Supermicro Server Management : IPMI Firmware Security

Introduction

Supermicro server architecture is built on advanced technologies that provide high performance/watt, flexible IO and management features that allow Enterprises/datacenters/ OEMs achieve the best ROI for their business. One of these technologies is the onboard baseboard management controller (BMC), which provides an efficient interface that enables IT administrators to manage the health of the server through temperature/voltage readings and common server maintenance tasks like BIOS upgrades and debug OS remotely through KVM consoles.

While this feature increases convenience and productivity, server administrators need to understand that BMCs are embedded computers with an operating system and network stack that can be vulnerable to attacks if not configured properly. This paper highlights some of the best practices and features on the BMC that will help fortify your servers against malicious attacks.

Configure BMC network settings on Supermicro servers

1.Password

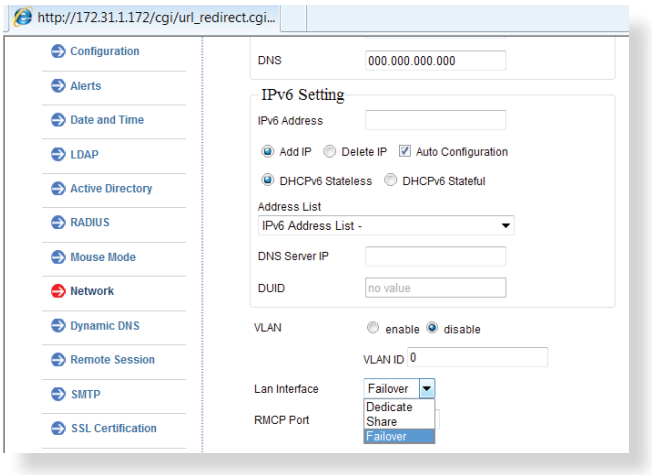
The default username ADMIN has a default password and that needs to be changed locally from within the operating system. Special characters like #,$ are not allowed into password field, as these characters can enable shell injection from intruders. Use strong passwords that are at least 8 characters long and include a mix of numbers, capital, and lower case letters.

2.IP Address Assignment

DHCP is the default protocol to receive IP addresses. Administrators are encouraged to set static IP addresses or restrict the assignment of DHCP addresses to a secure set of IP addresses or subnet.

3.LAN Access

The BMC can be accessed through either a dedicated Ethernet LAN interface (if available) or through a shared LAN (System LAN) Interface. The default setting is 'failover,' which means the BMC will first check for the presence of an active, dedicated LAN interface, other it will respond on through a shared LAN interface. The failover setting helps IT administrators receive default connectivity to the BMC, irrespective of their network topology and provision systems remotely . It is recommended that administrators configure BMCs LAN access to through a dedicated LAN interface instead a System LAN, so that the BMC is not exposed to the internet or to unauthorized user access outside of a firewall.

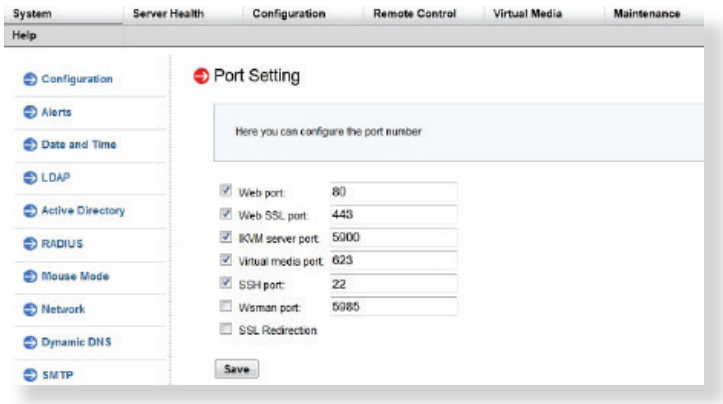


Note: Unhooking an Ethernet cable from dedicated LAN interface does not stop accessing BMCs from shared LAN interface.

4.Service ports

While the IPMI standard protocol defines UDP port 623 for RMCP communications, there are additional remote services that BMCs provide to efficiently provision and debug servers. Some of these services include VNC for debugging an OS, access to http/https ports for locally configuring BMC settings and reading server health, and Virtual media for remotely accessing files and images.

All these services run on TCP/UDP ports (please see the firmware user guide for the latest information) and it is important to restrict these ports in order to secure server management network. The administrator can alternatively reconfigure the port numbers on BMCs. For example, http can be configured to listen on port 76680 such that attackers cannot find the servers through common port scanning tools.



On X10 Products, there is an added security measure available to administrators to disable unneeded services.

5.RAKP

IPMI standard dictates using the RAKP protocol to authenticate RMCP sessions between IPMI clients and BMC servers. The current RAKP hash is typically weak, meaning that one can use brute methods to retrieve password. The Supermicro BMC provides a stronger hash option for RAKP authentication. Since this is an OEM implementation and may not be suitable in every environment, it is still recommended that administrators block UDP port 623 on unsecured networks.

6. IP Access Controls

BMC access should be restricted to include only known machine IP Addresses. This eliminates unwarranted access of corporate servers from inside the network accidentally or deliberately.

7.VLAN Configurations

Configure traffic from BMCs to IPMI clients on a unique VLAN so that management traffic can be segregated from rest of the server data.

Configuring BMC network

Though BMCs provide security features to defend against unwarranted attacks, it is strongly recommended that administrators follow the best practice of configuring BMCs on the networks where they are locally accessible and restrict traffic on sensitive ports between networks.

Traffic on default ports for BMCs such as TCP/5900 and, UDP/623 should be restricted to secure and known networks using firewall rules in routers. The latest suggested recommended best practices and guidelines are published on the Supermicro website at *http://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf*

Plan for periodic firmware updates

Supermicro releases periodic firmware updates that add new security features and provide fixes for issues on an on-going basis. Supermicro fixes high priority issues not only on its developed technologies but also for many underlying components included in its products, such as openssl. Hence, it is a collective responsibility of vendors and users of products to work together and ensure that the servers are updated and secured in deployments. Fixes to latest CVEs are published at *http://www.supermicro.com/products/nfo/files/IPMI/CVE_Update.pdf*

Please contact the Supermicro support teams for the latest information on security related issues.
http://www.supermicro.com/support/index.cfm

Using the right tools

Supermicro provides several options to upgrade and provision BMC firmware depending on the server deployment size, environment (e.g. datacenter vs. an appliance in network), operator's choice of CLI or webUI interfaces, and so on. Some common tools available on the website are Supermicro Server Manager (SSM), Supermicro Update Manager (SUM), SMCIPMITOOL, ipmicfg, and IPMIView, which can all be downloaded from *http://www.supermicro.com/sms* or *http://www.supermicro.com/ipmi*

Conclusion

Baseboard Management Controllers (BMC) using the IPMI protocol are designed to make the management of servers easy for IT operations. Because of the BMC's powerful capabilities, it is recommended that server administrators to take advantage of the security features that BMCs offer, while also restricting network access to the BMC on a protected subnet behind a firewall. IPMI Security is an evolving topic and Supermicro has been actively working with the IT security community and customers to provide timely firmware updates that continuously improve security on our products. Supermicro recommends planning for regular firmware upgrades and employing the right set of tools make upgrades and configurations easy.