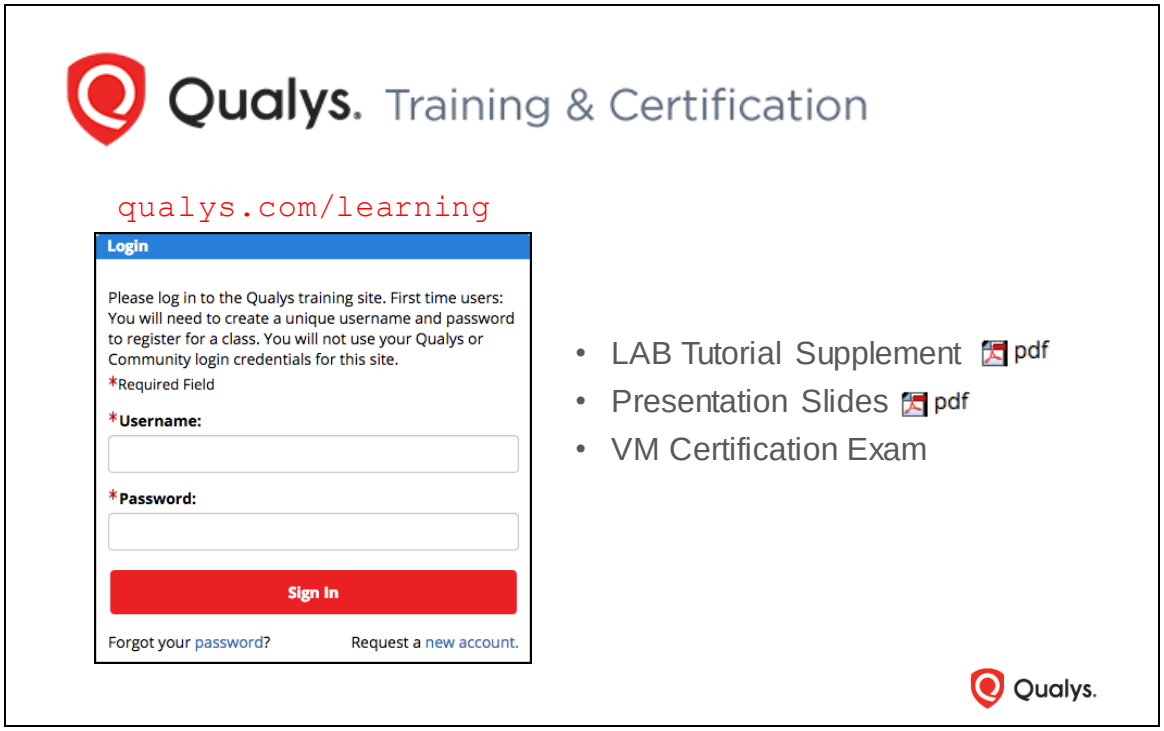
Vulnerability Management

Qualys.

Agenda

- VM Lifecycle & Sensors
- Account Setup
- Qualys KnowledgeBase and Search Lists
- Organize & Manage Assets
- Vulnerability Assessment
- Reporting
- User Management
- Remediation



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

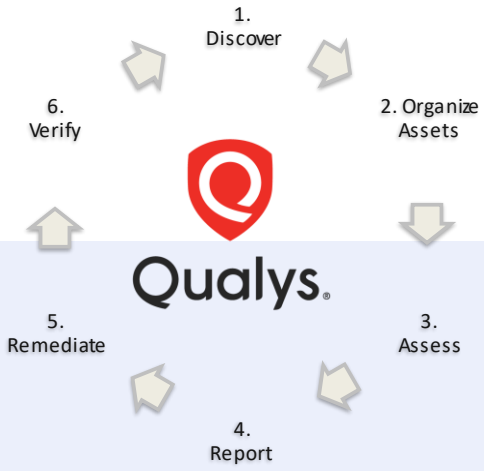
Here you will find the Vulnerability Management lab exercise document and presentation slides. You will need some type of pdf file reader, like adobe acrobat, to view these files.

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

VM Lifecycle & Sensors

Qualys.

Vulnerability Management Lifecycle



Qualys.

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.

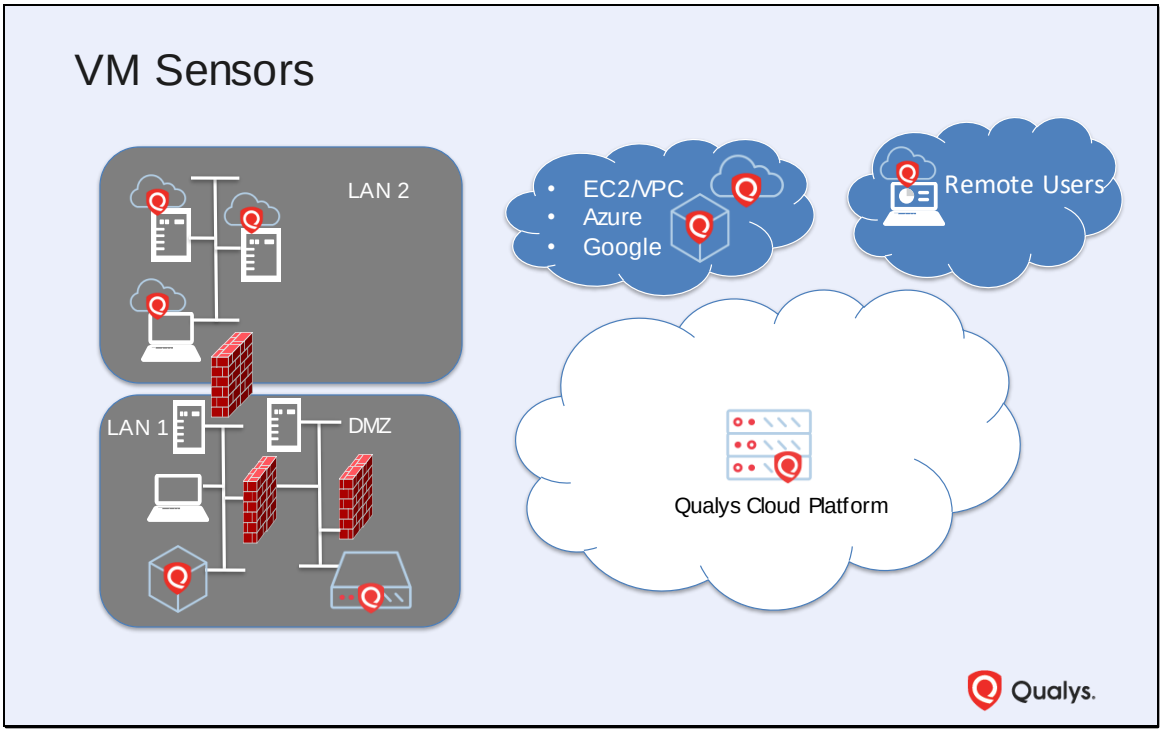
PHASE 3 - The primary objective of the assessment phase is finding vulnerabilities on the host assets in your VM subscription. The data needed to perform a vulnerability assessment can come from a combination of Qualys Sensors, Scanner Appliances, or Agents.

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 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.



To perform assessments that identify vulnerability findings, deploy Qualys Scanner Appliances, Qualys Cloud Agents, or both. It is very common for businesses and organizations to use both scanners and agents for this purpose.

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.

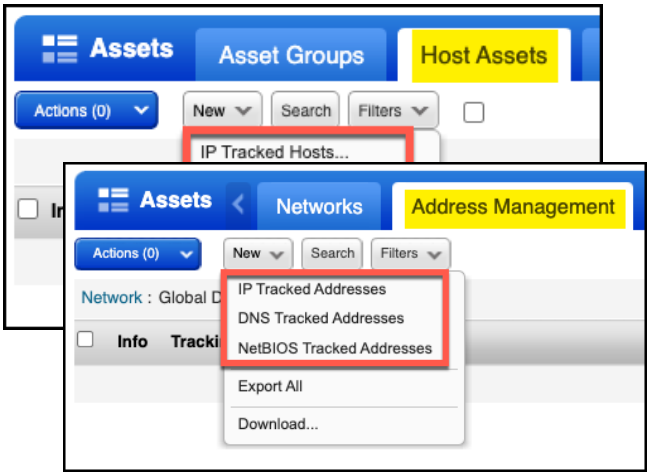
Internal scanner appliances are commonly used to scan host assets that reside on PRIVATE IP subnets like LAN 1 in this diagram. Deploying an internal scanner appliance as a member of this subnet, will allow you to scan subnet assets directly, without the obstacle of network filtering devices.

LAN 2 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 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.

Account Setup

Add Scannable Hosts



- Manager Users
  - Add assets to subscription
  - Remove assets from subscription
  - Delegate "Add assets" privilege to Unit Managers
- Tracking Method
  - IP Address (works best for static IPs)
  - DNS Name
  - NetBIOS Name

** Host Assets tab is replaced by the Address Management tab, when AGMS is enabled.*

Qualys.

Before you can scan and assess a host, 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.

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 the Qualys Host ID.

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

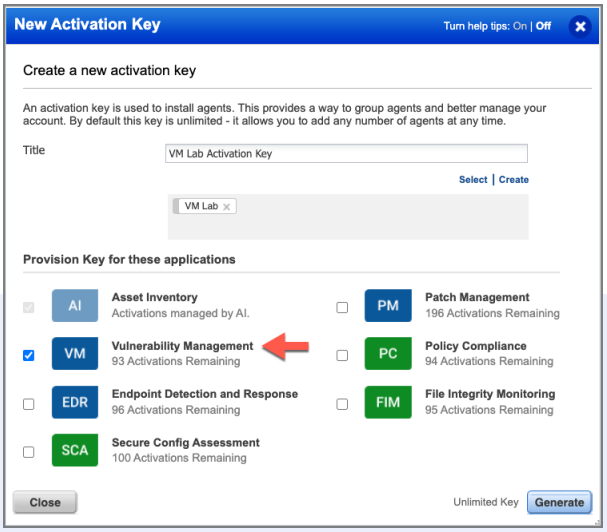
By default, IP address tracking is used to store (or index) the vulnerability findings for "scannable" host assets. IP address tracking is typically considered a poor choice, if host IPs are frequently changing (e.g., DHCP). It is best to use a tracking method that remains consistent for an extended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

Scans Setup options. Agentless Tracking requires scanning in “authenticated” mode.

Add Agent Hosts

- Install agent hosts with an Activation Key that has Vulnerability Management (VM) enabled.
- Alternatively, you can activate the VM module after Cloud Agent has been installed.



Qualys.

When installing agents on host assets, use an agent Activation Key that has the Policy Compliance module selected.

Alternatively, you can activate the PC module for agent hosts, using the Cloud Agent UI or API.

Lab Tutorial 1

Add Host Assets, pg. 4

Qualys.

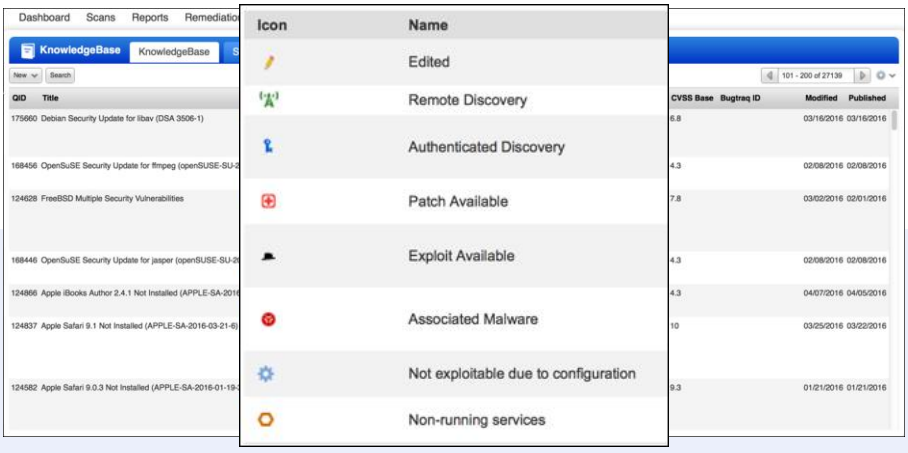
1. Activate account
2. Add host assets to your account
3. Launch and initial scan (untrusted)

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.

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

Qualys KnowledgeBase

VM KnowledgeBase

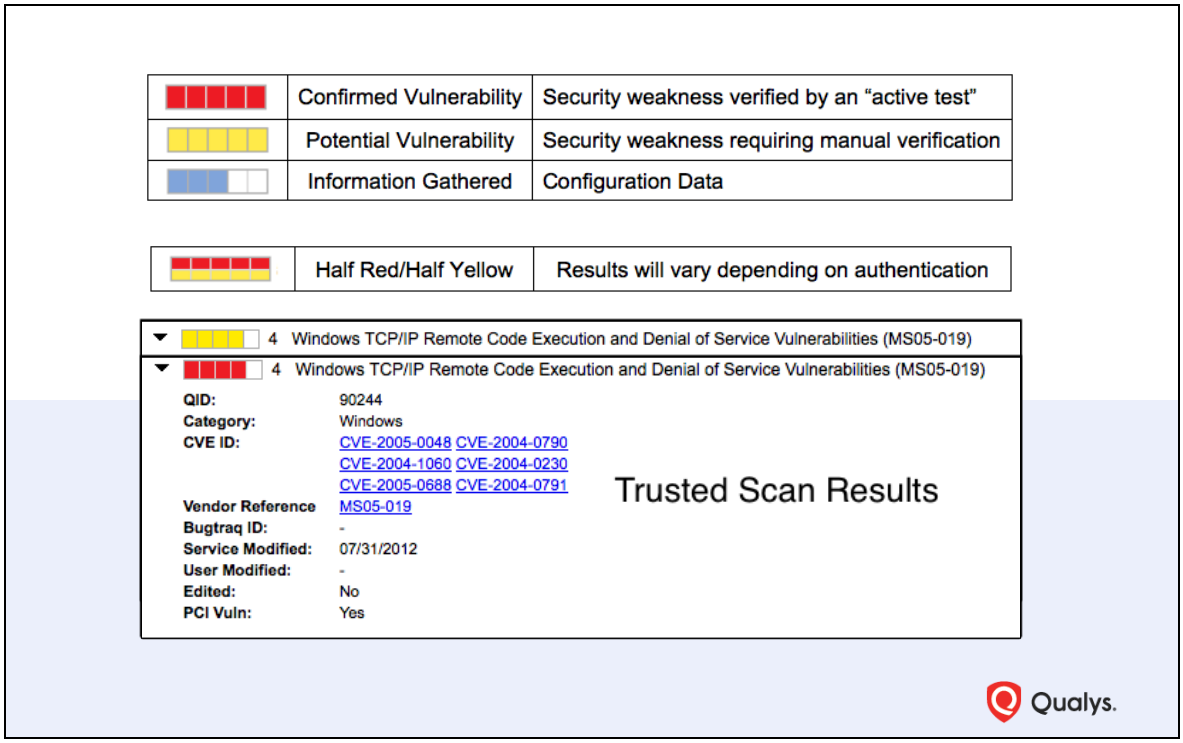


All QIDs are stored here

Qualys.

