##########################################################################

DELL(TM) REMOTE ACCESS CONTROLLER (DRAC) 5

##########################################################################

This document contains updated information about the Dell Remote Access Controller (DRAC) 5.

For more information about DRAC 5, including installation and configuration information, see the "Dell Remote Access Controller 5 User's Guide" and the "Dell OpenManage(TM) Server Administrator User's Guide." These documents are located on the Dell Support website at "www.support.dell.com" or on the "Dell Systems Management Tools and Documentation" DVD.

##########################################################################
TABLE OF CONTENTS
##########################################################################

This file contains the following sections:



##########################################################################
CRITICALITY
##########################################################################

3 - Optional

##########################################################################
MINIMUM REQUIREMENTS
##########################################################################

The following subsections list minimum requirements for the efficient working of the DRAC 5.

==========

## SUPPORTED SYSTEMS

DRAC 5 is supported on the following Dell PowerEdge(TM) systems:

* Dell PowerEdge 1900, 1950, 2900, 2950, 2970, 6950, R300, R900, T300, T605, R805 and R905.

## SUPPORTED MANAGED SERVER OPERATING SYSTEMS

The DRAC 5 is supported by the following operating systems:

* Microsoft(R) Windows(R) 2000 Server family

  - Windows 2000 Advanced Server(R) with Service Pack 4 (SP4).
  - Windows 2000 Server with SP4.

* Microsoft Windows Server 2003 family

  - Windows Server 2003 R2 x86 Enterprise and Standard Editions with SP2 (32-bit).
  - Windows Server 2003 R2 x64 Standard, Enterprise and Datacenter Editions with SP2.
  - Windows Server 2003 x86 Web, Standard and Enterprise Editions with SP2
  - Windows Server 2003 x64 Standard, Enterprise and Datacenter Editions with SP2
  - Windows Small Business Server 2003 R2 SP1 & SP2 Standard Edition.
  - Windows Storage Server 2003 R2 X64 Express, Workgroup, Standard and Enterprise Editions.

* Microsoft Windows Server 2008 family

  - Windows Server 2008 x86 Web, Standard, Enterprise, and Core Editions.
  - Windows Server(R) 2008 x64 Standard, Enterprise, DataCenter, and Core Editions.
  - Windows Small Business Server 2008 R2 SP1 & SP2 Standard and Premium Editions.
  - Windows Essential Business Server 2008.

* Microsoft Windows XP Professional X86.

* Microsoft Windows Vista(R) Business and Enterprise Editions.

  NOTE: Microsoft Windows Small Business Server 2008 is scheduled to be available in the second half of 2008. For latest information, see: http://www.microsoft.com/windowsserver/essential/sbs/default.mspx

  NOTE: Windows XP Professional and Windows Vista support is limited to managed console (web-based interface) and Management Station software (remote racadm CLI).

* Red Hat Enterprise Linux 4.5 WS, ES, and AS (x86_32 and x86_64).

* Red Hat Enterprise Linux 5 Update 2 (X86_32 and X86_64).

* SUSE(R) Linux Enterprise Server 9 with SP4 (x86_64).

* SUSE Linux Enterprise Server 10 with SP2 (x86_64) Gold.

==========
SUPPORTED WEB BROWSERS
==========

* Microsoft Internet Explorer(R) 6.0 (32-bit) with SP2 for Windows 2000, Windows XP and Windows 2003.

* Microsoft Internet Explorer 7.0 for Windows Vista, Windows 2003 and Windows 2008.

* Mozilla Firefox(R) 1.5 (32-bit) on SUSE Linux Enterprise Server 9 & 10 and Red Hat Enterprise Linux 4.5

* Mozilla Firefox 2.0 (32-bit) on SUSE Linux Enterprise Server 10.

