Monitoring & configuring Server Group by using iDRAC Group Manager

This Dell EMC technical white paper introduces the iDRAC Server Group Manager feature and describes the procedures to effectively set up and manage a group of Dell PowerEdge servers.

Dell Engineering
June 2017

Authors

Server Group Manager Team

Server Solutions Group

A Dell EMC Technical White Paper

Revisions

Date	Description
June 2017	Initial release

Contents

Revisions....2

Executive summary....5

1 Introduction....6

1.1 Terms and definitions....7

1.2 Network configuration requirements....8

1.3 Prerequisites....9

2 Group Manager workflows....10

2.1 Setting up and managing a local group....10

2.1.1 Create a local group....10

2.1.2 Joining a server group workflows....13

2.1.3 Detaching a server from a local group....16

2.2 Managing the group preferences....17

2.2.1 Changing server group name....17

2.2.2 Changing a group passcode....18

2.3 Deleting a local group....19

2.4 Monitoring and managing group inventory....20

2.4.1 Bookmarking Group Manager console address in a web browser....20

2.4.2 Accessing a Group Manager console from a member iDRAC home page....21

2.4.3 Accessing a group member iDRAC home page from Group Manager console....23

2.4.4 Performing power-control actions from Group Manager console....23

2.4.5 Accessing a group member virtual console....24

2.4.6 Exporting the Group Inventory....25

2.4.7 Exporting the Group Jobs audit log....26

2.5 Group Actions–Configure all iDRACs in the local group....26

2.5.1 Adding, removing, or updating iDRAC user....26

2.5.2 Setting up iDRAC email alert configuration....30

2.5.3 Cloning group email alert configuration settings....32

2.6 Group Job Manager – Jobs tracking and reporting....33

2.6.1 Feedback about job status and recovering from errors....33

2.7 Configuring Group Manager by using CLIs....36

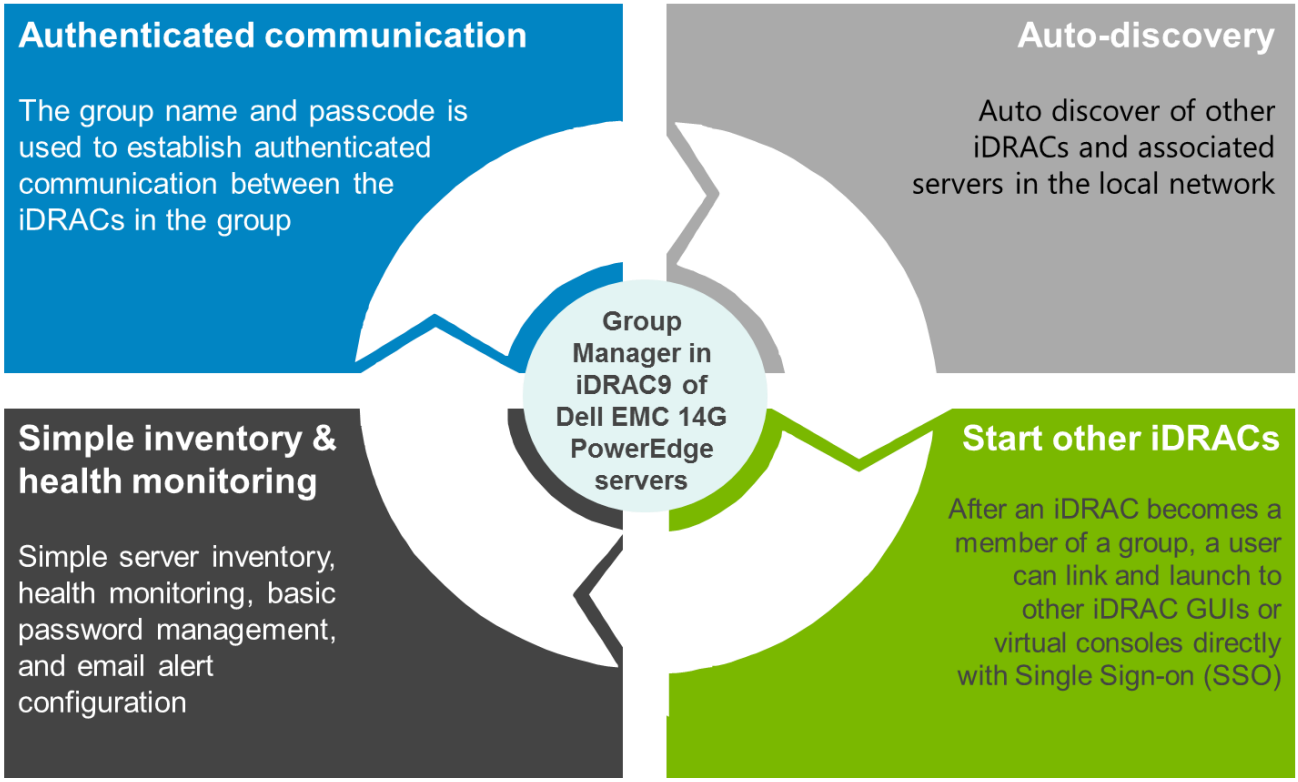
2.7.1 Configuring Group Manager by using WS-Man....36

2.7.2 Enabling or disabling the Group Manager feature....36

2.7.3 Group information 38
2.7.4 Joining an existing group 39
2.7.5 Leave a group 40
2.7.6 Deleting iDRAC local group 41
2.8 Configuring Group Manager by using RACADM 41
2.8.1 Enabling or Disabling the Group Manager feature 42
2.8.2 Group information 42
2.8.3 Joining an existing group 42
2.8.4 Leaving a group 42
2.8.5 Deleting iDRAC local group 42
3 Frequently asked questions and troubleshooting tips 43

Executive summary

The iDRAC Group Manager feature makes the basic server management tasks very simple. With an iDRAC9 Enterprise license, Group Manager provides built-in, one-to-many monitoring and inventory of local iDRACs and their associated 14th generation PowerEdge servers. It is ideal for small and mid-sized customers who do not want to install and maintain a separate monitoring console. However, Group Manager can scale to 99 additional nodes, making this a useful tool for many organizations, such as those IT admins who oversee server clusters. The prime functions of Group Manager are shown in the Infographics here.



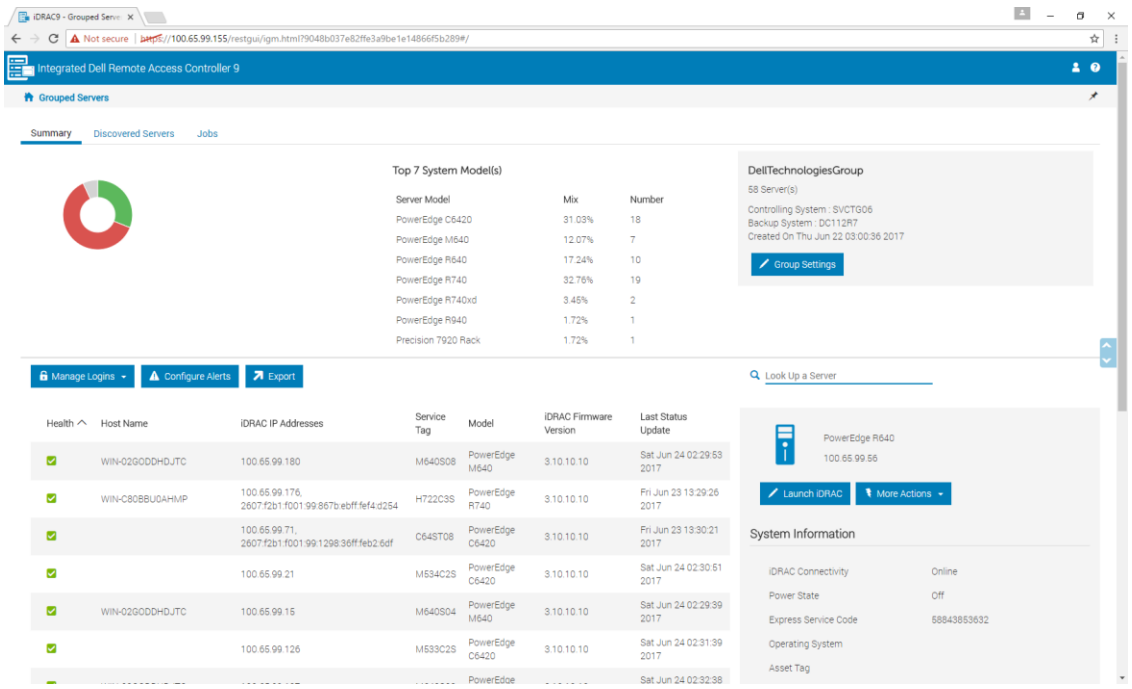
1 Introduction

With an iDRAC9 Enterprise license, Group Manager provides a simple 1XMany management console experience to monitor and manage a group of servers physically connected to the same link local network. Simplicity and ease of use are key tenets of Group Manager, which provides the ability to see a list of servers and quickly identify a server with an error and access that server with a single click. iDRAC Group Manager can:

- Auto-discover other iDRAC9s and associated servers, collect basic inventory, monitor health, perform basic password management and configure email alerting.
- Once an iDRAC has become a member of a group, administrative users can view a summary dashboard to determine the overall health of their group and link and launch to other member iDRAC GUIs or virtual consoles directly to troubleshoot issues without having to enter new credentials for each iDRAC connection.

Group Manager has three primary views: Summary, Discovered Servers, and Jobs. The Summary view provides a searchable dashboard for the health monitoring and inventory of all systems in the local group. The Discovered Servers view shows any iDRACs on the link local network that have been auto-discovered and have not been on-boarded to a group. The Jobs view shows the progress and history of group configuration actions. Group configuration actions include: setting up email alerting, adding a local iDRAC user, removing a local iDRAC user, changing a local iDRAC user password, changing the group passcode, changing the group name, and on-boarding newly discovered iDRACs. The screen shot here shows the **Summary** page of Group Manager.

The Group Manager workflows section describes the Group Manager workflows accomplished through web based GUI. The Configuring Group Manager by using CLIs section describes the scriptable workflows that can be accomplished by using WS-Man or RACADM CLIs.



The local group is uniquely identified by a user-defined group name and group passcode. The group name and passcode are used to establish authenticated and encrypted communication between the iDRACs in the group. After a group is created, Group Manager will automatically discover other enabled iDRACs in the local network and show them in a consolidated Discovered Servers view to enable user-driven quick onboarding into the group. Group Manager can be accessed from any iDRAC that has been configured to be part of the same group.

1. Click the **Open Group Manager** button on the iDRAC home page.
   The browser is redirected to the Group Manager **Summary** view.
2. The popup blockers may prevent the redirect. If that happens, disable popup blockers (allow popups) in the web browser, and then click **Open Group Manager**.

Up to 100 server nodes can be grouped under a server group and more than one server group can be set up in the local network, but an individual iDRAC can only be a member of one group at a time. To change (join a new group) group, iDRAC must first leave its current group, and then join the new group.

The iDRAC from where the group was created gets chosen as the primary controller of the group, by default. The primary controller iDRAC caches the group information and hosts the graphical user interface (GUI) workflows. The user does not define a dedicated Group Manager primary controller to control that group. The iDRAC members automatically self-select a new primary controller for the group, if the current primary goes offline for a prolonged duration, but that does not have any impact on the end user.

Only admin role (all privileges) iDRAC users have access to the Group Manager functionality. If a non-administrator user logs in to iDRAC, the Group Manager section remains invisible and inaccessible. Administrator users can seamlessly access the member iDRAC home page through single-sign-on from the Group Manager Summary screen.

1.1 Terms and definitions

For the purposes of this technical white paper, the following terms and definitions apply:

Summary View: The Group Manager Summary View (alternatively called the Group Manager home page) is broadly categorized into three sections. The first section shows rollup summary with aggregated summary details. The second section provides buttons for actions that are taken on the group as whole, and the third section displays the list of all iDRACs in the group.

Discovered Servers View: Discovered Servers displays the list of the iDRACs detected on the local network, which has not joined any group yet. For iDRACs to be displayed under Discovered Servers, Group Manager feature must be enabled in each iDRAC.

Group Jobs View: Jobs view allows the user to track the progress of a group job and helps with simple recovery steps to correct connectivity induced failures. The Jobs view allows the user to view the status of the last 50 jobs that have been run and any success or failures that has occurred. The user can use the jobs view to track the progress of the action across the group or to cancel an action that is schedule to occur in the future.

Primary Controlling System: Primary controlling system of the group is automatically selected. By default, it is the iDRAC from which the group was first configured. It hosts the Group Manager web interface by providing the GUI workflows. If a user logs in to any member and clicks Open Group Manager, the browser will be redirected to the primary controller through a single-sign-on.

Backup/Secondary Controlling System: Primary controller automatically selects a secondary controller to take over if the primary goes offline for an extended period of time (10 min. or more). If both primary and secondary goes offline for an extended duration (for more than 14 min.) a new primary and secondary controller gets selected. Keeps a copy of the Group Manager cache of members and group tasks.

Group Manager Single Sign On: All iDRACs in the group trust each other and are authenticated based on the group name and shared passcode secret. As a result an administrator user at a group member IDRAC is granted administrator-level privileges at any group member iDRAC when accessed through Group Manager Web interface single sign on. You can normally access the Group Manager home page from any member iDRAC by clicking the **Group Manager** button at iDRAC home page. Any member iDRAC home page can be seamlessly accessed from by double clicking the respective server row in the list at Group Manager home page. For auditing purposes, iDRAC logs <user>-<SVCTAG> as the user that logged on into peer members through Group Manager Single-Sign-On, where <SVCTAG> is the Service Tag of the iDRAC where the user <user> first logged in.

IDRAC Jobs and Job queue: iDRAC Job queue accessible from **Maintenance → Job Queue** provides a consolidated view of configuration actions performed at that server. Server configuration group actions performed through Group Manager is carried out on an iDRAC by using iDRAC Job Scheduler interface. Therefore, the audit log for any server configuration performed through Group Manager will be available in the iDRAC Job queue and Lifecycle logs.

1.2 Network configuration requirements

Group Manager uses IPv6 link local networking to communicate between iDRACs (excluding the web browser GUI). Link local communication is defined as non-routed packets which means any iDRAC separated by a router cannot be joined in a local group. If the iDRAC-dedicated port or shared LOM is assigned to a vLAN then the vLAN will also limit the number of iDRACs that can be joined in a group (iDRACs must be on same vLAN and traffic must not pass through a router).

When Group Manager is enabled, iDRAC enables an IPv6 Link Local address regardless of the iDRAC's current user defined network configuration. Group Manager can be used when iDRAC is configured for IPv4 or IPv6 ip addresses.

Group Manager uses mDNS to discover other iDRACs on the network and will send encrypted packets for normal inventorying, monitoring and management of the group using the link local IPv6 address. Using IPv6 link local networking means that the Group Manager ports and packets will never leave the local network or be accessible to external networks.

Ports (Specific to Group Manager unique functionality does not include all iDRAC ports)

- 5353 (mDNS)
- 443 (webserver) - configurable

- 5670 (Multicast group communication)
- C000 → F000 dynamically identifies one free port for each member to communicate in the group

1.2.1.1 Best networking practices

- Groups are intended to be small and on the same physical link local network.
- It is recommend to use the dedicated iDRAC network port for enhanced security. Shared LOM is also supported.

1.2.1.2 Additional network considerations

Two iDRACs that are separated by a router in the network topology are considered to be on separate local networks and cannot be joined in the same iDRAC local group. Meaning, if the iDRAC is configured for dedicated NIC settings, the network cable connected to IDRAC dedicated port in the rear of the server must be under a local network for all relevant servers.

If the iDRAC is configured for shared LOM network settings, the shared network connection used by both server host and IDRAC need to be connected under a local network for Group Manager to detect and onboard those servers into a common group. IDRACs configured with a mix of dedicated and shared LOM mode NIC settings could also be onboarded into a common group, if all the network connections do not pass through a router.

1.3 Prerequisites

- An Enterprise License is required on all iDRACs that are required to be grouped under a server group.
- Group Manager must be enabled.
- iDRACs must be connected on the same physical link local network. See Network configuration requirements.
- Group Manager is accessible only to administrator role user.
- Must be a 14G PowerEdge server with an iDRAC9.
- iDRAC must have an IP address that a web browser can connect to.

