Managing Dell EMC ScaleIO Ready Nodes using Dell EMC OpenManage Essentials

ScaleIO Ready Node is currently not available in the Greater China region—China, Taiwan, Hong Kong, and Macau.
## Contents

Executive summary .............................................................................................................................. 4

1 Introduction .................................................................................................................................... 5
  1.1 Audience .............................................................................................................................. 5
  1.2 Scope ................................................................................................................................... 5

2 Infrastructure Components ............................................................................................................ 6
  2.1 ScaleIO ................................................................................................................................ 6
  2.2 ScaleIO Ready Nodes ......................................................................................................... 7
  2.3 OpenManage Essentials (OME) .......................................................................................... 7
  2.4 Component Versions ........................................................................................................... 8

3 Management and monitoring of ScaleIO Ready Nodes ................................................................. 9
  3.1 Discovery and inventory of ScaleIO Ready Nodes ............................................................. 9
  3.2 Firmware updates and compliance on a ScaleIO Ready Node ........................................ 11
  3.3 Enforce device compliance on a ScaleIO Ready Node .................................................... 19
  3.4 Configure system alerts and notifications .......................................................................... 22
  3.5 ScaleIO Ready Node lockdown ......................................................................................... 25
  3.6 Monitor health of ScaleIO Ready Nodes ........................................................................... 26

4 References .................................................................................................................................. 29
## Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2017</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
Executive summary

The Dell EMC ScaleIO Ready Nodes help reduce time-to-value for customers who are building a ScaleIO environment. These pre-validated, tested, and optimized server nodes help deploy an enterprise-ready ScaleIO software-defined storage (SDS) infrastructure.

This white paper provides operational guidance on how to use Dell OpenManage Essentials (OME) to manage and monitor ScaleIO Ready Nodes. It explains how to configure and use OME to:

- Discover the ScaleIO Ready Nodes and perform inventory
- Update BIOS/firmware of ScaleIO Ready Nodes in a non-disruptive manner
- Enforce device compliance using a configuration baseline
- Configure system alerts and notifications
- Prevent unauthorized modification of system configuration using system lockdown
- Monitor the health of ScaleIO Ready Nodes
1 Introduction

The benefits of server virtualization are well understood in the modern data center. Dell EMC ScaleIO SDS applies the virtualization principles of abstraction, pooling, and automation to local storage in standard x86 servers, creating a high-performance shared storage service without the need for conventional storage arrays.

The Dell EMC ScaleIO Ready Node is the pre-validated, tested, and optimized building block for a software-defined block storage system that combines Dell EMC PowerEdge servers with ScaleIO software. This solution reduces the time IT organizations spend in planning and deploying a new infrastructure that is scalable and flexible.

However, IT administrators managing the ScaleIO Ready Node environment face several challenges such as managing system updates, tracking qualified versions of BIOS/firmware, and ensuring correct system configuration settings.

This white paper addresses these challenges and describes the procedure to update ScaleIO Ready Nodes to a qualified BIOS/firmware version. It also discusses how to enforce device compliance by using a configuration baseline within the Dell EMC ScaleIO Ready Node environment using OME.

1.1 Audience

The audience for this paper includes sales engineers, field consultants, IT administrators, customers and anyone else interested in configuring and using OME to manage and monitor Dell EMC ScaleIO Ready Nodes.

Readers are expected to have an understanding and working knowledge of ScaleIO, VMware, OME, and iDRAC.

1.2 Scope

As of the writing of this paper, OME supports only one source catalog. Therefore, it is recommended to use a separate instance of OME to manage the ScaleIO Ready Nodes. ScaleIO supports multiple operating systems and hypervisors including Windows, RHEL, ESXi, Hyper-V, and KVM. This document provides guidance only for ScaleIO Ready nodes based on the VMware vSphere environment.

This paper does not intend to provide detailed information about the ScaleIO architecture. For more information about ScaleIO architecture, see the Dell EMC ScaleIO Basic Architecture Documentation listed in the reference section. The document does not provide deployment guidelines for ScaleIO Ready Node, VMware vCenter, and OME.
2 Infrastructure Components

The following diagram shows various components of a hyper-converged ScaleIO Ready Node deployment. OME and ScaleIO GUI are installed on Windows virtual machines hosted on the management cluster along with vCenter Server Appliance (VCSA) and ScaleIO Gateway VM. The following subsections provide a high level overview of the key components.

