Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.17

February 1, 2022

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

Qualys Cloud Platform

Qualys Policy Compliance (PC/SCAP/SCA)

Qualys Vulnerability Management (VM)

Qualys 10.17 brings you many more improvements and updates! Learn more

Qualys Cloud Platform

Support for Scanning Hosts in CDN by DNS Name

This release provides support for scanning hosts in a Content Delivery Network (CDN) environment by DNS name and maintaining separate results for each host even if they resolve to the same IP address. This is supported for vulnerability and compliance scanning by DNS name.

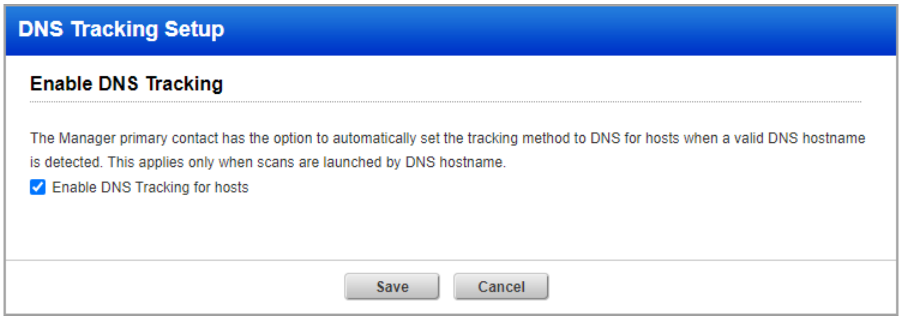
The issue:

When you launch a scan on multiple targets by DNS name and those DNS names resolve to the same IP address, then you will only get one set of scan results for one of the targets. For example, you launch a scan on 3 separate targets by DNS name: site1.test.com, site2.test.com and site3.test.com. All 3 DNS names resolve to the same IP address (10.10.10.1). When you launch the scan and the DNS names are all resolved to the same IP, two of the targets are removed from the scan because they are considered duplicates, and only one target is scanned. Only one asset record is saved for IP 10.10.10.1 and this record is updated with new scan results each time a scan is launched on a DNS name that resolves to this IP, even if these are different sites. This scanning model does not work for scanning hosts in a Content Delivery Network (CDN) environment where you have many sites with different DNS names but the same IP address.

The solution:

We have changed the scanning model in this release to allow users to launch scans on multiple targets by DNS name and get separate scan results for each target even if they resolve to the same IP address. Now if you launch a scan on site1.test.com, site2.test.com and site3.test.com, we will launch the scan on all 3 targets, and you will get separate scan results for all 3 targets. We will also save separate asset records for the different scan targets. The asset records will have the same IP address but different DNS names. When a new scan is launched by DNS name, only the appropriate asset record is updated with the new scan results.

To enable the DNS scanning, you need to enable DNS Tracking by going to **Scans** > **Setup** > **DNS Tracking**. If you scan by DNS hostname, the scan will be done based on DNS. DNS will be resolved to IP and the resolved IP will be DNS tracked irrespective of the earlier tracking defined. For example, if the resolved IP was configured as IP tracked, then after the DNS based scanning the IP will be DNS tracked.


DNS Tracking Setup

Enable DNS Tracking

The Manager primary contact has the option to automatically set the tracking method to DNS for hosts when a valid DNS hostname is detected. This applies only when scans are launched by DNS hostname.

☑ Enable DNS Tracking for hosts

Note for Scans on DNS Targets Behind a Load Balancer

Scans are launched on the IP address of an asset, and we use the authentication records in your account to authenticate to each scan target. Authentication is always used for compliance scans and is used for vulnerability scans when authentication is enabled in your option profile. When you launch a scan on a DNS name for a target behind a load balancer, the scanner will resolve the DNS name to the IP address of the load balancer and attempt authentication to the load balancer. This will not give you proper scan results. For targets behind a load balancer, launch the scan on the IP address instead of the DNS name and ensure you have authentication records for those IPs in your account.

Change to Reporting of DNS Hostname for EC2 Assets

We have made a change to how we report the DNS hostname for EC2 assets with cloud agents. This change will ensure that the expected hostname is displayed wherever asset details appear, including in Host-Based Scan Reports, Host Information page, other UI views and API outputs.

For EC2 assets with cloud agents, we will get the hostname from the agent scan results. For connector-only EC2 assets, we will use the private DNS name pulled from the connector.

For EC2 assets with a cloud agent

For EC2 assets with cloud agents, we get the DNS hostname for the asset from the agent scan results. When processing agent scan results, we first look at the value returned for FQDN, and we will use this value as the hostname for the asset whenever it is available. If the FQDN is not returned in the scan results, then we look at the value for DNS_HOSTNAME and we'll use this value if available. In the case where both the FQDN and DNS_HOSTNAME are not returned, we fall back to the private DNS hostname pulled from the connector.

To reiterate, when determining the hostname for an EC2 asset, we consider the following values in the order shown. If we get a value in the first step, then we are done. If not, we continue to the next step.

1 - FQDN value received in agent scan results. If available, this is the value used. If not available, continue to the next step.

2 - DNS_HOSTNAME value received in agent scan results. If available, this is the value used. If not available, continue to the next step.

3 - Private DNS Hostname pulled from the connector. This is used only when FQDN and DNS_HOSTNAME values are not returned in the agent scan results.

For EC2 agent assets, we will not overwrite the hostname value for the asset when processing scan results from internal EC2 scans or cloud perimeter scans. Instead, we will keep the value from the last agent scan.

For EC2 assets without a cloud agent (connector-only)

For connector-only EC2 assets, we will always report the private DNS hostname pulled from the connector as the hostname for the asset.