2 Group Manager workflows

This section describes the Group Manager tasks that can be performed by using web-based GUI.

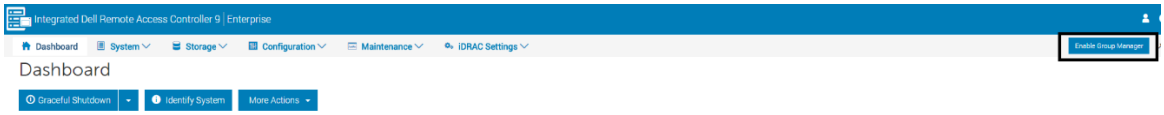
2.1 Setting up and managing a local group

Group Manager allows setting up more than one local iDRAC group on a local network. But, an individual iDRAC can only be a member of one group at a time. To change groups, iDRAC must first leave its current group and then join the new group. Group Manager welcome screen accessible from the iDRAC index page allows an administrator-privileged user to create a new server group or onboard that iDRAC into an existing local server group.

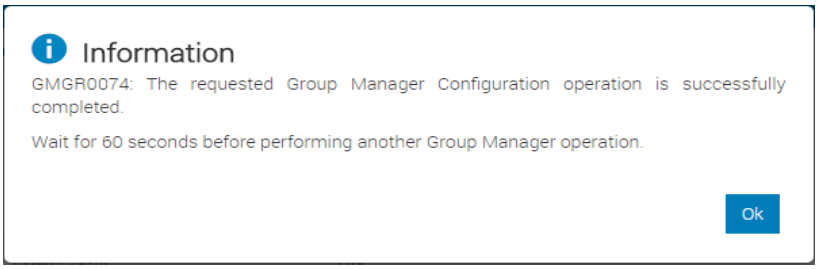
2.1.1 Create a local group

Group Manager can be ordered as ‘enabled’ or ‘disabled’, by default from the factory. If Group Manager is ordered as ‘Disabled’:

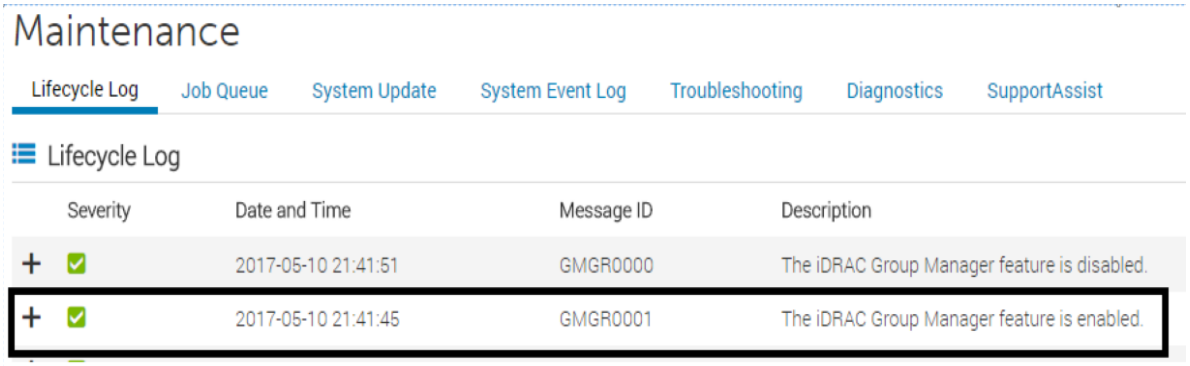
1. Enable it by logging in to iDRAC, and then clicking **Enable Group Manager** in the upper-right corner.



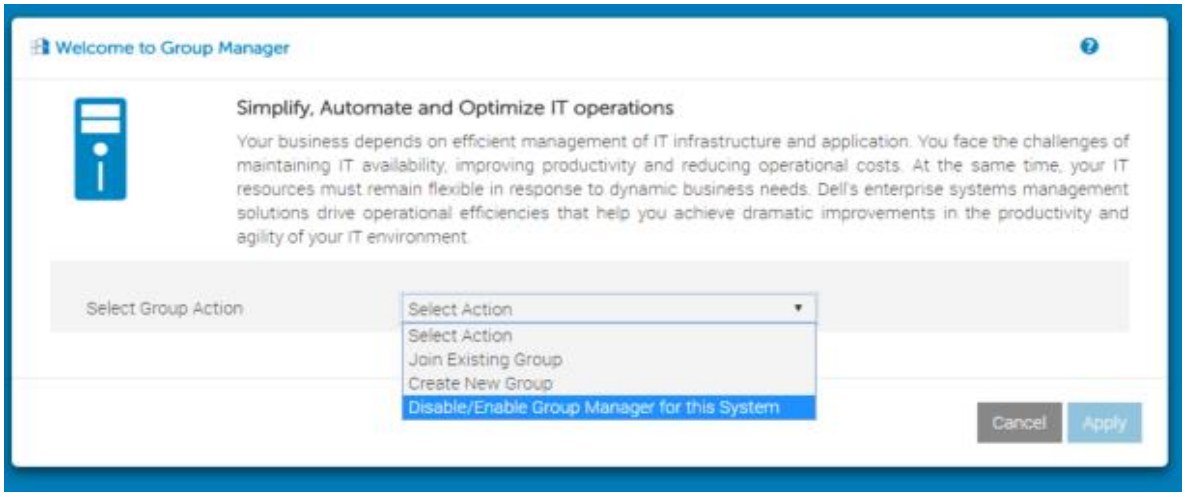
Wait for 60 seconds for the operation to complete.



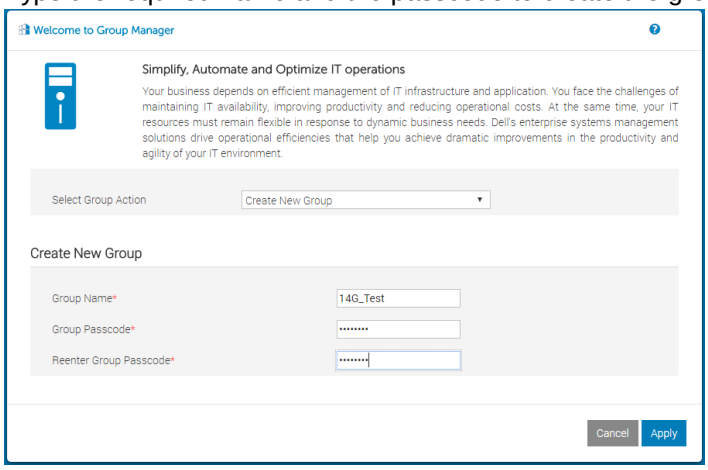
2. If necessary, check the Lifecycle Log for the successful message as shown in the screen shot.



3. After you confirm the log, navigate to the Dashboard and click **Open Group Manager**.
   The Welcome screen is displayed. You can select the required option of creating a new group, joining an existing group, or disabling Group Manager.



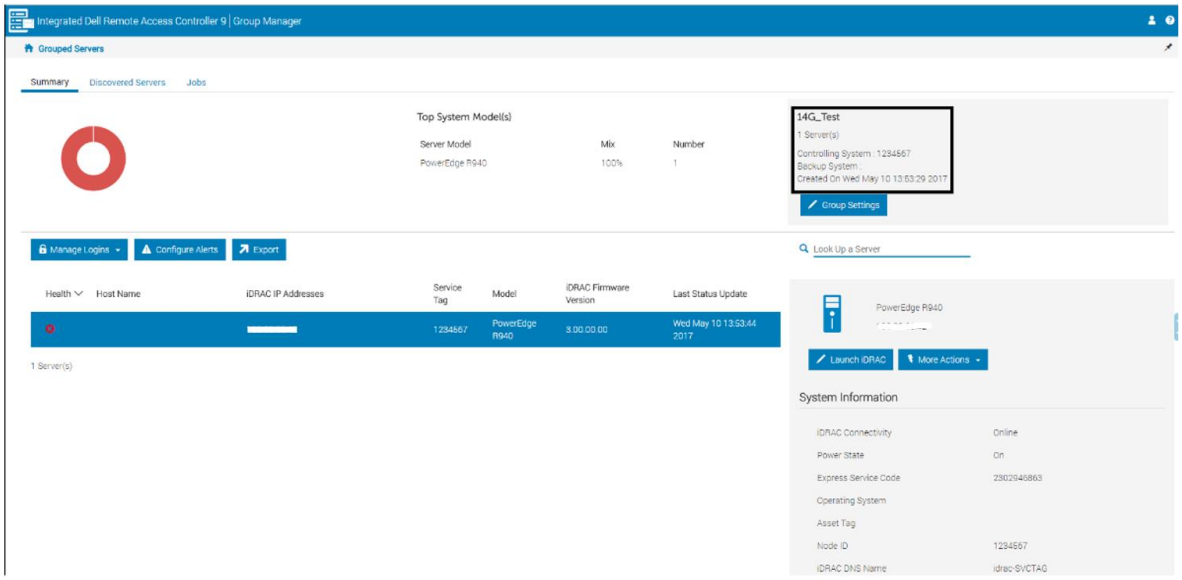
4. Click **Create New Group**.
   The **Welcome to Group Manager** dialog box is displayed.
5. Type the required name and the passcode to create the group.



Note: This passcode is used only for the group management activities and should be protected by the administrator. To improve security, it is recommended to use complex passcodes that have eight or more characters and include lowercase alphabets, uppercase alphabets, numbers, and special characters.

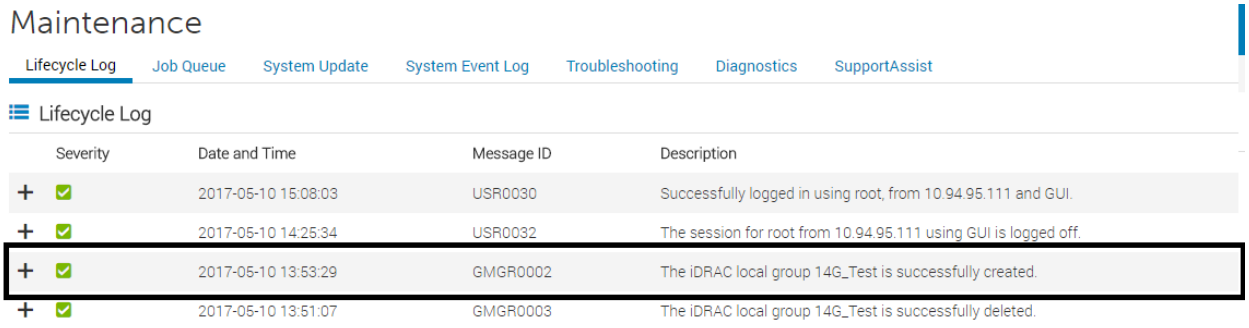
6. Click **Apply**.
   A message is displayed indicating the successful completion of the task.

7. Click **Ok**.
   You will be directed to the Group Manger home page of the Primary Controller Server. By default, when you create a server group, the iDRAC from where the group was created will be assigned as the primary controller of the group.



8. To return to the iDRAC index page, double-click the server row, or click **Launch iDRAC** in the right pane.

You can also check the lifecycle logs for the group creation as shown in the screen shot here.



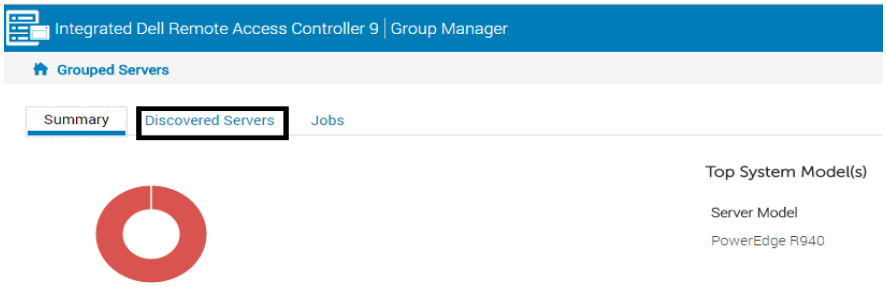
2.1.2 Joining a server group workflows

IDRACs that are physically on the same link local network can be added into a server group on the **Discovered Server** screen. Alternatively, the **Join Existing Group** option on the Group Manager Welcome page can be used to onboard a new iDRAC to an existing server group found in that local network. See Joining a group from new system.

2.1.2.1 Adding a new system into group from Group Manager console

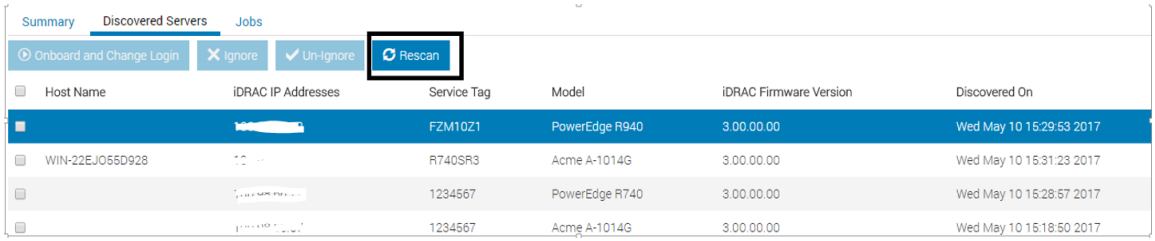
After enabling the Group Manager feature on all iDRACs that are required to be part of the server group:

1. Click **Discovered Servers** on the **Group Manager** home page.

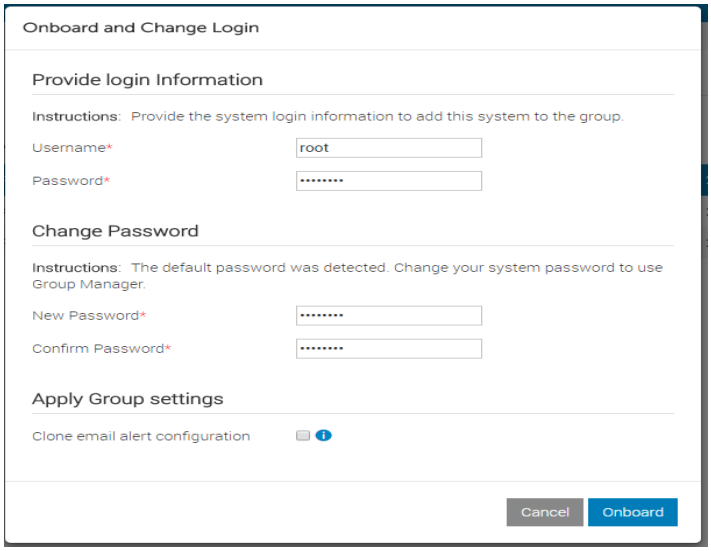


All the discovered iDRACs in the link local network (if Group Manager Feature is enabled) which are not part of a group yet, are displayed.

If you do not see the iDRAC you are searching for, see Frequently asked Questions and Troubleshooting tips.

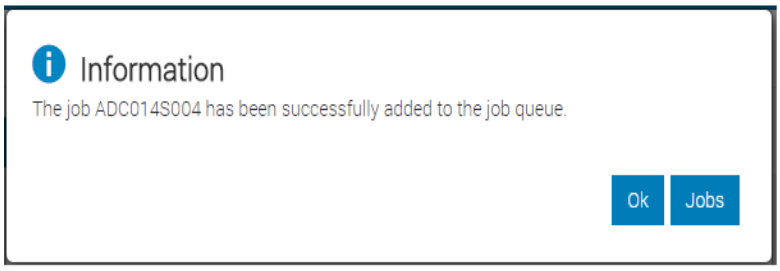


2. Select one or more servers to be joined and enter an administrator role iDRAC user name and password.
   If the **Clone email alert configuration** check box is selected and if there was any prior email configuration group job run on the group, those email alert settings will be applied to these servers after they are associated.

