

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

Revisions

Date	Description
June 2017	Initial release

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © June-2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [6/27/2017] [Technical White Paper]

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Re	isions/		2
Exe	ecutive	summary	5
1	Introd	uction	6
	1.1	Terms and definitions	7
	1.2	Network configuration requirements	8
	1.3	Prerequisites	9
2	Group	o 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.



Introduction

1

6

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

iDRAC9 - Groupe	ed Serve: ×							- 14	σ	×
← → C ▲N	ot secure bttps://100.65.99.155/	/restgui/igm.html?9048b037e82ffe3a9be1	e14866f5b289	#/					☆	:
integrated [Dell Remote Access Controller								10	í
📅 Grouped Ser	vers								*	
Summary	Discovered Servers Jobs									
		Тс	op 7 System	Model(s)			DellTechnologiesGroup			
		S	erver Model		Mix	Number	58 Server(s)			
		P	owerEdge C64	20	31.03%	18	Controlling System : SVCTG06 Backup System : DC112R7			
		P	owerEdge M64	40	12.07%	7	Created On Thu Jun 22 03:00:36 2017			
		P	owerEdge R64	0	17.24%	10	Group Settings			
		P	owerEdge R74	0	32.76%	19				
		P	owerEdge R74	l0xd	3.45%	2				
		P	owerEdge R94	0	1.72%	1				
		P	recision 7920	Rack	1.72%	1				
🔓 Manage L	ogins 🔸 🛕 Configure Alerts	Export					Q Look Up a Server			1
Health ^	Host Name	iDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update	PowerEdge R640			l
	WIN-02GODDHDJTC	100.65.99.180	M640S08	PowerEdge M640	3.10.10.10	Sat Jun 24 02:29:53 2017	100.65.99.56			
	WIN-C80BBU0AHMP	100.65.99.176, 2607:f2b1:f001:99:867b:ebff.fef4:d254	H722C3S	PowerEdge R740	3.10.10.10	Fri Jun 23 13:29:26 2017	✓ Launch iDRAC More Actions			
		100.65.99.71, 2607:f2b1:f001:99:1298:36ff:feb2:6df	C64ST08	PowerEdge C6420	3.10.10.10	Fri Jun 23 13:30:21 2017	System Information			
		100.65.99.21	M534C2S	PowerEdge C6420	3.10.10.10	Sat Jun 24 02:30:51 2017	iDRAC Connectivity Online			
	WIN-02GODDHDJTC	100.65.99.15	M640S04	PowerEdge M640	3.10.10.10	Sat Jun 24 02:29:39 2017	Power State Off Express Service Code 58843853632			
		100.65.99.126	M533C2S	PowerEdge C6420	3.10.10.10	Sat Jun 24 02:31:39 2017	Operating System			
-				PowerEdge		Sat Jun 24 02:32:38	Asseriag			

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 nonadministrator 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** \rightarrow **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)

8

• 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 <u>Network configuration</u> requirements.
- o Group Manager is accessible only to administrator role user.
- Must be a 14G PowerEdge server with an iDRAC9.
- o 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.

Integrated D									±
🕆 Dashboard	🗏 System 🗸	🛢 Storage 🗸	Configuration V	🖂 Maintenance 🗠	P _a iDRAC Settings ∨				Enable Group Manager
Dashboa	ard								
O Graceful Shu	tdown 👻 🕕	Identify System	More Actions -						

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.

Ma	aintena	ance					
Lif	ecycle Log	Job Queue	System Update	System Event Log	Troubleshooting	Diagnostics	SupportAssist
≡ ι	ifecycle Lo	g					
	Severity	Date ar	nd Time	Message ID	Desc	ription	
+		2017-0	5-10 21:41:51	GMGR0000	The i	DRAC Group Mana	ager feature is disabled.
+		2017-0	5-10 21:41:45	GMGR0001	The i	DRAC Group Mana	ager feature is enabled.

 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.

	Simplify, Automate and Optimize IT operations	
i	Your business depends on efficient management of IT infrastructure and application. Yo maintaining IT availability, improving productivity and reducing operational costs. At resources must remain flexible in response to dynamic business needs. Dell's enterpris solutions drive operational efficiencies that help you achieve dramatic improvements agility of your IT environment.	ou face the challenges of the same time, your is se systems management s in the productivity an
Select Group Actio	Select Action	
	Select Action Jain Existing Group	
	Create New Group	

- 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.

	CI			
Sim;	plify, Automate and Optimize	e IT operations		
Your main resou solut agilit	and application. You face the chall erational costs. At the same time eds. Dell's enterprise systems man- atic improvements in the product	enges of , your IT agement ivity and		
Select Group Action	Create New Gro	up	٣	
reate New Group				
Group Name*		14G_lest		
Group Passcode*				
Group Passcode* Reenter Group Passcode	e*			
Group Passcode*	e*	[]		

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.

Integrated Dell Remote Access Contro	oller 9 Group Manager							10
📅 Grouped Servers								*
Summary Discovered Servers Job	15							
0		Top System M Server Model PowerEdge R94	odel(s) 0	Mix 100%	Number 1	14G_Test 1 Server(s) Controlling System : 1284567 Bockup System : Created On Wed May 10 13 63 29 201 ✓ Croup Settings	7	
🔒 Manage Logins 👻 🔺 Configure A	Jerts 7 Export					Q Look Up a Server		
Health 🗸 Host Name	iDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update	PowerEdge R940		
0			PowerEdge R940		Wed May 10 13:53:44 2017	i centa		
1 Server(s)						Launch iDRAC 1 More A	Actions -	
						System Information		
						IDRAC Connectivity	Online	
						Power State	On	
						Express Service Code	2302946863	
						Operating System		
						Asset Tag		
						Node ID	1234567	
						IDRAC DNS Name	idrac-SVCTAG	

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.

