Qualys Cloud Platform (VM, PC) v8.x

Release Notes

Version 8.22.2
March 16, 2020

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

Qualys Policy Compliance (PC)

Pivotal Greenplum Authentication Support

Microsoft SharePoint Authentication Support

PostgreSQL Support for Windows

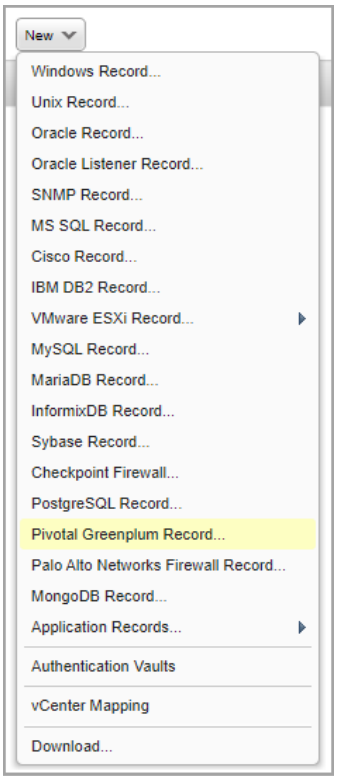
PostgreSQL 12.x Support for Unix

Microsoft SQL Server 2019 Support

Qualys 8.22.2 brings you more improvements and updates! Learn more

Qualys Policy Compliance (PC)

Pivotal Greenplum Authentication Support



We now support Pivotal Greenplum authentication for compliance scans on Unix hosts. Authentication is supported for Greenplum versions 5.x and 6.x.

You'll need a Pivotal Greenplum authentication record to authenticate to a Pivotal Greenplum database instance running on a Unix host, and scan it for compliance.

How do I get started?

Go to Scans > Authentication, then New > Pivotal Greenplum Record.

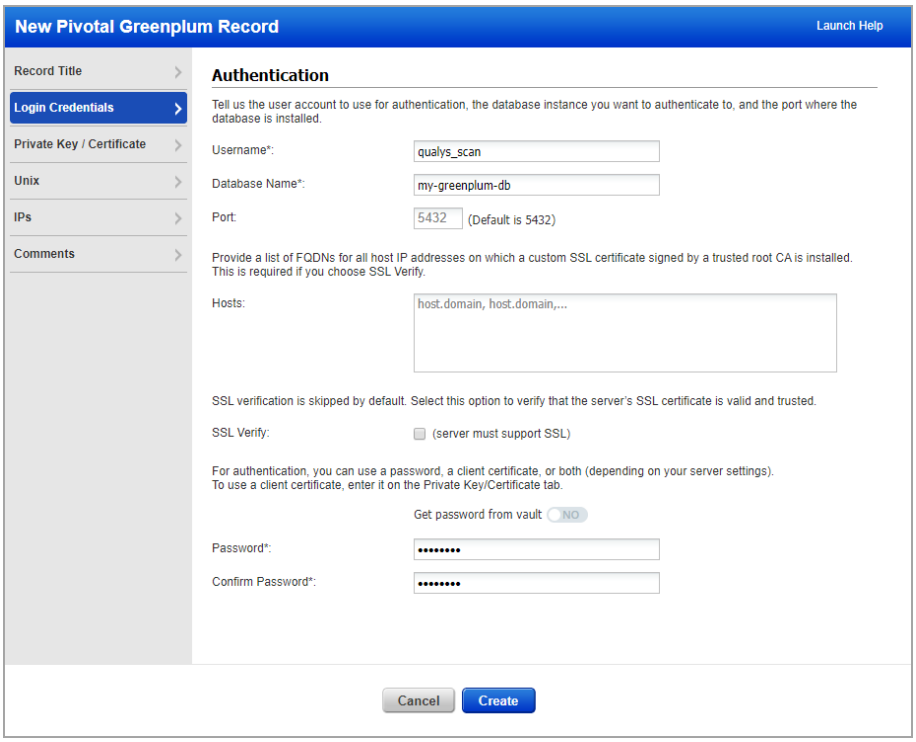
Pivotal Greenplum Record

In the record, you'll need to tell us the user account to be used for authentication, the database instance to authenticate to, and the port where the database is installed.

The type of authentication method you use depends on your server settings and how you've configured client authentication.

You can use:

- a password (enter it on the Login Credentials tab or get it from a password vault),
- a client certificate (enter it on the Private Key / Certificate tab),
- a password AND client certificate (enter values on both tabs).