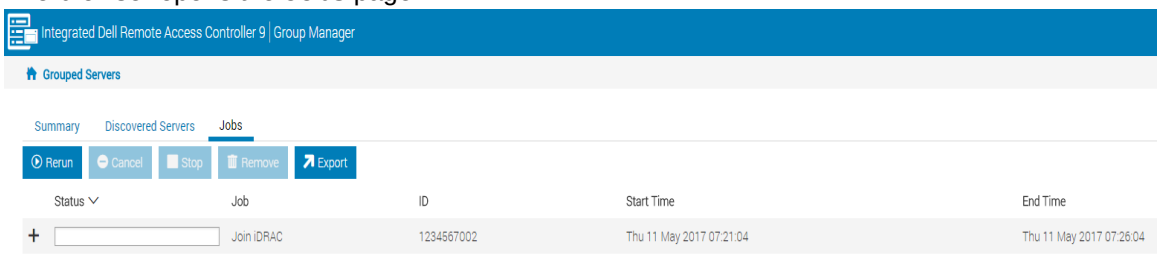


If the default factory-shipped credentials are detected for iDRAC, you will be provided an option to change the root user password at this time.

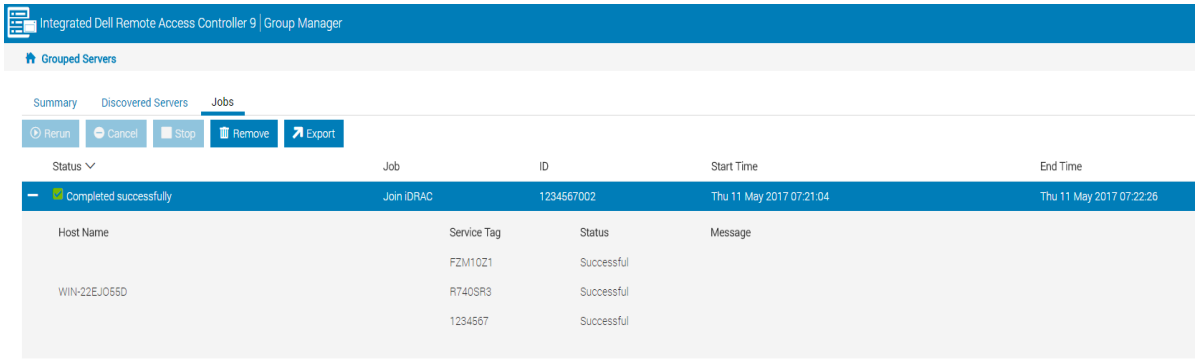
3. After entering all the required data, click **Onboard**.
   A group job to track the on-boarding progress is created. The status of the Onboarding group job can be monitored from **Jobs** tab.



4. Click **Jobs**.
   The browser opens the **Jobs** page.



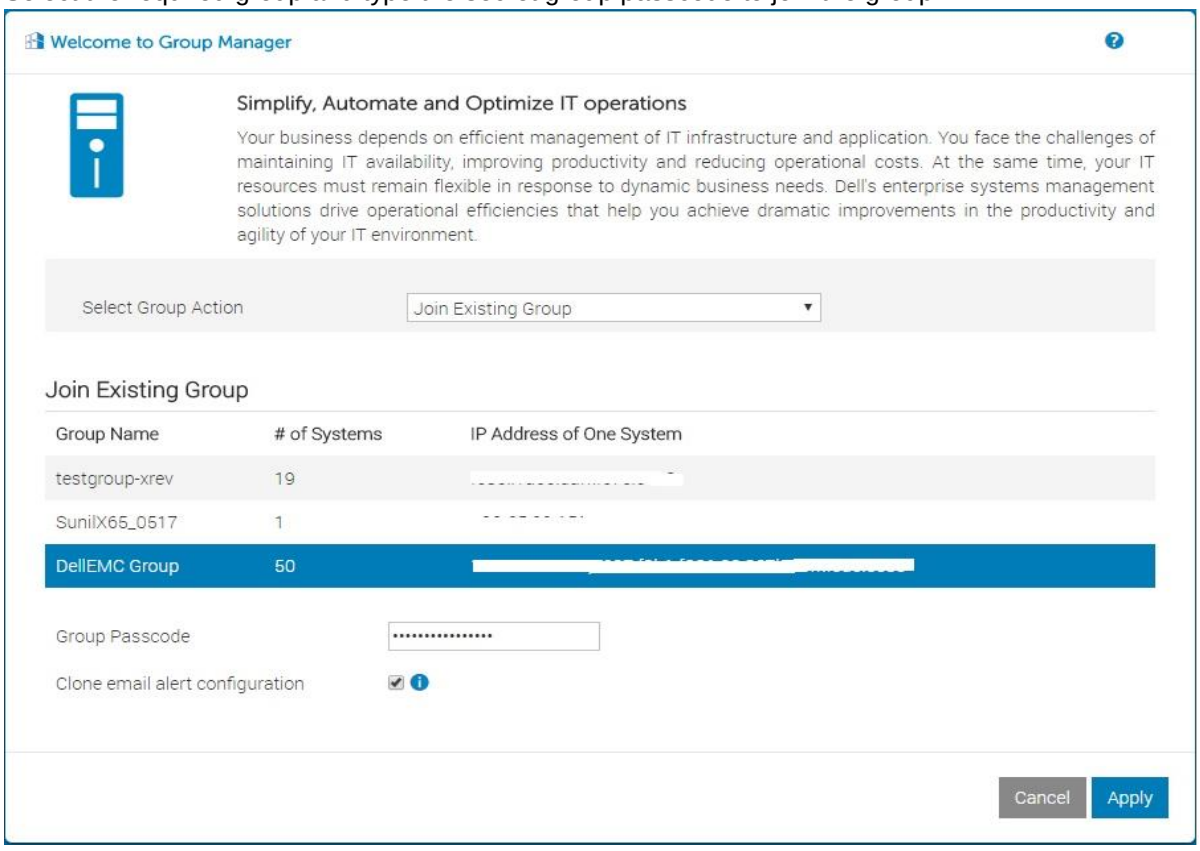
5. Expand the entry to view the onboarding status of each iDRACs.



After successful running of group job, the new members are displayed in **Summary**.

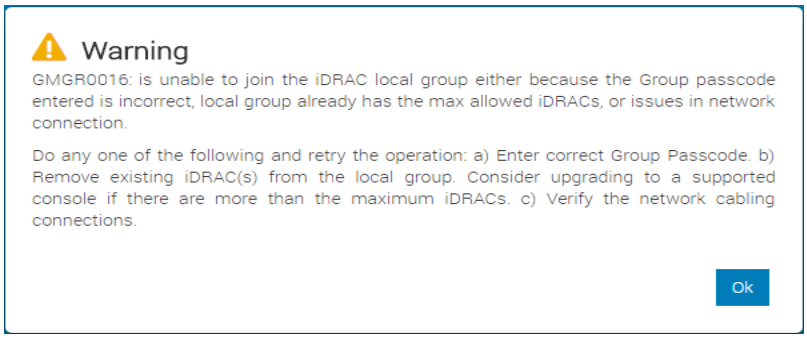
2.1.2.2 Joining a group from new system

1. To join the server group from an iDRAC which has not been part of a group, click **Open Group Manager**.
2. Navigate to the **Join Existing Group** section on the **Group Manager** welcome page.
   All discovered groups in the local network will be listed.
3. Select the required group and type the secret group passcode to join the group.



If the **Clone email alert configuration** check box is selected and a prior email configuration group job was executed on the group, those email alert settings will be applied to these server iDRACs as part of the joining process. After the group passcode validation is successful, the iDRAC becomes part of the required group, and your web browser will be redirected to the Group Manager home page hosted at the group primary controller by using a single-sign-on action.

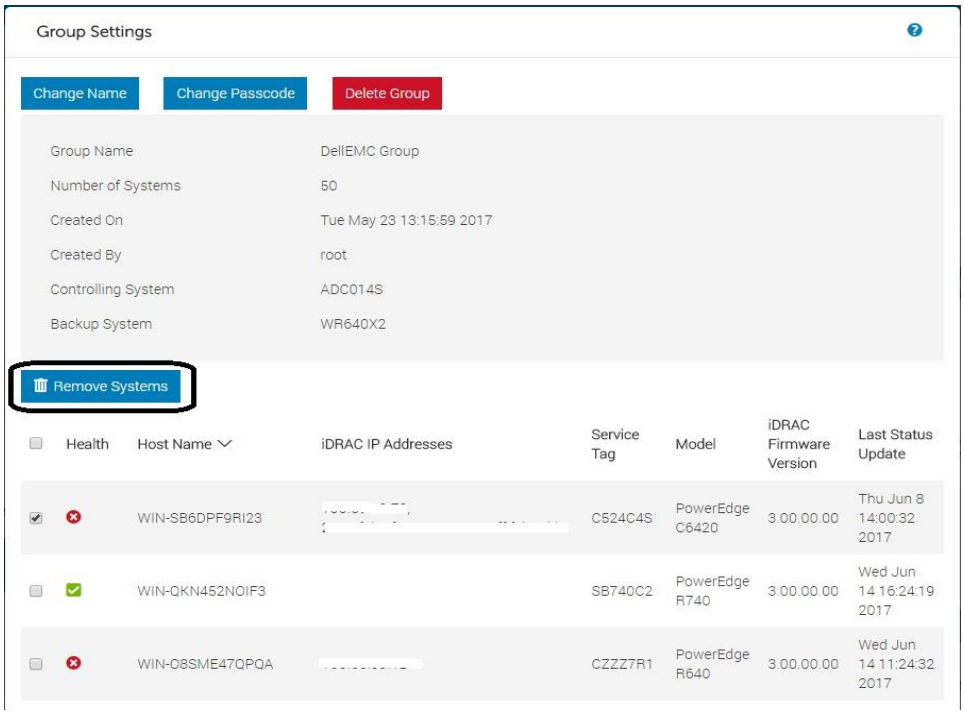
If the passcode validation fails, a message is displayed. You can retry with the correct passcode. However, after seven consecutive failed attempts, group onboarding will be locked for five minutes.



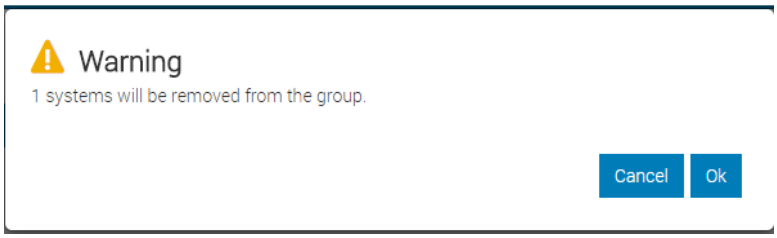
2.1.3 Detaching a server from a local group

You can remove a system from the local group in the Group Settings view.

1. Select the systems to be removed from Group Settings view and click **Remove Systems**.



A message is displayed to confirm the action.



2. Click **Ok**.
   A group job is created. Progress and completion status is updated and displayed in the Group Manager jobs tracking view.

Any in-progress jobs at that time are allowed to be completed. If the system being removed goes offline then Group Manager waits for 10 hours for the system to come back online to run the removal command. After the system is removed from the group, Group Manager removes the system from the **Summary** view.

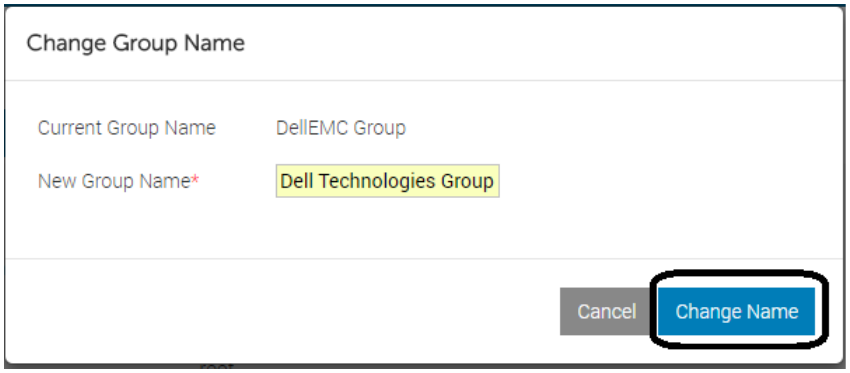
Note that iDRAC must be online for the 'remove' action to succeed. If the removed system comes online after 10 hours then it will automatically rejoin the group because it never received the 'remove' command from the primary controller.

2.2 Managing the group preferences

The Group Settings view is accessible from the Group Manager Summary view and allows an administrator user to view and configure the group name and passcode. Deleting the group can also be performed from the **Group Settings** view.

2.2.1 Changing server group name

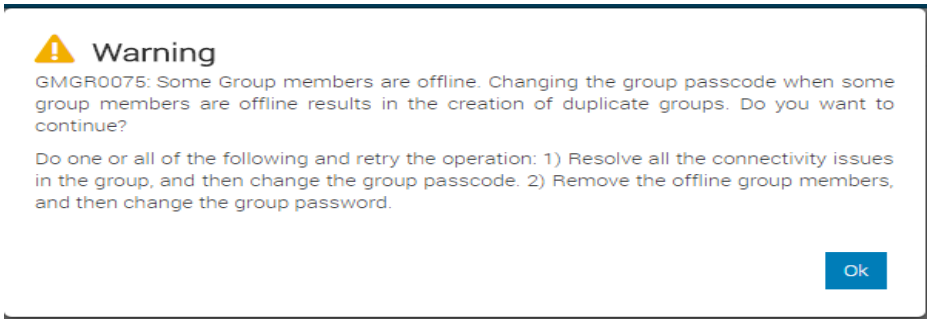
1. Click **Change Name** in the **Group Settings** view.
2. Type the new group name and click **Change Name**.



A group job is created. Progress and completion status can be viewed in the Group Manager jobs view. Group Manager continues to monitor both the old group and the new group until all members of the group have confirmed that they have updated the name identifier.

2.2.2 Changing a group passcode

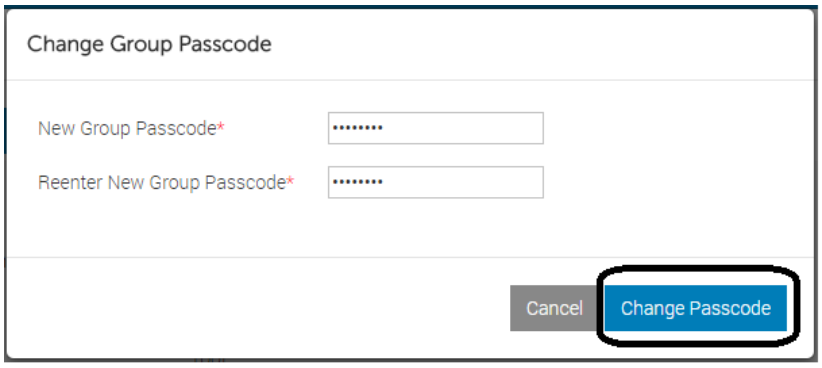
To support best practices for changing passcodes on a reccurring-basis, Group Manager has the ability to change the group password by selecting **Change Group Passcode** in the Group Settings view. If any of the group member(s) are offline, a message is displayed as in the screen shot.



Important Note: Make sure that all members are online before attempting to change a group passcode. Changing group passcode when some members are offline could cause the offline members to fail authentication with the group and will form a duplicate group when they come back online. See Frequently asked Questions and Troubleshooting tips.

To change the group passcode:

1. Type the new passcode twice to make sure it is entered correctly. To improve security, it is recommended to use complex passcodes that have eight or more characters and include lowercase alphabets, uppercase alphabets, numbers, and special characters.



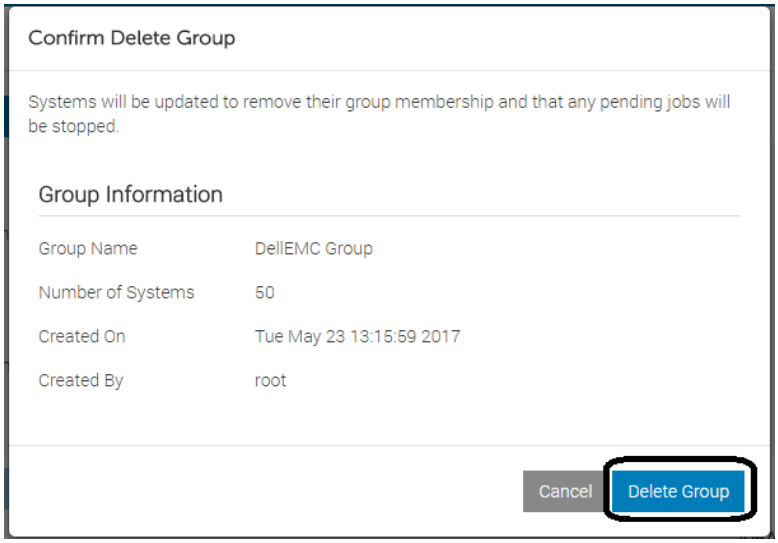
2. Type the necessary data and click **Change Passcode**.
3. A group job is created.
   Progress and completion status will be reflected in the Group Manager jobs tracking view.

