# Qualys Cloud Platform (VM, PC) v10.x

## Release Notes

Version 10.5

November 5, 2020 (Updated November 18, 2020)

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

**Qualys Policy Compliance (PC/SCAP/SCA)**

PostgreSQL/Pivotal Greenplum Database User-Defined Control Support

Multiline Regex Supported in Unix File Content Check UDC (Agent Only)

Support for New OCA Technologies

Support for OS Authentication-Based Technology CITRIX XenApp/XenDesktop 7.x (Windows)

**Qualys Cloud Platform**

Cloud Metadata Information from Agent Now Displayed

**Qualys 10.5 brings you more improvements and updates!** Learn more

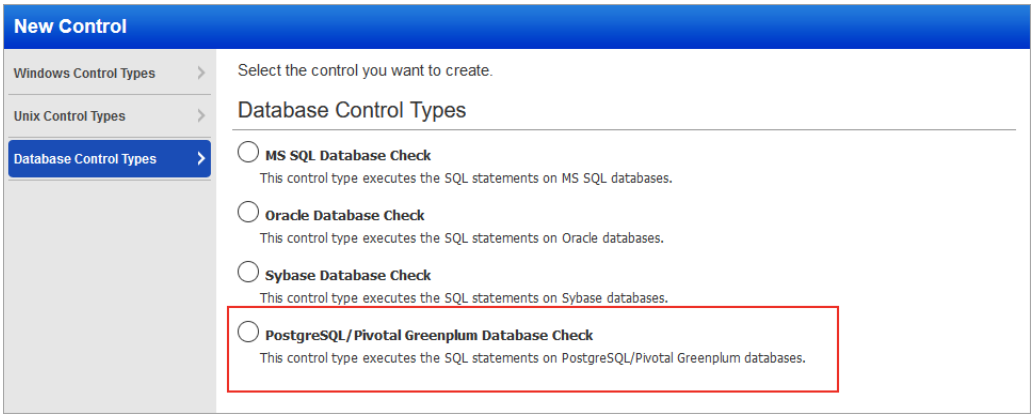
# Qualys Policy Compliance (PC/SCAP/SCA)

## PostgreSQL/Pivotal Greenplum Database User-Defined Control Support

You can now use PostgreSQL/Pivotal Greenplum database user-defined controls to create custom checks by executing SQL statements on databases. These controls can then be used to generate policy reports on your databases. We're already supporting MS SQL, Oracle, and Sybase databases. Follow the steps below to create a PostgreSQL/Pivotal Greenplum database control and generate a report.

### Step 1 – Add database controls

On the Qualys Cloud Platform, from the module picker, select Policy Compliance and then go to **Policies** > **Controls** > **New** > **Control**. Click the **Database Control Types** tab and then, click **PostgreSQL/Pivotal Greenplum Database Check**.




In each control, you'll define the SQL statement that you want to execute on your database.

**Note** - Only SELECT statements are supported for the database controls. For example, you can use the following SQL statement to list all fields from "Customers" where country is "Germany" AND city is "Berlin":

SELECT * FROM Customers WHERE Country='Germany' AND City='Berlin'

See the Help for sample queries and results.

