ACAS Best Practices

October 31, 2017

V5.2

Table of Contents

Change Log

Date	Version	Changes
31-Oct-2017	5.2	• Scan policy changes • Clarify SCAP scan processes • Improve CTO scanning guidance • Added guidance for ephemeral assets
31-May-2017	5.1	• Change CTO 13-0670 to 17-0019 • Remove SecurityCenter 4 references • Added PVS guidance • Added STIG scanning guidance (SCAP and audit file) • Updated vulnerability and discovery scan policies
30-Jan-2017	5	• Added CTO Compliance Section • Major updates to support SecurityCenter 5 • Major updates to support Red Hat 6 • Added Appendix Q • Updates to Appendix A • Updates to Appendix C • Updates to Appendix K
17-May-2016	4	• Removed step-by-step scan policy creation steps • Updated Plugin feed locations • Updated Kickstart information • Updates to Appendix I • Updates to Appendix J • Updates to Appendix O • Updates to Appendix N

07-Mar-2016	3	• Major revisions to Appendix C:
		  ○ Added coverage for which OSes are supported for credentialed checks, some plugins which are noted for STIG conflicts, and some plugins which require manual review / analysis.
		  ○ Clarified network scanning to better address one of the issues with JUNOS devices
		• Added Appendix O
		• Added Error 500 section.
		• Added Troubleshooting Oracle False Positive Plugins section to Appendix D

29-Jan-2016	2	• Major revisions, including addition of Baseline Model in Implementation Guidance, new Appendices, reworking other sections, editing. • Removed Appendix on Scanning Performance Benchmarks

		• Corrected appendixes numbering scheme with the removal of the last Appendix • Added more information to Appendix K: Tenable Software Error Codes
23-Jun-2015	1	• Initial document creation.

Introduction

This document covers the basic high-level concepts of setting up SecurityCenter for the DOD community using a planning approach based on pitfalls that have been noticed in the field when deploying the ACAS tools.

This document is broken into three distinct parts:

1. Basic deployment, configuration, and usage recommendations
2. CYBERCOM TASKORDER 17-0019 Compliance
3. Individual guides to brief on specific topics, covered as appendices

Prior to deployment, ACAS administrators will need to work with their information assurance, network operations, and systems administration teams to ensure the fidelity and integrity of the data produced by the tool. There are many factors, which affect ACAS deployments including network topology, firewalls and other application aware network components, software deployments, and system credentials.

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/sc/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

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

Getting Started

The ACAS program contains a number of documents and guides. Each ACAS component generally has one or more guides. SecurityCenter has multiple role-oriented guides. All guides are available from the Patch Repository (Appendix A contains the URL); however, the ACAS Program Office recommends starting with the following documents prior to reading each individual guide.

- USCYBERCOM TASKORD 17-0019 - Please refer to the USCYBERCOM TASKORD 17-0019 for ACAS Implementation, which is available on the USCYBERCOM webpage (https://www.cybercom.mil CAC-enabled website).
- ACAS Kickstart Installation Guide – Installing the Red Hat Enterprise Linux operating system and the ACAS components of your choice
- ACAS PKE and CAC Implementation Guide – procedures to get the SecurityCenter, Nessus scanner, and PVS sensor PK enabled for CAC or SSL certificate logon
- ACAS-HBSS Integration Guide – configuration guidance for HBSS when installed on ACAS components and targets to be scanned
- SC 5 Publishing Guide - procedures for publishing vulnerability data to the Continuous Monitoring & Risk Scoring (CMRS) system

The other documents (SecurityCenter, Nessus, and PVS guides) have a lot of useful information, and should be reviewed when the site engages in configuration or troubleshooting. The documents are written primarily for the vendor's commercial customers who have different operational requirements & expectations. As the software is updated quarterly, users are encouraged to check for updates for any documentation held offline or pulled for local use.

It is recommended that all ACAS components be deployed on discrete hosts. In small environments (< 2,000 hosts), deploying two or three components on a single host may be feasible. The recommended hardware guidance is cumulative (example: SecurityCenter + Nessus requirements), if the site intends to perform a lot of analysis on the SecurityCenter, adding RAM, CPU, and improving HDD I/O performance will improve performance. Non-IA software should not be installed on systems hosting ACAS components.

Virtualization is fully supported; however, the guidance provided within the ACAS documentation is based on 'bare-metal' installations. The vendor recommends a 35% overage in CPU and RAM to accommodate loss due to virtualization. This number should be tailored to your environment; virtualization admins familiar with the organization's implementation should be able to provide recommendations that are more accurate.

Information about ACAS is generally available in three locations:

- **ACAS site on DEPS Portal** – This site contains general program information, license request portal, support, user forums, feature request form, and contact information.
- **Patch Repository** – This site contains software, documentation, plugin, and patches which are fully accredited.
- **Software Forge** – This site contains software in all stages of the software release lifecycle – from alpha to obsolete. The software here has been tested by the integrator or the vendor, but not necessarily tested by DISA (or approved for release to the DOD.)

ACAS Implementation Guidance

At least one SecurityCenter (SC) instance is required to manage the plugins being pushed to the Nessus scanner(s), and to publish data to CMRS or equivalent CYBERCOM reporting solution. Use of the Nessus web interface should be limited to initial setup, troubleshooting, and disconnected environments. Access to the Nessus web interface may be required for troubleshooting false findings.

Plugins for SecurityCenter can be downloaded automatically, or downloaded manually from the DOD Patch Repository. There are a few requirements for a SecurityCenter to connect to the plugin server:

- Configure the URL, as an SC admin, under System > Configuration > License: 'Plugin Site' and 'SC Feed Site'.
- Configure the SC root Certificate Authority (CA) Certificate trusts in SecurityCenter (guidance is available in the ACAS PKE and CAC Implementation Guide); this will enable the SecurityCenter to trust the SSL certificate identifying the plugin server.
- Ensure the public IP from which connections to the plugin server will originate have a valid PTR (pointer) record to ensure the connection can be identified via reverse DNS lookup as originating from a .mil source.

SecurityCenter runs solely on the Red Hat Enterprise Linux (RHEL). CentOS will work and is tested by the ACAS integrator and vendor; however, it is not part of the accredited baseline (testing is not performed with Oracle or Scientific Linux), so support to the field will be limited to Red Hat. Customers must purchase and use Red Hat support for their servers, unless an enterprise agreement is already in place for your organization. Legally, an entitlement (license) is required to use the operating system. The system will functionally operate without an entitlement but the organization will be in violation of the user agreement.

DISA does not provide any operating system licenses. It is the responsibility of the deploying organization to purchase the Red Hat Enterprise Linux entitlement(s) prior to the deployment of ACAS. Connection to the DISA provisioned Satellite servers will also require a Smart Management license.

- Re-licensing the SecurityCenter application will result in system downtime and may require several maintenance tasks. Scope your SecurityCenter license at least twice the quantity of your expected IP range to avoid this downtime and maintenance.
- During SecurityCenter installation, no 'Maintenance License Code' is required for any ACAS component.
- LCE plugins download schedule should be set as never. You can edit this on the Administrator's interface (System > Configuration > Update). …Log Correlation Engine (LCE) is not included in the ACAS license; it can be procured directly from the vendor at a cost, and will operate properly with ACAS-licensed SecurityCenter instances.
- Guidance for configuring a RHEL 6 ACAS kickstart server to pull updates from the DOD Satellite server is yet to be defined. More information will be posted when details are final.

Red Hat offers training and certification opportunities specific to this Linux distribution, while CompTIA and the Linux Professional Institute offer training and certification which is vendor-agnostic, but still helpful for Red Hat Enterprise Linux.

Baseline/Model Implementation

Purpose

This section is designed to provide the high-level overview of how the Assured Compliance Assessment Solution (ACAS) baselines are created. It will give you the starting points needed to stand up the operating systems that eventually will have ACAS installed upon them. It will guide you through the creation of a server that matches the configurations used during Defense Information Systems Agency's (DISA's) certification and accreditation processes.

Approved images are available on the DOD Patch Repository (DOD PKI Certificate Required). The DOD Secure Host Baseline Repository includes images for the Windows baselines. Newer versions may be available for testing and evaluation on Software Forge .

Operating Systems:

1. **Windows Baselines -** The Windows operating systems used were built using Department of Defense (DOD) images obtained from the Information Assurance Support Environment (IASE) website.

    a. Secure Host Baseline Windows 7 x64
    Model: WIN7.0.03
    b. Secure Host Baseline Windows 2k8 R2 x64
    Model: 2008.R2.02
    c. Secure Host Baseline Windows 2k12 R2 x64 (being reviewed for accreditation)
    Model: 2012.R2.01

2. **Linux Baselines -** The ACAS Kickstart images were built from the following Red Hat operating systems:

    a. RHEL 6 x64
    Model: Kickstart version 17.05-0
    Build date: 2017May18
    ACAS RPM: acas_configure-17.05-0.noarch.rpm

Unique Configurations

Once the operating system is installed, there will be further configurations needed to mirror the ACAS baselines. The ACAS baselines are compliant with the latest Security Technical Implementation Guides (STIGs) and patched to-date with the latest vendor provided patches.

Each baseline has its own configurations that cannot be determined for every scenario. These we referred to as "Site Responsibility" and guidance has been provided on how they should be implemented.

Please refer to the ACAS Site Responsibility Guide (link provided in Appendix A).

Installation of ACAS Tools

Please refer to the appropriate guides of each ACAS tool, for instructions on installation and configuration of the individual tools.

Approved software and documentation is found on the DOD Patch Repository (link can be found in Appendix A).

The current baseline is posted on the ACAS DEPS site, at the link in Appendix A: Important URLs. This information is updated by the ACAS program manager based on the ATO issued by DISA for reciprocity. Each CC/S/A may further refine the baseline, or maintain an additional approval cycle before software should be used in the field.

Ideally, rebuilding the tools from scratch is cleaner for new installations, and reduces the risk of corruption when backups and restoring is involved. Sometimes, it makes more sense to start over when it comes to SecurityCenter. SecurityCenter 4.8 included a major change in the way users and groups were used. The majority of users migrated their SecurityCenter 4.7 installations to the new user/group model in SecurityCenter 4.8, and found that a different organizational model made more sense. In SecurityCenter 5, a major change comes in the repositories. With repositories having a capacity of 32 GB, you may find that you do not need as many in your deployment. Take a fresh look at the need of your organization and the features

the tools offer, combine them with the lessons learned from your organization and throughout this document to plan an ACAS deployment that fits your needs.

Sizing ACAS Solution

SecurityCenter Deployment Considerations

Each organization/site will need to run at least one SecurityCenter for each classification, and for any operationally air-gapped network. The basic hardware guidance is located at the DEPS Portal Site in Appendix A. This describes SecurityCenter's minimum requirements for hardware, network, and disk storage. Note that the particular needs of your organization must be factored into this guideline. 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.

Many functions within SecurityCenter can affect performance significantly. This is the basis for the guidance limiting the number of Repositories, Asset Lists, and Users. This is based on how the application parses data (who can see what data in what repositories, and which hosts belong in which asset lists).

Scan tasks, reports, and dashboards all require RAM and CPU allocations while they run. As a result, many of these tasks will cause the system user interface to be slower while they are running. Moving reports or scan jobs to after-hours will minimize their impact to the logged in user. The system administrator should periodically review the scheduled tasks to ensure users are not scheduling multiple tasks for the same time. The SecurityCenter does try to distribute tasks that are scheduled to occur at the same time. However, it may tax the Nessus scanner implementation if too many scan jobs are scheduled for the same time (3+ jobs). Work with customers to ensure there are at least 15 minutes between the start of any two scan-jobs. Concurrent scan jobs may adversely affect performance, the actual performance impacts of concurrent jobs is dependent upon system hardware, and network topology, configuration, and utilization. Additional guidance is available under Appendix F, Performance Tuning.

Each dashboard component is the product of a query of scan data in the repositories. Having a single user develop and share dashboards is more efficient than having individual users create or share their own. Similarly advising users to configure dashboards with daily or slower multi-hour updates can lessen the net impact of the number of dashboards being used.

There is no reason to have a dashboard update any more frequently than the underlying data changes. For example, if the data being shown in the dashboard component is coming from a monthly scan, the component should probably be set to refresh monthly, at a time after the scan is expected to complete.

If the data were coming from the PVS every hour, then hourly or every few hours would be appropriate.

Hardware requirements

Please see the tables for SecurityCenter, Nessus, and PVS hardware requirements at the DEPS site listed in Appendix A.

In addition to the guidance posted on DEPS, please consider the following suggestions:

- Use the aggregate of the individual software resource requirements for determining total hardware system requirements. For example, If Nessus or PVS is deployed on the same server as SecurityCenter, there will be less CPU and memory available during scans, causing slower performance.
- For deployments of SecurityCenter with more than 25 active users, adding additional memory or Central Processing Unit (CPUs) can improve performance.
- As more Passive Vulnerability Scanners are used, consider additional processor cores to increase performance.
- There is no hard limit on the number of scanners (Nessus or PVS), as the number of scanners is increased, SecurityCenter performance may be hindered. Additional resources may offset additional scanners.

Please research your VM software vendor for comparative recommendations as VMs typically see up to a 35% loss in efficiency compared with dedicated servers.

Nessus Scanner Deployment Considerations

One of the primary design considerations with ACAS and active scanning is identifying the best location for scanners and determining the number of scanners required for a given portion of the network or number of hosts.

There is no one right way to deploy Nessus scanners. Two primary deployment models are distributed and consolidated. Each model has its advantages and disadvantages. A single deployment may use both models.

- The distributed model is recommended for geographically distributed organizations so that scanners can be placed at remote locations located close to the targets they are configured to scan.
- The consolidated model is better for larger campus or datacenter environments so that a number of scanners located at a cental location can interrogate a large number of targets and shorten scan windows.

Some considerations:

- Does deploying a scanner to a site with < 50 hosts make sense?
- Does deploying a large number of scanners within firewalled subnets make sense?
- Ten centrally managed scanners may be able to interrogate a large number of targets regionally or even globally, but data fidelity may be diminished.

Specific hardware guidance is available within the General Requirements Guide. Nessus is designed to consume as much as possible of the available resources to accomplish scanning tasks as quickly as possible. More CPU, RAM, and faster HDD storage can improve performance. However, the network is a major factor in scanning performance.

Bandwidth availability and latency can have serious impacts on scanner performance. Scanning can easily overload networks that are at or near capacity. The hosts that are being scanned will also affect performance. Hosts with more vulnerabilities will take longer. Hosts with less processing capabilities or high utilization will take longer.

- Do not scan more than 2500-5000 (depending upon the number of scanners and hardware configuration) hosts in a single scan job. As the number of hosts in a scan job increases, the performance of the scan job decreases. A single large scan job can be broken into multiple scheduled jobs (requires manual effort and optimization) or set as dependent scans (automatic, but will not be run if the earlier scan failed)
- A scanner should not be assigned multiple scan zones. This can be done in the UI; however, it has been known to cause performance and availability issues. IP ranges within a scan zone can overlap, overlapping scan zones may slow overall performance, this is generally insignificant, but eliminating overlap may provide some performance improvements.
- Exercise care when deploying HBSS or any other security software (AV/HIPS) on the Nessus scanners. The Nessus scanner is designed to forge network packets and other tasks that will look malicious to most security software. Plugin update failures, slow or inconsistent scans have been reported when security software is inspecting the files or network connections from Nessus.
- Security software logs are helpful but not concrete. You may experience issues if HBSS (or equivalent) is not properly configured and no errors, quarantines, or drops will be reported to the ePO console. Guidance for configuring HBSS is available in the ACAS HBSS Integration Guide.
- If you use anything other than HBSS (Symantec Endpoint Protection for example), you need to assume responsibility for understanding the configuration delta may cause unexpected scan results. This is true of any security software installed on the targets or the scanner.
- Where possible, a scanner should be configured with two (or more) interfaces. One interface for connectivity from SecurityCenter or browser for administration, and one (or more) interface for interrogating production data networks.

In an ideal deployment, Nessus would be deployed adjacent to the targets it is responsible for interrogating, with no firewalls or other devices between the scanner and the target. This is rarely an option, and in most cases, the expected configuration is scanning across one or more routers connecting Local Area Networks (LAN). Scanning via Wide Area Network (WAN) or through a firewall can be done but requires scan policy tuning, firewall, and host configurations.

SecurityCenter connects to Nessus via the Extensible Markup Language Remote Procedure Call (XML-RPC) protocol over HTTPS on port 8834. This connection is often slow so using two firewall rules is recommended:

`<securitycenter ip>:<ephemeral port>` → `<nessus ip>:8834`

`<nessus ip>:8834` → `<securitycenter ip>:<ephemeral port>`

If the Nessus scanner is connected via WAN circuit, it may require extending the scanner timeout setting on the SecurityCenter. This configuration is per SecurityCenter and affects all scanners. This setting can be modified via the `setTimeout.sh` script provided with the Kickstart. This connection can be managed / limited via Quality of Service (QoS) rules similar to the way other HTTPS applications can be managed, but the application has rather limited timeout settings. If a situation occurs that may require sub-optimal scanner deployments refer to the Appendix E, Complex Scanning Situations, section for help ensuring the accuracy / integrity of your scan results.

Note: To support limited bandwidth environments, Nessus scanners may be detached from SecurityCenter (i.e., scans may be initiated from a Nessus scanner that is not currently connected via network connection to SecurityCenter). When possible, the Nessus scanner must receive updates and plugins only from SecurityCenter and the results from the detached Nessus scanner are exclusively uploaded to SecurityCenter (Due to contractual obligations, Nessus scanner results may only be exported to other applications via SecurityCenter).

Nessus Hardware requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Nessus deployments include raw IP count, and the configuration of the Nessus application. All approved versions of Nessus software, as well as the documentation, can be found on the Patch Repository (link provided in Appendix A). There is no specific configuration, which can be assured to scan a set number amount of hosts per hour. A basic average is that a scanner can enumerate a dead / unused IP address in 1-3 seconds, and will scan a live target in 30-40 minutes. The overhead associated with handling chunks of the job add about 30-50% to the total duration.

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.

Nessus can be run under a virtual environment, 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.

Please research your VM software vendor for comparative recommendations as VMs typically see up to a 35% 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.

Enterprise scanners within a scan zone should be configured with similar/identical hardware; this will help minimize performance gaps between scanners as chunks are being handled during an active scan.

In general, if scans are taking too long to complete, it may be wise to evaluate adding an additional scanner instead of improving the hardware on a single scanner.

Passive Vulnerability Scanner Deployment Considerations

The Passive Vulnerability Scanner (PVS) uses a promiscuous interface to monitor traffic and enumerate vulnerabilities on the network. This presents specific requirements on how to get the data into the scanner. Routing the data into the scanner is done the same way data would be sent to an IDS or network sniffer. The primary difference is accuracy requirements for PVS are much lower.

The data PVS gathers is highly repetitious. Information about web server version is relayed in the initial response from the service. The same response may be sent to 500 clients, but once PVS observes the first connection, the other responses are irrelevant. The situation is similar for clients as well. A web browser sends a user agent with every request it makes. The user may connect to 100 web servers during the course of the day, but as long as PVS records the user agent once, the browser will be enumerated. Additional deployment guidance is available under Network Topology Considerations for PVS.

PVS Hardware requirements

Hardware guidance is available in the PVS User Guide. PVS functions by tracking connections in memory and then writing them to an XML-formatted file for SecurityCenter to ingest. The system resources are highly dependent upon the volume (bandwidth) of monitored traffic as well as the number of hosts that are monitored.

If Nessus and PVS are installed on the same host, PVS results may not be available when Nessus scanners are running.

PVS 4.0 adds an XML-RPC over HTTPS web interface on port 8835, the site should ensure SecurityCenter and admin workstations are able to connect to this port.

PVS versions prior to 4.2 are not able to reliably parse more than 1 Gb/s of data. PVS 4.2 can parse more than 1 Gb/s of data. A special license and specific hardware are required for PVS 4.2.1 and greater to fully parse 10 Gb/s of data (not included on the ACAS contract).

