tenable network security

SecurityCenter 5.1 with Nessus Agent Support

October 22, 2015

Table of Contents

Introduction

With the introduction of SecurityCenter 5.1, Tenable continues to advance the only true continuous network monitoring solution on the market today. Tenable now provides customers the ability to automate imports of Nessus agent scan data from Nessus Cloud or Nessus Manager directly into SecurityCenter 5.1.

Nessus agent support in SecurityCenter helps customers address the following challenges:

- **Securing The Mobile Workforce** – Customers no longer have to worry about omitting assets that are not online during a vulnerability scan. Nessus agents will run the scans and then upload results to Nessus Manager or Nessus Cloud when a connection is available. From there, the results are uploaded to SecurityCenter and SecurityCenter Continuous View (SecurityCenter CV).

- **Securing Systems on Complex or Bandwidth Limited Networks** – Nessus agents remove the challenge of performing scans over segmented or complex networks and reduce network bandwidth usage, which is important for remote facilities connected by slow networks.

- **Removing Credential Headaches** – Many organizations struggle with credential management due to regular password change policies. With Nessus agents, host credentials for customers' hosts are no longer required, removing the need for password resets and maintenance of privileges on assets.

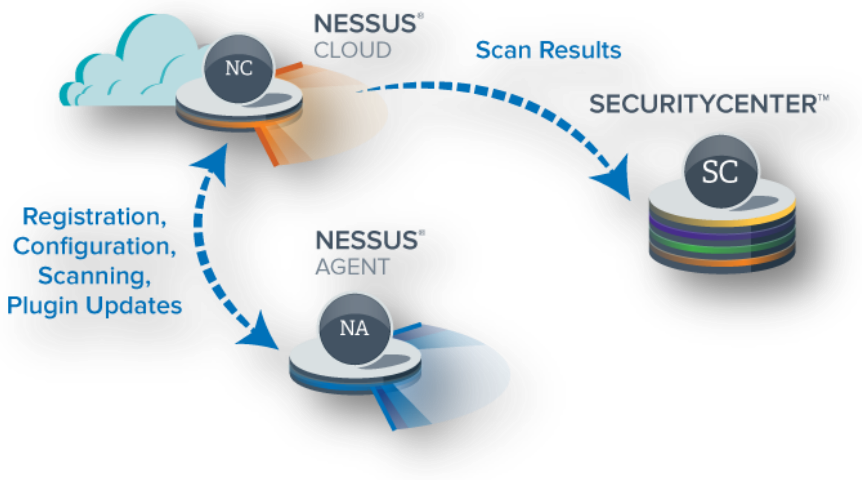
Nessus agent scans, which are configured, managed, and updated through Nessus Cloud or Nessus Manager, help identify vulnerabilities, policy-violating configurations, and malware on hard-to-reach hosts.

This document provides details about configuring SecurityCenter 5.1 to utilize the new agent data import feature. In addition, it also suggests recommendations, tips, and tricks to maximize the benefits of using Nessus agents with SecurityCenter 5.1.

Please email support@tenable.com with any comments or questions.

Recommended Deployment Model

Tenable recommends that customers use Nessus Cloud to manage Nessus agents and to transfer agent data to SecurityCenter 5.1, as illustrated below:



Nessus Manager can also be used to manage and update Nessus Agents, but Nessus Cloud offers several distinct advantages over Nessus Manager:

- Nessus agents can perform scans locally and upload the results to Nessus Cloud when an Internet connection becomes available. Nessus Manager is deployed on-premises and has to be placed in the DMZ to achieve similar functionality. If Nessus Manager is deployed without direct Internet access, the agent data will not be uploaded until the Nessus agent system is connected to the corporate network.
- Nessus agent data can be scheduled to import in bulk from Nessus Cloud into SecurityCenter 5.1 during off-hours, thereby preserving bandwidth for users during business hours. There is a reduction of administrative overhead by managing a single connection between Nessus Cloud and SecurityCenter 5.1 versus managing potentially thousands of connections between individual agents and Nessus Manager.
- With Nessus Cloud, customers will not need to upgrade their infrastructure to accommodate growth if the number of Nessus agents in use increases.

