

RSA Archer GRC
RSA Vulnerability Risk Management 1.2
Upgrade Guide
5.x and later

Revision 2



Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:

<http://www.emc.com/support/rsa/index.htm>.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.rsa.com/legal/trademarks_list.pdf.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Contents

Revision History	4
Preface	5
About This Guide	5
RSA Vulnerability Risk Management Data Dictionary	5
RSA Vulnerability Risk Management Documentation Set	5
Support and Service	6
Other Resources	6
Chapter 1: Upgrading RSA Vulnerability Risk Management	8
Upgrading to RSA Vulnerability Risk Management 1.2	8
Complete the Prerequisites to Upgrade to RSA Vulnerability Risk Management 1.2	8
RSA Vulnerability Risk Management Files	8
Chapter 2: Upgrade to RSA VRM 1.2	10
Upgrading the RSA Analytics Warehouse	10
Upgrading to JRE 8	10
Upgrading to MapR 4.1	11
Upgrade the RSA VRM RPM	13
Upgrading Vulnerability Analytics	13
Upgrade the JRE and JCE	14
Upgrade the Windows Installer	14
Upgrade the RSA Archer Vulnerability Risk Management Solution	15
Import and Install the RSA Archer Vulnerability Risk Management Solution Package	15
Change Key Field Configuration for Findings Application (Optional)	17
Appendix A: Troubleshooting	18

Revision History

Revision	Date	Description
1	6/10/2016	Updated " Upgrading to RSA Vulnerability Risk Management 1.2 " to reflect that upgrading from RSA Vulnerability Risk Management 1.1 SP1 P5 is supported.
2	6/14/2016	Updated " Upgrading to RSA Vulnerability Risk Management 1.2 " to reflect that upgrading from all RSA Vulnerability Risk Management 1.1 SP1 patches is supported.

Preface

About This Guide

This guide is for RSA® Archer® GRC administrators who need to upgrade the RSA Vulnerability Risk Management 1.2 solution. For more information, see the RSA Archer GRC Help.

This guide assumes that the reader is knowledgeable about the GRC industry and RSA Archer GRC.

RSA Vulnerability Risk Management *Data Dictionary*

The RSA Vulnerability Risk Management *Data Dictionary* contains configuration information for the solution.

The RSA Vulnerability Risk Management *Data Dictionary* is included in the rsa-vm-1.2.0-suite.zip file.

RSA Vulnerability Risk Management Documentation Set

For information about the RSA Vulnerability Risk Management solution, see the following documentation:

Guide	Description
RSA Vulnerability Analytics Help	Provides users and administrators with instructions on how to use the RSA Vulnerability Analytics UI.
Installation and Configuration Guide	Provides administrators with instructions on how to install and configure the solution.
Practitioner Guide	Provides design information about the solution and a use case highlighting how the solution works.
Release Notes	Introduces the RSA Vulnerability Risk Management solution, lists the documentation available, and provides information for obtaining support and service.
Upgrade Guide	Provides administrators with instructions on upgrading their existing RSA VRM setup.
Backup and Recovery Guide	Provides administrators with instructions on backing up and recovering their RSA VRM setup.

Guide	Description
RSA Vulnerability Analytics Search API Guide	Provides administrators with instructions on using the RSA VA Search API. Note: This is included in the RSA Vulnerability Analytics Help.
Extensions Guide	Provides administrators with instructions on configuring various extensions with which RSA VRM can be setup.
ACME Corp Sizing Guide	Provides detailed information about performance and sizing measurements pertaining to common business activities performed with RSA Vulnerability Risk Management.

You can access the RSA Vulnerability Risk Management solution documentation from the Documents page on the RSA Archer Exchange at https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange or on RSA SecurCare® Online at <https://knowledge.rsasecurity.com/>.

Support and Service

Customer Support Information	https://community.rsa.com/community/rsa-customer-support
Customer Support E-mail	archersupport@rsa.com

Other Resources

RSA Archer GRC Community on RSA Link: Our public forum, on the new RSA Link Community platform, brings together customers, prospects, consultants, RSA Archer GRC thought leaders, partners and analysts to talk about GRC as a practice, and includes product demos, GRC videos, white papers, blogs and more.

<https://community.rsa.com/community/products/archer-grc>

RSA Archer Community on RSA Link: Our private community, is a powerful governance, risk and compliance online network that promotes collaboration among Archer customers, partners, industry analysts, and product experts. Engaging with the RSA Archer Community on RSA Link enables you to collaborate to solve problems, build best practices, establish peer connections and engage with RSA Archer GRC Thought Leaders.