Administration Module Access for Administrator User

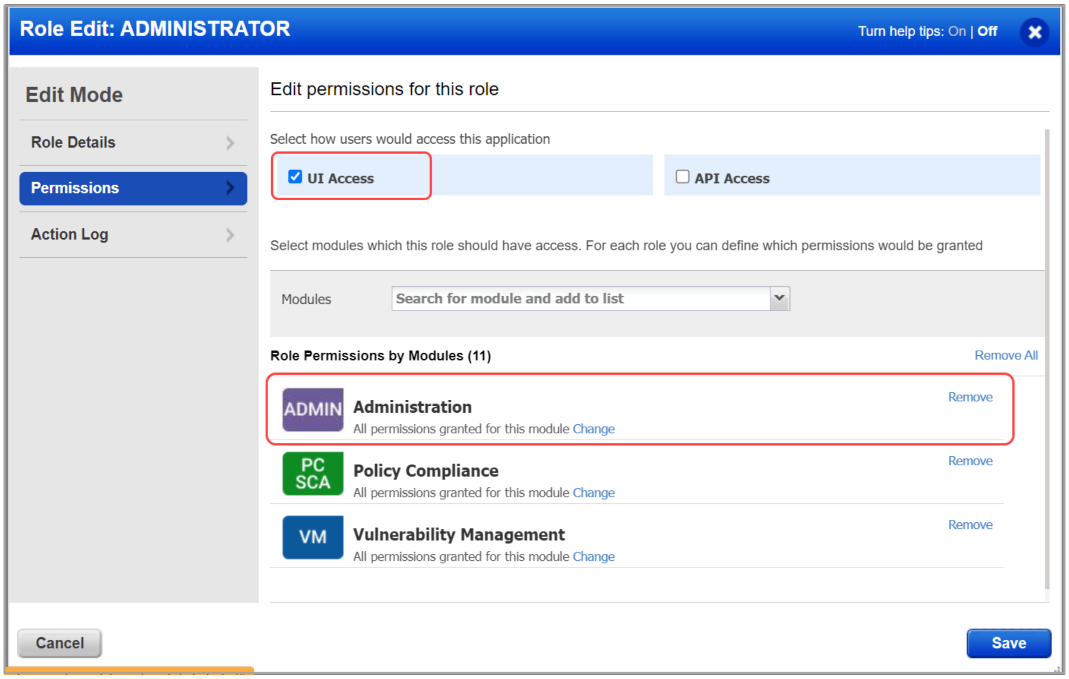
With this release, a Manager user can provide access to the Administration module for an Administrator user. Once this access is provided, the Administrator user can see the Administration module in the module picker.

A Manager user can provide this access from the Administration module using the following steps:

1) Click the **Administration** module from the module picker.

2) Select an Administrator user for which you need to provide 'Administration' module access.

3) Create or edit a role with the 'UI Access' enabled and the 'Administration' module is selected from the list of modules.



Role Edit: ADMINISTRATOR

Edit Mode

Edit permissions for this role

Select how users would access this application

☑ UI Access □ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

Modules: Search for module and add to list

Role Permissions by Modules (11)

Administration – All permissions granted for this module

Policy Compliance – All permissions granted for this module

Vulnerability Management – All permissions granted for this module

5) Click **Save** to apply your selections.

6) Now, log out from the Manager user and log in with the Administrator user for which you've provided access.

You'll notice that the 'Administration' module is displayed now in the module picker for the Administrator user.

Qualys Policy Compliance (PC/SCAP/SCA)

Include AWS Cloud Metadata in Compliance Policy Reports

Now you can include cloud asset metadata for your AWS assets in Compliance Policy Reports. Simply update your Policy Report Template in the UI and select the new “Cloud Metadata” option to include these details. This option is off by default.

When enabled, you’ll see the following cloud metadata for each AWS asset in your report:

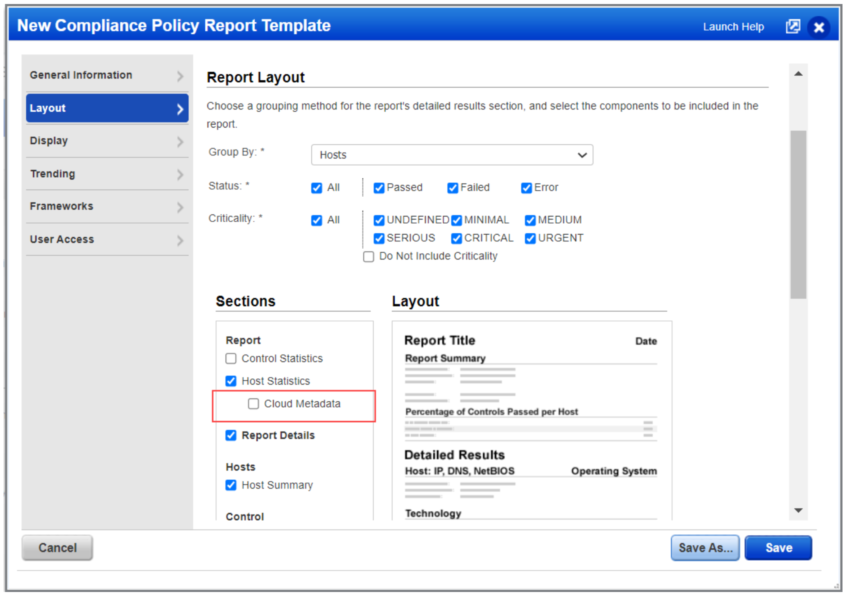
- Cloud Provider
- Cloud Service
- Cloud Resource ID
- Cloud Resource Type
- Cloud Account ID
- Cloud Image ID
- Cloud Resource Metadata

Cloud Resource Metadata for AWS includes: Public IP Address, Private IP Address, VPC ID, Subnet ID, Instance Type, Instance State, Group Name, Group ID, Region Code, Availability Zone, Reservation ID, Is Spot Instance, Local Hostname, MAC Address, Private DNS Name, Public DNS Name

Update to Compliance Policy Report Template

Select the new **Cloud Metadata** option in the report template to include this section in the report output for AWS assets. This option is off by default, and is only available when the **Host Statistics** option is also selected. The Cloud Metadata option is available whether you group the report by Hosts or Controls.

