Shutting Down and Restarting RSA Security Analytics Appliances

To avoid possible corruption in database and index files it is important to stop all Security Analytics services and shut down the appliances gracefully during planned maintenance windows.

Overview

Please follow these instructions to shut down, power off and restart RSA Security Analytics appliances. These instructions are written for appliances running CentOS 6.x with Security Analytics 10.3 and 10.4. Some Security Analytics appliances using CentOS 5.x will use different commands to stop and start services. The different commands are explained in Knowledgebase article 26468[1] titled "Managing NetWitness NextGen Services" and Knowledgebase article 26736[2] titled "Managing Services on a Security Analytics 10.3 SP2 Server."

If your specific appliance is not listed in this document, please contact RSA Security Analytics Support using one of the options listed below.

This Knowledgebase article adds additional details to Knowledgebase article 26814 titled "Best Practices in Rebooting a Security Analytics Appliance."[3] You may wish to refer to this solution as well prior to shutting down your appliance.

Physical access to RSA Security Analytics appliances and DACs is required to shut down many appliances. DACs and JBODs may not have power switches on the chassis. It is necessary to remove the power cables from these devices. All Series 4 and Series 4S appliances have iDRAC cards installed and you can use the iDRAC to shut down RSA Security Analytics appliances if the iDRAC is configured and accessible from your network.

When shutting down RSA Security Analytics appliances, start with appliances at the top of the hierarchy. First, shut down Malware. Next, shutdown Brokers, then Concentrators, then Decoders and finally shut down SA Server appliances.

Resources Required

In order to complete the steps listed in this document you will need the following tools:

- A communications tool such as putty, or HyperTerm, or other ssh tool.
- Access to SCOL Knowledgebase articles.
- A browser to access the Security Analytics Server 10.4 and iDRAC. Compatible browsers include Google Chrome, Apple Safari, Mozilla Firefox, and Internet Explorer 10 and above.

Optional Resources

You may find these tools helpful to complete the steps listed in this document:

- NWAdministrator thick client administration software.

[1] Formerly Primus article a60048.
[2] Formerly Primus article a64711.
[3] Formerly Primus article a58916.

Current RSA Security Analytics Appliances Covered

Not all RSA Security Analytics appliances support attached JBODs or DACs. The most common deployments are listed below and the procedures for shutting down and restarting these appliances are explained in this document.

- RSA Security Analytics Decoder
- RSA Security Analytics Decoder with DAC Attached
- RSA Security Analytics Concentrator
- RSA Security Analytics Concentrator with DAC Attached
- RSA Security Analytics Broker
- RSA Security Analytics Malware Broker
- RSA Security Analytics Hybrid
- RSA Security Analytics Hybrid with DAC Attached
- RSA Security Analytics All-In One
- RSA Security Analytics All-In One with DAC Attached
- RSA Security Analytics Log Decoder with DAC Attached
- RSA Security Analytics Server

Preparation before Shutting Down Appliances

Before shutting down an RSA Security Analytics appliance, please review Knowledgebase article 26721[4], "Temporarily Disabling Console Output to the Serial Port" and Knowledgebase article 26666[5], "Permanently Disabling Console Output to the Serial Port" to determine whether your appliance will redirect boot messages to the serial port when restarting. This should not apply to Series 4 and Series 4s appliances.

Contacting RSA Security Analytics Support

For assistance, open a case at SecurCareOnline at https://knowledge.rsasecurity.com or contact Security Analytics Technical Support at nwsupport@rsa.com.

Documentation Conventions

Commands that are to be entered at a command or shell prompt are entered in the Courier New font. For example, when asked to run one or more commands at a prompt, the commands will be listed like:

```
mount
cd /root
```

Documentation Updates

RSA Security Analytics strives to produce accurate, useful, and comprehensible technical documentation. If you have a question, suggestion or comment about a document, please contact us. Please refer to the document title, Primus article number, document revision and date when commenting. We appreciate your feedback.

[4] Formerly Primus article a58610.
[5] Formerly Primus article a58915.

Shutting Down and Restarting an RSA Security Analytics Decoder without an attached DAC (Series3 Decoders only)

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance. If your appliance has external capacity attached refer to the appropriate section of this document.

