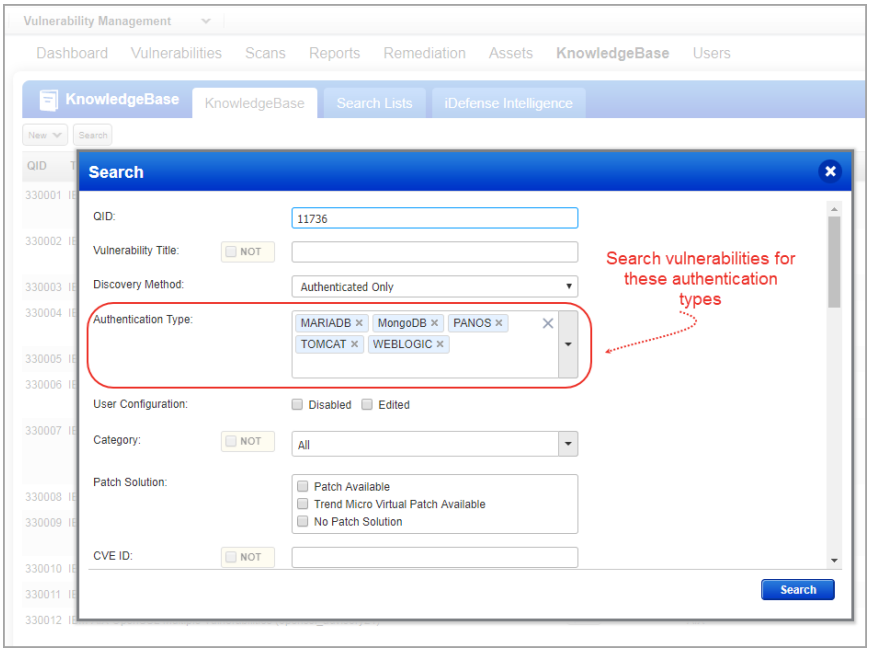
Simply got to VM and navigate to Scans > Scans > New > Cloud CertView Scan and provide setup the scan options and launch the scan.



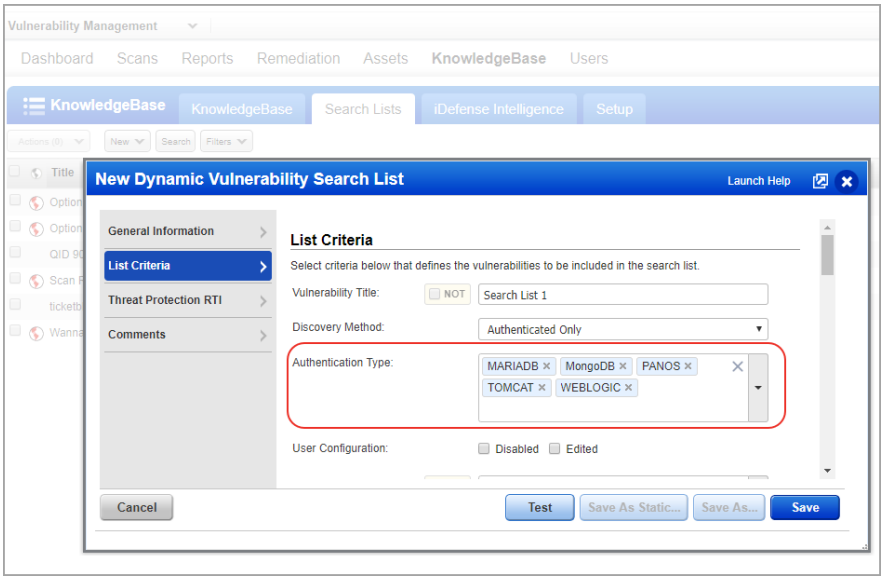
Support for New Authentication Types to Filter Vulnerabilities

Now you can also search in our KnowledgeBase for vulnerabilities that are under authenticated only/remote and authenticated categories with authentication types set as TOMCAT, MARIADB, MongoDB, WebLogic and PANOS. To filter such vulnerabilities we have added the following new authentication types: TOMCAT, MARIADB, MongoDB, WebLogic, PANOS for "Remote and Authenticated" and "Authenticated Only" discovery methods. These authentication types are also available when creating dynamic search lists.

Search for vulnerabilities in KnowledgeBase using the new authentication types.



