DISA Logo

ACAS General Requirements

October 16, 2015

v1

Table of Contents

[Change Log 4](#_Toc432773438)

[Introduction 5](#_Toc432773439)

[Standards and Conventions 5](#_Toc432773440)

[System Requirements 5](#_Toc432773441)

[SecurityCenter Hardware Requirements 5](#_Toc432773442)

[Network Interfaces 6](#_Toc432773443)

[Disk Space 7](#_Toc432773444)

[Disk Partitions 7](#_Toc432773445)

[Nessus Hardware Requirements 7](#_Toc432773446)

[PVS Hardware Requirements 8](#_Toc432773447)

[Software Requirements 9](#_Toc432773448)

[ACAS Product Compatibility 9](#_Toc432773449)

[SecurityCenter 10](#_Toc432773450)

[Supported Operating Systems 10](#_Toc432773451)

[IT Environment Requirements 10](#_Toc432773452)

[Virtualized Environments 10](#_Toc432773453)

[Securing the Environment 10](#_Toc432773454)

[Dependencies 11](#_Toc432773455)

[SecurityCenter Communications and Repositories 13](#_Toc432773456)

[Nessus 13](#_Toc432773457)

[Supported Operating Systems 13](#_Toc432773458)

[Dependencies 14](#_Toc432773459)

[Nessus Unix Library Requirements 14](#_Toc432773460)

[Nessus Windows Requirements 14](#_Toc432773461)

[Passive Vulnerability Scanner 14](#_Toc432773462)

[Supported Operating Systems 14](#_Toc432773463)

[Dependencies 15](#_Toc432773464)

[Licensing Requirements 15](#_Toc432773465)

[ACAS License Request Portal 15](#_Toc432773466)

[SecurityCenter 15](#_Toc432773467)

[Nessus 15](#_Toc432773468)

[Passive Vulnerability Scanner 16](#_Toc432773469)

[Pre-Installation 16](#_Toc432773470)

[License Request 16](#_Toc432773471)

[Disable Default Web Servers 16](#_Toc432773472)

[Modify Firewall Settings 17](#_Toc432773473)

[Log Rotation 17](#_Toc432773474)

[Useful links 18](#_Toc432773475)

[Certification and Accreditation Artifacts: 18](#_Toc432773476)

[ACAS TTP: 18](#_Toc432773477)

[Approved documentation/binaries are located on DoD Patch Repository: 18](#_Toc432773478)

[ACAS Homepage: 18](#_Toc432773479)

[ACAS License Request Portal: 18](#_Toc432773480)

[ACAS Build 1 Request Portal: 18](#_Toc432773481)

[ACAS Approving POC list: 18](#_Toc432773482)

[ACAS Monthly Working Group page: 18](#_Toc432773483)

[ACAS Front Door: 18](#_Toc432773484)

[ACAS Customer Support/OKC Helpdesk: 18](#_Toc432773485)

# Change Log

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Changes** |
| 16-Oct-2015 | 1 | * Initial document creation. |

# Introduction

This document provides prerequisite information about the hardware, software, and licensing requirements to support deployment of the Assured Compliance Assessment Solution (ACAS) using Tenable products. The goal is to enable Department of Defense (DoD) customers to be prepared for product installation.

## Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

# **pwd**/opt/sc4/daemons  
#

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Important notes and considerations are highlighted with this symbol and grey text boxes. |

|  |  |
| --- | --- |
| LoRes_Lightbulb2.png | Tips, examples, and best practices are highlighted with this symbol and white on blue text. |

# System Requirements

This section describes the requirements for hardware, network, and disk storage. Note that the particular needs of your organization must be factored into this guideline.

## SecurityCenter Hardware Requirements

SecurityCenter hardware requirements can vary widely depending on the types of scans you are running and the size of your network. The following chart outlines the basic hardware requirements for operating the SecurityCenter.

