NetIQ Cloud Manager 2.1.5 Readme

January 31, 2013

This Readme contains information about NetIQ Cloud Manager 2.1.5 issues you might encounter. The Readme is divided into the following sections:

- Section 1, “Installation Issues,” on page 1
- Section 2, “Upgrade Issues,” on page 2
- Section 3, “Cloud Manager Application Issues,” on page 2
- Section 4, “Cloud Manager Orchestration Issues,” on page 4
- Section 5, “Job developer documentation is archived,” on page 4
- Section 6, “Legal Notice,” on page 4

1 Installation Issues

The following issues might be encountered during Cloud Manager installation:

- Section 1.1, “Orchestration monitoring for RHEL resources is not included in the installation packages,” on page 1
- Section 1.2, “Orchestration Server high availability installation fails when the Cloud Manager Monitoring Server package is not installed,” on page 1

1.1 Orchestration monitoring for RHEL resources is not included in the installation packages

The Cloud Manager Orchestration installation media does not include the 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/) Web site and install it on the resources to be monitored. Create a `.conf` file similar to one that exists on a SLES machine, editing the node name in the file so that the monitoring metrics display for the resource in the Orchestration Console.

1.2 Orchestration Server high availability installation fails when the Cloud Manager Monitoring Server package is not installed

If you do not install the Cloud Manager Monitoring Server package during the installation of the Cloud Manager Orchestration components, later attempts to set up the server for high availability by running the `zos_server_ha_post_config.sh` script fail.

Workaround: If you intend to use the Orchestration Server in a high availability environment, you must install the Cloud Manager Monitoring Server package with it.

For information about the Cloud Manager Monitoring installation pattern, see “Cloud Manager Monitoring Server Pattern” in the *NetIQ Cloud Manager 2.1.5 Installation Planning Guide*.

For information about installing the Monitoring pattern in YaST, see Step 5 in the "Installing the Orchestration Server to a SLES 11 Pacemaker Cluster Environment"procedure of the *NetIQ Cloud Manager 2.1.5 Orchestration Server High Availability Configuration Guide*.

For information about configuring Cloud Manager Orchestration Monitoring, see "Configuring the Monitoring Server and Monitoring Agent" in the *NetIQ Cloud Manager 2.1.5 Orchestration Installation Guide*.

2 Upgrade Issues

The following issues might be encountered during Cloud Manager installation:

- Section 2.1, "Upgrading from a Pre-2.1.4 Version of Cloud Manager," on page 2

2.1 Upgrading from a Pre-2.1.4 Version of Cloud Manager

If you are upgrading from a version of Cloud Manager earlier that 2.1.4 and if your current Cloud Manager environment has resource groups that include repositories, it is necessary to execute a command at the Karaf console of the Cloud Manager Application Server after you upgrade to version 2.1.5 and before you start the upgraded workloads.

```
cm:repo-groups-upgrade
```

The command executes a number of operations:

- Ensures that the NCM_RGRepository policy is deployed on the Orchestration Server.
- Ensures that the repository group is created on the Cloud Manager 2.1.5 Orchestration Server.
- Sets the `resource.vm.ncm.repository_group` fact on the VMs that are associated with a resource group.

You should also run the command when you create a new workload in an upgraded business service or when you import a VM and associate it with an upgraded resource group.

3 Cloud Manager Application Issues

The following issues might be encountered with the Cloud Manager Application components:

- Section 3.1, "Intermittent interface display problem," on page 2
- Section 3.2, "Saving multiple Cloud Manager reports not possible when using the Firefox browser," on page 3
- Section 3.3, "Remote console for a workload does not launch from Internet Explorer with Chrome Frame plug-in," on page 3

3.1 Intermittent interface display problem

A Cloud Manager user might see intermittent display problems in the Cloud Manager Web console interface where some tabs are not properly displayed.

If you encounter this problem, we recommend that you restart the Cloud Manager Application Server.

3.2 Saving multiple Cloud Manager reports not possible when using the Firefox browser

When you attempt to save more than one Cloud Manager `.pdf` report from a Firefox browser (version 15.0.1) while viewing the Cloud Manager Application Server Console, attempts to save more than one `.pdf` report fail.

Workaround: Log out of the console and log back in to save one report at a time, or use another browser, such as Microsoft Internet Explorer 9, to view and save multiple reports in `.pdf` format in the same session.

3.3 Remote console for a workload does not launch from Internet Explorer with Chrome Frame plug-in

If you are using Microsoft Internet Explorer 9 with the Google Chrome Frame plug-in and a self-signed security certificate (in a test environment) to view the Cloud Manager Application Server console, and if you try to launch a remote session of a workload in a business service, the remote session fails.

Testing has shown that the failure occurs because Chrome Frame does not allow a self-signed security certificate.

Workaround: You can force Chrome Frame to accept the self-signed certificate as a trusted root in Windows by using the following steps:

NOTE: This procedure is effective only if the VNC proxy is configured to use the same certificate as the Cloud Manager Application Server console.

---

1. Open Internet Explorer as an Administrator, then, using Internet Explorer to open the Cloud Manager console, note the warning from the browser about an unrecognized certificate.
2. At the warning dialog, specify that you want to continue to the Website.
3. In the browser address bar, click the certificate warning, then click *View Certificates*.
4. In the certificate pop-up, click *Install Certificate* then click *Next*.

   TIP: The *Install Certificate* button does not display unless you are running the browser as Administrator.

   ---

5. Select *Place all certificates in the following store*, then click *Browse*.
6. From the list, select *Trusted Root Certification Authorities*, then click *OK*, click *Next*, then click *Finish*.
7. At the confirmation dialog, click *Yes*, then, at the next confirmation dialog, click *Close*.
8. At the certificate popup, click *Close*.

Test the workaround by closing the browser and reopening it to the Cloud Manager console. You should not see a certificate warning and you should be able to connect to the console using the Chrome Frame plug-in.

4 Cloud Manager Orchestration Issues

The following issues might be encountered with the Cloud Manager Orchestration components:

- Section 4.1, “Orchestration Server issues,” on page 4
- Section 4.2, “Citrix Xen VM issues in the Orchestration Console,” on page 4

4.1 Orchestration Server issues

The following information is included in this section:

- Section 4.1.1, “Support for VMware clusters,” on page 4

4.1.1 Support for VMware clusters

NetIQ Cloud Manager deploys workloads managed by the VMware ESX hypervisor only into resource pools that have been configured on an associated cluster. This requires that the Cloud Manager administrator assign these VMware resource pools to NetIQ Cloud Manager resource groups.

4.2 Citrix Xen VM issues in the Orchestration Console

The following information is included in this section:

- Section 4.2.1, “Xenserv provisioning adapter cannot deploy workloads to certain repositories,” on page 4

4.2.1 Xenserv provisioning adapter cannot deploy workloads to certain repositories

Testing has shown that using the Citrix XenServer (xenserv) provisioning adapter to provision a workload fails to properly set the `repository.vmhosts` fact to the set of XenServer hosts that can access the repository. This behavior is revealed if the display name of the datastore in XenCenter is “storage.”

Workaround: Rename the “storage” repository in XenCenter, then in the Orchestration Console click *Discover* > *VM Hosts & Repositories*.

5 Job developer documentation is archived

Documentation for custom job/policy writing is now archived in older versions (that is, Cloud Manager 2.1.1 and previous) of the product documentation. The most current *Job Development Guide* can be found in the `.zip` file (https://www.netiq.com/documentation/cloudmanager2/pdfdoc/cloudmanager21.zip) of product manuals at the product documentation Web site (https://www.netiq.com/documentation/cloudmanager2/) in *Previous Versions* > *Cloud Manager 2.1* > *Guides*. The file is `ncm2_orch_developer.pdf`.

6 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.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.