Ma	Maintenance											
Lif	ecycle Log Jo	b Queue	System Update	System Event Log	Troubleshooting	Diagnostics	SupportAssist					
ا ا	Elifecycle Log											
	Severity	Date an	d Time	Message ID	Descr	iption						
+		2017-05	5-10 15:08:03	USR0030	Succe	essfully logged in	using root, from 10.94.95.111 and GUI.					
+		2017-05	5-10 14:25:34	USR0032	The s	ession for root fro	m 10.94.95.111 using GUI is logged off.					
+		2017-05	5-10 13:53:29	GMGR0002	The if	RAC local group	14G_Test is successfully created.					
+		2017-05	5-10 13:51:07	GMGR0003	The it	RAC local group	14G_Test is successfully deleted.					

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 <u>Joining a group from new system</u>.

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.

Integrated Dell Remote Access Controller 9 Group Manager	
A Grouped Servers	
Summary Discovered Servers Jobs	
	Top System Model(s)
	Server Model
	PowerEdge R940

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 <u>Frequently asked Questions and</u> <u>Troubleshooting tips</u>.

Su	Immary Discovered Serve	ers Jobs		J		
۲	Onboard and Change Login	X Ignore VIn-Ignore	C Rescan			
	Host Name	iDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Discovered On
		10000	FZM10Z1	PowerEdge R940	3.00.00.00	Wed May 10 15:29:53 2017
	WIN-22EJ055D928	to	R740SR3	Acme A-1014G	3.00.00.00	Wed May 10 15:31:23 2017
		Jun 48 nn	1234567	PowerEdge R740	3.00.00.00	Wed May 10 15:28:57 2017
		Partie Care	1234567	Acme A-1014G	3.00.00.00	Wed May 10 15:18:50 2017

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.

Onboard and Change Login	
Provide login Information	
Instructions: Provide the system I	ogin information to add this system to the group.
Username*	root
Password*	•••••
Change Password	
Group Manager.	a was detected. Change your system password to use
New Password*	•••••
Confirm Password*	
Apply Group settings	
Clone email alert configuration	• •
	Cancel Onboard

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.

		1.0.0		
Integrated Dell Remote Acce	ess Controller 9 Group Manag	er		
🕆 Grouped Servers				
Summary Discovered Serve	rs Jobs			
Status ∨	Job	ID	Start Time	End Time
+	Join iDRAC	1234567002	Thu 11 May 2017 07:21:04	Thu 11 May 2017 07:26:04

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

I	Integrated Dell Remote Access Controller 9 Group Manager				
1	Grouped Servers				
	Summary Discovered Servers Jobs				
	Status 🗸	Job	ID	Start Time	End Time
	- Completed successfully	Join iDRAC	1234567002	Thu 11 May 2017 07:21:04	Thu 11 May 2017 07:22:26
	LinekName				
	Host Name	Service Tag	Status	Message	
	Host Name	Service Tag FZM10Z1	Status Successful	Message	
	Host Name	Service Tag FZM10Z1 R740SR3	Status Successful Successful	Message	
	Host Name	Service Tag FZM10Z1 R740SR3 1234567	Status Successful Successful Successful	Message	

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.

Helcome to Group	Manager	0	
i	Simplify, Autom Your business dep maintaining IT av resources must re solutions drive op agility of your IT e	nate and Optimize IT operations bends on efficient management of IT infrastructure and application. You face the challenges of vallability, improving productivity and reducing operational costs. At the same time, your IT emain flexible in response to dynamic business needs. Dell's enterprise systems management operational efficiencies that help you achieve dramatic improvements in the productivity and invironment.	งf T d
Select Group Act	ion	Join Existing Group 🔻	
Join Existing Gro	pup		
Group Name	# of Systems	IP Address of One System	
testgroup-xrev	19		
SunilX65_0517	1		
DellEMC Group	50		
Group Passcode Clone email alert coi	nfiguration	······	
		Cancel Appl	y

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.

Gr	oup Setti	ngs						0
Cha	ange Name	Change Passcode	Delete Group					
(Group Nam	ie	DellEMC Group					
1	Number of	Systems	50					
C	Created On		Tue May 23 13:15:59 201	7				
C	Created By		root					
C	Controlling	System	ADC014S					
E	Backu <mark>p</mark> Sys	stem	WR640X2					
	Remove Sy Health	Host Name 🗸	iDRAC IP Addresses		Service Tag	Model	iDRAC Firmware Version	Last Status Update
•	0	WIN-SB6DPF9RI23	, 1		C524C4S	PowerEdge C6420	3.00.00.00	Thu Jun 8 14:00:32 2017
		WIN-QKN452NOIF3			SB740C2	PowerEdge R740	3.00.00.00	Wed Jun 14 16:24:19 2017
	0	WIN-08SME47QPQA			CZZZ7R1	PowerEdge R640	3.00.00.00	Wed Jun 14 11:24:32 2017

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**.

Change Group Name			
Current Group Name New Group Name*	DellEMC Group Dell Technologies Group		
		Cancel	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 <u>Frequently</u> asked Questions and Troubleshooting tips.

To change the group passcode:

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.

Change Group Passcode		
New Group Passcode* Reenter New Group Passcode*]
	С	ancel Change Passcode

- 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.