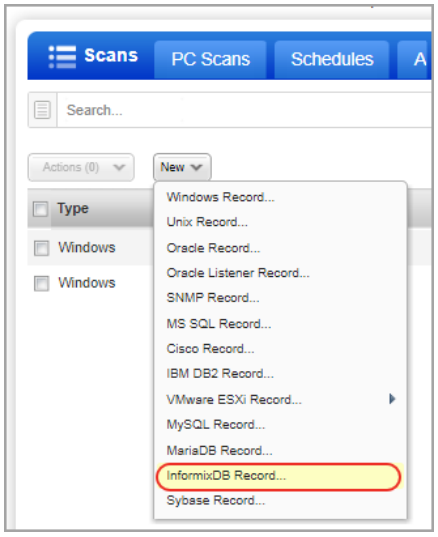
Create dynamic search lists using the new authentication types.



Qualys Policy Compliance (PC/SCA)

Support for InformixDB Authentication

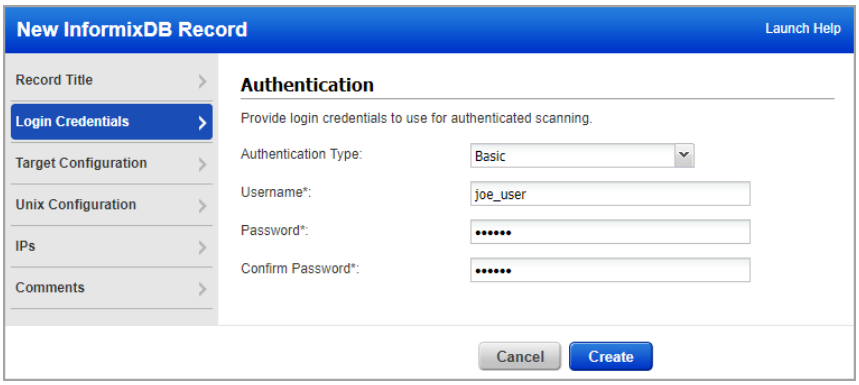
We now support InformixDB authentication for compliance scans using Qualys app PC and SCA. Simply create a InformixDB authentication record with details about your credentials to authenticate to a InformixDB database instance running on a host, and scan it for compliance. We are supporting authentication record creation only for InformixDB installed on Unix.



How do I get started?

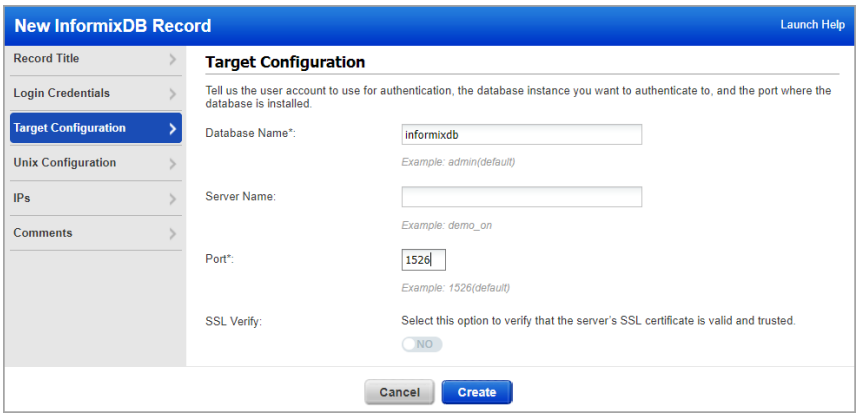
Go to Scans> Authentication, and choose New> InformixDB Record (as shown on the right).

Your InformixDB authentication record



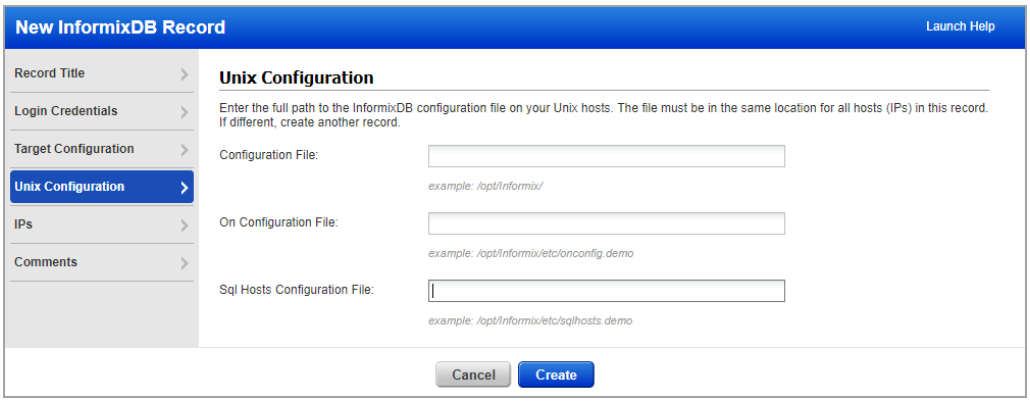
Each InformixDB record identifies account login credentials, database information and target hosts (IPs). Provide basic login credentials (username and password) to be used for authentication.

