

Vulnerability Management

1

Qualys, Inc. Corporate Presentation



Agenda

- **Introduction and Overview**
- **VM Account Setup (Lab 1)**
- **Qualys KnowledgeBase and Search Lists (Lab 2)**
- **Vulnerability Assessment (Lab 3)**
- **Assets and Asset Inventory (Lab 4)**
- **Threat Protection (Lab 5)**
- **Reporting (Lab 6)**
- **User Management (Lab 7)**
- **Remediation (Lab 8)**





Qualys. Training & Certification

qualys.com/learning

Login

Please log in to the Qualys training site. First time users: You will need to create a unique username and password to register for a class. You will not use your Qualys or Community login credentials for this site.

*Required Field

*Username:

*Password:

Sign In

[Forgot your password?](#) [Request a new account.](#)

- LAB Exercises pdf
- Presentation Slides pdf
- VM Certification Exam
- Click “Forgot your password?” link to reset your password



The Qualys Training and Certification portal (qualys.com/learning) is your source for all Qualys training material.

Here you will find the Vulnerability Management lab exercise document and presentation slides. You will need some type of pdf file reader, like adobe acrobat, to view these files.

A link to reset your password is located just below the “Sign In” button.

Qualys Student Trial Account

**from: support@qualys.com
subject: Qualys Registration – Start Now**

- The Learning Management System (LMS) will not send trial accounts to public email domains (e.g., gmail.com, yahoo.com, hotmail.com, etc...).
- Check your email inbox (and SPAM folder) for your student trial account credentials.
- Lab 1 in the VM lab exercise document provides instructions for activating and setting up your student trial account.



To perform the lab exercises in this course, each participant is provided with a Qualys student trial account. The account credentials are sent to the email address identified in your learning account user profile.

The Learning Management System (LMS) will not send a student trial account to a public email domain (e.g., gmail.com, yahoo.com, hotmail.com, etc...).

Be sure to check your spam or junk mail folders for your student trial account credentials.

You'll find instructions to activate and setup your student trial account in lab 1 of the VM lab document.

LAB Appendix E: Cloud Agent Installation

- **Recommended:** perform your agent installation on a “nonessential” host.
 - Use a hypervisor to create a virtual host.
 - Spin-up a host on your favorite cloud platform.
- Uninstall agent from production hosts, before your student trial account expires.



The lab exercises in this course demonstrate the various features and benefits of the Vulnerability Management application, using traditional Qualys Scanner Appliances; specifically, those that are in the Qualys Cloud's pool of external scanners.

If you would also like to see how Qualys Cloud Agent supports and interacts with the Vulnerability Management application, Lab Appendix E, will provide you with Cloud Agent installation instructions.



Qualys. Training & Certification

Course List

Self-Paced Training

- Vulnerability Management Self-Paced Training
- Scanning Strategies and Best Practices Self-Paced Training
- Reporting Strategies and Best Practices Self-Paced Training
- Policy Compliance Self-Paced Training
- PCI Compliance Self-Paced Training
- Web Application Scanning Self-Paced Training
- AssetView and Threat Protection Self-Paced Training
- Cloud Agent Self-Paced Training 
- Container Security Self-Paced Training

qualys.com/learning



6 Qualys, Inc. Corporate Presentation

For even more details and information on deploying and managing agents, see the "Qualys Cloud Agent" self-paced training course.



VM Lifecycle and Cloud Platform Overview

7

Qualys, Inc. Corporate Presentation



Vulnerability Management Lifecycle



The topics in this course will be presented in sections that reflect the various phases of the Vulnerability Management Lifecycle.

PHASE 1 - The Qualys Cloud Platform provides multiple technologies, including: scanner appliances, agents, sensors, and connectors to help you detect and discover both on-premise and cloud-based host assets.

PHASE 2 - With Qualys scanners, agents, sensors, and connectors working together to identify host assets throughout your entire enterprise architecture, the Qualys AssetView and Asset Inventory applications provide the type of features to help you manage and organize these assets.

PHASE 3 - The primary objective of the assessment phase is finding vulnerabilities on the host assets in your VM subscription. The data needed to perform a vulnerability assessment can come from a combination of Qualys Sensors, Scanner Appliances, or Agents.

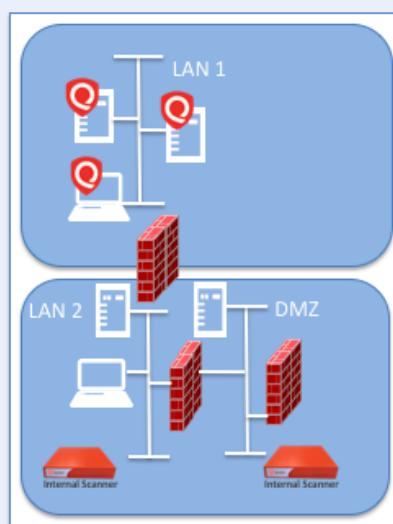
PHASE 4 - Regardless of the data collection techniques you use, all findings are securely stored in the Qualys Cloud Platform, where reporting tools and features allow you to identify the vulnerabilities that pose the greatest risk to your organization, and share these findings with your patch and operational teams.

PHASE 5 - The remediation tools and features built-in to the VM application, will help you to prioritize detected vulnerabilities and identify the vulnerabilities that have been successfully mitigated.

PHASE 6 - Verify any vulnerabilities that have been patched or fixed. This task is performed automatically every time a scanner appliance, agent or sensor provides new assessment data to the Qualys Cloud Platform. The same assessment test that was originally used to detect a vulnerability, will be used again to verify a patch or fix.

The steps or phases of this lifecycle model are designed to be repeated continuously as progress is made towards identifying and mitigating vulnerabilities within your organization.

Qualys Cloud Platform



9 Qualys, Inc. Corporate Presentation

Qualys.

Our training lab targets live in a typical DMZ environment, where the perimeter firewall has been configured to allow packets from Qualys' External Scanner Pool. External scanners are ideal for scanning public facing targets, or host assets with a public IP address. By default, any Qualys user with scanning privileges, has access to the External Scanner Pool.

Internal scanner appliances are commonly used to scan host assets that reside on PRIVATE IP subnets like LAN 2 in this diagram. Deploying an internal scanner appliance as a member of this subnet, will allow you to scan all LAN 2 assets directly, without the obstacle of network filtering devices.

LAN 1 in this diagram presently does not have a scanner appliance and is isolated from the rest of the network by a firewall. To meet the vulnerability management objectives for this subnet, Qualys Cloud Agent will be installed on each LAN 1 host. Each agent will collect metadata from its host and send it to the Qualys Cloud Platform for processing. Vulnerability assessment tests (all the heavy lifting) are intentionally kept off of the agent, and performed within the Qualys Platform. Qualys Cloud Agent is ideal for Remote Users (or any host assets that are difficult to scan), and it can be deployed on assets hosted by your Cloud Service Providers.

Cloud Agent OS Support

	Windows (.exe)	Windows Client Versions Windows Server Versions
	Linux (.rpm)	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux
	Linux (.deb)	Debian Ubuntu
	Mac (.pkg)	OS X
	AIX (.bff.gz)	IBM AIX

Qualys, Inc. Corporate Presentation



Presently, Qualys Cloud Agent supports the operating systems listed here:

- Windows
- RPM-based versions of Linux, including: Red Hat, Oracle, CentOS and others.
- Debian and Ubuntu Linux
- Mac OS X, and
- IBM AIX

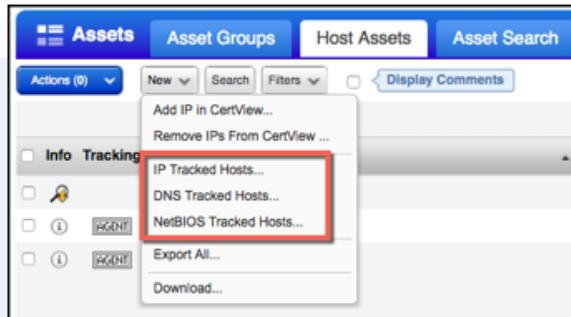


VM Account Setup

Adding and Removing IPs

Managers can:

- Add assets to the subscription
- Remove assets from the subscription
- Delegate “Add assets” privilege to Unit Managers



Before you can begin scanning a host asset, you must first add it to your Qualys subscription.

The "Tracking Method" you select, will determine how vulnerability findings are stored for each host. Your options include: IP address tracking, DNS tracking, or NetBIOS tracking.

A fourth tracking method, the Qualys Host ID, is used by default when you install or deploy Qualys Cloud Agent on a host asset.

The Qualys Host ID is also available for your "scannable" host assets through the Agentless Tracking feature.

Agent host assets can be added to your account through the Qualys Cloud Agent application. If you deploy one or more agents, they will appear under the Assets tab with the AGENT tracking method, which is the Qualys Host ID.

Host Tracking

- How do you want to store (track) host vulnerability findings?
 - IP Address (works best for static IPs)
 - DNS Name
 - NetBIOS Name
- Qualys Host ID tracking is available with Cloud Agent or, when "Agentless Tracking" is enabled (Scans > Setup).

Agentless Tracking

Accept Agentless Tracking in order to report on hosts by host ID.

[Go >](#)



The "Tracking Method" you select, will determine how vulnerability findings are stored for each host.

By default, IP address tracking is used to store (or index) the vulnerability findings for "scannable" host assets. IP address tracking is typically considered a poor choice, if host IPs are frequently changing (e.g., DHCP). It is best to use a tracking method that remains consistent for an extended period of time, or for the life of the host asset.

Qualys Cloud Agent (CA) automatically uses a Universally Unique ID (UUID) to track host vulnerability findings. The same type of UUID used by CA can be used for "scannable" host assets, by enabling the "Agentless Tracking" feature found in the Scans Setup options. Agentless Tracking requires scanning in "authenticated" mode.

Lab 1

Account Setup





Qualys KnowledgeBase

15 Qualys, Inc. Corporate Presentation



VM KnowledgeBase

The screenshot shows a dashboard with tabs for Dashboard, Scans, Reports, and Remediation. The KnowledgeBase tab is active. On the left, a sidebar lists QID and Title for various vulnerabilities. The main area displays a table of icons and names, followed by a detailed table of CVSS scores, Bugtag ID, Modified date, and Published date.

Icon	Name
-pencil	Edited
Wi-Fi	Remote Discovery
Key	Authenticated Discovery
Red Cross	Patch Available
Black Hat	Exploit Available
Red Circle	Associated Malware
Blue Gear	Not exploitable due to configuration
Hexagon	Non-running services

CVSS Base	Bugtag ID	Modified	Published
4.8	Q316/2016	03/16/2016	03/16/2016
4.3	Q308/2016	03/08/2016	03/08/2016
7.8	Q303/2016	03/03/2016	03/03/2016
4.3	Q308/2016	03/08/2016	03/08/2016
4.3	Q407/2016	04/07/2016	04/05/2016
10	Q305/2016	03/05/2016	03/03/2016
8.3	Q101/2016	01/01/2016	01/01/2016

All QIDs are stored here



The colorful icons associated with a QID represent the different properties or characteristics of its associated vulnerability:

A pencil icon identifies QIDs that have been edited by a Manager user. Only the Manager user role can edit QIDs in your account knowledgebase. The green wi-fi antenna icon identifies vulnerabilities that can be detected remotely by a (Qualys Scanner Appliance) without the use of authentication. If authentication is required for successful vulnerability detection, the QID will be associated with the blue key icon. The red cross icon identifies vulnerabilities that are patchable. QIDs with the red cross icon typically provide a direct link to the vendor's patch. The black hat icon is used to identify vulnerabilities that have a known exploit. The red, hazardous material icon identifies vulnerabilities associated with malware. The blue gear icon is associated with vulnerabilities that can potentially be protected from exploits, by making specific configuration changes on the target host. The hex icon identifies vulnerabilities that are associated with services that are not currently running.

	Confirmed Vulnerability	Security weakness verified by an "active test"
	Potential Vulnerability	Security weakness requiring manual verification
	Information Gathered	Configuration Data

	Half Red/Half Yellow	Results will vary depending on authentication
--	----------------------	---

	4 Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (MS05-019)
	4 Windows TCP/IP Remote Code Execution and Denial of Service Vulnerabilities (MS05-019)
QID:	90244
Category:	Windows
CVE ID:	CVE-2005-0048 CVE-2004-0790 CVE-2004-1080 CVE-2004-0230 CVE-2005-0688 CVE-2004-0791
Vendor Reference	MS05-019
Bugtraq ID:	*
Service Modified:	07/31/2012
User Modified:	-
Edited:	No
PCI Vuln:	Yes

Trusted Scan Results



Confirmed vulnerabilities have one or more active tests, that can be used to confirm the presence of the vulnerability. Vulnerabilities of this type are color coded: red.

If an active test is not available to confirm the presence of a vulnerability, it is categorized as a potential vulnerability and color coded yellow. Potential vulnerabilities will typically need to be verified through your own manual investigation.

Information gathered data or IG data for short, consists of various configuration settings and other host inventory and scan information. Information gathered QIDs are not vulnerabilities and are color coded: blue.

Vulnerability QIDs that are half-red/half-yellow, have two very predictable scan results, depending on your use of authentication. When scans are performed in authenticated mode, these vulnerabilities will be confirmed and colored red. When scan are performed without authentication, these vulnerabilities will be listed as potential and colored yellow.

Vulnerability Severity Levels

Confirmed	Potential	Severity Level	Description
		Minimal (1)	Intruders can collect information about the host via open ports or services, which can lead to the disclosure of other vulnerabilities.
		Medium (2)	Intruders can collect sensitive information from the host, such as software versions installed, which can reveal known vulnerabilities.
		Serious (3)	Intruders can gain access to security settings on the host, which could lead to: access to files and disclosure of file contents, directory browsing, denial of service attacks, and unauthorized use of services.
		Critical (4)	Intruders can potentially gain control of the host, or collect highly sensitive information including: read access to files, potential backdoors, or a listing of all user accounts on the host.
		Urgent (5)	Intruders can easily gain control of the host, which can lead to the compromise of your entire network. Vulnerabilities include: read and write access to files, remote execution of commands, and backdoors.

Severity 1 – Least Urgent

Severity 5 – Most Urgent



To help you determine which vulnerabilities to address or mitigate first, Qualys provides severity levels or rankings for both confirmed and potential vulnerabilities.

A severity level 5 vulnerability is the most urgent, because it presents the greatest risk to your organization. A severity 5 vulnerability could potentially allow an attacker to gain root or admin privileges to the vulnerable host.

Severity level 3 and 4 vulnerabilities also involve some type of potential compromise of the host system or one of its applications or services.

A severity level 1 vulnerability is the least urgent. Severity level 1 and 2 vulnerabilities involve the disclosure of sensitive data that could potentially be very useful to an attacker.

Organizations should develop a strategy for mitigating detected vulnerabilities based on these severity levels. Because of their increased risk and exposure most organizations address the severity 3, 4, and 5 vulnerabilities first. However, the collective risk created by numerous low severity vulnerabilities should not be overlooked.

Common Vulnerability Scoring System

- Defacto rating system for PCI DSS
- The Qualys KnowledgeBase provides CVSS scores (NIST) in addition to Qualys Severity

The screenshot shows a table of vulnerabilities from the Qualys KnowledgeBase. The columns include QID, Title, Severity, CVE ID, Vendor Reference, CVSS Base, Bugtraq ID, Modified, and Published. A red arrow points to the 'CVSS Base' column, which is described as 'Qualys Severity or CVSS'. The table lists three vulnerabilities:

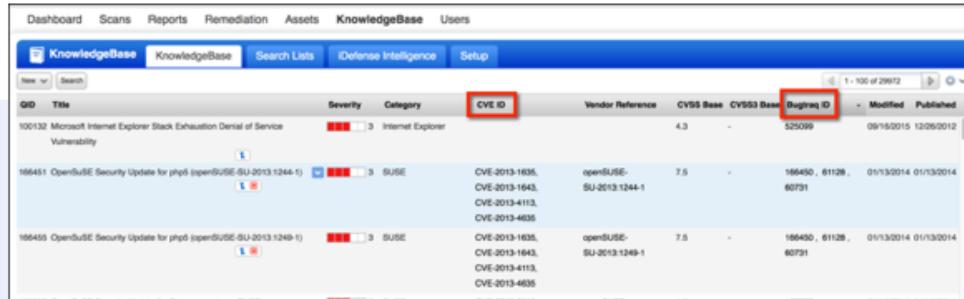
QID	Title	Severity	CVE ID	Vendor Reference	CVSS Base	Bugtraq ID	Modified	Published
27381	Pablo Software Solutions FTP Server Directory Disclosure Vulnerability	3			6.4	5283	04/16/2015	04/16/2015
167682	SUSE Enterprise Linux Security update for MySQL (SUSE-SU-2015:0620-1)	4	CVE-2015-0411, CVE-2015-0382, CVE-2015-0381, CVE-2015-0391...	SUSE-SU-2015:0620-1	8		04/16/2015	04/16/2015
167683	SUSE Enterprise Linux Security update for Mozilla Firefox (SUSE-SU-2015:0593-1)	4	CVE-2015-0817, CVE-2015-0818	SUSE-SU-2015:0593-1	7.5		04/16/2015	04/16/2015

Qualys Severity or CVSS

Column options are also available to view different types of CVSS scores. The common vulnerability scoring system is the standard for the PCI DSS.