Confirm Delete Group	
Systems will be updated to be stopped.	o remove their group membership and that any pending jobs will
Group Information	
Group Name	DellEMC Group
Number of Systems	50
Created On	Tue May 23 13:15:59 2017
Created By	root
	Cancel Delete Group

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: <u>https://<Group Member IDRAC IP Address/Domain Name>/restgui/gmlogin.html</u>

C A Not secure 14655// Frestgui/gmlogin.html	
	Integrated Dell Remote Access Controller 9
	ADC014S PowerEdge R640 Group Manager
	Type the User Name and Password and click Log In.
	Username: Password:
	Domain:
	This IDRAC •
	Security Notice. By accessing this computer, you confirm that such access complies with your organization's security policy
	Log In
	DELLEMC
	Online Halo Support Dell TechCenter About

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.

← → C 🔺	lot secure Dttps://masteridracip/rest	gui/igm.html?3cf3fda5b59198f540c371b832351	797&gmsso#/]					Ŕ
Integrated	Dell Remote Access Controller 9	Group Manager							10
🕈 Grouped Ser	rvers								root-720R740
Summary	Discovered Servers Jobs								Logout
			Top 7 System	Model(s)			DellEMC Grou	p	
			Server Model		Mix	Number	50 Server(s)		
			PowerEdge C64	20	36%	18	Controlling System : Backup System :	m : ADC014S WR640X2	
			PowerEdge R64	0	32%	16	Created On Tue I	/lay 23 13:15:59 2017	
			PowerEdge R74	0	20%	10	🖌 Group Set	ings	
			PowerEdge R74	Oxd	6%	3			
			PowerEdge R94		2%	1			
			Unavailable	hauk	2%	1			
🔓 Manage I	Logins - 🔺 Configure Alerts	7 Export					Q Look Up a S	erver	
Health \checkmark	Host Name	IDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update		WIN-BHHGC8PK4F1	
•	WIN-BHHGC8PK4F1			PowerEdge R740xd		Wed Jun 14 16:24:13 2017	i	PowerEdge R740xd	
0	WIN-HBUVCPLOPS9		794NDH2	PowerEdge R640	3.00.00.00	Wed Jun 14 15:44:08 2017	🖌 Launch	DRAC 🐧 More Actions 👻	l
0	WIN-6DVHR2KAEM5		R640613	PowerEdge R640	3.00.00.00	Tue Jun 13 14:10:44 2017	System Info	mation	
0	WIN-NIB3PQNQ0P1		720R740	PowerEdge R740	3.00.00.00	Thu Jun 15 09:22:33 2017	iDRAC Cont	ectivity	Online
0	ADC014S		ADC014S	PowerEdge R640	3.00.00.00	Wed Jun 14 15:32:50 2017	Power State	ina Cada	On
0			DC112R7	PowerEdge R740	3.00.00.00	Thu Jun 8 11:47:57 2017	Express Se	AND COULD	Microsoft Windows 2016 Server
•			1705000	DamarEdan D740	0.00.00.00	Wed Jun 14 18:24:50	Operating S	ystem	Datacenter x64 Edition

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.

🗲 🔶 😋 🛕 Not secure المُوَرَجَعَة المُعَامَة // MemberlDRACIF/restgui/igm.html?07b88baaa6cff27af1a27b768dcb97	íc#/	*
Integrated Dell Remote Access Controller 9 Group Manager		
A Grouped Servers	1 Information	
	Group Manager is launched in another browser tab. Please click Ok to logout.	
	Ok	
		,

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.

🕈 Dashboard 🛛 🗏 System	Storage	Maintenance V • iDRAC Settings V		B Open Group Manager
Dashboard				<u> </u>
0.0				
O Gracetul Shutdown →	Identify System More Actions			
Gracerul Shutdown	Identify System More Actions +	Outer Information	C Virtual Consolo	
System Health	Identify System More Actions	System Information	Sa Virtual Console	

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

← → C 🚺 N	⑦ C A Not secure は成功//mastendoracp/restgui/igm.html?3d3lda5b59198f540c371b832251797&gmsso#/										
Integrated I	Dell Remote Access Controller 9	Group Manager							1.0		
🔒 Grouped Ser	vers								root-720R740		
Summary	Discovered Servers Jobs								Logout		
			Top 7 System	Model(s)			DellEMC Grou	p			
			Server Model		Mix	Number	50 Server(s)				
			PowerEdge C64	20	36%	18	Controlling System	m : ADC014S WR640X2			
			PowerEdge R64	0	32%	16	Created On Tue I	lay 23 13:15:59 2017			
			PowerEdge R74	0	20%	10	🖌 Group Set	tings			
			PowerEdge R74	Oxd	6%	3					
			Precision 7920 P	u Back	2%	1					
			Unavailable		2%	1					
🔒 Manage I	ogins 👻 🛕 Configure Alerts	Report					Q Look Up a S	erver			
Health \checkmark	Host Name	iDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update		WIN-BHHGC8PK4F1			
0	WIN-BHHGC8PK4F1			PowerEdge R740xd		Wed Jun 14 16:24:13 2017	i	PowerEdge R740xd			
0	WIN-HBUVCPLOPS9		794NDH2	PowerEdge R640	3.00.00.00	Wed Jun 14 15:44:08 2017	🖊 Launch	iDRAC 🐧 More Actions 👻			
0	WIN-6DVHR2KAEM5		R640613	PowerEdge R640	3.00.00.00	Tue Jun 13 14:10:44 2017	System Info	mation			
0	WIN-NIB3PQNQ0P1		720R740	PowerEdge R740	3.00.00.00	Thu Jun 16 09:22:33 2017	iDRAC Con	nectivity	Online		
0	ADC014S	-	ADC014S	PowerEdge R640	3.00.00.00	Wed Jun 14 15:32:50 2017	Power State		On		
0			DC112R7	PowerEdge R740	3.00.00.00	Thu Jun 8 11:47:57 2017	Express Ser	vice Code	26957520253		
•			11705000	DeverEdge D740	2 00 00 00	Wed Jun 14 18:24:50	Operating S	ystem	Microsoft Windows 2016 Server, Datacenter x64 Edition		

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

C A Not secure Larg5// MANNEROPROP restgui/index.html?9931de020(c03344ab4a3red251cf183#/							
Integrated Dell Remote Access Controller 9 Enterprise		10					
📅 Dashboard 🛛 🗏 System 🗸 🛢 Storage 🗸 🔲 Configuration 🌱 🖾 Maintenance	1 Information	🔒 Open Group Manager 🚽 🗡					
Dashboard	Group Manager is launched in another browser tab.						
O Graceful Shutdown - Identify System More Actions -							

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>.