==========
FIRMWARE VERSIONS
==========

* RAC Firmware Version: 1.40

==========
DISABLE LOCAL VIDEO
==========

* Baseboard Management Controller (BMC) firmware version 1.29 or higher

==========
POWER MONITORING STATISTICS, POST and OS PLAYBACK LOGS
==========

* Baseboard Management Controller (BMC) version should be flashed to the following minimum versions:

  * PowerEdge 1900 - v2.29
  * PowerEdge 1950 - v2.28
  * PowerEdge 2900 - v2.28
  * PowerEdge 2950 - v2.28
  * PowerEdge 2970 - v2.29
  * PowerEdge 6950 - v2.29
  * PowerEdge R300 - v2.34
  * PowerEdge R900 - v2.27
  * PowerEdge T300 - v2.34
  * PowerEdge T605 - v2.30
  * PowerEdge R805 - v2.33
  * POwerEdge R905 - v2.31

==========

CONSOLE REDIRECTION USING JAVA VIEWER
==========

* JRE version 1.6.0 or later needs to be installed on the management
  station.

##########
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.40)
##########
* Power Monitoring Statistics and Charts.

* POST and OS Playback Logs.

* Pin Only Two Factor Active Directory Authentication/Single Sign On.

* Console Redirection using Java Viewer.

* SMCLP Support for additional profiles.

##########
USER NOTES
##########

This section provides information to help enhance your experience with
the Dell Remote Access Controller 5.

==========
NOTES FOR THE DRAC 5 Firmware Version 1.40
==========

* Console redirection using Java plug-in does not work on a Linux
  management station. To work around this problem, do the following:
  1. Save the JRE installer (jre-6u3-linux-i586-rpm.bin) in the
     location of your choice.
  2. Extract the RPM and install JRE.
  3. Create a soft link to this JRE in the plug-ins folder of the
     browser. For example, if you have installed the JRE in the
     default location, create the soft link by navigating to the
     plug-ins folder of your Web browser. From this folder, run the
     following command:

     ln -s /usr/java/jre1.6.0_03/plugin/i386/ns7/libjavaplugin_oji.so

     NOTE: To verify if the JRE plug-in was installed, type
     about:plugins in the browser's address bar, click Go, and check
     the information that is displayed.
  4. Close the Web browser and try Console Redirection again.

* The Smart Card CRL feature is no longer applicable for the Active
  Directory Smart Card users. The CRL feature is now valid for Local
  Smart card users. To enable the CRL feature for the local smart card
  users to work properly, the appropriate Active Directory CA root
  certificate ( containing the Certificate Distribution Point URL )
  must be uploaded to the DRAC using the Active Directory
  Configuration page.

* SMART Card login and Single Sign-On functionality will not be

supported on Windows 2000 Management Station.

* For updating DRAC 5 firmware through the Web GUI, make sure that a valid .d5 image file and path are provided in the text box on the firmware update page.

* To use the feature to specify the Association Object Domain IP address/FQDN for Active Directory Authentication using extended schema, use the following racadm command :

racadm config -g cfgActiveDirectory -o cfgAODomain=<domain>: <ip/fqdn>

where <domain> is the domain where the Association Object is present and IP/FQDN is the IP or FQDN of the specific machine where the Association Object is present.

##########################################################################
MAC Address Assignment between LOM & DRAC
##########################################################################

* When a NIC is in “Shared between LAN on the Motherboard” (LOM) and DRAC," the DRAC firmware assigns a separate MAC address for LOM and the DRAC 5.

##########################################################################
CONFIGURING THE RAC CARD FOR FLASH RECOVER MODE
##########################################################################

1. Connect the RAC card to a TFTP server using a network cable to the system network or a cross-over cable to the host system.

2. Point the TFTP server root path to the folder containing the firmware update image "firmimg.d5".

3. Using the BIOS setup screen, configure the system serial mux such that the RAC card is connected internally to the external DB-9 serial port.

4. Install a NULL modem cable between the system DB-9 serial port and a client machine.

5. On the client machine open a terminal communications program like "HyperTerminal" or "Mini-Comm" using, [1] baudrate=115200, [2] bits=8, [3] parity=none, [4] flow control=none

6. Enter a carriage return. A "RAC Recover Mode" prompt should appear. If not then you may not be in recover mode. Recheck the serial mux and terminal settings.

7. View recover network settings
   RAC Recover> recover getniccfg

8. If needed, set static network settings (DHCP is NOT supported in recover)
   RAC Recover> recover setniccfg <IPaddress> <Subnetmask> <Gateway>

9. Verify the settings and connection by pinging the TFTP server.
   RAC Recover> recover ping <TFTP server IP>
   (If ping does not work you may need to enter recover racreset
   first).

