Remote Re-Imaging of Client PCs

**Industry**
Remote re-imaging of client PCs across industries

**Business Challenge**
Saving costs by easily and remotely re-imaging client PCs

**Technology Solution**
Intel® vPro™ technology and Intel® Active Management Technology

**Enterprise Hardware Platform**
Intel® Core® vPro™ processor family
BUSINESS CHALLENGE

An intractable problem for an IT group is how to inexpensively maintain distant clients. While clients are healthy and communicating with the network, there are many traditional remote administration solutions. But what if a machine is not healthy—for example, if it has either a blue screen of death (BSOD) or is not turned on?

Intel® Advanced Management Technology (Intel® AMT) addresses those problems and more, providing a true full-feature remote administration solution for every Intel AMT-equipped client, regardless of initial state or geography. This enables tremendous savings on operating expenses by reducing the need for expensive client visits from professionally-trained service desk technicians. You can administer a global fleet of clients from a single service desk location, which you can correctly size for the fleet’s service level agreement.

This solution blueprint describes how to restore a remote client to service with a full reimage of the operating system with user personalization—no matter what the initial state of the client. Because a client’s initial state is unimportant, the solution even allows you to make a recover using an earlier, unsuccessful reimage task. The only requirement is for the client to be electrically attached to the network with power available.

As we describe the solution, we are basing it on a prototypical environment. We have made every effort to select an environment that represents actual networks worldwide. However, the incredible variety of possible networks inevitably means this solution will not precisely fit every network without adaptations. In most cases, the need for adaptation will be minimal.

TECHNOLOGY

ENTERPRISE PLATFORM

CONSOLE

You can integrate the solution described in this blueprint with many full-feature service consoles such as Symantec Altiris® or Microsoft System Center®, or enjoy the basic functionality using free tools from Intel and third parties in conjunction with the client’s own Intel AMT-hosted management interface. There are no hard dependencies on specific management suites or components.

Whichever console method you use, your service technician must have valid Intel AMT credentials for:

- IDEr and IDE redirection on the Intel AMT client
- SOL and serial-over-LAN on the Intel AMT client
- Remote control and KVM Remote Control of the Intel AMT client
CLIENTS
The manufacturer, model, and even physical execution of the client (i.e., notebook, desktop, or other form factor) are unimportant provided that the client is a network-attached, Intel AMT-activated system.

Each client being managed requires:

- **Intel AMT** version 6.0 or greater, activated. (Intel AMT version and connection type can be determined and verified remotely.)
- **Client must use Intel's integrated graphics** (i.e., the graphics solution provided by the Intel chipset, not a third-party add-in graphics card or solution. Intel integrated graphics are necessary for KVM access to the client). (This may be verified remotely.)
- **Windows* 7.** This solution blueprint describes the process to reimage a client with a Microsoft Windows 7 operating system. The underlying methods do not preclude reimagining clients with other operating systems, but the solution blueprint’s scope is limited to Windows 7.
- **Non-TLS* and Digest* credentials.** (Kerberos* credentials are also supported but not described in this solution blueprint.)
- **Physical network connection** (i.e., an active Ethernet connection to the client’s Ethernet port).
- **Enough power to support the duration of the activity,** if provided by a battery. (This can be verified remotely.)
- **Other requirements**, such as a local copy of the restore image, may be beneficial but are not required.
- **Network infrastructure.**

To administer a remote client, it must, of course, be attached to a network and accessible from the management console. The actual connection is unimportant (e.g., Fast Ethernet, Gigabit Ethernet, or wireless), as is the data path between the console and client, as long as basic network connectivity is provided. Machines on local and distant LAN segments attached by tunnels, or any combination of physical media not limited to Ethernet, DSL, fiber, etc., are acceptable.

The network between the client and console is insensitive to latency and typical packet losses. Most networks will be suitable without modification. However, the network must be transparent for TCP/IP protocol ports:

- **80 (HTTP, optional).** Used for Web User interface for direct client queries.
- **443 (HTTPS, optional).** Used for Web User Interface for direct client queries with SSL security.
- **5900 (VNC/KVM).** Used for extending client user-interface comprising keyboard, video, mouse to the management console or machine.
- **9971, (HELLO, reconfigurable).** Sent by an Intel AMT client’s OS resident service to announce presence to certain management consoles.
- **16992 (Intel AMT, non-TLS).** Used by the Intel Management Engine, ME, to communicate with the console without TLS security.
- **16993 (Intel AMT, with TLS).** Used by the Intel ME to communicate with the console with TLS security.
- **16994 (Intel AMT for SOL-IDER).** Used by the Intel ME for SOL and IDER activities using TLS security.
- **16995 (Intel AMT for SOL-IDER).** Used by the Intel ME for SOL and IDER activities without TLS security.
- **56666 (SOL-IDER).** Used by serial-over-LAN and IDE redirect communications.

Other considerations:
- **ARP:** Used over the local LAN subnet by the management engine to discover the local network.
- **ICMP:** Intel AMT implementations use ICMP for maximum transmission unit (MTU — i.e., maximum packet size) discovery and it is important that this succeeds in networks with constrained MTU segments such as over DSL, through VPNs, or other tunnels. Otherwise, networks comprising such segments will suffer packet losses, which may not be recovered. ICMP is also necessary for intermediate network nodes to report a dropped packet if, for example, it is corrupted. Without ICMP, transparency packets used by Intel AMT may be silently dropped in the network and end-to-end Intel AMT communication may be erratic or even completely blocked.

