```
####################################################################
```

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 documentation CD.

```
####################################################################
```
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, and R805.

==
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 with Service Pack 4 (SP4).
 - Windows 2000 Server with SP4.
 - Windows 2000 Professional with SP4.

 NOTE: Windows 2000 Professional with SP4 support is limited to
 managed console (web-based interface) and Management Station
 software (remote racadm CLI).

* Microsoft(R) Windows Server(R) 2003 family

 - Windows Server 2003 R2 (Enterprise and Standard Editions) with SP2
   (32-bit).
 - Windows Server 2003 (Web Edition) with SP2 (32-bit).
 - Windows Server 2003 R2 Standard and Enterprise Edition with SP2
   (32-bit x86_64).
 - Windows Server 2003 Standard and Enterprise Editions x64 Editions
   with SP1.
 - Windows Small Business Server 2003 Standard and Premium Editions.
 - Windows Small Business Server 2003 with SP1.
 - Windows Storage Server 2003 R2 Express and Workgroup x64 Editions
   (x86_64).

* Windows XP Professional SP2

* Windows Vista(TM)

 NOTE: Windows XP Professional SP2 and Windows Vista support is
 limited to managed console (web-based interface) and Management
 Station software (remote racadm CLI).

 NOTE: Microsoft Windows Server 2008 is scheduled to be available in
 the first half of 2008. For the latest information, see
 http://www.microsoft.com/windowsserver2008/default.mspx.

* Red Hat(R) Enterprise Linux(R) WS, ES, and AS (version 4)
  (x86 and x86_64).

* Red Hat Enterprise Linux 5 (x86 and x86_64).

* SUSE(R) Linux Enterprise Server 9 with Update 3 (x86_64).

* SUSE Linux Enterprise Server 10 (x86_64) Gold.

==
SUPPORTED WEB BROWSERS
==

* Microsoft Internet Explorer 6.0 (32-bit) with SP1 for Windows 2000
  Server family.

* Microsoft Internet Explorer 6.0 (32-bit) with SP2 for Windows XP and
  Windows Server 2003 family.

* Microsoft Internet Explorer 7.0 for Windows Vista, Windows XP, and
  Windows Server 2003 family.

* Mozilla Firefox 1.5 (32-bit) on SUSE Linux (version 10) only.

* Mozilla Firefox 2.0 (32-bit).

==
FIRMWARE VERSIONS
==

* RAC Firmware Version: 1.30

==
DISABLE LOCAL VIDEO
==

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

##
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.30)
##

* Enables Smart Card logon that provides a higher level of security by
  implementing the two-factor authentication.

* Provides a single default Microsoft Active Directory® Secure Sockets
  Layer (SSL) certificate for the DRAC 5. The DRAC 5 will no longer
  carry a default Dell certificate.

* Provides advanced security options for the local DRAC administrator

* Provides advanced security options for the remote DRAC administrator

* Supports a new macro—<RightCtrl>+<ScrlLock><ScrlLock> key code
  sequence to initiate a crash dump of the Microsoft Windows operating
  system. For more information, see the Microsoft Knowledge Base
  article at: http://support.microsoft.com/kb/Q244139.

  NOTE: You must keep the <RightCtrl> key pressed during the
      Additional keystrokes.

* Supports an option to allow users to specify LDAP or Global Catalog
  servers to handle user authentication.

* Provides the ability to specify a list of LDAP servers and Global

Catalog servers.

* Removed support for SSL version 2.0.

* Power Optimization Sensor status information for systems that
  Support the PM-BUS.

