Release Notes
RSA Access Manager Server 6.2 SP1

December 17, 2013

Introduction

This document lists what's new and changed in RSA Access Manager 6.2 SP1. 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:

These *Release Notes* may be updated. The most current version can be found on RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

What's New in This Release

This section describes the major changes introduced in this release. For detailed information on each change, see the appropriate *RSA Access Manager Guide*.

Log Server Enhancement. RSA Access Manager Server 6.2 SP1 Log server has been enhanced to accept logs from Web Agent and Application Server Agent.

Log server fail-over Capability. RSA Access Manager Server 6.2 SP1 supports Log Server fail-over for all the Server components, which is if the primary Access Manager Log server fails to receive log messages then the log messages are logged to the secondary log servers, when multiple instances of log servers are configured.

Request Tracking of Access Manager Server requests. RSA Access Manager Server 6.2 SP1 supports the ability to obtain the time elapsed at each component level for every Authorization server's request. This feature helps you to narrow down the root cause of performance issues to specific component in distributed environment.

Support for RSA Adaptive Authentication version 7.1. RSA Access Manager Server 6.2 SP1 supports integration with RSA Adaptive Authentication version 7.1.

Safari Browser Support. RSA Access Manager Server 6.2 SP1 supports Safari browser across Mac platform.

Support for Red Hat Enterprise Linux 6.3 (x86-64 bit) platform. RSA Access Manager Server 6.2 SP1 supports Red Hat Enterprise Linux 6.3 (x86-64 bit) platform.

Support for Oracle Directory Server 11.1.1.7.0 datastore. RSA Access Manager Server 6.2 SP1 supports Oracle Directory server 11.1.1.7.0 datastore.

Supported Platforms From Previous Releases

RSA Access Manager supports the following platforms.

- Microsoft Windows Server 2008 SP2 (x86)
- Microsoft Windows Server 2008 SP2 (x86-64 bit)
- Microsoft Windows Server 2008 R2 SP1 (x86-64 bit)
- Red Hat Enterprise Linux 5.0 (x86-64 bit)
- Red Hat Enterprise Linux 6.0 (x86-64 bit)

- Red Hat Enterprise Linux 5.5 Enterprise Server (x86-64 bit)
- Red Hat Enterprise Linux 5.5 Enterprise Server (x86)
- SUSE Linux Enterprise Server 10 (x86-64 bit)
- SUSE Linux Enterprise Server 11 (x86-64 bit)
- IBM AIX 6.1 PowerPC
- Oracle Solaris 11 (SPARC-64)
- Oracle Solaris 10 (SPARC-64)
- VMware vSphere 5.x

Supported Browsers for Self-Service Console and Admin Console

- Mozilla Firefox
- Microsoft Internet Explorer version 8 and 9
- Google Chrome
- Safari 6.0.5

Deprecated Components

The Distributed Credential Protection (DCP) authentication type is no longer supported. As a result, you must remove the following files:

- checkdcpconfig.bat file from AXM_HOME/bin directory
- dcp.conf file from AXM_HOME/conf directory

Following parameters are obsolete:

- cleartrust.dcp.configuration.file
- cleartrust.data.ldap.user.attributemap.dcppassword
- cleartrust.data.ldap.user.attributemap.dcppasswordhistory
- cleartrust.data.sql.user.attributemap.dcppassword

Fixed Issues

This section lists the issues that are fixed in this release under following sub-sections:

- Fixed Issues in RSA Access Manager 6.2 SP1 Release
- Hot fixes rolled up in RSA Access Manager 6.2 SP1 Release
- New Enhancements in RSA Access Manager 6.2 SP1 Release

Fixed Issues in RSA Access Manager 6.2 SP1 Release

Issue Number	Description
CTSRV-6090	Impersonation is allowed only for Administrator user when creating token.
CTSRV-6082	When ADAM is installed, the Group Entitlements settings gets disabled.
CTSRV-6072	Frequent intermittent outages in customer production environment.
CTSRV-6067	The RuntimeAPI WebServices WSDL file does not work with any current versions of Microsoft Visual Studios.
CTSRV-6065	Access Manager Instrumentation server log messages contains unknown message IDs and also does not contain any error details.
CTSRV-6063	OOBPHONE does not work with Access Manager server 6.2 and AAOP version 6.0.2.1 SP2 due to the changes done for OOBSMS.

