Qualys Policy Compliance

Database Security & Compliance for Hybrid Environments

Solution Overview

September 30, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Preface

This document highlights the capabilities of Policy Compliance for database security and compliance across datacenter and cloud environments for a multitude of incumbent and emerging technologies.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit http://www.qualys.com/support/.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at http://www.qualys.com/support/.

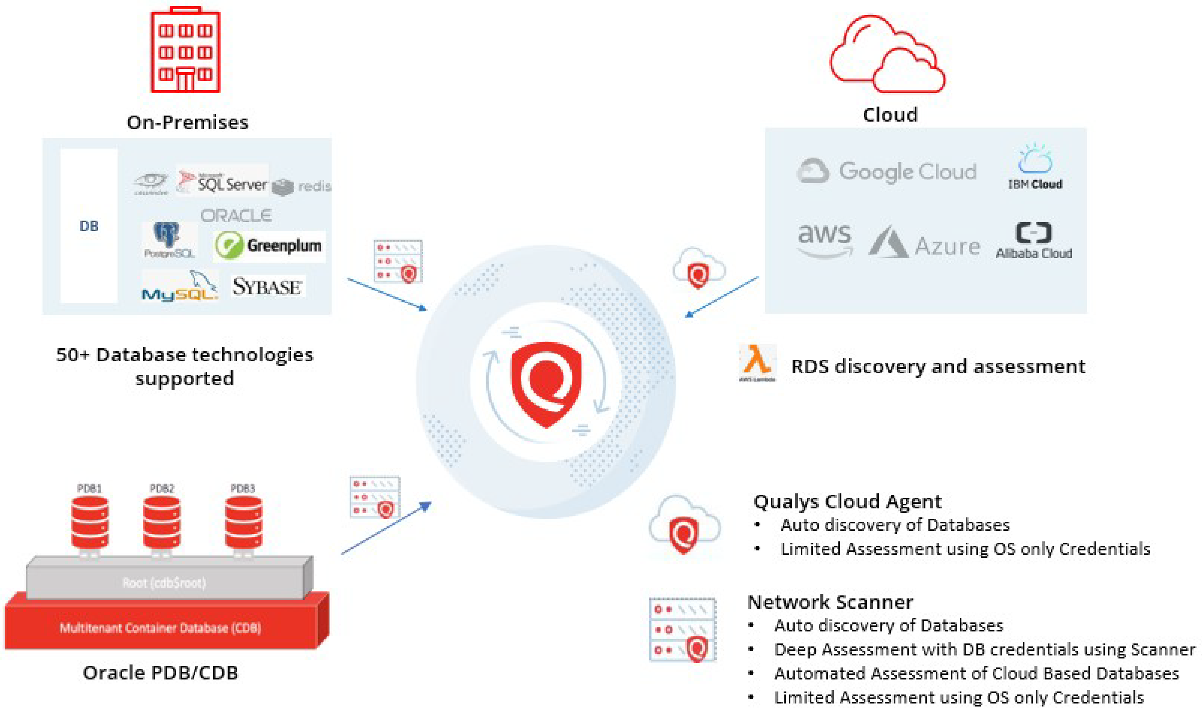
Objective

The aim of this document is to provide an overview of Qualys Policy Compliance (PC) solution capabilities with respect to database security and compliance for hybrid environments.

In the current digital era, securing databases is one of the most crucial and highly challenging aspects of security for any enterprise. Research shows that the most common reasons behind database security breakdowns are unpatched vulnerabilities and configuration errors. All organizations, no matter how small, need to be vigilant about their security posture and ensure that all their databases are protected.

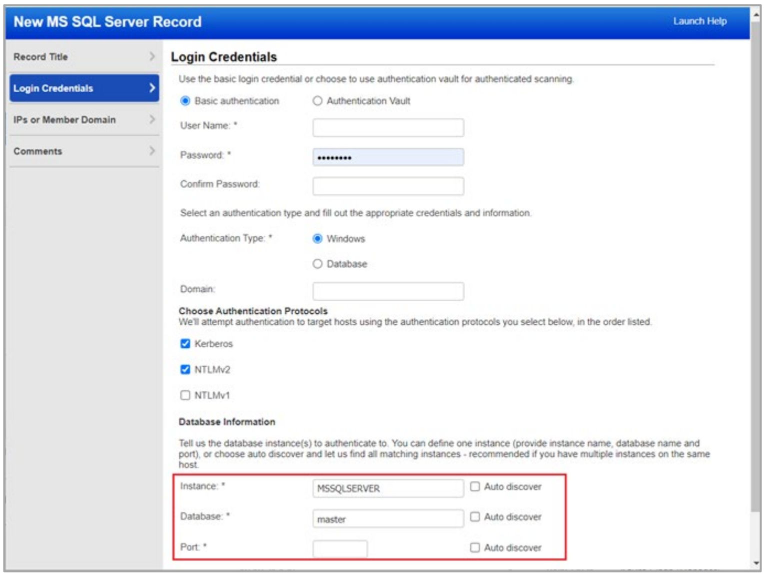
How Qualys helps you secure your databases

Qualys Policy Compliance (PC) supports a wide range of database security policies and provides your choice of data collection sensors, including scanners, cloud agents, and APIs. Qualys PC offers many usability focused features like User-Defined Controls, auto-discovery of database instances, real-time visibility and monitoring of overall compliance with dynamic dashboards, and compliance assessment reporting according to different mandates and frameworks. All this plus integration with third-party applications enables you to fast-track your compliance assessments. Let's look at the many ways Qualys PC helps you ensure that your databases are never exposed to vulnerabilities and malicious threats.


