Release Notes
RSA DLP 9.6.2.3

June, 2015

Introduction

This document lists what's new and changed in RSA DLP 9.6.2.3. 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:

Package Contents

RSA DLP 9.6.2.3 package contains:

- RSA_DLP_Suite_9.6-SP2-P3.zip
  - RSA DLP Exchange Agent 9.6-SP2-P3.msi
  - RSA DLP Installer Update 9.6-SP2-P3.exe
  - RSA DLP IPMapper 9.6-SP2-P3.msi
- DLP_Network_9.6-SP2-P3_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 or 9.6-SP2-P2 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 9.6.2.3 on Enterprise Manager, Enterprise Coordinator, Root Endpoint Coordinator, and Endpoint Coordinator:

1. Copy **RSA DLP Installer Update 9.6-SP2-P3.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-P3.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-P3_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.

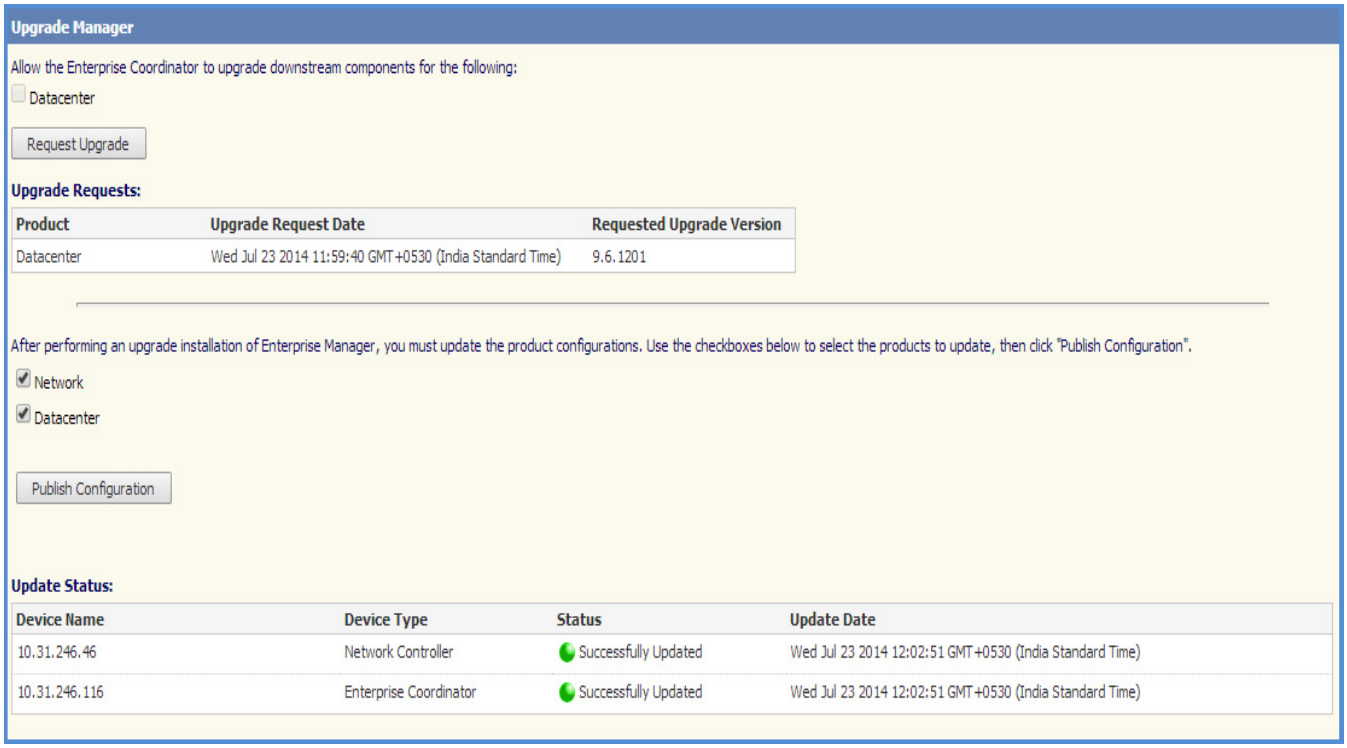
Publish Configuration

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 9.6.2.3.

- OpenSSL Vulnerabilities. For information, see the security advisory RHSA-2015:0066-2. The OpenSSL Vulnerabilities (CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275 CVE-2015-0204, CVE-2015-0205, CVE-2015-0206) affects only the DLP Network components.
- GHOST Vulnerability. For information, see the security advisory RHSA-2015:0092-2. The GHOST Vulnerability (CVE-2015-0235) affects only the DLP Network components.

Fixed Issues

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

DLP Network

- Interceptor service failed and queued the mails.

DLP Endpoint

- Empty file upload to custom background image results in incorrect Endpoint configuration.
- The URL transmission attribute in the Endpoint policy fails to accept asterisks (*).
- IE browser crashes on some of the Endpoint machines.
- Additional languages are not displayed on Endpoint pop-up notification.
- Endpoint unable to identify encrypted files.

DLP Enterprise Manager

- Unable to send Syslog messages greater than 1024 bytes to ArcSight.
- A frequent deadlock issue occurs while processing events.
- After upgrading from DLP 9.6 SP2 to DLP 9.6 SP2 P2 on FIPS enabled machine, unable to log in to Enterprise Manager.
- The transmission attributes fails when an incorrect URL is provided.
- The escalation rule policy does not work correctly.
- Unable to match correct Active Directory users.
- An URL ending with .local domain is not supported.
- ESA DLP engine fails to load due to missing package information from the policy push out.

DLP Datacenter

- Datacenter Agent fails to upgrade to 9.6 SP2 P3 as the upgradeTaskSpecification file is not updated.
- Crawler information takes more space in the C:\Windows\Temp folder.
- Discrepancy in the the grid scan history report.

Knowledge Engineering

- Remediation functionality fails to delete Read-only files.

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.

Microsoft Patch KB3045999 causes DLP Endpoint to hang

Problem: Whenever the Endpoint hooks an application, an error “The application was unable to start correctly (0x0000018)” occurs. This is due to Microsoft Patch KB3045999.

Workaround: You must uninstall Microsoft Patch KB3045999.

Note: The above workaround is applicable until a Hotfix is released.

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