Note that you must have an Unix record containing the IPs assigned to this record.



Tell us the database name to authenticate to and the port the database is running on. We provide default settings for both, but these may be customized. Use SSL Verify option to specify FQDNs of server hosts that use SSL for authentication.

Enter the full path to the InformixDB 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.



IBM WebSphere Application Server 9.x Support

We've extended our support for IBM WebSphere App Server authentication to include WebSphere Application Server 9.x for Unix. (See the help for other supported technologies.)

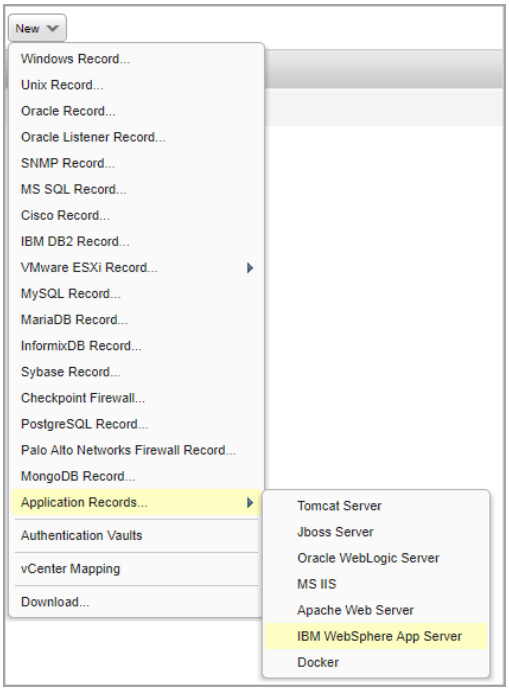
You'll need a IBM WebSphere App Server authentication record to authenticate to your web server, and scan it for compliance. You'll also need a Unix record for the host running the web server.

How do I get started?

- Go to Scans > Authentication.

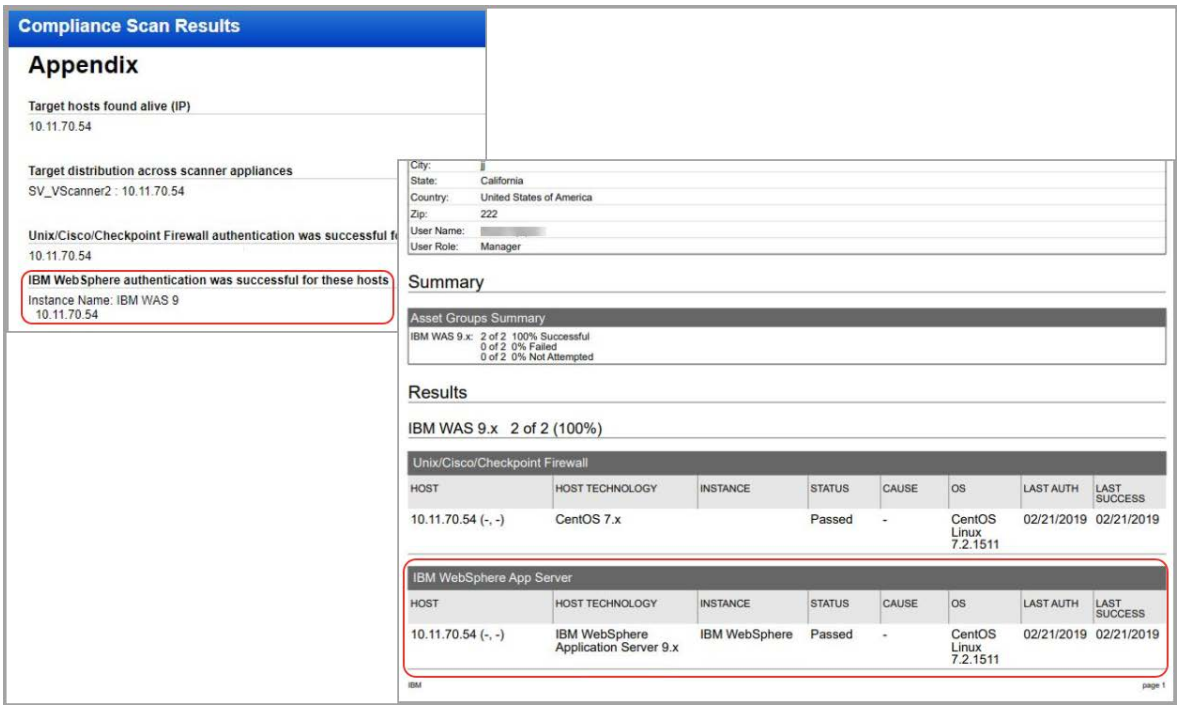
- Check that you already have a Unix record defined for each host running the web server.