<https://community.rsa.com/community/products/archer-grc>

RSA Ready: RSA's Technology Partner Program is where 3rd parties gain access to RSA Software in order to develop an interoperability and have it documented and certified. RSA Ready certifications are posted to an online Community and supported by RSA Support. <https://community.rsa.com/community/products/rsa-ready>

Chapter 1: Upgrading RSA Vulnerability Risk Management

<u>Upgrading to RSA Vulnerability Risk Management 1.2</u>	8
<u>Complete the Prerequisites to Upgrade to RSA Vulnerability Risk Management 1.2</u>	8
<u>RSA Vulnerability Risk Management Files</u>	8

Upgrading to RSA Vulnerability Risk Management 1.2

If you have installed RSA Vulnerability Risk Management 1.1 SP1 and any subsequent patches, you can upgrade the environment directly to version 1.2. The following components are included in this upgrade:

- MapR 4.1
- RSA VRM rpm
- RSA Vulnerability Analytics Host
- RSA Archer Vulnerability Risk Management solution

Complete the Prerequisites to Upgrade to RSA Vulnerability Risk Management 1.2

Procedure

1. Ensure that RSA Vulnerability Risk Management 1.1 SP1 is installed and fully functional.
2. Ensure that Microsoft .NET Framework 3.5 is installed and configured.
3. Ensure that your cluster(s) are running and have no alarms. Any alarms must be resolved before progressing.

RSA Vulnerability Risk Management Files

The RSA Vulnerability Risk Management installation package, rsa-vm-1.2.0-suite.zip, contains the following files:

File	Description
rsa-vm-1.2.0.xxx-installer.exe	The RSA Vulnerability Analytics Windows Installer.
vm-1.2.0-xxx.tar	A .tar file containing the RSA Analytics Warehouse upgrade Redhat Package Manager (RPM) file.
RSA_Vulnerability_Risk_Management_v1.2.zip	The RSA Archer VRM solution package. Important: Do not unzip this file.
RSA_Archer_Vulnerability_Risk_Management_1_2_Data_Dictionary.xlsx	The RSA Archer VRM solution Data Dictionary.

To download the RSA Vulnerability Risk Management installation file, contact your RSA customer representative or visit RSA Download Central at <https://download.rsasecurity.com>.

Chapter 2: Upgrade to RSA VRM 1.2

<u>Upgrading the RSA Analytics Warehouse</u>	10
Upgrading to JRE 8	10
Upgrading to MapR 4.1	11
Upgrade the RSA VRM RPM	13
<u>Upgrading Vulnerability Analytics</u>	13
Upgrade the JRE and JCE	14
Upgrade the Windows Installer	14
<u>Upgrade the RSA Archer Vulnerability Risk Management Solution</u>	15
Import and Install the RSA Archer Vulnerability Risk Management Solution Package	15
Change Key Field Configuration for Findings Application (Optional)	17

Upgrading the RSA Analytics Warehouse

In order to upgrade to RSA VRM 1.2, you must upgrade your RSA Analytics Warehouse. The the following must be completed before the RSA Analytics Warehouse can be fully upgraded:

1. Ensure you have a fully functioning MapR cluster.
2. Ensure that all Hadoop jobs have been completed.
3. Ensure you have a fully functioning RSA VRM solution.
4. Download the .tar file.
5. Upgrade to JRE 8.
6. Upgrade to MapR 4.1.
7. Upgrade the RSA VRM rpm.

Upgrading to JRE 8

Procedure

1. On the Oracle Java 8 download page, accept the license agreement.
2. Download the latest Linux-x64 version:
 - `jre-8uXX-linux-x64.tar.gz`
 Where *xx* is the JRE 8 update.
3. Copy the JRE 8 download onto each node in the cluster.
4. Install JRE 8 onto each node:

```
cd /usr/lib/jvm
```

```
tar -xvf jre-8uXX-linux-x64.tar.gz
```

5. Configure each node to use JRE 8 by default:

```
alternatives --install /usr/bin/java java
/usr/lib/jvm/jre1.8.0_XX/bin/java 2
```

```
alternatives --config java
```

6. Select the option for JRE 8.
7. Edit the /opt/mapr/conf/env.sh and add the following to the end of the file:

```
export JAVA_HOME=/usr/lib/jvm/jre1.8.0_XX
```

Where *XX* is the build/patch number for JRE 1.8.0

8. Restart the service:

```
service mapr-warden restart
```

Upgrading to MapR 4.1

The following prerequisites must be completed before MapR 4.1 can be fully upgraded:

- Ensure that you have enough storage to run the install.