**Table 1 – SecurityCenter Hardware Requirements**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Small | Medium | Medium High Use | Large | Large High Use |
| Active IPs | 2,500 | 10,000 | 25,000 | 75,000 | 100,000 |
| Concurrent Users | 25 | 25 | 60 | 25 | 60 |
| Total users | 50 | 75 | 75 | 100 | 100 |
| Repositories | 20 | 60 | 60 | 100 | 100 |
| Asset Lists | 50 | 75 | 75 | 100 | 100 |
| Threshold Limit of Scanners | 20 | 35 | 50 | 35 | 50 |
| CPU | 4 cores (2 dual-core) at 2 GHz | 8 cores (4 dual-core) at 3 GHz | 16 cores (8 dual-core) at 3 GHz | 24 cores (6 quad-core) at 3 GHz | 32 cores (8 quad-core) at 3 GHz |
| RAM | 8 GB | 16 GB | 32 GB | 64 GB | 128 GB |
| Disk Storage  (7,200/10,000 revolutions per minute (rpm) recommended) | 250 GB | 800 GB | 2 TB | 4 TB | 8 TB |
| Disk Space used for Vulnerability Trending | 90 days: 225 GB  180 days: 450 GB | 90 days: 900 GB  180 days: 1.8 TB | 90 days: 2.25 TB  180 days: 4.5 TB | 90 days: 5 TB  180 days: 8 TB | 90 days: 9 TB  180 days: 18 TB |

In addition to the above guidelines, please consider the following suggestions:

* If Nessus or Passive Vulnerability Scanner (PVS) is deployed on the same server as SecurityCenter, there will be less Central Processing Unit (CPU) and memory available during scans, causing slower performance. Consider configuring the server with multiple network cards and IP addresses. Combine the hardware recommendations for all installed software components to properly size the system. It is strongly recommended that the scanner(s) are placed on a secondary machine.
* For large deployments of SecurityCenter with more than 25 active users, consider increasing the amount of memory and/or CPUs to improve performance.
* If one or more Passive Vulnerability Scanners are in use, add additional processor cores to increase performance.
* Use the aggregate of the individual software product resource requirements for determining total hardware system requirements. Hosting multiple Tenable products on the same server is not recommended due to potential memory and CPU constraints.
* While there is no hard limit on the number of scanners (Nessus or PVS), the threshold limit described in the table above is the point at which SecurityCenter performance may be hindered. Additional resources may offset additional scanners.

### Network Interfaces

Network scanning consumes a few MB/s of bandwidth; however, the actual number of MB/s cannot be quantified since it varies depending on the scan environment. Many of Tenable’s customers use 100 MB interface cards for network scanning. There is no compelling requirement to use gigabit network cards at this time. However, such an interface may make sense to generally increase the overall performance of web sessions, emails, Log Correlation Engine (LCE) queries, and other network activities.

If Nessus is deployed on the same server as SecurityCenter, consider configuring the server with multiple network cards and IP addresses. Nessus uses default routes when scanning target networks, and will correctly scan a system from the appropriate interface.

### Disk Space

Adequate disk space is critical to a successful SecurityCenter deployment. An important consideration is that SecurityCenter saves a snapshot of the entire vulnerability archive each day. In addition, the size of the vulnerability data stored by SecurityCenter depends on the number and types of vulnerabilities, not just the number of hosts. For example, 100 hosts with 100 vulnerabilities each could consume as much data as 1,000 hosts with 10 vulnerabilities each. In addition, the output for vulnerability check plugins that do directory listings, etc. is much larger than “Open Port” plugins from discovery scans.

For networks of 35,000 to 50,000 hosts, Tenable has encountered data sizes of up to 25 GB. That number is based on storage of 50,000 hosts and approximately 500 KB per host.

Additionally, during active scanning sessions, large scans and multiple smaller scans have been reported to consume as much as 150 GB of disk space as results are acquired. Once a scan has completed and its results are imported, that disk space is freed up.

