Security Analytics 10.4 Upgrade

Agenda

- Introduction
- Resources Required
- Preparation
- Upgrade
- Validation

Introduction

RSA Security Analytics 10.4 Upgrade

Introduction

- RSA Security Analytics 10.4 offers a number of new features and improved performance.
- Health & Wellness monitoring capabilities allow a dashboard to review service status and performance.
- The upgrade process is enhanced and improved from previous versions.
  - Many update steps are now performed through the WebUI.
  - Please pay close attention to detail before, during and after the upgrade for a successful upgrade experience.
- This webinar will demonstrate how to prepare, upgrade and validate an SA Server and Decoder appliance.

Introduction

- This webinar will demonstrate how to prepare, upgrade and validate two SA appliances.
- The webinar will explain the material and then offer brief demonstrations of the process to upgrade
  - An SA Server version 10.3.2
  - An SA Packet Decoder version 10.3.2
- Schedule enough time to complete the upgrade.
  - Upgrading and validating the SA Server will take up to 50 minutes from the time you start the yum update.
  - Upgrading each other appliances will take 15 to 30 minutes.

Introduction (Continued)

- Have a plan, work the plan.
  - Identify and collect the resources required before you start.
  - Have a list of the required information including:
    - Number and type of appliances.
      - SA Server, SA Packet Decoder
    - Host names and IP Addresses.
      - CSTSAServer05: 192.168.1.
      - CSTPDecoder05: 192.168.1.
    - Ports used by Security Analytics.
      - 50004, 56004, 50104
  - Plan the order you will upgrade data centers and appliances.
    - SA Server
    - SA Packet Decoder

Preparation

RSA Security Analytics 10.4 Upgrade

Preparation

- Gather the necessary resources.
- Validate your existing installation.
- Review the SA 10.4 Upgrade Instructions.
- Prepare your upgrade script or plan.
- Stage upgrade files to SA Server.

Required Resources

- Download documentation from SCOL.
  - RSA Security Analytics v 10.4 Release Notes.
  - RSA Security Analytics v 10.4 Upgrade Instructions.
  - https://knowledge.rsasecurity.com/scolcms/set.aspx?id=10407
- Download upgrade files from DLC.
  - sa-v10.4-UpgradePack-EL6.zip (2.5GB)
- Download upgrade files from SCOL.
  - rsa-sa-gpg-pubkeys-10.4.0.1.1116-1.el6.noarch.rpm (11 KB)

Required Resources (Continued)

- Approved Browser
  - Chrome
  - Firefox
  - Internet Explorer
- SSH tool such as putty
- WinSCP or similar tool

Validate Existing Environment

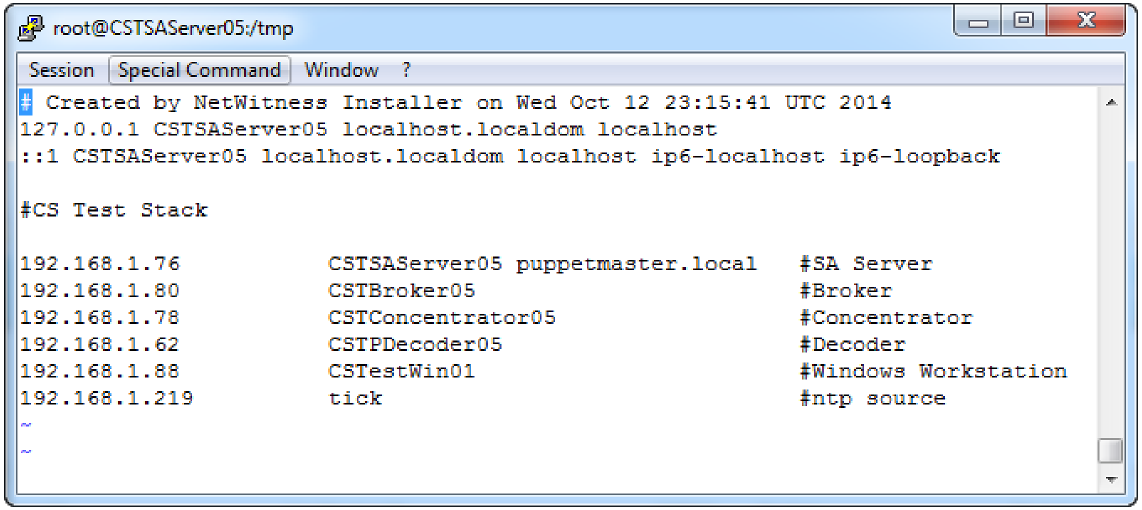
Confirm:

- All appliances have sufficient space available on all file systems.
  - Nothing over established thresholds.
  - Nothing at 100% utilization.
- DNS is working.

Validate Existing Environment (Continued)

Confirm

- Contents of /etc/hosts:
  - The localhost entries contain correct host names.
  - There are accurate entries for every appliance in your environment.



```
# Created by NetWitness Installer on Wed Oct 12 23:15:41 UTC 2014
127.0.0.1 CSTSAServer05 localhost.localdom localhost
::1 CSTSAServer05 localhost.localdom localhost ip6-localhost ip6-loopback

#CS Test Stack

192.168.1.76          CSTSAServer05 puppetmaster.local    #SA Server
192.168.1.80          CSTBroker05                         #Broker
192.168.1.78          CSTConcentrator05                   #Concentrator
192.168.1.62          CSTPDecoder05                       #Decoder
192.168.1.88          CSTestWin01                         #Windows Workstation
192.168.1.219         tick                                #ntp source
~
~
```

Validate Existing Environment (Continued)

Confirm

- NTP is configured and running on each appliance:
  - chkconfig starts ntpd on runlevel 2, 3, 4 & 5.
  - ntpd is started.
- Clocks are synchronized on each appliance.
  - Run clockdiff -o <target_appliance> to confirm synchronization.
  - Correct with ntpdate -u <timesource> as necessary.

Validate Existing Environment (Continued)

Verify

- All appliances are currently running SA 10.3.2 or above.
- All services are responsive in the WebUI.
- SSL is set as desired on all services on all appliances.
- All appliances are capturing and aggregating.
- Establish a baseline and make sure you know the state of all appliances to be upgraded.

Validate Existing Environment (Continued)

Verify

- Latest security patches and kernels installed.
- The /boot/grub/grub.conf is booting the expected kernel.
- Verify the kernel versions running on each appliance.

Validate Existing Environment (Demonstration)

Demonstrate the steps to validate your existing environment.

Review Upgrade Instructions

Check

- All appliances are at SA 10.3.2 or above:
  - You may upgrade directly to SA 10.4 from SA 10.3.2 and later versions.
  - Additional steps are required to upgrade older versions.
- All appliances are running EL6.
- Kernels installed on each appliance match the minimum kernel version:
  - Kernel 2.6.32-358.18.1.el6.x86_64 shipped with SA 10.3.2
  - Kernel 2.6.32-431.17.1.el6.x86_64 shipped with Q2 Security Patches
  - Kernel 2.6.32-431.23.3.el6.x86_64 shipped with SA 10.4
- All ports are open between appliances:
  - https://sadocs.emc.com/0_en-us/090_10.4_User_Guide/100_SitePlan/NetwrkPorts
  - See Knowledgebase article 29087 for additional ports.
  - See Appendix A of this presentation.

Review Upgrade Instructions (Continued)

Update the SA Yum Repository

- Remove the nw-erlang package if present.
- Clean out the repository on the SA Server
  - Disable repository synchronization in the SA WebUI.
  - Delete all files in:
    - /var/netwitness/srv/www/rsa/updates/RemoteRPMs.
    - /var/netwitness/srv/www/rsa/updates/SAUserUploaded.
  - Manually populate the SA Server Update Repository.
- Prepare the Log Collector services *(Not part of this demonstration)*.

