Novell Access Manager 3.1 SP3 IR1 Readme

April 4, 2011

Novell®

This Readme describes the Novell Access Manager 3.1 SP3 IR1 release.

- Section 1, “Documentation,” on page 1
- Section 2, “Installing Access Manager 3.1 SP3,” on page 1
- Section 3, “Bugs Fixed in Access Manager 3.1 SP3,” on page 5
- Section 4, “Bugs Fixed in Access Manager 3.1 SP3 IR1,” on page 10
- Section 5, “Known Issues in Access Manager 3.1 SP3 IR1,” on page 11
- Section 6, “Legal Notices,” on page 16

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 *Articles / Tips* in the *Advanced Search* options.
- Novell Access Manager Product Site (http://www.novell.com/products/accessmanager/).

2 Installing Access Manager 3.1 SP3

- Section 2.1, “Installing or Upgrading the Purchased Product,” on page 1
- Section 2.2, “Downloading the J2EE Agents,” on page 4
- Section 2.3, “Installing the Evaluation Version,” on page 4
- Section 2.4, “Installing the High-Bandwidth SSL VPN Server,” on page 5

2.1 Installing or Upgrading the Purchased Product

After you have purchased Access Manager 3.1 SP3 or a previous release of Access Manager, log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download the software.

The following files are available:

Filename	Description
AM_31_SP3_IR1_IdentityServer_Linux32.tar.gz	
AM_31_SP3_IR1_IdentityServer_Linux32.iso	

Filename	Description
	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server. Can be used for installation and upgrade from 3.1 SP2 to 3.1 SP3 IR1, from 3.1 SP2 IR3 to 3.1 SP3 IR1, and from the evaluation version to the product version.
`AM_31_SP3_IR1_IdentityServer_Win32.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2003. Can be used for installation and upgrade from 3.1 SP2 to 3.1 SP3, from 3.1 SP2 IR3 to 3.1 SP3, and from the evaluation version to the product version.
`AM_31_SP3_IR1_IdentityServer_Win64.exe`	Contains the Windows Identity Server and Windows Administration Console for Windows Server 2008. Can be used for installation and upgrade.
`AM_31_SP3_IR1_AccessGatewayAppliance_Linux_SLES11.iso`	Contains the CD image for the SUSE Linux Enterprise Server (SLES) 11 version of the Access Gateway Appliance and the Traditional SSL VPN Server. Can be used only for installation.
`AM_31_SP3_IR1_AccessGatewayAppliance_Linux_SLES11.tar.gz`	Contains the upgrade RPMs for SLES 11 version of the Access Gateway Appliance and the Traditional SSL VPN server. Can be used for upgrade from 3.1 SP2 to 3.1 SP3, from 3.1 SP2 IR3 to 3.1 SP3, and from the evaluation version to the product version.
`AM_31_SP3_IR1_AccessGatewayService_Win64.exe`	Contains the Access Gateway Service for Windows Server 2008 R2 with a 64-bit operating system. Can be used for upgrade from 3.1 SP2 to 3.1 SP3, from 3.1 SP2 IR3 to 3.1 SP3, and from the evaluation version to the product version.
`AM_31_SP3_IR1_AccessGatewayService_Linux64.bin`	Contains the Access Gateway Service for SLES 11 with a 64-bit operating system. Can be used for upgrade from 3.1 SP2 to 3.1 SP3, from 3.1 SP2 IR3 to 3.1 SP3, and from the evaluation version to the product version.

For upgrade and installation information:

- “Upgrade Instructions” on page 3
- “Installation Instructions” on page 3
- “Verifying Version Numbers Before Upgrading” on page 3
- “Verifying Version Numbers After Upgrading” on page 4

2.1.1 Upgrade Instructions

For instructions on upgrading from 3.1 SP2 (or 3.1 SP2 IR3) to 3.1 SP3 IR1, see "Upgrading Access Manager Components" (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bg5gcwy.html) in the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html). To verify that your components are running 3.1 SP2 (or 3.1 SP2 IR3), see "Verifying Version Numbers Before Upgrading" on page 3.

