RSA Archer GRC

RSA Vulnerability Risk Management1.2

Backup and Recovery Guide

5.x and later

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:
http://www.emc.com/support/rsa/index.htm.

Trademarks

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

License agreement

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

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

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

Third-party licenses

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

Note on encryption technologies

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

Distribution

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

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

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

March 2016

Contents

Preface

About This Guide

This guide is for RSA® Archer® GRC administrators who need to back up and recover RSA Vulnerability Risk Management. For more information, see the RSA Archer Online Documentation.

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. **Note:** This is included in the RSA Vulnerability Analytics Help.
Extensions Guide	Provides administrators with instructions on configuring various extensions with which RSA VRM can be setup.

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** 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-vrm-1.2.0-suite.zip file.

Support and Service

Customer Support Information	**http://www.emc.com/support/rsa/contact/phone-numbers.htm**
Customer Support Email	**archersupport@rsa.com**
RSA Archer Community	**https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
RSA Archer Exchange	**https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**
RSA SecurCare® Online	**https://knowledge.rsasecurity.com**
RSA Security Analytics Community	**https://community.emc.com/community/connect/rsaxchange/netwitness**

The Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer product roadmap.

The Exchange is an online marketplace dedicated to supporting GRC initiatives. The Exchange brings together on-demand applications along with service, content, and integration providers to fuel the success of RSA Archer clients.

RSA SecurCare Online offers a knowledge base that contains answers to common questions and solutions to known problems. SecurCare Online also offers information on new releases, important technical news, and software downloads.

Chapter 1: Backup and Recovery

Backup and Recovery Overview

RSA Vulnerability Risk Management has the capability to back up and recover its data. The following is a brief overview of the backup and recovery process:

- Create a backup of the HBase data on the RSA Analytics Warehouse (RAW) cluster.
- Create a backup of the RSA Vulnerability Analytics Host.
- Recover the HBase backup for a new or existing RAW cluster.
- Recover the RSA Vulnerability Analytics Host on a new or existing host.

Backup files for the RAW cluster only archive the HBase data. Solr data is not backed up. Data in HBase can be backed up automatically by scheduling backup scripts to run as cron jobs. The backup script only needs to be run on one RAW node, and it backs up all of the HBase data on the cluster. The backup script exports the HBase data into the MapR File System, and then it compresses the export into a gzip format (tar.gz).

The data recovered for the RAW cluster only includes the HBase data. If you are recovering data on an existing cluster, the data of that cluster is entirely replaced by the recovered data. The recovery process takes the compressed file generated by the backup process and restores the HBase data back into the RAW cluster. After recovering the HBase data, the indexing and metric jobs are triggered. The indexing job re-indexes the recovered data into Solr, and the metrics job runs historical metrics.

Backup and Recovery Requirements

To begin the backup and recovery process, you must meet the following requirements:

- On any one RSA Analytics Warehouse node, NFS Utilities must be installed.
- When recovering a RAW node, the backup files must be accessible from the new RAW node.

- On your RSA Vulnerability Analytics Host, complete one of the following:
  - Enable Windows Server Backup.
  - Install any Windows backup software according to your company's security policies.

    Important: The backup software should be able to use the Volume Shadow Copy Service or have the ability to backup open or locked files.

Chapter 2: RSA Vulnerability Risk Management Backup

Schedule the RSA Analytics Warehouse Backup

RSA recommends scheduling backup jobs when no other jobs are running.

Important: This procedure needs to be done on only one RSA Analytics Warehouse node. The data is backed up across the whole RAW cluster.

Procedure

1. Log on to any RAW node.
2. Ensure that the MapR system is NFS mounted on the RAW node. Enter the following command:

   ```
   mkdir /mapr && mount -o nolock,tcp 127.0.0.1:/mapr /mapr
   ```

3. Open the crontab file. Enter the following command:

   ```
   crontab -e
   ```

4. Create an entry to run the backup script. Enter the following command:

   ```
   cron entry /opt/rsa/vrm/disaster-recovery/vrm-dr-backup.sh
   -d destination
   ```

   where:

   - *cron entry* is the time you want the backup script to run in cron format. For example, a cron entry of 0 12 * * 0 runs the backup script at noon on every Sunday.
   - *destination* is the folder structure where you want to backup your files either locally or remotely.