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. For more guidance on the PVS installation, please reference Appendix B: Network Topology Considerations for PVS.

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.

Please research your VM software vendor for comparative recommendations as VMs typically see up to a 35% 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.

Scan data is collected from the PVS sensor on a configurable schedule. This is configurable by a SecurityCenter administrator. The default 'Results Pull Interval' is one hour. When bringing PVS sensors online, it is important to observe the impact on the SecurityCenter when PVS results are uploaded and parsed (Dynamic Asset Lists are recalculated after every scan job and every time PVS results are pulled).

SecurityCenter connects to PVS via XML-RPC over HTTPS on port 8835. This connection uses a single port and can be managed / limited via Quality of Service (QoS) rules similar to the way other HTTPS applications can be managed. This connection is often slow so using two firewall rules is recommended:

<securitycenter ip>:<ephemeral port> → <pvs ip>:8835

<pvs ip>:8835 → <securitycenter ip>:<ephemeral port>

User Management

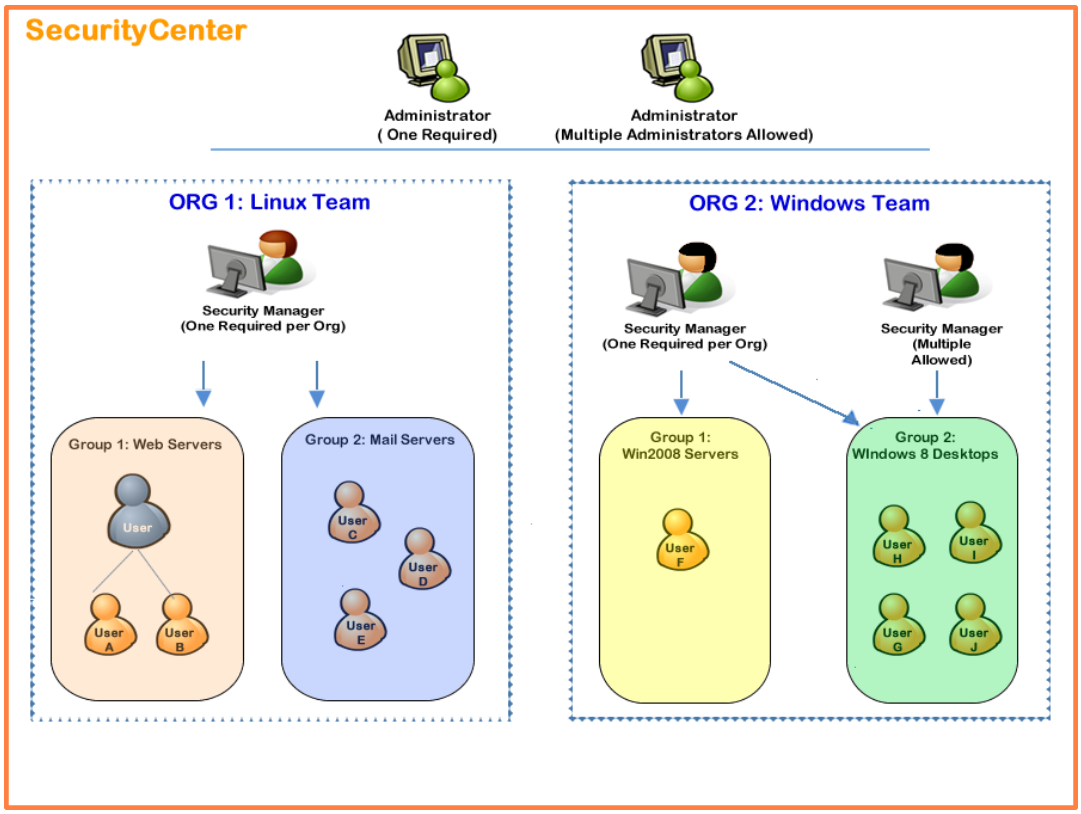
SecurityCenter user accounts are assigned roles and groups to determine the level of access they have; and may be assigned assets, depending on the level of access required. The list of users and actions is limited to the Organization and the permissions of the user viewing the list. It is best to take your time and develop a strategy for managing user accounts. Most DOD locations only need to have certain functions. With careful planning, the Organization can be built out only using a small amount of the roles provided below. The goal is to keep a small user set along with reusable asset list and a small concise repository set. This will allow the Security Center the ability to run more efficiently.

Organizations

Organizations are groups of users that are responsible for specific sets of assets. Organizations are assigned repositories and scan zones. “Users” refers to any non-administrator login account on SecurityCenter. “Zone” means that each Organization is made up of the systems within one or more IP networks.

Multiple Organizations can share the same repository; and the vulnerability data associated with the overlapping ranges will be shared between each Organization. Conversely, Organizations can be configured with their own discrete repositories to facilitate situations where data must be kept confidential between different organizational units.

The Organization is managed primarily by the Administrator and Security Manager users. The Administrator is responsible for Organization and Security Manager creation, as well as maintenance of scanners and scan zones. Users within the Organization are created by the Security Manager user or any user with the “Manage Users” permissions. User management is inherited and not-strictly hierarchical. For example, consider the diagram below:



It is important to consider these concepts when working with the predefined roles and creating custom roles as they relate to your DOD organizational structure.

Roles

SecurityCenter users can be created with default or customized roles. Roles are adjustable and allow for user creation based on specific business/security models and needs. User accounts created by other users inherit the creating user's permissions or a subset of the permissions as desired while not exceeding the access or permissions of the creating user. This granular user control and customization enables large organizations to comply with regulations and standards that mandate separation of duties and layers of control. It is not necessary to use all roles. Some agencies may want to build customer roles for their user population. These customer roles can be a combination of the standard roles that are built into the SecurityCenter.

Be careful assigning roles to users. Spending the time up front in analysis to design the users, roles, and groups that you need will reduce the need to fix problems later.

Roles and Descriptions:

- **Security Manager** - The Security Manager role has full access to all actions at the organization level. A Security Manager has the ability to create new groups and manage existing ones. A Security Manager can also define how users interact with other groups.
  The ability to manage other users and their objects can be configured using group permissions on the Group Permissions section of User add/edit. This includes viewing and stopping running scans and reports.
- **Security Analyst** - The Security Analyst role has the permission to perform all actions at the organizational level except managing groups and users. A Security Analyst is most likely an advanced user who can be trusted with some system-related tasks such as setting blackout windows or updating plugins.
- **Vulnerability Analyst** - The Vulnerability Analyst role can perform basic tasks within the application. A Vulnerability Analyst is allowed to look at security data, perform scans, share objects, view logs, and work with tickets.
- **Executive** - The Executive role is intended for users who are interested in a high-level overview of their security posture and risk profile. Executives would most likely be browsing dashboards and reviewing reports, but would not be concerned with monitoring running scans or managing users. Executives would also be able to assign tasks to other users using the Ticketing interface.
- **Credential Manager** - The Credential Manager role can be used specifically for handling credentials. A Credential Manager can create and share credentials without revealing the contents of the credential. This can be used by someone outside the security team to keep scanning credentials up to date.
- **Auditor** - The Auditor role can access summary information to perform 3rd party audits. An Auditor can view dashboards, reports, and logs but cannot perform scans or create tickets. Restricting access to vulnerability and event data can be achieved by placing the user in an appropriately configured group.
- **No Role** - This role is available as a catchall role if a user is deleted. It has virtually no permissions.

Role Permissions

Within the defined roles, granular permissions are applied that enable users assigned to that role to perform various tasks.

The table below defines the various permissions available within the SecurityCenter architecture:

Organizational Task Privileges

Permission	Description	Security Manager	Security Analyst	Vulnerability Analyst	Executive	Credential Manager	Auditor
Scan Privilege: No Scan	Cannot create scan jobs				X	X	X
Scan Privilege: Policy Scanning	Can create scan jobs, but must use a scan policy. Cannot create plugin scans or launch remediation scans						
Scan Privilege: Full Scanning	Can create scan jobs using either scan policies or a single plugin. Can launch remediation scans	X	X	X			
Upload Nessus Scan Results	Can upload `.nessus` files into SC from the Scan Results screen	X	X	X			
Create Audit Files	Can create (upload) Audit files for compliance scanning	X	X	X			
Create Policies	Can create (add) Scan policies	X	X	X			
Manage Blackout Windows	Can create/edit/delete blackout windows for their organization (Regardless of whether they created the blackout window themselves)	X	X	X			
Create LDAP Query Assets	Can create the LDAP type of asset lists	X	X	X			
Accept Risks	Can mark vulnerabilities as "accepted"	X	X				
Recast Risks	Can recast (change severity levels of) vulnerabilities	X	X				
Share Objects Between Groups	Can share objects (dashboards, scan results, asset lists, credentials, queries, scan policies) with other groups/users* in the same organization. *Some objects are shared at the group level, while others are shared at the individual user level.	X	X	X		X	

Permission	Description	Security Manager	Security Analyst	Vulnerability Analyst	Executive	Credential Manager	Auditor
	** This permission option does not affect the ability to share report results						
View Organizational Logs	Can view organizational logs: Path: **System** > **Logs**	X	X	X			X
Manage Roles	Can create organization-specific roles; limited to only the permissions that they, themselves have.	X					
Manage Groups	Can create new groups within their organization	X					
Manage Group Relationships	Can assign group permissions (Manage Objects, Manage Users) to other users. **Note:** User's must also have the Manage Users option selected in their own user definition in order for this role-based permission to be active for them.	X					
Manage Images	Can add/edit/delete watermark images **Note:** Header/Footer image options are not enabled in ACAS in order to support classification banners within the ACAS application.	X	X				
Manage Attribute Sets	Can add/edit/delete attribute sets for their organization (Regardless of whether they created the blackout window themselves)	X	X				
Update Feeds	Can upload plugins Can update plugins Can update SC feed (templates)	X	X	X			

Permission	Description	Security Manager	Security Analyst	Vulnerability Analyst	Executive	Credential Manager	Auditor
Purge Tickets	Can purge closed tickets from the system	X	X				
Create Alerts	Can add/edit/delete alerts. **Note:** An individual's ability to edit/delete objects owned by others is affected by the Manage User's settings in the user definition for that user.	X	X	X			
Create Tickets	Can add/edit/resolve/close tickets **Note:** An individual's ability to edit/resolve/close tickets owned by or assigned to others is affected by the Manage User's settings in the user definition for that user.	X	X	X	X		

Note: This table only addresses functionality that can be enabled/disabled. It does not address other functionality that is inherently available to all organizational users, for example: creating credentials, saving queries, running reports, and others.

Groups

User Groups are a way to predefine a specific set of permissions within an Organization for quick assignment to one or more users. When a user creates various objects such as reports, scan policies, dashboards, and other similar items, the objects are defaultly shared among the members.

Be careful assigning users to groups. Spend the time up front to design your groups, rather than fixing the mistakes later.

The first group created by default within every organization is the Full Access Group. This may be the only group needed in an organization. If you need to subdivide users, based on their access rights to assets, you can create multiple groups. When creating a new Group, assign a name and description of the Group being created. Then identify the Repositories, Viewable IP addresses, as well as shared Assets, Dashboards, Credentials, Policies, and Queries.

After the Group's initial creation, it may be edited, deleted, or have its details viewed from the main Groups page list.

Please refer to the ACAS SecurityCenter User Guide for more detail on setting up users and groups for DOD. Links to the User Guides and all documentation can be found in Appendix A.

The User/Organizational visibility construct has been replaced by the new Group model. Users within a group will be able to see/use each other's objects.

Asset Lists within ACAS

Each organization within a SecurityCenter maintains its own asset lists that identify logical groupings of IP addresses. Asset lists are not visible between organizations. You can group hosts/addresses into Asset Lists that are defined either statically by IP address, or dynamically rules-based criteria. They can be grouped by department or operating system, or whatever you wish, as long as SecurityCenter has access to the criteria. The categories of asset lists you can create are virtually limitless; however, be aware that creating too many asset lists is not an efficient practice and may become difficult to manage across the organization.

Asset lists can be shared within the group. It is recommended to share asset lists to reduce the ACAS system resource management. Security Managers need to monitor what users are creating if they have permission to create asset lists.

Five types of asset lists used by the ACAS system are:

Static lists (IP Addresses) can be inserted manually or uploaded in bulk via text files:

- Grouping machines that do not have common factors among them
- Grouping machines that do not have a unique factor
- Machines that change configuration, but are treated the same

Dynamic lists are computed based on the rich content of the vulnerabilities discovered by Nessus and the PVS. Templates are available, and some are predefined, including:

- Systems with Software Inventory
- Exploited by Malware
- Windows Computers

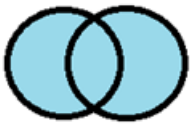
DNS Names

- List of hosts by DNS name

LDAP Query example is below

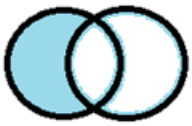
- Organizational information such as "DC Disa.mil"

Combination Asset Lists



SC4.x Union - Combines addresses from selected assets on the right with addresses on the left, removing duplicates.
SC5.x Combination - "Asset Left" OR "Asset Right"

SC4.x Intersection - Removes all addresses from the left that are not present in the selected asset lists on the right.
SC5.x Combination - "Asset Left" AND "Asset Right"



SC4.x Difference - Combines addresses from selected assets on the right with addresses on the left, and then removes any addresses that were in both.
SC5.x Combination - "Asset Left" AND NOT "Asset Right"

SC4.x Complement - Removes all addresses from the left that are present in the selected assets on the right.
SC5.x Combination - ("Asset Left" OR "Asset Right") AND NOT ("Asset Left" AND "Asset Right")

Recommended Repositories

In SecurityCenter 5 and greater, scan data is stored in proprietary data file format called a repository. Each repository can grow to 32GB in size. SecurityCenter does not limit the number of repositories it can use. However, the total number of repositories is a significant performance factor. Different filesystem options are available to Red Hat Enterprise Linux, and have different limitations of the maximum partition size and maximum file count.

DISA recommends three separate repositories to hold the following types of data (naming conventions should be planned as you design your SecurityCenter):

- Credentialed (IAVA, patch level checks) scan data
- Non-Credentialed (Network Check, socket level checks) scan data or ad-hoc scans
- Compliance scan data

SecurityCenter 5.4 resolves many situations where uncredentialed data would lead to false mitigation of credentialed scan findings. Separating credentialed and uncredentialed vulnerability scan data is still recommended to ensure scan data is accurate and clear.

Repositories can contain only, mobile device management (MDM) data, IPv4, or IPv6 addresses. Therefore, it is necessary to have a separate Repository for each IP addressing scheme.

Operationally, it often makes sense to store vulnerability (IAVA) and compliance (STIG) data in separate repositories. Splitting host data between multiple Repositories provides for more hosts per Repository. (This is a recommendation, not a requirement.) Any number of additional Repositories can be created for the Organization based on business cases or other metrics. If the site intends to use more than one compliance (STIG) benchmark per host, it may be preferable to use a separate repository for the extra compliance data.

Previous guidance was to separate vulnerability from compliance data. This was based on a requirement of the xTool component, which has been deprecated with the introduction of SecurityCenter 4.8. Separating compliance and vulnerability data has the advantage of allowing each repository to hold scan data for more targeted IP addresses. The disadvantage is that it complicates dynamic asset lists, and requires more data storage (a number of plugins should be executed alongside of compliance scans to enumerate OS type, hostname, and media access control (MAC) address).

Depending upon the site, storing PVS data in a separate repository may be advantageous. Conversely, having the PVS write to the same repository that Nessus is using will make cross-correlation between the two data sets easier.

Remote Repositories (Repository Replication)

Remote repsositories can allow a central SecurityCenter to analyze and perform reporting aginst data copied from other SecurityCenters. When a SecurityCenter copies a repository from another SecurityCenter, it is identified as a Remote Repository. No data can be written into a Remote Repository.

Repository replication does not use compression, nor does it perform a differential or incremental copy of the data stored within the repositories. This means up to 32 GB of data will be copied during each sync for each remote repository.

Each SecurityCenter functions as a single system and has its limitations. If a site determines that two SecurityCenter servers are required, using repository replication to create a unified reporting solution should be approached with caution. Replicating all of the scan data from two SecurityCenter servers, which are at capacity into a single SecurityCenter, is unlikely to be successful.

For more detail on setting up repositories, see Appendix A for a link to the ACAS Repository Guide.

CYBERCOM Tasking Order (TASKORD) 17-0019 Compliance

The ACAS SecurityCenter is dependent on the Nessus and Passive Vulnerability Scanner to provide scanner results to SecurityCenter. In the DOD, every network is different, and tuning your Nessus scan policy can yield great results. It is important to plan how you are going to stage scanning so you do not saturate the network or the asset being scanned.

SecurityCenter 4.8 went End-of-Life March 2017. Organizations running SecurityCenter 4.8 should refer to the FSO-authored TTP, as this section is intended to be used with SecurityCenter 5.x.

Identify organizational / site IP space and assets

This section refers to organizational / site assets, as those assets that are within a single accreditation boundary, or a distinct-subset that is recognized by the CC/S/A or by the CC/S/A's CYBERCOM representative (directly or indirectly). The use of these terms, "organization" and "site" should be interpreted as appropriate.

Global IP Space Documentation

Each site must identify, document, and scan 'All hosts, IP addresses, and IP ranges which are owned, operated, managed, or maintained by a DOD entity to conduct or support operations, including all external contractor/vendor assets residing in a DOD enclave'. Each organization / site will maintain a master Asset List covering the organization / site IP space as defined by CC/S/D to include all assets, signed by Network Operations team(s) and ISSM. However, if the organization maintains multiple SecurityCenter servers, they will maintain Asset Lists on all organizational SecurityCenter servers which includes the portion of the organization's IP space the SecurityCenter is responsible for. A sample Network Address Declaration (NAD) form is posted on the patch repository. This NAD is the standard form expected by the DODIN RSI during inspection, other auditors may utilize different documentation.

Program of Record IP Space Documentation

All Program Managed (PM) or Program of Record (POR) assets should be identified within DITPR (https://ditpr.DOD.mil/) and documented on the NAD or equivalent. The organization will create an Asset List for each program of record that is not maintained by the organization. Each asset list will uniquely identify the program(s) and all associated assets. Asset lists will be prefixed with 'PM-', 'POR-', or other organizationally defined identifier.

Similar asset list (DITPR identification, and NAD documentation) should be maintained for Tenant organizations, if those organizations are responsible for their own security posture and CYBERCOM IAVM reporting. Each asset list will uniquely identify the tenant(s) and all associated assets. Asset lists will be prefixed with 'Tenant-', or other organizationally defined identifier.

Ensure SecurityCenter and Nessus configurations

The site must ensure plugins are kept current, for sites connected to the NIPRNet or SIPRNet daily automatic downloads of Active, Passive, and SecurityCenter Feeds should be scheduled to occur at night, before local work hours.

Required SecurityCenter Configurations

Security Settings (System > Configuration > Security)
Session Timeout: 60
Maximum Login Attempts: 3
Minimum Password: Length 15
(SC 5.5+)Password Complexity: enabled ***read SC5.5 release notes, PKI accounts will be locked***
Startup Banner Text: Organization / Site defined text (server name recommended)
Classification Type: Closest classification available
(if available) Allow Session Management: enabled
(dependent upon Session Management) Session Limit: Any value greater than 4
(SC 5.5+) Disable Inactive Users: enabled
(SC 5.5+) Days Users Remain Enabled: 35
Login Notifications: enabled
(if available) FIPS 140-2 mode: FIPS Configuration ON

Feed Download Schedules (System > Configuration > Plugin/Feed Configuration)
SecurityCenter Feed: Daily, unique Organization / Site defined time
Active Plugins: Daily, unique Organization / Site defined time
Passive Plugins: If PVS is being used, daily, unique Organization / Site defined time
Event Plugins: Never, unless organization / site has their own LCE license

Schedules (System > Configuration > External Schedules)
Pull Interval1: >= 1 Hour
IDS Signatures: Never
Correlation Database: Never

Disable default admin account

Create one or more admin account(s), log in as an admin. Select Users > Users, find account with username 'admin', click on the account and enable the 'Account Locked' switch. Alternatively, permanently delete the account by clicking on the gear icon to the right of the account, and select Delete.

