Server Technology

Solutions for the Data Center Equipment Cabinet ™

White Paper

Best Practices for Secure Remote Power Management

Server Technology, Inc. Adds SSL & SSH Security for Protecting Remote Management Sessions

Overview

Inside the data center exists the enterprises' collective knowledge of products, research, services, customers, relationships and processes – keys to the firm's ability to successfully compete in its field. Every enterprise has the ability to achieve a competitive advantage with its ability to marshal this information quickly and efficiently to make strategic decisions. To minimize losses, it is imperative to maintain maximum 99.99% uptime of the devices within the data center that house and process this data. A Remote Power Management solution provides the ability to maintain maximum uptime by isolating individual components that are locked-up or failing and independently rebooting that device to bring it back to an operational state. Each server, router, switch or other network device is accessible for a remote reboot.

Accessing and protecting the devices supported by the Remote Power Management (RPM) solution presents another challenge. Direct TCP/IP access to each RPM device on the network is, of course, the fastest and most direct method to reboot an individual server or router, but the TCP/IP access method also presents the greatest security risk to the network. Non-secure network traffic can be penetrated and hackers can intercept sensitive information, such as usernames and passwords. This sensitive information can be exploited in an attack on the network and could lead to a system-wide shutdown. Additionally, former or disgruntled employees with malicious intent can carry sensitive information away from the job with them, potentially leading to the same disastrous results.

This document examines the major methods for securing network traffic for Remote Power Management devices and presents alternatives for successfully integrating an RPM solution with the network management system.

Trends & Drivers: Businesses Requirements to Reduce Downtime

Technology not only creates the opportunity for businesses to better serve their customers, but is also a requirement for them to stay abreast or ahead of competition. All stakeholders -- customers, partners, investors and employees – rely on the enterprise's ability to process and share data at peak levels of efficiency. Data centers are the hub between private and public networks and reliance on the efficiency of the data center continues to escalate with each new advancement in technology. The bottom line on the data center is uptime: if a single asset in the data center becomes unavailable for an extended period, the data center becomes a liability. Business and processes suffer as downtime spreads through the organization, and the responsibility to maximize uptime falls to the data center manager.

Reducing downtime in the data center has become an industry driver. The development of Remote Power Management solutions aides immensely in meeting this objective. Servers and network devices far outnumber available staff to manage these devices in the data center – or multiple distributed data centers – and RPM provides the ability to centralize management for rebooting failing equipment units.

With an RPM solution in place, the data center manager has the ability to:

- Expedite problem/solution response time
- Improve network availability
- Reduce field service visits and/or eliminate staff requirements to respond to trouble tickets
- Act Proactively
- Tighten facility security

The last point, security, has implications not only to the physical security of the data, but also the virtual security of the network. Deployment of RPM solutions decreases the reliance to send manpower to rectify failing or locked-up devices, thereby reducing the number of visitors passing through man-traps into the data center. By increasing reliance on network traffic to perform these sensitive operations, however, the data center must be able to filter the visitors and the requests on the network to access individual servers and network devices.

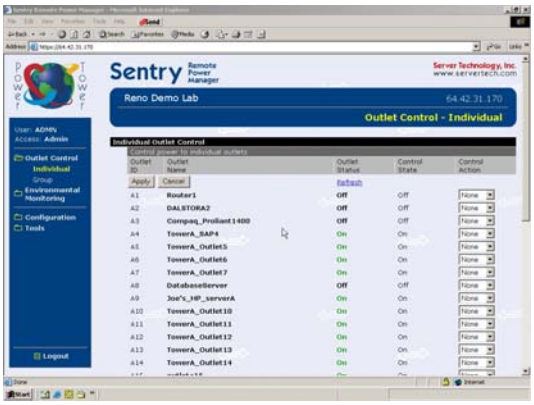
TCP/IP network traffic is the most common method for accessing RPM devices, but also poses the most common threat to security breaches for most enterprises. Each enterprise has its preferred method for integrating and communicating with RPM devices, including HTTP for Web GUI interfaces, Telnet for scripting or command-line interfaces, and SNMP management. Regardless of the chosen protocol, each access method presents security risk by transmitting text across an open network. The resolution to the security risk is to choose an RPM solution that provides data encryption and other security features.