On-Premises
DB
SQL Server
redis
ORACLE
PostgreSQL
Greenplum
MySQL
SYBASE
50+ Database technologies supported
PDB1
PDB2
PDB3
Root (cdb$root)
Multitenant Container Database (CDB)
Oracle PDB/CDB
Cloud
Google Cloud
IBM Cloud
aws
Azure
Alibaba Cloud
RDS discovery and assessment
Qualys Cloud Agent
Auto discovery of Databases
Limited Assessment using OS only Credentials
Network Scanner
Auto discovery of Databases
Deep Assessment with DB credentials using Scanner
Automated Assessment of Cloud Based Databases
Limited Assessment using OS only Credentials

Database Instance Auto Discovery

Sometimes security teams performing compliance assessments don’t have database credentials and don’t know where all the databases are located. Qualys provides an auto discovery option which can be leveraged to automatically find database instances, and you won't need to worry about database credentials. Database instance auto discovery will help you find all the database instances and perform the assessment on them.



New MS SQL Server Record Launch Help

Record Title
Login Credentials
IPs or Member Domain
Comments

Login Credentials

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

● Basic authentication ○ Authentication Vault

User Name: *

Password: * ••••••••

Confirm Password:

Select an authentication type and fill out the appropriate credentials and information.

Authentication Type: * ● Windows ○ Database

Domain:

Choose Authentication Protocols
We'll attempt authentication to target hosts using the authentication protocols you select below, in the order listed.

☑ Kerberos
☑ NTLMv2
□ NTLMv1

Database Information

Tell us the database instance(s) to authenticate to. You can define one instance (provide instance name, database name and port), or choose auto discover and let us find all matching instances - recommended if you have multiple instances on the same host.

Instance: * MSSQLSERVER □ Auto discover

Database: * master □ Auto discover

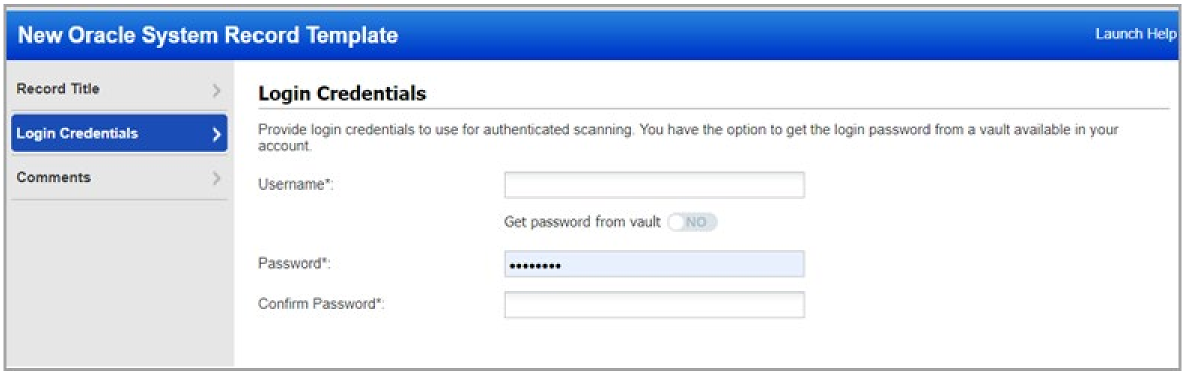
Port: * □ Auto discover

Simply check the “Auto discover” option within a database authentication record (when this option is available) instead of manually entering database details, and we’ll automatically detect all the database instances. This is especially useful when there are multiple database instances running on the same target host.

Check out the Auto discover options in the MS SQL Server record. Go to **PC** > **Scans** > **Authentication** and choose **New** > **Databases** > **MS SQL**. The **Auto discover** options appear on the **Login Credentials** tab. See Set Up MS SQL Server Authentication in the help for details.

For Oracle databases, Qualys PC can auto discover the target configuration for each instance but not the login credentials. You’ll need to create one or more “Oracle System Record Templates” containing the login credentials that you’ll want to apply to system created records. Then select the template in the scan option profile used for discovery scans. The template is linked automatically to the system created records created as a result of the discovery scan.

Go to **PC** > **Scans** > **Authentication** and choose **New** > **System Record Templates** > **Oracle System Record Template**. Go to the **Login Credentials** tab and provide the username and password (or choose a password vault). These credentials will be used for all system created records associated with this template. See Set Up Oracle System Record Template in the help.



New Oracle System Record Template Launch Help

Record Title
Login Credentials
Comments

Login Credentials

Provide login credentials to use for authenticated scanning. You have the option to get the login password from a vault available in your account.

Username*:

Get password from vault NO

Password*: ••••••••

Confirm Password*:

Database Policies and Controls

Extensive Database Technology Coverage

Considering the fact that databases hold extremely valuable and sensitive information, Qualys offers its support for an extensive range of platforms. Apart from the currently supported platforms, Qualys continues to add support at frequent intervals. With the wide range of platforms, it ensures to extend instant and comprehensive compliance visibility to your databases with ease.