Shutting Down the Decoder Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Decoder service.
3. Open the System tab for the Decoder service.
4. Stop capture on the Decoder.
5. Open an ssh session and logon to the appliance as root.
6. Stop all Security Analtyics services with the following commands:
```
stop nwdecoder
stop nwappliance
```
7. Verify all Security Analtyics services with the following commands:
```
status nwdecoder
status nwappliance
```
8. Confirm and note the mounted filesystems with the following command:
```
mount
```
9. Gracefully shutdown the OS and power off the appliance with the following command:
```
shutdown -h now
```
10. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the Decoder Appliance

1. Turn on the power to the appliance and allow it to boot.
2. Open an ssh session and logon to the appliance as root.
3. Verify all filesystems have mounted with the following command:
```
mount
```
4. Verify all Security Analytics services with the following commands:
```
status nwdecoder
status nwappliance
```
5. Logon to the Security Analytics Server as Admin
6. Navigate to Administration | Devices and select the Decoder service.
7. Verify that the Decoder is capturing and upstream devices are consuming.

Shutting Down and Restarting an RSA Security Analytics Decoder with DAC Attached

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Decoder Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Decoder service.
3. Open the System tab for the Decoder service.
4. Stop capture on the Decoder.
5. Open an ssh session and logon to the appliance as root.
6. Stop all Security Analtyics services with the following commands:
   ```
   stop nwdecoder
   stop nwappliance
   ```
7. Verify all Security Analtyics services with the following commands:
   ```
   status nwdecoder
   status nwappliance
   ```
8. Confirm and note the mounted filesystems with the following command:
   ```
   mount
   ```
9. Backup of the /etc/fstab file with the following command:
   ```
   cp /etc/fstab /etc/fstab.backup
   ```
10. Edit /etc/fstab and comment out any lines that mount filesystems under the directory /var/netwitness or /var/lib/netwitness. There may be several of these lines in the /etc/fstab file.
11. Save the /etc/fstab file.
12. Gracefully shutdown the OS and power off the appliance with the following command:
    ```
    shutdown -h now
    ```
13. Wait at least 5 minutes and confirm that all disk activity on the DAC has ended. Monitor the LED lights on the DAC to confirm disk I/O activity has ceased.
14. If the appliance did not power off after the shutdown command, press the power switch to shut it down.
15. Press the power switch on each attached DAC to power it down or, if the DAC does not have a power switch, disconnect the electrical power cords.

Starting the Decoder Appliance

1. Turn on the power to each DAC and allow it to power up.
2. Turn on the power to the appliance and allow it to boot.
3. Logon to the Security Analytics Server as Admin
4. Navigate to Administration | Devices and select the Decoder service.
5. Open the System tab for the Decoder service.
6. Stop capture on the Decoder.
7. Open an ssh session and logon to the appliance as root.
8. Stop all NetWitness services with the following commands:

```
stop nwdecoder
stop nwappliance
```

9. Restore the original /etc/fstab file with the following commands:

```
cp /etc/fstab /etc/fstab.nomount
```

This keeps the old file just in case you need to review or use it again.

```
cp /etc/fstab.backup /etc/fstab
```

This restores the original /etc/fstab file.

10. Mount all file systems with the following command:

```
mount –a
```

11. Verify all filesystems have mounted with the following command:

```
mount
```

12. Start all NetWitness services with the following commands:

```
start nwdecoder
start nwappliance
```

13. Verify all Security Analytics services with the following commands:

```
status nwdecoder
status nwappliance
```

14. Logon to the Security Analytics Server as Admin
15. Navigate to Administration | Devices and select the Decoder service.
16. Verify that the Decoder is capturing and upstream devices are consuming.

Shutting Down and Restarting an RSA Security Analytics Concentrator without an attached DAC (Series 3 Concentrators only)

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance. If your appliance has external capacity attached refer to the appropriate section of this document.

