Security Best Practices for managing servers with BMC features enabled in Datacenters

Baseboard Management controllers (BMC) are commonly used to manage servers. Most Supermicro server models support BMC Out-of-Band management either through a dedicated management interface or through a shared LAN. BMC provides powerful remote management capabilities in the datacenters but at the same time if not configured properly, causes unwarranted access to BMCs from Internet or within the company and can compromise the security of your machines.

Supermicro recommends the following steps that datacenters need to consider while using BMC to manage your servers.

1. Network Configuration
    a. Restrict inbound traffic over internet directly to BMCs. Logon to a secure management server in datacenter and manage all BMCs from the management server.
    b. Reserve special IP address range (private subnets) to BMC management interfaces and management servers. Don't use reserved IP subnets with LAN interfaces of the managed machines.
    c. Configure the firewall to restrict outbound traffic from BMC including alerts within the reserved IP range.
    d. Use dedicated management interfaces for managing BMCs. If dedicated management interfaces are absent and have to use shared LAN, then configure separate VLANs for BMC traffic.

2. BMC Configuration
    a. Customize service ports information on the BMC to your datacenter specifications. For example, you can configure HTTP port to 57880 instead of 80.
    b. Change the default password during installation and use strong passwords.
    c. Create user policies and roles on BMC.
    d. Use the IP Access Policy to enable access rules to BMC from management servers.
    e. Configure BMC management account security feature to monitor and deny unusual account authentication failed.
    f. Configure System lockdown feature to prevent unintentional system configuration changes.

g. Customize Notification and Alert for high severity system event log and maintenance event log entry.
h. Configure BIOS security features by OOB management. For example, user can enable UEFI Secure Boot.

3. Additional measures
    a. Monitor for unusual traffic between BMC and other machines in the network.
    b. Pay attention to firmware release notes (especially related to security fixes) and plan upgrades of the firmware during maintenance cycles.

For further questions, please contact support@supermicro.com