tenable network security

SecurityCenter 5.0 Upgrade Guide

May 11, 2015

(Revision 2)

Table of Contents

Introduction

This document describes the process of upgrading Tenable Network Security's SecurityCenter product to version 5.0. Hardware and software requirements, as well as detailed step-by-step instructions, are included along with important notes and warnings to help ensure the success of the upgrade to SecurityCenter 5.0.

Since many of Tenable's customers have requirements to maintain separation of duties, the SecurityCenter 5.0 documentation has been separated into the following documents to better organize the material based on the organizational role. Note that there may be some overlap in roles as well as content provided with each of the following guides:

- **SecurityCenter 5.0 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4. The target audience for this document is system administrators who need to install the SecurityCenter application. Included in this document are quick instructions for the **admin** user to add a Nessus scanner and create a user account to launch a test scan to ensure SecurityCenter is correctly installed.
- **SecurityCenter 5.0 Upgrade Guide** – This document describes the process of upgrading to version 5.0 of SecurityCenter.
- **SecurityCenter 5.0.1 Upgrade Guide** – This document describes the process of upgrading to version 5.0.1 of SecurityCenter.
- **SecurityCenter 5.0 Administration Guide** – This document provides instructions for the administration of SecurityCenter by the **admin** user. The **admin** user is the first user to log in to the SecurityCenter after the initial installation and is responsible for configuration tasks such as defining organizations, repositories, Nessus scanners, LCE servers, and PVS sensors. The **admin** user does not have the ability to create and launch Nessus scans.
- **SecurityCenter 5.0 User Guide** – This document provides instructions for using SecurityCenter by a Security Manager user or lesser account.

Please email any comments and suggestions to support@tenable.com.

Users are strongly encouraged to read this entire document before upgrading and utilize the steps provided to ensure deployment success.

A basic understanding of Linux/Unix, Windows, computer hardware, and vulnerability scanning with Nessus is assumed.

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.

Software Requirements

Supported Operating Systems

SecurityCenter 5.0 is available for Red Hat Enterprise Server 5 and 6 (64-bit) and CentOS 5 and 6 (64-bit).

Dependencies

Third-Party Packages

Either OpenJDK or the Oracle Java JRE along with their accompanying dependencies must be installed on the system along with any additional Java installations removed for reporting to function properly.

Although it is possible to force the installation without all required dependencies, if your version of Red Hat or CentOS is missing certain dependencies, this will cause problems that are not readily apparent with a wide variety of functions. Tenable's Support team has observed different types of failure modes for SecurityCenter when dependencies to the installation RPM are missing. If you require assistance or guidance in obtaining these dependencies, please contact our Support team at support@tenable.com.

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

- **java-1.7.0-openjdk** (or later) (or the latest Oracle Java JRE)
- **openssh**
- **expat**
- **gdbm**
- **libtool**
- **libtool-ltdl**
- **libxml2**
- **ncurses**
- **readline**
- **compat-libstdc++**
- **libxslt**

Using the latest stable production version of each package is recommended.

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

```
# rpm -qp SecurityCenter-5.x.x-es6.x86_64.rpm --requires
```

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

```
# rpm -qa | grep libtool
```

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

```
# yum -y install java-1.7.0-openjdk.x64
```

Tenable Applications

To upgrade to SecurityCenter 5.0, you must be running SecurityCenter 4.8 or greater. If you are running an older release of Security Center, upgrade to at least SecurityCenter 4.8 before upgrading to SecurityCenter 5.0.

Product	Minimum Version
Nessus	6.3.6
LCE	4.2
PVS	4.x
SecurityCenter (remote/offline repository*)	5.x
3D Tool	2.x

Licensing

A license key from SecurityCenter 4.8.x or later will work with SecurityCenter 5.0. This license key can be obtained from the Tenable Support Portal. The Nessus, PVS, and LCE (if applicable) Activation Code(s) from the upgraded system will be transferred during the upgrade. Please contact Tenable Support (support@tenable.com) or Licensing (licenses@tenable.com) with any issues regarding your key or Activation Code(s).

Disk Size

As a part of the upgrade process, existing **`application.db`**, **`plugins.db`**, **`jobqueue.db`**, **`messages.db`**, **`assets.db`**, and **`organization.db`** databases will be backed up, and the backup given an extension of **`.db.SCVERSION`**. Before performing an upgrade, ensure that there is sufficient space on the disk for copies of all the databases.

Changes in SecurityCenter 5.0

This section provides an overview of some of the new features and changes that are of particular interest to current SecurityCenter 4 customers. For more details on these features and changes, refer to the appropriate SecurityCenter 5.0 document as described in the Introduction.

New Features

- New HTML5 interface, eliminating the need to run Flash to interface with SecurityCenter
- Assurance Report Cards (ARCs) for quick, at-a-glance look at the current security posture based on pre-set conditions

- Updated workflow methodologies to provide easier access to your data and day to day operations
- 32 Gigabyte repositories to store more information in each repository
- New APIs for interacting with SecurityCenter
- Blackout windows now offer more granular control over when and what to block at the Organizational level

Upgrading SecurityCenter

To perform an upgrade, download the new RPM to your current SecurityCenter server from the Tenable Support Portal. Within SecurityCenter, wait for any in-progress scans to finish or manually pause them (scans are held in a state where they can be resumed at any point). Once the upgrade process has begun, normal usage of SecurityCenter will not be available until after the completion of the process.