10. Download and update the flash part.
   RAC Recover> recover fwupdate -g -a <TFTP server IP>

11. RAC card will now update and reboot on completion.

##########################################################################
CHANGE IN DEFAULT CONFIGURATION SETTINGS
##########################################################################

For Firmware Version 1.40: None

##########################################################################
KNOWN ISSUES FOR DRAC 5
##########################################################################

* When you use Internet Explorer version 6 SP2 or version 7 to log
  into the DRAC 5 Web GUI and the client is on a private network but
  without access to the Internet, you may experience a delay of up to
  30 seconds. To work around this issue, do the following:

  1. Disable the phishing filter.
  https://phishingfilter.microsoft.com/faq.aspx

  2. Disable CRL fetching:
    a. Click “Tools”-> “Options”-> “Advanced” [tab]-> “Security.”
    b. Clear “Check for publisher's certificate revocation.”

* Active Directory login will fail on DRAC 5 if the user certificate
  key length is 16K and DRAC 5 has more than 14 certificates per user,
  or if the user certificate key length is 1K and DRAC 5 has more than
  40 certificates per user. In order to remove older certificates,
  use the CERTUTIL tool. For more information, use the links below:

  The link below talks about an example of how to use CERTUTIL
  to delete the certificate.
  http://technet.microsoft.com/en-us/library/cc783979.aspx

  For the syntax, see the following link:
  http://technet.microsoft.com/en-us/library/cc772898.aspx

* Smart Card Login does not work with GemSAFE(TM) smart cards.

* When AC power is applied to the system but it is still powered down,
  the date and time in the DRAC 5 will be Jan 1, 1970. When the system
  is powered on, the DRAC 5 time is updated to the system time.
  Henceforth, DRAC5 syncs up with the system time every hour. Once in
  the OS, if the system time is changed, then in order to sync the
  DRAC 5 time with the system time immediately, please reboot the
  system.

* While uploading the kerberos key tab file to the DRAC 5 using racadm, please validate the file before uploading. Currently, there is no check performed for the validity of the key tab file.

* For Smart Card based authentication, currently, only Gem Alto cryptographic smart cards and compatible cryptographic smart card Service provider drivers are supported. Make sure that a supported smart card is used for authentication.

* For Smart card and single sign on authentication, DRAC5 does not support concurrent logins. If there is more than one user trying to login to DRAC5 at the same time using either single sign on or smart card Authentication, only one user will be authenticated. In this situation, try the login again to authenticate and login into DRAC 5.

* DRAC 5 currently does not support Windows 2008 Domain Controller as supported Active Directory configuration for smart card Active Directory authentication and single sign on Active Directory authentication. Make sure that the domain controllers in the Active Directory environment are either Windows 2003 or Windows 2000 Domain Controllers.

* User Configured Serial Console Redirection Key will only work with telnet/ssh. It will not work with any serial connection based terminal emulators like Hyperterminal, Putty or Minicom.

* For 64-bit Windows platforms, the DRAC5 Authentication plugin will not get installed properly if a 64-bit version of "Microsoft Visual C++ 2005 Redistributable Package" is deployed. Customers need to deploy the 32 bit version of "Microsoft Visual C++ 2005 Redistributable Package" for the plug-in to install and run properly.

* On a Windows Server 2003, you randomly receive the Stop 0x44 error with blue screen when peroforming DRAC5 DUP update. Apply the Microft Hot-fix as mentioned in http://support.microsoft.com/kb/942528 article.

* When Enhanced Security is enabled or installed in Windows(2003 or XP) for IE hardening, IE may not be able to parse the XML which may lead to DRAC GUI not working as desired. To fix this, download security fixes and Microsoft fixes provided in the Microsoft Website Microsoft XML Parser(MSXML) 3.0 SP5

* With Microsoft IE Enhanced Security Configuration, a pop-up message appears when trying to connect to any website using IE6, which resembles the following:

  "Microsoft Internet Explorer's Enhanced Security Configuration is currently enabled on your server. This enhanced level of security reduces the risk of attack from Web-based content that is not secure, but may also prevent web sites from displaying correctly and restrict access to network resources."