Any Access Manager version prior to 3.1 SP2 should be first upgraded to 3.1 SP2 before upgrading to 3.1 SP3 IR1. For more information on upgrading to 3.1 SP2, see Upgrading from Access Manager 3.1 to 3.1 SP2 (http://www.novell.com/documentation/novellaccessmanager312/installation/data/bk0lvlm.html) and Upgrading from Access Manager 3.1 SP1 to 3.1 SP2 (http://www.novell.com/documentation/novellaccessmanager312/installation/data/bn6ajpt.html) in the *Novell Access Manager 3.1 SP2 Installation Guide* (http://www.novell.com/documentation/novellaccessmanager312/installation/data/bookinfo.html).

IMPORTANT: If you have installed a previous version of the Administration Console or the Identity Server on a machine that does not have at least 1 GB (Linux) or 1.2 GB (Windows) of memory, the upgrade to SP3 fails. The installation script checks for available memory and exits the upgrade if the machine does not have the minimum required memory.

2.1.2 Installation Instructions

For installation instructions for the Access Manager Administration Console, the Identity Server, the Access Gateway Appliance, the Access Gateway Service, and the SSL VPN server, see the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).

2.1.3 Verifying Version Numbers Before Upgrading

If you are upgrading from Access Manager 3.0, all components must be first upgraded to Access Manager 3.1 SP2 before upgrading to Access Manager 3.1 SP3 IR1.

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version.*
2. Examine the value of the *Version* field to see if it displays a 3.1 SP2 version that is eligible for upgrading to 3.1 SP3 IR1.

Component	3.1 SP2	3.1 SP2 IR3	3.1 SP3 IR1
Administration Console	3.1.2.281	3.1.2.347	3.1.3.269
Identity Server	3.1.2.281	3.1.2.347	3.1.3.269
Linux Access Gateway	3.1.2.281	3.1.2.347	3.1.3.269
Access Gateway Services	3.1.2.281	3.1.2.347	3.1.3.269
SSL VPN	3.1.2.281	3.1.2.347	3.1.3.269

2.1.4 Verifying Version Numbers After Upgrading

When you have finished upgrading your Access Manager components, verify that they have all been upgraded.

1. In the Administration Console, click *Access Manager* > *Auditing* > *Troubleshooting* > *Version*.
2. Examine the value of the *Version* field to verify that the component has been upgraded 3.1 SP3 IR1.

Component	3.1 SP3 IR1
Administration Console	3.1.3.269
Identity Server	3.1.3.269
Linux Access Gateway	3.1.3.269
Access Gateway Services	3.1.3.269
SSL VPN	3.1.3.269

2.2 Downloading the J2EE Agents

The J2EE Agents are a free download and are available from Novell Downloads (http://download.novell.com/index.jsp). The following files are available:

Filename	Description
`AM_31_SP3_IR1_ApplicationServerAgents_Windows.exe`	Contains the J2EE Agents for Windows (JBoss, WebSphere, and WebLogic) and can only be used for installation.
`AM_31_SP3_IR1_ApplicationServerAgents_AIX.bin`	Contains the J2EE Agents for AIX (WebSphere) and can only be used for installation.
`AM_31_SP3_IR1_ApplicationServerAgents_Linux.bin`	Contains the J2EE Agents for Linux (JBoss, WebSphere, and WebLogic) and can only be used for installation.
`AM_31_SP3_IR1_ApplicationServerAgents_Solaris.bin`	Contains the J2EE Agents for Solaris (WebLogic) and can only be used for installation.

For installation instructions, see *Novell Access Manager J2EE Agent Guide* (http://www.novell.com/documentation/novellaccessmanager31/j2eeagents/data/bookinfo.html).

NOTE: The upgrade is not supported for the J2EE agents.

2.3 Installing the Evaluation Version

To install an evaluation version of Access Manager 3.1 SP3 IR1, download the following files from Novell Downloads (http://download.novell.com/index.jsp). When the evaluation version is installed, it displays 3.1.3.269 for the version number.