![Diagram of Infrastructure Components](image)

### Infrastructure components

#### ScaleIO

ScaleIO is a software solution that uses existing server storage in application servers to create a server-based storage area network (SAN). This SDS environment gives all member servers access to the unused storage in the environment, regardless of which server the storage is on. ScaleIO combines different types of storage (hard disk drives, solid-state disks and other persistent storage devices) to create a shared block storage. It is hardware agnostic and supports installation on dedicated physical and/or virtual application servers. Since ScaleIO does not require any dedicated SAN fabric or switch, it reduces the cost and complexity involved in using a traditional SAN.

ScaleIO consists of three main components:

**ScaleIO Data Client (SDC):** The SDC is a lightweight, block device-driver that presents ScaleIO shared block volumes to applications. The SDC runs on the same server as the...
application. This enables the SDC to fulfill IO requests issued by the application regardless of where the particular data blocks physically reside.

**ScaleIO Data Server (SDS):** The SDS manages the local storage that contributes to the ScaleIO storage pools. The SDS runs on each of the servers that contribute storage to the ScaleIO system. The SDS performs the back-end operations that SDCs request. For ESXi environments, the SDS driver is installed on the ScaleIO Virtual Machine (SVM) that runs on the local storage on each host.

**MetaData Manager (MDM):** The MDM configures and monitors the ScaleIO components. It contains all the metadata required for ScaleIO operations. For ESXi environments, the MDM driver is installed on the ScaleIO Virtual Machine (SVM) that runs on the local storage on each host.

### 2.2 ScaleIO Ready Nodes

Dell EMC ScaleIO Ready Nodes combine Dell EMC PowerEdge servers and ScaleIO software to create a reliable, quick, and easy-to-deploy building block for software-defined storage (SDS). Customers can take advantage of the scalability of ScaleIO on a rack-optimized 14G PowerEdge server designed to reduce the time spent in planning and deploying new infrastructure. ScaleIO Ready Nodes are tested and validated. Therefore, customers deploying a hyper-converged system can depend on this optimized building block to provide the resiliency and availability for their business demands.

Dell EMC ScaleIO Ready Nodes are tuned and optimized for ScaleIO. This includes checking that all components follow Dell EMC approved manufacturers’ lists (AMLs) for firmware, BIOS versions, hardware compatibility list (HCL) lookup and driver downloads, optional VMware ESXi installation, and driver installation.

### 2.3 OpenManage Essentials (OME)

OME is a lightweight, web-based, one-to-many console that provides a comprehensive view of Dell EMC systems, devices and its components in an enterprise network. It simplifies hardware management through the ease of use and automation. OME is interoperable with other Dell EMC tools and services like Dell Repository Manager (DRM). It is a single point for stack management and supports several third party integrations including VMware vCenter.

Designed for easy installation and use, OME also monitors the health status of both Dell and multi-vendor hardware environments—including anytime, anywhere access to status and alerts through OpenManage Mobile-equipped handheld devices. OME also makes it simple and quick to discover, provision, deploy, configure and monitor PowerEdge servers and its components.

In addition, OME performs extensive asset reporting. It tracks contract warranty and expiration information for discovered assets, which can be viewed through predefined reports. Field-replaceable unit and service-tag reporting are also included. The OME dashboard, automated alerts, and asset reporting functionality are designed to provide administrators with relevant and actionable information about their Dell hardware assets.
Note: For ScaleIO Ready Node customers using OpenManage Essentials, Dell EMC recommends the purchase of iDRAC Enterprise with OpenManage Essentials Server Configuration Management license. The OpenManage Essentials Server Configuration Management license is required for complete server configuration management capabilities.

For information about how to install OME, refer to the documentation Installing Dell EMC OpenManage Essentials listed in the reference section.