Go to **PC** > **Reports** > **Templates** > **New** > **Policy Template**. Then go to the **Layout** tab and **Sections** to pick the sections to include in the report.



Report Layout

Choose a grouping method for the report's detailed results section, and select the components to be included in the report.

Group By: * Hosts

Status: * ☑ All | ☑ Passed ☑ Failed ☑ Error

Criticality: * ☑ All | ☑ UNDEFINED ☑ MINIMAL ☑ MEDIUM ☑ SERIOUS ☑ CRITICAL ☑ URGENT

☐ Do Not Include Criticality

Sections

Report
☐ Control Statistics
☑ Host Statistics
☐ Cloud Metadata
☑ Report Details

Hosts
☑ Host Summary

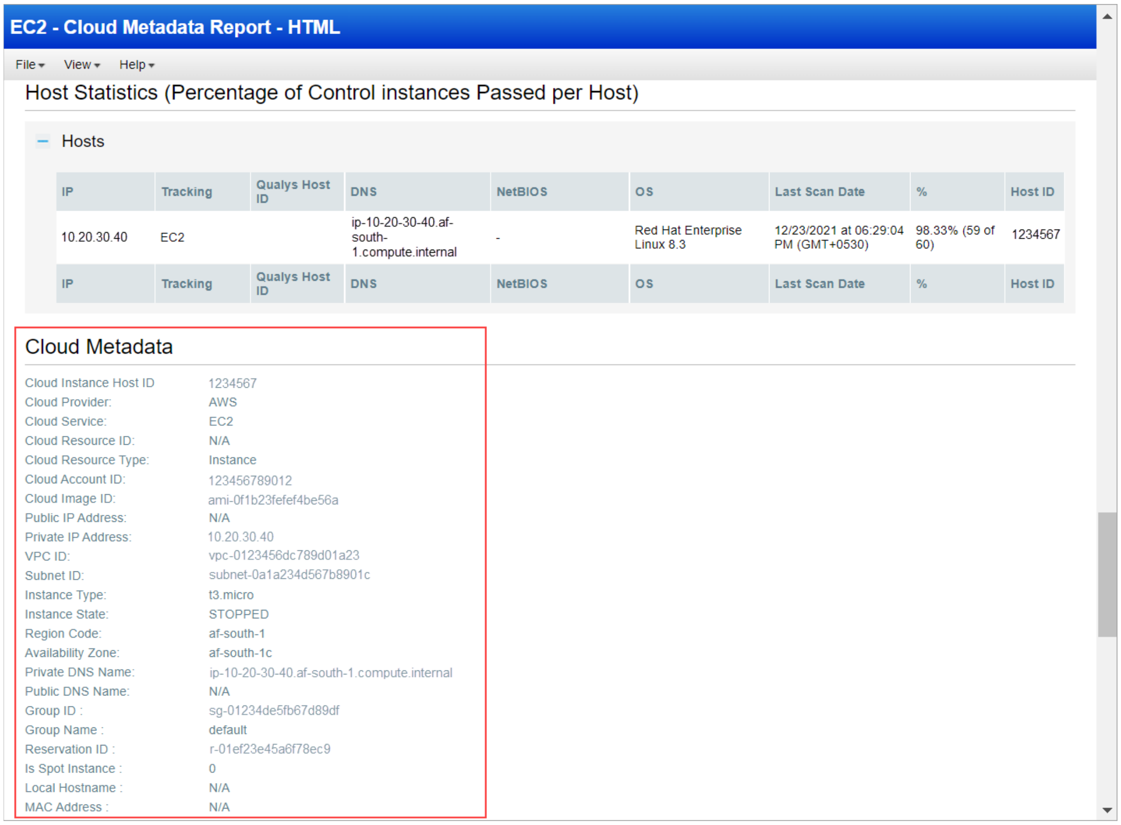
Control

Layout

Report Title — Date
Report Summary
Percentage of Controls Passed per Host
Detailed Results
Host: IP, DNS, NetBIOS — Operating System
Technology

Sample Policy Report

Here’s a sample policy report with the Cloud Metadata section shown for an AWS asset.



EC2 - Cloud Metadata Report - HTML

Host Statistics (Percentage of Control instances Passed per Host)

Hosts

IP	Tracking	Qualys Host ID	DNS	NetBIOS	OS	Last Scan Date	%	Host ID
10.20.30.40	EC2		ip-10-20-30-40.af-south-1.compute.internal	-	Red Hat Enterprise Linux 8.3	12/23/2021 at 06:29:04 PM (GMT+0530)	98.33% (59 of 60)	1234567
IP	Tracking	Qualys Host ID	DNS	NetBIOS	OS	Last Scan Date	%	Host ID