  This pop-up will have a checkbox "In the future do not show this message".

Select the check-box for the DRAC 5 login GUI to work properly on Microsoft Internet Explorer.

* When viewing the Web user interface on a Dell PowerEdge 1900 system that is configured with one NIC, the NIC Configuration page displays two NICs (NIC1 and NIC2). This behavior is normal. The PowerEdge 1900 system - and other PowerEdge systems that are configured with a single LOM - can be configured with NIC teaming. Shared and Teamed modes work independently on these systems.

* The allowed RACADM Serial Escape Key (cfgSerialConsoleQuitKey) values are as follows:

(a) ^ followed by any alphabetic (a-z, A-z)
(b) ^ followed by the listed special characters: [ ] \ ^ _

* The supported Console Redirection video refresh rates are:

- 720x400 [70 Hz]
- 640X480 [60, 72, 75, 85 Hz]
- 800X600 [60, 70, 72, 75, 85 Hz]
- 1024X768 [60, 70, 72, 75, 85 Hz]
- 1280X1024 [60 Hz]

Certain configurations of refresh rates may not work for Linux operating systems on the managed system. This may happen because the Linux operating systems allow a range of refresh rates instead of a fixed refresh rate.

* When you update the DRAC 5 firmware, the update resets the DRAC 5, detaches USB devices from the BUS, and disconnects remote Virtual Media. Before you perform a firmware update or RAC reset, it is recommended that you perform the following procedures:
- Ensure that Virtual Flash is unmounted or not in use by another user.
- Disconnect and unmount Virtual Media.

* When you access the DRAC 5 GUI through the Web browser, you are required to add the DRAC 5 IP address to the list of trusted domains if the IP address is missing from the list. When completed, click Refresh or relaunch the web browser to re-establish a connection to the DRAC 5 GUI.

* The DRAC 5 GUI is not supported on 64-bit Web browsers. If you open a 64-bit browser, access the "Console Redirection" page, and attempt to install the plug-in, the installation procedure fails. If this error was not acknowledged and you repeat this procedure, the "Console Redirection" page loads, even though the plug-in installation fails during your first attempt. This issue occurs because the Web browser stores the plug-in information in the profile directory even though the plug-in installation procedure failed. To fix this issue, install and run a supported 32-bit Web browser and log into the DRAC 5.

* If you are running Console Redirection on a Red Hat Enterprise Linux (version 4) client with a Simplified Chinese GUI, the viewer menu

and title may appear in random characters. This issue is caused by an incorrect encoding in the Red Hat Enterprise Linux (version 4) Simplified Chinese operating system. To fix this issue, access and modify the current encoding settings by performing the following steps:

1. Open a command terminal.
2. Type "locale" and press <Enter>.
   The following output appears.
   LANG=zh_CN.UTF-8
   LC_CTYPE="zh_CN.UTF-8"
   LC_NUMERIC="zh_CN.UTF-8"
   LC_TIME="zh_CN.UTF-8"
   LC_COLLATE="zh_CN.UTF-8"
   LC_MONETARY="zh_CN.UTF-8"
   LC_MESSAGES="zh_CN.UTF-8"
   LC_PAPER="zh_CN.UTF-8"
   LC_NAME="zh_CN.UTF-8"
   LC_ADDRESS="zh_CN.UTF-8"
   LC_TELEPHONE="zh_CN.UTF-8"
   LC_MEASUREMENT="zh_CN.UTF-8"
   LC_IDENTIFICATION="zh_CN.UTF-8"
   LC_ALL=
3. If the values include "zh_CN.UTF-8", no changes are required.
   If the values do not include "zh_CN.UTF-8", go to step 4.
4. Navigate to the “/etc/sysconfig/i18n” file.
5. In the file, apply the following changes:
   Current entry:
   LANG="zh_CN.GB18030"
   SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"

   Updated entry:
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
6. Log out and then login to the operating system.
7. Relaunch the DRAC 5.

When you switch from any other language to the Simplified Chinese language, ensure that this fix is still valid. If not, repeat the procedure. (53205)

* The Linux operating system mouse settings are used to control the mouse arrow in the DRAC 5 Console Redirection screen. If the user or the Linux operating system (Red Hat or Novell) changes the default mouse settings, there will be a mouse synchronization problem.

