

Intel® vPro™ Technology Use Case Reference Design

Enhanced Remote Repair with Drive Sharing

Revision 2.0

June, 2010

Document ID: 1040

Revision History

Revision	Revision History	Date
1.0.1	First release.	February 2010
2.0	Revisions for native read/write support for shared drive	June, 2010

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel, the Intel logo, Intel® AMT, and Intel® vPro™ are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2010 Intel Corporation. All rights reserved.

Contents

1	Preface	5
1.1	Document Scope	5
1.2	Intended Audience	5
1.3	Related Documentation and Software	5
2	Introduction	6
2.1	Example Usage Illustrated in This Document	6
2.2	Process Overview	7
3	Detailed Steps	8
3.1	Set Up the Console and Connect to the Managed Client Using SOL/IDER	8
3.2	Connect Using KVM Remote Control	11
3.3	Reboot the Managed Client to the Remote Linux* ISO	12
3.4	Remotely Access the Managed Client's Hard Drive	15
3.4.1	Mapping a Drive Using the Tools Menu in Windows Explorer	15
3.4.2	Mapping a Drive Using the net use Command	18
4	Building the ISO	19
4.1	Build System Requirements	19
4.2	Reference Links	19
5	Appendix A: Architectural Considerations for the Included ISO File	21
6	Appendix B: Remote Drive Share Error Messages	22
Figures		
Figure 1:	Connect and Control Panel, Connected to Selected Computer	9
Figure 2:	Remote Control Settings	10
Figure 3:	Serial-over-LAN Shows Connected	10
Figure 4:	Terminal Tool Redirection Menu	12
Figure 5:	The VNC* Viewer Plus IDE-Redirection Menu Icon	12
Figure 6:	Terminal Tool Information Panel at Bottom	13
Figure 7:	Remote Reboot to Redirect CD Menu	13
Figure 8:	The VNC Viewer Plus Power Menu Icon	14
Figure 9:	Remote Drive Sharing Main Menu	14
Figure 10:	Drive Share Information	16
Figure 11:	The Map Network Drive Dialog	16
Figure 12:	The Connect As Dialog	17
Figure 13:	SOL Window Showing net use Command Information	18

1 Preface

Intel® vPro™ technology gives the Information Technology (IT) professional the capability to remotely boot a managed client with Intel vPro technology to a remote ISO image file. The procedure described in this document boots a small Linux* OS on the remote managed client and then shares the entire contents of the client's hard drive on the local network. The client's shared hard drive can easily be accessed using a management console to map a network drive to the client's shared hard drive. This allows the IT professional to access files not usually shared when the OS is active, or to gain access to the client's file system in the event that the client's OS is corrupted.

1.1 Document Scope

This document does not include local language files.

The procedure in this document and its accompanying software are supported only on computers with Intel vPro technology. See section 2.1 for specific requirements.

1.2 Intended Audience

This document is intended for IT professionals who need out of band access to the hard drive data on a computer with Intel vPro technology. Readers should have a good working familiarity with Intel vPro Technology, including configuration and use of Intel AMT for out-of-band management. Readers should also be familiar with the basics of IT infrastructure, especially networked environments and their component technologies.

1.3 Related Documentation and Software

The download package for this Use Case Reference Design, including the Remote Drive Share software and supporting files referenced in this document, can be found at the following link:

<http://communities.intel.com/docs/DOC-4785>

Also of interest:

<http://communities.intel.com/docs/DOC-4910> (contains information on using RealVNC's VNC* Viewer Plus with KVM Remote Control)

2 Introduction

This Use Case Reference Design demonstrates how managed clients with Intel vPro technology can be remotely booted to a small Linux ISO in order to enable sharing of the hard drive for remote data access. This capability could be useful in remotely retrieving data from a system whose OS will not boot, or for remotely accessing system files not visible from within the OS.

The document provides a high-level summary of the process, a detailed step-by-step example, an overview of the included Linux ISO, and steps to rebuild the ISO. The detailed steps in this document are intended to be used as a reference or example, so that readers can adapt them to their own process tailored to their specific needs.