Cloud Metadata

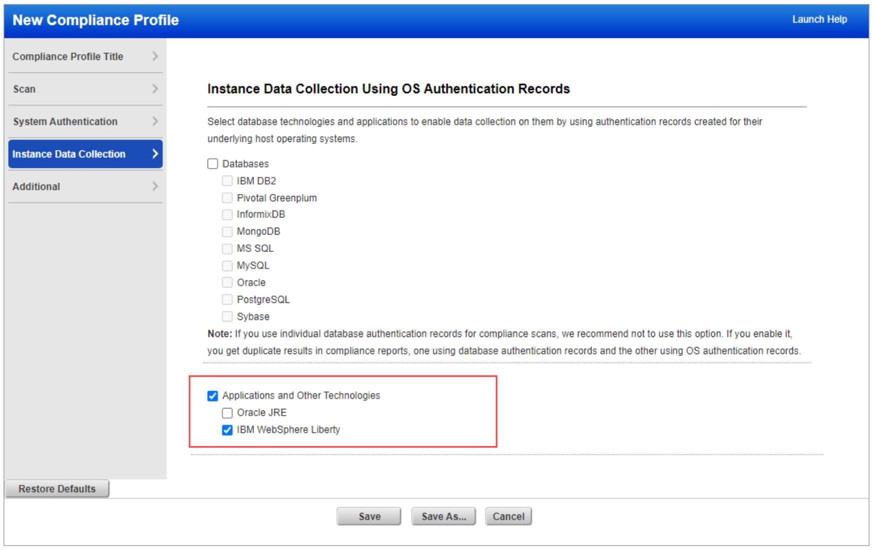
Cloud Instance Host ID	1234567
Cloud Provider:	AWS
Cloud Service:	EC2
Cloud Resource ID:	N/A
Cloud Resource Type:	Instance
Cloud Account ID:	123456789012
Cloud Image ID:	ami-0f1b23fefef4be56a
Public IP Address:	N/A
Private IP Address:	10.20.30.40
VPC ID:	vpc-0123456dc789d01a23
Subnet ID:	subnet-0a1a234d567b8901c
Instance Type:	t3.micro
Instance State:	STOPPED
Region Code:	af-south-1
Availability Zone:	af-south-1c
Private DNS Name:	ip-10-20-30-40.af-south-1.compute.internal
Public DNS Name:	N/A
Group ID :	sg-01234de5fb67d89df
Group Name :	default
Reservation ID :	r-01ef23e45a6f78ec9
Is Spot Instance :	0
Local Hostname :	N/A
MAC Address :	N/A

For samples in CSV and XML formats, see the Qualys Cloud Platform 10.17 API Release Notes.

Support for Instance Technology: IBM WebSphere Liberty 21.x

We've expanded our support of OS authentication-based technologies to include **IBM WebSphere Liberty 21.x**. We already support IBM WebSphere Liberty 19.x and 20.x. This support is available for Liberty instances running on Linux machines. Instance data collection for IBM WebSphere Liberty is performed using the underlying OS-based authentication record. This means you'll only need a Unix authentication record (with Sudo as root delegation). You do not need additional records for IBM WebSphere Liberty. The Unix record is used for the instance data collection.

As in previous releases, to perform instance data collection for IBM WebSphere Liberty using a scanner, you must select **IBM WebSphere Liberty** on the **Instance Data Collection** tab in the compliance profile. If you are using Cloud Agent for Policy Compliance (PC), IBM WebSphere Liberty instances are auto-discovered by the agent (see Middleware Assets).



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.

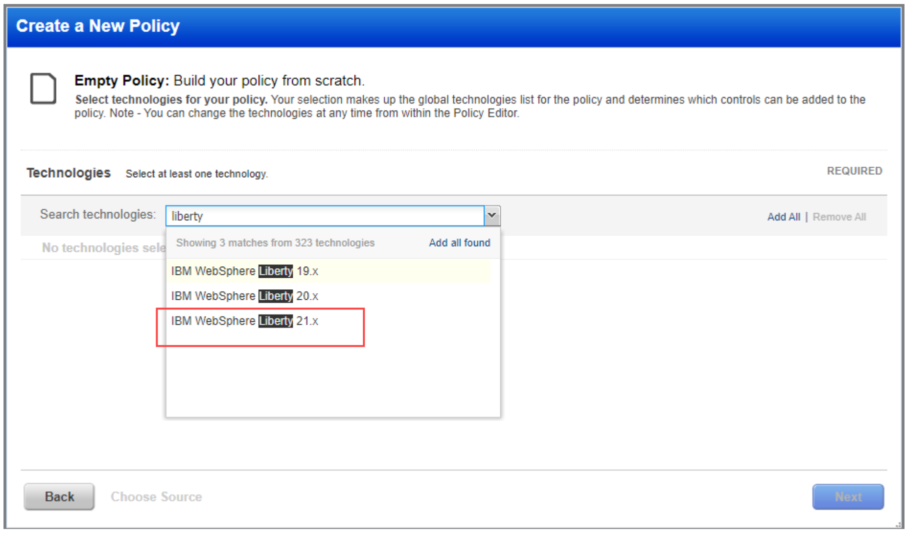
- ☐ Databases
  - ☐ IBM DB2
  - ☐ Pivotal Greenplum
  - ☐ InformixDB
  - ☐ MongoDB
  - ☐ MS SQL
  - ☐ MySQL
  - ☐ Oracle
  - ☐ PostgreSQL
  - ☐ Sybase

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
  - ☐ Oracle JRE
  - ☑ IBM WebSphere Liberty

Policies and Controls

You can include the IBM WebSphere Liberty 21.x technology in your compliance policies.



Empty Policy: Build your policy from scratch.
Select technologies for your policy. Your selection makes up the global technologies list for the policy and determines which controls can be added to the policy. Note - You can change the technologies at any time from within the Policy Editor.

