###

Integrated DELL(TM) REMOTE ACCESS CONTROLLER (iDRAC) Version 1.40

###

This document contains updated information about the Integrated Dell
Remote Access Controller (iDRAC).

For more information about iDRAC, including installation and
configuration information, see the "Integrated Dell Remote Access
Controller User's Guide" and the "Dell OpenManage(TM) Server
Administrator User's Guide." These documents are located on the Dell
Support website at "support.dell.com\manuals".

###
TABLE OF CONTENTS
###

This file contains the following sections:

* Criticality

* Minimum Requirements

* Release Highlights

* Known Issues for iDRAC version 1.40

* Known Issues for Documentation

###
CRITICALITY
###

2 - Recommended

###
MINIMUM REQUIREMENTS
###

The following subsections list operating systems that are compatible
with the iDRAC.

===
SUPPORTED SYSTEMS
===

iDRAC is supported on the following Dell PowerEdge(TM) systems in the
Dell PowerEdge M1000e system enclosure:

* Dell PowerEdge M600
* Dell PowerEdge M605

* Dell PowerEdge M805
* Dell PowerEdge M905

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.40)
##

* iDRAC version 1.40 has critical security enhancements
* support for 1:many firmware update through the Chassis Management
* Single Sign On from the Chassis Management
* Microsoft(R) Active Directory(R) performance improvement
* Regular Maintenance

##
KNOWN ISSUES FOR iDRAC FIRMWARE VERSION 1.40
##

This section provides additional information about known issues with
the iDRAC Firmware version 1.40.

* Flashing from pre-1.2 iDRAC on VMware(R) ESX

When attempting to flash earlier than iDRAC 1.2 releases, the Dell
Update Packages Utility does not have the logic to find the USB
devices correctly in the VMware ESX. Therefore, it is required
that other flashing methods be used instead on VMware ESX.

* Using virtual devices on VMware ESX Console, after an iDRAC Update

Please reboot the managed server running VMware ESX 3.x one time
after an iDRAC update is completed. This will ensure that the VMware
ESX re-enumerates the virtual devices and enables virtual floppy
and virtual CDROM features of the iDRAC. After that reboot, virtual
devices, including the Virtual Floppy, work fine.

* Disabling Local Configuration Access

In order for the disabling of local configuration access to work at
the iDRAC Configuration Utility level (Ctrl-E at bootup), the BIOS
in your system needs to be at least at the following level:

PowerEdge M600 - BIOS version 2.1.2
PowerEdge M605 - BIOS version 4.0.0
PowerEdge M805/M905 - BIOS version 0.2.3

* Possible Active Sessions versus Current Active Sessions in
  Dell OpenManage Server Administrator

In Server Administrator, the number of "Current Active Sessions"
displayed for iDRAC refers only to the number of currently
active IPMI transaction sessions, and does not include web GUI
or SSH/SM-CLP sessions.

* Using special keys in "keyboard passthrough" mode

Special keys such as the Microsoft Windows(R) key, CTRL-Prnt Scrn, and
ALT-Function key combinations in keyboard passthrough mode will be
problematic, as some combinations are sent to the Viewer itself
and might produce undesirable behavior. Special provision is made in
the Java and ActiveX viewers for macros under the Keyboard menu
pulldown which allow the user to send such combinations and special
keys directly to the managed server.

* Configuring iDRAC to use Static IP using 'syscfg' utility

Given below is the method to use the syscfg utility to set the iDRAC
to use a static IP address. It has to be done in two steps:

  Step 1: "syscfg lcp --ipaddrsrc=static"

  Wait at least 5 seconds. After this time, the change to static IP
  will be in effect and the next syscfg command will succeed.

  Step 2: "syscfg lcp --gateway=(gateway IP)
        --ipaddress=(valid IP address)
        --subnetmask=255.255.255.0"

* Configuring the 'Host Name String' using the iDRAC Configuration
  Utility

With Server Administrator installed:

Server Administrator takes precedence. Server Administrator sets the
Host Name String' every time it starts up. Given above, even if
'Host Name String' is set using the iDRAC Configuration Utility, it
will be overwritten by Server Administrator when it starts up.

With Server Administrator NOT installed:

The iDRAC Configuration Utility can be used to configure the 'Host
Name String'.

* Accessing remote floppy disks and CD-ROMs from (VMWare) VMs

Accessing remote floppy disks and CD-ROMs from (VMWare) VMs is NOT
supported.

Only devices directly connected to an ESX server or a floppy
or CD-ROM ISO image present in the ESX Service Console can be made
accessible to the VM. Avoid this issue by creating an image of the
floppy or CD-ROM and copying it to the Service Console.

* Updating iDRAC using DOS update utility, from a PXE network setup

iDRAC can be updated using the DOS utility when DOS is booted
using PXE. However, the new firmware image has to be on a local
media on the server for this to work properly. Local media can be
a RAMDISK, HD or USB key on the server. Alternatively, the update
of iDRACs on multiple servers has to be sequenced, for example done
one server after the other, with the first completing update
and the second starting the update and so on to the third after
the second is done, fourth after the third is done, and so on.