	Integrated Dell Remote Access Controller 9	Group Manager						1 0
1	Grouped Servers							*
1	Summary Discovered Servers Jobs							
	0		Top 3 System / Server Model Acme A-1014G PowerEdge R744 PowerEdge R944	Model(s)	Mix 33.33% 33.33% 33.33%	Number 1 1	14G_Test 3 Server(s) Controlling System : 1234567 Backup System : FZM1021 Created On Wed May 10 13 53 29 2017 ✓ Croup Settings	
]	â Manage Logins 🔹 🛕 Configure Alerts	Rxport					Q Look Up a Server	
	Health 🗸 Host Name	iDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update	WIN-22EJO55D928	
	WIN-22EJ055D928	_	R740SR3	Acme A-1014G	3.00.00.00	Thu May 11 00:28:26 2017	Acme A-1014G	
	0		FZM10Z1	PowerEdge R940	3.00.00.00	Thu May 11 16:26:21 2017	Launch iDRAC More Actions -	
	0		1234567	PowerEdge R740	3.00.00.00	Thu May 11 01:25:45 2017	System Information	

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 dropdown menu on the selected server.

Launch iDRAC More Actions Graceful Shutdown Power Cycle System (cold boot) Vistual Operation	Acme	-22EJO55D928 A-1014G
Graceful Shutdown System Information Power Cycle System (cold boot)	🖌 Launch iDRAC	💐 More Actions 👻
Virtual Console	System Information	Graceful Shutdown Power Cycle System (cold boot)

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.

ouped Ser	vers							
mary	Discovered Servers Jobs							
-	•		Top 7 System	Model(s)			Dell Technologies Group	
			Server Model		Mix	Number	50 Server(s) Controllion System : 5DC014S	
			PowerEdge C64	120	35%	18	Backup System : WR640X2	
			PowerEdge R64	10	32%	16	Created On Tue May 23 13:15:59 2017	
			PowerEdge R74	10	20%	10	/ Group Settings	
			PowerEdge R74	40×d	6%	3		
			PowerEdge R94	40	2%	1		
			Precision 7920	Rack	2%	1		
			Unavailable		4.70	1		
Manage L	ogins - \Lambda Configure Aler	ts Rxport					Q Look Up a Server	_
Manage L ealth 〜	ogins + 🛕 Configure Aler	ts Export	Service Tag	Model	iDRAC Firmware Version	Last Status Update	C Look Up a Server WIN-BHHGC8PK4	
Manage L ealth 〜	ogins - Configure Aler Host Name WIN-BHHGC8PK4F1	ts Report	Service Tag CDTT7R1	Model FowerEdge R740xd	iDRAC Firmware Version 3.00.00.00	Last Status Update Wed Jun 14 16:24:13 2017	Q Look Up a Server WIN-BHHGC8PK4 PowerEdge R74Dxd	
Manage L ealth 〜	ogins - A Configure Aler Host Name WIN-BHHGC8PK4F1 WIN-HBUVCPLOPS9	ts Roport	Service Tag COTT7A1 794NDH2	Model PowerEdge R740xd PowerEdge R640	IDRAC Firmware Version 3.00.00.00 3.00.00.00	Last Status Update Wed Jun 14 1624:13 2017 Wed Jun 14 15:44:08 2017	Look Up a Server WIN-BHHGC8PK4 PowerEdge R740xd Lookd DRAD Lookd DRAD Lookd DRAD Lookd Context Lookd Co	r5 →
Manage L ealth 🗸	ogins - 🛕 Configure Aer Host Name WIN-BHICCEPK4F1 WIN-HBUVCPLOPS2 WIN-60V-HR2KAEM5	ts Export	Service Tag CDTT7R1 794NDH2 R640613	Model PowerEdge R740xd PowerEdge R640 PowerEdge R640	IDRAC Firmware Version 3.00.00.00 3.00.00.00 3.00.00.00	Last Status Update Wed Jubn 14 16/24/13 2017 Wed Jubn 14 16/44/08 2017 Tue Jubn 13 14 10/44 2017	Look Up a Server WIN-BHHGC8PK4 PowerEdge R740vd Launch IDRAC More Action System Information	69
Manage L lealth \checkmark	egins - Configure Aler Host Name WIN-BHIGGERK4FT WIN-BUHGGERK4FT WIN-HBUVCPLOPSS WIN-6DVHR2KAEM5 WIN-HIBSPON00PT	ts Export	Service Tag CDTT7R1 794NDH2 R640613 720R740	Model PowerEdge R740xd PowerEdge R640 PowerEdge R640 PowerEdge R640	IDRAC Firmware Version 3 00 00 00 3 00 00 00 3 00 00 00 3 00 00 00	Last Status Update Wed Juan 14 1624:13 2017 Wed Juan 14 15:44:08 2017 Tue Juan 13 14:10:44 2017 The Juan 8 11:49:57 2017	Look Up a Server WIN-BHHGC8PK4 PowerEdge R740x4 Loundh IDHAC More Action System Information	r5 -
Manage L lealth ~	cgins -	ts DERAC IP Addresses	Service Tog CDTT781 79410H2 R640013 720R740 ADC0145	Model PowerEdge R740xd PowerEdge R640 PowerEdge R640 PowerEdge R740 PowerEdge R640	DPAC Firmware Version 3 00 00 00 3 00 00 00 3 00 00 00 3 00 00 00 3 00 00 00	Last Status Update Wed.Jun 14 15:24.13 2017 Wed.Jun 14 15:44.08 2017 Tue.Jun 13 14:10:44 2017 Thu Jun 8 11:49:57 2017 Wed.Jun 14 15:32:50 2017	Look Up a Server WIN-BHHGC8PKA PowerEdge R740xd Laurch IDHAD More Actio System Information IDRAC Connectivity Power State	rs - Onine On
Manage L kealth 🛩	egina - Configure Aler Host Name WIN-BHICGEPK4F1 WIN-BUVCPLOPS3 WIN-BOV-R2KAEMS WIN-HIBSPONCOP1 ADC0145	ts Depart	Service Tag CDTT7R1 794NDH2 R640013 720R740 ADC0145 DC11287	Model PowerEdge H740xd PowerEdge R640 PowerEdge R640 PowerEdge R640 PowerEdge R640 PowerEdge R640	UPAC Firmware Version 3 00 00 00 3 00 00 00 3 00 00 00 3 00 00 00 3 00 00 00	Last Status Update Wed Juln 14 16/24.13 2017 Wed Juln 14 15/44.08 2017 Tile Juln 13 1410 44 2017 Thu Juln 8 11/49.67 2017 Wed Juln 14 15/32.50 217	Look Up a Server WIN-BHHGC8PK4 PowerEdge R740vd Lausch IDHAC More Actio DBAC Connectivity PowerState Express Service Code	P1 Online On 25957522255
Manage L iealth 🗸 D D D D D D D D D D D D D D D D D D D	Image: Configure Aler Host Name WIN-BHHCCEPK4F1 WIN-BHCCEPK4F1 WIN-BUVCPLOPS9 WIN-BEVCPLOPS9 WIN-BEVCPLOPS9	ts DRAC IP Addresses	Service Tag CDITTRI 79440H2 R640613 7208740 ADC0145 DC11287 H72623B	Model PowerEdge R640	DRAC Firmware 3 00 00 00 3 00 00 00	Last Status Update Wed Jun 14 16:24:13 2017 Wed Jun 14 16:24:08 2017 Tue Jun 13 14:08 2017 Thu Jun 8 11:49:57 2017 Wed Jun 14 16:32:50 2017 Thu Jun 8 11:47:57 2017 Wed Jun 14 16:32:50 2017	Look Up a Server WIN-BHHGC8PKA PowerEdge R740xd Laurch IDHAC OrmedUnity Power State Express Service Code Cperating System	P1 Online On 26957520258 Microsoft Vindows 2016 Server; Datacetter 44- Edition