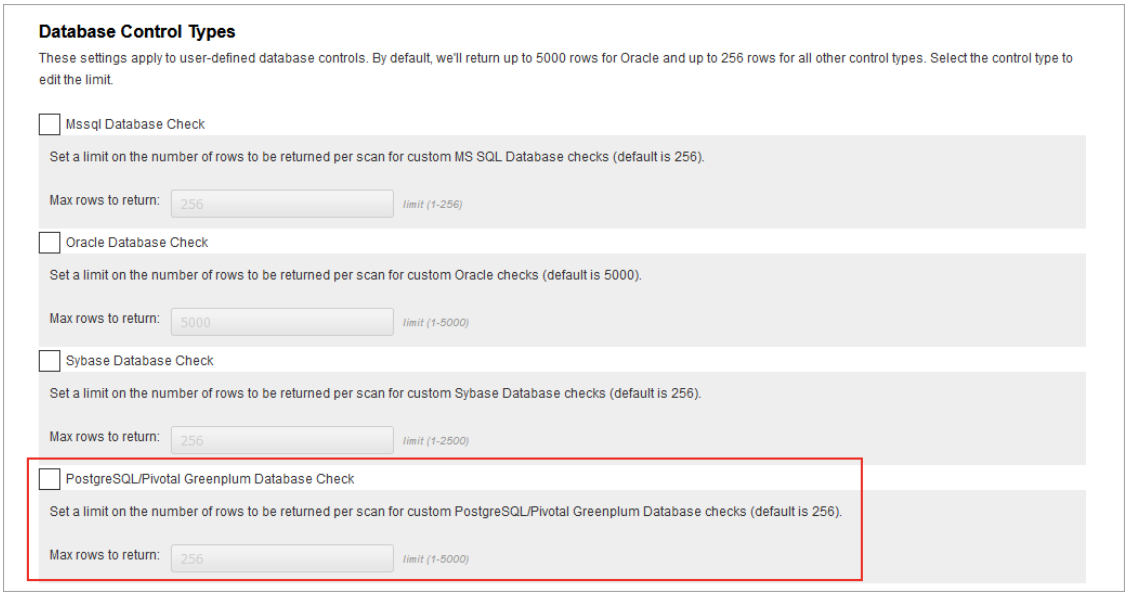
### Step 2 - Add database controls to a policy

Create a new compliance policy or edit an existing policy, and add your database controls to the policy. Make sure your policy has the database technologies selected in the control.

### Step 3 - Launch a compliance scan

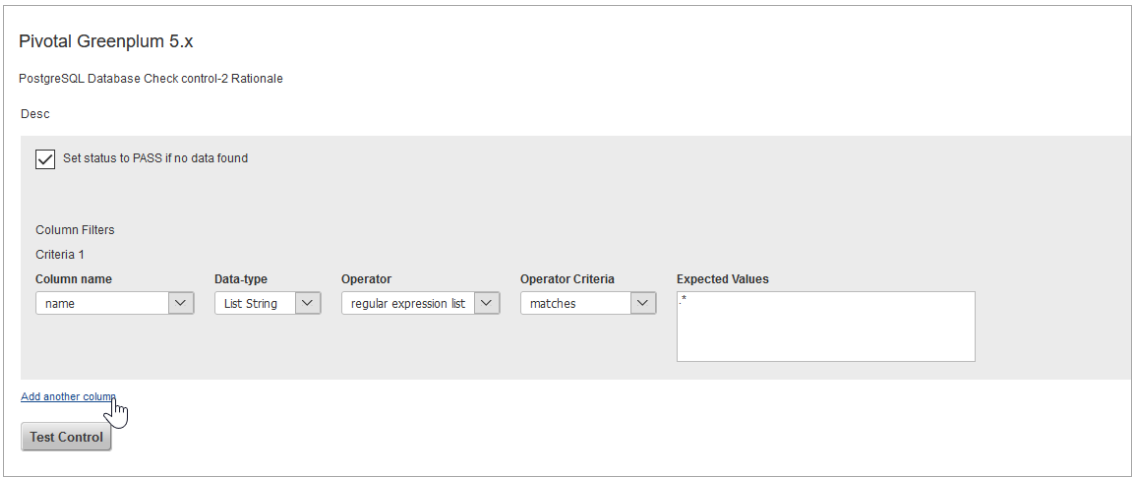
Launch a compliance scan on the host running the PostgreSQL/Pivotal Greenplum database.

You can edit the compliance option profile that you use for the scan to set the maximum number of rows you want the check to return. By default, we return up to 256 rows for a PostgreSQL/Pivotal Greenplum Database Check. To edit this limit, select the database control type in the compliance option profile and set a new value. The maximum value that you can set for a PostgreSQL/Pivotal Greenplum check is 5000 rows.