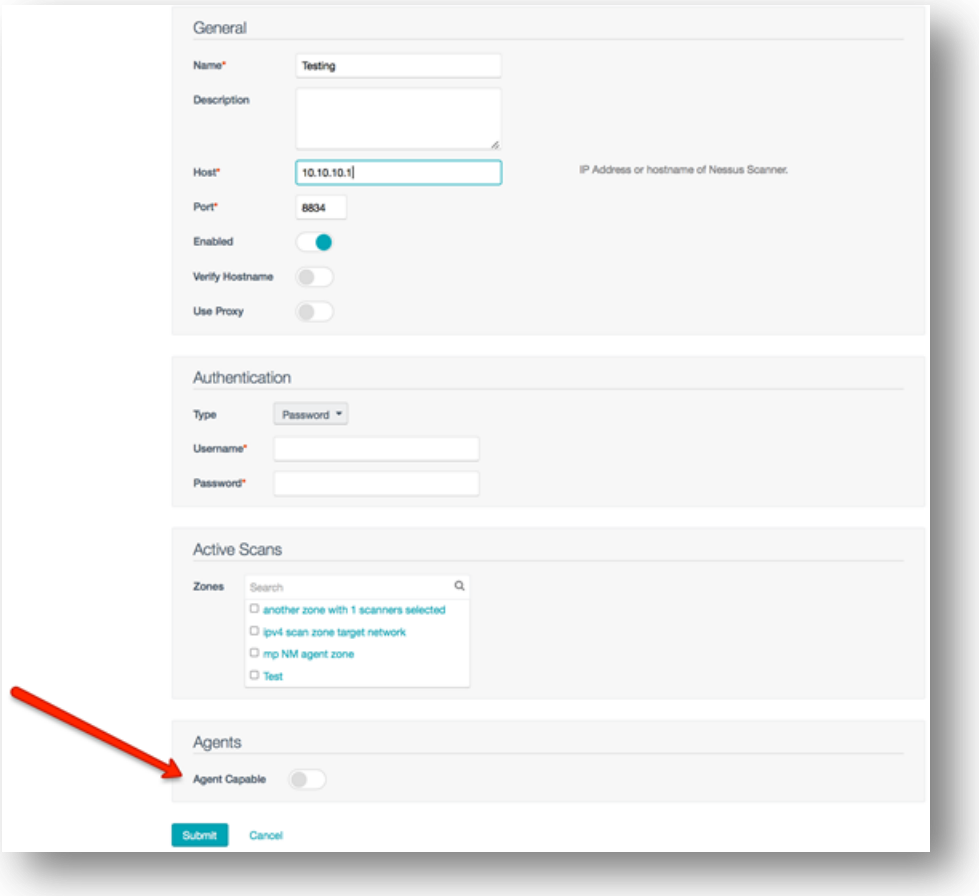
Note: If needed, Nessus Manager can be used in place of Nessus Cloud for agent management. Tenable recommends deploying Nessus Manager in the DMZ as a proxy between the agents and SecurityCenter 5.1.

Use a non-admin account on Nessus Manager to establish a connection from SecurityCenter 5.1 to Nessus Manager. The non-admin account on Nessus Manager must also be the one used to run agent scans.

To learn more about how to install and configure Nessus agents through Nessus Cloud and Nessus Manager, refer to the Nessus 6.5 Documentation. Also, please see the SecurityCenter 5.1 with Nessus Agents – Customer FAQ for the prerequisites needed to use SecurityCenter 5.1 with Nessus agents.

Configuring SecurityCenter 5.1 for use with Nessus Agents

Once Nessus agents have been deployed through Nessus Cloud or Nessus Manager and all prerequisites are met, customers are ready to begin configuring SecurityCenter 5.1 to import the Nessus agent data. The first step is to add a new agent-capable Nessus scanner into SecurityCenter 5.1. Existing SecurityCenter customers will notice that adding an agent-capable Nessus scanner follows the same basic steps as adding a traditional Nessus scanner with only a few slight differences. To add an agent-capable Nessus scanner, log in to SecurityCenter 5.1 as an admin user. Under the “Resources” drop-down, select “Nessus Scanner”. Add a new scanner by clicking on the “+Add” button in the top right-hand corner.



