

Prefailure alerts provided by Dell EMC PowerEdge server systems management

Abstract

Discover the various methods by which OpenManage tools can help provide better server uptime with prefailure alerts.

June 2020

Revisions

Date	Description
September 2015	Initial release
June 2019	First Revision
June 2020	Second Revision

Acknowledgments

Authors: Aparna Giri, Damon Earley, Doug Iler, Jeff Krebs, Lori Matthews, Vish Balakrishnan

Contributors: John Abrams

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 © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [6/25/2020] [White Paper] [ID 426]

Table of contents

Re	vision	IS	2
Acl	knowle	ledgments	2
Tal	ole of	contents	3
Exe	ecutiv	e summary	4
1	Intro	duction	5
	1.1	The integrated Dell Remote Access Controller (iDRAC)	5
	1.2	iDRAC monitoring and alerting	5
2	Alert	ts	7
	2.1	Drive alerts	9
	2.2	System Processor (CPU) alerts	10
	2.3	Memory alerts	11
	2.3.1	1 Memory Page Retire	11
	2.3.2	2 Fault Resilient Memory	11
	2.4	Temperature and fan alerts	12
	2.5	Power Supply alerts	13
3	Beyo	ond Alerts – policy-based actions	14
	3.1	Alerts and OpenManage Enterprise	14
	3.2	Alerts and Partner Consoles	16
4	Cond	clusion	19
Α	Tech	nnical support and resources	

Executive summary

The ability to receive and react to alerts for possible component issues is a critical task for any IT admin. Dell EMC PowerEdge servers provide a wide range of alerts using the integrated Dell Remote Access Controller (iDRAC) and other elements of the OpenManage portfolio. The iDRAC monitors the status of critical subsystems and notifies system administrators about any warning and critical threshold events. With this information, IT administrators can investigate and take corrective action before a component failure occurs, assuring higher server uptime and greater application availability. Often, Dell EMC PowerEdge systems use their embedded intelligence to act automatically. The OpenManage portfolio offers several methods for various IT environments. All the above is part of Dell EMCs comprehensive efforts to use agent-free management technologies to provide intelligent automation.

1 Introduction

The acronym PFA stands for prefailure alert or predictive failure analysis. Originally, PFAs focused on hard drives. The goal was, and still is, to avoid unplanned downtime. Over the years, PFAs have grown beyond hard drives, and now include many other components in the server. This expanded coverage has become increasingly important with the rise of virtualization. Today, there can be multiple virtual servers depending on the underlying physical hardware. This dependency makes taking care of the server more important than ever.

Not all failures are predictable, but the characteristics that are related to gradual mechanical wear and tear can be tracked and monitored. At a certain point, it becomes likely for a failure to occur and iDRAC triggers a warning alert. These alerts and parameters do not address every possible failure mode, but many customers find them useful.

By the end of the 1990s, the various analysis and alerting technologies began to come together under the Self-Monitoring Analysis and Reporting Technology (SMART) standard. Predictive Failure Analysis covers an entire category of predicting impending failures of various components such as drives, memory, and processors. PFA can also mean prefailure alert and predictive failure alert. This paper describes how IT administrators can use information iDRAC provides to best meet the needs of an organization.

1.1 The integrated Dell Remote Access Controller (iDRAC)

The Integrated Dell Remote Access Controller (iDRAC) is designed to make server administrators more productive and improve the overall availability of Dell EMC PowerEdge servers. The iDRAC sends alerts, helps perform remote server management, and reduces the need for physical access to a server.

The iDRAC is part of a larger data center solution that helps keep business-critical applications and workloads available. The technology allows IT administrators to deploy, monitor, manage, configure, update, troubleshoot, and remediate Dell servers from any location, and without the use of software agents. Because the iDRAC is embedded in the server, it can accomplish the above tasks regardless of operating system or hypervisor presence or state.

The iDRAC processor polls each subsystem approximately every five seconds using advanced heuristic algorithms. The iDRAC determines component performance and internal fault conditions that might lead to unscheduled downtime and provides local and remote warnings to IT staff and consoles. By monitoring alerts from the iDRAC, IT administrators can benefit from higher server availability and reduced total cost of ownership.

1.2 iDRAC monitoring and alerting

The iDRAC monitors and alerts the following PowerEdge server subsystems:

- Hard drives and SSDs
- CPU
- System memory
- System temperature
- Fans
- Power Supplies

Monitoring and alerting topics include:

- Health status
- Warning and Failure alerts
- Redundancy Warning and Failure alerts
- Predictive Failure alerts

Actions in response to these alerts include:

- SNMP traps
- Email alerts
- Redfish eventing
- IPMI events
- All events are logged and can be exported manually or remotely using Remote Syslog.
 - From the iDRAC GUI, IT administrators can export the full Lifecycle Controller log and review.
 - iDRAC Enterprise and Datacenter can connect to a Remote Syslog server for consolidation and additional auditing measures.
 - iDRAC9 Datacenter provides an option for telemetry streaming for deeper data analysis. This service sends data to ingress collectors such as Splunk or ELK stack for review.
- Integration into consoles such as Microsoft System Center Operations Manager (SCOM) and VMware vCenter to allow for seamless virtual machine migration.

