Remote Power Management of Client PCs

Industry
IT security management across industries

Business Challenge
Saving power and costs by remotely managing the power state of client PCs

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

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

There's much debate over how much an organization can save on power by having an enterprise-wide strategy for monitoring the power state of client machines. For example, how much credible savings do technologies such as Enhanced Intel SpeedStep® Technology provide? What about OS-level features such as automatic hibernation and sleep? One thing is certain: a running machine consumes more energy than a sleeping or hibernated machine, and a turned-off machine consumes less. The real issue comes down to the best way to manage client machines if they are unpredictably asleep, hibernated, or even turned off.

Intel® vPro™ technology with Intel® Advanced Management Technology (Intel® AMT) has always provided a way to power remote client computers on or off as easily as if their power button were accessible to the service technician. This solution blueprint explains how to extend that capability to include graceful shutdowns to power states other than off, and how to create alarm clock events that run on Intel AMT itself, which you can use to ensure machines are powered on in preparation for scheduled maintenance events. It also discusses a tool to automatically schedule alarm clock events using the management console.

This helps ensure that idle machines can spend more of their time in an off, hibernated, or sleeping power state without affecting IT's ability to effectively manage and administer the entire fleet of machines. The result is a green solution that provides clear cost savings through both reduced power consumption and effective out-of-hours fleet management.

TECHNOLOGY

ENTERPRISE PLATFORM

CONSOLE

It is easy to integrate power management into Microsoft's Windows PowerShell® scripts that are available to virtually any client management console or tool, or using free Intel and third-party tools in conjunction with the client's own Intel AMT hosted management interface. There are no hard dependencies on specific management suites or components.

A service technician must have valid credentials for using Intel AMT's remote control features.

CLIENTS

The manufacturer, model, or even physical execution of the client (notebook, desktop, or other form factor) is unimportant provided that the client is a network-attached Intel AMT-activated system. In fact, the solution is sophisticated enough to differentiate between different manufacturers and platforms and affect only the appropriate power state transitions for a particular machine.
Each client being managed must satisfy these requirements:

- **Intel AMT must be activated.** The information in this solution blueprint expects Intel AMT v6.0 or later, but does not require any functionality not provided in earlier Intel AMT versions.
- **This solution blueprint describes the process to manage a client with a Microsoft Windows* 7 operating system.** The underlying methods do not preclude managing clients with other operating systems, but our scope is limited to Windows 7.
- **Each client must have Microsoft .NET* 4 framework** installed and certain executables and dynamic link libraries (DLLs) provided by Intel installed to the same directory.
- **Non-Transport Layer Security (TLS) and digest credentials** must be available. (Kerberos* credentials are also supported but not described here).
- **There must be a physical network connection** (i.e., an active Ethernet* connection to the client's Ethernet port).
- **Power must be sufficient** for the duration of the activity, if provided by a battery. (This can be verified remotely.)

**NETWORK INFRASTRUCTURE**

To administer a remote client, you must, of course, attach it to the private network (i.e., not via a public network such as the public Internet). It must also be accessible from the management console. The actual connection (e.g., Fast Ethernet*, Gigabit Ethernet*, or wireless) is unimportant, as is the data path between the console and client, provided that basic network connectivity is available. 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, it is required that the network 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 (Intel® ME) to communicate with the console without TLS security.
- **16993 (Intel AMT, with LTS).** 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 are:

- **Address Resolution Protocol (ARP):** Used over the local LAN subnet by Intel ME to discover the local network.
- **Internet Control Message Protocol (ICMP):** Intel AMT implementations use ICMP for maximum transmission unit (MTU—i.e., maximum packet size) discovery. It is important that this succeeds in
networks with constrained MTU segments such as over DSL or 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.

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 will benefit from Active Directory likely already have Active Directory infrastructure in place.
- **A DNS or DDNS infrastructure.** If DHCP is used, this enables individual client machines to be unambiguously identified on the managed network.

### SOLUTION OVERVIEW

### BENEFITS OVER OTHER METHODS

#### WAKE METHODS

The system wake timer can trigger a wake from the system’s sleep state, but that method does not allow a system to be awakened from the off or hibernation states.

Using a wake-on-LAN packet requires the machine to be individually targeted, and unless further activity is initiated with two minutes, the system will resume the previous state.

None of the other solutions includes the capability to automatically schedule and wake a machine in preparation for previously-scheduled, console-administered maintenance tasks.

#### SHUTDOWN METHODS

Automatically shutting down a fleet of machines after a defined period of idleness, or at a predefined date or time, is an effective way to save power. However, it does not in itself allow the sleeping machines to be awakened for maintenance during idle hours.

The basic Intel AMT power on/off events, which can be triggered from either the management console or the basic Web management interface, provide for graceful power on, but will cause a hard and abrupt power-off event akin to the power button being held. Any unsaved work or other tasks in execution will be immediately and crudely terminated.

In contrast, the Intel AMT Green Power Solution allows any or all machines in a fleet to be gracefully power-transitioned on demand or according to some predefined or automated schedule to maximize user and maintenance effectiveness.
SOLUTION VALUE
Remote power management saves money in three ways:

1. **Saving power** by not running an idle machine, including all the ancillary power-saving benefits of reduced air conditioning loads, increased product life, and improved reliability/availability of each machine.

2. **Maintaining machines** while they are otherwise idle (e.g., overnight) without any prep work such as ensuring that targeted machines are powered on. (Prep work may not successfully reach all machines intended for maintenance.)

3. **Centralized management** that lets you automatically maintain a large, distributed fleet of machines from a single service location, with economies of scale and centralization.

Your actual savings will depend on how you implement these three factors, as well as on your local power costs and pricing schedules and on how much your new management set-up differs from your old one.

SOLUTION ARCHITECTURE
The solution deployed in an actual network may follow this solution blueprint precisely or, depending on the operating constraints of your network, be edited to improve performance, make better use of the network, or better conform to your enterprise’s policies.

The solution is a set of executables and DLLs positioned on each client using existing methods, perhaps including management via Intel AMT-enabled methods.

*PowerMgmt.exe* lets you schedule future wake events in the Intel AMT timer so that the system can be set to automatically wake from any state. You can also use it to trigger graceful shutdowns, which are implemented using the separate *Turnoff.exe* executable. A third executable, *exec_SCCM.exe*, integrates with Microsoft’s Configuration Manager* and discovers when future management events are scheduled. It then uses knowledge of the machine manufacturer and type, knowledge of whether the service event requires that particular machine to be on, and, if necessary, uses the *PowerMgmt.exe* executable to program appropriate wake events in the Intel AMT timer(s).

Remote power-on events are communicated and initiated by traditional Intel AMT methods. You can use additional executables to cause graceful shutdowns and automatically schedule appropriate wakes from any machine state, not just sleep or hibernate.

MORE INFORMATION
For more information on enterprise IT solutions, contact your Intel representative or visit the [Intel IT Center](https://www.intel.com/).