Shutting Down the Concentrator Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Concentrator service.
3. Open the System tab for the Concentrator service.
4. Stop aggregation on the Concentrator.
5. Open an ssh session and logon to the appliance as root.
6. Stop all NetWitness services with the following commands:

```
stop nwconcentrator
stop nwappliance
```

7. Verify all Security Analtyics services with the following commands:

```
status nwconcentrator
status nwappliance
```

8. Confirm and make note of mounted filesystems before the shutdown:

```
mount
```

9. Run the following command to cleanly shutdown the OS and power off the appliance:

```
shutdown -h now
```

10. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the Concentrator Appliance

1. Turn on the power to each DAC and allow it to power up.
2. Turn on the power to the appliance and allow it to boot.
3. Logon to the Security Analytics Server as Admin
4. Navigate to Administration | Devices and select the Concentrator service.
5. Open the System tab for the Concentrator service.
6. Stop aggregation on the Concentrator.
7. Open an ssh session and logon to the appliance as root.
8. Stop all NetWitness services with the following commands:

   ```
   stop nwconcentrator
   stop nwappliance
   ```
9. Restore the original /etc/fstab file with these commands:

   ```
   cp /etc/fstab /etc/fstab.nomount
   ```
   This keeps the old file just in case you need to review or use it again.

   ```
   cp /etc/fstab.backup /etc/fstab
   ```
   This restores the original /etc/fstab file.
10. Mount all file systems with the following command:

    ```
    mount –a
    ```
11. Verify all filesystems have mounted with the following command:

    ```
    mount
    ```
12. Start all NetWitness services with the following commands:

    ```
    start nwconcentrator
    start nwappliance
    ```
13. Logon to the Security Analytics Server as Admin
14. Verify that the Concentrator service is started and aggregating.
15. Verify that the Concentrator is consuming from all attached Decoders.

Shutting Down and Restarting an RSA Security Analytics Broker

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Broker Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Broker service.
3. Open the System tab for the Broker service.
4. Stop aggregation on the Broker.
5. Open an ssh session and logon to the appliance as root.
6. Stop all NetWitness services with the following commands:
```
stop nwbroker
stop nwappliance
```
7. Verify all Security Analtyics services with the following commands:
```
status nwbroker
status nwappliance
```
8. Confirm and make note of mounted filesystems before the shutdown:
```
mount
```
9. Run the following command to cleanly shutdown the OS and power off the appliance:
```
shutdown -h now
```
10. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the Broker Appliance

1. Turn on the power to the appliance and allow it to boot.
2. Open an ssh session and logon to the appliance as root.
3. Verify all filesystems have mounted with the following command:
```
mount
```
4. Verify all Security Analytics services with the following commands:
```
status nwbroker
status nwappliance
```
5. Logon to the Security Analytics Server as Admin
6. Verify that the Broker service is started and aggregating.
7. Verify that the Broker is consuming from all attached Concentrators.

Shutting Down and Restarting an RSA Security Analytics Malware Broker

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Malware Broker Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Broker service.
3. Stop aggregation on the Broker.
4. Open an ssh session and logon to the appliance as root.
5. Stop all NetWitness services with the following commands:

```
stop nwbroker
stop rsaMalwareDevice
stop nwappliance
```

6. Confirm and make note of mounted filesystems before the shutdown:

```
mount
```

7. Run the following command to cleanly shutdown the OS and power off the appliance:

```
shutdown -h now
```

8. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the Spectrum Broker Appliance

1. Turn on the power to the appliance and allow it to boot.
2. Open an ssh session and logon to the appliance as root.
3. Verify all filesystems have mounted with the following command:

```
mount
```

4. Verify all NetWitness services with the following commands:

```
status nwbroker
status rsaMalwareDevice
status nwappliance
```

5. Logon to the Security Analytics Server as Admin
6. Verify that the Broker service is started and aggregating.
7. Verify that the Broker is consuming from all attached Concentrators.

Shutting Down and Restarting an RSA Security Analytics Hybrid

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Hybrid Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Decoder service.
3. Open the System tab for the Decoder service.
4. Stop capture on the Decoder.
5. Navigate to Administration | Services and select the Concentrator service.
6. Open the System tab for the Concentrator service.
7. Stop aggregation on the Concentrator.
8. Open an ssh session and logon to the appliance as root.
9. Stop all NetWitness services with the following commands:
```
stop nwdecoder
stop nwconcentrator
stop nwappliance
```
10. Confirm and make note of mounted filesystems before the shutdown:
```
mount
```
11. Run the following command to cleanly shutdown the OS and power off the appliance:
```
shutdown -h now
```
12. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the Hybrid Appliance

1. Turn on the power to the appliance and allow it to boot.
2. Open an ssh session and logon to the appliance as root.
3. Verify all filesystems have mounted with the following command:
```
mount
```
4. Verify all NetWitness services with the following commands:
```
status nwdecoder
status nwconcentrator
status nwappliance
```
5. Logon to the Security Analytics Server as Admin
6. Verify that the Decoder service is started and capturing.
7. Verify that the Concentrator service is started and aggregating from the Decoder.