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 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

Qualys.

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.

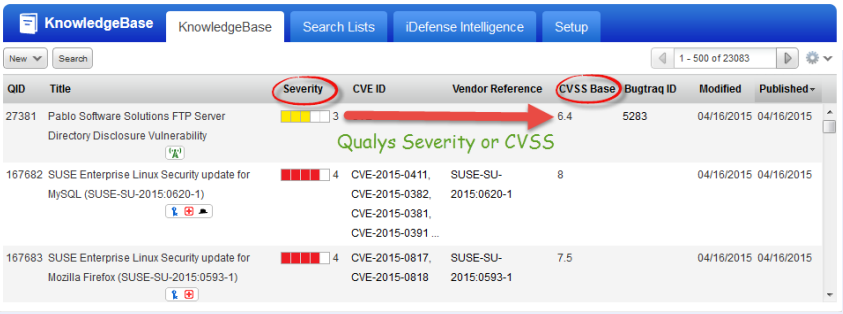
Severity level 3 and 4 vulnerabilities also involve some type of potential compromise of the host system or one of its applications or services.

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

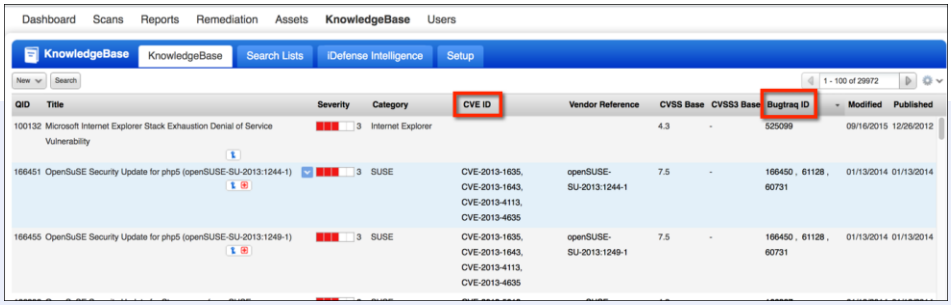


Qualys.

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)

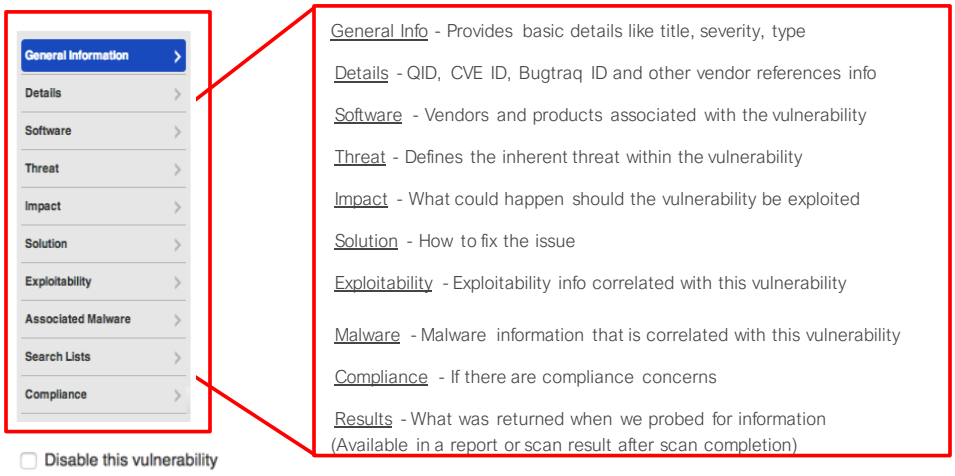


Although you'll find the most current and comprehensive vulnerability information within the Qualys knowledgebase, you'll find additional links for various QIDs that will connect you to:

- The Common Vulnerabilities and Exposers 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



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

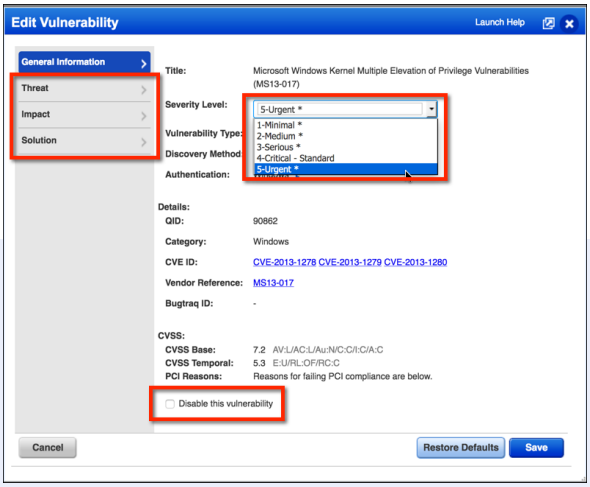
Qualys.

These are the components of a Qualys KnowledgeBase QID.

KnowledgeBase

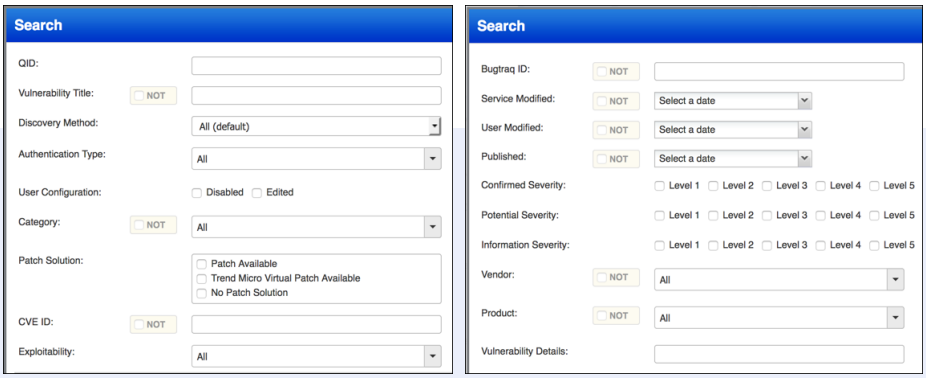
Editing Vulnerabilities

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



KnowledgeBase Search

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



Qualys.

With tens of thousands of QIDs in the Qualys knowlegebase, 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.

Lab Tutorial 2

Vulnerability KnowledgeBase, pg. 6

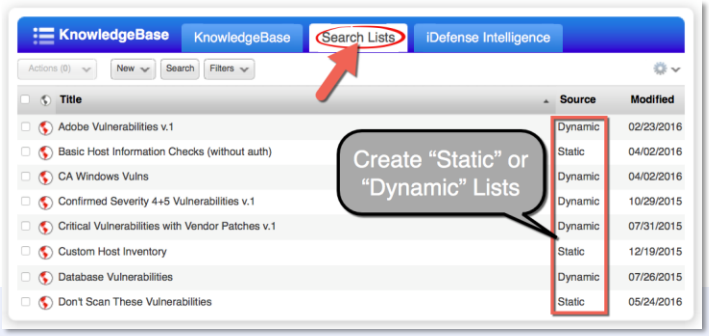
Qualys.

1. Customize KnowledgeBase rows
2. Import all Search Lists from library
3. Create dynamic Search List (low severity no patch)

KnowledgeBase Search List

Qualys.

Search List Overview



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.

Qualys.

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

Qualys.

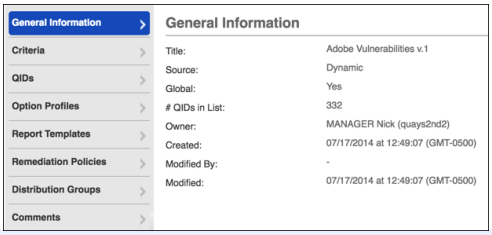
A search list is one of the most powerful filtering tools in the Qualys Vulnerability Management application for tasks such as scanning, reporting, and remediation. You can use search lists to create vulnerability reports that focus on specific groups of vulnerabilities that are high priority targets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

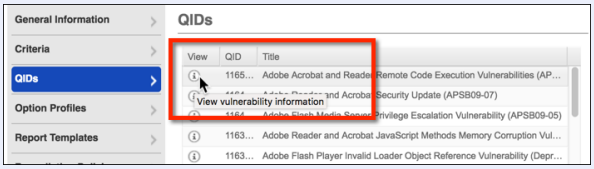
You may find the need to target a specific list of vulnerability QIDs, when scanning (especially on those occasions where you don't have time to wait for a complete scan to finish). Remember: Qualys normally recommends scanning for everything, and then using Report Templates containing targeted search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





Qualys.

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.

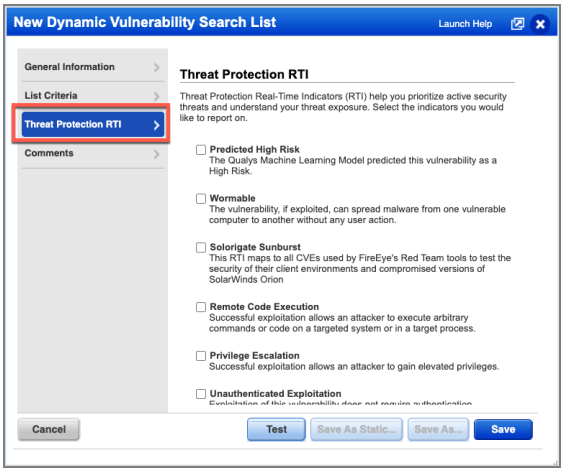
Lab Tutorial 3

KnowledgeBase Search List, pg. 8

Qualys.

1. Customize KnowledgeBase rows
2. Import all Search Lists from library
3. Create dynamic Search List (low severity no patch)

Using RTIs



- Risk = Threat x Vulnerability (Severity)
- *Severity = Impact if vulnerability is exploited.*
- Select one or more RTI options when creating a Search List.

Qualys.

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.

Search List

Use Cases

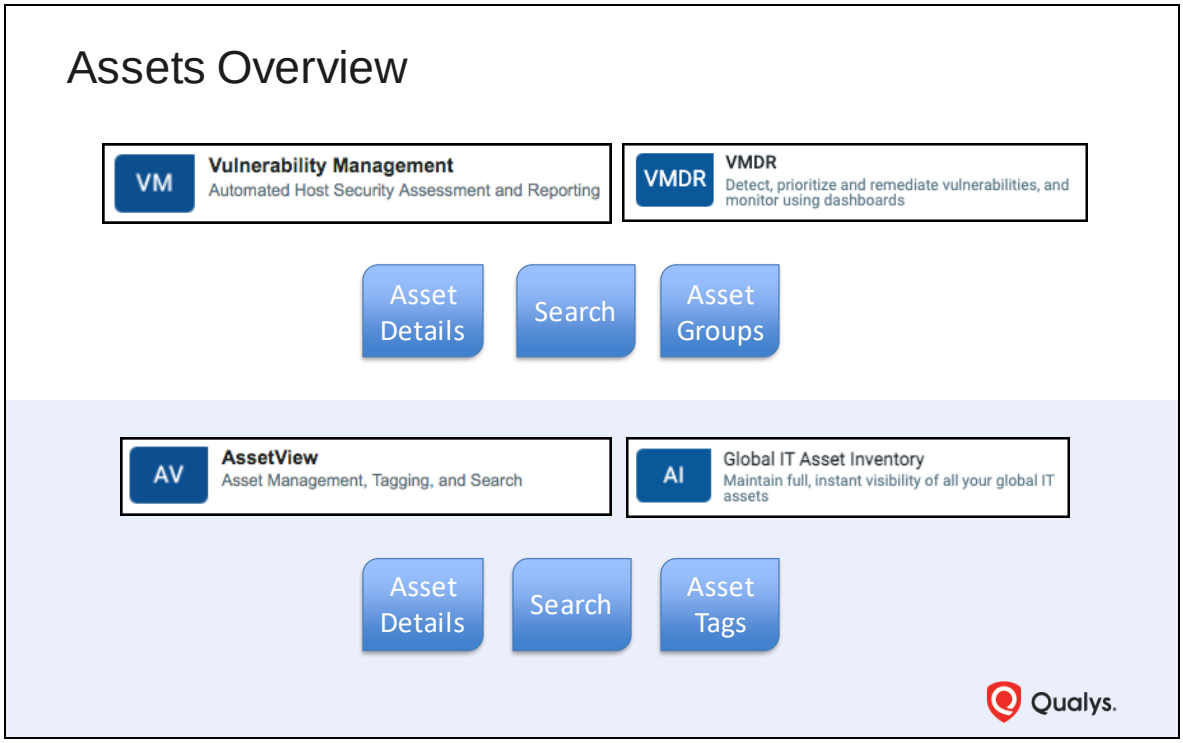
- Create reports for specific types of vulnerabilities:
  - Microsoft's Patch Tuesday vulnerabilities
  - PCI vulnerabilities
  - Only the vulnerabilities published in the last 30 days
- Scan for a specific type of vulnerability (when necessary):
  - Exchange Server, Solorigate Sunburst, etc...
  - High severity vulnerabilities with know exploits
- Create a Remediation Policy that assigns or ignores vulnerabilities (when they are detected).

Qualys.

