SecurityCenter 4.8.1 Upgrade Guide

May 29, 2014

(Revision 1)

Table of Contents

Introduction

This document describes the process of upgrading Tenable Network Security's SecurityCenter product to version 4.8.1. 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 4.8.1.

Since many of Tenable's customers have requirements to maintain separation of duties, the SecurityCenter 4.8 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 4.8 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4.8. 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 4.8 Upgrade Guide** – This document describes the process of upgrading to version 4.8 of SecurityCenter.

- **SecurityCenter 4.8.1 Upgrade Guide** – This document describes the process of upgrading to version 4.8.1 of SecurityCenter.

- **SecurityCenter 4.8 Administration Guide** – This document provides instructions for the administration of SecurityCenter and by the **admin** user. The **admin** user is the first user to log into 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 4.8 User Guide** – This document provides instructions for using SecurityCenter from 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/sc4/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 4.8.1 is available for Red Hat Enterprise Server 5 and 6 (32/64-bit). CentOS 5 and 6 (32/64-bit) are also officially supported.

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-1.6.0-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-4.x.x-es6.x86_64.rpm --requires
```

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

```
# rpm –qa | grep libtool
```

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

```
# yum -y install java-1.6.0-openjdk.i386
```

Tenable Applications

If you are running Tenable's Log Correlation Engine (LCE), please note that LCE 4.2 or higher is required for complete functionality with SecurityCenter 4.8.1. Using a combination of LCE 3.x and 4.x servers will result in most SecurityCenter LCE functionality of all connected servers being limited to what is available using the LCE 3.x server.

To upgrade to SecurityCenter 4.8.1, you must be running SecurityCenter 4.8. If you are running an older release of Security Center, upgrade to SecurityCenter 4.8 before upgrading to SecurityCenter 4.8.1.

Product	Minimum Version
Nessus	5.x
LCE	4.0 (3.6.1 with limited functionality) 4.2 or higher for LCE Vulnerability features
PVS	4.x
SecurityCenter (remote/offline repository*)	4.x
3D Tool	2.x

* SecurityCenter 4.8.1 can receive a repository from prior versions of SecurityCenter 4.0.x and above, but cannot share its repositories with previous versions.

Licensing

A license key from SecurityCenter 4.2.x or later will work with SecurityCenter 4.8.1. This license key can be obtained from the Tenable Support Portal. The Nessus 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 4.8.1

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 4.8 document as described in the Introduction.

New Features

- Updated user model to a more common "grouping" method vs the previously used hierarchal model
- Combination asset support adds the ability to create a new dynamic asset list based on exiting asset lists
- Combination asset filtering is supported when creating filters to apply set logic against multiple assets
- Defining User Responsibility by associating an asset list with a user
- Database Credentials are now created in SecurityCenter for ease of reuse and assigned to a scan policy versus the previous method of adding the database credentials to each scan policy individually

- Dynamic asset lists now support Perl Compatible Regular Expressions allowing for negative operators in addition to positive operators

- Full Perl Compatible Regular Expressions (PCRE) support is now available when filtering on vulnerability text. This can be used in all areas of SecurityCenter where vulnerability queries are used including Vulnerability Analysis, Dashboard, Reporting, and Alerts.

- To support Nessus functionality, the ability for a user to select ".k5login" has been added as an option in the privilege escalation drop-down for SSH credentials.

- Communication between SecurityCenter and PVS uses XMLRPC only. All attached PVS scanners must be 4.0 or newer

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.

SecurityCenter 4.8.x introduces a new user security model. Access to security data (Repositories and LCEs intersected with defining assets) is now controlled through groups instead of individual users. User access to security data is granted based on the user's group membership. Users will be able to automatically use Policies, Assets, and other objects created by others in the same group. The new group-based model also allows for more flexibility in user management, object management, and visibility into running scans and reports that is not constrained by the old user hierarchy. Utilizing groups in SecurityCenter makes it quicker and simpler to create, maintain, and assign resources to multiple users.

Important Prerequisites

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

SecurityCenter Version

SecurityCenter 4.8.1 upgrades require that the SecurityCenter currently be running version 4.8.

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.

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/sc4.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/sc4/admin/logs/install.log`**.

Attached PVS Versions and Logins

Ensure that all attached PVS scanners have been upgraded to version 4.0 or higher. SecurityCenter 4.8.1 will not communicate with earlier versions of PVS. Additionally, the logins must be changed from the current user and password to one that exists for the XMLRPC login on the PVS server.

SecurityCenter 4.8 to 4.8.1 Upgrade

Command Line Upgrades

To upgrade from Security Center 4.8 to SecurityCenter 4.8.1, 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-4.8.1-es6.x86_64.rpm
```

Sample SecurityCenter upgrade output:

```
# rpm -Uvh SecurityCenter-4.8.1-201405210759-DEV07-es6.x86_64.rpm
Preparing...                ########################################### [100%]
Shutting down SecurityCenter services: SecurityCenter is already stopped.
[  OK  ]
   1:SecurityCenter         warning: /opt/sc4/admin/users/1/messages.db created as
       /opt/sc4/admin/users/1/messages.db.rpmnew
warning: /opt/sc4/application.db created as /opt/sc4/application.db.rpmnew
warning: /opt/sc4/data/report/report.pdf.xsl saved as
       /opt/sc4/data/report/report.pdf.xsl.rpmsave
warning: /opt/sc4/data/report/report.rtf.xsl saved as
       /opt/sc4/data/report/report.rtf.xsl.rpmsave
warning: /opt/sc4/data/report/report.xsl saved as
       /opt/sc4/data/report/report.xsl.rpmsave
warning: /opt/sc4/jobqueue.db created as /opt/sc4/jobqueue.db.rpmnew
warning: /opt/sc4/plugins.db created as /opt/sc4/plugins.db.rpmnew
warning: /opt/sc4/support/conf/file.conf saved as
       /opt/sc4/support/conf/file.conf.rpmsave
warning: /opt/sc4/support/etc/php.ini created as /opt/sc4/support/etc/php.ini.rpmnew
########################################### [100%]

Applying database updates ... 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/sc4/admin/log/install.log** file.

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

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.cert
/opt/sc4/support/conf/SecurityCenter.crt (Select yes to overwrite the existing file)
```

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.pem
/opt/sc4/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/sc4/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/sc4/support/bin/openssl verify /opt/sc4/support/conf/SecurityCenter.crt
```

Then edit the **/opt/sc4/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/sc4/support/bin/apachectl restart
```

Or:

```
# service SecurityCenter restart
```

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com