* Closing the DRAC 5 GUI from a Microsoft Internet Explorer using the close button ("x") on the top right corner of the browser may generate an application error. To fix this issue, download the latest Cumulative Security Update for Internet Explorer from the Microsoft Support website located at “support.microsoft.com.” See Microsoft Knowledge Base article KB835193 for more information.

* When using Microsoft Active Directory credentials to log into the DRAC 5 GUI, the GUI supports passwords with a maximum length of 256 characters. However, Active Directory supports passwords with a maximum length of 127 characters. For more information about Active

Directory password policies, see the Microsoft Technet website at "technet.microsoft.com."

* If you access DRAC 5 GUI using Internet Explorer and click "Save As" in one of the GUI pages, the browser may open the file within the Web browser and avoid prompting you to save the file to your system's hard drive. To resolve this issue, download the Cumulative Security Update for Internet Explorer located on the Microsoft Support website at “support.microsoft.com.”

* When you input a single character, the keyboard driver expects make (press) and break (release) key input within 200 milliseconds. If the keyboard driver does not receive the break key input within this time frame, the driver assumes that you are pressing and holding down the key. As a result, the driver simulates multiple keystrokes.

To work around this issue, perform one of the following procedures:
- Disable the keyboard character repeat feature.
- Modify the server settings by extending the repeat delay and minimizing the repeat rate.

To work around the multiple keystrokes problem, the user can disable the keyboard character repeat feature or change the repeat delay to longer and the repeat rate to slower on the server side.

* You may encounter virtual drive issues when copying large files to the DRAC 5 virtual flash. To avoid these issues, you should not attempt to copy large files from the local drive to the DRAC 5 virtual flash on systems running Windows or Linux operating systems. If you need to copy large files, you can create an image of the files to be copied and then use the GUI flash update to update the virtual flash.

If you receive an error message from the host operating system that the copy failed when copying large files to the DRAC 5 virtual flash from a local drive, then your DRAC 5 virtual devices (DVD/CD ROM, floppy, and flash) will be offline. In order to get your DRAC 5 virtual devices back online, you can detach and re-attach the virtual devices from the DRAC 5 GUI or CLI, or you can reboot the server. (67123)

* In Windows Vista if the Internet Explorer Protected Mode is "ON" then you will not be able to use any of the drives available on the Virtual Media page in the GUI to establish a Virtual Media session. This is due to additional security by the browser to prevent unwanted execution of code through the browser using elevated privileges. For more information, see the Microsoft document at:

http://download.microsoft.com/download/c/2/9/
c2935f83-1a10-4e4a-a137-c1db829637f5/WindowsVistaSecurityWP.doc

(109414)

* When trying to access the GUI after updating the DRAC 5 firmware from a previous version to the latest version, you may encounter the error: "The XML page cannot be displayed". To resolve this

issue, clear the browser cache and re-launch the browser to access the GUI.

* When running the racadm command "racadm getconfig -f <filename>" locally or remotely, the file will not get the values for the groups cfgIpmiPef and cfgStandardSchema.

* If there is a delay in loading or installing plug-ins on the DRAC 5 GUI using any browser, install the following Certificate Revocation List within the browser:

http://csc3-2004-crl.verisign.com/CSC3-2004.crl

* If a non-root user attempts to execute the remote CLI (racadm) commands on a Linux operating system with Racadm utility already installed, the error: "Command not found" is displayed. This issue is because the Racadm utility is available only to users with root privileges.
(113871)

* The browser's <Ctrl><N> functionality to open a new browser instance on the DRAC out-of-band (OOB) GUI is not supported. When using the Internet Explorer, if you open multiple instances of the DRAC OOB GUI on the same client (using <Ctrl><N> or any other method), a log out from one session will result in a log out of all the other GUI sessions. On Linux operating systems using the Firefox browser, if you open multiple instances of the DRAC OOB GUI on the same client (not necessarily by using <Ctrl><N>), a log out from any one session will result in log out of all the other GUI sessions. This is because all the browser instances share the same cookies.
(117539)