Note: the passcode changes take effect immediately and will not wait for offline members to come online. The group passcode will not be changed on any offline system. Any offline systems when connected back to the network will form a duplicate group.

2.3 Deleting a local group

To delete a local group by navigating to the Group Settings view, users with administrator privileges must:

1. Click **Delete Group**.
   A message is displayed indicating that all systems in the group will be updated to remove their group membership and that any pending jobs will be stopped.



2. Click **Delete Group**.
   A group job is created. Progress and completion status is displayed in the Group Manager jobs tracking view.

After confirming the delete action, the group primary controller stops all running tasks, waits for all systems to reach an end state, and issues one final task to all the group members to remove themselves from the group. After all the systems in the group, except for the primary controller have completed the 'remove' task, the primary controller will shut down Group Manager and remove itself from the group. Only the primary controller will have a record of the overall delete group success or failure task. iDRAC Lifecycle logs provide an audit trail of any group configuration activity.

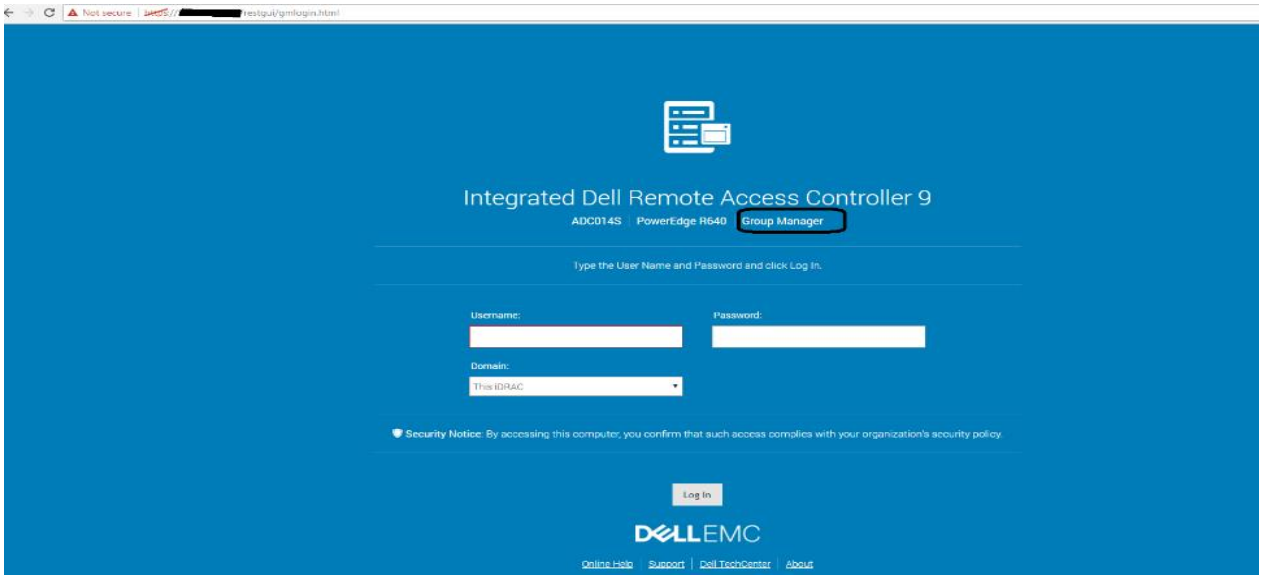
If a member system is offline when the group is deleted, the primary controller will wait for the system to come back online for up to 10 hours. After 10 hours the primary controller will log a message indicating that the system was offline and therefore failed to delete the group completely.

2.4 Monitoring and managing group inventory

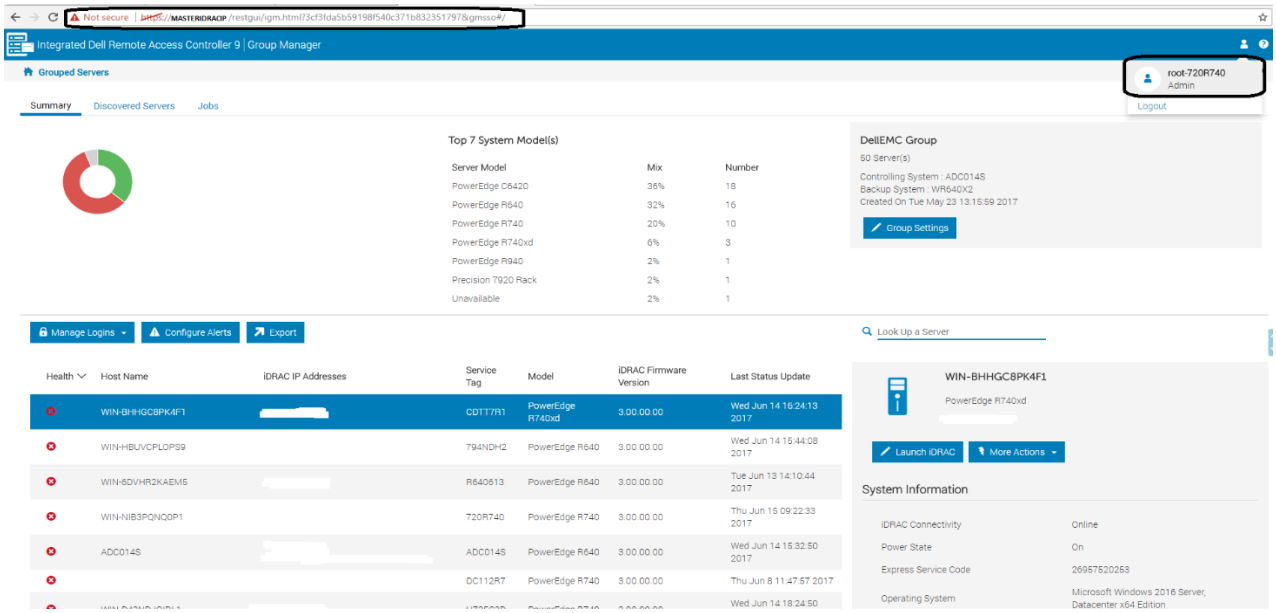
An iDRAC administrator user can monitor and manage grouped servers through a consolidated web-based Graphical User Interface (GUI) hosted at the group primary controller iDRAC.

2.4.1 Bookmarking Group Manager console address in a web browser

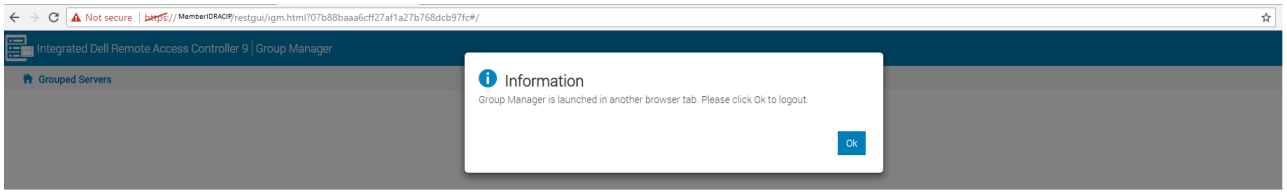
You can create a bookmark to quickly launch the Group Manager **Summary** view directly by using the following URL formatted appropriately in the browser address tab:
https://<Group Member IDRAC IP Address/Domain Name>/restgui/gmlogin.html



After providing a valid iDRAC administrator username and password, you will be redirected to the Group Manager summary page hosted on the group primary controller iDRAC. Group Manager SSO sessions are identified by <`UserLoggedInAtMember-MemberIDRACServiceTag`> (example, `root-1234567`). Any prior existing primary controller iDRAC sessions in the same browser window are ended.



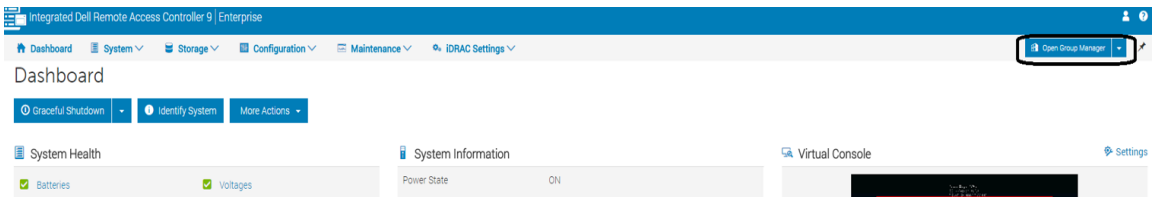
If the member IDRAC IP entered in the URL address is not the primary controller iDRAC IP when the redirect is performed, a message is displayed indicating that Group Manager has been launched in another browser tab. Click **Ok**. The member IDRAC session is ended.



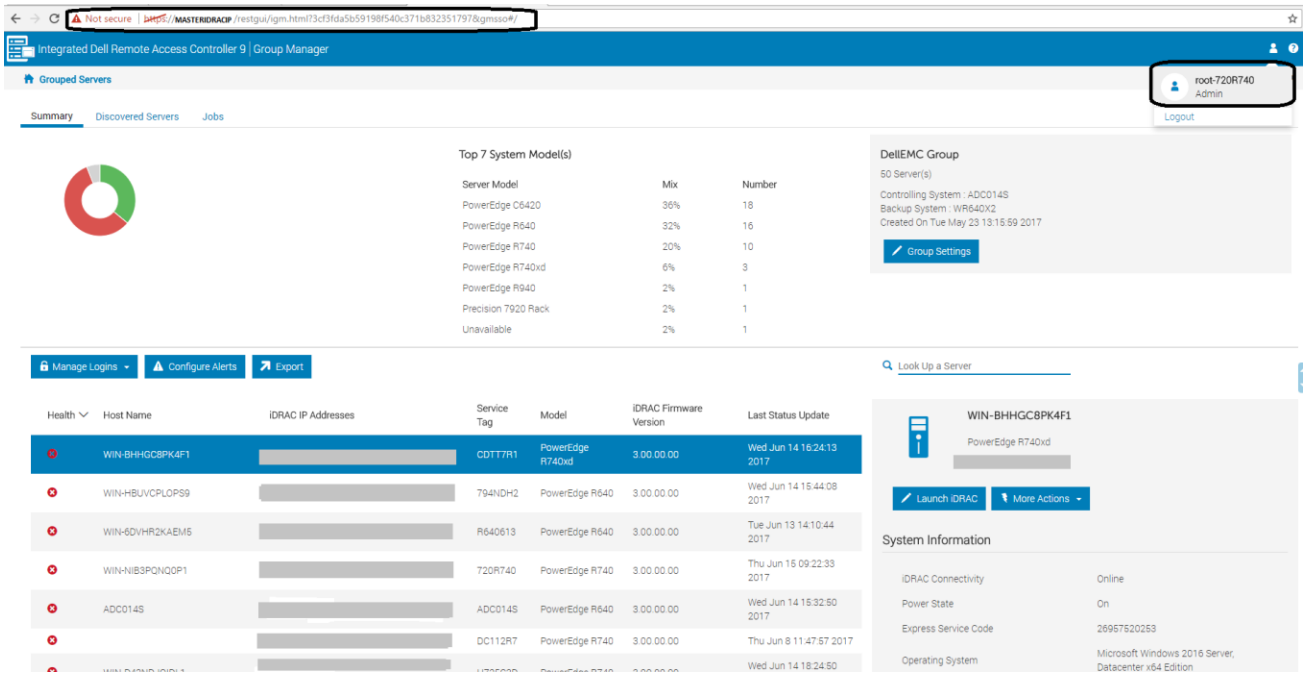
2.4.2 Accessing a Group Manager console from a member iDRAC home page

An administrator who has logged in to any member iDRAC home page can seamlessly access the Group Manager console:

1. Click **Open Group Manager**.
   The browser is redirected to the primary controller iDRAC which is hosting the Group Manager interface by using a single-sign-on redirect.



The primary controller session is established with <UserLoggedInAtMember-MemberIDRACServiceTag> as the username. Any prior existing sessions in the same browser window is ended.

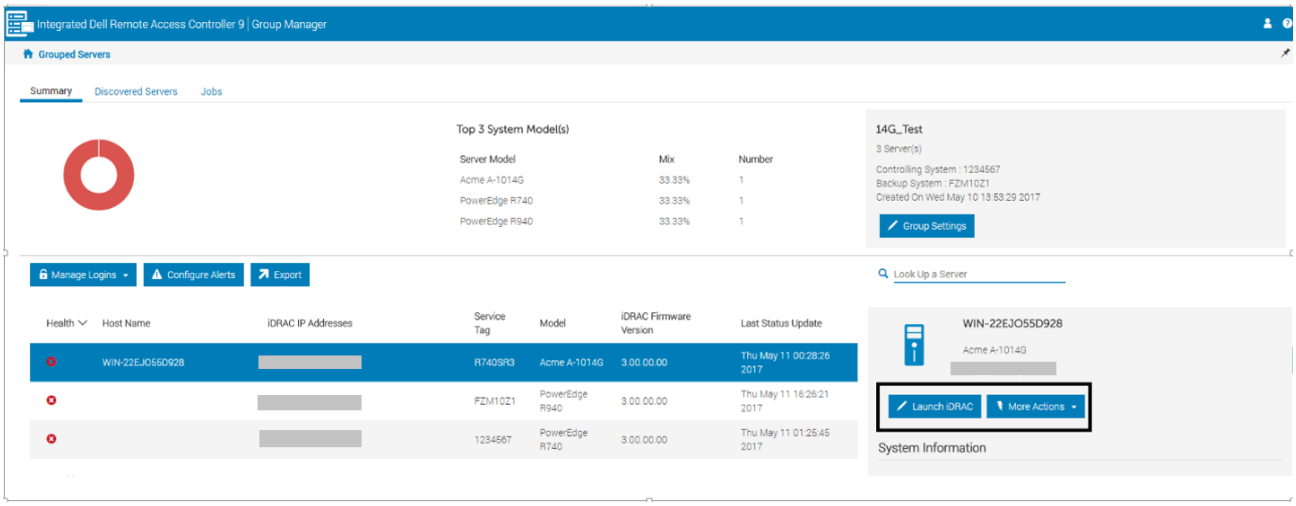


The member IDRAC GUI page displays a message indicating that Group Manager is launched in another browser tab.

2. Click **Ok**.
   The browser will stay on the member IDRAC home page.

2.4.3 Accessing a group member iDRAC home page from Group Manager console

You can access a group member server iDRAC home page by double-clicking the respective row in the Group Manager **Summary** view. Alternatively, in the right pane, click **Launch IDRAC**. The Dashboard displays the selected iDRACs. The Member IDRAC session is started with username in the format: `<IDRACLoggedInUsername-ServiceTag>`.