Please refer to the Authentication Technologies Matrix in the Qualys online help for a list of database platforms and other technologies that are currently supported. Qualys continues to add new technologies to the current list to ensure extensive platform support.

Content Library for Database Policies

Library policies provided by Qualys can be customized to meet your organization's security and compliance requirements. Whether you use the library content for strengthening a handful of control requirements or for building a comprehensive technical standard, Qualys' control library provides coverage of the most common critical security control objectives out-of-the-box.

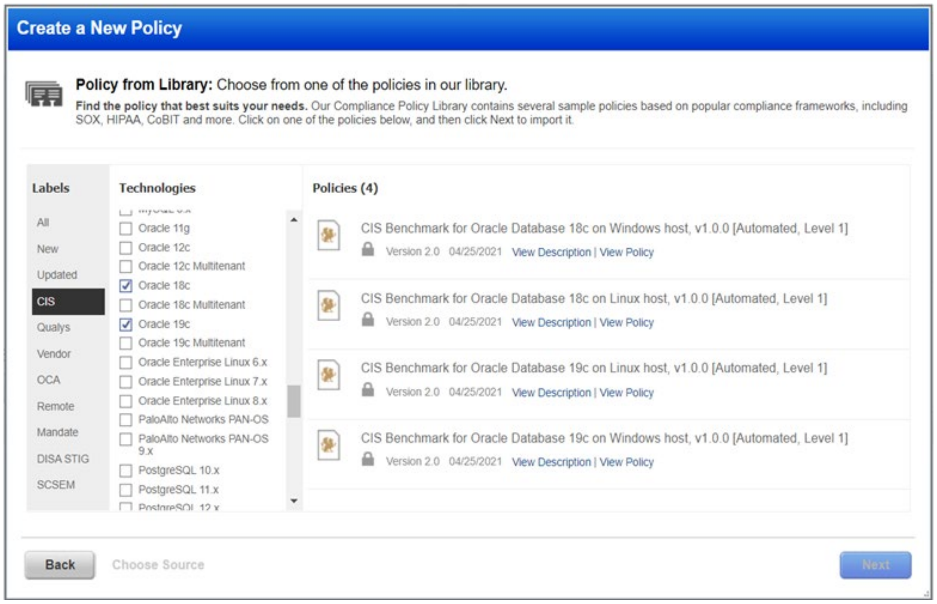
Learn more:

CIS Certified Policies for Qualys

Qualys Policy Library Update Notifications

How to import a policy from the Library

You can import a policy by going to **PC** > **Policies** > **New** > **Policy** > **Import from Library**. Select **Labels** and choose a database security policy from our Library. Click **Next** to import the policy.



Create a New Policy

Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Technologies

- □ Oracle 11g
- □ Oracle 12c
- □ Oracle 12c Multitenant
- ☑ Oracle 18c
- □ Oracle 18c Multitenant
- ☑ Oracle 19c
- □ Oracle 19c Multitenant
- □ Oracle Enterprise Linux 6.x
- □ Oracle Enterprise Linux 7.x
- □ Oracle Enterprise Linux 8.x
- □ PaloAlto Networks PAN-OS
- □ PaloAlto Networks PAN-OS 9.x
- □ PostgreSQL 10.x
- □ PostgreSQL 11.x

Policies (4)

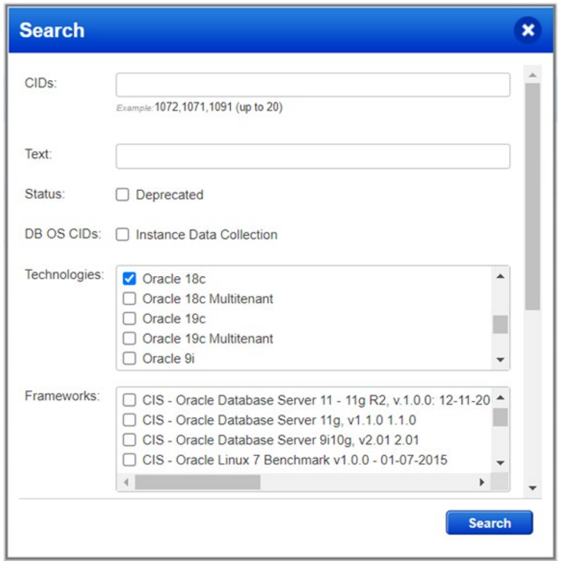
CIS Benchmark for Oracle Database 18c on Windows host, v1.0.0 [Automated, Level 1]
Version 2.0 04/25/2021 View Description | View Policy

CIS Benchmark for Oracle Database 18c on Linux host, v1.0.0 [Automated, Level 1]
Version 2.0 04/25/2021 View Description | View Policy

CIS Benchmark for Oracle Database 19c on Linux host, v1.0.0 [Automated, Level 1]
Version 2.0 04/25/2021 View Description | View Policy

CIS Benchmark for Oracle Database 19c on Windows host, v1.0.0 [Automated, Level 1]
Version 2.0 04/25/2021 View Description | View Policy

System-Defined Controls for Databases



Search

CIDs:

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

Text:

