Monitoring iDRAC7 Devices Using Dell SupportAssist

Dell Product Group Services
December 2013

A Dell Technical White Paper

Table of contents

Introduction 5

1 Discovery and inventory 6

1.1 Prerequisites 6

1.2 Discovery range configuration 6

2 Discovering iDRAC7 devices 8

2.1.1 ICMP configuration 8

2.1.2 SNMP Configuration 9

3 Setting up iDRAC7 11

4 Configuring SupportAssist 12

4.1 Default credentials 12

4.2 Custom credentials 13

5 Alerts in OpenManage Essentials 15

5.1 Alert threshold 15

6 Automatic case creation and execution of the collection tool 17

7 Scheduling periodic collection 18

8 Sending system logs manually (collection on demand) 19

Conclusion 19

Introduction

Dell SupportAssist is a remote support application providing proactive support capabilities that help identify and resolve issues faster and more accurately. It integrates with Dell OpenManage Essentials, and enables transparent visibility to your server, storage, and networking infrastructure, and proactively identifies hardware failures in your IT environment.

SupportAssist is designed with automated proactive features to help streamline support process steps, maintain your systems' health, and identify hardware failures faster and more accurately.

The key features of SupportAssist include:

- Remote monitoring for critical hardware alerts.
- Automatic collection of diagnostic logs and configuration information.
- Automatic case creation and alert notifications through email.
- Proactive support from a ProSupport Engineer, who has the information required to start resolving your case immediately.

SupportAssist gives you more oversight and control over your environment without the hassle of manual processes and more time. Equipping your OpenManage Essentials server with SupportAssist is voluntary, and results in improved support, products, and services designed to meet your needs.

OpenManage Essentials interacts with supported devices that are to be monitored and receives SNMP traps. The SNMP traps are periodically retrieved as alerts by the SupportAssist client. The alerts are filtered using various policies to decide if the alerts qualify for creating a new support case or updating an existing support case.

All qualifying alerts are securely sent to the SupportAssist server hosted by Dell, for a creating a new support case or updating an existing support case. After the support case is created or updated, the SupportAssist client, runs the appropriate collection tools on the devices that generated the alerts, and uploads the log collection to Dell.

The information in the log collection is used by Dell technical support to troubleshoot the issue and provide an appropriate solution.

This technical white paper provides information about monitoring iDRAC7 devices using Dell SupportAssist. The following are the high-level areas covered:

- Steps to perform discovery and inventory
- Configuring the iDRAC7 device credentials in SupportAssist
- Alert processing
- Automatic case creation for an alert
- Sending system logs manually

1 Discovery and inventory

Discovery and inventory aids understanding of what hardware and software are installed across your organization and is the most basic step to effective systems management. Areas such as license compliance, health monitoring, security and upgrades, and migrations all require the networked hardware to be available to the System Administrator on a single console to help ease the process. OpenManage Essentials provides these capabilities to initialize the discovery and inventory process and perform required actions on these devices.

1.1 Prerequisites

The following are the prerequisites for performing discovery and inventory:

Credentials: The discovery process in OpenManage Essentials communicates with the iDRAC7 devices using SNMP protocol. You may also be required to provide the SNMP community string during the discovery process.

Setting up the system to be managed: There are a few settings to be performed on the managed nodes to make them discoverable over the network. For more infomation, see the *Making Your Environment Manageable with Dell OpenManage Essentials* technical whitepaper at **delltechcenter.com/ome**.

Dell OpenManage Server Administrator (OMSA): OMSA should be installed on all the systems that are required to be managed with OpenManage Essentials.

1.2 Discovery range configuration

This section provides information about providing a discovery range for discovering devices in OpenManage Essentials.

i. In OpenManage Essentials, navigate to **Manage** → **Discovery and Inventory**.
   The **Discovery Range Summary** page is displayed.
ii. Under **Discovery Ranges**, right-click **All Ranges,** and click **Add Discovery Range**.