### Step 4 - Return to your policy to set control criteria

Edit your compliance policy by using the policy editor to see the actual data returned by your scan. Select a column and define the expected value. This is how you set the criteria that will determine pass/fail status for the control.

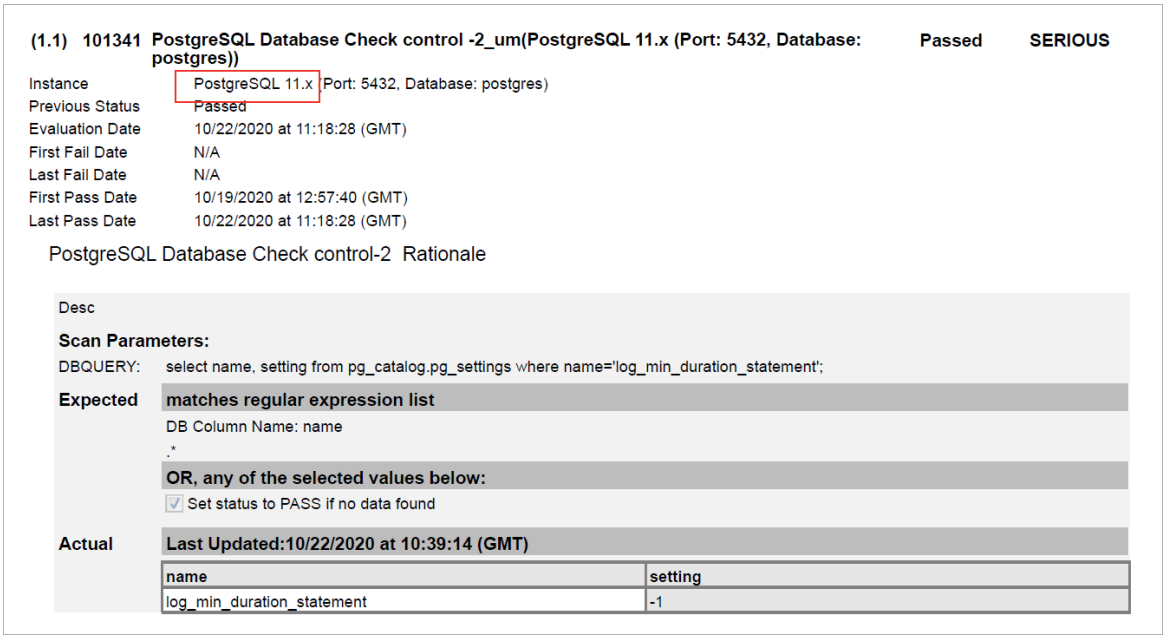



Click **Add another column** to add more criteria. You can add up to 5 criteria, i.e. Criteria 1, Criteria 2, Criteria 3 and so on.

You can choose AND or OR between each criteria. If you choose AND then both criteria must match to Pass. If you choose OR then at least one criteria must match to Pass. Click **Test Control** to verify the criteria you set. Then save your policy.

### Step 5 - Run a report

You'll see PASS or FAIL status in your report like you do with any control. If the columns returned by the most recent scan are different than previous scans then you'll want to edit your policy to modify the criteria selected for the control. Here's a sample report where the expected value matches the actual value, resulting in a status of Passed.



**(1.1) 101341 PostgreSQL Database Check control -2_um(PostgreSQL 11.x (Port: 5432, Database: postgres)) Passed SERIOUS**

| | |
|---|---|
| Instance | PostgreSQL 11.x (Port: 5432, Database: postgres) |
| Previous Status | Passed |
| Evaluation Date | 10/22/2020 at 11:18:28 (GMT) |
| First Fail Date | N/A |
| Last Fail Date | N/A |
| First Pass Date | 10/19/2020 at 12:57:40 (GMT) |
| Last Pass Date | 10/22/2020 at 11:18:28 (GMT) |

PostgreSQL Database Check control-2 Rationale

Desc

**Scan Parameters:**

DBQUERY: select name, setting from pg_catalog.pg_settings where name='log_min_duration_statement';