2.1 Example Usage Illustrated in This Document

This document focuses on sharing the hard drive of a managed client with Intel vPro technology and has the following requirements:

1. Managed Client(s) with Intel vPro technology, supporting SOL/IDER or KVM Remote Control:
 - Configured for use with Intel vPro technology
 - Wired network connection
 - No Software Disk Encryption - Software Disk Encrypted hard drives cannot currently be shared with Remote Drive Share
2. Management Console Application supporting Intel vPro technology's SOL/IDER feature
 - The document example uses Intel's Manageability Commander Tool

Other types of deployments, consoles, Intel AMT states, etc. are beyond the scope of this document.

2.2 Process Overview

The following table provides a high level overview of the remote client hard drive sharing and access process, to give you a general idea of what you will be doing in the step-by-step procedures in the remainder of the document. The steps in the overview table correspond to the major subsections of Chapter 3.



NOTE

As part of this process, system credential information (including a randomly generated user name and password) for the Managed Client is passed to the Management Console's SOL window, for use in mapping a shared drive to the client's hard drive. If the Managed Client has not been configured to use TLS or MTLS security for Serial over LAN (SOL) connections (for example, if the client was provisioned in SMB mode), this username and password will be passed as clear text. This is not the case when using KVM Remote Control, as KVM Remote Control does not pass information as clear text.

Description	The IT Professional ensures prerequisites are met and remotely accesses the Managed Client's hard drive.
Prerequisites	<ul style="list-style-type: none"> • SOL/IDER or KVM Remote Control must be enabled in Intel AMT on the Managed Client(s). • The Managed Client must be provisioned. • If using SOL/IDER to remotely connect to the client, a management console application capable of SOL/IDER functionality must be installed on a Management Console System. • If using KVM Remote Control to connect, a KVM Remote Control console such as RealVNC's VNC* Viewer Plus must be installed on the Management Console System • The Linux* ISO file included with this Use Case Reference Design (rds.iso) must be copied to a file location that is accessible by the Management Console System (for example, the Management Console System's hard drive).
Process flow	<ol style="list-style-type: none"> 1. Identify the Managed Client whose hard drive you need to access. 2. From the Management Console, establish a SOL/IDER session or KVM Remote Control session with the Managed Client. 3. Remotely reboot the Managed Client to the specified Linux ISO and automatically create a network share of the client's hard drive. 4. Map a drive to the Managed Client's remotely shared hard drive partition(s).
Expected outcome	The Managed Client's hard drive is accessible from the Management Console System via your Intranet.

3 Detailed Steps

This chapter and its subsections provide detailed, step-by-step procedures to remotely share your Managed Client's hard drive on your Intranet so that you can access it Out of Band (OOB) from a Management Console system. Section 3.1 applies to using SOL/IDER to connect to the managed client. Section 3.2 applies to using KVM Remote Control to connect to the managed client. Other sections are applicable to either connection method, with any exceptions noted in the actual steps.

3.1 Set Up the Console and Connect to the Managed Client Using SOL/IDER

Follow the steps in this section if you are planning to use SOL/IDER to connect to your managed client.



NOTE

The procedure described below for using SOL/IDER uses Intel's Manageability Commander Tool, included in the Intel AMT SDK available at the link below, as the management console application. However, the concept should be applicable to other management console applications. The intent is to provide a detailed example of how the remote OOB hard drive access process can be accomplished with the Manageability Commander Tool, which readers can then apply to their specific IT environment and whatever management console application they are using.

The Manageability Commander Tool is available here:

<http://software.intel.com/en-us/articles/download-the-latest-version-of-manageability-developer-tool-kit/>

If you wish to use Intel's Manageability Commander Tool, install the Manager Developer Toolkit and ensure that you select to install the Manageability Commander Tool during the installation process. Otherwise, adapt the following procedures to your particular management console application.

The first step is to set up your Management Console Application to perform SOL/IDER and connect to the Managed Client. The acronym SOL stands for Serial over LAN and IDER stands for IDE redirection. The SOL session connects the Management Console Application to a terminal on the Managed Client. IDER directs the Managed Client to boot from a location other than the internal hard drive. Follow the steps below to connect to an Intel vPro technology based client using the Manageability Commander Tool. The steps below assume that the Manageability Commander Tool has been installed on the Management Console System.

1. On the Management Console System, launch the Manageability Commander Tool by clicking **Start -> All Programs -> Manageability Toolkit -> Manageability Commander Tool**.
2. In the tool, select **File -> Add -> Add Intel AMT Computer....** Enter the requested information in the Add Intel AMT Computer window.
3. In the left-hand pane, right-click on the computer you just added and select **Connect** from the pop-up menu. The **Connect** button in the right-hand pane changes briefly to **Abort Connect**, then after a minute or so it changes again to **Disconnect** once the connection is established.

