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

## Release Notes

Version 10.3

August 28, 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)

Support for Microsoft Exchange Server 2019 in compliance scans
User-Defined Control Support for Microsoft SQL Server 2019
Windows Support for the Apache HTTP Server and IBM HTTP Server Records
Windows Support for the IBM WebSphere Application Server Record
Support for OS Authentication-Based Technology Apache Cassandra 3.x
Comprehensive information about 'Insufficient Privileges'
Support for Additional Middleware Technologies

### Qualys Cloud Platform

Separate Options for Use IP Network Range Tags for Include and Exclude
Perimeter Scan Supports Azure Virtual Machines Scanning in Azure Cloud
Accepted Special Characters while Creating Password
Network-specific IP Addresses for Asset Group Creation

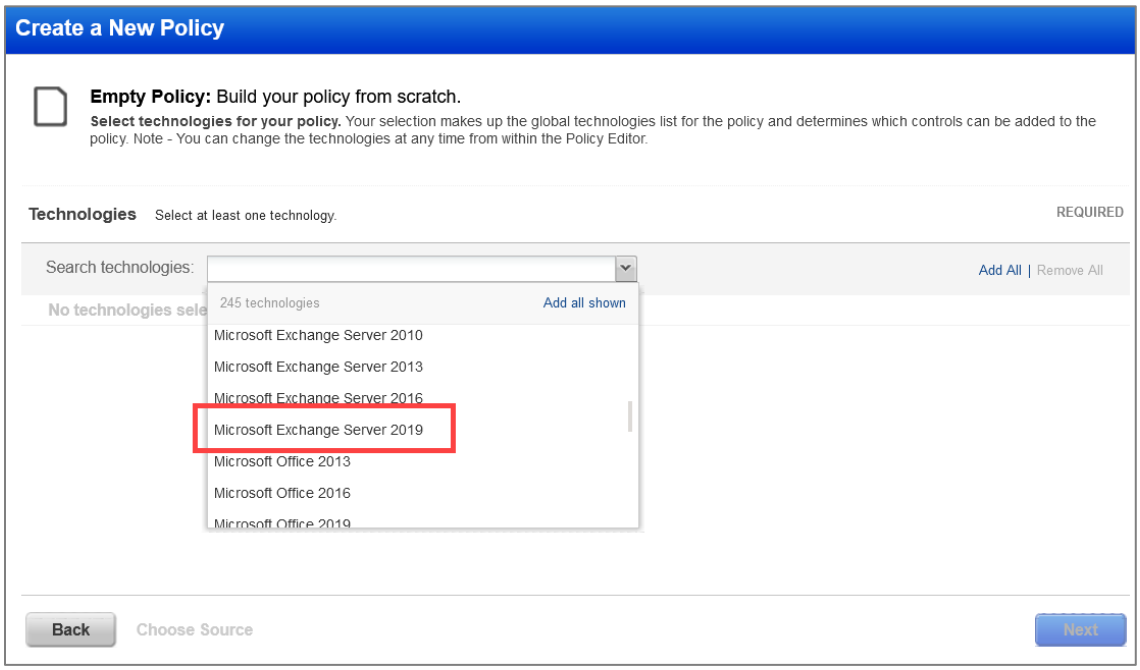
**Qualys 10.3 brings you more improvements and updates!** Learn more

# Qualys Policy Compliance (PC/SCAP/SCA)

## Support for Microsoft Exchange Server 2019 in compliance scans

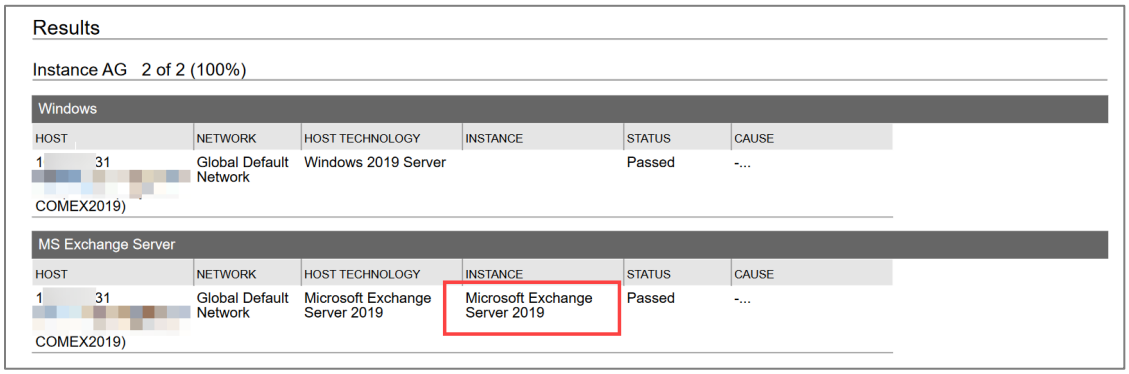
With this release, you can assess the compliance posture of the Microsoft Exchange Server 2019 web application installed on a Windows 2019 computer. Simply create an authentication record for MS Exchange Server running on a Windows host, add the Microsoft Exchange Server 2019 technology in your policy, and scan it for compliance.

The enhancement is highlighted below:




We'll use the credentials provided in your Windows authentication records to authenticate a Windows host, access the web server configuration by using the MS Exchange Server authentication records, and scan it for compliance.

Here's an example of a policy compliance report which displays the scan status of an MS Exchange Server 2019 instance:

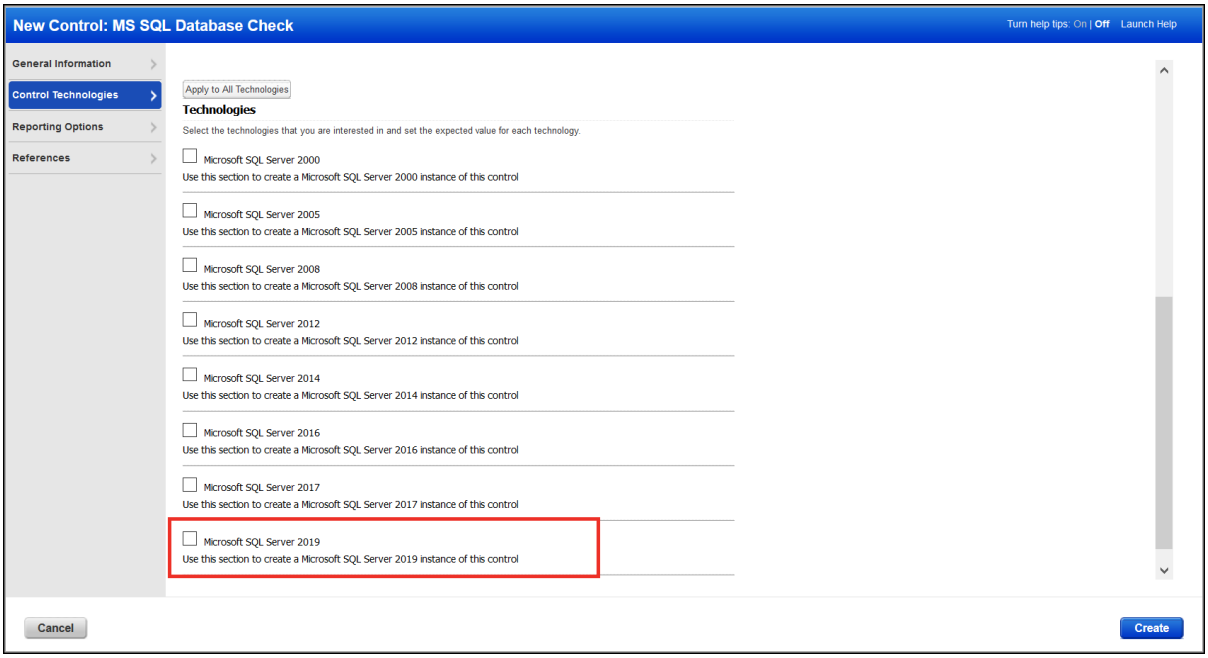


## User-Defined Control Support for Microsoft SQL Server 2019

With this release, we have extended support for MS SQL Database Check UDCs to include Microsoft SQL Server 2019 technology. Now you can create and configure UDCs to assess the compliance posture of your Microsoft SQL Server 2019 assets.

To create a UDC for Microsoft SQL Server 2019, in the **Policies** section, go to the **Controls** tab, click **New** > **Control...** > **Database Control Types**, and then click the **MS SQL Database Check** radio button. On the next screen where you configure the control, click the **Control Technologies** tab, and then in the **Technologies** section, select the **Microsoft SQL Server 2019** check box. Type the rationale statement for your control, SQL statement, description of the SQL statement, and remediation steps for the control. (You can always define the default values once and apply them to multiple technologies.)