**Expected** **matches regular expression list**

DB Column Name: name

.*

**OR, any of the selected values below:**

☑ Set status to PASS if no data found

**Actual** **Last Updated:10/22/2020 at 10:39:14 (GMT)**

| name | setting |
|---|---|
| log_min_duration_statement | -1 |

## Multiline Regex Supported in Unix File Content Check UDC (Agent Only)

We've enhanced the Unix File Content Check UDC to support multiline regex matching. This allows you to create a single UDC that checks for multiple values in a Unix file, and saves you from having to create several, separate UDCs to achieve the same goal. Multiline regex is supported by agent scans only, using Linux or AIX Cloud Agent 2.5.x or later.

### Agent vs. Scanner

You can get varying results between the scanner and agent when scanning the same UDC on the same host. The agent supports regex match on both single line and multiline text, and returns the matching text. The scanner supports single line regex match, and returns the entire line.

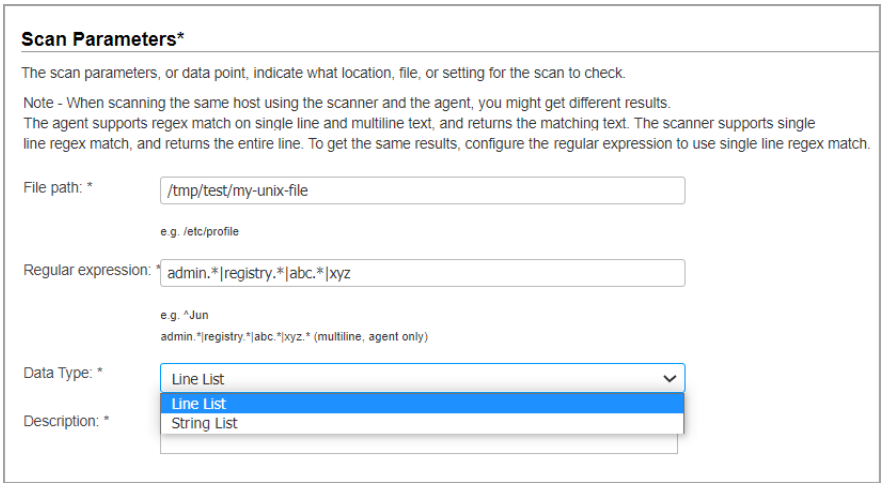
If the Unix File Content Check UDC is configured with multiline regex and you scan the UDC using a scanner, the results will be empty. If the expected value is an empty value, then the control will Pass. If the expected value is something else, then the control will Fail. To get the same results between the scanner and agent, configure the UDC to use single line regex.

### New data type

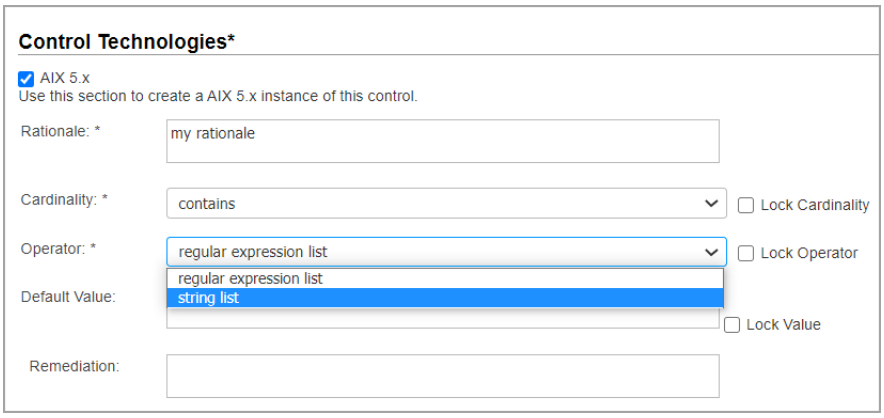
When you create or edit a Unix File Content Check UDC, you'll see the new data type "String List" under Scan Parameters. The data type "Line List" is also still supported. The data type you pick will determine which operators show up in the **Control Technologies** section.