CVE and Bugtraq

- Correlates Vulnerabilities and CVE ID (<http://cve.mitre.org/>)
- Correlates Vulnerabilities and Bugtraq ID (<http://securityfocus.com>)



GID	Title	Severity	Category	CVE ID	Vendor Reference	CVSS Base	CVSS3 Base	Bugtraq ID	Modified	Published
100132	Microsoft Internet Explorer Stack Exhaustion Denial of Service Vulnerability		3	Internet Explorer		4.3	-	525099	09/16/2015	12/05/2012
166451	OpenSUSE Security Update for php6 (openSUSE-SU-2013:1244-1)		3	SUSE	CVE-2013-1635, CVE-2013-1643, CVE-2013-4113, CVE-2013-4635	openSUSE-SU-2013:1244-1	7.5	-	166450 , 61128 , 60731	01/13/2014 01/13/2014
166455	OpenSUSE Security Update for php6 (openSUSE-SU-2013:1249-1)		3	SUSE	CVE-2013-1635, CVE-2013-1643, CVE-2013-4113, CVE-2013-4635	openSUSE-SU-2013:1249-1	7.5	-	166450 , 61128 , 60731	01/13/2014 01/13/2014



Although you'll find the most current and comprehensive vulnerability information within the Qualys knowledgebase, you'll find additional links for various QIDs that will connect you to:

- The Common Vulnerabilities and Exposures website,
- Software vendor websites, and
- Bugtraq data provided by the Security Focus website

Click on any CVE, software vendor, or bugtraq link to extend the information already provided within the Qualys knowledgebase

KnowledgeBase QID

The screenshot shows a user interface for a Qualys KnowledgeBase QID. On the left, there is a sidebar with a blue header labeled "General Information" and a list of categories: Details, Software, Threat, Impact, Solution, Exploitability, Associated Malware, Search Lists, and Compliance. Below this is a checkbox labeled "Disable this vulnerability". A red box highlights the "General Information" header and the "Details" category. A red arrow points from this highlighted area to a larger red box on the right, which contains detailed descriptions of the components:

- General Info - Provides basic details like title, severity, type
- Details - QID, CVE ID, Bugtraq ID and other vendor references info
- Software - Vendors and products associated with the vulnerability
- Threat - Defines the inherent threat within the vulnerability
- Impact - What could happen should the vulnerability be exploited
- Solution - How to fix the issue
- Exploitability - Exploitability info correlated with this vulnerability
- Associated Malware - Malware information that is correlated with this vulnerability
- Search Lists - If there are compliance concerns
- Compliance - What was returned when we probed for information (Available in a report or scan result after scan completion)

Disabled vulnerabilities are still scanned for but they are not reported or ticketed.

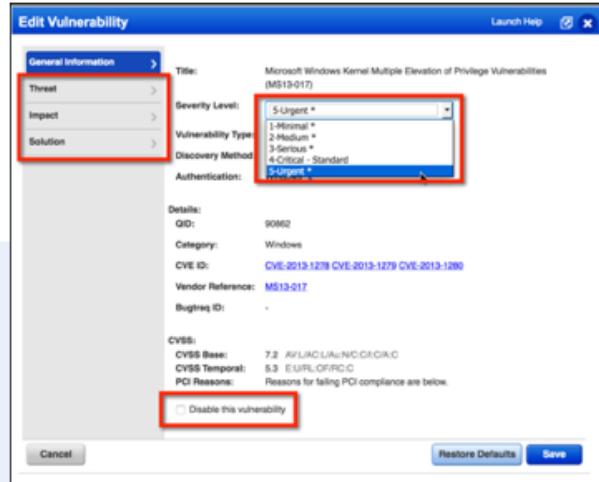
 Qualys.

These are the components of a Qualys KnowledgeBase QID.

KnowledgeBase

Editing Vulnerabilities

- Change Severity Levels
- Threat – Impact – Solution have user comments field
- Updates from the service not overridden
- Edited vulnerabilities are noted in Scan results



 Qualys.

KnowledgeBase Search

Use the search functionality to find vulnerabilities by QID, title, user configurations and many other criteria.

The image displays two versions of a search interface. The left version is a simplified form with fields for QID, Vulnerability Title, Discovery Method, Authentication Type, User Configuration, Category, Patch Solution, CVE ID, and Exploitability. The right version is a more detailed form with additional fields: Bugtraq ID, Service Modified, User Modified, Published, Confirmed Severity, Potential Severity, Information Severity, Vendor, Product, and Vulnerability Details. Both forms include NOT operators and dropdown menus for some fields.



With tens of thousands of QIDs in the Qualys knowledgebase, you'll want to take advantage of the numerous search options available in the knowledgebase search tool. The search tool provides more than 30 different options for locating specific QIDs or types of vulnerabilities within the knowledgebase.

Some of the search options feature a NOT operator, which allows you to exclude QIDs that match your search criteria.

You can perform searches using CVE IDs, various CVSS scores, bugtraq IDs, and even the date QIDs were published or modified.



KnowledgeBase Search List

Search List Overview

The screenshot shows the Qualys KnowledgeBase interface. At the top, there's a navigation bar with tabs for 'KnowledgeBase' and 'iDefense Intelligence'. Below the navigation bar is a toolbar with buttons for 'Actions', 'New', 'Search', and 'Filters'. A red arrow points to the 'Search Lists' button, which is highlighted with a red border. To the right of the button, a callout bubble contains the text 'Create "Static" or "Dynamic" Lists'. Below the toolbar is a table with columns for 'Title', 'Source', and 'Modified'. The 'Source' column is highlighted with a red box. The table lists several search lists, each with a checkbox next to it and a small icon. The 'Modified' column shows dates ranging from 02/23/2016 to 05/24/2016.

Title	Source	Modified
Adobe Vulnerabilities v.1	Dynamic	02/23/2016
Basic Host Information Checks (without auth)	Static	04/02/2016
CA Windows Vulns	Dynamic	04/02/2016
Confirmed Severity 4+5 Vulnerabilities v.1	Dynamic	10/29/2015
Critical Vulnerabilities with Vendor Patches v.1	Dynamic	07/31/2015
Custom Host Inventory	Static	12/19/2015
Database Vulnerabilities	Dynamic	07/26/2015
Don't Scan These Vulnerabilities	Static	05/24/2016

No limitation to the number of QIDs in a search list:

- Static search list - Defined and updated manually.
- Dynamic search list - Defined based on search criteria and updated when new QIDs are added to the knowledgebase.



You can create a static list, a dynamic list or import a search list from the Qualys search list library.

For a dynamic search list, targeted QIDs must be specified using a "List Criteria" consisting of any combination of the KnowledgeBase search options. The criteria you specify here will determine which QIDs are presently added to the list, and moving forward it will determine whether or not new QIDs get added. You can use any of the search options found here in the KnowledgeBase search tool to build your own custom search lists.

If the list of QIDs you have in mind does NOT have some type of common criteria, there's the static list option. A static search list (as its name implies) contains a fixed number of QIDs and can only be created and updated, manually.

Using Search Lists



A search list is one of the most powerful filtering tools in the Qualys Vulnerability Management application for tasks such as scanning, reporting, and remediation. You can use search lists to create vulnerability reports that focus on specific groups of vulnerabilities that are high priority targets within your organization.

You may find the need to target a specific list of vulnerability QIDs, when scanning (especially on those occasions where you don't have time to wait for a complete scan to finish). Remember: Qualys normally recommends scanning for everything, and then using Report Templates containing targeted search lists, to filter your scan results.

A remediation policy can be used to assign detected vulnerabilities to individuals (or operational teams) tasked with fixing or mitigating the vulnerabilities. You can also create a remediation policy that automatically ignores targeted QIDs.

Search List Info.

- Detailed information about a Search List is available by clicking the ⓘ icon.
- General Info, list criteria, and all QIDs that match the criteria are shown.
- Also shown is a list of all report templates, option profiles and remediation rules where the list is used.

General Information

Criteria >

QIDs >

Option Profiles >

Report Templates >

Remediation Policies >

Distribution Groups >

Comments >

General Information

Title: Adobe Vulnerabilities v.1
Source: Dynamic
Global: Yes
QIDs in List: 332
Owner: MANAGER Nick (quays2rd2)
Created: 07/17/2014 at 12:49:07 (GMT-0500)
Modified By: -
Modified: 07/17/2014 at 12:49:07 (GMT-0500)

View	QID	Title
 ⓘ	1165...	Adobe Acrobat and Reader Remote Code Execution Vulnerabilities (AP...
 ⓘ	4484...	Adobe Flash Media Server Privilege Escalation Vulnerability (APS09-07)
 ⓘ	1163...	Adobe Reader and Acrobat JavaScript Methods Memory Corruption Vul...
 ⓘ	1163...	Adobe Flash Player Invalid Loader Object Reference Vulnerability (Depr...



You can use the Quick Actions menu to edit an existing Search List or view its information.

Here you will find the list criteria, its list of QIDs, and any Option Profiles, Report Templates or Remediation Policies that use this list.

Distribution Groups can be created to receive email notifications about updates or additions to the QIDs in any list.

Search List

Use Cases

- Create reports for specific types of vulnerabilities:
 - Microsoft's Patch Tuesday vulnerabilities
 - PCI vulnerabilities
 - Only the vulnerabilities published in the last 30 days
- Scan for a specific type of vulnerability (when necessary):
 - Heartbleed, Shellshock, Spectre/Meltdown, etc...
 - High severity vulnerabilities with known exploits
- Create a Remediation Policy that assigns detected vulnerabilities to the right mitigation or patch team.



Lab 2

KnowledgeBase Search List

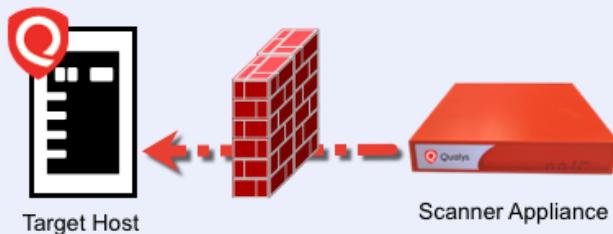




Vulnerability Assessment

Scanners and Agents

- Qualys Scanner Appliance targets host assets remotely:
 - Remote Scan (untrusted)
 - Authenticated Scan (trusted)
- Qualys Cloud Agent installs as a local system service:
 - An agent has SYSTEM level privileges to its host.
 - Collected data is sent back to Qualys Cloud Platform at regular intervals.



31 Qualys, Inc. Corporate Presentation



The Qualys Vulnerability Management application provides more than one option for collecting the data needed to perform a host vulnerability assessment.

A Qualys Scanner Appliance has a REMOTE perspective of any host you target. Its ability to perform a vulnerability assessment test, is directly impacted by the number and type of open service ports on any given host, as well as the presence of any network filtering devices that might potentially obstruct individual scan packets.

Qualys Cloud Agent; on the other hand, is installed as a local system service on each host; one agent per host. Agents operate with system level privileges, automatically sending assessment data back to the Qualys Cloud Platform at regularly scheduled intervals.

It is common for businesses and organizations to combine both agents and scanners to meet their vulnerability assessment needs.

Appendix E in the lab document provides steps for installing Qualys Cloud Agent.

Qualys VM Scanning Engine

Core Engine

- Inference-Based Scanning Engine.
- Intelligently launches modules specific to each unique host.
- Provides for optimal performance and accuracy.

Modules

- Collect configuration data from targeted hosts:
 - Open ports
 - Active services
 - Host operating system
 - Installed software applications
- Assessment modules are then launched based upon information collected.
- Hundreds of modules can coexist during a single scan.



The Qualys Vulnerability Management application uses an inference-based scanning engine that only launches the appropriate modules and assessment tests for each targeted host, which helps to increase the performance and accuracy of your vulnerability scans.

Initial modules are launched at the beginning of an assessment scan to collect the data needed by the scanning engine to select the appropriate vulnerability assessment modules and tests.

Data Collection Modules

Host Discovery Module

Requires : {IP ADDRESS}
Task : Checks if remote host is alive
Produces : {HOST STATUS:HOST ALIVE/DEAD}

Port Scanning Module

Requires : {HOST STATUS:ALIVE}
Task : Finds all open TCP/UDP ports
Produces : {Open Ports}

Service Detection Module

Requires : {Open Ports}
Task : Detects which service is running on an open port
Produces : {Active Services}

OS Detection Module

Requires: {Open Port} (at least one open TCP port)
Task: Detects host OS
Produces: {OS}



The primary modules that collect the host configuration data include: Host Discovery, Port Scanning, Service Detection and Operating System Detection. The data collected from these modules will be used later by the scanning engine to select the appropriate assessment modules

The Host Discovery Module will begin the data collection process by performing some checks and probes to determine the present status of each targeted host; either alive or dead.

Once the host discovery module has completed its task, a list of your LIVE targets is passed to the Port Scanning Module. It's the job of the port scanning module to determine which TCP and UDP ports are open (depending of course on the number of ports that you are actually targeting in your scan).

Once the TCP and UDP port scanning modules have completed their respective tasks. The list of open TCP and UDP ports is passed on to the Service detection module.

Once the active services have been identified, the OS Detection Module will then attempt to identify the operating system installed on each targeted host. At least one open TCP port is required, for this task.

Host Discovery Module

GOAL: Identify “LIVE” hosts and eliminate “DEAD” hosts from your vulnerability scans (default).

- 13 TCP ports (configurable to 20)
 - Half-open/SYN scan
- 6 UDP ports
- ICMP
- ARP (scanner must reside on local subnet of target)
- An option to “Scan Dead Hosts” can be used to override default behavior.

Host Discovery

TCP Ports

TCP (maximum 20)
 Standard Scan (13 ports) [View list](#)
 Additional

(ex: 1-6, 1024)

UDP Ports

UDP (maximum 6)
 Standard Scan (6 ports) [View list](#)
 Custom [Configure...](#)

ICMP

The host discovery module will begin the data collection process by performing some checks and probes to determine the present status of each targeted host; either alive or dead. You'll find the host discovery configuration options and settings inside each option profile, within the additional section.

One of the primary goals of host discovery is to eliminate dead hosts from your vulnerability scans.

Here you can choose and customize the different probes that are used to detect host status, including TCP, UDP, or ICMP probes.

Information contained in the ARP cache will also be used, if your scanner appliance resides on the same subnet as the host assets you are scanning.

TCP Port Scanning Module

TCP (connection-oriented):
0 to 65535 ports

- Standard Qualys scan uses about 1900 TCP ports.
- **Half-open/Syn Scan:**
Scanner appliance sends a RST packet, after receiving acknowledgement from host.

TCP Ports

Select the TCP ports you want scanned. A "Full" setting may increase scan time and is not recommended for Class C or larger networks.

- None
 Full
 Standard Scan (about 1,900 ports) [View list](#)
 Light Scan (about 160 ports) [View list](#)
 Additional (up to 12,500 ports)

(ex: 1-1024, 8080)

- Perform 3-way Handshake



35 Qualys, Inc. Corporate Presentation

Once the host discovery module has completed its task, a list of your LIVE targets is passed to the port scanning module. It's the job of the TCP port scanning module to determine which TCP ports are open (depending of course on the number of ports that you are actually targeting in your scan).

The "Scans" section of an option profile is where you specify the TCP port numbers to target in an assessment scan. The Standard Scan option is the most commonly used and default setting. It targets the most commonly used TCP port numbers in a typical network environment (about 1900 TCP ports), which can save a considerable amount of time, especially when compared to the FULL option, which targets all 65,535 TCP ports.

Use the "Additional" check box for any additional port numbers you may need.

Although the TCP protocol is connection oriented, the task of port scanning (discovering which ports are open) does not require the completion of a TCP 3-way handshake. After receiving an acknowledgement from an open port on the target host, the Qualys scanner will follow with a reset packet, instead of the final acknowledgement (or what is called a half-open syn scan). Although the option to "Perform a 3-way Handshake" is available, it should typically be avoided, unless you experience challenges or issues with the half-open syn scan used by the port scanning module.

UDP Port Scanning Module

UDP (connectionless):

0 to 65535 ports

- Standard scan uses 180 UDP ports.
- Open UDP ports do not always respond to packets sent.
- Closed UDP ports will typically respond with ICMP "Port Unreachable" (which may be blocked by filtering rules).
- Because of the unpredictable nature of UDP probes, UDP Service Detection is implemented during UDP port scanning.

UDP Ports

Select the UDP ports you want scanned.