* Usage of virtual CD-ROM in SLES 9

Use the auto-attach option in the vMedia area of the Web GUI of the
iDRAC when using CD-ROM devices in SUSE(R) Linux Enterprise Server 9.

Another way to do the same when using SM-CLP is to set the
/system1/sp1/oemdell_vmservice1 enabledstate to VMEDIA_AUTO_ATTACH.

* RACADM restore default configuration behavior

The racresetcfg command in RACADM restores all properties except
cfgDNSRacName in the cfgLanNetworking group to their default values.

* Configuring iDRAC using RACADM config

The actual time the user needs to wait after executing the
racresetcfg command within racadm may vary depending on the
network speed.

* iDRAC Media Redirection using floppy disks on Windows Vista(R)
management station with IE7 and ActiveX

The iDRAC's IP address needs to be added to the 'Trusted Sites' list,
before launching the Console Redirection session on a management
station running Vista with IE7.

1 Click Tools-> Internet Options-> Security-> Trusted sites.
2 Click "Sites" and enter the IP address or DNS name of the iDRAC.
3 Click "Add".

* Configuring specific DNS parameters using
  'racadm config -f <filename>'

DHCP has to be enabled on the iDRAC for the following two DNS
parameters to be configurable, using 'racadm config -f <filename>' -
1) cfgDNSServersFromDHCP, 2) cfgDNSDomainNameFromDHCP.

* Behavior of the iDRAC Virtual Media functionality, when the media
is removed on Windows:

When the media is removed, the Explorer window(s) for this media do
not close by themselves.

User action IS required. Please close the Explorer window(s),
when the media is removed.

On Linux:

When the media is removed, the file browser window(s) for this media
do close by themselves.

User action is NOT required.

* Using the iVMCLI tool from within a system running Windows Vista

To use iVMCLI from within a system running Windows Vista:

The user has to start up the 'cmd' with 'Run as Administrator'.
(iVMCLI requires that the user has 'administrator' privileges
when it is used.)

Note -

User can log in as a non-admin user, but when using iVMCLI, the user
has to start 'cmd' with 'Run as Administrator' thereby giving them
admin privileges to enable using iVMCLI.

###
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.20)
###

iDRAC ver. 1.20 has critical security enhancements, new operating
system and browser support, and new features like Boot Capture Replay
and improved health status visibility.

Fixes and Enhancements in 1.20
----

* Windows Server(R) 2008 (Longhorn),ESX (latest version),
  Windows Server 2003 R2 and Red Hat(R) Enterprise Linux(R) 5
  operating system support as managed server operating systems.

* Added support for 64-bit Firefox and IE browsers

* Generate a default Self Signed SSL certificate.

* An option to disable access to iDRAC configuration by any user or
  local RACADM.

* SSL 2.0 is no longer supported due to security risks in SSL 2.0.

iDRAC will negotiate to use SSL 3.0 if both (SSL 2.0 and SSL 3.0)
are present

* Expanded Health Error Reporting Tree

* Java Runtime Engine and Java Development Support updated to Version
  6 Update 7 (JRE1.6u7)

* Two Concurrent KVM Sessions are now supported (from different
  clients) to the same iDRAC

* iDRAC Console Viewer now supports Mouse Scrolling

* iDRAC Web Interface will list the MAC/WWN present on the server and
  support the persistent MAC functionality of FlexAddress

* iDRAC Web Interface will list Storage Daughter card and I/O
  Mezzanine Card population.

* Boot Capture console replay for last three boot sequences.

* Improved Power Usage Reporting

* Improved support for non-US-ASCII keyboards

###
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.11)
###

iDRAC version 1.11 has key fixes for Active Directory,
Services (SSH, SOL) and in addition supports the FlexAddress feature.

###
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.03)
###

Enhanced TOE key detection.

###
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.02)
###

A few fixes in the version display, SM-CLP, last crash screen
page and so on are included in this release.

###
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.0)
###

* Initial release of iDRAC firmware.

###
KNOWN ISSUES FOR DOCUMENTATION

##

This section provides additional information about known issues with
the iDRAC Firmware version 1.4 User's Guide:

* None

##

Information in this document is subject to change without notice.
(C) 2009 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without
the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: "Dell", "OpenManage", and
"PowerEdge" are trademarks of Dell Inc.; "Microsoft", "Windows",
"Windows Server", "Windows Vista", and "Active Directory" are
trademarks or registered trademarks of Microsoft Corporation
in the United States and/or other countries; "SUSE" is a registered
trademark of Novell, Inc.; "Red Hat" and "Linux" are registered
trademarks of Red Hat, Inc in the United States and other countries;
VMware is a registered trademark of VMware, Inc. in the United States
and/or other jurisdictions.

Other trademarks and trade names may be used in this document to refer
to either the entities claiming the marks and names or their products.
Dell Inc. disclaims any proprietary interest in trademarks and trade
names other than its own.

March 2009