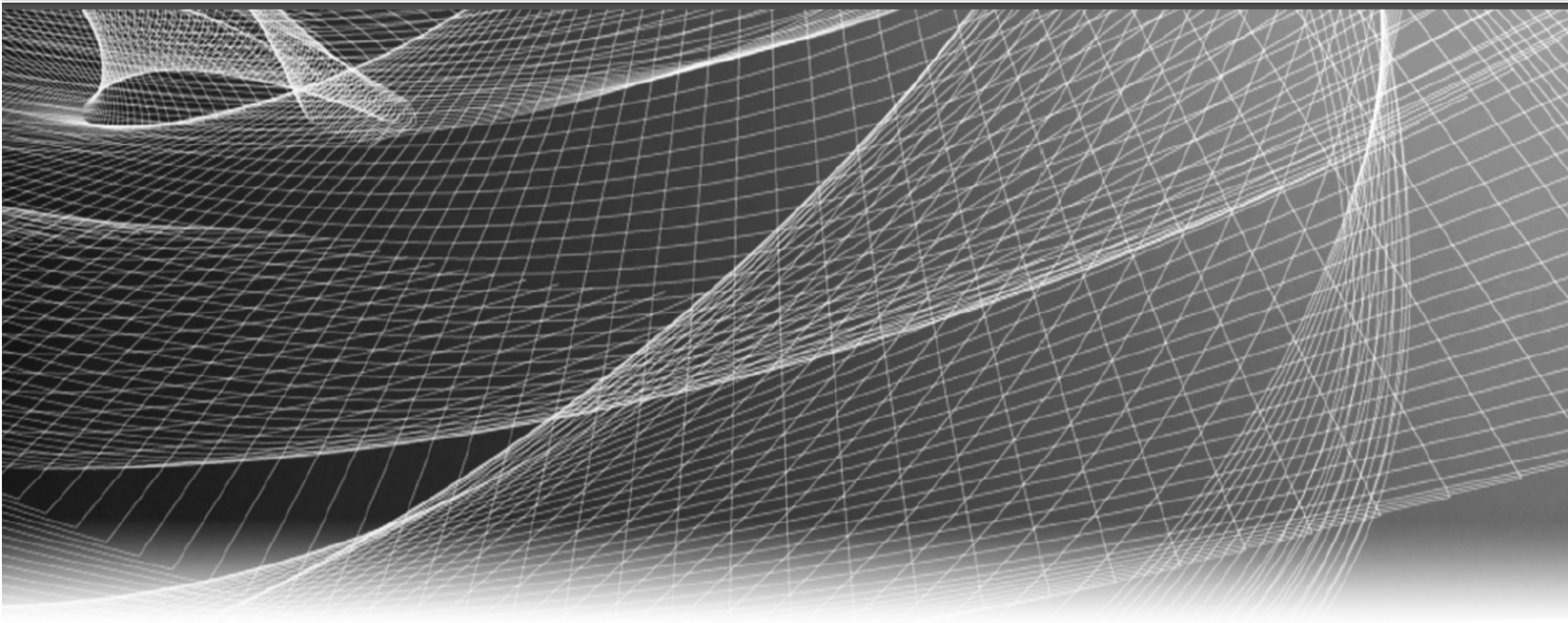


RSA Security Analytics

Configuration Data Backup and Restore Guide

for Version 10.6.6

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

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. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

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

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

December 2018

Contents

Backup and Restore Process Overview

These instructions apply to Security Analytics 10.6.6.0 or a later 10.6.x.x version exclusively. They tell you how to back up configuration data from, and restore configuration data to, the Security Analytics Server (SA Server) Host and all other component hosts in your deployment. You can use the backup and restore scripts for return merchandise authorizations (RMAs), hardware refreshes, and general backup and restore requirements. Download the "RSA Configuration Backup and Restore Scripts" zip file from RSA Link (https://community.rsa.com/docs/DOC-81514).

Note: For instructions that apply to 10.6.2.0 to 10.6.5.x, refer to the *RSA Security Analytics Configuration Data Backup and Restore Guide* available from RSA Link (https://community.rsa.com/docs/DOC-79456). For instructions that apply to 11.2.0.0 and later 11.x.x.x versions, refer to the *RSA NetWitness Recovery Tool User Guide* available from RSA Link (https://community.rsa.com/docs/96841).

Reasons to Backup and Restore Configuration Data

The following scenarios may require you to restore Security Analytics configuration data from backup.

- **Failure** - loss of services and systems on a physical or virtual host caused by either equipment of software issues. This may require a re-imaging of existing hardware or replacement hardware.
- **Hardware Refresh** - Migrate to new physical host equipment.
- **Return Merchandise Authorization (RMA)**. Customer returns RSA hardware that has problems for replacement hardware. RSA no longer replaces Series 4 or Series 4S physical hosts with Series 4 hardware. The new hardware will be Series 5 or Series 6 with a base image of Security Analytics 10.6.0.0 CentOS 6. You must update Security Analytics to 10.6.6 as described in the *RSA Security Analytics 10.6.6 Update Guide* (https://community.rsa.com/docs/DOC-95880) before you restore configuration data.