To create a new Unix File Content Check, go to **Policies** > **Controls** > **New** > **Control**. Then choose **Unix Control Types**, and pick **File Content Check**. Go to the **Scan Parameters** section to tell us the file you want to evaluate and the content you want to look for in the Unix file. You'll do this by entering the regex value(s) you want to match in the **Regular expression** field.

In the following example, a multiline regex is entered. This control will check for admin, registry, abc and xyz values in the file called "my-unix-file".




The String List data type supports operators "regular expression list" and "string list". You'll pick the **Operator** in the **Control Technologies** section when setting the expected value for this control for different technologies.



## 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.

- **Aruba ClearPass Policy Manager (CPPM) 6.x**
- **Extreme Networks VOSS 6.x, 7.x, 8.x**
- **Microsemi SyncServer 3.x**
- **Extreme Networks BOSS 5.x**
- **Cisco IOS 12.x and 15.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.

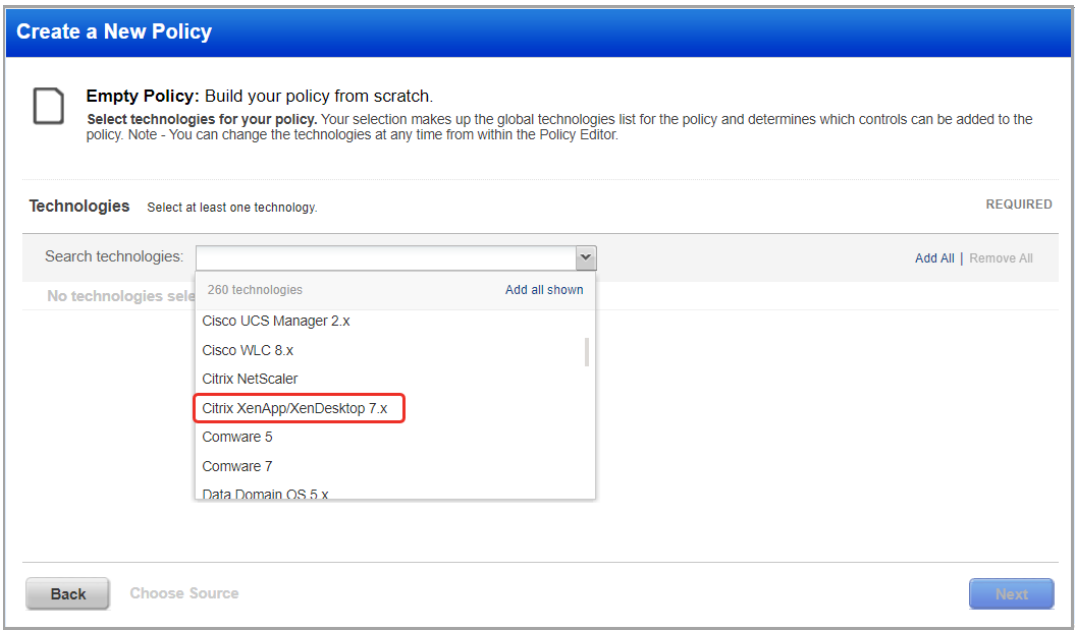
## Support for OS Authentication-Based Technology CITRIX XenApp/XenDesktop 7.x (Windows)

We've expanded our support of OS authentication-based technologies to include '**CITRIX XenApp/XenDesktop 7.x**'. For these technologies, you can collect technology data and scan it for middleware compliance assessment using the underlying OS technology (in this case Windows) without the need to create authentication records.

The **CITRIX XenApp/XenDesktop 7.x** technology is now available for inclusion in your compliance policies and when searching controls. You'll also see **CITRIX XenApp/XenDesktop 7.x** host instance information in policy compliance authentication reports, scan results, and policy reports.