Status: □ Deprecated

DB OS CIDs: □ Instance Data Collection

Technologies:
☑ Oracle 18c
□ Oracle 18c Multitenant
□ Oracle 19c
□ Oracle 19c Multitenant
□ Oracle 9i

Frameworks:
□ CIS - Oracle Database Server 11 - 11g R2, v.1.0.0: 12-11-20
□ CIS - Oracle Database Server 11g, v1.1.0 1.1.0
□ CIS - Oracle Database Server 9i10g, v2.01 2.01
□ CIS - Oracle Linux 7 Benchmark v1.0.0 - 01-07-2015

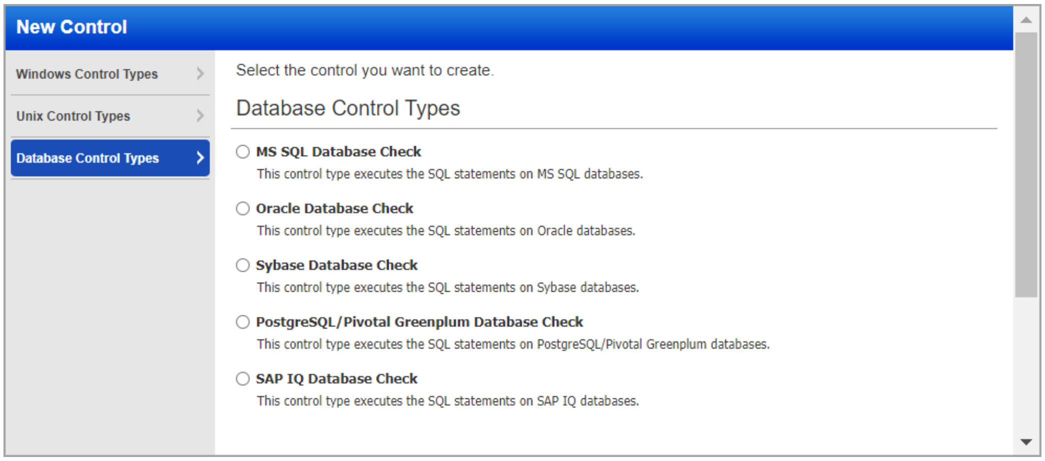
Controls are the building blocks for policies that are used to scan the security posture of your assets. Qualys provides system-defined controls (SDCs) that you can use to scan your databases. These out-of-the-box controls are generic and ready to be used for security and compliance evaluation of databases on any of the supported platforms. As a part of its continuous effort to extend its current capabilities, Qualys continues to add new SDCs.

Search for controls to see the technologies covered by SDCs by going to **PC** > **Policies** > **Controls** and clicking the **Search** button. In the **Search** window, select from various filters to find controls for different technologies, frameworks, and more.

User-Defined Controls for Databases

Qualys PC includes the flexibility of user-defined controls (UDCs) for databases. UDCs, as opposed to the system-defined controls, are the controls that customers can create on their own. UDCs allow customers to easily extend the Qualys controls without complex programming to meet unique internal needs and to assess databases on supported platforms. UDCs can be added to compliance policies and subsequently be included in compliance reports just like system-defined controls. Qualys supports UDCs for several database technologies and will continue to add support for new technologies.

To create a new database UDC, go to **PC** > **Policies** > **Controls** > **New** > **Control**. Select **Database Control Types**. Then click the control type you want to create. Refer to the online help for guidance on control settings.



New Control

Select the control you want to create.

Database Control Types

○ **MS SQL Database Check**
This control type executes the SQL statements on MS SQL databases.

○ **Oracle Database Check**
This control type executes the SQL statements on Oracle databases.

○ **Sybase Database Check**
This control type executes the SQL statements on Sybase databases.

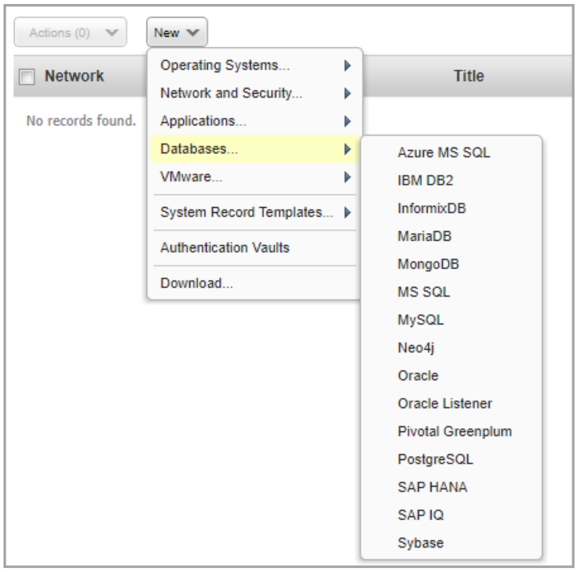
○ **PostgreSQL/Pivotal Greenplum Database Check**
This control type executes the SQL statements on PostgreSQL/Pivotal Greenplum databases.

○ **SAP IQ Database Check**
This control type executes the SQL statements on SAP IQ databases.

