Integrated Lights-Out technology: enhancing the manageability of ProLiant servers

technology brief, 2nd edition

Abstract

Integrated Lights-Out is an autonomous management subsystem that resides in a host server to manage it remotely through any server state: initial power-on testing, before the operating system (OS) is loaded, while the OS is functional, and even if there is an OS failure. In effect, Integrated Lights-Out is an autonomous computer within a computer. The Integrated Lights-Out Advanced functionality provides an administrator with comprehensive management technologies such as a Graphical Remote Console to view the host server console at any time, with any OS, in essentially any graphics mode. Customers using Microsoft® Windows® Terminal Services can optionally leverage a high performance software-based remote console while still maintaining availability of the hardware-based console. Integrated Lights-Out provides a virtual power button to power up or down the server, virtual media functions to upgrade firmware or deploy an operating system remotely and a virtual serial port to access a server console program. Integrated Lights-Out Advanced also supports the use of directory services to enhance security and provide scalability in enterprises that use large numbers of management processors.

Introduction

As companies globalize and industry-standard servers proliferate, it is no longer practical to administer servers locally. Remote management is becoming critical, even in corporate data centers, to meet increasing demands for IT efficiency and responsiveness. Integrated Lights-Out is an HP innovation that integrates industry-leading Lights-Out functionality and basic system management capabilities on selected ProLiant platforms. HP first introduced Lights-Out capabilities for remote server management in 2000 and continues to develop and expand the functionality of the technology. In fact, Lights-Out is an enabling technology for the HP Adaptive Enterprise.[1]

The HP Integrated Lights-Out management processor provides 24-hour, remote browser access to select ProLiant DL and BL servers through a seamless, hardware-based remote console. Integrated Lights-Out (iLO) is an autonomous management subsystem that resides on the system board of a host server. It operates out of band, so it is always active with full functionality, regardless of the state of the operating system (OS) or the host server. By means of iLO, system administrators can manage ProLiant servers remotely through their entire life cycle (initial deployment, operation, and redeployment). They can apply software and firmware updates over the network, diagnose OS or server problems remotely, take preemptive action, and respond quickly to downtime events to increase uptime and reduce the loss of business revenue.

This paper will identify technologies that HP implemented in iLO to provide both Standard and Advanced functionality, will explain how the device works, and will indicate its practical applications and value for IT organizations. This paper is written with the assumption that readers have basic knowledge of system administration in a networked environment.

Integrated Lights-Out architecture

Integrated Lights-Out is an autonomous management system consisting of two major components:

- Sophisticated firmware that can provide either of two levels of functionality—Standard or Advanced
- An application-specific integrated circuit (ASIC) that resides on the system

[1] For more information about the HP Adaptive Enterprise, see http://h71028.www7.hp.com/enterprise/cache/6842-0-0-0-121.aspx

Firmware

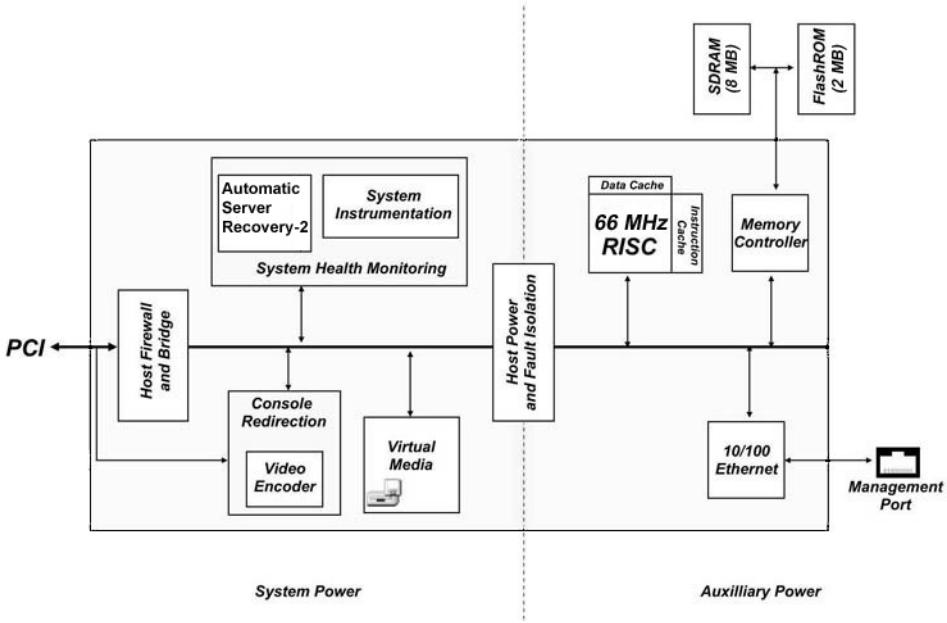
Integrated Lights-Out Standard functionality includes remote console access when the OS is in text mode; basic system management functions such as the ability to power on and off the host server remotely, update the iLO firmware, and access SNMP alerts; and access to server diagnostics such as the Integrated Management Log and server status.

Integrated Lights-Out Advanced functionality can be licensed with the optional HP ProLiant Essentials Integrated Lights-Out Advanced Pack. All ProLiant BL p-Class server blades[2] ship with the Advanced functionality enabled. Advanced functionality offers sophisticated virtual administration features for full control of servers in dynamic data center and remote locations. This includes a graphical remote console for servers with a graphical OS, integration with Windows Terminal Services for enhanced graphical performance while the OS is operating, virtual media support to use standard floppy and CD media anywhere on the network, and directory services support to simplify management of multiple iLO devices.