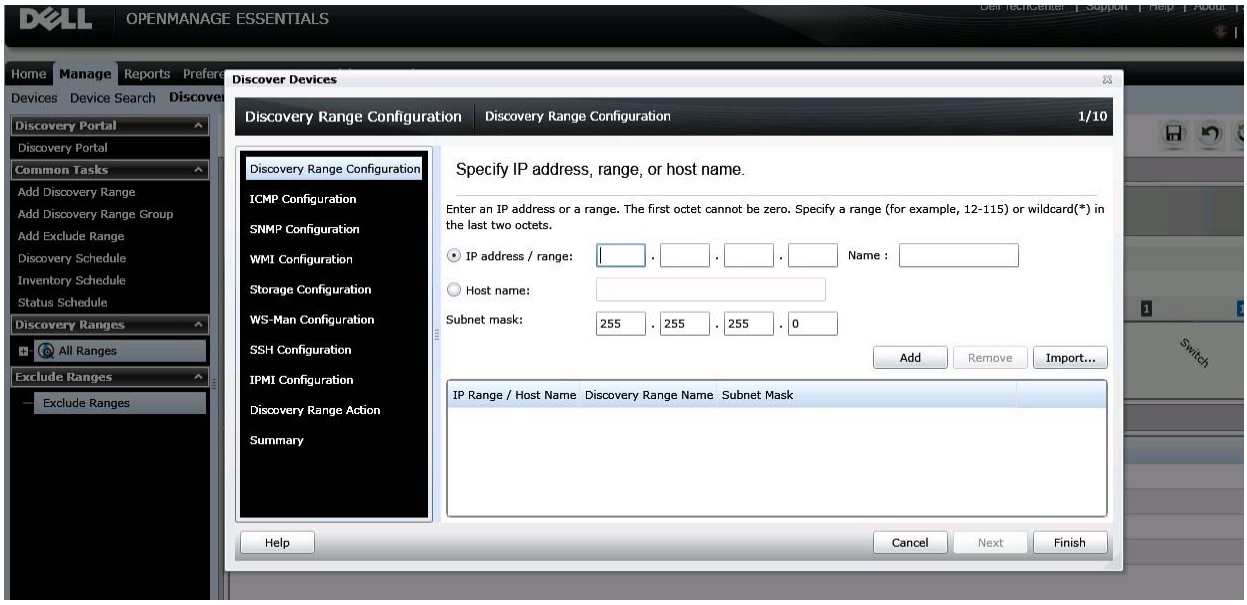


Figure 1 Discovery Range Wizard

iii. Specify the IP ranges of the devices in the environment. The following are examples of valid IP ranges that you can provide.

IP Range	193.109.112.*
	193.104.20-40.*
	192.168.*.*
	192.168.2-51.3-91
	193.109.112.45-99
Hostname	WIN-17L2JS8
Single IP	193.109.112.99

Figure 2 Sample IP ranges

Additionally, an Import functionality provided in OpenManage Essentials helps with importing a Discovery Range which is defined in a .csv file format, as shown in Figure 3. The maximum numbers of devices that can be imported using this method is 500.

Name	Type	Data
1750-win-r03-03	Host (A)	10.94.172.180
1750-win-r04-02	Host (A)	10.94.172.184
1850-win-r04-05	Host (A)	10.94.172.179
2650-win-r01-04	Host (A)	10.94.172.193
2800-W2K3	Host (A)	10.94.168.32
2850-win-r01-03	Host (A)	10.94.161.71
2900-win-r03-07	Host (A)	10.94.161.72
2970-esx	Host (A)	10.94.168.203
4600-WIN-R04-14	Host (A)	10.94.172.168

Figure 3 Sample .csv file

2 Discovering iDRAC7 devices

To discover iDRAC7 devices:

i. In the **IP address/range** field, type the IP address range.
ii. In the **Name** field, provide a range name (optional).
iii. Click **Add**.

NOTE: If required, repeat step i to step iii to add more discovery ranges.

iv. Click **Next** to proceed.

