Access Manager Appliance 4.5 Service Pack 3 Hotfix 1 Release Notes

December 2020

Access Manager Appliance 4.5 Service Pack 3 Hotfix 1 (4.5.3.1) supersedes Access Manager Appliance 4.5.3.

For the list of software fixes and enhancements in the previous release, see Access Manager Appliance 4.5 Service Pack 3 Release Notes (https://www.netiq.com/documentation/access-manager-45-appliance/accessmanager453-release-notes/data/accessmanager453-release-notes.html#).

For information about Access Manager support lifecycle, see the Product Support Lifecycle page.

If you have suggestions for documentation improvements, click **Comment on this topic** at the top or bottom of the specific page in the HTML version of the documentation posted at the Documentation (https://www.netiq.com/documentation/access-manager/) page.

What's New?

This release includes the following enhancements:

Enhanced Analytics Dashboard

This release introduces a significantly enhanced Analytics Dashboard built on top of the latest Elasticsearch, Logstash, and Kibana (ELK) components. The Dashboard offers significant advantages over the previous versions, including a smaller footprint, better manageability, ease of upgrade, and maintenance.

The following are some of the significant updates included in this release:

- Significantly reduced hardware requirements:

For the demonstration purpose	For a production environment
• CPU: 2 Cores • Memory: 4 GB • Hard disk: 50 GB	• CPU: 4 Cores • Memory: 16 GB

- Built on top of the latest ELK stack and uses most of the Kibana functions including search, visualizations, custom graphs, and more.
- Built-in geo-location identification.
- An option to create a custom dashboard using the existing data.
- Customized view of the graphs.
- Significant performance improvement. Supports 600 logins/sec.
- Enhanced security with updated libraries.
- Flexibility to install on SLES and RHEL.
- Clustering for high availability.
- Does not depend on Sentinel for the storage and processing of events.

  NOTE: Access Manager still supports sending the Audit events to Sentinel, which works as an independent SIEM system.

For more information, see Analytics Dashboard in the "*NetIQ Access Manager Appliance 4.5 Administration Guide*".

Before installing the new Analytics Dashboard, ensure to delete Analytics Server nodes of the earlier version from Administration Console.

The latest version is independent of the SIEM server and uses logstash that acts as the aggregator and replaces the Analytic Server aggregator. The events are processed by ELK. Therefore, reports and offline Analytics Dashboard are not supported, and the existing events cannot be migrated.

However, you can use the new Analytics Dashboard along with the earlier Sentinel-based Analytics Dashboard for events to be captured in both until all the data become available in the new dashboard. For this, you need to configure two target servers, one for the old and one for the new Analytics Dashboard. For more information, see Setting Up Logging Server and Console Events.

However, you cannot launch the old Analytics Dashboard and reports from Administration Console. Instead, you can access the old data using the following direct access links:

- **Dashboard:** `https://<Analytics IP>:8445/amdashboard/login`
- **Reports:** `https://<Analytics IP>:8443/sentinel`

Support to Choose the OAuth Attribute Type

This release introduces a new property, OAUTH_CLAIMS_TO_USE_LDAP_ATTR_FORMAT, to configure the OAuth Claims data type according to the LDAP attributes' schema data type. When you configure this property, and the LDAP attribute data type is single-valued, the claims data is returned as a string. If the LDAP attribute data type is multi-valued, the claims data is returned as a string array irrespective of the value count.

By default, this option is not configured in Access Manager 4.5 Service Pack 3 Hotfix 1. Hence, if the LDAP attribute data type is single-valued, the claims data is returned as a string. If the LDAP attribute data type is multi-valued but contains only one value, the claims data is returned as a string. However, if it has more than one value, the claims data is returned as a string array.

For more information about this property, see Configuring Identity Server Global Options in the "*NetIQ Access Manager Appliance 4.5 Administration Guide*".

Software Fixes

This release includes the following software fixes:

Component	Bug ID	Issue
NIDS-OAuth2.0	273176	OAuth and OpenID Connect client applications fail after upgrading to Access Manager 4.5 Service Pack 3. This issue occurs because Access Manager 4.5 Service Pack 3 fixes the inconsistent handling of OAuth attributes by sending the single value attribute as a string and multiple value attributes as an array. However, this approach breaks several existing client applications. **NOTE:** To continue with the same behavior as Access Manager 4.5 Service Pack 3, set the OAUTH_CLAIMS_TO_USE_LDAP_ATTR_FORMAT property to true. See "Support to Choose the OAuth Attribute Type" on page 3.
Administration Console	273010	Administration Console can hang or become unresponsive while modifying a SAML 2.0 account management application. This issue occurs when a large number of users are part of LDAP user stores.

Verifying Version Numbers Before Upgrading to 4.5.3.1

To ensure that you have the Access Manager 4.5.3 files before upgrading to Access Manager 4.5.3.1, verify the existing Access Manager version by clicking **Troubleshooting > Version**.

Upgrading to Access Manager 4.5.3.1

IMPORTANT: In a cluster setup, ensure that you install the hotfix on each node of the Access Manager setup.

- "Downloading the Hotfix" on page 4
- "Upgrading to Access Manager 4.5.3.1 on Linux" on page 4
- "Silent Hotfix Upgrade on Linux" on page 5
- "Managing Hotfix" on page 5

Downloading the Hotfix

The hotfix helps in upgrading to the latest Access Manager with ease.

If you have multiple components installed on the same system, the hotfix installation process takes care of updating all the binaries of these components. For example, if you have both Identity Server and Administration Console installed on a system, installing the hotfix takes care of updating the binaries of Identity Server and Administration Console.

IMPORTANT: Ensure that you are currently on Access Manager 4.5.3 before upgrading to Access Manager 4.5.3.1.

To download Access Manager Appliance 4.5.3.1, perform the following steps:

1 Go to NetIQ Downloads Page.

2 Under **Patches**, click **Search Patches**.

3 Specify `AM_4531.zip` in the search box and download the file.

4 Save the hotfix file to the server running Access Manager. If you have multiple servers in your set up, ensure that you copy this zip file to all the servers.

Upgrading to Access Manager 4.5.3.1 on Linux

You can upgrade to Access Manager 4.5.3.1 by using the proceeding steps. This requires few manual interventions to continue the upgrade process. If you do not require any manual intervention while upgrading to the hotfix, see "Silent Hotfix Upgrade on Linux" on page 5.

1 Extract the hotfix file by using the `unzip AM_4531.zip` command.

After extraction, the following files and folders are created in the `AM_4531` folder:

Table 1 Files and folders created in the AM_4531 folder after extracting the hotfix installer ZIP file

File/Folder Name	Description
`rpm`	Contains rpm files for the hotfix to run on a Linux server.
`installPtool.sh`	Script to install the hotfix and the hotfix tool on a Linux server.
`installPatch.sh`	Script to install the hotfix tool and the updated binaries on a Linux server.

2 Log in as the root user.

3 (Conditional) To automate the hotfix installation, perform the steps mentioned in "Silent Hotfix Upgrade on Linux" on page 5, else continue with Step 4.

4 Go to the location where you have extracted the hotfix files.

5 Run the `installPatch.sh` command.

This command installs the hotfix and the bundled binaries.

NOTE: To manage the Access Manager hotfix file, refer to "Managing Hotfix" on page 5.

If the hotfix is already installed, the installer exits with a message.

Silent Hotfix Upgrade on Linux

Perform the following steps to automate the installation of the hotfix:

1 Go to `/opt/novell/nam/patching/bin/` and add the following in the `patch` file:

-Dcom.netiq.nam.patching.enableautomation=true

This updates the patch file as following:

```
/opt/novell/java/bin/java -cp ../lib/*: \
-Dcom.netiq.nam.patching.enableautomation=true -
Djava.util.logging.config.file=logging.properties
com.netiq.nam.patching.PatchInstaller $@
```

2 Run the following command at `/opt/novell/nam/patching/bin/`:

```
./patch -i /<path where you extracted the hotfix>/AM_4531/AM_4531-20.patch
```

Managing Hotfix

1. After the hotfix is installed, go to the following folder:

   ```
   /opt/novell/nam/patching/bin
   ```

2. Use the following options to manage the Access Manager hotfix file:

Option	Description	Command on Linux server
-qa	Lists all installed hotfixes.	`patch -qa`
-q	Lists details of an installed hotfix.	`patch -q` Example: `patch -q HF1-20`
-i	Installs a hotfix. During installation of a hotfix, all running services are stopped temporarily. After a hotfix is installed, all services are restarted and details of the operation are written to log files.	`patch -i <location and hotfix name>` Example: `patch -i /opt/novell/nam/ Patches/AM_4531/AM_4531-20.patch`
-e	Removes an installed hotfix. The hotfix maintains content relationship among hotfixes. So, if you have installed hotfix 1 and hotfix 2, hotfix 1 cannot be removed without removing hotfix 2. This is because hotfix 2 contains details of hotfix 1 as well. During the hotfix process, all the running services are stopped temporarily.	`patch -e <hotfix name>` Example: `patch -e HF1-20`
-qpl	Lists details of a hotfix that is not installed. If you want to view the changes that are included in the hotfix file without installing it on your server, use this option	`patch -qpl <location and hotfix name>` Example: `patch -qpl /opt/novell/ nam/Patches/AM_4531/ AM_4531- 20.patch`

Option	Description	Command on Linux server
-v	Verifies integrity of a hotfix.	`patch –v <location and hotfix name>` Example: `patch –v /opt/novell/nam/ Patches/AM_4531/ AM_4531-20.patch`
-t	Verifies if services can be restored by the installer. Use this option to stop/start all services after the installation of hotfix.	`patch –t <location and hotfix name>` Example: `patch –t /opt/novell/nam/ Patches/AM_4531/ AM_4531-20.patch`

Verifying Version Numbers After Upgrading to 4.5.3.1

After upgrading to Access Manager 4.5.3.1, verify the version numbers of Administration Console, Identity Server, and Access Gateway. To verify the version numbers, perform the following steps:

1 In Administration Console Dashboard, click **Troubleshooting > Version**.

2 Verify that the **Version** fields display as follows:

Component	Version
Administration Console	4.5.3.1-20
Identity Server	4.5.3.1-20
Access Gateway	4.5.3.1-20

Installing Analytics Dashboard

You can only perform a fresh installation of Analytics Dashboard 4.5.3.1. Upgrading from a previous version of Analytics Dashboard is not supported.

After downloading the new Analytics Dashboard version with Access Manager 4.5.3.1, the following file is available:

Filename	Description
`AM_4531_50_AnalyticsDashboard.tar.gz`	Contains Analytics Dashboard .tar file for Linux.

For information about installing Analytics Dashboard, see Installing Analytics Server in the "*NetIQ Access Manager Appliance 4.5 Installation and Upgrade Guide*".

After installing or upgrading to Analytics Dashboard 4.5.3.1, verify the version number of Analytics Dashboard. To verify the version number, perform the following steps:

1 In Administration Console Dashboard, click **Troubleshooting > Version**.

2 Verify that the **Version** field display as follows:

Component	Version
Analytics Server	5.0.0.0.624

Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issue is currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

Token Validation at the OAuth Endpoint Fails

Issue: CORS request to OAuth endpoints fails if the CORS domain URLs are separated by a space after the comma.

For example, **Limit to:** `https://zoom.novell.com:8443, https://mgalloway24.lab.novell.com:8443`

Workaround: Remove the space between the URLs.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright © 2020 NetIQ Corporation, a Micro Focus company. All Rights Reserved.