Novell Access Manager 3.1 SP2 IR3a Readme

December 04, 2010

Novell

This Readme describes the Novell Access Manager 3.1 SP2 IR3a release.

1 Documentation

The following sources provide information about Novell Access Manager:

- Documentation Web Site (http://www.novell.com/documentation/novellaccessmanager31/index.html)
- Access Manager Support (http://www.novell.com/support/microsites/microsite.do). For TIDs and Cool Solutions articles, select *Access Manager* for the *Product* and select *Articles / Tips* in the *Advanced Search* options.

2 Installing the Access Manager 3.1 SP2 IR3a Patch

Your system must be upgraded to 3.1 SP2 or 3.1 SP2 IR2 before applying this patch release. For version information, see Section 3, “Verifying Version Numbers,” on page 3.

The patch updates all Access Manager components. The files for the IR3a release can be downloaded from the Novell Downloads Web site (http://download.novell.com/index.jsp). This patch contains the following files:

Filename	Description
`AM_31_SP2_IR3a_IdentityServer_Linux32.tar.gz`	Contains the Linux Identity Server, the Linux Administration Console, the SSL VPN Server that is installed with an Embedded Service Provider, and the SSL VPN Server that must be protected by an Access Gateway.
`AM_31_SP2_IR3a_IdentityServer_Win32.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2003.

Filename	Description
AM_31_SP2_IR3a_IdentityServer_Win64.exe	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008.
AM_31_SP2_IR3a_AccessGatewayAppliance_Linux_SLES11.tar.gz	Contains the upgrade RPMs for the SLES 11 version of the Access Gateway Appliance and the SSL VPN Server that must be configured as a protected resource of the Access Gateway.
AM_31_SP2_IR3a_AccessGatewayAppliance_Linux_SLES9.tar.gz	Contains the upgrade RPMs for the SLES 9 version of the Access Gateway Appliance and the SSL VPN Server that must be configured as a protected resource of the Access Gateway.
AM_31_SP2_IR3a_AccessGatewayService_Win64.exe	Contains the Access Gateway Service for Windows Server 2008 with a 64-bit operating system.
AM_31_SP2_IR3a_AccessGatewayService_Linux64.bin	Contains the Access Gateway Service for SLES 11 with a 64-bit operating system.
AM_31_SP2_IR3a_ApplicationServerAgents_Windows.exe	Contains the J2EE Agents for Windows (JBoss, WebSphere, and WebLogic) and can only be used for installation.
AM_31_SP2_IR3a_ApplicationServerAgents_AIX.bin	Contains the J2EE Agents for AIX (WebSphere) and can only be used for installation.
AM_31_SP2_IR3a_ApplicationServerAgents_Linux.bin	Contains the J2EE Agents for Linux (JBoss, WebSphere, and WebLogic) and can only be used for installation.
AM_31_SP2_IR3a_ApplicationServerAgents_Solaris.bin	Contains the J2EE Agents for Solaris (WebLogic) and can only be used for installation.

For instructions on upgrading from 3.1 SP2 or 3.1 SP2 IR1 to 3.1 SP2 IR3a, see the following sections in the *Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html) and for instructions on installing the J2EE Agents, see the details in J2EE Agents Guide (http://www.novell.com/documentation/novellaccessmanager31/j2eeagents/data/b6vazq1.html)

- "Upgrading the Administration Console" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bh7s2b8.html)
- "Upgrading the Identity Server" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bh7s9jb.html)
- "Upgrading the Linux Access Gateway Appliance" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bbycmhz.html)
- "Upgrading the Access Gateway Service" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bl13nj2.html)

- "Upgrading SSL VPN Servers" (http://www.novell.com/documentation/novellaccessmanager31/sslvpn_serverguide/data/bhxr4ea.html)
- "Installing the J2EE Agents" (http://www.novell.com/documentation/novellaccessmanager31/j2eeagents/data/b6vazq1.html)

3 Verifying Version Numbers

The components of Access Manager 3.1 SP2 and its interim releases have the following version numbers:

Component	3.1 SP2	3.1 SP2 IR1	3.1 SP2 IR2	3.1 SP2 IR3	3.1 SP2 IR3a
Administration Console	3.1.2.281	3.1.2.310	3.1.2.328	3.1.2.345	3.1.2.347
Identity Server	3.1.2.281	3.1.2.310	3.1.2.328	3.1.2.345	3.1.2.347
Linux Access Gateway	3.1.2.281	3.1.2.310	3.1.2.328	3.1.2.345	3.1.2.347
Access Gateway Services	3.1.2.281	3.1.2.310	3.1.2.328	3.1.2.345	3.1.2.347
J2EE Agents (all versions, all platforms)	3.1.2.281	3.1.2.310	3.1.2.328	3.1.2.345	3.1.2.347
SSL VPN	3.1.2.281	3.1.2.310	3.1.2.328	3.1.2.345	3.1.2.347

4 Bugs Fixed

4.1 Bugs Fixed in 3.1 SP2 IR3a

Fixed an issue where the user was not able to view devices such as Access Gateway, SSLVPN or J2EE Agents on the Administration Console, when a new cluster is created. For more information, see TID 7007288 (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7007288&sliceId=1&docTypeID=DT_TID_1_1&dialogID=187968816&stateId=0%200%20187972132)

4.2 Bugs Fixed in 3.1 SP2 IR3

4.2.1 Administration Console

- Fixed an issue that caused slow logins because the certificate revocation list (CRL) was downloaded from the certificate authority (CA) but not added to cache for quick access.
- Fixed an issue that caused a silent upgrade or install to hang forever on a Linux primary Administration Console. [The script was waiting for the administrator's input, which was not visible on the install/upgrade screen].
- Fixed an issue related to import of newly installed Linux Access Gateway Appliance on existing Administration Console. Earlier the import was failing due to invalid JCC certificate.
- Fixed an issue related to auto generation of certificate.
- Fixed a null pointer exception error in iManager trying to display the Linux Access Gateway Appliance configuration.

4.2.2 Identity Server

- Fixed an issue with the Access Manager SAML Service Provider accepting SAML assertions that have recently expired. For more information on SAML assertions, see TID 7007213 (http://www.novell.com/support/viewContent.do?externalId=7007213&sliceId=1).
- Fixed an issue with the problem that was displayed in the production environment while installing the Access Manager components, by adding an Identity Server to the existing Identity Server cluster on different Windows 2003 Server.
- Fixed an issue with the session time extension in scenarios where users were inactive for certain period of time and becomes active again.

  After certain period of inactivity, the users may observe any one of the following symptoms:

  - Infinite redirects
  - 403 error messages appearing on their browsers
  - Asked for credentials

  The error message that is logged in the `ics_dyn`.log file is *"invalid-user: An error has occurred which may have invalidated your authentication"*.

4.2.3 Linux Access Gateway Appliance

- Fixed an issue where there is only one proxy service with SSL enabled, then No-Cache/No-store headers are not sent to the browser.
- Fixed an issue in scenarios with services having multiple cookie domains, and authentication service for non-authenticated domains which have failed, with some non-browser user agents. These user agents were encoding a *space* in the url to + symbol, which Linux Access Gateway Appliance was not handling.
- Fixed an issue with the Linux Access Gateway Appliance while sending a request to the origin server. The Linux Access Gateway Appliance adds a port component to the http host header, without having the port defined in *Web Server Host Name*.
- Fixed an issue where users are asked to authenticate again prematurely when session appears to, and should still be active. For more information see, TID 7007222 (http://www.novell.com/support/viewContent.do?externalId=7007222&sliceId=1).
- Fixed an issue with the Linux Access Gateway Appliance, which had few missing elements in the `config.xml` file. The missing elements resulted in looping after upgrading from 3.1.1 to 3.1.2.

4.2.4 SSL VPN

- Fixed an issue with the installation of SSL VPN server with more than 45 IP addresses.
- Fixed an issue with the openvpn component which fails to load after a configuration change is made and applied on the SLES11 Linux Access Gateway Appliance with on-box SSL VPN.

4.3 Bugs Fixed in 3.1 SP2 IR2

4.3.1 Administration Console

- An alert is now sent to the Audit Server in addition to the `app_sc log` file whenever the automatic certificate renewal fails.
- Fixed an issue related to the renewal of the expired SSL certificates which caused the Tomcat start command to fail and the Administration Console to become inaccessible.
- Fixed the `Invalid domain format` error that occurred when the Identity Server base URL started with a number.

4.3.2 Identity Server

- Fixed an issue with the CRL Distribution Point when the CRL is stored under the certificateRevocationList;binary attribute. This issue prevented the check from running on the LDAP server.
- Fixed an issue in mapping the ContextClassReference in Liberty and SAML 2.0 assertions to a local contract as specified in the Identity Server configuration. (In the Administration Console, click *Devices* > *Identity Servers* > *Edit* > *Local* > *Defaults*.)
- Fixed an ArrayIndexOutOfBound exception that occurred when validating certificates.
- Fixed an issue that injected a default target value for SAML 1.1 when requests came without a target value.