Actions are user-definable, and a detailed log tracks all alerts that are received. Information from the log includes

- The date and time the alert was received.
- The type and severity associated with the alert.
- The identification of the component that generated the alert.
- Any text that was generated.
- Any actions taken.

As Dell continues to improve its agent-free monitoring and alerting capabilities, a broader range of alerts have become available, reducing the need for software agents. This out-of-band management has the principal benefit of providing critical information, regardless of what operating system or hypervisor, if any, is installed or operational.

The table below provides a high-level overview of the alerts iDRAC provides.

Device	Health status	Warning and Failure alerts	Redundancy Warning and Failure alerts	Predictive Failure Alerts
Drives	✓	✓	✓	✓
CPU	✓	✓	N/A	✓
Memory	✓	✓	✓	✓
Temperature	✓	✓	N/A	N/A
Fans	✓	✓	N/A	N/A
Power supplies	✓	✓	✓	N/A

2

Alerts

This section reviews the various devises and alerts in greater detail.

- o Drives Hard Disk Drive and Solid-State Drive
- o CPU
- o Memory
- o Temperature
- Fans
- Power supplies
- GPUs (requires iDRAC9 firmware 4.00 or higher)
- SFP I/O (requires iDRAC9 firmware 4.00 or higher)

The iDRAC home page, or dashboard, provides a quick view of the health status of the server and storage.

	Il Remote Access Controller 9 Datacenter					વ 🚡 🛔 🕗
Dashboard Dashboard	III System∨ III Storage∨ III Configurat	ion 🗸 🖂 Maintenance 🗸 🌼 iDRAC Sett	ings∨			Erable Group Manager 🕺
	lown + 10 Identify System More Actions +					
🗎 Health Infor		•	System Information		😨 Task Summary	View All Jobs
Ticalarinio		1.07	Power State	ON	🖾 Pending Jobs : 0	
	SYSTEM IS HEALT	нү	Model	PowerEdge R640	No Pending Jobs	
System Health			Host Name Operating System			
Healthy	Detais> 🖾 Heat	hy Details>	Operating System Version		O In Progress Jobs : 0 No In-Progress Jobs	
			Service Tag BIOS Version	JYDP0M2 235		
			BIOS Version	23.6 4.00.00.00	⊙ Completed Jobs : 41	
			IP Address(es)	100.65.242.172	0 with Errors 1 Failed	
			iDRAC MAC Address	588a.5a.e807.76		
			License	Z Detacenter Edit		
Recent Log Severity	S Description			Date and Time \vee	view all 🗔 Virtual Console	Settings
2	The input power for power supply 2 has been restor	rd.		Mon May 27 2019 11:19:39		
0	The power input for power supply 2 is lost.			Thu May 23 2019 09:32:13	 - ignizing or for Nau-Penting Systems Firmers - map (notice) is a foreign state of the Systems Fill for Head Headpoint Systems is foreign at a Institute System 20 Sector 3: foreign at a System 5. 	ten 1
•	The chassis is closed while the power is off. The chassis is open while the power is off.			Thu Apr 18 2019 07:21:45 Thu Apr 18 2019 07:21:40	[PR] De madia advantad Nucl Produkt JPE Sevens 3: Extegrated REC 3 Port 1 Portik Reading from Violana Sant Reager Nucl Product Violana Sant Reager	ion I
2	The chassis is closed while the power is off.			Thu Apr 18 2019 06:08:53	No hand desire excludie or questing Spates detected. Finance means a compatible handsite mails in excludie. Ann black data and the second seco	
0	The chassis is open while the power is off.			Thu Apr 18 2019 06:08:48	File far Estança bardenikar - doublinder same desket General Flowers - being landslike an derenting Station - being landslike an derenting Station Fill find beside Menager	
0	The input power for power supply 1 has been restore The power input for power supply 1 is lost.	rd.		Fri Apr 12 2019 14:07:28 Fri Apr 12 2019 13:31:25		
	The input power for power supply 1 has been restor	rd.		Fri Apr 12 2019 13:31:00	Launch Vinual Conecte	
0	The power input for power supply 1 is lost.			Fri Apr 12 2019 13:30:55		
🕜 Notes				view all 🕂 a	dd note	
Date and Time			Description			\sim
	tegrated Dell Remote A	_			Patt	
	ashboard 🔳 System Shboard	n∨ 🛢 Storage∨	✓ I Configuration ✓		sen	
Da	shouaru					
0 G	raceful Shutdown 🔸	() Identify System	More Actions 👻			
🗏 H	ealth Information				_	
		SX:	STEM IS HEALTHY			
Sys	tem Health		Storage Health			
	Healthy	Deta	ails) 🔽 Healthy	Details		
			<u></u>			

If there were an issue with the server, the 'details' link would show the issue as listed in the Lifecycle Controller log.