   Important: The backups are unencrypted. If you want to back up to a remote directory, RSA recommends you secure the channel first.

   Note: This command sets the backup script to run on automatic intervals. To run the script manually, see **Manual Backup and Recovery Script Options**.

5. Save and exit the file.

Note: The RAW administrator should monitor the destination of the backup output files for storage space usage. Backup output files are not overwritten each time the backup is run. Backup output files continue to accumulate in the destination folder until it is out of space. If the /tmp folder has 0 free disk space, cluster services become unavailable on that particular node.

Back Up the RSA Vulnerability Analytics Host

Important: This procedure assumes you are using Windows Server Backup. If you are using another backup software, ensure that you back up the folders specified in step 4.

Procedure

1. On your Windows Host, open Windows Server Backup.
2. Click Action > Backup Schedule.
3. On the Select Backup Configuration window, select Custom, and click Next.
4. On the Select Items window, select the following folders, and click OK.
   - *Installation Directory*\RSA
   - *Root*/rsa

     where:
     - *Installation Directory* is the location you selected during the RSA Vulnerability Analytics installation.
     - *Root* is the root directory of the hard disk.

       Note: The default locations are C:\Program Files\RSA and C:\rsa respectively.
5. On the Select Items for Backup window, click Next.
6. Select a backup time frequency in accordance with your security policy, and click Next.

   Important: Subsequent backups override the previous backup. Only one backup is kept at any time.
7. On the Specify Destination Type window, select a destination for the backup, and click Next.

   Note: RSA recommends that you store the backup files on a secure remote location.
8. (Optional) If you selected Shared Network Folder for the destination, enter the location, and click Next.
9. Review the selected options, and click Finish.

Chapter 3: RSA Vulnerability Risk Management Recovery

Recover the RSA Analytics Warehouse

Procedure

1. Logon to the new RSA Analytics Warehouse node that you want to recover.
2. Mount the RAW node using NFS. Enter the following command:

   `mkdir /mapr && mount -o nolock,tcp Internal-IP:/mapr /mapr`

   where *Internal-IP* is the internal IP address of your RAW node.
3. Run the recovery script. Enter the following command:

   `/opt/rsa/vrm/disaster-recovery/vrm-dr-restore.sh -f /tmp/backup-Backup-Number.tar.gz`

   where *Backup-Number* is the date and number associated with the backup that was previously made.

   Note: The default setting wipes out all existing data on the cluster and recovers the data from the backup created in **Schedule the RSA Analytics Warehouse Backup**. It then indexes all HBase tables and runs the metrics jobs for the last six (6) days. To change the default settings, see **Note: Additional Recovery Script Capabilitie**

Recover the RSA Vulnerability Analytics Host

Important: This procedure assumes you are using Windows Server Backup. If you are using another backup software, ensure that you recover the files and folders specified in step 9.

Procedure

1. On your Windows Host, stop the following services:
   - RSA Vulnerability Management - User Interface
   - RSA Vulnerability Management - Data Collector
2. Open Windows Server Backup.
3. Click Action > Recover.

4. On the Getting Started window, select where your backup is stored, and click Next.
5. On the Specify Location Type window, select where your backup is stored, and click Next.
6. (Optional) If you selected Remote Shared Folder in step 5, enter the location, and click Next.
7. On the Select Backup Date window, select the date of the backup, and click Next.
8. On the Select Recovery Type window, select Files and Folders, and click Next.
9. On the Select Items to Recover window, select one of the following, and click Next.