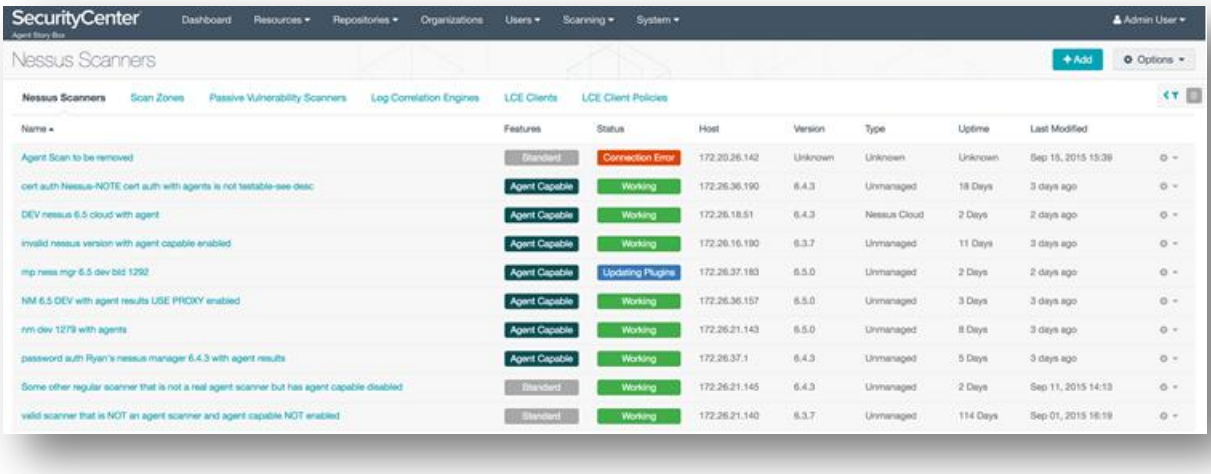
Configure the "Add Nessus Scanner" screen to connect the Nessus scanner to SecurityCenter 5.1 (see "*Table 1 – Nessus Scanner Options*" below for details of each field). Please make note of the new "Agents" section at the bottom of the screen. Enabling the "Agent Capable" option is required to import the Nessus scanner's agent scan results into SecurityCenter 5.1.

Table 1– Nessus Scanner Options

Option	Description
Name	Descriptive name for the Nessus scanner.
Description	Scanner description, location, or purpose.
Host	Hostname or IP address of the scanner.
Port	TCP port that the Nessus scanner listens on for communications from SecurityCenter. The default is port 8834.
Enabled	A scanner may be "Enabled" or "Disabled" within SecurityCenter to allow or prevent access to the scanner.
Verify Hostname	Adds a check to verify that the hostname or IP address entered in the "Host" field matches the CommonName (CN) presented in the SSL certificate from the Nessus server.

Use Proxy	Instructs SecurityCenter to use its configured proxy for communication with the scanner.
Authentication Type	Select Password or SSL Certificate for the authentication type to connect to the Nessus scanner.
Username	Username generated during the Nessus install for daemon to client communications. This must be an administrator user in order to send plugin updates to the Nessus scanner. If the scanner will be updated by a different method, such as through another SecurityCenter, a standard Nessus user account may be used to perform scans. This field is only available if the Authentication Type is set to "Password".
Password	The login password must be entered in this field. This field is only available if the Authentication Type is set to "Password".
Certificate	This field is available if the Authentication Type is "SSL Certificate". Select the "Browse" button, choose a SSL Certificate file to upload, and upload to the SecurityCenter.
Active Scan Zones	IP address(es), ranges, or CIDR blocks that the Nessus scanner can perform active scans on.
Agent Capable	Enable this option to allow agent scan job results to be scheduled and imported into SecurityCenter 5.1

Once you complete the configuration and click "Submit", SecurityCenter will return to the "Nessus Scanners" page, which shows the list of Nessus scanners attached to SecurityCenter 5.1. The new "Features" column shows which Nessus scanners are now "Agent Capable".