FireEye Red Team Tools

SolarWinds Orion

Organize & Manage Assets



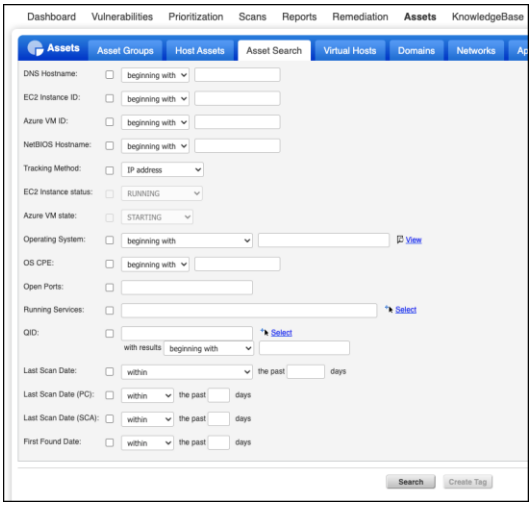
Qualys VM, VMDR, AssetView, AND Asset Inventory provide features and services for viewing host assets and asset details.

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

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

Search For Assets

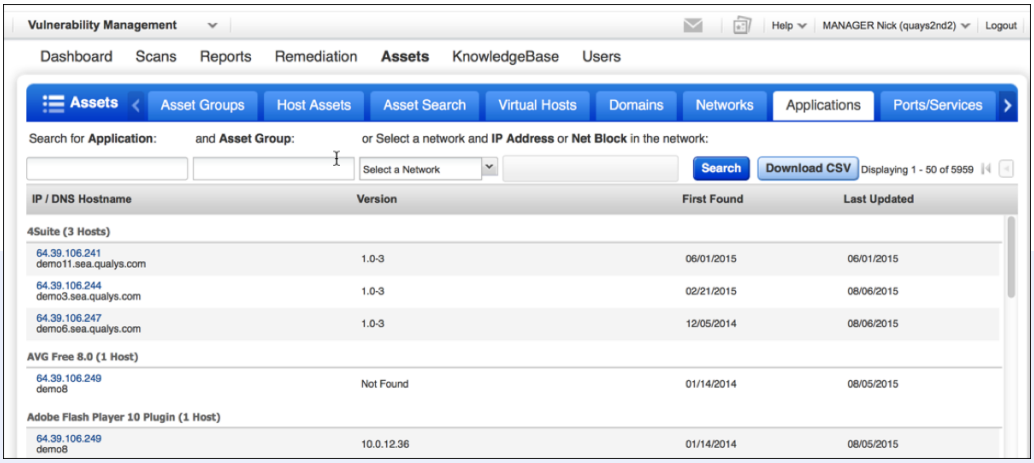
VM Asset Search



- The “Asset Search” tab provides multiple options and criteria for locating assets within your subscription.
- Search or create tags based on the criteria you select.

Qualys.

Applications Inventory



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

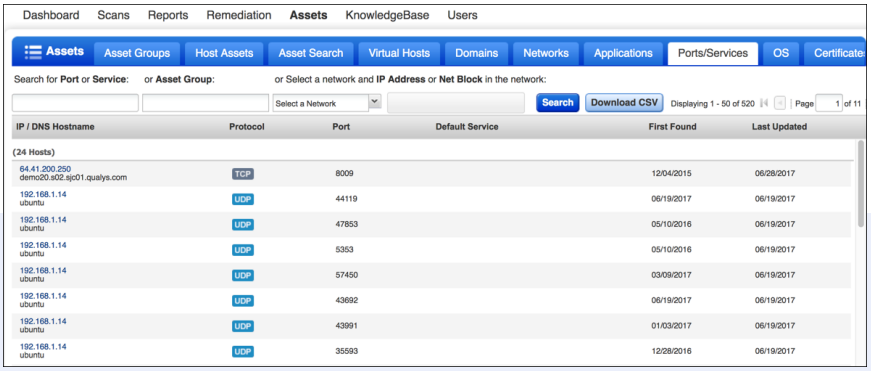
Here you'll find a comprehensive list of all the software applications discovered on the host assets in your subscription.

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.

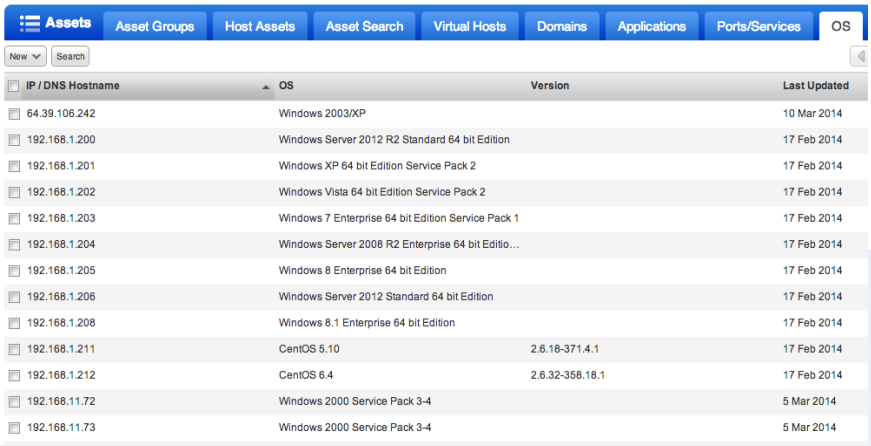
Ports and Services Inventory



Qualys.

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

Host Operating Systems Inventory

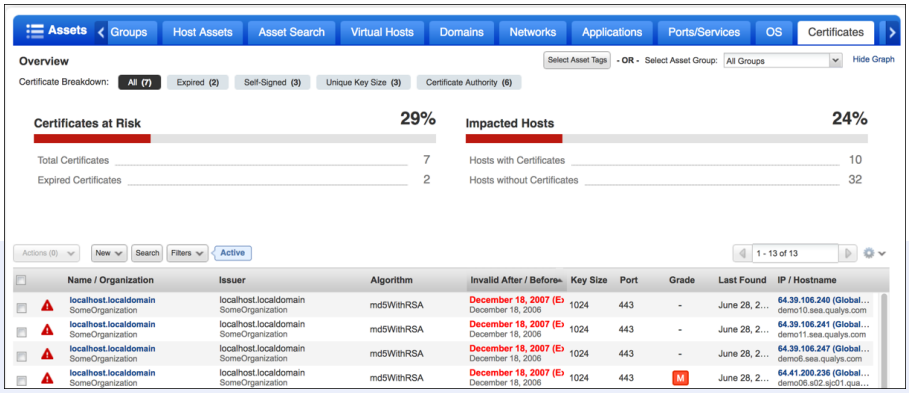


IP / DNS Hostname	OS	Version	Last Updated
64.39.106.242	Windows 2003/XP		10 Mar 2014
192.168.1.200	Windows Server 2012 R2 Standard 64 bit Edition		17 Feb 2014
192.168.1.201	Windows XP 64 bit Edition Service Pack 2		17 Feb 2014
192.168.1.202	Windows Vista 64 bit Edition Service Pack 2		17 Feb 2014
192.168.1.203	Windows 7 Enterprise 64 bit Edition Service Pack 1		17 Feb 2014
192.168.1.204	Windows Server 2008 R2 Enterprise 64 bit Editio…		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

Qualys.

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

Certificates Inventory



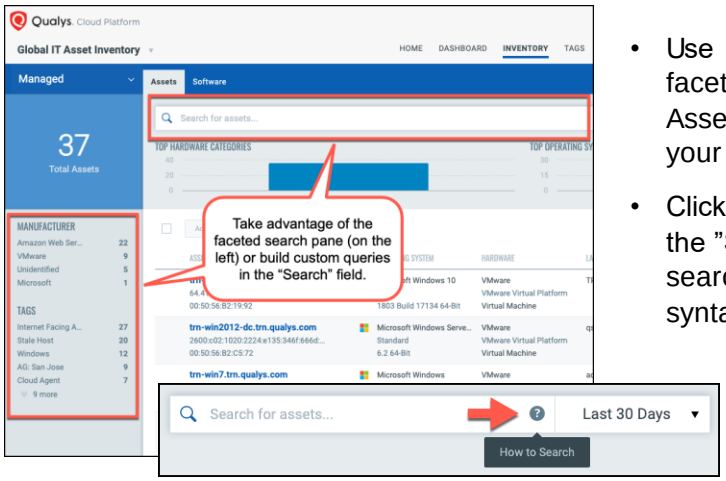
Certificate related information such as certificates by expiration date, by key size, by certificate authority, by port, and self-signed certificates as well as the certificates detail.

Qualys.

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.

Search Queries



- Use the "Search" field or faceted search pane in Asset Inventory to locate your assets and software.
- Click the "Help" icon within the "Search" field for search token options and syntax examples.

Qualys.

Lab Tutorial 4

Search for Assets, pg. 9

Qualys.

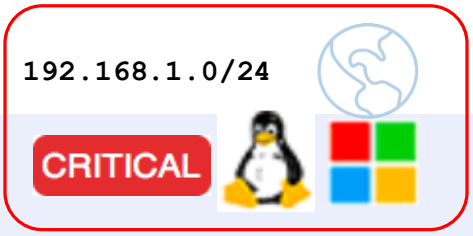
1. Customize KnowledgeBase rows
2. Import all Search Lists from library
3. Create dynamic Search List (low severity no patch)

Asset Groups

Qualys.

Asset Groups

- Asset groups allow you to manually group "scannable" assets in your account.
- Asset groups can contain a random collection of "scannable" assets or they can be designed around specific characteristics, such as:
  - Device type
  - System priority or criticality
  - Geographic or network boundaries
  - Asset ownership
  - and more ...



- Asset Groups cannot be nested.
- A matching Asset Tag is created for each Asset Group.

Qualys.

Asset groups provide one way to make logical groupings of the host assets in your Qualys account. You can add host members to an Asset Group randomly or based on some other criteria (like geographic location, subnet, or device type). Asset groups are created manually and a matching Asset Tag is automatically generated for every Asset Group you add to your account.

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 that meet the specific needs of your various user groups, without exceeding the access privileges required.

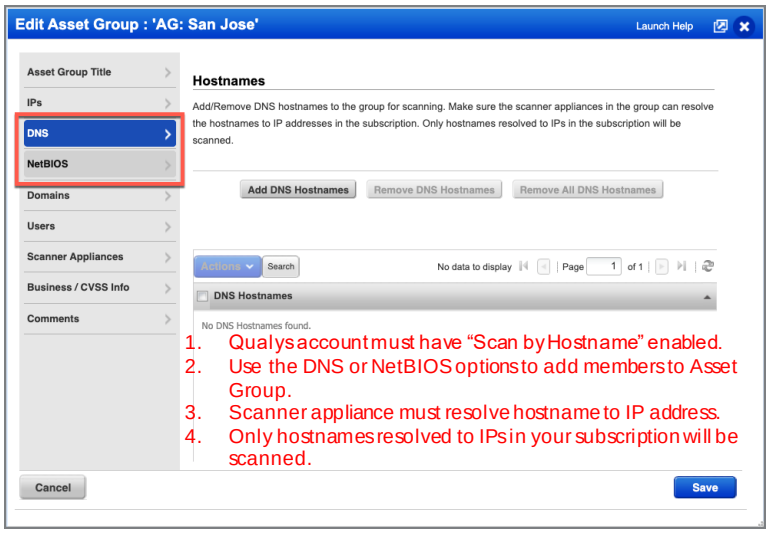
Lab Tutorial 4

Asset Groups, pg. 9

Qualys.

1. Customize KnowledgeBase rows
2. Import all Search Lists from library
3. Create dynamic Search List (low severity no patch)

Scan by Hostname



- **Add hosts by DNS or NetBIOS names.**
- **Use Asset Groups to "scan by hostname."**

42

Qualys.

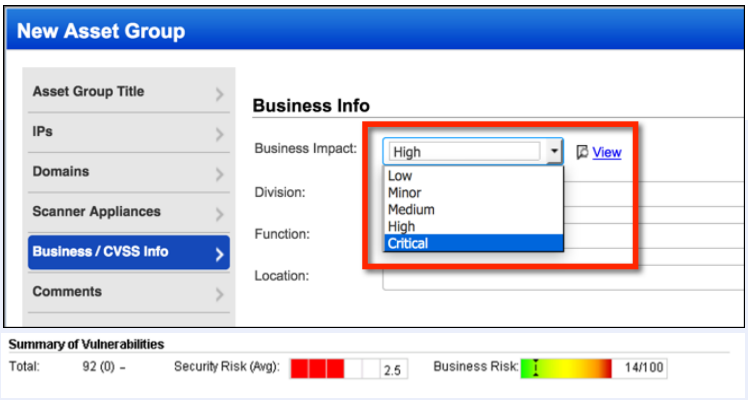
Although it is common to use IP addresses (or Asset Groups that contain IP addresses) as scanning targets, with the "Scan by Hostname" feature enabled for your account, you can identify the targets of your scans using DNS names or NetBIOS names.

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 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.



Qualys.

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.

Asset Tags

Qualys.

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.

Qualys.

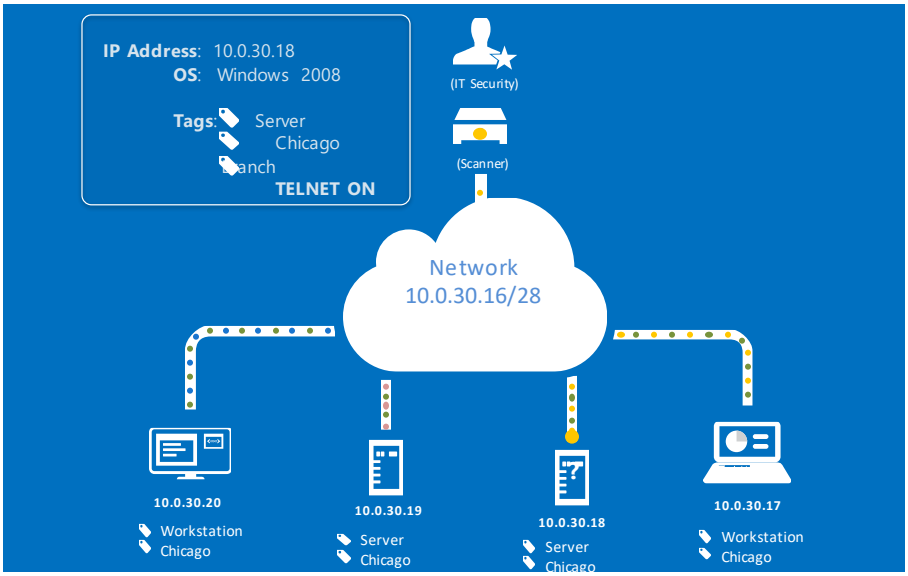
Basic Asset Tag behaviors and characteristics:

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



Qualys.