### Disk Partitions

SecurityCenter is installed into **/opt/sc4** by default. Tenable highly recommends that the **/opt** directory be created on a separate disk partition. For higher performance, using two disks, one for the operating system and one for the system deployed to **/opt**, can be more efficient.

|  |  |
| --- | --- |
| LoRes_Lightbulb2.png | If required disk space exists outside of the /opt file system, mount the desired target directory using “mount –-bind <olddir> <newdir>”. Make sure that the file system is automatically mounted on reboot by editing the /etc/fstab file appropriately. |

Deploying SecurityCenter on a server configured with Redundant Array of Independent Disks (RAID) can also dramatically boost performance.

|  |  |
| --- | --- |
| LoRes_Lightbulb2.png | SecurityCenter does not require a RAID configuration for even our largest customers. However, in one instance, response times for queries with a faster RAID configuration for a customer with more than 1 million managed vulnerabilities moved from a few seconds to less than a second. |

## Nessus Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Nessus deployments include raw IP address count, and the configuration of the Nessus application. There is no configuration which can be assured to scan X amount of hosts per hour. The following chart outlines the basic hardware requirements for operating Nessus:

**Table 2 – Nessus Hardware Requirements**

|  |  |  |
| --- | --- | --- |
| CPU | RAM | Disk Storage  (for Nessus data) |
| 4 cores (1 quad-core) at 3 GHz | 8-12+ GB RAM | 80 GB |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Note: The ability to monitor a given number of hosts rests heavily on the memory, and processor power available to the system running Nessus Scanner. More Nessus hardware will decrease the amount of time to complete a scan. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Nessus can be run under a VMware instance, but if the virtual machine is using Network Address Translation (NAT) to reach the network, many of Nessus’ vulnerability checks, host enumeration, and operating system identification will be negatively affected. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Please research your VM software vendor for comparative recommendations as VMs typically see up to a 30% loss in efficiency compared with dedicated servers. |

Processor requirements will increase with greater throughput and number of network interfaces. Memory requirements will increase for networks with more hosts. The requirements for both of these components are affected by options such as a long report-lifetime and enabling some or all of the Nessus optional services in the configuration file.

If scans are taking too long to complete, consider increasing the number of scanners deployed in the environment.

## PVS Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for PVS deployments include raw network speed, the size of the network being monitored, and the configuration of the PVS application.

The following chart outlines some basic hardware requirements for operating PVS:

**Table 3 – PVS Hardware Requirements**

|  |  |  |
| --- | --- | --- |
| CPU | RAM | Disk Storage  (for PVS data) |
| 4 cores (1 quad-core) at 3 GHz | 8-12+ GB RAM | 80 GB |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Note: The ability to monitor a given number of hosts rests heavily on the bandwidth, memory, and processor power available to the system running PVS. |

|  |  |
| --- | --- |
| LoRes_Lightbulb2.png | For optimal data collection, PVS needs to be connected to the network segment via a hub, spanned port, or network tap to have a full, continuous view of the network traffic. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Please research your Virtual Machine (VM) software vendor for comparative recommendations as VMs typically see up to a 30% loss in efficiency compared with dedicated servers. |

Processor requirements will increase with greater throughput and number of network interfaces. Memory requirements will increase for networks with more hosts. The requirements for both of these components are affected by options such as a long report-lifetime and enabling some or all of the PVS optional services in the configuration file.

Disk space requirements for PVS will vary depending on usage based on the amount and length of time data is stored on the system.

# Software Requirements

## ACAS Product Compatibility

If you are running Tenable’s Log Correlation Engine (LCE), which is currently not part of the ACAS contract, please note that LCE 4.2 or higher is required for complete functionality with SecurityCenter 4.8. Using a combination of LCE 3.x and 4.x servers will result in most SecurityCenter LCE functionality of all connected servers being limited to what is available using the LCE 3.x server.