Without network security, data center managers put their entire networks at great risk when logging onto a remote management device via the Internet. The chosen RPM solution should provide encrypted security solutions for the most common types of network traffic, including HTTP (Web GUI) and Telnet. It is important to note that several RPM manufacturers claim to include "access security" in their product, but, in fact, only include authentication – an unencrypted username and password feature. True access security is provided only when integrating one of the commonly used security protocols, such as Server Technology, Inc.'s Sentry Remote Power Managers that integrate SSLv3 and SSHv2 SSL security protocols. Both of these protocols provide for the strongest encryption of the entire session.

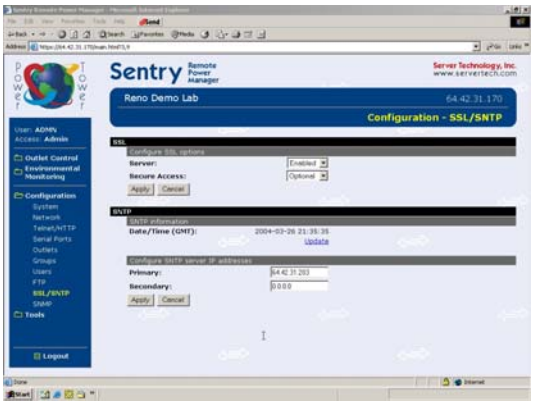
SSL: Securing Web GUI Sessions

Several manufacturers of Remote Power Management solutions provide a Web interface for initiating remote reboots and other remote management applications. While using a Web interface has become the preferred method of quickly logging into and accessing each device for data center managers, only basic encoding of user authentication information -- *until now* -- has guarded these sessions. Server Technology introduces the use of Secure Sockets Layer (SSLv3/TLSv1) to encrypt HTTP sessions between a Sentry Remote Power Manager and a remote network manager accessing the Sentry to reboot a selected device.

Sentry's SSL secure HTTPS interface prevents hackers from intercepting or sniffing open text across a network. Sensitive information such as user accounts and passwords are protected from outside observers with malicious intentions. The potential damage from criminal interception could be devastating – entire networks and enterprises virtually shut down. Only SSL-protected Web browsers can prevent such damaging acts of corporate espionage.



Sentry's 128-bit SSL HTTPS GUI for secure Remote Power Management



Sentry's SSL HTTPS GUI can be set to optional or required for log-ins

Encryption Technology and SSL Certificates

Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Encryption, the process of transforming information to make it unintelligible to all but the intended recipient, forms the basis of data integrity and privacy necessary for e-commerce. Customers submit sensitive information via the Web only when they are confident that their personal information is secure. The solution for businesses that are serious about online business is to implement a trust infrastructure based on encryption technology.

An SSL Certificate is an electronic file that uniquely identifies individuals and Web sites and enables encrypted communications. SSL Certificates serve as a kind of digital passport or credential.

The Sentry products' SSL Certificate enables the user to verify the Sentry's authenticity and to communicate with it securely via state-of-the-art SSL encryption, which protects confidential information from interception and hacking. 128-bit SSL, included with Sentry products,

enables the world's strongest SSL encryption with both domestic and export versions of Microsoft® and Netscape® browsers. 128-bit SSL is the standard for large-scale online merchants, banks, brokerages, health care organizations, and insurance companies worldwide. All exchanges of SSL Certificates occur within seconds, and require no action by the customer.

SSH

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. Server Technology has integrated SSH[1] into its Ethernet interface to provide strong encryption, robust authentication and data integrity for Sentry products throughout an enterprise. Use of SSH virtually eliminates the risk of remote management as all session data is encrypted using strong ciphers with keys exchanged dynamically using RSA/DSA public key algorithms.