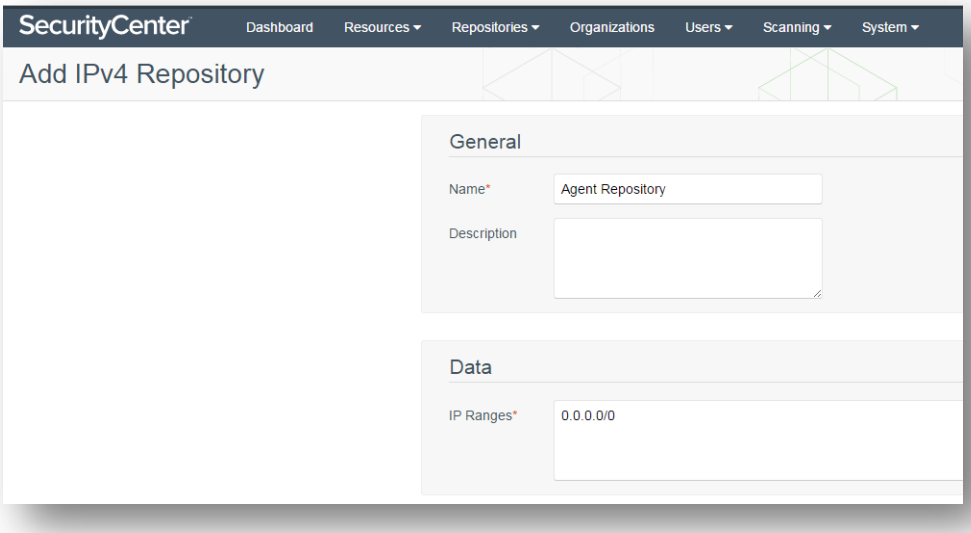


Adding an Agent Repository

Tenable recommends creating a new repository specifically for agent data. In SecurityCenter 5.1, click on the "Repositories" drop-down and select "Repositories". Click the "+Add" button in the top-right corner to add a new repository.

To configure the agent repository, enter a descriptive name and configure the IP ranges in the "Data" section.

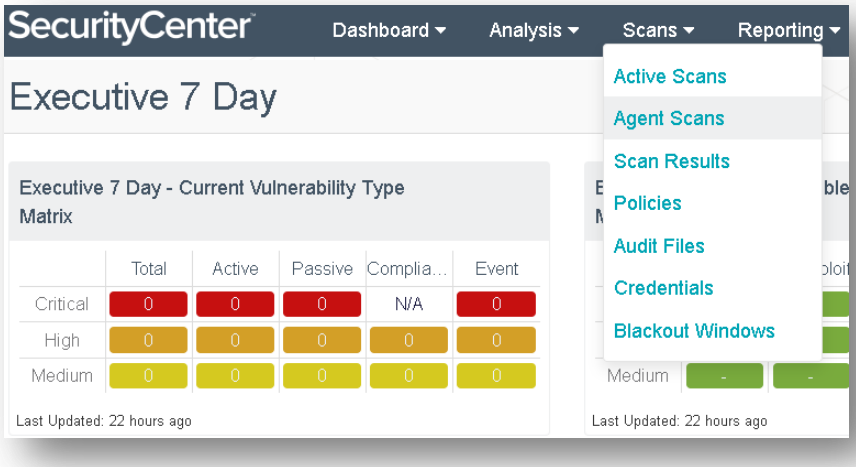
As a best practice, Tenable recommends using "0.0.0.0/0" in the "IP Ranges" field to ensure all agent systems are accounted for.



Add Agent Scans and Import Agent Scan Results

Agents and their scan results are managed and collected by Nessus Cloud (or Nessus Manager). Once you have configured an agent-capable scanner and created a new repository for agent data in SecurityCenter 5.1, the results of the Nessus agent scan jobs can now be imported on a scheduled basis.

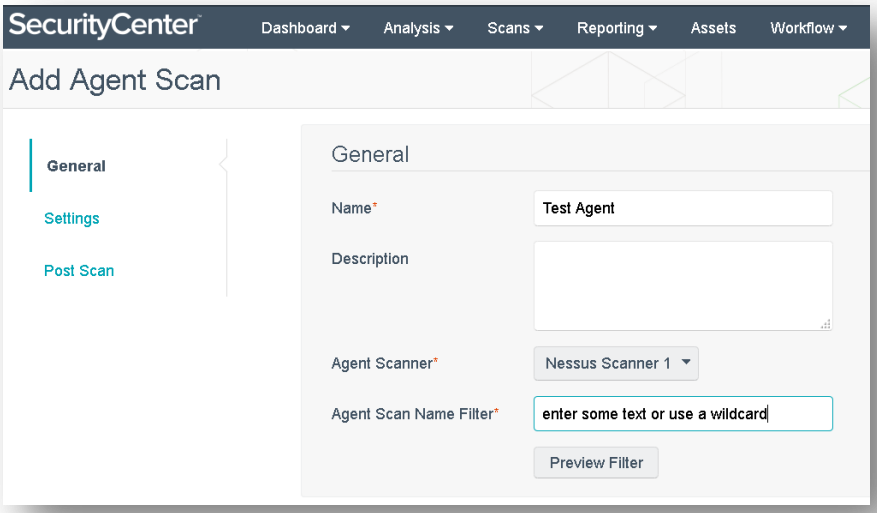
In SecurityCenter 5.1, click on the "Scans" drop-down and select "Agent Scans". On the "Agent Scans" screen, click the "+Add" button in the top-right corner.