Ensure the organization has two or more admin accounts, and no account usernames are common or default names (admin, administrator, root, toor, user, username, or any other questionable name).

For organization's which cannot automatically download feeds:

- Active plugins should be updated daily, each workday (plugin updates are uncommon on the weekend). Active plugins must be updated within 24 hours before CTO compliance scanning.
- SecurityCenter feed should be updated weekly, and no less than monthly or 24 hours before CTO compliance scanning.
- If the site has PVS sensors deployed, passive plugins should be updated weekly.

Admins must check to verify updates in logs

ACAS scan data is only as up-to-date as the plugins that are being used for scanning. Each SecurityCenter administrator must check the logs on the same interval (preferably daily) plugins are updated on the SecurityCenter, and ensure the scanners are updated as well. Logs can be filtered when logged in as an admin, click on System > System Logs, apply a keyword filter "pdate". Below is an example search string to look for SecurityCenter plugin update tasks from the RHEL command line:

```
# grep "Update|"  /opt/sc/admin/logs/$(date +'%Y%m').log | grep -E "$(date
+'%d %b %Y')|$(date -d '-1 day' +'%d %b %Y')"
```

Looking for update failures and timeouts for communication with the scanners is also important

Scan zones / repository cover (all ip/assets)

The organization will be able to demonstrate that the configured Scan Zone(s) cover the organization's entire IP space. Each Nessus scanner should be assigned to one scan zone. IP space can overlap between Scan Zones; however, overlapping IP ranges may degrade performance.

The organization should provision Nessus scanners and Scan Zones, to ensure the organization can scan all of their assets in 48 – 72 hours (2-3 days). During audit / inspection, the review staff generally has only one week to evaluate the assets on the network, analyze the data, and report their findings. If the site is unable to scan all assets in 72 hours, the reason for the shortcoming should be identified and documented with the Authorization Official (AO).

Repository coverage (vulnerability isolation)

The organization will be able to demonstrate that the configured Repositories cover the organization's entire IP space. If IPv6 repositories are not being used, the site should be able to demonstrate that IPv6 is disabled throughout the organization.

Document scanner settings (rules etc…)

Some configurations are set at the Nessus or PVS sensor. These configurations may be more difficult to track in an enterprise situation where Nessus scanners may be geographically dispersed or under the control of disparate teams or commands. Each organization should work up a process for defining a baseline configuration and validating adherence to it.

Nessus Scanner Settings

SecurityCenter/ACAS administrator will semi-annually validate the Nessus scanner version(s). In the SecurityCenter web UI, Resources > Nessus Scanners, verify values listed in the 'Version' column are ACAS PM recommended or compliant with the current CYBERCOM TASKORD. Nessus administrators will report to the ISSM any configuration changes within 30 days of configuration change.

The nessus configurations are best reviewed from the command line:
Linux:

```
# /opt/nessus/sbin/nessuscli --list
```

Windows:

```
# …\Program Files\Tenable\Nessus\nessusclie.exe fix --list
```

…The command can be augmented with | grep "keyword" on Linux or | findstr "keyword" on Windows.

```
report_crashes: no
user_max_login_attempt: 3
xmlrpc_idle_session_timeout: 10
acas_classification: CLASSIFICATION // FREE-TEXT CAVEAT
login_banner: You are accessing a U.S. Government (USG) Information System
(IS) that is provided for USG-authorized use only. By using this IS (which
includes any device attached to this IS), you consent to the following
conditions:\nThe USG routinely intercepts and monitors communications on this
IS for purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.\nAt any time,
the USG may inspect and seize data stored on this IS.\nCommunications using,
or data stored on, this IS are not private, are subject to routine
monitoring, interception, and search, and may be disclosed or used for any
USG authorized purpose.\nThis IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\nNotwithstanding the above, using this IS does
not constitute consent to PM, LE or CI investigative searching or monitoring
of the content of privileged communications, or work product, related to
personal representation or services by attorneys, psychotherapists, or
clergy, and their assistants. Such communications and work product are
private and confidential. See User Agreement for details.
min_password_len: 15
listen_address: Site/Organization defined value, except "0.0.0.0"
safe_checks: yes
ssl_cipher_list: strong
nasl_no_signature_check: no
rules: /opt/nessus/etc/nessus/nessusd.rules …other value must be documented
disable_ntp: yes
```

The organization will document and semi-annually audit the nessusd.rules file and SecurityCenter's Nessus user account (the account used by SecurityCenter to connect to the Nessus scanner) rules file. The following files should be subject to file integrity monitoring:
Linux:

```
# /opt/nessus/etc/nessus/nessusd.rules
# /opt/nessus/var/nessus/users/<SecurityCenter's Nessus user>/auth/rules
```

Windows:

```
# …\ProgramData\Tenable\Nessus\conf\nessusd.rules
# …\Users\All Users\Tenable\Nessus\conf\nessusd.rules
# …\ProgramData\Tenable\Nessus\nessus\users\<Nessus User>\auth\rules
```

The ACAS Kickstart configuration scripts set AIDE to monitor /opt/nessus/etc/nessus/nessusd.rules, but do not configure AIDE to monitor any user rules files. This will be addressed in a future release of the acas_configure rpm

The global nessusd.rules file contains a number of comments, but should contain only one uncommented line, which should contain only the words: “default accept”. There may be a few blank lines, which is fine. The SecurityCenter scan user rules file should be empty.

If either of these files contain additional configuration lines, they should be documented and know by the ISSO, ISSM, and AO.

Passive Vulnerability Scanner Settings

SecurityCenter/ACAS administrator will periodically validate the PVS scanner version(s). In the SecurityCenter web UI, Resources > Passive Vulnerability Scanners, verify values listed in the ‘Version’ column are ACAS PM recommended or compliant with the current CYBERCOM TASKORD.

The pvs configurations are best reviewed from the command line:
Linux:

```
# /opt/pvs/bin/pvs --config --list
```

Windows:

```
# …\Program File\Tenable\PVS\pvs.exe --config --list
```

…The command can be augmented with | grep “keyword” on Linux or | findstr “keyword” on Windows.

```
Monitored Network Interfaces: Site/Organization defined, must not be empty
Enable SSL for Web Server: 1
Minimum Password Length: 15
PVS Web Server Address: Site/Organization defined value, except “0.0.0.0”
Enable SSL Client Certificate Authentication: 1
Enable Debug Logging for PVS Web Server: 0
Maximum User Login Attempts: 3
Max Sessions Per User: 5
Enforce Complex Passwords: 1
Login Banner: You are accessing a U.S. Government (USG) Information System
(IS) that is provided for USG-authorized use only. By using this IS (which
includes any device attached to this IS),you consent to the following
conditions: \n-The USG routinely intercepts and monitors communications on
this IS for purposes including,but not limited to,penetration testing,COMSEC
monitoring,network operations and defense,personnel misconduct (PM),law
enforcement (LE),and counterintelligence (CI) investigations. \n-At any
time,the USG may inspect and seize data stored on this IS. \n-Communications
using,or data stored on,this IS are not private,are subject to routine
monitoring,interception,and search,and may be disclosed or used for any USG-
authorized purpose. \n-This IS includes security measures
```

```
(e.g.,authentication and access controls) to protect USG interests -- not for
your personal benefit or privacy. \n-Notwithstanding the above,using this IS
does not constitute consent to PM,LE or CI investigative searching or
monitoring of the content of privileged communications,or work
product,related to personal representation or services by
attorneys,psychotherapists,or clergy,and their assistants. Such
communications and work product are private and confidential. See User
Agreement for details.
Restrict Access to TLS 1.2 or higher: 1
ACAS Classification: Valid values: "UNCLASSIFIED", "CONFIDENTIAL", "SECRET",
"TOP SECRET", and "NOFORN"
```

Conduct Active Scan

The organization will scan the entire active IP space NLT every 30 days with a policy equivalent to the Vulnerabililty scan policy described in Appendix Q. The organization has two options:

- Conduct a Vulnerability scan against all organization IP addresses and ranges (Sites should be prepared to support this option, as this is the preferred option for auditors).
- Conduct a discovery scan against all organization IP addresses and ranges and create an asset list of live hosts, which is then utilized for conducting vulnerability scans. The organization's vulnerability scan will be initiated NLT 72 hours after the discovery scan is 'Completed'.

Active Scan Policy

Review the required, documentable, and unacceptable deviation lists in Appendix Q to verify what scan preference / plugin options can be changed and still maintain compliance. Vulnerability or discovery scans will be executed against targets defined by IP address range(s), or static asset lists that define the IP address ranges the organization/site are using. If a discovery scan is used, a vulnerability scan may leverage dynamic asset list(s), but a scan against IP space or a static asset list must occur first.

If the site chooses to leverage a discovery scan, the site must be able to demonstrate that all hosts are accounted for NLT every 30 days in addition to the actual discover of IP space.

Active Scan Settings

Each active scan will utilize an appropriate (valid type and IP space), site-defined repository. The scan zone can leverage automatic distribution, or be manually selected, as long as the site is certain the most effective scanners are being used to interrogate the targets of the scan.

Basic Settings

Scan Timeout Action: Import Completed Results and Create Rollover Scan
Rollover Schedule: On Demand

Advanced Settings
Scan Virtual Hosts (e.g. Apache VirtualHosts, IIS Host Headers): Disabled
Track hosts, which have been issued new IP address, (e.g. DHCP): Enabled, if DHCP, BOOTP, or other protocols are used, or if assets transition in and out of the network on a regular basis.
Immediately remove vulnerabilities from scanned hosts that do not reply: Enabled for CTO vulnerability scan, and Disabled (Number of days to wait before removing dead hosts should be NLT 30 days) for all other scans that can write into production repositories (repositories used for CTO reporting, the site is responsible to ensure they're gathering and reporting accurate data).
Max scan duration (hours): Unlimited

Deviations from the settings are ISSM acceptable if the reasons are documented. If a rollover scan is not being created, the site must document the process that is being used to track down failed scans and ensure the affected IP space is still being scanned.

Credential Use

The vulnerability scan must be credentialed, unless the target of the scan is restricted to known unsupported OSes. Each scan will use a single credential set for each credential type (Windows / SSH / SNMP / Database). The reason for this is to minimize the potential for locked accounts. If a site needs to use more than one credential set for one or more credential types, this is acceptable as long as the site has documented the justification and the appropriate ISSM/IAM and SA's have accepted the potential risk to the target systems' availability.

The account(s) utilized to scan each target must have the minimum privileges required to conduct the authenticated scan. The site will document any exceptions where they are not able to utilize separate accounts for each PM/POR, tenant enclave(s), and security boundary. Enterprise authentication systems (example: Microsoft Active Directory Domains), will also separate accounts by system type (desktop vs server). Configurations details are covered in Appendix N: Enabling Credentialed Security Checks.

Compliance Check Process

Sites will scan at least monthly using the applicable audit files or SCAP benchmarks. Where possible, the site should use the DISA authored SCAP benchmarks. If SCAP is not an option because the target OS is not supported or no benchmark is available for the target OS or device, the site should utilize vendor-authored audit files. Supported SCAP and audit file targets are outlined in in Appendix C.

The audit files can be selected from the Scans > Audit Files page in the SecurityCenter WebUI. SCAP benchmarks require more manual effort, working with SCAP is explained in Appendix L. These files are updated as part of the SecurityCenter feed that is manually or automatically downloaded from the DISA Plugin or Patch Repository servers. An organization- or site-defined audit file can be up loaded as a custom audit file.

CMRS reporting and other specifics about SCAP scanning are covered in Appendix L.

Discovery Scan Result Review

The most common uses for discovery scans are to identify hosts within large swaths of IP space and to identify online hosts at a given period. The policy provided with this guide is intended to provide a middle ground and support both of these tasks with a single documented policy.

For each scan, the total list of online IP addresses can identified by:

10180 – Ping the remote host

Hosts which have received OS identification are generally ready for follow-up scan, but it is important that the scanner-enumerated OS is validated to be accurate. CPE can be helpful; as a secondary mechanism to identify assets by OS and or application, but its data is not included in the built-in OS, based asset lists, so it is not a direct alternative for OS identification. Device type is a data point, which should help the organization identify resources within scan results and understand the network topology being evaluated.

11936 – OS Identification
45590 – Common Platform Enumeration (CPE)
45615 - Device type

The target's hostname, DNS name, and MAC address are useful in correlating data between scans (updating scan data to match current DHCP deployments or hardware redeployments.)

Vulnerability Scan Result Review

Identify hosts with good scan data. These are hosts that local security checks are available, and as a result, high accuracy IAVM data is available. An Asset List is available in Appendix Q to assist with verifying which hosts have good scan data. Depending upon the OS version, the organization should look for appropriate plugins listed below:

For each Windows host, if a scan completed **SUCCESSFULLY** you **MUST** have these plugins triggered:
10394 - Login possible
10400 - Remote registry accessible
24269 - WMI available

For each Windows host, if any of the following plugins **ARE NOT** triggered, the organization should **validate the scan results**, and account for the lack of each plugin occurrence or prepare to document the reason the plugin did not trigger:
34252 - Netstat Portscanner (WMI)
20811 - Microsoft Windows Installed Software Enumeration

For each UNIX/Linux host, if a scan completed **SUCCESSFULLY** you **MUST** have these plugins triggered:
12634 - OS Name and Installed Package Enumeration
22869 - Software Enumeration (SSH)

For each UNIX/Linux host, if any of the following plugins **ARE NOT** triggered, the organization should **validate the scan results**, and account for the lack of each plugin occurrence or prepare to document the reason the plugin did not trigger:
14272 - Netstat Portscanner (SSH)

Many issues might cause a system to fail to respond to a scanner, or to respond with insufficient data. Below are plugins that can be helpful in identifying scan results that may not be accurate or sufficient.

For each host, the scan completed **INCORRECTLY** if **ANY** of these plugins triggered:
21745 - Authentication Failure - Local Checks Not Run (Indicates credential failure unless 12634 or 97993 are triggered. In which case it indicates that local checks were not run)
24786 - Nessus Windows Scan Not Performed with Admin Privilege
26917 - Microsoft Windows SMB Registry: Nessus Cannot Access the Windows Registry
10919 - Open Port Re-check (Previously open ports are now closed)
35705 - SMB Registry: Starting the Registry Service during the scan failed
35706 - SMB Registry: Stopping the Registry Service after the scan failed

For each Windows host, if any of the following plugins **ARE** triggered, the organization should **validate the scan results**, an account for each plugin occurrence or prepare to document the reason for the plugins occurrence:
38153 - Microsoft Windows Summary of Missing Patches
26921 - Windows Service Pack Out-of-Date

For each UNIX/Linux host, if the following plugin identifies **binaries other than** those included in **HBSS**, the system should be scanned with 'thorough checks' enabled, and the **SA** will **verify specific version information for each binary listed** per host:
33851 - Network daemons not managed by the package system

Look for Unsupported Hosts (No Credential Checks)

A list of supported target OSes is available in Appendix C, in the section labelled 'Ensure the Target OS is Supported'. Plugin 12634 or 97993 also contains information useful in identifying if the Nessus scanner will be able to perform credentialed or local security checks of a given host. If the scanner is able to log into the target via SSH, it will attempt to identify the host OS using a **`uname`** command. If this command fails to execute, or the output of the command unexpected, the scanner will log this in the plugin text for 12634/97993 including a note that contains "Local security checks have been disabled". A report is available in Appendix Q, which will report the name, and IP of all machines for which no local security checks are available. For each

occurrence, the organization will evaluate the target to verify that it is not on the supported target OS list.

Host Coverage and Data Retention

CCRI auditors expect the site to have NLT 95 percent authenticated-scan success rate. Currently, this figure is based on a relationship between total number of assets (plugin 19506) and failed authentication (plugins 21745, 26917, and 24786).

Number of hosts scanned: IP Summary - Plugin ID set to = 19506
Failed Creds & Access: IP Summary - Plugin ID set to = 21745, 26917, 24786

After these two values have been found, the math is simple:
Number of hosts scanned = X (1000 in example below)
Failed Creds/No Registry Access = Y (45 in example below)

(X-Y)/X = % of Good Scans
(1000-45)/1000 = .955 or 95.5%

The ACAS PM is continuing to work with the vendor, DODIN RSI, and service representatives to develop improved guidance to assess the quality of ACAS scan coverage.

Data Retention

While no formal data retention requirement exists for ACAS, auditors will need to see no less than 90 days' worth of scan data or report results that demonstrate the organization is consistently performing CTO compliance scanning. Currently we recommend storing report results offline or in other systems to demonstrate historical CTO compliance.

Using report results (PDF, RTF, and CSV) to verify consistency is recommended, Appendix Q contains a sample report template that contains the required information. If other than recommended report is used then then the report(s) at a minimum must contain vulnerability results and host counts, failed credentials/system access, and OS List.

Program Timelines and Intervals

Different elements of ACAS are released based on availability and readiness. Tenable generally releases SecurityCenter and PVS updates quarterly and Nessus updates are closer to monthly or bi-monthly. DISA tries to limit the frequency of changes, but many releases are unavoidable due to security fixes.

Plugins are updated to the NIPR plugin server every 12 hours. The updates to the SIPR plugin server and the Patch Repositories (NIPR and SIPR) are daily. Contractually, plugins should be updated with IAVM data within 48 hours of the IAVM announcement.

SCAP benchmarks are authored by the STIG writing teams, and are updated as STIG changes are released, generally quarterly.

Tenable audit files are updated on a 'best effort' basis. More commonly used audit files are updated more regularly than others. Importantly, Tenable does not guarantee that the audit files will be updated on any given interval.

Appendix A: Important URLs

Below are URLs to the ACAS guides, which contain important information or tools:

Patch Repository (DOD PKI Certificate Required)

ACAS Approved documentation, software and patches:

https://patches.csd.disa.mil/CollectionInfo.aspx?id=442 (*CAC is required for access).

Click **ACAS** > **ACAS Software** > then whichever application you need

Plugin Updates

Manual Plugin Updates

https://patches.mont.disa.mil/CollectionInfo.aspx?id=552

Automated Plugin Updates

Files are posted at https://acas-update.csd.disa.mil/

Red Hat Updates

DISA does not provide the RHEL OS Licenses. It is the responsibility of the deploying organization to purchase the Red Hat Entitlement prior to deployment of ACAS (Entitlements are not version specific).

Curated RHEL patches are no longer being provided. During the six years of the ACAS contract, no OS patch has broken functionality of ACAS programs. The ACAS program office recommends that sites apply OS patches in a timely manner instead of waiting for the ACAS program to announce approval. This same process has been in place for the Windows OSes since the beginning of the ACAS contract.

Offline updates for the Red Hat operating system are no longer being provided via the DOD Patch Repository at the request of Red Hat. Red Hat has a number of resources available to assist with offline patching (instead of downloading patches directly from Red Hat).
https://access.redhat.com/solutions/29269

DEPS Portal (DOD PKI Certificate Required; Select Email certificate):

DOD Secure Host Baseline Repository

https://disa.deps.mil/ext/cop/iase/DOD-images/Pages/index.aspx

Hardware Requirements

https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/Components.aspx

ACAS Wiki location

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

Guidance and Informational URLs:

ACAS License Request Portal
https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/requestPortal/LicenseRequest.aspx

Certification and Accreditation Artifacts
Posted at ACAS SIPR Wiki: http://www.intelink.sgov.gov/wiki/ACAS

Site Responsibility Guide
Posted at ACAS SIPR Wiki: http://www.intelink.sgov.gov/wiki/ACAS

Software Forge (DOD PKI Certificate Required)
https://software.forge.mil/sf/frs/do/listReleases/projects.acas/frs.kickstart_image

ACAS Announcements Subscription (*requires a .mil e-mail address):
https://public.govdelivery.com/accounts/USDISA/subscriber/new?topic_id=USDISA_150

ACAS Portal
Portal for all links to ACAS resources:
http://www.disa.mil/cybersecurity/network-defense/acas

Monthly Working Group
https://connectcol.dco.DOD.mil/acaswg

USCYBERCOM TASKORD 17-0019 (supersedes CTO 13-0670)

USCYBERCOM webpage at the following link **(DOD PKI Certificate Required)**:
https://www.cybercom.mil/J3/orders/TASKORDsEXORDs/Forms/ByDocNumDesc.aspx

Customer Support

DISA DECC Oklahoma City
NIPR: disa.tinker.eis.mbx.okc-disa-peo-service-desk@mail.mil
SIPR: disa.tinker.esd.mbx.okc-service-desk@mail.smil.mil
DSN 850-0032 or COMM 844-347-2457, opt 1, then 5

Training Resources

IASE - Cyber Product Training - ACAS Supplemental Training:
https://powhatan.iiie.disa.mil/cyber_tools_training/ctt/acas.asp

Cyber Defense Training Cloud
https://cdtc.cert.org/lms

Training Schedule and Registration Information
IASE 2015 ACAS Schedule page (A-Z):
https://disa.deps.mil/ext/cop/iase/classroom_training/Registration/Lists/TrainingSchedule/Events.aspx

In addition, students may access the ACAS calendar schedule using the following link:
https://disa.deps.mil/ext/cop/iase/classroom_training/Registration/Pages/index.aspx

Appendix B: Network Topology Considerations for ACAS

The Nessus and PVS sensors are greatly affected by their position in a network environment.