Review Upgrade Instructions (Continued)

Update the SA Yum Repository

- Update NwIpdbextractor.cfg file. *(Not part of this demonstration.)*
- Check host name and IP Addresses. *(Reviewed in previous steps.)*
- Back Up existing configurations
  - See https://sadocs.emc.com/0_en-us/090_10.4_User_Guide/215_SysAdmin/BackupRest
  - Backing up configuration will enable a more rapid recover of any unforeseen difficulties during upgrade.

Review Upgrade Instructions (Demonstration)

Demonstrate the steps to review your existing environment prior to upgrade

Upgrade

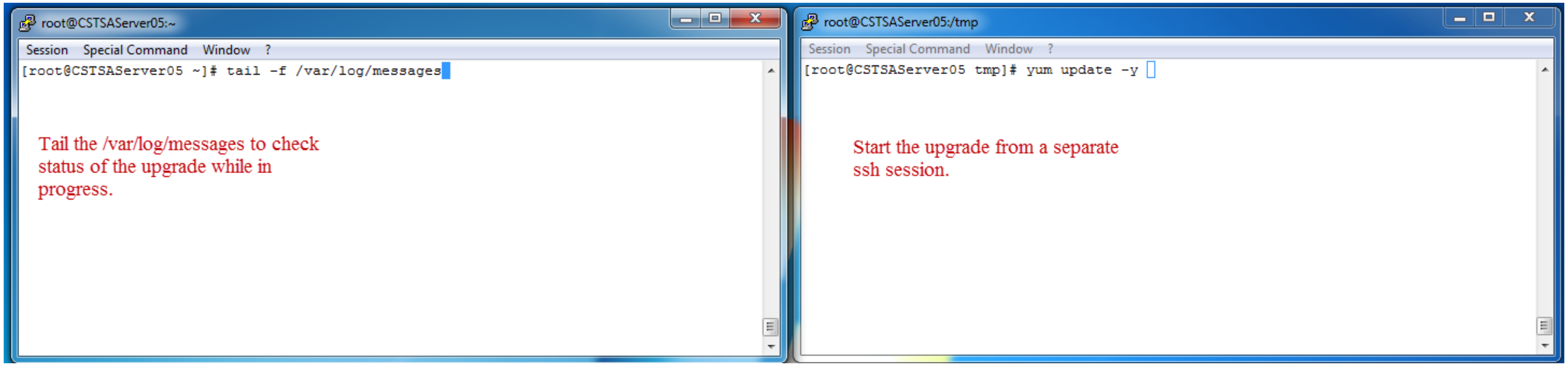
RSA Security Analytics 10.4 Upgrade

Upgrade

- Upgrade the Primary SA Server.
  - This takes up to 45 minutes.
  - Don’t rush and don’t reboot the SA Server prematurely.
- Upgrade Other Appliances.
  - There is a recommended order for upgrading appliances in Appendix D of the upgrade document.
    - SA Server
    - ESA and Malware
    - Decoders
    - Concentrators
    - Broker

Upgrade the Primary SA Server (Continued)

- Upgrade the Primary SA Server
  - Open TWO ssh sessions to the SA Server and logon to the SA Server via a browser
  - Use ssh session 1 to start the upgrade
  - Use ssh session 2 to tail the /var/log/messages during the upgrade


root@CSTSAServer05:~
Session Special Command Window ?
root@CSTSAServer05:/tmp
Session Special Command Window ?

```
[root@CSTSAServer05 ~]# tail -f /var/log/messages
```

Tail the /var/log/messages to check status of the upgrade while in progress.

```
[root@CSTSAServer05 tmp]# yum update -y
```

Start the upgrade from a separate ssh session.

Upgrade the Primary SA Server (Continued)

- Upgrade the Primary SA Server.
  - Verify the repository is ready.

    ```
    yum check-update
    yum check-update | grep server
    ```

  - Install the rsa-sa-gpg-pubkeys rpm.