Ensure that your MapR license is valid.

- Ensure you are running MapR 3.1. To verify your MapR version, enter the following command:

```
cat /opt/mapr/MapRBuildVersion
```

Note: The MapR upgrade script only supports an upgrade from MapR 3.1 to 4.1.

- Ensure that all nodes in the cluster have been upgraded to JRE 8.
- Ensure that MapR has no critical alarms. Any alarms must be fixed before upgrading MapR. To check for alarms, enter the following command on one of the nodes:

```
maprcli alarm list
```

The following are potential critical alarms:

CLUSTER_ALARM_UPGRADE_IN_PROGRESS

NODE_ALARM_SERVICE_CLDB_DOWN

NODE_ALARM_DUPLICATE_HOSTID

NODE_ALARM_SERVICE_FILESERVER_DOWN

NODE_ALARM_SERVICE_HBMASTER_DOWN

```

NODE_ALARM_SERVICE_HBREGION_DOWN
NODE_ALARM_INCORRECT_TOPOLOGY_ALARM
NODE_ALARM_OPT_MAPR_FULL
NODE_ALARM_SERVICE_JT_DOWN
NODE_NO_HEARTBEAT
NODE_ALARM_ROOT_PARTITION_FULL
NODE_ALARM_TT_LOCALDIR_FULL
NODE_ALARM_TIME_SKEW
NODE_ALARM_NO_HEARTBEAT

```

- The MapR script must be run with root account. In a multiple nodes environment, ensure that you have the root credentials for all of the nodes in the cluster.
- In a multiple nodes environment, ensure that the connectivity between the node in which you are running the MapR upgrade script and the other nodes in the cluster is up and running.

Upgrade to MapR 4.1

The scripts and libraries required for the MapR 4.1 upgrade are included in the vrm-1.2.0-nnn.tar file. Upgrading to MapR 4.1 is required before you can fully upgrade to RSA VRM 1.2.

Important: Commands must only be typed in directly. Do not copy and paste them.

Procedure

1. To ensure that you have a fully functioning MapR Cluster, display and fix the list of alarms. Enter:


```
mapcli alarm list
```
2. To ensure that all Hadoop jobs have been completed, display and complete the list of currently running Hadoop jobs. Enter:


```
hadoop job =list
hadd
```
3. Download the vrm-1.2.0-xxx.tar file and transfer it to the /tmp directory on one of the cluster nodes.
 - a. Log into the node where your .tar file is located.
 - b. Change to the tmp directory where your .tar file is located.


```
cd/tmp
```
4. Untar the vrm-1.2.0-xxx.tar file. Enter:


```
tar -xvf vrm-1.2.0-xxx.tar
```

5. Enter the directory:
`cd vrm-1.2.0`
6. Run the script to upgrade to MapR 4.1. Enter:
`./upgrade-mapr-to-4.1.sh`
7. When prompted if you want to continue connecting, enter:
`yes`
8. When prompted, enter your password.

Note: The upgrade only needs to be run on one node in the cluster. The script continues to install the script on all of the nodes. If you encounter any errors, you must investigate and resolve them before MapR 4.1 will install properly.

Note: The script may take some time to execute, but can be monitored while running.

Upgrade the RSA VRM RPM

If you are upgrading from RSA Vulnerability Risk Management 1.1 SP1, you must upgrade your RSA Analytics Warehouse RPM.

Procedure

1. On the first node in the RAW cluster, copy and move the `vrm-x.x.tar` file from the `rsa-vrm-1.2-suite.zip` file to the `/tmp` directory.
2. On one of the nodes in the RAW cluster, start the automated upgrade script. Enter the following command:
`./vrm-upgrade.sh`

Important: You may be prompted for root passwords for remote nodes. Do not leave the installer unattended as prompts for the root passwords may time out

Note: Running the script file restarts the MapR and Solr services. Do not run any other script on any other node during this time.

Upgrading Vulnerability Analytics

After you have upgraded the RAW, you need to upgrade the Vulnerability Analytics. The following upgrades must be completed before the Vulnerability Analytics upgrade can be completed:

- JRE 8
- JCE
- Windows Installer

Upgrade the JRE and JCE

Procedure

1. Download and install JRE 8 from Oracle's website.

Note: Ensure that you have the latest Windows Installer x64 version.