Topology Considerations for Nessus

Each organization will need to consider their hardware availability and support, performance requirements, network topology, along with IP and asset counts.

Nessus is a well-threaded application, and will benefit from high-performance hardware. However, in many cases, adding more scanners will do more to improve performance than improved hardware. Where possible, we recommend identical scanner hardware and OS to minimize issues with under-loading / over-loading scanners.

Performance requirements / expectations are important to understand as well. In a closed / static environment, scanning all of the organization's assets between 1700 Friday and 0500 Monday might work well, and with 60 hours to scan performance might not be a serious concern. However, environments with teleworking laptops and other dynamic assets that leave the network, may require faster scaning and scans during the work day.

Since firewalls, slow data links, and other inteligent networking devices can skew scan results extra scanners may be required to accomidate minimize issues such as failed OS identificaation, ghost hosts, missing hosts, or false findings.

Providing reliable recommendation on scanner implementations is difficult. Topology, scanner hardware, network performance, target host performance all play major roles in how long scans actually take to complete. There are two major drivers, total IP space, and total asset count.

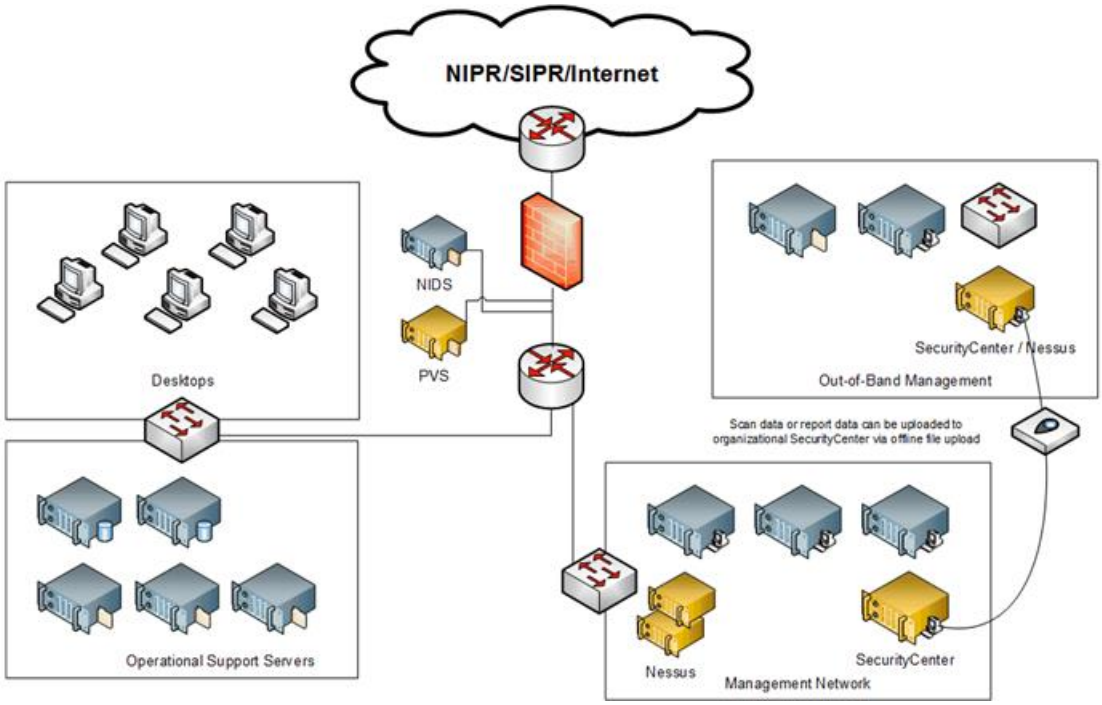
A general starting point is to provide one Nessus scanner for every 5,000 assets or every 16,000 IPs. For example an organization with 10,000 assets and 65534 IP addresses (class B or /16 network) would want 2 – 4 scanners. This does not account for WAN connections or network gateways or filters which might require additional scanners. More scanners would yield shorter scan windows, but the cost of the ACAS implementation and mainencance will be higher.

Topology Considerations for Nessus

There is no one right way to deploy PVS sensors. Due to the requirement for a promiscuous interface, the number of PVS sensors an organization is able to deploy may be limited. Deployment options may also be limited by availability of the data, network span/monitor sessions are often limited, and hardware network taps may be cost-prohibitive. You can start by reading the PVS User Guide and the PVS Scanner Background and Theory guide available on the Patch Repository (link provided in Appendix A). The ACAS program provides and supports the 1 Gb/s PVS solution.

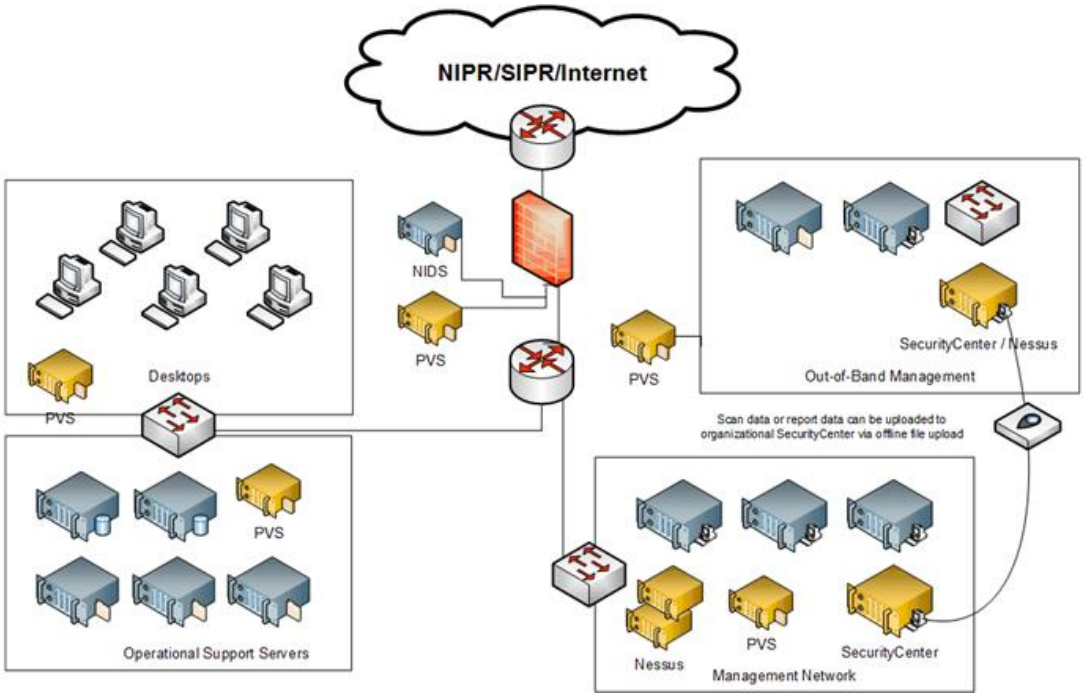
Intrusion Detection System (IDS) Mindset Deployment

IDS sensors are primarily located at ingress/egress points so attacks from external sources can be identified as such. The PVS monitors network traffic at the packet layer to determine topology, clients, applications and related security issues.



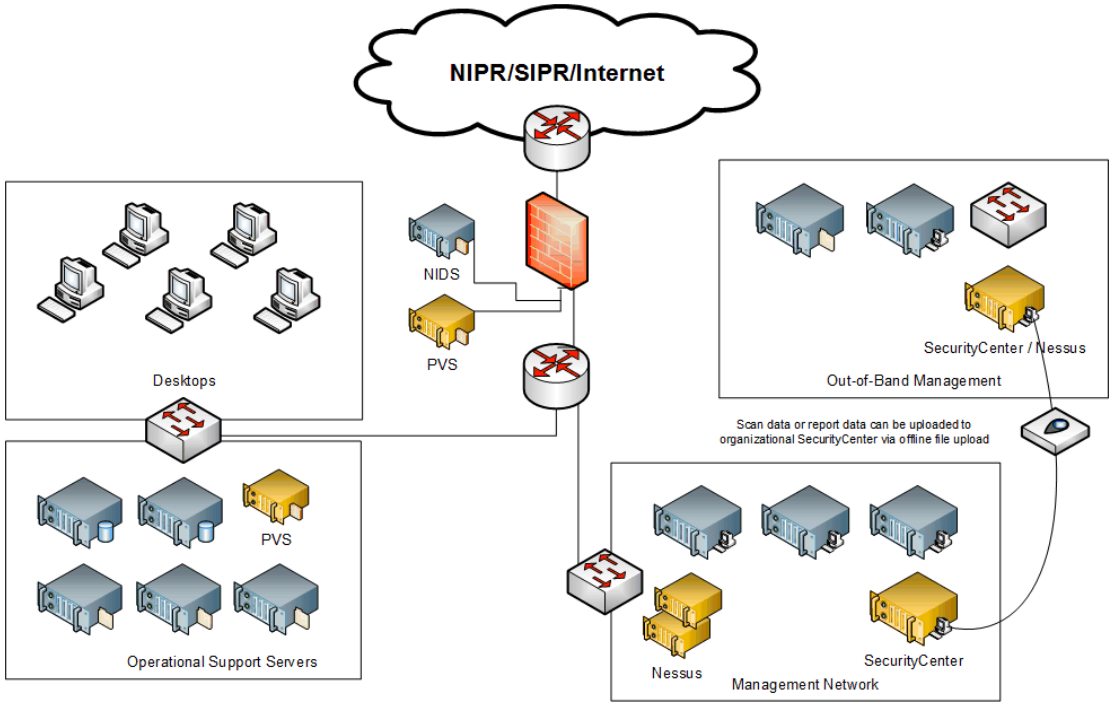
Thorough or Heavy Deployment

Mirroring the deployment requirements of HBSS' Rogue Detection System (RDS) and putting a PVS on every network will provide a large amount of data. Like many other tools, being Layer-2 adjacent has advantages in the fidelity of data that can be captured. However, such a deployment is expensive, and may capture the same data in multiple locations.



Balanced Deployment

In most cases, an organization can get a good perspective of the assets on their network by monitoring the networks which house operational support services (DHCP/DNS/Active Directory/LDAP/OCSP responder), and watching the traffic entering and exiting the network to gather information about browser clients and other software which are connecting to external resources



Implementation Strategies

Passive Vulnerability Scanner (PVS) data does not have the same fidelity as that of credentialed Nessus scan data. PVS data is similar to Nessus network checks, as the findings are based on protocol analysis and are reliably accurate, while others are based on application banners and are not accurate in many cases. It is often better to use PVS as its own tool, and not expect it to be a passive Nessus scanner.

Host Discovery

Host discovery is an automatic part of PVS, Security Center 5.x includes a default Asset List that provides asset/host discover based on OS identification or Hop count enumeration. Stale host detection can be improved using PVS using the same guidance provided in Appendix M.

Rogue Host Discovery

The following are instructions for creating dynamic combination asset lists to identify stale hosts in a dynamic network.

Description of the process:

1. Schedule a frequent ping sweep scan; running one or more times per day.
2. Create an asset list that includes hosts/devices, which have been pinged in the last 24 hours. This is the closest way to assert that a host is online without using PVS.
3. Create an asset list that provides a tally of hosts that need to be scanned, based upon showing old credentialed scan data. For testing and demonstration, this example uses one week as the date criterion. Your definition of "old" may vary.
4. Create a combination asset list that includes both of the asset lists previously created. This asset list contains hosts which are online (ping sweep) that also require scanning (old credentialed scan data).
5. Create an alert that triggers when a new IP address populates the combination asset list. This alert causes a scan of the targets in the combination asset list.

Steps:

Step	Action

1	Create a Dynamic Asset list that contains the IPs of hosts not included in a credentialed scan within the past *"n"* days. Note: Use this with Windows & UNIX/Linux targets.
	
	• ALL of the following are true:
	  ○ ANY of the following are true:
	  ▪ Days since Observation is less than 1 where plugin ID 12
	  ▪ Days since Observation is less than 1 where plugin ID 10180
	  ○ ANY of the following are true:
	  ▪ Days since Observation is less than 1 where plugin ID 10394 (Authenticated Check: OS Name and Installed Package Enumeration)

	▪ Days since Observation is less than 1 where plugin ID 12634 (Microsoft Windows SMB Log In Possible)
2	Create an active scan; scheduled to run daily to ping sweep the networks where dynamic hosts reside or use the host and OS discovery scan policy from Best Practice Scan Policies
3	Create an active scan; set to run On Demand, based on the organization's vulnerability scan policy or use the vulnerability scan policy from Best Practice Scan Policies. • If the site is monitoring hosts in multiple repositories, create a scan template for each repo.
4	Create an alert (Workflow > Alerts +Add). Schedule hourly, every 1-4 hours; perform actions on every trigger. Trigger IP Count >= 1. Action > Launch a Scan and select the scan defined in step 3.

Isolated Stub Network Enumeration

The following are instructions for enumerating the hygiene of a network, where active scanning is unreliable or cannot be performed reliably. Some examples of Isolated Stub Networks include networks dedicated to support printers, thin clients, and storage (NFS / iSCSI) appliances.

Description of the process:

1. Define the expected behavior of the network. This might include connections from print server(s) to printers and multi-function devices. Enumerating connections to assets within the isolated network from a central host should be based on plugin 15 (example: print servers connecting to printers). Connections from assets to a central host should be based on plugin 3 (example: thin/zero clients reporting to a management system).
2. Define the expected benchmark of the assets in the network. This would include the known good OS name(s) enumerated by plugin 1
3. Define a static asset list that includes the IP ranges associated with the isolated network.
4. Create a combination asset list that includes both of the static asset list from step 3 and the default "Systems Discovered Passively" asset list and not the static asset lists defined in step 1 or 2.
5. Create an alert that triggers when a new IP address populates the combination asset list. This alert should email or notify an appropriate user.

Steps:

Step	Action
1	Define the expected behavior of the network ANY of the following are true: • Plugin Text contains the pattern "known good source IP address" where plugin ID is 15 • Plugin Text contains the pattern "known good destination IP address" where plugin ID is 3 …

2	Define the expected OS baseline of the network ANY of the following are true: • Plugin Text contains the pattern “known good OS name (partial)” where plugin ID is 1 • Plugin Text contains the pattern “known good OS name (complete)” where plugin ID is 1 …
3	Define the IP address range(s) assigned to the network • Static asset list based on IP range or ranges
4	If the default “Systems Discovered Passively” asset list is not available, it can be recreated: ANY of the following are true: • Plugin ID is equal to 1 • Plugin ID is equal to 12
5	Create a combination asset list (("Asset List from Step 3" AND " Asset List from Step 4") AND NOT (“Asset List from Step 1” OR “Asset List from Step 2”))

Appendix C: Scan & Reporting Troubleshooting

The following ACAS scanning troubleshooting suggestions will help with difficult scans and other issues. Other situations and fixes may be found at the ACAS Discussion Forums.

Scan Policy Issues

Scan Policy

Plugin 10287 (Traceroute) can increase scan times depending on the topology traversed to each asset. Since this plugin is purely informational and not a compliance requirement, the plugin may be disabled in some DOD agencies scan policies.

Network device scanning

It has been noted that there is an adverse impact to the transport layer while scanning network devices. Many network devices do not have the same processing capabilities of a workstation or server. While this is particularly noticeable with older, legacy routers, it can also affect network switches and other devices.

To minimize this impact, try to exclude router interfaces during network scans and instead conduct scans against a management interface. Network devices are 'Sensitive Devices', and ideally should be interrogated with a separate scan policy and scan job separately so the policy can be de-tuned to minimize impact to the target.

When scanning network devices, "de-tuning" the scan policy is recommended that **max checks per host** be set to **1** or **2** (Advanced tab). Additionally, **max host per scan** should be lowered **(=<10)** to minimize the distributed load across the infrastructure.

Inaccurate Scan Result Issues

Scanning with good access to target hosts and valid credentials is critical to generate meaningful high-fidelity scan data. In order to provide credentialed scan results the Nessus scanner must have access to targets via SSH (UNIX/Linux) or CIFS, WMI, and Remote Registry access (Windows). The scanner must also have valid administrative credentials to the target. Lastly, the target OS must have a plugin family or a compliance plugin (within the Policy Compliance Family) associated.

If the site is having issues with scanning a host, plugin 19506 is a good place to start looking. This plugin contains Nessus Scan Information, and contains the Nessus scanner's version, IP address, and plugin feed version. Additionally this plugin will indicate the duration of the scan and if credentialed checks were run against the target.

```
Credentialed checks : yes
```

Potential Causes for Credentialed checks not running include:

- No SSH/CIFS Access
- Bad or non-admin credentials
- No local security plugins available for platform

Ensure Proper Access

Ideally, no firewall should be between the Scanner and the target. Firewalls (including routers with ACLs or other 'screening host' implementations) can cause Nessus to incorrectly enumerate the target OS or fail to access ports required for local security checks. Most targets in the DOD are protected by host-based firewalls, restrict in-bound management traffic, and run security software to prevent attacks from external hosts. If the scanner does not have access to Secure Shell (UNIX/Linux) or CIFS (Windows) 21745 will NOT trigger.

If Nessus cannot connect to application ports (such as HTTP), it cannot perform direct enumeration of application vulnerabilities.

Ensure Proper Credentials

For Windows hosts, the scanner should utilize a domain user with administrative access to the target workstation. A domain admin account should only be used to scan domain controller servers. If a local account is required (the target does not belong to a domain), UAC requires modification. For more information about authentication to Windows targets, refer to Credentialed Checks in Windows.

For UNIX/Linux hosts, the scanner will likely need to be configured to use some form of escalation (`su`/`sudo`/`su+sudo`) to execute with admin level rights. Log into the target with the credentials provided and verify the commands can be run as expected, watch for additional banners or confirmation prompts. (Both forms of escalation should prompt for nothing more than a password). For more information about authentication via SSH, refer to Enable SSH Local Security Checks.

To troubleshoot authentication issues and failures, refer to Validating Credentialed Access in Scan Data.

Ensure the Target OS is Supported

Many appliances are based on a Linux or BSD kernel, however, Nessus will not leverage the surrogate OSes local security checks. Leveraging such checks would be inaccurate because of the way that vendor's package and maintain their software. The best place to see which Local Security Checks are available is to look in the Plugins tab in the scan policy. More information about local and network checks is in appendix D. The supported OSes include:

Local Security Checks (Vulnerability Analysis) are available for (as of 31 October 2017):
AIX, HP-UX, Amazon Linux, CentOS, Fedora Core, Gentoo Linux, Mandriva Linux, Oracle (Linux and VM), Red Hat Enterprise Linux, Slackware Linux, SuSE Linux, Ubuntu Linux, Solaris, FreeBSD,

and MacOS X. Cisco (IOS & CatOS), F5 Networks BIG-IP, Huawei, Junos, Palo Alto, Virtuozzo, VMware ESX, and Microsoft Windows.