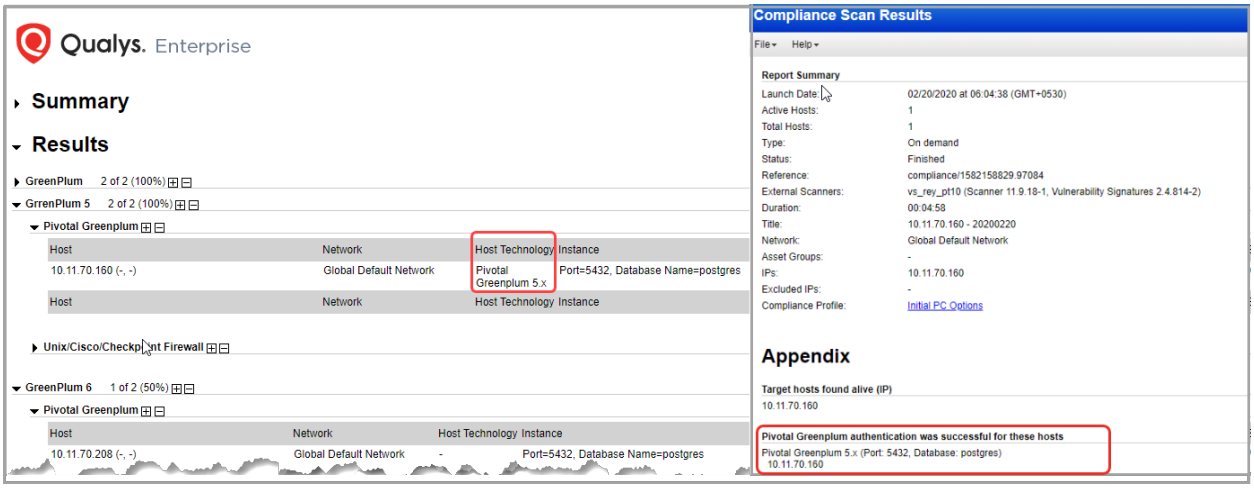
Unix installation

If you want to perform OS-dependent compliance checks, you'll need to tell us where the PostgreSQL configuration file is located on your Unix hosts. Unix authentication is required for these types of checks, so you'll need a Unix record for the same hosts in this record.

Note that the configuration file must be in the same location on all hosts (IPs) in the record. If the file is in a different location for some, then create additional Pivotal Greenplum records.

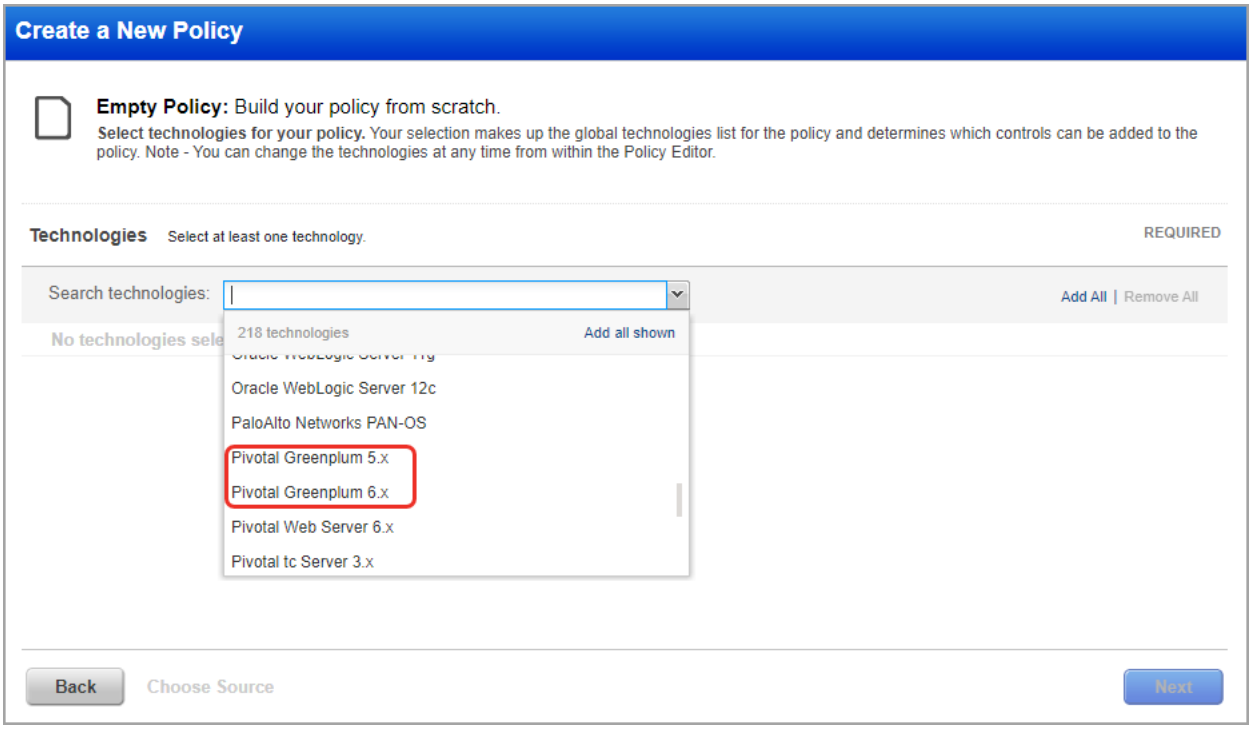
Sample Reports

You'll see the Pivotal Greenplum technology in authentication reports and in compliance scan results. Check out these samples.