Shutting Down and Restarting an RSA Security Analytics Hybrid with DAC Attached

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Hybrid Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Decoder service.
3. Open the System tab for the Decoder service.
4. Stop capture on the Decoder.
5. Navigate to Administration | Services and select the Concentrator service.
6. Open the System tab for the Concentrator service.
7. Stop aggregation on the Concentrator.
8. Open an ssh session and logon to the appliance as root.
9. Stop all NetWitness services with the following commands:
```
stop nwdecoder
stop nwconcentrator
stop nwappliance
```
10. Confirm and make note of mounted filesystems before the shutdown:
```
mount
```
11. Backup the /etc/fstab file with the following command:
```
cp /etc/fstab /etc/fstab.backup
```
12. Edit /etc/fstab and comment out any lines that mount filesystems under the directory /var/netwitness or /var/lib/netwitness. There may be several of these lines in the /etc/fstab file.
13. Save the /etc/fstab file.
14. Gracefully shutdown the OS and power off the appliance with the following command:
```
shutdown -h now
```
15. Wait at least 5 minutes and confirm that all disk activity on the DAC has ended. Monitor the LED lights on the DAC to confirm disk I/O activity has ceased.
16. If the appliance did not power off after the shutdown command, press the power switch to shut it down.
17. Press the power switch on each attached DAC to power it down or, if the DAC does not have a power switch, disconnect the electrical power cords.
18. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the Hybrid Appliance

1. Turn on the power to each DAC and allow it to power up.
2. Turn on the power to the appliance and allow it to boot.
3. Logon to the appliance via ssh.
4. Verify all filesystems have mounted with the following command:
   ```
   mount
   ```
5. Verify all NetWitness services with the following commands:
   ```
   status nwdecoder
   status nwconcentrator
   status nwappliance
   ```
6. Logon to the Security Analytics Server as Admin
7. Navigate to Administration | Devices and select the Decoder service.
8. Open the System tab for the Decoder service.
9. Stop capture on the Decoder.
10. Navigate to Administration | Services and select the Concentrator service.
11. Open the System tab for the Concentrator service.
12. Stop aggregation on the Concentrator.
13. Open an ssh session and logon to the appliance as root.
14. Stop all NetWitness services with the following commands:
    ```
    stop nwdecoder
    stop nwconcentrator
    stop nwappliance
    ```
15. Restore the original /etc/fstab file with the following commands:
    ```
    cp /etc/fstab /etc/fstab.nomount
    ```
    This keeps the old file just in case you need to review or use it again.
    ```
    cp /etc/fstab.backup /etc/fstab
    ```
    This restores the original /etc/fstab file.
16. Mount all file systems with the following command:
    ```
    mount –a
    ```
17. Verify all filesystems have mounted with the following command:
    ```
    mount
    ```
18. Start all NetWitness services with the following commands:
    ```
    start nwdecoder
    start nwconcentrator
    start nwappliance
    ```
19. Verify all Security Analytics services with the following commands:
    ```
    status nwdecoder
    status nwconcentrator
    status nwappliance
    ```
8. Logon to the Security Analytics Server as Admin
9. Verify that the Decoder service is started and capturing.
10. Verify that the Concentrator service is started and aggregating from the Decoder.

Shutting Down and Restarting an RSA Security Analytics All-In-One

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the All-In-One Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Decoder service.
3. Open the System tab for the Decoder service.
4. Stop capture on the Decoder.
5. Navigate to Administration | Services and select the Concentrator service.
6. Open the System tab for the Concentrator service.
7. Stop aggregation on the Concentrator.
8. Navigate to Administration | Services and select the Broker service.
9. Open the System tab for the Broker service.
10. Stop aggregation on the Broker.
11. Navigate to Administration | Services and select the Malware service.
12. Open the System tab for the Malware service.
13. Stop aggregation on the Malware.
14. Open an ssh session and logon to the appliance as root.
15. Stop all NetWitness services with the following commands:

```
stop nwdecoder
stop nwconcentrator
stop nwbroker
stop rsaMalwareDevice
stop rsasoc_re
stop nwappliance
stop jettysrv
```