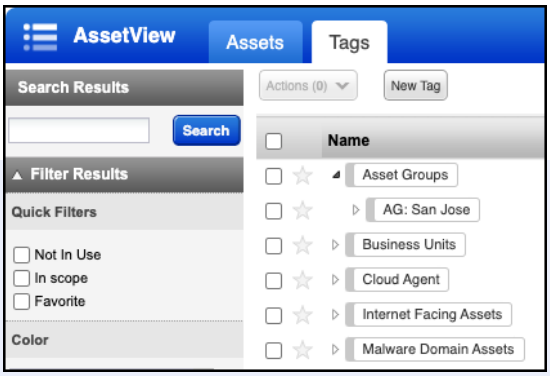
USE CASES

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
- Business Units
- Cloud Agent
- Internet Facing Assets
- Malware Domain Assets



Qualys.

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.

Lab Tutorial 5

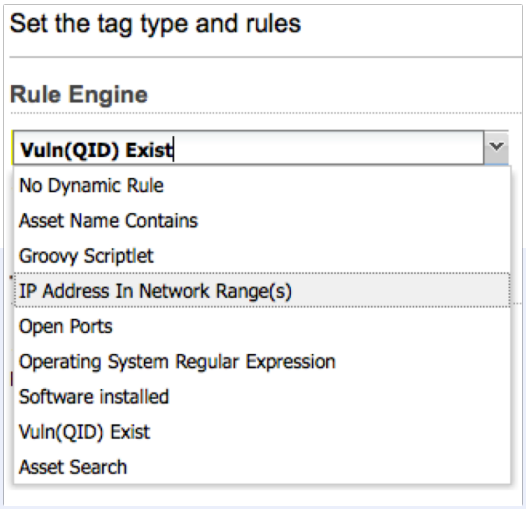
OS Asset Tag Hierarchy, pg. 11

Qualys.

1. Customize KnowledgeBase rows
2. Import all Search Lists from library
3. Create dynamic Search List (low severity no patch)

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.



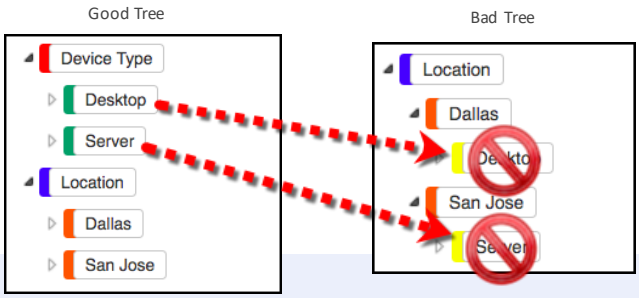
Qualys.

Each dynamic rule engine focuses on a different asset charcteristic:

- 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

Qualys.

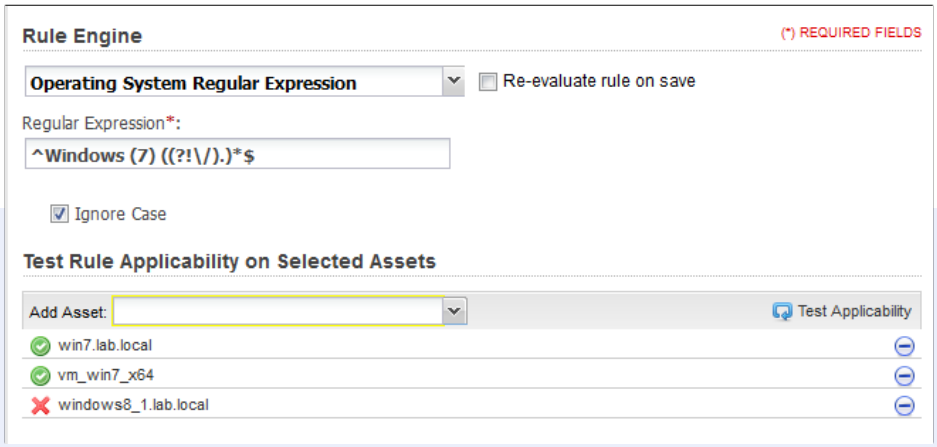
Do your best to choose tag names that are descriptive, but brief.

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.

Testing Asset Tags



Qualys.

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. Help to automate scanning and reporting tasks.

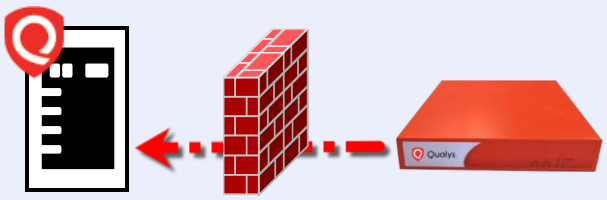
Qualys automatically creates asset tags to match each asset group.

Vulnerability Assessment

Qualys.

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 agents has SYSTEM level privileges to its host.
  - Collected data is sent back to Qualys Cloud Platform at regular intervals.



Qualys.

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 organization 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.

Qualys.

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}

Qualys.

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.

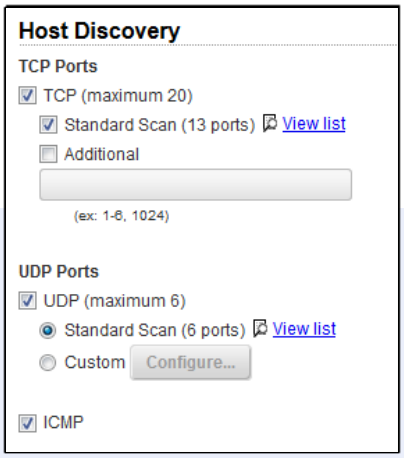
Once the TCP and UDP port scanning modules have completed their respective tasks. The list of open TCP and UDP ports is passed on to the Service detection module.

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)



Qualys.

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.

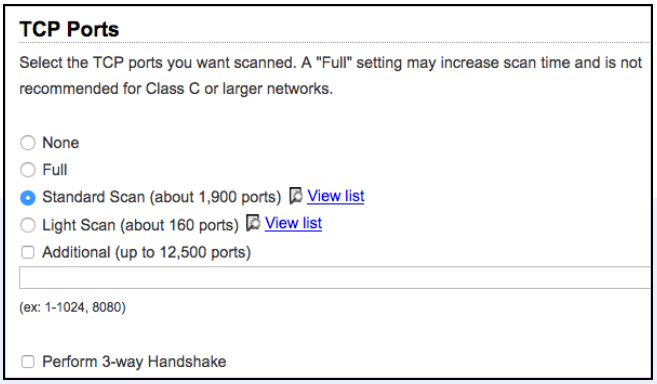
Here you can choose and customize the different probes that are used to detect host status, including TCP, UDP, or ICMP probes.

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



Qualys.

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.

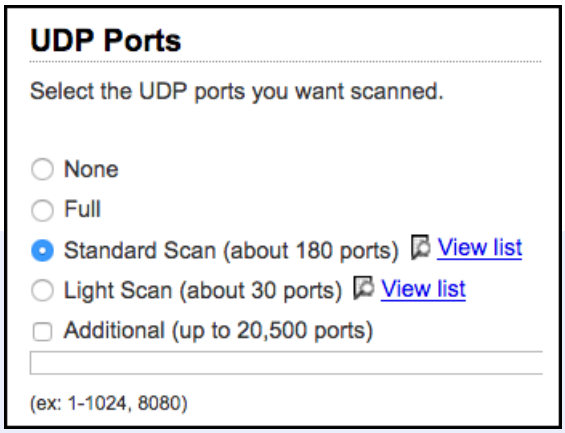
Use the "Additional" check box for any additional port numbers you may need.

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 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).
- UDP Service Detection is performed during UDP port scanning.



Qualys.

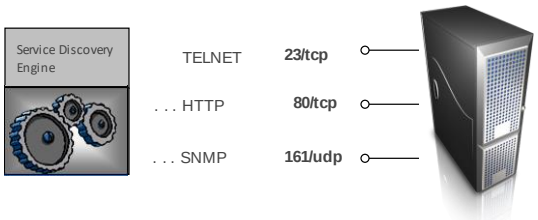
Once the host discovery module has completed its task, a list of your LIVE targets is passed to the port scanning module. it's the job of the UDP port scanning module to determine which UDP ports are open (depending of course on the number of ports that you are actually targeting in your scan).

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).
- Qualys will continue to test open ports until the correct service is identified.
- Some services may be configured to use non-standard port numbers (contrary to IANA guidelines).
- Some services may be configured with non-standard banners.

Qualys.

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. Howerver, 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.

Qualys.

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.

Qualys.

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

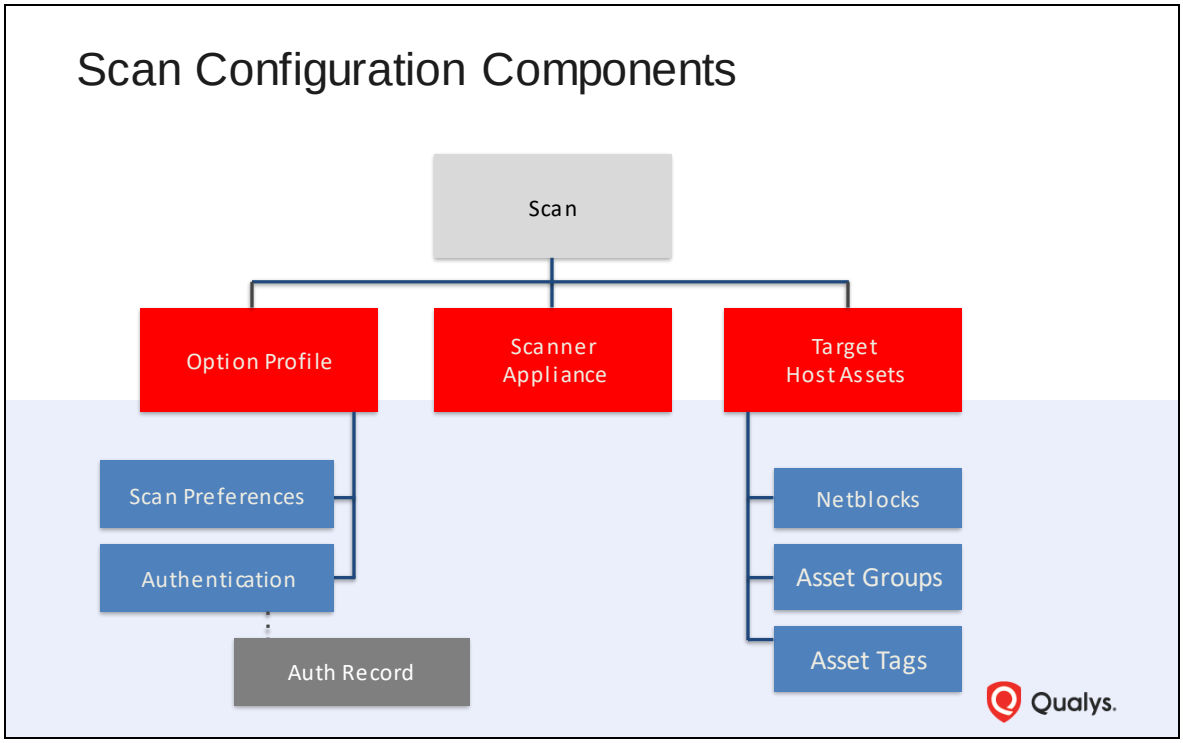
Vulnerability Assessment
- Based on 1) Operating System, 2) Active Services, and 3) Installed Software

Qualys.

Here is a review of the entire process.

Scan Configuration

Qualys.



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 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
- 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.

Qualys.

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.

Lab Tutorial 7

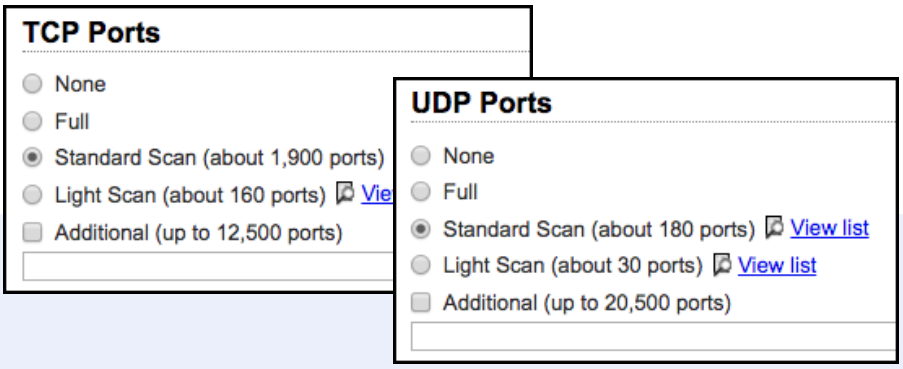
Scanning Option Profile, pg. 16

Qualys.

Create Window and Unix auth. records.
Create Option Profile: standard scan, complete vuln. testing with authentication

Option Profile

Targeted TCP and UDP Ports



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

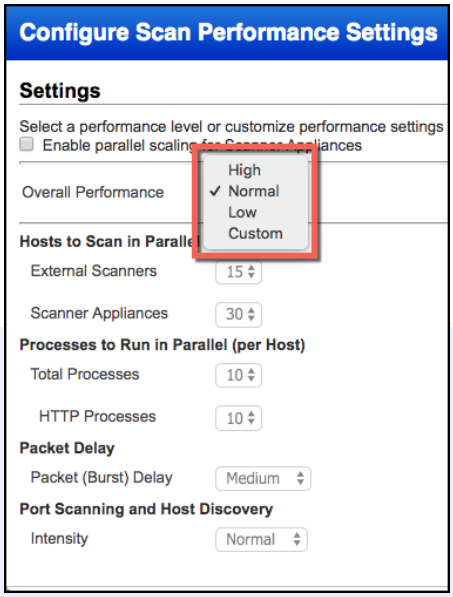
Qualys.