SSH commands are encrypted and secured in several ways. Both ends of the client/server connection are authenticated using a DSA public key, and passwords are protected by being encrypted. It is intended as a replacement for telnet among other protocols.

Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecure channels. In other words, SSH never trusts the net; in the event that somebody hostile has taken over the network, he can only force SSH to disconnect, but cannot decrypt or play back the traffic, or hijack the connection.

SSH requires public and private keys to authenticate both ends of the channel

Secure Shell protects against:

- IP spoofing, where a remote host sends out packets, which pretend to come from another, trusted host. SSH even protects against a spoofer on the local network, who can pretend he is a router to the outside.
- IP source routing, where a host can pretend that an IP packet comes from another, trusted host.
- DNS spoofing, where an attacker forges name server records.
- Interception of clear text passwords and other data by intermediate hosts.
- Manipulation of data by people in control of intermediate hosts.

[1] *Sentry SSH provided by Mocana Embedded SSH Server*

Console Ports: Secure Communication through SSH

In addition to using Sentry's secure SSH connection to access individual RPM devices and perform a reboot operation to any connected server or network devices, the network administrator can also use Sentry's SSH connection to securely connect to the serial console port of an attached data center devices as if her were sitting in front of it. This complementary function of using a Sentry as an RPM appliance allows the network manager to aggregate the serial console ports for several devices into the one SSH connection. For instance, by launching an SSH session directly to the serial console port of a Unix server through the Sentry connection, the network manager accesses the Command Line Interface (CLI) of the server itself.

MD5

SSH and SSL represent the strongest security protocols available for communicating and managing an RPM device via TCP/IP network. If for reasons that make it unpractical for an enterprise to utilize either SSL or SSH, Server Technology also provides MD5 digest for security and validation of the username-password. The MD5 digest method provides protection utilizing one-way encoded hash numbers, never placing the username-password on the network. Instead, the sending browser creates a challenge code based on the hash algorithm, provided username-password and unique item such as the device IP address and timestamp, which is compared against the HTTP server internal database of valid challenge codes. The MD5 digest method offers a higher level of security than basic username-password authentication, but may not be supported by all browsers. MD5 is know to be fully supported by Internet Explorer 5.0+.

Active Directory

SSL, SSH and MD5 provide best-in-class security for users authenticating with a Sentry unit across an open IP network. They prevent hackers from intercepting clear text username-passwords and from spoofing where an attacker forges IP packets, which pretend to come from a trusted host. They cannot, however, prevent an unauthorized user, who *used to be an authorized user,* from sending legitimate username-password combinations in order to carry out malicious actions. For these situations, a requirement for easier management of a large number of remote power managers on a global scale has been recognized.

There are many management tasks that an enterprise faces with the deployment of large numbers of internetworking equipment. These include, but certainly are not limited to, assigning network configuration settings (e.g. IP address), assignment of user names and password, configuration of access rights, security configuration, SNMP configuration, and configuration specific to the device. Not only does the configuration need to be setup initially, it often must also be changed as needed to match changing network conditions, or on a periodic basis for security reasons. One common example is that security policies within enterprises require that user passwords be changed once a week.

The management problems are obvious. If there are hundreds or thousands of a particular internetworking device, each with its own IP address, and with the configuration interface only being reachable by Telnet or HTTP to each target address, then a single simple configuration operation (such as changing an administrative password) must be done hundreds or thousands of times. Using Telnet or HTTP, for each target device, the user must point to each IP address, login, make the configuration change, and logout. Time and manpower are greatly expended, which has a definite measurable cost associated with it.

Network equipment vendors that have addressed this issue in a variety of manners. Some have created scripting applications to automate common management tasks to numerous devices. Others have created their own global management software. Others have relied on third-party management software, providing full, partial, or no integration.

Different vendors using different approaches, however, has itself has become a problem. While they simplify configuration management of a particular vendor's devices, they do not alleviate the management of configuration items that are common across multiple vendors' devices.

