

**RSA Archer GRC**

**RSA Vulnerability Risk Management 1.2**

**Installation and Configuration Guide**

**5.x and later**

Revision 1



## **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](http://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

<b>Revision History</b>	<b>5</b>
<b>Preface</b>	<b>6</b>
About This Guide	6
RSA Vulnerability Risk Management Documentation Set	6
RSA Vulnerability Risk Management Data Dictionary	7
Support and Service	7
Other Resources	7
<b>Chapter 1: RSA Vulnerability Risk Management</b>	<b>9</b>
RSA Vulnerability Risk Management	9
RSA Vulnerability Risk Management Architecture	9
RSA Vulnerability Risk Management Port Usage	11
Secure the RSA VA Host with Windows Firewall	14
Secure RAW Cluster Nodes With IP Tables	14
RSA VRM Installation Overview	16
RSA Vulnerability Risk Management Requirements	17
RSA Analytics Warehouse Requirements	18
RSA Vulnerability Analytics Host Requirements	18
RSA Vulnerability Analytics Supported Browsers	19
RSA Archer Vulnerability Risk Management Solution Requirements	19
Tenable Nessus User Account Requirements for Scan Results	19
Tenable Security Center User Account Requirements for Scan Results	19
QualysGuard API Requirements for Scan Results	19
Rapid7 User Account Permission Requirements for Use as Endpoint	20
RSA Vulnerability Risk Management Supported Endpoints	20
RSA Vulnerability Risk Management Files	22
<b>Chapter 2: Install and Configure Vulnerability Risk Management 1.2</b>	<b>23</b>
Installing the RSA Analytics Warehouse	23
Install the RSA Analytics Warehouse	23
Installing JRE 8	37
Upgrading to MapR 4.1	38
Install the RSA VRM Framework on the RAW Cluster	40
Installing the RSA Vulnerability Analytics	40
Install the JRE and JCE	41
Install the RSA Vulnerability Analytics User Interface	41
Install the RSA Archer Vulnerability Risk Management Solution	42
Apply the RSA Archer Vulnerability Risk Management Solution License Key	42
Import and Install the RSA Archer Vulnerability Risk Management Solution Package	43
Edit the RSA Vulnerability Risk Management Group	45
Create a User Account for Web Service Client	45
Add VRM Group to Enterprise Management Workspace	46

Change Key Field Configuration for Findings Application (Optional) .....	47
Post Install Activities .....	47
Deleting Obsolete Objects .....	47
Validating Formulas and Calculation Orders .....	48
Verifying Key Fields .....	48
Configure the RSA Archer Platform to Communicate with RSA Vulnerability Risk Management .....	48
Connect the RSA Vulnerability Analytics Interface to the RSA Analytics Warehouse .....	49
Run the Connection Manager .....	50
Confirm the Installation .....	52
Configure Single Sign On (Optional) .....	53
<b>Appendix A: Configure Endpoints .....</b>	<b>54</b>
Configure a Mapped Share Drive (for Nessus, Security Center, and Custom Data Only) .....	54
Configure Custom Data .....	55
Edit Custom Fields .....	56
Edit Custom Field Display Labels in RSA Vulnerability Analytics .....	57
Configure Custom Endpoint .....	57
Configure Security Center Endpoint .....	59
Configure Nessus Endpoint .....	61
Configure Qualys Endpoint .....	62
Configure Rapid7 Endpoint .....	63
Set Up and Configure McAfee Vulnerability Manager Endpoint .....	64
Export the McAfee CA Certificate .....	64
Install the McAfee CA Certificate .....	65
Configure the McAfee Endpoint .....	66
<b>Appendix B: Troubleshooting RSA Vulnerability Risk Management .....</b>	<b>67</b>
<b>Appendix C: Uninstalling RSA Vulnerability Risk Management .....</b>	<b>73</b>
Uninstall RSA Vulnerability Risk Management .....	73
<b>Appendix D: Installing Customer Certificates .....</b>	<b>74</b>
Create a New SSL Certificate .....	74
Generate a Certificate Signing Request .....	75
Import the CA Signed Certificate and Supporting Certificates into the New Keystore .....	75
Edit the vrm-jetty-ssl.xml File .....	76
<b>RSA VRM Glossary .....</b>	<b>78</b>

## Revision History

Revision	Date	Description
1	5/19/2016	<a href="#">Appendix D: Installing Customer Certificates</a> was added.

## Preface

### About This Guide

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

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

### 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.
RSA Vulnerability Analytics Search API Guide	Provides administrators with instructions on using the RSA VA Search API. <b>Note:</b> 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.

Guide	Description
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](https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange) or on RSA SecurCare® Online at <https://knowledge.rsasecurity.com/>.

## 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.

## Support and Service

---

Customer Support Information	<a href="https://community.rsa.com/community/rsa-customer-support">https://community.rsa.com/community/rsa-customer-support</a>
Customer Support E-mail	<a href="mailto:archersupport@rsa.com">archersupport@rsa.com</a>

---

## 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: RSA Vulnerability Risk Management

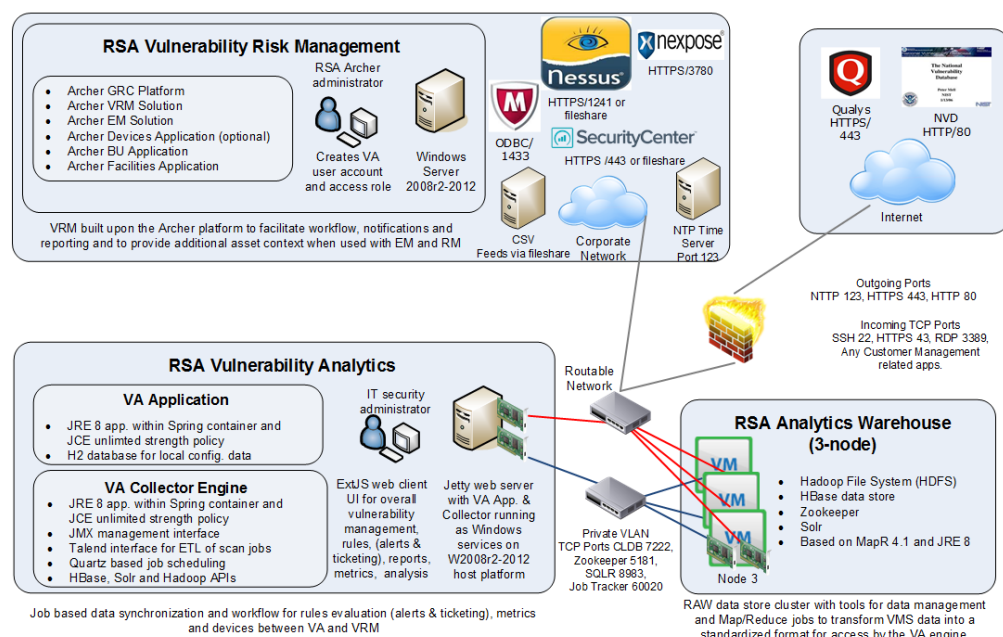
<a href="#">RSA Vulnerability Risk Management</a>	9
<a href="#">RSA Vulnerability Risk Management Architecture</a>	9
<a href="#">RSA Vulnerability Risk Management Port Usage</a>	11
<a href="#">RSA VRM Installation Overview</a>	16
<a href="#">RSA Vulnerability Risk Management Requirements</a>	17
<a href="#">RSA Vulnerability Risk Management Supported Endpoints</a>	20
<a href="#">RSA Vulnerability Risk Management Files</a>	22

## RSA Vulnerability Risk Management

RSA Vulnerability Risk Management (RSA VRM) takes a Big Data approach to helping security teams identify and prioritize high-risk threats. Built on the RSA Archer platform, RSA VRM helps organizations proactively manage IT security risks by combining asset business context, actionable threat intelligence, vulnerability assessment results, and comprehensive workflows.

## RSA Vulnerability Risk Management Architecture

### RSA VRM 1.2: Reference Architecture



RSA Vulnerability Risk Management is deployed with a specific networking topology for security, performance, and dependencies of the underlying technologies used.

RSA VRM is comprised of four main components:

- **RSA Vulnerability Analytics Windows Host (Customer Provided Virtual Machine or Hardware).** Requires a minimum of two network interfaces; one connected to a corporate network with access to off-premise and on-premise data sources and RSA Archer, and the other on a private network utilized for communication with the RSA Analytics Warehouse cluster.
- **RSA Analytics Warehouse (RSA Provided OVA or RSA Security Analytics 4S Hardware Appliance).** Requires a minimum of two network interfaces; one connected to a management network for the system administrator with the ability to synchronize with the NTP Server, and the other on a private network utilized for MapR, Hadoop, and RSA VA Cluster services.
- **RSA Archer Host.** A platform host with the RSA Vulnerability Risk Management solution, RSA Archer Enterprise Management solution, and RSA Archer Issue Management solution installed.
- **External Data Sources.** The National Vulnerability Database for populating vulnerabilities within RSA Vulnerability Analytics and other external data sources such as Qualys QualysGuard.

RSA Vulnerability Risk Management utilizes a networking topology comprised of Internal and External networks. The Internal network should be a private non-routable network to isolate MapR and SOLR related traffic from management or corporate networks.

**Note:** To minimize potential security risks, RSA recommends placing only the RSA VA Host and the RSA Analytics Warehouse cluster nodes on the Internal network. The Cluster services should not be accessible from the External network.

The following is a table of component requirements by the network:

Component	Internal	External
RSA VA Host	x	x
RAW Cluster Nodes	x	x
RSA Archer		x
Rapid7		x
Custom Data Source		x
Tenable Security Center		x

Component	Internal	External
McAfee		x
Tenable Nessus		x
National Vulnerability Database	N/A	N/A
Qualys	N/A	N/A

## RSA Vulnerability Risk Management Port Usage

Component	Protocol or Service	Port	Default Network	Required Network	Service Notes and Requirements
VA Host	HTTPS	443	N/A	External	Default port jetty web server binds to for Vulnerability Analytics UI.
VA Host	RDP	3389	N/A	External	RDP connection to the RSA VA host is required for setup and configuration of RSA VRM.
RAW Node	ICMP		External and Internal	Not Required	Not required but enabled in RSA RAW OVA and RAW Hardware Appliance, should be evaluated individually.
RAW Node	SSH	22	External and Internal	External and Internal	Required for RSA VRM installation, configuration, troubleshooting. Access to the External IP address of RAW nodes should be limited to network / IT administrators only.
RAW Node	NFS	2049	External and Internal	Internal Only	Required for MapR and RSA VRM Backup and Restore functionality. Only required for internal network.
RAW Node	Zookeeper	2888	External and Internal	Internal Only	Zookeeper is coordination service for Hadoop related services and SOLR - Required for RSA VRM.
RAW Node	Zookeeper	3888	External and Internal	Internal Only	Zookeeper is coordination service for Hadoop related services and SOLR - Required for RSA VRM.

Component	Protocol or Service	Port	Default Network	Required Network	Service Notes and Requirements
RAW Node	Zookeeper	5181	External and Internal	Internal Only	Zookeeper is coordination service for Hadoop related services and SOLR - Required for RSA VRM.
RAW Node	MapR-FS API	5660	External and Internal	Internal Only	MapR / CLDB Related service required for MapR Cluster - Required for RSA VRM.
RAW Node	CLDB JMX	7220	External and Internal	Internal Only	MapR / CLDB Related service required for MapR Cluster - Required for RSA VRM.
RAW Node	CLDB Web UI	7221	External and Internal	Internal Only	MapR / CLDB Related service required for MapR Cluster - Required for RSA VRM.
RAW Node	MapR-FS API	7222	External and Internal	Internal Only	MapR / CLDB Related service required for MapR Cluster - Required for RSA VRM.
RAW Node	Web UI HTTP	8080	External and Internal	Not Required	Security Analytics Deployments Only - Not Required for RSA VRM.
RAW Node	Puppet	8140	External and Internal	Not Required	Security Analytics Deployments Only - Not Required for RSA VRM.
RAW Node	MapR Control Panel Web UI	8443	External and Internal	Not Required	For troubleshooting cluster issues, this port should be open on at least one cluster node, but is not required.
RAW Node	SOLR	8983	External and Internal	Internal Only	SOLR holds most RSA VRM data in the cluster for caching purposes from Hbase and queried through the RSA VRM API / UI Web Service - Required for RSA VRM.
RAW Node	JobTracker / TaskTracker	9001	External and Internal	Internal Only	Required for Map Reduce Jobs to be run on the cluster - Required for RSA VRM.