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



Qualys.

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

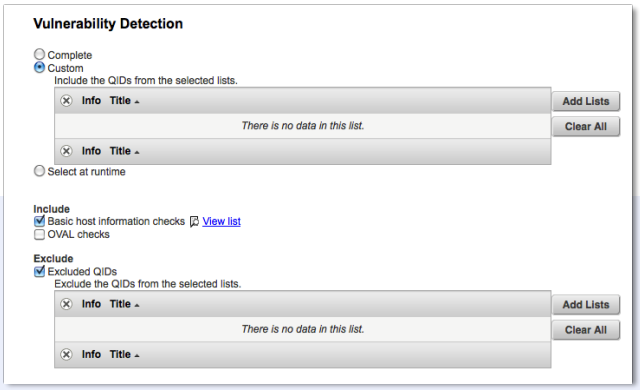
The “Low” option reduces scan performance and should be used for bandwidth restricted networks or heavy traffic environments.

“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



- When possible, avoid "Custom" scans in favor of "Complete" scans.
- Custom scans require a QID Search List.

Qualys.

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.

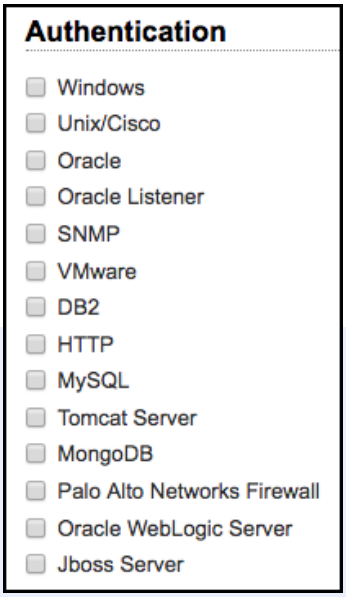
However, when configuring Vulnerability Detection, Qualys recommends using the Complete option.

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

Authentication

- Allows scanner appliances to login to host to extract more meaningful data.
- Discover vulnerabilities not detected by untrusted scan.
- Confirm Potential Vulnerabilities.
- Application-based records are used by Qualys Policy Compliance.



Qualys.

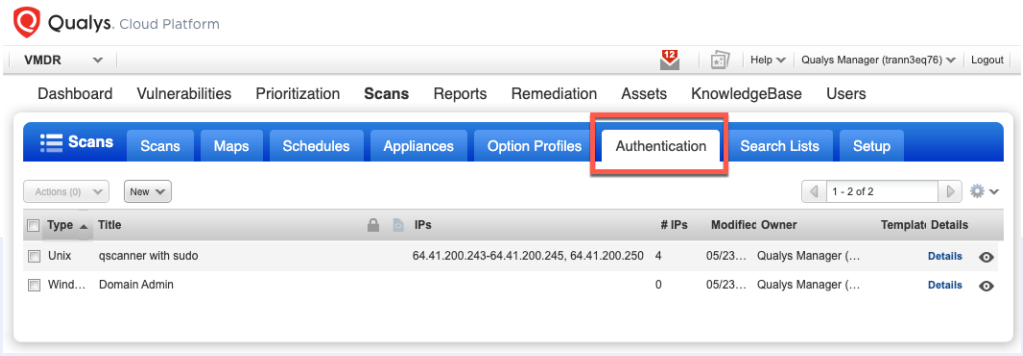
It's considered a "best practice" to perform your assessment scans in "authenticated" mode.

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

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

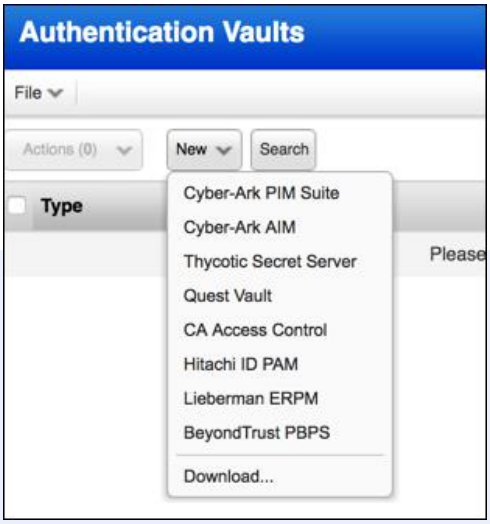
Remember, you'll need to create an appropriate authentication record (under the Authentication tab) for each authentication option you select here in the Option Profile.

Authentication Records



Qualys.

Authentication Vaults

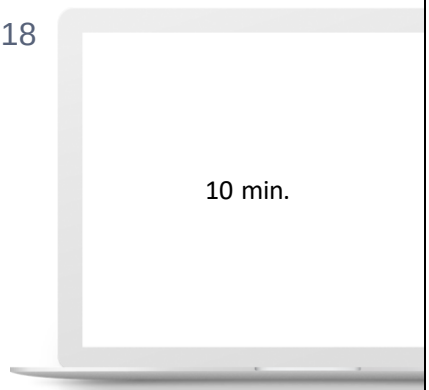


- In large organizations where thousands of machines are scanned regularly for vulnerabilities, managing passwords is a challenge.
- Some organizations are reluctant to let their credentials leave the network

Qualys.

Lab Tutorial 8

Windows & Linux Authentication Records, pg. 18

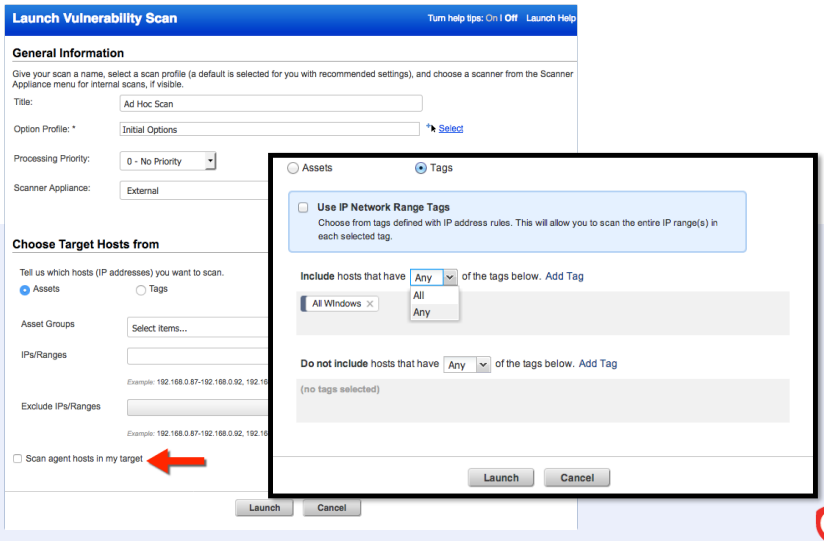


Qualys.

Create Window and Unix auth. records.
Create Option Profile: standard scan, complete vuln. testing with authentication

Launch Vulnerability Scan

Scan Settings



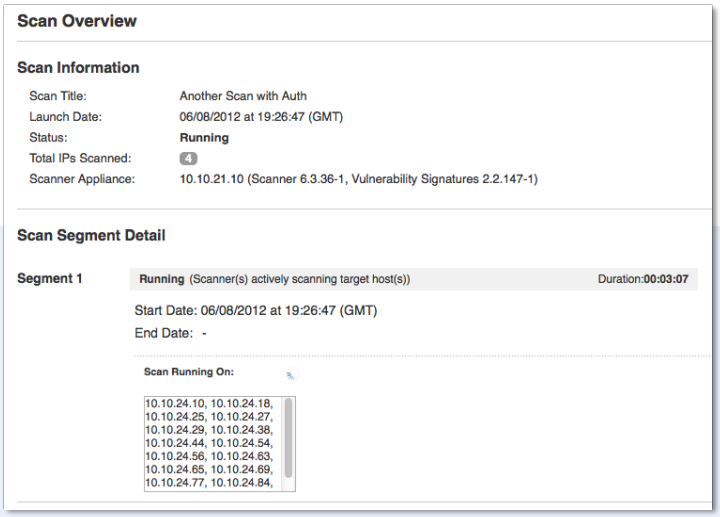
Qualys.

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

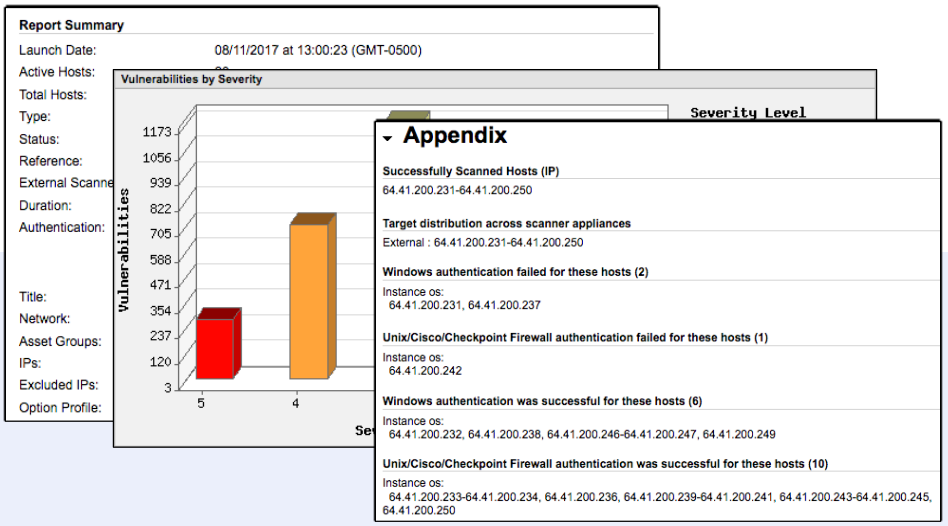
"On Demand"



Qualys.

You can monitor scans as they run.

Scan Results Summary

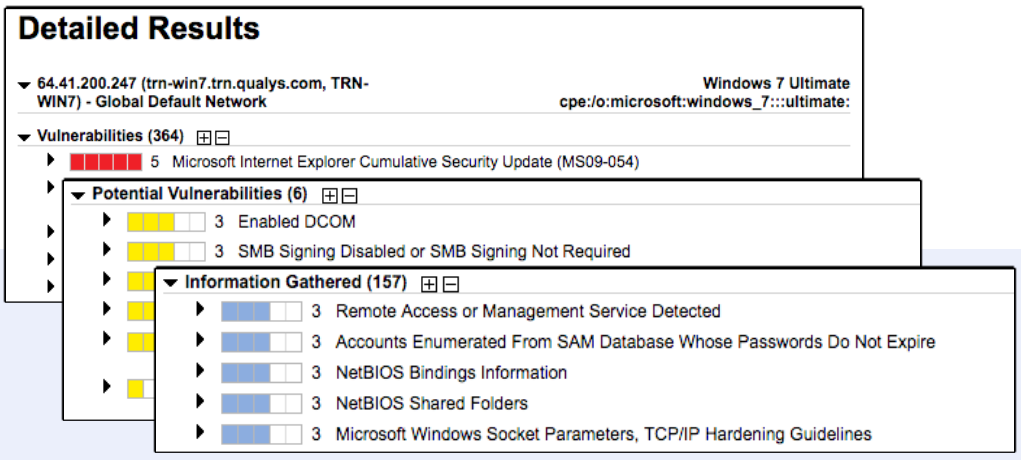


The "summary" section at the top of the report includes information like:

- 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



Unfiltered, raw data of your scan targets

Qualys.

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.

Lab Tutorial 9

Launch Scan & View Results, pg. 22

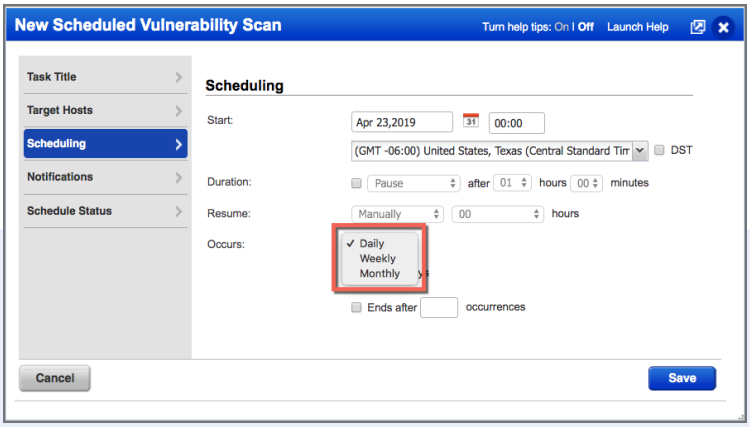
Qualys.

Create Window and Unix auth. records.
Create Option Profile: standard scan, complete vuln. testing with authentication

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.



Qualys.

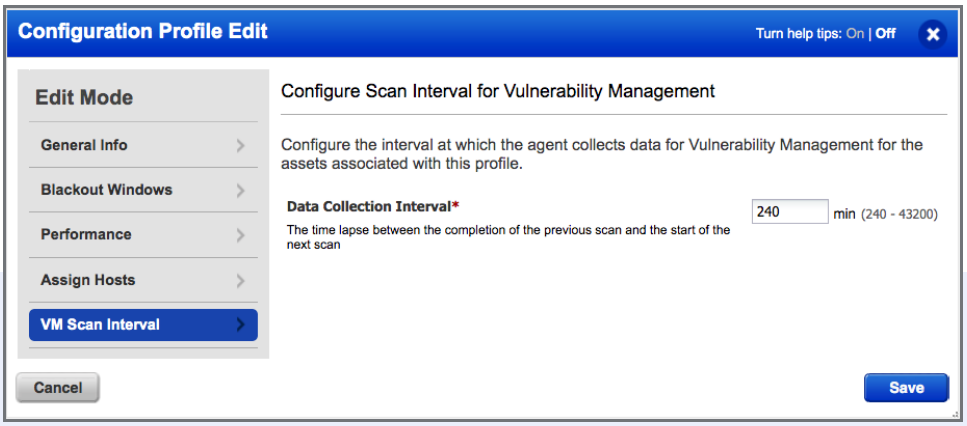
What obviously makes a scheduled scan different are the Scheduling options. Begin by selecting the date and time for this scheduled scan to start. The start time for each scheduled scan will reflect the time zone you specify.