Technologies Select at least one technology. REQUIRED

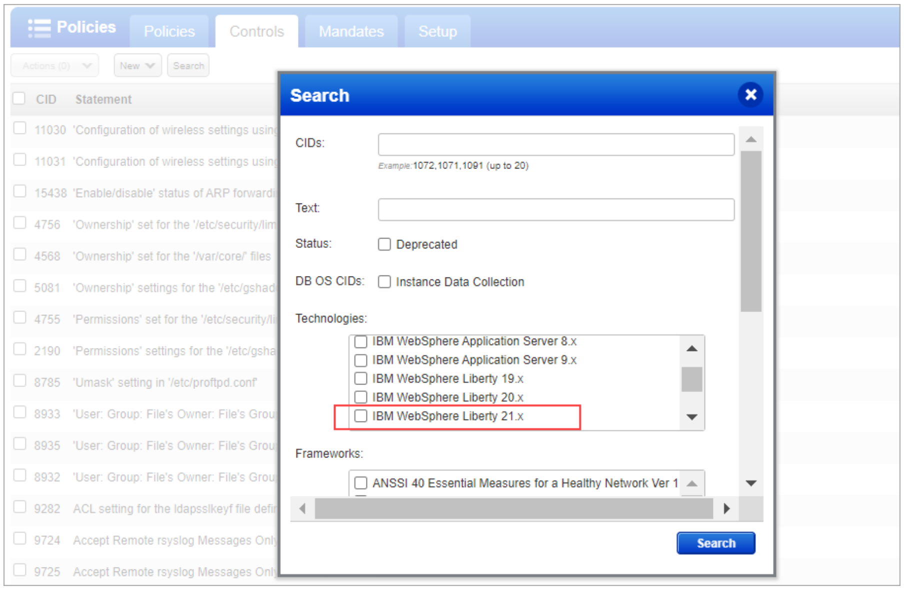
Search technologies: liberty

No technologies sele

Showing 3 matches from 323 technologies

IBM WebSphere Liberty 19.x
IBM WebSphere Liberty 20.x
IBM WebSphere Liberty 21.x

You can select IBM WebSphere Liberty 21.x technology when searching controls.



CID	Statement
11030	'Configuration of wireless settings usin
11031	'Configuration of wireless settings usin
15438	'Enable/disable' status of ARP forwardi
4756	'Ownership' set for the '/etc/security/lim
4568	'Ownership' set for the '/var/core/' files
5081	'Ownership' settings for the '/etc/gshad
4755	'Permissions' set for the '/etc/security/li
2190	'Permissions' settings for the '/etc/gsha
8785	'Umask' setting in '/etc/proftpd.conf'
8933	'User: Group: File's Owner: File's Grou
8935	'User: Group: File's Owner: File's Grou
8932	'User: Group: File's Owner: File's Grou
9282	ACL setting for the ldapsslkeyf file defi
9724	Accept Remote rsyslog Messages Only
9725	Accept Remote rsyslog Messages Only

Search

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

Text:

Status: □ Deprecated

DB OS CIDs: □ Instance Data Collection

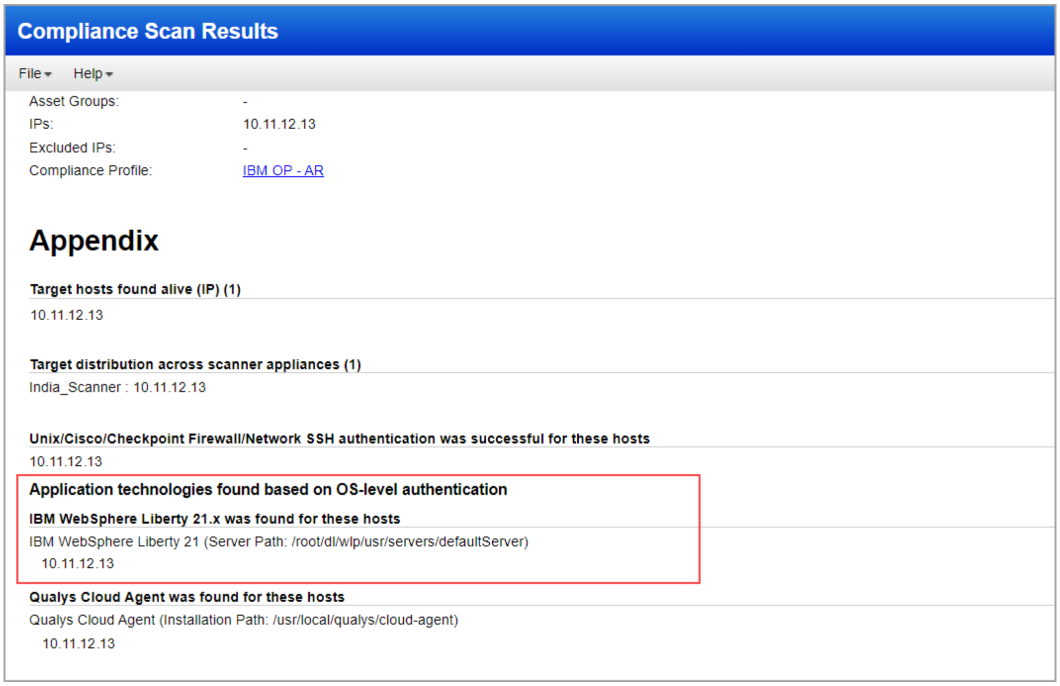
Technologies:
- □ IBM WebSphere Application Server 8.x
- □ IBM WebSphere Application Server 9.x
- □ IBM WebSphere Liberty 19.x
- □ IBM WebSphere Liberty 20.x
- □ IBM WebSphere Liberty 21.x

Frameworks:
- □ ANSSI 40 Essential Measures for a Healthy Network Ver 1

Search

Scan Results and Reports

You'll see host instance information in Policy Compliance authentication reports, scan results, and policy reports. The sample compliance scan results below shows a host on which IBM WebSphere Liberty 21.x was identified.