None

Full

Standard Scan (about 180 ports)  [View list](#)

Light Scan (about 30 ports)  [View list](#)

Additional (up to 20,500 ports)

(ex: 1-1024, 8080)

Once the host discovery module has completed its task, a list of your LIVE targets is passed to the port scanning module. It's the job of the UDP port scanning module to determine which UDP ports are open (depending of course on the number of ports that you are actually targeting in your scan).

The "Scans" section of an option profile is where you specify the UDP port numbers to target in an assessment scan. The Standard Scan option is the most commonly used and default setting. It targets the most commonly used UDP port numbers in a typical network environment (about 180 ports).

Use the "Additional" check box for any additional port numbers you may need.

Keep in mind that UDP is a connectionless protocol and therefore unreliable. Open UDP ports and services do not always respond to the packets they receive.

Service Detection Module



Note: Qualys VM can detect more than 600 different services on TCP and UDP ports. To review these services go to the [Help > About](#) Section.

- Detection by valid protocol negotiation (non-destructive).
- Some services may be configured to use non-standard port numbers (contrary to IANA guidelines).
- Some services may use non-standard or unpredictable banners.
- Qualys will continue to negotiate communications, until the correct service is identified (may result in service impact).



Once the TCP and UDP port scanning modules have completed their respective tasks. The list of open TCP and UDP ports is passed on to the Service detection module.

The Qualys Vulnerability Management application can detect over 600 different services running on both TCP and UDP ports. This is accomplished using valid protocol negotiation;

IANA guidelines will initially be used to select the protocol for the very first service detection test. However, some services may be configured to use non-standard port numbers and other services may be configured to use non-standard or unpredictable banners, which also play a role in the service detection process.

If the initial test is not successful, Qualys will continue to negotiate communications with the targeted port, until the correct service is identified.

OS Detection Module

- Authenticated scans provide the most accurate OS detection:
 - Collected directly from Windows Registry.
 - Unix command such as uname -a or cat /etc/redhat-release, etc...
 - Authentication also allows for the enumeration of installed software.
- Scans performed without authentication rely on TCP/IP stack fingerprinting, with some enhanced protocol interrogation:
 - Packets are sent to target host to collect replies and build an OS fingerprint (using TTL, MSS, window size, etc...)
 - More accurate results can potentially be obtained by interrogating useful protocols, such as NetBIOS, HTTP, SNMP, and others.

Once the ports and active services have been discovered on the LIVE host assets in your scanning target, the OS Detection Module will then attempt to identify the operating system installed on each targeted host. At least one open TCP port is required, for this task.

For the most accurate operating system detection, Qualys recommends performing scans in "authenticated" mode. This will allow the Qualys Scanner Appliance to identify the exact OS vendor and version number directly from the Windows system registry or by executing the appropriate command.

An additional benefit to scanning in authenticated mode comes from the enumeration of installed software applications, which will trigger additional vulnerability assessment modules (and potentially vulnerability findings) for the installed software applications on the target hosts.

Scans performed without authentication will rely on a combination of TCP/IP stack fingerprinting with some enhanced protocol interrogation, for the purpose of detecting the host operating system.

Vulnerability Assessment and Detection

Specific vulnerability modules are loaded based on:

- Host Operating System
 - Active Services (and port numbers)
 - Installed Software (authentication required)
-
- Active (non-intrusive) tests use template-based vulnerability signatures.
 - Multiple tests validate each others' results to "confirm" the vulnerability.



Once all of the data collection tasks have been completed:

- Host operating system
- Active services and ports
- Installed software applications

The vulnerability management scanning engine will have the information it needs to begin selecting the appropriate vulnerability assessment modules for each targeted host:

- Vulnerability assessment modules perform active tests using non-intrusive vulnerability signatures.
- Some vulnerability assessment modules contain multiple tests, making it possible to compare and validate the collective test results, and confirm the presence of a vulnerability.

Vulnerability Scanning Summary

Host Discovery

- Checks for availability of target hosts. One response from the host indicates the host is "alive"

Port Scanning

- Finds all open TCP and UDP ports on target hosts (based on scan preferences)

Service Discovery

- Identify which services are running on open ports

Device Identification (OS Detection)

- Attempts to identify the operating system on the first open port

Vulnerability Assessment

- Based on 1) Operating System, 2) Active Services, and 3) Installed Software

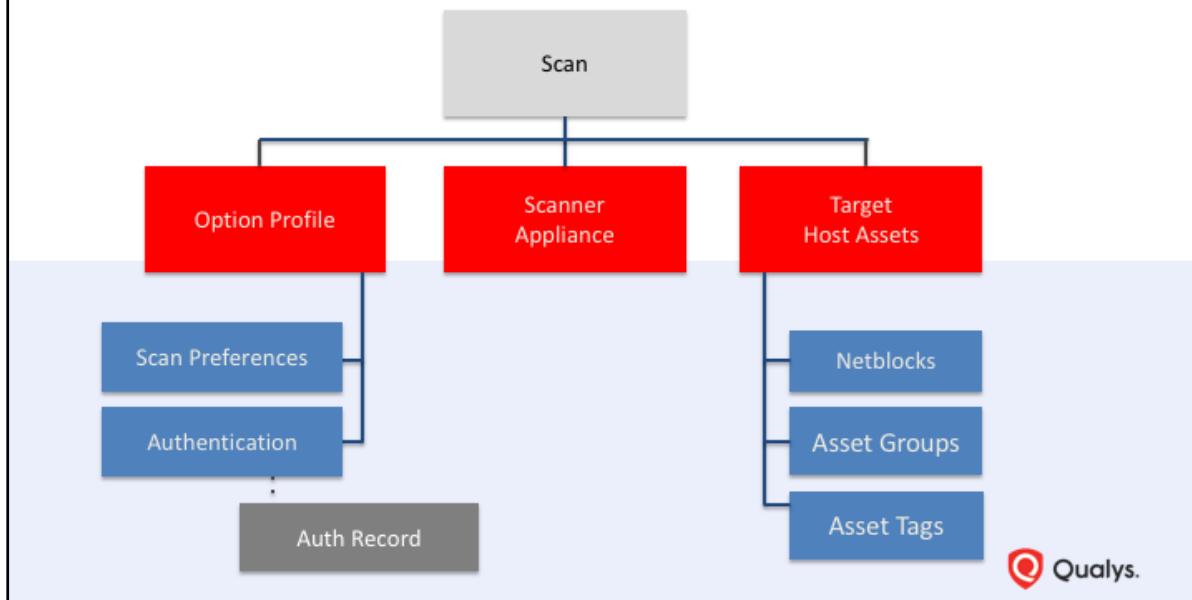


Here is a review of the entire process.



Scan Configuration - Launching a Scan

Scan Configuration Components



This diagram illustrates the basic components that comprise a vulnerability scan. To launch a vulnerability assessment scan you will certainly need at least one scanner appliance. The lab exercises in this course use the Qualys Cloud's Pool of External Scanners, which is the default setting for the Qualys student trial account you may be using. When selecting a scanner appliance for any scan task, you will need to consider the host assets your scan intends to target, which is another required component for launching a scan.

Your scanning targets include netblocks or specific ranges of IP addresses or even a single IP address in your Qualys subscription. Host IPs must be added to your subscription first, before you can scan them. Any host asset in your Qualys subscription can be added to an Asset Group which is another option for targeting a scan.

Asset Tags, the last scan target option, provide a dynamic and automated solution for managing host assets in your Qualys subscription.

Every vulnerability assessment scan must select an Option Profile, containing various scan preferences and scanning options. If your scan uses an Option Profile with authentication enabled, one more component, an authentication record, is added to this of required scan components.

Option Profile Scan

Option Profile Options:

- TCP & UDP Port config
- Authoritative Scanning
- Scan Dead Hosts
- Close Vulnerabilities on Dead Hosts
- Performance
- Load Balancer Detection
- Password Brute Forcing
- Vulnerability Detection
- Authentication
- Load Balancer Detection
- Password Brute Forcing
- Vulnerability Detection
- Authentication
- Additional Cert Detection
- Dissolvable Agent
- Lite OS scan
- Add a Custom HTTP header value
- Host-Alive Testing

Please see Qualys' "Scanning Strategies and Best Practices" self-paced training class for a more detailed discussion and analysis of scan settings and features found in the Option Profile.



In this course we focus on the basic configuration settings in an option profile, such as the TCP and UDP port settings, preset scan performance options, vulnerability detection options, and the different options for performing a scan in authenticated mode.

For an extended discussion of these and other scanning topics, please see the Qualys Scanning Strategies and Best Practices training course.

Option Profile

Targeted TCP and UDP Ports

TCP Ports

- None
- Full
- Standard Scan (about 1,900 ports)
- Light Scan (about 160 ports) [View list](#)
- Additional (up to 12,500 ports)

UDP Ports

- None
- Full
- Standard Scan (about 180 ports) [View list](#)
- Light Scan (about 30 ports) [View list](#)
- Additional (up to 20,500 ports)

- Configure network filtering devices and host-based firewalls to permit traffic on the ports your scan is targeting.



Typically it's best to avoid scanning thru network filtering devices, but when left with no choice, you'll want to ensure that network filtering devices (including host-based firewalls) that would normally impede your scanning traffic, are configured to allow scanning packets on the ports you are targeting.

Option Profile

Scan Performance Settings

- High
- Low
- Normal

Configure Scan Performance Settings

Settings

Select a performance level or customize performance settings

Enable parallel scaling for Scanner Appliances

Overall Performance

High
 Normal
 Low
 Custom

Hosts to Scan in Parallel

External Scanners: 15

Scanner Appliances: 30

Processes to Run in Parallel (per Host)

Total Processes: 10

HTTP Processes: 10

Packet Delay

Packet (Burst) Delay: Medium

Port Scanning and Host Discovery

Intensity: Normal



The preset performance settings identify the amount of bandwidth used by the scanner appliance: High, Normal and Low.

The “Low” option reduces scan performance and should be used for bandwidth restricted networks or heavy traffic environments.

“High” provides the best scan performance and works best in network environments with ample bandwidth or light traffic.

“Normal” provides the best balance between scan performance and bandwidth usage.

Option Profile

Vulnerability Detection

Add a Search List:

Vulnerability Detection

Complete
 Custom
Include the QIDs from the selected lists.

Select at runtime

Include
 Basic host information checks [View list](#)
 OVAL checks

Exclude
 Excluded QIDs
Exclude the QIDs from the selected lists.

Add Lists **Clear All**

Add Lists **Clear All**

Although recommended in some cases, in general it is better to attach a Search List to a Report or Remediation Rule.



The Custom Vulnerability Detection option will allow you to target and test a specific list of QIDs from the Qualys KnowledgeBase, using a Search List that you add here using the Add List button.

You'll also find the option to exclude a list of QIDs from a scan.

However, when configuring Vulnerability Detection, Qualys recommends using the Complete option.

The idea is to scan for everything, and then use the filtering options in a Report Template to help you focus on specific types or groups of vulnerabilities.

Option Profile

Authenticated (Trusted) Scanning

- Connect to service to extract more meaningful data.
- Discover vulnerabilities not detected by untrusted scan.
- Confirm Potential Vulnerabilities.
- Application Records & SQL server records are used by Policy Compliance module.

Authentication

- Windows
- Unix/Cisco
- Oracle
- Oracle Listener
- SNMP
- VMware
- DB2
- HTTP
- MySQL
- Tomcat Server
- MongoDB
- Palo Alto Networks Firewall
- Oracle WebLogic Server
- Jboss Server



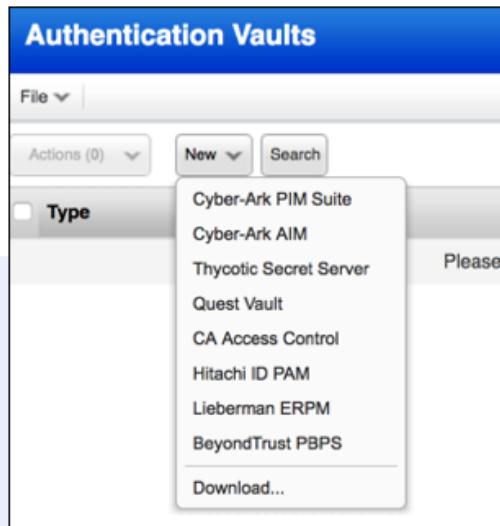
It's considered a "best practice" to perform your assessment scans in "authenticated" mode.

You'll find authentication options for various devices, operating systems and protocols.

The lab targets in this course require Windows and Unix authentication.

Remember, you'll need to create an appropriate authentication record (under the Authentication tab) for each authentication option you select here in the Option Profile.

Authentication Vaults



- In large organizations where thousands of machines are scanned regularly for vulnerabilities, managing passwords is a challenge.
- Some organizations are reluctant to let their credentials leave the network



Launch Vulnerability Scan

Scan Settings

The screenshot shows the 'Launch Vulnerability Scan' interface with the 'Scan Settings' step selected. A modal window titled 'Choose Target Hosts from' is displayed, allowing users to specify their scanning targets. The modal includes sections for 'Assets' and 'Tags', with the 'Tags' section currently active. It features fields for 'Include hosts that have' and 'Do not include hosts that have', both set to 'Any'. Below these are dropdown menus for 'All Windows', 'All', and 'Any'. The 'Exclude IP Ranges' field contains an example of ranges separated by commas. At the bottom of the modal, there is a checkbox labeled 'Scan agent hosts in my target' with a red arrow pointing to it. The 'Launch' and 'Cancel' buttons are also visible at the bottom.



To launch a vulnerability scan:

1. Enter a descriptive Title.
2. Select an Option Profile.
3. Select appropriate scanner appliance(s).
4. Select scanning target(s).
5. Click the “Launch” button.

Vulnerability Scan

“On Demand”

Scan Overview

Scan Information

Scan Title:	Another Scan with Auth
Launch Date:	06/08/2012 at 19:26:47 (GMT)
Status:	Running
Total IPs Scanned:	25
Scanner Appliance:	10.10.21.10 (Scanner 6.3.36-1, Vulnerability Signatures 2.2.147-1)

Scan Segment Detail

Segment 1	Running (Scanner(s) actively scanning target host(s))	Duration: 00:03:07
Start Date:	06/08/2012 at 19:26:47 (GMT)	
End Date:	-	
Scan Running On:	10.10.24.10, 10.10.24.18, 10.10.24.25, 10.10.24.27, 10.10.24.29, 10.10.24.38, 10.10.24.44, 10.10.24.54, 10.10.24.58, 10.10.24.63, 10.10.24.65, 10.10.24.69, 10.10.24.77, 10.10.24.84,	

The Qualys logo, which consists of a red stylized 'Q' icon followed by the word "Qualys" in a black sans-serif font.

You can monitor scans as they run.

Scan Results Summary

Report Summary

Launch Date: 08/11/2017 at 13:00:23 (GMT-0500)

Active Hosts: 1173

Total Hosts: 1173

Type: 1056

Status: 939

Reference: 822

External Scanner: 705

Duration: 588

Authentication: 471

Title: 354

Network: 237

Asset Groups: 120

IPs: 3

Excluded IPs: 5

Option Profile: 4

Vulnerabilities by Severity

Severity Level	Vulnerabilities
5	354
4	1173

Appendix

Successfully Scanned Hosts (IP)
64.41.200.231-64.41.200.250

Target distribution across scanner appliances
External : 64.41.200.231-64.41.200.250

Windows authentication failed for these hosts (2)
Instance os:
64.41.200.231, 64.41.200.237

Unix/Cisco/Checkpoint Firewall authentication failed for these hosts (1)
Instance os:
64.41.200.242

Windows authentication was successful for these hosts (6)
Instance os:
64.41.200.232, 64.41.200.238, 64.41.200.246-64.41.200.247, 64.41.200.249

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts (19)
Instance os:
64.41.200.233-64.41.200.234, 64.41.200.236, 64.41.200.239-64.41.200.241, 64.41.200.243-64.41.200.245, 64.41.200.250

 Qualys.