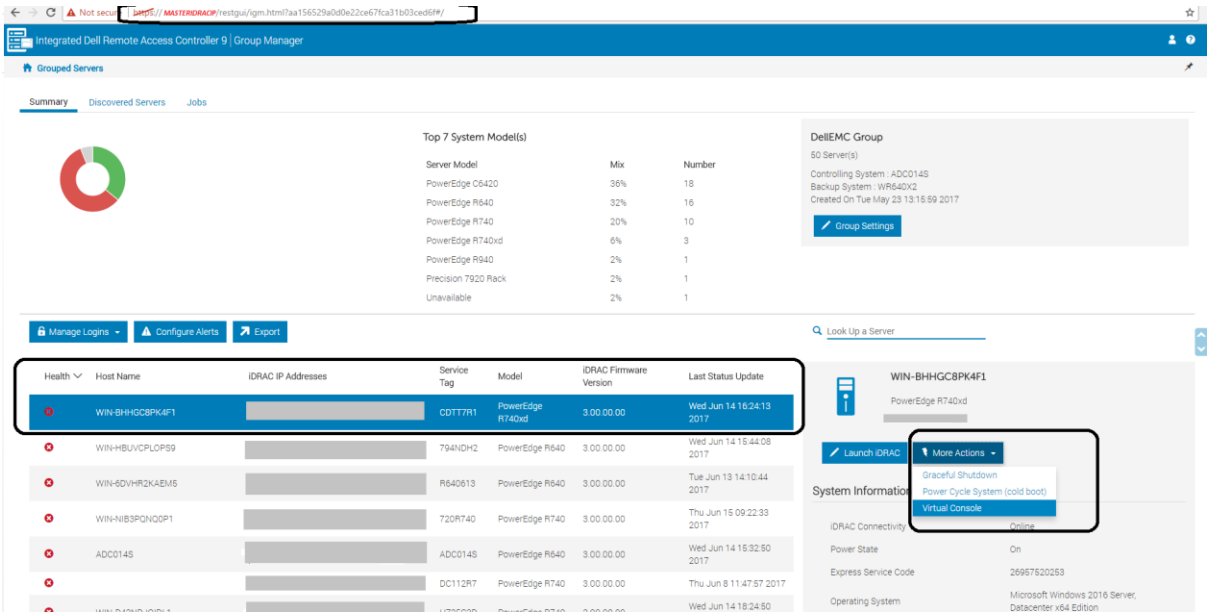
2.4.4 Performing power-control actions from Group Manager console

You can perform actions such as server host graceful shutdown or host power cycle from the available drop-down menu on the selected server.

2.4.5 Accessing a group member virtual console

As an administrator:

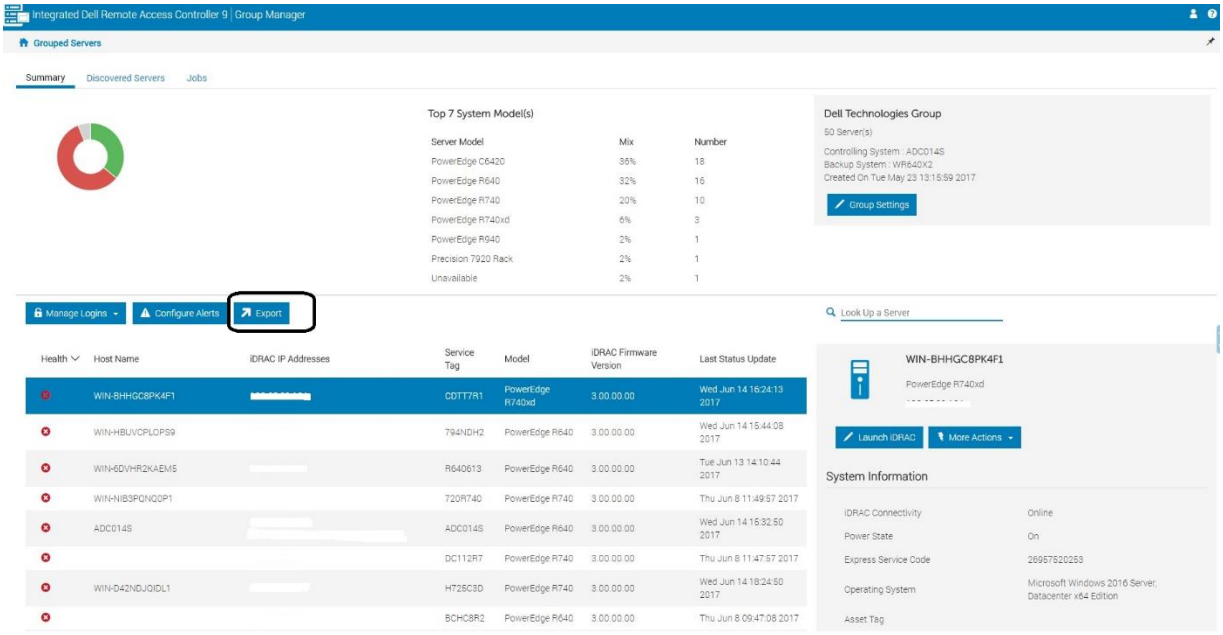
1. Launch a member IDRAC Virtual Console from the **Summary** view by selecting a member iDRAC row, and then click **More Actions**.
2. Click **Virtual Console**.



The member iDRAC HTMLv5 Virtual Console is launched in another browser tab in the same browser window by using single-sign-on redirect. The Member iDRAC session is started with username shown in the format: `<IDRACLoggedInUsername-ServiceTag>`

2.4.6 Exporting the Group Inventory

You can export all the inventory data that Group Manager has as a csv file. On the **Summary View** page, click **Export**. The browser downloads a file with the name of grouped_servers.csv. All exported attributes are in the English language.

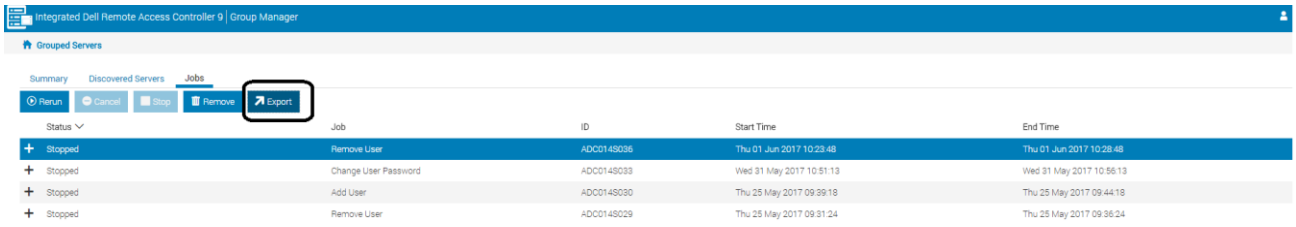


The CSV export contains the following inventoried data:

- Health
- Host Name
- iDRAC
- IPV4 Address
- iDRAC IPV6 Address
- Asset Tag
- Model
- iDRAC Firmware Version
- Last Status Update
- Express Service Code
- iDRAC Connectivity
- Power State
- Operating System
- Service Tag
- Node ID
- iDRAC DNS Name
- BIOS Version
- CPU System Memory(MB)
- Location Details

2.4.7 Exporting the Group Jobs audit log

To export the Group Manager Jobs information, click **Export** under **Jobs View**. A file with the jobs.csv name is downloaded to the browser.



2.5 Group Actions–Configure all iDRACs in the local group

Group Manager **Summary** view enables you to perform group actions by using the action buttons listed above the server list. Group actions are performed on all members in the group. If an action is scheduled for the future and new members have been added to the group, they will be included in the group change action. If a task is in progress then the newly added member will not be included in the group action.

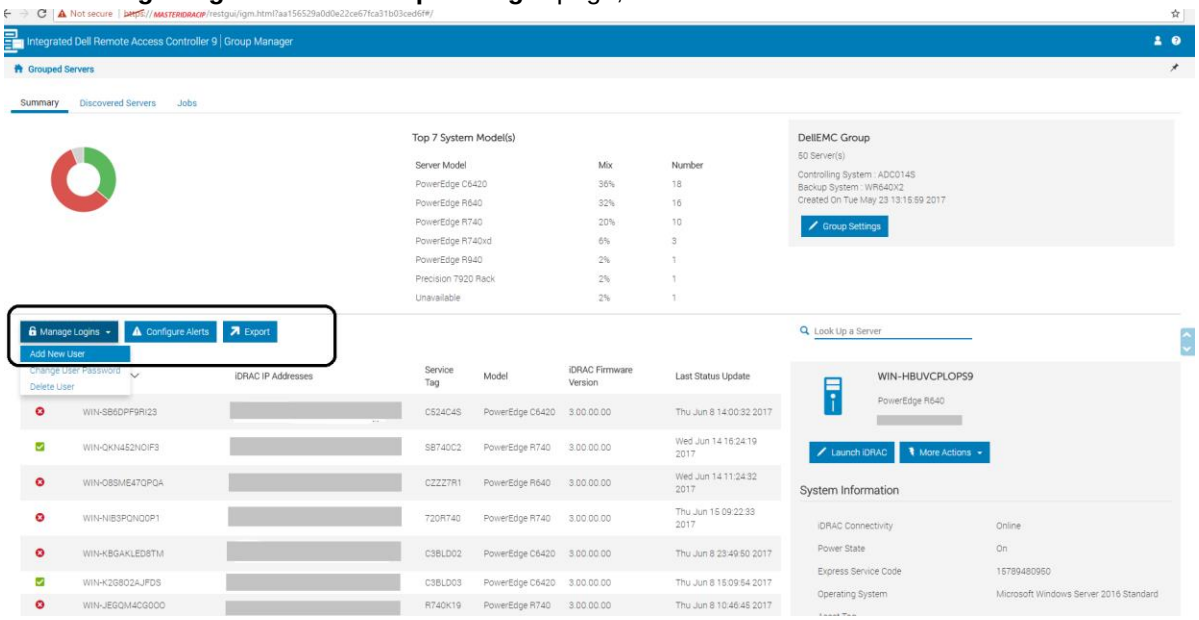
2.5.1 Adding, removing, or updating iDRAC user

iDRAC local users can be added or deleted by selecting from the Manage Login drop-down menu on the Group Manager home page.

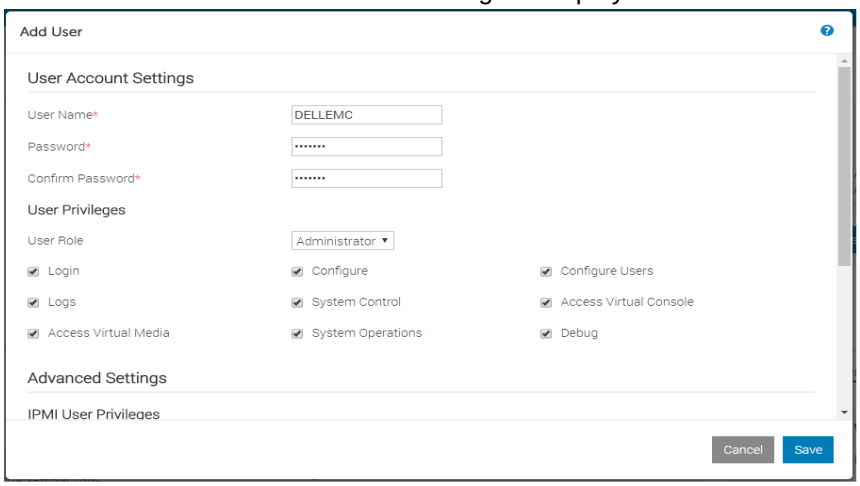
2.5.1.1 Adding iDRAC user with password

Add iDRAC user workflow adds a new local user to all the iDRACs in the group.

1. Click **Manage Logins** on the **Group Manager** page, and then click **Add New User**.



2. In the **Add User** dialog box, type or select data in the fields. If the password and password confirmation do not match then a message is displayed.



3. Click **Save**.
   A group job is created. Group Job progress and completion status will be reflected in the Group Manager jobs tracking view.

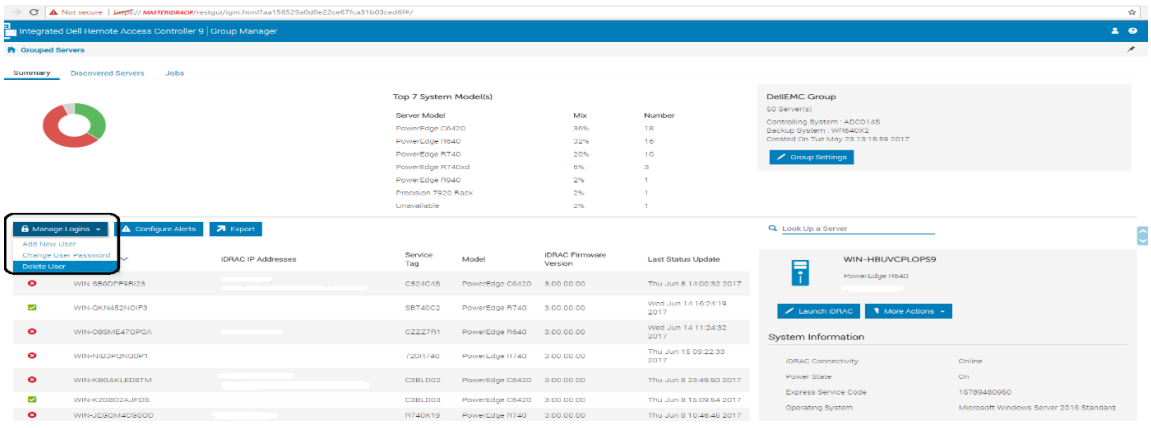
   If the user already exists on a member iDRAC, the user is updated with the privileges and password defined in the **Add User** configuration.

Note: Users are added to the first available user slot in each member. Not all members will add a user to the same slot. If a member iDRAC has 16 local users then the job will fail to add a new user on that specific iDRAC, but all other iDRACs will create the local user on their first available slot.

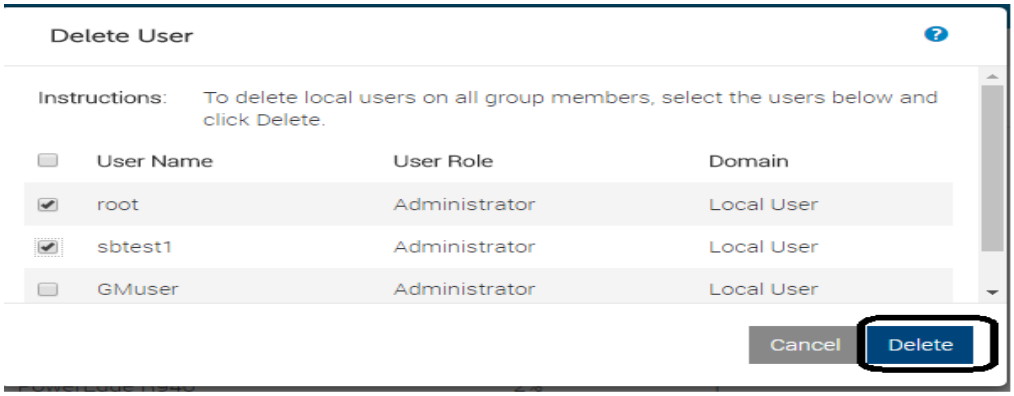
2.5.1.2 Deleting iDRAC user

The Delete iDRAC user group feature removes one or more local users from all group member iDRACs. Users are not removed based on slot number but are removed based on a matching name only.

1. Click **Manage Logins** from the Group Manager page.
2. Click **Delete User option**.



The Delete User dialog box displays a list of all the local iDRAC users on the primary controller.

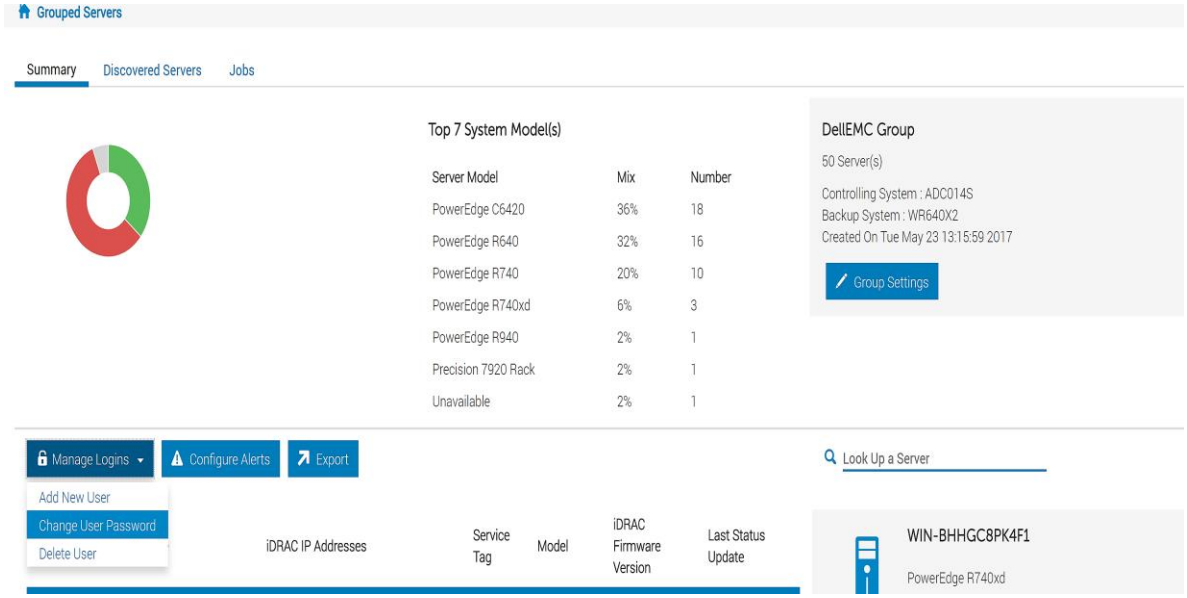


3. Select one or more local iDRAC users and click **Delete**.
   A group job is created. Job progress and completion status will be reflected in the Group Manager jobs tracking view.