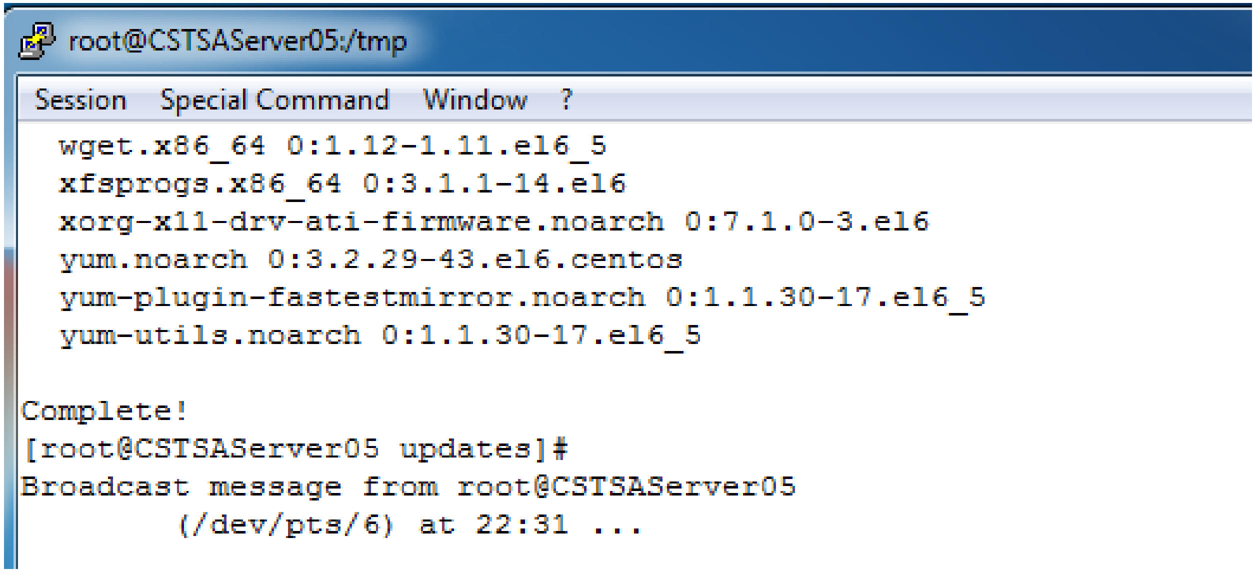
    ```
    yum install rsa-sa-gpg-pubkeys
    ```

  - Start the yum upgrade on an SA Server with no Broker service

    ```
    yum update -y
    ```

Upgrade the Primary SA Server (Continued)

- The yum update command should complete within 30 minutes.
  - Wait for the confirmation in ssh session 1



```
  wget.x86_64 0:1.12-1.11.el6_5
  xfsprogs.x86_64 0:3.1.1-14.el6
  xorg-x11-drv-ati-firmware.noarch 0:7.1.0-3.el6
  yum.noarch 0:3.2.29-43.el6.centos
  yum-plugin-fastestmirror.noarch 0:1.1.30-17.el6_5
  yum-utils.noarch 0:1.1.30-17.el6_5

Complete!
[root@CSTSAServer05 updates]#
Broadcast message from root@CSTSAServer05
        (/dev/pts/6) at 22:31 ...
```

Upgrade the Primary SA Server (Continued)

- Reboot the SA Server.
- Wait for the server to restart.
  - 1 to 2 minutes for a virtual machine
  - 7 to 9 minutes for a physical machine
- Connect to ssh session 1 and session 2 again.
- Resume the “`tail -f /var/log/messages`” command on ssh session 2.
- Jettysrv, the SA WebUI will take 7 to 10 minutes to restart after the appliance is rebooted.
- Allow 15 to 20 minutes for the post-reboot processing to complete.

Upgrade the Primary SA Server (Demonstration)

- Perform an upgrade on an SA 10.3.2 SA Server virtual machine.