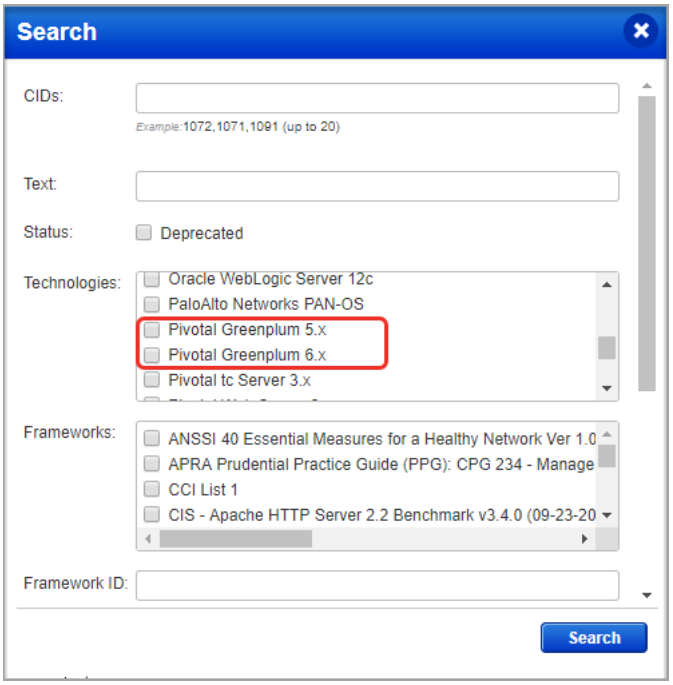


Policies and Controls

You'll see Pivotal Greenplum 5.x and 6.x in the technologies list when creating a new policy.

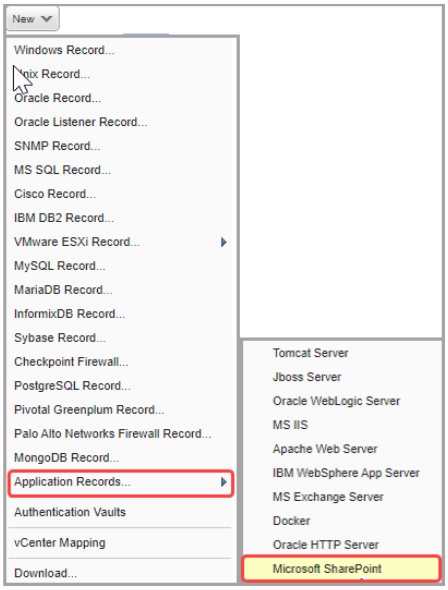


You'll see Pivotal Greenplum 5.x and 6.x when searching controls by technologies.



Microsoft SharePoint Authentication Support

We now support Microsoft SharePoint authentication for compliance scans. Authentication is supported for SharePoint versions 2010, 2013, 2016, and 2019.



Windows authentication is required so you'll also need a Windows record for the host running Microsoft SharePoint. The Microsoft SharePoint record type is only available in accounts with PC or SCA and is only supported for compliance scans.

SharePoint instance will be auto discovered through the Windows Authentication Record. To connect to the MS SQL server, you'll need to provide information under MS SQL Login credentials in Microsoft SharePoint Record.

Which technologies are supported?

We've added support for Microsoft SharePoint 2010, 2013, 2016, 2019 authentication for compliance scans.

How do I get started?

- Go to Scans > Authentication.