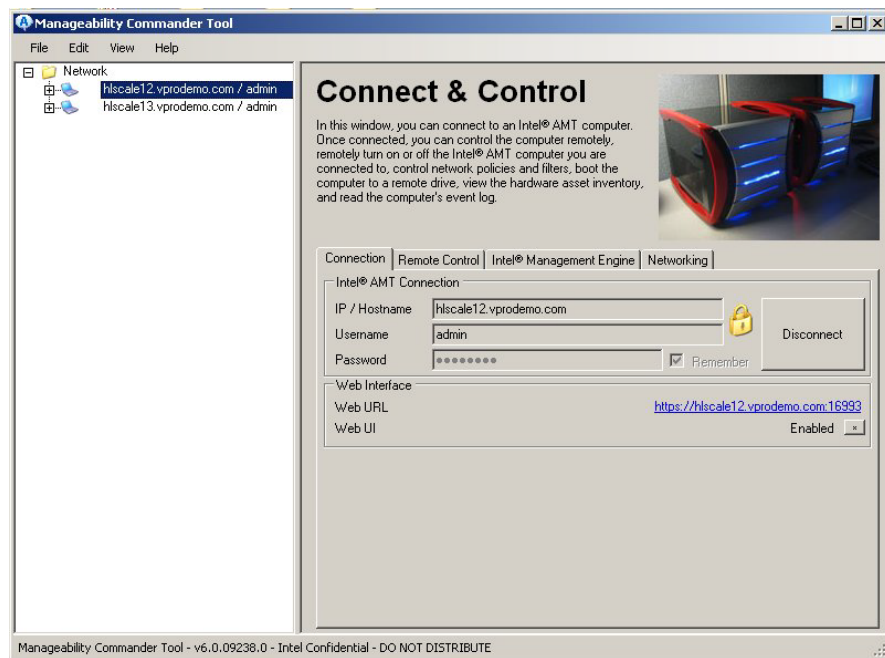


Figure 1: Connect and Control Panel, Connected to Selected Computer

- In the Connect and Control panel, click the Remote Control tab. Verify that **Serial over LAN**, **IDE Redirect**, and **Redirection Port** are **Enabled**, as shown below. If any of the items are **Disabled**, click on the * button to enable the item. If the item is still not enabled, you may need to enable the item in Intel AMT by rebooting the Managed Client and entering the Intel® Manageability Engine BIOS Extension (Intel® MEBX) to enable the item manually. See Intel MEBX documentation for details.

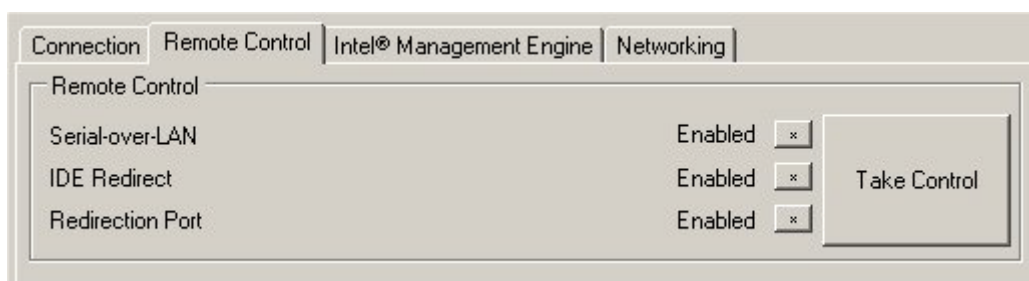


Figure 2: Remote Control Settings

- On the Remote Control tab, click the **Take Control** button. Verify that the Manageability Terminal Window opens (as shown below) and that **Serial-over-LAN** is shown as **Connected**.

