NetIQ Cloud Manager 2.3 Patch 3 Release Notes

January 2015

Cloud Manager 2.3 Patch 3 (`NCM_2.3.0_Patch3.zip`) is a cumulative patch: all of the files needed to update the Cloud Manager Application Server 2.3 and the Cloud Manager Orchestration Server 3.3 (including Patch 1, Patch 2, and Patch 3) are included.

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

The documentation for this product is available on the NetIQ website in HTML and PDF formats. If you have suggestions for documentation improvements, click **Comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the NetIQ Cloud Manager 2.3 Documentation (https://www.netiq.com/documentation/cloudmanager23/) page.

1   Issues Fixed in Patch 1

The following bugs are fixed when you apply the files included Cloud Manager 2.3 Patch 1:

- Bug 876774: *cmMobile: Unable to create workload template - error: Missing Selection*.
- Adjustments for null pointer exception in IdentityContextManager.
- Adjustments to `ForceWorkflowCompletionCommand` command to attempt to clean up Business Service Requests and Change Requests that have no workflow.
- Enhanced workflow-related logging.
- Bug 861085 - *[FTF] NCM 2.2.0/2.2.2 Imported machine adding new NIC fails - Error No root disk found.*
- Fixed an issue with datastore search: Searching from the root directory rather than the subdirectory, which caused provisioning jobs to take a long time to complete.
- Fixed an issue with detecting a virtual machine's (VM's) VNC port configuration: Occasionally, vSphere reflected an empty string `""` as the value, causing a failure when casting an empty string to an integer. The fix added a check to make sure there is a value in the extra configuration port setting for a VM before trying to cast it to an integer.
- Formerly, the contents of the `.../config`, `.../console`, and `.../plugins` directories located on the Cloud Manager Application Server were accessible with a web browser, making those folder listings visible to users. This potential security issue was resolved by making those folders forbidden to browsing.

2 Issues Fixed in Patch 2

The following bugs are fixed when you apply the files included Cloud Manager 2.3 Patch 2:

- SR10907978361 - In some configured vSphere environments, customers would change a workload on the ESX server and that change would not be replicated in the vSphere Updater job in the Cloud Manager Orchestration Server. This could be manifest with errors such as `VM Tools Not Running`. The updater has been modified to function correctly after applying the Orchestration Server Patch.

  For further implementation details, see Enabling a Log Trace of Calls to the Orchestration Server REST Interface in this document.

- SR10918026811 - Formerly, running the **Business Service Cost Details** report without a start date parameter (the default) could stall the report builder. The report can now be generated without a start date.

- SR10918270071 - If you have multiple blocks in your IPAM with the same `NCMNetworkID` and then import a VM using that network into Cloud Manager, the VM could end up in a state where it has no association to its IPAM address, which would cause it to fetch a new IP address on a change request. The product now detects duplicate `NCMNetworkID` values and cleans them up.

  For further implementation details, see Recovering IPAM Configuration Data in this document.

- SR10919554851 - Formerly, email notifications were being sent only to the business service requester. With this patch, a Cloud Administrator can add a specific property to the `/opt/netiq/cloudmanager/etc/system.properties` file, any user with specified permission(s) on the business service receives an email notification.

  For further implementation details, see Enabling Email Notifications for Users with Specific Permissions in this document.

- SR10920711341 - A user (such as a Business Group Owner or Business Group Viewer) can now search for values in the Hostname field on the deployed workloads list.

- Bug 901327 - Formerly, if you were to select a deployed business service and then select **Change**, the Hostname field was not included in the list of workloads. The hostname field has now been added on the workload list for the Change operation.

3 Issues Fixed in Patch 3

The following bugs are fixed when you apply the files included Cloud Manager 2.3 Patch 3:

- Bug 908705 - *Bulk Import with internal IPAM not fully configured deletes VM after failed import*. The behavior for bulk import is now similar to a single import. If IPAM is not configured for a VM, the Cloud Manager Application Server reports the configuration error and creates a related delete task that will remove only the entry for the failed import from the workload. Approval of the task will not delete the referenced VM.