Hardware

The 32-bit, PCI-based iLO ASIC includes its own 66-MHz RISC processor core with separate instruction and data caches, memory controller, 8 MB of SDRAM, 2 MB of Flash ROM, and a 10/100 Ethernet controller (Figure 1). For video support, it uses the video chip embedded in the host server.

Figure 1. Block diagram of the iLO ASIC functions



The iLO management processor obtains its power through a separate connection to the auxiliary power plane of the server. Even if the host server is powered down, the essential Lights-Out management functions are still available. As long as the server is connected to a power source, the iLO ASIC can power itself up and remain fully functional. If the server provides redundant power

[2] Information about the ProLiant BL p-Class Server blade family is available from http://h18004.www1.hp.com/products/servers/platforms/index-bl.html

supplies, then iLO will use redundant power and will continue operation in the event of a power supply failure.

The iLO management processor contains several important logic blocks designed to monitor and control the host server.

System health monitoring

The system health monitoring logic monitors hot-plug fans, power supplies, environmental sensors, and various chipset components. It also implements Automatic Server Recovery-2, which reboots the server automatically after recoverable faults.

Console redirection

The console redirection logic enables the hardware-based remote console functions. It monitors the PCI bus for video activity, captures the video information, and then encodes and compresses text-based information before transmitting it to the management console. This process allows iLO to provide secure and fast remote console operations.

Virtual media

Through the virtual media logic, iLO provides a virtual USB floppy drive and virtual USB CD-ROM drive that can augment existing storage peripherals in the host server. Because iLO contains all the necessary USB hardware and firmware, the host OS recognizes the remotely connected virtual floppy or virtual CD-ROM exactly as it would a physical drive plugged into a USB port on the server.

Host firewall and bridge

The host firewall and bridge logic enables the embedded processor to control the flow of information between the host server and the management console. It protects against unauthorized access through the system PCI interface and shields sensitive information that may be stored in memory or firmware.

Host power and fault isolation

The host power and fault Isolation logic provides robustness to the iLO design. It essentially splits the ASIC into two separate areas, one operating under normal host system power and the embedded processor subsystem that operates under auxiliary power (see Figure 1). The host power and fault isolation logic monitors the host system for any unexpected behavior such as a system power fault or PCI bus fault. If a fault occurs, the embedded processor subsystem is notified of the fault, and it continues to operate normally on auxiliary power, providing key functions such as web browser access, alerting, and access to event logs.

The iLO power and fault isolation logic allows either the embedded processor subsystem or the host system to reset independently of the other. Therefore, the embedded processor subsystem is resilient across server resets and provides administrators seamless access to the server. Conversely, an administrator can upgrade the firmware on iLO without resetting or affecting the host server in any way.

Integrated Lights-Out technologies

Using the Lights-Out technologies of the remote console, virtual media, virtual power, and virtual serial port, system administrators can control iLO-managed servers as if they were sitting right in front of them. The iLO firmware innovations include the ability to scale management of iLO devices easily through directory services and provide enhanced remote console performance through Terminal Services. The iLO processor makes possible true headless operation of the ProLiant BL p-Class family of servers: It provides an intelligent communication channel to support the modular infrastructure of the blades. Finally, the iLO hardware and firmware incorporate security in multiple layers of functionality to ensure that servers are not compromised by remote access.

Remote console

The remote console is one of the most powerful technologies within iLO, because it provides system administrators with access to the managed server at any time. Since it is hardware-based, the remote console is independent of the state of the OS and can be available even before the OS is installed on the host server. The remote console is always available, allowing administrators to watch the entire boot process remotely. System administrators can use iLO Standard to view the managed server if the server is running in text mode. By activating the iLO Advanced option, administrators can view the managed server when it is running a graphical OS.

The iLO hardware captures three essential components for the managed (host) server: the keyboard input to the console, mouse input to the console, and the video output. When an administrator activates the remote console on the management workstation, iLO sends to the host server all the keyboard and mouse input received from the remote console applet.

For video capture, the iLO processor operates in one of two modes, based on whether the OS is in text mode or graphics mode. In text mode, the console redirection logic (see Figure 1) encodes the text character and attributes, compresses the code for that character, and redirects the text-based information from the host server console to the remote console applet on the management workstation. The encoder "packetizes" the information to reduce processing of text-based information.

In graphics mode, the console redirection logic works with the embedded firmware to direct the graphics-based information to the remote console applet. It uses the bitmap image of the host output from the graphical frame buffer. To reduce processing for graphics, iLO divides the host server screen image into blocks, calculates the hash value[3] of each block, and then continually scans the blocks to detect changes in the image. When it detects changes, it transmits only those changes to the remote console applet—not the entire image.

This provides the administrator with full text and graphical mode video, keyboard, and mouse access through a standard web browser. Since this functionality is hardware based and OS independent, it uses no host-server processor cycles and requires no special drivers or emulation software for the operating system.

Graphic mode support

The iLO processor supports all graphics modes—from legacy EGA and VGA modes such as 16- or 256-color, up to 32-bit, true-color settings. This is important, for example, in setup and OS installation programs that commonly use 16- and 256-color graphics modes. Because of this unique ability, an administrator can always see the server console and is not restricted to a limited set of video modes.

Furthermore, iLO gives excellent color fidelity, which is especially noticeable in 16- and 256-color legacy modes. The iLO processor tracks the color palette in use by the video controller on the system, and interprets the remote console colors to closely match that of the actual host server console. The improved color fidelity allows administrators to perform actions using the accustomed host console, without the distraction of unfamiliar color schemes.