Policy Compliance Checks via .audit scan are available for (as of 31 October 2017):
Adtran AOS, Amazon AWS, Arista EOS, BlueCoat ProxySG, Brocade FabricOS, CheckPoint GAiA, Cisco IOS, Citrix XenServer, Dell Force10 FTOS, Extreme ExtremeXOS, F5, FireEye, Fortigate FortiOS, HP ProCurve, Huawei VRP, IBM iSeries, Juniper Junos, Microsoft Azure, NetApp ONTAP, OpenStack, Palo Alto PAN-OS, Rackspace, RHEV, Salesforce.com, SonicWALL SonicOS, VMware vCenter/vSphere, WatchGuard, Microsot Windows

Policy Compliance Checks via SCAP scan are available for (as of 31 October 2017):
Windows and Red Hat Enterprise Linux 5 & 6

Tenable-authored .audit files are not authoritative, nor is ACAS authoritative as a SCAP compliance tool. CYBERCOM has directed the field to utilize SCAP and .audit files via ACAS, as a best practice to validate configurations, the findings of the ACAS tool should not be used to contest to findings of authoritative tools (SCC and HBSS PA). Users should open OKC service desk tickets if a false finding is identified.

Plugins Which Conflict with Other Policy or Guidance

The ACAS vendor writes plugins to find vulnerabilities and enumerate risk. The plugins are not written to match or confirm DOD or US Government guidance. Compliance is the responsibility of audit or SCAP scanning.

If a plugin does not match the STIG guidance, any associated findings should have the risk accepted or recast to informational following manual analysis of the plugin findings. Any recast or accepted risk should be accepted by the AO, annotated with trouble ticket from the ACAS support desk, and documented to ensure the status of the plugins is clear to a visiting auditor or other organizational security staff.

Known examples are commented below:

Antivirus Software Check – Plugin 16193
This plugin enumerates how old the host's anti-virus definitions are. If the delay exceeds a user-defined value (between 0 and 7 days) the plugin will trigger. This value can be changed on the Assessment tab in the scan policy, but the recommended value is 0. However, STIG accepts a delay of up to 7 days. If the site has a document maximum acceptable virus definition age that is between 0 and 6 days that should be used. Note: OPORD 16-0080 directs organizations to accept no more than 24-hour delay, if this order is applicable to the organization, 0 or 1 are the recommended values.

Microsoft Windows Guest Account Belongs to a Group - Plugins 10907
Some sites are adding guest accounts / groups to the group "DenyNetworkAccess". This is called out in the automated benchmarks to ensure specific accounts / groups are prevented

from accessing the network. If the site has configured their systems in this manner, they will need to reconfigure to remove the guest access from this account.
Per the DISA Risk Management Executive Cyber Standards Branch (RE11), “The intent of that group is to include all local admin accounts for assigning them to a couple of Deny user rights. The requirement that defined it in the STIGs never included the Guest account in the group. "

Microsoft Windows SMB Registry: Winlogon Cached Password Weakness – Plugin 11457
The DISA STIG specifies a maximum cached login value of ‘2’. This setting is a DISA identified acceptable level of risk. The plugin will trigger for any host with a value greater than ‘0’, as it is designed to enumerate overall risk instead of DISA identified acceptable level of risk. A report is provided in Appendix Q to report on hosts that are configured outside of STIG recommendations. The site can utilize this report, or a demonstrably equivalent process, and recast the risk associated with plugin 11457 to informational where the target value is less than or equal to ‘2’.

SSH Server CBC Mode Ciphers Enabled – Plugin 70658
This plugin does not review the target’s OS. While RHEL-06-000243 states that Counter (CTR) mode is also preferred over cipher-block chaining (CBC) mode, it does not explicitly forbid the use of CBC ciphers. The basis for allowing CBC ciphers is "Based on … the CBC vulnerability was mitigated with version 5.3 (the OpenSSH version used with RHEL 6)." This release note for 5.3 was published on February 23, 2009

The ACAS vendor identified the basis for the plugin as an article Red Hat published (https://access.redhat.com/solutions/420283) which encourages users of RHEL5 & RHEL6 to disable CBC Ciphers.

Because the Red Hat article was updated 6 years after OpenSSH 5.3, and still encourages users to disable CBC, we recommend people adhere to the guidance in the plugin.

Plugins Which Trigger Against Hosts in a Configured Role

Some applications and services represent security issues if improperly used. In many of these cases, Nessus is not able to enumerate if a service is deployed appropriately to mitigate any associated risk. In general, this type of plugin includes text or references to help the site understand if the finding is valid. This process requires manual analysis of the target and the associated networks, requesting assistance from the ACAS Customer Support desk is recommended if the site is in doubt.

IP Forwarding enabled - 50686
If this plugin triggers against a host that is known to be a router, it can be accepted or recast.

HTTP Proxy POST Request Relaying – Plugin 10194
This plugin will trigger against many ‘forward’ or ‘explicit’ web proxies, and, while it requires further confirmation, in most cases the proxy vendor can provide configuration guidance.

DNS Server Recursive Query Cache Poisoning Weakness- Plugin 10539

Recursive DNS servers will be flagged, as the Nessus scanner is not able to enumerate if access control lists are used to limit access. The DNS STIG should be used to validate the server's configurations prior to the risk being accepted or recast.

DNS Server Spoofed Request Amplification DDoS – Plugin 35450

Recursive or forwarding DNS servers will be flagged, as the Nessus scanner is not able to enumerate if access control lists are used to limit access. The DNS STIG should be used to validate the server's configurations prior to the risk being accepted or recast.

LDAP NULL BASE Search Access – Plugin 10722

This plugin is designed to trigger if certain queries receive 'excessive' NULL bind responses from the LDAP server. While this plugin generally works well for Microsoft Active Directory Domain Controllers, many UNIX/Linux based LDAP servers are customized to work in a specific manner for certain applications.

The responses, which are considered acceptable, include (as of 20 December 2016):

```
currentTime,
subschemaSubentry,
dsServiceName,
namingContexts,
defaultNamingContext,
schemaNamingContext,
configurationNamingContext,
rootDomainNamingContext,
supportedControl,
supportedLDAPVersion,
supportedLDAPPolicies,
highestCommittedUSN,
supportedSASLMechanisms,
dnsHostName,
ldapServiceName,
serverName,
supportedCapabilities,
isSynchronized,
domainFunctionality,
domainControllerFunctionality,
forestFunctionality,
isGlobalCatalogReady
```

The site should work with the LDAP system admin and any associated application developers to validate the responses provided by the LDAP server are the minimum set required, once a list of minimal responses is identified and AO accepted, the risk could be recast or accepted.

Scan Performance Issues

ACAS Scans Fail General Error

Problem: Scans fail during the last part of the scanning process due to a general error: database is locked.

Fix: Delete the failed scan and rescan as needed. Anyone having this on a regular basis should seek assistance with the DISA's ACAS Customer Support desk to troubleshoot the root cause.

Detailed Information On Large Currently Running Scans

Problem: Unable to find detailed information on large currently running scans.

Fix: Right click on the gear icon for the currently running scan and select View. View information includes, scan status, import status and total IPs scanned.

Large Workday Scans Slow To Complete

Problem: Large workday (0600 to 1700 Monday-Friday) scans take hours to complete.

Fix: Network and target resource utilization may cause performance issues, where possible, scan off-hours to minimize impact and leverage decreased network utilization.

ACAS Web Console Displays Incorrectly

Problem: Web console displays out-of-date scan information and dashboards are not updating.

Fix: Clear browser cache.

Completed ACAS Scans Return No Information

Problem: Completed scans return no information due to a dead IP address.

Fix 1: Verify the ACAS scanner can communicate with the target system that is returning no scan information.

Fix 2: Verify the IP address of the system returning no scan information is in a scan zone, accessible by the organization, and within appropriate IP ranges for the import repository.

Fix 3: Rebuild Plugin Database on Nessus Scanner

Completed ACAS Scans Only Return Informational Results

Problem: Completed scans only return informational results (no "Critical", "High", "Medium", or "Low").

Fix: Check plugin 19506 to identify if credentials were enabled (Credentialed checks : yes). If no, verify the scan had credentials enabled, then verify the target OS is Supported. If yes, refer to Validating Credential Access in Scan Data.

ACAS Not Reporting Latest Vulnerabilities on Unpatched Systems

Problem: Scan results do not contain the latest vulnerabilities on unpatched systems.

Fix: Verify plugins are up to date. Most SecurityCenter instances receive new and updated plugins daily.

ACAS Reports Issues

ACAS Reports Slow To Complete

Problem: Reports take a long time to complete.

Fix: Change the scope of the report to include only a specific asset list or IP address range. Reports against over 10k assets may have decreased performance or additional issues.

Appendix D: False Plugin Finding Troubleshooting

If you identify a False Positive or False Negative finding, open a ticket with DISA's ACAS Customer Support desk. You will be asked to provide some basic information in order to expedite the issue. Specifcially; kb/db files, DVL, .nessus file(s), fix actions, screenshots, registry exports, command results, and the closed case information from the vendor of the product.

Local Checks

If the plugin in question is in a plugin family defined by an OS, it is a local security check and requires the use of credentials.

- Download the Scan Result (`.nessus` format), and provide evidence that supports that the patch is really installed or the 'vulnerable' software is not installed.
  - ACAS Customer Support will review this information, and may ask for additional information if needed.
  - If ACAS Customer Support agrees that there is a false finding, they will request that you provide a kb/db file from the Nessus scanner. See Appendix J for instructions on obtaining the kb file.
  - ACAS Customer Support will require that you provide explicit permission to release all of the information you have provided to the vendor (Tenable).

- Once Tenable determines what needs to happen, one of the following actions will occur:
  - Tenable will update the plugin.
  - Tenable will not change the plugin, but will defer the issue to engineering or the PM, for a potential feature request, workaround or exception.

Network Checks

If the plugin in question is not in a family associated with a specific OS (misc. or web servers for example):

- Download the Scan Result (`.nessus` format) for any finding in question.

- Identify which port the issue was triggered on, what application(s) known to be monitoring that port, if the service is atypical or custom and any basic information about its purpose/design.

- ACAS Customer Support will review the information provided by the customer. ACAS Customer Support does not anticipate validating the information provided; just that it logically makes sense.

- ACAS Customer support will attach all available information and evidence to the ticket.

Troubleshooting Duplicate / Superseded Findings (Oracle False Positives)

Review your scan results by looking inside the .nessus file. Check to see if the "Display the superseded patches in the report" setting is enabled. If you turn off the setting, the false positive(s) should be removed from the results. On SecurityCenter: The setting can be found in the scan policy in the Processing section on the Report Tab: “Show missing patches that have been superseded".

Using this setting can significantly reduce the number of findings displayed. While this is not an issue when reporting missing patches to system administrators, using this setting may reduce a site’s awareness relative to a formal inspection.

Audit File Compliance Checks

Each audit file contains XML formatted configuration checks. The audit files provided within the SecurityCenter are updated as part of the SecurityCenter Feed. Additionally, each site can modify existing audit files or create their own custom audit files.

Audit File and SCAP Troubleshooting (False Findings)

Validate the OS coverage against the OSes listed in Appendix C. If the OS is supported, validate that the scanner is successfully authenticating to the target and that the required access is available.

For many of the audit files, when they are enabled, the user may be prompted for information about the expected values, particularly values (file paths, or user names for example) that are site specific. These values may not be uniform across the enterprise, so it is important to validate the expected configurations.

Request Audit File Updates / New Technology Coverage

Submit requests for new / updated audit files via Software Forge Change Request (https://software.forge.mil/sf/go/projects.acas/tracker.change_request). Explicitly include technology (hardware or software), benchmark along with revision or release information.

Appendix E: Complex Scanning Situations

Events may arise where the default scanning policies will be problematic, or the tool cannot be used in optimal configurations due to operational concerns outside of the Assured Compliance Assessment Solution (ACAS).

With any situation where a policy needs to be tailored, there should be two major processes involved:

- Identify which plugins, ports, or processes are causing the issue, with a focus to maintain conformance with "equivalent" best practices scan policy.
- Document and validate your deviation from policy with the appropriate stakeholders.

Scanning through Intelligent Network Devices

Scanning through firewalls is not recommended, as firewalls and other security devices may introduce false negatives or positives. Other intelligent devices (Intrusion Detection System (IDS), proxy servers, load balancers, or Wide Area Network (WAN) accelerators) should be avoided as any device, which alters the flow of network traffic can lower the fidelity of the scan, by lowering the accuracy or confidence of the data gathered.

Firewalls often filter Internet Control Message Protocol (ICMP) traffic and are generally designed to prevent the remote enumeration of hosts. As such, sweeping a network beyond a firewall may result in 'phantom' hosts.

- In the Scan Policy, it may be useful to disable ping host (**Host Discovery Tab**), or to limit it to using ICMP (**Host Discovery Tab > Ping Methods**), if ICMP is permitted within the enclave.
- Identifying a list of hosts on the network and scanning just the live hosts will minimize 'phantom' hosts. The Passive Vulnerability Scanner (PVS) can help identify assets without requiring a topology scan. Sweeping the network is often considered part of a rogue asset detection process; however, this process is better left to PVS, as a rogue system is likely not to respond to the scanner, and if the rogue asset is behind a firewall, the chances of detection via network scan are even lower.

Most firewalls offer methods of detecting and protecting against SYN-floods and port scans. In some cases, these features are difficult or impractical (such as if the feature must be configured globally) to disable.

- In the Scan Policy, limiting the max Transmission Control Protocol (TCP) connections (**Advanced Tab**) may prevent the firewall from identifying a scan as a SYN-flood. Alternatively, you may find changing **'Max Checks Per Host'** or **'Max Hosts Per Scan'** easier in a multi-scanner environment.
- If the scan is going to be credentialed, disabling the port scanner may be a viable option (**Port Scanning Tab**), but you should ensure **'SSH (netstat)'** and **'WMI (netstat)'** are left enabled.

Some ACAS plugins may match application vulnerability signatures in firewalls, intrusion detection, or other security devices. Using credentialed checks should minimize this issue; however, some plugins may need to be disabled. The firewall logs will generally provide some details about the vulnerability, which is associated with dropped connections, using the vulnerability name, Common Vulnerability Enumeration (CVE), or vendor bulletin. You should track down and disable the individual plugins that are causing the issue.

Sensitive Applications and Devices

In most cases, Nessus is unlikely to cause issues for target systems. However, some fragile applications, systems, or networked devices do not respond well to network scanning. These applications, systems, or networked devices would be considered by individual sites and organizations to be more susceptible to a denial of service. Some of these devices should not be scanned, if the risk of loss of availability or integrity is too significant. In other situations, a scan policy can be tailored to handle these fragile applications and devices.

Awareness of a given system is critical in profiling fragile applications or devices. Ideally, system components should be scanned in a lab environment prior to using Nessus against the target in production. There are situations where system components do not respond as expected, based on lab testing. For example, a lab may not include assets under load, resources may not be scaled out to the same level, and resources may not match production resources exactly.

- In the Scan Policy, use **'Max Checks Per Host'** or **'Max Hosts Per Scan'** to minimize impact to a target host (**Advanced tab**).
- In the Scan Policy, disable specific plugins or if necessary, disable plugin families to eliminate adverse effects for the host.

Constrained Network Systems

ACAS requires network connectivity between SecurityCenter and Nessus and between Nessus and the target host. Depending upon your network topology and asset distribution, you may need to deploy scanners into positions with low bandwidth or high latency. Ideally, Nessus will scan targets via a Local Area Network (LAN) with ample bandwidth and minimal latency. Latency, bandwidth throttling, or router buffer failures can cause false negatives or other inaccuracies.

Low Bandwidth or High Latency between SecurityCenter and Nessus

Two major factors affect the viability of using a Nessus scanner connected to SecurityCenter via constrained network links including some Wide Area Network (WAN) links. These factors include pushing the plugins to and pulling the scan results from the Nessus scanner.

SecurityCenter allocates 120 seconds (2 minutes) to perform communications with Nessus scanners by default. This value can be expanded to 900 seconds (15 minutes). This setting can

be updated by using the `setTimeout.sh` script that is included on the Kickstart image. If you have network connections with less than 1 Megabyte per second (MB/s) the SecurityCenter to Nessus connection will likely benefit from increasing this setting. See Appendix O - Scanner Time Outs / Plugin Out Of Sync for more details.

SecurityCenter 4.4+ and 5.x use the `sc-plugins-diff.tar.gz` file to provide incremental plugin updates to scanners. SecurityCenter can push the entire plugin set if needed or just the last 2, 8, 15, 30, or 60 days of plugins. This is advantageous, but reliance on these smaller files can result in a situation where if a Nessus scanner can be maintained for day-to-day operations, but unable to push a full plugin load if the system needs to be rebuilt. A tested and reliable backup and recovery process may be the best solution for dealing with this.

SecurityCenter sends chunks of target Internet Protocol (IP) addresses to each scanner. Each chunk includes eight IP addresses, and the total number of chunks sent to the scanner is generally controlled by the **'Max Hosts Per Scan'** setting in SecurityCenter (**Advanced tab**). When Nessus completes scanning a chunk, it signals its completion, and SecurityCenter will begin to pull the data back from the scanner. In a bandwidth-constrained environment, it is possible for this chunk of data to take more than two hours to download. Evidence of this issue can be reviewed in the organization's System Logs. In this case, lowering the value of the **'Max Hosts Per Scan'** parameter to less than 8 will allow for a single smaller chunk size, and therefore, less data to pull back to SecurityCenter.

Primary indicators for network issues include: Nessus scanner(s) stuck in "Updating Plugins" status, timeout errors in the admin logs, and scans that complete but contain no data.

Low Bandwidth or High Latency between Nessus Scanner and Target

In situations where deploying a Nessus scanner 'beyond' a constrained network is unfeasible or unacceptable, it ***may*** be possible to scan targets over the constrained network via a centrally-positioned scanner. Scanning a target OS involves hundreds or thousands of 'checks' against individual files to verify if patches have been successfully installed. The time delay added by including a second of latency to each 'check' involved in interrogating the target could add hours to total scan duration.

This configuration is not recommended, and there is no formula to ensure that such a scan will work. Running an un-credentialed scan via a WAN is especially disadvantageous, as it requires more connections to enumerate target vulnerabilities, and scan fidelity can be significantly affected by slow or dropped packets.

In the Scan Policy, increasing the value of the **'Max Checks Per Host'** parameter may improve performance, as the latency involved will limit the resource impacts on the target. Additionally, disabling the TCP/SYN/UDP port scanners (**Port Scanning tab**) and instead relying on **'Max Checks Per Host'** or **'Max Hosts Per Scan'** will generally reduce the total number of

connections. Each chunk will need to complete in less than two hours, this may not be possible with high latency connections or very low bandwidth (under 256 Kilobytes per second (KB/s)).

Scanning Ephemeral Virtual Environments

Some modern workstation environments are leveraging centralizing processing power or utilizing software components to dynamically build and destroy virtual desktop operating systems. This process can occur regularly (every day/week) or dynamically (when prompted by an admin, or as a user logs in). Similar capabilities may be used by servers, including virtual IP addresses associated with clustered applications, containers, software-defined networks, and dynamically allocated server systems. All of these are short lived / non-persistent resources.

Non-persistent environments have two main challenges:

- Data is meaningless in a short period of time, the OS a user is working on may be deleted in hours or days. This can affect retention requirements and the accuracy of the vulnerability data within ACAS
- Over subscription of central resources means that interrogating each host in the network at the same time may have a serious impact on

This section is intended to be vendor agnostic, as such some terminology may differ from a deployed environment:

Ephemeral / non-persistent - transitory, existing only briefly

Persistent – existing for a longer-term or open-ended duration

Image – an operating system that can be presented to the user as “their desktop”

Virtual – no discrete or specific physical existence

Leverage ACAS with Ephemeral Software and Hardware

If the organization is leveraging software or hardware (VMware, Wyse, Citrix, etc….) which is being used to present a non-persistent work environment. It is important that it is document, so that the AO an ACAS team understand what is and is not ephemeral. Sometimes, VIP users or workstations running certain software may have persistent images mixed in the environment, which provides non-persistent images for the majority of users.