On the "System" page, an extended view of the various components and status can be seen.

Integrated Dell Remote Access Controller 9 Datacenter											
A Dashboard System ∨ Storage ∨	🔟 Configuration 🗸 🛛 📼	Maintenance 🗸 🔹 iDRAC Setting	s∨								
System											
Overview Details Inventory Performance	Host OS										
	Summary	Batteries		CPUs/Accelerators	Intrusion						
	Memory	Network Devices	😝 💙 Power	Removable Media	Voltages						

This visual provides an IT admin with quick access to key components. For example, if a warning or critical error happens in "cooling," the icon would change color. The admin can choose that icon to directly access details to pinpoint and correct a warning or critical alert.

Alerts are not limited to the components mentioned previously. The iDRAC also monitors the following, with no need for a software agent in the operating system or hypervisor:

- Network interface cards (NICs)
- Converged network adapters (CNAs)
- PowerEdge RAID controllers (PERCs)
- Chassis intrusion

2.1 Drive alerts

Drive alerts are based on the SMART industry-standard specification for system drives. SMART drives are engineered to provide early warning of certain drive failure indicators. These indicators are meant to give advanced warning of certain types of failures. These warnings do not include defective components, improper handling, or static electricity discharge. However, roughly 60% of drive failures are due to gradual wear and tear. These kinds of failures usually have warning signs that trigger a SMART alert, thus enabling IT administrators to take preventive action.

The iDRAC heuristic algorithms use SMART indicators to monitor drive reliability and data availability. If certain reliability thresholds are exceeded, a predictive failure alert is generated. The iDRAC notes the event in a system log; and, if configured, sends an SNMP trap to a monitoring server. And, if configured with Dell SupportAssist, a trouble ticket is opened automatically, and can dispatch a replacement drive without any human intervention. The iDRAC interface displays a great deal of drive information, including prefailure information and remaining rated write endurance for SSDs.

Integ	rated D	ell Rem	ote Access	Controller 9 Data	acenter									
🕇 Dast	board	🔳 Sy	rstem ∨	🛢 Storage 🗸	Configuration \	Maintenance 🗸	🗣 iDRAC Setti	ngs 🗸						
	Statu	IS	Name		State	Slot Number	Size	Security Status	Bus Protocol	Media Type	Hot Spare	Remaining Rated Write Endurance		
+ 🗆	$\langle \rangle$		SSD 0		Online	0	223.57 GB	Not Capable	SATA	SSD	No	100%		
+ 🗆	Ŷ		SSD 1		Online	1	223.57 GB	Not Capable	SATA	SSD	No	100%		
- 0			Solid State	Disk 0:1:0	Ready	0	111.25 GB	Not Capable	SATA	SSD	No	100%		
	Adv	anced	Properties	S										
	De	vice Desc	cription		Disk 0 in	Backplane 1 of Integrated R	AID Controller 1		Manufacturer			INTEL		
	Op	erational	State		Not Appli	cable			Product ID			SSDSC2BB120G7R		
	Blo	ock Size			512 byte:				Revision			N201DL43		
	Fai	ilure Pred	licted		No				Serial Number			BTDV732400WL150MGN		
	Re	maining I	Rated Write B	Endurance	100%				Manufactured Day			Not Applicable		
	Po	wer Statu	JS		On		Man					Not Applicable Not Applicable		
	Pro	ogress			Not Appli	cable				Manufactured Year Form factor				
			Disk Space		0 GB							2.5 inch		
			AID Disk Spa	ce	111.25 G	3	T10 PI C					Not Capable		
		gotiated			6 Gbps		Encryption Cap				Not Capable			
		pable Spi			6 Gbps		System erase Capability					CryptographicErasePD Capable		
		S Addres				5602C799603 TIT20078S035GA00						Capable PERC H740P Mini (Embedded)		
	Pd	IT NUMBE	:1		CN05947	111200785056GA00	200785035GA00			Enclosure				
									Enclosure			BP14G+ 0:1		
Adva	ance	d Pro	opertie	S										
Dev	vice De	escript	tion			Disk 0 in Back	Disk 0 in Backplane 1 of Integrated RAID Controller 1							
Operational State						Not Applicabl	Not Applicable 512 bytes							
Blo	Block Size													
Fai	ure Pr	redicte	ed			No								
Rer	nainin	ng Rate	ed Write	Endurance		100%								