2.4 Component Versions

The following table lists the versions of software components used in this solution. For guidance on newer versions of this document refer the following link:

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScaleIO</td>
<td>2.0.1.3</td>
</tr>
<tr>
<td>OME</td>
<td>2.3</td>
</tr>
<tr>
<td>VMware vSphere ESXi</td>
<td>6.0u3</td>
</tr>
<tr>
<td>VMware vCenter Server Appliance</td>
<td>6.0u3</td>
</tr>
</tbody>
</table>
3 Management and monitoring of ScaleIO Ready Nodes

Administrators can use OME to perform the following operational aspects of managing and monitoring the ScaleIO Ready Nodes:

**Discovery and inventory of ScaleIO Ready Nodes:** ScaleIO Ready Nodes can be discovered and inventoried using OME. After Ready Nodes are discovered and inventoried in a ScaleIO cluster, complete hardware configuration information (including disk information) and BIOS and firmware versions of all the nodes are available from a single OME console.

**Firmware updates and compliance on a ScaleIO Ready Node:** OME can be used to simplify firmware updates of all the Ready Nodes. Using a catalog, all the Ready Nodes can be updated seamlessly to a qualified set of BIOS/firmware.

**Device compliance on a ScaleIO Ready Node:** OME can be used to track BIOS and other system configuration. A system configuration baseline can be first established that saves all the system configuration. Whenever the configuration needs to be updated, the baseline is updated and OME can be used to apply this update to all the nodes in the ScaleIO cluster.

**Configure system alerts and notifications:** ScaleIO Ready Nodes generate SNMP alerts for hardware events. OME can be used to monitor these alerts from all the ScaleIO Ready Nodes. Administrator can then configure actions to specific alerts such as generating email notifications upon disk failures.

**System lockdown:** System lockdown is a new capability introduced in PowerEdge 14th generation servers that prevents unauthorized or unintentional modification of the system configuration. Administrators can put a ScaleIO Ready Node under System Lockdown so that any updates to BIOS/IDRAC configuration settings and firmware updates are blocked.

**Monitor health of ScaleIO Ready Nodes:** OME can be used to monitor the health status of all the nodes in a ScaleIO cluster, including hardware health information.

The following subsections describe each task in detail.

### 3.1 Discovery and inventory of ScaleIO Ready Nodes

OME supports agentless discovery and inventory of ScaleIO Ready Nodes by communicating directly with server’s integrated Dell Remote Access Controller (iDRAC) using WS-MAN protocol. Once discovered, the ScaleIO Ready Node is inventoried automatically and provides detailed information about the Ready Node and all of its components such as processor, memory, NIC, hard disks, BIOS version, controller firmware version and so on.

The following steps can be used to discover and inventory ScaleIO Ready node using OME:

1. Launch OME console, and then click **Start → Dell OpenManage Applications → Essentials.**
2. Access the OME discovery and inventory portal by using the following steps:
   a. Click **Manage → Discovery and Inventory.**
   b. Provide a discovery IP range, click **Add**, and then click **Next.**
   c. Select **iDRAC** as the Device Type, and click **Next.**
   d. Provide iDRAC credentials, click **Next** and **Finish.**
There are also options for excluding IP ranges while discovery, scheduling discovery and inventory etc. After discovering the nodes, a custom group can be created and respective devices can be added to that group for easy management and monitoring. Create a custom device group by using the following steps:

1. Select Add New Group.
2. Specify a name (for example, ScaleIO Ready Nodes) for the group, and click Next.
3. Select ScaleIO Ready Nodes from the tree, click Next and Finish.

Once the group is created, it will be displayed in the home portal filter by drop-down list. The Ready Node hardware configuration including processor, memory, disk, OS and firmware versions is listed for each discovered and inventoried node as shown in the following screenshot:

### Processor Information

<table>
<thead>
<tr>
<th>Family</th>
<th>Speed (MHz)</th>
<th>Core</th>
<th>Brand</th>
<th>Model</th>
<th>Staging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel(R) Xeon(TM)</td>
<td>2.05</td>
<td>24</td>
<td>Intel</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Intel(R) Xeon(TM)</td>
<td>2.00</td>
<td>24</td>
<td>Intel</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Memory Device Information

<table>
<thead>
<tr>
<th>Size (MB)</th>
<th>Type</th>
<th>Bank</th>
<th>Asset</th>
<th>Type</th>
<th>Details</th>
<th>Failure Mode</th>
<th>Form Factor</th>
<th>Name</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>B</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>A</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>B</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>A</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>B</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>A</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>B</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
<tr>
<td>32768</td>
<td>DDR4</td>
<td>A</td>
<td>N/A</td>
<td>DDR4</td>
<td>DIMM</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Hynix Semiconductor</td>
</tr>
</tbody>
</table>