Component	Protocol or Service	Port	Default Network	Required Network	Service Notes and Requirements
RAW Node	NFS VIP Management	9997	External and Internal	Not Required	RSA Security Analytics Deployments Only - Not Required for RSA VRM.
RAW Node	NFS VIP Management	9998	External and Internal	Not Required	RSA Security Analytics Deployments Only - Not Required for RSA VRM.
RAW Node	Hive	10000	External and Internal	Not Required	RSA Security Analytics Deployments Only - Not Required for RSA VRM.
RAW Node	Job Tracker Web UI	50030	External and Internal	Internal Only	Required for Map Reduce Jobs to be run on the cluster - Required for RSA VRM.
RAW Node	Task Tracker Web UI	50060	External and Internal	Internal Only	Required for Map Reduce Jobs to be run on the cluster - Required for RSA VRM.
RAW Node	Hbase Server Service	60000	External and Internal	Internal Only	Hbase service / database is heavily utilized by RSA VRM - Required for RSA VRM.
RAW Node	Hbase Web UI	60010	External and Internal	Internal Only	Hbase service / database is heavily utilized by RSA VRM - Required for RSA VRM.
RAW Node	Hbase Server Service	60020	External and Internal	Internal Only	Hbase service / database is heavily utilized by RSA VRM - Required for RSA VRM.
RSA Archer Platform Server	HTTPS	443	N/A	External	RSA VA Host must be able to connect to RSA Archer Server on port 443.
RSA Archer Platform Server	RDP	3389	N/A	External	RDP connection to the RSA Archer host is required for setup and configuration of RSA VRM.
Qualys API	HTTPS	443	N/A	N/A	RSA VA Host needs outgoing access to this off-premise data source.

Component	Protocol or Service	Port	Default Network	Required Network	Service Notes and Requirements
NVD	HTTPS	443	N/A	N/A	RSA VA Host needs outgoing access to this off-premise data source.
Nessus	HTTPS	1241	N/A	N/A	RSA VA Host needs outgoing access to this on-premise data source
McAfee	ODBC	1433	N/A	N/A	RSA VA Host needs outgoing access to this on-premise data source
Nexpose / Rapid7	HTTPS	3870	N/A	N/A	RSA VA Host needs outgoing access to this on-premise data source
Tenable Security Center	HTTPS	443	N/A	N/A	RSA VA Host needs outgoing access to this on-premise data source
Custom Data Source	SMB	445	N/A	N/A	RSA VA Host needs outgoing access to this on-premise data source

## Secure the RSA VA Host with Windows Firewall

You must allow the following ports through an Incoming Windows Firewall:

- Port 3389 - RDP is required for the setup of RSA VRM.
- Port 443 - HTTPS is required to access the RSA VA Web Interface.

No other ports aside from your business's security policies must be enabled through Windows Firewall.

## Secure RAW Cluster Nodes With IP Tables

By default, the ports needed for cluster services and the RSA VA host to cluster communication are open on both the management and private network interfaces on RSA Analytics Warehouse nodes. You must lock down the cluster services to only the internal network interface.

### Procedure

1. Open the `/etc/sysconfig/iptables` file. Enter the following command:  

```
vi /etc/sysconfig/iptables
```
2. Add the following code to every open port line except for SSH (22) and ICMP Protocol:  

```
-i ethx
```

Where *x* is the eth interface for your internal network, the default is eth0.

**Important:** If you do not know if eth0 or eth1 is the private interface, check the IP address listed in the /etc/hosts file. The interface assigned to this address should be used with the -i (interface) parameter

**Note:** To know which ports to open, refer to the port usage table in [RSA Vulnerability Risk Management Port Usage](#)

- Restart the service to apply the changes. Enter the following command:

```
service iptables restart
```

**Important:** Do not modify the following lines or you may lose connectivity to the device.

```
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j
ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

The following is an example of a finished /etc/sysconfig/iptables file:

```
/etc/sysconfig/iptables - modified / secured
# Generated by iptables-save v1.4.7 on Fri Nov 21 21:52:51
2014
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [1:140]
-A INPUT -i eth0 -p tcp -m tcp --dport 8983 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j
ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
8140 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
2049 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
2888 -j ACCEPT
```

```

-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
3888 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
5181 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
5660 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
7220 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
7221 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
7222 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
8080 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
8443 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
9001 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
9997 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
9998 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
10000 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
50030 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
50060 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
60000 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
60010 -j ACCEPT
-A INPUT -i eth0 -p tcp -m state --state NEW -m tcp --dport
60020 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Fri Nov 21 21:52:51 2014

```

## RSA VRM Installation Overview

Installing RSA Vulnerability Risk Management follows this general sequence.



1. Setup and configure the RSA Analytics Warehouse.
  - a. Install the RSA Analytics Warehouse.
  - b. Install JRE 8 on the RAW nodes.
  - c. Upgrade to MapR 4.1.
  - d. Install the RSA VRM Solution Framework on the RAW Cluster.
2. Install RSA Vulnerability Analytics.
  - a. Install JRE 8.
  - b. Replace the JCE 8 files.
  - c. Install the Vulnerability Analytics User Interface.
3. Install and configure the RSA Archer VRM solution.
  - a. Install the RSA Archer Solution.
  - b. Post Install Activities.
  - c. Configure the RSA Archer Platform to Communicate with RSA VRM.
4. Configure RSA Vulnerability Risk Management.
  - a. Connect the Vulnerability Analytics Interface to the RSA Analytics Warehouse.
  - b. Run the RSA VA Connection Manager.
5. Confirm the whole installation.

## **RSA Vulnerability Risk Management Requirements**

Before you begin to install and configure RSA Vulnerability Risk Management, your system must meet the requirements for the following components:

- [Installing the RSA Analytics Warehouse](#)
- [Installing the RSA Vulnerability Analytics](#)
- RSA Vulnerability Analytics Browser
- RSA Archer GRC

Also, there are specific requirements for interfacing with the following endpoints:

- Nessus
- Security Center
- McAfee
- Qualysguard
- Rapid7

## RSA Analytics Warehouse Requirements

- For virtual setups, you must have administrative access to VMware ESXi 5.0, 5.1, or 5.5.
- Administrative access to each node within your RSA Analytics Warehouse cluster.
- Each node within your RSA Analytics Warehouse cluster and Windows RSA Vulnerability Analytics host must be located on the same private network and able to communicate with the other nodes on the network.
- Your RSA Archer machine, Windows RSA Vulnerability Analytics host, cluster, and API user should be set to the same time zone; they must be in sync with each other, down to the minute.
- Each RSA Analytics Warehouse node must have a minimum of three (3) 100 GB storage disks.
- Each RSA Analytics Warehouse node must have one additional disk dedicated to SOLR Data, with a minimum size of 125 GB.
- The minimum requirements for a full production environment on each RSA Analytics Warehouse node are four (4) cores and thirty two (32) GB of RAM.

**Important:** The RAW administrator must monitor the disk space in the SOLR file system. If the SOLR cores are at 75% capacity, additional disk space is needed. In a virtual setup, the location to monitor is /vrmdata. In a physical hardware setup, the location to monitor is /opt/rsa/vrm/solr1.

- Your Windows Host Server, RSA Archer machine, cluster, and API user should be set to the same time zone; they must be in sync with each other, down to the minute.

## RSA Vulnerability Analytics Host Requirements

- Administrative access to a Windows Host Server, running Microsoft Windows Server 2008 R2 or Microsoft Windows Server 2012 R2.
- Your Windows Host Server must contain at least two (2) cores, sixteen (16) GB of RAM, and one hundred (100) GB of hard disk space.
- Depending on the number of assets, you may need to add additional hard disk space.
- If you are deploying in a virtual environment, you must provision an additional hard disk for the virtual RAW cluster nodes.
- Your Windows Host Server must be dedicated to RSA Vulnerability Analytics and not shared with any other services.
- Your Windows Host Server must be locked down and secured using your company's best practices.

- Your Windows Host Server, RSA Archer machine, cluster, and API user should be set to the same time zone; they must be in sync with each other, down to the minute.

### **RSA Vulnerability Analytics Supported Browsers**

- Google Chrome (all versions).
- Mozilla FireFox 28 or later.
- MS Internet Explorer 9 and later.

### **RSA Archer Vulnerability Risk Management Solution Requirements**

- A configured RSA Archer Platform instance running version 5.5.x or later.
- Administrative access to the RSA Archer Host Server.
- Administrative access to the RSA Archer Platform.

**Note:** RSA Vulnerability Risk Management is not currently supported in the RSA Archer SaaS environment.

### **Tenable Nessus User Account Requirements for Scan Results**

- Create a new Nessus user account with System Administrator rights that include scan data results.
- Use an existing Nessus user account that includes scan data results.
- Allow user access to move/delete all processed files in the remote share feature.

**Note:** This is specific to Fileshare and is not supported with API.

### **Tenable Security Center User Account Requirements for Scan Results**

- The Security Center user can have any roles, other than Administrator, to pull scan data results.
- Allow user access to move/delete all processed files in the remote share feature.

### **QualysGuard API Requirements for Scan Results**

- The user account must have Reader privileges.
- The user account must have API access.
- The user account must have username/password authentication.

**Note:** Two-factor authentication is not supported.

## Rapid7 User Account Permission Requirements for Use as Endpoint

- Allow user to access all asset groups.
- Allow user to access all sites.
- Create Reports.
- View asset group data.
- View asset site data.

## RSA Vulnerability Risk Management Supported Endpoints

**Note:** Endpoints listed as N/A are not versioned.

RSA VRM Version 1.2 supported endpoints:

Supported Endpoints For RSA VRM 1.2	Supported Endpoint Version
RSA Archer Solution	1.2
RSA Archer Platform	5.5.x and higher
RSA Analytics Warehouse	10.3 SP 4, 10.4 SP 2
McAfee Vulnerability Manager	7.5
QualysGuard	5.13.40-1
Rapid7	6.1.8
Tenable Nessus	6.5.4
Tenable Security Center	5.1.0

RSA VRM Version 1.1 SP 1 supported endpoints:

<b>Supported Endpoints For RSA VRM 1.1 SP 1</b>	<b>Supported Endpoint Version</b>
RSA Archer Solution	1.1 SP 1
RSA Archer Platform	5.4 SP1 P1, 5.5 SP 2
RSA Analytics Warehouse	10.3 SP 4, 10.4 SP 2
McAfee Vulnerability Manager	7.5
QualysGuard	N/A
Rapid7	5.8, 5.10.2, 5.11.6
Tenable Nessus	5.2.4

RSA VRM Version 1.1 supported endpoints:

<b>Supported Endpoints for RSA VRM 1.1</b>	<b>Supported Endpoint Version</b>
RSA Archer Solution	1.1
RSA Archer Platform	5.4 SP 1, 5.5
RSA Analytics Warehouse	10.3 SP 2
McAfee Vulnerability Manager	7.5
QualysGuard	N/A
Rapid7	5.8
Tenable Nessus	5.2.4

RSA VRM Version 1.0 supported endpoints:

<b>Supported Endpoints for RSA VRM 1.0</b>	<b>Supported Endpoint Version</b>
RSA Archer Solution	1.0
RSA Archer Platform	5.4
RSA Analytics Warehouse	10.2

Supported Endpoints for RSA VRM 1.0	Supported Endpoint Version
McAfee Vulnerability Manager	7.5
QualysGuard	N/A
Rapid7	Not Supported
Tenable Nessus	Not Supported

## RSA Vulnerability Risk Management Files

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

File	Description
rsa-vrm-1.2.0-xxx-installer.exe	The RSA Vulnerability Analytics Windows Installer.
vrm-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. <b>Important:</b> 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: Install and Configure Vulnerability Risk Management 1.2

<a href="#"><u>Installing the RSA Analytics Warehouse</u></a>	23
<a href="#"><u>Installing the RSA Vulnerability Analytics</u></a>	40
<a href="#"><u>Install the RSA Archer Vulnerability Risk Management Solution</u></a>	42
<a href="#"><u>Post Install Activities</u></a>	47
<a href="#"><u>Configure the RSA Archer Platform to Communicate with RSA Vulnerability Risk Management</u></a>	48
<a href="#"><u>Connect the RSA Vulnerability Analytics Interface to the RSA Analytics Warehouse</u></a>	49
<a href="#"><u>Run the Connection Manager</u></a>	50
<a href="#"><u>Confirm the Installation</u></a>	52
<a href="#"><u>Configure Single Sign On (Optional)</u></a>	53

### Installing the RSA Analytics Warehouse

In order to install RSA VRM 1.2, you must have a fully functioning RSA Analytics Warehouse. The following must be completed before the RSA Analytics Warehouse can be fully installed:

1. Download the .tar file.
2. Install JRE 8.
3. Upgrade to MapR 4.1.
4. Upgrade the RSA VRM rpm.

### Install the RSA Analytics Warehouse

**Important:** If you have an existing RSA Analytics Warehouse (RAW) cluster set up, skip to [Install the RSA VRM Framework on the RAW Cluster](#). Only versions 10.3.4 and 10.4.x are supported with VRM 1.2.

RSA Vulnerability Risk Management relies on the RSA Analytics Warehouse as its data storage component.

#### Procedure

1. [Collect the Information Needed](#)
2. [Deploy the RSA Analytics Warehouse Virtual Appliance OVA](#)
3. [Create Data Partition \(Virtual\)](#)
4. [Update the Network Time Protocol Settings](#)

5. [Configure the Network Interfaces](#)
6. [Configure the Hostname and Hosts File](#)
7. [Generate and Update the Default UUID in the Appliances](#)
8. [Edit the Configuration Template File in the RAW Virtual Appliance](#)
9. [Configure the Warehouse Cluster](#)
10. [Install the RAW License File](#)

### Collect the Information Needed

**Important:** You must have access to the three emails sent to you upon purchasing RSA Vulnerability Risk Management.

### Procedure

1. Download the RSA VRM License file.
  - a. Logon to Download Central (DLC) at <https://download.rsasecurity.com>.
  - b. On the Software License Verification page, in the Enter RSA Product License number field, enter the RSA Archer Platform Serial Number.
  - c. On the Order Detail page, click License(s).
  - d. On the License Information page, click Download.
2. Download the RSA Analytics Warehouse OVA.
  - a. On DLC, on the Software License Verification page, in the Enter RSA Product License number field, enter the Warehouse Node Serial Number.
  - b. On the Order Detail page, click Product List.
  - c. On the RSA Security Analytics Product Information page, from the Product Information list, click the appropriate version of the Warehouse Node.
  - d. Download the SA-x-x.zip file.
3. Download the RSA VRM .zip file.
  - a. On DLC, click Product Download > Product List > RSA Archer Platform > RSA Vulnerability Risk Management.
  - b. Click the version you want to download.
  - c. Download the rsa-vrm-1.2.0-suite.zip file.
4. Note the following details.

Information Needed	Value
Network IP addresses, netmask, and gateway IP addresses for the virtual appliances.	



Information Needed	Value
Network names for all appliances in the cluster.	
DNS or hostname information for the cluster.	
Administrative access for virtual appliances.	N/A

### Deploy the RSA Analytics Warehouse Appliance OVA (Virtual)

Deploy the RSA Analytics Warehouse appliance OVA file on the ESX Server using the vSphere client.

**Important:** This procedure is for virtual warehouse clusters only. If you are not using a virtual appliance, proceed to [Update the Network Time Protocol Settings](#).

#### Procedure

1. Log on to the vSphere Client using credentials with administrator rights.
2. Select File > Deploy OVA Template.
3. In the Source section, click Browse to navigate and select the downloaded OVA file. Click Next.
4. Verify the OVA details, and click Next.
5. Accept the license agreement, and click Next.
6. In the Name and Location section, perform the following:
  - a. Enter a name for the virtual appliance in the Name field.
  - b. If prompted, select the inventory location in the Inventory Location field.
  - c. Click Next.
7. If prompted, in the Host / Cluster section, select the host or cluster on which you want to run the virtual appliance, and click Next.
8. If Distributed Resources Scheduler (DRS) is enabled, select the resource pool within which you want to deploy the virtual appliance, and click Next.
9. In the Datastore section, select the datastore where you want to store the virtual appliance files, and click Next.
10. In the Disk Format section, select one of the following based on your environment:
  - Thin provisioned format.
  - Thick provisioned format.

**Note:** Thick provisioning is typically better if you have ample disk space, while thin provisioning typically uses less disk space. Neither thick or thin provisioning should cause any noticeable performance impact in most cases.

11. Click Next.
12. If prompted, in the Network Mapping section, select the network mapping for the internal private network, and click Next.
13. In the Ready to Complete section, review the details provided under Deployment Settings and make any edits necessary, and click Finish. The virtual appliance appears under the appropriate resource pool in the Inventory.
14. Set the External Network.
  - a. Right-click the virtual appliance, and click Edit Settings.
  - b. Click the Hardware tab.
  - c. Click Network Adapter 2.
  - d. From the Network Connection drop-down menu, select Network Mapping for External Network.
15. Set the CPUs.
  - a. Click CPUs.
  - b. Set the number of virtual sockets to 4.
  - c. Set the number of cores per socket to 1.
16. Set the memory.
  - a. Click Memory.
  - b. Set the memory size to 32 GB.
17. Add an additional virtual disk.
  - a. Click Add.
  - b. Select Hard Disk, and click Next.
  - c. Select Create a New Virtual Disk, and click Next.
  - d. Set the capacity to 125 GB.
  - e. Choose your preference of Thin or Thick provisioning, and click Next.
  - f. Click Next.
  - g. Click Finish.
  - h. Click OK.
18. Once the virtual machine finishes configuring, power on the virtual appliance.
19. Accept the license agreement.

The virtual appliance reboots and the wizard appears on the console.

### Create Data Partition (Virtual)

**Important:** This procedure is for virtual setups only. If you are not using a virtual appliance, proceed to [Update the Network Time Protocol Settings](#).

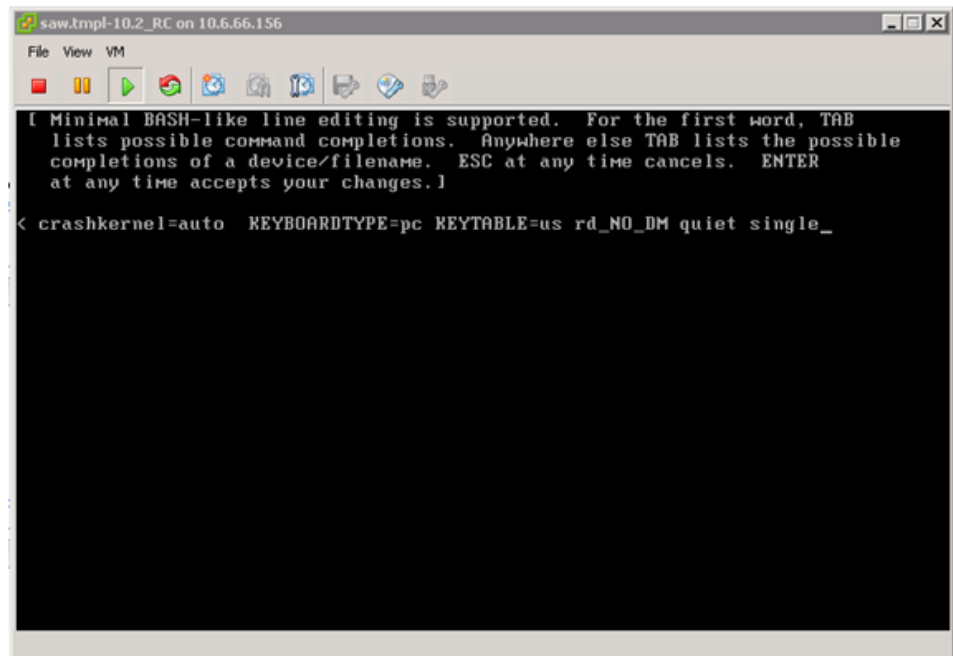
This task creates data partitions for the new virtual machines to use.

#### Procedure

1. Right-click the RSA Analytics Warehouse virtual machine, and click Open Console.
2. Do one of the following:
  - Power on the virtual machine.
  - Logon and restart the virtual machine.

**Important:** The first boot needs to be completed before making any changes to the file system. A first boot includes accepting the license agreement, automated system configuration, and a reboot.

3. At the GRUB menu, press any key to interrupt the boot process.
4. Press p, and enter the following password:  
netwitness
5. Press a to edit the boot parameters.
6. Add the word `single` to the end of the line, and press Enter:



The system boots into single user mode, and displays the following:

```
saw.tmpl-10.2_RC on 10.6.66.156
File View VM

/dev/mapper/VolGroup00-tmp: clean, 94/393216 files, 60631/1572864 blocks
/dev/mapper/VolGroup00-vartmp: clean, 11/655360 files, 79663/2620416 blocks
[ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
Welcome to CentOS
Starting udev: [ OK ]
Setting hostname NWAPPLIANCE15133: [ OK ]
Setting up Logical Volume Management: 6 logical volume(s) in volume group "VolGroup00" now active
[ OK ]
Checking filesystems
/dev/sda1: clean, 18215/524288 files, 316909/2097152 blocks
/dev/mapper/VolGroup00-usr: clean, 44119/262144 files, 371457/1048576 blocks
/dev/mapper/VolGroup00-usrhome: clean, 14/131072 files, 25391/524288 blocks
/dev/mapper/VolGroup00-var: clean, 1372/393216 files, 79982/1572864 blocks
/dev/mapper/VolGroup00-log: clean, 46/262144 files, 51632/1048576 blocks
/dev/mapper/VolGroup00-tmp: clean, 94/393216 files, 60631/1572864 blocks
/dev/mapper/VolGroup00-vartmp: clean, 11/655360 files, 79663/2620416 blocks
[ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
[root@NWAPPLIANCE15133 /]#
```

7. Enter the following LVM commands:
 

```
lvm pvcreate /dev/sdf
lvm vgextend VolGroup00 /dev/sdf
lvm lvcreate -L 110G -n vrmdata VolGroup00
lvm lvresize -l 3869 /dev/mapper/VolGroup00-tmp
```
8. Enter the following commands:
 

```
mkfs.ext4 /dev/mapper/VolGroup00-vrmdata
umount /dev/mapper/VolGroup00-tmp
e2fsck -f /dev/mapper/VolGroup00-tmp
resize2fs /dev/mapper/VolGroup00-tmp
mkdir /vrmdata
```
9. Use vi to edit /etc/fstab and add /dev/mapper/VolGroup00-vrmdata as shown:

```

#
# /etc/fstab
# Created by anaconda on Wed May  8 22:08:34 2013
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=55a838df-b617-4965-91b6-0c0dbbe40f3d /          ext3      defaults
ts      1 1
UUID=7a0cffce-77dd-4833-afac-bfb0f97dfcf4 swap        swap      defaults
ts      0 0
tmpfs   /dev/shm        tmpfs     defaults      0 0
devpts  /dev/pts        devpts    gid=5,mode=620 0 0
sysfs   /sys            sysfs     defaults      0 0
proc    /proc           proc      defaults      0 0
#
#
/dev/mapper/VolGroup00-vrmda /vrmda ext4 defaults 1 2
/dev/mapper/VolGroup00-usr /usr ext4 defaults 1 2
/dev/mapper/VolGroup00-usrhome /home ext4 defaults,nosuid 1 2
/dev/mapper/VolGroup00-var /var ext4 defaults 1 2
/dev/mapper/VolGroup00-log /var/log ext4 defaults 1 2
/dev/mapper/VolGroup00-tmp /tmp ext4 defaults,nosuid 1 2
/dev/mapper/VolGroup00-vartmp /var/tmp ext4 defaults,nosuid 1 2

```

mount -a

df -h

Ensure that the results look exactly like the following image:

```

[root@NWAPPLIANCE9121 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        7.9G  396M  7.1G   6% /
tmpfs            7.8G   0  7.8G   0% /dev/shm
/dev/mapper/VolGroup00-vrmda
                109G  188M  103G   1% /vrmda
/dev/mapper/VolGroup00-usr
                4.0G   1.4G   2.5G  36% /usr
/dev/mapper/VolGroup00-usrhome
                2.0G   70M   1.9G   4% /home
/dev/mapper/VolGroup00-var
                4.0G  181M   3.6G   5% /var
/dev/mapper/VolGroup00-log
                4.0G  137M   3.7G   4% /var/log
/dev/mapper/VolGroup00-tmp
                15G  155M   14G   2% /tmp
/dev/mapper/VolGroup00-vartmp
                4.0G  136M   3.7G   4% /var/tmp
/dev/mapper/VolGroup00-opt
                4.0G   1.3G   2.5G  35% /opt
/dev/mapper/VolGroup00-rabmq
                14G   33M   14G   1% /var/lib/rabbitmq
[root@NWAPPLIANCE9121 ~]#

```

**Note:** If your results do not exactly match the image, review the previous steps for errors and ensure the fstab entry is correct.

10. Reboot the virtual appliance.

11. Return to [Deploy the Appliance OVA \(Virtual\)](#) and repeat for cluster nodes 2 and 3.

**Note:** Do not clone cluster nodes. This could lead to a security risk.

### Update the Network Time (NTP) Protocol Settings on the RAW Appliance

#### Procedure

1. Log on to the appliance as a root user.
2. Edit the /etc/ntp.conf file. Enter the following command:  