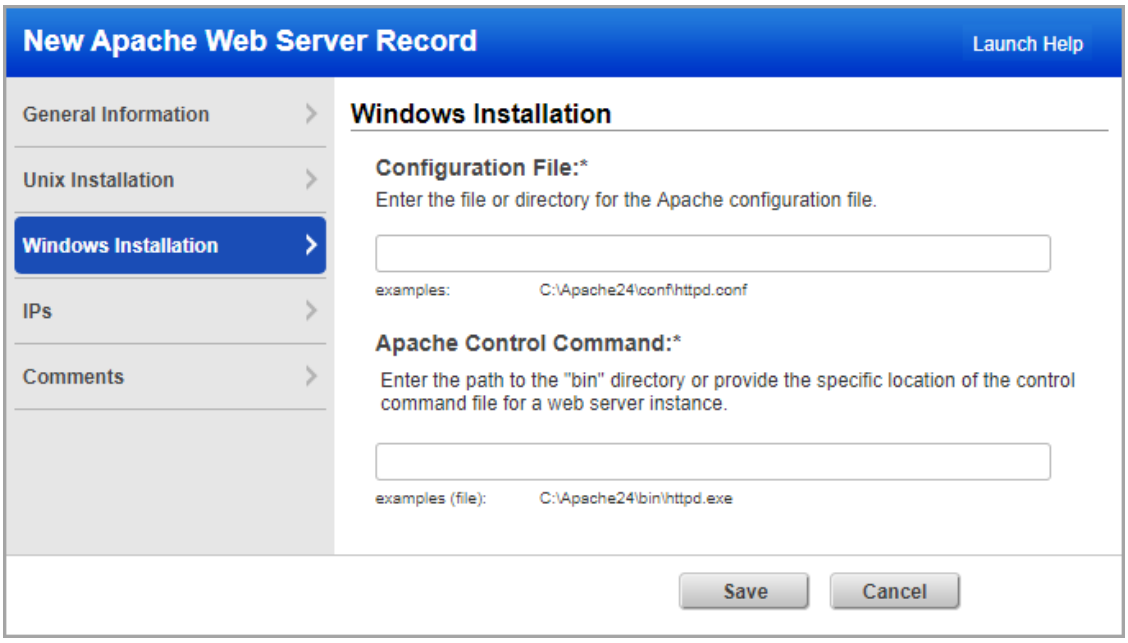
The enhancement is highlighted below:



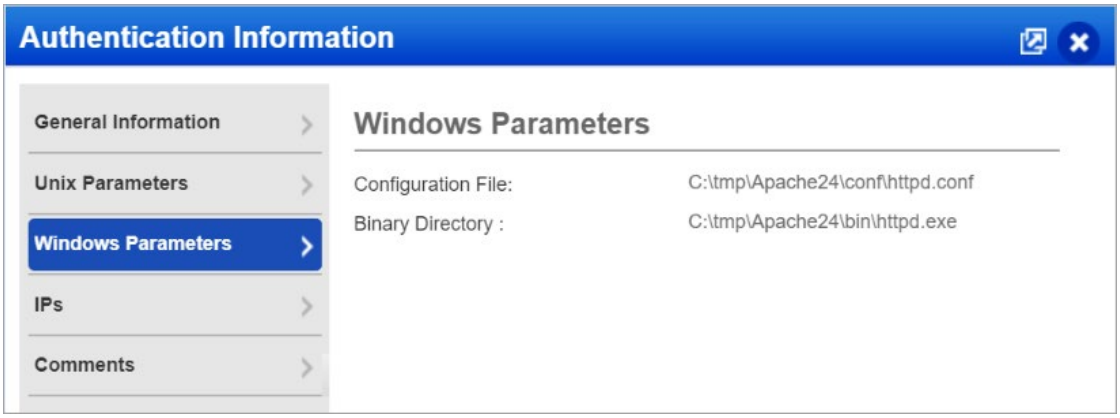
## Windows Support for the Apache HTTP Server and IBM HTTP Server Records

You can now create and update Apache Web Server records for Apache HTTP server and IBM HTTP server in order to authenticate to Apache HTTP and IBM HTTP servers running on a Windows host, and scan them for compliance. Windows authentication is required so you'll also need a Windows record for the host running the web server.

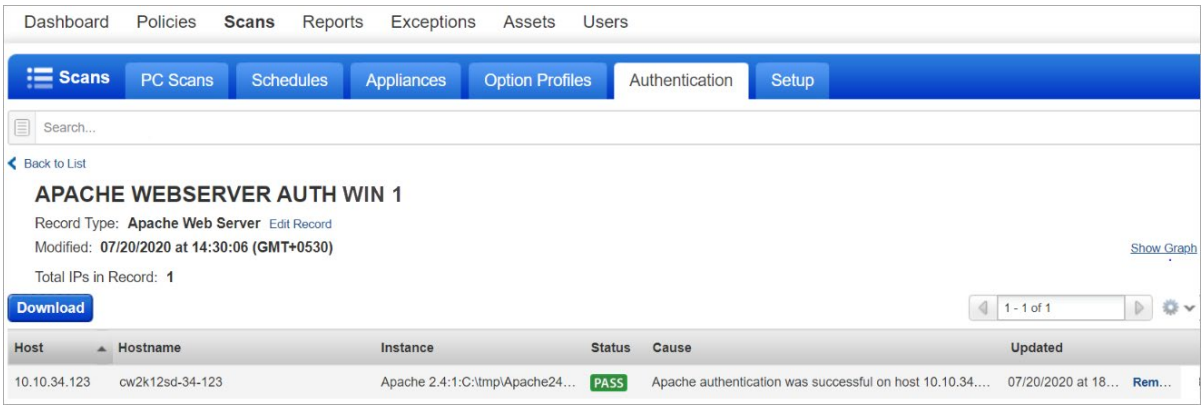
When you create or edit Apache Web Server Records, you'll see a new **Windows Installation** tab. The tab contains two fields: **Configuration File** and **Apache Control Command**. To support authenticated scans for these web servers running on Windows host, you need to specify the Windows path to the 1) Apache configuration file and 2) bin directory to Apache control command file or the specific location of the control command file.



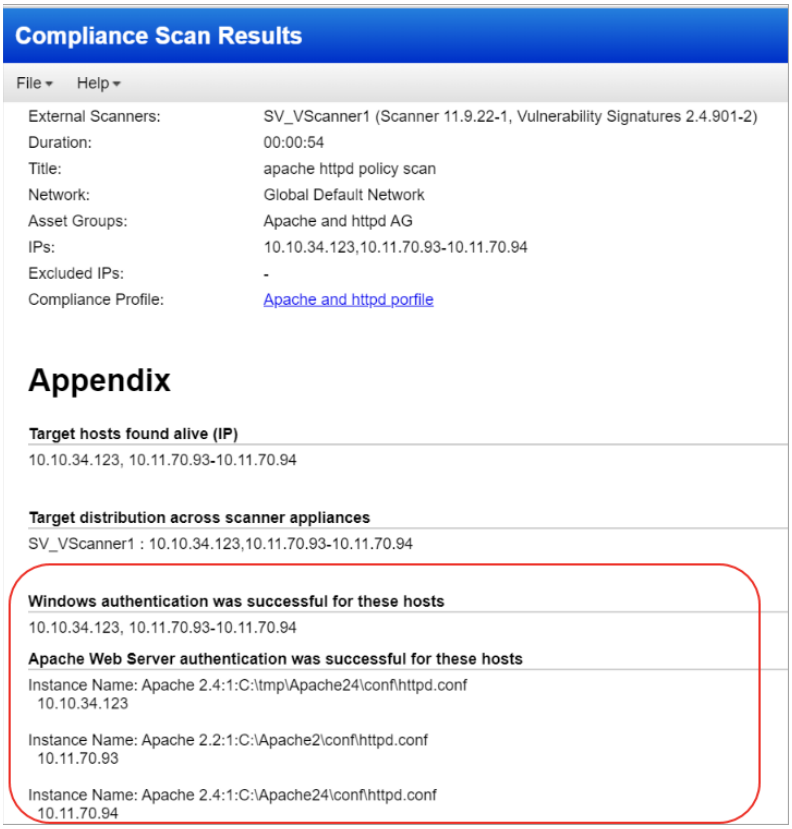

When you view the authentication record details, the **Windows Parameters** tab shows the configuration file and the binary directory paths that you have provided when creating or editing the record for the web server instance.



Sample authentication status for the Apache Web Server instances on Windows host.



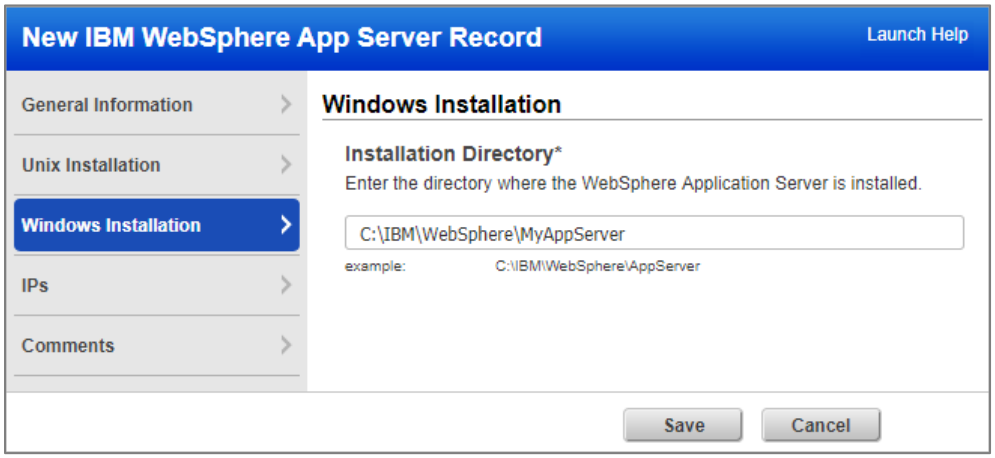

Here's sample Compliance Scan Results showing successful authentication for Apache Web Server instances on Windows hosts.