Database Assessments On-Premise

For on-premise databases running on Unix or Windows hosts, we recommend using a scanner appliance with database authenticated scanning. You'll be able to perform a deep assessment by logging into each database instance using the credentials provided in database authentication records. Optionally, you can perform a limited assessment with only OS credentials in the case where database authentication is not available. For this you can use a scanner or an agent.

Deep Assessment with Database Credentials Using Scanner (Recommended)



Use privileged database user accounts in addition to host credentials to authenticate into your database instances running on Unix or Windows hosts. Qualys PC offers authenticated scanning for several database technologies. Simply create authentication records to allow the scanner to connect directly to a database using credentials that you provide, and scan it for compliance.

Each record identifies an authentication type, account login credentials and target IP addresses. You may also need to provide OS specific details like the path to the database configuration file on your Windows or Unix host. See the online help for each record type to know what's required.

Authentication records in your account are used automatically for compliance scans. Being able to log into each database with a scanner provides the most in-depth coverage. To create database authentication records, go to **PC** > **Scans** > **Authentication** and choose **New** > **Databases**. Select from the list of database technologies.

Limited Assessment With Only OS Credentials

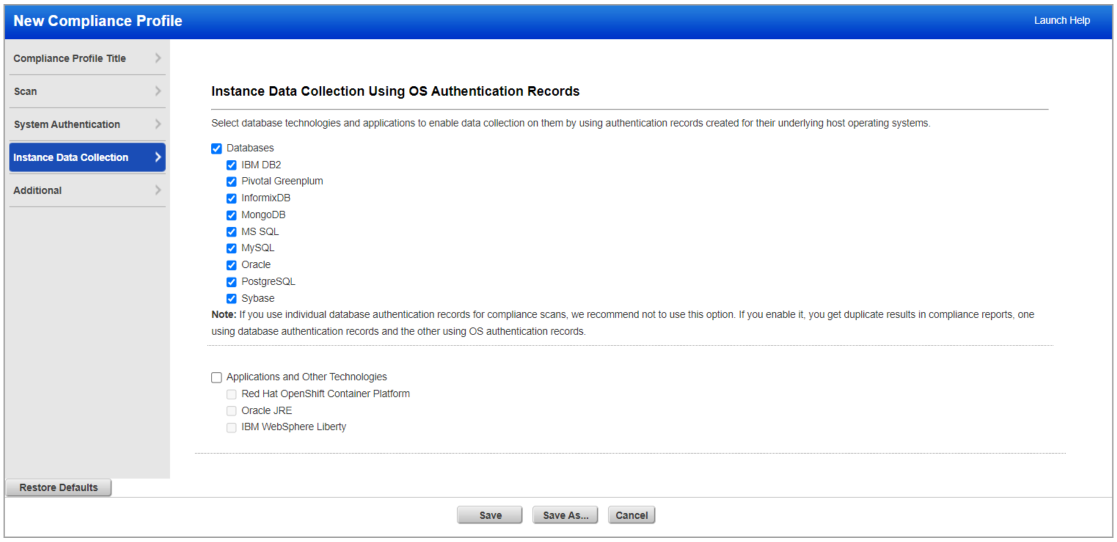
Organizations have traditionally used privileged database user accounts in addition to host credentials to authenticate into their database instances running on Unix or Windows hosts. But sharing database credentials with security teams presents a security and governance challenge for organizations, and the teams performing these assessments may not have privileged access to the databases.

We offer the ability to perform a limited assessment with only OS credentials when database authentication is not possible. This makes assessments simpler and more secure as customers do not need to create any additional restricted user accounts on their databases running on Unix or Windows hosts.

Limited assessment using Scanner

If you're using a scanner, the Compliance Option Profile has the option to enable OS-based instance data collection. Selecting this option enables data collection for the supported databases using the underlying OS-based authentication records. Once the compliance profile is updated, simply launch compliance scans with this option profile for authenticated scanning. Note that only OS-dependent database controls supported by Scanner will be evaluated in this case.

To enable instance data collection, go to **PC** > **Scans** > **Option Profiles** > **New** > **Compliance Profile**. Select **Instance Data Collection**. Click **Databases** and select each database technology you're interested in. Apply this profile to your next compliance scan. See Configure Your Scan Option Profile (PC) in the online help to learn more about this feature.



New Compliance Profile

Instance Data Collection Using OS Authentication Records

Select database technologies and applications to enable data collection on them by using authentication records created for their underlying host operating systems.

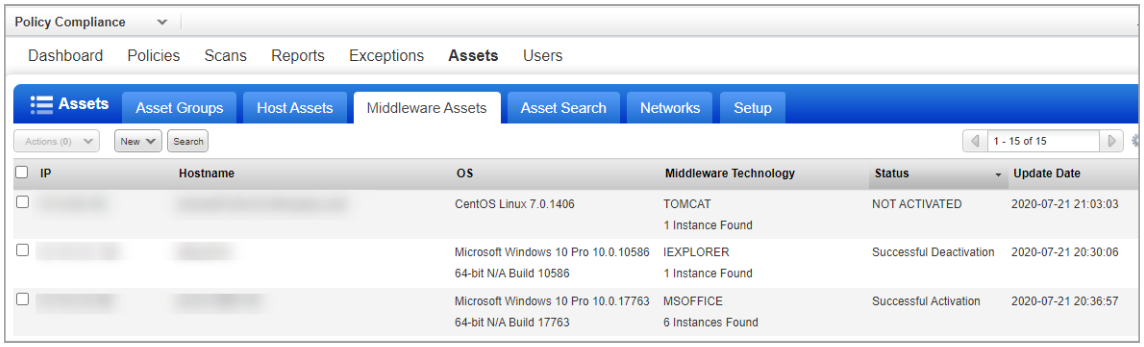
- ☑ Databases
  - ☑ IBM DB2
  - ☑ Pivotal Greenplum
  - ☑ InformixDB
  - ☑ MongoDB
  - ☑ MS SQL
  - ☑ MySQL
  - ☑ Oracle
  - ☑ PostgreSQL
  - ☑ Sybase