16. Confirm and make note of mounted filesystems before the shutdown:

```
mount
```

17. Run the following command to cleanly shutdown the OS and power off the appliance:

```
shutdown -h now
```

18. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the All-In-One Appliance

1. Turn on the power to the appliance and allow it to boot.
2. Open an ssh session and logon to the appliance as root.
3. Verify all filesystems have mounted with the following command:

```
mount
```

4. Verify all NetWitness services with the following commands:

```
status nwdecoder
status nwconcentrator
status nwbroker
status rsaMalwareDevice
status rsasoc_re
status nwappliance
status jettysrv
```

5. Logon to the Security Analytics Server as Admin
6. Verify that the Decoder service is started and capturing.
7. Verify that the Concentrator service is started and aggregating from the Decoder.
8. Verify that the Broker service is started and aggregating from the Concentrator.
9. Verify that the Malware service is started and processing threats.

Shutting Down and Restarting an RSA Security Analytics All-In-One with DAC Attached

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Hybrid Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the Decoder service.
3. Open the System tab for the Decoder service.
4. Stop capture on the Decoder.
5. Navigate to Administration | Services and select the Concentrator service.
6. Open the System tab for the Concentrator service.
7. Stop aggregation on the Concentrator.
8. Navigate to Administration | Services and select the Broker service.
9. Open the System tab for the Broker service.
10. Stop aggregation on the Broker.
11. Open an ssh session and logon to the appliance as root.
12. Stop all NetWitness services with the following commands:

```
stop nwdecoder
stop nwconcentrator
stop nwbroker
stop rsaMalwareDevice
stop rsasoc_re
stop nwappliance
stop jettysrv
```

13. Confirm and make note of mounted filesystems before the shutdown:

```
mount
```

14. Backup the /etc/fstab file with the following command:

```
cp /etc/fstab /etc/fstab.backup
```

15. Edit /etc/fstab and comment out any lines that mount filesystems under the directory /var/netwitness or /var/lib/netwitness. There may be several of these lines in the /etc/fstab file.
16. Save the /etc/fstab file.
17. Gracefully shutdown the OS and power off the appliance with the following command:

```
shutdown -h now
```

18. Wait at least 5 minutes and confirm that all disk activity on the DAC has ended. Monitor the LED lights on the DAC to confirm disk I/O activity has ceased.
19. If the appliance did not power off after the shutdown command, press the power switch to shut it down.
20. Press the power switch on each attached DAC to power it down or, if the DAC does not have a power switch, disconnect the electrical power cords.
21. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the All-In-One Appliance with DAC

1. Turn on the power to each DAC and allow it to power up.
2. Turn on the power to the appliance and allow it to boot.
3. Logon to the appliance via ssh.
4. Verify all filesystems have mounted with the following command:
   ```
   mount
   ```
5. Verify all NetWitness services with the following commands:
   ```
   status nwdecoder
   status nwconcentrator
   status nwbroker
   status rsaMalwareDevice
   status rsasoc_re
   status nwappliance
   status jettysrv
   ```
6. Logon to the Security Analytics Server as Admin
7. Navigate to Administration | Devices and select the Decoder service.
8. Open the System tab for the Decoder service.
9. Stop capture on the Decoder.
10. Navigate to Administration | Services and select the Concentrator service.
11. Open the System tab for the Concentrator service.
12. Stop aggregation on the Concentrator.
13. Navigate to Administration | Services and select the Broker service.
14. Open the System tab for the Broker service.
15. Stop aggregation on the Broker.
16. Open an ssh session and logon to the appliance as root.
17. Stop all NetWitness services with the following commands:
    ```
    stop nwdecoder
    stop nwconcentrator
    stop nwbroker
    stop rsaMalwareDevice
    stop rsasoc_re
    stop nwappliance
    stop jettysrv
    ```
18. Restore the original /etc/fstab file with the following commands:
    ```
    cp /etc/fstab /etc/fstab.nomount
    ```
    This keeps the old file just in case you need to review or use it again.
    ```
    cp /etc/fstab.backup /etc/fstab
    ```
    This restores the original /etc/fstab file.

