Release Notes
RSA DLP 9.6.2.2

December, 2014

Introduction

This document lists what's new and changed in RSA DLP 9.6.2.2. It includes additional installation information, as well as workarounds for known issues. Read this document before installing the software. This document contains the following sections:

What's New

This section lists what's new and changed in RSA DLP 9.6.2.2.

Support for Server Components on Windows 2012 R2

With this release, all DLP Server components and End Point Agent are now supported on Windows 2012 R2 OS.

Support for Hyper-V on Windows 2012 R2

With this release, Windows Server 2012 R2 Hyper-V is a supported Hypervisor environment.

Support for Exchange Transport Agent on Exchange 2010 SP2, and 2010 SP3

With this release, Exchange Transport Agent is now supported on Exchange 2010 SP2, and 2010 SP3.

Support for PCI 3.0 DSS Audit Log

With this release, PCI 3.0 DSS Audit Log is now supported to track and monitor access to RSA DLP Network resources.

Package Contents

RSA DLP 9.6.2.2 package contains:

- RSA_DLP_Suite_9.6-SP2-P2.zip
  - RSA DLP Exchange Agent 9.6-SP2-P2.msi
  - RSA DLP Installer Update 9.6-SP2-P2.exe
  - RSA DLP IPMapper 9.6-SP2-P2.msi

- DLP_Network_9.6-SP2-P2_Upgrade.gpg

Patch Installation

Follow the instructions in this section to install the patch.

Important: You must be running 9.6-SP2 or 9.6-SP2-P1 before applying the patch.

Steps to install the patch:

1. Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator
2. Do the following, in any order:
   - Upgrade Network Components
   - Upgrade Datacenter Components
   - Upgrade Endpoint Agents

Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator

Important: If the Enterprise Manager, Enterprise Coordinator, and the Root Endpoint Coordinator reside on different machines, perform this procedure on all the machines. You must install the patch on the Enterprise Manager first, and then on the Enterprise Coordinator and the Root Endpoint Coordinator machines.

After installing the patch on the Root Endpoint Coordinator, you must install the patch on all the Endpoint Coordinator machines.

To install RSA DLP 9.6.2.2 on Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator:

1. Copy **RSA DLP Installer Update 9.6-SP2-P2.exe** to the machine hosting the Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.
2. Double-click **RSA DLP Installer Update 9.6-SP2-P2.exe** to start the installation.
3. Follow the instructions on the installation wizard to complete the installation.

Upgrade Network Components

Perform the following procedure to upgrade the Network Controller and all the Sensors, Interceptors, and ICAP servers.

Important: You must install the patch on the Network Controller first, and then on the Sensors, Interceptors, and ICAP servers, in any order.

Before You Begin

- Install the patch on the Enterprise Manager. See Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.

To upgrade the Network components:

1. Copy the **DLP_Network_9.6-SP2-P2_Upgrade.gpg** file to the **/home/tablus** directory.
2. On the Network appliance, go to the DLP Network Main Menu.
3. Select option 4, Check for Updates.
4. Select option 2 -- Check for updates from the update file on the local system.

5. Follow the remaining prompts as the Network appliance moves through the installation.

   After the installation is completed, you will see the updated DLP version number on the tab menu.
6. Reboot the appliance.
   a. From the Main Menu on the appliance, select Option 6.
   b. Select Option 2.
7. Repeat steps 1 - 6 on the remaining network appliances.
8. Publish the updated configuration. See Publish Configuration.

Upgrade Datacenter Components

Perform the following procedure to upgrade the permanent Discovery agents and the grid workers.

Before You Begin

- Install the patch on the Enterprise Manager and the Enterprise Coordinator. See Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.

To request Datacenter upgrade and publish updated configuration:

1. On Enterprise Manager, click **Admin** > **Support** > **Upgrade Manager**.

   The Upgrade Manager appears.
2. Select **Datacenter**, and click **Request Upgrade**.
3. Once the Upgrade Requests table shows the latest version, publish the updated configuration. See Publish Configuration.

   The permanent Discovery agents and the grid workers are upgraded during the next scan.

Upgrade Endpoint Agents

Perform the following procedure to upgrade all the Endpoint agents.

Before You Begin

- Install the patch on the Enterprise Manager, Root Endpoint Coordinator, and all the Endpoint Coordinators. See Upgrade Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator.

To upgrade the Endpoint agents:

1. In Enterprise Manager, click **Admin** > **Support** > **Upgrade Manager**.

   The Upgrade Manager page appears.
2. Under the **Agent Patch Deployment** section, click **Deploy Agent Patch**.

