NetIQ Privileged Account Manager 3.2 Patch Update 2 Release Notes

January 2018

NetIQ Privileged Account Manager 3.2 P2 includes few enhancements and resolves some of the previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Privileged Account Manager Community Support Forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click the comment icon on any page in the HTML version of the documentation posted at the Privileged Account Manager Documentation website. To download this product, see the NetIQ Downloads website.

1 What's New?

The following sections outlines the enhancements and issues resolved in this release:

1.1 OpenSSL Upgrade

OpenSSL library in Privileged Account Manager is upgraded to 1.0.2l to eliminate OpenSSL security vulnerabilities.

1.2 Enhanced Change Management Reports

The Change Management report is enhanced to provide the following additional information in the Change Report Data:

- Name of the Command Control object that is deleted. This helps you to identify the object that was deleted.
- All the attributes of the Command Control object before and after modification. This helps you to verify the values of the object after modification.

1.3 Enhanced Session Capture

The session capture feature now captures all the user activities such as, keystrokes and mouse clicks in the Command Control Keystroke reports. The user activities are logged in the form of screen shots and keystroke logs. This helps the administrator to track all the user activities in the RDP session. The Command Control Keystroke report captures all the keystrokes except the function keys.

1.4   Software Fixes

Privileged Account Manager 3.2 P2 includes software fixes for the following issues:

1.4.1   Privileged Account Manager User Authentication through Active Directory Fails with an Error

Issue: When there are large number of user objects in the AD domain, Privileged Account Manager user authentication through Active Directory (AD) fails with the error message `Warning, LDAP search failed, error 1 (Operations error)`.

Fix: Privileged Account Manager user authentication through AD is now successful. (`Bug 1054000`)

1.4.2   SSH Relay Fails If the Username Contains Special Characters

Fix: SSH Relay now accepts username with special characters such as, period (.), hyphen (-), and underscore (_). (`Bug 1052756`)

1.4.3   Command Control Report Displays SSH Relay Server Password

Fix: Command Control Reports now do not display SSH relay password. (`Bug 1045751`)

1.4.4   Error Message Is Not Displayed When Unauthorized Users Configure Syslog Server Connection

Issue: When an unauthorized user configures Syslog server connection, a success message is displayed even though the update fails. (`Bug 1047149`)

Fix: Error message is displayed when unauthorized users configure Syslog server connection.

1.4.5 Applications Hang When You Access Multiple Applications Simultaneously in an RDP Relay Session

Issue: When you access multiple applications simultaneously with the session and the video capture is enabled in an RDP session, the applications hang. This issue occurs only on Windows 7 and Windows 10. (`Bug 1047045`)

Fix: RDP relay session works successfully when accessing multiple applications in Windows 7 and Windows 10.

1.4.6 SQL Server Management Studio 2008 Crashes with an Error in an RDP Relay Session

Fix: SQL Server Management Studio 2008 does not crash in an RDP relay session. (`Bug 1055320`)

1.4.7 Video Audits of Multi-Display Setup Are Not Captured Properly

Issue: The video audits of the multi-display setup contains a black area instead of the extended display content when you connect or disconnect the extended display. (`Bug 1047047`)

Fix: Video audits of multi-display setup are now captured properly.

1.4.8 Reporting Console Does Not Display Any Error Message for Audit Failure

Issue: When there is an audit failure for the Direct RDP session due to incorrect Command Control policy, the Reporting Console does not display any error message. (`Bug 1057691`)

Fix: Reporting Console displays appropriate error messages for audit failure.

1.4.9 Privileged Session to Windows Is Unstable When the Color Depth of the Windows Machine Is Low

Issue: When the color depth of the target Windows machine is 256 colors or 8bpps, various applications on the Widows privileged session crashes. Due to the application crash, the session becomes unstable and screen shots and videos are not captured. (`Bug 1067386`)

Fix: Privileged Session to Windows machine with low color depth is now stable, and the screen shots and the videos are captured successfully.

1.4.10 Privileged Account Manager 3.2.0.1 Crashes Intermittently in Windows

Issue: Privileged Account Manager 3.2.0.1 crashes intermittently with the error `C0000005 ACCESS_VIOLATION` in Windows. (`Bug 1069254`)

Fix: Privileged Account Manager does not crash in Windows.

1.4.11 Privileged Account Manager Does Not Audit all the SQL Queries Executed in Oracle 12c

Privileged Account Manager audits all the SQL Queries executed in Oracle 12c. (`Bug 1069832`)

1.4.12 Linux or UNIX Privileged Shell Does Not Override the Group Privileges of the Logged In User

Issue: In Linux or UNIX Privileged Shell (`pcksh`), privileges of the logged in user is applied to the groups instead of the user configured in the Command Control Policy. (`Bug 1069799`)

Fix: In Linux or UNIX Privileged Shell, group privileges are assigned according to the user configuration in the Command Control Policy.

2 System Requirements

For information about hardware requirements, supported operating systems and browsers, and software requirements, see "Installation Requirements" in the *NetIQ Privileged Account Manager 3.2 Installation Guide*.

3 Installing the Patch Update

Privileged Account Manager supports two ways to install the patch update. You can use any of the following ways:

WARNING: When you install this patch update on versions less than 3.2, Privileged Account Manager agents and framework managers on Windows reboot automatically. This happens because some of the Windows components required by Privileged Account Manager are updated in this patch update. Therefore, plan for a system downtime before installing this patch update.

NOTE: When you are installing this patch update on Windows Server 2008 R2, ensure that the Windows server contains the security update 3033929 or any update that supersedes it. This security update is required to support SHA-2 signing and verification. For more information about the security update, see Rexec package offline after updating to 3.2.0.1 on Windows 2008 R2.

- ◆ You can configure your system to use the NetIQ Customer Center (NCC) and use the Package Manager to distribute the patch update. See Section 3.1, "Using the Package Manager with NCC," on page 5.
- ◆ You can download the patch update from the download site, install it on a local system, then use the Package Manager to distribute the patch update. See Section 3.2, "Using the Package Manager with a Local Server," on page 6.

NOTE: Privileged Account Manager 3.2 P2 is a cumulative update that also includes software fixes from 3.2 P1. Therefore, ensure that you install all the following packages.

- ◆ Command Control Manager (`cmdctrl`) 3.2.0.1
- ◆ Registry Manager (`registry`) 3.2.0.1
- ◆ SSH Relay Agent (`sshrelay`) 3.2.0.1
- ◆ Audit Manager (`audit`) 3.2.0.1
- ◆ Privileged Credential Manager (`prvcrdvlt`) 3.2.0.1
- ◆ Access Manager (`auth`) 3.2.0.1
- ◆ Reporting Console (`audit`) 3.2.0.1
- ◆ Administration Manager (`admin`) 3.2.0.2
- ◆ Agent console (`servers`) 3.2.0.2

- Database Monitoring Manager (`dbaudit`) 3.2.0.2
- Command Reporting Console (`report command`) 3.2.0.2
- Framework Patch (`spf`) 3.2.0.2
- Command Control Agent (`rexec`) 3.2.0.2

3.1 Using the Package Manager with NCC

1 Configure the Package Manager by using the Novell Update Server:

   1a Log in to the Framework Manager console.

   1b Click **Package Manager** > **Settings**.

   1c From the drop-down, select **Novell Update Server**.

   1d Configure the following fields:

     User name: Specify the user name that allows you to log in to the NetIQ Customer Center.

     Password: Specify the password that is associated with this account.

   1e To view the update server information, select **Advanced Settings**.

     - Select the **Packages** checkbox, the following URL is configured:

       `https://nu.novell.com:443/PUM/packages`

   1f Click **Finish**.

2 (Conditional) Configure the Package Manager by using the Local Package Manager:

   2a Log in to the Framework Manager console.

   2b Click **Package Manager** > **Settings**.

   2c From the drop-down, select **Local Package Manager**.

   2d Fill in the following fields:

     Host name: Specify the DNS name of the host.

     Port: Specify the communication port. The default is 29120.

     The Local Package Manager is a Framework host that has been configured to store the packages.

3 (Conditional) If you do not have the Framework patch loaded in your Package Manager:

   3a Click **Package Manager** on the home page of the console, then click **Add Packages**.

   3b Configure the **Package Filter** to display the packages you need.

     Platform: Select required platforms. Make sure you select **Cross Platform**, which displays the console packages that run on all platforms.

     Types: Select at least **Console, Module**, and **Patch**.

     Components: Select all of them: **Command Control**, **Framework**, and **Miscellaneous**.

   3c Select all the packages that are listed. Make sure you select the **Framework Patch**.

   3d Click **Next**, then click **Finish** when the packages have been successfully downloaded.

   3e To ensure that all packages are up-to-date, click **Check for Updates**.

   3f Select any packages that are listed.

   3g Click **Next**, then click **Finish** when the packages have been successfully downloaded.

4 Load the updates:

    4a In the Package Manager page, click **Check for Updates**.

    4b If updates are listed, select the packages, then click **Next**.

    4c After the patch update is loaded, click **Finish**.

5 To push the patch update to your host machines, continue with Section 3.3, "Installing the Patch Update on Host Machines," on page 7.

3.2   Using the Package Manager with a Local Server

1 Download the patch update manually:

    1a On the NetIQ Downloads site, select the **Basic Search** tab.

    1b On the right pane, select **Search Patches**.

    1c On the Patch Finder page, select **Privileged User Manager** from the list of products.

    1d Click **Search**, then click **Privileged Account Manager 3.2**.

        This displays the current patch update.

    1e Download **Privileged Account Manager 3.2 Patch Update 2.**

2 Extract and publish packages into the Framework:

    2a Copy the `netiq-npam-packages-3.2.0.2.tar.gz` file to any of the Privileged Account Manager machines.

    2b Extract `netiq-npam-packages-3.2.0.2.tar.gz` into a temporary location, for example, `/tmp/framework/` directory.

```
tar -xvf netiq-npam-packages-3.2.0.2.tar.gz
```

    2c Use the following command to publish the packages to the Package Manager:

        Replace *<admin>* with the name of your admin user.

        For Linux and UNIX platforms:

```
/opt/netiq/npum/sbin/unifi -u <admin> distrib publish -d /tmp/framework
```

NOTE: If you are using PUM 2.3.3 or earlier versions, run the following command:

```
/opt/novell/npum/sbin/unifi -u <admin> distrib publish -d /tmp/framework
```

        For Windows platforms:

```
c:\Program Files\netiq\npum\bin\unifi -u <admin> distrib publish -d
c:\tmp\framework
```

NOTE: If you are using PUM 2.3.3 or earlier versions, run the following command:

```
c:\Program Files\novell\npum\bin\unifi -u <admin> distrib publish -d
c:\tmp\framework
```

    2d When prompted, enter the name and password for the administrator.

3 To push the patch update to your host machines, continue with Section 3.3, "Installing the Patch Update on Host Machines," on page 7.

3.3 Installing the Patch Update on Host Machines

During the process of installing the packages through the Framework, you can create a backup of the existing packages that you are replacing. To create the backup, you need to leave the **Create backup** option enabled when installing the patch update. Then, if you want to remove the update, you can use the **Rollback Packages** option.

NOTE: Installing this patch update on Windows Client Operating Systems such as Windows 7, 8.1, or 10 fails with an error. To workaround this issue, see Section 4.8, "Package Update Fails with an Error in Windows Client Operating System," on page 9

You can choose to install the patch update on all hosts or on selected hosts.

1 Log in to the Framework Manager console.

2 (Conditional) If you want to install the patch update on all the hosts, perform the following:

    2a On the Home page, click **Hosts**.

    2b Select the root domain.

    2c In the left pane, select **Update Domain Packages**.

    2d Select the desired packages for the respective hosts.

    2e Click **Next**.

    2f Click **Finish**.

3 (Conditional) If you want to install the patch update on selected hosts, perform the following:

    3a Click **Hosts** > **Update Packages** on the home page of the console.

    3b Select the desired packages for the respective hosts.

    3c Click **Next**.

    3d Click **Finish**.

4 Reboot all the hosts on which you have installed this patch update.

4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

- Section 4.1, "Moving Multiple Objects Does Not Work," on page 8
- Section 4.2, "The Run as privileged user Option Is Not Displayed on a Windows 2012 Server," on page 8
- Section 4.3, "The Command Control Objects Are Not Displayed When Large Number of Objects Are Added Simultaneously," on page 8
- Section 4.4, "The Unregistered Hosts List Is Not Displayed," on page 8
- Section 4.5, "The Changes to the Syslog Settings Do Not Get Applied," on page 8
- Section 4.6, "Cannot Uninstall Privileged Account Manager 3.2 through Windows Add/Remove Programs," on page 8
- Section 4.7, "NPAM Service Commands Do Not Work in SUSE Linux Enterprise Server 12 or Later," on page 9

4.1 Moving Multiple Objects Does Not Work

Issue: Selecting and moving multiple objects by using the Shift/ Ctrl key does not work.

Workaround: To move multiple objects, you can use shift + select the required objects, or use **Select All**. (`Bug 915307`)

4.2 The Run as privileged user Option Is Not Displayed on a Windows 2012 Server

Issue: When you right-click **Start** on a Windows 2012 server, the **Run as privileged user** option does not get displayed. (`Bug 901032`)

Workaround: To workaround this issue, right-click an application in the folder where the application is installed to execute **Run as privileged user**.

4.3 The Command Control Objects Are Not Displayed When Large Number of Objects Are Added Simultaneously

Issue: When Command Control Objects are added simultaneously in large numbers, the objects do not appear in the console. This is an intermittent behavior. (`Bug 908307`)

Workaround: No Workaround.

4.4 The Unregistered Hosts List Is Not Displayed

Issue: In the **Administration** console, when you search for unregistered hosts by clicking **Hosts > List Unregistered Hosts > IP Range**, the `Failed to list unregistered agents` error is displayed. (`Bug 832747`)

Workaround: Ensure that when you install Agents, you register it with the Manager for Privileged Account Manager.

4.5 The Changes to the Syslog Settings Do Not Get Applied

Issue: In the **Reporting** console, when you save the changes to Syslog settings, such as **select SSL**, or **Allow Persistent Connections,** the changes are not applied. (`Bug 895993`)

Workaround: To workaround this issue, restart Privileged Account Manager.

4.6 Cannot Uninstall Privileged Account Manager 3.2 through Windows Add/Remove Programs

Issue: Uninstalling Privileged Account Manager 3.2 through Windows Add/Remove Programs displays an error. This issue occurs only when the Privileged Account Manager is upgraded to 3.2 using Privileged Account Manager 3.2 installer. (`Bug 1029461`)

Workaround: Uninstall Privileged Account Manager through command line or Privileged Account Manager 3.2 installer.

4.7 NPAM Service Commands Do Not Work in SUSE Linux Enterprise Server 12 or Later

Issue: The NPAM service commands such as start, stop, restart and status does not work in SUSE Linux Enterprise Server 12 or later. (`Bug 1041284`)

Workaround: To workaround this issue, perform one of the following:

- Reboot the system using the following command:

  `reboot`

  (or)

  `shutdown -r now`
- Kill and restart the NPAM process using the following command:

  `pkill unifid`

  `/etc/init.d/npum start`

After performing one of the preceding steps, you can verify the NPAM process status by executing the following command:

`/etc/init.d/npum status`

4.8 Package Update Fails with an Error in Windows Client Operating System

Issue: Package update in Windows 7, 8.1, or 10 fails with the message `Failed to copy PUMCredProv.dll. Ensure LogonUI.exe process is not running on the target host and try again.` (`Bug 1072645`)

Workaround: Perform the following on all the hosts in which you are updating the packages:

1. Disconnect all the RDP sessions to the host.
2. Log in to the console of the host.
3. Continue with the steps in the Section 3.3, "Installing the Patch Update on Host Machines," on page 7.

4.9 Performance Drop in Privileged Account Manager Monitored Windows System

Issue: System performance of Privileged Account Manager monitored Windows machine is slow when the video fps value is set to 10. This is apparent on Windows machine having a single CPU. (`Bug 1074472`)

Workaround: Click **Command Control > Video Settings** and set the value of **Video fps** to 5 or lower.

5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto: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 (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

6 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/.