Terminal Services

Beginning with iLO firmware version 1.50, the iLO device can leverage the OS functionality of Windows Terminal Services[4] to significantly increase the responsiveness of the graphical remote console. Terminal Services complements the technology within iLO by providing a software-based remote console while the host OS is functioning normally. If the host OS is not functioning normally, the iLO device can revert to the hardware-based console at any time. This gives customers the

[3] A hash function transforms a string of characters into a fixed-length numeric value or "key" that represents the original string. The hash is substantially smaller than the text itself. The hash is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

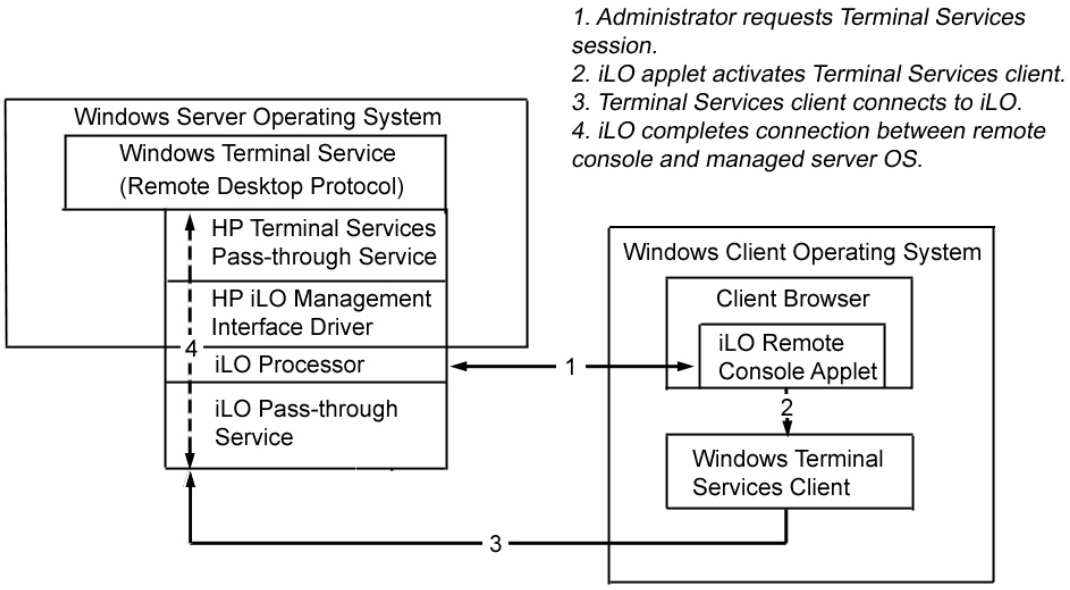
[4] Terminal Services is available with the Windows 2000 Server and later Microsoft Windows operating systems.

performance of an OS-based, graphical remote console (using Terminal Services in console mode) with the assurance that the hardware-based iLO remote console is available at all times. The Terminal Services capability is an expansion of the iLO graphical remote console technology; therefore, it is part of the iLO Advanced feature set.

The iLO processor takes advantage of the Terminal Services application by the use of the iLO pass-through service (HPLOPTS.EXE) and version 1.50 of the iLO firmware, which can access the Windows Terminal Services Remote Desktop Protocol. As shown in Figure 2, these software blocks sit underneath the Windows Server OS on the host. A Windows Terminal Services application resides on the client computer. System administrators can use either a manual or automatic method to open a Terminal Services connection from the iLO web browser to the host server. When the administrator requests a Terminal Services connection, the iLO remote console applet activates the Terminal Services client application, which connects to iLO on the host server. The iLO device passes all the Terminal Services traffic to the managed server and completes the connection between the iLO browser and the Windows OS.

Because Terminal Services is OS-based, it has the primitives that tell the OS how to open a window, the size and color of the window, and so on. Therefore, the Terminal Services application transmits only small amounts of information across the network, which improves the graphical remote console performance significantly in most cases.

Figure 2. Architectural diagram showing iLO with Terminal Services



The requirements to use the Terminal Services pass-through include:

- iLO Advanced 1.50 firmware or later with the pass-through service enabled
- Windows .NET 1.1 framework installed on the host OS
- iLO Management Interface Driver
- HP Terminal Services pass-through service installed on the host OS

Port security

To enhance security, administrators can configure iLO to encrypt remote console sessions and configure the remote console port to meet corporate security requirements. The iLO processor uses128-bit RC4 encryption[5] to encrypt remote console information. The 128-bit encryption provides security without requiring excessive processing overhead. Administrators can enable or disable this capability in the iLO configuration web pages.

Whenever a user requests a remote console session from the web browser client, the remote console applet initiates and opens the remote console port (port 23) of iLO in the host server. The iLO processor automatically disables the remote console port when the remote console session has ended. This default configuration (called auto-enable) enhances security by allowing only remote console sessions to connect to port 23, blocking any other connection attempts.

Finally, administrators can change the default port for the remote console if they need to designate a different port for security or other reasons.

Virtual media

Virtual media support, part of the iLO Advanced feature set, provides administrators with a virtual floppy disk drive and a virtual CD drive that connect through the network to the managed server, just as if they were physically connected. The virtual media device can be a physical floppy or CD drive on the management workstation, or it can be an image file stored on a local disk drive or network drive. Booting from the iLO virtual floppy or CD allows administrators to upgrade the host system ROM, upgrade device drivers, deploy an OS from network drives, create an emergency repair diskette, and perform disaster recovery of failed operating systems, among other tasks.

The iLO device uses a client-server model to perform the virtual media functions. The iLO device streams the virtual media data across a live network connection between the remote management console and the host server. The virtual media Java™ applet provides data to iLO as it requests it.