   All the existing endpoint agents are automatically upgraded.

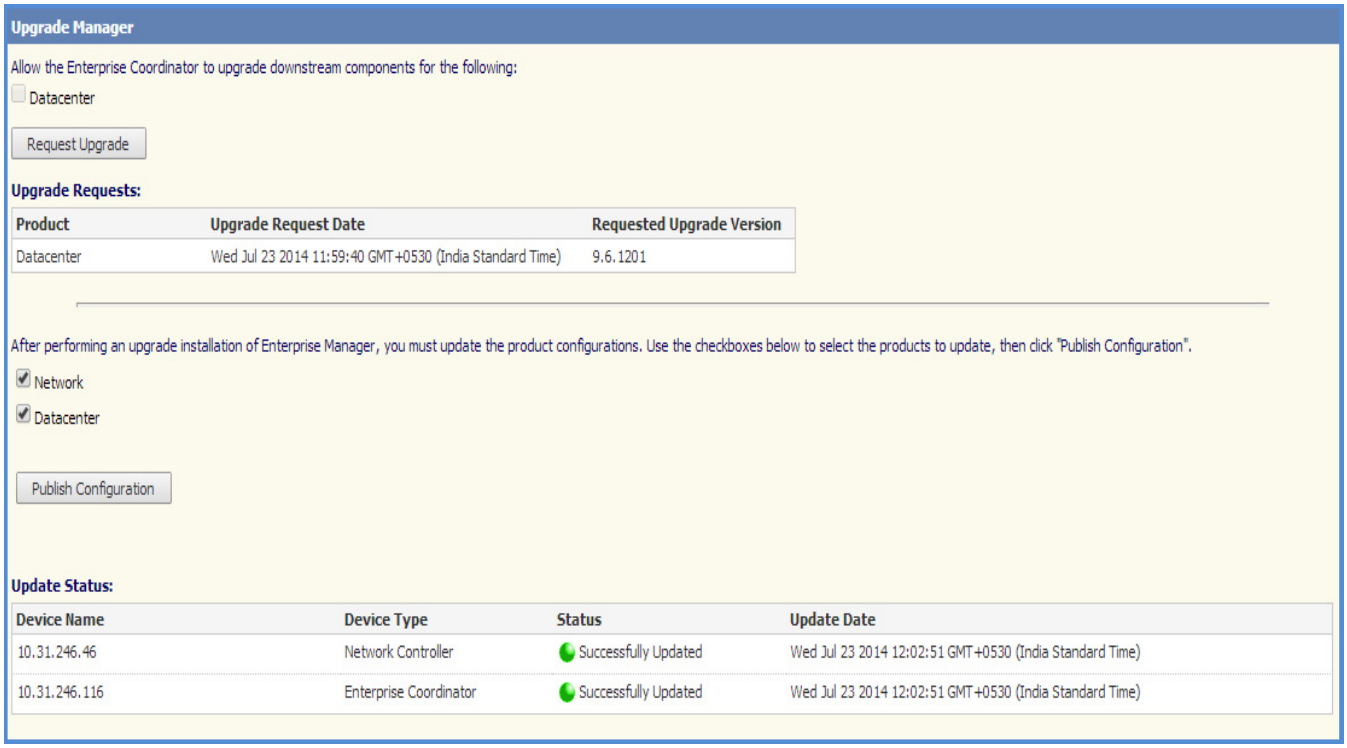
Publish Configuration

Note: Perform this procedure only if you are using DLP Datacenter or DLP Network.

1. On Enterprise Manager, click **Admin** > **Support** > **Upgrade Manager**.

   The Upgrade Manager appears.

2. In the middle of the page, select the product configurations to update by selecting **Network**, **Datacenter**, or both.



3. Click **Publish Configuration**. A dialog appears, explaining that the operation will take place over time.
4. Click **OK** to continue.

   The **Update Status** section displays a status and the date and time when Enterprise Manager started deploying updated configuration information to other components.

   Wait several minutes before performing additional operations in Enterprise Manager—in particular, avoid changing the configuration and starting scans. This should allow time for configurations to be updated and avoid possible conflicts and problems that may be caused by mismatched configuration information.

Security Fixes

This section includes the potential security vulnerabilities and issues that have been fixed in RSA DLP 9.6.2.2.