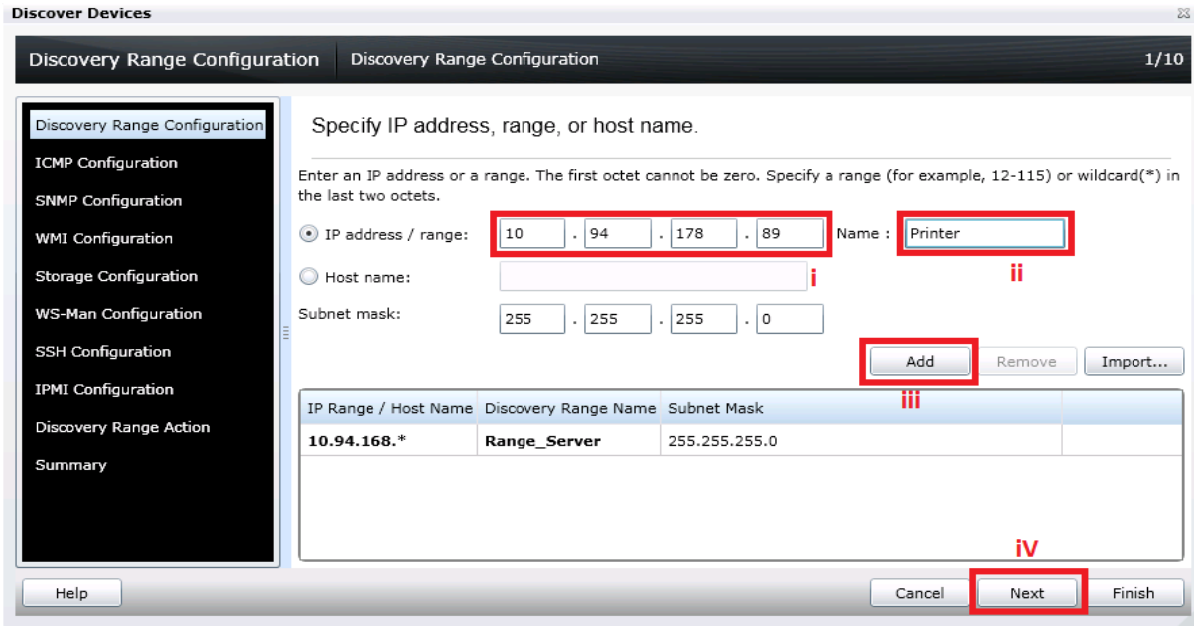


Figure 4 Specifying an IP range

2.1.1 ICMP configuration

i. Set ping timeout for pinging the device on the network.
ii. Specify the number of attempts to be tried.
iii. Click **Next** to proceed.

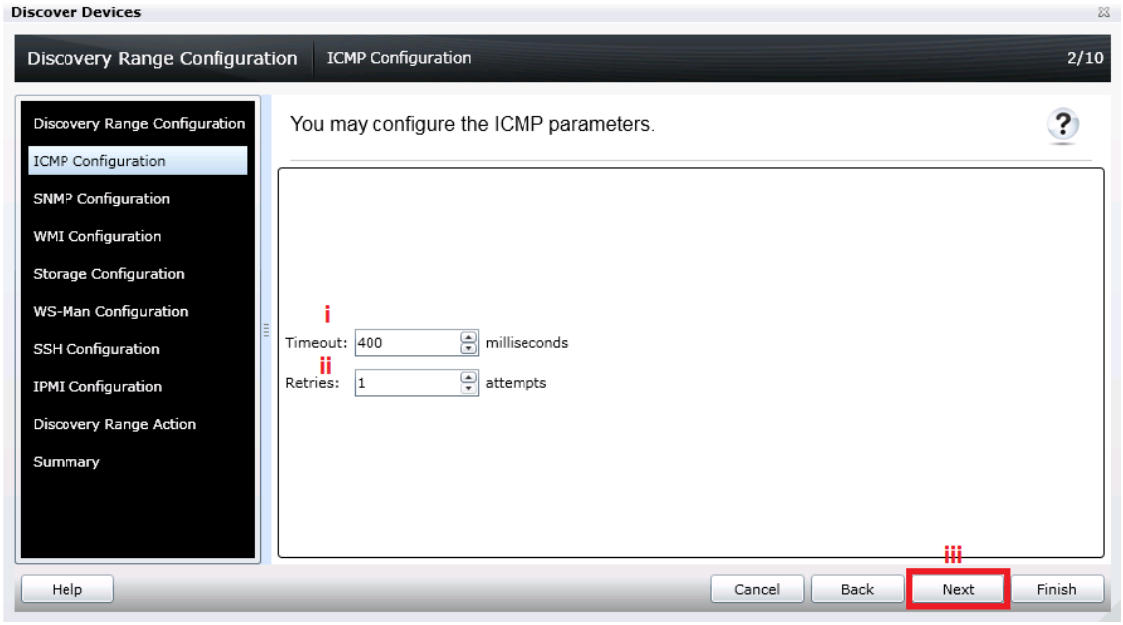


Figure 5 ICMP configuration

2.1.2 SNMP Configuration

i. In the SNMP Configuration screen, select the **Enable SNMP discovery** option.
ii. Type the community name in the **Get community** field.
iii. Click **Next** to proceed with the default settings until the **Discovery Range Action** page.