- Create a WebSphere App Server record for the same host. Go to New > Application Records > IBM WebSphere App Server.



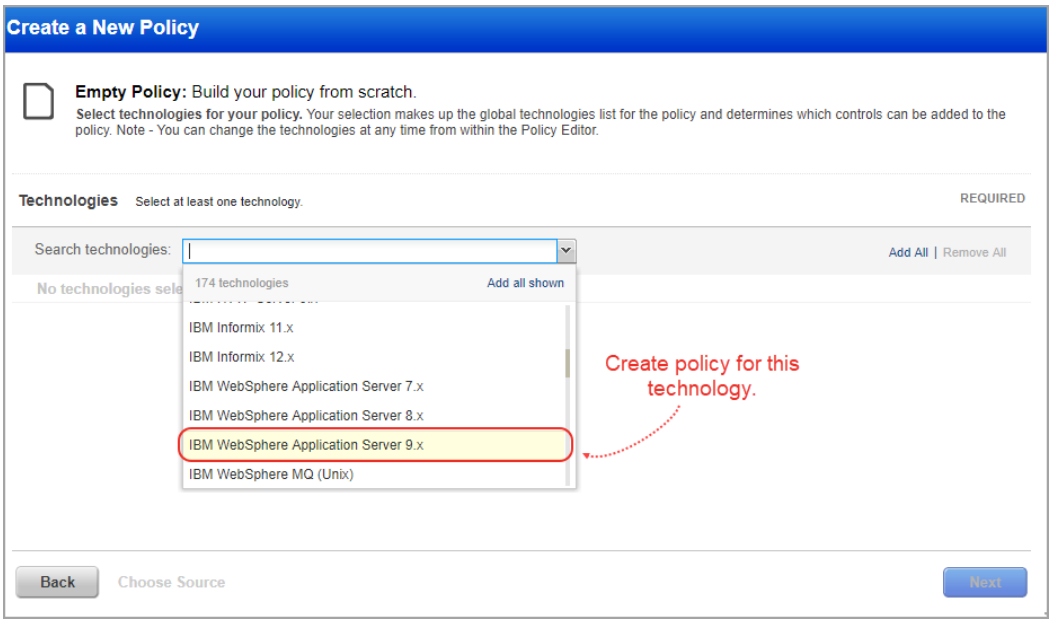
Sample Reports

You'll see IBM WebSphere App Server 9.x instances in compliance scan results and reports.