File or Folder	Default Location
MapR cluster configuration	C:/Program Files/RSA/VRM/data-collector/mapr/conf/mapr-clusters.conf
Configuration folder except for the Lockbox folder and the jssecacerts file	C:/Program Files/RSA/VRM/config
Data Collector folder except any sub-folder	C:/Program Files/RSA/VRM/data-collector
Temporary feeds folder	C:/rsa/vrm/incoming/feeds/tmp

10. On the Specify Recovery Options window, select values for recovery options as follows, and click Next.

Recovery Option	Selection
Recovery destination	Another location > Enter the location that you chose in step 9.
When this wizard finds items in the backup that are already in the recovery destination	Overwrite the existing versions with the recovered versions.
Security settings	Restore access control list (ACL) permissions to the file or folder being recovered.

11. On the Confirmation window, click Recover.

12. If you are recovering on a fresh RSA VA Host:
    a. Repeat steps 2 - 11 for each of the four locations shown in step 9.
    b. Run the RSA VA Connection Manager.
    c. Remove all of the existing endpoints.
    d. Add all of your endpoints back.
13. Restart the following services:
    - RSA Vulnerability Management - User Interface
    - RSA Vulnerability Management - Data Collector

Appendix A: Manual Backup and Recovery Script Options

Additional Backup Script Capabilities

The Backup script can be modified with additional capabilities based on the following examples.

Example	Sample Command
Back up all of the HBase tables using the default parameters.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-backup.sh`
Back up all of the HBase tables to a specific directory using the default parameters.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-backup.sh -d /remote-directory`

Example	Sample Command
Back up individual HBase tables using the default parameters. The following tables are available to back up: • alert • asset • counter • device_index • issue • lookup_value • revision • ticket • timeline • vuln_index • vulnerability **Important:** The tables must be separated by commas and without spaces. **Note:** Only use this option when needed, and then with caution. For example, there might be a need to do a quick backup for the lookup_value table that has no relationships and needs to be restored in another system.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-backup.sh -e asset,vulnerability`
Displays help text for all of the available parameters.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-backup.sh -h`

Additional Recovery Script Capabilities

The Recovery script can be modified with additional capabilities based on the following examples.

Example	Sample Command
Recover all HBase tables using the default parameters.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-restore.sh -f /tmp/backup-`*`Backup-Number`*`.tar.gz` where *Backup-Number* is the date and number associated with the backup that was previously made.
Recover all HBase tables and recover the previous 120 days of historical metrics using the default parameters.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-restore.sh -f /tmp/backup-`*`Backup-Number`*`.tar.gz -n 120` where *Backup-Number* is the date and number associated with the backup that was previously made.

Example	Sample Command
Recover individual HBase tables and index data using the default parameters. The following table are available to recover if you previously backed up all of the tables: • alert • asset • counter • device_index • issue • lookup_value • revision • ticket • timeline • vuln_index • vulnerability **Important:** The tables must be separated by commas and without spaces. **Note:** Only use this option when needed, and then with caution. For example, there might be a need to do a quick recovery of the lookup_value table that has no relationships and needs to be restored in another system.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-restore.sh -f /tmp/backup-`*`Backup-Number`*`.tar.gz -e asset,issue` where *Backup-Number* is the date and number associated with the backup that was previously made.
Displays help text for all of the available parameters.	`/opt/rsa/vrm/disaster-recovery/vrm-dr-backup.sh -h`

Appendix B: Troubleshooting

Problem	Remediation

vrm-dr-backup.sh or vrm-dr-restore.sh fails on VRM 1.2 Warehouse cluster. Output backup file is empty or doesn't exist after running vrm-dr-backup.sh
 	
/opt/rsa/vrm/logs/vrm-dr.log has the following error repeated conitnuously:
 	
INFO [main] ipc.Client: Retrying connect to server: 0.0.0.0/0.0.0.0:8032. Already tried 0 time(s); retry policy is RetryUpToMaximumCountWithFixedSleep (maxRetries=10, sleepTime=1000 MILLISECONDS)
	Procedure
	
	1. Check the cluster mode:
	`maprcli cluster mapreduce get`
	2. If the cluster mode is not set to classic, run the following command:
	`maprcli cluster mapreduce set -mode classic`
	3. Retry the backup with vrm-dr-backup.sh.