Upgrade a Decoder Appliance

Upgrade Other Appliances

- In Security Analytics 10.4 most of the upgrade steps for other appliances are performed through the WebUI.
- Only one step must be performed at the CLI.
- There is a recommended order for upgrading appliances. (See Appendix D in the upgrade documentation.)
    - SA Server
    - ESA and Malware
    - Decoders
    - Concentrators
    - Broker

Upgrade (Continued)

Upgrade a Packet Decoder

- Logon to the SA Server WebUI.
- Open TWO ssh sessions, one to the SA Server and one to the Decoder.
  - Use ssh session 1 to install the public keys and tail the /var/log/messages on the Decoder.
  - Use ssh session 2 to tail the /var/log/messages on the SA Server.
- Logon to the SA Server via a browser.

Upgrade a Decoder Appliance (Continued)

- Go to the Appliance screen and select the Packet Decoder.
- Use the update menu icon to check for updates.
- Once updates are found the “Upgrade to 10.4” button will appear next to the Packet Decoder.
  - Float the mouse pointer over the “Upgrade to 10.4” button to see a list of pending updates.
- DO NOT CLICK “Upgrade to 10.4” YET!

Upgrade a Decoder Appliance (Continued)

- Go to the ssh session for the Packet Decoder and verify the repository state and install the rsa-sa-gpg-pubkeys package:
  - Verify the repository is ready

    ```
    yum check-update | grep nwdecoder
    ```

  - Install the rsa-sa-gpg-pubkeys rpm

    ```
    yum install rsa-sa-gpg-pubkeys
    ```

Upgrade a Decoder Appliance (Continued)

- Go to the SA Server WebUI and click "Upgrade to 10.4".
  - Allow 6 t 10 minutes for the upgrade to proceed.
  - Watch the /var/log/messages on the Packet Decoder to monitor the status of the update.
- Check the status of the upgrade.
  - If the update status is "Error" please contact Customer Support.
  - If the update status is "Reboot Required" please reboot the appliance.
- Reconnect to the Packet Decoder via ssh and tail –f /var/log/messages again.

Upgrade a Decoder Appliance (Continued)

- Reconnect to the Packet Decoder via ssh and tail –f /var/log/messages again.
- Check the status of the upgrade and click “Enable”.
  - This will exchange keys between the SA Server and the Packet Decoder.
  - No additional reboot is required after this step.
  - Monitor the /var/log/messages on the SA Server and Packet Decoder
  - Watch the key exchange and other configuration in logs and other log entries to track the upgrade progress.

Upgrade a Decoder Appliance (Demonstration)

Perform an upgrade on an SA 10.3.2 Packet Decoder virtual machine.

Upgrade Additional Appliances

- Continue upgrading additional appliances using the steps outlined above.
- Follow the steps and upgrade appliances in the established order.
- You may upgrade multiple appliances of the same type simultaneously.
- Validate each appliance after the upgrade.

Post Upgrade steps

RSA Security Analytics 10.4 Upgrade

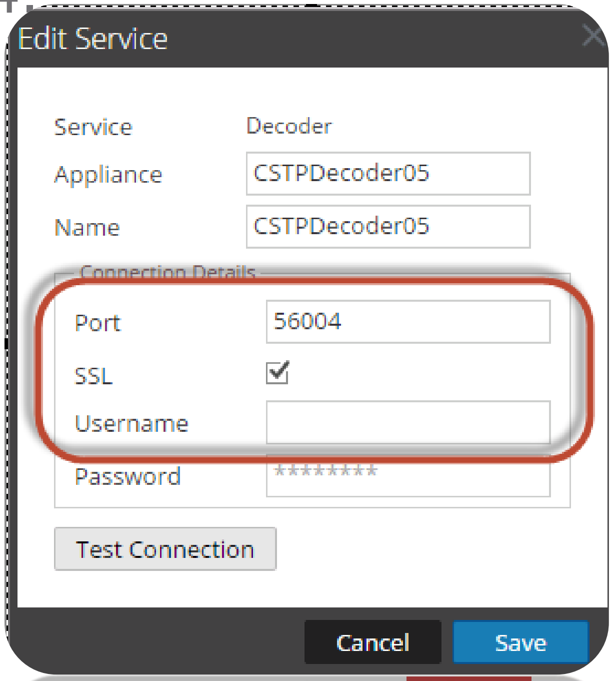
Post Upgrade Tasks

- Configure SSL ports on appliances.
- Reconfigure Reporting Engine and ESA sources.
- Upgrade MapR to latest components. *(Not part of this demonstration)*.
- Enable or disable IPDBExtractor service device parsers. *(Not part of this demonstration).*
- STIG the appliance. *(Not part of this demonstration)*.