The iLO management processor contains a complete USB device controller that is viewed by the host OS as if it were a physical USB device that has been plugged into the server. Under the control of iLO firmware, a virtual USB device can be remotely "inserted" into the host server. When the virtual media is inserted, an OS that is USB-aware loads the standard USB mass storage device driver that is part of the server OS. Because iLO uses these built-in USB drivers, the iLO virtual media devices are available to host operating systems that support USB, without any additional HP drivers running on the server.[6] Additionally, the system BIOS of the host server is extended to support USB virtual devices. As a result of the BIOS extensions and the OS support, the iLO virtual media is available "end-to-end"—in a pre-boot environment, through OS loading, and while the OS is operational.

Virtual power

Using a supported browser interface, a system administrator can use iLO to remotely operate the power button of a host server, just as if he were pushing the physical power button. Virtual power support allows the user to power on, power off, and power cycle the host.

Like other aspects of iLO, the virtual power feature is independent of the OS and will work regardless of the state of the OS. However, it can leverage OS-supported power features, if available. For example, with operating systems that are ACPI-compliant such as Windows 2000, the "Momentary

---

[5] RC4 encryption was developed by RSA Data Security, Inc. It is an encryption technique that essentially takes a random number and performs a Boolean XOR operation with the original data to produce the encrypted data. For more information see the RSA website at http://www.rsasecurity.com/.

[6] Different operating systems provide varying levels of USB support, which can affect the iLO virtual media functions. See the iLO User Guide at http://h18004.www1.hp.com/products/servers/management/ilo/documentation.html for additional information.

Press" of the virtual power button will initiate a graceful shutdown of the OS before turning off the power. An administrator may observe the shutdown process through the remote console window.

Some operating systems can establish power policies whereby the server can only be shutdown through the OS or by pressing the power button for an extended time. The virtual power feature of iLO allows the administrator to override such a host power policy and force a server shutdown if needed.

Virtual serial port

Some operating systems, such as Windows Server 2003 and Linux®, provide text-based access to the server from the host server serial port. An administrator can connect a laptop to the serial port of the host server and perform basic management tasks. For example, the Windows EMS Console, if enabled, displays the processes that are running and allows administrators to halt processes. This capability can be important in cases where video, device drivers, or other OS features have prevented normal operation and normal corrective actions.

With the virtual serial port feature of iLO, an administrator can access a console application such as Windows EMS remotely over the network. The iLO device contains the hardware equivalent of the standard serial port (16550 UART) register set, and the iLO firmware provides a Java applet that connects to the server serial port. If the serial redirection feature is enabled on the host server,[7] iLO intercepts the data coming from the serial port, encrypts it, and sends it to the web browser applet or telnet application.

Directory services

Administrators can use directory services to authenticate user access and authorize user privileges for groups of iLO management processors.[8] Directory services use a central, scalable database to provide a consistent way to store information about objects such as servers, shared volumes, printers, network user accounts, and security policies. Maintaining this data in a central repository makes it possible for all servers on the network to access the same user accounts, settings, and authentication services.

The iLO directory services integration feature uses the industry-standard Lightweight Directory Access Protocol (LDAP) to participate in the authentication and authorization processes of an existing user database. HP chose to layer the LDAP protocol on top of SSL to transmit the directory services information securely to the directory servers.

HP provides snap-in management programs to ease directory-based lights-out administration. The snap-in management programs understand how to render, display, and manipulate lights-out objects stored in the directory. They integrate with existing management applications (Microsoft Management Console for Active Directory and Novell ConsoleOne for eDirectory) so that a separate administration application is unnecessary.

Using directory services simplifies user administration by:

- Providing a single repository for all user accounts and Lights-Out devices
- Using the same security (password) policies as rest of network
- Supporting thousands of users
- Providing role-based administration with access and time restrictions
- Providing consistent access rights across all Lights-Out devices

---

[7] Linux users must also set up a login shell to the serial port (TTYS0) and configure the host server to allow root access.
[8] Directory services are available for all Lights-Out devices: iLO, the optional Remote Insight Lights-Out Edition, and the optional Remote Insight Lights-Out Edition II. The term Lights-Out devices refers to all three.

Single repository

Directory services allow IT managers to scale their IT infrastructure easily by managing all users' rights—including those for iLO management processors—in a single database. Corporate environments already have directory structures with user account information. Those existing user accounts in the directory can simply be expanded to include the rights for iLO.

Without LDAP support, administrators must change the local user database on each iLO management processor each time they need to change user's privileges, change passwords, disable an account, or add a new user. Although administrators can automate the process by using scripting, it can still be time-consuming. With LDAP support and the use of directories, a single change in the directory is reflected for all Lights-Out devices associated with a user. Besides increasing efficiency, this use of directories reduces the risk of an administrator making an error as he performs the same function repeatedly.

Enhanced security policies

Because directory services allow an administrator to authenticate a user by means of the same login process employed throughout the rest of the network, corporate standards for security can be easily enforced. For example, corporate standards for password length, character requirements, and password rotation policies (changing passwords) are enforced through the directory service. Without directory services integration, iLO requires only a minimum password length, enforced only when a user changes passwords.

By using a single login process for all user rights, a user no longer needs to remember (or write down in a non-secure area) a separate password for iLO access.

Scalable number of users

Without directory integration, the iLO management processor supports 12 user accounts. This level of support reflects a trade-off between flexibility, expected usage, and necessary support hardware. Directories, however, can provide thousands of user accounts. By integrating with directory services, iLO management processors inherit the same expandable range of user accounts.