The "summary" section at the top of the report includes information like:

- Scan date, time and duration
- Information about the host assets targeted
- IP address of the scanner appliance
- Short summary of authentication results

The "Appendix" at the bottom provides more details about the hosts that were successfully or unsuccessfully scanned and a breakdown of the scanning options configured within the option profile

Scan Results Detail

Detailed Results

The screenshot shows a scan results interface for a Windows 7 Ultimate system (cpe:/o:microsoft:windows_7:::ultimate). The main pane displays a hierarchical list of findings:

- 64.41.200.247 (trn-win7.trn.qualys.com, TRN-WIN7) - Global Default Network
- Vulnerabilities (364):
 - 5 Microsoft Internet Explorer Cumulative Security Update (MS09-054)
 - Potential Vulnerabilities (6):
 - Enabled DCOM (3)
 - SMB Signing Disabled or SMB Signing Not Required (3)
 - Information Gathered (157):
 - Remote Access or Management Service Detected (3)
 - Accounts Enumerated From SAM Database Whose Passwords Do Not Expire (3)
 - NetBIOS Bindings Information (3)
 - NetBIOS Shared Folders (3)
 - Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines (3)

Unfiltered, raw data of your scan targets



By default, a raw scan report is designed to display all scan findings and details, including:

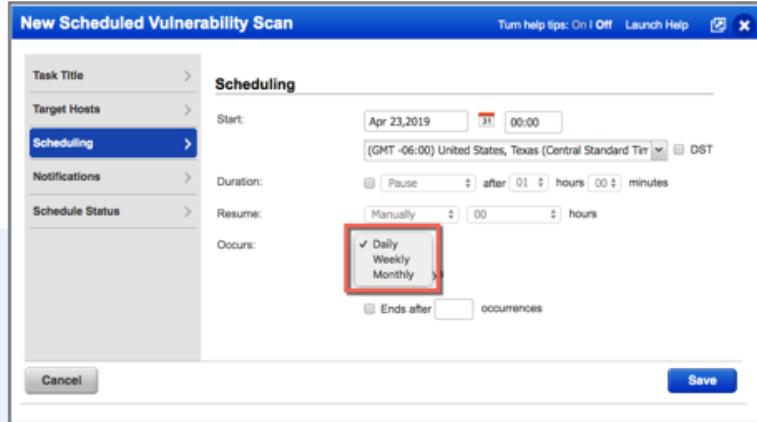
- information gathered findings
- potential vulnerability findings
- confirmed vulnerability findings

Simply expand any of the findings to view the vulnerability details, such as: the vulnerability title, QID number, Solution for fixing or mitigating the vulnerability, and all other QID data items and information found in the Qualys KnowledgeBase; a raw scan report contains everything.

Scheduling Assessment Scans

Automate Your Scans

- Assessment scans can be scheduled to run at daily, weekly or monthly intervals.
- Schedules can be paused to comply with maintenance windows.
- Send notifications before and after each scan.



What obviously makes a scheduled scan different are the Scheduling options. Begin by selecting the date and time for this scheduled scan to start. The start time for each scheduled scan will reflect the time zone you specify.

To keep this scan from bumping into high-demand or peak capacity times of day, you can choose a maximum scan duration and the action to take, if any scan reaches this threshold. If you configure the option to pause a long running scan, you'll need to specify how and when you would like it to resume.

You can schedule your scans to run daily, weekly, or monthly. You can schedule scans that have an unlimited number of occurrences, or select the option to deactivate a scheduled scan after a set number of occurrences is reached. Notifications will automatically be sent to the owner of a scheduled scanning task.

Additional options are available for sending notifications before and after a scan, to any email distribution groups you create.

Agent Data Collection Interval

Configuration Profile Edit

Turn help tips: On | Off X

Edit Mode

Configure Scan Interval for Vulnerability Management

General Info >

Configure the interval at which the agent collects data for Vulnerability Management for the assets associated with this profile.

Blackout Windows >

Performance >

Assign Hosts >

VM Scan Interval > VM Scan Interval

Data Collection Interval*
The time lapse between the completion of the previous scan and the start of the next scan

240 min (240 - 43200)

Cancel Save



- Qualys Cloud Agent can be configured to collect assessment data as frequently as every four hours (240 min.).



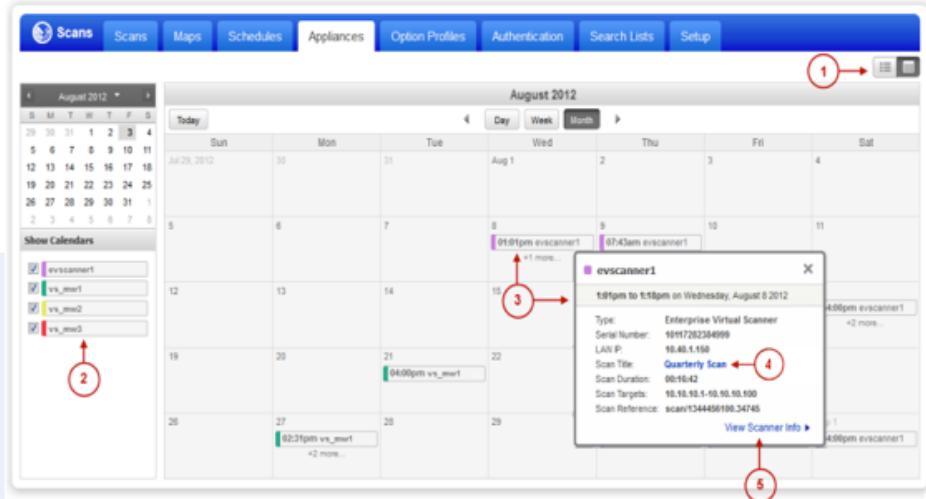
Somewhat similar to scheduled scanning, Qualys Cloud Agent is configured with a setting called the data collection interval.

Qualys cloud agent is designed to collect assessment data from its host at regular intervals, which it then sends to the Qualys cloud platform for processing.

By default, Agent data collection occurs every four hours (or 240 minutes).

The agent data collection interval can be set anywhere from 4 hours to 30 days.

Qualys Scan Calendar



New Scan Calendar

Your Scan calendar provides immediate insight into your scans and maps, giving you the most recent security information on your IT assets, so you can take actions as needed. A user with any role (except Auditor) can view this calendar. For a Unit Manager, Scanner or Reader, the user has permission to view calendars for assets they have permission to view in their account.

- 1) **View your scan calendar.** Go to a Scans list (Scans, Maps or Schedules tab) and click the calendar button .
- 2) **Add to my Calendar.** Click to copy and paste your calendar URL into your favorite calendar application (must be iCal format). Once imported, your calendars stay in sync.
- 3) **Show Calendars.** Select the scan types you want to see.
- 4) **View scan summary.** Click any scan or schedule or map to display a pop-up summary of the event.
- 5) **View scan details.** Click the scan event to view details. For a completed scan, click View report to see the scan results report. For a schedule, click More details to view and edit the schedule settings.

Lab 3

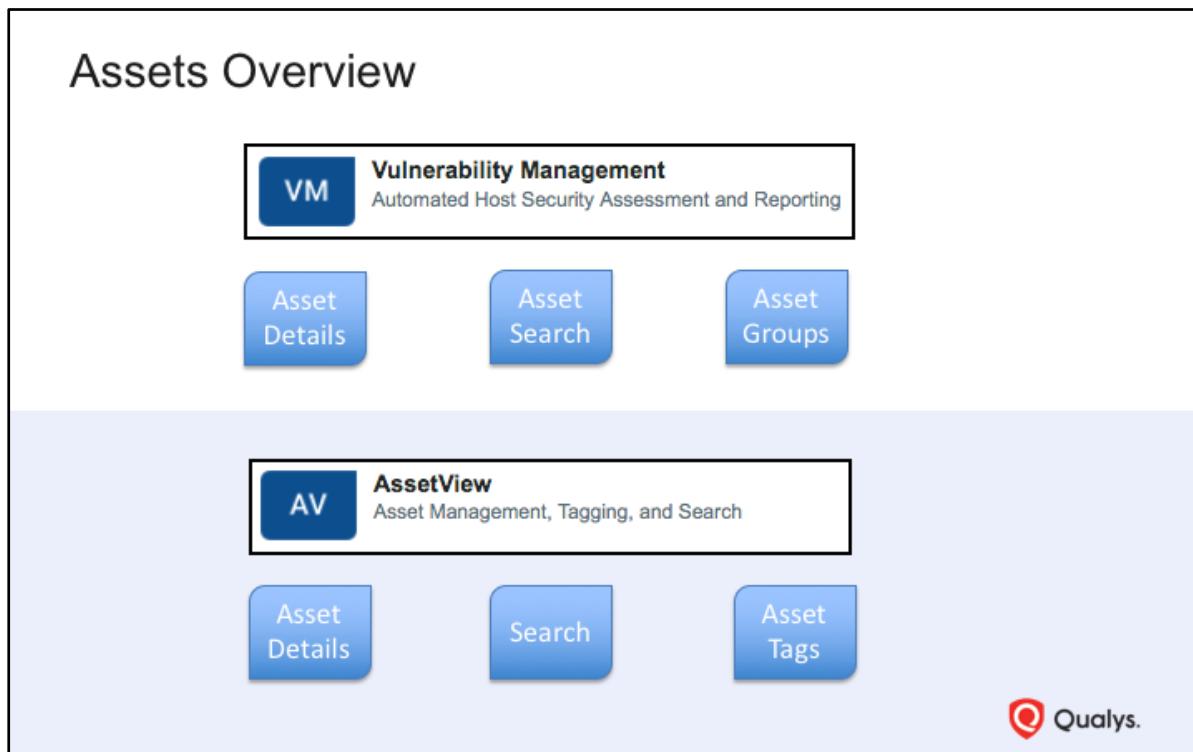
Vulnerability Scanning





Assets and Asset Inventory

Assets Overview



Both Qualys VM and AssetView provide features and services for viewing host assets and asset details.

They both provide the capability to search or query your host asset inventory to quickly identify and view host assets you wish to act upon.

and for more effective asset management, they both provide a mechanism for grouping and labeling host assets within your subscription.

We'll begin our overview inside the Vulnerability Management application, before moving on to Qualys AssetView

Applications Inventory

The screenshot shows the 'Assets' tab selected in the navigation bar. Below it, there's a search bar for 'Application' and 'Asset Group'. A dropdown menu for 'Select a Network' is open. To the right, there are 'Search' and 'Download CSV' buttons, along with a note that 1-50 of 5959 results are displayed. The main area is a table with columns: IP / DNS Hostname, Version, First Found, and Last Updated. It lists several entries:

IP / DNS Hostname	Version	First Found	Last Updated
4Suite (3 Hosts)			
64.39.106.241 demo11.sea.qualys.com	1.0-3	06/01/2015	06/01/2015
64.39.106.244 demo3.sea.qualys.com	1.0-3	02/21/2015	08/06/2015
64.39.106.247 demo6.sea.qualys.com	1.0-3	12/05/2014	08/06/2015
AVG Free 8.0 (1 Host)			
64.39.106.249 demo8	Not Found	01/14/2014	08/05/2015
Adobe Flash Player 10 Plugin (1 Host)			
64.39.106.249 demo8	10.0.12.36	01/14/2014	08/05/2015



For a different view or perspective of your host assets click the "Applications" tab.

Here you'll find a comprehensive list of all the software applications discovered on the host assets in your subscription.

Remember, scans must be performed in "authenticated" mode to produce a list of installed software applications.

Use the search fields to find a specific application or filter the application list by Asset Group or IP address.

Download an application list into a CSV file.

Ports and Services Inventory

IP / DNS Hostname	Protocol	Port	Default Service	First Found	Last Updated
(24 Hosts)					
64.41.200.290 demo020.ap01.qualys.com	TCP	8009		12/04/2015	06/08/2017
192.168.1.14 ubuntu	UDP	44119		06/19/2017	06/19/2017
192.168.1.14 ubuntu	UDP	47853		06/10/2016	06/19/2017
192.168.1.14 ubuntu	UDP	5353		09/10/2016	06/19/2017
192.168.1.14 ubuntu	UDP	57450		03/09/2017	06/19/2017
192.168.1.14 ubuntu	UDP	43692		06/19/2017	06/19/2017
192.168.1.14 ubuntu	UDP	43691		01/03/2017	06/19/2017
192.168.1.14 ubuntu	UDP	35683		12/06/2016	06/19/2017



The ports and services tab provides the same function as the Applications tab, only for host services rather than applications.

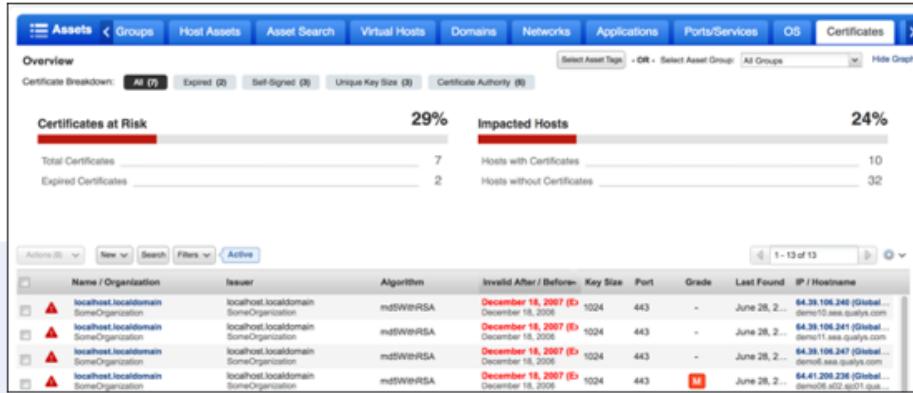
Host Operating Systems Inventory

IP / DNS Hostname	OS	Version	Last Updated
64.39.106.242	Windows 2003/XP		10 Mar 2014
192.168.1.200	Windows Server 2012 R2 Standard 64 bit Edition		17 Feb 2014
192.168.1.201	Windows XP 64 bit Edition Service Pack 2		17 Feb 2014
192.168.1.202	Windows Vista 64 bit Edition Service Pack 2		17 Feb 2014
192.168.1.203	Windows 7 Enterprise 64 bit Edition Service Pack 1		17 Feb 2014
192.168.1.204	Windows Server 2008 R2 Enterprise 64 bit Edition		17 Feb 2014
192.168.1.205	Windows 8 Enterprise 64 bit Edition		17 Feb 2014
192.168.1.206	Windows Server 2012 Standard 64 bit Edition		17 Feb 2014
192.168.1.208	Windows 8.1 Enterprise 64 bit Edition		17 Feb 2014
192.168.1.211	CentOS 5.10	2.6.18-371.4.1	17 Feb 2014
192.168.1.212	CentOS 6.4	2.6.32-358.18.1	17 Feb 2014
192.168.11.72	Windows 2000 Service Pack 3-4		5 Mar 2014
192.168.11.73	Windows 2000 Service Pack 3-4		5 Mar 2014



The "OS" tab provides a breakdown of the operating systems discovered on host assets in your VM subscription.

Certificates Inventory



Certificate related information such as certificates by expiration date, by key size, by certificate authority, by port, and self-signed certificates as well as the certificates detail.



The "Certificates" tab identifies the certificates installed on all host assets.

Here you can quickly identify host assets with expired certificates or other certificate issues that may need to be addressed.

VM

Asset Groups

Asset Group Design

Asset groups can be based on:

- Device type or OS
- System priority or criticality
- Geographic or network boundaries
- Asset ownership
- and more ...



192.168.1.0/24

CRITICAL



How do you intend to use the Asset Group(s) you create?

- **Scanning target** - Do you scan by subnet, OS, or something else?
- **Report source** - Only include host assets of interest to the target audience.
- **Remediation Policy condition** - Are there any "patch" teams responsible for specific groups of host assets?
- **Assign access privileges to Qualys users** - Which assets can other Qualys user accounts access?



There are many different ways to build and design an asset group. The question that will help you determine which asset groups you need is:

"How do you intend to use the asset groups that you create?"

For example, asset groups are commonly used as targets for performing vulnerability scans. You can typically build multiple Asset Groups that reflect your customary or regular scanning targets.

When building asset groups for reporting (when using asset groups as the report source) the objective is to include only those host assets that are of interest to your target audience. Host assets that fall outside of this scope, will simply add noise and complexity to a report.

If you have operational or patch teams that are dedicated to specific groups of host assets, you can construct remediation policies for these assets using Asset Groups.

Asset groups provide a mechanism for assigning host access privileges to the various user accounts within your Qualys subscription. It is best to design and use asset groups that meet the specific needs of your various user groups, without exceeding the access privileges required.

Asset Group: Business Impact

- Business Impact is used to calculate the Business Risk Score, which assigns a higher weight to critical host assets.
- Demonstrate progress by lowering the Business Risk Score or your Asset Groups.

The screenshot shows the 'New Asset Group' interface. On the left, there's a sidebar with options: Asset Group Title, IPs, Domains, Scanner Appliances, Business / CVSS Info (which is selected and highlighted in blue), and Comments. The main area is titled 'Business Info' and contains fields for Business Impact (dropdown menu), Division, Function, and Location. A red box highlights the 'Business Impact' dropdown menu, which lists: High, Low, Minor, Medium, High, and Critical. Below this is a 'Summary of Vulnerabilities' section showing Total: 92 (0) - Security Risk (Avg): 2.5 - Business Risk: 14/100. At the bottom right is the Qualys logo.

The Business Impact setting is best used when all asset group members reflect the same level of importance or criticality to your organization.

Asset groups can be labeled from low to critical.

The setting you choose here will be factored into something called the "Business Risk Score" which gives a higher weight to vulnerabilities that are detected on more critical host assets.

High is the default Business Impact setting for all new asset groups.

Business Risk

The screenshot illustrates the calculation of Average Security Risk and its integration with Business Impact.