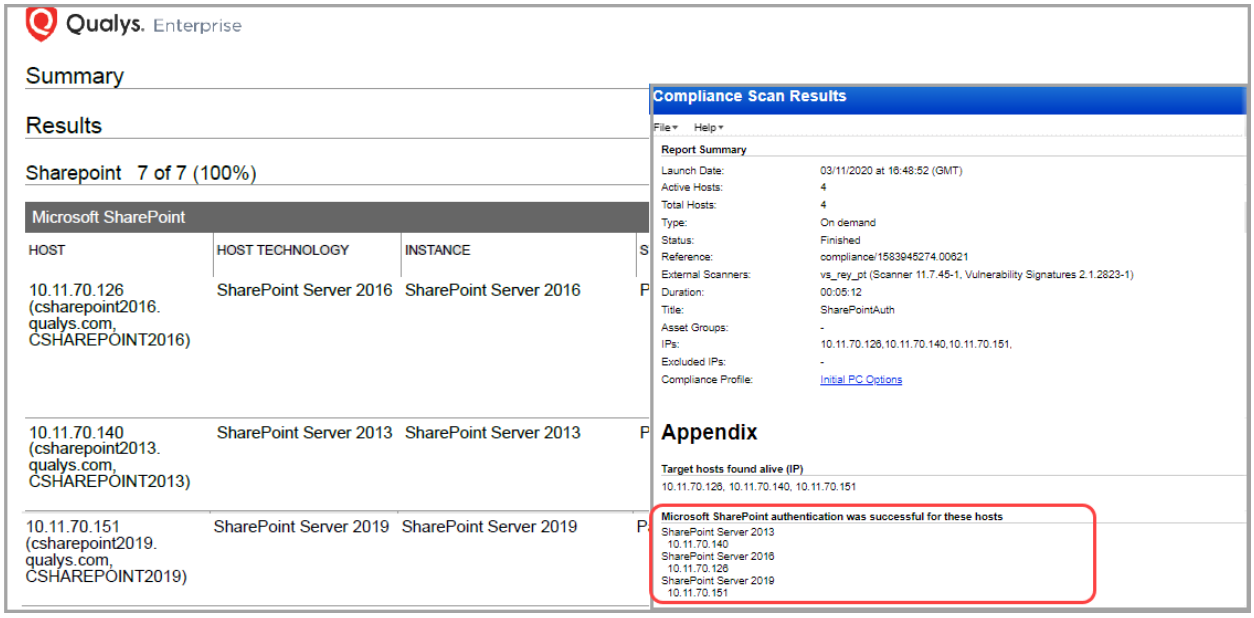
- Check that you have a Windows record already defined for the host running SharePoint.

- Create a Microsoft SharePoint record for the same host. Go to New > Application Records > Microsoft SharePoint.

Sample Reports

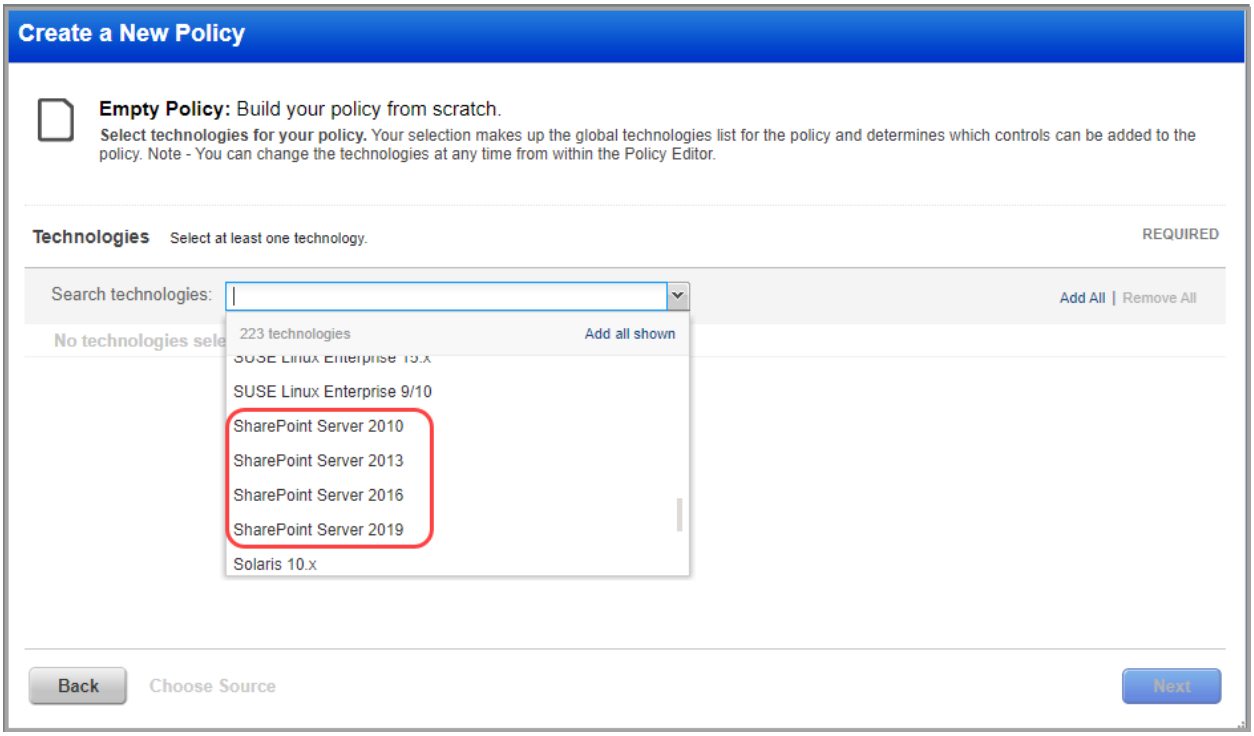
You'll see the Microsoft SharePoint technology in authentication reports and in compliance scan results.