Terminology

Term	Definition in the Context of Backup and Restore
Component Host	All hosts other than the SA Server Host. A component host is often dedicated to a single service, but it may host multiple, related services.
Host	Physical or virtual machine that hosts Security Analytics services, databases, and so on.)
SA Server Host	The Security Analytics (SA) Server Host is the host on which the SA Server runs. This host can be Stand-Alone or it can house multiple services in addition to the SA Server.
Stand-Alone Host	Host dedicated to a single service.

Hosts You Can Back Up and Restore

You can back up and restore the following hosts.

- **SA Server Host**: May include Malware Analysis, Incident Management, Health and Wellness, IPDB Extractor, and Reporting Engine
- **Broker**: Stand-Alone Broker
- **Event Stream Analysis**: also hosts Context Hub and Incident Management database
- **Remote Log Collector**: also referred to as the Virtual Log Collector (VLC)
- **IPDB Extractor**: Stand-Alone
- **Archiver**: Log Archiver
- **Concentrator**: Packet or Log
- **Log Decoder**: also hosts the Local Log Collector and Warehouse Connector, if installed
- **Log Hybrid**
- **Packet Decoder**: also hosts the Warehouse Connector, if installed
- **Packet Hybrid**

- **Malware Analysis**: Stand-Alone
- **Warehouse Connector**: Stand-Alone

You can back up several hosts in a single execution of the backup script, but you must restore them one host at a time.

Note: The **nw-backup.sh** script will back up all files that are in the `/home`, `/root/`, or `/etc` directories. RSA recommends that you place any custom files that are important and need to be backed up in one of these directories.

Backup and Restore Scripts

The following scripts are included in the Download the "RSA Configuration Backup and Restore Scripts" zip file available on RSA Link (https://community.rsa.com/docs/DOC-81514).

- **get-all-systems.sh**: creates an **all-systems-master-copy** file, and the **all-systems** file, which contains a list of all your SA Server Host and other hosts to be backed up.

  Note: The **all-systems-master-copy** file and the **all-systems** file are not archived into the backup tar. RSA recommends that after you run the **get-all-systems.sh** script, you create copies of these files and store them in a secure location. During an upgrade (that is, when you specify the `-u` option with the `nw-backup.sh` script), the backup script creates the **appliance_info**, **service_info**, and **<hostname>-<host-UP-address>-network.info.txt** files, but the `nw-restore.sh` script does not refer to them. These files do not affect the backup and restore process.

- **ssh.propagate.sh**: automates key sharing between the hosts you are backing up and the backup host so that you are not prompted for passwords multiple times.
- **nw-backup.sh**: backs up the configuration data of your hosts.
- **nw-restore.sh**: restores data on your hosts.

For small deployments, you can use the SA Server Host as the backup host. You can also use an external backup host, but the backup host must be running CENTOS 6.

Caution: When you are ready to backup and restore data that has been backed up, you must work with the RSA Professional Services team or Customer Support. Do not use the restore script without assistance. For information about how to contact Customer Support, go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).

Caution: The backup script (**nw-backup.sh**) only backs up configuration files that were created by using the Security Analytics console or user interface. RSA recommends that you test the restore process before you delete the original versions of the files that you are backing up.

Note: The backup and restore scripts do not support backup and restore for STIG- or FIPS-hardened services.

Back Script Options

Options	Description
Configuration Options	
`-d`	Checks disk space in 'fast' mode,estimating disk space quickly using un-compressed data. If you specify `-u`, the script does this quick disk check automatically. Default: (no)
`-D`	Checks disk space in 'full' mode estimating disk space using compressed data which is about 10 times slower than `-d`. Default: (no)
`-l`	Stores backup content locally on each host. If you specify `-u`, the script stores backup content locally automatically. Default: (no)
`-e`	`<path-to-mount-point>`: Copies backup of all devices to the specified external mount point. Default: `/mnt/external_backup`
`-x`	Moves all backups to external mount point. Default: (no) - Copy
`-b`	`<path-to-write-backups>`: Stores backup in the specified path on backup server. Default: `/var/netwitness/database/nw-backup`
Content Selection Options	
`-c`	Back up Co-located Malware Analysis on SA servers. Default: (no)
`-i`	Back up IPDB Data `/var/netwitness/ipdbextractor`. Default: (no)
`-m`	Back up Malware Analysis File Repository. Default: (no)
`-r`	Back up Reporting Engine Report Repository. Default: (no)
`-v`	Back up System Logs `/var/log`. Default: (no)
`-y`	Back up YUM SA Server and RPM Repository. Default: (no)
`-S`	Does not back up SMS RRD files. Default: (backs up SMS RRD files)
`-C`	Does not back up Context-Hub Configuration and Database. Default: (backs up Context-Hub Configuration and Database)

Options	Description
`-E`	Does not back up ESA Mongo Database. Default: (backs up ESA Mongo Database)
`-u`	Runs backup for 10.6.6.x to 11.x upgrade. Default: (no)
Help	
`-h`	

Examples of How to Run Backup Script

The following table includes examples of how to specify the Backup script.