**Table 4 – SecurityCenter 4.8 Product Compatibility**

|  |  |
| --- | --- |
| Product | Minimum Version |
| Nessus | 6.5.x |
| LCE | 4.0 (3.6.1 with limited functionality)  4.2 or higher for LCE Vulnerability features |
| PVS | 4.x |
| SecurityCenter (remote/offline repository\*) | 4.x |
| 3D Tool | 2.x |

\* SecurityCenter 4.8 can receive a repository from prior versions of SecurityCenter 4.0.x and above, but cannot share its repositories with previous versions.

## SecurityCenter

### Supported Operating Systems

|  |  |
| --- | --- |
|  | Note that not all operating systems are supported as an ACAS baseline. Please visit the Department of Defense (DoD) Patch Repository for a list of supported installation packages. |

SecurityCenter 4 is available for Red Hat Enterprise Linux (RHEL) Server 5 (32/64-bit) and 6 (32/64-bit). SELinux policy configuration is supported by Tenable in a “Permissive” mode. See the section labeled “Modify Firewall Settings” for more information.

|  |  |
| --- | --- |
| LoRes_Lightbulb2.png | Other SELinux modes are known to work, but the required configuration varies based on policies and custom configurations that may be in place on-site. It is strongly recommended that SELinux implementation configurations are tested prior to deployment on a live network. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | However, per RHEL-06-000020 of the RHEL 6 Security Technical Implementation Guide (STIG), SELinux must be set in “Enforced” mode. |

### IT Environment Requirements

#### Virtualized Environments

SecurityCenter is well suited to virtual platforms and comes prepackaged along with Nessus and PVS on the ACAS Kickstart image. The ACAS Kickstart is available for download on the DoD Patch Repository website. Multiple VM images may be deployed on the network to support multiple products. Because of the unique performance considerations with virtualized platforms, please consult your VM software vendor for recommendations, as VMs typically see up to 30% loss in efficiency compared with dedicated servers.

#### Securing the Environment

It is assumed that organizations have the appropriate skill set required to maintain the operating system (OS) environment in a secure manner and that they are configured and maintained with the following conditions:

* The operating system must be configured in a secure manner to ensure that security controls cannot be bypassed.
* The network must be configured to ensure that the SecurityCenter system resides in a secure network segment that is not accessible from the Internet.
* Network time synchronization must be enabled to ensure that accurate time stamps are recorded in reports and log files.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | The time zone is set automatically during the installation process with no user interaction. If steps are required for manual time zone configuration, please refer to the following Knowledge Bulletin (KB) article: https://support.tenable.com/support-center/index.php?x=&mod\_id=2&root=92&id=444. Important: The time zone configured in php.ini must be synchronized with the system time zone in /etc/sysconfig/clock. |

* Access control mechanisms must be in place to ensure that only authorized users have access to the OS platform.

Of particular importance is the requirement to monitor system resources to ensure that adequate disk space and memory are available. If system resources are exhausted, there is a risk that audit data could be prevented from being logged due to the system becoming dysfunctional. Refer to the “Troubleshooting” section of the SecurityCenter Administration Guide for information on how system administrators can recover the system should SecurityCenter become inoperative due to resource exhaustion. During recovery processes, actions by the system administrator may not be logged by SecurityCenter until sufficient resources have been made available.

The following resource provides details for secure administration of a Red Hat installation:

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Even though the security concepts from this guide are written for RHEL 6, most of the concepts and methodologies apply to earlier versions of RHEL that are supported with SecurityCenter. |

* Red Hat Enterprise Linux 6 Security Guide - A Guide to Securing Red Hat Enterprise Linux. <http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html>.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | As with any application, the security and reliability of the installation is dependent on the environment that supports it. It is strongly recommended that organizations deploying SecurityCenter have an established and applied IT management policy that covers system administration integrity, resource monitoring, physical security, and disaster recovery. |