### Firmware Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Enclosure ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS</td>
<td>1.1.7</td>
<td>0</td>
<td>BIOS</td>
</tr>
<tr>
<td>Lifecycle Controller</td>
<td>3.03.00.00</td>
<td>0</td>
<td>Lifecycle Controller</td>
</tr>
</tbody>
</table>

Figure 2  Sample screenshot of OME showing processor, memory and BIOS information of a ScaleIO Ready Node
### 3.2 Firmware updates and compliance on a ScaleIO Ready Node

OME can be used to perform firmware updates on ScaleIO Ready Nodes. The following are the high level steps for updating the firmware version on a ScaleIO Ready Node:

1. **Satisfy prerequisites for maintenance**
2. **Place SDS and ESXi in maintenance**
3. **Obtain the firmware catalog**
4. **Update ScaleIO Ready Node**
5. **Verify compliance and exit maintenance modes**

![Workflow diagram](image)

#### 3.2.1 Meet prerequisites for maintenance

The following prerequisites should be met:

- ESXi servers should be in a cluster with high availability (HA), Distributed Resource Scheduling (DRS) and vMotion enabled. This will allow the administrator to update and reboot the server without impacting the virtual machines' availability.
- The administrator must verify in the ScaleIO GUI that:
  - No SDC or SDS is disconnected.
  - No other Fault Unit (standalone SDS) is in Maintenance Mode.
  - There must be adequate space on other SDSs for additional backup.
  - No rebuild or rebalance is running in the background.
  - No degraded capacity exists.
  - No SDS device is in error state.
Figures 4 and 5 show the overview and health of a sample ScaleIO cluster with four ScaleIO Ready Nodes:

- Ensure that the MDM cluster is not in degraded mode, including the Tie-Breaker. This can be verified using ScaleIO vSphere plugin, as illustrated below.

- If the node that is going to be updated is a Master MDM, switch MDM ownership to a slave MDM using the following steps:
  - Identify the MDM master from the ScaleIO vSphere plugin, as shown in the figure below.
13 Managing Dell EMC ScaleIO Ready Nodes using Dell EMC OpenManage Essentials

3.2.2 Place SDS and ESXi in Maintenance Mode

After ensuring that the above pre-requisites are met and before performing the system update, the ScaleIO Ready Node must be placed in Maintenance Mode. There are two maintenance modes: SDS Maintenance Mode and ESXi Maintenance Mode. The ScaleIO Ready Node must be placed in both these maintenance modes.

3.2.2.1 SDS Maintenance Mode

ScaleIO SDS Maintenance Mode enables a server that hosts an SDS to be restarted with minimal impact on the ScaleIO cluster. This avoids the disruption and effort caused by disorderly shutdown. ScaleIO system always uses two copies of user data. Invoking Maintenance Mode ensures that two copies of all the writes created during maintenance to an SDS or Fault Set are kept in both primary location and a new location. This copy prevents data loss if a single failure occurs. When the SDS or Fault Set is returned from Maintenance Mode, only the new writes are required to be resynchronized, thus minimizing data transfer during and after the update.

While an SDS is in Maintenance Mode, application IOs are not interrupted. Any number of member servers inside a Fault Set can be in Maintenance Mode at the same time. In addition, Fault Sets in different Protection Domains can be in Maintenance Mode at the same time. While an SDS is in Maintenance Mode, most ScaleIO operations (such as adding a volume) cannot be performed in the Fault Set, Protection Domain, or Storage...
Pool in which the SDS and its devices reside. It should also be noted that only one Fault Unit (standalone SDS) can be in Maintenance Mode at any given time.

It is recommended to use Maintenance Mode when there is relatively low system activity, as the time taken by an SDS to exit Maintenance Mode depends on the amount of data that needs to be synchronized back into the server.

To place an SDS in Maintenance Mode, perform the following steps (as illustrated in Figure 8):

1. Log in to the ScaleIO GUI as an admin user.
2. In the Backend view, select the desired SDS.
3. Select Enter Maintenance Mode, and click OK.

![ScaleIO GUI showing how to enter Maintenance Mode](image)

### 3.2.2.2 ESXi Maintenance Mode

After placing the Ready Node in SDS Maintenance Mode, perform the following steps to place the server in ESXi Maintenance Mode:

1. Using vCenter GUI, gracefully shutdown the SVM located on the server host that needs to be updated.
2. Enter ESXi Maintenance Mode. This automatically migrates all the VMs to other nodes in the cluster.