2.5.1.3 Changing iDRAC user password

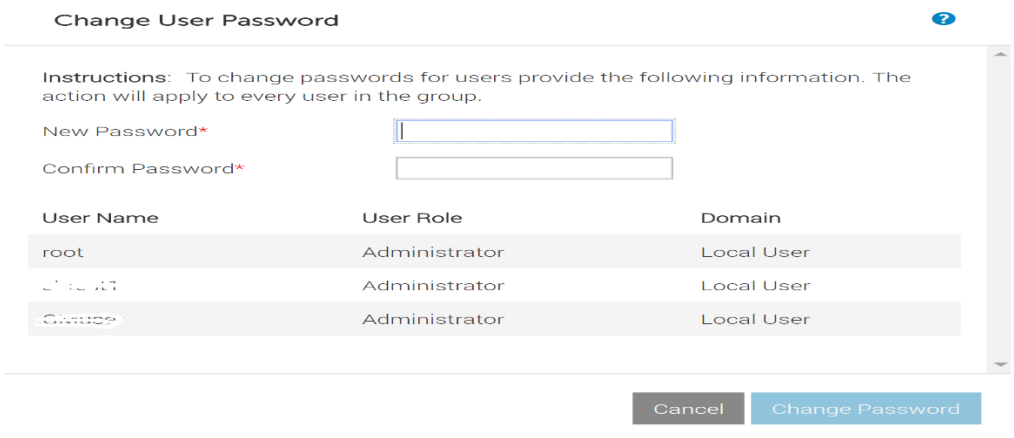
The Change User Password group feature enables you to change password of the specified user on all group member iDRACs.

1. Click **Manage Logins** on the Group Manager page, and then click **Change User Password**.



A list of all the local users on the group primary controller iDRAC is displayed.

2. Select the username and type the new password twice for the selected user.

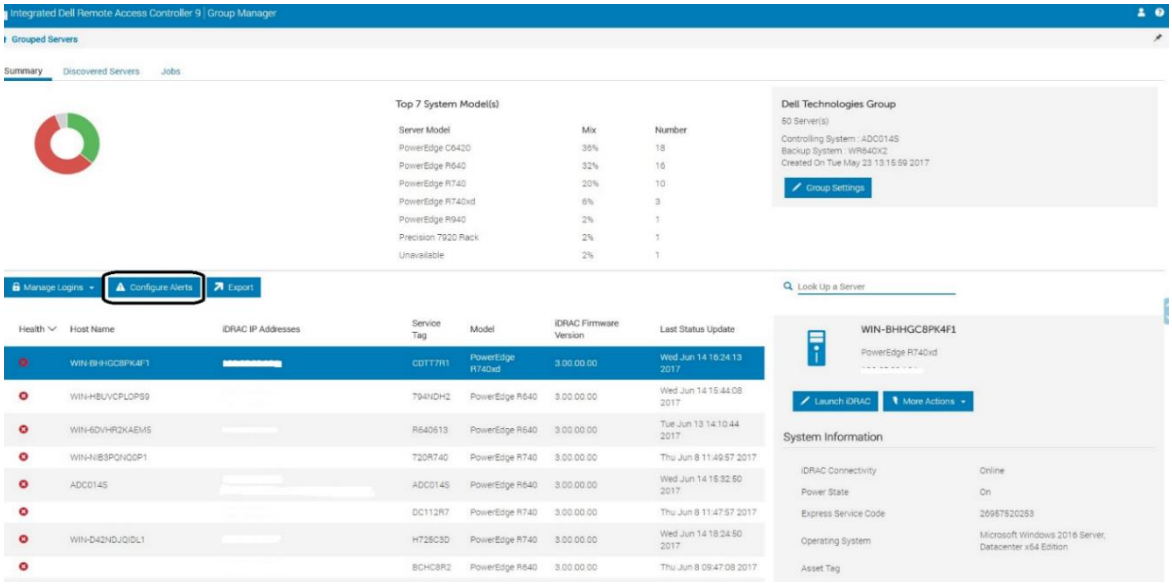


3. Click **Change Password**.
   If the password validation succeeds, a group job is created. Group Job progress and completion status will be reflected in the Group Manager jobs tracking view.

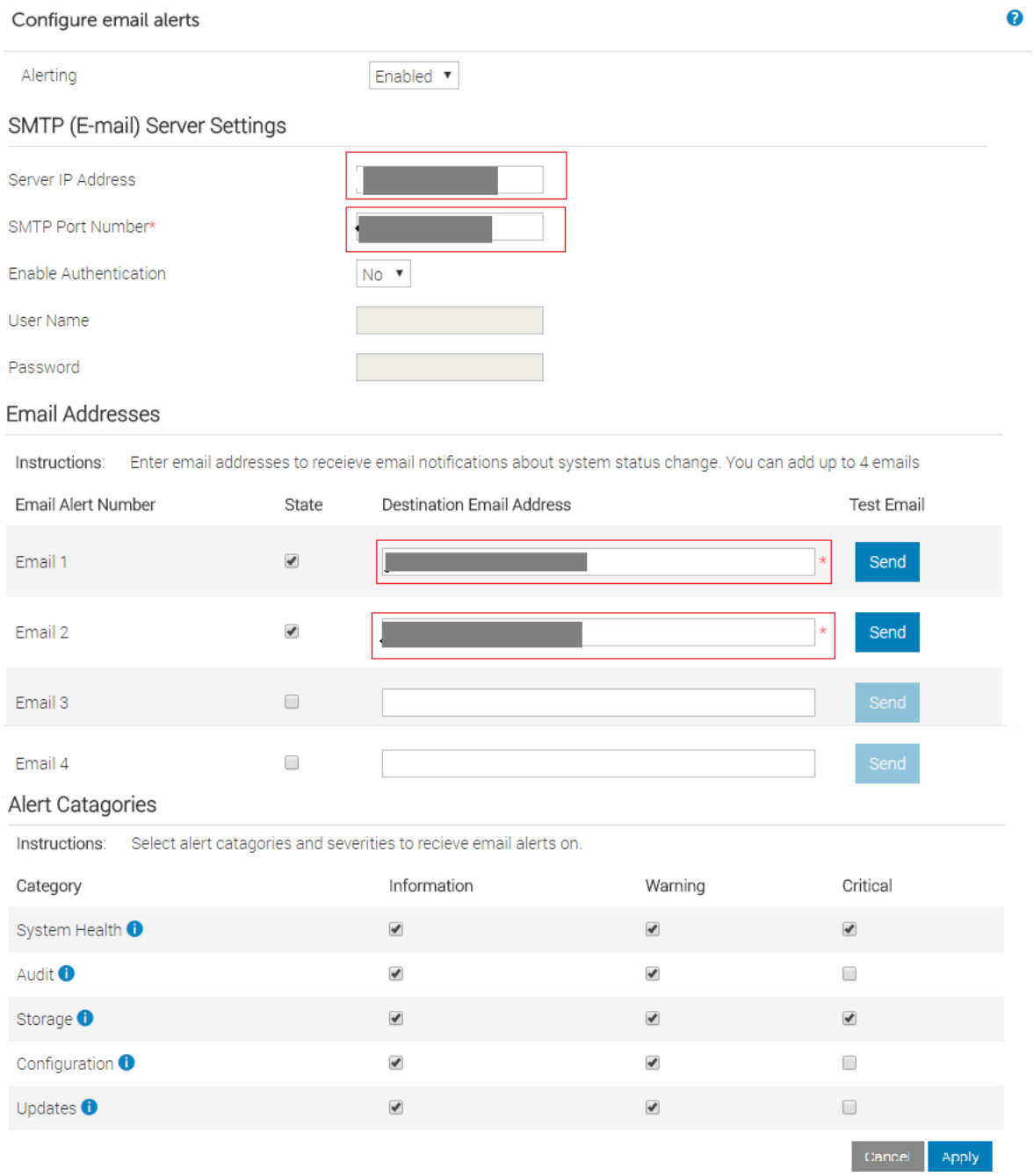
2.5.2 Setting up iDRAC email alert configuration

The Configure Alerts feature enables you to configure the SMTP (E-mail) Configuration for all group member iDRACs.

1. To configure email alerts, click **Configure Alerts** in **Summary**.



The currently configured settings of the primary controller iDRAC shall be auto-populated in the **Configure Email Alert** window (These settings can also be viewed on **iDRAC Home Page → Configuration → System Settings →SMTP (E-mail) Configuration)**.

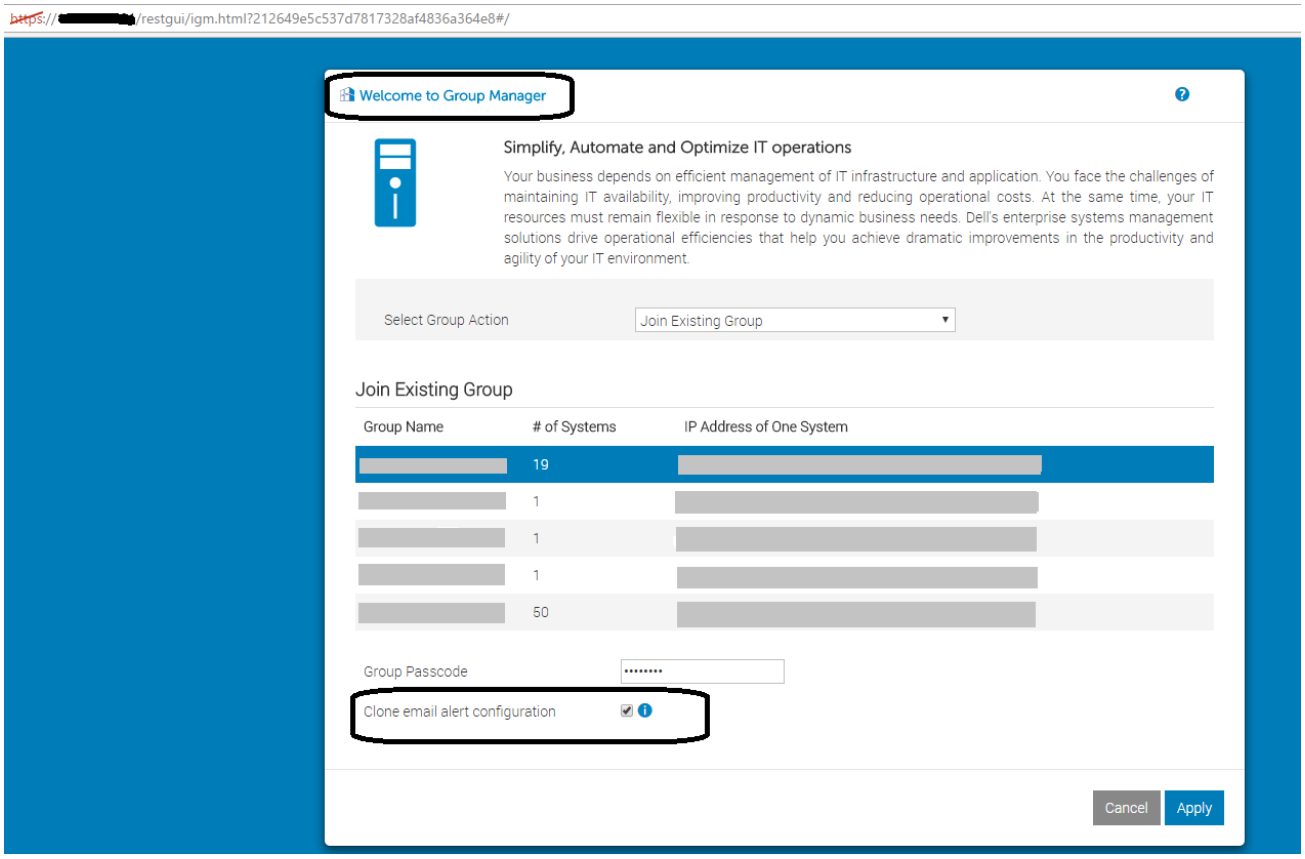

Configure email alerts
Alerting
Enabled
SMTP (E-mail) Server Settings
Server IP Address
SMTP Port Number*
Enable Authentication
No
User Name
Password
Email Addresses
Instructions: Enter email addresses to receieve email notifications about system status change. You can add up to 4 emails
Email Alert Number
State
Destination Email Address
Test Email
Email 1
Send
Email 2
Send
Email 3
Send
Email 4
Send
Alert Catagories
Instructions: Select alert catagories and severities to recieve email alerts on.
Category
Information
Warning
Critical
System Health
Audit
Storage
Configuration
Updates
Cancel
Apply

2. After entering and updating the required details for SMTP Email configuration, click **Apply**.
   A group job is created. Group Job progress and completion status is reflected in the Group Manager jobs tracking view.
   After the group job is completed successfully, the settings entered by the user is applied to every member iDRAC. Email alerting values can be verified on the **iDRAC Alert** page by clicking **Configuration → System Settings → Alert Configuration →Alerts**.

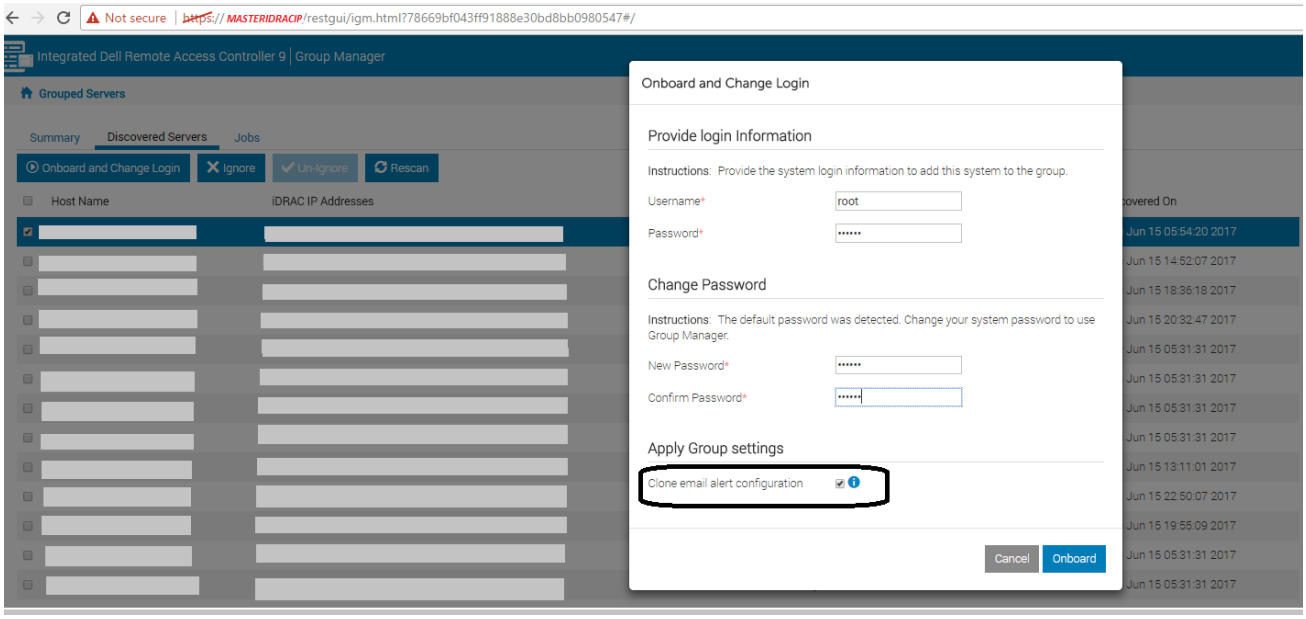
2.5.3 Cloning group email alert configuration settings

When a server joins the group, the email alert configuration settings for that group can be cloned on that iDRAC as part of the joining sequence.