Example	Description
`./nw-backup.sh`	Runs the script without any options using the options in the Header of the script.
`./nw-backup.sh -dmrye /mnt/external_backup`	Runs a normal backup using the **BUPATH** defined in the script, with the following options: `-d` - Runs a disk check on backup storage (and external storage because `-e` is also specified). `-m` - Backs up the Malware File Repository. `-r` - Backs up the Report Repository. `-y` - Backs up the Yum Repository. `-e` - Copies the backup files to external mount point, mounted on `/mnt/external_backup`

Restore Script Options

Options	Description
Host Identification Option	
`<hostname>`	Identifies the host to which you are restoring data.
Backup Area Selection Option	
`<backup-folder-hostname>`	Identifies the area from which you are pulling the backup data to restore to the hosts.
Help	

Options	Description
`-h`	Displays help.

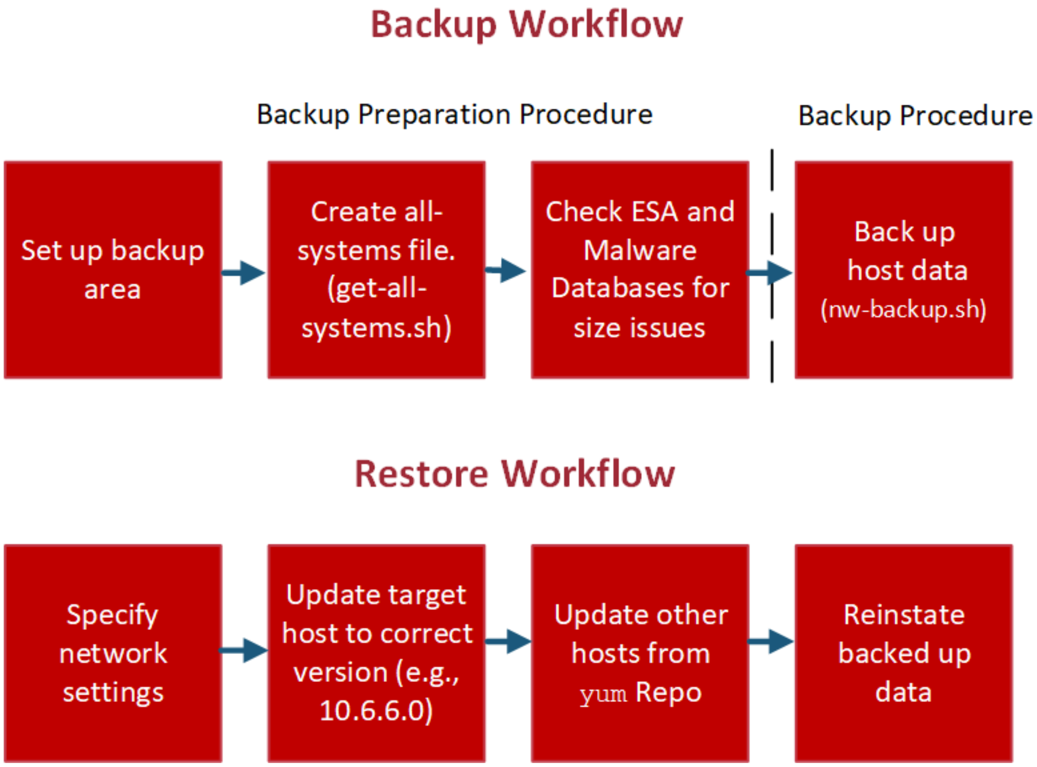
Examples of how to Run the Restore Script

The following table includes examples of how to specify the Backup script.

Example	Description
`./nw-restore <SA-Server-hostname> <backup-date-folder-name-yyyy-mm-dd>`	Restores the SA Server host from the backup area specified.

Backup and Restore Workflow

The following diagram shows the high-level Backup and Restore tasks.


Backup Workflow
Backup Preparation Procedure
Backup Procedure
Set up backup area
Create all-systems file. (get-all-systems.sh)
Check ESA and Malware Databases for size issues
Back up host data (nw-backup.sh)
Restore Workflow
Specify network settings
Update target host to correct version (e.g., 10.6.6.0)
Update other hosts from yum Repo
Reinstate backed up data

The following sections describe each of the backup tasks.

1. Backup Preparation Procedure

   Task 1 - Set Up a Backup Area

   Tasks 2 - Create all-systems File

   Task 3 - Check Sizing for ESA and Malware Disks and Adjust If Required

2. Back Up Procedure

3. Basic Restore Procedure

   Task 1 - Specify Network Settings on the Host

   Task 2 - Update the Host to the Correct Version (for example, 10.6.6.0)

   Restore Procedure

   Task 4 - Reinstate Backed Up Configuration Data to the Host

Backup Preparation Procedure

Before you back up Security Analytics 10.6.6. configuration data you need to complete the following three tasks.