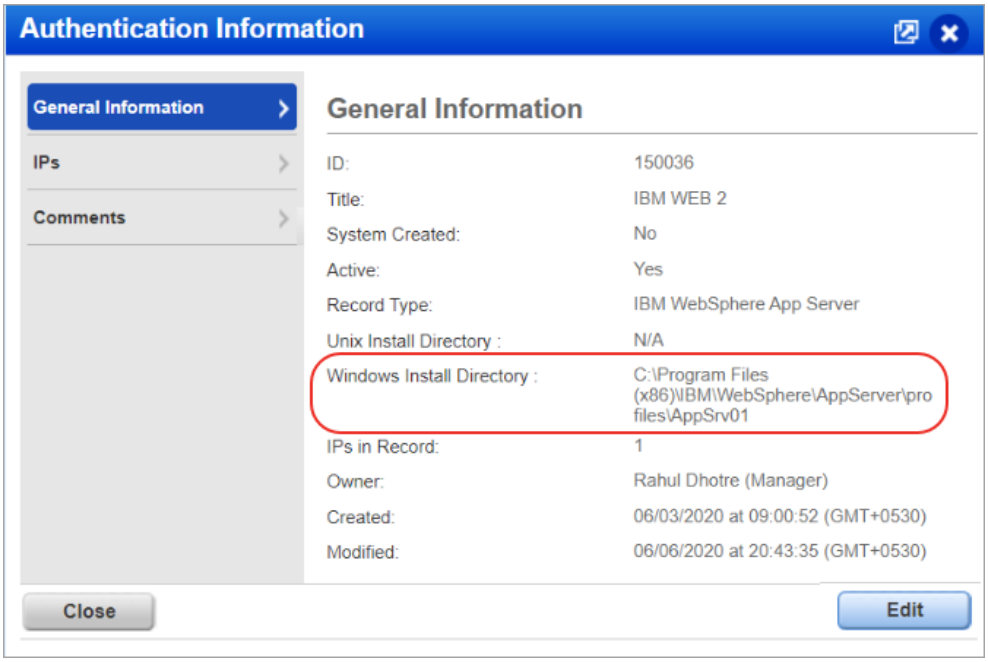
## Windows Support for the IBM WebSphere Application Server Record

You can now create and update IBM WebSphere Application Server record to authenticate to a WebSphere Application Server 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 web server.

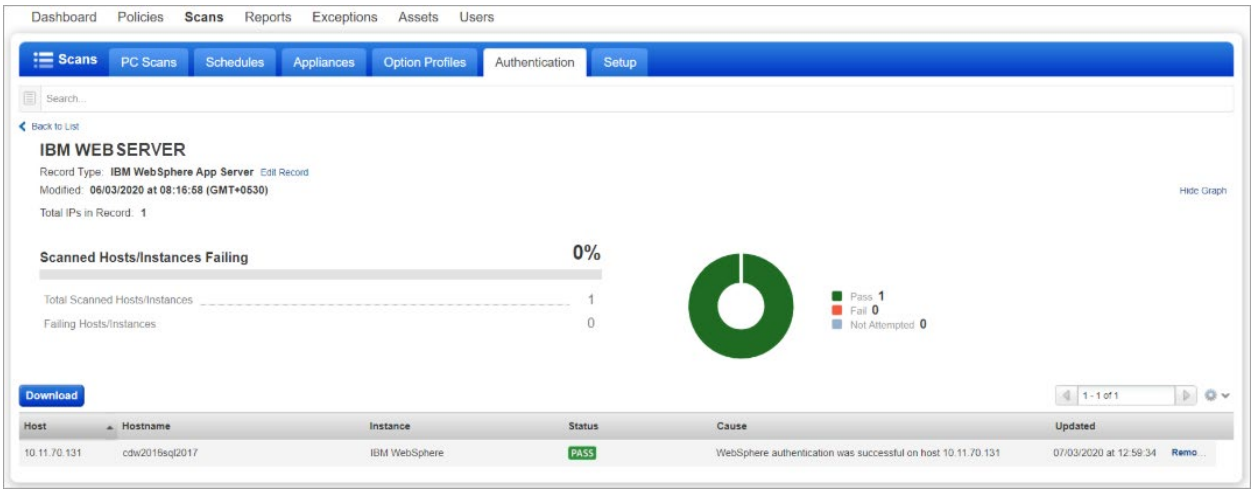
To support authenticated scans for IBM WebSphere App Server Record server running on a Windows host we have added a new **Windows Installation** tab. You will see the new tab when you create or edit an IBM WebSphere App Server Record. In the tab, you have to specify the Windows directory where the WebSphere Application Server is installed.



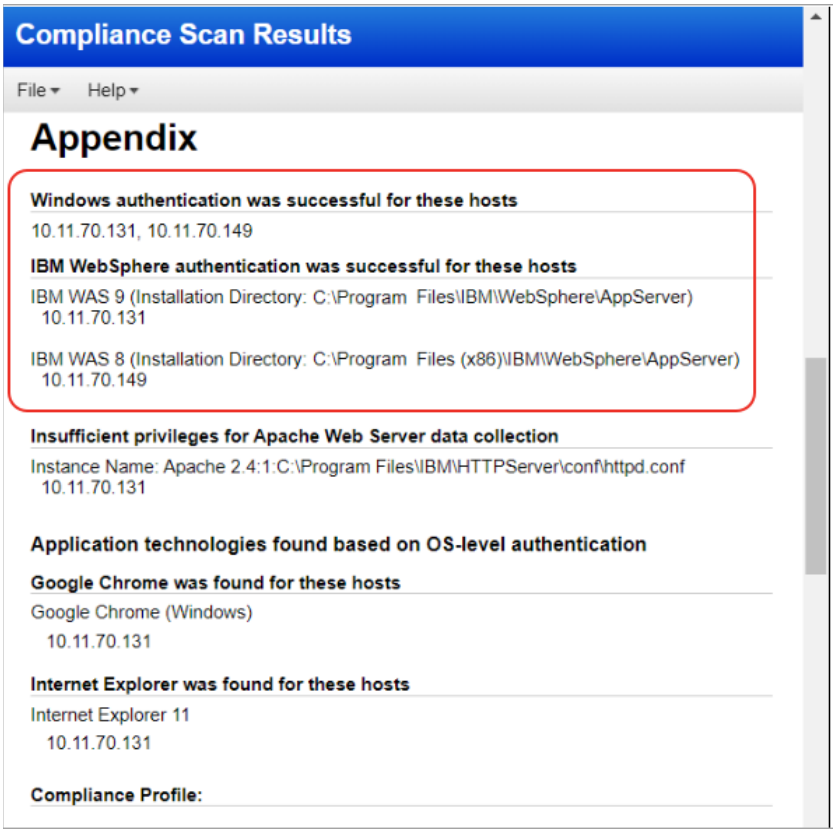

When you view the authentication record details, the **General Information** tab shows the Windows installation directory that you have provided when creating or editing the record for the web server instance.



Sample authentication status of the IBM WebSphere App Server record for Windows.




Sample Compliance Scan Results showing authentication successful for IBM WebSphere instances running on Windows hosts.



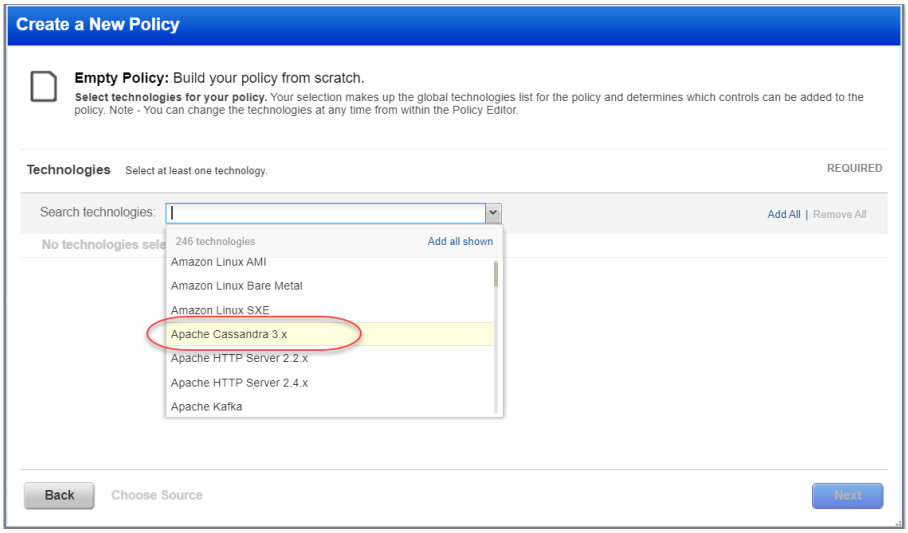
## Support for OS Authentication-Based Technology Apache Cassandra 3.x

We've expanded our support of OS authentication-based technologies to include 'Apache Cassandra 3.x'. For these technologies, you can collect technology data using the underlying OS technology (in this case Unix) without the need to create authentication records.

The Apache Cassandra 3.x technology is now available for inclusion in your compliance policies and when searching controls. You'll also see Apache Cassandra 3.x host instance information in policy compliance authentication reports, scan results and policy reports.

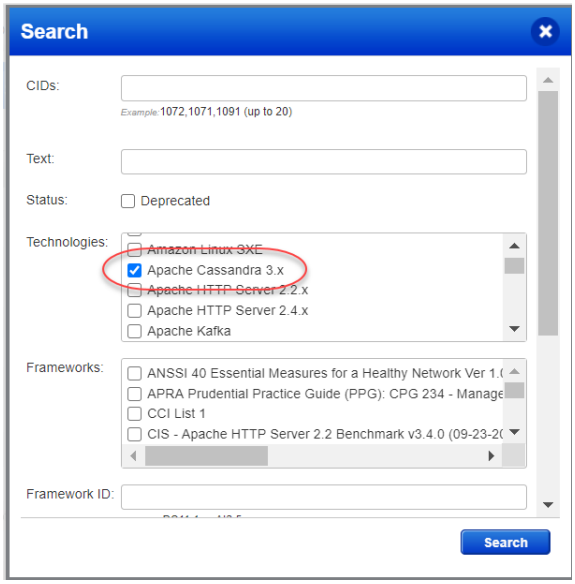
### Policy Editor

You can now select the Apache Cassandra 3.x technology for your compliance policies.