- SR 10911613451 - *NCM 2.3 problem with importing workload*. Formerly, some workload imports failed because of timeout issues. The import process was optimized to improve performance so that timeout issues are avoided.

- Bug 909533 - *Cloud Manager is vulnerable to POODLE (Padding Oracle On Downgraded Legacy Encryption)*. In this patch, Cloud Manager disabled the SSL v3 protocol in Java Jetty, thereby addressing the vulnerability to potential POODLE attacks. Some files must be modified manually. For more information, see Section 5.6, "Disabling SSL v3 in Java Jetty," on page 7.

For more information about POODLE, see Common Vulnerabilities and Exposures CVE-2014-3566 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566).

 ◆ Bug 912970 - *Unable to discover network settings for adapter configured with manual MAC address and uppercase letters* and SR #10926208931 - *Don't see network facts for an imported VM with manual MAC address configuration*. Formerly, after you imported a VMware VM with manual MAC address configuration that used uppercase letters, the Cloud Manager Orchestration Server did not find and report values for the VM's network settings (such as IP address, netmask, DNS, suffixes, and so on). Discovery now handles lowercase and uppercase letters in manual MAC addresses. The MAC address is case insensitive. It finds the network information and populates it for the Orchestration Server.

4 Applying the Orchestration Server Patch

The `cmos.zip` file found in `NCM_2.3.0_Patch3.zip` file is specifically for the Cloud Manager Orchestration Server 3.3. The file is a cumulative patch; that is, it contains *all* of the updated files for *every* patch that has been released to date. You apply all of the patch files to the Cloud Manager Orchestration Server 3.3.

4.1 Patch Installation Prerequisites

Ensure that the following prerequisites are met before you install this patch:

 ◆ Cloud Manager Orchestration Server 3.3 is installed, and is up and running.
 ◆ Extract the `cmos.zip` file from Cloud Manager 2.3 Patch 3 (`NCM_2.3.0_Patch3.zip`) and copy the following files to an accessible directory on the Cloud Manager Orchestration Server:
   ◆ `libvsphere.pylib` (fixes made in Patch 1 and in Patch 3)
   ◆ `vmprep.sar` (fixes made in Patch 1)
   ◆ `vi-client.jar` (fixes made in Patch 2)
   ◆ `vsphere.sar` (fixes made in Patch 2)

NOTE: If you have *never* applied a patch to the Cloud Manager Orchestration Server 3.3, you must apply all of the files listed above: if you applied Patch 1 or Patch 2, you need apply only the files for Patch 3.

4.2 Installing the Orchestration Server Patch Files

NOTE: If you see an incorrect FQDN on a workload after applying the files in this patch, you might need to rediscover the VMs.

4.2.1 Applying the `libvsphere.pylib` Patch File

To apply the `libvsphere.pylib` patch file to the Orchestration Server:

1 Copy `libvsphere.pylib` to the following location:

`/opt/novell/zenworks/zos/server/components/pylib/libvsphere.pylib`

2 In the Explorer Tree of the Orchestration Server console, expand the **Public JDL Libraries** container, right-click the **libvsphere** object, then select **Undeploy**.

3 Right-click the **Public JDL Libraries** container, select **Deploy**, then browse to the location of the new library (see Step 1 above):

`/opt/novell/zenworks/zos/server/components/pylib/libvsphere.pylib`

This redeploys the `libvsphere` library.

4.2.2 Applying the `vmprep.sar` Patch File

To apply the `vmprep.sar` patch file to the Orchestration Server:

1 Copy `vmprep.sar` to the following location:

`/opt/novell/zenworks/zos/server/components/jobs/vmprep.sar`

2 In the Explorer Tree of the Orchestration Server console, expand the **Jobs** container and then the **all** container, right-click the **vmprep** object, then select **Undeploy**.