Check out these samples:

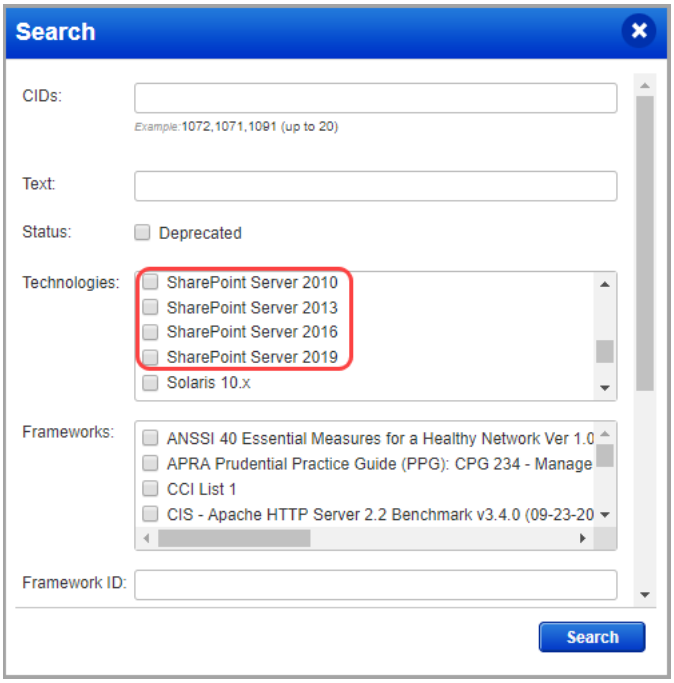


Policies and Controls

You'll see SharePoint Server in the technologies list when creating a new policy.



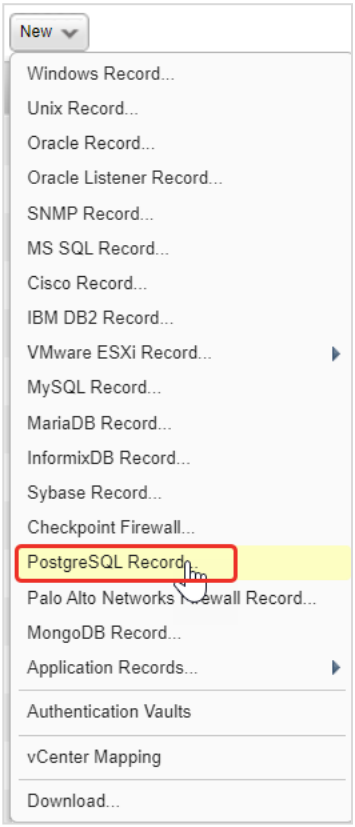
You'll see SharePoint Server 2010, 2013, 2016, and 2019 when searching controls by technologies.



PostgreSQL Support for Windows

We've extended our support for PostgreSQL authentication to include PostgreSQL Windows hosts. We already support PostgreSQL on Unix hosts.

You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a Windows host, and scan it for compliance. Windows authentication is required so you'll also need a 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.



Which technologies are supported?

We've added support for PostgreSQL 9.x, PostgreSQL 10.x, PostgreSQL 11.x and PostgreSQL 12.x authentication for compliance scans on Windows hosts.

How do I get started?

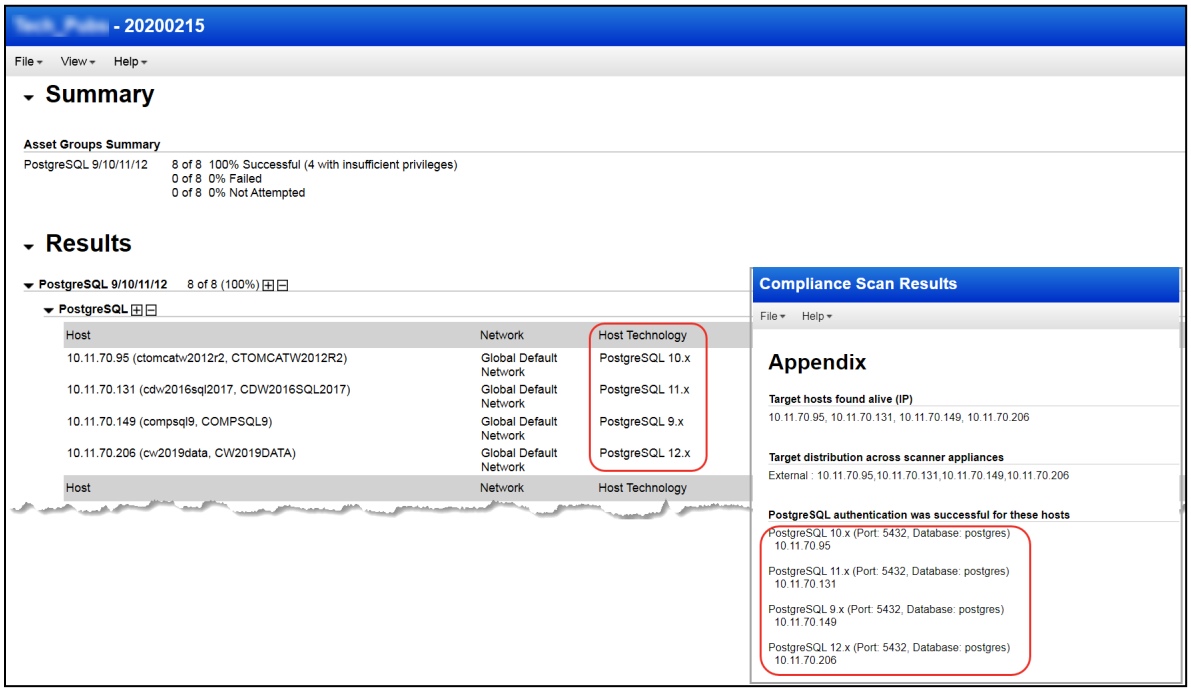
- Go to Scans > Authentication.