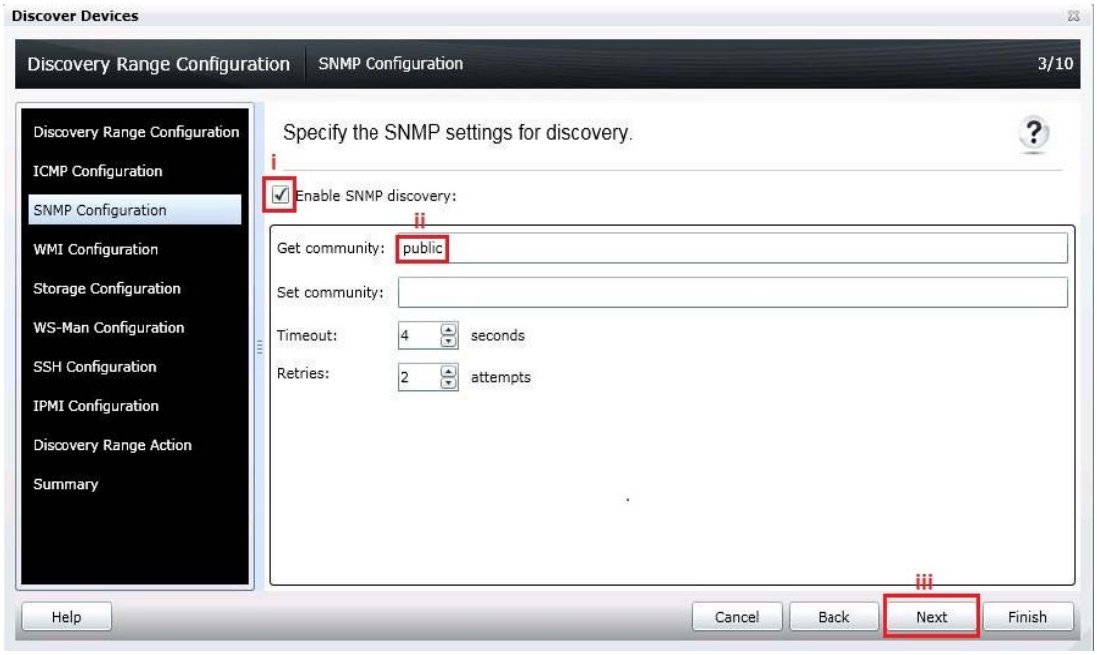
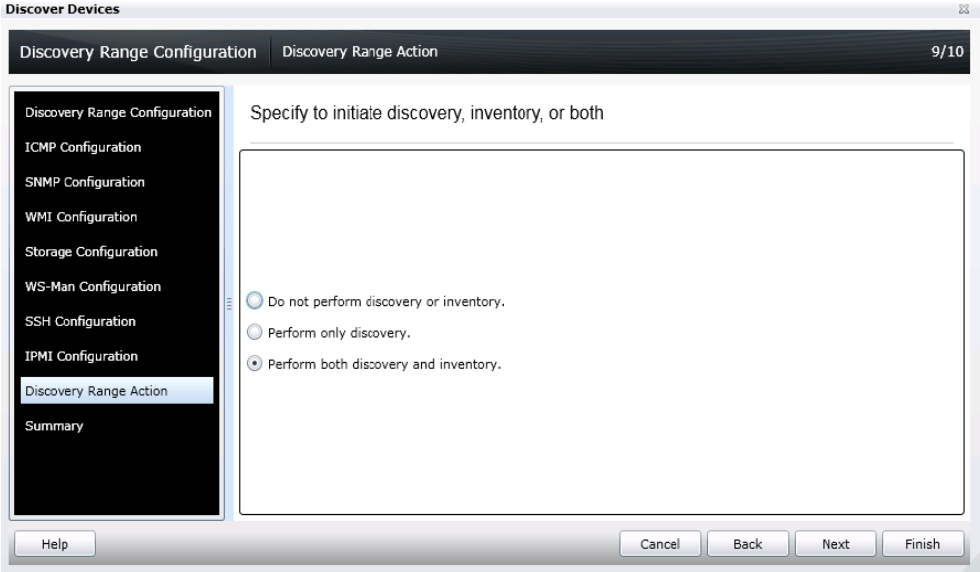


Figure 6 SNMP Configuration

iv. In the **Discovery Range Action** screen, select one of the options, and click **Finish**.



The discovery range you provided is added to the **Include Range** list, and the discovered iDRAC7 device is displayed in the device tree in OpenManage Essentials.

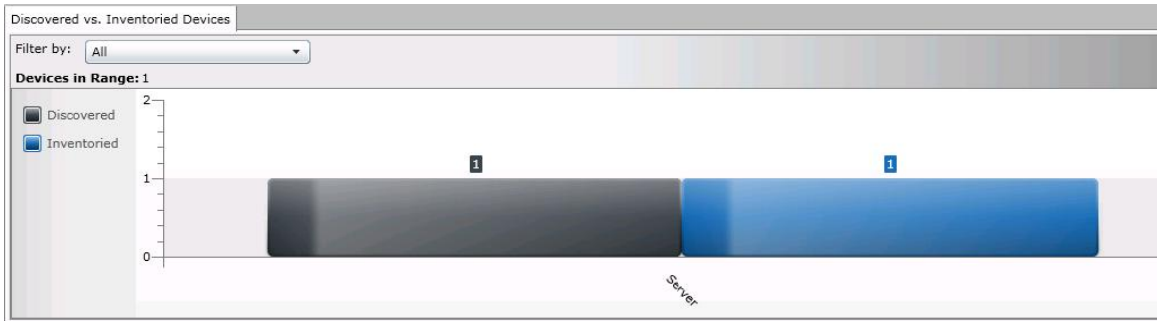


Figure 7 iDRAC7 device in OpenManage Essentials

3 Setting up iDRAC7

i. Launch the iDRAC console of the discovered iDRAC device.
ii. Click **Alerts**.
iii. Navigate to the **SNMP and Email Settings** tab.
iv. Type the alert destination IP address.
v. Click **Apply**.
vi. Under **Test SNMP Trap**, click **Send**.