For example, consider an enterprise's IT department. In the IT department are the personnel that manage the various internetworking devices from many different vendors. The personnel that manage the equipment are the same people, regardless of whether they are managing equipment from Vendor A or Vendor B. So, should they have a different username and password for each vendor's equipment? The clear answer is no. Each user should have one username and one password. But, if each vendor's device must use a different solution for configuration management, then changing a single users' password across multiple vendors' devices is still time intensive, as it must involve each vendors' own solution to repeat what is essentially a single change from the IT department's perspective.

The problem of different solutions from different vendors is solved by directory services.

What are Directory Services?

Directory services are repositories for information about network-based entities, such as applications, files, printers, and people. Directory services are important because they provide a consistent way to name, describe, locate, access, manage, and secure information about these resources. Many vendors build specialized repositories or directory services into their applications to enable the specific functionality their customers require. As such, enterprise class directories take an important step towards the consolidation of corporate directories by offering standards-based interfaces allowing for interoperability and centralized directory management.

Directory Services are a part of many server operating systems. Microsoft, Novell, and Linux server environments all support some form of directory services. In consultation with existing and prospective customers, Server Technology has found that the most prevalent directory service in use is Active Directory, from Microsoft.

Active Directory (AD), which is an essential component of the Windows 2000 and 2003 Server architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory allows organizations to centrally manage and share information on network resources and users while acting as the central authority for network security. In addition to providing comprehensive directory services to a Windows environment, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies require. Active Directory reduces costs and simplifies management by eliminating the time consuming, redundant tasks usually associated with running a distributed network.

How does Active Directory solve the management problem?

By acting as a central repository for information, the redundancy of management tasks is eliminated. For example, instead of changing a user's password in hundreds or thousands of individual devices, or changing it in multiple devices' management software, the change need only occur in one place – the directory. Further, the change is made through a consistent management interface, regardless of the device. The Active Directory resides on a Windows Server that is accessible over the network.

Instead of a device storing configuration information locally, a device accesses the configuration information in an Active Directory by use of a network protocol. Active Directory supports multiple protocols for this purpose. The most common network protocol for accessing directory services access is the Lightweight Directory Access Protocol (LDAP). A secure version of LDAP over SSL (LDAP/S) can also be used.

User Accounts

As in the case of other network devices, a need often exists to create multiple user accounts with limited access rights to each Remote Power Manager. Server Technology provides this base functionality in Sentry products. The Sentry has one predefined administrative user account and supports a maximum of 128 defined user accounts. Only an administrative-level user may perform operations such as creating/removing user accounts and command privileges, changing passwords and displaying outlet and user information. An administrator may also view the status of and control power to all outlets. The administrator may create additional user accounts and then grant these users the right to view the status of and control power to specific outlets, groups and ports. Usernames and passwords may contain from 1-16 characters.

Using tools such as Active Directory, of course, facilities the management of assigning and managing multiple user accounts across the enterprise.

Proactive Management: SNMP Traps

Beyond the concerns of authenticating securely with a Remote Power Manager over an IP network, network managers need also consider the security of the equipment cabinet in the data center. While hackers prowl in the virtual realm, predators lurk in the physical world of the data center. Unauthorized visitors in the data center – or even authorized personnel with malicious intent – can cause serious harm to the servers and network equipment in the data center. Mother nature, too, sometimes can wreak havoc on the data center as well as failures in technology and infrastructure. Regardless of the cause, environmental factors in the data can be monitored and catastrophes avoided.

The Sentry family of products supports the Simple Network Management Protocol (SNMP). This allows network management systems to use SNMP requests not only to control power to the Sentry's individual outlets, but also to retrieve information about the power and environmental conditions.

Administrators often become aware of failed systems through user complaints. By the time complaints are received, however, business may likely have already been negatively impacted. To mitigate damage, network administrators need to respond to system failures before they have impacted the business network(s). SNMP traps are tools for administrators to take proactive steps to reducing downtime from failures.