Important Prerequisites

It is important to ensure that the following conditions are met prior to beginning the upgrade process.

SecurityCenter Version

SecurityCenter 5.0 upgrades require that the SecurityCenter currently be running version 4.8.x or greater.

Java Version

If the Oracle Java JRE or OpenJDK is not installed, the following warning is displayed:

```
[WARNING] SecurityCenter has determined that Oracle Java JRE and OpenJDK is not
installed.
One of two must be installed for SecurityCenter reporting to function properly.
```

Remove any existing non-compatible versions and install the latest version of either of these software packages before running any reports.

Perform Backup

Prior to upgrading, it is recommended that the "**/opt/sc4**" directory be backed up to a separate location. After stopping the SecurityCenter services, run the following command from a directory outside of **/opt/sc4** (such as **/** or **/home)** to create the backup:

```
# tar -pzcf sc4_backup.tar.gz /opt/sc4
```

After running this backup command, move the **sc4_backup.tar.gz** file to a different location if the backup leaves too little space to perform the upgrade.

Halt or Complete Running Jobs

The SecurityCenter processes do not need to be stopped manually prior to the upgrade, but is recommended. However, if any jobs are currently running on SecurityCenter (e.g., Nessus scans), the following message is displayed along with the related process names and their PIDs:

```
"SecurityCenter has determined that the following jobs are still running. Please wait a
few minutes before performing the upgrade again. This will allow the running jobs to
complete their tasks"
```

Either stop the processes manually or try the upgrade again after the jobs complete.

Maintain Installation Log

During the upgrade process, SecurityCenter will produce the log file **/tmp/sc.install.log**. This file is important for debugging purposes and should not be removed. Once the upgrade process is complete, the file will be moved to **/opt/sc/admin/logs/install.log**.

Renaming Mount Point

If the existing **/opt/sc4** directory is or contains a mount point to another location it must be updated. During the rpm upgrade process, a message will be displayed with information about the discovered mount point and instruct you to contact Tenable Support for a mount point tool to help identify and migrate your mount points for the upgrade to continue.

CoSign Authentication

The use of CoSign as an authentication method is not supported in SecurityCenter 5. If the existing SecurityCenter 4 installation uses CoSign servers for authentication, the authentication method must be changed to a supported method prior to performing the upgrade.

SecurityCenter 4.8 or Higher to 5.0 Upgrade

Command Line Upgrades

To upgrade from Security Center 4.8.x to SecurityCenter 5.0, use **rpm** with the "**-Uvh**" switches from the command-line of the SecurityCenter server. Use "**sudo -i**" when performing **sudo** upgrades of SecurityCenter to ensure the proper use of environmental variables. Upgrade SecurityCenter using a command similar to the following:

```
# rpm -Uvh SecurityCenter-5.0.0-es6.x86_64.rpm
```

Sample SecurityCenter upgrade output:

```
# rpm -Uvh SecurityCenter-5.0.0-es6.x86_64.rpm
Preparing...                ########################################### [100%]
Shutting down SecurityCenter services: [  OK  ]
Backing up previous application files ... complete.
   1:SecurityCenter         ########################################### [100%]

Applying database updates ... complete.
Beginning data migration.
Starting plugins database migration...complete.
(1 of 4) Converting Repository 1 ...  complete.
(2 of 4) Converting Repository 2 ...  complete.
(3 of 4) Converting Repository 3 ...  complete.
(4 of 4) Converting Repository 4 ...  complete.
Migration complete.
Starting SecurityCenter services: [  OK  ]
~]#
```

Upgrading Custom SSL Certificates

After an upgrade of a SecurityCenter where custom Apache SSL certificates were in use prior to the upgrade they are backed up as part of the upgrade process. The existing custom SSL certificates are copied to the Apache configuration backup directory that is created during the upgrade in the **/tmp/[version].apache.conf-########** directory. The exact name of the directory will vary, but is displayed during the upgrade process and is reported in the **/opt/sc/admin/log/install.log** file.

The commands to restore the custom SSL certificates are as follows:

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.cert
/opt/sc/support/conf/SecurityCenter.crt
```
(Select yes to overwrite the existing file)

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.pem
/opt/sc/support/conf/SecurityCenter.key
```
(Select yes to overwrite the existing file)

Ensure that the newly copied files have permissions of 0640 and ownership of tns:tns.

Modify the Servername parameter in **/opt/sc/support/conf/servername** to match the Common Name (CN) of the SSL certificate. To obtain the CN run the following command and note the CN= portion of the result.

```
# /opt/sc/support/bin/openssl verify /opt/sc/support/conf/SecurityCenter.crt
```

Then edit the **/opt/sc/support/conf/servername.conf** file at the ServerName parameter to match your certificate's CN value.

Once complete, restart the Apache server with one of the following commands:

```
# /opt/sc/support/bin/apachectl restart
```

-or-

```
# service SecurityCenter restart
```

Troubleshooting

In the event that the SecurityCenter upgrade fails for any reason, please contact Tenable Support via an appropriate method. Contact methods are available on the Support website at https://support.tenable.com.

About Tenable Network Security

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