The CSV export contains the following inventoried data:

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

Integrated Dell Remote Access Controller 9 Group Manager				4
* Grouped Servers				
Summary Discovered Servers Jobs	`			
O Rerun ○ Cancel ■ Stop ■ Remove ■ Export				
Status 🗸	Job	ID	Start Time	End Time
+ Stopped	Remove User	ADC014S036	Thu 01 Jun 2017 10:23:48	Thu 01 Jun 2017 10:28:48
+ Stopped	Change User Password	ADC014S033	Wed 31 May 2017 10:51:13	Wed 31 May 2017 10:55:13
+ Stopped	Add User	ADC014S030	Thu 25 May 2017 09:39:18	Thu 25 May 2017 09:44:18

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.

G A	Not secure perps:// MASTERIDRA	(#/restgui/igm.ntmi/aa156529a0d0e22ce6/	1ca31b03ced61#/							¥
Integrate	ed Dell Remote Access Contro	ller 9 Group Manager							18	1 0
# Grouped	Servers									*
Summary	Discovered Servers Jobs									
			Top 7 System	n Model(s)			DellEMC Grou	p		
1			Server Model		Mix	Number	50 Server(s)			
			PowerEdge C6	420	36%	18	Controlling System Backup System	m : ADC0145 WB640X2		
			PowerEdge R6	40	32%	16	Created On Tue N	Nay 23 13:16:59 2017		
			PowerEdge R7	40	20%	10	/ Group Sett	ings		
			PowerEdge R7	'40×d	6%	3	-			
			PowerEdge R9	40	2%	1				
			Precision 7920) Rack	2%	1				
Add New Change I Delete Lis	v User User Password	iDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update	в	WIN-HBUVCPLOPS9		
0	WIN-S86DPF9RI23		C524C4S	PowerEdge C6420	3.00.00.00	Thu Jun 8 14:00:32 2017	i	PowerEdge R640		
	WIN-QKN452NOIF3		S8740C2	PowerEdge R740	3.00.00.00	Wed Jun 14 16:24:19 2017	🖌 Launch i	DRAC Nore Actions		
0	WIN-OBSME47QPQA		CZZZ7R1	PowerEdge R640	3.00.00.00	Wed Jun 1411:2432 2017	System Infor	mation		
•	WIN-NIE3PONG0P1		7208740	PowerEdge R740	3.00 00.00	Thu Jun 15 09:22:33 2017	IDRAC Conn	ectivity	Online	
•	WIN-KBGAKLEDSTM		C3BLD02	PowerEdge C6420	3.00.00.00	Thu Jun 8 23:49:50 2017	Power State		On	
	WIN-K2G802AJFDS		C3BLD03	PowerEdge C6420	3.00.00.00	Thu Jun 8 15:09:54 2017	Express Sen	vice Code	15789480950	
0	WIN-JEGQM4CG000		R740K19	PowerEdge R740	3.00.00.00	Thu Jun 8 10:46:45 2017	Operating Sj	ystem	Microsoft Windows Server 2016 Standari	\$

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.