Average Security Risk Calculation:

$$\text{Average Security Risk} = \frac{\text{Sum of Security Risk values for all hosts in the report}}{\text{Number of hosts matching filters}}$$

Business Risk Setup:

The Business Risk Setup window shows the configuration of business impact levels and their corresponding risk values. The 'Business Impact' section contains a grid of values for Critical, High, Medium, Minor, and Low impact levels across various risk levels (1 to 5).

	Critical	High	Medium	Minor	Low
5	100	64	36	16	9
4	64	36	16	9	4
3	36	16	9	4	2
2	16	9	4	2	1
1	9	4	2	1	1

Reports:

Two progress bars are shown at the bottom:

- Security Risk (Avg):** A red progress bar with three segments, indicating a value of 3.0.
- Business Risk:** A yellow progress bar with a green segment, indicating a value of 30/100.

Qualys Logo: The Qualys logo is visible in the bottom right corner of the interface.

The overall Business Risk is calculated as Security Risk x Business Impact.

Scan by Hostname Requirements

To use DNS or NetBIOS names as scanning targets:

- Qualys account must have “Scan by Hostname” enabled.
- Use the DNS or NetBIOS options to add members to Asset Group.
- Scanner appliance must resolve hostname to IP address.
- Only hostnames resolved to IPs in your subscription will be scanned.

Although it is common to use IP addresses (or Asset Groups that contain IP addresses) as scanning targets, with the "Scan by Hostname" feature enabled for your account, you can identify the targets of your scans using DNS names or NetBIOS names.

To accomplish this, you must meet the requirements listed here:

- The "scan by hostname" service must be enabled for your Qualys account. If you are using a Qualys student trial account, scan by hostname is already enabled.
- Use the DNS or NetBIOS options to add members to an asset group. This asset group (with its hostname members) will then become your scanning target.
- Any scanner appliance that will be used to perform the scan, must be configured with a DNS server that can resolve the hostname to its IP address.
- Only hostnames resolved to IPs in your subscription will be scanned.



Asset Tags

AssetView and Tagging



AssetView

Discover assets and use dynamic tags to keep your assets automatically organized.

AssetView provides the following capabilities*:

- Dynamic tagging automatically assigned based on any detectable attribute
- Custom, dynamic, Dashboards
- Query all your asset data obtained via scans and Cloud Agents in one centralized location, instantaneously

* Asset Tagging feature must be enabled within your subscription



Asset Tags are a core component within the Qualys platform, and through the use of Asset Tag Rule Engines, they adjust dynamically and automatically to changes made to your host assets.

Asset Tag Basics

Static Tags

- Assigned manually to host assets.
- Commonly used as the starting point of an Asset Tag Hierarchy.

Dynamic Tags

- Host assignment is determined by Asset Tag Rule Engine.
- Tags dynamically change with updates to host.

Asset Tag Hierarchy

- Tags are typically nested, creating various parent/child relationships.
- A child tag should represent a subset of host assets represented by its parent tag.



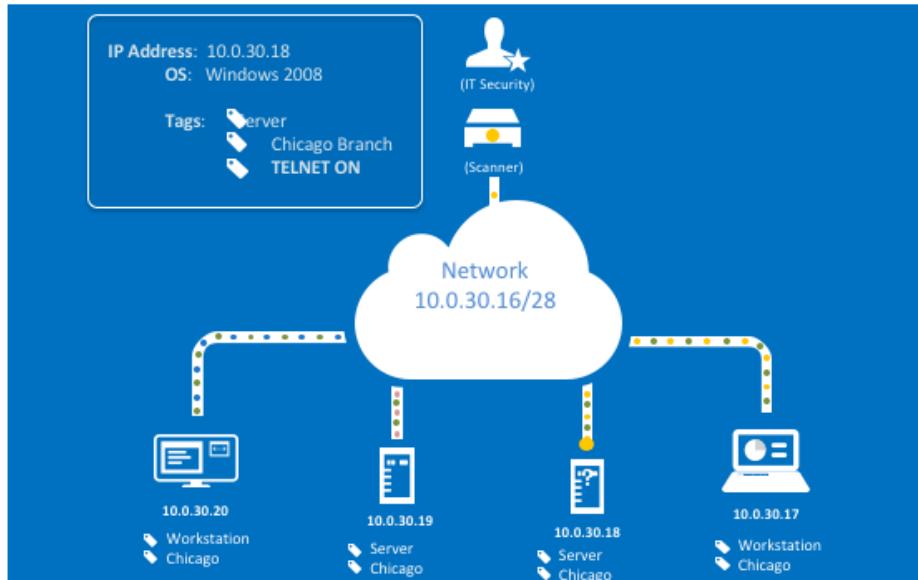
Basic Asset Tag behaviors and characteristics:

First, not all asset tags are dynamic. You can build static tags that you would then manually assign to selected host assets within your account. Static tags are commonly used to establish the starting point for individual asset tag hierarchies.

Dynamic tags; on the other hand, are automatically assigned to host assets, based on their rule engine. Asset tag rule engines focus on different host attributes, and when these attributes change, so do their respective tags.

Asset tags are commonly grouped or organized into Asset Tag Hierarchies. These hierarchies allow you to nest one asset tag below another, creating various parent/child relationships(the idea or objective is to build child tags that represent a subset of host assets represented by its associated parent tag).

Automated discovery and tagging



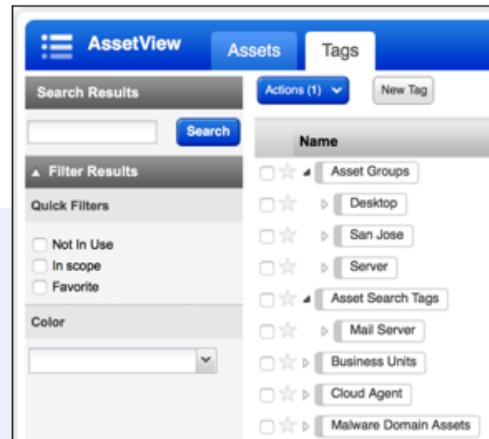
USE CASES

Now we can simply gather data from the end devices and perform analysis on that data using the Qualys cloud computing infrastructure. This means that once a target has been scanned, we can apply asset tags on that device. The tags can be used in an extremely practical way such as simply allowing the security organization to identify Workstation and Servers, perhaps apply a tag to the asset identifying what network it belongs to.

Initial Asset Tags

The service creates some initial asset tags based on existing objects in your account:

- Asset Groups
- Cloud Agent
- Business Units
- Malware Domain Assets
- Web Application Assets



The service creates some initial asset tags based on the existing objects (configurations) in your account, and these are not assigned to assets automatically to start.

Asset Groups. The service creates an Asset Groups tag and a sub-tag for each of the asset groups defined in your subscription. For example, if you have asset groups called Unix and Windows, you'll have a tag called Asset Groups, which will sub-tags called Unix and Windows.

Business Units. The service creates a Business Units tag and a sub-tag for each of the business units defined in your subscription. For the Unassigned business unit, the service creates a sub-tag called Global. For a custom business unit, the service creates a sub-tag with the business unit's name. For example, if your business units are called EU and US, you'll have a tag called Business Units, which will have sub-tags called Global, EU and US.

Malware Domain Assets. If Malware Detection Service (MDS) is enabled for your subscription, the service creates a Malware Domain Assets tag.

Web Application Assets. If Web Application Scanning (WAS) is enabled for your subscription, the service creates a Web Application Assets tag.

Asset Tag Rule Engine

Although tags can be created statically (No Dynamic Rule), Dynamic Asset Tags provide the most flexible and scalable way to automatically discover, organize and manage your assets.

Set the tag type and rules

Rule Engine

Vuln(QID) Exist

No Dynamic Rule

Asset Name Contains

Groovy Scriptlet

IP Address In Network Range(s)

Open Ports

Operating System Regular Expression

Software installed

Vuln(QID) Exist

Asset Search

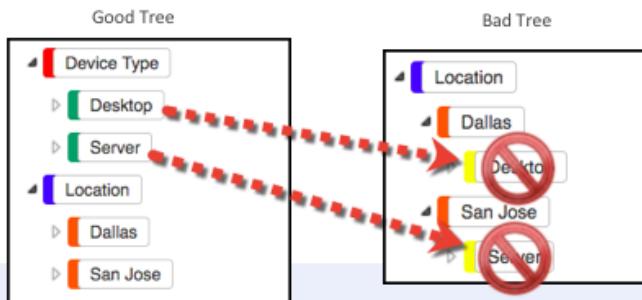


Each dynamic rule engine focuses on a different asset characteristic:

- Name of the asset
- Asset's IP address,
- Open ports discovered
- Host operating system
- Software installed on the host
- Vulnerabilities detected on the host

The Asset Search engine pertains to tags created using VM's Asset Search, and the Cloud Asset Search engine will help you create tags for your assets hosted by a Cloud Provider, such as Amazon, Microsoft, or Google.

Asset Tag Hierarchy Design



- Attempt to group tag hierarchies (parent/child relationships) around some type of common criteria.
- Child tags do NOT inherit the attributes or properties of their parent tags.
- Multiple tags can be combined when selecting targets for scanning and reporting



Do your best to choose tag names that are descriptive, but brief.

To help organize Asset Tag hierarchies, avoid mixing multiple types of rule engines in a single hierarchy.

With this design structure in place, multiple Asset Tags can be combined when selecting targets for scanning and reporting.

The "Desktop" and "Server" tags in the "Bad Tree" do not inherit location information from their parents.

Regular Expressions (regex)

Asset Tagging Rule Engines that support regex:

1. Asset Name Contains
 2. Operating System Regular Expression
 3. Software Installed
- Powerful mechanism for searching and matching character strings.
 - Metacharacters are similar to wildcard characters such as * and ?, but much more powerful.



The foundation for regular expression usage in QualysGuard is based on Perl Compatible Regular Expression (PCRE).

Testing Asset Tags (regex)

The screenshot shows the Qualys Rule Engine interface. At the top, it says "Rule Engine" and "(*) REQUIRED FIELDS". Below that is a dropdown menu set to "Operating System Regular Expression" and a checkbox "Re-evaluate rule on save". A red asterisk (*) is next to the word "REQUIRED FIELDS".

The "Regular Expression*" field contains the regex pattern: `^Windows (7) ((?!\\/).)*$`. Below this is a checked checkbox "Ignore Case".

The "Test Rule Applicability on Selected Assets" section has a "Add Asset:" dropdown menu. It lists three assets: "win7.lab.local" (green checkmark), "vm_win7_x64" (green checkmark), and "windows8_1.lab.local" (red X). To the right of the asset list is a "Test Applicability" button.

In the bottom right corner of the interface is the Qualys logo.

The Testing Tool will allow you to apply (or test) a rule against your current asset inventory

Assets will display a check mark if it matches the expression in the rule.

Assets that do not have data or applications matching the expression, will display an X.

Asset Groups vs. Asset Tags

Asset Groups:

1. Manually updated.
2. Used to assign access rights to Qualys users.
3. Identifies the “Business Impact” of host assets.

Asset Tags:

1. Dynamically updated.
2. Hierarchical organization of assets (nesting).
3. Automates scanning and reporting tasks.

Qualys automatically creates asset tags to match each asset group.



Asset Tag Challenge

How do you perform a scan that uses Asset Tags, if the hosts you are scanning have not yet been tagged?

The screenshot shows a user interface for selecting target hosts. At the top, it says "Choose Target Hosts from". Below that, there's a note: "Tell us which hosts (IP addresses) you want to scan." Two radio buttons are shown: "Assets" (unchecked) and "Tags" (checked). A blue box surrounds the "Tags" option and contains the text: "Use IP Network Range Tags" with a checked checkbox, followed by the explanatory text: "Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag." Below this box, there's a dropdown menu set to "Any" with the text "Include hosts that have [dropdown] of the tags below. Add Tag". At the bottom of the list is a single item: "Order Processing X".

Solution: Use an Asset Tag based on the “IP Address In Range” rule engine, and select the “Use IP Network Range” check box when launching the scan.



This scanning option only works with the “IP Addresses in Network Range” Asset Tags.

A typical NETBLOCK scan will be performed, even though an Asset Tag is used as the scanning target.

AssetView Data Sources

- Scanner Appliances



- Virtual Scanners



- Agents



- Connectors



The Qualys AssetView application collects its data and asset inventory information, using one or more data collection technologies, including:

- Qualys scanner appliances
- Qualys virtual scanners
- Qualys Cloud Agents

This first group of technologies provides data that is used for both host assessment and asset inventory purposes.

When enabled for AssetView, connectors provide an additional stream of asset inventory data from your assets hosted by popular cloud providers, including:
Amazon, Microsoft, and Google.

Lab 4

Assets and Asset Inventory



VM

Reporting

Qualys Reporting

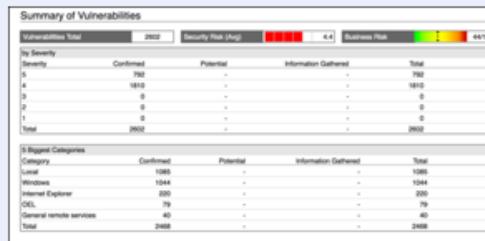
Report Types:

- Scan Reports
- Remediation Reports
- Patch Reports
- Map Reports
- Scorecards

Uses a central repository for users to store reports for multiple viewers

Report Summary

User Name:	Administrator
Login Name:	qualysadmin
Company:	Qualys Training
User Role:	Manager
Address:	123 Main Street
City:	Mountain View
State:	CA
Country:	United States of America
Created:	2017-06-22 10:43:26 (GMT)
Template Title:	High Security Report
Asset Groups:	All
IPs:	2002
Hosts:	Host
Trend Analysis:	Lastest vulnerability date
Date Range:	January 21, 1999 - June 22, 2017
Active Hosts:	41
Host-Matching Filters:	27



A scan report will help you view and analyze the findings from your vulnerability scans as well as data collected by Qualys Cloud Agents. A scan report template provides numerous options for displaying the technical details associated with each detected vulnerability.

On the other end of the spectrum, scorecard reports present a high-level view of your scan results with summary statistics and graphic illustrations of useful metrics.

The mapping feature in Qualys VM provides a useful service for discovering new host assets. Some of the features that you'll find in a map report can simplify the tasks of creating asset groups or adding new assets to your account.

A patch report is similar to a scan report in that it provides evidence of detected vulnerabilities. However, the focus of this report is on the patches that can be used to fix or mitigate detected vulnerabilities. Patch reports make it easier to see the number of host assets impacted by a single patch.

Remediation reports will help you identify the patch or mitigation teams responsible for specific vulnerabilities and help you to assess their performance. These reports can be especially useful for quickly locating overdue patches and preventing potential process bottlenecks.

Reporting Objectives

1. Use reports to drive your mitigation and patching activities:

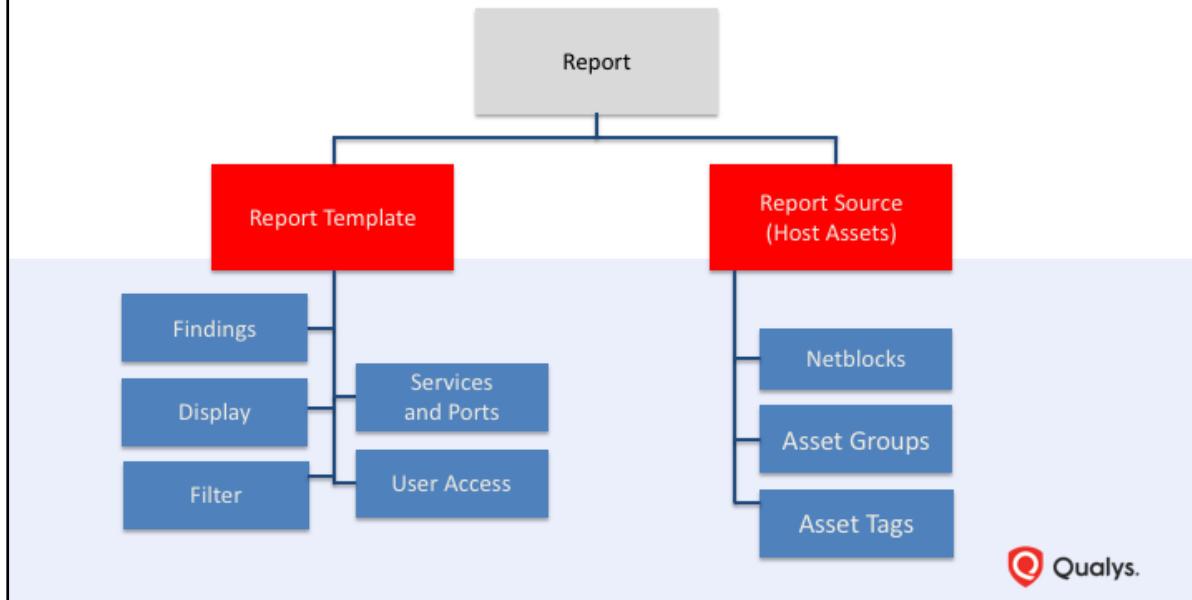
- Patch Report created at the START of a patch cycle, to help operational teams calculate and schedule patching priorities.
- Scan Report to identify CRITICAL assets with HIGH risk vulnerabilities, or HIGH risk vulnerabilities with known threats.