Role-based administration

Directories provide role-based access to iLO. A Lights-Out management role is an object in the directory that associates users with Lights-Out device objects and defines the rights granted to a particular set of users. Roles can manage multiple devices, and users can be members of multiple roles. Each role grants associated users additional rights to all the devices the role manages.

Administrators can limit each role through specifying DNS name, IP address, ranges of IP addresses, or time restrictions. The role grants access only to users that satisfy the restrictions. The access restrictions can be used inclusively to allow access only from the specified list, or they can be used exclusively to prevent access from all members of the specified list. Administrators can allow or deny access at specific times using the time restrictions. A 7-day week is broken into 30-minute access windows that can be toggled individually to allow or deny access. For example, the administrator might set up a role called "local admin" and a role called "regional admin." If someone is defined as having the role of "local admin," then that person can access only the rights specified for that role (such as login access and remote console) and only at specified times (such as from 8:00 a.m. to 5:00 p.m.) and locations (such as from a specific IP address).

The role-based access of directories alleviates the common problem of account sharing for Lights-Out processors. A group of administrators will often share the management responsibilities for iLO-enabled servers. If a generic "administrator" account is shared by the group, then all access using that account is ambiguous; and an action can be identified by account, but not by an individual. However, with directories, each user maintains his or her identity, password rotation is per user rather than per role, and users have no reason to share their account password.

Consistent access rights

Using directory services provides IT administrators a consistent set of access rights across all Lights-Out devices: the iLO management processor, Remote Insight Lights-Out Edition (RILOE), and Remote Insight Lights-Out Edition II. This allows administrators to use the same management practices across any Lights-Out device. These access rights include:

- Login—controls whether users can log in to the associated devices.
- Remote console—enables the user to access the Remote Console.
- Virtual media—enables the user to access the iLO virtual media functionality.
- Server reset and power—enables the user to access the iLO virtual power button to remotely reset the server or power it down.
- Administer local user accounts—enables the user to administer accounts. The user can modify his account settings, modify other user account settings, add users, and delete users.
- Administer local device settings—enables the user to configure the iLO management processor settings. These settings include the options available on the Global Settings, Network Settings, SNMP Settings, and Directory Settings screens of the iLO Web browser.

Additional information about these access rights is available in the *Integrated Lights-Out User Guide*.

Operating system support and iLO requirements

At the time of this writing, directory-enabled iLO management processors support Microsoft Active Directory running on Windows 2000 and Windows Server 2003. They also support Novell eDirectory running on Windows 2000, NetWare 6.0, or Red Hat Linux 7.2/7.3.

To enable directory services, customers must have firmware version 1.40 or greater, the iLO Advanced feature set, and the HP Smart Component installation software. The installation software is available for download from the HP website at http://h18013.www1.hp.com/products/servers/management/directorysupp/softwaredrivers.html.

Security

The cornerstone of an effective remote management tool is its security technology. If the solution is not secure, the tool is potentially a far greater liability than an asset. Some vendors have tried to push management tools designed for desktop computers into the enterprise. These tools offer the promise of increased manageability, but they are fundamentally flawed due to the lack of a secure infrastructure. HP, on the other hand, carefully considered security requirements of the enterprise when architecting iLO. The iLO management processor provides multiple levels of security, including:

- Directory-integrated authentication and access control
- Encryption of web pages and the remote console session
- Digitally signed firmware
- Digitally signed applets
- Configurable port assignments
- Event generation for failed login attempts
- Ability to disable configuration utilities and other services
- Hardware protection of stored data

Directory-integrated authentication and access control

If the directory services capability of iLO Advanced is enabled, iLO can authenticate a user by means of the same login process employed throughout the rest of the network. As previously discussed in the "Directory Services" section, using a single login process allows corporate security standards to be applied and eliminates the need for users to have a separate iLO password. Administrators can also

define very specific roles and privileges to control access to iLO when using directory services. Finally, using directory services can provide greater protection against malicious attacks on the network. If an attacker tried to log in to iLO using a local account, after several unsuccessful tries, the iLO would lock the attacker out of the login process. However, there is nothing to prevent this same attacker from trying other iLO devices on the network. With directory services, an attacker is locked out of the directory, preventing further attacks against multiple iLO devices, thus reducing the chance that an attacker could compromise an iLO.

Encryption

The iLO processor uses industry-standard 128-bit SSL encryption technology to encrypt web pages. SSL encryption ensures that all information and commands issued through the web pages are private. Even the login credentials on the web browser screen are encrypted using a secure hash algorithm. The remote console information, including the virtual media and virtual serial port data streams, is encrypted using 128-bit RC4 encryption. Using 128-bit encryption protects the confidentiality of sensitive data and transactions without consuming excessive processing resources from either the host or the iLO management processor.

Digitally signed firmware

The iLO processor ensures the legitimacy and integrity of any iLO firmware images by including a digital signature. A digital signature is generated using a private "key," or encryption code, known only to HP. The iLO firmware verifies the digital signature by using a corresponding public key. The firmware contents cannot be modified without generating a new digital signature, which requires the original private key from HP. If iLO cannot verify the digital signature, iLO will not execute or even load the firmware. This prevents loading corrupt or rogue firmware.

Digitally signed applets

The virtual media and remote console applets are also digitally signed. The digital signature ensures that when an administrator views the applet window, he can be confident that the code originated from the iLO processor, and that it has not been altered or tampered with after the signature was applied.

After the digital signature has been verified, the virtual media applet can read or write to the management console's physical floppy, CD drive, or the associated image files. Likewise, after the digital signature has been verified, the remote console applet can automatically start the Microsoft Terminal Services client.