Asset Groups:	-
IPs:	10.11.12.13
Excluded IPs:	-
Compliance Profile:	IBM OP - AR

Appendix

Target hosts found alive (IP) (1)

10.11.12.13

Target distribution across scanner appliances (1)

India_Scanner : 10.11.12.13

Unix/Cisco/Checkpoint Firewall/Network SSH authentication was successful for these hosts

10.11.12.13

Application technologies found based on OS-level authentication

IBM WebSphere Liberty 21.x was found for these hosts

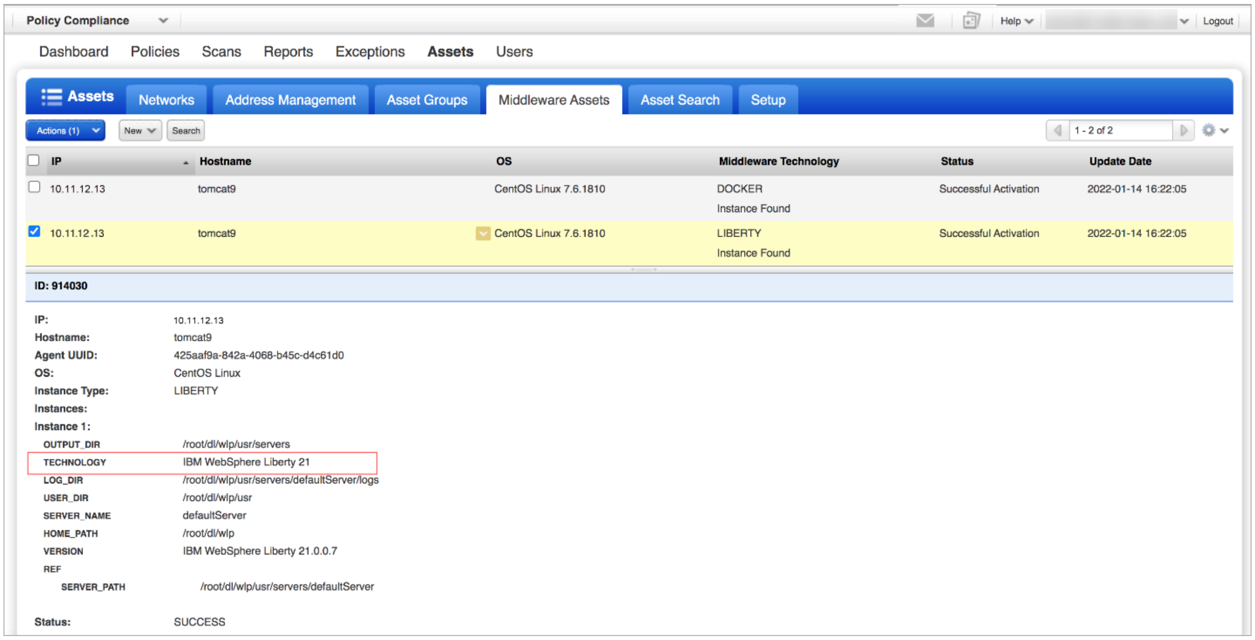
IBM WebSphere Liberty 21 (Server Path: /root/dl/wlp/usr/servers/defaultServer)
10.11.12.13

Qualys Cloud Agent was found for these hosts

Qualys Cloud Agent (Installation Path: /usr/local/qualys/cloud-agent)
10.11.12.13

Middleware Assets

If you are using Cloud Agent for Policy Compliance (PC), IBM WebSphere Liberty instances are auto-discovered by the agent. When a Liberty instance is detected on a host by an agent scan, it will appear on the **Assets** > **Middleware Assets** tab.



☐	IP	Hostname	OS	Middleware Technology	Status	Update Date
☐	10.11.12.13	tomcat9	CentOS Linux 7.6.1810	DOCKER Instance Found	Successful Activation	2022-01-14 16:22:05
☑	10.11.12.13	tomcat9	CentOS Linux 7.6.1810	LIBERTY Instance Found	Successful Activation	2022-01-14 16:22:05

ID: 914030

IP:	10.11.12.13
Hostname:	tomcat9
Agent UUID:	425aaf9a-842a-4068-b45c-d4c61d0
OS:	CentOS Linux
Instance Type:	LIBERTY
Instances:	
Instance 1:	
OUTPUT_DIR	/root/dl/wlp/usr/servers
TECHNOLOGY	IBM WebSphere Liberty 21
LOG_DIR	/root/dl/wlp/usr/servers/defaultServer/logs
USER_DIR	/root/dl/wlp/usr
SERVER_NAME	defaultServer
HOME_PATH	/root/dl/wlp
VERSION	IBM WebSphere Liberty 21.0.0.7
REF	
SERVER_PATH	/root/dl/wlp/usr/servers/defaultServer
Status:	SUCCESS

Qualys Vulnerability Management (VM)