2.2 System Processor (CPU) alerts

Servers have multiple CPUs, each with multiple cores, and are typically used for virtualization and highperformance applications. As system uptime service level requirements have become increasingly stringent, CPU manufacturing and testing processes have become correspondingly sophisticated. CPU faults are typically unrecoverable errors. If CPU errors occur frequently, certain problems such as L2 cache error corrections can lead to server failure. The iDRAC monitors the number of corrected errors that a CPU reports. If the number of frequencies crosses the heuristic threshold, iDRAC writes an alert to the system log. If configured, iDRAC sends an SNMP trap to a monitoring server. The failing CPU can then be replaced proactively, during a scheduled maintenance window. As with SMART alerts for hard drives, a trouble ticket can be generated, and a replacement part issued proactively.

Special actions can be put in place for servers running a hypervisor from Microsoft or VMware. If configured, the server can go into "maintenance mode" and migrate virtual machines when a CPU alert is received. Detailed information about how alerts work in tandem with virtual machine consoles is covered later in this paper.

Beginning with iDRAC8, PowerEdge servers offer Compute Usage per Second (CUPS) functionality which allows an IT administrator to monitor real-time performance the CPU, memory, and I/O. This data collection operation is independent of operating system and does not consume CPU resources. This out-of-band, real-time monitoring is available by RACADM, Redfish, and the iDRAC web Interface.



An example of CUPS is shown below.

2.3 Memory alerts

With the growing importance of memory in today's compute environment, Dell is taking steps beyond the standard monitoring and alerting on memory errors. In addition to the stand alerts, Dell has pioneered the following solutions: Memory Page Retire and Fault Resilient Memory.

2.3.1 Memory Page Retire

All Dell EMC servers ship standard with Error-Correcting Code (ECC), a first line of defense on errors in system memory. ECC looks for single-bit errors in memory and automatically corrects them, keeping the system running smoothly. Most ECC corrected errors are not isolated. Addresses that experience error corrections once tend to experience them again. If these errors cascade into nearby bits, it can expand beyond what ECC can deal with. In turn, the operating system processes the uncorrectable error and fails the system. With the introduction of iDRAC7 based systems, Dell EMC worked with hypervisor partners Microsoft and VMware to introduce Memory Page Retire (MPR).

The basic flow of MPR is:

- 1. The hypervisor monitors baseline ECC memory faults.
- 2. Should certain regions produce recoverable errors beyond a certain threshold, the section, or page, is retired.
- 3. After 64 Kb of page retires have occurred, the event is logged in the system event log.
- 4. The address and adjoining space is mapped off and unavailable to the hypervisor.
- 5. The defective memory can be replaced during scheduled service time.

Memory Page Retire is supported on Microsoft Windows 2012 R2 and VMware ESXi 5.1 U1 and beyond.

2.3.2 Fault Resilient Memory

Within a virtualization environment, the hypervisor is the brain that sits below the virtual machines, controlling the server resources and distributing them as needed. Hypervisors are exposed to uncorrectable memory errors like any other operating system. However, if a hypervisor fails, they generally bring down more than one application. Fault Resilient Memory (FRM) is a patented technology Dell EMC has introduced aimed at creating more resilient memory protection for the hypervisor.

FRM works with VMware vSphere v5.5 and higher, which uses its Reliable Memory feature to work with FRM.

FRM creates a fault-resilient memory zone for the hypervisor within socket 0 and communicates that address up for the hypervisor to place itself into. The ESXi hypervisor in vSphere v5.5 or higher looks for this address communication, and if found, places itself in the protected zone. The protection FRM provides is as robust as Memory Mirroring. An uncorrectable error that occurs in socket 0 is logged as a System Event, without requiring a full 50% of system memory. This log event gives administrators time to become aware of the issue. They can place the system in Maintenance Mode to clear off running VMs, and then deal with the memory module showing errors.

2.4 Temperature and fan alerts

Temperature alerts provide advanced warning that either the ambient temperature is at or exceeding preset temperature ranges. Dell offers a wide array of alerts and other technologies that help monitor and manage temperature alerts. Temperatures are monitored at server CPU and at the system board inlet. Fans and blowers are well placed within the chassis to provide maximum cooling.

ashboard	🗏 System 🗸	🛢 Storage 🗸	Configuration V	📼 Maintenance 🗸	Ø₀ iDRAC Settings ∨			Enable Group Manager			
emperature	Probes										
					Warning Threshold		Critical Threshold				
status	Probe Name			Reading	Min	Max	Min	Мах			
2	CPU1 Temp			26 °C (78.8 °F)	N/A	N/A	3 °C (37.4 °F)	89 °C (192.2 °F)			
2	CPU2 Temp			26 °C (78.8 °F)	N/A	N/A	3 °C (37.4 °F)	89 °C (192.2 °F)			
2	System Board E	xhaust Temp		25 °C (77 °F)	8 °C (46.4 °F)	75 °C (167 °F)	3 °C (37.4 °F)	80 °C (176 °F)			
2	System Board Ir	nlet Temp		20 °C (68 °F)	3 °C (37.4 °F) Edit	43 °C (109.4 °F) Edit	-7 °C (19.4 °F)	47 °C (116.6 °F)			
resh Air											
Fresh Air Cor	mpliant Configuration	n		No							
Total Operati	otal Operation Time			196 Days							
	pent in Warning Threshold Range			0%	on.						