Task 1 - Set up a backup area.

Task 2 - Create an all-systems file.

Task 3 - Check sizing for ESA and Malware disks and adjust if required.

Task 1 - Set Up a Backup Area

Before you run the **nw-backup.sh** script, make sure that you have:

- A computer that is running CentOS 6 distribution, with a large amount of free hard drive space. For small installations, you can use the SA Server Host.

> **Note:** There are two options provided in the **nw-backup.sh** script that check disk space that is required for the files that are being backed up.
> **-d** checks disk space in 'fast' mode that estimates disk space quickly using uncompressed data.
> **-D** checks disk space in 'full' mode that estimates disk space using compressed data. **-D** is about ten times slower than **-d**, but it is more accurate.

- A path in which to store the backup files. You can use the **df -h** command to ensure that the path you have selected is on a partition with adequate free space.

- Host names for the hosts that you are backing up and restoring that are resolvable on the backup host machine, either by DNS or listed in the **/etc/hosts** file.

> **Note:** The **ssh.propagate.sh** script adds host names that are in the **all-systems** file to the **/etc/hosts** directory.

Tasks 2 - Create all-systems File

RSA recommends that the first time you use the backup script, you start with a small subset of the hosts to back up so that you can get an estimate of the time it will take for a full backup of all your hosts.

- The subset can be a logical grouping of the hosts in your environment or a grouping by geographical location of the host. It is up to the administrator.
- You can create a backup run of a subset of files by editing the **all-systems** file to retain only the entries for the subset to be run at this time. For subsequent runs, you can add the remaining entries from the **all-systems-master-copy** file.

Caution: BEFORE you restore any host (especially the SA Server host), you must run the **get-all-systems.sh** script against ALL hosts in your deployment to generate a complete **all-systems-master-copy** file. If you do not do this, you may lose information from the **all-systems** file which would require you to manually create entries in **all-systems** files for subsequent backup runs.

- If you manually add entries to the **all-systems** file AFTER you run the **get-all-systems.sh** script, make sure these entries are ALSO manually entered into the **all-systems-master-copy** file, and back up the **all-systems-master-copy** file in a safe location for reference.

Note: If any hosts are down while you are running the `get-all-systems.sh` script, the script creates a list of hosts for which it cannot find information. After the script completes and the **all-systems** file is created, you must edit the **all-systems** file manually and add the missing information for these hosts.

To create the **all-systems** file with the `get-all-systems.sh` script:

1. Open the `get-all-systems.sh` script for editing and enter the backup directory where you want your backups to be stored on the backup host, between the quotes on line 4, `BUPATH=" "`. The default location for storing the backup files is `/var/netwitness/database/nw-backup`.
2. From your SA Server Host, run the `get-all-systems.sh` script to generate the **all-systems** file:
   `./get-all-systems.sh <IP Address of Security Analytics server>`
   This script saves the **all-systems** file and the **all-systems-master-copy file** to the directory that is specified by `BUPATH`. The default location is `/var/netwitness/database/nw-backup/`.

   Note: The `get-all-systems.sh` script generates a list of hosts that were defined in the Security Analytics user interface. Make sure that all hosts are provisioned properly. If any host is not provisioned properly, it will not be backed up. RSA recommends that when you add a host to Security Analytics, you use the Security Analytics user interface to make sure that it is provisioned properly. If you have any hosts that were not defined in the user interface, you must add them to the `all-systems` file manually.

Warning: When you complete the steps to run the `get-all-systems.sh` script, the script automatically performs a key exchange between the backup host and the SA Server Host (if it is not already configured), and you are prompted for the `root` password of the SA Server Host.

Note: At the end of the `get-all-systems.sh` script, the script checks for differences between the hosts that the SA Server Host has listed, and the hosts for which the script was able to find all the required information. If a Node ID or host name is listed as missing, make sure that this host exists, that its service or services are all running, and that it is properly communicating with the SA Server Host. (Any Windows Legacy Collectors or AWS Cloud Collectors are not added to the **all-systems** file, and may account for discrepancies. **DO NOT add these items to the all-systems file manually**.)

3. RSA recommends that you run the **ssh-propagate.sh** script to automate sharing keys between the backup host and the host systems. If you do not to run the **ssh-propagate.sh** script, the backup script prompts you to manually enter passwords several times, which slows down the backup process. If you run the **ssh-propagate.sh** script, the backup only prompts you to enter the password once per host.

```
ssh-propagate.sh /<path-to-all-systems-file>/all-systems
```

Note: If you have SSH keys that are protected with pass phrases, you can use the ssh-agent to save time.

Task 3 - Check Sizing for ESA and Malware Disks and Adjust If Required

The following table shows you the maximum size of Malware databases that you can back up, by hardware type, with the actions you can take to reduce them to the maximum size.