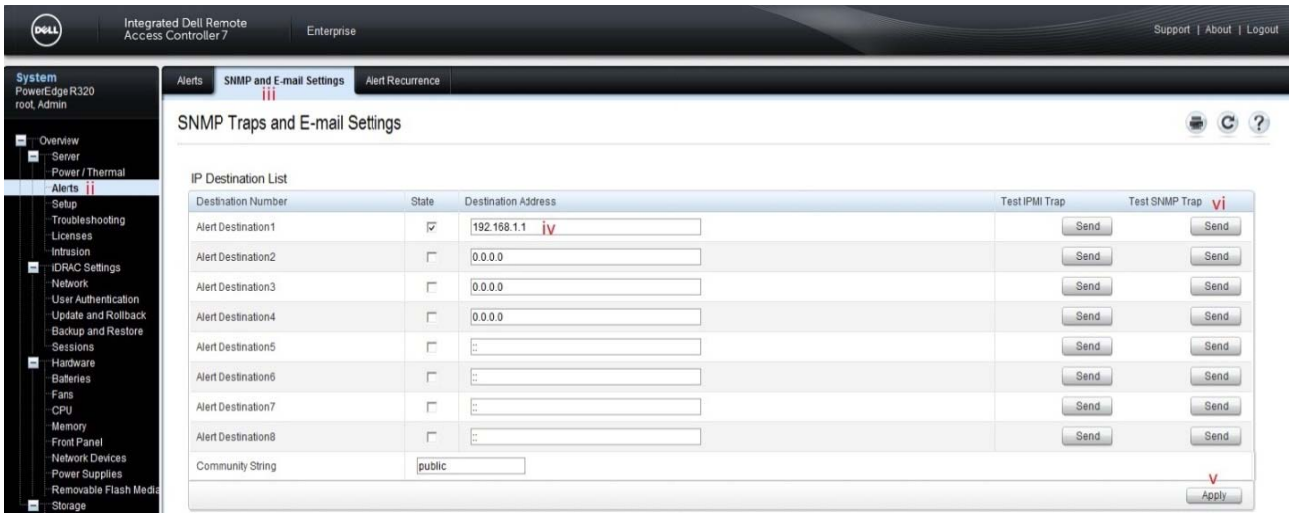


Figure 8 Adding a trap destination in the iDRAC7 console

vii. Navigate to the **Alerts** tab.
viii. Select **Enabled**.
ix. Click **Apply**.

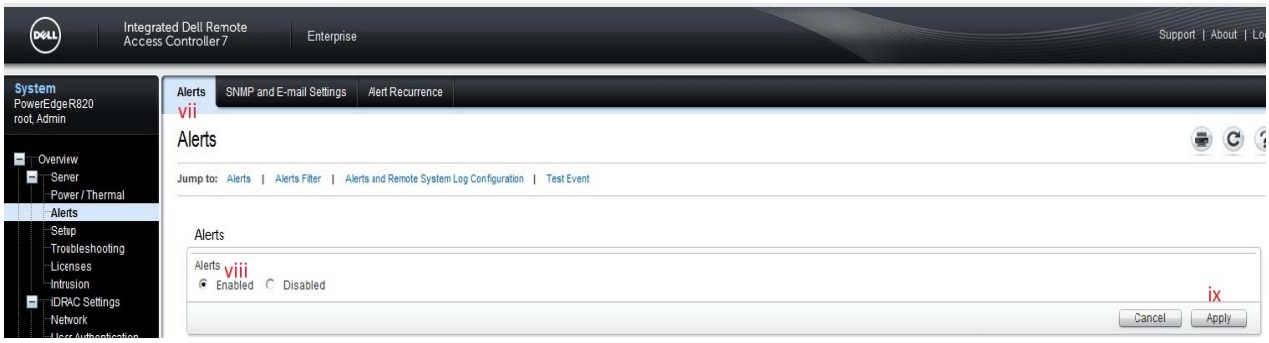


Figure 9 Enabling alerts

4 Configuring SupportAssist

After successful discovery of the iDRAC7 device in OpenManage Essentials, the iDRAC7 device is displayed in the **Devices** tab in SupportAssist.

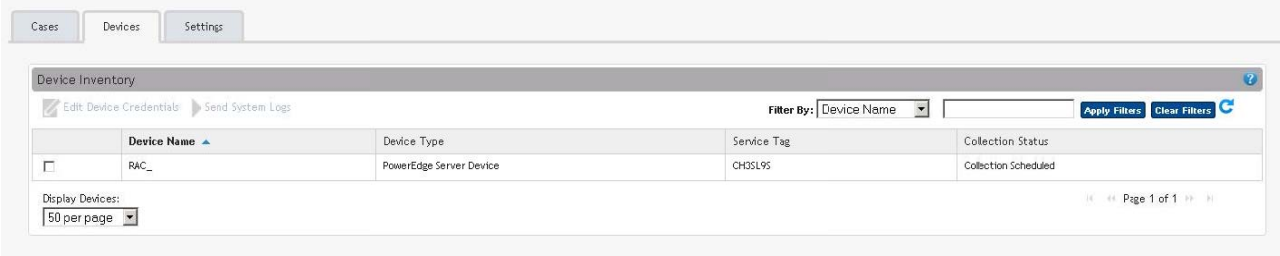


Figure 10 Devices tab

4.1 Default credentials

SupportAssist runs the appropriate collection tools and gathers the system logs from OpenManage Essentials-managed Dell server, storage, and switch devices. To run the collection tools on your IDRAC7 devices, you must configure SupportAssist with the Administrator (default) credentials of the iDRAC7 device. The Administrator credentials you provide are encrypted and saved locally.