### 3.2.3 Obtain the firmware catalog for ScaleIO Ready Nodes

For ScaleIO Ready Node, the recommended option is to use a ScaleIO specific custom catalog for a qualified set of firmware and BIOS. The catalog file along with all the qualified firmware can be download as a ZIP file from the following location: [https://support.emc.com/downloads/42216_ScaleIO-Ready-Node--PowerEdge-14G](https://support.emc.com/downloads/42216_ScaleIO-Ready-Node--PowerEdge-14G)

Once downloaded, extract the ZIP file to a location in the OME server.

Note that the current version of OME supports only one source catalog. The downloaded custom catalog file and qualified firmware are applicable only to 14G ScaleIO Ready Nodes.
Perform the following steps to select a catalog source:

1. From OME, click Manage → System Update → Select a Catalog Source.
2. Select Use repository manager file, and browse to the location where the ZIP file is extracted, select Catalog.xml file, and click Import now.

3.2.4 Update ScaleIO Ready Node

Use the OME to update the ScaleIO Ready Node by performing the following steps:

1. Click Manage → Devices. Verify that the Ready Node is discovered and classified under RAC device group. The discovered iDRAC will be present either under the compliant or non-compliant systems section in the compliance pie-chart.
2. Click System Update → Advanced Settings.
3. Set preferred update mode to Out-of-Band (iDRAC).
4. Click Ok to save the settings and close the Advanced Settings window. The figure below shows a screenshot of the advanced settings window:

![Advanced Settings](image)

Figure 9 System update settings

5. If the discovered iDRAC is non-compliant, it will be listed under Non-Compliant tab. Select the iDRAC that is non-compliant and the package to be updated on the system and click Apply Selected Updates.
6. When the User Preferred Delivery Mode is set to iDRAC, the Update Method will display Out-of-Band for all the available components.
7. The System Update Task window is displayed. Type a task name.
8. Select the Run now option.
9. Enter the user name and password of the iDRAC.
10. Click Finish to create system update task.

The system update task is created with the name provided and “- iDRAC” appended to the task name. This indicates that the preferred mode of delivery is Out-of-Band. After all
the selected components (DUPs) are successfully applied on the selected managed system, the task status is set to Complete. About 20 minutes after the task is complete, an auto inventory task is initiated to gather the updated inventory information.

3.2.5 Verify compliance and exit Maintenance Mode

After the server is rebooted and re-inventoried by OME, ensure that the updated ScaleIO Ready Node is compliant.

To view compliant servers:

1. Click Manage → System Update.
2. In System Update, select the Compliant Systems tab.

To view non-compliant systems:

1. Click Manage → System Update.
2. In System Update, select the Non-Compliant Systems tab.
3. Systems with drivers and firmware versions that are different from the catalog are displayed.

3.2.5.1 Exit ESXi Maintenance Mode and verify ScaleIO cluster state

After updating the ScaleIO Ready Node, perform the following steps to exit the Ready Node from ESXi Maintenance Mode:

1. Verify the status of host hardware components using vSphere web client (as illustrated by an example screenshot below).

![vSphere web client showing ESXi hardware sensor status](image)

Figure 10  vSphere web client showing ESXi hardware sensor status

2. Exit ESXi Maintenance Mode.
3. Start the SVM hosted on that node.
4. Verify that the SDC state is connected and the SDC drivers are loaded using the following steps:
   a. SSH to master MDM as root and change the user role to SuperUser (admin).
   b. Verify that the state of SDC is connected using the following command and substituting [SDC Name] with name of the corresponding SDC:

   ```
   scli --query_sdc --sdc_name [SDC Name]
   ```

   Figure 11 Command and example output to illustrate SDC connection state

   c. SSH to the corresponding ESXI server.
   d. Verify the SDC state in ESXI by using the following command:

   ```
   esxcli system module list | grep scini
   ```

   e. The output must be "scini true". This implies that the SDC driver is loaded and enabled.