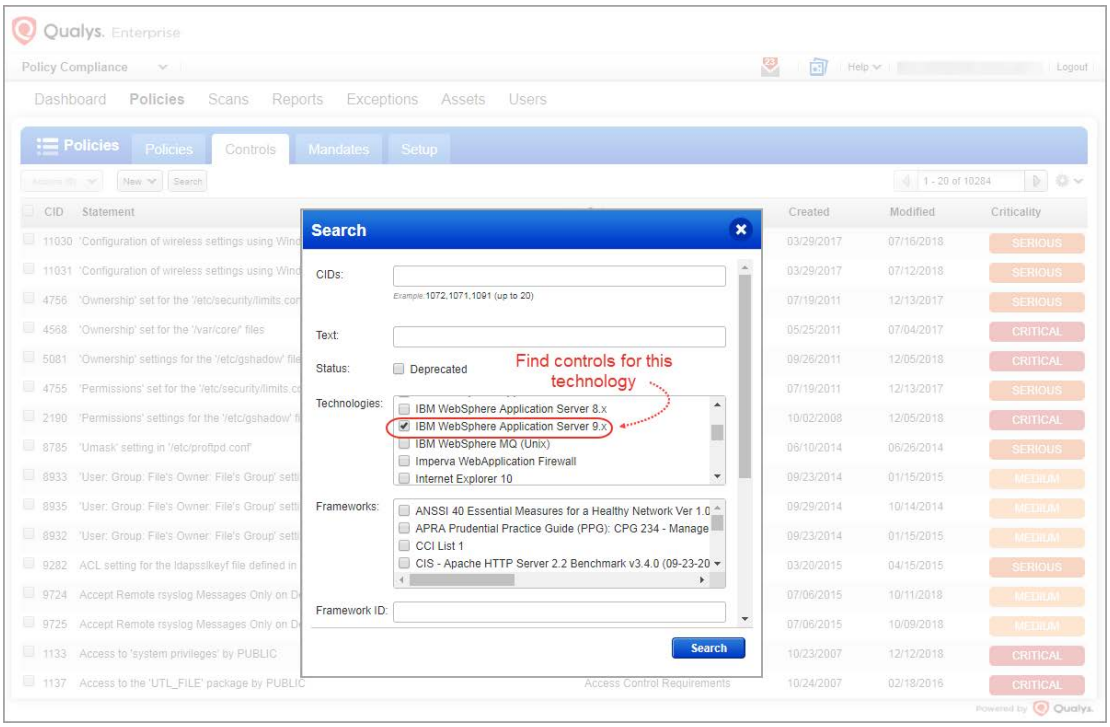
Policies and Controls

You'll also see IBM WebSphere Application Server 9.x in the technologies list when creating a new policy.



Search Controls

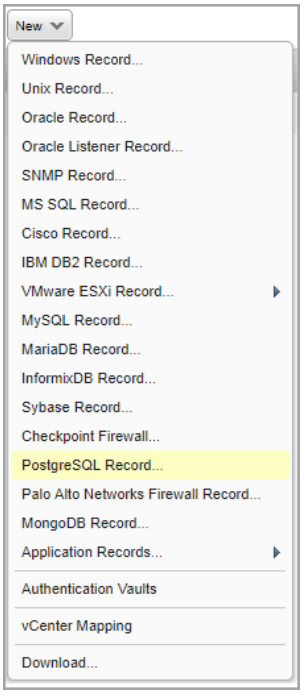
You'll see IBM WebSphere Application Server 9.x when searching controls by technologies.



PostgreSQL 10.x Support

We've extended our support for PostgreSQL database authentication to include PostgreSQL 10.x for Unix. (See the help for other supported technologies.)

You'll need a PostgreSQL authentication record to authenticate to your web server, and scan it for compliance. You'll also need a Unix record for the host running the web server.



How do I get started?

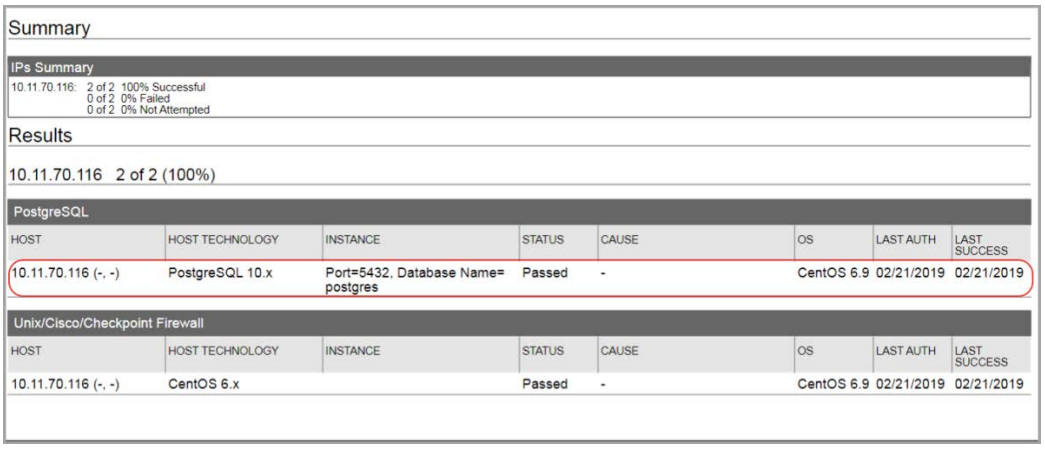
- Go to Scans > Authentication.