Option 1: Select the **Clone email alert configuration** check box while joining a group from the iDRAC Group Manager welcome screen.



Option 2: From the Group Manager **Discovered Servers** list, when onboarding servers, select the **Clone email alert configuration** check box. At the end of joining sequence, the email configuration will be cloned to the joined servers.



2.6 Group Job Manager – Jobs tracking and reporting

The purpose of the Jobs view is to provide a way for the user to track the progress of a group action to take simple recovery steps to correct connectivity induced failures and to show a history of the last group actions that were performed as an audit log. All jobs or actions are initiated from Summary View and Discovered Servers View.

The Jobs view is used to track the progress of group actions across the group or to cancel an action that is scheduled to occur in the future.

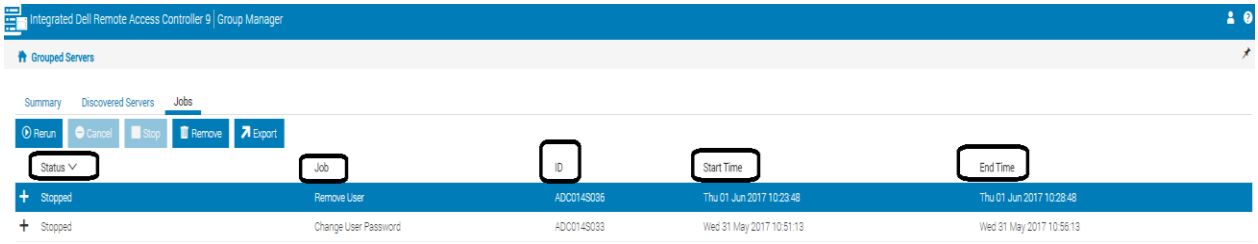
A unique ID is created for every group action. The Jobs view provides an audit log for the last 50 jobs that have been run on the group along with the completion status on the individual group member servers.

2.6.1 Feedback about job status and recovering from errors

The top level job list view shows the following information:

- Status (The job overall status is represented by an icon this is the worst-case rolled-up status of all devices the job is running against)
  - Running (Progress bar displaying the job completion %)
  - Completed successfully
  - Completed with errors
  - Retrying the job has been Scheduled
  - Stopped
  - Cancelled

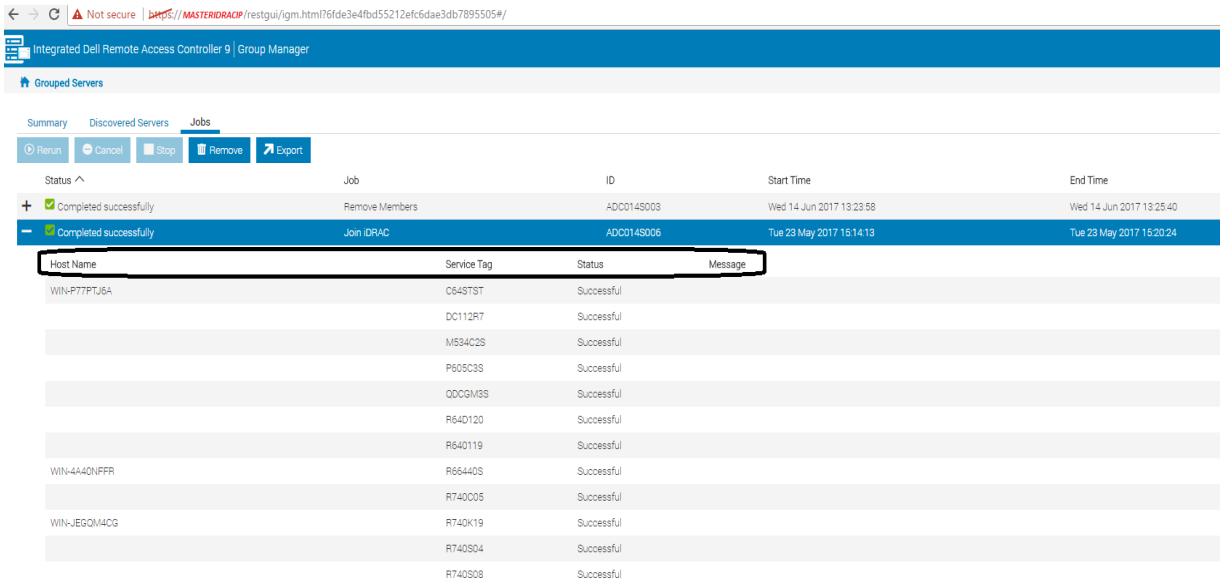
- Job Type
  - Add User
  - Change user password
  - Remove user
  - Change Group Passcode
  - Change Group Name
  - Delete Group
  - Remove Members
  - Configure Email
  - Join iDRAC
- JOB Unique ID
- Start Time
- End Time



The second level job list details shows the job status for every member of the group. All actions and data are specific to that member iDRAC:

- Host Name
- Service Tag
- Status
  - Successful: The group action is successfully applied on this specific server.
  - Failed: The group action failed because Group Manager timed out trying to communicate with the remote server, the remote server responded with an error message, or it was stopped by the user. See Frequently asked Questions and Troubleshooting tips.
  - Not Running: The group action has not started. Group Manager could be waiting for the system to become available or the server is busy on other operations and will run the command in the near future.
  - In Progress: The group action is running on this specific server
    - Error Occurred. Retrying the Job: Some error occurred and therefore retrying the job on this specific server.

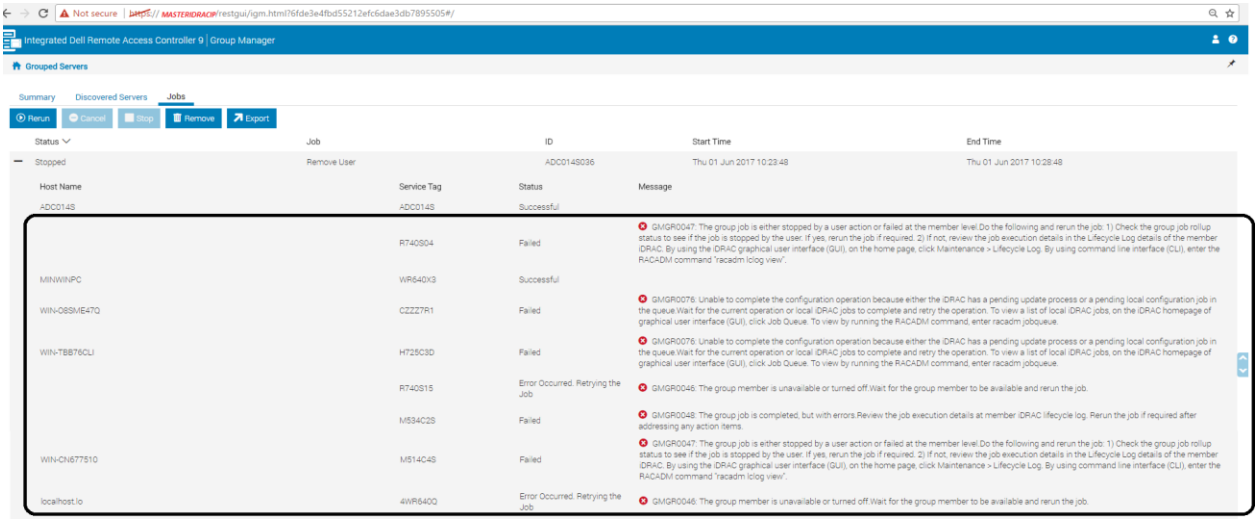
- Message
  - A specific message is displayed for the member server where the job execution was not successful.



When job fails at a particular member iDRAC, the reason for the failure can be viewed as shown below. If a job is running, a user may select the job and click **Stop** to stop the job execution. It does not roll back but stops all tasks and puts it in an error state identified by “stopped by user”.

The rerun action is only enabled if the job is in a failure state. The job is only rerun on the specific servers that failed the job in the prior run. When the rerun is performed the overall job status will be placed in pending status.

The job list is circular and only the last 50 jobs are displayed in the view. As new jobs are created, the oldest ones are removed from the list.



2.7 Configuring Group Manager by using CLIs

iDRAC Group Manager is predominantly a graphical user interface (GUI) based feature where most of the configuration and monitoring activities can only be performed through the web based graphical user interface. For those customers who are using Group Manager in larger environments, the following section describes the actions which can be performed by using WS-Man and RACADM CLIs.

2.7.1 Configuring Group Manager by using WS-Man

WS-Man (Web Services-Management) is a DMTF open standard, defining a SOAP-XML based protocol for the management of servers, devices, and applications used by systems management consoles or management applications.

2.7.2 Enabling or disabling the Group Manager feature

To enable or disable the Group Manager feature, management application can use the `DCIM_iDRAService.ApplyAttribute()` method from iDRAC Card Profile to set the `GroupManager.1#Status` attribute. This enumeration attribute can be set to Enabled or Disabled.

For more information, see the *iDRAC Card Profile_4.0.0 Session 8.21 and 7.5.52* available on DTC http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.

If not already enabled, the feature status must be changed to Enabled before any other actions can be performed.

Here is an example WS-Man workflow by using SOAP to set `GroupManager.1#Status`. In this workflow, the current value of `GroupManager.1#Status` will be checked and sent the invoke request to set a new value to the `GroupManager.1#Status` attribute.

- Management applications can send the GET request for the following form to check the current value of the `GroupManager.1#Status` attribute.

  SOAP Request for the `GET GroupManager.1#Status` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd">
    - <s:Header>
        <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
        <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-
            schema/2/DCIM_iDRACCardEnumeration</wsman:ResourceURI>
      - <wsa:ReplyTo>
            <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsa:Action s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/09/transfer/Get</wsa:Action>
        <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
        <wsa:MessageID s:mustUnderstand="true">urn:uuid:94e0a180-2fcd-11e7-9f7b-340286bae004</wsa:MessageID>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
      - <wsman:SelectorSet>
            <wsman:Selector Name="InstanceID">iDRAC.Embedded.1#GroupManager.1#Status</wsman:Selector>
            <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
        </wsman:SelectorSet>
    </s:Header>
    <s:Body/>
</s:Envelope>
```

SOAP Response for the `GET GroupManager.1#Status` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/DCIM_iDRACCardEnumeration" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:s="http://www.w3.org/2003/05/soa
envelope">
  - <s:Header>
      <wsa:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:To>
      <wsa:Action>http://schemas.xmlsoap.org/ws/2004/09/transfer/GetResponse</wsa:Action>
      <wsa:RelatesTo>urn:uuid:94e0a180-2fcd-11e7-9f7b-340286bae004</wsa:RelatesTo>
      <wsa:MessageID>uuid:abcfced0-4ea0-1ea0-af6f-74d5ac5ed502</wsa:MessageID>
    </s:Header>
  - <s:Body>
    - <n1:DCIM_iDRACCardEnumeration>
        <n1:AttributeDisplayName>Feature Status</n1:AttributeDisplayName>
        <n1:AttributeName>Status</n1:AttributeName>
        <n1:CurrentValue>Enabled</n1:CurrentValue>
        <n1:DefaultValue>Disabled</n1:DefaultValue>
        <n1:Dependency xsi:nil="true"/>
        <n1:DisplayOrder>1</n1:DisplayOrder>
        <n1:FQDD>iDRAC.Embedded.1</n1:FQDD>
        <n1:GroupDisplayName>Group Manager</n1:GroupDisplayName>
        <n1:GroupID>GroupManager.1</n1:GroupID>
        <n1:InstanceID>iDRAC.Embedded.1#GroupManager.1#Status</n1:InstanceID>
        <n1:IsReadOnly>false</n1:IsReadOnly>
        <n1:PendingValue xsi:nil="true"/>
        <n1:PossibleValues>Disabled</n1:PossibleValues>
        <n1:PossibleValues>Enabled</n1:PossibleValues>
      </n1:DCIM_iDRACCardEnumeration>
    </s:Body>
</s:Envelope>
```

- Management applications can send the request for the following form to set the `GroupManager.1#Status` attribute.

SOAP request for the `ApplyAttribute` method to set the `GroupManager.1#Status` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd">
  - <s:Header>
      <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
      <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService</wsman:ResourceURI>
    - <wsa:ReplyTo>
        <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:Action s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/ApplyAttribute</wsa:Action>
      <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
      <wsa:MessageID s:mustUnderstand="true">urn:uuid:4b5e81b0-2fcf-11e7-82d5-340286bae004</wsa:MessageID>
      <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
    - <wsman:SelectorSet>
        <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
        <wsman:Selector Name="SystemCreationClassName">DCIM_ComputerSystem</wsman:Selector>
        <wsman:Selector Name="SystemName">DCIM:ComputerSystem</wsman:Selector>
        <wsman:Selector Name="CreationClassName">DCIM_iDRACCardService</wsman:Selector>
        <wsman:Selector Name="Name">DCIM:iDRACCardService</wsman:Selector>
      </wsman:SelectorSet>
    </s:Header>
  - <s:Body>
    - <n1:ApplyAttribute_INPUT>
        <n1:AttributeName>GroupManager.1#Status</n1:AttributeName>
        <n1:Target>iDRAC.Embedded.1</n1:Target>
        <n1:AttributeValue>Enabled</n1:AttributeValue>
      </n1:ApplyAttribute_INPUT>
    </s:Body>
</s:Envelope>
```

SOAP Response for the `ApplyAttribute` method to set the `GroupManager.1#Status` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:s="http://www.w3.org/2003/05/soap-envelope">
  - <s:Header>
      <wsa:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:To>
      <wsa:Action>http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/ApplyAttributeResponse</wsa:Action>
      <wsa:RelatesTo>urn:uuid:ac969d5e-3186-11e7-88fe-340286bae004</wsa:RelatesTo>
      <wsa:MessageID>uuid:4eb1b7d0-4e60-1e60-baeb-3a6ad5eb7b84</wsa:MessageID>
    </s:Header>
  - <s:Body>
    - <n1:ApplyAttribute_OUTPUT>
        <n1:Message>The command was successful.</n1:Message>
        <n1:MessageID>RAC001</n1:MessageID>
        <n1:ReturnValue>0</n1:ReturnValue>
        <n1:SetResult>Set CurrentValue</n1:SetResult>
      </n1:ApplyAttribute_OUTPUT>
    </s:Body>
</s:Envelope>
```

3. Repeat the tasks to ensure that the value of `GroupManager.1#Status` has changed.

2.7.3 Group information

The `GroupManager.1#GroupName` and `GroupManager.1#GroupUUID` read-only attribute are available in DCIM_iDRACCardString to get the Group Name and Group UUID of the local group to which the iDRAC is subscribed to.

For more information, see the *iDRAC Card Profile_4.0.0 Session 7.5.52* profile document available at http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.

1) Management application can send the SOAP request as described in the sample here to get the GroupName of the local group which iDRAC part of.

   SOAP request for the `GET GroupManager.1#GroupName` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    - <s:Header>
        <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
        <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardString</wsman:ResourceURI>
      - <wsa:ReplyTo>
          <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsa:Action s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/09/transfer/Get</wsa:Action>
        <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
        <wsa:MessageID s:mustUnderstand="true">urn:uuid:441a7d30-2fcc-11e7-a277-340286bae004</wsa:MessageID>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
      - <wsman:SelectorSet>
          <wsman:Selector Name="InstanceID">iDRAC.Embedded.1#GroupManager.1#GroupName</wsman:Selector>
          <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
        </wsman:SelectorSet>
    </s:Header>
    <s:Body/>
</s:Envelope>
```

   SOAP response for the `GET GroupManager.1#GroupName` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardString"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:s="http://www.w3.org/2003/05/soap-envelope
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    - <s:Header>
        <wsa:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:To>
        <wsa:Action>http://schemas.xmlsoap.org/ws/2004/09/transfer/GetResponse</wsa:Action>
        <wsa:RelatesTo>urn:uuid:441a7d30-2fcc-11e7-a277-340286bae004</wsa:RelatesTo>
        <wsa:MessageID>uuid:fc92fb00-4ea3-1ea3-83b6-11f36eda6618</wsa:MessageID>
    </s:Header>
    - <s:Body>
      - <n1:DCIM_iDRACCardString>
          <n1:AttributeDisplayName>Group Name</n1:AttributeDisplayName>
          <n1:AttributeName>GroupName</n1:AttributeName>
          <n1:CurrentValue>testgroup-xrev</n1:CurrentValue>
          <n1:DefaultValue xsi:nil="true"/>
          <n1:Dependency xsi:nil="true"/>
          <n1:DisplayOrder>2</n1:DisplayOrder>
          <n1:FQDD>iDRAC.Embedded.1</n1:FQDD>
          <n1:GroupDisplayName>Group Manager</n1:GroupDisplayName>
          <n1:GroupID>GroupManager.1</n1:GroupID>
          <n1:InstanceID>iDRAC.Embedded.1#GroupManager.1#GroupName</n1:InstanceID>
          <n1:IsReadOnly>true</n1:IsReadOnly>
          <n1:MaxLength>32</n1:MaxLength>
          <n1:MinLength>0</n1:MinLength>
          <n1:PendingValue xsi:nil="true"/>
        </n1:DCIM_iDRACCardString>
    </s:Body>
</s:Envelope>
```

2) Management application can send the SOAP request by following for to get the GroupUUID of the local group which iDRAC part of it.