* Provides support for the auto-attach virtual media. When this
  feature is enabled, DRAC 5 will automatically attach a virtual
  device to the system only when a device is virtualized (connected)
  on a supported client.

```
############################################################################
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 and a "RAC Recover Mode" prompt should
    appear. If not then you many not be in recover mode, or 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 serve.
    RAC Recover> recover ping <TFTP server IP>
    (If ping does not work you may need to enter recover racreset
    first).

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

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

##
KNOWN ISSUES FOR DRAC 5
##

* 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 reestablish 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.

* When viewing the Console Redirection online help, the second note under Console Redirection should state as follows:

  "The recommended display resolution on the management station (or client) is at least 1280 x 1024 pixels at 60 Hz with 128 colors. You cannot view the console in Full Screen Mode if your monitor resolution is less than this minimum."

* 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, 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 the all browser instances share the same cookies.
  (117539)

* The DRAC firmware version as displayed on the OMSA GUI firmware page
  is mistakenly reported as 1.14 instead of 1.20.

* The DRAC 5 OOB GUI Alert Management on Platform Event: "Automatic
  System Recovery" does not support these shutdown actions:
  Reboot System, Power Cycle System, and Power Off System. The online
  help for this page does not mention this.

* 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
     properly show the host name of the DRAC 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 properly show the
     host name of the DRAC 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 show 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 correctly show the
     host name of the DRAC 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 correctly show the
     host name of the DRAC and the DDNS functionality will work.

* If you are using GemSAFE(TM) 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 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 DRAC5 have a power supply supporting PM-Bus,
  the voltage page on DRAC5 shows the voltage reading of power supply
  as N/A.

* On VMware(R) ESX Server(R), DUP update fails with a error message "The DRAC
  update requires that virtual media be attached to perform the
  update. After attaching virtual media rerun the update to
  upgrade the DRAC firmware."
  To work around this issue, do the following:
  Attach virtual media (ensure that Virtual Flash is enabled)
  Bind any free raw character device to the Virtual Flash
  using the 'raw' command like following example:
  raw /dev/raw/raw1 /dev/sdc
  Where /dev/raw/raw1 is any raw device which is not already bound
  to any block device and /dev/sdc is the Virtual Flash device.
  You can find the list of raw devices already bound to a block
  device using the following command:
  raw –qa
  This command will list query all the raw device bindings.
  After this run the DUP update.

##
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.

* After updating firmware update to 1.30 from any previous release, it
  takes about 5 minutes before the DRAC is fully functional.

##
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 the 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
  PowerEdge Installation and Server Management" CD 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.

* When viewing the Virtual Media Configuration online help,
  note the following corrections in the Attributes section:

  - "Maximum Number of Sessions" should state:

    "Maximum Number of Sessions displays the maximum number of
    simultaneously active Virtual Media sessions."

  - "Number of Active Sessions" should state:

    "Displays the current number of active Virtual Media sessions"

  - "Virtual Media Port Number" should state:

    "Display and set the port number (in decimal) for Virtual Media
    connection. Valid numbers are unused DRAC 5 port numbers between
    0 and 65535. Default=3668."

  - "Virtual Media SSL Port Number" should state:

    "Display and set the Secure Socket Layer communications port
    number (in decimal). Valid numbers are unused DRAC 5 port numbers
    between 0 and 65535. Default=3669."

* 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.

##
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 OS 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 1.20 User's Guide.

* On page 56, the remote RACADM commands listed for the "Enabling the
  Serial/Telnet/SSh Console Remotely" procedure is incorrect. The
  correct remote RACADM commands are as follows:

  racadm -u <username> -p <password> -r <DRAC 5 IP address> config -g
  cfgSerial -o cfgSerialConsoleEnable 1

  racadm -u <username> -p <password> -r <DRAC 5 IP address> config -g
  cfgSerial -o cfgSerialTelnetEnable 1

  racadm -u <username> -p <password> -r <DRAC 5 IP address> config -g
  cfgSerial -o cfgSerialSshEnable 1

* On page 263, the default value listed for the cfgFloppyEmulation
  property is incorrect. The correct default value is 0.

* In Table 1-5 on pages 21-22, some of the supported operating systems
  listed in the table are incorrect:

  - Red Hat Enterprise Linux WS, ES, and AS (version 3)
    (x86 and x86_64) is not supported.
  - Red Hat Enterprise Linux WS, ES, and AS (version 4)
    (ia32 and x86_64) and Red Hat Enterprise Linux WS, ES, and AS
    (version 4) (x86 and x86_64) are the same operating systems. The
    correct listing should be Red Hat Enterprise Linux WS, ES, and
    AS (version 4) (x86 and x86_64).
  - SUSE Linux Enterprise Server 9 with Update 2 (x86_64) Gold
    is not supported. Only SUSE Linux Enterprise Server 9 with
    Update 3 (x86_64) Gold is supported.
  - Windows Server 2003 R2 (Web Edition) with SP2 (32-bit) is not
    supported. Only Windows Server 2003 (Web Edition) with SP2
    (32-bit) is supported

* In Table 1-6 on pages 22, some of the browser's supported operating
  systems listed in the table are incomplete. Please refer to the
  Supported Web Browsers section of this readme for the latest browser
  support list.

October 2007