Configurable port assignments

Administrators can configure all the network (TCP/IP) ports and the remote console port. The administrator may change the default port numbers and protect these ports from any additional changes by defining login privileges. For the remote console port, the administrator has the option of enabling, disabling, or setting it to accept remote console sessions "automatically." If administrators select the auto-enable setting, the remote console port is disabled except when iLO senses the remote console applet starting. This ensures that only remote console sessions connect to the remote console port.

Event generation

The iLO processor tracks all login attempts and maintains a record of all login failures. When login attempts fail, iLO generates alerts and sends them to a remote management console. In addition, iLO adds progressive delays at each failed login attempt. After an initial failed login, iLO imposes a delay of 5 seconds; after a second failed attempt, iLO imposes a delay of 10 seconds; after the third failed attempt, iLO imposes a delay of 60 seconds. This feature assists in defending against possible dictionary attacks against the browser login port.

Disabling iLO services

The following utilities can be disabled entirely using the iLO web pages: the ROM-Based Setup Utility (RBSU), SNMP, and Terminal Services pass-through utilities.

RBSU is the recommended method to set up a single iLO device initially. However, because RBSU is available every time the server is booted, there is the possibility that an unauthorized person at the host server could use RBSU to reconfigure the iLO processor and gain access. Therefore, administrators can require RBSU login or disable RBSU to prevent reconfiguration from the host.

Because SNMP uses passwords (known as community strings) sent across the network in clear text, administrators may choose to disable SNMP access entirely.

Although no Terminal Services vulnerabilities are known at this time, this utility does represent another avenue for access to the host server. An administrator can disable the Terminal Services support if it is not being used. Alternatively, the "automatic" setting disables the service unless the Remote Console applet initiates a connection.

Hardware protection

All login credentials, passwords, and encryption keys are stored in the embedded volatile and non-volatile RAM in the iLO ASIC. Because the iLO ASIC has built-in firewall functionality, these variables are secured from the view of any host software. Without this hardware protection, it would be possible for malicious code running on the host server to scan the embedded memory image and obtain these variables. The hardware-based Host Bridge/Firewall protects against unauthorized access to sensitive data crossing the host server's PCI interface. This protection provides both privacy and data integrity.

Blade server infrastructure

Because ProLiant BL p-Class systems[9] consist of multiple components (server blades, server blade enclosure, power supplies, and power supply enclosure), it is essential that these components communicate important information to each other. Each server blade in the ProLiant BL p-Class family contains the iLO management processor for intelligent management of the server blades and intelligent communication within the server blade infrastructure. All features of iLO are enabled by default on ProLiant p-Class systems, so the administrator has full and immediate access to the powerful graphical remote console and virtual media capabilities. The iLO firmware provides specific functionality within BL p-Class systems to ensure adequate power resources for the server blades, tailored web pages specific to the modular blade architecture, and an intelligent communication channel to provide location data for diagnostics, event reporting, and deployment data.

The power infrastructure in the BL p-Class system separates the power supplies from the server blades themselves. For a p-Class server blade to power on, the necessary power must be available from the power infrastructure. One of the primary responsibilities of iLO in the server blade architecture is to assist in managing those power resources. The iLO management processor verifies with the Power Management Module that there is sufficient power before sending any power-on request to the server blade.

The iLO web interface provides an additional page that appears only for ProLiant BL p-Class systems (Figure 3). This web page provides specific information such as rack name, enclosure name, and server blade bay numbers associated with the server blade system. If a rack or enclosure name changes, iLO receives an alert from the Server Blade Management Module and propagates the name change to the other server blades in the affected enclosure.

[9] Information about the ProLiant BL p-Class systems is available from http://h18004.www1.hp.com/products/servers/platforms/index-bl.html

Figure 3. Example of the iLO web interface specific to ProLiant BL p-Class systems

The iLO management processor provides a direct communication channel between the management agents, the host OS, the server blade management module, and the power management module of the BL p-Class System. This is important because in the ProLiant BL p-Class system, management alerts and events must be forwarded from shared resources (such as power supplies) to any server blades that may be affected. For example, if a power supply were removed from a power supply enclosure, the power management module would send an alert to the server blade management module, which would propagate these alerts to all iLO processors on the affected server blades.

Administration of the iLO processor

HP designed the iLO management processor for easy configuration and management. Administrators can choose the method that works best for their IT environment in both configuration and management tools. HP has paid special attention to the needs of administrators in large IT environments by incorporating advanced scripting tools that provide an easy and efficient way to configure and maintain management processors. In addition, administrators that are deploying large numbers of iLO processors can obtain special licensing agreements to facilitate deployment of iLO Advanced functionality.

Configuration

Administrators can configure individual iLO management processors in one of three ways: through RBSU, through the web browser interface, or through a scripted setup.

For configuring large numbers of iLO processors, HP has developed sample XML script files that can be used along with the Lights-Out Configuration Utility (CPQLOCFG.EXE) to configure iLO management processors. Administrators can use a bar code reader to scan all the passwords and Domain Name System or Service (DNS) names from the network settings tag into a spreadsheet or database. This process is much less time-consuming and error-free than manually entering passwords and DNS names into a spreadsheet. Then, using the appropriate XML script, the administrator can configure the group of iLO devices, add license keys for the iLO Advanced functionality, upgrade firmware on the iLO devices, add a new user, or change user privileges.

Both CPQLOCFG.EXE and the sample scripts files are available from the website at http://h18013.www1.hp.com/products/servers/management/ilobest-practice.html. Administrators must use the CPQLOCFG.EXE version 2.0 or greater with iLO processors.

Management

Administrators can use script files or directory services to perform routine maintenance (such as adding or deleting users, updating firmware, or changing user rights) on large groups of iLO processors simultaneously.