Fan alerts

∨ 券 Fans				
Fan Status				
			Current Speed	
Status	Name	Туре	PWM (% of Max)	RPM
	System Board Fan1A	Standard Performance	100%	17400
	System Board Fan1B	Standard Performance	100%	15840

Fan status, warnings, and critical thresholds are simple and easy to read. System fan alerts provide warning that a fan may soon fail. As shown in the figure above, iDRAC monitors the system fans for circumstances when RPM speeds fall below, or exceed, certain thresholds. If a single fan has failed, PowerEdge servers are designed with redundant cooling fans, so they can continue operating in a safe temperature range.

The combination of redundant cooling fans and proactive alerts results in a well-designed solution that provides protection against failures due to overheating.

2.5 Power Supply alerts

Power-conditioning uninterruptible power supplies are a highly cost-effective step in defending servers from electrical dangers to their sophisticated and delicate electronic circuits. Once power going to servers has been conditioned properly, the next critical server subsystems to protect are their power supplies. Dell EMC PowerEdge servers are designed to offer redundant power supplies.

As shown in the figure below, iDRAC monitors power supply fan functionality and for voltage variances from preset upper and lower thresholds. If either fan performance or voltage readings are out of tolerance, iDRAC generates an entry in the log and send the alert. As with CPUs, this type of alert is often visible on properly configured hypervisor consoles and can trigger an automatic live migration of VMs, if necessary.



3 Beyond Alerts – policy-based actions

Getting an alert is one thing; acting on it is another. Some companies still have IT staff patrol the aisles of their data center, taking notes of flashing or amber lights. This process is a time-consuming task with the potential for overlooked or missed information.

For customers with a smaller IT shop with a few servers, the emailed alert option from iDRAC can be an effective solution. An iDRAC email alert is both informative and actionable. It provides the server name, service tag, an exact, easy-to-understand description of the error and the error message ID.

But for larger data centers, a more comprehensive solution is required to ensure proper uptime. This section discusses how tools such as OpenManage Enterprise, VMware vCenter, and Microsoft System Center use and consume alerts.

3.1 Alerts and OpenManage Enterprise

For IT shops of all sizes, Dell EMC offers the OpenManage Enterprise console. OpenManage Enterprise is a "one to many" console that can monitor and manage 8000+ PowerEdge servers. Also, OpenManage Enterprise can be set up to receive SNMP traps from almost any servers, storage, or networking device using the MIB importer. OpenManage Enterprise also allows users to set up a policy to trigger an action when the alert is received. IT administrators can also write a script to automate the actions they want to take after receiving certain alerts.

Dpei	Manage Ente	erprise					Search Everything		S 541	F 3125	📑 31	💄 admin	0	٠
Home	Devices	Seconfiguration - P Alerts	🗸 🛛 📼 Monitor 🗸	Application Settings ~	Rever Management -									
🛛 Mon	itor													
Audit Logs	Jobs	Discovery Server Initiated Di	scovery Inventor	ry Warranty Reports	МІВ									
Export +														
Advan	ed Filters													
	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION							
	0	Jun 16, 2020 6:10:38 AM	admin	CUSR0001	10.134.68.55	Audit	Successfully logged in from GUI .							
	8	Jun 16, 2020 6:10:33 AM	adm	CUSR1219	10.134.68.55	Audit	Unable to log in because the prov	ded usernam	e or credent	ials are invalid				
	0	Jun 16, 2020 5:44:18 AM	admin	CUSR0003	10.135.154.1	Audit	Successfully logged off from GUI							
	0	Jun 16, 2020 5:19:22 AM	admin	CUSR0001	10.135.154.1	Audit	Successfully logged in from GUI .							
	0	Jun 16, 2020 5:19:14 AM	admin	CUSR0003	10.135.154.1	Audit	Successfully logged off from GUI							
	0	Jun 16, 2020 4:58:54 AM	admin	CUSR0001	10.135.154.1	Audit	Successfully logged in from GUI .							
	0	Jun 16, 2020 4:55:15 AM	admin	CAPP1322	10.135.154.1	Audit	The action Install is successfully s	tarted for ext	ension Powe	r Manager ver	sion 1.1.0.4	7 by the user ad	tmin .	
	0	Jun 16, 2020 4:54:58 AM	admin	CAPP1322	10.135.154.1	Audit	The action Download is successful	lly started for	extension P	ower Manager	version 1.	1.0.47 by the use	er admi	n .
	0	Jun 16, 2020 4:54:33 AM	admin	CAPP0178	10.135.154.1	Configuration	Console setting automatically uod	ate the conso	le after dowr	nload is compl	ete modifie	d.		
				CJOB0172	10.135.154.1	Configuration	The job Default Console Update T	sek with id 1	0014 of type	consoleundate	hac heen	applad		
	0	Jun 16, 2020 4:54:33 AM	admin	CJOB0172	10.130.104.1	Comgulation		ask with to th	ours or type	consolcupuan	nus occii	enableu.		