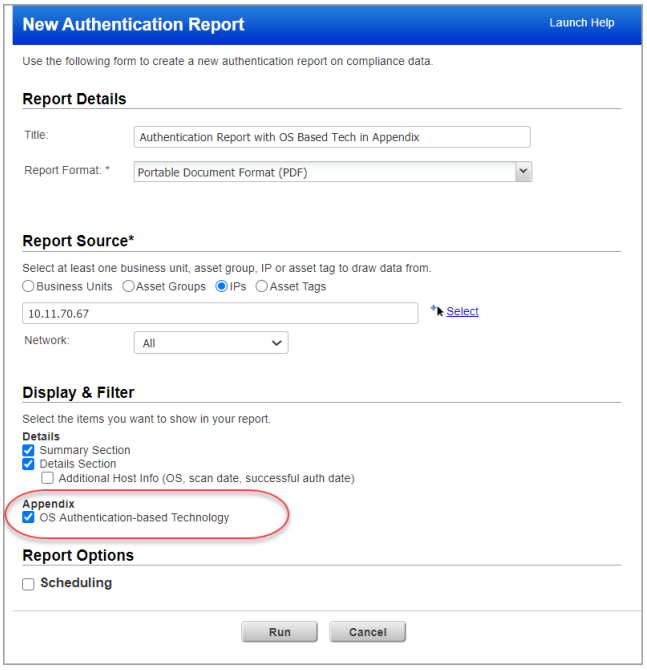

### Search Controls

You'll also see Apache Cassandra 3.x when searching controls. Go to Policies > Controls > Search and select Apache Cassandra 3.x in the list of Technologies.

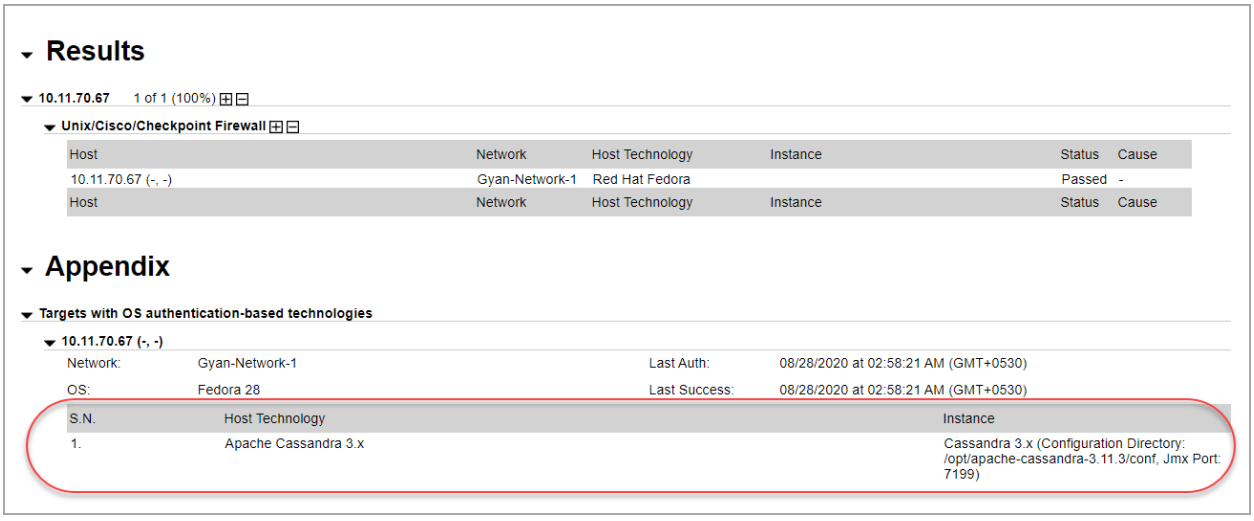


### Authentication Reports

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**.

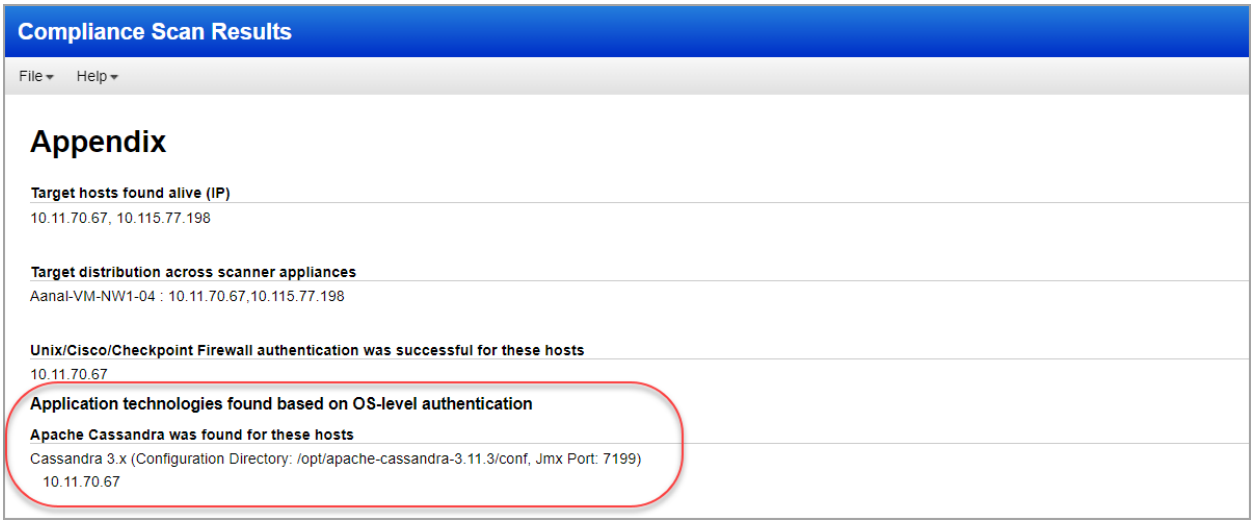



Scroll down to the **Appendix** section of your report to see **Targets with OS authentication-based technologies**.



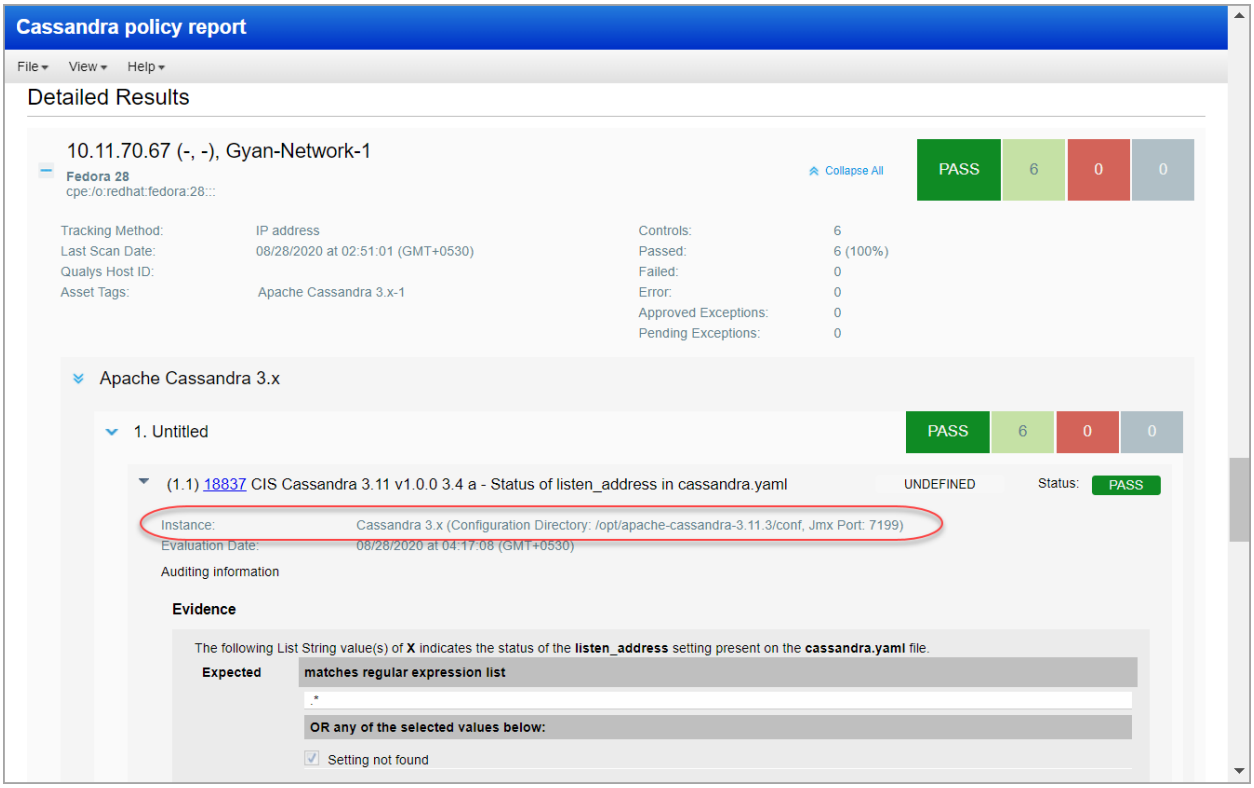
### Scan Results

You'll see Cassandra 3.x listed in the **Appendix** section of compliance scan results under **Application technologies found based on OS-level authentication**.