Host	Source Hardware	Target Hardware	Database	Maximum Size for Backup	Actions to Reduce Size to Backup Maximum
Malware	Series 4S Hybrid	Series 5 Hybrid	`/var/lib/rsamalware`	1.2TB	Configure a rollover. Purge data that you do not need from the database.
Malware	Series 4S Hybrid	Series 5 Hybrid	`/var/lib/pgsql`	390GB	Configure a rollover. Purge data that you do not need from the database.
ESA	Series 4S Hybrid	Series 5 Hybrid	`/opt/rsa`	<3TB	Configure a rollover. Purge data that you do not need from the database.

Back Up Procedure

Complete the follow steps to back up the configuration data for each host.

> **Note:** RSA recommends that you read the Special Task Required to Back Up ESA Hosts below. You may want to back up all hosts except ESA hosts first to make sure that the Mongo database is handled correctly.

1. SSH to the host.

   > **Note:** 1.) All command-line options are optional. With no options defined, the script will use the options set in the file. 2.) Do not use the `-u` option because it is specifically used for upgrading data to from version 10.6.6.x to 11.x.x.x. 3.) You must use the same backup path in this procedure that you defined when you ran the **get-all-systems.sh** script to Tasks 2 - Create all-systems File.

2. Make the backup script executable by running the following command.

   ```
   chmod u+x nw-backup.sh
   ```

   You can specify the options after the script in the command line or edit the script.

   > **Note:** You must specify `-m` option with the backup script to persist the Malware repository.

   - Example of the backup script with basic options specified after the script in the command line.

     ```
     ./nw-backup.sh [-d|-D] -l -x -e -m <external-mnt> -b <backup file path>
     ```

   - Example of how to edit the backup script.

     Open the **nw-backup.sh** for editing, place the backup path between the quotes on line 4, and select any of the "***optional***" backups (by replacing **"no"** with **"yes"**), as shown in the following example.

     ```
     #!/bin/bash
     # nw-backup.sh v2.0
     # Enter the backup path between the quotes and change any options below
     BUPATH="/var/netwitness/database/nw-backup"
     ###################
     # Content Options #
     ###################
     # Include /var/netwitness/ipdbextractor directory?
     IPDB="no"
     # Include rsaMalwareDeviceCoLo files from NW Server?
     MACOLO="no"
     # Include system logging directory /var/log?
     VARLOG="no"
     # Include /home/rsasoc/rsa/soc/reporting-engine/resultstore directory
     ```

```
(contains previously run reports/rules/charts)?
RERPTS="no"
# Include /var/netwitness/www directory (contains yum repo files)?
YUMREPO="no"
# Include /var/lib/rsamalware/spectrum/repository directory (contains
malware file repository)?
MALREPO="no" # Include /opt/rsa/context directory for Context Hub
configuration?
CTXTHUB="yes" # Include ESA Mongo Databases?
ESADB="yes" # Include /var/lib/collectd/rrd directory?
SMSRRD="yes"
##################
# Output Options #
##################
# Option to copy (scp) backup files to each node locally
LOCAL="no"
# 'yes' = backup archives will be copied to $BUPATH on each node after
backup completes.
# 'no' = backup archives will be written to $BUPATH on the system where
nw-backup script is running
#
# Option to move completed backups to a mounted filesystem (USB/NFS/SMB)
on the system where nw-backup script is running
EXTERNAL="no"
# Set the external storage mount directory (only used if EXTERNAL=yes),
make sure path exists and media is mounted
EXTERNAL_BUPATH="/mnt/external_backup"
# Option to MOVE or COPY the backups to the external storage (only used
if EXTERNAL="yes"), valid values are "move" and "copy"
EX_MODE="copy"
# Run a sanity check for DISK SPACE to verify enough space available for
storing the backups.
DISK_SPACE_CHECK="no"
#Disk Space Check operation Mode. “fast” does a rough estimate using
uncompressed file sizes, “full” takes longer and checks what the
compressed data would be.
DSC_MODE=“fast”
#
####################
# Upgrade Option #
####################
```

```
#Upgrade flag for 10.6.x to 11.0
UPGRADE="no"
#
#
# --------------------DO NOT EDIT BELOW THIS LINE-------------------
```

3. Run the backup script at the root directory level.
   `./nw-backup.sh`
   or
   `./nw-backup.sh <options>`
   The backup script creates a log file (for example, `rsa-nw-backup-2017-03-15.log`) in the backup directory. This log lists information on the files you are backing up.

4. Run the following command after the backup completes to make sure that the intended files are backed up. The following command lists all the files that were backed up.

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   The backup script creates the following two archive files, one file contains a backup of the `root` user home directory and the other file contains all the backup data for the Security Analytics services running on that host.

   ***hostname-IPaddress*-root.tar.gz**

   ***hostname-IPaddress*-backup.tar.gz**

   The files are located in the **/BUPATH/yyyy-mm-dd/** directory. If any of the tar files appear smaller than expected, open them to be sure that the files were properly backed up.