Filename	Description
AM_31_SP3_IdentityServer_Linux32_Eval-1031.tar.gz AM_31_SP3_IdentityServer_Linux32_Eval-1031.iso	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server.
AM_31_SP3_IdentityServer_Win32_Eval-1031.exe	Contains the Windows Identity Server and Windows Administration Console.
AM_31_SP3_IdentityServer_Win64_Eval-1031.exe	Contains the Windows Identity Server and Windows Administration Console.
AM_31_SP3_AccessGatewayAppliance_Eval-1031.iso	Contains the Linux Identity Server, the Linux Administration Console, the ESP-enabled SSL VPN Server, and the Traditional SSL VPN Server.
AM_31_SP3_AccessGatewayService_Linux64_Eval-1031.bin	Contains the Linux Access Gateway Service.
AM_31_SP3_AccessGatewayAppliance_Win64_Eval-1031.exe	Contains the Windows Access Gateway Service.

For installation instructions, see the *Novell Access Manager Installation Guide* (http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).

2.4 Installing the High-Bandwidth SSL VPN Server

The key for the high-bandwidth SSL VPN server does not ship with the product because of export laws and restrictions. The high-bandwidth version does not have the connection and performance restrictions that are part of the version that ships with the product. Your regular Novell sales channel can determine if the export law allows you to order the high-bandwidth version at no extra cost.

After you have obtained authorization for the high-bandwidth version, log in to the Novell Customer Center (http://www.novell.com/center) and follow the link that allows you to download the high-bandwidth key.

3 Bugs Fixed in Access Manager 3.1 SP3

- Section 3.1, “Administration Console,” on page 6
- Section 3.2, “Identity Server,” on page 6
- Section 3.3, “Linux Access Gateway Appliance,” on page 7
- Section 3.4, “Access Gateway Service,” on page 9
- Section 3.5, “SSL VPN,” on page 9

3.1 Administration Console

Fixed an issue where unauthorized users could upload arbitary files without authentication on Windows Administration Console.

It is possible for an anonymous user to to use external scripts to upload arbitrary files without authentication on the Administration Console Windows platform.This issue is caused by the way the iManager server handles the path separators on Windows. This issue is not visible on the Administration Console Linux platform.

Fixed an issue with Administration Console XML validation errors.

Fixed an issue with Administration Console backup/restore by changing the value of the `ambkup.sh` file.

Fixed an issue that caused an Install error to be displayed when upgrading the Administration Console on the Windows platform.

Fixed an issue with password validation of the Novell Access Manager Administration Console, which was not starting after an SP2 upgrade. If users provide a wrong password for the Administration Console during the upgrade, it prompts for the correct password a maximum of three times and then the script terminates.

Fixed an issue with using the NSS library based on a CERT-In Advisory CIAD-2010-25 vulnerability. The Novell Access Manager has been updated with JDK 1.6.0_22-1 to resolve the issue.

Fixed an issue with Apache Tomcat transfer that resulted in an encoding header vulnerability. The Novell Access Manager Tomcat version 5.5.30 resolved this vulnerability issue.

Fixed an issue with the backup of the Administration Console configuration in Access Manager 3.1 SP2 IR1 on Windows 2008 R2 by adding a command to delete the backup file in a data backup action.

Fixed an XML validation issue with the Linux Access Gateway alert profile where check boxes were missing.

Novell Access Manager Administration Console now starts after the SP2 upgrade.

Fixed an issue that caused Access Managr SP3 upgrade to break the identity provider management through the user interface.

3.2 Identity Server

Fixed an issue with the Identity Servers Java process, which was displaying 6000% utilization every one or two days and forcing a reboot.

Roles in an assertion are now found properly in the Identity Provider instead of resulting in a 403 Forbidden error.

Fixed an issue with a custom LDAP server.

Fixed an issue with the Web.xml init parameter, which can be added to disable the question about whether a user consents to federate with a service provider.