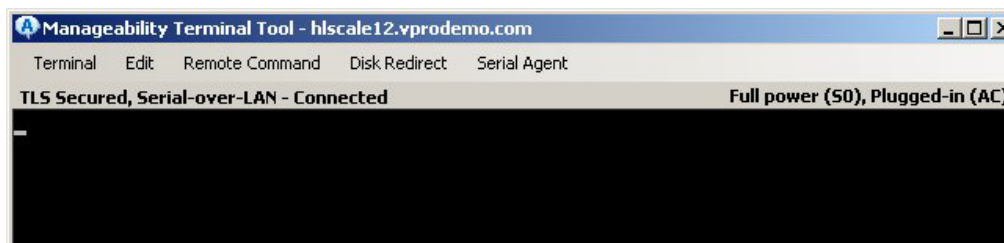


Figure 3: Serial-over-LAN Shows Connected

You are now ready to initiate a SOL/IDER session with the Managed Client. Using the SOL/IDER session, you will reboot the Managed Client to the specified Linux ISO, which will enable you to share the Managed Client's hard drive on your Intranet and access the hard drive's data from your Management Console System.



NOTES

- If the Managed Client has been fully powered off, and it has a hard drive password enabled, instruct the client's owner to power it up and enter the hard drive password locally, then allow the client to continue booting to the point of failure (for example, the OS will not boot). At that point, you are ready to remotely reboot the Managed Client from the Management Console as described in the following section.*

- *Software Disk Encrypted hard drives cannot be shared with Remote Drive Share.*

3.2 Connect Using KVM Remote Control

Follow the steps below:

1. Click **Start -> Programs -> RealVNC -> VNC Viewer Plus**.
2. On the New Connection screen, set the following (the order is important):
 - For **Connection Mode** select **Intel AMT KVM**.
 - For **AMT Server** enter the IP address of the remote PC.
 - For **Encryption** select **None**.
3. Click **Connect**.
4. Enter your Intel AMT credentials. The document example uses **admin**, **P@sswOrd**.
Note: these credentials must have administrative rights to Intel AMT.
5. Click **OK**.
6. The KVM Remote Control session starts. Depending on how KVM Remote Control was configured you will either be prompted for user consent or be at the remote client's desktop. If the latter, you are done with these steps. Proceed to the conclusion paragraphs after these steps.
 - For more details on User Consent, refer to the UCRD document *Quick KVM Remote Control for Brand New 2010 Intel® Core™ vPro™ Processor Based PCs*, section 6, available at the link below.
<http://communities.intel.com/docs/DOC-4795>
7. On the Managed Client screen a sprite is displayed with a consent code. Enter this code into the viewer window on the console. **Note:** Do not use the number pad.
 Once the code is entered you will have remote keyboard, video, and mouse control of the remote client.

At this point it is almost as if you are sitting in front of the remote client. You can do many of the same things allowed by a VNC or RDP server such as walk the user through a set of steps, type in the user's recovery passphrase, or install/uninstall software for the user. This reference design will only cover benefits of a KVM Remote Control session with Intel AMT over the current in band services mentioned above.

3.3 Reboot the Managed Client to the Remote Linux* ISO

The next step is to remotely reboot the Managed Client to the remote Linux ISO (included with this Use Case Reference Design). In the following steps we will use the Management Console Application to remotely reboot the Managed Client to a specified Linux ISO file.

1. If you have not already done so, copy the Linux ISO file **rds.iso** (included in this Use Case Reference Design's download .zip file) to a location that is accessible to the Management Console System, such as the Management Console System's hard drive.
2. In the Manageability Terminal Tool, select **Disk Redirect** from the menu bar at top, then select **Change Target CD-ROM > Redirect to Image File**, as shown in Figure 4 below. If using KVM Remote Control, click the IDE-Redirection menu icon, shown in Figure 5 below.



NOTE

Older versions of the Manageability Commander Tool may require you to specify a floppy image as well. If your version requires this, you can specify *rds.iso* as the floppy image, but keep in mind that it is the CD ROM image that will be used for the redirected boot.