To configure default credentials:

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

i. Navigate to the **Settings** tab. By default, the **System Logs** page is displayed.
ii. In the **System Logs** page, under **Edit Device Credentials**, select the **Device Type** as **Server**.
iii. In the **Credential Type** list, select **iDRAC7**.

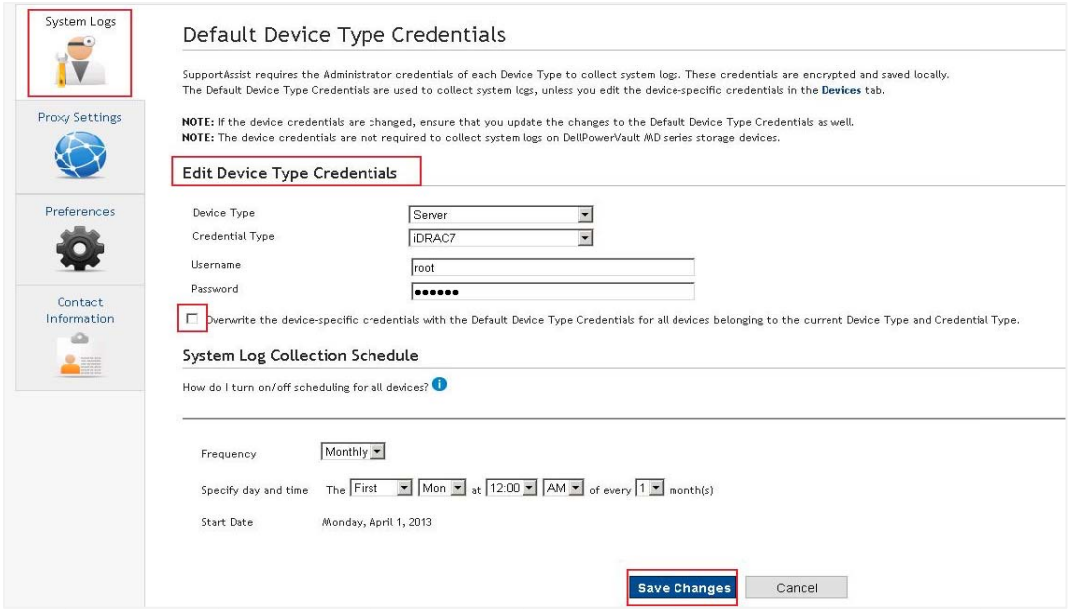


Figure 11 Providing the device credentials

iv. Provide the username and password in the appropriate fields.
v. Click **Save Changes**.

NOTE: When the administrator credentials of a device is changed, make sure that the default credentials is also updated in SupportAssist.

4.2 Custom credentials

If you have more than one iDRAC7 device, and the Administrator (default) credentials of a particular iDRAC7 device is different, you can configure the credentials for that particular iDRAC7 device through the **Devices** tab.

To provide custom credentials:

i. Click the **Devices** tab.
ii. Select the appropriate IDRAC7 device.
iii. Click **Edit Device Credentials**.

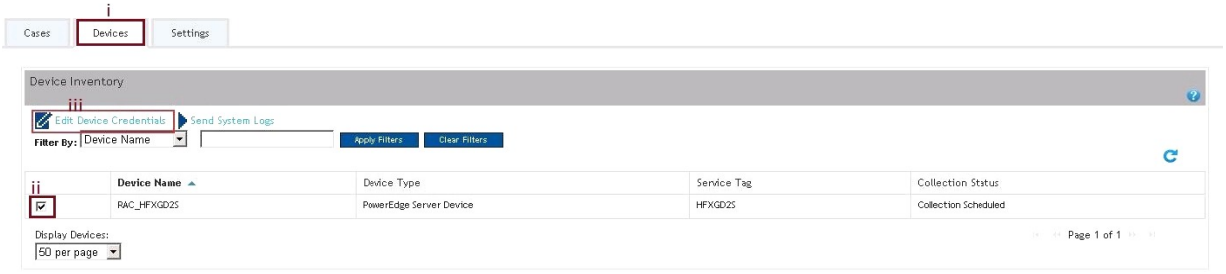


Figure 12 Devices tab

iv. In the **Edit Device Credentials** screen, provide the Username and Password as appropriate.
v. Click **Save Changes**.
vi. At the confirmation prompt, click **Yes**.