New Pwnkit Search Lists and Option Profile Available in Library

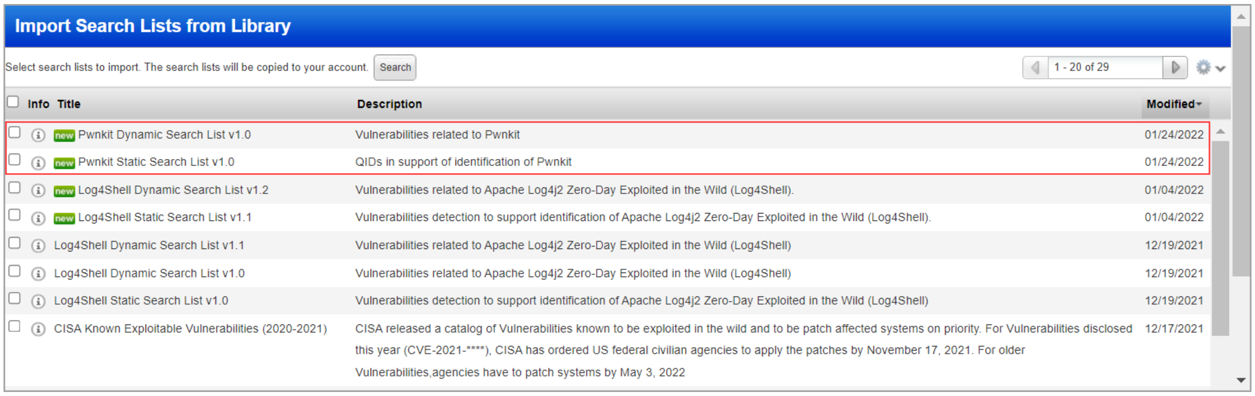
To help customers detect the Pwnkit vulnerability, we've introduced 2 new Pwnkit search lists (dynamic and static) and a new option profile that can be imported directly into your account from our Library.

Refer to the following blog post to learn more about this vulnerability:

https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

How to import search lists

Go to the **Search Lists** tab (under Scans, Reports or KnowledgeBase) and pick **New** > **Import from Library**. Select the new search list and click **Import**.



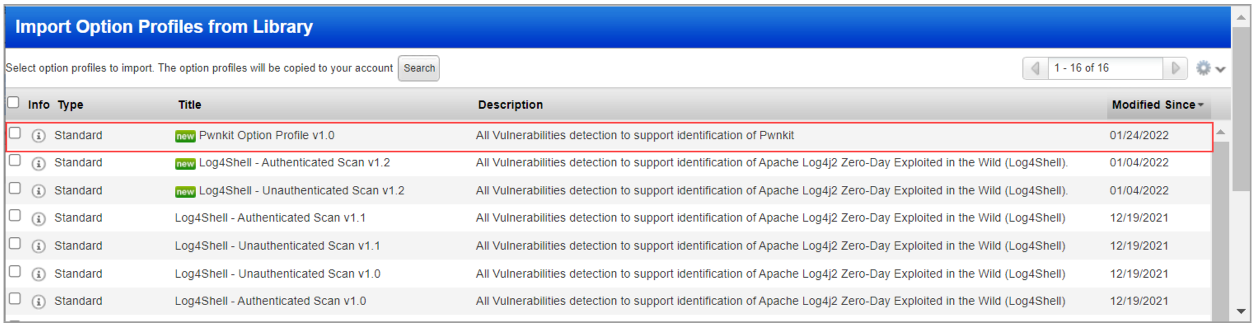
Import Search Lists from Library

Select search lists to import. The search lists will be copied to your account. Search 1 - 20 of 29

□	Info	Title	Description	Modified
□	ⓘ	new Pwnkit Dynamic Search List v1.0	Vulnerabilities related to Pwnkit	01/24/2022
□	ⓘ	new Pwnkit Static Search List v1.0	QIDs in support of identification of Pwnkit	01/24/2022
□	ⓘ	new Log4Shell Dynamic Search List v1.2	Vulnerabilities related to Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell).	01/04/2022
□	ⓘ	new Log4Shell Static Search List v1.1	Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell).	01/04/2022
□	ⓘ	Log4Shell Dynamic Search List v1.1	Vulnerabilities related to Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021
□	ⓘ	Log4Shell Dynamic Search List v1.0	Vulnerabilities related to Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021
□	ⓘ	Log4Shell Static Search List v1.0	Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021
□	ⓘ	CISA Known Exploitable Vulnerabilities (2020-2021)	CISA released a catalog of Vulnerabilities known to be exploited in the wild and to be patch affected systems on priority. For Vulnerabilities disclosed this year (CVE-2021-****), CISA has ordered US federal civilian agencies to apply the patches by November 17, 2021. For older Vulnerabilities,agencies have to patch systems by May 3, 2022	12/17/2021

How to import option profiles

Go to the **Option Profiles** tab (under Scans) and pick **New** > **Import from Library**. Select the new option profile and click **Import**.



Import Option Profiles from Library

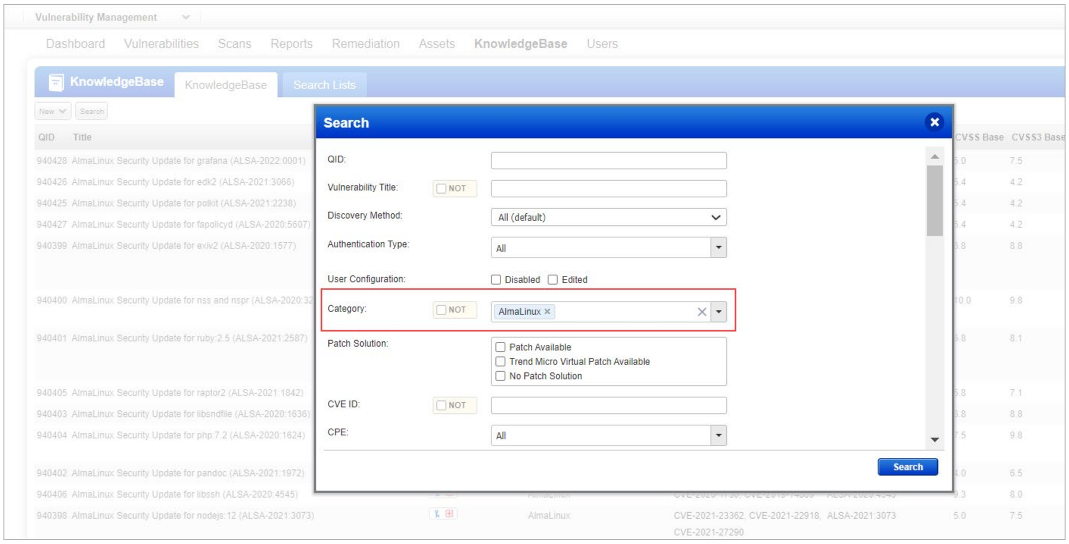
Select option profiles to import. The option profiles will be copied to your account Search 1 - 16 of 16