   Figure 12 Command and output to illustrate SDC state in ESXI

5. Check the SDS state using the following command and verify the states (membership-state, connection-state and SDS-state) of all devices. Replace [SDS Name] with the name of a corresponding SDS:

   ```
   scli --query_sds --sds_name [SDS Name]
   ```

   Figure 13 Command and example output that show SDS connection and device state

6. Query all SDS connectivity status within a Protection Domain with the following command and ensure that all SDSs are connected. Replace [Protection Domain Name] with the name of a corresponding protection domain.

   ```
   scli --query_sds_connectivity_status --protection_domain_name [Protection Domain Name]
   ```
7. Query the cluster to verify that the cluster state is normal by using the following command:

```
scli --query_cluster
```

3.2.5.2 Exit SDS Maintenance Mode

Once the validation steps are complete, place the SDS back into regular service by exiting the Maintenance Mode. This will begin a ScaleIO operation to Rebuild and Rebalance the data to ensure protection and load balancing.

To exit the Maintenance Mode, perform the following steps:

1. Log in to the ScaleIO GUI as an admin user.
2. In the Backend view, select the desired SDS.
3. Select Exit Maintenance Mode, and click OK.

The status area at the bottom of the window indicates when the operation is complete. Once the operation is successfully complete, the SDS returns to normal operation, and data deltas collected on other SDSs during the maintenance period are copied back to the SDS.

After exiting Maintenance Mode, perform the following steps to verify that operations are normal:

1. Ensure that all SDCs and SDSs are connected using ScaleIO GUI.
2. Check for alerts in ScaleIO GUI.
3. Ensure that rebuild operations are complete before initiating maintenance on the next node.

3.3 Enforce device compliance on a ScaleIO Ready Node

OME can be used to track BIOS, iDRAC and other system configuration. A device configuration baseline can be first established and all the ScaleIO Ready Nodes can be updated to meet that configuration baseline.

The following are the high level steps for enforcing device compliance on a ScaleIO Ready Node:
Managing Dell EMC ScaleIO Ready Nodes using Dell EMC OpenManage Essentials

3.3.1 Configure the Deployment File Share

Before creating or deploying a configuration template from a device, a deployment file share on the server running OME must be configured. The deployment file share temporarily stores the configuration file that is used to retrieve and apply the configuration settings on a target server or chassis. To configure the deployment file share:

1. Click Deployment. In the Common Tasks pane, click File Share Settings. The File Share Settings window is displayed.
2. Type the domain\user name and password of the server running OME in the appropriate fields.
3. Click Apply. If the file share is configured correctly, the File Share Status displays Ok.

3.3.2 Create a Device Configuration Baseline and Associate Devices to the Baseline

To create a baseline, perform the following steps:

1. Click Manage → Configuration.
2. In the Common Tasks pane, click Create Baseline. The Create Baseline Wizard is displayed.
3. In the Name field, type a name for the baseline.
4. Select one of the following:
   a. Create from File: To create a baseline by importing the XML template. The ZIP file mentioned in Section 3.2.3 also includes a configuration baseline XML file for 14G ScaleIO Ready Nodes.
   b. Create from Device: To create a baseline from a device.
5. If Create from Device option is selected, perform the following:
   a. Select the device type Server.
   b. Select a device from the All Applicable Devices tree.
   c. Under Execution Credentials, provide the device credentials that have the Administrator rights.

6. Click Finish.

The Associate Devices to a Baseline task designates the baseline to be used for verifying the compliance status of target devices. To associate devices to a baseline, perform the following steps:

1. Click Manage → Configuration.
2. In the Common Tasks pane, click Associate Devices to a Baseline.
3. The Associate Devices to a Baseline wizard is displayed.
4. On the Select Baseline page, click Server Baseline.
5. Select a device configuration baseline from the list, and click Next.
6. On the Select Devices page, select the target devices from the All Applicable Devices tree, and then click Finish.

3.3.3 Meet prerequisites for maintenance and place SDS and ESXi in Maintenance Mode

Select a non-compliant device (such as a device with incorrect BIOS and/or iDRAC settings) and place it in Maintenance Mode. Refer to Section 3.2.1 and 3.2.2 for the steps. Note that all the steps needs to be executed manually for each non-compliant ScaleIO Ready Node in the cluster (one at a time).