Ephemeral user environment instances are often produced by merging a ‘master’ image of the desired OS, the user’s profile or customizations, and the user or organization’s files. Identifying the master image(s) is important to fully validating the risk of the environment. The organization should:

- Know which hosts are persistent and which are not

- Know the maximum capacity of the system
- Know how many master images are in use
- Request recommendations from hardware/software vendor for advice with vulnerability scanning

Validate Ephemeral Software and Hardware

Scan master images on regular basis (determined by reporting requirements, how often the images are updated, and when the ephemeral instances will be updated)

Scan persistent hosts on regular basis (In Accordance With (IAW) reporting requirements), but consider treating the target as resource constrained (as host server may be oversubscribed)

Utilize Nessus and PVS to validate image findings

Between scans of the master image(s), the organization should conduct some form of validation scans to ensure that the user images are in conformance with the master image(s).

- PVS should be utilized for this task as it will provide the good coverage without impacting host performance
- If PVS is not available, utilize Nessus to conduct periodic scans of random targets using target as resources are available

Leveraging Passive Vulnerability Scanner Data

The Passive Vulnerability Scanner (PVS) sensor detects unencrypted network traffic, and uses signatures to vulnerabilities and weaknesses based on observable signatures in the network traffic. PVS leverages data gathered from the headers and payloads of various services and protocols (Examples: HTTP, SSH, or SMTP).

This process is similar to Nessus' network checks, as they are described in Appendix C, and can be very vague or accurate depending upon the plugin in question. If the source of the plugin's assertion that a target is vulnerable is based on the header data, this is prone to generate false positives, as the PVS will not be able to enumerate if for example an Apache web server has been backported to include security features associated with a current release. The opposite of this is that some PVS plugins are triggered based on known bugs which manifest in the actual data, observations of credentials in a URL string, or other weaknesses are very accurate.

Because of the method PVS uses to trigger a plugin is not visible to the user, confidence in PVS identified vulnerabilities should be treated with lower confidence compared to Nessus scan results. It is also important to note, that Nessus scan results do not overwrite PVS results. While a Linux server will often trigger PVS OpenSSH results, if the same host has Nessus results indicating the OpenSSH version is current, the PVS results can be ignored. However, if the

target cannot be scanned via Nessus, the vendor should be engaged to provide assertions that the findings are not accurate.

Leveraging Behavioral PVS Data

Much of the data produced by PVS does not explicitly identify vulnerabilities, these plugins are useful because they can provide network topology and traffic insight.

Appendix F: Performance Tuning

All tasks or functions in SecurityCenter consume resources, some more so than others do. It is beneficial to consider the scheduling of resource intensive tasks and encourage the functions to run in the evening or staggered throughout the day to minimize performance impacts such as database locks.

SecurityCenter Schedule Cleanup

Verify that the scheduled tasks within SecurityCenter are reasonably spaced out. Multiple scans or reports can be configured to run at the same time by multiple users in any/all organizations. SecurityCenter attempts to distribute jobs that are scheduled to occur at the same time while minimizing the interval of time. This distribution method can be easily overcome if a large number of tasks are scheduled to occur at the same time.

```
# /opt/acas/bin/maint-scripts/sc-schedule-enum.sh
```

The script will produce a **.csv** output file, which will be written into the user's home directory. This version of the script parses an existing SecurityCenter debug file, optionally the SQLite database can be queried (this should be done when the SecurityCenter is not under high utilization). For example:

Organization_name(#ID)	Owner ID	Schedule	Object ID	Object Type	Schedule Type	Repeat Rule	Start Time	Dependent upon Schedule ID
...								
Application	1	29	-1	feedUpdate	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170308T014000(0540Z)	
Application	1	30	-1	IcePluginUpdate	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170308T030500(0705Z)	
...								
Test Organization(#1)	a.test	1	Severity Trending|Vulnerability Overview	evaluateDashboardElement	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170308T111411(1514Z)	
Test Organization(#1)	a.test	2	Vulnerability Trending|Vulnerability Overview	evaluateDashboardElement	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170308T111411(1514Z)	
Test Organization(#1)	a.test	3	Top 10 Vulnerabilities|Vulnerability Overview	evaluateDashboardElement	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170308T111411(1514Z)	
...								
Example Organization(#2)	j.example	24	Executive 7 Day - Mitigated Vulnerability Type Matrix	evaluateMatrixCluster	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170420T134456(1744Z)	
Example Organization(#2)	j.example	25	Executive 7 Day - Mitigated Vulnerability Type Matrix	evaluateMatrixCluster	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170420T134456(1744Z)	
Example Organization(#2)	j.example	26	Executive 7 Day - Mitigated Vulnerability Type Matrix	evaluateMatrixCluster	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170420T134456(1744Z)	
Example Organization(#2)	j.example	27	Executive 7 Day - Mitigated Vulnerability Type Matrix	evaluateMatrixCluster	ical	FREQ=DAILY;INTERVAL=1	TZID=America/New_York:20170420T134456(1744Z)	
...								

SecurityCenter Configuration Tuning

If users run resource-intensive reports during the day, schedule scans for nights or weekends. Use Post Scan settings to run reports automatically at the end of a scan so that they are ready for users without needing to be run manually.

You can reduce scan run times using the following techniques:

- Stagger scans so that less is running simultaneously. One way to do this is to chain dependent scans so that dependent scans do not start until the previous scan finishes. Note however, that if a scheduled scan fails, the subsequent dependent scans will not run. Another way to do this is to estimate based on the average run time of a scheduled scan how long it should take, and arrange scans based on this information.
- Add scanners to the scan zones. This helps with being able to stagger the scans.
- Optimize the scan policies. Use `netstat` local port enumerators over network port scanners when possible.
- Separate web application tests and compliance checks (SCAP & Tenable audit) into separate scans and run them less often if possible.
- Configure dashboards to evaluate less often or manually, and when possible share dashboards rather than creating copies.

Minimize Historical Data

Keeping the data in SecurityCenter will adversely affect performance, our recommendations are (System > Configuration > Data Expiration):

Vulnerability Data Lifetime

- Active 30-90
- Passive 7
- Event 365 (LCE customers should tailor this value down to 30-90 days)
- Compliance 30
- Mitigated 60

User Generated Object Lifetime

- Closed Tickets 365
- Scan Results 30-90
- Report Results 30-90

To download plugins from the DOD (DISA) plugin server, a client machine must be connected to the NIPRNet or SIPRNet as appropriate. This setting is configured, by an Admin user.

Feed Locations:

NIPR: https://acas-update.csd.disa.mil/
SIPR: https://acas-update.csd.disa.smil.mil/

Configure SecurityCenter 5.x:

System > Configuration > License, place the links under the ACAS Feeds section for Plugin Site and SC Feed Site.

Pre-checks

The plugin server is in a network where legacy controls (reverse DNS lookup) are enforced, so there are a few pre-checks:

- Reverse DNS entry - The server's public IP address should have a PTR record to ensure the IP address resolves to a .mil hostname
  - `# nslookup <ip address>`
  - Ensure a proper response returns with .mil
- Ensure that systems are networked to the NIPR or SIPR. DREN and S/DREN are not supported.
- Ensure that the correct URL in the 'Plugin Site' field is entered.
- Provide a screen capture image to ACAS Customer Support, if requested, showing the entire string. Ensure that the system has the DOD root certificates for the appropriate classification:
  - `# ls -la --sort=t /opt/sc*/data/CA/`
  - Response should include a hash file for each certificate, and the hash and certificate should have very close updated times/dates.
- If problems occur with automatic or manual updates AND manual uploads, start with Disk checks.

Connectivity Tests

If pre-checks are okay:

- Test basic connectivity, including DNS, and capturing the CA certificate that signed the plugin server's identity certificate
  - NIPR: `# openssl s_client -connect acas-update.csd.disa.mil:443`
  - SIPR: `# openssl s_client -connect acas-update.csd.disa.smil.mil:443`

- Check for blatant errors, check for accurate "subject=" and "issuer=" lines to ensure the certificate's CN is correct and it is signed by the correct CA server.

- Test downloading from the plugin server, using the SecurityCenter's root DOD certificates:
  - NIPR: **`# curl -O --capath /opt/sc*/data/CA https://acas-update.csd.disa.mil/sc-plugins.tar.gz`**
  - SIPR: **`# curl -O --capath /opt/sc*/data/CA https://acas-update.csd.disa.smil.mil/ sc-plugins.tar.gz`**
  - Check for errors that point to bad CA certificates. If this is received, attempt to reload CA root certificates. If a reload does not help, check for proxy, or any other intelligent network device that might be mangling packets.
  - If this command works without error, move to disk checks.
- Test downloading from the plugin server, without checking server identity certificate:
  - NIPR: **`# curl -Ok https://acas-update.csd.disa.mil/sc-plugins.tar.gz`**
  - SIPR: **`# curl –Ok https://acas-update.csd.disa.smil.mil/ sc-plugins.tar.gz`**
  - Check to ensure file downloads properly, if this fails, verify local firewall settings and route ticket to the Consolidated Communications Center (CCC).
- Test connectivity to another DOD server, using the SecurityCenter's root DOD certificates:
  - NIPR: **`# curl --capath /opt/sc*/data/CA https://www.disa.mil/index.html`**
  - SIPR: **`# curl --capath /opt/sc*/data/CA https://www.disa.smil.mil/index.html`**
  - If this fails, have user check local firewall settings.
- Test downloading from another DOD server, using the SecurityCenter's root DOD certificates:
  - NIPR: **`# curl -O --capath /opt/sc*/data/CA https://www.disa.mil/index.html`**
  - SIPR: **`# curl -O --capath /opt/sc*/data/CA https://www.disa.smil.mil/index.html`**
  - If the connection fails, have user check local firewall settings.

Disk Tests

The final sets of checks are for disk access / permissions. The objective is to ensure all files have the correct ownership – Tenable Network Security (TNS) - (**`tns:tns`**) and the default file permissions.

- Verify the disk has available space:
  - **`# df -h /opt/sc*`**
  - Check the 'Avail' column to ensure free space is > 1 GB
- Verify that Anti-Virus is configured IAW ACAS-HBSS Integration Guide.
  - Although you may not be able to send any verification to ACAS Customer Support, it is important to ensure that you have verified this as it will greatly slow troubleshooting if AV/HBSS logs are not verified.

- Verify that no changes have been made to any directory or file ownership or permissions:
- **# find /opt/sc* ! -user tns -type f**
- **# find /opt/sc* ! -group tns -type f**
- (user and group should be identical) index.html & httpd.pid are acceptable
- **# find /opt/sc* ! -user tns -type d**
- **# find /opt/sc* ! -group tns -type d**
- (user and group should be identical) the www directory and any other directories where the user may have 'bind mounted' a separate partition for more storage are acceptable

Plugin Upload Error

There are known issues with PHP settings in SecurityCenter 4 and 5, which can affect uploading plugins.

Troubleshooting manual upload of plugins:

```
# df -h
# free -m
# vmstat -a
# top
```

Hash of **.tar.gz**

The **sc-upload-fix.sh** script will apply the settings below, script can be found on the patch repository. The example below has resolved most customer issues (as of June 2016). If the values below do not resolve the issue, try incrementing all values up by .2, until 'memory_limit' is 2.0G or contact the ACAS Customer Support Desk:

Stop SecurityCenter

Edit **/opt/sc/support/etc/php.ini**

Increase the max upload file size:

```
# sed -i  '/upload_max_filesize =/c\upload_max_filesize = 1.5G' \
/opt/sc*/support/etc/php.ini
```

Increase the max http post size:

```
# sed -i  '/post_max_size =/c\post_max_size = 1.7G' \
/opt/sc*/support/etc/php.ini
```

Increase the memory limit:

```
# sed -i  '/memory_limit =/c\memory_limit = 1.0G' \
/opt/sc*/support/etc/php.ini
```

ACAS Customer Support

If there is no clear solution, open a ticket with a sanitized diagnostic/debug file and the output of the above commands. The site should begin manually updating the SecurityCenter, as some of these issues are exceptionally difficult to troubleshoot.

- Contact information for the ACAS (OKC) Customer Support Service Desk appears in Appendix A.
- Instructions for obtaining sanitized diagnostic/debug information from ACAS appears in Appendix I.

Appendix H: SecurityCenter DB Lock Troubleshooting Detail

Database locks are a commonly reported problem by our customers, but in some cases, it can be difficult to pinpoint exactly what is causing them. The most common causes are resource bottlenecks, database corruption, and hardware failure. You will always want a full SecurityCenter debug to investigate database lock issues, and if the locks have been happening since before the earliest date in the admin log in the debug, you will want full admin logs going back to when the problem started.

Essentially, a database lock occurs when a process tries to access a database that is locked as in use by another process. This can happen under normal conditions, and does not always indicate that there is a major problem. Database locks become a major problem if they are happening frequently and interfering with functionality.

When a customer reports that they are experiencing frequent database locks, or if they report other issues such as errors and slowness in the web interface or certain functions failing, and you discover frequent database locks in their logs, the first recommendation should be to check the hardware.

Hardware issues are not the most likely cause of database locks, but they are the most likely to cause data loss if they are not discovered. Our first priority should be preventing data loss. As a precaution, before further troubleshooting is performed, the customer should stop the SecurityCenter and all of its processes and take a full backup of the `/opt/sc` directory, and move the backup to a safe location on different hardware. This means that saving the backup on another VM in the same cluster should not be done – if the hardware is failing, they could lose the whole cluster, and their backup along with it. Once they have a good backup, they should test the hardware integrity and resolve any hardware issues before proceeding. If they have hardware monitoring configured, they may be able to check for hardware issues through the monitoring interface as well.

If the locks are caused by database corruption, analysis of the logs should help to identify the issue. The most common causes of database corruption are the disk becoming full while a database is in use or an unexpected crash while a database is in use.

SecurityCenter will log to the Administrator log if the disk is full - just search for "disk is full". If you want to search further back than the debug for previous issues of the disk being full, have the customer log in to SecurityCenter as admin, go to Status > Logs, switch the Source to Administrator, and search the logs for "disk is full". This should search all existing logs.

Checking for crashes is not quite as simple. If SecurityCenter was terminated unexpectedly as part of a system crash, it likely did not have the opportunity to log the incident. Instead, you

can look for SecurityCenter starting back up with an unexplained gap in logs just prior. When SecurityCenter starts, **Jobd** will also start, so search the logs for "`Jobd starting`".

Example results:

```
Mon, 04 Aug 2014 11:37:35 -0400||message|INFO|0|Jobd starting...
Mon, 18 Aug 2014 07:56:34 -0400||message|INFO|0|Jobd starting...
Tue, 19 Aug 2014 16:36:57 -0400||message|INFO|0|Jobd starting…
```

Jobd should only be starting if SecurityCenter is starting or restarting, or if the Job Scheduler has been manually stopped and started from the System Status screen. If it is starting without explanation, then it was stopped for some reason, possibly because **Jobd** crashed, SecurityCenter crashed, or the host OS crashed.

Normally, the SecurityCenter admin log will contain regular logs from jobs that run every hour, every 15 minutes, etc. For example, "Applying recast and accept risk rules" should happen every hour. If you see **Jobd** starting and a long gap in time between the "`Jobd starting`" log and the log immediately prior, then the system may have been down. The customer can check with their system administrator to find out if there was an outage or other system issue during that time, and they can check the system logs on the host OS for more information.

If it is found that the issue started in response to a full disk or unexpected outage, databases may have been damaged. A full restore to a backup taken prior to the incident is often the best way to recover in these situations. If the disk is currently full, the disk capacity should be expanded prior to restoring the backup. If you can determine that a specific database was affected based on the Administrator logs, it may be possible to recover with the help of the vendor's development team, however SecurityCenter stability and consistency depends upon several interrelated databases being in a consistent state. It is generally inadvisable to restore individual files or databases in a SecurityCenter installation. Again, a full restore to a complete backup that was taken while SecurityCenter was stopped is usually the ideal recovery from corrupted database issues.

If the hardware integrity is sound, and no incidents were found of the disk becoming full or outages occurring prior to the time when the database locks occurred, probably the most common cause of database locks is overloaded resources.

Common activities that may incur heavy resource usage and contribute to database locks are scans and reports. When many scan jobs or reports are running simultaneously, starting at the same time, or ending at the same time, this can cause database locks. To look for these patterns, search the debug files, including `sc-logs.txt`, or admin logs. The logs will not report the number of simultaneous scans or reports, but you can look for when these jobs are starting and ending as well as when the locks are occurring to see if there is a pattern. Regex searching in Notepad++ is a great way to do this.

For example, you can search with the following search term:

```
(^(?=.*\bScan job\b)(?=.*\bstarting\b).*$)|(^(?=.*\bScan
job\b)(?=.*\bacquired\b).*$)|(^(?=.*\bScan job\b)(?=.*\bhas
ended\b).*$)|(^(?=.*\bReport
job\b)(?=.*\bstarting\b).*$)|(^(?=.*\bReport
job\b)(?=.*\bacquired\b).*$)|(^(?=.*\bReport job\b)(?=.*\bhas
ended\b).*$)|(is locked)
```

Open **sc-logs.txt** or the admin log(s) in Notepad++. CTRL+F to open the search box and paste in the string above. At the lower left of the search window, select Regular expression. In the list of Find buttons near the upper right of the search box, click Find All in Current Document.

Look through the search results and see if there are many jobs starting before previous jobs have ended. You can tally in your head (or on paper) how many jobs may be running simultaneously by counting when jobs start and down when they end. SecurityCenter can handle simultaneous jobs, but the number of simultaneous jobs it can handle depends heavily upon resources and whether or not the jobs are using the same databases.
To check the current resources for obvious red flags such as allocations below the minimum recommendations, check **sc-systeminfo.txt**.

- To jump to memory, search for "`Results of "free" are:`" - this will take you to output similar to the following, showing about 8 GB total memory:

```
Results of "free" are:
                 total       used  free    shared    buffers     cached
Mem:             8174580     6470596     1703984       0         34896
      4782120
-/+ buffers/cache:           1653580     6521000
Swap:                  4095992 0   4095992
```

- To jump to CPUs, search for "`Brought up`" - this will take you to the CPU count, followed by additional information:

```
Brought up 1 CPUs
time.c: Using 3.579545 MHz WALL PM GTOD TSC Timekeeping timer.
time.c: Detected 1997.386 MHz processor.
```

To check storage information, search for "`scsi0`" - this should jump you to near the beginning of information about the types of storage devices attached. This information can be used to estimate IOPS, but the database locks debugging is more reliable to check actual usage and wait. This information is good for getting a general idea of what type of storage is used, for example:

```
scsi0 : ioc0: LSI53C1030 B0, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=51
 Vendor: VMware Model: Virtual disk Rev: 1.0
 Type: Direct-Access ANSI SCSI revision: 02
target0:0:0: Beginning Domain Validation
target0:0:0: Domain Validation skipping write tests
target0:0:0: Ending Domain Validation
target0:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
```

```
SCSI device sda: 220200960 512-byte hdwr sectors (112743 MB)
```

or:

```
scsi0 : LSI SAS based MegaRAID driver
megasas: 0x1000:0x0060:0x1028:0x1f0c: bus 25:slot 0:func 0
megaraid_sas 0000:19:00.0: PCI INT A -> GSI 17 (level, low) -> IRQ 17
megaraid_sas 0000:19:00.0: setting latency timer to 64
megasas: FW now in Ready state
megasas_init_mfi: fw_support_ieee=0
megasas: INIT adapter done
scsi 0:0:33:0: Enclosure DELL MD1000 A.04 PQ: 0 ANSI: 5
scsi 0:0:34:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:35:0: Direct-Access ATA ST1000NM0011 PA09 PQ: 0 ANSI: 5
scsi 0:0:36:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:37:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:38:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:39:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:40:0: Direct-Access ATA ST31000524NS KA05 PQ: 0 ANSI: 5
scsi 0:0:41:0: Direct-Access ATA ST1000NM0011 PA09 PQ: 0 ANSI: 5
scsi 0:0:42:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:43:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:44:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
scsi 0:0:45:0: Direct-Access ATA ST31000340NS MA0D PQ: 0 ANSI: 5
megaraid_sas 0000:19:00.0: Controller type: MR,Memory size is: 256MB
megaraid_sas: fw state:c0000000
megasas: fwstate:c0000000, dis_OCR=0
```

If hardware monitoring enabled, you can also check resources that way. To determine the disks that **`/opt/sc`** is mounted on search **`sc-systeminfo.txt`** for "**`df -a`**" for this info. Are there resource spikes correlating with the database locks in the SecurityCenter logs? If the SecurityCenter host is running as a virtual machine, does the management software for the virtual machine (such as vCenter for VMware, for example) show any issues logged for that host or for resource usage in general?