### Policy Reports

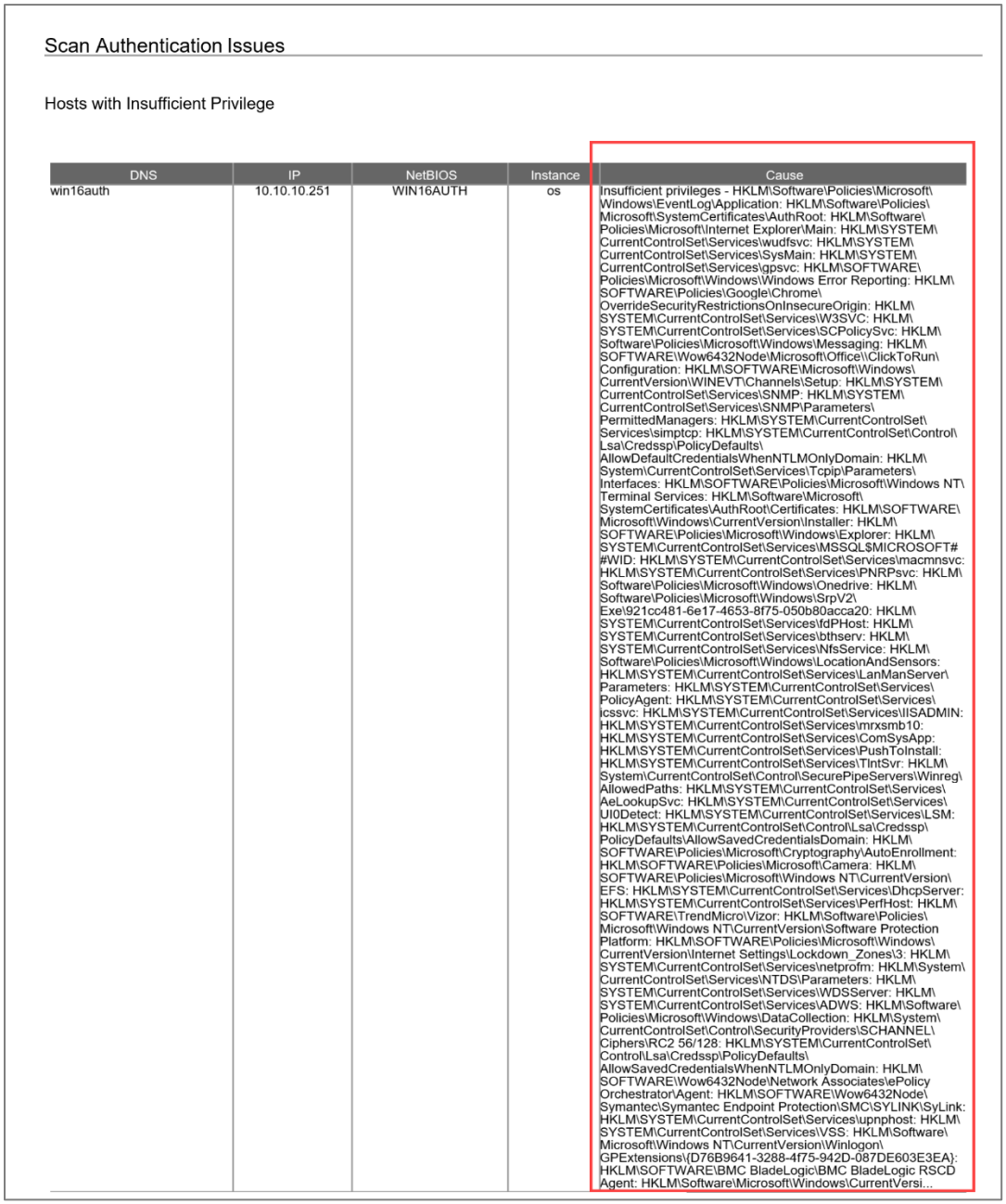
You'll also see Cassandra 3.x host instance information in your compliance policy reports.



## Comprehensive information about ‘Insufficient Privileges’

Passing a scan with ‘Insufficient Privileges’ can be as problematic as a ‘failed’ authentication attempt. In case of an ‘Insufficient Privileges’ result, it’s necessary to know the registries or directories to which the Qualys scanning account needs access for scanning. Based on this information, you can take corrective actions to ensure successful assessment of compliance posture of your IT assets. With this release, you find a more comprehensive reason for the ‘Insufficient Privileges’ result. This information is available in a compliance scan result and an authentication report.

Here’s a sample compliance scan result. In the **Cause** column of the **Scan Authentication Issues** table, you can view the list of registries on which the Qualys scanning account needs access privileges to execute a compliance scan on the host having the 10.10.10.251 IP address.