Fixed an issue with an incorrect SAML AuthnResponse, which caused Identity Provider failure at user login.

Fixed an issue with Identity Provider session failover when there is no Access Gateway available in the setup.

Fixed an issue with passing query parameters while calling `/nesp/app/plogout`.

Fixed an issue with X509 CRL checks, which were failing because of the anonymous bind syntax.

The Identity Server now successfully re-imports after an upgrade.

Fixed a bug with SAML NMAS methods so the administrator can now install the SAML method to the secondary server by using command line instructions on SLES11 eDirectory to support libraries.

Access Manager now works in the NAT environment.

Fixed an issue with SAML AuthnRequest including certain types that were causing `AuthnContextClassRef` to return an invalid authentication type.

Fixed an issue with SAML 2.0 integration that required assertion time to be valid for 90 secs.

Fixed a stability issue that was caused because of SSL VPN upgrade to SP2.

Policy information can now be retrieved after upgrading from 3.1.1 to 3.1.2.

The Access Gateway Identity Injection Policy now works as expected.

Fixed the looping login issue.

Fixed the issue in which the IDP portal page displayed when the intersite transfer URL was accessed with a specific contact.

Fixed an issue with SP Brokering where a null pointer exception is generated when logging out from the target service provider

Fixed an issue where the relogin page did not pre-populate the user name in the user name field.

Fixed an issue with the SAML 1.1 post profile to include the assertion consumer URL within the “Recipient” tag.

Fixed an issue where intruder lockouts occur in a multiple replica environment when a user grace login count is less than number of LDAP replicas configured.

Fixed an issue where “There are no login connections are available. Please try again later” message is returned after entering the incorrect login credentials.

Fixed an “Array Index Out of Bounds” exception accessing an Access Gateway appliance protected resource after removing an IDP server from a 2 node cluster and applying update.

3.3 Linux Access Gateway Appliance

Fixed an issue with updating individual cluster members on an Access Gateway Service cluster.

Fixed an issue with downloads through the Linux Access Gateway slow down or freeze or result into broken files.

Enabled the rewrite inbound query string data to fix an issue with the rewriter rules that was creating loops when used in path-based multi-homing proxy services.

The Access Gateway Appliance is now adding a port to the host header in a Web server request.

The Access Gateway Appliance security channel update has the latest security patches.

Fixed an issue with Patch.pm errors while updating the Access Gateway Appliance patch channel using the SMT server.

Fixed an issue with the SLES 11 Access Gateway Appliance boot process which was delayed on initializing Network Interfaces reporting that was waiting for mandatory devices.

Fixed an issue with static routing entries which were not applied after the Access Gateway Appliance reboot. Based on the device manager configurations, every apply overwrites the configurations and you can add the `/chroot/lag/opt/novell/bin/postapply.sh` command to your requirements.

Changing authorization policies that are running on the Access Gateway Appliance now displays an alert for updating the Access Gateway Appliance.

Fixed an issue with error -649 when the server ran out of memory after creating 100+ roles. This issue is resolved by adding a schema and modifying the build.xml file.

All authorization policies are now applied to all the cluster members in an Appliance Gateway cluster.

Fixed an issue with passing query parameters while calling `/nesp/app/plogout` to logoutSuccess.jsp

Increased the number of IP addresses that can be assigned to the Access Gateway Appliance from 100 to 500.

Identity Injection now happens for requests to public resources after a soft time out with the Access Gateway Appliance.

Applying changes is now faster with the Access Gateway Appliance because an issue with restarting the loopback interface has been fixed.

Fixed an issue with `/var/novell/.Passwdmgmt` touch file. The Access Gateway Appliance no longer uses an old form fill policy cache even after changing the password at the password management service.

Fixed a DNS mismatch on the Access Gateway Appliance.

Fixed the form fill passed/failed event ID in Sentinel Log Manager.

Modified the rewriter configuration so the Access Gateway Appliance no longer crashes the rewriter multiple times a day.