- Check that you have a Windows record already defined for the host running the database.

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

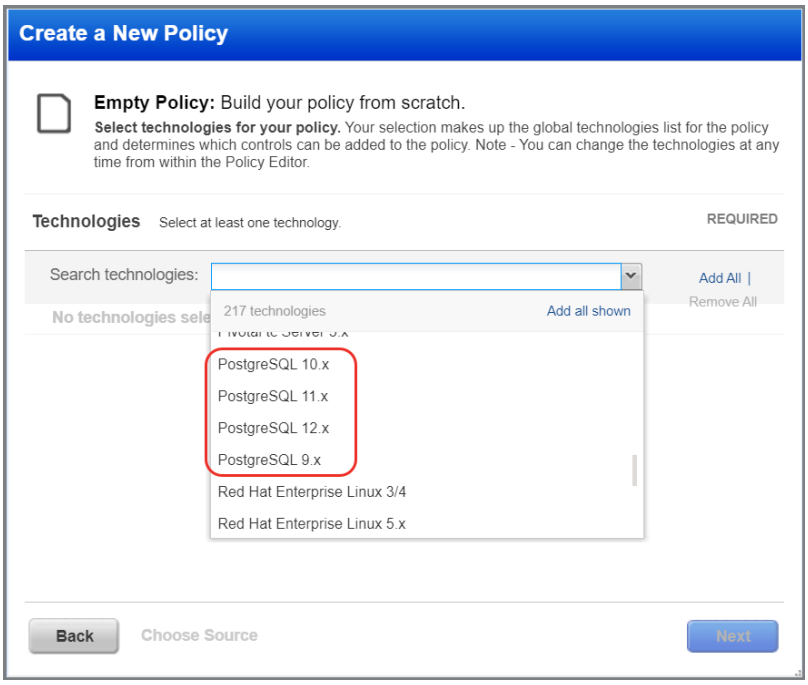
Sample Reports

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

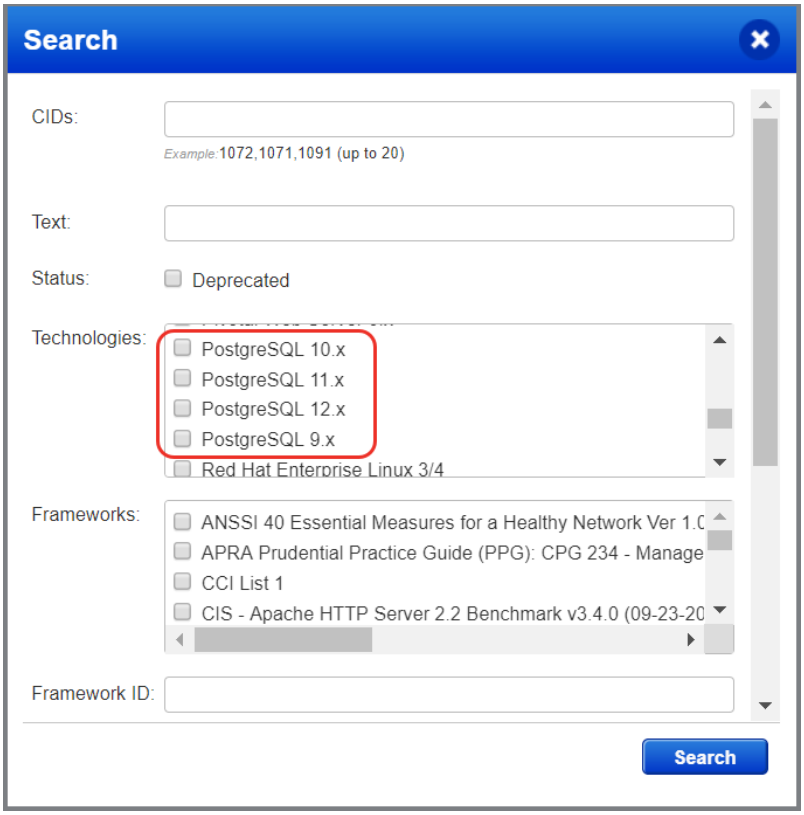


Policies and Controls

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



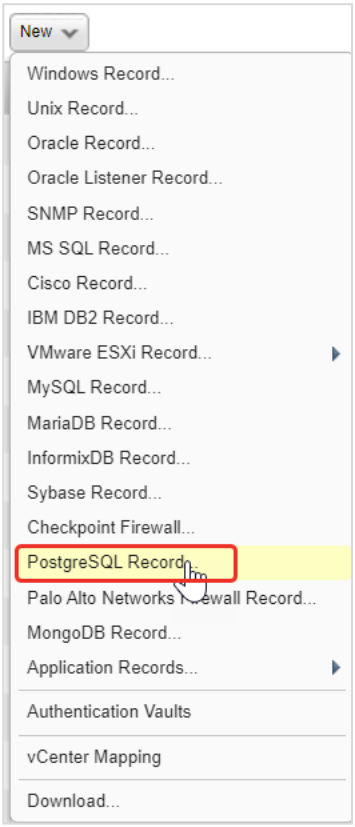
You'll see PostgreSQL when searching controls by technologies.



PostgreSQL 12.x Support for Unix