2. Use report metrics to assess the progress of your vulnerability management program and teams:

- Patch Report created at the END of a patch cycle, to help monitor and evaluate patch activity and accuracy.
- Remediation Report to quickly identify "overdue" patches.
- Trend Report to assess "Business Risk by Asset Group Over Time" (e.g., Executive Report).
- Vulnerability Scorecard Report to compare vulnerability distribution by status (e.g., NEW, ACTIVE, RE-OPENED and FIXED)



Report Configuration Components



This diagram illustrates the basic components needed to build a report (scorecard reports, authentication reports and asset search reports, do not require a report template).

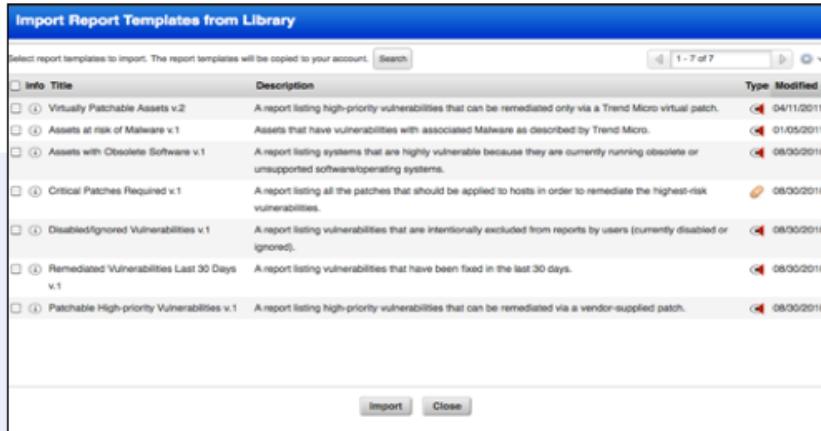
All report types require that you select a report source or the assets you intend to target in your report. You can accomplish this using a range of IP addresses or even a single IP, or any asset groups or asset tags you've created.

For the report types that require a report template, you can choose a custom template that you have created, or select one from the Qualys Report Template Library. A report template provides dozens of options for selecting the data and findings that will be included in your report, how that data will be displayed, and who will be able to view the reports that are generated.

Notice that a Qualys scanner appliance is not included in this diagram. Running a report does not in any way launch a scan. Scanning and reporting are separate tasks, and therefore scans must be completed, prior to building their associated reports.

Report Templates

Qualys has a set of standard templates that assist in reporting on scans, maps, and remediation.



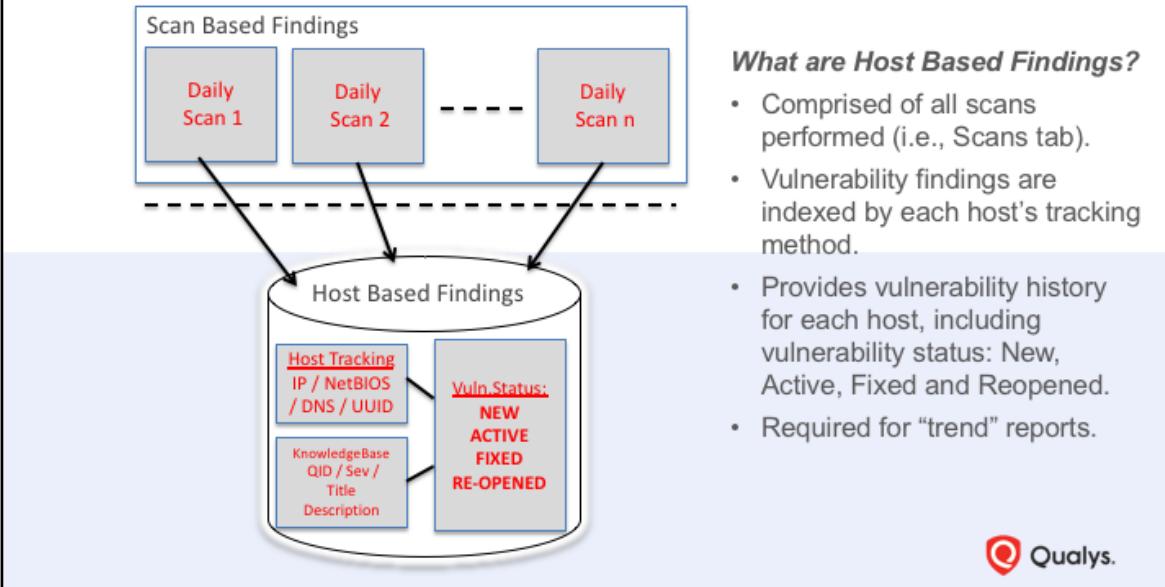
Report templates allow you to select from dozens of filtering and display options, which are then saved and used again and again to conveniently reproduce the same report behavior. Report templates can be customized for different target audiences within your organization. A report template simply takes the data and information from your RAW scan results and formats, filters, and displays this information in a way that is meaningful and useful to its target audience.

For example the Executive template will present vulnerability findings in a fashion that is more suitable for executive or managerial members of your organization, providing helpful graphics and summary statistics, but omitting the type of details that are more useful to patching and mitigation teams.

The Technical report template; on the other hand, is more suitable for members of your operational teams, because it focuses on the information and details needed to patch and mitigate detected vulnerabilities.

Under the Templates tab you'll find pre-built templates for many useful reporting tasks, and you can import more templates from the Template library.

Scan Based vs. Host Based Findings



The "scan-based" findings in your account are comprised of each individual vulnerability scan performed, where each scan tells a unique story based on its position or placement within your scanning timeline. Reports that use scan-based findings are often referred to as "snapshot" reports, because they represent an individual snapshot in time without any influence from scans that have been performed previously or scans that have occurred later in time. You'll find all of your scan-based findings listed under the Scans tab.

All scan based findings are poured into another bucket or database known as the host-based findings. The host-based findings database collects data from completed scans and indexes each detected vulnerability according to the "tracking method" you have selected for each host asset. Host-based findings will allow you to view the vulnerability history of any host asset, and unlike scan-based findings; host-based findings allow you to create vulnerability "trend" reports that track the status of any vulnerability (from new, to active, fixed, or reopened) on any host.

Qualys Patch Report

Actionable and prioritized list of patches to apply - KB
supersede information included, so only the most relevant patches displayed.

The screenshot shows a Qualys Enterprise interface titled "Windows Workstations". At the top, there's a summary box with the following data:

Total Patches	407
Hosts Requiring Patches	12
Vulnerabilities Addressed	2,031

Below the summary is a table titled "PATCHES" which lists various vulnerabilities and their details. The table has columns for "Vulnerability ID", "Severity", "Title", "Published", and "Hosts". One row in the table is highlighted in yellow, indicating it is selected or important. The table also includes a "HOSTS requiring Microsoft Windows Update for Vulnerabilities in Adobe Flash Player" section.

Vulnerability ID	Severity	Title	Published	Hosts
MBS18-04	5	Oracle Java Unspecified Vulnerabilit...	20 days ago	2
Mozilla A...	3	Mozilla Firefox Multiple Vulnerabilit...	61 days ago	1
MBS18-05...	5	Microsoft Windows Update for Vulnerabilit...	63 days ago	3
APB18-04	5	Adobe Flash Player and AIR Securi...	63 days ago	3
MBS18-03	4	Microsoft Windows PDF Library Re...	63 days ago	3
MBS18-02	4	Microsoft Windows Journal Remote ...	63 days ago	3
MBS18-01	4	Microsoft WebDAV Privilege Escalati...	63 days ago	3
MBS18-00	4	Microsoft Windows Remote Code Ex...	63 days ago	3

Online Format - Provides more interactivity (sorting, filtering)



A patch report is similar to a scan report in that it provides evidence of detected vulnerabilities. However, the focus of this report is on the patches that can be used to fix or mitigate detected vulnerabilities.

Patch reports make it easier to see the number of host assets impacted by a single patch.

Qualys Scorecard Reports

Provide vulnerability data and statistics appropriate for different business groups and functions.

Easy to create and customize (quickly)

- Most Vulnerable Hosts
- Most Prevalent Vulnerabilities
- Vulnerability Scorecard Report

The screenshot shows a Qualys Enterprise interface for a 'Vulnerability Scorecard Report'. At the top right is the date 'August 06, 2015'. The report title is 'Vulnerability Scorecard Report' with a subtitle 'Type: Vulnerability Scorecard Report'. Below the title, there's a table of report details:

Report Title	Vulnerability Scorecard Report
Created	Created 08/06/2015 at 10:25:11 (GMT-0500)
User Name	MANAGER-Nick
Login Name	qualysHQ2
User Role	Manager

On the right side, there's a 'Company Address' section:

Qualys Training
123 Cold Street
Cleveland, Ohio
United States of America

Below the report details, there are two main sections: 'Report Settings' and 'Results Summary'.

Report Settings includes 'Filter settings' and 'Display settings'.

Filter settings includes:

- Source: Asset Groups (All Operating)
- Operating System: Business Risk Goal (Off)
- Systems: Vulnerability Type (Confirmed)
- Vulnerability Type: Vulnerability Status (Off)
- Display non-running kernels: Vulnerability Age (Off)
- Exclude non-running kernels: Off
- Exclude non-running services: Off
- Exclude QID not exploitable due to configuration: Off

Display settings includes:

- Business Risk Goal: Off
- Vulnerability Type: Off
- Vulnerability Status: Off
- Vulnerability Age: Off

Results Summary includes a 'Vulnerability Distribution by Severity' section.

Qualys.

Scorecard reports present a high-level view of your scan results with summary statistics and graphic illustrations of useful metrics.

Qualys Authentication Report

The Authentication Report shows the authentication status for each scanned host:

- Passed
- Failed
- Passed with insufficient privileges
- Not Attempted

* Run this report after an authenticated scan to verify that authentication was successful to the target hosts

The screenshot shows the 'New Authentication Report' dialog box. It has several sections: 'Report Details' (Title: [empty], Report Format: * HTML pages), 'Report Source*' (Asset Groups selected), 'Display & Filter' (Details, Summary Section, Details Section, Additional Host Info (OS, scan date, successful auth date) checked), and 'Report Options' (Scheduling). At the bottom are 'Run' and 'Cancel' buttons.

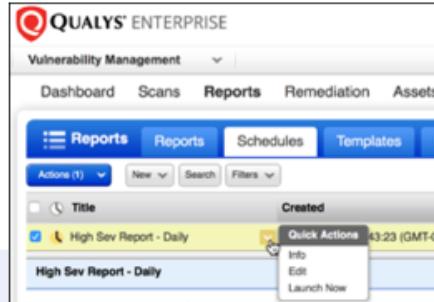
Authentication Reports can also be scheduled.



Qualys recommends performing scans in authenticated mode. However, the benefits gained from this practice, will not be seen, if the authentication attempted by your scanner appliance, fails or is obstructed in some other way.

The authentication report will help you to quickly identify authentication issues, with details that will help you to resolve the problem at hand.

Scheduled Reporting



Several report types that can be scheduled:

- Template-based scan reports (using Host Based Findings)
- Scorecard reports
- Patch reports
- Template-based compliance reports
- Remediation reports



Scheduled Reporting

Users have the ability to schedule reports to run automatically at a scheduled time, on a recurring basis, and can also set options to notify select distribution groups when a report is complete and ready for viewing.

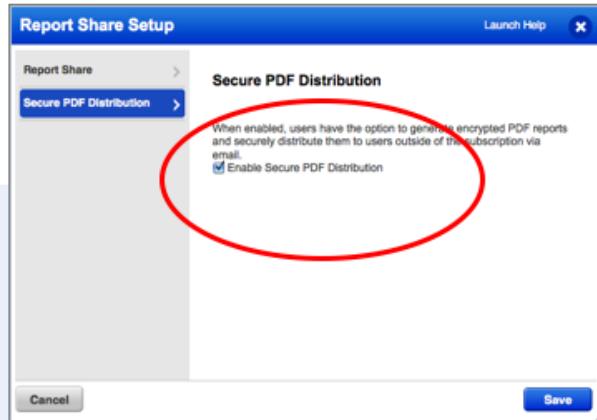
Schedule a Report

You can schedule template-based scan reports (set to Auto source selection), scorecard reports, patch reports, template-based compliance reports and remediation reports.

To create a new report schedule, go to Reports > Schedules and select the type of report you're interested in from the New menu. In the example below, a new template-based scan report will be scheduled.

Subscription Report Share Setup

- Report Share is a centralized location for storing and sharing reports
- When enabled for subscription, Managers specify the maximum amount of report data that each user may save
- Managers have the option to enable secure PDF distribution of reports



 Qualys.

Configure the user limit for report storage space and enable Secure PDF Distribution.

Reporting Use Case

The screenshot shows the Qualys reporting interface. On the left, there's a 'Scheduling' section where a report is set to run automatically at 3:00 AM on Aug 01, 2013, for every week. On the right, there are 'Asset Groups' and 'IP Ranges' fields, along with a 'Vulnerability Filters' section. Under 'Status', 'New' is checked, while 'Active', 'Re-Opened', and 'Fixed' are unchecked. A red dotted line connects the 'Scheduling' and 'Vulnerability Filters' sections to the scenario text below.

Scenario: I need a weekly report of all the new vulnerabilities found on my Windows desktops. My Windows admins complain, "the reports are too long." They just want to know what the vulnerability is and how to fix it. They are also only interested in the vulnerabilities that can be confirmed, and those that have the greatest security risk (severity level) – how can we accomplish this?

The screenshot shows the 'Selective Vulnerability Reporting' section. It includes a list of items to include in the report: Text Summary, Vulnerability Details (which is checked), Threat, Impact, Solution, and Patches and Workarounds. To the right, there's a 'Complete' or 'Custom' selection, with 'Custom' selected. Under 'Custom', there's a dropdown menu showing 'Info Title' and a 'Confirmed Severity 4+5 Vulnerabilities < 1'. A red dotted line connects the 'Vulnerability Details' checkbox in the first section to the 'Confirmed Severity 4+5 Vulnerabilities < 1' option here.



Reporting Use Case

Scenario: What type of vulnerability is more prevalent in my network? How can I tell?

The screenshot shows a Qualys Enterprise dashboard titled 'Most Prevalent Vulnerabilities Report'. It includes fields for Report Title, Created, Last Modified, Login Name, and User Role. On the right, it shows Company Address and a date stamp of August 06, 2015. Below these are sections for Business Unit, Asset Group, Asset Tags, and Operating System. A detailed list of asset types is provided, such as All, All PCI, and various internal and external network segments.

Scenario: My manager wants to see what we have accomplished with Qualys. Where can I find that?

This screenshot shows the 'Reports' section of the Qualys interface. A dropdown menu is open under the 'Reports' tab, listing several report types: Scan Report, Scorecard Report..., Map Report..., Patch Report..., Authentication Report, Remediation Report... (which is highlighted with a yellow box), and Compliance Report... A 'Type L' label is visible next to the dropdown menu.

Qualys.

Reporting Use Case

Scan Report Template

Vulnerability Filters

Status

New Active Re-Opened Fixed

64.41.200.349 (trn-win2012-dc.trn.qualys.com, TRN-WIN2012-DC) - Global
Default Network
Total: 0 (0) - Security Risk: 0.0

Windows 2012 Standard 64 bit Edition AD
Windows Server 2012 - x64

Status	Confirmed	Potential	Total
New	0	-	0
Active	0	-	0
Re-Opened	0	-	0
Total	0	-	0
Fixed	3	-	3
Changed	0	-	0

Severity	Confirmed (Trend)	Potential (Trend)	Total (Trend)
5	0 (0) +	-	0 (0) +
4	0 (0) -	-	0 (0) -
3	0 (0) -	-	0 (0) -
2	0 (0) -	-	0 (0) -
1	0 (0) -	-	0 (0) -
Total	0 (0) -	-	0 (0) -

Category	Confirmed (Trend)	Potential (Trend)	Total (Trend)
Total	0 (0) -	-	0 (0) -

Vulnerabilities (3)

- Microsoft Windows SMB Remote Code Execution - Shadow Broker CVSS: - CVSS3: 7.6 Fixed
- Microsoft Internet Explorer Security Update for May 2017 CVSS: - CVSS3: 7.6 Fixed
- Microsoft Windows .NET Framework Information Disclosure Vulnerability (MS16-091) CVSS: - CVSS3: 6.0 Fixed

What information can you show to reflect progress?

- Fixed Vulnerabilities
- Trending (Include on the vulnerabilities you are trying to address. Ex. 4's and 5's)



Reporting Best Practices

1. Determine what reports need to be run. What are your goals?
2. Assign reports to users within Qualys or share them via secure distribution.
3. Schedule reports to run automatically after scans complete.