Created a new PKCS#12 / KMO object that stores the trust chain and includes only the Entrust Cross Certificate, so the Access Gateway can provide cross-domain certificates that are available in a certificate root chain.].

Fixed an issue with Disabled the Session stickiness option so the failover policies are exercised properly on the Access Gateway Appliance when accessing protected resource from different clients.

Enhanced the style sheet to fix an issue with the non-redirected login enabled features

Fixed an Access Gateway appliance crash after applying configuration changes immediately after a purge cache when the high availability feature is enabled.

To workaround the JRE security vulnerability issue, see (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008129&sliceId=1&docTypeID=DT_TID_1_1&dialogID=216290409&stateId=0%200%20216288812) in the TID.

Fixed an issue with the Web server sending incorrect content length that caused the Access Gateway appliance to crash intermittently.

Fixed an issue when a user is not redirected to the password management servlet after authenticating to the identity provider server in an active directory environment.

Fixed a cross site scripting issue with the embedded service provider.

Fixed a potential ics_dyn gateway process restart issue which occured when the system configuration was applied.

Fixed an issue where 300101032 error generated processing a SAML assertion when “Assertion Validity Window” parameter is configured.

Fixed an issue with the Access Gateway appliance prompting for reauthentication when the password management touch file was enabled, despite the user having a valid session.

Fixed an issue where the Access Gateway appliance did not do a complete TLS handshake during the health check to the backend server.

Fixed a random Access Gateway appliance crash that caused while updating the configuration with a new protected resource when upgrading from 3.1.2 IR2 to 3.1.2 IR3.

Fixed an issue where the users could not access SAML Intersite transfer URL target parameter after upgrading to 3.1 SP3.

3.4 Access Gateway Service

Fixed an issue that caused the parent process to crash whenever one of the child process crashed in the Windows platform.

3.5 SSL VPN

Fixed an issue with the Internet Explorer security updates by manually entering the registry sub key.

Fixed an issue with SSL VPN authentication configuration settings by enhancing the stylesheet.

Fixed an issue with installing SSL VPN client on Windows 7 64-bit running IE.

Fixed an issue where users could not connect to the OpenVPN service when 60 static route entries were present on the SSL VPN server.

Fixed a DNS update issue with MAC Leopard, when the IP address configuration along with the DNS server entries are obtained from the DHCP server.

Fixed an issue with the MAC OS Java process hitting 100% CPU utilization immediately after connecting to the SSL VPN.

4 Bugs Fixed in Access Manager 3.1 SP3 IR1

- Section 4.1, “Administration Console,” on page 10
- Section 4.2, “Identity Server,” on page 10
- Section 4.3, “Linux Access Gateway Appliance,” on page 11
- Section 4.4, “Access Gateway Service,” on page 11
- Section 4.5, “SSL VPN,” on page 11

4.1 Administration Console

Fixed a PasswordMush exception issue while accessing the local identity provider in the user store.

4.2 Identity Server

Fixed an issue associated with SP Brokering where a null pointer exception is generated when logging out from the target service provider.

Fixed an issue where the login page did not pre-populate the username in the user name field after an initial login request failed.

Fixed an issue with the SAML 1.1 post profile to include the assertion consumer URL within the “Recipient” tag.

Fixed an issue where 300101032 error generated processing a SAML assertion when the “Assertion Validity Window” parameter is configured.

Fixed an issue where intruder lockouts occur in a multiple replica environment when a user grace login count is less than the number of LDAP replicas configured. 677587

Fixed an issue where “"There are no login connections available. Please try again later." message is returned to the user after entering incorrect credentials.

Fixed an “Array Index Out of Bounds” exception which occurred while accessing an Access Gateway appliance protected resource after removing an IDP server from a 2- node cluster and applying update.

Fixed an issue when a user is not redirected to the password management servlet after authenticating to the identity provider server in an active directory environment.

Fixed an issue where the users could not access SAML Intersite transfer URL target parameter after upgrading to 3.1 SP3.

Fixed an issue where the debug logs were being printed without enabling logging into the identity provider server.