In the "General" section, enter a name for the Agent Scan. Next, click the drop-down next to "Agent Scanner" and select the appropriate scanner. Note: only scanners that are agent-capable will be displayed as options.

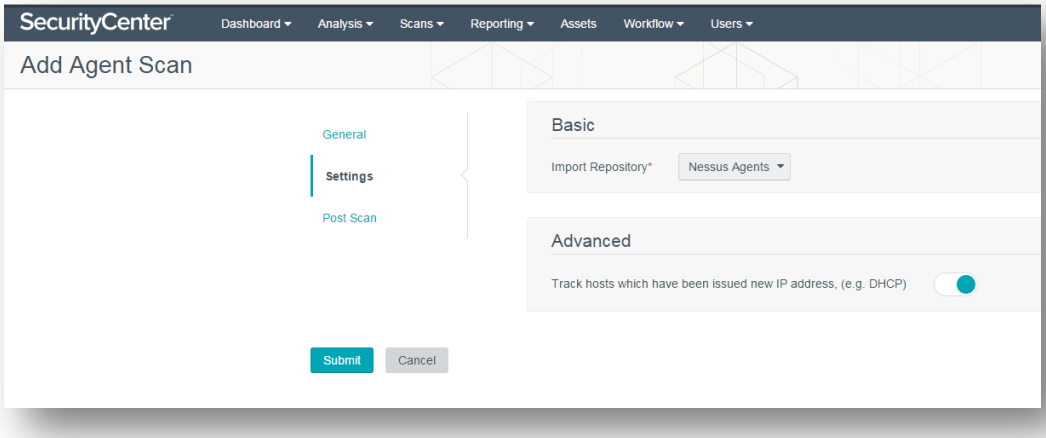
In the "Filter by Nessus Agent Scan Name" field, enter your desired search criteria or a valid wildcard ("*" and "?") to find completed scan jobs on the selected Agent Scanner.

Clicking on "Preview Filter" will display the agent scan jobs that correspond to the agent scanner selected above and are ready to be imported into SecurityCenter. Each agent scan job will show the number of scan results that will be imported during the next scheduled occurrence. Agent scans that have not run or that have no results will not be displayed.



Set the frequency that SecurityCenter 5.1 will poll Nessus Cloud (or Nessus Manager) to import the completed agent scan jobs by editing the "Schedule". Please see the "Tips and Tricks" section for best practices to align scheduling with agent completion time.

Click the drop-down next to "Import Repository" and select the repository that will contain agent results.



Once you have finished configuring the "Add Agent Scan" screen, click "Submit".

Tips and Tricks

Organize Your Devices by Creating a Repository for Agent Scan Results

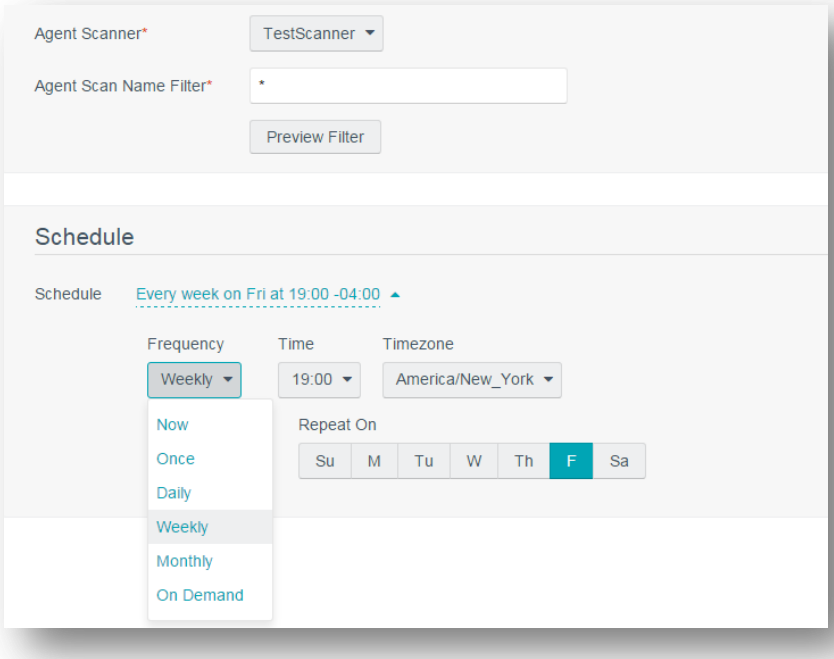
Creating a separate and unique repository for agent scan results will keep a separate list for all agent-enabled systems, which may or may not be located in their standard environment at the time of scanning. Systems with Nessus agents are potentially far more transient than other systems, therefore adding their vulnerability data to a dedicated repository and setting a relatively low data retention time helps ensure that old systems and their data are removed from the repository in a timely manner.