Hot fixes rolled up in RSA Access Manager 6.2 SP1 Release

Issue Number	Hot Fix	Description
CTSRV-6064	6.1.0.01	SQLsequencehelper .java code contains defect.
CTSRV-6179	6.1.4.18	AxM - SQL connection manager issues when resultset is not released.
CTSRV-6006,CTSRV-6041, CTSRV-6059,CTSRV-6055	6.2.0.01	HF rollup which includes 6.1.4.10, 6.1.4.12, 6.1.4.13 along with the following case: • AAOP 6021 SP2 does not support OOBSMS.
CTSRV-4592, CTSRV-6078	6.1.4.16, 6.2.0.02	Group entitlements fails with ADAM
CTSRV-6049,CTSRV-6084	6.1.4.15, 6.2.0.03	Access Manager RuntimeAPI WebServices WSDL is incompatible with VS 2012.
CTSRV-6115	6.2.0.04	Cannot edit properties with new Administrative role which is created under a new Administrative Group 2.
CTSRV-6124, CTSRV-6152	6.2.0.05, 6.1.4.17	CPU usage in Access Manager 6.2 is much higher than that in Access Manager 6.0.
CTSRV-6156	6.2.0.06	User status does not get expired when password change and when **expire Now** button used in the same flow.
CTSRV-6162	6.2.0.07	Custom log4j appenders that worked with Access Manager 6.1 version does not work with Access Manager 6.2.
CTSRV-6168	6.2.0.08	LDAPException thrown while creating a group from admingui.
CTSRV-6174	6.2.0.09	session.hijacking=false causes expired session when you try to hit a page after logon.

New Enhancements in RSA Access Manager 6.2 SP1 Release

Issue Number	Description
CTSRV-6102	Redirect Access Manager Agent logs to centralized Access Manager log server.
CTSRV-6101	Require Access Manager Log server fail over capability.
CTSRV-5418	Require Access Manager debug facility to track response times of authentication and authorization requests

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted or referenced in detail. For many of the workarounds in this section, you must have administrative privileges. If you do not have the required privileges, contact your administrator.

Certificate Tool does not accept an underscore character.

Tracking Number: CTSRV-1743
Problem: When attempting to generate a keystore file, the certool prints the error message, “Error generating PKCS#12 file”. The Certificate Tool (certool) does not accept any certificate authority common name that includes an underscore character.
Workaround: None.

Runtime API TOKEN_ERRORs contains insufficient information.

Tracking Number: CTSRV-1745
Problem: If an API client program passes a broken token to the Runtime API, the API returns insufficient error details. The return values depend on the method called:

- IsUserInGroup() and getGroupsForUser() returns an empty map.
- createToken(), getTokenValue(), getTokenValues(), setTokenValue(), setTokenValues(), and validateToken() throws a sirrus.runtime.TokenException.
- All other methods of sirrus.runtime.RuntimeAPI, which take a user argument, return the map with a single entry: { "EXCEPTION_MESSAGE", "<SOME TOKEN ERROR MESSAGE>" }. These methods are authenticate(), authorize(), getUserProperty(), and getUserProperties().

Workaround: None.

Token problems can occur when running under Linux on VMware.

Tracking Number: CTSRV-2983
Problem: When running the Authorization Server under a Linux guest operating system on top of VMware, the RSA Access Manager token may not be updated as expected in response to Runtime API or Agent requests, even though the interval specified by .notouch_window has elapsed. This is due to a problem in VMware.
Workaround: For information, see this support page on the VMware web site.

Server side sorting is not supported for OpenDJ.

Tracking Number: CTSRV-5436
Problem: Server side sorting is not supported for OpenDJ. This is a limitation with SDK.
Workaround: None.

FIPS mode not supported for SecurID Authentication.

Tracking Number: CTSRV-5533
Problem: SecurID is not FIPS 140 compliant. For this reason, FIPS mode cannot be enabled for the Access Manager Server when SecurID authentication is configured.
Workaround: None.

Fix display of Breadcrumb Links on Admin GUI.

Tracking Number: CTSRV-5931
Problem: Breadcrumb links on Admin GUI pages needs to be changed as per UxD GTK standards
Workaround: None

In watcher list m/c Bind device option is displayed in the passcode page.

Tracking Number: CTSRV-6009
Problem: Remember me checkbox is displayed on the user's watcher machine list.
Workaround: None

uus.conf is added during upgrade to 6.2 even if Unique User Session is not configured in 6.1.

Tracking Number: CTSRV-6010
Problem: As per the expected behavior for upgrade, if Unique User Session is not configured in 6.1, the related conf file (uus.conf) should not be added to the conf folder in upgraded 6.2 servers.
Workaround: None

Special symbols appear in License agreement in the installers.

Tracking Number: CTSRV-6016
Problem: When you read through the license agreement in the installers, you will find some special symbols.
Workaround: None.

Apply Re-skinning to Online Help UI on the Access Manager Admin GUI.

Tracking Number: CTSRV-6022
Problem: The Online Help UI of Admin GUI does not have the same look-and-feel as the re-skinned UI.
Workaround: None

Invalid error message is displayed on the Access Manager Admin GUI.

Tracking Number: CTSRV-6154
Problem: When a user wants to logout while editing one of the following object (User, AdminGroup, User Group) an error message (Invalid session or request. please log on again) is displayed on the UI.
Workaround: User must navigate to non-edit page for above mentioned objects before opting to logout.

Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	www.rsa.com/support
RSA Secured Partner Solutions Directory	www.rsasecured.com

Trademarks