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



- Qualys Cloud Agent is configured to collect vulnerability assessment data at regular intervals (240 – 43200 min.).

Qualys.

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.

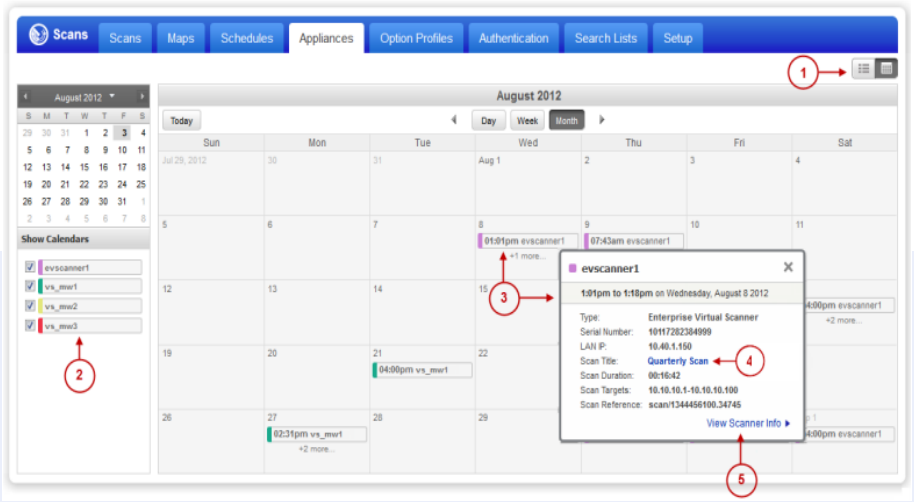
Lab Tutorial 10

Scheduled Scans, pg. 26

Qualys.

Create Window and Unix auth. records.
Create Option Profile: standard scan, complete vuln. testing with authentication

Qualys Scan Calendar



Qualys.

New Scan Calendar

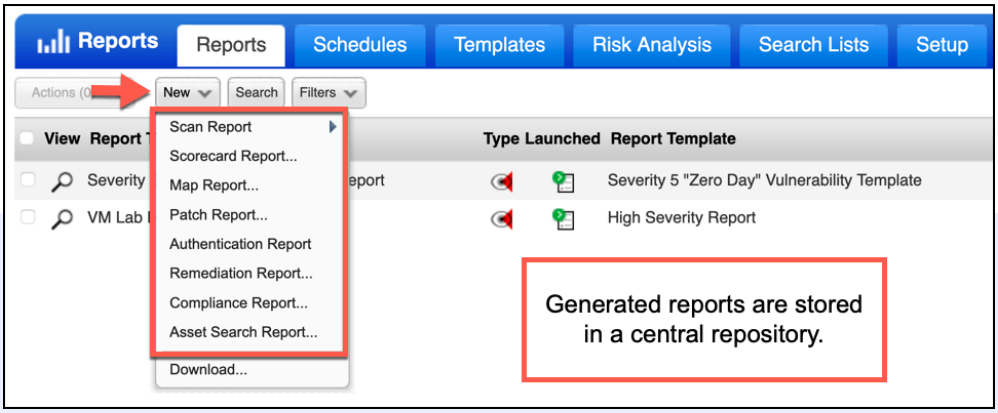
Your Scan calendar provides immediate insight into your scans and maps, giving you the most recent security information on your IT assets, so you can take actions as needed. A user with any role (except Auditor) can view this calendar. For a Unit Manager, Scanner or Reader, the user has permission to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

Reporting

Qualys.

Report Types



Qualys.

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.

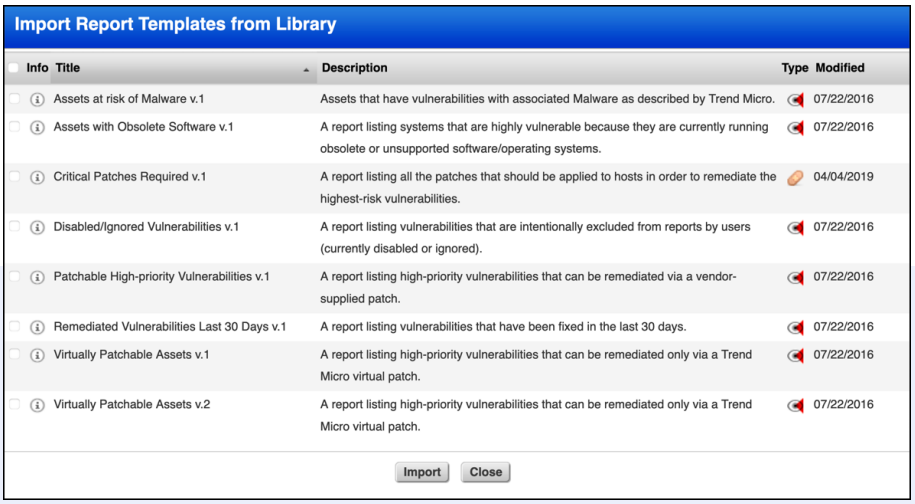
On the other end of the spectrum, scorecard reports present a high-level view of your scan results with summary statistics and graphic illustrations of useful metrics.

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 asses their performance. These reports can be especially useful for quickly locating overdue patches and preventing potential process bottle necks.

Report Template Library



Qualys.

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.

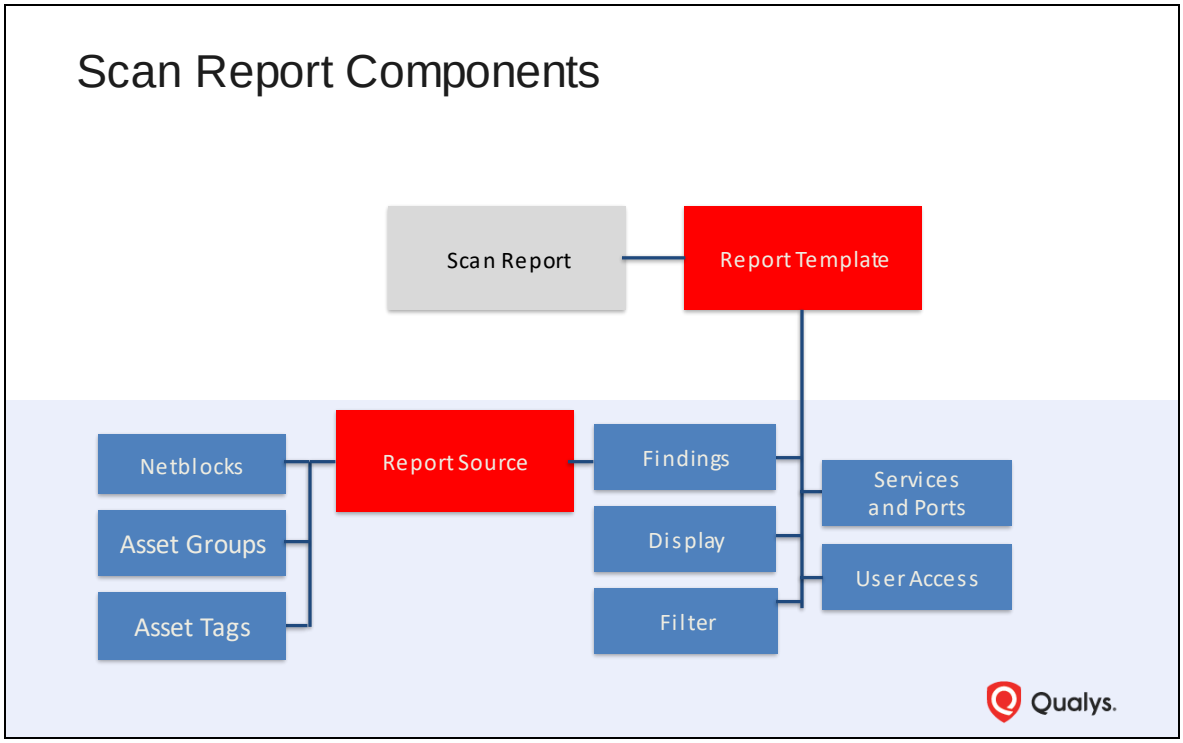
The Technical report template; on the other hand, is more suitable for members of your operational teams, because it focuses on the information and details needed to patch and mitigate detected vulnerabilities.

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.

Lab Tutorial 11

High Severity Report, pg. 27

Qualys.



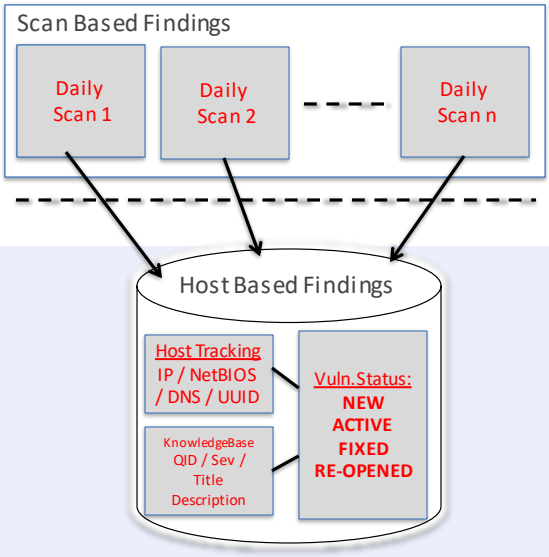
This diagram illustrates the basic components needed to build a report (scorecard reports, authentication reports and asset search reports, do not require a report template).

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 thier associated reports.

Scan-Based vs. Host-Based Findings



What are Host Based Findings?

- Comprised of all completed scans.
- Vulnerability findings are indexed by each host's tracking method.
- Provides vulnerability history for each host, including vulnerability status: New, Active, Fixed and Reopened.
- Required for "trend" reports.

Qualys.

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.

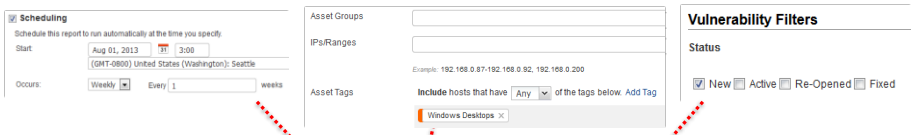
Lab Tutorial 12

Custom Report Template, pg. 28

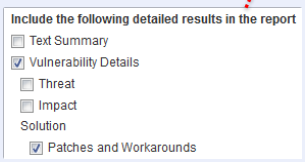
Qualys.

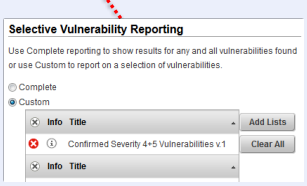
Create Window and Unix auth. records.
Create Option Profile: standard scan, complete vuln. testing with authentication

Reporting Use Case



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

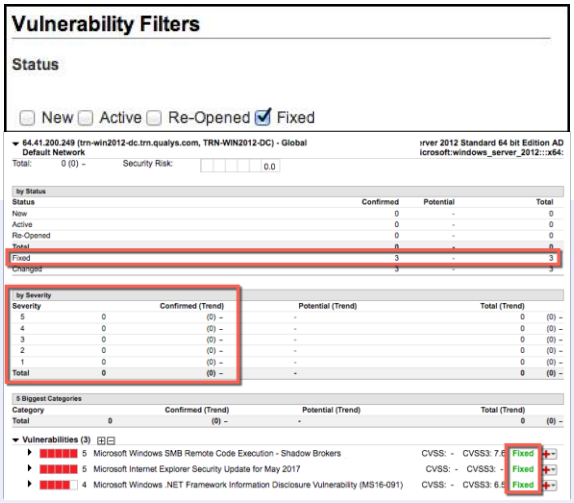




Qualys.

Reporting Use Case

Scan Report Template



What information can you show to reflect progress?

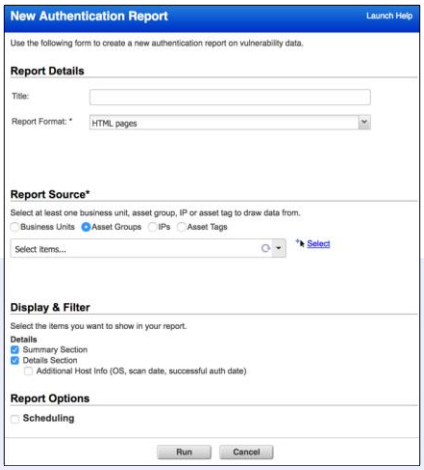
- *Fixed Vulnerabilities*
- *Trending (Include on the vulnerabilities you are trying to address. Ex. 4's and 5's)*

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



Authentication Reports can also be scheduled.

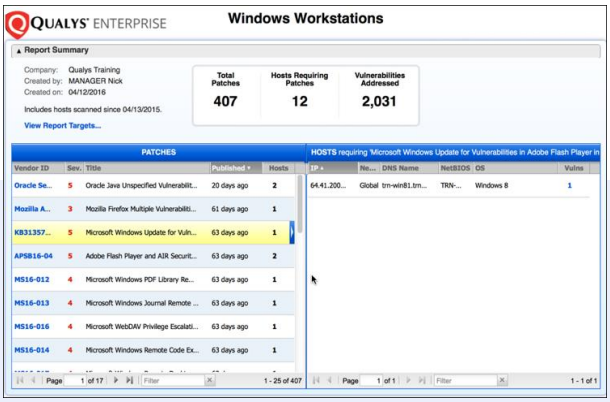
Qualys.

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.

Qualys Patch Report

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



Online Format - Provides more interactivity (sorting, filtering)

Qualys.

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.

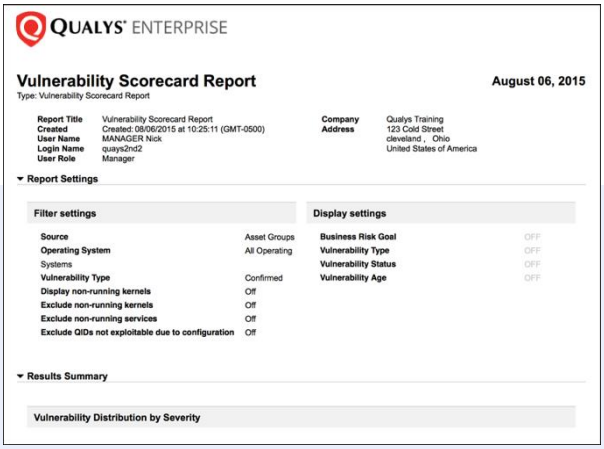
Patch reports make it easier to see the number of host assets impacted by a single patch.