19. Mount all file systems with the following command:

```
mount –a
```

20. Verify all filesystems have mounted with the following command:

```
mount
```

21. Start all NetWitness services with the following commands:

```
start nwdecoder
start nwconcentrator
start nwbroker
start rsaMalwareDevice
start rsasoc_re
start nwappliance
start jettysrv
```

22. Verify all Security Analytics services with the following commands:

```
status nwdecoder
status nwconcentrator
status nwbroker
status rsaMalwareDevice
status rsasoc_re
status nwappliance
status jettysrv
```

23. Logon to the Security Analytics Server as Admin
24. Verify that the Decoder service is started and capturing.
25. Verify that the Concentrator service is started and aggregating from the Decoder.

Shutting Down and Restarting an RSA Security Analytics Log Decoder with DAC Attached

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the Appliance

1. Logon to the Security Analytics Server as Admin.
2. Navigate to Administration | Services and select the LogCollector service.
3. Open the System tab for the LogCollector service.
4. Stop all log collections and wait until queues have emptied.
5. Navigate to Administration | Services and select the LogDecoder service.
6. Open the System tab for the LogDecoder service.
7. Stop capture on the Log Decoder.
8. Open an ssh session and logon to the appliance as root.
9. Stop all NetWitness services with the following commands:
```
stop nwlogdecoder
stop nwlogcollector
stop nwappliance
```
10. Confirm and make note of mounted filesystems before the shutdown:
```
mount
```
11. Make a backup of the /etc/fstab file:
```
cp /etc/fstab /etc/fstab.backup
```
12. Edit /etc/fstab and comment out any lines that mount under the directory /var/netwitness or /var/lib/netwitness. There may be several of these lines in the /etc/fstab file.
13. Save the /etc/fstab file.
14. Run the following command to cleanly shutdown the OS and power off the appliance:
```
shutdown -h now
```
15. Wait at least 5 minutes and confirm that all disk activity on the DAC has ended. Monitor the LED lights on the DAC to confirm this.
16. If the appliance did not power off after the shutdown command, press the power switch to shut it down.
17. Press the power switch on each attached DAC to power it down.

Starting the Log Decoder Appliance

1. Turn on the power to each DAC and allow it to power up.
2. Turn on the power to the appliance and allow it to boot.
3. Logon to the Security Analytics Server as Admin and connect to the LogDecoder service on the appliance.
4. Stop capture on the Log Decoder.
5. Open an ssh session and logon to the appliance as root.
6. Stop all NetWitness services with the following commands:

```
stop nwlogdecoder
stop nwlogcollector
stop nwappliance
```

7. Restore the original /etc/fstab file with these commands:

```
cp /etc/fstab /etc/fstab.nomount
```

This keeps the old file just in case you need to review or use it again.

```
cp /etc/fstab.backup /etc/fstab
```

This restores the original /etc/fstab file.

8. Mount all file systems with the following command:

```
mount –a
```

9. Verify all filesystems have mounted with the following command:

```
mount
```

10. Start all NetWitness services with the following commands:

```
start nwlogdecoder
start nwlogcollector
start nwappliance
```

11. Logon to the Security Analytics Server as Admin
12. Verify that the LogDecoder service is started and capturing.
13. Verify that the LogCollector service is started and capturing.

Shutting Down and Restarting an RSA Security Analytics Server

Follow these detailed steps to shut down and restart your RSA Security Analytics appliance.

Shutting Down the SA Server Appliance

1. Logon to the Security Analytics Server as Admin.
2. Open an ssh session and logon to the appliance as root.
3. Stop all NetWitness services with the following commands:

```
stop nwappliance
stop rsasoc_re
stop rsaMalwareDevice
stop jettysrv
```

4. Verify all Security Analtyics services with the following commands:

```
status nwappliance
status rsasoc_re
status rsaMalwareDevice
status jettysrv
```

5. Confirm and make note of mounted filesystems before the shutdown:

```
mount
```

6. Run the following command to cleanly shutdown the OS and power off the appliance:

```
shutdown -h now
```

7. If the appliance did not power off after the shutdown command, press the power switch to shut it down.

Starting the SA Server Appliance

1. Turn on the power to the appliance and allow it to boot.
2. Open an ssh session and logon to the appliance as root.
3. Verify all filesystems have mounted with the following command:

```
mount
```

4. Verify all Security Analytics services with the following commands:

```
status nwappliance
status rsasoc_re
status rsaMalwareDevice
status jettysrv
```

5. Logon to the Security Analytics Server as Admin
6. Verify that the SA Server is communicating with all attached Devices and Services.