To resolve database locks caused by resource bottlenecks, there are two basic options: increase resources, or decrease/spread out usage. To spread out usage, try the following:

- Lower scan run time by optimizing the scan policies, as discussed in SecurityCenter Configuration Tuning.
- If users run resource-intensive reports during the day, schedule scans for nights or weekends.
- Use post-scan settings to run reports automatically at the end of a scan so that they are ready for users without needing to be run manually.
- Configure dashboards to evaluate less often or manually, and when possible share dashboards rather than creating copies.

If there is not a consistent pattern of heavy usage around the time of the locks, look for other patterns. Are locks happening every time a certain job starts? There may be an issue with that particular job. Are they happening at the same time every day? There may be other processes

on the SecurityCenter host that are incurring heavy resource usage, such as an automated backup or scheduled **`cron`** job.

Appendix I: Generate Debug Data for Support

SecurityCenter debug:

WebUI (SecurityCenter 5.x):

1. Login as an administrator, click on 'System > Diagnostics'
2. Click 'Create Diagnostics File'
3. Toggle "Strip IPs from Chapters"
4. Ensure all Chapters are selected (enabled)
5. Click 'Generate File' …generation may take some time, you can wait or return later
6. Click 'Download Diagnostics File'

Linux CLI (SecurityCenter):

```
# /opt/sc*/support/bin/php /opt/sc*/src/tools/debug.php -at
```

Nessus debug:

Linux (Nessus 6.X)

Run the debug script from an administrator-level command prompt.

```
/opt/nessus/sbin/nessuscli bug-report-generator
```

Windows (Nessus 6.X)

Run the debug script from an administrator-level command prompt.

```
…\Program Files\Tenable\Nessus\nessuscli bug-report-generator
```

Then select 'full', and wait for the message 'Finished Nessus Debug Utility:'

RESULTS (Windows Vista, 2008, 7, 8 and 2012):

```
…\ProgramData\Tenable\Nessus\nessus\logs\nessus-bug-report-archive.txt
```

Linux (PVS 4.2+ & 5.x)

Run the debug script from an administrator-level command prompt.

```
/opt/pvs/bin/debug.sh
```

- Choose 'full' for standard debug, 'limited' for sanitized debug

Windows (PVS 4.2+ & 5.x)

Run the debug script from an administrator-level command prompt.

```
…\Program File\Tenable\pvs\debug
```

- Choose 'full' for standard debug, 'limited' for sanitized debug

Appendix J: Generating a Nessus KB or DB file

If you encounter an issue that requires engineering assistance, you will likely be asked to provide either a `.nessus` and KB file or a Nessus DB file. These files contain the information that was used to determine each vulnerability.

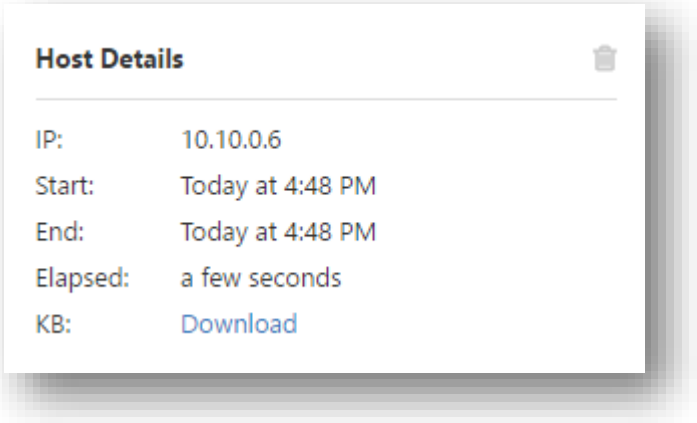
A `.nessus` and KB file or a Nessus DB file is only available from a scan launch directly from Nessus. Troubleshooting issues is the only time scans should be launched directly from Nessus.

Follow these steps:

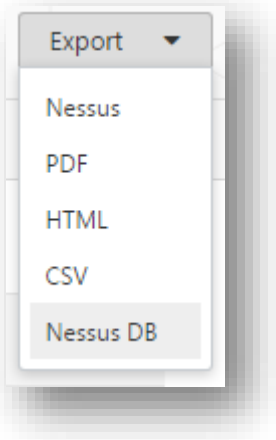
1. In SecurityCenter, download the scan policy.
2. Log into Nessus.
3. Select the "policies" tab.
4. Import the scan policy that you downloaded from SC.

After the policy has been uploaded, double click on it and go the "Credentials tab" to provide valid credentials for that host that will be scanned (ideally the same credentials SecurityCenter is configured to use). Finally, go to "Scans" click “Add” and input the name, type, policy, and the host target IP address.

A KB file is available for each host. Drill into a host by clicking on its IP address and locate the download link on the right.



The **Nessus DB** is best described as the entire database of the scan. When those are imported into Nessus you can see scan results, KBs, and audit trails. It is located under the Export tab. The `.nessus` file (**Nessus**) is also located under the Export tab. The `.nessus` file would just contain the scan result. You wouldn't be able to pull the KB or audit trail from it, and wouldn't be able to launch the scan either.



Appendix K: Tenable Software Error Codes

The SecurityCenter logs with a numeric error code but have no idea what the number means.
Example:

```
8182:Sat, 12 Jun 2010 04:30:02 -0400||error|CRITICAL|0|Job #3152 (type: passivePluginUpdate
id: -1) exited with error code #146.
```

What is error code #146?
…In most cases, viewing the context of the error message helps more than the actual numeric code with diagnosing the root cause. In our example above, the following logs surround our error:

```
8178:Sat, 12 Jun 2010 04:30:01 -0400|PassivePluginUpdate|message|INFO|0|Passive Plugin Update
job #3152 has started.
8179:Sat, 12 Jun 2010 04:30:01 -0400|PassivePluginUpdate|error|CRITICAL|0|Invalid response
'302' from 'www.tenablesecurity.com'.
8180:Sat, 12 Jun 2010 04:30:01 -0400|PassivePluginUpdate|error|INFO|0|Invalid response '302'
from 'www.tenablesecurity.com'.
8181:Sat, 12 Jun 2010 04:30:01 -0400|PassivePluginUpdate|message|INFO|0|Passive Plugin Update
job #3152 has ended.
8182:Sat, 12 Jun 2010 04:30:02 -0400||error|CRITICAL|0|Job #3152 (type: passivePluginUpdate
id: -1) exited with error code #146.
```

In the example above, "`passivePluginUpdate error code #146`" is not very helpful, nor is the associated code description (see below) of "`RESPONSE_INVALID_DATA`". The surrounding messages indicate that the server: www.tenablesecurity.com returned a '302' error, which is not a typical HTTP response for daily SecurityCenter activity. In this case, the context contained the most detail for debugging the issue.

Error 500

The "`Error(500)`" message in Nessus is a generic error that can occur for different reasons. In most cases, reloading the plugins or resetting the scanner will eliminate the issue. In other cases, you can force the scanner to rebuild the global.db file:
Linux:

```
# service nessusd stop
# mv /opt/nessus/var/nessus/global.db  /opt/nessus/var/nessus/global.db.bak
# service nessusd start
```

Windows:

```
# Net stop "Tenable Nessus"
# Move …\ProgramData\Tenable\Nessus\nessus\global.db
…\ProgramData\Tenable\Nessus\nessus\global.db.bak
# Net start "Tenable Nessus"
```

Verify the proxy settings are correct as appropriate, and if the scanner does not switch to 'Working' status contact the OKC service desk.

SecurityCenter Error Codes

The numeric error code may assist an administrator in debugging an issue.
See the code list below for the error string descriptions:

Description	Code
RESPONSE_UNKNOWN	-1
RESPONSE_OK	0

RESPONSE_WARNING	65536 (Warnings are all > 65535)
RESPONSE_NO_MODULE	10
RESPONSE_NO_ACTION	11
RESPONSE_BAD_TOKEN	12
RESPONSE_BAD_JSON	13
RESPONSE_CONFIGURATION_ERROR	60
RESPONSE_NOT_CONFIGURED	61
RESPONSE_UNAVAILABLE	62
RESPONSE_DENIED	63
RESPONSE_DISABLED	64
RESPONSE_EXPIRED	65
RESPONSE_REREGISTER	66
RESPONSE_CONNECTION_ERROR	67
RESPONSE_STOPPED	68
RESPONSE_KILLED	69
RESPONSE_CANTFORK	70
RESPONSE_FILE_READ_ERROR	101
RESPONSE_FILE_WRITE_ERROR	102
RESPONSE_FILE_FORMAT_ERROR	103
RESPONSE_MISSING_FILE	104
RESPONSE_FILE_OPEN_ERROR	105
RESPONSE_FILESYSTEM_ERROR	106
RESPONSE_UPLOAD_ERROR	107
RESPONSE_FILE_COPY_ERROR	108
RESPONSE_UNEXPECTED_DATA	141
RESPONSE_MISSING_REQUIRED_INPUT	142
RESPONSE_INVALID_FILTER	143
RESPONSE_NAME_EXISTS	144
RESPONSE_DATA_DOES_NOT_EXIST	145
RESPONSE_INVALID_DATA	146
RESPONSE_NOT_FOUND	147
RESPONSE_EXISTS	148
RESPONSE_INVALID_CREDENTIALS	161
RESPONSE_INVALID_USER_OBJECT	162
RESPONSE_NO_PERMISSION	163
RESPONSE_LDAP_ERROR	171
RESPONSE_DATABASE_SETUP_FAILURE	201
RESPONSE_DATABASE_ERROR	202

Appendix L: SCAP (STIG) Scanning with ACAS

The Security Content Automation Protocol, or SCAP, is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The National Vulnerability Database (NVD) hosts the U.S. Government content repository for SCAP.

General SCAP / Audit Scanning Recommendations:

- Use a different repository for SCAP & STIG scan data.
- Use the same scan credential used for vulnerability scans.
- ACAS cannot resolve the difference between a Windows Member Server and Domain Controller. Separate Member Server and Domain Controller audit files between different scan policies.
- Use plugin 66758 - SCAP XML Results for overall IP address counts.
- SecurityCenter's WebUI incorrectly reuses severity for compliance check status:
    - Severity High: Benchmark Failed (setting wrong).
    - Severity Informational: Benchmark Passed (setting correct)
    - Severity Medium: Benchmark Undetermined (setting cannot be verified). If a lot of medium findings are shown in the same scan, the scan credential used maybe incorrect (locked, expired, etc.). Also a medium finding may indicate the system requires a reboot or busy with a process.

SCAP assigns a Severity Code to each system IA security weakness to indicate the risk level associated with the IA security weakness, and the urgency with which the corrective action must be completed.

Note the SCAP Severity Codes are not the same as the CVSS based Severity Codes used in ACAS used to denote vulnerability risk levels. SCAP severities are direct corelations, high = CAT I, medium = CAT II, and low = CAT III

SCAP reuses many internal functions that support '.audit' files, as a result the web UI will often refer to audit, but in most cases SCAP content can be used interchangeably.

SCAP benchmarks should be downloaded from the IASE website, do not use benchmarks that are labeled (SCC tool use only), additionally the organization should use content containing OS benchmarks. The benchmark is loaded as an audit Scans > Audit Files, click '+Add', then click Advanced, For 'Audit File' select the SCAP benchmark's zip file. Dropdown boxes will appear, Benchmark Type and Benchmark Name should be prepopulated, Profile should be selected as

appropriate for the environment/targets. A name is required and a description is recommended.

When executing a SCAP, start with the Configuration scan policy template, or an organizational equivalent policy. A new policy will need to be created that includes any audit or SCAP configuration assessments to be performed. As a result, it is often easier to copy the provided configuration scan policy, then rename the copy and associate audit files to the policy and save as a final policy.

The actual scan should be executed against a static or dynamic asset list to minimize running the SCAP benchmarks against the wrong target OSes. The SCAP module will evaluate the target OS against the benchmark, if the benchmark does not match it will not be run against the target.

ACAS can provide reports that present the analyst with vulnerability information within the environment. Data is presented on the number of SCAP Severity vulnerability concerns, networks that have SCAP vulnerability results, when audits have been performed, IP Summary, and a SCAP vulnerability summary with failing items.

The report and its components are available in the SecurityCenter Feed, an app store of dashboards, reports, and assets. The report can be easily located in the SecurityCenter Feed by selecting the category Threat Detection & Vulnerability Assessments, and then selecting the tag SCAP.

SCAP benchmarks must be used in a scan before they become selectable in ASR/ARF reports templates.

The report should contain the following chapters:

1. Audit Summary - This chapter displays an indication of SCAP Nessus scans present over the last 7, 30, or more than 30 days. A bar chart is displayed with vulnerability severity/totals by Class C address, and an IP Summary that presents pass/fail results.
2. Severity High - This chapter displays the failed compliance results for SCAP Severity Level High. SCAP Severity Levels are assigned to specific vulnerabilities to indicate the associated risk level. The Severity Level can assist in determining the urgency with which the corrective action must be completed. The Severity High table provides details if vulnerability results exist for the specified Severity level. This is accomplished using the Vulnerability Summary – IP Detail tool, and text filters.
3. Severity Medium - This chapter displays the failed compliance results for SCAP Severity Level Medium. SCAP Severity Levels are assigned to specific vulnerabilities to indicate the

associated risk level. The Severity Level can assist in determining the urgency with which the corrective action must be completed. The Severity Medium table provides details if vulnerability results exist for the specified Severity level. This is accomplished using the Vulnerability Summary – IP Detail tool and text filters.

4. Severity Low - This chapter displays the failed compliance results for SCAP Severity Level Low. SCAP Severity Levels are assigned to specific vulnerabilities to indicate the associated risk level. The Severity Level can assist in determining the urgency with which the corrective action must be completed. The Severity Low table provides details if vulnerability results exist for the specified Severity level. This is accomplished using the Vulnerability Summary – IP Detail tool and text filters.

Appendix M: Scanning Stale Hosts in Dynamic Networks

The following are instructions for creating dynamic combination asset lists to identify stale hosts in a dynamic network.

Description of the process:

1. Schedule a frequent ping sweep scan; running one or more times per day.
2. Create an asset list that includes hosts/devices that have been pinged in the last 24 hours. This is the closest way to assert that a host is online without using PVS. Create an asset list that provides a tally of hosts that need to be scanned based upon showing old credentialed scan data. For testing and demonstration, we used one week as the date criterion. Your definition of "old" may vary. Newer versions of SecurityCenter can accomplish this in one asset list, example below.
3. Create a combination asset list that includes both of the asset lists previously created. This asset list contains hosts which are online (ping sweep) that also require scanning (old credentialed scan data).
4. Create an alert that triggers when a new IP address populates the combination asset list. This alert causes a scan of the targets in the combination asset list.

Steps:

Step	Action
1	Create an active scan; scheduled to run daily to ping sweep the networks where dynamic hosts reside or use the host and OS discovery scan policy from Best Practice Scan Policies

2	Create a Dynamic Asset list that contains the IPs of hosts not included in a credentialed scan within the past *"**N**"* days. Note: Use this with Windows & UNIX/Linux targets.
	• ALL of the following are true:
	  ○ ANY of the following are true:
	  ▪ Days since Observation is less than 1 where plugin ID 12
	  ▪ Days since Observation is less than 1 where plugin ID 10180
	  ○ ANY of the following are true:
	  ▪ Days since Observation is greater than ***N*** where plugin ID 10394 (Authenticated Check: OS Name and Installed Package Enumeration)
	  ▪ Days since Observation is greater than N where plugin ID 12634 (Microsoft Windows SMB Log In Possible)

3	Create an active scan; set to run On Demand, based on the organization's vulnerability scan policy or use the vulnerability scan policy from Best Practice Scan Policies. • If the site is monitoring hosts in multiple repositories, create a scan template for each repo.
4	Create an alert to filter on the asset list (presumably based on a specific repository), trigger if IP count >= 1, add action type scan, with the policy defined in step 3.
5	If the site is monitoring multiple repositories, create an alert for each repository and include the repository in question in the filter. Under scan action, use the scan template defined in step 3.


ASSURED COMPLIANCE
ACAS
ASSESSMENT SOLUTION

Appendix N: Enabling Credentialed Security Checks

Enable SSH Local Security Checks

This section applies to Unix/Linux and Network Devices

This section is intended to provide a high-level procedure for enabling SSH between the systems involved in the Nessus credentialed checks. It is not intended to be an in-depth tutorial on SSH. It is assumed the reader has the prerequisite knowledge of UNIX/Linux system commands.

Generate SSH Public and Private Keys

The first step is to generate a private/public key pair for the SecurityCenter/Nessus scanner to use.

This key pair can be generated from any of your UNIX/Linux systems, using any user account. However, it is important that the keys be owned by the defined Nessus user.

To generate the key pair, use **`ssh-keygen`** and save the key in a safe place. In the following example, the keys are generated on a Red Hat Enterprise Linux installation:

```
# ssh-keygen -b 4096

Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
/home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
```

The private key can be used as a credential in SecurityCenter. When ssh-keygen asks you for a passphrase, enter a strong passphrase or hit the Return key twice (i.e., do not set any passphrase). If a passphrase is specified, it must be specified in the Credentials → SSH settings options in order for SecurityCenter to use key-based authentication.

Create a User Account and Setting up the SSH Key

On every target system to be scanned using local security checks, create a new user account dedicated to Nessus. This user account must have exactly the same name on all systems. For this document, we will call the user nessus, but you can use any name.

Once the account is created for the user, make sure that the account has no valid password set. On Linux systems, new user accounts are locked by default, unless an initial password was explicitly set. If you are using an account where a password had been set, use the **`passwd -l`** command to lock the account.

You must also create the directory under this new account's home directory to hold the public key. For this exercise, the directory will be **`/home/nessus/.ssh`**. An example for Linux systems is provided below:

```
# passwd -l nessus
# mkdir /home/nessus/.ssh
# chown -R nessus /home/nessus * this should be run again, after the public
key has been copied to the target
```

For Solaris 10 systems, Sun has enhanced the **`passwd`** command to distinguish between locked and non-login accounts. This is to ensure that a user account that has been locked may not be used to execute commands (e.g., cron jobs). Non-login accounts are used only to execute commands and do not support an interactive login session. These accounts have the NP token in the password field of **`/etc/shadow`**. To set a non-login account and create the SSH public key directory in Solaris 10, run the following commands:

```
# passwd -N nessus
# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
```

Now that the user account is created, you must transfer the key to the system, place it in the appropriate directory and set the correct permissions.