   > **Note:** The location of the backup files may change depending on the output options that you selected when you ran the backup script.

Special Task Required to Back Up ESA Hosts

If you have ESA (Event Stream Analysis) hosts in your deployment, the `nw-backup.sh` script prompts you for a password. You need the Mongo database Admin password to complete the backup process.

> **Note:** These steps are only required for the live backup of the ESA host databases (no services are shut down during the backup). The `nw-restore.sh` script does not require the password because it shuts the services down before it restores the database.

There are two options available for handling this requirement:

- Run the backup interactively. You are prompted for the password at the start of the backup session.
- Run the backup in batch mode (for example, from a Cron job), or interactively without being prompted:

  1. Create a file named `tokumx.info` in the same directory (that is the backup path directory) as the `all-systems` file using the following command.

     ```
     echo "<esa-hostname>:$(echo '<admin_password>' | base64)" > /<path-to-backup-directory>/tokumx.info
     ```

     If you have multiple ESA hosts, run the following command to add additional hosts to the backup file:

     ```
     echo "<esa-hostname>:$(echo '<admin-password>' | base64)" >>/<backup-directory-path>/tokumx.info
     ```

     > **Note:** If you do not know the password, contact Customer Support (https://community.rsa.com/docs/DOC-1294) for instructions on how to change or create a new password.

  2. Change the permissions to read-only for `root` to secure the file.

     ```
     chmod 400 tokumx.info
     ```

Restore Procedure

This procedure is exclusively for restoring hosts running Security Analytics 10.6.6.x.

If you are storing to new hardware, the base image you receive on this hardware is 10.6.5.2. You must update 10.6.5.2 to your 10.6.6.0 or later version.

If you are restoring to a virtual host, Contact Customer Support to get the appropriate OVA files for your restore scenario. For information about how to contact Customer Support, go to the "Contact Customer Support" page in RSA Link (https://community.rsa.com/docs/DOC-1294).

You must restore data on each SA Server Host or component host individually. The target restore host must have the same IP address and host name as the host that was backed up. However, if you are restoring to an RMA host, you can restore to a host with a different IP address if you keep the original host that was backed up running while you restore the data.

> **Warning:** 1). When you are using these scripts for a tech refresh (hardware upgrade) or an RMA replacement, **DO NOT** perform a `Remove` or `Remove and Repurpose` procedure from the Security Analytics User Interface Hosts view. All the information that is needed by the host to communicate with the back-end services will be restored, and the new host will come back online with the identity of the old host intact.

Complete the following tasks on each host in your deployment to restore your deployment. RSA recommends that you start with the SA Server Host.

Task 1 - Specify network settings.

Task 2 - Update the host to the correct version (for example,10.6.6.0).

Task 3 - Reinstate backed up configuration to the host.

The examples in this procedure show your responses to script prompts in boldface type (for example, **`response`** type. If the response is a variable, it is also enclosed in brackets (for example, **`<response>`**).

Task 1 - Specify Network Settings on the Host

> **Note:** You can update the SA Server Host by using the Security Analytics user interface. However, for component hosts, you must follow the procedure documented here for using `yum update`.

Prerequisite: Make sure that version to which you want to restore (for example, 10.6.6) RPMs are uploaded to the SA Server Host. See the *RSA Security Analytics 10.6.6.x or Later Version Update Instructions Guide* (https://community.rsa.com/docs/DOC-95880) for more information.

> **Warning:** Do not enter an IP Address in response to the `Enter the IP address for the <host>` prompt in step 4. Press **Ctrl-C** in response to this prompt.

1. Start the target host and log in as `root` .

```
RSA Security Analytics Host
Kernel 2.6.32-573.12.1.el6.x86_64 on an x86_64
NWHOST9876 login: root
Password: nnnnnnnnn
-----------------------------------------------------------------
This script configures the management, network interface settings
<CTRL><C> to Cancel Without Saving

Please enter the requested network settings, or enter for none
You will be prompted to confirm selections or quit without saving
-----------------------------------------------------------------
```

2. Respond to a series of network configuration prompts as illustrated in the following example.

```
please enter system IP address or d for DHCP? <IP-address>
please enter system netmask? <system-netmask>
please enter default gateway? <default-gateway>
please enter primary DNS server IP address? <primary-DNS-server-IP-address>
please enter secondary DNS server IP, press enter for none? <secondary-DNS-
server-IP> or none
please enter local domain name, press enter for none? <local-domain-name>
or none
please enter unqualified host name, press enter for none? <unqualified-
host-name> or none
```

The settings you specified are displayed so you can confirm them.

```
you entered the following network parameters
IP Address: <nnn.nnn.nnn.nnn>
Netmask: <nnn.nnn.nnn.nnn>
Default Gateway: <nnn.nnn.nnn.nnn>
Primary DNS: ><nnn.nnn.nnn.nnn
Secondary DNS: nnn.nnn.nnn.nnn
Local Domain: <mydomain.com>
Host Name: <my-decoder-01>
------------------------------------------------------------
```

