NetIQ Cloud Manager 2.4 Release Notes

March 2015

NetIQ Cloud Manager 2.4 includes new features, improves usability, and resolves several 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 our products meet all your needs. You can post feedback in the NetIQ Cloud Manager discussion on *NetIQ Forums*, our community website that also includes product notifications, blogs, and product user groups.

The documentation for this release of the 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 Cloud Manager 2.4 Documentation (https://www.netiq.com/documentation/beta/cloud-manager-24) website.

Cloud Manage requires you to provide a license file during the installation of the Cloud Manager Orchestration Server. None of the Cloud Manager components functions properly without a licensed server installation. You can purchase a license from NetIQ Sales, or you can obtain an evaluation license for a free 90-day trial. The trial key controls the number of users and managed nodes you can configure, and sets an expiration date. After 90 days, you must purchase a license, or discontinue use of the product.

To purchase the product or to initiate a 90-day trial, contact an authorized NetIQ Sales representative at 888-323-6768, or go to the NetIQ Cloud Manager *How to Buy* (https://www.netiq.com/products/cloud-manager/how-to-buy/) web page. Your representative will send a purchased license key file or a trial key file for Cloud Manager to your account at the NetIQ Customer Center (https://www.netiq.com/customercenter). (If you do not have an eLogin account for the Customer Center, click here to create one.) From the Customer Center, save the file to a location that you can access during the Cloud Manager Orchestration Server installation.

1 What’s New?

Cloud Manager 2.4 includes the following new features and enhancements, as well as issues resolved in this release.

1.1 Supported Workflow Operating Systems

Cloud Manager 2.4 added support for the following operating systems for workloads:

CentOS 7
Red Hat Enterprise Linux 6.6
Red Hat Enterprise Linux 7
SUSE Linux Enterprise Server 12
Ubuntu 14.04

1.2 Security Improvements

Cloud Manager 2.4 disabled the SSL v3 protocol in Java Jetty, thereby addressing the vulnerability to potential POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks. Some files must be modified manually. For more information, see Section 5.4, “Disabling SSL v3 in Java Jetty,” on page 8. (Bug 909533)

For more information about POODLE, see Common Vulnerabilities and Exposures CVE-2014-3566.

1.3 Software Features and Enhancements

- Increases the maximum workload disk count to 20
- Provides the ability to retire a Zone, a Workload Template, or a Service Level
- Provides the ability to initiate the discovery of Hosts, Repositories, and Virtual Machines from the Zone dialog
- Provides the ability for line item discounts
- Provides the ability to hide costs on a per-user basis
- Provides the scheduled reboot list widget and respect for the time zone used for reboot
- Provides password optimizations, including a per Business Group password strength setting for workload admin passwords
- Includes the identity of the person who requests the Change Request in approval workflows and email notifications
- Provides the ability to generate a report that lists workloads
- Provides the ability to hide run once commands from end users
- Provides a preview of brokering for Amazon Web Services and SUSE Cloud

1.4 Software Fixes

Cloud Manager 2.4 includes software fixes that resolve the following issues:

- **Bug 913370 - Costs hidden in Cloud Manager.** Formerly, costs that were hidden in Organization and Business Group were exposed in reports. This issue is resolved.

- **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.
- **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.
- **Bug 905805 - system.properties has the Windows ^M in the file.** This issue is resolved.
- **Bug 903076 and SR10922150691 - Disk size does not show properly in Cloud Manager.**

  This issue is resolved.
- **Bug 901327 - Change Business Service is missing the hostname field.** 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.
- **Bug 894591 - Unassigned Virtual Machines list takes time and might timeout.** This issue is resolved.
- **Bug 892789 - /opt/netiq/cloudmanager/etc/org.apache.karaf.features.cfg has ^M on every line.**
- **Bug 892788 - `Features:install cloudmanager-workload-deploy-notification-plugins` must be run each time a reload runs or product will not work.** You can now add the `cloudmanager-workload-deploy-notification-plugins` feature to the `featuresBoot` boot property in the `/opt/netiq/cloudmanager/etc/org.apache.karaf.features.cfg` file. This is a comma separated list of features to install at `karaf` startup. Add a comma and the feature name at the end of the list.
- **885501 - Selecting to request Public IP creates deadlock situation.** This issue is resolved.
- **Bug 861085 - [FTF] NCM 2.2.0/2.2.2 Imported machine adding new NIC fails - Error No root disk found.** This issue is resolved.
- **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.
- **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.
- **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.
- **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.

- **SR 10911613451.** Formerly, some workload imports failed because of timeout issues. The import process was optimized to improve performance so that timeout issues are avoided.
- **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.
- Made adjustments for null pointer exception in IdentityContextManager.
- Made adjustments to `ForceWorkflowCompletionCommand` command to attempt to clean up Business Service Requests and Change Requests that have no workflow.
- Enhanced workflow-related logging.
- Fixed an issue with datastore search. It was 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 System Requirements, Supported Technologies, and Installation

For information about the system requirements, platform support, and installation procedures for this product, see the *NetIQ Cloud Manager Installation and Upgrade Guide*.

IMPORTANT: This release supports only the VMware vSphere hypervisor. Although workloads from other hypervisor technologies are discovered in Cloud Manager, only VMware VMs have been tested.

---

3 Installation Issue

You might encounter the following issue as you install Cloud Manager 2.4:

3.1 Orchestration Monitoring for RHEL Resources Is Not Included in the Installation Packages

The Cloud Manager Orchestration installation media does not include the Red Hat Enterprise Linux (RHEL) monitoring packages.

If you want to monitor RHEL resources, we recommend that you download Ganglia 3.1.7 from the SourceForge (http://sourceforge.net/projects/ganglia/files/ganglia%20monitoring%20core/3.1.7/) website and install it on the resources to be monitored. Create a `.conf` file similar to one that exists on a SUSE Linux Enterprise Server machine, editing the node name in the file so that the monitoring metrics display for the resource in the Orchestration Console.

4 Upgrade Issues

You might encounter the following issues as you upgrade from Cloud Manager 2.3.*x* to Cloud Manager 2.4:

4.1 PostgreSQL Database Format Upgrade from 8.3 to 9.1 Is Necessary after Upgrade

SUSE Linux Enterprise Server 11 SP3 introduces an upgrade of PostgreSQL from version 8.3 to version 9.1. This upgrade involves a change of the database format. After you upgrade the operating system from SP2 to SP3, you must manually migrate your existing PostgreSQL database to the new format before PostgreSQL can run again. After you upgrade the database format to PostgreSQL 9.1, its daemon is not automatically started.

PostgreSQL 9.1 provides a new `pg_upgrade` tool to migrate the PostgreSQL database to the new format. Both the 8.3 version and 9.1 version of the software are included in SLES 11 SP3 to accommodate the use of this tool. For information about how to perform a database migration using the `pg_upgrade` tool, see the `pg_upgrade` tool documentation (`/usr/share/doc/packages/postgresql91/html/pgupgrade.html`) on the server (requires the `postgresql91-docs` package). Follow the instructions in this section to upgrade your Cloud Manager database instance.

When you migrate the data to the new format with the `pg-upgrade` tool, the server must have enough free disk space to temporarily hold a copy of the database file. You can run the `du -hs /var/lib/pgsql/data` command to determine the size of the database.

NOTE: NetIQ recommends that you back up your database before you upgrade its format.

To upgrade the PostgreSQL database format for your Cloud Manager database instance:

1 Stop the PostgreSQL process:

```
rcpostgresql stop
```

2. Ensure that you apply the latest patches for PostgreSQL 8.3 to upgrade to version 8.3.19 or higher.

   The patch relocates the software from its standard location to a versioned location `/usr/lib/postgresql83/bin`. It uses symbolic links to make the software available in the standard location.

3. Install PostgreSQL 9.1 and its dependent packages. The `pg_upgrade` tool is found in the `postgresql91-contrib` package.

   ```
   zypper in postgresql91-contrib
   ```

   PostgreSQL 9.1 installs to a versioned location `/usr/lib/postgresql91/bin`. It uses symbolic links to make the version 9.1 software available in the standard location instead of version 8.3.

4. Rename `/var/lib/pgsql/data` to `/var/lib/pgsql/data.old`.

5. Initialize a new data directory:

   ```
   initdb --pgdata=/var/lib/pgsql/data --locale=en_US.UTF-8
   ```

6. Use the `pg_upgrade` tool to migrate the PostgreSQL database format from version 8.3 to version 9.1.

   ```
   pg_upgrade -b /usr/lib/postgresql83/bin/ -B /usr/lib/postgresql91/bin/ -d /var/lib/pgsql/data.old/ -D /var/lib/pgsql/data
   ```

7. Start the PostgreSQL process:

   ```
   rcpostgresql start
   ```

4.2 Custom Jetty Modifications Are Necessary after Upgrade

Because the Jetty server used for communication between the Cloud Orchestration Server and the Cloud Manager Application Server is upgraded when you move from Cloud Manager 2.3 to Cloud Manager 2.4, you need to reapply any modifications you might have made to `jetty.xml` or `jetty-ssl.xml` after you complete the upgrade. See Section 5.4, “Disabling SSL v3 in Java Jetty,” on page 8.

5 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.

NOTE: Issues not listed here might be addressed in the “Troubleshooting” sections of the *NetIQ Cloud Manager Administrator Reference*. Most such issues are ongoing and will not be fixed in the product.

5.1 Do Not Use OpenVMTools

If you use OpenVMTools (`open-vm-tools`) on your workload VMs, the gateway data is not available because of a defect in the tools, which impacts discovery. OpenVMTools is aware of this issue, but the resolution date is unknown. (Bug 916077)

Red Hat Enterprise Linux 7 includes (and recommends) the use of OpenVMTools instead of VMware tools. However, when you use OpenVMTools, Cloud Manager does not properly pick up IP address information from DHCP workloads. OpenVMTools is aware of the issue, but the resolution date is unknown.

Workaround: Ensure that you install the VMware-tools package on your workload VMs. Do not use OpenVMTools.

5.2 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.

5.3 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 email notifications 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
...
...
```

5.4 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]
```

5.5 Cloud Manager Application Issue

You might encounter the following issues with the Cloud Manager Application components:

- Section 5.5.1, “Network configurations are not applied correctly for Ubuntu workloads,” on page 9

5.5.1 Network configurations are not applied correctly for Ubuntu workloads

If you configure the network configuration for an Ubuntu workload with a static IP address and then choose to use DHCP for DNS, or if you select DHCP for the network address and then you choose a static address for DNS servers, Cloud Manager does not apply these mixed configurations as expected.

For this release, we recommend that you set *both* of the network configuration settings (that is, the network IP address and the name servers) to either static or DHCP.

5.6 Cloud Manager Orchestration Issues

You might encounter the following issues with the Cloud Manager Orchestration components:

- Section 5.6.1, “Enabling a Log Trace of Calls to the Orchestration Server REST Interface,” on page 9
- Section 5.6.2, “A VM without VMware Tools Fails to Build for Change Request,” on page 9

5.6.1 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
```

5.6.2 A VM without VMware Tools Fails to Build for Change Request

Currently, Cloud Manager cannot properly shut down a VM for reconfiguration and rebuild if the VM does not include VMware Tools: the build fails and the VM crashes.

To resolve this issue, you must install the VMware Tools software in the VMs. See also Do Not Use OpenVMTools in this document.

5.7 Cloud Manager Mobile Client Issue

The Cloud Manager Mobile Client for iPad and iPhone app is not supported for use with Cloud Manager 2.4.

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. 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 Qmunity (http://community.netiq.com/), our community website that offers product forums, product notifications, blogs, and product user groups.

7 Legal Notice