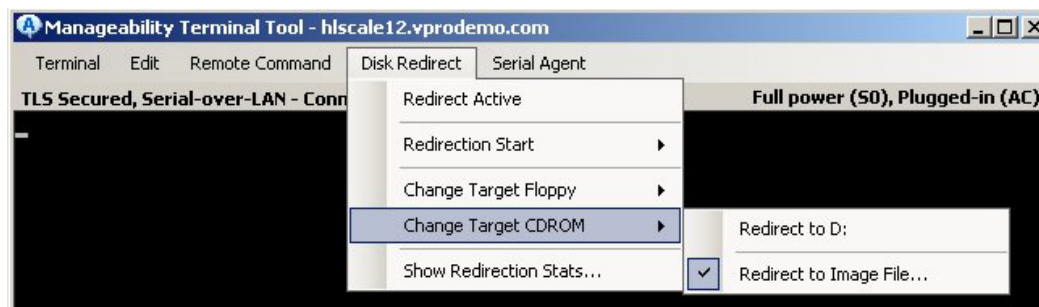


Figure 4: Terminal Tool Redirection Menu



Figure 5: The VNC* Viewer Plus IDE-Redirection Menu Icon

3. Browse to the location where you copied the rds.iso file. Select the desired file and click **Open**. In Commander, the filename appears in the **CDROM** value displayed at bottom (as shown in Figure 6 below). For KVM Remote Control, be sure to click **Share** in the VNC Viewer Plus IDE-Redirection window (to share the ISO with the remote client), then skip to step 7.
4. In Commander, from the menu bar, select **Disk Redirect > Redirect Active**. The message **IDE Redirect Active** appears at bottom (as shown below).



Figure 6: Terminal Tool Information Panel at Bottom

5. From the menu bar, select **Remote Command > Remote Reboot to Redirect CD**.



NOTE

If the Managed Client has not been configured to use TLS or MTLS security for SOL connections (for example, if the client was provisioned in SMB mode), be aware that a generated system name, user name, and password for the Managed Client will be passed as clear text to the Management Console's SOL window upon completing this step. This is not the case when using KVM Remote Control, as KVM Remote Control does not pass information as clear text.

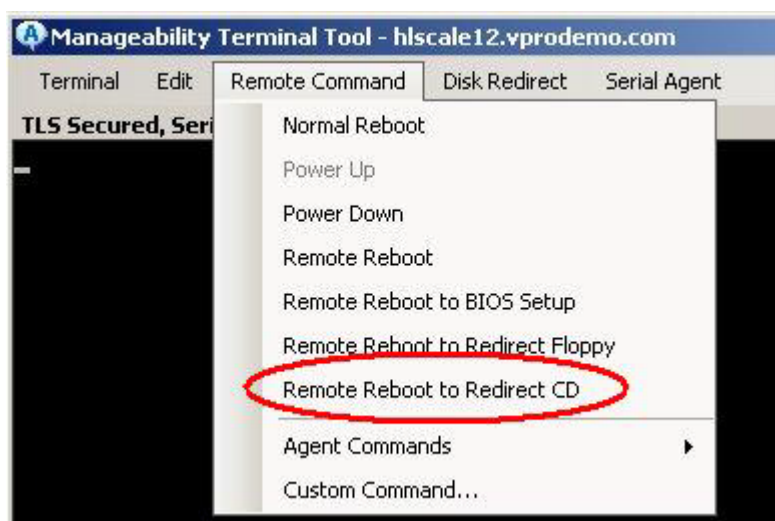


Figure 7: Remote Reboot to Redirect CD Menu

6. Click **Yes** in the **Reboot Computer to Remoted CDROM?** dialog. Wait for the Managed Client to finish rebooting and for the RDS main screen, which contains credential information for the Managed Client, to appear in the SOL window (shown in Figure 9 below).
7. For KVM Remote Control, in the session window, click **Start > Shutdown > Restart** (on the remote client) to restart the client and boot it to the ISO image you previously shared. If Windows is not running on the remote client, then click the **Power** button as shown in Figure 8 below:



Figure 8: The VNC Viewer Plus Power Menu Icon

All hard drive partitions found on the Managed Client are listed using Linux device nomenclature. Boot drives are designated by an asterisk (*). Figure 9 shows the Commander SOL/IDER window, but the same content should appear in the KVM Remote Control session window.