□	Info	Type	Title	Description	Modified Since
□	ⓘ	Standard	new Pwnkit Option Profile v1.0	All Vulnerabilities detection to support identification of Pwnkit	01/24/2022
□	ⓘ	Standard	new Log4Shell - Authenticated Scan v1.2	All Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell).	01/04/2022
□	ⓘ	Standard	new Log4Shell - Unauthenticated Scan v1.2	All Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell).	01/04/2022
□	ⓘ	Standard	Log4Shell - Authenticated Scan v1.1	All Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021
□	ⓘ	Standard	Log4Shell - Unauthenticated Scan v1.1	All Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021
□	ⓘ	Standard	Log4Shell - Unauthenticated Scan v1.0	All Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021
□	ⓘ	Standard	Log4Shell - Authenticated Scan v1.0	All Vulnerabilities detection to support identification of Apache Log4j2 Zero-Day Exploited in the Wild (Log4Shell)	12/19/2021

Scanner Support for Alma Linux OS

Now when performing vulnerability scans using a scanner, you can detect vulnerability QIDs on hosts running the Alma Linux Operating System. You'll want to set up Unix authentication records for these hosts to perform authenticated scanning.

To find a list of QIDs specific to the Alma Linux OS, go to the **KnowledgeBase** tab and perform a search for **Category: AlmaLinux**.



Search

QID:

Vulnerability Title: □ NOT

Discovery Method: All (default)

Authentication Type: All

User Configuration: □ Disabled □ Edited

Category: □ NOT AlmaLinux ×

Patch Solution:
□ Patch Available
□ Trend Micro Virtual Patch Available
□ No Patch Solution

CVE ID: □ NOT

CPE: All

Issues Addressed

- We fixed an issue where an empty response was returned when fetching scan results using the API for IPv6 targets.
- Fixed an issue where the ‘Dashboard’ tab of the Policy Compliance module was accessible to the Administrator user role when it shouldn’t have been. With this fix, the Administrator user won't see the ‘Dashboard’ tab of the Policy Compliance module.
- We fixed an issue for Batch Exception Requests where an error was occurring with the ‘Error saving exception’ message in the case when the OS technology for the asset changed and the user was requesting the exception for the new technology.
- Compliance scan results pdf report was not showing the IPs in the ‘Scan Paused by User (IP)’ section of the report which is fixed now and the correct number of total IPs paused during the scan are displayed in the scan reports.
- We fixed an issue where Control ID 100321 evaluation was stuck in processing for a long time.
- We fixed an issue where uniqueness criteria was not present for the Docker Authentication Record.
- We fixed an issue where the same IP was accepted in the authentication record of the same type (CISCO).
- The issue with the number of IPs appearing incorrect in the Asset Group IP section is now resolved. We have now corrected the page numbers on the IPs listing page.
- We fixed an issue, now the SAML user's account will not get locked due to failed login attempts while making API calls.
- We have updated the note on scan results; now, the user gets a note “Results were truncated” for pdf and CSV scan results when data is truncated.
- We fixed an issue where the user could not update scheduled EC2 scans.
- We fixed an issue where user got an error while adding Internal hosts from VM to CertView module by using the Add Hosts to Apps option.
- We fixed the error message that appears when the user does not have an authentication record for the specified IP.
- We fixed an issue where the Unit Manager users could not view Windows Authentication Record created by themselves.
- We fixed an issue where the Fixed check box was selected by default when disabled while creating a report template with host-based findings. Now, while creating a report template with host-based findings, the Fixed check box is not selected when disabled.
- We fixed an issue where you could not select a scanner appliance for scanning if the scanner name contained numerical characters.
- We fixed an issue where even though no patch was available for a QID, the Solution Section incorrectly showed the message: Following are links for downloading patches to fix the vulnerabilities.
- We fixed an issue with the API showing an extra links attribute in the CEF format output due to a missing check not to show the links attribute if the next host ID was null.

- We fixed an issue where the user got an error when trying to launch a vulnerability scan using an option profile with the Vulnerability Detection option set to "Select at runtime" and the scan target as FQDN.
- We fixed an issue where scheduled scan notifications were being sent 5 minutes earlier than the expected time.
- We have now updated "/api/2.0/fo/asset/ip/" API to process IPs of a single network only. It will not update multiple network IPs in a single request.
- We fixed an issue where offline scan results were getting stuck in uploading state.
- If you update the report template through UI, the update did not reflect through API. Similarly, if you update the report template through the API, it did not reflect on the UI. We have now fixed the issue so that if you update the report template, the update is reflected correctly on UI and API.
- Deleting a certificate resulted in an incorrect count of Certificates on the Certificates tab. We have now fixed the issue so that the correct count of certificates is reflected on the Certificates tab.
- The Potential Vulnerability by Severity section in the VM report did not earlier reflect the potential vulnerabilities graph. We have now fixed the issue so that the potential vulnerabilities are correctly reflected in the graph in the VM report.
- We have fixed an issue where we will skip private QID processing if that private vulnerability provider is not enabled for the subscription.