2. Replace the Java Cryptography Extension (JCE) files with the JCE 8 files as follows:
 - a. Download the JCE 8 files from Oracle's website.
 - b. Replace the files in the `<install_dir>\java\jre1.8.0_xx\lib\security` folder.

Upgrade the Windows Installer

Procedure

1. Make a backup copy of the license.xml file located in the *VA Installation Directory*\config directory.
where *VA Installation Directory* is the RSA Vulnerability Analytics installation directory.
2. Ensure that the following services are stopped:
 - RSA Vulnerability Management - Data Collector
 - RSA Vulnerability Management - User Interface
3. Close any open applications, processes, and files, including the Connection Manager sessions, related to the previous version of RSA VRM.
4. Copy and paste the rsa-vrm-1.2.0-x.x-installer.exe file to the RSA Vulnerability Analytics host.
5. Double-click the rsa-vrm-1.2.0-x.x-installer.exe file.
6. Follow the on-screen steps to install the upgrade.

Note: The following configured files remain unchanged during the install process and are saved to a timestamped backup folder:

- Configuration Directory
- ETL Jobs Directory
- Jetty SSL Configuration Directory

Note: The following items remain unchanged:

- Configured Warehouse IPs and names
 - Configured RSA VA Users
 - Configured Rules
 - Configured Endpoints
 - Configured Workflow Schedules
 - Installed Certificates
7. Restore the license.xml file from the backup made in step 1 in the *VA Installation Directory*\config directory.
 8. Ensure that the following services are running on the RSA Vulnerability Analytics host:
 - RSA Vulnerability Management - Data Collector
 - RSA Vulnerability Management - User Interface

Note: The RSA Vulnerability Analytics host installer automatically starts the services after completing the upgrade.

Upgrade the RSA Archer Vulnerability Risk Management Solution

Procedure


1. [Import and Install the RSA Archer Vulnerability Risk Management Package](#)
2. [Change Key Field Configuration for Findings Application \(Optional\)](#)

Import and Install the RSA Archer Vulnerability Risk Management Solution Package

Installing the RSA Archer VRM Package overwrites any other previously installed version of the RSA Archer VRM solution.

Procedure

1. Backup your RSA Archer GRC database.
2. Logon to the RSA Archer Platform user interface with system administrator access.
3. Click Navigation > Administration > Application Builder > Install Packages.
4. In the Available Packages section, click Import.
5. Click Add New.

6. Locate and select the RSA_Vulnerability_Risk_Management_v1.2.zip package file.
7. Click OK.
8. Perform Advanced Package Mapping. For detailed instructions, see "Advanced Package Mapping" in the Packaging section of the *RSA Archer GRC Online Documentation*.
9. In the Available Packages section, locate the RSA Vulnerability Risk Management v1.2 package:
RSA_Vulnerability_Risk_Management_v1.2.zip
10. Click Install .
11. Follow these steps to modify the components of the installation package:
 - a. In the Configuration section, select the components of the package that you want to install.

Note: By default, RSA Archer only selects new applications, so you must select all other applications and questionnaires as needed.

- b. In the Install Method section, for each component, select one of the following options.


Option	Description
Create New Only	Only creates new objects that do not currently exist in the instance. Does not update existing objects. Important: You must manually update any existing items that you want to change. See the <i>Data Dictionary</i> for field information.
Create New and Update	Creates new objects and updates existing objects that match objects in the package.

- c. In the Layout section, for each component, select one of the following options.

Option	Description
Override Layout	Replaces the existing layout with the layout in the package. Moves fields that were previously on the layout that are not on the package layout to the Available Fields list.

Option	Description
Do Not Override Layout	No changes are made to the existing layout, but you may have to modify the layout after installing the new package.

Note: RSA recommends using the Create New and Update and the Override Layout options, except for customizations.

12. Click Install . If you receive a warning message, click OK.

Note: If you are seeing any failures in the package installation log, please contact RSA customer support for assistance.

Change Key Field Configuration for Findings Application (Optional)

Optionally, change the way Findings record tracking IDs are shown in RSA Archer to be similar to how they are shown in RSA Vulnerability Analytics.

Procedure

1. Click Navigation > Administration > Application Builder > Manage Applications
2. Click the Findings application.
3. Click the Fields tab.
4. Click the Finding ID field.
5. Click the Options tab.
6. In the Configuration section, select System ID.
7. Click Save to save the field changes.
8. Click Save to save the application changes.