SOAP request for the `GET GroupManager.1#GroupUUID` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    - <s:Header>
        <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
        <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardString</wsman:ResourceURI>
      - <wsa:ReplyTo>
          <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsa:Action s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/09/transfer/Get</wsa:Action>
        <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
        <wsa:MessageID s:mustUnderstand="true">urn:uuid:44f3780f-2fcc-11e7-81b3-340286bae004</wsa:MessageID>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
      - <wsman:SelectorSet>
          <wsman:Selector Name="InstanceID">iDRAC.Embedded.1#GroupManager.1#GroupUUID</wsman:Selector>
          <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
        </wsman:SelectorSet>
    </s:Header>
    <s:Body/>
</s:Envelope>
```

SOAP response for the `GET GroupManager.1#GroupUUID` attribute:

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardString"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    - <s:Header>
        <wsa:To>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:To>
        <wsa:Action>http://schemas.xmlsoap.org/ws/2004/09/transfer/GetResponse</wsa:Action>
        <wsa:RelatesTo>urn:uuid:44f3780f-2fcc-11e7-81b3-340286bae004</wsa:RelatesTo>
        <wsa:MessageID>uuid:fc9bfbb0-4ea3-1ea3-83b7-11f36eda6618</wsa:MessageID>
    </s:Header>
    - <s:Body>
      - <n1:DCIM_iDRACCardString>
          <n1:AttributeDisplayName>Group UUID</n1:AttributeDisplayName>
          <n1:AttributeName>GroupUUID</n1:AttributeName>
          <n1:CurrentValue>2FA1C5C5BE983A71C52213F2F6A5BEA6</n1:CurrentValue>
          <n1:DefaultValue xsi:nil="true"/>
          <n1:Dependency xsi:nil="true"/>
          <n1:DisplayOrder>3</n1:DisplayOrder>
          <n1:FQDD>iDRAC.Embedded.1</n1:FQDD>
          <n1:GroupDisplayName>Group Manager</n1:GroupDisplayName>
          <n1:GroupID>GroupManager.1</n1:GroupID>
          <n1:InstanceID>iDRAC.Embedded.1#GroupManager.1#GroupUUID</n1:InstanceID>
          <n1:IsReadOnly>true</n1:IsReadOnly>
          <n1:MaxLength>32</n1:MaxLength>
          <n1:MinLength>0</n1:MinLength>
          <n1:PendingValue xsi:nil="true"/>
        </n1:DCIM_iDRACCardString>
    </s:Body>
</s:Envelope>
```

2.7.4 Joining an existing group

If Group Manager feature is enabled in iDRAC, management application can use the DCIM_iDRACCardService.JoinGroup() from iDRAC Card profile to join with existing group.

Refer the iDRAC Card Profile_4.0.0 Session 8.16 in http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile for more details.

Below is an example WSMAN workflow using SOAP to join with existing group, by invoke the DCIM_iDRACCardService.JoinGroup() function .

1) Client can use the DCIM_IDRACCardService.JoinGroup() method from iDRAC Card Profile to Join with existing group.

SOAP Request for JoinGroup

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService"
  xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    - <s:Header>
        <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
        <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService</wsman:ResourceURI>
      - <wsa:ReplyTo>
          <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsa:Action s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/JoinGroup</wsa:Action>
        <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
        <wsa:MessageID s:mustUnderstand="true">urn:uuid:f05f70f0-2fcc-11e7-b0fb-340286bae004</wsa:MessageID>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
      - <wsman:SelectorSet>
          <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
          <wsman:Selector Name="SystemCreationClassName">DCIM_ComputerSystem</wsman:Selector>
          <wsman:Selector Name="SystemName">DCIM:ComputerSystem</wsman:Selector>
          <wsman:Selector Name="CreationClassName">DCIM_iDRACCardService</wsman:Selector>
          <wsman:Selector Name="Name">DCIM:iDRACCardService</wsman:Selector>
        </wsman:SelectorSet>
    </s:Header>
  - <s:Body>
      - <n1:JoinGroup_INPUT>
          <n1:GroupName>testgroup-xrev</n1:GroupName>
          <n1:GroupPasscode>testgroup-xrev</n1:GroupPasscode>
          <n1:GroupUUID>2FA1C5C5BE983A71C52213F2F6A5BEA6</n1:GroupUUID>
          <n1:CloneConfiguration>1</n1:CloneConfiguration>
        </n1:JoinGroup_INPUT>
    </s:Body>
</s:Envelope>
```

2.7.5 Leave a group

Management application can use `DCIM_iDRACCardService.RemoveSelf()` from iDRAC Card profile to remove itself from the local group it is subscribed to.

Refer to the iDRAC Card Profile_4.0.0 Session 8.15 in http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile for more details.

GroupManager.1#GroupName attribute is available in DCIM_iDRACCardString to get the name of the group the iDRAC is subscribed to.

1) Management application can send the SOAP request as shown in the sample here to remove itself from the local group.

   SOAP Request for `DCIM_iDRACCardService.RemoveSelf()`

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService"
  xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    - <s:Header>
        <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
        <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService</wsman:ResourceU
      - <wsa:ReplyTo>
          <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsa:Action s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/RemoveSelf</wsa:Action>
        <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
        <wsa:MessageID s:mustUnderstand="true">urn:uuid:f0c89300-2fcc-11e7-8247-340286bae004</wsa:MessageID>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
      - <wsman:SelectorSet>
          <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
          <wsman:Selector Name="SystemCreationClassName">DCIM_ComputerSystem</wsman:Selector>
          <wsman:Selector Name="SystemName">DCIM:ComputerSystem</wsman:Selector>
          <wsman:Selector Name="CreationClassName">DCIM_iDRACCardService</wsman:Selector>
          <wsman:Selector Name="Name">DCIM:iDRACCardService</wsman:Selector>
        </wsman:SelectorSet>
    </s:Header>
  - <s:Body>
      - <n1:RemoveSelf_INPUT>
          <n1:GroupName>testgroup-xrev</n1:GroupName>
        </n1:RemoveSelf_INPUT>
    </s:Body>
</s:Envelope>
```

2.7.6 Deleting iDRAC local group

Management application can use the DCIM_iDRACCardService.DeleteGroup() from iDRAC Card profile to initiate deletion of the local group the iDRAC is a member of.

For more information, see the *iDRAC Card Profile_4.0.0 Session 8.17* profile document available at http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile.

The `GroupManager.1#GroupName` attribute is available in DCIM_iDRACCardString to get the name of the group iDRAC is a member of.

Here is an example WS-Man workflow by using SOAP to delete the iDRAC group and invoking the `DCIM_iDRACCardService.DeletGroup()` function to delete the group.

1) Management application can send the SOAP request as shown in the sample to delete the Group by giving GroupName.

   SOAP Request for `DCIM_iDRACCardService.DeleteGroup()`

```
<?xml version="1.0" encoding="UTF-8"?>
- <s:Envelope xmlns:n1="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService"
  xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
  xmlns:s="http://www.w3.org/2003/05/soap-envelope">
    - <s:Header>
        <wsa:To s:mustUnderstand="true">https://iDRAC_IP_ADDRESS:PortNo/wsman</wsa:To>
        <wsman:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService</wsman:ResourceURI>
      - <wsa:ReplyTo>
          <wsa:Address s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsa:Action s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/DeleteGroup</wsa:Action>
        <wsman:MaxEnvelopeSize s:mustUnderstand="true">512000</wsman:MaxEnvelopeSize>
        <wsa:MessageID s:mustUnderstand="true">urn:uuid:f8ad72c0-2fcc-11e7-8010-340286bae004</wsa:MessageID>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout>
      - <wsman:SelectorSet>
          <wsman:Selector Name="__cimnamespace">root/dcim</wsman:Selector>
          <wsman:Selector Name="SystemCreationClassName">DCIM_ComputerSystem</wsman:Selector>
          <wsman:Selector Name="SystemName">DCIM:ComputerSystem</wsman:Selector>
          <wsman:Selector Name="CreationClassName">DCIM_iDRACCardService</wsman:Selector>
          <wsman:Selector Name="Name">DCIM:iDRACCardService</wsman:Selector>
        </wsman:SelectorSet>
    </s:Header>
  - <s:Body>
      - <n1:DeleteGroup_INPUT>
          <n1:GroupName><john&john></n1:GroupName>
        </n1:DeleteGroup_INPUT>
    </s:Body>
</s:Envelope>
```

2.8 Configuring Group Manager by using RACADM

The RACADM command-line utility provides a scriptable interface that allows you to locally or remotely configure your iDRAC. The RACADM utility supports the following interfaces:

- Local - Supports running RACADM commands from the managed server's operating system. To run local RACADM commands, install the OpenManage software on the managed server.
- SSH or Telnet — Also known as Firmware RACADM. Firmware RACADM is accessible by logging in to iDRAC by using SSH or Telnet. Similar to Remote RACADM, at the RACADM CLI, directly run the commands without the `racadm` prefix.
- Remote — Supports running RACADM commands from a remote management station such as a laptop or desktop. To run Remote RACADM commands, install the DRAC Tools utility from the OpenManage software on the remote computer.

Administrator privileges are required for a user to run any of the following Group Manager commands successfully.

2.8.1 Enabling or Disabling the Group Manager feature

Following command allows to check if Group Manager Feature is enabled on a server.

```
racadm get idrac.groupmanager.GlobalState
```

Group Manager Feature must be enabled before any other command can be executed. To enable the feature you can make use of following command.

```
racadm set idrac.groupmanager.GlobalState Enabled
```

2.8.2 Group information

To identify the server group to which the iDRAC is a member of, run the following command.

```
racadm get idrac.groupmanager.GroupName
```

To identify the server group unique identifier, run the following command.

```
racadm get idrac.groupmanager.GroupUID
```

2.8.3 Joining an existing group

To join a server to an existing server group, run the following command. A server group is uniquely identified using the group name, UID and passcode parameters.

```
racadm groupmanager joingroup –g <group name> -uid <group UID> -pcode <group passcode>
```

2.8.4 Leaving a group

To leave the server group the iDRAC is part of, run the following command.

```
racadm groupmanager removeself –g <group name>
```

2.8.5 Deleting iDRAC local group

To delete the server group the iDRAC is part of, run the following command.

```
racadm groupmanager delete –g <group name>
```

3 Frequently asked questions and troubleshooting tips

This section lists frequently asked questions and offers troubleshooting tips for common scenarios you might observed:

1) **Some of the servers are no longer listed, or offline, in the Group Manager console.**
   You have onboarded a server into the group and that server no longer shows up in the summary view. This can typically happen if the feature was disabled or the enterprise license expired on that iDRAC. The iDRAC reset to default process resets the feature status to disabled. You should install a valid enterprise license and enable the feature for the server to rejoin the group.

   If the above steps does not work out, you could also check if the server iDRAC is still connected on the same local network. Verify that the iDRAC is reachable by pinging the server iDRAC. Group Manager primary controller keeps a non-persistent cache of all group members. A disconnected server will show up in the Group Manager summary view with iDRAC connectivity status as “offline” until the primary and secondary controllers reboot.

   Duplicate groups may form as a result of a network disruption. Locally reachable iDRACs may coalesce together in this scenario. The duplicate groups will not be detected in the management console until the network is restored. After which, the duplicate groups should merge automatically.

2) **The group configuration job status at Jobs view shows as “Completed with errors”. How can I get more information on errors?**
   The roll up job status provides a consolidated view of job execution status across the group members. Expand the rollup row to view job execution status at a member iDRAC. You could view more information on the job execution at the iDRAC Maintenance->Job Queue or Maintenance->Lifecycle Logs.

3) **Why is user configuration and alert configuration failing on few members where system lock down mode is enabled?**
   The iDRAC9 system lockdown mode feature allows a server system to be locked down from any further system configuration activities. Therefore, user configuration and alert configuration will not be executed on member iDRACs where system lockdown mode is enabled.

4) **You cannot onboard an iDRAC in to a group as the group is not listed in the welcome screen drop down list on that iDRAC.**
   Ensure that the server iDRAC is still connected on the same local network as other group members. Verify that the iDRAC is reachable by pinging the server iDRAC. If the group does not show up still in the list, you could reset the iDRAC to initiate a fresh network discovery. On the iDRAC select iDRAC Settings -> Diagnostics -> Reset iDRAC.

If that still does not work then restart the primary controller iDRAC.

1. Start Group Manager on one of the member iDRACs.
2. In the search box, type the controlling system's Service Tag.
3. Double-click the iDRAC that matches the search results and navigate to **iDRAC Settings → Diagnostics**.
4. Select **Reset iDRAC**.
   When both iDRACs fully restart, the group should be visible.

5) You cannot onboard an iDRAC in to a group from Group Manager console as the server is not listed in the discovered servers view.

- Ensure that the server iDRAC is still connected on the same local network as other group members.
- Ensure that the iDRAC is reachable by pinging the server iDRAC.
- If the server still does not appear in the list, you could reset iDRAC to initiate a fresh network discovery.
- IP address conflicts (duplicate IP addresses) may also cause this issue.
- Therefore, ensure this condition does not exist.
- To reset iDRAC, click **iDRAC Settings → Diagnostics → Reset iDRAC**.

If that still does not work then restart the primary controller iDRAC:

1. Start Group Manager on one of the member iDRACs.
2. In the search box, type the controlling system's Service Tag.
3. Double-click the iDRAC that matches the search results and navigate to **iDRAC Settings → Diagnostics**.
4. Select **Reset iDRAC**.
   When both iDRACs fully restart the group should be visible

6) Duplicate group detected error banner shows up in the Group Manager home page.

A duplicate group can be formed when a group passcode change job fails to execute on few members because those servers were offline during the job execution time. When they get back online they fail to authenticate successfully with the group primary controller as they no longer share a common passcode secret and forms a separate group on their own even though they still share the group name. You could recover by changing the group passcode on the second group. After they share a common passcode, the groups should eventually merge, automatically.

If the duplicate group banner still persists, you could reset the feature status at the controller iDRACs to initiate a fresh network discovery and auto merge if the group members share a common secret passcode.

7) Does leaving a group change any email alert setting or local users?
Leaving a group does not change any iDRAC configuration settings except for removing the group name and passcode. All users and email alert settings remain as is.

8) **My network security scanner indicated that iDRAC was sending mDNS announcements.**
Group Manager uses mDNS announcement on the IPv6 link local network to discover neighbor iDRACs. iDRAC sends group name, Service Tag, and IPv6 address in the mDNS record.

9) **Why does iDRAC have an IPv6 link local address when IPv6 is disabled under network settings?**
iDRAC group management requires IPv6 link local addresses to communicate with peer iDRACs. If you do not want IPv6 traffic then disable Group Manager.

10) **Why does deleting a group take 10 hours?**
iDRAC Group Manager will wait for 10 hours if a member is offline to tell it to leave the group. If all members are online the group Delete will only take a couple of minutes to complete.

11) **What happens in the event of power failure on the Group Primary server?**
On group primary controller server power failure:
    - All in-progress jobs are indicated as 'failed'.
    - When the server comes back online or alternate group primary controller takes over, all the scheduled jobs that have not started will be run, provided they have passed their start time in the order they were scheduled,
    - Failed jobs can be rerun.