Note: If you use individual database authentication records for compliance scans, we recommend not to use this option. If you enable it, you get duplicate results in compliance reports, one using database authentication records and the other using OS authentication records.

- ☐ Applications and Other Technologies
  - ☐ Red Hat OpenShift Container Platform
  - ☐ Oracle JRE
  - ☐ IBM WebSphere Liberty

Limited assessment using Cloud Agent

The auto-discovery feature in Qualys Cloud Agent discovers the database instances on the system where Cloud Agent is running. Cloud Agent running on Windows or Unix discovers and inspects the database instances through registry keys or running processes, without logging into the database. Once the assets are discovered and middleware technology details are listed on the Middleware Assets page in Policy Compliance as shown below, you can activate the assets for middleware assessment, either selectively or choose default activation (recommended) for assessment to begin as soon as they are discovered.



☐ IP	Hostname	OS	Middleware Technology	Status	Update Date
☐ [redacted]	[redacted]	CentOS Linux 7.0.1406	TOMCAT 1 Instance Found	NOT ACTIVATED	2020-07-21 21:03:03
☐ [redacted]	[redacted]	Microsoft Windows 10 Pro 10.0.10586 64-bit N/A Build 10586	IEXPLORER 1 Instance Found	Successful Deactivation	2020-07-21 20:30:06
☐ [redacted]	[redacted]	Microsoft Windows 10 Pro 10.0.17763 64-bit N/A Build 17763	MSOFFICE 6 Instances Found	Successful Activation	2020-07-21 20:36:57

If middleware assessment is already enabled, Cloud Agent will auto-discover the database instances and assess for OS-dependent database controls. No additional user action is required to enable this functionality.

Learn more:

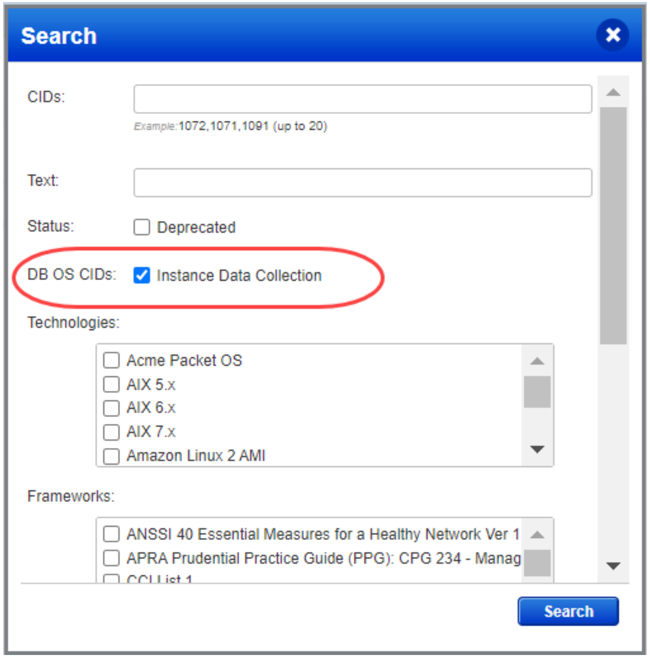
Evaluate Middleware Assets by Using Cloud Agent – Provides instructions for identifying middleware assets and activating assets for middleware assessment.

Middleware Technologies (Agent Only) – Provides a list of middleware technologies that are auto-discovered by cloud agents.

OS-dependent database controls

Only OS-dependent database controls are used in data collection and evaluation for limited assessments.

You can search for these controls by going to **PC** > **Policies** > **Controls** and clicking the **Search** button. In the **Search** window, select **Instance Data Collection** next to **DB OS CIDs**. The search returns OS-dependent database controls that are system-defined and supported by Scanner.



CIDs:

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

Text:

Status: □ Deprecated

DB OS CIDs: ☑ Instance Data Collection

Technologies:

□ Acme Packet OS
□ AIX 5.x
□ AIX 6.x
□ AIX 7.x
□ Amazon Linux 2 AMI

Frameworks:

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

Database Assessments in the Cloud

As organizations across the globe are shifting towards adopting cloud-based technology for their processes and business operations, you can now leverage a broader set of technologies support on AWS, GCP, Azure and others. The same techniques which we are using for auto discovery to find database instances running can be leveraged by using the agent.

It's important for customers to maintain an inventory of their RDS instances in the cloud but this can be challenging. Tracking and assessing RDS instances with dynamic IPs is also a challenge customers face. Qualys offers Lambda RDS Discovery and Scan Service (LRDSS) as a solution, helping customers manage the security and compliance of their RDS instances using Qualys Policy Compliance (PC).