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

You'll need a PostgreSQL authentication record to authenticate to a PostgreSQL database instance running on a Unix host, and scan it for compliance. Unix authentication is required so you'll also need a Unix 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.



How do I get started?

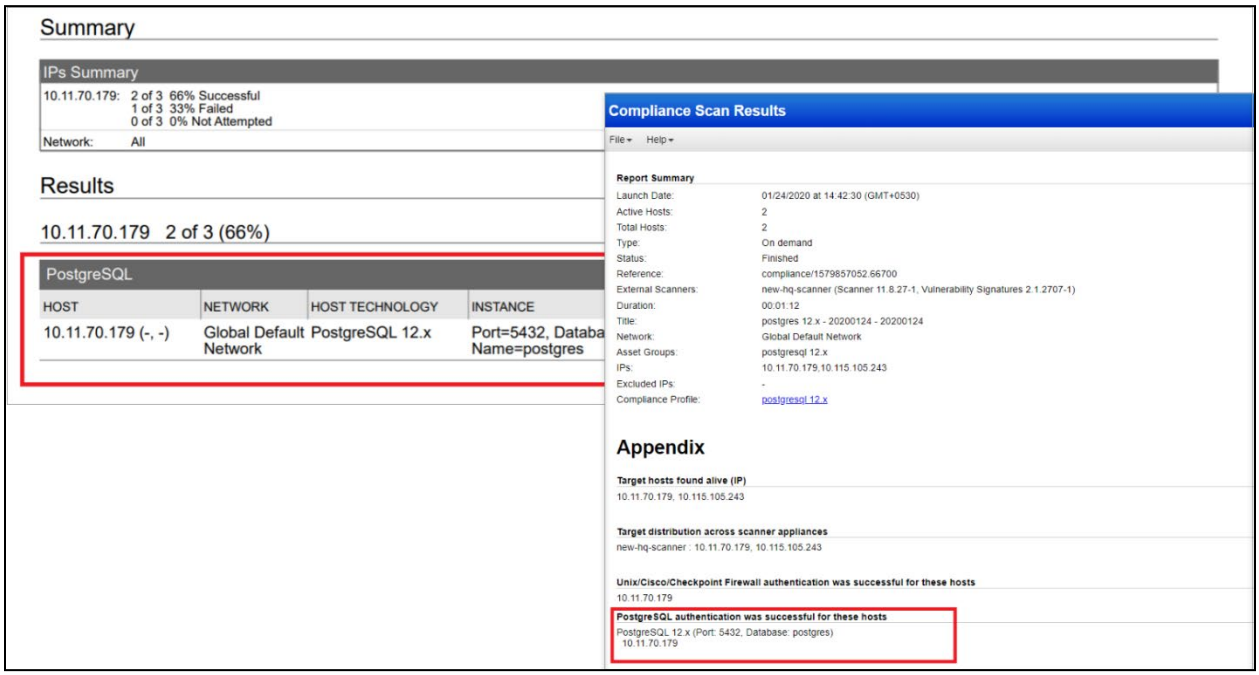
- Go to Scans > Authentication.

- Check that you have a Unix record already defined for the host running the database.