* The DRAC 5 OOB GUI intermittently may display "undefined" strings in the tool bar when using the Firefox browser. This occurs if the page loads prior to the strings being loaded by the browser's transformation engine. To avoid this issue, log out of the DRAC 5 and log back in.
(118618)

* If you are using Hyperterminal version 6.3 on Windows 2003 SP2 as a client to access serial port for serial communication, Hyperterminal may fail. (116875)

* Mozilla Firefox version 2.0.0.2 is not supported in this release. If you get a blank page when accessing DRAC 5 from the Firefox 2.0.0.2 browser, type the following full path to get to the DRAC 5 login page:

https://<drac_ip>//cgi-bin/webcgi/login

* If the DRAC is configured to register the DRAC Host Name with DNS using DHCP (cfgDNSRegisterRac object value to 0 and cfgNicUseDhcp object value to 1), you must configure the DHCP to have the "Dynamically update DNS A and PTR records for DHCP clients that do not request updates" option enabled and a minimum of Option 15 (DNS Domain Name) added to the specific DHCP scope.

Be aware of the following behaviors when configuring the DRAC:

-- If the DRAC is set up with "cfgDNSRegisterRac=0" and "cfgNicUseDhcp=1" with NO scope options added and the "Dynamically update DNS A and PTR records for DHCP clients that do not request updates" disabled, the DHCP database will display the host name of the DRAC correctly but the DDNS functionality will NOT work.

-- If the DRAC is set up with "cfgDNSRegisterRac=0" and "cfgNicUseDhcp=1" with NO scope options added and "Dynamically update DNS A and PTR records for DHCP clients that do not request updates" enabled, the DHCP database will display the host name of the DRAC correctly but the DDNS functionality will NOT work.

-- If the DRAC is set up with "cfgDNSRegisterRac=1" and "cfgNicUseDhcp=1" with NO scope options added and "Dynamically update DNS A and PTR records for DHCP clients that do not request updates" disabled, the DHCP database will NOT display the host name of the DRAC correctly but the DDNS functionality will work.

-- If the DRAC is setup with "cfgDNSRegisterRac=0" and "cfgNicUseDhcp=1" with scope option 15 added and "Dynamically update DNS A and PTR records for DHCP clients that do not request updates" disabled, the DHCP database will display the host name of the DRAC correctly but the DDNS functionality will NOT work.

-- If the DRAC is setup with "cfgDNSRegisterRac=0" and "cfgNicUseDhcp=1" with scope option 15 added and "Dynamically update DNS A and PTR records for DHCP clients that do not request updates" enabled, the DHCP database will display the host name of the DRAC correctly and the DDNS functionality will work.

* If you are using GemSAFE smart cards, you may get an incorrect PIN message even after entering the correct PIN for the smart card. (155784)

* Legal values for “cfgDNSRacName” are strings of up to 254 ASCII characters. At least one of the characters must be alphabetic. Characters are restricted to alphanumeric and '-'.

* The user password can consist of 16 characters if you configure it through the Remote Access Configuration Utility. However, if you configure the user password through the DRAC Web GUI, the password can consist of 20 characters. This is a known limitation of the Remote Access Configuration Utility (that you can access during the system POST).

* While authenticating to the DRAC 5 using Active Directory, the login may fail due to different time zone offsets on the DRAC card and the operating system. To enable DRAC to have the same time zone offset, use racadm to set “cfgRacTuneTimeZoneOffset” to the time zone offset as the operating system time. For more details, see the racadm User Guide on the Dell Support website at “support.dell.com.”

* Enabling remote console redirection from managed node using “racadm localConRedirDisable 0” command can return a failure status under some conditions. This error message is not correct and the actual command works correctly and enables the console redirection feature.

* When the servers with DRAC 5 have a power supply supporting PM-Bus, the voltage page on DRAC 5 shows the voltage reading of power supply as N/A.

* DRAC stops DHCP requests if the traffic is > 6000frames/sec with 512 size. DRAC stops responses for local racadm and other IPMI comm for > 9000Frames/sec.

##########################################################################
KNOWN ISSUES FOR DRAC 5 WITH FIRMWARE UPDATE
##########################################################################

* Network traffic may cause the firmware update to time-out. If the firmware download procedure exceeds 15 minutes, the DRAC 5 will time out, cancel the firmware download procedure, reset, and then return to normal operation. To work around this issue, transfer the firmware flash image to a local drive on the server. Using Console Redirection, connect to the remote system and install the firmware locally using local racadm.