4.3.3 Linux Access Gateway Appliance

- Fixed an issue with the rewriter code that caused the Linux Access Gateway Appliance to crash.
- Fixed the random redirection errors on the Linux Access Gateway Appliance which caused user authentication to fail when opening a page that generated too many redirections.
- Fixed an issue that restarted or crashed the Linux Access Gateway Appliance when common or extended file logging was enabled.
- Fixed an issue that prevented access to the NetStorage WebDAV server from *My Computer* > *My Network Places* on a Windows XP machine.
- Fixed an issue that caused the NTPD service to stop functioning when configuration changes were applied to a Linux Access Gateway Appliance with multiple network cards.

4.3.4 Access Gateway Service

- Added a default log profile and a default log filter for the Access Gateway Service.
- Fixed issues with the HTML rewriter code.
- Fixed issues related to Form Fill and shared secrets.

4.3.5 J2EE Agents

- J2EE Agents is now supported on WebSphere 7.0.

4.4 Bugs Fixed in 3.1 SP2 IR1

4.4.1 Administration Console

- Fixed an upgrade issue that caused the Administration Console on a Windows Server 2008 to become inaccessible after upgrading from the evaluation version to the licensed version.

4.4.2 Identity Server

- Fixed an issue that caused logout to randomly fail when the Identity Servers were in a cluster.
- Fixed an issue that caused the Identity Server to send a request-denied response to users who were already logged in via a SAML 2 trusted relationship.
- You can now use 64-bit eDirectory with SecretStore as a remote SecretStore because the 64-bit SAML NMAS method is now available.

  If your eDirectory user store is running on SLES 11 64-bit operating system on x86-64 hardware, the eDirectory server is missing some support libraries that this SAML method requires. For information on installing these libraries, see TID 7006437 (http://www.novell.com/support/viewContent.do?externalId=7006437&sliceId=1).
- Fixed an upgrade issue so that users can change their passwords after you have upgraded from iChain to Novell Access Manager.
- Fixed a login looping issue when users access protected resources.
- Fixed an issue that prevented users who were accessing protected resources from receiving the error code with the `unable to authenticate` message.
- Fixed an issue that cause the Credential Profile to store an incorrect value for the cn field when Active Directory was used for the user store.

4.4.3 Linux Access Gateway Appliance

- Fixed an issue with the SLES 11 version of the Access Gateway Appliance that prevented users from downloading files when Gzip is enabled and the file is chunked and encoded.

- Fixed an issue that caused the Linux Access Gateway Appliance to crash after restarting the Access Gateway or the operating system after an upgrade.
- Fixed an issue that caused a `keystore missing` error message after migrating from SLES 9 to SLES 11.
- Fixed an issue that caused the round robin option for load balancing to unevenly distribute requests to Web servers, which can cause a Web server to become overloaded.
- In an Access Gateway cluster, a specific IP address can now be configured for SOAP back channel communication.
- Fixed an issue that caused an Identity Injection policy on a public resource to fail after a soft timeout because the Linux Access Gateway Appliance was not filling the authorization header.

4.4.4 Access Gateway Service

- Fixed an issue that prevented the rewriter from correctly rewriting URLs in a domain-based multi-homing service.
- Fixed an issue that caused segmentation errors when malformed requests were received.
- Fixed an issue with the Form Fill policy so that the hostname is included when the action element is empty.
- Fixed the format of Form Fill log event files for the Linux and Windows Access Gateway Service to be identical.
- Corrected the tooltip and the documentation for creating a log profile (click *Devices* > *Access Gateways* > *Edit* > *Logging* > *[Profile Name]*). When you set a value for the *Maximum Backup Files* option, a 0 (zero) value indicates that you do not want any backup files created and a blank value indicates that you want one backup file created.

4.4.5 Policies

- Fixed an issue with the Day of Week and the Current Date conditions of an Authorization policy that caused policy creation to fail.
- Fixed an issue that caused an Identity Injection policy with custom headers to incorrectly prepend cn to multi-valued attributes.
- When you create an Access Gateway Authorization policy with the Current Date condition, you need to specify the format of the Value field. Fixed an issue that prevented you from creating a policy with a format that used letters to specify the month.