The following image shows the 'wizard' to help create a policy action based on event.

OpenManage Enterprise				Search Everything	
🖌 Home 🔳 Devices 🔗 Configuration 🗸 🔰 Alerts 🗸 📼 Monitor	Create Alert Policy				0 ×
✓ Alerts	Name and Description	Name			
Alert Log Alert Policies Alert Definitions	Category	Description			
	Target				
Create Edit Enable Disable Delete	Date and Time				
ENABLED NAME DESCRIPTION	Severity	Enable Policy	V		
□ [✓] Mobile Push Notification - C This policy is applicable t	Actions				
□ [✓] Default OnDemand Health This policy is applicable t					
□ [✓] Mobile Push Notification - Al… This policy is applicable t	Summary				
□ [✓] Arris	Step 1 of 7				
□ [✓] Mobile (created by Manoj) Test alert policy for OMM				Next	ancel
□ [✔] gm			[] []	[]	[]
□ [✓] Customer A Test Alert Policy Push All Alerts to Mobile			[] []	[]	[]
□ [] test			[] []	[]	[~]

OpenManage Enterprise Power Manager is a plug-in to OpenManage Enterprise. Power Manager uses power capping to ensure power for a group of servers remains within the envelope the customer sets for the server group. An admin defines a group of servers by rack, row, or room of a data center. This policy ensures that a rack does not spike power over the allotted WATTs in order to prevent breaker tripping or grid failure. In addition, Power Manager uses power capping to immediately lower power on a group of servers that exceeds the customer set temperature. Power capping can prevent an outage of servers due to high temperatures.

OpenManage Enterprise Power Manager uses alerts to warn the customer using the OpenManage Enterprise console, email, or mapped to another vendor console. This integration allows the customer to react to the power or thermal alert for a group of servers before experiencing an outage.

OpenManage Enterprise	Create Policy										Θ×
Home Devices Opfiguration V Merts V Power Management	General 🖌 Devices/Groups	Policy Type: Selected Group:		Static Datacenter	BDC						
Power Management Overview Devices and Groups Policies Emergen Create CEE Enterie Constitue ** Advanced Filters DRABED NAME DESCR DRABED NAME DESCR DREm(s) found. D Item(s) selected: Displaying items 0 - 0.	Devices/Groups Policy Settings Policy Schedule Summary Step 3 of 5	Seeced Group: Power Capping and Power capping and Power capping and Power capping and Power cap for the term the selected devices or ef- defined value. Power cap Power cap for to Configure the powe DEVICE NAME 100.96.27.38 R740XDN02.vac. Iocalhoat bir arme Iocalhoat b	ures that power ried d valuested devices of the the power canon propose do not exceent devices in gr cap value or pe service TAG 3N67HV2 3LH2033 3LG2033 3LG2033 3LG2033 4JR56Z1 4JB2552 9VL7F02 8JX60T2	consumption or groups oup ercentage for power cal 382 721 554 557 394 0 1653 13891 13891 13891 2733	1 Day 71044 80.13	Watt	~	Power Data d Minim Avera Maxin Lower Upper	History (W bollected on: num: 3164 ge: 4841 mm: 7159 Bound: 237 Bound: 237 Bound: 237 Bound: 827 426 0 1757 16685 2734	att) 6/15/20 3/1 00 83 MINIMUM 142 204 272 272 272 272 274 5 160 194 338 1088 118	AVERAGE 144 206 277 263 6 163 212 372 1312 × × Cancel

The following image shows the granular choices on the "Policy Settings" page of the wizard.

Step 4 shows the details of the "Policy Schedule."