Post Upgrade Tasks (Continued)

Configure SSL ports on appliances.

- Open the SA WebUI and select the Decoder service.
- Edit the Decoder service:
  - Change the port from 50004 to 56004.
  - Click on the SSL checkbox.
  - Remove the Username.
  - Click “Test Connection”.
  - Save the change.



Edit Service

Service	Decoder
Appliance	CSTPDecoder05
Name	CSTPDecoder05

Connection Details

Port	56004
SSL	☑
Username	
Password	********

Post Upgrade Tasks (Continued)

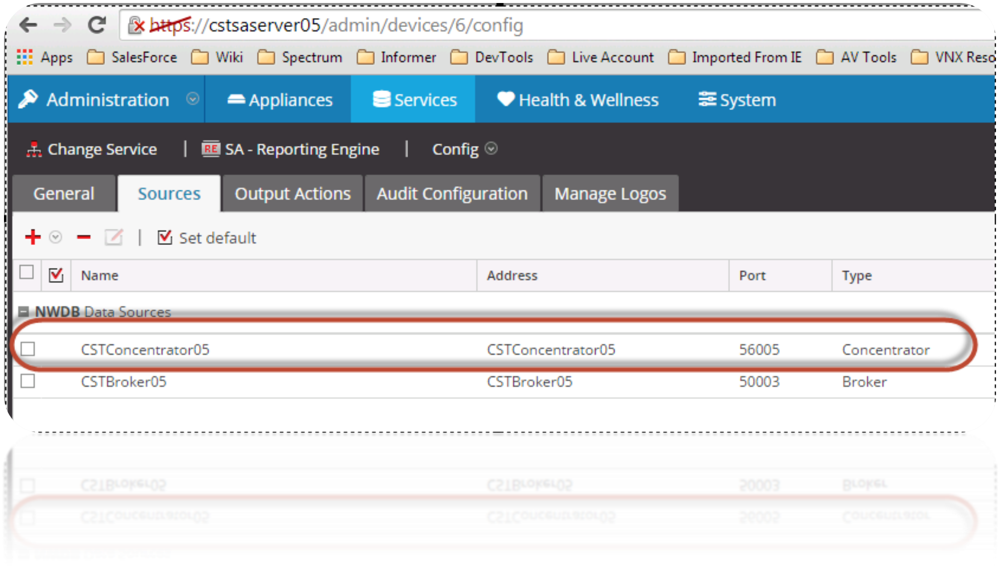
Configure Reporting Engine Sources.

- Logon to the SA WebUI and go to the Services screen.
- Select the Broker and Concentrator services after they have been upgraded.
- Edit the Broker and Concentrator services to use the SSL ports (56003 and 56005) like the Decoder service.

Post Upgrade Tasks (Continued)

Configure Reporting Engine Sources.

- From the WebUI Services go to Reporting Engine > Config > Sources tab.
- Remove any Report sources and add again.
- Confirm the new sources are using the new SSL ports.



☐	☑ Name	Address	Port	Type
NWDB Data Sources				
☐	CSTConcentrator05	CSTConcentrator05	56005	Concentrator
☐	CSTBroker05	CSTBroker05	50003	Broker

Wrap Up and Final Thoughts

RSA Security Analytics 10.4 Upgrade

Wrap Up and Final Thoughts (Continued)

- Plan sufficient time to upgrade appliances.
  - Observe the status of the upgrade carefully.
  - Avoid rebooting appliances unless required by the upgrade process.
  - Don’t reboot appliances prematurely.
- Document your upgrade.
  - Keep detailed notes during your upgrade process.
    - Document the upgrade process.
    - Note start and stop time for steps for each appliance.
  - Consider recording your upgrade sessions even if you can’t share the recordings with Support.
  - These notes will be helpful if you need to open a case in the event of complications.