5 Enhancements

In 3.1 SP2 IR3, the Identity Server now supports the following:

- Enhanced Access Manager auditing information to log IP addresses of the users that are failed to log in for NIDP authentications.
- Enhanced the passwordfetch method to work with Kerberos method assigned to an Active Directory user store.

6 Known Issues

For a list of issues that exist in SP2 see the "Access Manager 3.1 SP2 Readme" (http://www.novell.com/documentation/novellaccessmanager31/readme/accessmanager_readme.html).

6.1 Refreshing Policies in the Linux Access Gateway Appliance Displays javax.servlet.ServletException

The configured policies in the Linux Access Gateway Appliance when they are edited and refreshed, it displays javax.servlet.ServletException.

To workaround this issue, the administrator has to refresh the references from the policy page.

Go to *Administration Console* > *Policies* > *Refresh References*.

6.2 The Access Gateway Trust Store Corrupts When You Assign a Server to a Cluster or Remove it From a Cluster Multiple Times

Multiple time assigning and removing the server from/to a cluster might corrupt the Access Gateway trust store.

To workaround this issue, Trust store can be re-pushed from Troubleshooting > Certificate page.

1. Go to *Administration Console* >*Auditing* > *Troubleshooting* > *Certificates*.
2. Select the Trust Store Name checkbox that you want to re-push.
3. Click *Re-push Certificate* to re-push the selected trust store to the device.

6.3 When forceJRE is Enabled and Java is Not Installed, You Are Shown as Connected But Policies Displayed Are Not Effective

When you configure SSL VPN server to use forceJRE, it forces Internet Explorer to use Java applet to connect and download policies. Using Internet Explorer 8 browser, when you are connected to SSL VPN server from Windows7 machine, the policies are displayed but they are not effective.

To workaround this issue, disable forceJRE in the SSLVPN server configuration.

1. In the Administration Console, click *Devices* > *SSL VPNs* > *Edit*.
2. Select Client Policies from the policies section.
3. Disable *Force JRE for all Clients Using Internet Browser* checkbox.
4. To save your modifications, click *OK*, then click *Update* on the Configuration page.

6.4 Configuration Changes to the Linux Access Gateway Disrupts the SSL VPN Service

When you make configuration changes to the Linux Access Gateway, the IP forwarding is getting disabled and Onbox traditional SSL VPN stops communicating with resources.

NOTE: The Onbox indicates that the Linux Access Gateway Appliance, with SSL VPN on the same Appliance.

To re-enable IP forwarding, do the following:

Add this below one line to the script:

```
/chroot/lag/opt/novell/bin/postapply.sh

echo "1" > /proc/sys/net/ipv4/ip_forward
```

6.5 Access Gateway Service Fails to Process Some Configuration Changes

Some configuration changes such as deleting an authentication procedure can occasionally result in a state where the Access Gateway Service cannot process the configuration update. When this happens, the health turns red and a pending configuration file is never processed.

If you encounter this problem, contact Novell Support for a fix.

6.6 On Windows Server 2008, You Cannot Uninstall the Administration Console

When you install the Administration Console and the Identity Server on a Windows Server 2008 machine, you cannot completely uninstall the components with the uninstall program. The uninstall program hangs before it cleans up all the files and the registry entries.

To uninstall all Access Manager files and registry entries:

1. Run the uninstall program.

   The program removes most of the files.
2. When the program hangs, exit the program.
3. Delete the following directories:
   - `C:\Novell`
   - `C:\Program Files (x86)\Novell`
   - `C:\Program Files\Novell\Nsure Audit`
4. Run `regedit` and remove the following entries:
   - `\HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\AccessManager`
   - `\HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\NDS`
   - `\HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\nici_x64`
5. Restart the machine.

6.7 Under Heavy Load, the Access Gateway Service Generates Header and Connection Errors

When the option to make TCP connections persistent is enabled (which is the default) and the Access Gateway Service is under heavy load, the Access Gateway Service can run out of threads. When this happens, health checks are dropped and the Access Gateway Service machines are marked as down by the L4 switch. The default value for the *Keep Alive Interval* option (click *Devices* > *Access Gateways* > *Edit* > *[Name of Reverse Proxy]* > *TCP Listen Options*) is five minutes. Apache recommends 5 seconds.

To work around this issue, reduce the value of the *Keep Alive Interval*. The recommended value is five seconds.

7 Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the

Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

All third-party trademarks are the property of their respective owners.