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


QUALYS® ENTERPRISE

Vulnerability Scorecard Report August 06, 2015

Type: Vulnerability Scorecard Report

Report Title	Vulnerability Scorecard Report	**Company**	Qualys Training
Created	Created: 08/06/2015 at 10:25:11 (GMT-0500)	**Address**	123 Cold Street
User Name	MANAGER Nick		cleveland , Ohio
Login Name	quays2nd2		United States of America
User Role	Manager		

▾ **Report Settings**

Filter settings

Source	Asset Groups
Operating System	All Operating Systems
Vulnerability Type	Confirmed
Display non-running kernels	Off
Exclude non-running kernels	Off
Exclude non-running services	Off
Exclude QIDs not exploitable due to configuration	Off

Display settings

Business Risk Goal	OFF
Vulnerability Type	OFF
Vulnerability Status	OFF
Vulnerability Age	OFF

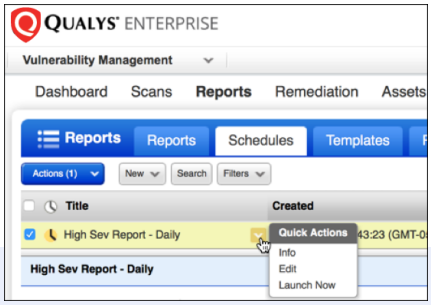
▾ **Results Summary**

Vulnerability Distribution by Severity

Qualys.

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

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

Qualys.

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.

Lab Tutorial 13

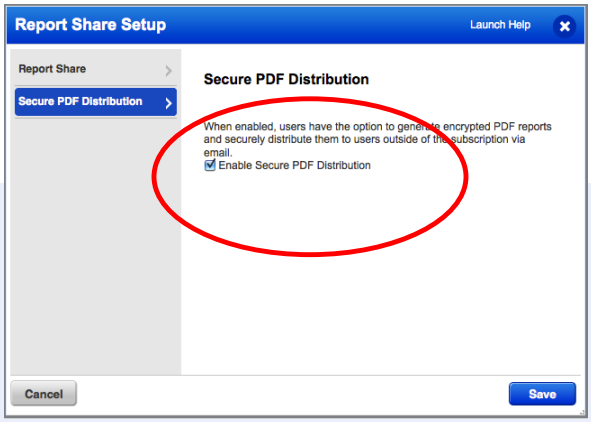
Scheduled Reports, pg. 30

Qualys.

Create Window and Unix auth. records.
Create Option Profile: standard scan, complete vuln. testing with authentication

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 Best Practices

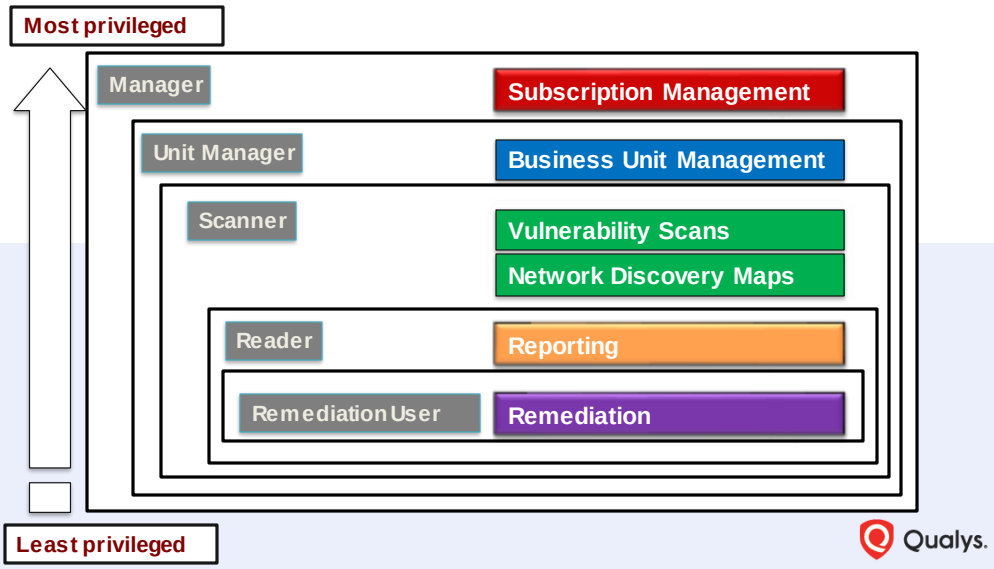
1. Determine what reports need to be run. What are your goals?
2. Assign reports to users within Qualys or share them via secure distribution.
3. Schedule reports to run after scans complete.

User Management

Qualys.

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.

Qualys.

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

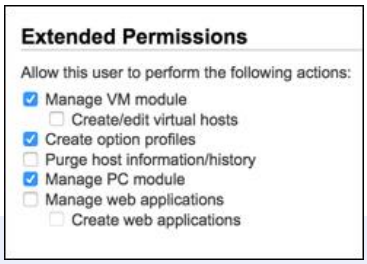
A contact user can be configured to receive email notification from the Qualys Cloud Platform. Contact users do not have login credentials.

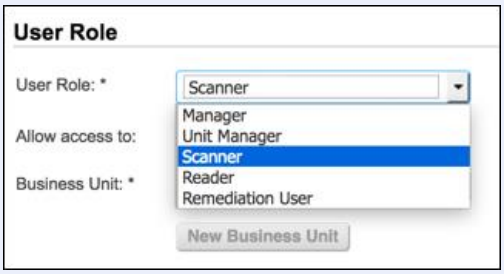
Similar to the Unit Manager, the User Administrator was designed to help manage other user accounts in your subscription (while avoiding the risk of creating to many Manger accounts). This role only has access to users, asset groups, business units, and distribution groups.

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.





Qualys.

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

Lab Tutorial 14

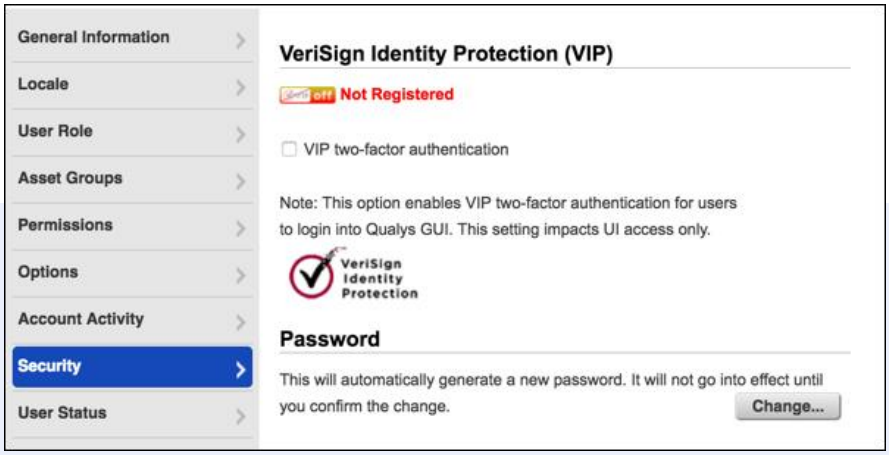
Create User Account, pg. 32

Qualys.

1. Activate account
2. Add host assets to your account
3. Launch and initial scan (untrusted)

User Management

VIP and Password Resets

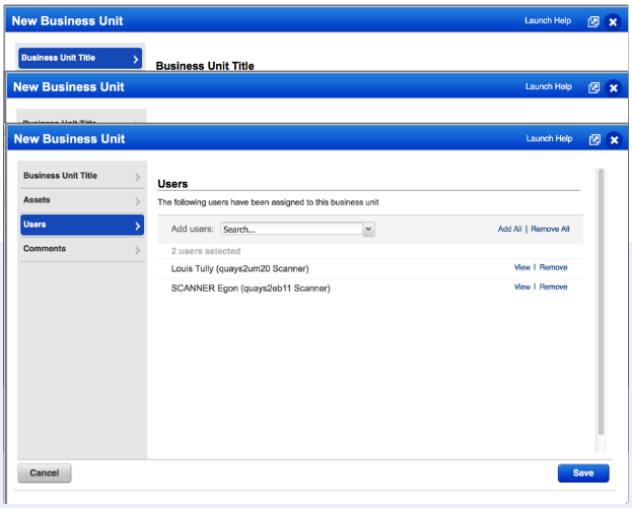


Qualys.

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)



Qualys.

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

Business Unit Manager

Privileges:

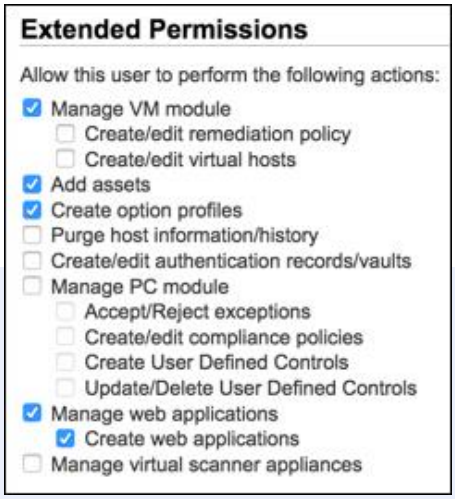
- Perform all vulnerability management functions:
  - Map, Scan
  - Remediation
  - Reporting
- Manage assets, add users, and publish template reports within their Business Unit

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

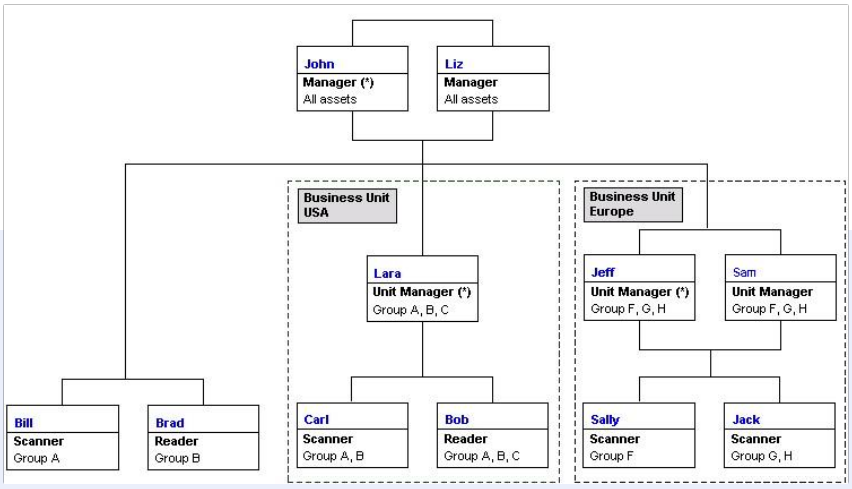


Qualys.

The role of Business Unit manager comes with special extented 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



Qualys.

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 user account security settings
(Users > Setup > Security):

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

Qualys.

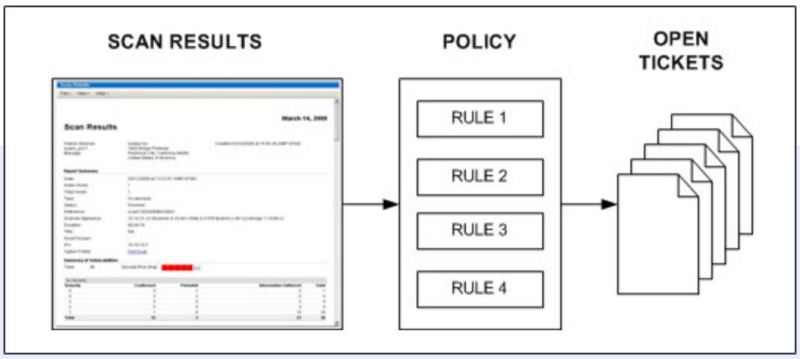
- Only Manager users can edit the default security options for your Qualys account. The Security setup changes you make here, will affect all user accounts in your subscription.
- You can restrict access to your to your account subscription by client IP address or IP address range. Be very carful with 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

Qualys.

Remediation Workflow

- Remediation Policies (rules) automatically create tickets, when vulnerability scans are performed.



Qualys.

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 Basics

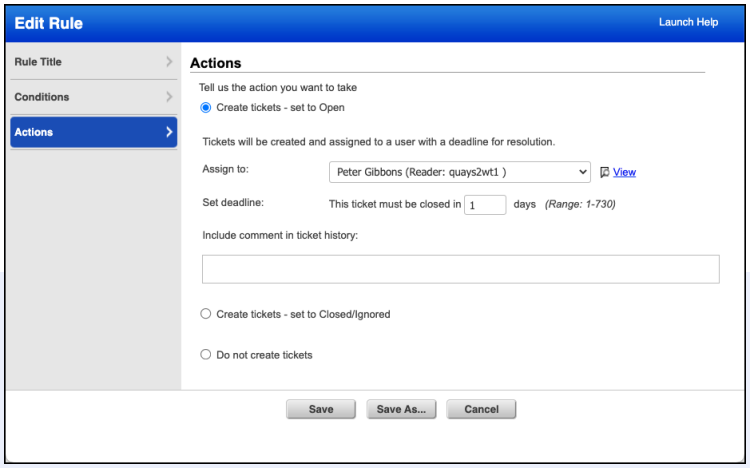
- Remediation Policy can be used to assign a vulnerability to a specific user account (for mitigation).
- Remediation Policy can be used to ignore specific lists of vulnerabilities.
- Qualys automatically updates “Fixed” vulnerabilities (when no longer detected).
- Resolved Date indicates when a vulnerability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

Qualys.

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.

Assign Vulnerabilities to User



Assignment

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

Set Deadline for remediation

Qualys.