### Dependencies

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Either Open Java Development Kit (OpenJDK) or the Oracle Java Runtime Environment (JRE) along with their accompanying dependencies must be installed on the system along with any additional Java installations removed for reporting to function properly. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Although it is possible to force the installation without all required dependencies, if your version of Red Hat is missing certain dependencies, this will cause problems that are not readily apparent with a wide variety of functions. Defense Information Systems Agency (DISA’s) Assured Compliance Assessment Solution (ACAS) Support team has observed different types of failure modes for SecurityCenter when dependencies to the installation Red Hat Package Manager (RPM) are missing. If you require assistance or guidance in obtaining these dependencies, please contact our ACAS Support team at [disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil](mailto:disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil). |

The following programs must be installed on the system prior to installing the SecurityCenter package. While they are not all required by the installation RPM file, some functionality of SecurityCenter may not work properly if the packages are not installed. The packages listed below are among those that are most often not installed by default:

* **java-1.6.0-openjdk** (or later) (or the latest Oracle Java JRE)
* **openssh**
* **expat**
* **gdbm**
* **libtool**
* **libtool-ltdl**
* **libxml2**
* **ncurses**
* **readline**
* **compat-libstdc++**
* **libxslt**

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Using the latest stable production version of each package is recommended. |

For a list of required packages, run the following command against the SecurityCenter RPM file:

# **rpm –qp SecurityCenter-4.x.x-es6.x86\_64.rpm –requires**

To determine which version of a dependency is installed on your system, run the following command for each of the packages (replace “**libtool**” with the appropriate package):

# **rpm –qa | grep libtool**

If one of the prerequisite packages is missing, it can be installed using the “**yum**” or “**rpm**” package managers. For example, install **Java 1.6.0** with “**yum**” using the command below:

# **yum -y install java-1.6.0-openjdk.x86\_64**

### SecurityCenter Communications and Repositories

The following table summarizes the components’ primary repositories and communication methods.

**Table 5 – Repositories and Communication Methods**

|  |  |
| --- | --- |
| SecurityCenter | |
| Installation Directory | **/opt/sc4** |
| User Data | **/opt/sc4/orgs/<Organization Serial Number>** |
| Repositories | **/opt/sc4/repositories/<Repository Number>** |
| Audit Log | **/opt/sc4/admin/logs/** |
| Organization Logs | **/opt/sc4/orgs/<Organization Number>/logs/** |
| Communication Interfaces | User Access: Hypertext Transfer Protocol Secure (HTTPS)  Plugin Updates:  Acquired over Secure Socket Layer (SSL) from Tenable servers directly to SecurityCenter or for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures. |

## Nessus

### Supported Operating Systems

|  |  |
| --- | --- |
|  | Note that not all operating systems are supported as an ACAS baseline. Please visit the Department of Defense (DoD) Patch Repository for a list of supported installation packages. |

Nessus is available and supported for a variety of operating systems and platforms:

* Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
* Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 and x86-64) [Server, Desktop, Workstation]
* Windows Server 2008, Server 2008 R2\*, Server 2012, Server 2012 R2 (x86-64)
* Windows 7 and 8 (i386 and x86-64)

|  |  |
| --- | --- |
|  | Note that on Windows Server 2008 R2, the bundled version of Microsoft Internet Explorer (MSIE) does not interface with a Java installation properly. This causes Nessus not to perform as expected in some situations. Further, Microsoft’s policy recommends not using MSIE on server operating systems. |

|  |  |
| --- | --- |
|  | Nessus utilizes several third-party software packages distributed under varying licenses. Running nessusd (or nessusd.exe on Windows) with the -l argument will display a list of those third-party software licenses. |

### Dependencies

#### Nessus Unix Library Requirements

Before installing Nessus on Unix/Linux, there are several libraries that are required. Many operating systems install these by default and typically do not require separate installation.