- Check that you already have a Unix record defined for each host running the web server.

- Create a PostgreSQL record for the same host. Go to New > Application Records > PostgreSQL Record.

Sample Reports

You'll see PostgreSQL database instances in compliance scan results and reports.



Summary

IPs Summary

10.11.70.116: 2 of 2 100% Successful
0 of 2 0% Failed
0 of 2 0% Not Attempted

Results

10.11.70.116 2 of 2 (100%)

PostgreSQL

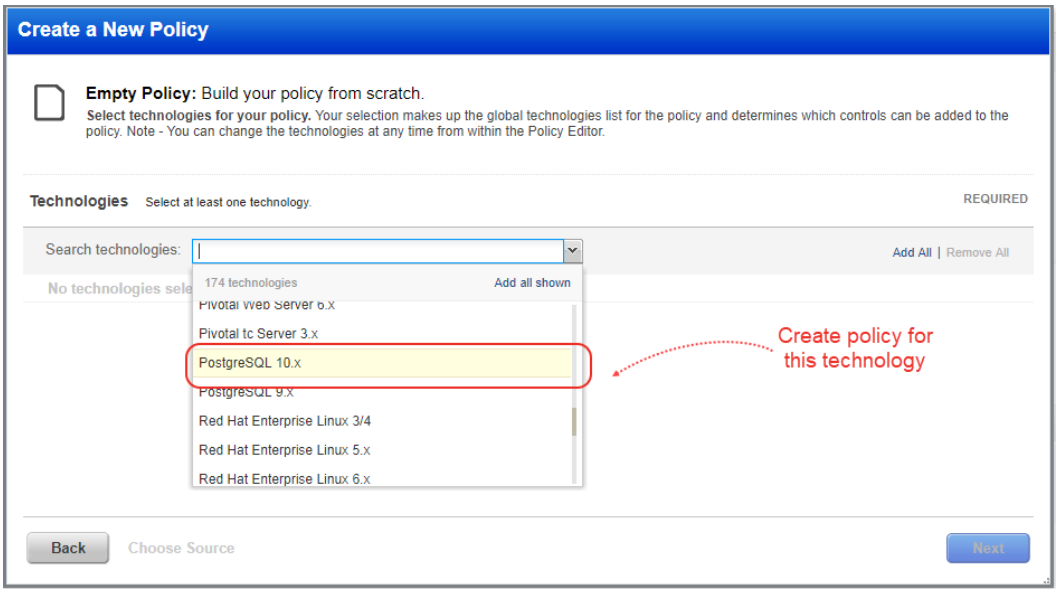
HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
10.11.70.116 (-, -)	PostgreSQL 10.x	Port=5432, Database Name=postgres	Passed	-	CentOS 6.9	02/21/2019	02/21/2019

Unix/Cisco/Checkpoint Firewall

HOST	HOST TECHNOLOGY	INSTANCE	STATUS	CAUSE	OS	LAST AUTH	LAST SUCCESS
10.11.70.116 (-, -)	CentOS 6.x		Passed	-	CentOS 6.9	02/21/2019	02/21/2019