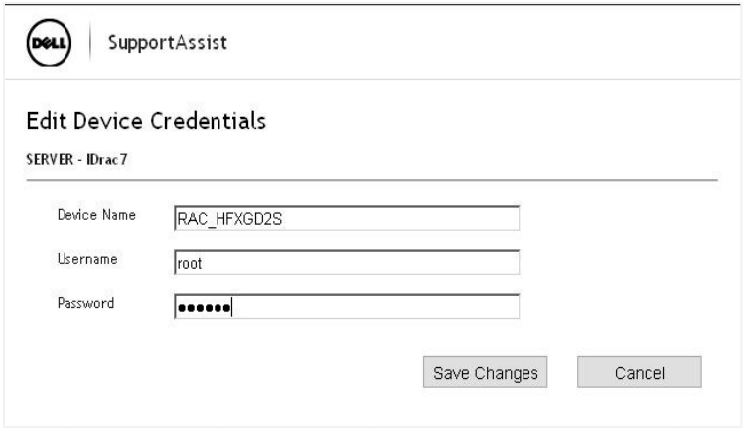


Figure 13 Edit Device Credentials screen

5 Alerts in OpenManage Essentials

Dell OpenManage Essentials administrators can monitor the health of discovered assets through a centralized, easy-to-use dashboard and through automated, custom alerts. The dashboard provides an at-a-glance view and a scoreboard displaying the health and well-being of the infrastructure.

5.1 Alert threshold

The alert threshold specifies under what conditions the alert should cause a support case to be created (or appended). The syntax resembles a programming method, and optionally may take additional arguments to refine its behavior.

Currently there are two possible values:

- FirstMatch () – The case should be created/appended each time this alert is detected.
- Occurs (count,duration) – The case should be created/appended only when the alert has occurred so many times within a specified duration.

The duration argument of the Occurs threshold defines a relative time in days, hours, minutes, and seconds and is formatted as dd-hh:mm:ss. The following are some examples of the Occurs threshold and their descriptions

Table 1 Examples of Occurs threshold

Example	Description
Occurs (5,1-00:00:00)	Create/append a case if the alert occurs 5 or more times within the previous 1 day
Occurs (3,0-05:00:00)	Create/append case if the alert occurs 3 or more times within the previous 5 hours
Occurs (8,1-12:00:00)	Create/append case if the alert occurs 8 or more times within the previous day and a half

Valid duration values – Days: 0 to 365, Hours: 0 to 23, Minutes: 0 to 59, Seconds: 0 to 59

Policies which specify the Occurs () threshold instruct the SupportAssist server to retain the timestamps of each alert. With each new alert occurrence, the SupportAssist server evaluates if the number of alerts within the duration exceeds the count, and if so, creates/appends the case. The timestamps are discarded to ensure the Occurs () threshold will not append the case until an entirely new set of alerts are received which fulfills the criteria.

Table 2 Example of a policy criteria for an alert

Policy Property	Description	Example
clientType	Type of client reporting the alert	"OME"
eventSourceType	Source of the alert	".1.3.6.1.4.1.674.10892.5.3.2.1"
trapId	Trap identifier	"2153"
eventId	Event identifier	"FAN0001"
severity	Severity of the alert	"CRITICAL"
description	Description of the alert	"Fan RPM is less than the lower critical threshold."
autoCase	Indicates if the alert should be processed.	True
alertThreshold	Policy filter used when a case is created.	"FIRST MATCH()"
deltaSeverity	Severity code passed to delta.	"3"

Only alerts with Enterprise OID .1.3.6.1.4.1.674.10892.5.3.2.1, .1.3.6.1.4.1.674.10892.5.3.2.2, and .1.3.6.1.4.1.674.10892.5.3.2.4 for Client Type OME are processed as alerts from IDRAC7 devices.

SupportAssist processes all the alerts with Force10 OIDs, but only some specified alerts will be considered to create the case (Service Requests or SR).

6 Automatic case creation and execution of the collection tool

SupportAssist processes all alerts from OpenManage Essentials, but a support case is created only if:

- The policies qualify the alert for a support case creation.
- SupportAssist is configured to automatically generate support cases.

Once the support case is created for an iDRAC7 device, the corresponding collection tool (Dell System Esupport Tool [DSET]) is invoked, and the system log collection is generated and uploaded to Dell.

NOTE: For devices covered under Basic Support service contract type, the support case is not created, but the collection tools are invoked.

Figure 14 Support case created for an IDRAC7 device

7 Scheduling periodic collection

By default, SupportAssist generates the system log collection from IDRAC7 devices every month, and uploads the system log collection to Dell. You can modify the frequency at which the system log collection is generated based on your preference.

To schedule the periodic collection:

i. Click the **Settings** tab.
ii. Under **Edit Device Type Credentials**, select **Device Type** as **Switch** and **Credential Type** as **iDRAC7**.
iii. Under **System Log Collection Schedule**, select the frequency, date, and time as required.
iv. Click **Save Changes**.