3. Enter `y` in response to the next prompt to confirm and save your responses. For example:

```
enter y to confirm and save
enter q to quit without saving
enter d for don't save or ask me this
enter 1 to re-enter NIC selection
enter 2 to re-enter IP address
enter 3 to re-enter netmask
enter 4 to re-enter default gateway
enter 5 to re-enter primary DNS
enter 6 to re-enter secondary DNS
enter 7 to re-enter local domain
enter 8 to re-enter host name
enter a to re-enter all network data
-------------------------------------
? y
restarting network service
Shutting down interface em1: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface em1:
Determining if ip address nnn.nnn.nnn.nnn is already in use for device
em1...
[ OK ]
------------------------------------------------------------
You can run this script again to change the network settings
Location: /usr/sbin Usage: netconfig.sh
------------------------------------------------------------
```

Note: For a hardware refresh or RMA or a newly-imaged device, you must enter the network configuration information when you first log in. However, DO NOT enter the SA Server Host IP address when you are prompted. Instead, enter **Ctrl-C** and continue with the update. From this point forward, anytime you log in (at least until the restore is completed), whenever you are prompted for the IP address of the SA Server Host, enter **Ctrl-C** instead.

4. At the `Enter the IP address for SA Server:` prompt, press **[Ctrl]-C** to exit out of the script. For example.

   ```
   Enter the IP address for SA Server: Ctrl-C
   Traceback (most recent call last):
   File "/usr/sbin/saApplPuppetInit.py", line 226, <in module>
   main()
   File "/usr/sbin/saApplPuppetInit.py", line 201, in main
   configPuppetAgent(theUuid)
   File "/usr/sbin/saApplPuppetInit.py", line 84, in configPuppetAgent
   theAddr = raw_input('Enter the IP address for SA Server: ')
   KeyboardInterrupt
   [root@NWHOST9876 ~]#
   ```

> **Note:** After each reboot, the `Enter the IP address for SA Server` prompt displays. Whenever this prompt displays, enter **`Ctrl-C`** to exit until after you run the restore script (step 3 under Reinstate Backed Up Configuration Data on Each Host in Your Deployment). At the end of the restore script, after the final reboot, the host has all the information it needs to connect to the SA Server Host, and the prompt no longer displays

Task 2 - Update the Host to the Correct Version (for example, 10.6.6.0)

1. SSH to the target host.
2. Run the following commands to access the **RSASoftware.repo** for editing.

```
vi /etc/yum.repos.d/RSASoftware.repo
```

> **Note:** You can only retrieve RPMs from the RSA Software repository for a <major-release.minor-release.service-pack> (for example 10.6.6). If you need to restore to a patch, (for example, 10.6.6.**1**) you must restore all your hosts to version 10.6.6.0. After all your hosts are at 10.6.6.0, you apply the 10.6.6.1 patch to each host from the Security Analytics 10.6.6.0 Hosts view in the User Interface).

3. Edit the `RSASoftware.repo` file to match the following text. Specify the IP address of the SA Server Host for the `baseurl` so that the target host can access the RPMs for version to which you want to restore (for example, 10.6.6.0). For example:

```
[RSASoftware]
name= $sarelease - Base
baseurl=http://<ip-address-of-SA-server/rsa/updates/$sarelease/>
enabled=1
gpgcheck=1
sslverify=1
```

4. Run the following commands to access the correct RPMs (for example, 10.6.6.0).

```
echo "10.6.6" > /etc/yum/vars/sarelease
```

5. Run the following commands to verify the repository.

```
yum clean all && yum check-update
```

6. Run the following commands to update the repository.

```
yum update
```

7. At the confirm prompt, enter `y`.
8. After the update completes, run the following command.

```
sed -i -e 's/default../default=0/g' /boot/grub/grub.conf
```

9. Type `reboot` to reboot the host.

10. Run the following commands to verify that the target host was updated to 10.6.6.x or later Version (for example, 10.6.6).

    ```
    yum clean all && yum check-update
    ```

    The results should indicate that there are no more updates available.

    The following example demonstrates this:

    ```
    [root@rsaarchiver-0 ~]# yum clean all
    Loaded plugins: fastestmirror
    Cleaning repos: RSASoftware
    Cleaning up Everything
    Cleaning up list of fastest mirrors
    [root@rsaarchiver-0 ~]# yum check-update
    Loaded plugins: fastestmirror
    Determining fastest mirrors
    RSASoftware | 2.9 kB 00:00
    RSASoftware/primary_db | 1.4 MB 00:00
    [root@rsaarchiver-0 ~]#
    ```

Task 4 - Reinstate Backed Up Configuration Data to the Host

> **Note:** If you have not configured SSH key authorization from the source restore host to the target host prior to running the `nw-restore.sh` script, the script will configure the authorization and prompt you for the `root` password of the target host.