3.3.4 Remediate Non-Compliant Device

Perform the following steps to remediate the ScaleIO Ready Nodes that are not compliant with the associated device configuration baseline:

1. Click Manage → Configuration → Make Device(s) Complaint. The Name page is displayed.
2. Enter the Name for the remediation task, and click Next.
3. On the Select Devices page, the list of non-compliant servers with the corresponding non-compliant attributes is displayed. Select the non-compliant device from the list, and click Next. Ensure that the selected non-compliant device is already in Maintenance mode.
4. On the Options page, select Automatic Server Reboot and click Next.
5. On the Set Schedule page:
   a. Select Run now.
   b. Under Execution Credentials, type the credentials of the selected device, and click Next.
6. On the Summary page, review the information that has been provided, and then click Finish.

3.3.5 Verify Device Compliance and exit Maintenance Mode

After the Device Configuration Baseline has been applied to a device (ScaleIO Ready Node), its compliance should be verified. Once the compliance has been verified, the device can be brought out of the Maintenance Mode.
To view the compliance status of devices on the associated configuration baseline:

1. Click **Manage → Configurations → Device Compliance Portal**. The **Device Compliance** graph and grid display the compliance status of the devices.
2. Click the **Device Compliance** graph to verify the compliance status of the device.
3. Once the compliance of the device has been verified, bring the device out of the Maintenance Mode by following the procedures in Section 3.2.5.1 and 3.2.5.2.

### 3.4 Configure system alerts and notifications

PowerEdge servers generate alert for hardware events through iDRAC. These alerts can be filtered and viewed through OME. Actions such as email notifications can be configured on these filtered alerts. This section explains the procedure to configure iDRAC alerts using OME. It also describes how to view alerts and configure email alerts and warranty notifications using OME.

#### 3.4.1 Configure iDRAC alerts using OME

This method helps in configuring all the iDRACs simultaneously. Separate RACADM command line tasks must be created in OME to enable alerts, set the destination IP address (OME server IP), set the community name, and enable all possible alerts.

1. Create a batch file with the following commands:

   ```
   racadm -r %1 -u %2 -p %3 config -g cfgipmilan -o cfgipmilanalertenable 1
   racadm -r %1 -u %2 -p %3 eventfilters set -c idrac.alert.all -a none -n snmp
   racadm -r %1 -u %2 -p %3 set idrac.snmp.alert.1.enable 1
   racadm -r %1 -u %2 -p %3 set idrac.snmp.alert.1.destaddr %4
   ```

2. Save the batch file to the OME server.
3. From any web browser, open the OME console and select **Manage → Remote tasks → Create Command line task**.
4. In the Command field, enter the path to the batch file.
5. In the Arguments field, enter the following:

   ```
   $rac_ip $username $password <IPofOMEServer>
   ```

   **Note:** Replace `<IPofOMEServer>` with the IP address for the SNMP destination.

6. Enter iDRAC credentials in the `$USERNAME` and `$PASSWORD` fields, and click **Next**.
7. Select the iDRACs to be enabled for SNMP traps, and then click **Next**.

8. Enter credentials with the appropriate privileges to run the task on the system, and click **Finish**.
3.4.2 Create email notifications

Perform the following steps to configure email notifications when an alert is received:

1. Select **Manage → Alerts → Common Tasks → New Alert Email Action.**
2. In the **Name** and **Description** fields, provide email alert action name and description respectively, and then click **Next.**
3. In the E-mail Configuration window, enter the following information and then click **Next.**
   a. Provide e-mail information for the To: and From: recipients. Separate each recipient or distribution list with a semi-colon.
   b. Customize the e-mail message format with any of the following substitution parameters as shown in the following screenshot:

![Alert Email Action E-mail Configuration](image)

   - Click **Email Settings** and provide SMTP server name or IP Address to test e-mail settings, and click OK.
   - Click **Test Action** to send test e-mail.
4. In **Severity Association**, assign the alert severity, and then click **Next.**
5. In **Categories and Sources Association**, assign the alert categories or alert sources, and then click **Next.**
6. In **Device Association**, select ScaleIO Ready Nodes device group, then click **Next.**
7. By default, the Email Notification is always active. To limit activity, in **Date Time Association**, enter a date range, time range, or days, and then click **Next.**
8. In **Summary**, review the inputs and click **Finish.**
3.4.3 Configure warranty email notifications
OME can be configured to send a warranty notification of ScaleIO Ready Nodes at periodic intervals through email. Perform the following steps to configure Warranty Email Notifications:

1. Click Settings → Warranty Notification Settings.
2. Under Warranty Email Notifications, select Enable Warranty Email Notifications.
3. In the To field, type the email addresses of the recipients.
4. In the From field, type the email address from which the warranty notification email is to be sent.
5. To set the criteria for the devices to be included in the warranty notification email, in the All Devices with x Days or less of warranty field, select the number of days.
6. To set the desired frequency for receiving the warranty notification email, in the Send email every x Days field, select the number of days.
7. To include devices with expired warranty or no warranty information in the warranty notification email, select Include Expired Warranties.
8. In the Next Email will Send On field, select the desired date and time to receive the next warranty notification email.
9. Click Email Settings to configure the SMTP server.
10. Click Apply.

Figure 22 Screenshot showing warranty notification settings

3.5 ScaleIO Ready Node lockdown
The Dell EMC 14th generation ScaleIO Ready Node servers offer a new capability called System Lockdown mode. After the initial deployment/update is complete and the ScaleIO cluster is functional, Dell EMC recommends locking down the system configuration so that any updates to BIOS/iDRAC configuration settings and firmware updates are blocked. This ensures that the system configuration stays compliant to a validated baseline.

In this mode, system configuration cannot be changed from any of the out-of-band or in-band interfaces that are supported. This does not prevent the system from running routine monitoring and maintenance tasks such as power operations, power budget and profiles, identifying operations such as blinking drive LEDs, and running diagnostics.
Note that the system lock down feature will be effective only when non-root or non-admin users are configured on iDRAC to perform the activities allowed during system lockdown mode.

Perform the following steps to enforce system lockdown mode by using RACADM command line task:

1. Open the OME console and select Manage → Remote tasks → Create Command line task.
2. In the Command field, add: `set idrac.lockdown.systemlockdownmode enabled`.
3. Click Next, and select the servers to enable the system lockdown mode.
4. Click Next, enter iDRAC credentials, and click Finish.

3.6 Monitor health of ScaleIO Ready Nodes

Once ScaleIO Ready Nodes are discovered, administrators can monitor the health of the Ready Nodes through OME’s dashboard. The dashboard provides an at-a-glance view and a scoreboard displaying the health of the ScaleIO infrastructure.

OME polls the status of all ScaleIO Ready Nodes at regular intervals and reflects the status in the device tree. Status polling performs a health and power check for all discovered servers.

The Devices by Status web part displayed on the Home portal provides a pie-chart representation of the overall health status of all the servers. This chart is divided into multiple segments based on the severity of all the discovered nodes as shown in the following figure. The user can click any of the segments in the chart to drill-down to a more detailed view of the overall status of the corresponding devices.
To view alerts page, alert logs, and alert categories, perform the following steps:

- To view the alerts page, from OME, click Manage → Alerts.
- To view alert logs, click Manage → Alerts → Alert Logs.
- To view alert categories, click Manage → Alerts → Alert Categories.

The following screenshot shows a sample alert message when a disk drive is removed from one of the ScaleIO Ready Node. After action on an alert is completed, flag the alert as acknowledged. Acknowledging an alert indicates that it has been resolved or does not require further action.

Track faulty servers by using the rack location in a data center, as shown in the following screenshot. For more details on configuring data center location information, refer to the iDRAC user guide.
To troubleshoot issues, view the hardware logs as shown in the following screenshot:

Figure 27  Screenshot showing hardware logs of a ScaleIO Ready Node

In addition, performance information about CPU, memory and IO usage of ScaleIO Ready Nodes can also be viewed as shown in the following screenshot. This will be useful for performance monitoring and analyzing the resource usage trends of the servers.

Figure 28  Sample screenshot showing performance information of a ScaleIO Ready Node
4 References

- Dell EMC OpenManage Essentials Version 2.3 User's Guide
- Installing Dell EMC OpenManage Essentials (OME)
- Updating Dell Server Hardware with Dell OpenManage Essentials
- EMC ScaleIO Basic Architecture Documentation
- DELL EMC ScaleIO for VMware Environments
- EMC ScaleIO Design Considerations and Best Practices
- Dell Validated System for EMC ScaleIO
- EMC ScaleIO v2.0.x User Guide (included with the ScaleIO software package)