Appendix A: Troubleshooting

Problem	Remediation
The RSA Vulnerability Analytics host installer encounters an error.	<p>The installer backs up the original configuration. The backup is stored at the default directory of <code>c:\program files\rsa\vrml\upgrade-backup.<i>Timestamp</i></code> where <i>Timestamp</i> is the date and backup number of the stored backup.</p> <p>The folders that are backed up include:</p> <ul style="list-style-type: none"> • Configuration directory. <ul style="list-style-type: none"> ◦ <code>c:\program files\rsa\vrml\config</code> • ETL Jobs directory. <ul style="list-style-type: none"> ◦ <code>c:\program files\rsa\vrml\data collector\jobs</code> • Jetty SSL Configuration. <p>Restore the backup files to their original directories and run the RSA Vulnerability Analytics host installer again. If this does not work, contact Customer Support with the install log files.</p>
The RSA Vulnerability Analytics host installer does not start the RSA Vulnerability Management - Data Collector Service and the service cannot be restarted.	<p>Procedure</p> <ol style="list-style-type: none"> 1. On the Window Host, click Start > Control Panel > Uninstall a program. 2. Right-click RSA Vulnerability Risk Management, and select Repair.
During RAW RPM installation, the installer hangs at Checking HBase Availability.	<p>While the installer hangs, open a new command window on the same node and enter the following command:</p> <pre>/opt/rsa/vrml/setup/vrml-util.sh -a restartHBaseCluster</pre>

Problem	Remediation
In a cluster with more than five nodes, an error is given when adding the warehouse node.	Procedure <ol style="list-style-type: none">1. Complete the following on each node in the cluster:<ol style="list-style-type: none">a. Enter the following commands:<pre>service mapr-warden stop service mapr-zookeeper stop</pre>b. Enter the following commands:<pre>service mapr-zookeeper start service mapr-warden start</pre>
An error is received when trying to trigger a workflow due to the endpoint connecting successfully with wrong proxy credentials.	Procedure <ol style="list-style-type: none">1. Exit and restart the connection manager session.2. Delete the existing endpoint for which workflows fail.3. Re-add the endpoint with correct proxy credentials.

Problem	Remediation
The upgrade to MapR 4.1 fails.	<p>Procedure</p> <ol style="list-style-type: none"> Find the CLDB master node. Enter the following: <pre>maprccli node cldbmaster</pre> On the nodes that are not the CDLB master, enter: <pre>service mapr-warden stop</pre> On the CDLB master node, enter: <pre>service mapr-warden stop</pre> On all nodes, enter: <pre>service mapr-zookeeper stop</pre> <p>Important: Ensure that services have fully stopped on all nodes before proceeding.</p> <p>Note: If a node returns the following output, it is in a running or stopped state: <pre>'service servicename status'</pre> </p> On all nodes, enter: <pre>service mapr-zookeeper start</pre> On the node that was previously the CDLB master, enter: <pre>service mapr-warden start</pre> <p>Important: Ensure that step 7 has been completed before proceeding.</p> On all other nodes, enter: <pre>service mapr-warden start</pre> To ensure that all nodes are fully functioning, display and fix the list of alarms. Enter: <pre>maprccli alarm list</pre> Upgrade to MapR 4.1.
The upgrade to MapR 4.1 fails before the RPM packages have been installed.	Re-run the MapR upgrade script after investigating and resolving issues.

Problem	Remediation
The upgrade to MapR 4.1 fails after the RPM packages have been installed.	Contact Customer Support for assistance.
The upgrade to MapR 4.1 script fails and exits when attempting to stop hive2.	While upgrade-to-mapr-4.1.sh runs, open a new command window on the node where the error occurs and enter: <code>start hive2</code>
The Scans workflow runs successfully on any scanner, but the Vulnerabilities workflow fails and data is not loaded into VRM.	Procedure <ol style="list-style-type: none"> 1. Stop the RSA Vulnerability Management - Data Collector service. 2. Open the collector-config.properties file in the <install_directory>\config folder. 3. Change the lastTimeRun parameter for the Scans workflow to 0 to load all data. Enter: <code>rapid7.default.getRapid7Scans.lastTimeRun.getRapid7Scans = 0</code> 4. Delete the state file for the Scans workflow, in the <incoming_data_directory>\incoming\feeds\tmp folder. The following is an example of a state file: <code>default-getRapid7Scans-state.txt</code> 5. Start the RSA Vulnerability Management - Data Collector service. 6. Run the Vulnerabilities workflow. 7. Ensure that the Vulnerabilities workflow is successful and that the vulnerabilities have been loaded into VRM. 8. Run the Scans workflow.