OpenManage Enterprise				Search Eventithing	. a .
🐂 Home 🔳 Devices 🗇 Configuration 🗸 🏲 Alerts 🗸	Create Policy				0 ×
Power Management	General	Time Span	○ Always	Range	
Overview Devices and Groups Policies Emergenc	Devices/Groups	 Inne span 	· · · · · · · · · · · · · · · · · · ·	AM To 10 00 AM	
Create Edit Emple	Policy Settings 👻	•			
> Y Advanced Filters	Policy Schedule 😽	Day(s)	○ Always	Daily	
ENABLED NAME DESCRIP	Summary	•	Every	⊠SUN ⊠MON ⊠TUE ⊠WED ⊠THU ⊠FRI ⊠SAT	
0 item(s) found, 0 item(s) selected. Displaying items 0 - 0.				0	
		Active Date	Always	○ Range	
	Step 4 of 5			Previous Next	Cancel

Step 5 is the summary slide.

Home Devices © Configuration Alerts Create Power Management Overview Devices and Groups Policies Emergenc	il 🛩	Review your inputs ar	ud aliak Tiniak to postinu	e ×
Crower Management		Review your inputs an	ud aliak Tiniah ta aantinu	
Overview Devices and Groups Policies Emergence				
	s/Groups 🗸			
	Settings 🗸 🗸	ATTRIBUTE	VALUE	
Create Est English Cleable De		Name	Policy 1	
> T Advanced Filters	Schedule 🗸	Policy Description	Policy to cap power at 80%	% for all but 2 servers in Rack 3, Row 12
	ary 💞	Enabled	True	
		Selected Group	Datacenter BDC	
0 item(s) found, 0 item(s) selected. Displaying items 0 - 0.		Power cap value	71044 Watt	Contractor Tractor Made and Theorem
		Date Range	Always	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
		Time Span	02:00 AM - 10:00 AM	
		Day(s)	Sunday, Monday, Tuesday	r, Wednesday, Thursday, Friday, Saturday

3.2 Alerts and Partner Consoles

For virtualized environments running Microsoft Hyper-V or VMware ESXi, Dell EMC offers OpenManage integrations with both System Center Virtual Machine Manager (SCVMM) and VMware vCenter. This integration allows customers to set different actions that are based on alert type and severity.

Dell EMC and Microsoft have worked together since 2009 developing PRO packs which can take standard server alerts and translating them into end-user actionable events.

IT administrators can set a certain policy that is based on a specific action. For example, it is possible to place a server in maintenance mode and vacate virtual machines if a server loses a redundant power supply. Alternately, such alerts can inform an administrator without triggering a specific action.

In the examples below, an IT administrator receives a PRO alert, such as a memory device or redundancy lost alert. Then, the administrator can decide to implement the action, dismiss it, or take other action.

Monitoring	Dell Server PRO Alerts (2)						
🖂 🌉 Monitoring	Look for:		Find Now Clear	Find Now Clear			
Agentless Exception Monitoring	🚇 Path	Source	Name	🔨 Resolu	io Created		
Crash Listener View 1:2 Error Events Error Group View	E Severity: Warning (1)						
	Hyperv5.propa	k.lab Hyperv5.propack	Dell OMSA Event: Temperatur	e sensor detected a wa New	4/15/200		
System Error Group View	🖻 Severity: Critical (1)						
Cell Server PROPack	🚫 Hyperv5.propad	k.lab Hyperv5.propack	Dell OMSA Event: Memory dev	rice is in error state. New	4/15/200		
 Dell PROPack Monitored Servers Dell Server PRO Alerts Dell Server PRO Alerts Microsoft Audit Collection Services 							

	Source	Tip		State	
7	PRO6950.mp4.com	Dell OMSS Event: Redundancy lost.		Active	
0	PRO6950.mp4.com	Dell OMSS Event: Storage Management has lost communication v	with the controller.	Active	
P	RO6950.mp4.com				
	Dell OMSS Eve	nt: Redundancy lost.	Host Summ	ary	
Re	dundancy lost warning.		Name:	PR06950.mp4.com	
Dell OMSS Event: Redundancy lost.			Host group:	All Hosts	
Cause and Resolution A virtual disk or an enclosure has lost data redundancy. In the case of a virtual disk, one or more physical disks included in the virtual disk have failed. Due to the failed physical disk or disks, the virtual disk is no longer maintaining redundant (mirrored or parity) data. The failure of an additional physical disk will result in lost data. In the case of an enclosure, more than one enclosure component has failed.		Average CPU:		3%	
		Memory:		19 \$	
		Storage:		9%	
		ce from the virtual workloads, it is recommended that all s be migrated from this server to another healthy server			

Alert integration is also available for VMware customers. The Dell EMC OpenManage Integration for VMware vCenter inserts custom alarm definitions that enable administrators to remediate failures in an automated fashion, as shown below. By integrating into VMware "events, alarms, and actions mechanism," administrators can see and react to hardware errors. Options include placing the server in maintenance mode, running a batch file, or sending an email. This integration reduces workload downtime by ensuring virtual machines can be moved to another host in the cluster before a catastrophic physical error occurs.