Add User				0	
User Account Settings					*
User Name*	DELLEMC				
Password*					
Confirm Password*	•••••				
User Privileges					
User Role	Administrator 🔻				
🖉 Login	 Configure) Configure Users			
✓ Logs	 System Control 	Access Virtual Console			
 Access Virtual Media 	 System Operations 	Debug			
Advanced Settings					
IPMI User Privileges					Ŧ
			Cancel	Save	

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.

Integrate	d Dell Remote Access Controli	er 9 Group Manager							
Grouped :	Servera								
	Discovered Servers Jobs								
			Top 7 System Server Model	Model(s)	Mix	Number	DellEMC Gron 50 Server(s) Controlling Syst	4 P em: ADC0148	
			PowerEdge R6 PowerEdge R7	40 40	32% 20%	16	Created On Tue	: W1640X2 May 23 13:18:59 2017 tings	
			PowerEdge R9 Precision 7920	40 I Back	2%	1			
Add New	e Logins • Configure Aler	ts 🛛 🛪 Export	Unavailable		2%	1	C Look Up a S	erver	
Change U Delete Us	er Password	IDRAC IP Addresses	Service Tag	Model	IDRAC Firmware Version	Last Status Update		WIN-HBUVCPLOPS9	
•	WIN-SB6DPE9BI23		C524C45	PowerEdge C6420	8.00.00.00	Thu Jun 8 14:00:32 2017		PowerEdge R640	
	WIN-QKN452N0IF3		SB740C2	PowerEdge R740	3.00.00.00	Wed Jun 14 16:24:19 2017	🖌 Launch	IDRAC 📑 More Actions 👻	
0	WIN-08SME470PQA		CZZZ7R1	PowerEdge R640	3.00.00.00	Wed Jun 14 11:24:32 2017	System Info	rmation	
•	WIN-NIB3PQNQ0P1		7208740	PowerEdge R740	3.00.00.00	Thu Jun 16 00:22:33 2017	IDRAC Con	nectivity	Online
•	WIN-KEGAKLEDETM		C3BLD02	PowerEdge C6420	3.00.00.00	Thu Jun 8 23:49:50 2017	Power Stat		On
•	WIN-K20802AJFDS		CBBLDOB	PowerEdge C6420	3.00.00.00	Thu Jun 8 16:09:64 2017	Express Se	rvice Code	16789480950
~	WINE IFOOM (COOO)		0740K10	RowerEdge 0740	3.00.00.00	Thu: Jun B 10:46:46 2017	operating		

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

De	elete User	r		0
Inst	ructions:	To delete local us click Delete.	sers on all group members, sel	ect the users below and
	User Nar	ne	User Role	Domain
	root		Administrator	Local User
	sbtest1		Administrator	Local User
	GMuser		Administrator	Local User 🗸
				Cancel Delete

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 Grouped Servers						
Summary Discovered Servers Jobs						
	1	Top 7 System Mo	del(s)			DellEMC Group
		Server Model		Mix	Number	50 Server(s)
		PowerEdge C6420		36%	18	Controlling System : ADC014S Backup System : WR640X2
		PowerEdge R640		32%	16	Created On Tue May 23 13:15:59 2017
		PowerEdge R740		20%	10	/ Group Settings
		PowerEdge R740xd		6%	3	
		PowerEdge R940		2%	1	
		Precision 7920 Racl	k	2%	1	
		Unavailable		2%	1	
6 Manage Logins 👻 🔺 Configure Alerts	s 🛛 Export					Q Look Up a Server
Add New User				10040		
Change User Password Delete User	iDRAC IP Addresses	Service Tag	Model	IDHAC Firmware Version	Last Status Update	WIN-BHHGC8PK4F1 PowerEdge R740xd

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.

Change User Password			•
Instructions: To change pass action will apply to every use	swords for users provide the follo r in the group.	owing information. The	*
New Password*			
Confirm Password*			
User Name	User Role	Domain	
root	Administrator	Local User	
132.17	Administrator	Local User	
Gividoe	Administrator	Local User	
			-
	Ca	ncel Change Passv	vord

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**.

Integrated I	Dell Remote Access Controli	ler 9 Group Manager								1 0
Grouped Ser	vers									1
Summary	Discovered Servers Jobs									
			Top 7 System	Model(s)			Dell Technolo	gies Group		
			Server Model		Mix	Number	50 Server(s)			
			PowerEdge C64	20	36%	18	Backup System	WR640X2		
			PowerEdge R64	10	32%	16	Created On Tue I	Aay 23 13 15 59 2017		
			PowerEdge R74	10	20%	10	/ Group Set	tings		
			PowerEdge R74	10xd	6%	3	-			
			PowerEdge R94	10	2%	1				
			Precision 79201	Flack.	2%	1				
			Unavailable		2%	1				
🔒 Manage I	ogins - 🔺 Configure Aler	rts 🗖 Export					Cook Up a S	erver		
Health \sim	Host Name	IDRAC IP Addresses	Service Tag	Model	iDRAC Firmware Version	Last Status Update		WIN-BHHGC8PK4F1		
۰				PowerEdge R740xd		Wed Jun 14 16:24.13 2017	i.	PowerEdge R740xd		
0	WIN-HBUVCPLOPS9		794NDH2	PowerEdge R640	3.00.00.00	Wed Jun 14 15:44:08 2017	🖌 Launch	DRAC 1 More Actions +	í.	
•	WIN-60VHR2KAEM5		R640613	PowerEdge R640	3 00 00 00	Tue Jun 13 14:10:44 2017	System Infor	mation		
•	WIN-NIB3PON00P1		720R740	PowerEdge R740	3.00.00.00	Thu Jun 8 11:49:57 2017				
0	ADC0145		ADC014S	PowerEdge R640	3 00 00 00	Wed Jun 14 15:32:50 2017	IDRAC Conr Power State	ectivity	Online	
•			DC112R7	PowerEdge R740	3.00.00.00	Thu Jun 8 11:47:57 2017	Express Ser	vice Code	26967620253	
•	WIN-D42NDJQIDL1		H725C3D	PowerEdge R740	3.00.00.00	Wed Jun 14 18 24 50 2017	Operating S	ystem	Microsoft Windows 2016 Server, Datacenter x64 Edition	
0			BCHC8R2	PowerEdge R640	3.00.00.00	Thu Jun 8 09:47:08 2017	Asset Tag			