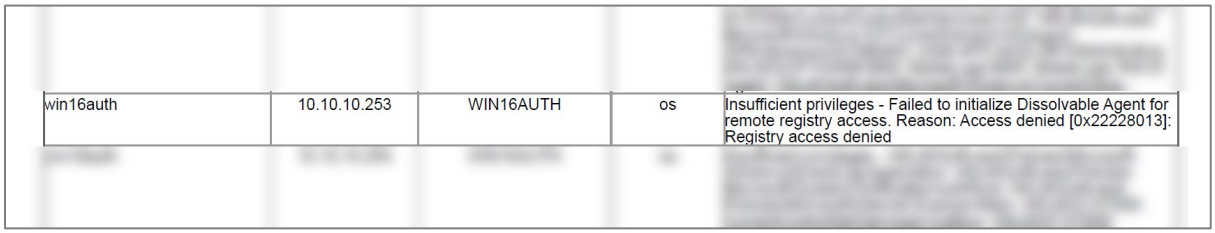


Scan Authentication Issues

Hosts with Insufficient Privilege

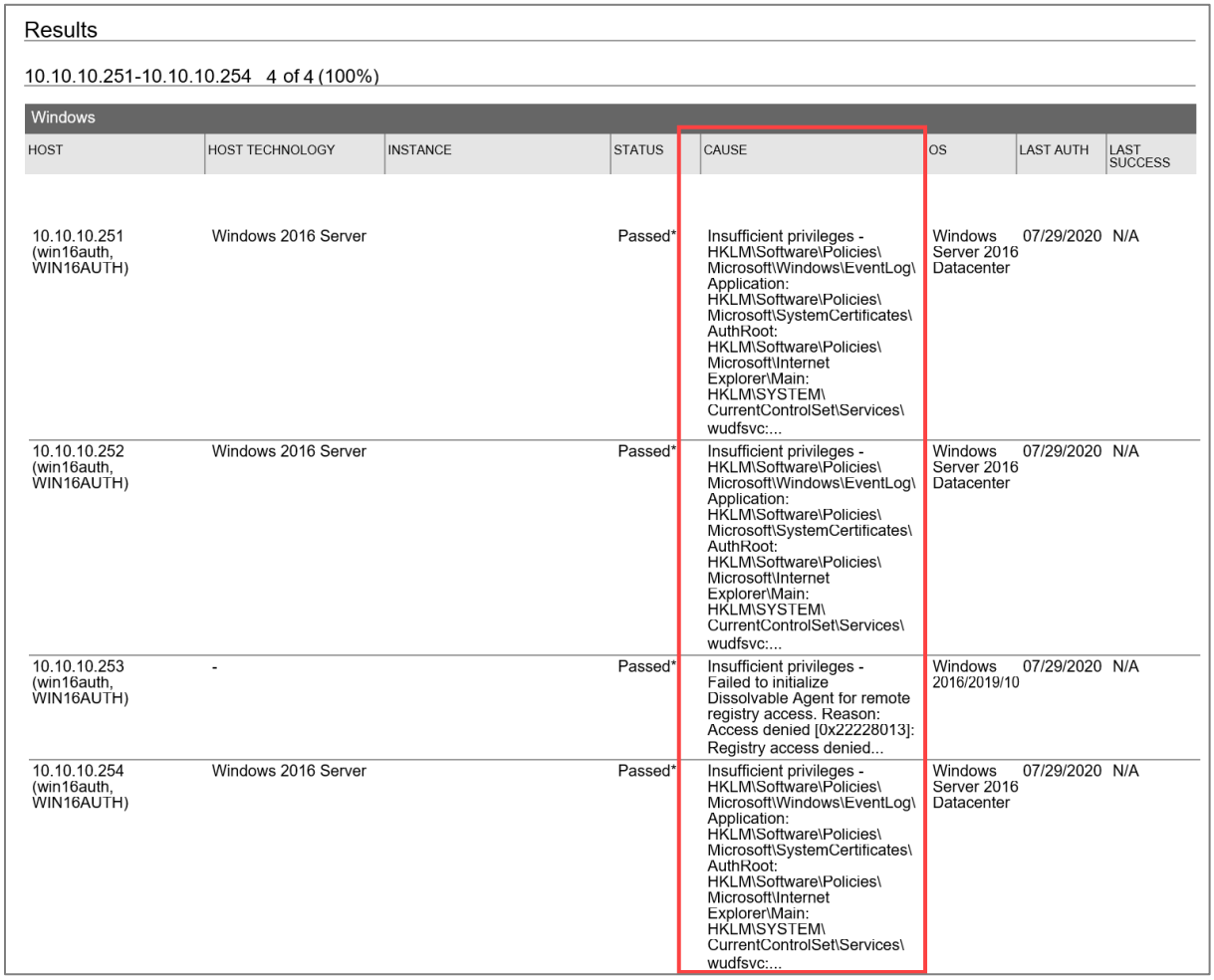
| DNS | IP | NetBIOS | Instance | Cause |
|---|---|---|---|---|
| win16auth | 10.10.10.251 | WIN16AUTH | os | Insufficient privileges - HKLM\Software\Policies\Microsoft\ Windows\EventLog\Application: HKLM\Software\Policies\ Microsoft\SystemCertificates\AuthRoot: HKLM\Software\ Policies\Microsoft\Internet Explorer\Main: HKLM\SYSTEM\ CurrentControlSet\Services\wudfsvc: HKLM\SYSTEM\ CurrentControlSet\Services\SysMain: HKLM\SYSTEM\ CurrentControlSet\Services\gpsvc: HKLM\SOFTWARE\ Policies\Microsoft\Windows\Windows Error Reporting: HKLM\ SOFTWARE\Policies\Google\Chrome\ OverrideSecurityRestrictionsOnInsecureOrigin: HKLM\ SYSTEM\CurrentControlSet\Services\W3SVC: HKLM\ SYSTEM\CurrentControlSet\Services\SCPolicySvc: HKLM\ Software\Policies\Microsoft\Windows\Messaging: HKLM\ SOFTWARE\Wow6432Node\Microsoft\Office\\ClickToRun\ Configuration: HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\WINEVT\Channels\Setup: HKLM\SYSTEM\ CurrentControlSet\Services\SNMP: HKLM\SYSTEM\ CurrentControlSet\Services\SNMP\Parameters\ PermittedManagers: HKLM\SYSTEM\CurrentControlSet\ Services\simptcp: HKLM\SYSTEM\CurrentControlSet\Control\ Lsa\Credssp\PolicyDefaults\ AllowDefaultCredentialsWhenNTLMOnlyDomain: HKLM\ System\CurrentControlSet\Services\Tcpip\Parameters\ Interfaces: HKLM\SOFTWARE\Policies\Microsoft\Windows NT\ Terminal Services: HKLM\Software\Microsoft\ SystemCertificates\AuthRoot\Certificates: HKLM\SOFTWARE\ Microsoft\Windows\CurrentVersion\Installer: HKLM\ SOFTWARE\Policies\Microsoft\Windows\Explorer: HKLM\ SYSTEM\CurrentControlSet\Services\MSSQL$MICROSOFT# #WID: HKLM\SYSTEM\CurrentControlSet\Services\macmnsvc: HKLM\SYSTEM\CurrentControlSet\Services\PNRPsvc: HKLM\ Software\Policies\Microsoft\Windows\Onedrive: HKLM\ Software\Policies\Microsoft\Windows\SrpV2\ Exe\921cc481-6e17-4653-8f75-050b80acca20: HKLM\ SYSTEM\CurrentControlSet\Services\fdPHost: HKLM\ SYSTEM\CurrentControlSet\Services\bthserv: HKLM\ SYSTEM\CurrentControlSet\Services\NfsService: HKLM\ Software\Policies\Microsoft\Windows\LocationAndSensors: HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\ Parameters: HKLM\SYSTEM\CurrentControlSet\Services\ PolicyAgent: HKLM\SYSTEM\CurrentControlSet\Services\ icssvc: HKLM\SYSTEM\CurrentControlSet\Services\IISADMIN: HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10: HKLM\SYSTEM\CurrentControlSet\Services\ComSysApp: HKLM\SYSTEM\CurrentControlSet\Services\PushToInstall: HKLM\SYSTEM\CurrentControlSet\Services\TlntSvr: HKLM\ System\CurrentControlSet\Control\SecurePipeServers\Winreg\ AllowedPaths: HKLM\SYSTEM\CurrentControlSet\Services\ AeLookupSvc: HKLM\SYSTEM\CurrentControlSet\Services\ UI0Detect: HKLM\SYSTEM\CurrentControlSet\Services\LSM: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Credssp\ PolicyDefaults\AllowSavedCredentialsDomain: HKLM\ SOFTWARE\Policies\Microsoft\Cryptography\AutoEnrollment: HKLM\SOFTWARE\Policies\Microsoft\Camera: HKLM\ SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\ EFS: HKLM\SYSTEM\CurrentControlSet\Services\DhcpServer: HKLM\SYSTEM\CurrentControlSet\Services\PerfHost: HKLM\ SOFTWARE\TrendMicro\Vizor: HKLM\Software\Policies\ Microsoft\Windows NT\CurrentVersion\Software Protection Platform: HKLM\SOFTWARE\Policies\Microsoft\Windows\ CurrentVersion\Internet Settings\Lockdown_Zones\3: HKLM\ SYSTEM\CurrentControlSet\Services\netprofm: HKLM\System\ CurrentControlSet\Services\NTDS\Parameters: HKLM\ SYSTEM\CurrentControlSet\Services\WDSServer: HKLM\ SYSTEM\CurrentControlSet\Services\ADWS: HKLM\Software\ Policies\Microsoft\Windows\DataCollection: HKLM\System\ CurrentControlSet\Control\SecurityProviders\SCHANNEL\ Ciphers\RC2 56/128: HKLM\SYSTEM\CurrentControlSet\ Control\Lsa\Credssp\PolicyDefaults\ AllowSavedCredentialsWhenNTLMOnlyDomain: HKLM\ SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent: HKLM\SOFTWARE\Wow6432Node\ Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink: HKLM\SYSTEM\CurrentControlSet\Services\upnphost: HKLM\ SYSTEM\CurrentControlSet\Services\VSS: HKLM\Software\ Microsoft\Windows NT\CurrentVersion\Winlogon\ GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}: HKLM\SOFTWARE\BMC BladeLogic\BMC BladeLogic RSCD Agent: HKLM\Software\Microsoft\Windows\CurrentVersi... |

Here's another sample. In this case, you get to know that on the host having the 10.10.10.253 IP address, Qualys dissolvable agent could not be initialized due to lack of registry access.



| | | | | |
|---|---|---|---|---|
| win16auth | 10.10.10.253 | WIN16AUTH | os | Insufficient privileges - Failed to initialize Dissolvable Agent for remote registry access. Reason: Access denied [0x22228013]: Registry access denied |

In the authentication report, we provide the same details in the **CAUSE** column of the **Results** table.



Results

10.10.10.251-10.10.10.254 4 of 4 (100%)

Windows

| HOST | HOST TECHNOLOGY | INSTANCE | STATUS | CAUSE | OS | LAST AUTH | LAST SUCCESS |
|---|---|---|---|---|---|---|---|
| 10.10.10.251 (win16auth, WIN16AUTH) | Windows 2016 Server | | Passed* | Insufficient privileges - HKLM\Software\Policies\ Microsoft\Windows\EventLog\ Application: HKLM\Software\Policies\ Microsoft\SystemCertificates\ AuthRoot: HKLM\Software\Policies\ Microsoft\Internet Explorer\Main: HKLM\SYSTEM\ CurrentControlSet\Services\ wudfsvc:... | Windows Server 2016 Datacenter | 07/29/2020 | N/A |
| 10.10.10.252 (win16auth, WIN16AUTH) | Windows 2016 Server | | Passed* | Insufficient privileges - HKLM\Software\Policies\ Microsoft\Windows\EventLog\ Application: HKLM\Software\Policies\ Microsoft\SystemCertificates\ AuthRoot: HKLM\Software\Policies\ Microsoft\Internet Explorer\Main: HKLM\SYSTEM\ CurrentControlSet\Services\ wudfsvc:... | Windows Server 2016 Datacenter | 07/29/2020 | N/A |
| 10.10.10.253 (win16auth, WIN16AUTH) | - | | Passed* | Insufficient privileges - Failed to initialize Dissolvable Agent for remote registry access. Reason: Access denied [0x22228013]: Registry access denied... | Windows 2016/2019/10 | 07/29/2020 | N/A |
| 10.10.10.254 (win16auth, WIN16AUTH) | Windows 2016 Server | | Passed* | Insufficient privileges - HKLM\Software\Policies\ Microsoft\Windows\EventLog\ Application: HKLM\Software\Policies\ Microsoft\SystemCertificates\ AuthRoot: HKLM\Software\Policies\ Microsoft\Internet Explorer\Main: HKLM\SYSTEM\ CurrentControlSet\Services\ wudfsvc:... | Windows Server 2016 Datacenter | 07/29/2020 | N/A |

### Truncated text in Cause column

The maximum character limit up to which the text in the Cause column in a compliance scan result is visible is set to 4000. In an authentication report, this limit is set to 256 characters. If the text exceeds this limit, it is truncated by using an ellipsis (…). In such a case, you can see the complete text in your database records.

## Support for Additional Middleware Technologies

We have now added support on the following technologies for Middleware Assessment.

Applicable on Windows Agent 4.0.x

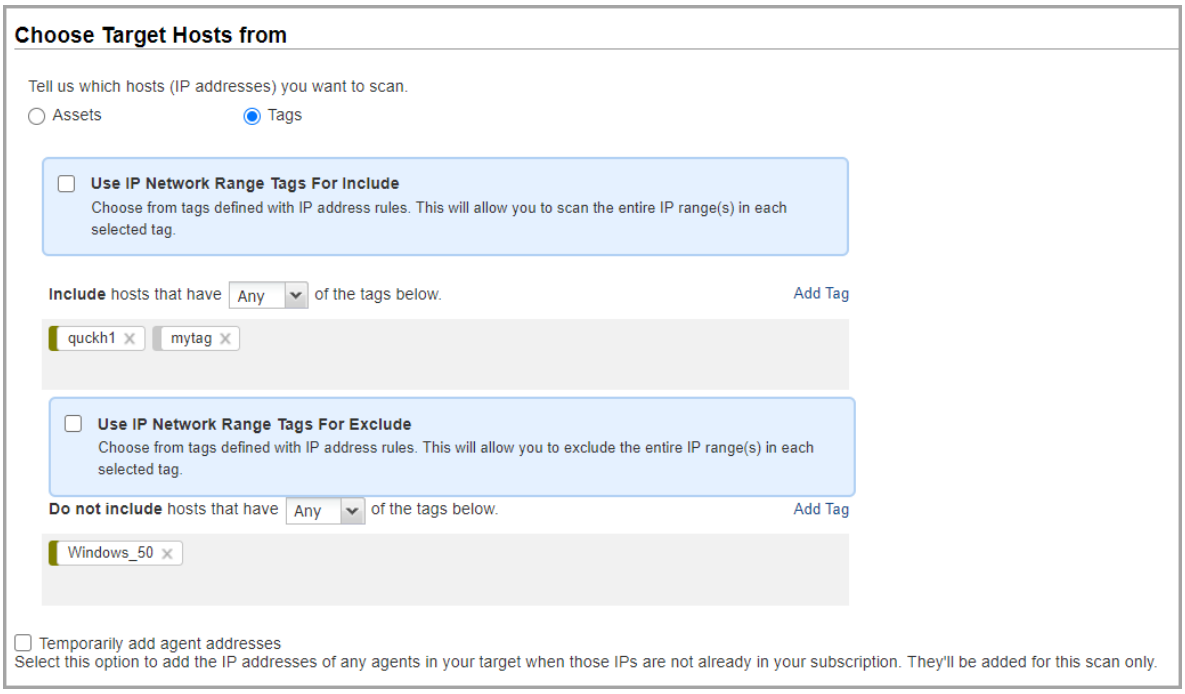
- Internet Explorer 9, 10, 11
- Microsoft Office 2013, 2016, 2019
- Microsoft Office Access 2013, 2016, 2019
- Microsoft Office Excel 2013, 2016, 2019
- Microsoft Office Outlook 2013, 2016, 2019
- Microsoft Office PowerPoint 2013, 2016, 2019
- Microsoft Office Word 2013, 2016, 2019

# Qualys Cloud Platform

## Separate Options for Use IP Network Range Tags for Include and Exclude

With this release, we are providing separate options for the Use IP Network Range Tags option for include and exclude tags. These new options are available when specifying the scan target using tags when you launch and schedule vulnerability and compliance scans.