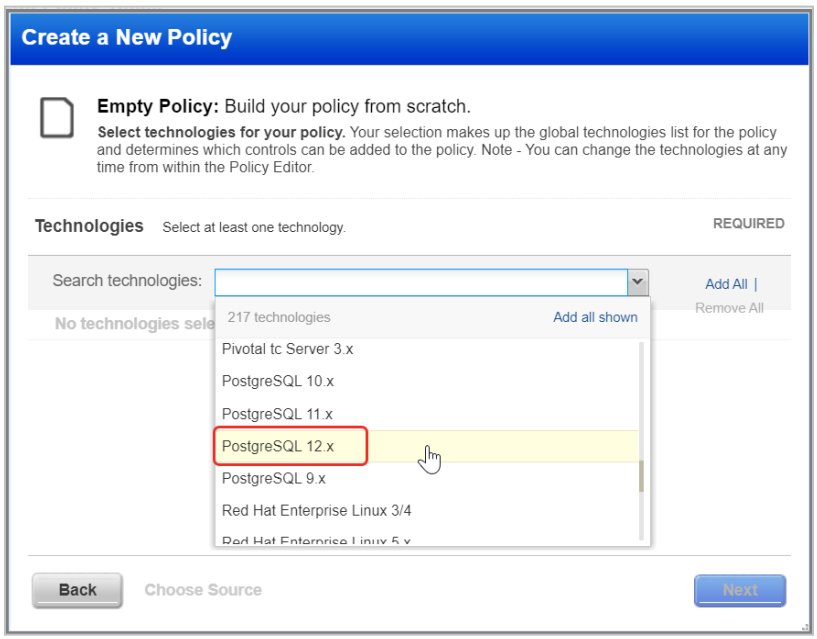
- Create a PostgreSQL record for the same host. Go to New > PostgreSQL Record.

Sample Reports

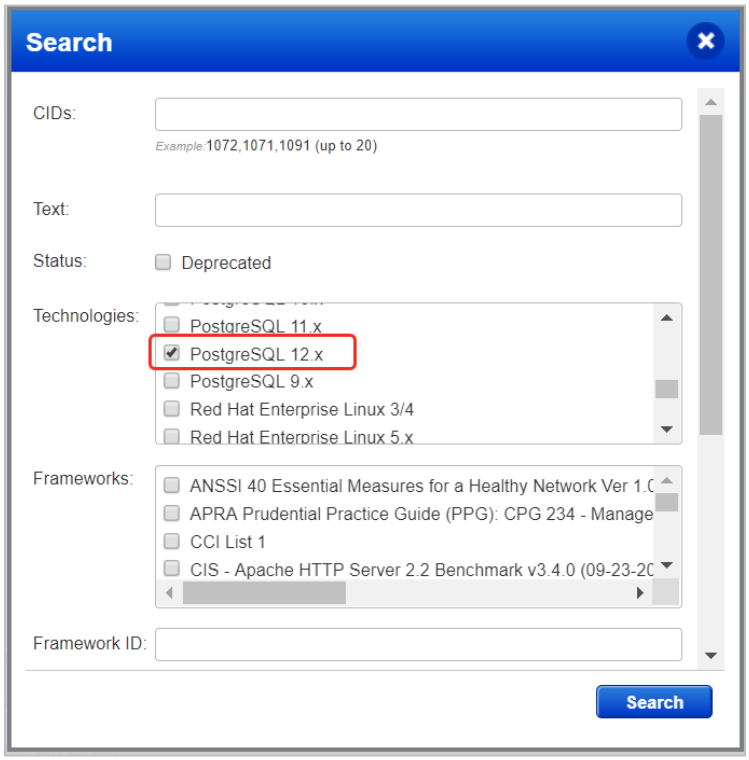
You'll see the PostgreSQL 12.x technology in compliance reports and in compliance scan results.



You'll see PostgreSQL 12.x in the technologies list when creating a new policy.



You'll see PostgreSQL 12.x when searching controls by technologies.



Microsoft SQL Server 2019 Support

We've extended our support for MS SQL Server authentication to include Microsoft SQL Server 2019. These technologies are already supported: Microsoft SQL Server 2000, 2005, 2008, 2012, 2014, 2016 and 2017.

You'll need a MS SQL Server record to authenticate to your Microsoft SQL Server 2019 database, and scan it for compliance.

How do I get started?

Go to Scans > Authentication, and choose New > MS SQL Record. This authentication type is supported for compliance scans only.

Issues Addressed

- Updated the online help for Search Lists to explain that vulnerabilities with the half red / half yellow severity icon match search lists for both confirmed and potential vulnerabilities. If you create a search list that includes all confirmed QIDs and excludes all potential QIDs, then the QIDs with half red / half yellow severity will be excluded.
- Updated the online help to explain that only the Manager user has privileges to edit storage settings to auto delete scan results.
- Updated the online help for CheckPoint Firewall Authentication to list supported technology versions as CheckPoint Gaia R75 and above, and CheckPoint SecurePlatform PRO R75 and above.
- Updated the System Requirements help to state that we do not support browsers on mobile devices at this time.
- Updated the online help for the VM Scan Summary Notification to clarify that this email includes vulnerability trend information based on the processed results including the total number of new, reopened, active and closed vulnerabilities. Please keep in mind that this email includes trend data, not the actual scan results.
- Updated the online help for OPatch Checks to explain that some Oracle detections use the OPatch method and others do not. In all cases database authentication is required in addition to host authentication for successful Oracle scanning.