Like with scanning your on-premise databases, Qualys PC can perform a deep assessment with login to each cloud database using a scanner (recommended). The same scanners that you're using for scanning IP assets in your cloud environments can also be leveraged for assessment of your databases in the cloud. We support common databases in the cloud environment, and we're constantly adding support for new technologies.

Automate Assessment of Cloud-Based Database (Lambda RDS)

In the last several years, there has been a major shift towards adopting Platform as a Service (PaaS) solutions. When it comes to security and compliance, PaaS environments differ from traditional on-premises data centers. Changing the focus from network-centric security parameters to identity-specific ones comes with inherent challenges. The risk mitigation model used for on-prem instances cannot be replicated in cloud environments for various reasons.

Qualys offers an innovative solution for securing databases in Amazon AWS PaaS environments. Lambda RDS Discovery and Scan Service (LRDSS) enables you to manage the security and compliance of your RDS instances via Qualys Policy Compliance (PC), so that you secure them the same as your on-premises services. Being a shared platform, security and compliance for database PaaS services become the shared responsibility of the PaaS vendor and its customers. Due to the underlying infrastructural and architectural complexities, the way you secure your PaaS infrastructure is a big differentiator in security and compliance assessments.

LRDSS helps you overcome a number of challenges in managing the security and compliance of RDS instances, particularly around integrating them into an organization's global compliance program. It also automates the end-to-end workflow including creation of authentication records, handling the dynamic IPs of the RDS instances, initiating scans and so on, without any manual intervention, which substantially reduces the users' efforts.

The Qualys Compliance Team has developed a Lambda function that will automate the assessment by doing the following tasks:

- Auto-discovery of RDS instances & their IPs across the regions
- Adding IPs to Qualys subscription and creating respective Auth records
- Auto-discovery of scanners in VPCs and associating them with respective RDS instances.
- Create asset group with respective VPC & associated scanner appliance(s)
- Launching PC scan on RDS instances per VPC

After the scans are processed, the reports can be generated as usual. The Lambda function can be run manually on a defined schedule or based on other supported triggers in AWS.

Learn more:

https://blog.qualys.com/product-tech/2020/08/18/automated-discovery-and-assessment-of-paas-databases-with-lambda-service-for-qualys-policy-compliance

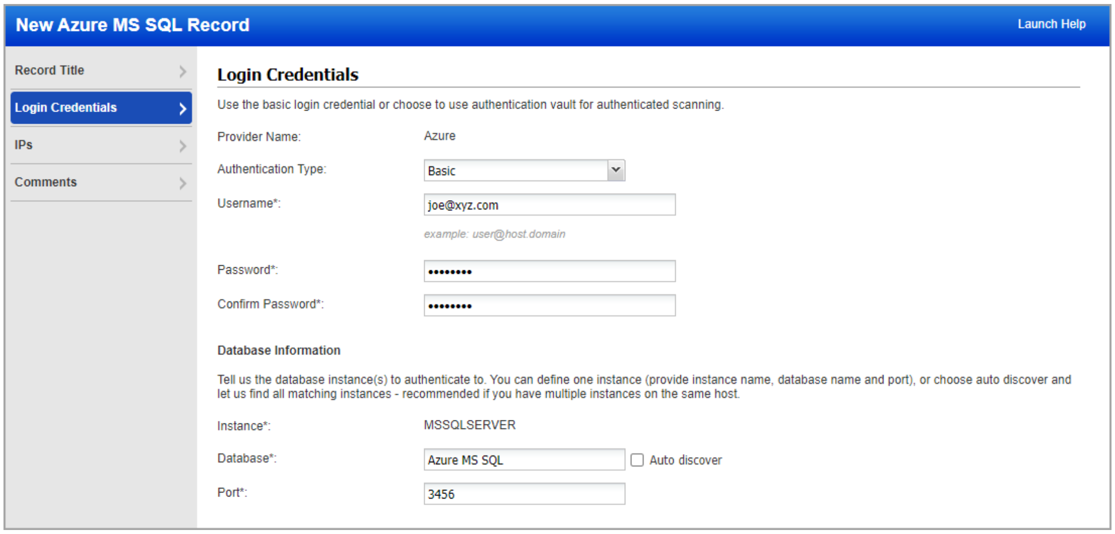
Interested in this functionality?

Please reach out to your Technical Account Manager or Qualys Support.

Support for Microsoft Azure

We recently added support for Azure MS SQL authentication within Qualys PC. You can create Azure MS SQL authentication records to authenticate to an Azure MS SQL database instance and scan it for compliance. Each record identifies account login credentials, database information (unless you use auto discovery) and targets.

Want to create an Azure MS SQL authentication record? Go to **PC** > **Scans** > **Authentication** and choose **New** > **Databases** > **Azure MS SQL**. See Set Up Azure MS SQL Server Authentication in the help for complete details.



New Azure MS SQL Record

Login Credentials

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

Provider Name: Azure

Authentication Type: Basic

Username*: joe@xyz.com

example: user@host.domain

Password*: ••••••••

Confirm Password*: ••••••••

Database Information

Tell us the database instance(s) to authenticate to. You can define one instance (provide instance name, database name and port), or choose auto discover and let us find all matching instances - recommended if you have multiple instances on the same host.