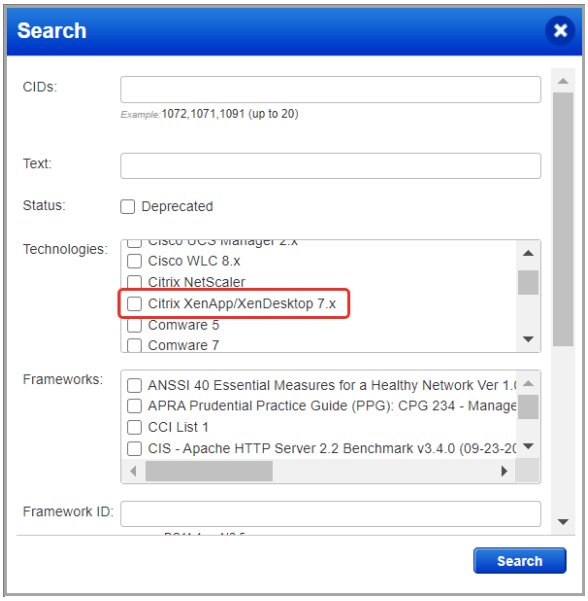
### Policy Editor

You can select the **CITRIX XenApp/XenDesktop 7.x** technology for your compliance policies.



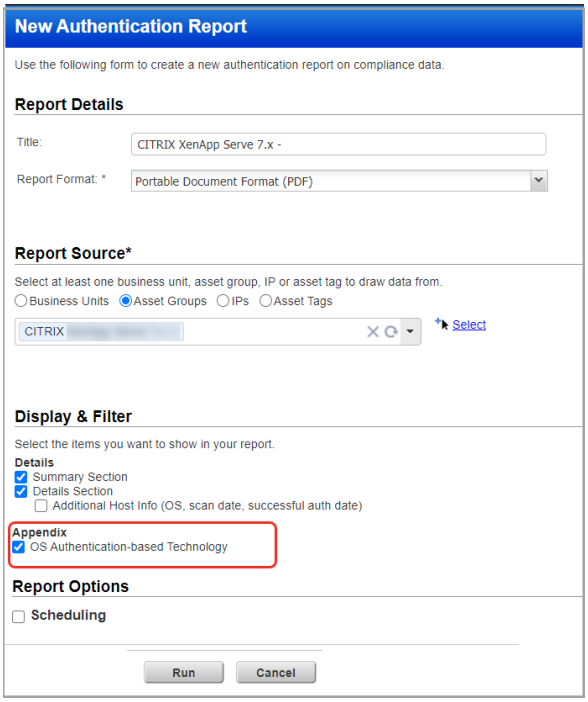
### Search Controls

You'll also see Microsoft Edge Chromium when searching controls. Go to **Policies** > **Controls** > **Search** and select **CITRIX XenApp/XenDesktop 7.x** in the list of **Technologies**.

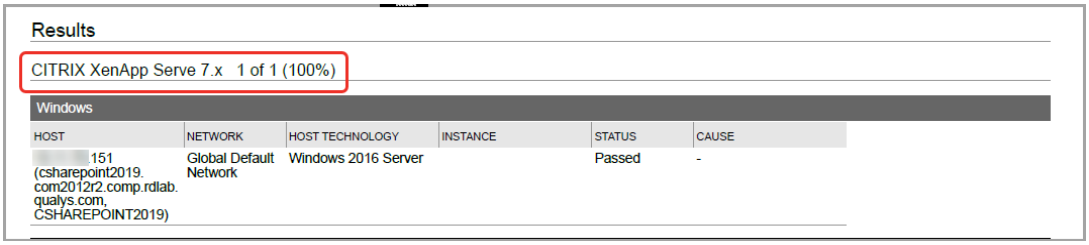



### Authentication Reports

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.