Fixed an issue where the Tomcat version was displayed on the error pages.

Fixed a potential security vulnerability issue on the identity provider login page with the localized help file frames.

Fixed a 302 redirect issue in the “Relay State” which was URL encoded after consuming a SAML response. For more information, see “302 Redirect to 'RelayState' URL after consuming a SAML Response is being sent to an incorrect URL”

4.3 Linux Access Gateway Appliance

Fixed an Access Gateway appliance crash after applying the configuration changes immediately after a purge cache when the high availability feature is enabled.

Fixed an issue associated with the Access Gateway Appliance crashing in the rewriter by changing the configuration. The rewriter configuration now works as expected with vmc restarts that are related to the Purge Cache command.

Fixed a cross site scripting issue with the embedded service provider.

Fixed a potential ics_dyn gateway process restart issue, which occurred when the system configuration was applied.

Fixed an issue associated with the Access Gateway appliance that occured when sending duplicate range requests to the backend server.

Fixed an issue with the Access Gateway appliance prompting for reauthentication when the password management touch file was enabled, despite the user running a valid session.

Fixed an issue where the Access Gateway appliance did not do a complete TLS handshake during the health check to the backend server.

Fixed a random Access Gateway appliance crash that caused while updating the configuration with a new protected resource when upgrading from 3.1.2 IR2 to 3.1.2 IR3.

Fixed an issue where the SAML authorization response did not include the authorization request when authentication to the identity server fails.

4.4 Access Gateway Service

Fixed an issue that caused the parent process to crash whenever one of the child processes crashed in the Windows platform.

4.5 SSL VPN

Fixed an issue where users could not connect to the OpenVPN service when 60 static route entries were present on the SSL VPN server.

Fixed a DNS update issue with MAC Leopard, when the IP address configuration along with the DNS server entries are obtained from the DHCP server.

Fixed an issue with the MAC OS java process hitting 100% CPU utilisation immediately after connecting to the SSL VPN.

5 Known Issues in Access Manager 3.1 SP3 IR1

- Section 5.1, “The Access Gateway Service Reimport Screen on SLES 11 Displays Only the 127.0.0.2 Address,” on page 12
- Section 5.2, “The Brokering OR Condition Rules Are Not Updated,” on page 12
- Section 5.3, “Stopping the naudit Service Subsequently Stops JCC and Tomcat Services,” on page 13
- Section 5.4, “Upgrading NTPD Running on SLES 10 and SLES 11,” on page 13

- Section 5.5, “The Access Gateway Service Performance Drops by 90% When the Audit Server Is Not Reachable,” on page 13
- Section 5.6, “The SP Brokering Functionality Does Not Work with Shibboleth IDP as the Origin IDP,” on page 13
- Section 5.7, “Error while Upgrading the Administration Console from Accss Manager 3.1.2 IR3 to 3.1.3,” on page 13
- Section 5.8, “J2EE Agents Deny New Authentication Because of Low System Memory,” on page 14
- Section 5.9, “Error while Downloading Logs through the Administration Console on Windows,” on page 14
- Section 5.10, “Authentication Error If the Overwrite Real User/Overwrite Temporary User Option Is Enabled,” on page 14
- Section 5.11, “Access Manager Identity Server Installation Issues on Windows 2003 R2 32-Bit Enterprise Edition French OS,” on page 14
- Section 5.12, “The Applet and ActiveX Versions Do Not Match the Build Number,” on page 15
- Section 5.13, “On Windows, openVPN Fails to Download the Traffic Policies to a Destination Having a Subnet Mask,” on page 15
- Section 5.14, “The SSL VPN Causes a Windows Explorer Crash in Kiosk Mode,” on page 15
- Section 5.15, “On SLES Platforms, the Administration Console Installation Takes Approximately 45 Minutes to Complete,” on page 15
- Section 5.16, “Vulnerability Issues in JRE Security,” on page 15
- Section 5.17, “Lotus iNotes Issues,” on page 15
- Section 5.18, “Service Unavailability Caused by a SLES 11 Issue,” on page 16
- Section 5.19, “DNS Resolution using DNS Servers pushed from SSL VPN fails on Mac Leopard,” on page 16

5.1 The Access Gateway Service Reimport Screen on SLES 11 Displays Only the 127.0.0.2 Address

The `./conf/reimport_ags.sh` script imports the Access Gateway device to the device manager. In this process, the script displays only the 127.0.0.2 IP address instead of displaying the Access Gateway device static IP, so the import of device to device manager fails.