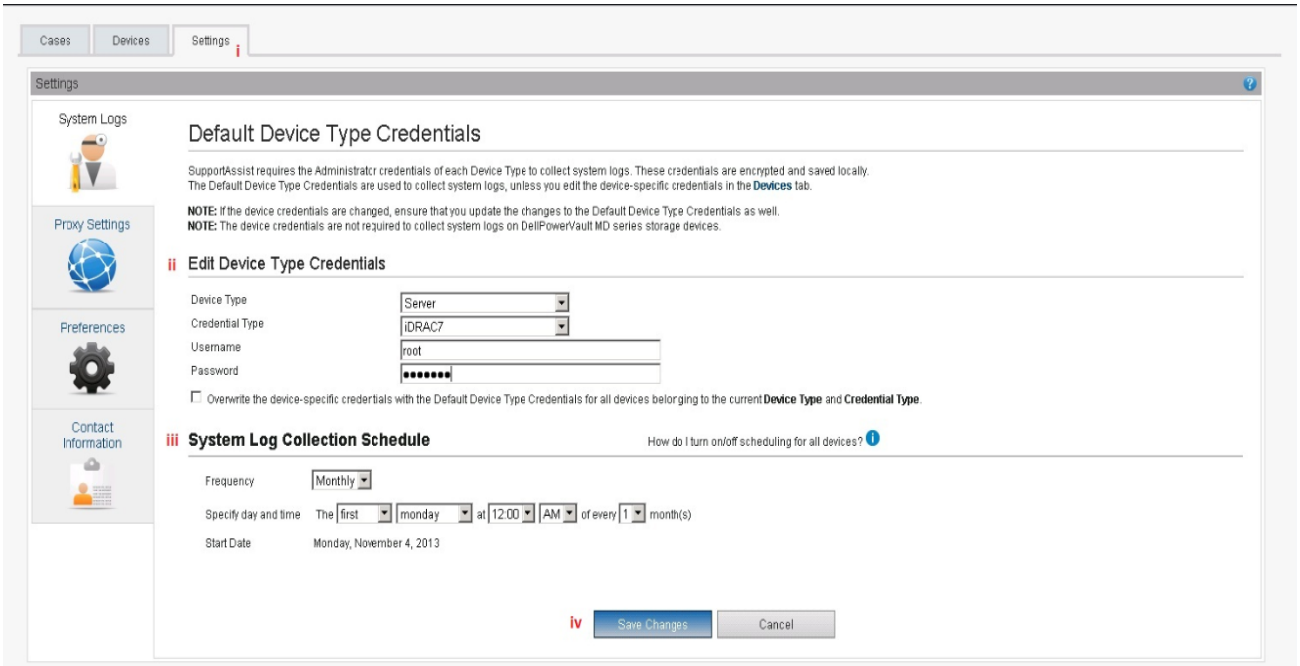


Figure 15 Configuring periodic collection

8 Sending system logs manually (collection on demand)

When a support case is opened or updated, the SupportAssist client, runs the collection tools on the devices that generated the alerts, and then uploads the system logs to Dell. In certain conditions, if required by Dell technical support, you may be required to manually collect the system logs and send it to Dell.

To send the system logs manually:

i. Click the **Devices** tab.
ii. Select an IDRAC7 device in the **Device Inventory** table.
iii. Click **Send System** logs.

The collection tool is invoked and the generated system log collection is uploaded to Dell.

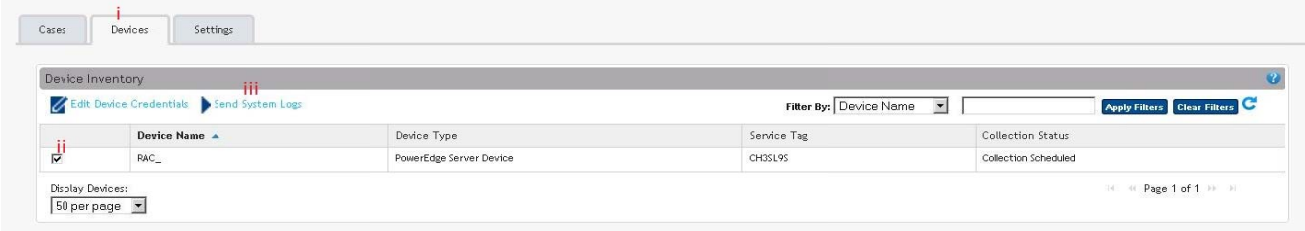


Figure 16 Sending system logs manually

Conclusion

Dell SupportAssist identifies hardware failures on supported devices quickly and more accurately. It automates and streamlines the support process steps without much interaction from your side. With SupportAssist, integrated with OpenManage Essentials, you have a single systems management console to remotely monitor and manage your environment, giving you instant insight into how your systems are performing at all times.