Lab 5

Reporting



TP

Threat Protection

Threat Protection

Risk = Threat x Vulnerability (Severity)

Severity = Impact if vulnerability is exploited.

- Pinpoint assets with highest exposure to the latest threats.
- Prioritize vulnerability findings so you can:
 - Remediate biggest threats quickly.
 - Reduce chances of breach*

*Majority of breaches happen because exploitation of known vulnerabilities

98 Qualys, Inc. Corporate Presentation



Traditionally the Qualys Vulnerability Management application has relied on severity levels (exclusively) to help you calculate the risk associated with your detected vulnerabilities. The higher the severity level the greater the risk.

With the addition of the Threat Protection application to the Qualys cloud platform, this calculation is improved by including known threats into the equation, which can have a significant impact on vulnerabilities of all severity levels.

The goal of Qualys Threat Protection is to help you pinpoint your assets that have the highest exposure to the latest known threats, so that you can prioritize and mitigate the high risk vulnerabilities quickly.

Real-time Threat Intelligence (RTI) Feed

Public Exploit	Easy Exploit
Actively Attacked	No Patch Available
Zero Day	High Data Loss
High Lateral Movement	Denial of Service
Exploit Pack	Malware

99 Qualys, Inc. Corporate Presentation



- Vulnerabilities with public exploits are those where exploit knowledge is well-known and working exploit code is publicly available.
- Easily exploited vulnerabilities are associated with attacks that can be carried out easily, and typically do not require additional information.
- Actively Attacked vulnerabilities are those where active attacks are being observed in the wild.
- If a vendor has not provided an official fix for a vulnerability it will be listed as No Patch Available
- Zero day vulnerabilities are characterized by active attacks observed in the wild and no patch available from the vendor.
- High Data Loss vulnerabilities can potentially result in massive data loss on the affected host.
- a High Lateral Movement vulnerability that is successfully exploited, will potentially allow an attacker to compromise other assets on the network.
- Denial of Service vulnerabilities can adversely impact host and application availability.
- Some vulnerabilities are associated with exploit kits like Angler, Nuclear, Rig and others.
- And other vulnerabilities are associated or targeted by known malware applications.

Query Token

```
vulnerabilities.vulnerability.threatIntel.easyExploit:true
```

Key token to query RTIs in ThreatPROTECT Specific RTI

```
vulnerabilities.vulnerability.threatIntel.activeAttacks: true
```

```
vulnerabilities.vulnerability.threatIntel.denialOfService: true
```

```
vulnerabilities.vulnerability.threatIntel.easyExploit: true
```

```
vulnerabilities.vulnerability.threatIntel.exploitKit: true
```

```
vulnerabilities.vulnerability.threatIntel.exploitKitName: 'Angler'
```

```
vulnerabilities.vulnerability.threatIntel.highDataLoss: true
```

```
vulnerabilities.vulnerability.threatIntel.highLateralMovement: true
```



Threat Intel Query Tokens

Query Token

```
vulnerabilities.vulnerability.threatIntel.easyExploit:true
```

Key token to query RTIs in ThreatPROTECT Specific RTI

```
vulnerabilities.vulnerability.threatIntel.malware: true
```

```
vulnerabilities.vulnerability.threatIntel.malwareName: `JS_EXPLOIT.MEA`
```

```
vulnerabilities.vulnerability.threatIntel.noPatch: true
```

```
vulnerabilities.vulnerability.threatIntel.publicExploit: true
```

```
vulnerabilities.vulnerability.threatIntel.publicExploitName: `MSpamAssassin spamd  
Remote Command Execution`
```

```
vulnerabilities.vulnerability.threatIntel.zeroDay: true
```



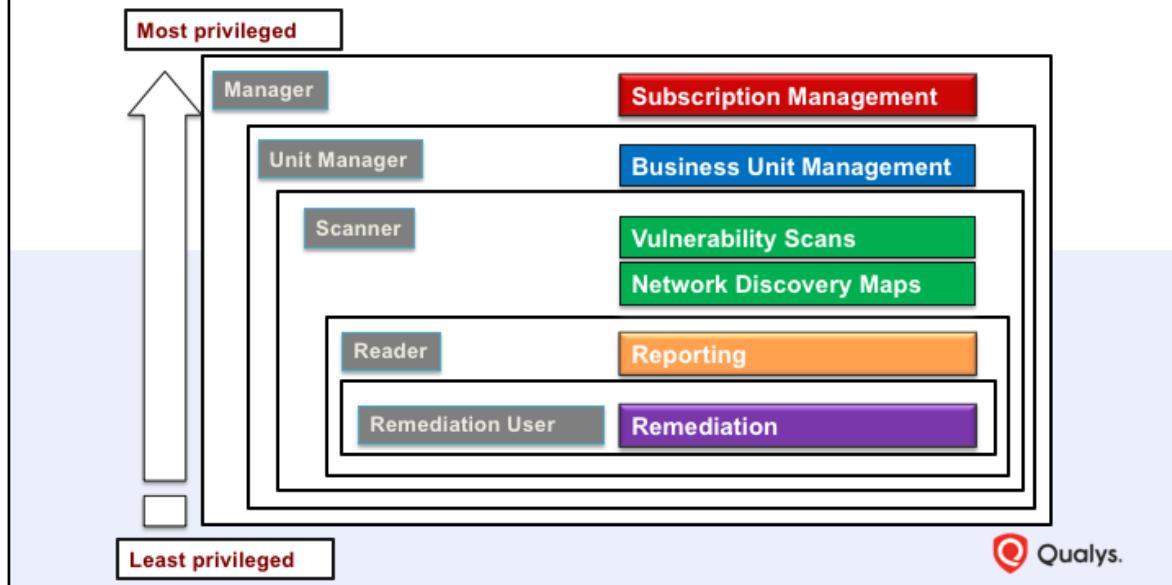
Threat Intel Query Tokens



User Management

User Privilege Hierarchy

Standard User Roles



This diagram illustrates the standard user roles that are typically assigned to Qualys user accounts.

The least privileged roles are near the bottom of the diagram and the roles with the greatest privileges are listed near the top. In typical hierarchical fashion, higher level roles automatically include the privileges of roles listed beneath them. For example the default privileges for the scanner role automatically include the privileges of both the reader and remediation user roles.

The REMEDIATION USER role provides a convenient way to assign detected vulnerabilities to specific Qualys users. READERS can run reports, and depending on their host access privileges, read reports created by other Qualys users. The SCANNER role performs SCANNING tasks (which also include mapping). The UNIT MANAGER ROLE has special extended privileges designed for the management of BUSINESS UNITS. The most privileged users are Managers - they have full privileges and access to all assets in the subscription. Managers have management authority for the your entire subscription, while Unit Managers only have authority over their assigned business units.

Other User Roles

- **Auditor**
 - This role is used exclusively by the Policy Compliance application and has no privileges within VM.
- **Contact**
 - This role only receives email notifications from Qualys Cloud Platform Services and is not assigned login credentials.
- **User Administrator**
 - Has access to Users, Asset Groups, Business Units, and Distribution Groups.
 - Can create and edit other user accounts (including Managers), but cannot create or edit other User Administrators.
- **Knowledgebase Only (not enabled by default)**
 - Has limited access to the UI, but can view QIDs in the Qualys KnowledgeBase.
 - This role can send and receive vulnerability notifications.

104 Qualys, Inc. Corporate Presentation



The auditor user role was created for the Qualys Policy compliance application and does not have privileges in Qualys VM.

A contact user can be configured to receive email notification from the Qualys Cloud Platform. Contact users do not have login credentials.

Similar to the Unit Manager, the User Administrator was designed to help manage other user accounts in your subscription (while avoiding the risk of creating too many Manager accounts). This role only has access to users, asset groups, business units, and distribution groups.

The KnowledgeBase only role is not enabled by default and is used primarily for accessing the Qualys KnowledgeBase.

Extended Permissions

Different Roles

Each role has its own permission set

Each user can get extended permissions

Extended permissions vary from role to role.

User Role

User Role: *

Allow access to:

- Manager
- Unit Manager
- Scanner**
- Reader
- Remediation User

Business Unit: *

Extended Permissions

Allow this user to perform the following actions:

- Manage VM module
 - Create/edit virtual hosts
- Create option profiles
- Purge host information/history
- Manage PC module
- Manage web applications
- Create web applications

The Qualys logo, which consists of a red stylized 'Q' icon followed by the word "Qualys" in a black sans-serif font.

Extended permissions can be added to the default privileges of most user roles.

User Management

VIP and Password Resets

The screenshot shows a user management interface with a sidebar menu on the left and a main configuration area on the right.

Left Sidebar (Menu):

- General Information >
- Locale >
- User Role >
- Asset Groups >
- Permissions >
- Options >
- Account Activity >
- Security >** (The selected menu item is highlighted in blue)
- User Status >

Main Configuration Area:

VeriSign Identity Protection (VIP)

Status: Not Registered

VIP two-factor authentication

Note: This option enables VIP two-factor authentication for users to login into Qualys GUI. This setting impacts UI access only.

VeriSign Identity Protection: Enabled

Password

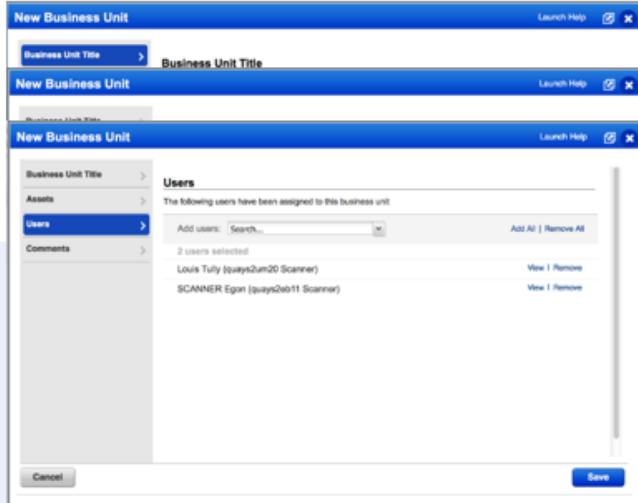
This will automatically generate a new password. It will not go into effect until you confirm the change. **Change...**



Two-factor authentication can be enabled for individual or selected user accounts.

Business Unit

- Create Business Unit in Users Section
- Add Asset Groups to the Business Unit
- Assign Scanner & Reader Users (optional)



Business Units provide an effective way to divide and distribute the vulnerability management tasks and responsibilities within your Qualys subscription.

Business Unit Manager

Privileges:

Perform all vulnerability management functions:
Map, Scan
Remediation
Reporting
Manage assets, add users, and publish template reports within their Business Unit

Extended Permissions :

Add assets
Create profiles
Purge host information
Create/edit configurations (remediation policy, authentication records/vaults, virtual hosts)
Manage compliance, web applications
Manage virtual appliances

Restrictions:

Can only be in one Business Unit
Can only be created if the Business Unit has been established
Limited to Asset Groups defined in their Business Unit
May not have rights to run specific reports via the API

Extended Permissions

Allow this user to perform the following actions:

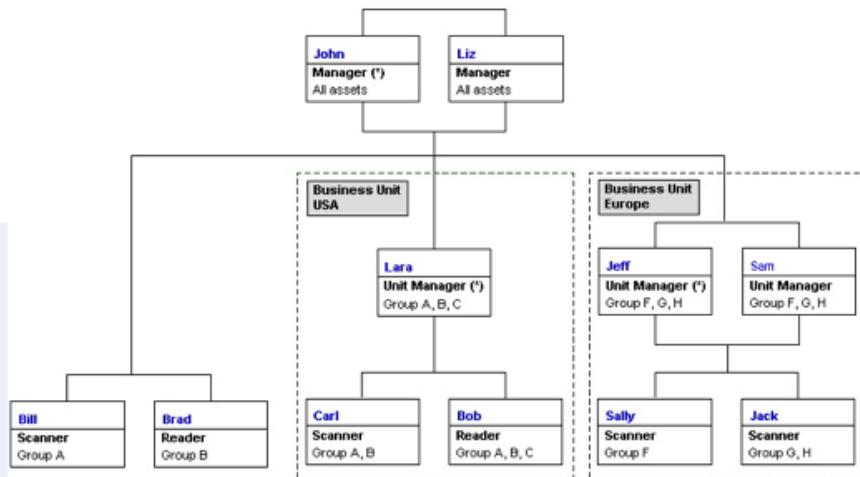
- | | |
|--|---|
| <input checked="" type="checkbox"/> Manage VM module | <input type="checkbox"/> Create/edit remediation policy |
| <input type="checkbox"/> Create/edit virtual hosts | |
| <input checked="" type="checkbox"/> Add assets | |
| <input checked="" type="checkbox"/> Create option profiles | |
| <input type="checkbox"/> Purge host information/history | |
| <input type="checkbox"/> Create/edit authentication records/vaults | |
| <input type="checkbox"/> Manage PC module | |
| <input type="checkbox"/> Accept/Reject exceptions | |
| <input type="checkbox"/> Create/edit compliance policies | |
| <input type="checkbox"/> Create User Defined Controls | |
| <input type="checkbox"/> Update/Delete User Defined Controls | |
| <input checked="" type="checkbox"/> Manage web applications | |
| <input checked="" type="checkbox"/> Create web applications | |
| <input type="checkbox"/> Manage virtual scanner appliances | |



The role of Business Unit manager comes with special extended privileges for managing assets and users, within the scope of a Business Unit.

The successful implementation of Business Units (with unit managers) provides an effective way to limit the total number of Manager accounts in your Qualys subscription.

Business Unit Illustration



Business Units Contain Assets and Users.

Adding assets to a business unit is accomplished by adding Asset Groups

User accounts can be added in the same way.

The Unit Manager is the primary contact for each business unit and will handle the administrative needs of the BU members.

A business unit can have more than one manager.

Subscription Setup

Security

Define Qualys user account security settings

Users > Setup > Security

- Restrict IP access
- Set Password Security
- Enable VIP for all users
- External IDs
- Session Timeout
- Verify New Data Security Model

Password Security

Password expires after months

Lock account after failed login attempts

Allow user defined passwords

Minimum length of password is characters (Range: 6 - 16)

Password must contain alpha and numeric characters

Force password change at initial login

Notify user to change password days before expiration

Allow users to change expired password at login



- Only Manager users can edit the default security options for your Qualys account. The Security setup changes you make here, will affect all user accounts in your subscription.
- You can restrict access to your to your account subscription by client IP address or IP address range. Be very careful with this option, as a mistyped IP address could potentially lock-out all user accounts, including Managers.
- The password security options will allow you set password expiration intervals, account lockout thresholds, password strength requirements and even an option to let users define their own passwords.
- If two-factor authentication is enabled here, it will affect all user accounts in your subscription. Your other option is to configure two-factor authentication individually for each user account.
- The New Data Security Model should be enabled to leverage advanced features and services, and the session timeout threshold configured here will become the default session timeout threshold for all user accounts.



Remediation

Remediation Basics

- Remediation Policy can be used to assign a vulnerability to a specific user account (for mitigation).
- Remediation Policy can be used to ignore specific lists of vulnerabilities.
- Qualys automatically updates “Fixed” vulnerabilities (when no longer detected).
- Resolved Date indicates when a vulnerability has been resolved, ignored, or fixed (the earliest of the three)



Remediation Policies are commonly used to assign detected vulnerabilities to specific Qualys users.

Remediation Policies can be created to ignore vulnerabilities you do not plan to address.

Remediation Policies

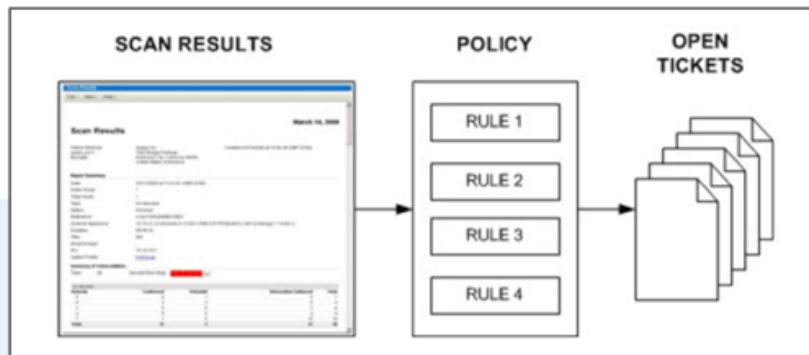
Use Remediation Policies to measure the effectiveness of your vulnerability mitigation and remediation operations:

- Design Remediation Policies to address and measure specific problem areas and concerns
 - OS patching (according to impact and risk)
 - Application patching (according to impact and risk)
 - Exploitable Vulnerabilities (according to impact and risk)
- Assign an expiration date to targeted policies, and then focus on overdue tickets to identify potential process issues.
- Don't create policies for vulnerabilities that won't be measured.



Remediation Workflow

Automatic Ticket Creation based on order of policies.



1. Set achievable remediation goals.
2. Start creating tickets in phases.
3. Regularly run Remediation reports to monitor progress.