The following image shows the page for enabling alarms and events in OpenManage Integration for VMware vCenter console.

vm vSphere Client Menu ∽ Q						٢
Ym vSphere Client Menu ∨ Q OpenManage Integration	Stearch in all environments OpenManage TM Integration for VMw. Dashboard Hosts & Chassis Compliance & Deploym Appliance Settings Notifications > Deployment Credentials Override Severity for Proactive HA Initial Configuration Wizard Firmware Update Settings VCenter Settings Data Retrieval Schedule > License Support		vCenter IP/FODN: 100.68.121.220	C @ ~	Administrator@VSPIERELOCAL ~	0
Recent Tasks Alarms Task Name Validate the cluster specification Target Validate the cluster specification Im XX/40c vSAN	Support About	APPLY CANCEL Initiator Com.vmvare.vsan.heelth 13 ms	 ✓ Start Time 06/17/2020, 9:59:14 AM 	 Completion Time 06/7/2020. 9-5 		**************************************
					Ν	More Tasks

The next image shows the alarm definitions at the host level in vCenter.

vm vSphere Client Menu ∨ Q	Search in all environments		C 🧷 Administrator@VSPHERE.LOCAL V 😳
	🚡 f10-vcfhost01.delllabs.r	net Actions 🗸	
Comparing the second seco	Summary Monitor Configure VM Startup/Shutdown Agent VM Settings Default VM Compatibility Swap File Location System V Licensing (Host Profile Time Configuration Authentication Services (Permissions VAs Datastores Networks Updates Larm Definitions App EDIT ENABLE/DUSABLE DELETE App EDIT ENABLE/DUSABLE DELETE Adam Name 1 v Object type v Dethod n v Enabled Dell - Physical disk failure Host Enabled Pro-center. Enabled Dell - Physical disk warring Host Enabled Pro-center. Enabled Dell - Power Supply audit failure or Host Pro-center. Enabled Dell - Power Supply audit maine Host Enabled Pro-center. Enabled Dell - Power Supply audit maine Host Enabled Pro-center. Enabled Dell - Power Supply audit failure or Host Pro-center. Enabled Dell - Power Supply audit failure or Host Pro-center Enabled Dell - Power Supply detected a fail Host Pro-center Enabled Dell - Power Supply detected a fail Host Pro-center Enabled	v Last modified v 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM 06/16/2020, 9:33:54 AM
	Firewall Services Security Profile System Swap Packages Hardware V Overview PCI Devices	Description A power supply has been disconnected or has falled. Targets All hosts in vCenter server f10-venterol1.deliabs.net Alarm Rules IF A power supply has been disconnected or has failed. THEN trigger the alarm as ① critical and enter failed. Last modified OG/f6/2020, 9:3350 AM Dell - Power supply detected a wa_ Host 1/2 f10-venter_ Enabled	06/16/2020, 9:33:50 AM
	Firmware () Virtual Flash V () Virtual Flash Resource Mana ()	>> Dell - Power supply inserted Host ⁽²⁾ fl0-vcenter Enabled >> Dell - Power supply returned to no Host ⁽²⁾ fl0-vcenter Enabled >> Dell - Power supply sensor detect Host ⁽²⁾ fl0-vcenter Enabled >> Dell - Power usage audit failure or Host ⁽²⁾ fl0-vcenter Enabled	06/16/2020, 9:33:49 AM 06/16/2020, 9:33:51 AM 06/16/2020, 9:33:50 AM 06/16/2020, 9:33:54 AM BI - 100 of 14:3 sems K (5 / 23 > X)
Recent Tasks Alarms Task Name Validate the cluster specification Target Validate the cluster specification MX740c vSAN	✓ Status ↑ ✓ De ✓ Completed ✓ Completed	tails Initiator Queued For V Start Time comumicare usan health 13 ms 06/17/2020, 10:02:28 AM comumicare usan health 13 ms 06/17/2020, 9:5914 AM	Completion Time Server Ob/17/2020, 10:02:28 AM TD-vcenterOI delilabs.net Ob/17/2020, 9:59:14 AM TD-vcenterOI delilabs.net
			More Tasks

4 Conclusion

Dell EMC delivers an extensive PFA and performance monitoring technology by the iDRAC embedded in every PowerEdge server. The iDRAC and the comprehensive OpenManage portfolio provide effective, proactive management that is designed to make IT administrators more effective and efficient. PFA monitoring and alerts from iDRAC are the first steps in this process. The solution becomes more powerful when combined with "one to many" consoles such as OpenManage Enterprise, Microsoft System Center, or VMware vCenter.

Dell EMC systems management technology is dedicated to monitoring and managing your servers so you can manage your business.

A Technical support and resources

The iDRAC support home page provides access to product documents, technical white papers, how-to videos, and more.

www.dell.com/support/idrac

iDRAC User Guides and other manuals www.dell.com/idracmanuals

Dell Technical Support www.Dell.com/support