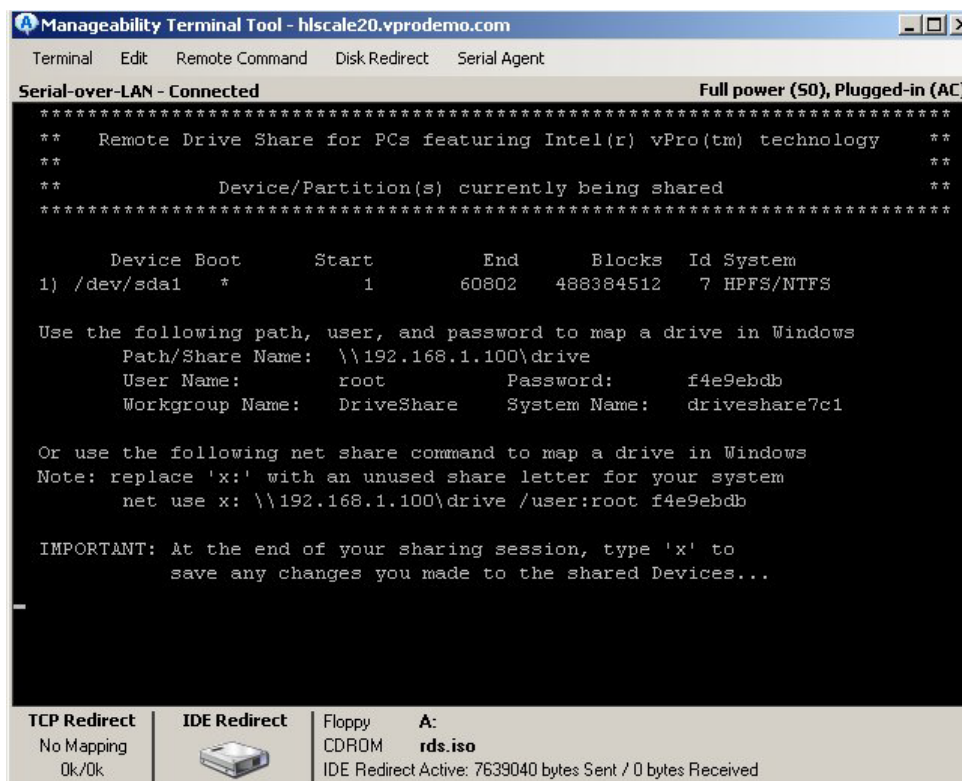


Figure 9: Remote Drive Sharing Main Menu

**NOTE**

The system name and user password are randomly generated by the Remote Drive Share software.

At this point you are ready to access the Managed Client's hard drive from the Management Console System. Proceed to the next section.

3.4 Remotely Access the Managed Client's Hard Drive

Now that you have shared the Managed Client's hard drive partitions on your Intranet, you are ready to access them from the Management Console System. As the text in the SOL window states, this can be done using either of two methods:

- Use the provided path, user name, and password to map a drive on the Management Console System to one of the listed drives, using the **Tools > Map Network Drive** menu command in Windows Explorer (note that you must use the **Connect using a different user name** option, as described below).
- Use the provided `net use` command to map a drive on the Management Console System to one of the listed drives from the command prompt or a command file.

These methods are explained in further detail below.

**NOTE**

Regardless of whether the Managed Client is set up to use TLS/MTLS, the Windows Explorer mapped drive connection to the Managed Client's hard drive will NOT be encrypted.

3.4.1 Mapping a Drive Using the Tools Menu in Windows Explorer

Follow the steps below:

1. On the Management Console System, launch Windows Explorer and click **Tools > Map Network Drive** from the Windows Explorer menu bar.

2. Choose an unused drive letter to map to. In the **Folder** field, enter the share information from the SOL window. For the example SOL window shown in Figure 10 below, you would enter `\\192.168.1.101\drive` in the Folder field. Do NOT click **Finish** at this point.

```
Device Boot      Start         End      Blocks   Id System
1) /dev/sda1      1           20       160618+  de Unknown
2) /dev/sda2     21          282       2097152   7 HPFS/NTFS
3) /dev/sda3      *        282       19458     154031104  7 HPFS/NTFS

Use the following path, user, and password to map a drive in Windows
Path/Share Name:  \\192.168.1.101\drive
User Name:        root          Password:         b36fcc94
Workgroup Name:    MapDrive      System Name:      mapdrive551

Or use the following net share command to map a drive in Windows
Note: replace 'x:' with an unused share letter for your system
net use x: \\192.168.1.101\drive /user:root b36fcc94
```