Remediation policies contain two basic components:

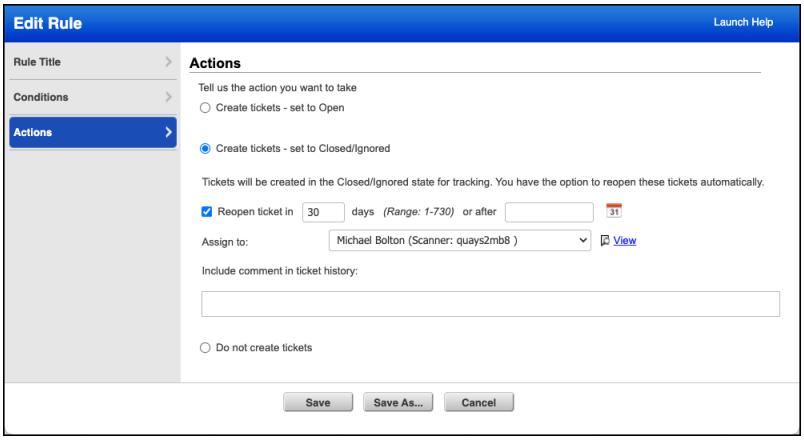
1. Conditions (that identify the targets of the policy)
2. and Actions (that identify the task to be performed, if the target conditions are met).

Lab Tutorial 15

Assign Vulnerabilities, pg. 35

Qualys.

Ignore Vulnerabilities



Lab Tutorial 16

Ignore Vulnerabilities, pg. 36

Qualys.

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

Qualys.

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

Lab Tutorial 17

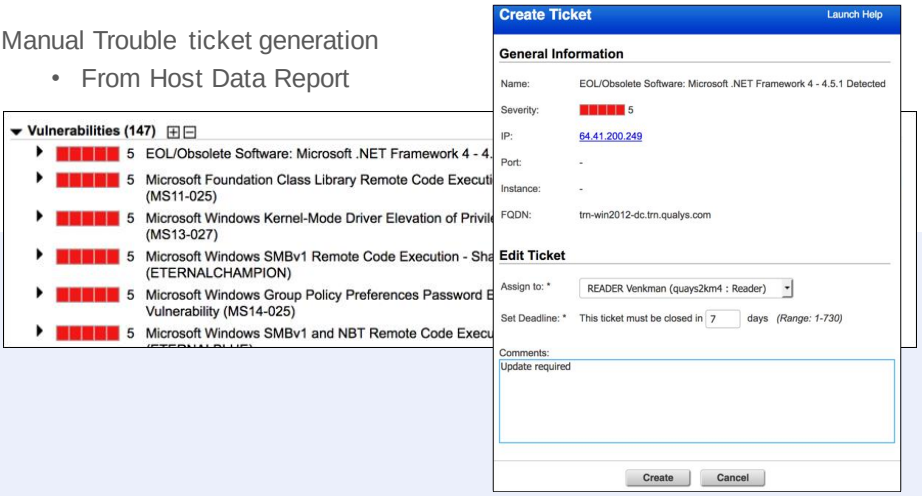
Remediation Report, pg. 38

Qualys.

Manual Ticket Creation

Manual Trouble ticket generation

- From Host Data Report



Qualys.

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

Remediation Objectives

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.
- Ignore vulnerabilities to keep them out of reports.

Qualys.

Exam

Qualys.

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.

Qualys.

Useful Resources

- 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

Qualys.

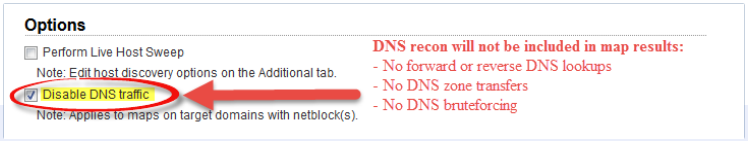
Mapping

Qualys.

Mapping Options

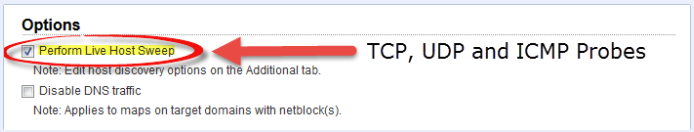
DNS Reconnaisiance

- 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)



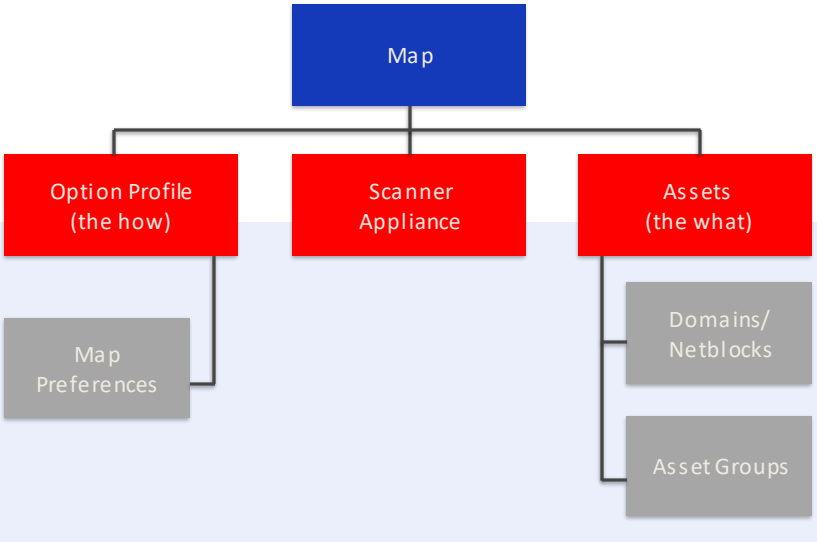
Host Sweep (via ICMP, TCP and UDP probes)

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



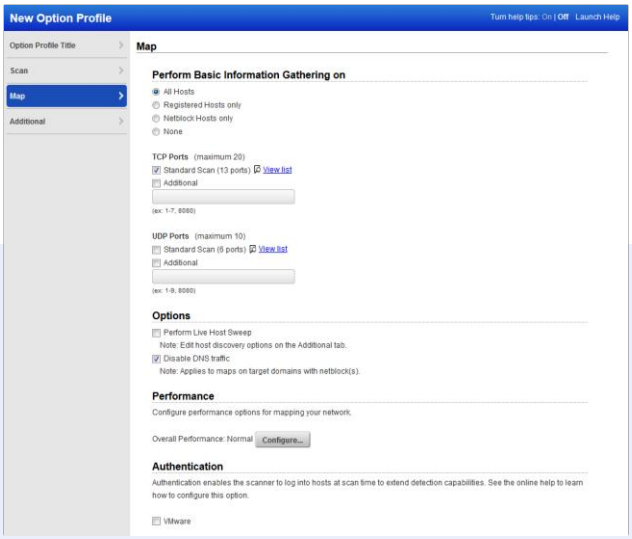
Qualys.

Mapping Configuration



Qualys.

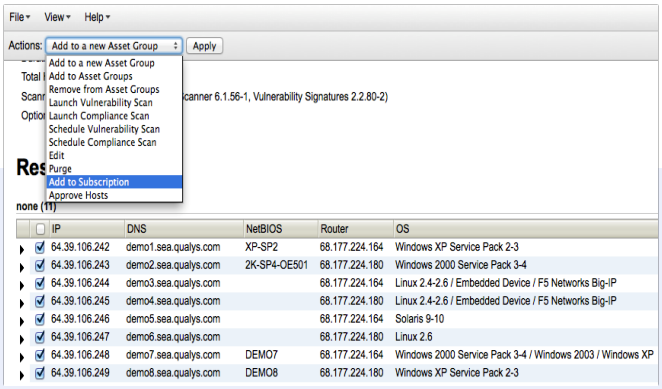
Mapping Options



Qualys.

Mapping Benefits

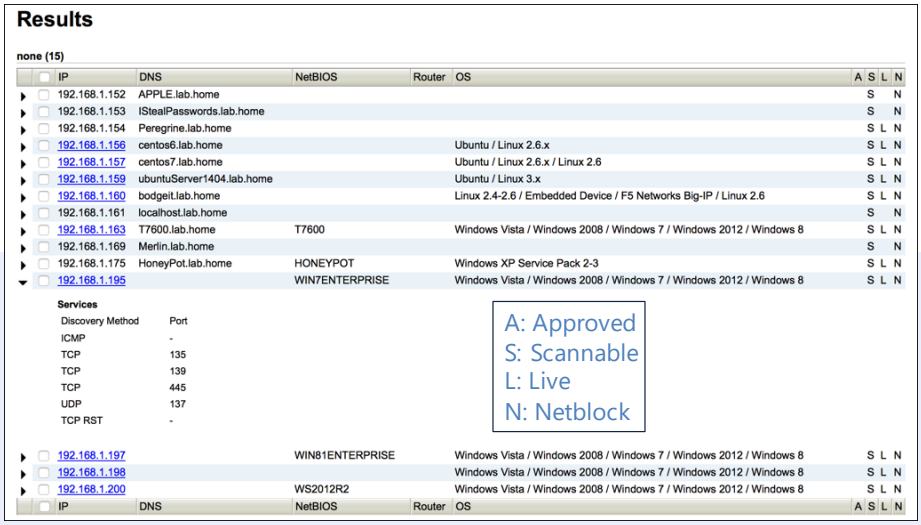
Shows an overall view of your corporate assets



Mapping is the foundation for proper asset management

Qualys.

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	ISteaIPasswords.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	HONEYPOT		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

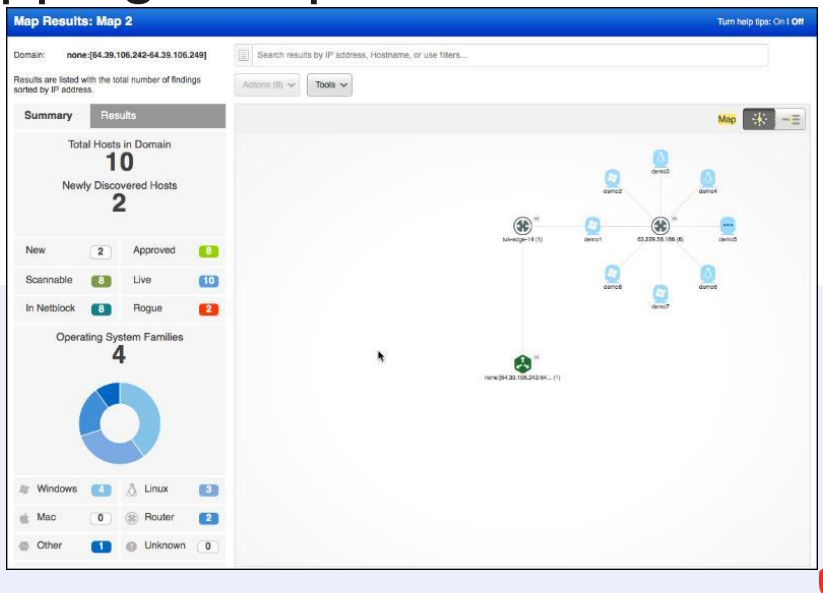
Discovery Method	Port
ICMP	-
TCP	135
TCP	139
TCP	445
UDP	137
TCP RST	-

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

▸	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

Qualys.

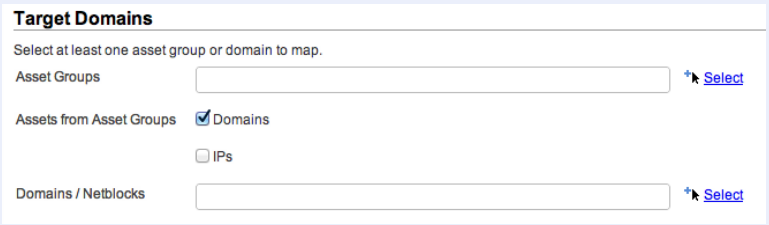
Mapping: Graphic Mode



Qualys.

Mapping: Choosing A Target

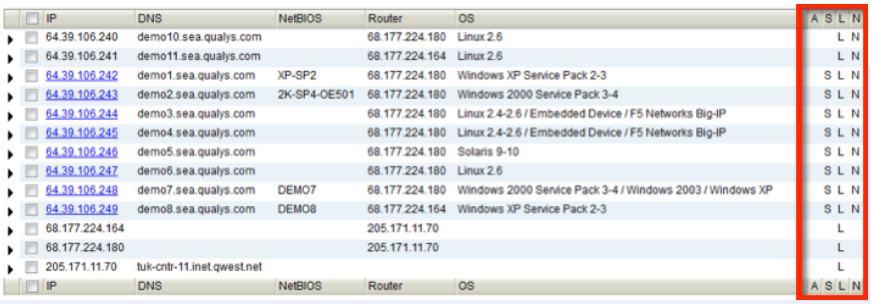
1. **Domain** - Qualys service will identify domain members via DNS interrogation.
2. **Netblock** - Target a specific netblock range using the “none” domain.
3. **Domain + Netblock** – Use an IP address range to identify the upper and lower boundaries of a domain.
4. **Asset Group**
   - Associated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



Qualys.

Mapping Goals

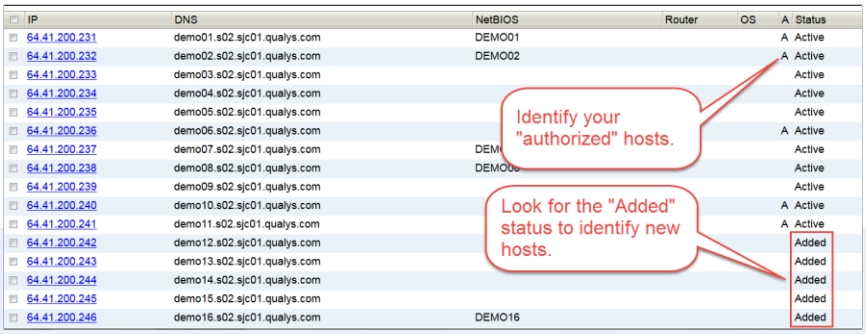
1. Use map results and reports to discover and add new hosts to your subscription and identify dead and rogue hosts.
2. Ensure network and system admin teams participate in the Mapping and Reporting responsibilities.



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-cntr-11.inet.qwest.net						L	
IP	DNS	NetBIOS	Router	OS	A	S	L	N

Qualys.

Unknown Devices Report



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

Qualys.

Thank You

training@qualys.com