From the system containing the keys, secure copy the public key to systems that will be scanned for host checks as shown below. 192.1.1.44 is an example remote system that will be tested with the local security checks.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
```

Credentialed Checks in Windows

Prerequisites

A very common mistake is to create a local account that does not have enough privileges to log on remotely and do anything useful. By default, Windows will assign new local accounts Guest privileges if they are logged into remotely. This prevents remote vulnerability audits from succeeding. Another common mistake is to increase the amount of access that the Guest users obtain. This reduces the security of your Windows server.

Enable Windows Logins for Local and Remote Accounts

The most important aspect about Windows credentials is that the account used to perform the checks should have privileges to access all required files and registry entries, and in many cases, this means administrative privileges. If Nessus is not provided the credentials for an administrative account, at best it can be used to perform registry checks for the patches. While this is still a valid method to determine if a patch is installed, it is incompatible with some third party patch management tools that may neglect to set the key in the policy. If Nessus has administrative privileges, then it will actually check the version of the dynamic-link library (.dll) on the remote host, which is considerably more accurate.

Configure a Local Account

To configure a stand-alone Windows server with credentials to be used that is not part of a domain, simply create a unique account as an administrator.

Make sure that the configuration of this account is not set with a typical default of 'Guest only: local users authenticate as guest'. Instead, switch this to 'Classic: local users authenticate as themselves'.

To configure the server to allow logins from a domain account, the Classic security model should be invoked.

1. Open Group Policy by clicking on start, click Run, type gpedit.msc and then click OK.
2. Select Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.
3. From the list of policies, open Network access: Sharing and security model for local accounts.
4. In this dialog, select Classic – local users authenticate as themselves and click OK to save this.

This will cause users local to the domain to authenticate as themselves, even though they are actually not physically local on the particular server. Without doing this, all remote users, even real users in the domain, will actually authenticate as a Guest and will likely not have enough credentials to perform a remote audit.

The gpedit.msc tool is not available on some version such as Windows 7 Home, which is not supported by Tenable.

Configure a Domain Account for Authenticated Scanning

To create a domain account for remote host-based auditing of a Windows server, the server must first be Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Windows 7, and Windows 8, Windows 10, and be part of a domain.

Create a Security Group called Nessus Local Access

1. Log onto a Domain Controller, open Active Directory Users and Computers.

2. Create a security Group from 'Menu' select Action → New → Group.
3. Name the group Nessus Local Access. Make sure it has a Scope of Global and a Type of Security.
4. Add the account you will use to perform Nessus Windows Authenticated Scans to the Nessus Local Access group.

Create Group Policy called Local Admin GPO

1. Open the Group Policy Management Console.
2. Right click on Group Policy Objects and select New.
3. Type the name of the policy Nessus Scan GPO.

Add the Nessus Local Access group to the Nessus Scan GPO

1. Right click Nessus Scan GPO Policy then select Edit.
2. Expand Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups.
3. In the Left pane on Restricted Groups, right click and select Add Group.
4. In the Add Group dialog box, select browse and type Nessus Local Access and then click Check Names.
5. Click OK twice to close the dialog box.
6. Click Add under This group is a member of:
7. Add the Administrators Group.
8. Click OK twice.

Nessus uses SMB (Server Message Block) and WMI (Windows Management Instrumentation) for this we need to make sure that the Windows Firewall will allow access to the system.

Allow WMI on Windows Vista, 7, 8, 10, 2008, 2008R2 and 2012 Windows Firewall

1. Right click Nessus Scan GPO Policy then select Edit.
2. Expand Computer configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules
3. Right-click in the working area and choose New Rule…
4. Choose the Predefined option, and select Windows Management Instrumentation (WMI) from the drop-down list.
5. Click on Next.
6. Select the Checkboxes for:

```
Windows Management Instrumentation (ASync-In)
Windows Management Instrumentation (WMI-In)
Windows Management Instrumentation (DCOM-In)
```

7. Click on Next
8. Click on Finish

Later, you can edit the predefined rule created and limit the connection to the ports by IP Address and Domain User to reduce any risk for abuse of WMI.

Link the GPO

1. In Group policy management console, right click on the domain or the OU and select Link an Existing GPO
2. Select the Nessus Scan GPO

Configure Windows 2008, Vista, and 7

1. Under Windows Firewall → Windows Firewall Settings, File and Printer Sharing must be enabled.
2. Using the gpedit.msc tool (via the Run.. prompt), invoke the Group Policy Object Editor. Navigate to Local Computer Policy → Administrative Templates → Network → Network Connections - > Windows Firewall → Standard Profile → Windows Firewall : Allow inbound file and printer exception, and enable it.
3. While in the Group Policy Object Editor, navigate to Local Computer Policy → Administrative Templates → Network → Network Connections → Prohibit use of Internet connection firewall on your DNS domain and ensure it is set to either Disabled or Not Configured.
4. The Remote Registry service must be enabled (it is disabled by default). It can be enabled manually for continuing audits, either by an administrator or by Nessus. Using plugin IDs 42897 and 42898, Nessus can enable the service just for the duration of the scan.

Enabling this option grants Nessus permission to enable and disable the Remote Registry service—even if you have explicitly set it to 'Disabled'.

Windows User Account Control (UAC) can be disabled alternatively, but that is not recommended. To turn off UAC completely, open the Control Panel, select User Accounts and then set Turn User Account Control to off. Alternatively, you can add a new registry DWORD key named LocalAccountTokenFilterPolicy and set its value to 1.

This key must be created in the registry at the following location:
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy.`

For more information on this registry setting, consult the MSDN 766945 KB. In Windows 7 and 8, if UAC is disabled, then EnableLUA must be set to 0 in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System as well.`

Validating Credentialed Access in Scan Data

SecurityCenter Dashboards

SecurityCenter has dashboards that can be useful in identifying the quality of scans and the validity of credential access to targets. These dashboards are available in SecurityCenter 4.x and 5.x. If the dashboards cannot be found, update the SecurityCenter Feed.

Credentialed Windows Scanning - This dashboard monitors the results of Windows credentialed scans, and should be paired with an asset list, which includes all Windows hosts.

Credentialed Linux Scanning - Monitoring the status of Linux/UNIX credentialed scanning is important in supporting both patch and compliance auditing of Linux/UNIX systems, an asset list to filter the organization's Linux or UNIX hosts will benefit this dashboard.

Nessus Scan Summary – This dashboard content is more focused around understanding how well the scans actually worked across the network (scan duration, percentage hosts credentialed checks were run against, scanner versions and types, etc…)

SecurityCenter Asset Lists

One issue that these dashboards do not address is the clear identification of hosts, which failed in an unexpected manner. The following process outlines creation of asset lists to assist the site in understanding which host scans are anomalous and require review. These instructions include using dynamic and combination asset lists. First, we will describe what is happening, and then we list the steps you will take.

Description of the process:

1. Create an asset list that includes any hosts where login failed, or where the credentials provided were insufficient to provide full access to the target.
2. Create an asset list that includes Windows hosts which did not have required services, or the scanning credentialed account did not have specific permission. This includes access to ADMIN CIFS/SMB shares, remote registry, and Window Management Instrumentation (WMI). All of these services are required to perform a complete scan of a Windows host.
3. Filter the output from plugin 19506 to find un-credentialed scans. This plugin will, also catch those hosts which local security checks are not available. This includes network appliances and other devices, which do not run operating systems that can be fully interrogated by ACAS.
4. Create an asset list to act as a mechanism to whitelist appliances from being flagged in the final asset list.
5. Create an asset list that contains a list of all targets for which further review of the scan process or target configuration is required. The scan data is for hosts that do not have sufficient integrity to be uploaded to use for CYBERCOM reporting.

Steps:

Step	Action

1	Create a Dynamic Asset list for authentication failures ANY of the following are true: • Plugin ID is equal to 21745 • Plugin ID is equal to 24786
2	Create a Dynamic Asset list for windows targets which did not have full access / permissions ALL of the following are true: • Operating System contains the pattern 'indows' ANY of the following are true: • Plugin ID is NOT equal to 24269 (Windows Management Instrumentation (WMI) Available) • Plugin ID is NOT equal to 10394 (Microsoft Windows SMB Log In Possible) • Plugin ID is NOT equal to 10400 (Microsoft Windows SMB Registry Remotely Accessible)
3	Create a Dynamic Asset list for un-credentialed: ANY of the following are true: • Plugin Text contains the pattern 'Credentialed checks : no' where Plugin ID is 19506 (Nessus Scan Information)
4	Create a Static Asset list for hosts where authenticated scanning is not possible. Asset list should list individual IP addresses.
5	Create a Combination Asset list: • (Asset list from step 3 AND NOT asset list from step 4) OR "asset list from step 1" OR "asset list from step 2" • The "ACAS – Bad Credentials" asset list can replace the asset lists from step 1 and 2

Appendix O: Scanner Time Outs / Plugins Out of Sync

Scanner Time Outs

- Nessus Scanners can experience time outs due to lack of resources. According to the ACAS General Requirements document, Tenable recommends 8 GB of RAM for the Nessus Scanner.
- Scanner time outs can also occur when attempting to scan through a firewall.

Tenable does not recommend scanning through a firewall if it can be avoided.

- What does "Load" mean on the scanner details?

The first number is the current load of the system (as you would see with the top command in Linux). The second number in parenthesis is the number scans the scanner is currently running

- Nessus Scanners can experience plugins out of sync errors due to low bandwidth connections between SecurityCenter and the Nessus scanner.

Increasing the scanner timeout setting can help in low bandwidth situations.

Checking and Changing the Scanner Timeout Setting:

The ACAS Kickstart comes with a script to view and modify the timeout setting called **`setTimeout.sh`**, it can be called from the setup script. If the organization is not using the kickstart image or scripts, they can use the manual process described below:

This command will find the currently configured amount of seconds configured for the timeout value for attached scanners.

```
# /opt/sc*/support/bin/sqlite3 /opt/sc*/application.db "select value from
Configuration where name='ScannerStatusTimeout'"
```

Here is example output:

```
300
```

The value is set to 300, so this SecurityCenter is configured to timeout in `300` seconds, or 5 minutes.

This setting controls how long SecurityCenter will wait for a response from the scanner after we have negotiated a secure connection and have made our service request. It applies to all SecurityCenter -> Nessus, and SecurityCenter -> PVS connections. This includes scan processing, plugin updates, status checks, etc.

The configuration variable `'ScannerStatusTimeout'` determines how long SecurityCenter will wait while attempting to negotiate that secure connection and by default is `120` seconds.

For example: SecurityCenter asks a scanner to process plugins after a new plugin set is uploaded. SecurityCenter will negotiate a secure connection (within the `120` second timeout window) and then send the "`process plugins`" request and wait for the response. If SecurityCenter does not get an answer within `'ScannerStatusTimeout'` seconds, it throws an error.

If scanner timeouts are occurring, this value can be increased. In most cases, Tenable does not recommend setting the `ScannerStatusTimeout` greater than `900` seconds. Such cases where bandwidth is extremely low, satellite links for example, may warrant a higher setting. For example, 3 hours or `10800` seconds, may be needed in environments with connectivity is not constant. Remember to test all settings in the lab before deploying in production.

These commands will set the value to `300`, and you can adjust that value as needed.

1. Stop all running scans
2. Log into CLI as root and stop the SC Service

```
# service SecurityCenter stop
```

3. Kill all processes of tns user

```
# kill -l -u tns
```

4. Make the timeout change

```
# /opt/sc/support/bin/sqlite3 /opt/sc/application.db "Update
Configuration set value='300' where name='ScannerStatusTimeout'"
```

5. Start the SC service

```
# service SecurityCenter start
```

Plugins Out of Sync

Nessus Scanners can experience "`plugins out of sync`" errors due to low bandwidth connections between SecurityCenter and the Nessus scanner. Increasing the "`ScannerStatusTimeout`" as shown in the Scanner Timeouts section above will also likely resolve plugins out of sync errors.

Reset the Nessus or Passive Vulnerability Scanner in SecurityCenter

Resetting the connection between the SecurityCenter and Nessus scanner can also reestablish this connection. To do this, the admin can edit the scanner and make no changes or re-input

the password, and select 'submit'. This should be done anytime the scanner is reset or plugins are rebuilt.

Rebuild Plugin Database on Nessus Scanner

To rebuild the Nessus scanner plugins database you can perform the following commands. Examples below include Windows or UNIX/Linux command line examples, but none of the commands are OS dependent.

Linux:

```
# service nessusd stop
# /opt/nessus/sbin/nessuscli fetch --security-center
# /opt/nessus/sbin/nessusd -R
# service nessusd start
```

Windows:

```
# net stop "Tenable Nessus"
# …\Program Files\Tenable\Nessus>nessuscli fetch –security-center
# …\Program Files\Tenable\Nessus>nessusd –R
# net start "Tenable Nessus"
```

Side-load Plugins

Loading plugins into the SecurityCenter or Nessus scanner is not recommended. This is not a vendor supported process, but they have approved the guidance outlined below and DISA provides testing and integration support.

Side-load Nessus Scanner

If the site experiences prolonged connectivity issues, loading the plugins directly into the Nessus scanner can be done when connectivity to the SecurityCenter is not reliable. The tar file required to perform this update is available on the Patch Repository. Using the diff-since-* files is preferred, as the all-2.0 file may cause license issues. License issues may be resolved by uploading a more current diff-since-* file or a plugin push from the SecurityCenter.

```
# …\program files\Tenable\Nessus>nessuscli update diff-since-2
```
Or
```
# /opt/nessus/sbin/nessuscli update all-2.0.tar.gz
# /opt/nessus/sbin/nessuscli fetch –security-center
```

Prior to side-loading plugins into the scanner, you may need to configure the scanner explicitly:

```
# /opt/nessus/sbin/nessuscli fix --secure --set managed=SecurityCenter
# service nessusd restart
```

This command will need to be run after every time the Nessus scanner (application binary, not the plugin feed) is updated.

Side-load SecurityCenter

If the site experiences issues while attempting to manually upload plugins to the SecurityCenter, copying the plugins to the SecurityCenter's RHEL file system via SCP may be an option. Once the plugins are on the local file system the plugins can be side-loaded using php:

```
# /opt/sc/support/bin/php /opt/sc/support/src/tools/pluginUpdate.php sc-plugins-diff.tar.gz
```

Resetting the Nessus Scanner (protocol error):

In order to reset the connection, you can try removing the scanner from the SecurityCenter, rebuilding the plugins database, reset the scanner's registration (below), and then add the scanner back to the SecurityCenter.

```
# net stop "Tenable Nessus"
# …\program files\Tenable\Nessus>nessuscli fix --reset
# …\program files\Tenable\Nessus>nessuscli fetch –security-center
# net start "Tenable Nessus"
```

Resetting the PVS Scanner:

Full configuration reset:

1. Stop the pvs service

```
# service pvs stop
```

2. Remove the following files:

```
# rm –f /opt/pvs/var/pvs/db/config.db
# rm –f /opt/pvs/var/pvs/plugins/tenable_plugins.prmx
# rm –f /opt/pvs/var/pvs/plugins/pvs_feed_info.inc
```

3. Restart pvs

```
# service pvs start
```

Appendix P: Migrating your SecurityCenter on RHEL 5 to RHEL 6

Prerequisites

It is critical that the same version of SecurityCenter be installed on both versions of RHEL.

- RPM files intended to be installed on RHEL 5 will have ***es5*** or ***el5*** in their file name
- RPM files intended to be installed on RHEL 6 using the ***es6*** or ***el6*** in their file name

Note: SecurityCenter 4.x directory is ***/opt/sc4*** while SecurityCenter 5.x directory is ***/opt/sc***

Steps

1. Stop the SecurityCenter service
2. Make a compressed backup of the SecurityCenter directory on RHEL 5
    a. Script Method for RHEL 5 ACAS Kickstarted Servers
        i. Use the **backup-restore.sh** script
        NOTE: Using the script will create the backup name of "/opt/acas_backup.tgz"
    b. Manual Method
        i. **# tar -Pzcf backupName.tgz <SecurityCenter_Directroy>**
3. Copy the **backupName.tgz** file to your RHEL 6 instance in the **/opt** directory (do this via SCP or file transfer protocol)
4. Inflate the **backupName.tgz** over the installed SecurityCenter directory on RHEL 6 in the **/opt** directory
    a. Script Method for RHEL 6 ACAS Kickstarted Servers
        i. Navigate to **/opt/acas** and run the **setup.sh** script
        ii. Go to the "SecurityCenter Tasks"
        iii. Select the **DRrestore.sh**
    b. Manual Method
        i. **# tar -Pxzf backupName.tgz -C <SecurityCenter_Directory>**
5. Force installs the same version of SecurityCenter on the RHEL 6 instance.
    a. **# rpm –ivh --force SecurityCenter.[version]-es6.x86_64.rpm**
6. Start the SecurityCenter service (IP, Hostname, and HIPS changes may require additional tasks)

Appendix Q: CTO 17-0019 Scan Policies, Asset Lists, and Reports

The section contains XML files, which are intended to be uploaded into SecurityCenter 5.x. In order for the uploaded policies, reports, and asset lists to work correctly, the site should ensure that the SecurityCenter Feed is up to date. In SecurityCenter 5.x the Feed can be updated/uploaded by the admin user (System > Configuration > Plugins/Feed). The site will ensure the Feed is updated no more than one week before files are uploaded to the SecurityCenter.

Scan Policy XML files are uploaded by a user or admin, select Scans, select Policies, click Options button in top right corner. Select 'Upload Policy', choose the appropriate file (optionally provide a custom name, description, and tag), and click Submit.

All active scans that support CTO 17-0019 compliance should be conducted using credentials. This includes the OS/Host discovery scan; authenticated data is used to improve quantity and fidelity of scan data.

Asset Lists are uploaded by user(s). Select Assets, click Add, scroll down to the Custom section and click 'Import Asset'. Choose the appropriate file (optionally provide a custom name and tag), and click Submit

Reports are uploaded by user(s). Select Reporting, select the Reports, click Options button in top right corner. Select 'Upload Report', choose the appropriate file, and click Submit.

Best Practice Scan Policies

Scan policy files are for SecurityCenter 5.x, but require current (< 5 days old) SecurityCenter Feed.

```
MD5:  946b212a9284df3a0de97024726745e7
SHA1: 7019e2272b404c09c57152384aee40b4c476e51c
```

Vulnerability Scan XML File: Regular recurring vulnerability scan policy to gather IAVM compliance evidence and evaluate the organization's assets security posture

OS Discovery Scan XML File: Discovery scan to augment the vulnerability scan policy for host discovery in large networks, or live host enumeration in a dynamic environment. Targets that respond to ping (10180) but do not have an OS or CPE (11936 or 45590) should be investigated. Note: this scan is not ideal for an initial discovery of organizational IP space.To perform an initial discovery scan, enable the SYN port scanner and use the "common or default" ports.

Pre Deployment Example XML File: Thorough scan policy for hosts in lab or pre-production environments, prior to deployment. This policy will generate more false-positives and may cause availability or integrity issues on the target.

Configuration (STIG) Scan XML File: Regular recurring STIG scan policy to gather STIG configuration compliance evidence

The individual XML file hashes are contained within the .zip above. Using Microsoft's FCIV tool, the files can be validated using the following command:
`fciv.exe -v -both -xml .\acas_polices-20170103.hashes.xml`

Acceptable Deviations Microsoft Excel file is posted to the patch repository:

```
MD5:  869755deee4aab284ee3c9c15db161d1
SHA1: 7fbcb2cfcd8981ba91d4cc034c2d8b954c44e05d
```

If a deviation is acceptable, it can be implemented with ISSM documentation (reason, date, and (if possible) XML file hash), and does not require explicit AO approval.

If a setting has no acceptable or unacceptable value, or a different value is required, it is an AO documentable configuration (including an OKC Service Desk ticket and AO approval).

Best Practice Asset Lists

Assets List files are for SecurityCenter 5.x, but require current (< 5 days old) SecurityCenter Feed.

```
MD5:  a4d6bd44e1971f609f0774c3b01b79ac
SHA1: 481872eadf945f0aad20de87d8759db73c1b2782
```

Good Access Asset List: Identify hosts that have correct credentials and required access settings. This asset list can be used in combination with reporting to CYBERCOM to ensure IAVM reporting is accurate.

Bad Access Asset List: Identify hosts which do not have the correct credentials or access settings. This asset list can be used to track down hosts that require modification to enable full access.

Stale Hosts Asset List: Identify hosts that have been seen in the last 24 hours, but credentialed scan data is more than 7 days old.

Best Practice Reports

```
MD5:  55407ffac1b1a78aee96ca05edf36785
SHA1: 19b94126ed26c357cd2615c770ccf6079db4c8f3
```

Monthly Scan Report: CYBECOM monthly example report

No Local Check Report: No local security checks are available

SSH Escalation Failure Report: Hosts which SSH escalation (su, sudo, su+sudo, etc…) failed.

Windows Cached Logins Report: Enumerates hosts that permit more than two (2) cached logins (plugin 11457).

Checklist for CTO 17-0019

Forthcoming, best practice version 6