To work around this issue, modify the file `/etc/hosts` to have the host entry with actual IP address come before the entry associated with the IP address 127.0.0.2. This should be done before running the import.

For more information on this Java API error, see Bug 4665037 (http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4665037).

5.2 The Brokering OR Condition Rules Are Not Updated

When you initially use the Brokering tab to create rules for role conditions first time, the rules display correctly. However, if you modify the existing role with OR conditions, it is not updated or displayed correctly.

To work around this issue, delete existing role condition and re-create a new role condition.

5.3 Stopping the naudit Service Subsequently Stops JCC and Tomcat Services

Sometimes when the naudit service is stopped by using `/etc/init.d/novell-naudit stop` command, other important services such as Tomcat and JCC also stop, which causes interruption of services.

To work around this issue, manually restart the Tomcat and JCC services.

5.4 Upgrading NTPD Running on SLES 10 and SLES 11

A Nessus scan against Access Manager components installed on SLES 10 and SLES 11 reports that the version of ntpd running on these hosts have a denial of service vulnerability.

To work around this issue, upgrade ntpd to 4.2.4p8 or later.

NOTE: Ntpd version 4.2.0a is used on SLES 10 and ntpd version 4.2.4p6 is used on SLES 11.

5.5 The Access Gateway Service Performance Drops by 90% When the Audit Server Is Not Reachable

In the Access Gateway service, caching is disabled by default. When the Sentinel Log Manager is down, the logging API tries to connect to it for each request.

To work around this issue, do one of the following:

- Enable the Access Gateway service caching by changing the `<param name="EnableCaching" value="false"/>` to `<param name="EnableCaching" value="true"/>` in the `/etc/opt/novell/amlogging/config/log4j.xml` file.
- Force the Sentinel Log Manager audit server to cache all events by setting the LogForceCaching=Y in the `/etc/logevent.conf` file.

5.6 The SP Brokering Functionality Does Not Work with Shibboleth IDP as the Origin IDP

If you try to access the Brokering URL after configuring an SP Brokering group with the Shibboleth Identity Provider, it fails to access the target application.

5.7 Error while Upgrading the Administration Console from Accss Manager 3.1.2 IR3 to 3.1.3

The Administration Console upgrade is successful, but an error message is logged in the `upgr_edir.log` file.

It is safe to ignore the error message.

5.8 J2EE Agents Deny New Authentication Because of Low System Memory

New authentications are denied because of low system memory.

To work around this issue, add memory to the machine or click the *Update from server* option for the respective agent until the threshold value reaches zero.

5.9 Error while Downloading Logs through the Administration Console on Windows

Downloading logs through the Administration Console displays the following error message:

```
"There were logs that failed to download."
```

To work around this issue, specify the correct log file name from the UI, then download it from the Admininstration Console.

5.10 Authentication Error If the Overwrite Real User/Overwrite Temporary User Option Is Enabled

If you have two contracts, and the *Overwrite Real User* option is enabled for one of them, the first user authentication does not overwrite the second user authentication. It displays the following error message:

```
"Unable to authenticate. (409-esp-7271673232708786)."
```

This issue is not observed with the Linux Access Gateway.

5.11 Access Manager Identity Server Installation Issues on Windows 2003 R2 32-Bit Enterprise Edition French OS

The installation completes successfully without errors. When you restart the system, the Tomcat service fails to start. If only the Administration Console is installed, no logs are generated. If the Identity Server is installed, the `jakarta_service_aaammdd.log` file reports errors.