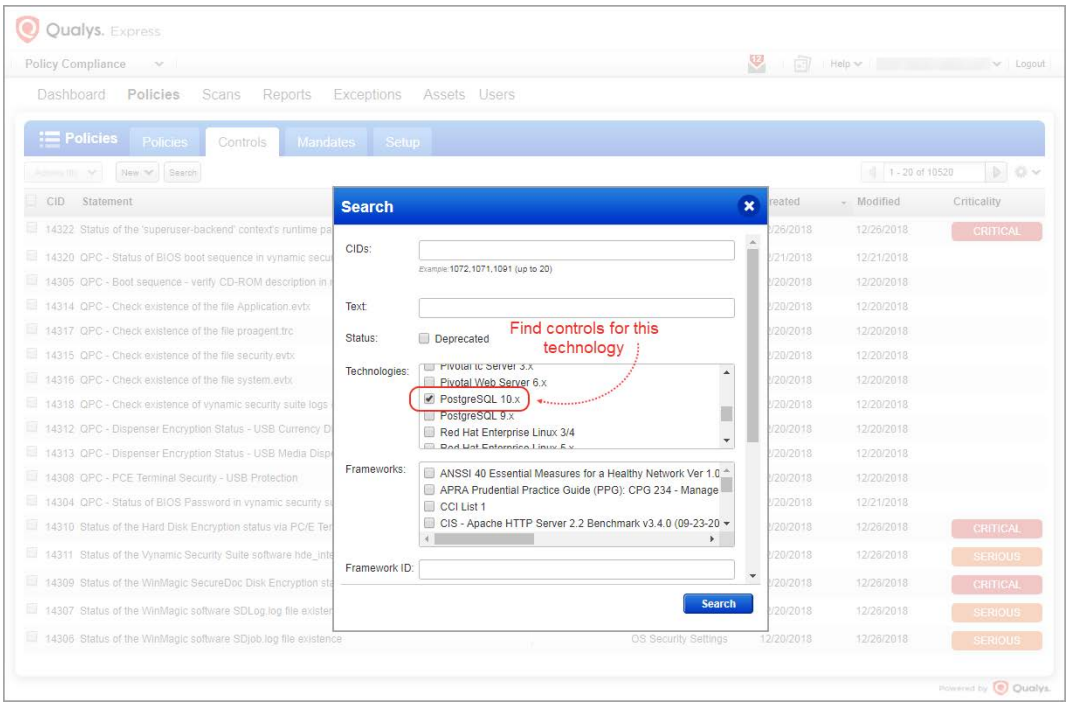
Policies and Controls

You'll also see PostgreSQL 10.x in the technologies list when creating a new policy.



Search Controls

You'll see PostgreSQL 10.x when searching controls by technologies.



Issues Addressed

- We have fixed an issue where the Scorecard Report was not showing scan results for Agent Tracked Assets even if the tag used in the scan has Agent Tracked Assets. Now Scorecard Report shows scan data for Agent Tracked Assets when a scan is run on a tag that also has Agent Tracked Assets.
- When uploading vCenter – ESXi mappings (under Scans > Authentication), the user can upload a CSV file with the column header as vCenter IP.
- The issue of run history data not available for the scheduled reports is fixed. Now the Run History tab on the Scheduled Task Information screen shows the run history data.
- The Service Now user when connecting to Qualys Cloud Platform was getting an error "The account does not have Service Now integration feature enabled". This issue is fixed and the user will able to connect to the Qualys Cloud Platform.
- We have fixed an issue where the compliance report was showing control status as failed for inactive controls. This issue is fixed by showing only active controls data for policy summary and Policy Compliance dashboard.
- We have fixed an issue where the new customers were not navigated to the Vulnerability Management module when changing the module to VM. This issue was due to an error in calculating a condition which was returning an incorrect value that showed that the new customer account did not have permission to access VM.
- We have fixed an issue where multiple Tomcat instances were not detected on Windows 2012 during authenticated PC scan. Now if we have multiple Tomcat authentication record for instances running on the single node and different installation path/directory, these instances are now getting detected and come in compliance scan report.
- We now correctly display summary of Added/Removed/Modified files or directories in a Policy Editor.
- We now display correct information about the QIDs excluded for the scan in Host information of the Vulnerabilities Tab in AssetView.
- We have now fixed the issue so that the cancel and pause feature for Cloud Perimeter scan functions correctly. Previously, it was adding cancel and pause time to the next schedule date instead of current schedule date, making it pause and cancel at incorrect time.
- The Posture API request with tag_set_include filter now returns correct posture information on hosts for specified tag names/id.
- We have now fixed the issue to correctly display list of SCAP Enabled Scanners during Launch and/or Scheduling SCAP Scan.
- We have now fixed the asset tag palette so that on clicking any parent Asset tag the child tags are now displayed properly.
- We updated the screen text that appears below the support options on the Help > Contact Support page.
- We have updated the online help and added information about Certificates.
- We have fixed an issue in the API Quick Reference guide where the Scan API (/api/2.0/fo/scan) has a couple of options missing for the output_format parameter. We have added the missing parameters: csv_extended | json_extended in the guide.

- We have now updated the Qualys API User Guide (VM, PC) with correct example for API /msp/report_template_list.php.
- We have updated the Windows Authentication document to reflect registry related information on page 15 in “Agentless tracking”.