Transient hosts can obtain different IP addresses from being connected to different networks. Tenable recommends leaving the "Track hosts which have been issued new IP addresses" option enabled to prevent the same host from being discovered multiple times and duplicating its vulnerability data. The order for reconciliation is DNS, then NetBIOS, and finally MAC address.

Newly discovered devices count against your SecurityCenter IP license. Please refer to the SecurityCenter 5.1 Administration Guide for details about SecurityCenter licensing.

Align Agent Data Import Schedules with the Completion Times of Agent Scan Jobs

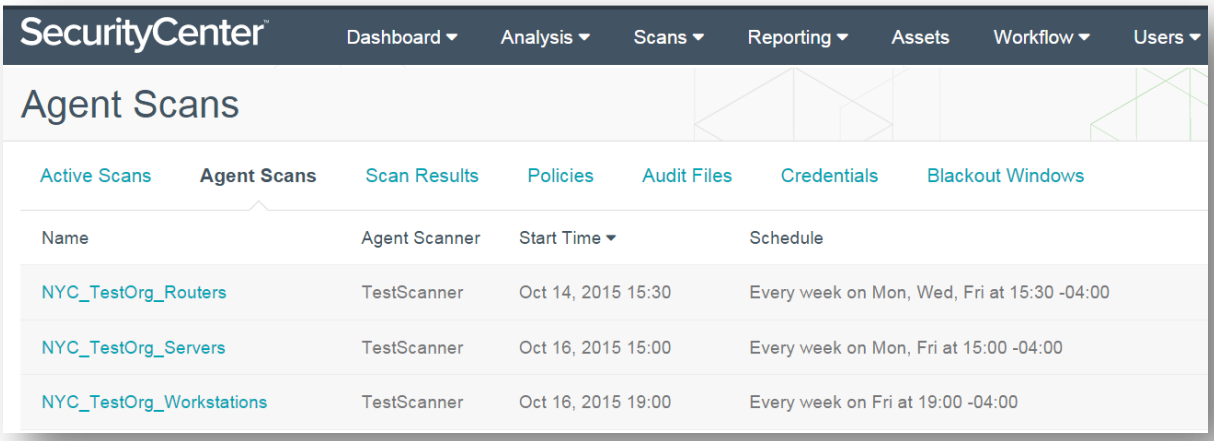
When scheduling imports of Nessus agent data into SecurityCenter, it is recommended to schedule the imports as near to the completion time of the agent scans as possible. For example, if the agents complete scans of systems on a Thursday afternoon and SecurityCenter is scheduled to import the data on a Saturday night, SecurityCenter will show the data as found on the Saturday night import time. This can be confusing to administrators when determining when particular vulnerabilities were discovered in the network. In the example above, it would be recommended to either schedule the agent scans to complete on Saturday afternoon or evening, or to schedule the agent data import for Thursday evening soon after the scans complete.



Use Informative Naming Conventions for Scans

Using informative descriptions for agent scan data imports makes it easier to identify where the data was obtained from. Running multiple scans named "NYC_AgentScan" gives little detail about the systems from which information is being gathered. Tenable suggests that each agent scan job uses a naming convention that is descriptive, easily understood, and that allows for coverage of the entire environment.

In the screenshot below, agent scans are given similar but unique names that specify the physical location of the systems (NYC), the environment (TestOrg), and the types of systems (Routers, Workstations, and Servers) that were scanned:



Conclusion

With the use of Tenable's agent technology, SecurityCenter 5.1 helps organizations eliminate blind spots within their networks by collecting and analyzing data from previously inaccessible systems. Agents perform scans on transient and mobile systems that are often disconnected from the network during traditional scan times. Agents help remove the challenges of performing scans over segmented or complex networks while also reducing bandwidth usage. The use of agents also helps eliminate the difficulties of credential management by delivering the detailed visibility normally found with credentialed scans but without the struggles of password resets and maintenance of privileges. SecurityCenter 5.1 customers can now automatically import agent scan data into SecurityCenter and Security Center Continuous View to help identify vulnerabilities, reduce risk, and ensure compliance across virtually all assets.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.