To work around this issue,

1. Start Tomcat in both the Administration Console and the Identity Server installation.
2. Use regedit to go to the following keys:

   ```
   \HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Fundation\Procrun
   2.0\Tomcat5\Parameters\Java\JvmMs
   ```

   ```
   \HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Fundation\Procrun
   2.0\Tomcat5\Parameters\Java\JvmMx
   ```
3. Change the decimal value of the keys to 512 from 1024. This allows the Tomcat service to successfully start.
4. Reduce the amount of RAM below 4 GB, then restart the server.

   This allows JCC to start successfully. If Tomcat is already started, the registration process automatically displays the Identity Servers in the Admin Console.

5.12 The Applet and ActiveX Versions Do Not Match the Build Number

It is safe to ignore the different version numbers.

5.13 On Windows, openVPN Fails to Download the Traffic Policies to a Destination Having a Subnet Mask

This issue occurs only when a traffic policy has a destination with a subnet mask. If the traffic policy has only one host and no destination with a subnet mask, it works as expected. This issue is not observed with the default policies.

This issue has not been observed while using Java.

5.14 The SSL VPN Causes a Windows Explorer Crash in Kiosk Mode

On Windows XP, the SSL VPN client works properly in Enterprise mode, but crashes Windows Explorer using ActiveX.

If you restore/downgrade the Windows XP client to Windows XP SP3, the SSL VPN client works properly in Kiosk mode.

This issue is not observed with Firefox using Java.

5.15 On SLES Platforms, the Administration Console Installation Takes Approximately 45 Minutes to Complete

5.16 Vulnerability Issues in JRE Security

To workaround the JRE security vulnerability issue, see (http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7008129&sliceId=1&docTypeID=DT_TID_1_1&dialogID=216290409&stateId=0%200%20216288812) in the TID.

5.17 Lotus iNotes Issues

- "Lotus iNotes Prompts for Authentication" on page 15
- "On Linux, Refreshing Lotus iNotes Mail boxes Prompts for Authentication" on page 16
- "Error while Accessing Lotus iNotes through Multiple Access Gateways on Linux" on page 16

5.17.1 Lotus iNotes Prompts for Authentication

If you access Lotus iNotes through the Access Gateway service with domain-based multihoming, it prompts for authentication for most operations.

Authentication is not required for these operations in path-based multihoming.

5.17.2 On Linux, Refreshing Lotus iNotes Mail boxes Prompts for Authentication

In Lotus iNotes, if more than one mail boxes is active, every refresh of a mailbox prompts for authentication when path-based multihoming is enabled with the *remove path on fill* option.

Authentication is not required for these operations in domain-based and path-based multihoming.

5.17.3 Error while Accessing Lotus iNotes through Multiple Access Gateways on Linux

You cannot perform any operation on Lotus iNotes through the multiple Access Gateways when path-based multihoming is enabled with the *remove path* option. The following error message is displayed:

```
"Ä problem has occured which may have caused the current operation to fail."
```

These operations work properly in domain-based and path-based multihoming.

5.18 Service Unavailability Caused by a SLES 11 Issue

Because of an issue, the operating system returns the 27.0.0.2 entry when the hostname is resolved. This causes the 127.0.0.2 to be the default address of the listener when the device is added to the cluster.

To workaround this issue:

1. Go to the proxy service page. Change the listening IP address to the other cluster member, then select the correct IP address again.
2. Click *Update* to save the changes.
3. Verify the correct address and add the device to the cluster.

IMPORTANT: Do not refer to the deployment senarios in the context sensitive help available with the Access Manager 3.1.3 build. Refer to this information in the Identity Server Guide.

5.19 DNS Resolution using DNS Servers pushed from SSL VPN fails on Mac Leopard

If the IP address and DNS servers are configured statically on MAC Leopard and a successful SSL VPN connection is established from it, then the DNS resolution fails to use the DNS server IP address pushed from the SSL VPN server.

6 Legal Notices

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/).

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