In the following example for launching a vulnerability scan, you'll see separate options for the Use IP Network Range Tags option for include and exclude tags.




**Use IP Network Range Tags Include** - This option lets you scan all IPs defined in a tag with the IP address tag rule even if the IPs don't already have the tag assigned to them. We'll apply the tag to each IP that doesn't already have it.

**Use IP Network Range Tags Exclude** - This option lets you exclude all IPs defined in a tag with the IP address tag rule.

You can include or exclude hosts having certain tags. Simply, click **Add Tag** and select tags to include or exclude in the scan.

## Perimeter Scan Supports Azure Virtual Machines Scanning in Azure Cloud

This release introduces the ability to scan public facing virtual machines in your Azure cloud environment using Cloud Perimeter Scanning for VM and PC.

### Good to Know

- The "Cloud Perimeter Azure VM Scan" feature must be enabled for your subscription. You'll also need these features enabled: Cloud Perimeter Scanning, EC2 Scanning, Scan by Hostname.

- Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.

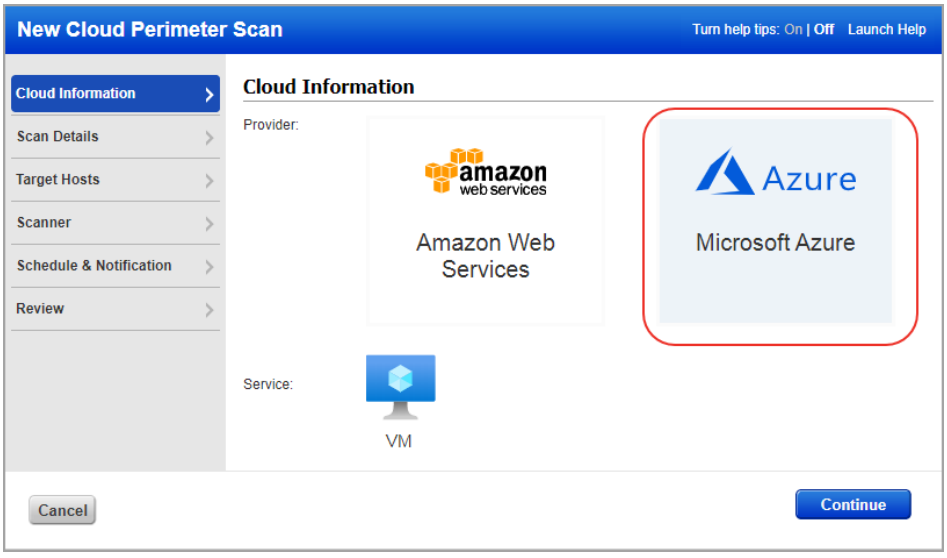
- We allow you to create/update a cloud perimeter scan job through Cloud Perimeter Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

### Create/Update Cloud Perimeter Scan Job

To create a cloud perimeter scan job for Azure cloud, go to **Scans** > **Scans** > **New > Cloud Perimeter Scan**.

1) In the **Cloud Information** tab, you will now see **Azure** cloud provider. Select the Azure icon to scan the Azure VM machines.

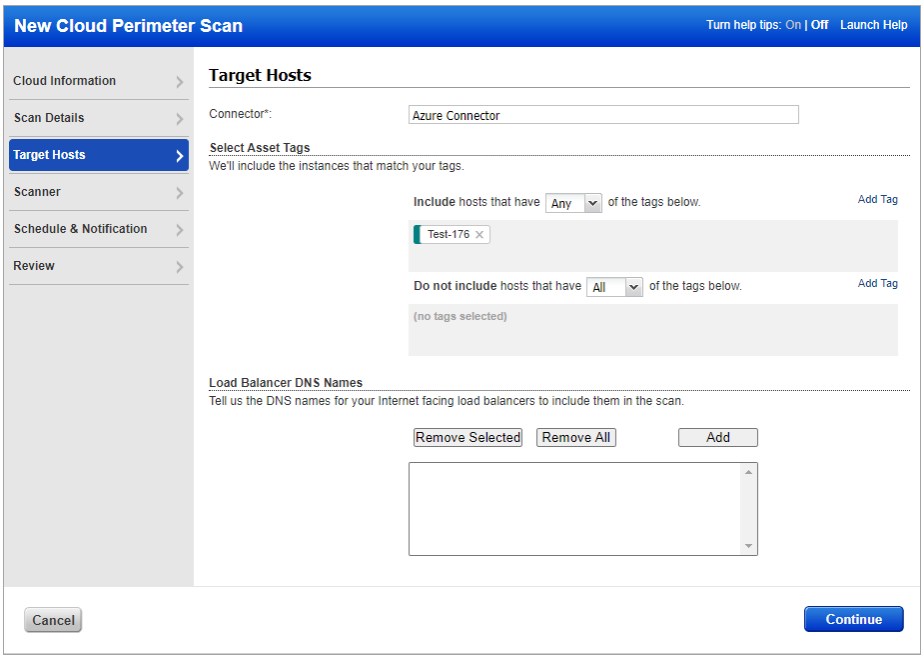
Note that while updating the scan, you do not have to option to change the Provider. We will populate the values that you provided for the scan for the Cloud Provider selected at the time of creating the scan.




2) Go to the **Scan Details** tab and give the scan a name and select the option profile as you do for EC2 scans.

3) Go to the **Target Hosts** tab to select the public facing Azure VM machines on which you want to run the Cloud Perimeter scan. From the **Connectors** drop-down, select an Azure connector. The Connector drop-down lists the connectors that you have configured in AssetView.

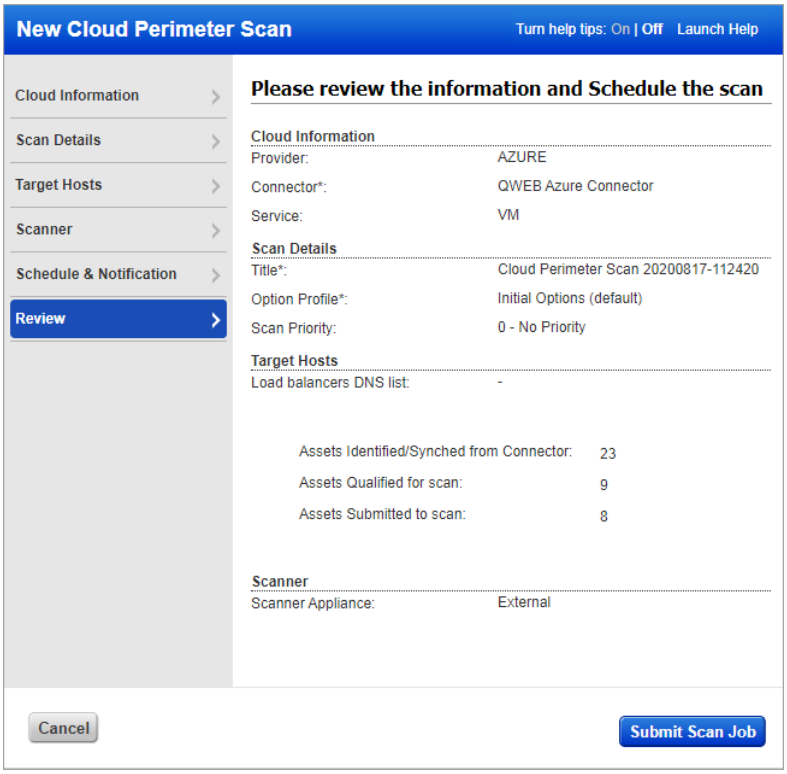
Select asset tags to further filter the Azure VM assets fetched from the Azure connector. For load balancers, manually add the DNS names of internet facing load balancers. For Azure VM scan, we do not support pulling load balancer DNS names from the CloudView module.




4) Go to the **Scanner** and **Schedule & Notification** tabs to select the External/Internal scanner and schedule the scan as you do for EC2 scans. We will allow you to select internal scanner for the scan if using internal scanners for cloud perimeter scan is enabled for your subscription.