* zlib
* GNU C Library (i.e., libc)
* Oracle Java (for PDF reporting only)

|  |  |
| --- | --- |
|  | Java must be installed on the host before Nessus is installed. If Java is installed afterwards, then Nessus will need to be reinstalled. Further, the same architecture version must be installed, meaning Nessus 6 64-bit will only recognize a 64-bit installation of Java. Many web browsers are 32-bit, meaning visiting the Java download page will automatically provide the 32-bit version of Java. You may need to manually download the 64-bit version. |

|  |  |
| --- | --- |
|  | Please research your Virtual Machine (VM) software vendor for comparative recommendations as VMs typically see up to a 30% loss in efficiency compared with dedicated servers. |

|  |  |
| --- | --- |
|  | Nessus does not support installing to a directory or location via a symbolic link. If required disk space exists outside of the /opt file system, mount the desired target directory using “mount --bind <olddir> <newdir>”. Make sure that the file system is automatically mounted on reboot by editing the /etc/fstab file accordingly. |

#### Nessus Windows Requirements

For increased performance and scan reliability, it is highly recommended that Nessus Windows be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2. For more information on this issue, please see the “Nessus Windows Troubleshooting” section of the Nessus Installation and Configuration Guide.

## Passive Vulnerability Scanner

### Supported Operating Systems

The Passive Vulnerability Scanner is available for the following platforms:

* Red Hat Linux ES 5 / CentOS 5 64-bit
* Red Hat Linux ES 6 / CentOS 6 64-bit
* Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012

### Dependencies

WinPcap is required for PVS installations on the Windows operating system. The PVS installation package for Windows will either install WinPcap on systems that do not already have it installed, or upgrade WinPcap on systems with older versions of the software.

# Licensing Requirements

## ACAS License Request Portal

In order to use the ACAS software, a license key is required. A request for a license key must be submitted via the ACAS License Request Portal:

<https://east1.deps.mil/disa/cop/mae/netops/acas/SitePages/requestPortal/LicenseRequest.aspx>

Once the requested license key(s) are ready, the requestor will receive an email containing a link to download the license key(s). License key(s) are provided in either a zip file or a KEY file format.

Contact the DISA Integrated Command and Control (ICC) team if there are questions regarding ACAS license key requests at the following mailbox: [disa.meade.peo-ma.mbx.iccacas@mail.mil](mailto:disa.meade.peo-ma.mbx.iccacas@mail.mil).

## SecurityCenter

SecurityCenter is licensed by the total number of active IP addresses it manages and the hostname of the system on which it is installed. For example, a customer can purchase a 500-IP SecurityCenter license for the hostname of “security”. This key allows that particular server to scan several networks, but as soon as 500 IP addresses are discovered, the license limit becomes active.

SecurityCenter generates a warning in the web interface if the license limit has been exceeded or is approaching capacity. Contact ACAS Customer Support for an expanded license key.

You will need to provide the hostname of the machine on which SecurityCenter will be installed. This can be obtained by entering the “**hostname**” command at the shell prompt.

SecurityCenter does not support an unlicensed “demo” mode – a license key is required.

Once installation is complete, the initial web interface will generate an upload form to add the license key.

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Disable any pop-up blockers for this interface, as they will prevent the license key upload interface from working correctly. |

## Nessus

Nessus is available to operate either as a subscription or managed by SecurityCenter.

ACAS is using Tenable’s SecurityCenter to manage your Nessus scanner, the Activation Code and plugin updates are managed through SecurityCenter. A license key is not required.

Nessus needs to be started to be able to communicate with SecurityCenter, which it will normally not do without a valid Activation Code and plugins. To have Nessus connect to SecurityCenter, select “Managed by SecurityCenter” at the Product Registration screen during the initial setup. Refer to the Nessus Installation and Configuration Guide to complete installation and configuration of Nessus.

## Passive Vulnerability Scanner

PVS is available for operation either as a subscription or managed by SecurityCenter.

ACAS is using Tenable’s SecurityCenter to manage the plugins and activation codes of PVS. PVS needs to be started to enable communication with SecurityCenter, which it will normally not do without a valid Activation Code and plugins. To have PVS ignore this requirement and start (so that it can get the information from SecurityCenter), input “SecurityCenter” (case insensitive) without quotes into the Activation Code box during setup. After starting PVS, SecurityCenter users have completed the initial installation and configuration of their PVS scanner.

Refer to the PVS User Guide for more information on Licensing and complete installation and configuration of PVS.