Instance*: MSSQLSERVER

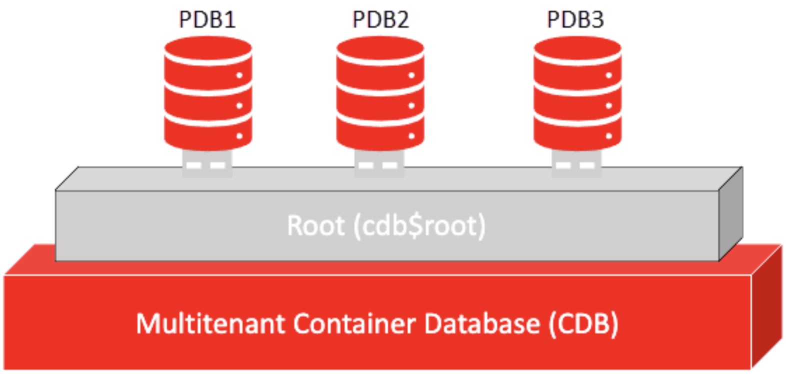
Database*: Azure MS SQL ☐ Auto discover

Port*: 3456

Oracle Multitenant (CDB/PDB) Discovery and Assessment

Customers have the option to assess their Oracle multitenant databases for compliance via the container database (CDB). For this, customers simply select the option "Is CDB" in the Oracle authentication record. There is no need for customers to create individual records for each pluggable database in the CDB.

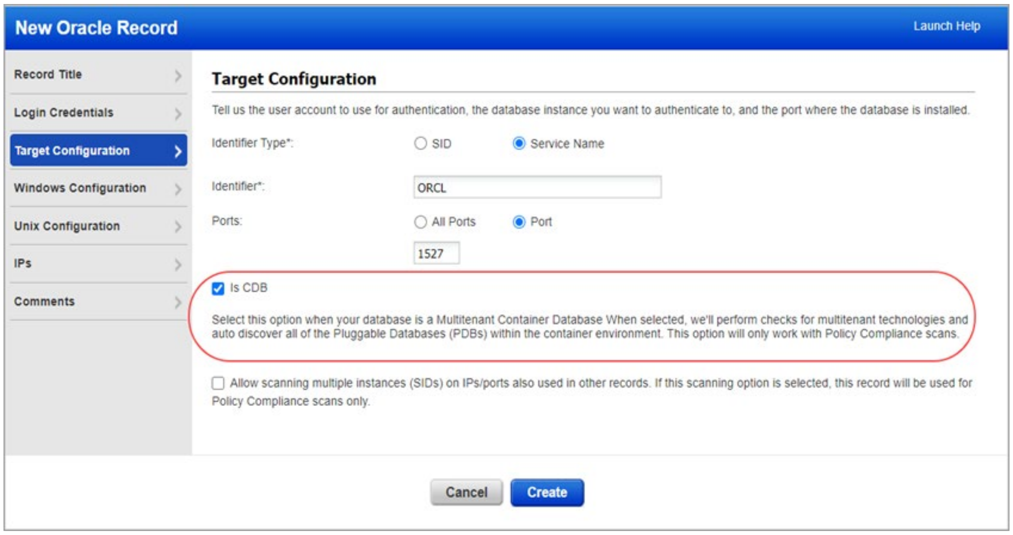
When "Is CDB" is selected in the Oracle record, the compliance scan will auto discover and assess all accessible Pluggable Databases (PDBs) within the container database (CDB). The assessment is performed through the CDB, which means there is no need for the scanner to connect directly to individual PDBs.



Identifying the Oracle database as a CDB in the Oracle record also ensures the right compliance checks are performed for multitenant technologies (Oracle 12c/18c/19c Multitenant).

Here's a sample container database with 3 pluggable databases. You'll only need one record for the entire CDB.

To create an Oracle record for CDB/PDB, go to **PC** > **Scans** > **Authentication** and choose **New** > **Databases** > **Oracle**. Select the **Is CDB** option on the **Target Configuration** tab. See Perform Compliance Assessment of Oracle Multitenant Databases via Container Database in the help.



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.

Identifier Type*: ○ SID ● Service Name

Identifier*: ORCL

Ports: ○ All Ports ● Port

1527

☑ Is CDB

Select this option when your database is a Multitenant Container Database When selected, we'll perform checks for multitenant technologies and auto discover all of the Pluggable Databases (PDBs) within the container environment. This option will only work with Policy Compliance scans.

□ Allow scanning multiple instances (SIDs) on IPs/ports also used in other records. If this scanning option is selected, this record will be used for Policy Compliance scans only.

In Summary

Being well acquainted with the fact that enterprises usually do not have the visibility into the vulnerabilities that their databases are exposed to, Qualys has efficiently devised its Policy Compliance solution with granular details. The primary aspect of maintaining a robust and secure enterprise lies in gaining visibility. Qualys helps enterprises gain deeper knowledge into the current state of their database security with the help of the extensive library of controls and policies. With an extensive support for database instances on a wide range of platforms, on-prem & cloud assessment, CIS-certified policies, system-defined and user-defined controls, Qualys ensures that your databases are never exposed to security vulnerabilities and threats.