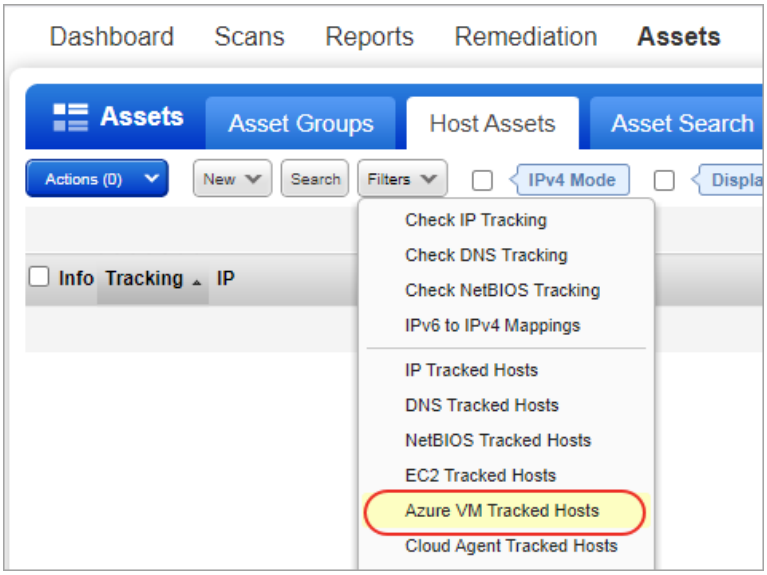
5) Go to the **Review** tab. In the **Target Hosts** section, we will show you 1) how many public facing Azure VM assets are fetched from the connector, 2) assets that are qualified for the scan and 3) out of the qualified assets, how many assets are activated in VM on which the scan will be launched.

6) Finally, submit the scan job.

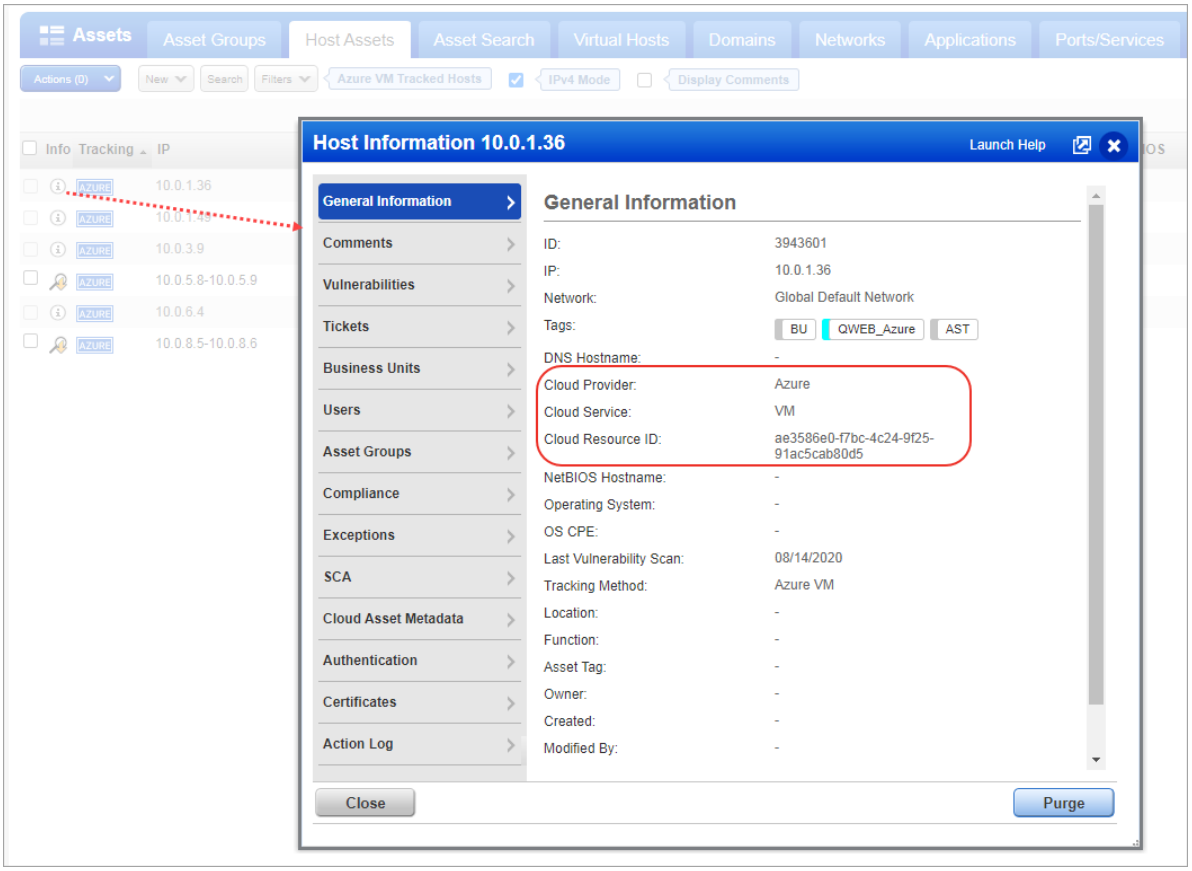


### View Azure VM Tracked Host Assets in Host Assets

Go to **Assets** > **Host Assets** > **Filters** to search for the Azure VM tracked assets.




Click the info button to view the cloud provider name (which is Azure for Azure VM assets), cloud service name (VM for Azure VM assets), and resource ID for the Azure Virtual Machine in the **Host Information** screen. The **Cloud Asset Metadata** tab will show the metadata information for the host.



## Accepted Special Characters while Creating Password

You can now use the following special characters while creating a user-defined password.

( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /

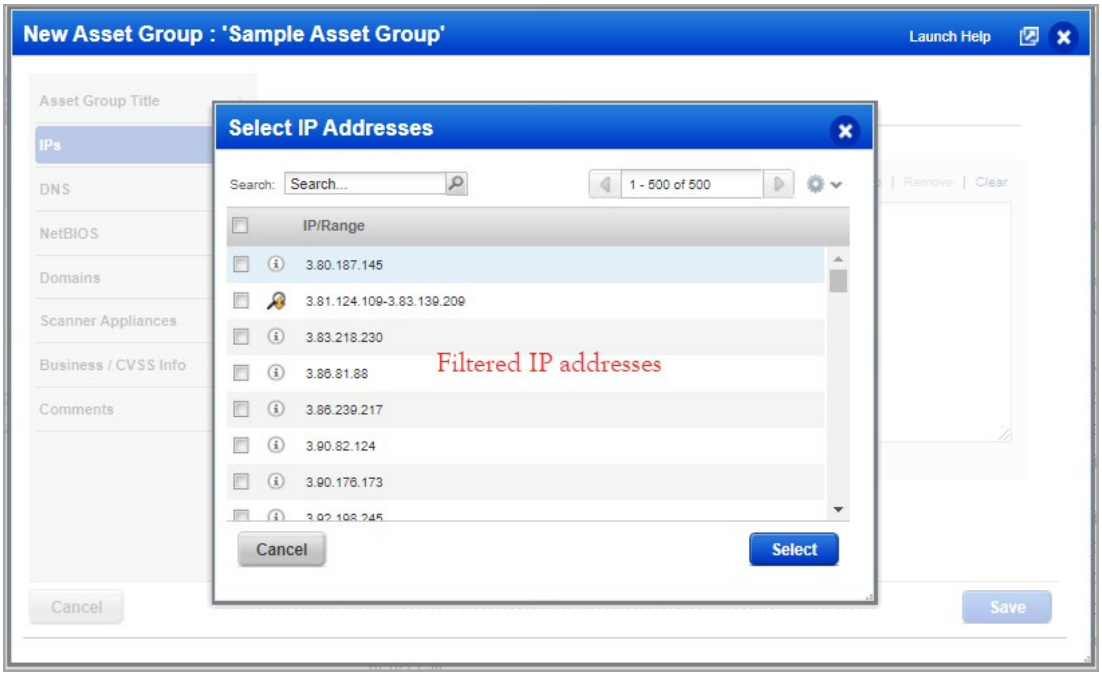
These special characters can be used when you create a password during:

- First login (new account creation)
- Change password
- Forgot password

## Network-specific IP Addresses for Asset Group Creation

When you create an asset group using custom network, we will now filter the list of IP addresses you can add to the asset group, based on your network selection. Earlier, the list of IP addresses was not filtered and if the user picked an IP address that was not associated with the network selected for the asset group, they would get an error.

Navigate to **Assets** > **Asset Groups** > **New** > **Asset Group**. Go to the IPs tab and choose "Select IPs" and you can pick from a list of IPs associated with the network you selected.



## Issues Addressed

- Updated information related to How to configure Email Contact for notifications in the online help for better clarity and understanding.
- Updated information and removed references related to penetration testing form in the online help and related PDF documents.
- Updated the VM/PC API User Guide to provide more information for 'Aborted' and 'Blocked' status.
- Updated Online Help to include information for cloud agent assets in remediation policy.
- Updated Online Help to fix the 'Learn more' link in the Setting up EC2 Connector topic.
- When creating or editing a Palo Alto auth record with empty auth vault fields, the error message now displays the blank vault fields that need to be populated with information.
- You can now create multiple Apache Web Server authentication records with the same IP address as long as the values for Apache Configuration File and Apache Control Command are unique. Note that the paths in Windows are case-sensitive.
- Updated the VM/PC Online help to standardize the operating system names and list the authentication technologies in alphabetical order in the Authentication Technologies Matrix topic.
- Fixed an issue to show you the asset group information for asset groups added to a scheduled scan. Go to Scans > Schedules > Info > Target Tab, select an asset group, and click the View button to view the information of the asset group.
- Updated the VM/PC API Quick Reference guide to add the Azure key vault information and the VM/PC API guide to fix the parameter name from cert to certificate.
- Fixed an issue where hack_attempt error was occurring while downloading PC interactive report which was launched with IP in the custom network.
- Fixed an issue where the Asset Group List API returned a generic message asking the user to contact customer support.
- Fixed an issue where report generation was interrupted and an exception message was displayed in the logs.
- Updated the online help for the Unix File Content Check UDC to help you avoid discrepancy in agent-based results and scanner-based results of a compliance scan of the same host.