For example, using the CPQLOCFG utility, an administrator might write a script to remotely upgrade the system BIOS for every server in a rack. The script might instruct the iLO device in each server to do the following: power down the server, download the new BIOS, and then power up the server. With XML-based remote scripting capabilities, every function or task an administrator can do using Lights-Out technology and a web browser can also be done in a secure environment through an XML script running at a remote site.

As previously described, administrators can use directory services to authenticate user access and authorize user privileges for groups of iLO management processors. This allows administrators to perform maintenance functions just once rather than multiple times. This reduces the risk of an administrator's making an error as he or she performs the same function repeatedly. By using directory services, administrators can also provide a virtually unlimited number of user accounts.

Master license agreements

Customers that have a large installed based of iLO processors and frequently add more may want to purchase a Master License Agreement (MLA) from HP. An MLA allows the customer to purchase a single activation key for multiple licenses of the ProLiant Essentials Value Packs, such as the iLO Advanced Pack. After the MLA is in place with HP, the customer simply purchases the desired number of license-only part numbers whenever additional iLO Advanced licenses are needed. This simplifies the software licensing process and reduces the amount of physical documentation shipped to the customer.

Additional information about ProLiant Essentials licensing options is available from the website at: http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/licensing.html.

Related management tools

The iLO management processor is tightly integrated with other leading HP management tools. Administrators can use the Insight Management Suite and the ProLiant Essentials Rapid Deployment Pack to gain easy access to iLO information and capabilities.

Insight Manager integration

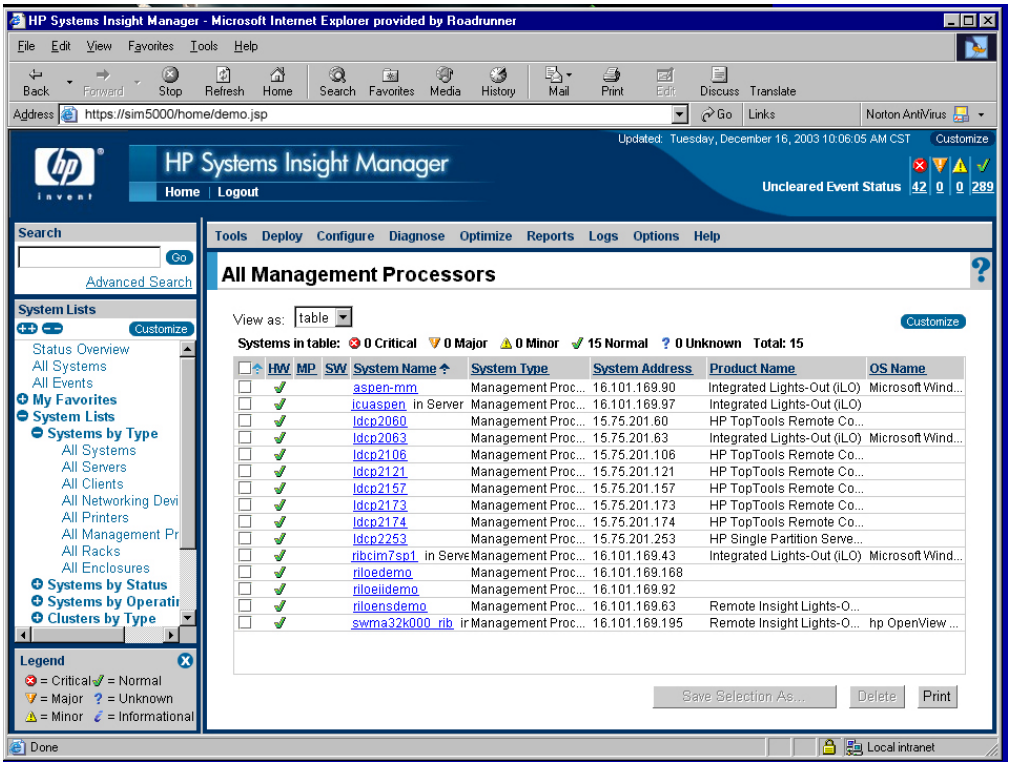
The Insight Management Suite—whether Insight Manager 7 or HP Systems Insight Manager[10]—and the management agents are tightly integrated with iLO. This allows administrators to view subsystem and status information from a web browser. The iLO processor performs the monitoring for the server hardware (such as fan performance and internal board temperatures) and then forwards this information to the Insight Manager agents. The information can be accessed either through the Insight Manager web page or through a link on the iLO web pages.

[10] Systems Insight Manager is the next generation in the Insight Manager family. See the website at http://h18004.www1.hp.com/products/servers/management/hpsim/index.html for more information.

The iLO processor may be configured to send iLO SNMP alerts to Insight Manager or other SNMP-based management consoles. These iLO SNMP alerts include server events, such as a host server power outage or host server reset, and iLO events, such as an unauthorized login attempt or a change to the Security Override Switch.

Furthermore, an administrator can use the query mechanism of Insight Manager to discover each iLO processor and store it on a device list. The device list provides direct hyperlink access to each iLO processor (Figure 4), giving the administrator a single location for accessing all Lights-Out management devices.