Furthermore, certain infrastructure configuration and components are either required or advisable for trouble-free and predictable operation. These include:
- **A common name-space (domain)** used throughout the network (workarounds available).
- **A unique name space** not used elsewhere in the private or public network (workarounds available).
- **Microsoft Active Directory** is required for larger networks to simplify the administration of per-client and per-user configuration and personalization data. While individual or small numbers of clients may be administered without Active Directory, it quickly becomes burdensome to perform client operations as the number of clients increases. Client fleets that would benefit from Active Directory likely already have the infrastructure in place.
- **A DNS or DDNS infrastructure** if DHCP is used so that individual client machines can be unambiguously identified on the managed network.
- **A DHCP server** supporting options 66 and 67 is required where reimaging using Microsoft’s Windows Deployment Services is performed. (This issues a pre-boot execution environment, PXE, information for the client to locate the image server, and a bootable image file).

**SOLUTION OVERVIEW**

**BENEFITS OVER OTHER METHODS**

Reimaging is the repair of last resort. Traditionally, reimaging has required the service technician and the affected machine to be brought together, either by the technician visiting the client or the user bringing the client machine to the service desk. Both these are, of course, expensive and, in a distributed organization, time-consuming. An alternative remote imaging method has long been sought.

One solution in widespread use in large organizations is a PXE boot to a network hosted image, which then invokes a network reinstall of the machine. Though these methods can be mostly hands-off and designed to execute without further interaction, the user must first be coached on how to invoke the correct PXE boot, the network reinstall infrastructure must be present, and the appropriate OS licensing must be in place. Furthermore, after the reinstall, the user must manually reinstall applications and restore any data that was previously backed up or archived. All this does not lend itself to a successful and timely return to work by employees, who might be
unmotivated or lack the skills to follow complex verbal instructions. At the very least, it requires some on-site and hands-on activity which likely mandates that such reinstallations occur during working hours. Typically, a day’s work is lost to the reinstall activity.

Another method is the most primitive of all. A physical optical disk is presented to the affected client and the machine is manually reimaged with all the close supervision and data entry that requires. Again, even if such an install media is available, the reinstall operation consumes a day’s work and the user is deprived the machine for the duration.

Earlier Intel AMT solutions used IDE redirection (IDEr) to mount a remote operating system installation disk or reinstallation image. That method is more vulnerable to network problems and can be slow. A successful first-time reimage is less likely.

All those alternate methods are inferior in execution to the Intel AMT methods described herein.

SOLUTION VALUE

The cost advantages of remote reimaging come from three factors:

1. **Fewer client visits.** Performing a task demands fewer man-hours and lower capital costs for transporting equipment to the client’s location.

2. **Less down time.** More efficient repairs allow the user to resume full productivity much sooner than with other methods.

3. **Shared resources.** By letting more users share central resources, resources can be sized appropriately for the enterprise’s service level agreement or expectations. Fewer expensive, highly trained professionals can maintain a distributed fleet of clients and the organization can be flatter, with centralized, co-located, and empowered service technicians.

Your actual savings depend on the degree to which you implement these three factors and on how the new solution differs from your current model.

SOLUTION ARCHITECTURE

The solution deployed in your network may follow this solution blueprint precisely or, depending on network constraints, be edited to improve performance, better utilize the network, or better conform to your enterprise’s policies.
PHYSICAL IMPLEMENTATION

SEQUENCE OVERVIEW

1. **Detection.** An error condition is detected either by automated client query routine, a user call for assistance, or a remote call for help trigger initiated by the user.

2. **Diagnosis.** The user and machine are identified and a trouble ticket is created if necessary. The system is queried to determine capabilities including Intel vPro technology and the behavior of the system confirmed or identified.

3. **Repair identified.** The system diagnosis triggers a decision to reimage the client and the method, variations on method, and timing are decided. The appropriate reimaging image is identified from a library of prepared images.

4. **Repair initiated.** The repair (re-image) request is transferred to the service desk, which initiates a remote reimage activity at the agreed time (perhaps immediately).

5. **Repair executed.** An IDE redirect (IDEr) is begun on the affected client, which is first rebooted or powered on so that it is in a known receptive state. The client then loads a small recovery OS image provided by the console into memory, which is then booted. The small recovery image then repartitions and reformats the affected mass storage device. Which storage devices and partitions are affected can be selected according to criteria decided in advance. For example, if a drive is fully repartitioned and reformatted, it’s possible to make sure the new layout incorporates a recovery partition which will facilitate any future recovery activities. Next, a connection is made to the image repository, which might be attached to the WAN, the LAN, or even a recovery volume on the client itself. Finally, the flat image file either transfers from a network location to the client’s usual operating system volume or initiates an unattended install from the install media represented by the network connected install media or image. This provides a higher-level remote management capability to the service desk, including KVM access to the affected machine, and thus the ability to manipulate the freshly installed client image. (Note: There are variations on this core stage.)

6. **Machine restored to service.** The reimaged client is personalized with the user’s identity and configuration, and (optionally) populated with the user’s archived or backed-up data. This personalization may be implemented by the service desk technician using the Intel AMT KVM capabilities, or by the user, perhaps with the service desk technician’s guidance.

7. **Repair concluded.** Finally, the user is notified that the system is repaired. After the user signs off, the trouble ticket is marked for follow-up survey and/or closed.
For more information on enterprise IT solutions, contact your Intel representative or visit the Intel IT Center.