##########################################################################
KNOWN ISSUES FOR DRAC 5 WITH DISABLING LOCAL VIDEO
##########################################################################

* If the video is turned OFF locally on the server, the LCD displays a message indicating the video is OFF. However, if the baseboard management controller (BMC) is reset or there is a BMC firmware update, the LCD message will not be displayed.

  The LCD "Video OFF" message will only be displayed if the Video is turned ON and turned OFF again.

##########################################################################
KNOWN ISSUES FOR DRAC 5 WITH VIRTUAL MEDIA
##########################################################################

* Virtual Media may not function properly on Windows operating system clients that are configured with Internet Explorer Enhanced Security. To resolve this issue, see your Microsoft operating system documentation or contact your administrator.

* If you use Virtual Media and the Windows 2000 operating system CD to install Windows 2000 with Service Pack 4, your system may momentarily lose its connection to the CD drive during the installation procedure, and the operating system may fail to install properly. To fix this issue, download "usbstor.sys" from the Microsoft Support website at "support.microsoft.com" and run the program only on systems that experience this issue. See Microsoft Knowledge Base article KB823086 for more information.

* If Virtual Flash is enabled and does not contain a valid image (for example the virtual flash contains a corrupted or random image), you may not be able to install Windows 2000/2003 locally or remotely. To fix this issue, install a valid image on Virtual Flash or disable Virtual Flash if it will not be used during the installation procedure.

* Installing network and chipset drivers on the server causes the Virtual Media connection to drop when configured in the Shared-NIC mode. Installing the network or chipset drivers causes the LOM to reset, which in turn causes network packets to time-out and the Virtual Media connection to time-out and drop. To work around this issue, copy the drivers from your virtual drive to the server's local hard drive. To prevent a dropped Virtual Media connection from interfering with your driver installation procedure, start the driver installation directly from the server.

* If you are installing the Windows operating system using the "Dell Systems Management Tools and Documentation" DVD and a slow network connection, the installation procedure may require an extended amount of time to access the DRAC 5 GUI due to network latency. While the installation window does not indicate the installation progress, the installation procedure is in progress.

* You may not be able to format the Virtual Flash with the Linux GUI. You can format Virtual Flash with the fdisk and mkfs commands.

* The new version of the Virtual Media plugin 2,1,0,14 is not getting updated automatically.
Do the following steps:
For IE 6 Browser:
IE Tools->Internet Options->General Tab ->Settings->view objects. Delete rac5vm control object and reload the Virtual media page to get the newer plugin.

For IE 7 Browser:
IE Tools->Manage Add-ons->Enable or Disable Add-ons->select Downloaded ActiveX Controls. Now delete the plug-in named rac5vm Control. Click OK and reload the virtual media page.

##########################################################################
FREQUENTLY ASKED QUESTIONS ON VIRTUAL MEDIA
##########################################################################

Q: I am viewing the contents of a floppy drive or USB memory key. If I try to establish a Virtual Media connection using the same drive, I receive a connection failure message and am asked to retry. Why?
A: Simultaneous access to Virtual Floppy drives is not allowed. Close the application used to view the drive contents before you attempt to virtualize the drive.

Q: How do I configure my virtual device as a bootable device?
A: On the managed system, access the BIOS Setup and navigate to the boot menu. Locate the virtual CD, Virtual Floppy, or Virtual Flash and change the device boot order as needed. For example, to boot

from a CD drive, configure the CD drive as the first drive in the boot order.

Q: What types of media can I boot from?
A: The DRAC 5 allows you to boot from the following bootable media:
- CDROM/DVD Data media
- ISO9660 image
- 1.44 Floppy disk or floppy image
- DRAC 5 embedded virtual flash
- A USB key that is recognized by the operating system as a removable disk
- A USB key image

Q: How can I make my USB key bootable?
A: Perform one of the following procedures:
1) Format your USB key with Windows 98 DOS using a Windows 98 startup disk.
   a) Boot your system from a Windows 98 startup disk.
   b) Copy the system files from the startup disk to your USB key.
      For example, from a DOS prompt, type:
      sys a: x: /s
      where "x" is the USB key that you want to make bootable.
2) Use the Dell boot utility. This utility is only compatible with Dell-branded USB keys. To download the utility, launch a supported Web browser, navigate to the Dell Support website at “support.dell.com,” and search for "R122672.exe."