When host assessments are processed, they are evaluated against your remediation rules, in order, in a top down approach. Policies at the top of the list have precedence over the policies below them.

The service will open tickets based on what's discovered via scan or cloud agent detection.

Think of a ticket as an audit trail for each detected vulnerability; an audit trail that identifies the specific Qualys user assigned to this vulnerability, and the deadline (in number of days) this user has to fix or mitigate the associated vulnerability.

Your tickets will automatically close when future assessments verify the vulnerability has been fixed.

Remediation SLA

Implement a Service Level Agreement for remediation:

- Build a remediation report based on tickets per asset group or tickets per user.
- “How well am I meeting my SLA?”

Tickets per Asset Group						
Group	# of Tickets	Open	Resolved	Closed	Avg. Resolution	Overdue
All	636	237	4	395	75.3	213
Qualys DMZ	458	215	4	239	75.3	191
LAB	178	22	0	156	N/A	22
Windows	140	22	0	118	N/A	22
Unix	143	0	0	143	N/A	0

Tickets per User						
Name	# of Tickets	Open	Resolved	Closed	Avg. Resolution	Overdue
Milton Waddams	204	200	4	0	75.3	200
Bill Lumbergh	37	37	0	0	N/A	13
Philip Niegos	395	0	0	395	N/A	0

115 Qualys, Inc. Corporate Presentation



Reports that display Tickets per Asset Group or Tickets per User provide useful information for monitoring your remediation service level agreements.

Remediation

Create a new Rule

Conditions
Tell us the hosts and vulnerabilities this rule applies to.

Hosts:

Assets Tags

Use IP Network Range Tags
Choose from tags defined with IP address rules. We will include the entire IP range(s) in each selected tag.

Include hosts that have Any All of the tags below.

Win-Servers

Tell us the action you want to take

Create tickets - set to Open

Tickets will be created and assigned to a user with a deadline for resolution.

Assign to:

Set deadline: This ticket must be closed in days (Range: 1-730)

Include comment in ticket history:

Create tickets - set to Closed/Ignored

Do not create tickets

Assignment

- A specific user
- Asset Owner
- The user who launched the scan

Set Deadline for remediation

Ignore - do not create a ticket



Remediation policies contain two basic components:

1. Conditions (that identify the targets of the policy)
2. and Actions (that identify the task to be performed, if the target conditions are met).

Remediation

Manual Ticket Creation & Verification

Manual Trouble ticket generation

- From Host Data Report

▼ Vulnerabilities (147) □ □

- 5 EOL/Obscure Software: Microsoft .NET Framework 4 - 4.
- 5 Microsoft Foundation Class Library Remote Code Execution (MS11-025)
- 5 Microsoft Windows Kernel-Mode Driver Elevation of Privilege (MS13-027)
- 5 Microsoft Windows SMBv1 Remote Code Execution - ShadowCopy (ETERNALCHAMPION)
- 5 Microsoft Windows Group Policy Preferences Password Enforcement Vulnerability (MS14-025)
- 5 Microsoft Windows SMBv1 and NBT Remote Code Execution (MS14-025)

Create Ticket Launch Help

General Information

Name: EOL/Obscure Software: Microsoft .NET Framework 4 - 4.5.1 Detected
Severity: ██████ 5
IP: 64.41.200.249
Port:
Instance:
FQDN: tm-win2012-dc.tm.qualys.com

Edit Ticket

Assign to: * READER_Venkman (quayn2km4 : Reader)
Set Deadline: * This ticket must be closed in days (Range: 1-730)

Comments:
Update required



Manually create tickets directly from within a vulnerability report (HTML format). Alternatively, individual vulnerabilities can be ignored.

Labs 6 and 7

User Management and Remediation





Exam

Exam Tips and CPE

- You have five attempts to pass
- The test is linear, no going back to an older question
- Passing score: 75% and above
- No negative marking
- Test can be taken anytime
- 30 questions (Multiple choice included)
- You may use presentation slides, lab exercises, Qualys Community, and you may have an active Qualys session open while attempting the exam.
- No set time limit (please start a new LMS session, before launching the exam).
- A CPE credit is earned for each hour of attendance.



Useful Resources



The screenshot shows the Qualys Community homepage. The header includes the Qualys logo and navigation links: Home, Discussions, Blogs, Social Media, Events, Training, Help Center, and Members. Below the header, a banner reads "A Community for Security Professionals" and "Learn. Share. SECURE." It features a "Start a discussion" button and a "View discussions" button.

Qualys Platform Status		
This page reports known incidents affecting Qualys shared platforms. If you're experiencing a problem that isn't shown here, please report it .		
Platform	URL	Status
US Platform 1 View notifications	qualysguard.qualys.com portal.qualys.com	Online
US Platform 2 View notifications	sg2.qualys.com portal.sg2.qualys.com	Online

- Your LMS account does not expire
- Register for training sessions on www.qualys.com/training
- Qualys Community and Qualys LMS are not SSO logins
- Qualys Architecture : <http://www.qualys.com/enterprises/architecture/>

Free Tools & Trials

- BrowserCheck
- SSL Server Test
- FreeScan
- Patch Tuesday Audit
- SCAP Scan





Mapping

Mapping Options

DNS Reconnaissance

- Domain Lookup <whois> (identifies DNS servers)
- DNS Zone Transfer (collects host records from DNS database)
- DNS Brute Force (www.qualys.com, ftp.qualys.com, mail.qualys.com)
- Reverse DNS Lookups (based on IPs already discovered/known)

Options	
<input type="checkbox"/> Perform Live Host Sweep	DNS recon will not be included in map results: - No forward or reverse DNS lookups - No DNS zone transfers - No DNS bruteforcing
<small>Note: Edit host discovery options on the Additional tab.</small>	
<input checked="" type="checkbox"/> Disable DNS traffic	<small>Note: Applies to maps on target domains with netblock(s).</small>

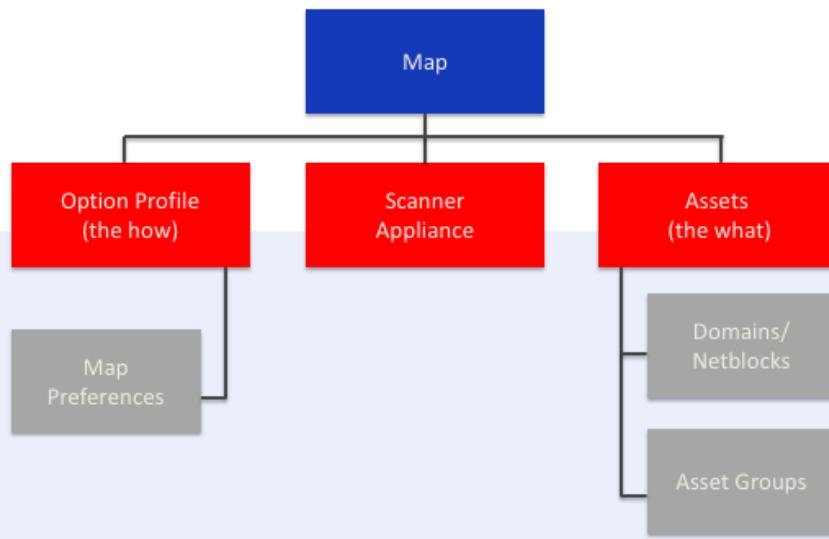
Host Sweep (via ICMP, TCP and UDP probes)

- Very important for mapping netblocks.
- Provides "Live" host status in map results via "Host Discovery"

Options	
<input checked="" type="checkbox"/> Perform Live Host Sweep	TCP, UDP and ICMP Probes
<small>Note: Edit host discovery options on the Additional tab.</small>	
<input type="checkbox"/> Disable DNS traffic	<small>Note: Applies to maps on target domains with netblock(s).</small>



Mapping Configuration



Mapping Options

New Option Profile

Scan > Map > Additional

Map

Perform Basic Information Gathering on

All Hosts (selected)

Registered Hosts only

Netblock Hosts only

None

TCP Ports (maximum 20)

Standard Scan (13 ports) [View list](#)

Additional

Spec. 1-7, 8990

UDP Ports (maximum 10)

Standard Scan (8 ports) [View list](#)

Additional

Spec. 1-8, 6550

Options

Perform Live Host Sweep
Note: Edit host discovery options on the Additional tab.

Disable DNS traffic
Note: Applies to maps on target domains with netblock(s).

Performance

Configure performance options for mapping your network.

Overall Performance: Normal [Configure...](#)

Authentication

Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.

VMware



Mapping Benefits

Shows an overall view of your corporate assets

The screenshot shows a software interface for managing corporate assets. At the top, there's a menu bar with 'File', 'View', and 'Help'. Below it is a toolbar with various icons. A context menu is open over a list of assets, with the 'Add to Subscription' option highlighted. The main area displays a table of assets with columns for IP, DNS, NetBIOS, Router, and OS. The table lists several hosts, each with a checkmark in the first column and a dropdown arrow in the second.

	IP	DNS	NetBIOS	Router	OS
> <input checked="" type="checkbox"/>	64.39.105.242	demo1.qualys.com	XP-SP2	68.177.224.164	Windows XP Service Pack 2-3
> <input checked="" type="checkbox"/>	64.39.105.243	demo2.qualys.com	2K-SP4-OE501	68.177.224.180	Windows 2000 Service Pack 3-4
> <input checked="" type="checkbox"/>	64.39.105.244	demo3.qualys.com		68.177.224.164	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP
> <input checked="" type="checkbox"/>	64.39.105.245	demo4.qualys.com		68.177.224.180	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP
> <input checked="" type="checkbox"/>	64.39.105.246	demo5.qualys.com		68.177.224.164	Solaris 9-10
> <input checked="" type="checkbox"/>	64.39.105.247	demo6.qualys.com		68.177.224.180	Linux 2.6
> <input checked="" type="checkbox"/>	64.39.105.248	demo7.qualys.com	DEMO7	68.177.224.164	Windows 2000 Service Pack 3-4 / Windows 2003 / Windows XP
> <input checked="" type="checkbox"/>	64.39.105.249	demo8.qualys.com	DEMO8	68.177.224.180	Windows XP Service Pack 2-3

Mapping is the foundation for proper asset management



Map Results

Results

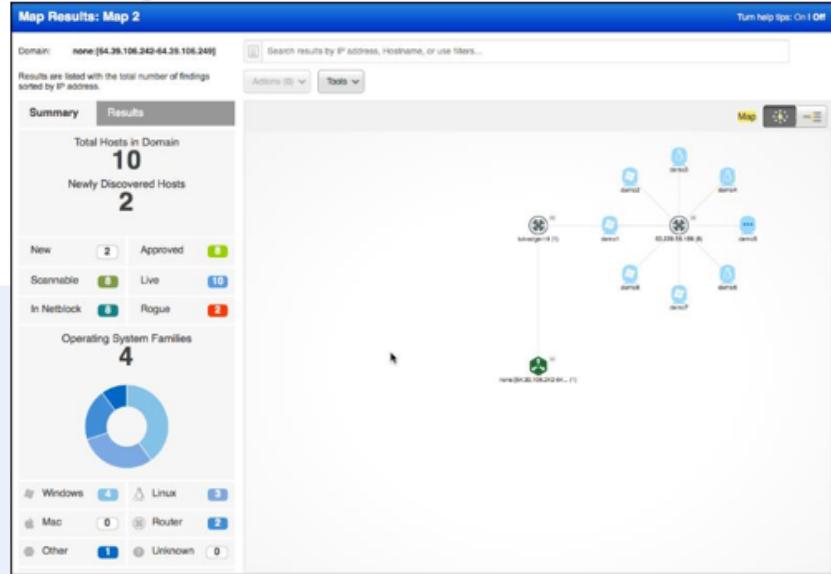
none (15)

	IP	DNS	NetBIOS	Router	OS	A S L N
▶	192.168.1.152	APPLE.lab.home				S N
▶	192.168.1.153	iStealPasswords.lab.home				S N
▶	192.168.1.154	Peregrine.lab.home				S L N
▶	192.168.1.156	centos6.lab.home			Ubuntu / Linux 2.6.x	S L N
▶	192.168.1.157	centos7.lab.home			Ubuntu / Linux 2.6.x / Linux 2.6	S L N
▶	192.168.1.159	ubuntuServer1404.lab.home			Ubuntu / Linux 3.x	S L N
▶	192.168.1.160	bodgeit.lab.home			Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Linux 2.6	S L N
▶	192.168.1.161	localhost.lab.home				S N
▶	192.168.1.163	T7600.lab.home	T7600		Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8	S L N
▶	192.168.1.169	Merlin.lab.home				S N
▶	192.168.1.175	HoneyPot.lab.home	HONEYBOT		Windows XP Service Pack 2-3	S L N
▶	192.168.1.195		WIN7ENTERPRISE		Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8	S L N
Services						
Discovery Method	Port					
ICMP	-					
TCP	135					
TCP	139					
TCP	445					
UDP	137					
TCP RST	-					
▶	192.168.1.197		WIN81ENTERPRISE		Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8	S L N
▶	192.168.1.198				Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8	S L N
▶	192.168.1.200		WS2012R2		Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8	S L N
▶	IP	DNS	NetBIOS	Router	OS	A S L N

A: Approved
 S: Scannable
 L: Live
 N: Netblock



Mapping: Graphic Mode



Qualys.

Mapping: Choosing A Target

1. **Domain** - Qualys service will identify domain members via DNS interrogation.
2. **Netblock** - Target a specific netblock range using the “none” domain.
3. **Domain + Netblock** – Use an IP address range to identify the upper and lower boundaries of a domain.
4. **Asset Group**
 - Associated Domains
 - Associated IPs (already in your subscription)

Target Domains

Select at least one asset group or domain to map.

Asset Groups [Select](#)

Assets from Asset Groups Domains
 IPs

Domains / Netblocks [Select](#)



Mapping Goals

1. Use map results and reports to discover and add new hosts to your subscription and identify dead and rogue hosts.
2. Ensure network and system admin teams participate in the Mapping and Reporting responsibilities.

	IP	DNS	NetBIOS	Router	OS	A S L N
▶	64.39.106.240	demo10.sea.qualys.com		68.177.224.180	Linux 2.6	L N
▶	64.39.106.241	demo11.sea.qualys.com		68.177.224.164	Linux 2.6	L N
▶	64.39.106.242	demo1.sea.qualys.com	XP-SP2	68.177.224.180	Windows XP Service Pack 2-3	S L N
▶	64.39.106.243	demo2.sea.qualys.com	2K-SP4-OE501	68.177.224.180	Windows 2000 Service Pack 3-4	S L N
▶	64.39.106.244	demo3.sea.qualys.com		68.177.224.180	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP	S L N
▶	64.39.106.245	demo4.sea.qualys.com		68.177.224.180	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP	S L N
▶	64.39.106.246	demo5.sea.qualys.com		68.177.224.180	Solaris 9-10	S L N
▶	64.39.106.247	demo6.sea.qualys.com		68.177.224.180	Linux 2.6	S L N
▶	64.39.106.248	demo7.sea.qualys.com	DEMO7	68.177.224.180	Windows 2000 Service Pack 3-4 / Windows 2003 / Windows XP	S L N
▶	64.39.106.249	demo8.sea.qualys.com	DEMO8	68.177.224.164	Windows XP Service Pack 2-3	S L N
	68.177.224.164			205.171.11.70		L
	68.177.224.180			205.171.11.70		L
	205.171.11.70	tuk-cnfr-11.inet.qwest.net				L
	IP	DNS	NetBIOS	Router	OS	A S L N



Unknown Devices Report

IP	DNS	NetBIOS	Router	OS	A. Status
64.41.200.231	demo01.sjc01.qualys.com	DEMO01		A	Active
64.41.200.232	demo02.sjc01.qualys.com	DEMO02		A	Active
64.41.200.233	demo03.sjc01.qualys.com			Active	
64.41.200.234	demo04.sjc01.qualys.com			Active	
64.41.200.235	demo05.sjc01.qualys.com			Active	
64.41.200.236	demo06.sjc01.qualys.com			A	Active
64.41.200.237	demo07.sjc01.qualys.com			Active	
64.41.200.238	demo08.sjc01.qualys.com			Active	
64.41.200.239	demo09.sjc01.qualys.com			Active	
64.41.200.240	demo10.sjc01.qualys.com			A	Active
64.41.200.241	demo11.sjc01.qualys.com			A	Active
64.41.200.242	demo12.sjc01.qualys.com			Added	
64.41.200.243	demo13.sjc01.qualys.com			Added	
64.41.200.244	demo14.sjc01.qualys.com			Added	
64.41.200.245	demo15.sjc01.qualys.com			Added	
64.41.200.246	demo16.sjc01.qualys.com	DEMO05		Added	

Identify your "authorized" hosts.

Look for the "Added" status to identify new hosts.

Compare the results of two separate Asset Maps to identify changes in host status.

Lab

Mapping





Qualys.

Thank You

training@qualys.com