Wrap Up and Final Thoughts (Continued)

- Appliances of the same type can be updated simultaneously.
  - Follow the upgrade order.
  - Don't upgrade more appliances than you can observe and validate simultaneously.
  - Validate your appliances early in the post-update process.
  - Confirm services are working before proceeding to upgrade other appliances.

How To Contact RSA Technical Support

- Should you need assistance with your upgrade, please contract RSA Technical Support using any of the following:
  - SCOL - https://knowledge.rsasecurity.com
  - Email: nwsupport@rsa.com
  - Phone: 800.995.5095, Option 9

Appendix A: Ports

RSA Security Analytics 10.4 Upgrade

SA 10.4 Ports

Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
Appliance	50006	
Appliance (REST)	50106	
Archiver	50008	56008
Archiver (REST)	50108	
Broker	50003	56003
Broker (REST)	50103	
rsaCAS	50010	
CLDB	7222	
CLDB JMX Monitor port	7220	
CLDB Web Port	7221	
Concentrator	50005	56005
Concentrator (REST)	50105	
Decoder	50004	56004
Decoder (REST)	50104	

Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
ESA	50030	
HBase Master	60000	
Incident Management	50040	
IPDB Extractor	50009	
IPDB Extractor	50025	56025
IPDB Extractor (REST)	50125	
JobTracker	9001	
JobTracker Web	50030	
Local Log Collector (NwLogCollector on Log Decoder)	50001, Pulls from Remote Log Collector through 5671	56001
LDAP	389	

SA 10.4 Ports (Continued)

Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
Log Decoder	50002	56002
Log Decoder (REST)	50102	
Log Decoder Protobuf	50202	
Log Decoder Protobuf	56202	
Log Decoder Syslog	514	
Log Decoder Syslog	6514	
Malware Analysis	60007	
MFS Server	5660	
NFS	2049	
NFS Management	9998	
NFS Monitor (For HA)	9997	
NFS Port Mapper	111	
Remote Log Collector (NwLogCollector on remote VM)	50001, Pushes to Local Log Collector through 5671	56001
Reporting Engine	51113	

Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
Log Decoder	50002	56002
Log Decoder (REST)	50102	
Log Decoder Protobuf	50202	
Log Decoder Protobuf	56202	
Log Decoder Syslog	514	
Log Decoder Syslog	6514	
Malware Analysis	60007	
MFS Server	5660	
NFS	2049	
NFS Management	9998	
NFS Monitor (For HA)	9997	
NFS Port Mapper	111	
Remote Log Collector (NwLogCollector on remote VM)	50001, Pushes to Local Log Collector through 5671	56001
Reporting Engine	51113	

Appendix B: Update the Repository Manually

RSA Security Analytics 10.4 Upgrade

Update the SA Repository Manually

- In some cases uploading large .zip files to an SA Server fails.
- This is more likely in virtual environments.
- It is possible to manually update the SA Server repositories using the following steps.

Update the SA Repository Manually (Continued)

Manually update the files to the SA Server and create the repo with these steps.

- Disable repository synchronization in the SA WebUI
- Delete all files in:
  - /var/netwitness/srv/www/rsa/updates/RemoteRPMs
  - /var/netwitness/srv/www/rsa/updates/SAUserUploaded
- Use SCP or WinSCP to move the .zip file to the SA Server in /var/netwitness/srv/www/rsa/updates/
- Unzip the update.zip file into /var/netwitness/srv/www/rsa/updates/SAUserUploaded
- From /var/netwitness/srv/www/rsa/updates/ run the "`createrepo .`" command.
- Run "`yum clean all`" and "`yum check-update`" from the command line to verify the repository.
- Verify the update files in the SA WebUI.