Figure 10: Drive Share Information

3. Deselect **Reconnect at Logon**.
4. Click **Connect using a different user name** as shown in Figure 11 below.

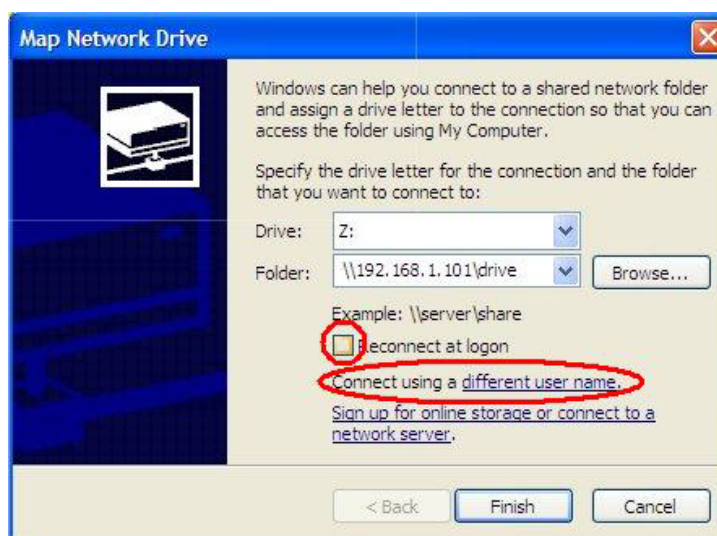


Figure 11: The Map Network Drive Dialog

5. In the Connect As dialog, enter the user name and password from the SOL window (in Figure 10, this is `root` and `b36fcc94`), as shown in Figure 12 below.

**NOTE**

The user name and password will be passed to the client unencrypted.

6. Click **OK**.



Figure 12: The Connect As Dialog

7. In the Map Network Drive dialog, click **Finish**.

At this point, you should have a drive (Z: in this example) mapped to the Managed Client's hard drive, and should be able to access it from the Management Console like any other shared network drive. The partitions listed in the SOL window (i.e., `sda1`, `sda2`, and `sda3` in the example) appear as subfolders under the root of the "drive" share.

When you are done accessing the Managed Client's hard drive, press the "X" key while in the SOL or KVM Remote Control window so that the client stops sharing its hard drive on the Intranet and any changes you made get written out to the client's hard drive.

3.4.2 Mapping a Drive Using the net use Command

As an alternative to using the Tools menu in Windows Explorer to map a drive to the shared partitions of the Managed Client's hard drive, you can use the net use command shown in the SOL window (see Figure 13 below).

```

      Device Boot      Start         End      Blocks   Id System
  1)  /dev/sda1             1          20       160618+  de Unknown
  2)  /dev/sda2            21         282       2097152    7 HPFS/NTFS
  3)  /dev/sda3            *        282       19458      154031104    7 HPFS/NTFS

Use the following path, user, and password to map a drive in Windows
  Path/Share Name:  \\192.168.1.101\drive
  User Name:        root           Password:          b36fcc94
  Workgroup Name:   MapDrive       System Name:       mapdrive551

Or use the following net share command to map a drive in Windows
Note: replace 'x:' with an unused share letter for your system
  net use x: \\192.168.1.101\drive /user:root b36fcc94

```

Figure 13: SOL Window Showing net use Command Information

1. On the Management Console System, open a command prompt window and enter the net use command shown in the SOL window (be sure to specify an unused drive letter). For example, to map the Management Console System's "X:" drive (assuming X: is not already mapped) to the Managed Client's hard drive, you would enter the following command:

```
net use x: \\192.168.1.101\drive /user:root b36fcc94
```
2. Navigate to the Management Console System's X: drive (either in Windows or at the command prompt) to access the Managed Client's hard drive. The listed drive partitions (sda1, sda2, and sda3 in this example) are shown as subfolders under the root of X:.

When you are done accessing the Managed Client's hard drive, press the "X" key while in the SOL or KVM Remote Control window so that the client stops sharing its hard drive on the Intranet and any changes you made get written out to the client's hard drive.

4 Building the ISO

The components needed to rebuild the drive share ISO file have been included in this Use Case Reference Design download package.

4.1 Build System Requirements

The ISO must be built using a Linux system. We have included the necessary components and files to rebuild the included ISO file `rds.iso` or `rds_kvm.iso`.

Prepare your system as follows:

1. Install Ubuntu 9.1 on an x86 based system.
2. Verify that your system is connected to the Internet.
3. Launch a terminal and type the following commands to install required packages:
 - `sudo apt-get install build-essential`
 - `sudo apt-get install zlib1g-dev`
 - `sudo apt-get install libncurses5-dev`
 - `sudo apt-get install upx`
 - `sudo apt-get install nasm`

4.2 Reference Links

The following components were included in the Use Case Reference Design download package and do NOT need to be downloaded. They are included here for your reference. If you need to update one of these packages, you will need to edit the makefile to include the new .tar file name.