Following is a list of the key SNMP traps for monitoring the availability of the Sentry and its functions:

Tower Status Trap	Generated when communication to the Tower (e.g., Sentry) has been lost, (i.e., the network connection).
Infeed Status Trap	Generated when power infeed to the Sentry is supposed to be available, but no current is sensed.
Outlet Status Trap	Generated when current is not sensed at the outlet level.
Change Trap	Generated for all outlet status changes between any on/off conditions.

In particular, the Change Trap is a very valuable security tool for network administrators as it generates a notification every time an outlet is changed from its on/off status, thereby alerting the administrator of a potentially unauthorized user committing an unauthorized action.

Heat and power continue to be two of the biggest factors affecting the performance of the data center. New, higher density servers and network devices require greater power consumption; moreover, a one percent (1%) rise in optimal temperatures can increase the risk of damage to a server by 2-3%[2]. SNMP Traps designed to monitor these environmental elements and prevent unnecessary damage from them have also been included in the Sentry SNMP MIB.

Following is a list of the environmental conditions that Sentry monitors via SNMP.

Load Trap	Generated whenever the total input load on an infeed exceeds a present threshold (either low or high).
Temperature Trap	Generated whenever ambient temperatures decrease or exceed minimum or maximum defined thresholds (low or high).
Humidity Trap	Generated whenever relative humidity exceeds defined thresholds (low or high).
Water Trap	Generated when water is detected.
Contact Closure Trap	Generated when error conditions occur to the status of a contact closure (e.g., an equipment cabinet is opened).

The Sentry MBI can be compiled by a third-party SNMP management system such as HP Openview, Tivoli Enterprise Manager and What's Up Gold among others, allows the network manager to obtain SNMP trap information. When integrated the Sentry traps can be send to tow destinations, such as email, phone or pager.

Physical Security: Wake Last & Power-up Sequencing

As noted previously, the physical world of the data center can be just as inviting as the virtual network world for intruders and network predators. At stake is the performance of the network and business that is reliant upon it. Whether it be caused by mother nature, technology failure or human contact, changes affecting the input power feed to each data center cabinet could potentially cause system-wide pain.

In particular, a power cycle to an entire equipment cabinet and its computing contents can be fatal. Today's servers and network devices in large part utilize switching power supplies. While effective for powering each device itself at nominal conditions, these switching power supplies draw extremely large power in-rush current during boot-up, sometimes as great as 30x the normal operation current. Because of the power in-rush, an entire rack of equipment booting-up at once could produce devastating effects. Instead of power-on all the devices in a rack, the power in-rush could cause the branch circuit protection for the entire equipment cabinet to blow, at the primary power distribution point (a fuse or circuit breaker). With the branch circuit exceed and blown, none of the devices on the power supply can boot-up and run.

To prevent a power-in rush, the Sentry products utilize a Power-Up Sequencing feature. When power is applied to the Sentry, each of the power outlets are powered sequentially with a two-second delay between each outlet. Power sequencing staggers the individual loads, eliminating the potential of a blown fuse or circuit breaker due to excessive in-rush current and allows circuit support for operating load capacities in the range of 80-90 percent.

Another power-related physical security feature of the Sentry products is the Wake Last feature. After a power loss and recovery, the outlets return to their last controlled position.

[2] *Source: IBM*

Thereby, outlets that were set to an “off” position return to the same “off” position to prevent power consumption on those outlet s that might otherwise exceed the available input current limit.

About Server Technology, Inc.

Server Technology designs, manufactures and distributes the Sentry Remote Power Management products, providing it customers with Solutions for the Data Center Equipment Cabinet. Sentry solutions integrate intelligent power distribution, remote management, power monitoring, environmental monitoring and pass-thru console port access into a seamless management interface. Server Technology, Inc. is located in Reno, NV with representatives located throughout the U.S. and international locations. Server Technology can be found on the Web at www.servertech.com.