Figure 4. Device list in Insight Manager 7



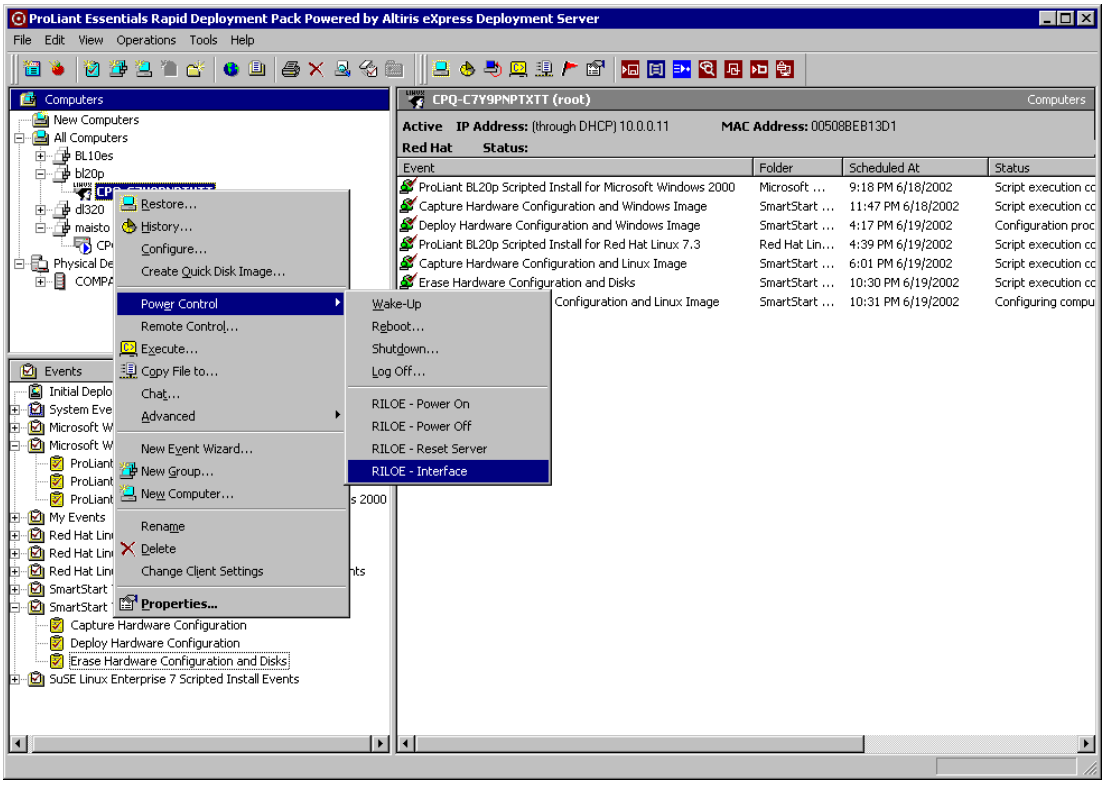
RDP integration

The ProLiant Essentials Rapid Deployment Pack (RDP)[11] gives administrators the ability to easily deploy one or many servers in an unattended, automated fashion. It combines the Altiris eXpress Deployment solution with the ProLiant Integration Module to provide a "drag and drop" solution for deploying a standard server configuration from a remote console. The Deployment Server function within RDP provides capabilities that incorporate the iLO management features of powering on, powering off, or cycling power on a target server. Each time a computer connects to the Deployment Server function, the server polls the computer to see if iLO is installed. If so, the server gathers information such as the DNS name and IP address and displays it in the **Properties** page of the Deployment Server application.

[11] Available at http://h18004.www1.hp.com/products/servers/management/rdp/index.html

An administrator can also use RDP to browse to an iLO management processor and access the iLO interface (Figure 5). This provides easy access to the iLO management features.

Figure 5: Using RDP to browse to the iLO management interface. Note that the RDP Interface text uses the term *RILOE* for connecting to either a Remote Insight Lights-Out Edition (RILOE) or an iLO management processor.



Using the Altiris Boot Disk Creator Utility, an administrator can also create boot floppies with the target server configuration. The administrator can then use these boot floppies with the virtual media function in iLO to create a bootable image anywhere on the network. The administrator can boot from these virtual floppies and connect to the RDP Deployment Server to complete the installation and deployment process.

Conclusion

Because the iLO processor is based on hardware, it provides system administrators a robust, out-of-band, connection to the managed server. The comprehensive remote management capabilities are always available, regardless of the state of the server—whether the server is powered on, the OS is loaded, or the OS is functioning. The iLO processor is a secure management system, incorporating multiple layers of security that encompass the hardware, firmware, and communication interfaces. Administrators can enable or disable security features as needed. With Terminal Services, the iLO remote console has the high performance of a software-based console when the OS is functioning, with the assurance of an always-available hardware-based remote console.

Finally, the iLO management processor is designed for scalability: Using directory services or scripting tools, administrators can easily deploy and manage tens or hundreds of iLO processors. Integrated Lights-Out functionality improves the efficiency of system administration so that customer IT groups can operate more productively.

For more information

For additional information, refer to the resources listed below.

Resource description	Web address
Integrated Lights-Out Documentation	http://h18004.www1.hp.com/products/servers/management/ilo/documentation.html
Directory support on Lights-Out management products	http://h18004.www1.hp.com/products/servers/management/directorysupp/index.html
Best practices for iLO includes information about directory services, best practices to improve performance, and sample scripts to download.	http://h18013.www1.hp.com/products/servers/management/ilobest-practice.html
Linux for ProLiant website contains software, hardware certification matrices, and documentation for ProLiant servers running Linux.	http://h18000.www1.hp.com/products/servers/linux/index.html
ProLiant Essentials Rapid Deployment Pack	http://h18004.www1.hp.com/products/servers/management/rdp/index.html
Information about evaluation licenses for iLO Advanced 1.5 (or greater)	http://h18013.www1.hp.com/products/servers/management/iloadv/index.html

Call to action

To help us better understand and meet your needs for ISS technology information, please send comments about this paper to: TechCom@HP.com.

TC040106TB, 01/2004

invent