1. Log in to the host that will execute the restore scripts and has access to the backup area.

2. Change the directory to the location of the backup scripts.

   ```
   cd /backup-script-directory
   ```

3. Run the following command to reinstate the backed up configuration data.

   ```
   ./nw-restore.sh hostnamedate
   ```

   Make sure that there is a space between the host name and the date. The host name must match the one that was used for the `all-systems` file, and it must resolve to the IP address that is in the `all-systems` file. The date must be in ***`yyyy-mm-dd`*** format, and it must match the date that the host was backed up. You can find this in the backup directory.

   The following command line example shows you how to format the hostname.

   ```
   ./nw-restore-root.sh My-Broker-hostname 2017-03-15
   ```

Note: Copies of the following original files from the backup are stored in the `/etc/backup` directory on the restored host. The following files are listed so you can refer to them if they were customized after the default install.

```
/etc/passwd
/etc/hosts
/etc/resolv.conf
/etc/shadow
/etc/sysconfig/network
/etc/group
/etc/sysconfig/network-scripts/ifcfg-e*
```

Warning: DO NOT directly copy **ANY** of the following files over the existing OS files. Doing so may make the host unusable. Instead, perform the following steps for each file:

- Copy any External Mount Points (DACs) from `/etc/backup/fstab` to the end of `/etc/fstab`.
- Copy any custom host entries from `/etc/backup/hosts` to `/etc/hosts`.
- Copy any custom users from `/etc/backup/passwd` to `/etc/passwd`.
- Copy any custom users and passwords from `/etc/backup/shadow` to `/etc/shadow`.
- Copy any custom groups from `/etc/backup/group` to `/etc/group`.
- Copy any extra search domains from `/etc/backup/resolv.conf` to `/etc/resolv.conf`.

4. Reboot the restored host.
5. Log into the Security Analytics User Interface to make sure that the files are restored by verifying your configuration data.
6. Repeat steps 1 through 5 inclusive for each host that you need to restore.

Logs for the restore process are located in the backup directory, and are named:
`rsa-nw-restore-`*`hostname`*`-`*`date`*`.log`

Hardware Refresh Only - Maximize Additional Space in New Hardware Hosts

Refer to the *RSA Security Analytics Core Tuning Guide* (https://community.rsa.com/docs/DOC-83084) for instructions on how to use all the space you have available on your new hardware.

Troubleshooting

This topic describes issues that you may encounter while using scripts to back up and restore configuration data, and suggests solutions to these problems.

Problem	**Recently-created host artifacts are not being restored**
Possible cause	Recently-created host artifacts (for example, Global Auditing configurations) might not be restored because they are not backed up completely. Automated backups of the database are generated every 12 hours, so if you make a change and then immediately perform a backup, the changes may not be contained in the automated backup depending on where the host is in its database backup schedule.
Solution	To make sure that recent changes are backed up, restart jettysrv to force a backup of the database with the current settings. Run the command `restart jettysrv`.

Problem	**Not all hosts attached to the SA Server Host appear in `all-systems file` output from run of `get-all-systems.sh`**
Possible cause	The `all-systems` file only contains hosts that are under the control of the SA Server Host Puppet master. Hosts that were added manually or hosts that have not been properly enabled in Security Analytics are not included in the file.
Solution	Check the `all-systems` file for host information and manually add the information for the missing host, for example: `decoder,hostname,10.0.0.18,uuid,host-nw-version`.

Problem	**Backup errors caused by the `immutable` attribute setting**
Possible cause	If you have any files that have the `immutable` flag set (to keep the Puppet process from overwriting a customized file), the file will not be included in the backup process and an error will be generated.

Solution	If `immutable` files are active:
	1. On the host with the immutable files:
	a. Run the following command to stop the Puppet agent service.
	`service puppet stop`
	b. Run the following command to remove the `immutable` setting from the files.
	`chattr -i filename`
	c. Repeat step **1a** and **1b** for all of the files that are set to `immutable`.
	2. On the host running the backups, run the following command.
	`./nw-backup.sh`
	3. On the hosts that contain the immutable files:
	a. Run the following command to reset the `immutable` flag on the files.
	`chatter +i` *`filename`*
	b. Run the following command to restart the Puppet agent.
	`service puppet start`

Problem	**The backup script (`nw-backup.sh`) does not back up files from symbolic links**
Possible Cause	If any custom symbolic links have been defined on a host (for example, linking `/var/lib/rabbitmq` to another location on an older host build with more file space), the `nw-backup.sh` script will not back up the files over the symbolic link.
Solution	Manually back up files that are the target of a custom symbolic link.

Problem	**Unable to restore files from `/var/netwitness` databases**
Possible Cause	The backup and restore scripts do not back up the `/var/netwitness` database files.
Solution	The backup and restore scripts only back up and restore configuration files that were created using the Security Analytics console or user interface. You must manually back up and restore `/var/netwitness` database files.