```
vi /etc/ntp.conf
```
3. Scroll to the server lines containing the NTP servers and update the servers listed on your on-premise NTP servers to the addresses of your on-premise NTP servers.

**Important:** Remove any additional public servers.

### Configure the Network Interfaces for the RSA Analytics Warehouse Virtual Appliance

#### Procedure

1. Configure the eth0 interface for the warehouse cluster internal network.
  - a. Enter the following command:  

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```
  - b. Enter the values in the following table:

Field	Value
DEVICE	eth0
BOOTPROTO	static
IPADDR	<i>ip address</i>
NETMASK	<i>netmask</i>
ONBOOT	yes

2. Configure the eth1 interface for the external management network.
  - a. Enter the following command:  

```
vi /etc/sysconfig/network-scripts/ifcfg-eth1
```
  - b. Enter the values in the following table:

Field	Value
DEVICE	eth1
BOOTPROTO	static
IPADDR	<i>ip address</i>
NETMASK	<i>netmask</i>
GATEWAY	<i>gateway address</i>
ONBOOT	yes
TYPE	Ethernet
DOMAIN	<i>domain name</i>
DNS1	<i>DNS address</i>

- Restart the network. Enter the following command:

```
service network restart
```

### Configure the Hostname and Hosts File

Configure the machine hostname in the `/etc/sysconfig/network` file, and add the hostnames of all the appliances in the cluster to configure the hosts file in the individual appliances.

#### Procedure

- Set the hostname of the appliance.
  - Enter the following command:
- Enter the values in the following table:

Field	Value
NETWORKING	yes
NETWORKING_ IPV6	no
HOSTNAME	<i>Fully qualified domain name</i>

- Save the changes and exit the vi editor. Enter the following command:

```
ESC :wq
```

2. Configure the host file to add the IP address and hostname of each RSA Analytics Warehouse node in the cluster.

- a. Enter the following command:

```
vi /etc/hosts
```

- b. Add the following lines to the hosts file for each of the RSA Analytics Warehouse cluster nodes:

```
node_private_ip_address node_fqdn node_hostname
```

where:

- *node\_private\_ip\_address* is the private interface of the node in the RSA Analytics Warehouse cluster.
- *node\_fqdn* is the Fully Qualified Domain Name of the node in the RSA Analytics Warehouse cluster.
- *node\_hostname* is the hostname of the node in the RSA Analytics Warehouse cluster.

The following is an example of the /etc/hosts file with details of all of the nodes in the RSA Analytics Warehouse cluster:

```
127.0.0.1 localhost.localdomain localhost
```

```
192.168.1.10 rawnode1.domainname.com rawnode1
```

```
192.168.1.11 rawnode2.domainname.com rawnode2
```

```
192.168.1.12 rawnode3.domainname.com rawnode3
```

- c. Save the changes and exit the vi editor. Enter the following command:

```
ESC :wq
```

3. Modify the sysctl.conf file.

- a. Enter the following command:

```
vi /etc/sysctl.conf
```

- b. Add the following lines to the file:

```
net.ipv6.conf.all.disable_ipv6=1
```

```
net.ipv6.conf.default.disable_ipv6=1
```

- c. Save the changes and exit the vi editor. Enter the following command:

```
ESC :wq
```

4. Enable HBase server ports in the firewall.

- a. Enter the following commands:

```
iptables -I INPUT 23 -p tcp -m state --state NEW -m tcp
```

```
--dport 60010 -j ACCEPT
```



```
iptables -I INPUT 24 -p tcp -m state --state NEW -m tcp
--dport 60020 -j ACCEPT
```

```
service iptables save
```

**Note:** To verify that the rules have been added, run the command `iptables -L` to list all rules.

## Generate and Update the Default UUID in the Appliances in the RAW Cluster

### Procedure

1. Generate and update the UUID. Enter the following command:

```
/opt/mapr/server/mruuidgen | tee /opt/mapr/hostid
/opt/mapr/conf/hostid.*
```

**Important:** This is one command, all on the same line.

2. Restart the appliance. Enter the following command:

```
reboot
```

3. Return to [Update the Network Time \(NTP\) Protocol Settings on the Appliance](#) and repeat for nodes 2 and 3 before proceeding.

### Edit the Configuration Template File in the RAW Virtual Appliance

By default, a configuration template is provided with the RAW virtual appliance. You must edit the default configuration.

**Important:** Ensure all prior steps have been completed for each node in the cluster before proceeding.

### Procedure

1. Log on to the master appliance as root user.
2. Navigate to `/opt/rsa/maprwh/config`. Enter the following command:
 

```
cd /opt/rsa/maprwh/config
```
3. Create a copy of the configuration template. Enter the following command:
 

```
cp conf.template conf.template-name
```

 where *name* is the custom name of the configuration template file.
4. Edit the configuration template file.
  - a. Enter the following command:
 

```
vi conf.template-name
```
  - b. Provide details for the following parameters:

Parameter	Description
nodes	List the IP address of the appliances in the cluster. Ensure that each IP address is separated by spaces. All the appliances in the cluster must be listed in the same order in every configuration file for every RAW appliance.
internalnetworks	List the network addresses in CIDR format separated by spaces. This RAW appliance cluster communication is limited to the provided network addresses.  <b>Note:</b> RSA requires that you do not leave this parameter blank.
clustername	Name of the cluster. The cluster name is used to identify the Network File System (NFS) share.
disks	Displays the list of disks recognized by the operation system and these disks will be formatted in HDFS for RAW when this configuration script is executed.

Here is an example of a configured `conf.template-name` file for a 3-node virtual warehouse cluster:

```
[global]
# nodes: List of the first 5 node IP addresses in the
cluster, separated by
# spaces. Use addresses on internal network if restricting
network traffic
nodes=192.168.1.10 192.168.1.11 192.168.1.12
# internalnetworks: List of network addresses, in CIDR
format separated by
# spaces, that cluster communication will be limited to.
# Leave blank to allow communication over any network
internalnetworks=192.168.1.0/24
# clustername: Name of cluster. NFS share will be
/mapr/<clustername>
clustername=saw
# authentication: Type of authentication to use.
#
# local: Use local passwd database
# ads: Use Active Directory (see [ads] section)
authentication=local
[ads]
# domain: Windows domain to join
domain=
# realm: Active Directory realm to authenticate users
against
realm=
```

```
# servers: Active Directory authentication servers,
separated by spaces. Must
# match names in AD
servers=
# user: Privileged user with authority to add computers to
the domain
user=
# Internal settings - changing these may result in
unsupported behavior
[internal]
# *Caution* disks listed here will be overwritten
#disks=/dev/sdb /dev/sdc /dev/sdd /dev/sde /dev/sdf
/dev/sdg /dev/sdh /dev/sdi /dev/sdj
# default mapr warehouse virtual machine setup
disks= /dev/sdc /dev/sdd /dev/sde
```

5. Use scp to copy /opt/rsa/maprwh/conf.template-name to nodes 2 and 3.  
For example:

```
scp conf.template-rawcluster root@raw-node-
02:/opt/rsa/maprwh/config/conf.template-rawcluster

scp conf.template-rawcluster root@raw-node-
03:/opt/rsa/maprwh/config/conf.template-rawcluster
```

## Configure the Warehouse Cluster

### Procedure

1. Verify connectivity on each warehouse node.
  - a. Enter the following command:
 

```
hostname
```
  - b. Ensure that the returned hostname matches the appropriate entry in /etc/hosts.
  - c. Repeat steps 1a-1b for each warehouse node.
  - d. Use the ping command to verify connectivity between nodes using the FQDN entries in /etc/hosts.
2. Prepare the nodes.
  - a. Enter the following commands:
 

```
service mapr-zookeeper stop
rm -fr /opt/mapr/zkdata/version-2/*
```
  - b. Change directories. Enter the following command:
 

```
cd /opt/mapr/hadoop/hadoop-0.20.2/conf
```
  - c. Enter the following command:

- ```
cp mapred-site.xml.template mapred-site.xml
```
- d. Repeat steps 2a-2c for each warehouse node.
  3. Set up the first node.
    - a. On the first node, change directory to `/opt/rsa/maprwh/config`.
    - b. Enter the following command:  
`./configure.py conf.template-name`
    - c. When `configure.py` output reports succeeded and asks to reboot, enter the following command:  
`reboot`
    - d. Wait for the login screen to appear on the node.
  4. Set up the second node.
    - a. On the second node, change directory to `/opt/rsa/maprwh/config`.
    - b. Enter the following command:  
`./configure.py conf.template-name`
    - c. When `configure.py` output reports succeeded and asks to reboot, enter the following command:  
`reboot`
    - d. Wait for the login screen to appear on the node.
  5. Set up the third node.
    - a. On the third node, change directory to `/opt/rsa/maprwh/config`.
    - b. Enter the following command:  
`./configure.py conf.template-name`
    - c. When `configure.py` output reports succeeded and asks to reboot, enter the following command:  
`reboot`
    - d. Wait for the login screen to appear on the node.

### Install the RSA Analytics Warehouse License File

**Important:** If you have a cluster of RAW virtual appliances, install the license on the first RAW virtual appliance in the cluster.

#### Procedure

1. Ensure that you have the RAW license file from step 1 of [Collect the Information Needed](#).
2. Transfer the license file to the `/root/` directory on the first RAW appliance in the cluster.

3. Log on to the appliance as root user.
4. Navigate to /root. Enter the following command:  
`cd /root`
5. View the Java Services. Enter the following command:  
`watch jps`

**Note:** The console screen refreshes every two seconds. Wait until a service named cldb is stable and active for more than 30 seconds and then proceed to step 6.

6. Install the license file. Enter the following command:  
`maprccli license add -is_file true -license license_file_name`  
where *license\_file\_name* is the file name of the RAW license file.

**Note:** The license files are installed without any output messages. If you have included a network range in the `internalnetworks` parameter in the configuration template file, a warning message appears stating that the RAW is configured only to communicate with the network entered in the configuration template file. Ignore this warning as this does not have any functional issue.

7. Confirm the license file installation. Enter the following command:  
`maprccli license list`  
Output messages appear on the console screen. The last 2 lines of the output message are similar to the following sample:  
`hash: "F8x01f1W83LNSqq7ziun8D27XnQ="`  
`Dec 14, 2016`
8. Ensure that the listed date is set in the future or set to permanent.

## Installing JRE 8

**Important:** This procedure must be done on each node in the cluster.

### 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 build number.
3. Transfer the JRE 8 download to the `/usr/lib/jvm` folder on 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-xxx.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:
 

```
maprccli 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
```
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.

## Install the RSA VRM Framework on the RAW Cluster

Install the RSA VRM framework onto the RAW cluster to allow it to communicate with RSA Vulnerability Analytics.

**Note:** Run this install after the `upgrade-to-mapr-4.1.sh` has successfully completed.

### Procedure

1. On the node where the installer is located, enter the following command:

```
/tmp/vrm-1.2.0/vrm-install.sh
```

**Important:** Running the script file restarts the MapR and Solr services. This script may take some time to execute and should be monitored. Wait until the MapR and Solr services are running again before continuing to step 4. Do not run any other script on any other node during this time.

**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.

2. Confirm that the MapR and Solr services are running again. Enter the following:  
`jps`

If the command returns some output, the MapR and Solr services are running. If you do not receive an output, wait a few minutes and try again. If you still do not receive an output, call RSA Support Services.

## Installing the RSA Vulnerability Analytics

After you have installed the RAW, you need to install the Vulnerability Analytics. The following must be completed before the Vulnerability Analytics install can be completed:



- [Install the JRE and JCE](#)
- [Install the RSA Vulnerability Analytics User Interface](#)

## Install 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. Run the JRE 8 executable and install it.
3. 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.

## Install the RSA Vulnerability Analytics User Interface

RSA Vulnerability Risk Management includes a separate web-based user interface called RSA Vulnerability Analytics. Install the RSA Vulnerability Analytics user interface on your Windows Host Server.

### Procedure

1. Logon to the Windows Host Server with Administrator access.
2. Install all available security updates.
3. Double-click the `rsa-vrm-1.2.xxx-installer.exe` installation file.
4. Read and accept the license agreement.
5. Click Next.
6. On the Directory Setup page, choose a directory to install to and a directory to house the data.
7. Click Next.
8. On the Confirmation page, click Install.
9. After installation is complete, click Finish.  
**Note:** The RSA VRM installer adds two new Windows Services, RSA Vulnerability Management - Data Collector and RSA Vulnerability Management - User Interface. These are set to run once installed.
10. Navigate to and open the `installation directory\rsa\vrms\config\collector-config.properties`  
where *installation directory* is the directory you selected in step 6.
11. Save the collector-config.properties file.

12. Open the C:\Windows\System32\drivers\etc\hosts file for edit.

**Important:** Editing this file requires administrator privileges.

13. Enter the same values that you created in step 2b of [Configure the Hostname and Hosts file](#). Enter the commands in the following format:

*node\_private\_ip\_address node\_fqdn node\_hostname*

where:

- *node\_private\_ip\_address* is the private interface of the node in the RSA Analytics Warehouse cluster.
- *node\_fqdn* is the Fully Qualified Domain Name of the node in the RSA Analytics Warehouse cluster.
- *node\_hostname* is the hostname of the node in the RSA Analytics Warehouse cluster.

14. Save and close the file.

## Install the RSA Archer Vulnerability Risk Management Solution

RSA Vulnerability Risk Management includes a corresponding RSA Archer Vulnerability Risk Management solution.

### Procedure

1. [Apply the RSA Archer Vulnerability Risk Management Solution License Key](#)
2. [Import and Install the RSA Archer Vulnerability Risk Management Package](#)
3. [Edit the RSA Vulnerability Risk Management Group](#)
4. [Create a User Account for Web Service Client](#)
5. [Add RSA Archer VRM Group to Enterprise Management Workspace](#)
6. [Change Key Field Configuration for Findings Application \(Optional\)](#)

## Apply the RSA Archer Vulnerability Risk Management Solution License Key

**Note:** The license key needs to be applied to both the RSA Archer VRM Solution and RSA Vulnerability Analytics.

### Procedure

1. Logon to your RSA Archer host server.
2. Click Start > RSA Archer Control Panel.
3. In the Instance Management pane, right-click the RSA Archer instance.
4. Click Update License Key.

5. In the Activation Method section, select Manual.
6. Follow the on-screen instructions to manually activate your license key.
7. Copy the activated license key, and click Paste Key.
8. Note the Serial Number and activated License Key listed on this screen, without the begin and end comments.
9. Click Activate.
10. Click Save.
11. On your RSA Vulnerability Analytics host machine, navigate to C:\Program Files\rsa\vrml\config\.
12. Edit the license .xml file.
13. In the license .xml document, enter the following information:  

```
<serial_number>serial number</serial_number>  
<license_key>license key</license_key>
```

Where:

  - *serial number* is the RSA Archer serial number noted in steps 4-7. It is 25 characters long.
  - *license key* is the activated license key noted in step 7.
14. Remove any comments remaining in the license.xml document.
15. Save the license.xml document.


## 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.<br><br><b>Important:</b> 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. |
| 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.

## Edit the RSA Vulnerability Risk Management Group

Edit a user group to use the new subgroups that were added during installation.

### Procedure

1. Click Navigation > Administration > Access Control > Manage Groups.
2. In the Manage Groups section, for the Vulnerability Risk Management group, click Edit .
3. In the Members section, locate and select the following groups from the Available list:
  - VRM - Archer Admin
  - VRM - IT Executive
  - VRM - IT Security
  - VRM - Device Owner
  - VRM - Business Manager
  - VRM - Read Only
  - VRM - Web Service API
4. Click Save.

## Create a User Account for Web Service Client

Create a user account for the Web Service API to use to transfer data into the RSA Archer Platform. The Web Service API uses the web service client to transfer data.

### Procedure

1. Click Administration > Access Control > Manage Users > Add New.
2. In the Full Name fields, enter a first and last name.

**Note:** The RSA Archer Platform creates the user name from the first and last name when you save this new user account.
3. In the Default Email field, enter the e-mail address to be associated with this new user account.

4. In the Time Zone field of the Localization section, select the appropriate timezone.

**Important:** Your RSA Archer machine, Windows Host machine, cluster, and API user should be set to the same time zone; they must be in sync with each other, down to the minute.


5. For the Locale field, select English (United States).
6. Click the Groups tab.
7. From the Available list, select VRM - Web Service API.
8. Click the Access Rights tab.
9. From the Available Roles list, select both of the following:
  - VRM - Web Service API
  - System Administrator
10. From the Selected Roles list, remove General User. Click Save.
11. Click the user account that you just created.
12. Click the Account Maintenance tab.
13. In the Password field, click Change Password and enter a new password.

**Important:** Note the user name shown for the new user account that you created. Also, remember the new password that you created in step 13.
14. When prompted, click Continue.
15. Clear Force Password Change On Next Sign-In.
16. Click Save.

## Add VRM Group to Enterprise Management Workspace

Add the RSA Vulnerability Risk Management group to the RSA Archer Enterprise Management solution workspace.

### Procedure

1. Click Navigation > Administration > Workspaces and Dashboards > Manage Workspaces.
2. In the Manage Workspaces section, of the Enterprise Management workspace, click Edit .
3. Click the Access tab.
4. Click Lookup.
5. From the Available list, select Groups > Vulnerability Risk Management.
6. Click Save.

## 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.

## Post Install Activities

The package installation does not update some attributes of objects, or delete obsolete objects that are not included in the RSA Archer Vulnerability Risk Management solution. RSA recommends that you compare the objects in your database with the information in the *Data Dictionary* to determine which objects are obsolete or have been updated.

### Deleting Obsolete Objects

Packaging does not delete obsolete objects. RSA recommends that you delete these objects because they may affect how the applications function. Follow these guidelines on deleting obsolete objects:

- If you select Override Layout when you install the RSA Archer VRM solution install package, the Packager does not remove old fields from the layout. You must delete the old fields.
- Evaluate your need for certain data driven events (DDE), pre-existing rules, and actions that were not updated through Packaging. Delete any obsolete rules and actions.
- Verify the DDE order and update it if necessary.
- Evaluate pre-existing notifications and reports that Packaging did not update. Delete obsolete notifications and reports.

For more information about objects, see the "Managing Packages" section of the *RSA Archer GRC Online Help*.

## Validating Formulas and Calculation Orders

Follow these guidelines on validating formulas and calculation orders:

- The packaging process logs an error if a formula does not validate. This error may be caused by a formula that references applications or fields that do not exist in the instance and were not part of the package (for example, fields in applications that are part of a different core solution). Review those fields to determine if they are needed.
  - If a field is needed, modify the formula to remove references to applications or fields that do not exist in your instance. Fields that do not exist in your instance are identified with an exclamation mark.
  - If a field is not needed, delete the field or remove it from the layout. If the field is not deleted, removing the formula prevents errors from being written in the log files when records are saved.
- Verify the order of calculations for each application and sub-form in the solution. See the *Data Dictionary* for calculation orders for each individual application or sub-form.
- Update the order of calculations as needed for each application and subform in the solution.

For more information about deleting objects, see the "Managing Calculations" section of the *RSA Archer GRC Online Help*.

## Verifying Key Fields

Packaging does not change key fields. To verify the key fields in each application, see the RSA Vulnerability Risk Management *Data Dictionary*.

## Configure the RSA Archer Platform to Communicate with RSA Vulnerability Risk Management

Configure the RSA Archer platform to communicate with RSA Vulnerability Risk Management through the RSA Archer REST API.

### Procedure

1. Log into the RSA Archer host machine.
2. Open Internet Information Services (IIS) Manager.
3. Click on the hostname on the left pane.
4. Double-click Server Certificates.
5. Do one of the following:
  - If you want to use the self-signed certificate, in the Actions pane, click Create self-signed certificate. Go to step 6.



- If you want to use a certificate signed by your CA, proceed according to your system administrator. Go to step 8.
  - 6. Enter a name for the certificate.
  - 7. In the left pane, click Sites > Default Web Site.
  - 8. In the Actions pane, click Bindings.
  - 9. Do one of the following:
    - If https exists, select https. Click Edit.
    - If https does not exist, click Add. Select https for a Type.
  - 10. In the SSL Certificate field, select the newly created Self-Signed Certificate.
- Note:** Ensure that the API application is set to use an application pool that utilizes version 4.0/4.5 of .net framework. RSA recommends using the same application pool as the RSA Archer application.
11. Ensure that the RSA Archer instance is accessible using an https URL in any web browser. For example:  
`https://Archer web server/api/core`

## Connect the RSA Vulnerability Analytics Interface to the RSA Analytics Warehouse

### Procedure

1. Logon to RSA Vulnerability Analytics with Administrator access. The address is `https://<data collector hostname>/.`

**Important:** RSA Vulnerability Analytics ships with a self-signed certificate so that the user interface can be accessed using an HTTPS connection. If you receive an SSL error when accessing RSA Vulnerability Analytics, proceed with the logon as normal. You can also use your own self-signed certificate instead. For detailed instructions on installing your own self-signed certificate, see [Install a Customer Certificate](#).

**Important:** RSA recommends you change the default Administrator password.

2. Click Administration > Data Warehouse.
3. Click Add (+).
4. Enter the following details:

| Field | Value                           |
|-------|---------------------------------|
| Name  | A descriptive name of your RAW. |

| Field             | Value                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zookeeper Node(s) | The private network Zookeeper Nodes of your RAW nodes.<br><br><b>Note:</b> Add each host as separate entry rows.<br><br><b>Important:</b> If your RAW cluster includes more than three (3) nodes, only a certain subset of the nodes may include zookeeper nodes. |
| Hadoop CLDB Port  | 7222                                                                                                                                                                                                                                                              |
| Zookeeper Port    | 5181                                                                                                                                                                                                                                                              |

- Click Test Connection to ensure the connection with the RAW is successful.
- Click Save.
- On your Windows Host, restart the RSA Vulnerability Management - Data Collector service.

## Run the Connection Manager

To import data into RSA Vulnerability Analytics, you must set up the different endpoints in which you want to import the data from. Each night, RSA Vulnerability Analytics automatically scans the configured endpoints, imports the collected data, and forwards that data to the RAW.

**Important:** RSA Archer device records must provide data that matches the imported RSA Vulnerability Analytics records from the scans (for example, IP Address or DNS).

### Procedure

- Determine which of the following supported endpoints you want to connect to RSA Vulnerability Analytics.
  - Custom Data Sources
  - National Vulnerability Database
  - McAfee Vulnerability Manager
  - QualysGuard
  - Rapid7 Nexpose
  - RSA Archer

- Tenable Nessus
  - Tenable Security Center
2. On your Windows Host Server, change directories to <VRM Installation Directory>\data-collector\ where <VRM Installation Directory> is the directory you chose in step 4 of [Install Vulnerability Analytics User Interface](#).

**Note:** The default directory is C:\Program Files\RSA\VRM\data-collector\

3. Run the runConnectionManager.bat batch file with Administrator access.
4. From the VA Connection Manager Wizard main menu, select Add Endpoint.
5. Select the Archer Endpoint.
6. Complete the following:
  - a. Enter the Archer Endpoint URL:https://<Web Server>/rsaarcher
  - b. Enter your instance.
  - c. Enter the username and password created in [Create a User Account for Web Service Client](#).
  - d. Enter the REST URL:https://<Web Server>/RSAarcher/api/core

**Note:** Ensure that the web server name exactly matches the CN name of the web certificate in the RSA Archer VRM user interface. An IP address cannot be used here. Ensure that this name is resolvable in the RSA Vulnerability Analytics host system.

7. Configure the supported endpoints you identified in step 1. For detailed instructions, see [Configure Endpoints](#).
8. (Optional) To immediately run the workflows:
  - a. Restart the RSA Vulnerability Management - Data Collector service.
  - b. From the main menu, select: Run Workflows.
  - c. Select the option corresponding to the data you want to import.

**Note:** Run only one job at a time.
9. (Optional) To immediately run the RSA Vulnerability Analytics rules:
  - a. From the main menu, select: Run Rules.
  - b. Select option 2 to run all of the jobs.
10. (Optional) To test the connection, from the main menu, select: Test Connection. Any status code other than "Successfully connected to Endpoint" is considered a failure. If the status code fails, run it again.
11. End the session, select: Exit

## Confirm the Installation

**Important:** If the installation does not comeback as 100% confirmed, refer to [Troubleshooting RSA Vulnerability Risk Management](#).

### Procedure

1. Confirm the RAW installation.
  - a. Logon to the RAW appliance.
  - b. Confirm that the web servers for the Solr search engine are running.
    - i. Run the following command:
 

```
service rsa-vrm-web1 check
```
    - ii. In the returned output, look for the following value:
 

```
Jetty running pid=process_id
```
  - c. Confirm that each node of the Solr web application is accessible.
    - i. Run the following command:
 

```
curl -I1 http://localhost:8983/solr/
```
    - ii. In the returned output, look for the following value:
 

```
200 OK
```
  - d. Confirm that the HBase tables were created properly.
    - i. Run the following command:
 

```
echo "list" | hbase shell
```
    - ii. In the returned output, look for the following values:
 

```
list
TABLE
alert
asset
counter
device_index
issue
lookupvalue
revision
ticket
timeline
vulnIndex
vulnerability
11 row(s) in x seconds.
```
2. Confirm the RSA Vulnerability Analytics installation.
  - a. Logon to the RSA Vulnerability Analytics web host.
 