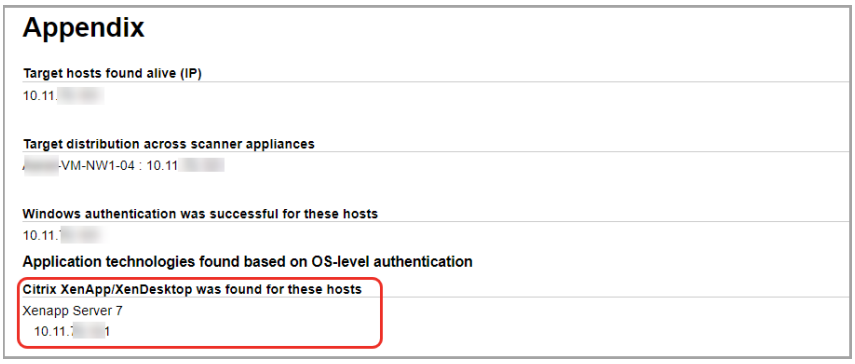


Scroll down to the **Appendix** section of your report to see **Targets with OS authentication-based technologies**.



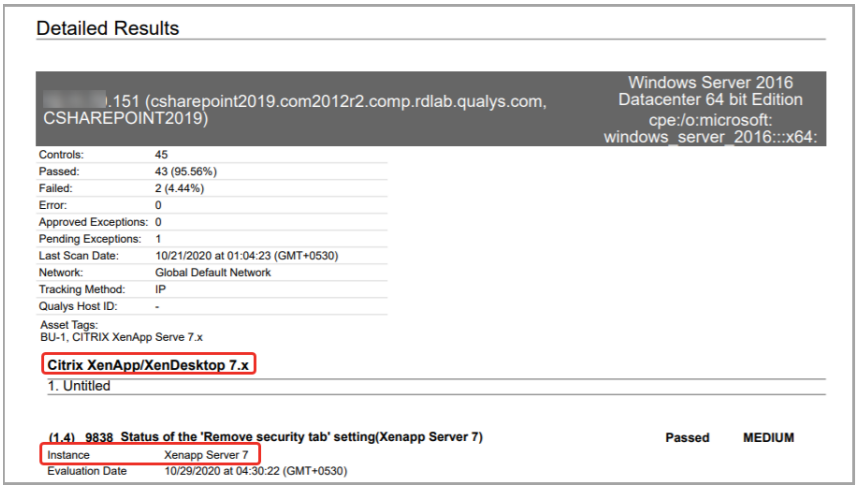

## Scan Results

You'll see **CITRIX XenApp/XenDesktop 7.x** listed in the **Appendix** section of **Compliance Scan Results** under **Application technologies found based on OS-level authentication**.




## Policy Reports

You'll also see **CITRIX XenApp/XenDesktop 7.x (Windows)** and above host instance information in your **Compliance Policy** reports.



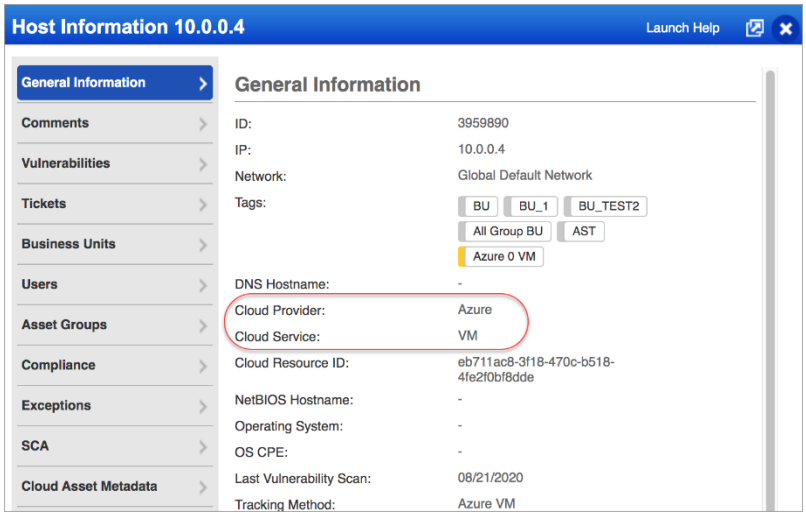

You can also evaluate the compliance posture of **CITRIX XenApp/XenDesktop 7.x** by using your PC agents. All you need to do is set up Cloud Agent on your Windows assets and activate them for middleware assessment.