Q: Do I need Administrator privileges to install the ActiveX plug-in?
A: You must have Administrator or Power User privileges on Windows systems to install the Virtual Media plug-in.

Q: What privileges do I need to install and use the Virtual Media plug-in on a Red Hat Linux management station?
A: You must have write privileges on the browsers directory tree to successfully install the Virtual Media plug-in.

Q: I cannot locate my Virtual Floppy device on a system running Red Hat Enterprise Linux or the SUSE Linux operating system. My Virtual Media is attached and I am connected to my remote floppy.
A: Some Linux versions do not automount the Virtual Floppy and the Virtual CDROM in a similar manner. In order to mount the Virtual Floppy, locate the device node that Linux assigns to the Virtual Floppy. Perform the following steps to correctly find and mount the Virtual Floppy:
1) Open a Linux command prompt and run the following command:
   grep "Virtual Floppy" /var/log/messages
2) Locate the last entry to that message and note the time.
3) At the Linux prompt, run the following command:
   grep "hh:mm:ss" /var/log/messages
   where hh:mm:ss is the time stamp of the message found in step 1.
4) Read the result of the grep command in step 3 and locate the device name given to the "Dell Virtual Floppy"
5) Ensure that you are attached and connected to the Virtual Floppy.
6) At the Linux prompt, run the following command:

mount /dev/sdx  /mnt/floppy
where "/dev/sdx" is the device name found in step 4 and
"/mnt/floppy" is the mount point.

Q: What file system types are supported on my Virtual Floppy or
Virtual Flash?
A: Your Virtual Floppy or Virtual Flash supports FAT16 or FAT32 file
systems.

Q: When I performed a firmware update remotely using the DRAC 5 GUI,
my virtual drives at the server were removed. Why?
A: Firmware updates cause the DRAC 5 to reset, drop the remote
connection, and unmount the virtual drives. The drives will
reappear when the DRAC 5 reset is complete.

Q: When enabling or disabling the Virtual Flash, I noticed that all
my virtual drives disappeared and then reappeared. Why?
A: Disabling or enabling the Virtual Flash causes a USB reset and
causes all virtual drives to detach from and then re-attach to
the USB bus.

Q: Sometimes I notice my Virtual Media client connection drop. Why?
A: When a network time-out occurs, the DRAC 5 firmware drops the
connection, disconnecting the link between the server and the
Virtual Drive. To reconnect to the Virtual Drive, use the Virtual
Media feature.

##########################################################################
KNOWN ISSUES FOR DOCUMENTATION
##########################################################################

This section provides additional information about known issues with
the DRAC 5 Firmware version 1.40 User's Guide.

* On page 278, there is insufficient information regarding power
monitoring charts and statistics.

* On page 268, information for POST and OS boot capture logs needs to
be updated.

* Chapter 7 requires various changes for the Smart Card Login page,
because the page design has changed for DRAC 5 FW 1.40.

* UG is missing information on the Specify Server option for Standard
Schema Active Directory.

* SMART Card help page has incorrect information regarding the Smart
Card CRL enable feature.

* On page 244 and 246, information on configuring two new platform
event filters, 'System Power Probe Failure' and 'System Power Probe
Warning' is missing.

* On Page 124, the following paragraph provides insufficient details
regarding the usage of specify server option:

"If you configure the Domain Controller under the 'Specify Server'

option on the DRAC and if the Association Object contains the user and RAC object on the same domain, the Active Directory login using Extended Schema will be successful. However, if either the user or the RAC object on the association is from a different domain, and if you provide only the domain controller information, the Active Directory login using Extended Schema will fail. In this case, you should configure the global catalog Option to be able to login"

In the above Paragraph, in addition to specifying the global catalog option (last sentence in the paragraph), we also have to specify the AO domain option for the login to be successful.

##########################################################################



September 2008