# Pre-Installation

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | In order to ensure audit record timestamp consistency between SecurityCenter and its external components, make sure that the underlying OS for SecurityCenter and all components are configured properly and enabled to use Network Time Protocol (NTP) as described in: <http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Date_and_Time_Configuration-Command_Line_Configuration-Network_Time_Protocol.html>. |

## License Request

Ensure you have an ACAS license key before you begin installing and using ACAS. See the “ACAS License Request Portal” section for more information.

## Disable Default Web Servers

SecurityCenter provides its own Apache web server listening on port 443. If the installation target already has another web server or other service listening on port 443, that service needs to be disabled on that port or SecurityCenter must be adjusted to use a different port after installation.

Confirm what, if any, services are listening on port 443 with the following command:

# **netstat -pan | grep ':443 '**

## Modify Firewall Settings

The default Red Hat firewall settings cause issues with SecurityCenter’s web services. To easily alleviate this, SELinux must be either set to “Disabled” or enabled in “Permissive” mode. You can disable SELinux “Enforcing” mode using the following steps:

1. Navigate to: **/etc/selinux**
2. Edit the file named “**config**”.
3. Change the SELINUX line from “**SELINUX=enforcing**” to “**SELINUX=disabled**” or “**SELINUX=permissive**”.
4. Save the file.
5. Reboot the system.

Ensure the following incoming services are permitted by the firewall rules:

* SSH (port 22 by default)
* HTTPS (port 443 by default)

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | Please consult local security and best practices within your environment for the proper usage and configuration of SELinux. SecurityCenter is known to work with SELinux in “Enforcing” mode with some customization of the SELinux rules. However, permitted rules vary from organization to organization. |

|  |  |
| --- | --- |
| 11769225_Caution_HiRes.png | For Red Hat 6 users, it is now considered a STIG requirement to have SELinux be set in “Enforced” mode (per RHEL-06-000020). |

## Log Rotation

The installation does not include a log rotate utility; however, the native Linux “**logrotate**” tool is supported post-installation. In most Red Hat environments, **logrotate** is installed by default. The following logs will be rotated if the **logrotate** utility is installed:

1. All files in **/opt/sc4/support/logs matching \*log**
2. **/opt/sc4/admin/logs/sc4-error.log**

During an install or upgrade, the installer will drop a file named “SecurityCenter4” into **/etc/logrotate.d/** that contains log rotate rules for the files mentioned above.

Log files are rotated on a monthly basis; these files will be owned by root/root.

# Useful links

## Certification and Accreditation Artifacts:

* Posted at ACAS SIPR Wiki: <https://www.intelink.sgov.gov/wiki/ACAS>

## ACAS TTP:

* Posted at: <https://powhatan.iiie.disa.mil/ttp/capability/capability.html>

## Approved documentation/binaries are located on DoD Patch Repository:

* Posted at: <https://patches.csd.disa.mil/CollectionInfo.aspx?id=442>

(CAC is required for access). Click on ACAS > ACAS Software > then whichever application you need. All of our latest Plugins files and Red Hat patches can be found here also.

## ACAS Homepage:

* <https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/Home.aspx>

## ACAS License Request Portal:

* <https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/requestPortal/LicenseRequest.aspx>

## ACAS Build 1 Request Portal:

* <https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/requestPortal/ACASBuild1.aspx>

## ACAS Approving POC list:

* <https://disa.deps.mil/ext/cop/mae/netops/acas/Lists/ACASLROrganizationPOCs/AllItems.aspx>

## ACAS Monthly Working Group page:

* <https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/ACAS%20Working%20Group.aspx>

## ACAS Front Door:

* <http://www.disa.mil/Cybersecurity/Network-Defense/ACAS>

## ACAS Customer Support/OKC Helpdesk:

* Toll-free: 844-347-2457 (Select options 1,5, and 4)
* DSN: 850-0032 (Select options 1,5, and 4)
* Email: [disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil](mailto:disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil)