Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for EMC Celerra Server

Release 12.1.0.2.0

E27541-03

September 2012

This document provides a brief description about the Oracle System Monitoring Plug-in for EMC Celerra Server, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

The System Monitoring Plug-in for EMC Celerra Server extends Oracle Enterprise Manager Cloud Control to add support for managing EMC Celerra Network Attached Storage (NAS) servers. By deploying the plug-in in your Enterprise Manager Cloud Control 12*c* environment, you gain the following management features:

- Monitor EMC Celerra NAS servers.
- Gather configuration and track configuration changes for NAS servers.
- Raise alerts and violations based on thresholds set on monitoring and configuration data.
- Provide rich out-of-box reports for the user interface based on the gathered data.
- Support monitoring by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as the Celerra Server.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Cloud Control 12*c* Release 1 Management Service
- EMC Celerra servers with Clariion (NS 600/700 and NS 700G), and future versions of EMC Celerra servers provided that they are backward-compatible
- Enterprise Manager Cloud Control 12*c* Release 1 Agent on any UNIX platform (such as Linux, HP UX, and Solaris)
- EMC Celerra Software/CLI version 5.3

Prerequisites

The following prerequisites must be installed before you can deploy version 12.1.0.2.0 of the plug-in:

- Oracle Enterprise Manager Cloud Control 12*c* Release 1 system and Agent.
- The EMC Celerra Plug-in can only be deployed on UNIX Agents, not Windows.

ORACLE

- Secure Shell (SSH) must be configured to bypass the Control Station host user password. See Configuring SSH to Bypass the Password for the procedure.
- SSH should be installed in:

  `/usr/bin:/usr/sbin:/bin:/usr/local/bin`
- This version of the plug-in with SNMP support requires the following:
  - Oracle Management Services (OMS) version 12.1.0.1
  - One-off patch for Enterprise Manager version 12.1.0.1 based on Oracle bug #5349647
  - Version 12.1.0.2 of the Agent

Deploying the Plug-in

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to deploy the plug-in:

`http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm`

Adding Instances for Monitoring

After successfully deploying the plug-in, follow these steps to add the plug-in target to Cloud Control for central monitoring and management:

1. Log in to Enterprise Manager Cloud Control as root.
2. Click **Setup**, then **Add Targets**, and finally **Add Targets Manually**.
3. Select **Add Non-Host Targets by Specifying Target Monitoring Properties**. From the Target Type drop-down, select the **EMC Celerra Server** target type. Click **Add Manually**.
4. Provide the following information for the parameters:
   - **Name** — Name for the plug-in
   - **Celerra Control Station Host or IP Address** — Name/IP address of the Control Station
   - **Celerra Admin User** — Keep the default name if SSH set up for nasadmin, or change the name if SSH is set up for a different user
5. Click **Test Connection** to make sure the parameters you entered are correct.
6. Reenter the encrypted parameters from step 4 if the connection test was successful, then click **OK**.

Note: After you deploy and configure the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is a part of.

Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the **EMC Celerra Server** target link from the Agent home page Monitored Targets table. The EMC Celerra Server home page appears.
2. Verify that no metric collection errors are reported in the Metrics table.
3. Ensure that reports can be seen and no errors are reported by selecting the **Reports** property page.
4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not immediately appear, click **Refresh** in the View Configuration page.

Configuring SSH to Bypass the Password

Follow the steps below to set up SSH from the host, where the Enterprise Manager Agent is installed on the EMC Celerra control station.

1. Log in to the host where the Enterprise Manager Cloud Control Agent is installed that monitors EMC Celerra. Log in as the user under which the Agent is running.
2. Connect to the EMC Control Station using SSH as shown below. Ensure that the SSH client is installed on the host. If this is the first time you are accessing the Control Station, type **Yes** when the system asks whether you want to save the RSA key of the Control Station to the local file.

```
# ssh -l nasadmin erpcel01-con
The authenticity of host 'erpcel01-con (140.20.176.75)' can't be established.
RSA key fingerprint is 72:2c:f8:db:76:c9:8d:35:ae:b1:ab:74:30:f5:69:af.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'erpcel01-con, 140.20.176.75' (RSA) to the list of
known hosts.
nasadmin@ erpcel01-con 's password: [Type the password for nasadmin]
Last login: Sat Oct 15 22:18:21 2005 from stach28.us.oracle.com
EMC Celerra Control Station Linux Thu Mar 24 08:27:43 PST 2005
slot_0 primary control station ***
[nasadmin@erpcel01-con nasadmin]$ [Type exit and exit SSH]
```

3. Generate a pair of authentication keys on the Agent host by entering:

```
# cd ~/.ssh
# ssh-keygen -t dsa -f id_dsa

Generating public/private dsa key pair.
Enter passphrase (empty for no passphrase): [Leave empty]
Enter same passphrase again: [Leave empty]
Your identification has been saved in id_dsa.
Your public key has been saved in id_dsa.pub.
The key fingerprint is:
e2:24:fa:d2:f9:48:e6:1e:85:7e:86:d1:b5:52:79:fb spanchum@ stach28.us.oracle.com
```

4. Upload the public key (`id_dsa.pub`) to the Control Station in the home directory for user nasadmin.

```
# scp id_dsa.pub nasadmin@erpcel01-con:~/.ssh/
nasadmin@erpcel01-con's password: [Type the password for nasadmin]
id_dsa.pub 100% |*********************************************| 600 00:00
```

5. Log in to the Control Station (`erpcel01-con`) and rename the uploaded file (`id_dsa.pub`) to the `authorized_keys` file. If the file already exists, add the contents of the `id_dsa.pub` file to the `authorized_keys` file by entering:

```
# ssh -l nasadmin erpcel01-con
nasadmin@erpcel01-con's password: [Type the password for nasadmin]
Last login: Sat Oct 15 22:53:22 2005 from stach28.us.oracle.com
EMC Celerra Control Station Linux Thu Mar 24 08:27:43 PST 2005
*** slot_0 primary control station ***
[nasadmin@erpcel01-con nasadmin]$ cd .ssh
[nasadmin@erpcel01-con .ssh]$ cat id_dsa.pub >> authorized_keys
[nasadmin@erpcel01-con .ssh]$ logout
Connection to erpcel01-con closed.
```

6. Run the following command to verify that a password is not required for any of the secure programs:

```
# ssh -l nasadmin erpcel01-con date
Sat Oct 15 23:04:46 PDT 2005
```

Configuring EMC Celerra SNMP Traps

The following sections provide the configuration steps to be performed on the EMC Celerra control station to send SNMP traps to the Enterprise Manager EMC Celerra Plug-in. For more information about the EMC Celerra event and notification system, refer to the following EMC-provided documentation:

Celerra Network Server Technical Module — Configuring Celerra Events and Notifications

Configuring the SNMP Trap Configuration File

The SNMP Trap Configuration file specifies the SNMP Manager to which the trap should be sent. To receive SNMP traps from the Celerra Control Station, you can modify the default trap configuration file `/nas/site/trap.cfg` or create a new configuration file. A different file is required if more than one SNMP manager is listening for different SNMP traps. The SNMP Trap Configuration file is referenced in the Notification Configuration file, which is described in the next section.

If you plan to use the default Notification Configuration file specific to Enterprise Manager as described in the next section, you should create a new SNMP Trap Configuration file (`em_trap.cfg`) by performing the following steps.

1. Ensure that the prerequisites for SNMP are met. See Prerequisites.
2. Log in to the EMC Celerra control station as a NASADMIN user.
3. Enter:

```
cd /nas/site
```

4. Enter:

```
cp trap.cfg em_trap.cfg
```

5. Modify the contents of em_trap.cfg by uncommenting and changing snmpmanager to point to the emagenthost:emagentport format, as shown in the following example:

```
snmpmanager 140.87.1.84:5125 ; communityname public
```

Creating and Loading a Notification Configuration File

The Notification Configuration file specifies the list of events for which notifications are to be sent. The default notification file, `/nas/sys/nas_eventlog.cfg`, contains all the default notification events with different types of notification methods (call home, SNMP trap, e-mail, log, exec, and so forth).

You can either modify the default notification file, `/nas/sys/nas_ eventlog.cfg`, or create a new one specific to Enterprise Manager with a subset of events. The following procedure provides a sample Notification Configuration File, em_snmp_ eventlog.cfg, which contains power status, fan status, reboot events, and failover events. You can add more events as required. Refer to the EMC-provided documentation, Celerra Network Server Technical Module — Configuring Celerra Events and Notifications, for details on the format of the Notification Configuration file.

Perform the following steps to create and load the file:

1. Log in to the EMC Celerra control station as a NASADMIN user.
2. Create the `em_snmp_eventlog.cfg` file with the following contents:

```
#
# Notification file for Enterprise Manager plug-in for EMC Celerra
#
# BoxMonitor
# Fan status, power status events for CNS-14, Reboot events for  ALL platforms
facilitypolicy  131, 4
    disposition range=1-1, trap "/nas/site/em_trap.cfg 2"
    disposition range=3-15, trap "/nas/site/em_trap.cfg 2"
    disposition range=18-21, trap "/nas/site/em_trap.cfg 2"
    disposition range=38-39, trap "/nas/site/em_trap.cfg 2"
    disposition range=43-43, trap "/nas/site/em_trap.cfg 2"
    disposition range=57-58, trap "/nas/site/em_trap.cfg 2"
    disposition range=62-67, trap "/nas/site/em_trap.cfg 2"
    disposition range=70-70, trap "/nas/site/em_trap.cfg 2"
    disposition range=73-73, trap "/nas/site/em_trap.cfg 2"
    disposition range=100-115, trap "/nas/site/em_trap.cfg 2"
    disposition range=200-215, trap "/nas/site/em_trap.cfg 2"
    disposition range=300-315, trap "/nas/site/em_trap.cfg 2"

#
# Enclosure Monitor
# Fan status, power status events for NS platform
facilitypolicy 86, 7
    disposition severity=0-3, trap "/nas/site/em_trap.cfg 2"
    disposition severity=4-4, trap "/nas/site/em_trap.cfg 3"
```

3. Edit the file to add any other events if needed.
4. Enter the `nas_event` command as shown in the following example:

```
[nasadmin@erpcel01-con site]$ nas_event -Load /nas/site/em_
event_config.cfg
```

```
EventLog : will load /nas/site/em_snmp_eventlog.cfg... done
```

5. Verify if the file is loaded by entering the `nas_event` command as shown in the following example:

   ```
   [nasadmin@erpcel01-con site]$ nas_event -Load -info
   ```

   Loaded config. files:

   1: /nas/sys/nas_eventlog.cfg

   2: /nas/http/webui/etc/web_client_eventlog.cfg

   3: /nas/jserver/event_config/events.cfg

   4: /nas/site/em_snmp_eventlog.cfg

To map EMC severities (0-7) to Enterprise Manager severities, use the following required Oracle SNMP Enterprise-specific traps:

- SNMP trap 2 to send critical alerts (EMC-defined severity <= 3)
- SNMP trap 3 to send warning alerts (EMC-defined severity <= 4)

Sending an SNMP Trap Test

After you deploy the plug-in and set up a target, you can use the `nas_snmptrap` command to send SNMP trap tests.

1. Log in to the EMC Celerra control station as a NASADMIN user.
2. Run the `nas_snmptrap` command.
   - The syntax of the command is as follows:

     ```
     /nas/sbin/nas_snmptrap <config_file_path> -m
     /nas/sys/emccelerra.mib -r <trap_number> -f <facility_id> -i
     <event_id> -s <severity_level> -d "<description>"
     <config_file_path> = the path of the trap configuration file
     /nas/sys/emccelerra.mib = the Celerra MIB file
     <trap_number> = the unique trap number for the event
     <facility_id> = the ID number of the facility generating the event
     <event_id> = the event ID number
     <event_id> = the event ID number
     <description> = the description of the trap
     ```

   - The following example shows how to send a critical alert:

     ```
     /nas/sbin/nas_snmptrap /nas/site/em_trap.cfg -m
     /nas/sys/emccelerra.mib -r 2 -f 64 -i 2 -s 2 -d "Test SNMP
     trap Critical Alert"
     ```

   - The following example shows how to send a warning alert:

     ```
     /nas/sbin/nas_snmptrap /nas/site/em_trap.cfg -m
     /nas/sys/emccelerra.mib -r 3 -f 65 -i 3 -s 3 -d "Test SNMP
     trap Warning Alert"
     ```

3. Verify the alerts as follows:
   1. Log in to Enterprise Manager Cloud Control.

2. Go to the EMC Celerra Target. Under the Reports Tab, view the EMC Celerra SNMP Trap-based Alerts Report. This should list the alert corresponding to the trap test that is sent.
3. Go to the Cloud Control Console Home Page. Under All Targets Alerts, Click the **Critical** or **Warning** link. Filter the targets by EMC Celerra Server type. You should see the alert corresponding to the trap test that is sent. You can then select and clear the alert.

Undeploying the Plug-in

To undeploy the EMC Celerra Server Plug-in from an Agent:

1. Log in to Enterprise Manager Cloud Control as root.
2. Click **Setup**, then **Extensibility**, and finally **Plug-ins**.
3. Select the EMC Celerra Server Plug-in target and click **Undeploy From**. Select either **Management Servers** or **Management Agent**.
4. Confirm the plug-in removal. Enterprise Manager notifies the connected and relevant Enterprise Manager users and begins the de-configuration process.

For more information about plug-ins, see the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Enterprise Manager System Monitoring Plug-in Installation Guide Release 12.1.0.2.0 for EMC Celerra Server
E27541-03

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.