3 Right-click the **all** container, select **Deploy**, then browse to the location of the new library (see Step 1 above):

`/opt/novell/zenworks/zos/server/components/jobs/vmprep.sar`

This redeploys the `vmprep` job.

4.2.3 Applying the `vi-client.jar` Patch File

To apply the `vi-client.jar` patch file to the Orchestration Server:

1 Copy `vi-client.jar` to the following location:

`/var/opt/novell/zenworks/zos/server/store/deployed/vsphere.sar-<jobid>/`
`vSphereUpdate.job/vi-client.jar`

2 Restart the `vSphereUpdate` scheduled job.

   2a In the Scheduler view of the Orchestration Server console, locate and select the `vSphereUpdate` scheduled job.

   2b On the **Job Arguments** page of the Job details section of the view, locate the **mode** field, ensure that the accompanying **Lock** check box is deselected, and type `stop` in the field.

   2c In the console toolbar, click the **Save** icon, in the Scheduler view click **Run Now**, then monitor the job progress.

   2d When the Job status shows **success**, delete the `stop` argument you previously entered in the **mode** field at Step 2b, then repeat Step 2c.

     This step ensures that the new `vi-client.jar` library you applied to the Orchestration Server is transferred to the Orchestration Agent running the `vSphereUpdate` job. The new library fixes the vSphere updater on the agent.

4.2.4 Applying the `vsphere.sar` Patch File

To apply the `vsphere.sar` patch file to the Orchestration Server:

1 Copy `vsphere.sar` to the following location:

`/opt/novell/zenworks/zos/server/components/jobs/vsphere.sar`

Copying the file ensures that the patched `vi-client.jar` is included in the vsphere job if it is ever re-deployed.

5 Running the Patch RPM on the Application Server

The `netiq-cloudmanager-2.3.0-188.noarch.rpm` file found in `NCM_2.3.0_Patch3.zip` is specifically for the Cloud Manager Application Server 2.3. The RPM is an installer program that applies cumulative patch files (that is, *all* of the updated `.jar` files for *every* patch that has been released to date) to the Cloud Manager Application Server 2.3.

This section includes the following information:

5.1 Patch Installation Prerequisites

Ensure that the following prerequisites are met before you run the RPM:

- Cloud Manager Application Server 2.3 is installed, and is up and running.
- Extract the `netiq-cloudmanager-2.3.0-188.noarch.rpm` file from the patch (`NCM_2.3.0_Patch3.zip`) and copy it to an accessible directory on the Cloud Manager Application Server.

  For example: `/tmp/ncm2.3_patch/netiq-cloudmanager-2.3.0-188.noarch.rpm`

5.2 Running the Patch RPM

After you have copied the patch file to the server, use the following steps to install the file:

1 From the location where you copied `netiq-cloudmanager-2.3.0-188.noarch.rpm`, run the following command:

` rpm -Uvh --nodeps netiq-cloudmanager-2.3.0-188.noarch.rpm`

2 Run the Cloud Manager configuration program from the following location:

`/opt/netiq/cloudmanager/configurator/config`

3 Choose to run an upgrade for the Cloud Manager Server.

4 Verify that the `netiq-cloudmanager-2.3.0-188.noarch.rpm` file is installed.

    4a Log in to the Cloud Manager Web Console.

    4b In the Web Console, click **Help > About**.

4c In the About box, verify the following:

- ◆ Server version is `2.3.0` and build number is `79.0.185`
- ◆ Web UI version is `2.3.0` dated `01/22/15`

5.3 Enabling a Log Trace of Calls to the Orchestration Server REST Interface

Cloud Manager 2.3 Patch 2 and later includes a Karaf command that surfaces the timings of calls to the REST interface of the Cloud Manager Orchestration Server.

The following command turns on a log trace for the elapsed time of all REST calls to the server:

```
karaf> log:set TRACE com.novell.cm.psoservice.impl
```

The following command resets the log level to default so these timing messages no longer appear in the log:

```
karaf> log:set INFO com.novell.cm.psoservice.impl
```

5.4 Recovering IPAM Configuration Data

Cloud Manager 2.3 Patch 2 and later includes a Karaf command that attempts to recover IPAM configuration data for all workloads whose IPAM configuration information has been cleared because more than one entry existed in IPAM for one network.

Run the following command from the Karaf shell:

```
cm:recover-ipam-releasedata
```

You can add the `-b` *business service ID* option to the command if you want to recover IPAM configuration data for all workloads in a business service. For more options for this command, use the `--help` option.

5.5 Enabling Email Notifications for Users with Specific Permissions

You can control the individuals who can receive email notification when a business service is deployed or a change request has completed if you add the `ncm.bs.deploy.perms` property to the `/opt/netiq/cloudmanager/etc/system.properties` file.

As you add this new property, you also need to add the permissions to be honored on the business service. Any user with those permissions will receive the email notifications. For example, if you wanted a user with `SYSTEM_SUPPORT` permission or `MODIFY_BS` or `VIEW_BS` permission to receive emails when the business service is being deployed or changed, you would modify the `/opt/netiq/cloudmanager/etc/system.properties` file like this:

```
...
...
ncm.bs.deploy.perms=SYSTEM_SUPPORT,MODIFY_BS,VIEW_BS
...
...
```

5.6   Disabling SSL v3 in Java Jetty

If SSL v3 is enabled for Java Jetty, you must disable it to prevent possible POODLE attacks. To make this change on your existing Cloud Manager Application Server, you must manually modify the `/opt/netiq/cloudmanager/deploy/jetty/etc/jetty.xml` file.

1 Navigate to the `/opt/netiq/cloudmanager/deploy/jetty/etc/jetty.xml` file and save a copy as `jetty-xml-OLD`.

2 Open the `jetty.xml` file in a text editor.

3 If SSL is enabled, the `jetty.xml` file contains a section that looks like the following. Delete this section from the file.

NOTE: You must remove the old section. Commenting it out can cause the configuration script to fail when you perform an upgrade.

```
<Call name="addConnector">
  <Arg>
    <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
      <Set name="Port">[SSL Port Number]</Set>
      <Set name="maxIdleTime">120000</Set>
      <Set name="keystore">
        <SystemProperty name="karaf.home" default="." />[Keystore File Name]
      </Set>
      <Set name="password">[Keystore Password]</Set>
      <Set name="keyPassword">[Key Password]</Set>
      <Set name="wantClientAuth">true</Set>
    </New>
  </Arg>
</Call>
```

4 Replace the old section of the `jetty.xml` file with the following:

```
<Call name="addConnector">
  <Arg>
    <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
      <Arg>
        <New class="org.eclipse.jetty.http.ssl.SslContextFactory">
          <Set name="keyStore">
            <SystemProperty name="karaf.home" default="." />[Keystore File Name]
          </Set>
          <Set name="keyStorePassword">[Keystore Password]</Set>
          <Set name="keyManagerPassword">[Key Password]</Set>
          <Set name="ExcludeProtocols">
            <Array type="java.lang.String">
              <Item>SSLv3</Item>
            </Array>
          </Set>
        </New>
      </Arg>
      <Set name="Port">[SSL Port Number]</Set>
      <Set name="maxIdleTime">120000</Set>
      <Set name="wantClientAuth">true</Set>
    </New>
  </Arg>
</Call>
```

5 Save the changes.

6 Verify that the SSL v3 protocol is disabled.

   ◆ The Cloud Manager secure URL (HTTPS) should be functional.

- ◆ There should be an entry in the log that shows that the SSLv3 protocol is not in the enabled protocol list. For example:

```
[12 Jan 2015 06:37:08] INFO  | g.ops4j.pax.web) | SslContextFactory   | 96
| Enabled Protocols [SSLv2Hello, TLSv1, TLSv1.1, TLSv1.2] of [SSLv2Hello,
SSLv3, TLSv1, TLSv1.1, TLSv1.2]
```

6 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.

7 Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.