- Busybox 1.16.2:
<http://www.busybox.net/downloads/busybox-1.16.2.tar.bz2>
- Linux Kernel 2.6.33.2:
<http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.33.2.tar.bz2>
- SAMBA 3.4.1:
<http://samba.org/samba/ftp/stable/samba-3.4.1.tar.gz>
- Syslinux 3.84:
<http://www.kernel.org/pub/linux/utils/boot/syslinux/syslinux-3.84.tar.gz>
- Zlib 1.2.3:
<http://www.zlib.net/zlib-1.2.3.tar.gz>
- NTFS-3G 2010.3.6:
<http://tuxera.com/opensource/ntfs-3g-2010.3.6.tgz>

4.3 Building the ISO

Perform the following steps to build the ISO file rds.iso.

1. Extract the rds.tar.gz file onto your Linux system in any directory. The .tar is extracted to create a directory structure with the root directory "rds".



NOTE

Do not extract the .tar file on a Windows system and open the .txt files. Windows adds control characters to the files which will corrupt the build process.

2. Open a terminal session and navigate to the rds directory.
3. Type "sudo make" and wait for the rds.iso file to build.

Upon build completion, the rds.iso file is built, which reads and writes NTFS, FAT, and FAT 32 partitions using a SOL/IDER connection or KVM Remote Control connection.

5 Appendix A: Architectural Considerations for the Included ISO File

The remote share ISO was developed to be as small as possible in order to facilitate quick SOL/IDER sessions. The Managed Client must transfer the entire ISO to memory over the network before booting. The small size was made possible by only including components in the Linux ISO that were necessary for remote share functionality.

The major components are:

- Linux Kernel – Provides core OS features. Compiled with minimal driver and module support
- Samba – SMB file sharing support. Configured with minimal options.
- Busybox – Shell support and drive mounting. Configured with default configuration options.
- NTFS-3g –NTFS read-write mount support.

6 Appendix B: Remote Drive Share Error Messages

```
*****
** Remote Drive Share for PCs featuring Intel(r) vPro(tm) technology **
**
** A remote serial connection was not found on this system. **
** Remote Drive Share requires this connection and will now halt. **
*****
```

This message is only displayed on the client screen. It will appear if the system being booted is not an Intel vPro technology based system or Intel AMT is not enabled on the system. One possible reason for this message to be displayed is if the rds.iso image has been burned to a CD and then used to boot a system that does not have Intel vPro technology. If you establish a SOL/IDER connection to an Intel vPro technology based client and then boot the client with rds.iso, this message should not be displayed.

```
*****
** Remote Drive Share for PCs featuring Intel(r) vPro(tm) technology **
**
** An appropriate Intel network adapter was not found on this system. **
** Remote Drive Share requires this adapter and will now halt. **
*****
```

This message is displayed on both the client screen and the SOL terminal. It will be displayed if the client system does not have an Intel LAN adapter installed. If the client system is an Intel vPro technology based system, this message should never be displayed.

However, it might be displayed if the managed client has a non Intel LAN adapter installed or if the managed client has been booted with a CD of the rds.iso image and does not have an Intel LAN adapter. However, in that case the previous message would be displayed and Remote Drive Share would likely exit before displaying this message.

```
*****
**   Remote Drive Share for PCs featuring Intel(r) vPro(tm) technology   **
**                                                                    **
**       No available Device/Partitions were found on this system.       **
**   Remote Drive Share requires an available device and will now halt.   **
*****
```

This message is displayed on both the client screen and the SOL terminal. This message occurs if there are no SATA drives installed in the system. It also might occur if the hard drive has completely failed or lost power and is no longer recognized by the client system.

```
*****
**   Remote Drive Share for PCs featuring Intel(r) vPro(tm) technology   **
**                                                                    **
**       A working DHCP server was not found on this network.           **
**   Remote Drive Share requires a valid IP address and will now halt.   **
*****
```

This message is displayed on both the client screen and the SOL terminal. This message can occur if there is no DHCP server for Remote Drive Share to use. This should be a rare case since the SOL/IDER connection also needs the DHCP server to be running. This message might be displayed in the event that a system without a network connection was booted from a CD with rds.iso.