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** \rightarrow **Configuration** \rightarrow **System Settings** \rightarrow **SMTP (E-mail) Configuration**).

Configure email alerts

Storage 🕕

Updates 🕕

Configuration 🚺

Configure email alerts					?
Alerting		Enabled •			
SMTP (E-mail) Server S	Settings				
Server IP Address					
SMTP Port Number*	[
Enable Authentication	L	No 🔻			
User Name					
Password					
Email Addresses					
Instructions: Enter email a	addresses to receie	eve email notifications about system	n status change. You ca	n 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 of	catagories and seve	erities to recieve email alerts on.			
Category		Information	Warning	Critical	
System Health 🕕		V			
Audit 🕕			s		

.

1

1

1

Cancel Apply

1

-

1

 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** \rightarrow **System Settings** \rightarrow **Alert Configuration** \rightarrow **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.

restgui/igm.html?212649e5c537d7817328af4/	1836a364e8#/		
🔂 Welcome	to Group Manager	0	
	Simplify, Automate Your business depend maintaining IT availa resources must rema solutions drive opera agility of your IT envir	te and Optimize IT operations ids on efficient management of IT infrastructure and application. You face the challenges of ability, improving productivity and reducing operational costs. At the same time, your IT ain flexible in response to dynamic business needs. Dell's enterprise systems management ational efficiencies that help you achieve dramatic improvements in the productivity and ronment.	
Select	Group Action	Join Existing Group	
Join Exis	sting Group		
Group Na	me # of Systems	IP Address of One System	
	19		
	1		
	1		
	1		
	50		
Group Pa	sscode	·····	
Clone em	ail alert configuration	0	
		Cancel Apply	

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.

← → C ▲ Not secure bttps:// MASTERIDRACIP/restgui/igm.html?78669bf043ff91888e30bd8bb0980547#	÷/		
Integrated Deli Remote Access Controller 9 Group Manager			_
* Grouped Servers	Onboard and Change Login		
Summary Discovered Servers Jobs	Provide login Information		
Onboard and Change Login X Ignore Vin-Ignore C Rescan	Instructions: Provide the system I	login information to add this system to the group.	
Host Name iDRAC IP Addresses	Username*	root	overed On
	Password*	•••••	Jun 15 05:54:20 2017
			Jun 15 14:52:07 2017
	Change Password		Jun 15 18:36:18 2017
	Instructions: The default passwor	rd was detected. Change your system password to use	Jun 15 20:32:47 2017
	New Decement		Jun 15 05:31:31 2017
	New Password"		Jun 15 05:31:31 2017
	Confirm Password*		Jun 15 05:31:31 2017
	Apply Group settings		Jun 15 05:31:31 2017
			Jun 15 13:11:01 2017
	Clone email alert configuration	× 0	Jun 15 22:50:07 2017
			Jun 15 19:55:09 2017
		Cancel Onboard	Jun 15 05:31:31 2017
0			Jun 15 05:31:31 2017

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
- o Start Time

0

• End Time

Integrated Dell Remote Access Controller 9 Group Manager					10
A Grouped Servers					*
Summary Discovered Servers Jobs	Job	ID	Start Time	End Time	
+ Stopped	Remove User	ADC014S036	Thu 01 Jun 2017 10:23:48	Thu 01 Jun 2017 10:28:48	
+ Stopped	Change User Password	ADC0145033	Wed 31 May 2017 10:51:13	Wed 31 May 2017 10:56:13	

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
 - o 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 <u>Frequently asked Questions and Troubleshooting tips</u>.
 - 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.
 - o 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.

🗧 🔶 🗴 Not secure 以政策:/// <i>MASTEREDRACEP</i> /restgui/igm.html?6fde3e4fbd55212efc6dae3db7895505#/									
integrated Dell Remote Access Controller 9 Group Manager									
📅 Grouped Servers									
Summary Discovered Servers Jobs									
Rerun Cancel Stop Remove Accord									
Status ^	Job	ID	Start Time	End Time					
+ Completed successfully	Remove Members	ADC014S003	Wed 14 Jun 2017 13:23:58	Wed 14 Jun 2017 13:25:40					
- Completed successfully	Join iDRAC	ADC014S006	Tue 23 May 2017 15:14:13	Tue 23 May 2017 15:20:24					
Host Name	Service Tag	Status	Message						
WIN-P77PTJ6A	C64STST	Successful							
	DC112R7	Successful							
	M534C2S	Successful							
	P605C3S	Successful							
	QDCGM3S	Successful							
	R64D120	Successful							
	R640119	Successful							
WIN-4A40NFFR	R66440S	Successful							
	R740C05	Successful							
WIN-JEGQM4CG	R740K19	Successful							
	R740S04	Successful							
	R740S08	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.