```
https://<hostname>
```

The default credentials are:

- Username: admin
  - Password: rsavrm!!!
- b. Confirm that the following services are running:
- RSA Vulnerability Management - Data Collector
  - RSA Vulnerability Management - User Interface

## Configure Single Sign On (Optional)

RSA Vulnerability Risk Management supports single sign on through integrating with Site Minder.

### Procedure

1. Logon to the RSA Vulnerability Analytics Host.
2. Stop the RSA Vulnerability Management - User Interface service.
3. Navigate to and open the *installation directory\RSA\VRM\config\uiconfiguration.properties* file.
4. Set the `ssoEnabled=false` property to `ssoEnabled=true`.
5. Set the `ssoHeader=SM_User` property to `ssoHeader=SM User`.  
where *SM User* is the user name for the Site Minder account connecting to RSA Vulnerability Analytics.
6. Save and exit the `uiconfiguration.properties` file.
7. Restart the RSA Vulnerability Management - User Interface service.

## Appendix A: Configure Endpoints

|                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------|----|
| <a href="#"><u>Configure a Mapped Share Drive (for Nessus, Security Center, and Custom Data Only)</u></a> ..... | 54 |
| <a href="#"><u>Configure Custom Data</u></a> .....                                                              | 55 |
| <a href="#"><u>Configure Custom Endpoint</u></a> .....                                                          | 57 |
| <a href="#"><u>Configure Security Center Endpoint</u></a> .....                                                 | 59 |
| <a href="#"><u>Configure Nessus Endpoint</u></a> .....                                                          | 61 |
| <a href="#"><u>Configure Qualys Endpoint</u></a> .....                                                          | 62 |
| <a href="#"><u>Configure Rapid7 Endpoint</u></a> .....                                                          | 63 |
| <a href="#"><u>Set Up and Configure McAfee Vulnerability Manager Endpoint</u></a> .....                         | 64 |

### Configure a Mapped Share Drive (for Nessus, Security Center, and Custom Data Only)

RSA Vulnerability Risk Management allows you to configure a mapped network share drive for either a Nessus or custom data source endpoint. You must first create a special user account with the correct privileges to access your network share drive.

#### Procedure

1. On your Windows Host computer, click Start > Control Panel > Administrative Tools > Computer Management.
2. Click System Tools > Local Users and Groups > Users.
3. Right-click Users > New User.
4. Enter a user name and password.

**Note:** Note the new user name and remember the password you create.

5. Right-click the new user name > Properties.
6. Click the Member Of tab.
7. Click Add.
8. Add the Administrators group to the user. Click OK.
9. Log out of the Windows Host with the current user.
10. Log in to the Windows Host with the newly created user (from step 4).
11. Click Start > Control Panel > Administrative Tools > Local Security Policy.
12. Click Local Policies > User Rights Assignment.
13. Double-click Log on as a service.

14. Click Add User or Group.
15. Add the newly created user (from step 4). Click OK.
16. Click Start > right-click Computer > Map Network Drive.
17. Assign a letter to the folder share you want to access, and enter the Folder you want to share. For example:  
`\\10.10.10.10\files\share\customShare`
18. Select Reconnect at logon and clear Connect using different credentials. Click Finish.
19. When prompted, enter the credentials to connect to the share.
20. Select Remember Credentials. Click OK.
21. Open the Windows Services menu.
22. Stop the RSAVulnMgmtDC service.
23. Double-click the RSAVulnMgmtDC service.
24. Click the Log On tab.
25. Select This account.
26. Click Browse.
27. Enter the newly created user. Click OK.
28. Enter the password. Click OK.
29. Start the RSAVulnMgmtDC service.

## Configure Custom Data

Once you have set up a custom endpoint in the RSA VA Connection Manager wizard, you can import custom vulnerability, asset, scan results, and .csv data.

### Procedure

1. Before importing the data, run the schema for each corresponding data type to ensure that they are configured properly. The schema are located on your VRM Windows host at:
  - *VRM-install-directory*\RSA\VRM\config\transforms\generic-vulnerability-schema.xsd
  - *VRM-install-directory*\RSA\VRM\config\transforms\generic-asset-schema.xsd
  - *VRM-install-directory*\RSA\VRM\config\transforms\generic-scan-results-schema.xsd
2. Ensure that a corresponding custom endpoint is set up in the RSA Connection Manager. For details, see [Configure Custom Endpoint](#).

3. From the endpoint which you configured in [Configure Custom Endpoint](#), copy the files that you want to import to the Source Directory you designated for the endpoint.
4. Navigate to the Source Directory you designated.
5. For each vulnerability, asset, scan results, or .csv file that you want to import, ensure that they are named according to the following table.

| Data Type     | Naming Convention | Example                                |
|---------------|-------------------|----------------------------------------|
| Vulnerability | "vuln_"           | vuln_custom.xml or vuln_custom.csv     |
| Asset         | "device_"         | device_custom.xml or device_custom.csv |
| Scan Results  | "scan_"           | scan_custom.xml                        |

**Note:** .csv scan results are not supported.

**Note:** Ensure that all of the data files are placed in the Source Directory, and not in subfolders within the Source Directory.

6. From your RSA VRM Windows Host, run the Connection Manager.
7. From the Connection Manager main menu, select: Run Workflow.
8. From the Run Workflow menu, select: Run Workflow for Custom Data.
9. From the Run Workflow for Custom Data menu, select the endpoint you configured in [Configure Custom Endpoint](#).
10. From the endpoint menu, select the data you want to import.

## Edit Custom Fields

For custom fields used in .csv or .xml files, you can change the field names used. The configuration files support the idea of defining an "alias" for the regular field name. For example, if you want to refer to the "custom1" field as, "my\_field," you can add an entry in the configuration file, such as:

```
<property>vrml.fieldMap.custom1.alias</property>
<value>my_field</value>
```

The names used in the .csv or .xml file do not need to match the display names in the RSA Vulnerability Analytics user interface. This aliasing can be done for non-custom fields as well. If, for example, you wanted to rename "ip\_addr" to "ip" in the .csv or .xml file, then you can add the property:

```
<property>vrml.fieldMap.ip_addr.alias</property>
<value>ip</value>
```



**Procedure**

1. Navigate to C:\Program Files\RSA\VRM\config
2. Perform one of the following:
  - Edit device field names. Open the conf-vm-devicecustom.xml file.
  - Edit vulnerability field names. Open the conf-vm-vulncustom.xml file.
3. Make the changes to the file.
4. Save and exit the file.

**Edit Custom Field Display Labels in RSA Vulnerability Analytics****Procedure**

1. From the webapp install directory, perform one of the following:
  - Edit device display names. Open the app/store/asset/CustomFields.js file.
  - Edit vulnerability display names. Open the app/store/vulnerability/CustomFields.js file.
2. Make the changes in the file.
3. Save and close the CustomFields.js file.

**Configure Custom Endpoint**

Configure a custom endpoint in the RSA VA Connection Manager Wizard to import customer vulnerability, asset, scan results, and .csv data into RSA Vulnerability Risk Management.

**Procedure**

1. If you are configuring a mapped share drive, see [Configure a Mapped Share Drive](#) first.
2. From the Connection Manager main menu, enter: Configure Endpoint.
3. From the Select Endpoint list, enter: Custom Data.
4. Complete one of the following tables for either a local data source/mapped share drive or a remote data source.

For a local data source or mapped share drive:

| Parameter     | Value              |
|---------------|--------------------|
| Endpoint Name | Name the endpoint. |

| Parameter                | Value                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------|
| Authentication Type      | Local                                                                                                         |
| Source Directory         | Directory that contains the custom data you want to import. For example:<br><br>C:\data or \\10.10.10.10\data |
| Copy To Backup Directory | Type one of the following:<br><br>True - create a backup<br><br>False - do not create a back up               |

For a remote data source:

| Parameter               | Value                                                                                                                                   |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Endpoint Name           | Enter a name for the endpoint.                                                                                                          |
| Authentication Type     | Remote                                                                                                                                  |
| Custom Host Name        | Host name for the remote machine.                                                                                                       |
| Domain Name             | Domain name for the endpoint.                                                                                                           |
| Authentication Username | Username used to access the endpoint.                                                                                                   |
| Authentication Password | Password associated with the username.<br><br><b>Note:</b> For security purposes, the cursor does not move when characters are entered. |
| Reenter Password        | Reenter the password associated with the username.                                                                                      |
| Source Directory        | Directory that contains the custom data you want to import. For example:<br><br>share/dataDirectory                                     |

| Parameter                | Value                                                                                                                                                                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Copy To Backup Directory | Type one of the following:<br>True - create and copy to a backup directory<br>False - do not create and copy to a backup directory<br><br><b>Note:</b> If you elect to create and copy to a backup directory, the source file is removed from its original location. |

When completed, a confirmation message states that the custom endpoint was successfully configured.

- From the Connection Manager main menu, enter: Exit.

## Configure Security Center Endpoint

### Procedure

- If you are adding a mapped share drive, see [Configure a Mapped Share Drive](#) first.
- If the Security Center endpoint is connected to VRM through a proxy, ensure that the hostname configured in the Apache Proxy server matches the Nessus hostname.
- Add the Security Center IP Address and hostname to the hosts file located in the C:\Windows\system32\drivers\etc\ folder on your Windows Host machine.

**Important:** The hostname you add to the hosts file must match the CN name in the Security Center certificate.

- From the Connection Manager main menu, enter the option for Configure Endpoint.
- From the Select Endpoint list, enter the option for Security Center.
- Enter the following information:

| Parameter               | Action                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------|
| Fileshare/API           | Provide API if you are using the server API. Use Fileshare if you are using an air-gapped environment. |
| Endpoint URL (API only) | Endpoint URL in the following format:<br><i>https://host:port</i>                                      |

| Parameter                                     | Action                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                                      | Username used to access Security Center.                                                                                                                                                                                                                                                                                                                                         |
| Password                                      | Password associated with the username.<br><br><b>Note:</b> For security purposes, the cursor does not move when characters are entered; however, the characters are still entered.                                                                                                                                                                                               |
| Reenter Password                              | Password associated with the username.                                                                                                                                                                                                                                                                                                                                           |
| Days of historical scans to load on first run | Number of days worth of scan data to load during the initial run.                                                                                                                                                                                                                                                                                                                |
| Fileshare Authentication Type                 | Type one of the following:<br><br>Local - if the data directory is on the local drive or is mapped to a share drive<br><br>Remote - If the data directory is on a remote host<br><br>For remote Fileshare authentication, you must provide the following: <ul style="list-style-type: none"> <li>• Hostname</li> <li>• Domain</li> <li>• Username</li> <li>• Password</li> </ul> |
| File Share Path                               | Type one of the following:<br><br>C:\data - for a local set up<br><br>/data/ - for a remote Fileshare path                                                                                                                                                                                                                                                                       |

When completed, a confirmation message states that the Security Center endpoint was successfully configured.

7. From the Connection Manager main menu, enter: Exit.

## Configure Nessus Endpoint

### Procedure

1. If you are adding a mapped share drive, see [Configure a Mapped Share Drive](#) first.
2. If the Nessus endpoint is connected to VRM through a proxy, ensure that the hostname configured in the Apache Proxy server matches the Nessus hostname.
3. Add the Nessus IP Address and hostname to the hosts file located in the C:\Windows\system32\drivers\etc\ folder on your Windows Host machine.

**Important:** The hostname you add to the hosts file must match the CN name in the Nessus certificate.

4. From the Connection Manager main menu, enter:  
Configure Endpoint
5. From the Select Endpoint list, enter:  
Nessus
6. Enter the following information:

| Parameter                                     | Action                                                                                                                                                                             |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fileshare/API                                 | Provide API if you are using the server API. Use Fileshare if you are using an air-gapped environment.                                                                             |
| Endpoint URL<br>(API only)                    | Endpoint URL in the following format:<br><i>https://host:port</i><br><br>The default port is 1241.                                                                                 |
| Username                                      | Username used to access Nessus.                                                                                                                                                    |
| Password                                      | Password associated with the username.<br><br><b>Note:</b> For security purposes, the cursor does not move when characters are entered; however, the characters are still entered. |
| Reenter Password                              | Password associated with the username.                                                                                                                                             |
| Days of historical scans to load on first run | Number of days worth of scan data to load during the initial run.                                                                                                                  |

| Parameter                     | Action                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fileshare Authentication Type | <p>Type one of the following:</p> <p><b>Local</b> - if the data directory is on the local drive or is mapped to a share drive</p> <p><b>Remote</b> - If the data directory is on a remote host</p> <p>For remote Fileshare authentication, you must provide the following:</p> <ul style="list-style-type: none"> <li>• Hostname</li> <li>• Domain</li> <li>• Username</li> <li>• Password</li> </ul> |
| Fileshare Path                | <p>Type one of the following:</p> <p><b>C:\data</b> - for a local set up</p> <p><b>/data/</b> - for a remote set up</p>                                                                                                                                                                                                                                                                               |

When completed, a confirmation message states that the Nessus endpoint was successfully configured.

7. From the Connection Manager main menu, enter: Exit.

## Configure Qualys Endpoint

### Procedure

1. From the Connection Manager main menu, enter: Configure Endpoint.
2. From the Select Endpoint list, enter: Qualys.
3. Enter the following information:

| Parameter    | Action                                                                  |
|--------------|-------------------------------------------------------------------------|
| Endpoint URL | <p>Endpoint URL in the following format:</p> <p><i>https://host</i></p> |
| Username     | Username used to access Qualys.                                         |

| Parameter              | Action                                                                                    |
|------------------------|-------------------------------------------------------------------------------------------|
| Password               | Password associated with the username.                                                    |
|                        | <b>Note:</b> For security purposes, the cursor does not move when characters are entered. |
| Reenter Password       | Password associated with the username.                                                    |
| Trust the certificate? | y                                                                                         |

When completed, a confirmation message states that the Qualys endpoint was successfully configured.

4. From the Connection Manager main menu, enter: Exit.

## Configure Rapid7 Endpoint

### Procedure

1. Add the Rapid7 IP Address and hostname to the hosts file located in the C:\Windows\system32\drivers\etc\ folder on your Windows Host machine.

**Important:** The hostname you add to the hosts file must match the CN name in the Rapid7 certificate.

2. From the Connection Manager main menu, enter: Configure Endpoint.
3. From the Select Endpoint list, enter: Rapid7.
4. Enter the following information:

| Parameter     | Action                                                                  |
|---------------|-------------------------------------------------------------------------|
| Endpoint Name | Name for the endpoint.                                                  |
| Endpoint URL  | Endpoint URL in the following format:<br><code>https://host:port</code> |
|               | <b>Note:</b> The default Rapid7 port is 3780.                           |
| Username      | Username used to access the Rapid7 API.                                 |

| Parameter                                     | Action                                                                                                                                                                             |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password                                      | Password associated with the username.<br><br><b>Note:</b> For security purposes, the cursor does not move when characters are entered; however, the characters are still entered. |
| Reenter Password                              | Password associated with the username.                                                                                                                                             |
| Days of Historical Scans to Load on First Run | Number of days of historical scans that you want to import on the first run.                                                                                                       |

When completed, a confirmation message states that the Rapid7 endpoint was successfully configured.

- From the Connection Manager main menu, enter: Exit.

**Note:** Rapid7 does not provide temporal metrics; however, the Rapid7 scanner results provide metrics on exploit availability.

## Set Up and Configure McAfee Vulnerability Manager Endpoint

The following procedures apply for a default installation, in which McAfee Vulnerability Manager creates its own Certificate Authority and issues certificates to all of its components.

### Procedure

- [Export the McAfee CA Certificate](#)
- [Install the McAfee CA Certificate](#)
- [Configure the McAfee Endpoint](#)

### Export the McAfee CA Certificate

Export the McAfee Vulnerability Manager Certificate Authority certificate from the database host that you want to connect to.

### Procedure

- Logon to the McAfee database host.
- Click Start > Run.
- In the Open field, enter:



mmc

4. Click File > Add or Remove Snap-ins.
5. Add the snap-in to manage certificates for the "Computer account" for the local host.
6. In the Certificates panel, click Trusted Root Certificate Authorities > Certificates.
7. Right-click the Foundstone Configuration Manager CA certificate.
8. Select All Tasks > Export.
9. Select the file format Base-64 encoded X.509 (CER).
10. Click OK.
11. In the Certificates panel, click Personal > Certificates.
12. Right-click the certificate that has the same name as the McAfee Host VM, and select All Tasks > Export.
13. Select the file format Base-64 encoded X.509 (CER).
14. Click OK.

## Install the McAfee CA Certificate

### Procedure

1. Copy and paste both of the exported certificates onto the RSA Vulnerability Analytics host machine.
2. Create a new directory anywhere on the RSA Vulnerability Analytics host machine.
3. Place the exported certificates in the new directory.
4. Open a command prompt, and run the runConnectionManager.bat script.
5. From the main menu, select Install Trusted Certificates From Directory.
  - a. For the host values, enter the Subjects of the exported certificates.
  - b. Enter the directory where the certificates are located on the local host.
  - c. When prompted, enter:

y

When completed, a confirmation message states that the certificates were stored in the trust store.

## Configure the McAfee Endpoint

### Procedure

1. From the Connection Manager main menu, enter: Configure Endpoint.
2. From the Select Endpoint list, enter: McAfee.
  - a. Enter the Subject as noted in step 9 of [Export the McAfee CA Certificate](#).

**Note:** If the database host Subject can't be reached from the RSA Vulnerability Analytics host, you must configure the local hosts file to resolve this issue.

- b. Enter the following information:

| Parameter         | Value     |
|-------------------|-----------|
| Database Name     | faultline |
| Database Username | faultline |
| Port              | 1433      |

When completed, a confirmation message states that the McAfee endpoint was successfully authenticated and the credentials were validated.

- 
3. From the Connection Manager main menu, enter: Exit.

## Appendix B: Troubleshooting RSA Vulnerability Risk Management

| Problem                                                                                                                 | Remediation                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The log on session timed out due to inactivity.                                                                         | <p>The default time limit for inactivity is 30 minutes.</p> <p>To change the time out duration:</p> <ol style="list-style-type: none"> <li>1. Open the C:\Program Files\RSA\VRM\web-ui\webapps\ROOT\web.xml file for edit.</li> <li>2. Change the &lt;session-timeout&gt; value to what you want it to be.</li> </ol> <p><b>Note:</b> The &lt;session-timeout&gt; value is in minutes.</p>                                |
| <p>An error is given when trying to create a device rule with a scheduled run time. For example:</p> <p>0 5 * * * *</p> | <p>Due to the CRON format syntax, * cannot be a wildcard for both day-of-month AND day-of-week. One of the values must be a ? instead. For example:</p> <p>0 5 * ? * *</p> <p>or</p> <p>0 5 * * * ?</p> <p><b>Note:</b> Some cron expressions support seven fields, but spring cron does not currently have that option.</p> <p><b>Note:</b> The six-field cron format is also applicable for all workflow schedules.</p> |
| You receive a license error even though you have a valid license.                                                       | Ensure that a valid license is installed. Contact Customer Support.                                                                                                                                                                                                                                                                                                                                                       |
| The Affected Devices field is not populated in RSA Archer Findings.                                                     | The Affected Devices field is only populated if the issues were found on RSA Archer devices. Ensure that you have run a getArcherAssets job in the RSA VA Connection Manager.                                                                                                                                                                                                                                             |

| Problem                                                                                                      | Remediation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In RSA Vulnerability Analytics, the Source field is empty when it should be showing as an RSA Archer device. | Ensure that you have run a getArcherAssets job in the RSA VA Connection Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| When configuring an RSA Archer endpoint in the VA Connection Manager, the password is not accepted.          | When using special characters, use only !                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| RSA Vulnerability Analytics isn't picking up the devices from RSA Archer.                                    | <p>To fix this problem:</p> <ol style="list-style-type: none"> <li>1. Stop the RSA Vulnerability Management - Data Collector service.</li> <li>2. Delete the following directory:<br/> <i>data directory \rsa\vrn\incoming\feeds\backup\getArcherAssets</i></li> <li>3. Restart the RSA Vulnerability Management - Data Collector service.</li> <li>4. Open the RSA VA Connection Manager.</li> <li>5. Delete and then re-add the Archer Endpoint.</li> <li>6. Run the Workflow for importing RSA Archer assets.</li> <li>7. Go to the RSA VA user interface, and verify that the devices are now displayed.</li> </ol> |
| RSA Archer errors occur during package import.                                                               | If the package is being imported on Archer 5.5 SP1 or later, the errors are benign and can be ignored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Problem                                                                                                                             | Remediation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Remediation Percentage metric only includes Fixed, Verified, and Closed issues. It does not include Pending Remediation issues. | <p>To include Pending Remediation issues:</p> <ol style="list-style-type: none"> <li>1. Navigate to and open the VRM_INSTALLATION/config/conf-metric-combined.xml file on the RSA VA Windows Host.</li> <li>2. Un-comment the appropriate property for the respective metric type: <pre> &lt;!-- REMEDIATION PERCENTAGE METRIC &lt;property&gt; &lt;name&gt;metric.issue.states.rpc&lt;/name&gt; &lt;value&gt;FIXED,CLOSED,VERIFIED,PENDING_REMEDIATION&lt;/value&gt; &lt;description&gt; Issue states separated by commas to override the metric calculation &lt;/description&gt; &lt;/property&gt;  AVERAGE TIME TO REMEDIATE &lt;property&gt; &lt;name&gt;metric.issue.states.atr&lt;/name&gt; &lt;value&gt;FIXED,CLOSED,VERIFIED,PENDING_REMEDIATION&lt;/value&gt; &lt;description&gt;Issue states separated by commas to override the metric calculation &lt;/description&gt; &lt;/property&gt;  AVERAGE ISSUE AGE &lt;property&gt; &lt;name&gt;FIXED,CLOSED,VERIFIED,PENDING_REMEDIATION&lt;/name&gt; &lt;value&gt;FIXED,CLOSED,VERIFIED,PENDING_REMEDIATION&lt;/value&gt; &lt;description&gt;Issue states separated by commas to override the metric calculation &lt;/description&gt; &lt;/property&gt; --&gt; </pre> </li> </ol> <ol style="list-style-type: none"> <li>3. Restart the RSA Vulnerability Management - Data Collector service.</li> </ol> |

| Problem                                                                                                                                                               | Remediation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Some jobs on some hardware RAW 4s series setups may fail due to process underutilization.</p> <p><b>Note:</b> This is not a problem for 3-node virtual setups.</p> | <p>Change the &lt;value&gt; value to the following in each file:</p> <pre>&lt;property&gt; &lt;name&gt;mapred.reduced.tasks&lt;/name&gt; &lt;value&gt;Tasktracker Nodes&lt;/value&gt; &lt;description&gt;Number of reduced tasks to use. Increase this for higher throughout.&lt;/description&gt; &lt;/property&gt;</pre> <p>where <i>Tasktracker Nodes</i> is (16 times the number of tasktracker nodes). For example, for a 3-node cluster, the value is 48.</p> <p>The files to be edited are:</p> <ul style="list-style-type: none"> <li>• conf-vrm-index-devices.xml</li> <li>• conf-vrm-index-issues.xml</li> <li>• conf-vrm-index-vulns.xml</li> <li>• conf-metric-combined.xml</li> <li>• conf-mcafee-hostscan-issue.xml</li> <li>• conf-nessus-hostscan-issue.xml</li> <li>• conf-qualys-hostscan-issue.xml</li> <li>• conf-vrm-device-archer.xml</li> <li>• conf-vrm-devicemcafee.xml</li> <li>• conf-vrm-devicenessus.xml</li> <li>• conf-vrm-devicequalys-hostlist.xml</li> <li>• conf-vrm-devicequalys-scans.xml</li> <li>• conf-vrm-devicereconciler.xml</li> <li>• conf-vrm-issuechanges.xml</li> <li>• conf-vrm-rules-ticket-issue-rel.xml</li> <li>• conf-vrm-vulnmcafee.xml</li> <li>• conf-vrm-vulnnvd.xml</li> <li>• conf-vrm-vulnnessus.xml</li> <li>• conf-vrm-vulnqualys.xml</li> <li>• conf-vrm-vulnreconciler.xml</li> <li>• conf-historical-metric-combined.xml</li> </ul> |

| Problem                                                                                                                          | Remediation                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nessus users cannot access other users' scan results.                                                                            | <p>Nessus does not support sharing scan reports between different users out of the box. RSA VRM can only download the configured user's scan reports</p> <p><b>Note:</b> Security Center does support this feature.</p>                                                                                                                                           |
| 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/vrm/setup/vrm-util.sh -a restartHBaseCluster</pre>                                                                                                                                                                                    |
| In a cluster with more than five nodes, an error is given when adding the warehouse node.                                        | <p><b>Procedure</b></p> <p>Complete the following on each node in the cluster.</p> <ol style="list-style-type: none"> <li>1. Enter the following commands: <pre>service mapr-warden stop service mapr-zookeeper stop</pre> </li> <li>2. Enter the following commands: <pre>service mapr-zookeeper start service mapr-warden start</pre> </li> </ol>               |
| An error is received when trying to trigger a workflow due to the endpoint connecting successfully with wrong proxy credentials. | <p><b>Procedure</b></p> <ol style="list-style-type: none"> <li>1. Exit and restart the connection manager session.</li> <li>2. Delete the existing endpoint for which workflows fail.</li> <li>3. Re-add the endpoint with correct proxy credentials.</li> </ol>                                                                                                  |
| The historical metrics workflow fails due to a schedule conflict with the metrics workflow.                                      | <p>The historical metrics workflow should not be run repeatedly; it should only be run on an as-needed basis. To avoid a schedule conflict with the metrics workflow, RSA recommends running the historical metrics workflow only once: during the VRM initial setup.</p> <p>Only the metrics workflow should be scheduled to run daily for accurate metrics.</p> |

| Problem                                                                                                                                               | Remediation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Scans workflow runs successfully on any scanner, but the Vulnerabilities workflow fails and data is not loaded into VRM.                          | <p><b>Procedure</b></p> <ol style="list-style-type: none"> <li>1. Stop the RSA Vulnerability Management - Data Collector service.</li> <li>2. Open the collector-config.properties file in the &lt;install_directory&gt;\config folder.</li> <li>3. Change the lastTimeRun parameter for the Scans workflow to 0 to load all data. Enter:<br/> <code>rapid7.default.getRapid7Scans.lastTimeRun.getRapid7Scans = 0</code></li> <li>4. Delete the state file for the Scans workflow, in the &lt;incoming_data_directory&gt;\incoming\feeds\tmp folder. The following is an example of a state file:<br/> <code>default-getRapid7Scans-state.txt</code></li> <li>5. Start the RSA Vulnerability Management - Data Collector service.</li> <li>6. Run the Vulnerabilities workflow.</li> <li>7. Ensure that the Vulnerabilities workflow is successful and that the vulnerabilities have been loaded into VRM.</li> <li>8. Run the Scans workflow.</li> </ol> |
| vrn-dr-backup.sh or vrn-dr-restore.sh fails on VRM 1.2 Warehouse cluster. Output backup file is empty or doesn't exist after running vrn-dr-backup.sh | <p><b>Procedure</b></p> <ol style="list-style-type: none"> <li>1. Check the cluster mode:<br/> <code>maprcli cluster mapreduce get</code></li> <li>2. If the cluster mode is not set to classic, run the following command:<br/> <code>maprcli cluster mapreduce set -mode classic</code></li> <li>3. Retry the backup with vrn-dr-backup.sh.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



## Appendix C: Uninstalling RSA Vulnerability Risk Management

### Uninstall RSA Vulnerability Risk Management

#### Procedure

1. Logon to your Windows Host Server with Administrator access.
2. Click Start > Control Panel > Programs > Programs and Features.
3. Within the program list, select RSA Vulnerability Risk Management.
4. Click Uninstall.
5. Logon to any node within your RSA Analytics Warehouse cluster with root access.
6. Run the uninstall script. Type:

```
/opt/rsa/vrm/setup/vrm-uninstall-all.sh
```

The vrm-uninstall-all.sh script file uninstalls the data and the rpm file from all nodes in the cluster.

**Important:** You may be prompted for root passwords for remote nodes. Do not leave the uninstaller unattended as prompts for the root passwords may time out. If it times out, you must restart the procedure from a different remote node.

## Appendix D: Installing Customer Certificates

RSA Vulnerability Analytics automatically comes with a self-signed SSL certificate. Users can opt to install their own Certificate Authority (CA) signed SSL certificate.

### Procedure

1. [Create a New SSL Certificate](#)
2. [Generate a Certificate Signing Request](#)
3. [Import the CA Signed Certificate and Supporting Certificates into the New Keystore](#)
4. [Edit the vrm-jetty-ssl.xml File](#)

### Create a New SSL Certificate

#### Procedure

1. Log onto the Windows Host server.
2. Ensure that the JRE1.8\bin is in the system path environment variable:
  - a. In the control panel, search for Environment Variable.
  - b. Select the PATH variable.

**Important:** Ensure that c:\Program Files\Java\JRE1.8<version\_number\_in\_your\_host>\bin\ is located in the path. If it is not, add c:\Program Files\Java\JRE1.8<version\_number\_in\_your\_host>\bin\ at the end of the PATH variable.

**Note:** If you have an existing environment, separate it with a ";". For example:

```
%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;C:\Program Files\Java\jre7\bin
```

- c. Open the command prompt.
3. Navigate to the RSA Vulnerability Analytics web-ui\etc folder:
 

```
Installation Directory\RSA\VRM\web-ui\etc
```

 where *Installation Directory* is the name of your directory.
4. Create a new keystore. Enter the following command:

```
keytool -genkeypair -alias vrm -keyalg RSA -keysize 4096 -sigalg SHA256withRSA -keystore keystore_name -ext san=dns:VA Server FQDN -ext san=ip:VA Server IP
```

where:

- *keystore\_name* is what you want to name your new keystore.
- *VA Server FQDN* is the Fully Qualified Domain Name for your RSA Vulnerability Analytics server.
- *VA Server IP* is the IP address for your RSA Vulnerability Analytics server.

**Note:** If you want to continue using self-signed certificate, you must generate a SHA256withRSA certificate and continue to complete the steps in [Edit the vrm-jetty-ssl.xml File](#).

5. When prompted, complete the following:
  - Enter a new password.
  - Enter the FQDN of the RSA Vulnerability Analytics server.
  - Select "Yes" to confirm the parameters.
  - Press Enter for the key password for *vrms*.

**Note:** For all other parameters, consult with your Certificate Authority on how to fill these in.

## Generate a Certificate Signing Request

### Procedure

1. Navigate to the RSA Vulnerability Risk Management installation folder and identify the version of jetty-util present.
2. Open a Command Prompt.
3. Enter the following command using your new keystore name and keystore password created earlier.

```
keytool -certreq -alias vrm -keystore keystore_name -file vrm.csr
```

where *keystore\_name* is the name of your new keystore.

4. When prompted, enter a password for your new keystore.

## Import the CA Signed Certificate and Supporting Certificates into the New Keystore

### Procedure

1. Ensure that all of the certificates provided by the CA are in the *VRM Installation Directory\ web-ui\etc* folder.
2. Navigate to the RSA Vulnerability Analytics etc folder:

<Installation Directory>\RSA\VRM\web-ui\etc

- Complete the following to import the different types of certificates. For each imported certificate, enter your keystore password, and enter Yes to trust the certificate.

| Certificate               | Command                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Certificate          | <pre>keytool -import -trustcacerts - keystore mgmkeystore -alias root - file root.crt</pre>                                                                                                                                                                                                                                                                                             |
| Intermediate Certificates | <p>If you are importing more than one intermediate certificate, import them in order of proximity to the root certificate (highest to lowest place in the certificate chain).</p> <pre>keytool -import -trustcacerts - keystore mgmkeystore -alias int1 - file primaryint.crt</pre> <pre>keytool -import -trustcacerts - keystore mgmkeystore -alias int2 - file secondaryint.crt</pre> |
| CA Signed Certificate     | <pre>keytool -import -trustcacerts - keystore mgmkeystore -alias vrm - file vrm.crt</pre> <p><b>Note:</b> After entering your password, "Certificate reply was installed in keystore" appears. If you receive an error, it is likely that the certificates present in the CA signed certificate's chain are not in the keystore.</p>                                                    |

## Edit the vrm-jetty-ssl.xml File

### Procedure

- Navigate to the RSA Vulnerability Analytics web-ui\lib folder:  
*Installation Directory*\RSA\VRM\web-ui\lib
- Generate an OBF of the keystore password. Enter the following command:  

```
java -cp jetty-util-8.1.10.v20130312.jar
org.eclipse.jetty.util.security.Password keystore_password
```

where *keystore\_password* is your new keystore password.
- Copy the OBF string.

4. Navigate to the RSA Vulnerability Analytics web-ui\etc folder.  
*Installation Directory*\RSA\VRweb-ui\lib
5. Open the vrm-jetty-ssl.xml for edit.
6. Enter the new keystore and new keystore password.
7. Save the vrm-jetty-ssl.xml.
8. Restart the RSA Vulnerability Risk Management - User Interface service.
9. Confirm that the new certificate is working in the RSA Vulnerability Analytics user interface.

## RSA VRM Glossary

| Term          | Definition                                                                                                                |
|---------------|---------------------------------------------------------------------------------------------------------------------------|
| Apache Avro   | A remote procedure call and data serialization framework for Apache Hadoop.                                               |
| Apache Hadoop | An open source software framework for distributed storage and distributed processing of Big Data on data clusters.        |
| Apache HBase  | A column-oriented database management system.                                                                             |
| Apache Solr   | An open source enterprise search platform.                                                                                |
| API           | Automated Programming Interface.                                                                                          |
| CA            | Certificate Authority.                                                                                                    |
| CLDB          | Container Location Database.                                                                                              |
| Cluster       | A collection of three or more RAW nodes.                                                                                  |
| CVSS          | Common Vulnerability Scoring System used by the NVD to measure a vulnerability's impact.                                  |
| DLC           | RSA Download Central.                                                                                                     |
| FQDN          | Fully Qualified Domain Name.                                                                                              |
| GRUB          | Grand Unified Bootloader.                                                                                                 |
| GUID          | Globally Unique Identifier.                                                                                               |
| JSON          | JavaScript Object Notation.                                                                                               |
| KPI           | Key Performance Indicator.                                                                                                |
| LVM           | Logical Volume Manager.                                                                                                   |
| MapR          | This is the framework used by RSA VRM for processing the large volume of data typically associated with VMS scan outputs. |
| NFS           | Network File System.                                                                                                      |
| NTP           | Network Time Protocol.                                                                                                    |

| <b>Term</b>    | <b>Definition</b>                                                                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NVD            | National Vulnerability Database. This database provides updated information on all known vulnerabilities.                                                                                   |
| OBF            | OSM Binary Format.                                                                                                                                                                          |
| ODBC           | Open Database Connectivity.                                                                                                                                                                 |
| OVF            | Open Virtualization Format.                                                                                                                                                                 |
| RAW            | RSA Analytics Warehouse. This may be referenced in other documentation as RSA VRM Data Warehouse (RVDW) or Security Analytics Warehouse (SAW).                                              |
| RPM            | Redhat Package Manager.                                                                                                                                                                     |
| RSA Archer EM  | RSA Archer Enterprise Management. This is also referred to as one of the core RSA Archer solutions. This is required for RSA VRM to leverage asset data relating to the asset scan results. |
| RSA Archer VRM | RSA Archer Vulnerability Risk Management. The RSA Archer solution component of RSA VRM. Also referred to as one of the core RSA Archer solutions.                                           |
| RSA VA         | RSA Vulnerability Analytics. RSA VA analyzes the aggregation of data in the RSA Analytics Warehouse to discover and prioritize vulnerability issues for device assets.                      |
| RSA VRM        | RSA Vulnerability Risk Management. The product as a whole.                                                                                                                                  |
| SSL            | Secure Sockets Layer.                                                                                                                                                                       |
| TLS            | Transport Layer Security.                                                                                                                                                                   |
| UUID           | Universally Unique Identifier.                                                                                                                                                              |
| VLAN           | Virtual Local Area Network.                                                                                                                                                                 |
| VM             | Virtual Machine.                                                                                                                                                                            |
| VMS            | Vulnerability Management System. This term is used in association with the scanners from Qualys, Nessus, Rapid7, and McAfee.                                                                |