# Qualys Cloud Platform

## Cloud Information from Agent Now Displayed

Previously, the Cloud Provider and Cloud Service information for assets hosted in a public cloud like AWS or Azure was only displayed on the Host Information page (under General Information) when the customer had a cloud connector configured in AssetView. Now, even when a cloud connector is not set up, if the asset has a Qualys Cloud Agent installed, we will get the Cloud Provider and Cloud Service information from the Agent and display it to the user. You'll also see Cloud Provider and Cloud Service details in Asset Search Report, Host List API and Host List Detection API for these types of assets.

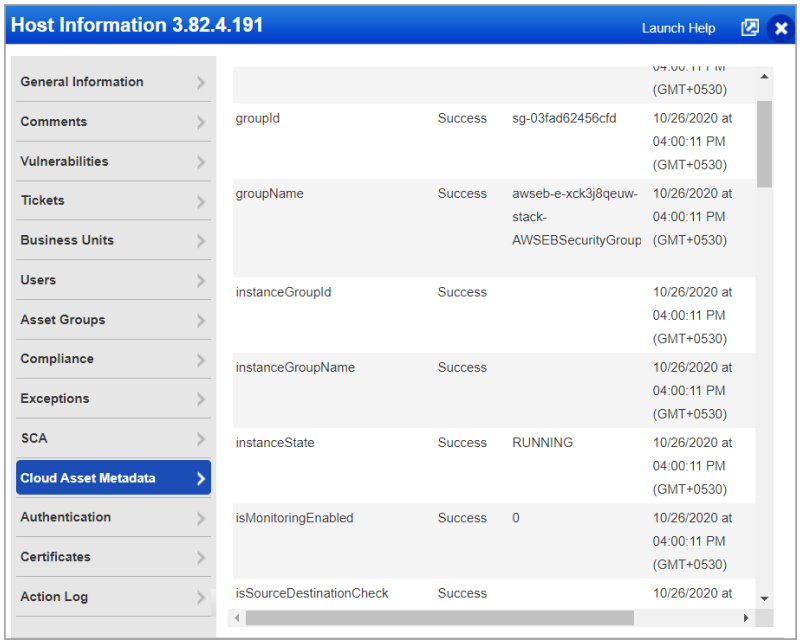
Here's a sample Azure asset where Cloud Provider and Cloud Service are shown.




Similarly, you'll see cloud asset metadata for these types of assets on the Cloud Asset Metadata tab on the Host Information page.

Here's a sample AWS asset with Cloud Asset Metadata shown.

Please note that we also fixed a related issue where the cloud asset metadata information did not appear in Host-based Scan Reports in certain cases (when only Information Gathered QIDs were reported for the asset).



## Issues Addressed

- We fixed an issue where custom WMI Query Check UDCs were not included in the scan when Scan by Policy was enabled in the compliance option profile even though the selected policy had these checks.
- We fixed an issue in the WMI Query Check UDC where double quotes ("") in the query string will now be escaped automatically so that agent scan processing for this UDC will work as expected.
- We fixed an issue where users saw an error when running the Asset Search Report using a combination of asset groups and IP ranges. With this fix, users can successfully run the Asset Search Report with a combination of IP addresses + Asset Groups + Network.
- We fixed an issue where any change to a scheduled scan like a change to the owner or option profile resulted in the next launch date being updated even though the scan date/time details were not changed. With this fix, the next launch date will only be changed if the date/time scheduling details are changed.
- We fixed an issue where the wrong posture status was returned in cases where the “item not found” error was returned for a control. The option “Set status Passed for 'item not found' error” in the policy was not being correctly interpreted when evaluating the control.
- We fixed an issue where Unit Managers could not download map reports because the report was interrupted before it could finish.
- Earlier, while creating a User-Defined Control (UDC) in Policy Compliance, using unbalanced brackets as a regular expression in an evaluation string was not allowed. Now, you can use unbalanced brackets, but you must escape them in your regular expression.