C 🔺	Not secure https:// MASTERIDRACP/restgui/igm.html?6	de3e4fbd55212efc6da	e3db7895505#/					0,☆
Integrated D	ell Remote Access Controller 9 Group Manager							1 0
🕈 Grouped Serv	ers							*
Summary	Discovered Servers Jobs							
Rerun	Cancel Stop III Remove 7 Export							
Status 🗸		Job		ID	Start Time		End Time	
- Stopped		Remove User		ADC014S036	Thu 01 Jun 2017 10:23:48		Thu 01 Jun 2017 10:28:48	
Host Nam	e .		Service Tag	Status	Message			
ADC014S			ADC014S	Successful				
			R740S04	Failed	GMGR0047: The group job is either stopped by a u status to see if the job is stopped by the user. If yes, re iDRAC. By using the IDRAC graphical user interface (G RACADM command 'racadm Iclog view'.	user action or failed at the member erun the job if required. 2) If not, rev GUI), on the home page, click Maint	r level.Do the following and rerun the job: 1) Check the group job r view the job execution details in the Lifecycle Log details of the m tenance > Lifecycle Log. By using command line interface (CLI), e	ollup nember nter the
MINWINP	°		WR640X3	Successful				
WIN-OBSN	ME47Q		CZZZ7R1	Failed	GMGR0076: Unable to complete the configuration the queue.Wait for the current operation or local iDRA graphical user interface (GUI), click Job Queue. To vie	operation because either the iDRA C jobs to complete and retry the op w by running the RACADM comma	AC has a pending update process or a pending local configuration peration. To view a list of local IDRAC jobs, on the IDRAC homepa and, enter racadm jobqueue.	i job in ge of
WIN-TB87	76CLI		H725C3D	Failed	GMGR0076: Unable to complete the configuration the queue Wait for the current operation or local IDPA graphical user interface (GUI), click Job Queue. To vie	operation because either the iDRA C jobs to complete and retry the op w by running the RACADM comma	AC has a pending update process or a pending local configuration peration. To view a list of local IDRAC jobs, on the IDRAC homepa and, enter racadm jobqueue.	n job in ige of
			R740S15	Error Occurred. Retrying the Job	O GMGR0046: The group member is unavailable or t	turned off.Wait for the group memb	ber to be available and rerun the job.	
			M534C2S	Failed	GMGR0048: The group job is completed, but with addressing any action items.	errors.Review the job execution de	etails at member IDRAC lifecycle log. Rerun the job if required afte	ĸ
WIN-CN67	77510		M514C4S	Failed	GMGR0047: The group job is either stopped by a status to see if the job is stopped by the user. If yes, n IDRAC, By using the IDRAC graphical user interface (CRACADM command 'racadm lclog view'.	user action or failed at the member erun the job if required. 2) If not, re SUI), on the home page, click Maint	r level.Do the following and rerun the job: 1) Check the group job : view the job execution details in the Lifecycle Log details of the m tenance > Lifecycle Log. By using command line interface (CLI), e	ollup tember nter the
localhost.	lo		4WR640Q	Error Occurred. Retrying the Job	GMGR0046: The group member is unavailable or	turned off.Wait for the group mem	ber to be available and rerun the job.	

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 <u>http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile</u>.

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>
      <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:



• 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:

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

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:

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>
```

 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"</pre>
  xmlns:s="http://www.w3.org/2003/05/soap-envelope">
     <s:Heade
         <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: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">unt:uuid:44f3780f-2fcc-11e7-81b3-340286bae004</wsa:MessageID>

         <wsman:OperationTimeout>PT120.0S</wsman:OperationTimeout</pre>
       - <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:
```

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 <u>http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile</u> for more details.

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

 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
            recuer /
<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>
             vmst.ction s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/JoinGroup</wsa:Action>
            <wsa:MaxEnvelopeSize>
<wsa:MaxEnvelopeSize>
<wsa:MaxEnvelopeSize>
<wsa:MessageID s:mustUnderstand="true">s12000</wsa:MaxEnvelopeSize>
<wsa:MessageID s:mustUnderstand="true">urn:uuid:f05f70f0-2fcc-11e7-b0fb-340286bae004</wsa:MessageID>
<wsa:MessageID s:mustUnderstand="true">urn:uuid:f05f70f0-2fcc-11e7-b0fb-340286bae004</wsa:MessageID>
</wsa:MessageID>

    <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_ComputerSystem</wsman:Selector>

      <wsman:Selector Name="CreationClassName">DCIM:ComputerSystem</wsman:Selector
<wsman:Selector Name="Name">DCIM:iDRACCardService</wsman:Selector>
</wsman:SelectorSet>
</s:Header>
      <s:Body>
           sbouy =
chl:JoinGroup_INPUT>
<n1:GroupName>testgroup-xrev</n1:GroupName>
<n1:GroupPasscode>testgroup-xrev</n1:GroupPasscode>
<n1:GroupUUID>zFA1C5C5BE983A71C52213F2F6A5BEA6</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 <u>http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile</u> for more details.

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

 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()



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 <u>http://en.community.dell.com/techcenter/systems-management/w/wiki/1906.dcim-library-profile</u>.

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"?>
scient version="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:ReplyTo>
          /wsa:Action s:mustUnderstand="true">http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_iDRACCardService/DeleteGroup</wsa:Action>
</wsa:Action s:mustUnderstand="true">512000</wsa:Action>

          vsran:MaxEnvelopeSize s:mustUnderstand="true">512000</msran:MaxEnvelopeSize>
<wsran:MaxEnvelopeSize s:mustUnderstand="true">512000</msran:MaxEnvelopeSize>
<wsa:MessageID s:mustUnderstand="true">urn:uuid:f8ad72c0-2fcc-11e7-8010-340286bae004</msrane=UD</pre>
        <wsman:OperationTimeout>PT120.0S</wsman:OperationTi
- <wsman:SelectorSet>
               assant 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** \rightarrow **Diagnostics** \rightarrow **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**.
- 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.