- Investigate Shellshock Vulnerability. For information, see the security advisory RHSA-2014:1293-1. The Investigate Shellshock Vulnerability (CVE-2014-6271) affects only the DLP Network components.
- Open SSL Vulnerability. For information, see the security advisory ESA-2014-806. The Open SSL Vulnerability (CVE-2014-3505) affects only the DLP Network components.
- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE). The POODLE Vulnerability (CVE-2014-3566) affects only the DLP Enterprise Manager.
- CentOS Security Updates. The following table lists the various CentOS Security Updates:

CentOS Update
CentOS Security Update for java-1.7.0-openjdk (CESA-2014:0026)
CentOS Security Update for java-1.7.0-openjdk (CESA-2014:0406)
CentOS Security Update for Kernel (CESA-2013:1801)
CentOS Security Update for libXfont (CESA-2014:0018)
CentOS Security Update for kernel (CESA-2014:0159)
CentOS Security Update for Kernel (CESA-2014:0328)
CentOS Security Update for kernel (CESA-2014:0475)
CentOS Security Update for Kernel (CESA-2014:0771)
CentOS Security Update for libjpeg-turbo (CESA-2013:1803)
CentOS Security Update for nss (CESA-2013:1861)
CentOS Security Update for ca-certificates (CESA-2013:1866)
CentOS Security Update for BIND (CESA-2014:0043)
CentOS Security Update for openldap (CESA-2014:0126)
CentOS Security Update for net-snmp (CESA-2014:0321)
CentOS Security Update for curl (CESA-2014:0561)
CentOS Security Update for wget (CESA-2014:0151)

Fixed Issues

This section lists the issues that have been fixed in this release.

DLP Network

- NAPTECH drivers built on new Kernel and qualified as part of 9.6.2.2.
- VerityFilter terminated with exit status 99 error on specific xls file attachment.
- Issue with reading AD RMS Policy Name from AD RMS Protected Files for Network.
- Memory leak issue with ICAP.
- Network policy based on file attributes not detecting files.
- TCP-Flood overflow on ICAP.
- ICAP unable to process files.

DLP Endpoint

- Policy Block and justify still allows the user to copy the contents from VDI clipboard to another machine.
- Files copied from one location to another on the network drive causes files to be copied incorrectly. That is, alternate files gets copied correctly and the rest are copied with zero data.
- DLP Endpoint .msi installation changed access permission on files or folders of Endpoint machine.
- IE8 hangs when uploading large file size with DLP Endpoint 9.6 SP2 service running.
- The receipent receives an empty email with an attachment that cannot be opened when sent from Outlook with RMS encryption.
- Existence of DLP Endpoint Enforce Agent's Outlook Add-in (RSADLPOLAddin.VSTO) is causing issues within outlook for users.
- Issue to read AD RMS Policy Name from AD RMS Protected Files for Endpoint.
- Agent gaps - Print from MS Office Excel 2013 and copy file via RDP to desktop of the agent machine not monitored/blocked.
- Outlook plugin generates events where email address appears in x.500 format.

DLP Enterprise Manager

- Policy Rule Transmission attributes for URL does not accept ‘&’ symbol.
- Exporting all results from an Agent Group Status tab by clicking the Export All results link resulted in system error.
- Running an export from the Incident tab on Events is slow or unresponsive.
- Firefox browser shows "A server error has occurred" when viewing matched content for network events.
- Add network device name to sylog.
- CLI intermittently fails to delete events or times out.
- Administrator has to discard quarantined emails repeatedly prior to closing an incident.

DLP Datacenter

- Grid scan stopped prematurely when Site Coordinator was rebooted during Operating System patching.
- Issue to read AD RMS Policy Name from AD RMS Protected Files for Data Center.
- Exchange 2013 scanning by specifying a single Exchange server name times out.
- Datacenter scan status is failed though scan is still in paused state.

- EC will not allow EM connection using certificate from public CA on SP2 or later versions.

Knowledge Engineering

- Update PCI policy name and documentation to version 3.0.

Known Issues

Network Controller javax.net.ssl.SSLException unable to communicate with EM

Problem: The Network Controller is unable to send event.zip to EM due to an error message seen on Network Controller *messages.log* file.

Workaround: If Network Controller is unable to communicate with EM, do the following:

1. Logon to Network Controller as a root user and execute the following commands:

   ```
   chmod o-r /usr/java/latest/lib/security/java_nonfips.security
   chmod o-r /usr/java/latest/lib/security/java_fips.security
   ```

2. Restart the Network Controller services.

Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	http://www.emc.com/support/rsa/index.htm
RSA Solution Gallery	https://gallery.emc.com/community/marketplace/rsa

Trademarks