ICS 35.020
CCS L 62

团　体　标　准

T/CESA 1218—2022

服务器基板管理控制器（BMC）技术要求

Technical requirement for server BMC

2022-07-21 发布　　2022-08-20 实施

中国电子工业标准化技术协会　发布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国电子技术标准化研究院提出。

本文件由中国电子技术标准化研究院、中国电子工业标准化技术协会归口。

本文件起草单位：中国电子技术标准化研究院、华为技术有限公司、天津飞腾信息技术有限公司、中电科技（北京）有限公司、南京百敖软件股份有限公司、无锡先进技术研究院、海光信息技术股份有限公司、上海兆芯集成电路有限公司、龙芯中科技术股份有限公司、浪潮电子信息产业股份有限公司、统信软件技术有限公司、同方股份有限公司、新华三技术有限公司、阿里巴巴技术有限公司、中国长城科技集团股份有限公司、系微软件科技（上海）有限公司。

本文件主要起草人：李雪莲、钟伟军、任翔、尹航、赵鑫、宋博伟、陈颖、杜晓东、陈战、聂永丰、刘勇鹏、舒奕棋、陈小春、任彤、吴平、 汪涛、丁琳、沈金祥、樊青松、何治平、牛彦奎、张文杰、李超、陈继平、刘宝阳、苏孝、张磊 占俊、耿成山、杨蔚才、刘如冰、傅先刚、李羿、李志兵、黎建根、方小明。

服务器基板管理控制器(BMC)技术要求

1 范围

本文件规定了服务器基板管理控制器的基本技术要求，包括远程访问、电源和热管理、告警监控、升级、部署和配置、维护诊断、硬件管理接口、软件管理接口、安全要求和性能要求。

本文件适用于服务器产品BMC的设计和测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

智能平台管理接口规范 （IPMI Spefification, V2.0 ）

DSP0266 Redfish规范 （Redfish Specification Version 1.11.0）

RFC3411-RFC3418（STD0062）简单网络管理协议 （Simple Network Management Protocol v3）

3 术语和定义

下列术语和定义适用于本文件。

3.1

基于LAN的串口重定向 serial over LAN

将原本只能从近端串口线输出的系统串口数据重定向到网络设备输出，并能接受远程网络设备的输入。

3.2

远程访问 remote access

从另一网络，或者从一个并不永久连接到所访问服务器bmc上的网络资源的过程。

3.3

硬盘背板 hard disk backboard

用于连接存储介质和CPU的关键器件，为存储介质提供标准接口、状态指示以及热插拔；部分硬盘背板支持端口扩展功能。

3.4

BMC共享网口 BMC shared network port

利用边带(NC-SI)技术使管理系统与主机系统共用主机物理网口。

4 缩略语

下列缩略语适用于本文件。

BIOS：基本输入输出系统(Basic Input Output System)
BMC：基板管理控制器 (Baseboard Management Controller)
CIFS：通用网络文件系统（Common Internet File System）
DHCP：动态主机设置协议 （Dynamic Host Configuration Protocol）
GPIO：通用输入输出（General Purpose Input Output）
IP：网际互连协议 （Internet Protocol）
ISO： 国际标准化组织 （International Organization for Standardization）
KVM：键盘视频和鼠标（Keyboard, Video, and Mouse）
NFS：网络文件系统（Network File System）
NCSI：边带网络接口控制器（Network Controller Sideband Interface）
OS：操作系统 (Operating System)
SOL：串口重定向（Serial Over LAN）
SNMP：简单网络管理协议 （Simple Network Management Protocol）
VNC：虚拟网络控制台（Virtual Network Console）
FRU: 现场可更换单元（Field Replaceable Unit）
WEB GUI: 网络图形用户界面（Web Graphical User Interface）
PMBUS: 电源管理总线（Power Management Bus）

5 组成部分与分级

5.1 组成部分

BMC是服务器的核心管理系统，兼容服务器业界管理标准IPMI 、SNMP、Redfish、支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能。BMC作为服务器核心管理系统，在服务器系统中发挥重要作用。

本标准给出了BMC远程访问、告警管理、电源管理、升级管理、接口管理等技术要求。

5.2 分级

结合服务器系统管理技术发展，本文件将BMC的技术要求划分为第一级别、第二级别和第三级别。

第一级别：是BMC的基本技术要求，规定服务器管理的基本能力。（Level1）

第二级别：是BMC对服务器的全面管理能力。（level2）

第三级别：是BMC的高级或扩展要求，体现服务器系统管理的发展方向，满足用户对服务器管理能力更高的需求。（level3）

6 功能要求

6.1 远程访问

远程访问的要求包括：

a) 应支持通过 Http、IPMI、SNMP 和 Redfish 接口对服务器单板的上下电控制，并能查询服务器的上下电状态；（Level1）
b) 应支持服务器系统启动选项配置，包括不限于系统启动设备、是否单次生效；（Level1）
c) 应提供基于 LAN 的串口重定向(SOL)功能；将原本只能从近端串口线输出的系统串口数据重定向到网络设备输出，并能接受远程网络设备的输入；（Level2）

d) 应提供虚拟 KVM 功能，支持鼠标同步，组合键，支持传输数据加密；（Level1）
e) 应提供虚拟媒体功能，可以把本地主机的媒体设备通过网络虚拟为远端服务器主机的媒体设备，支持虚拟的媒介包括光驱虚拟，ISO 文件虚拟；（Level2）
f) 应支持远程文件协议；（Level3）
g) 虚拟 KVM 支持 HTML5 或 VNC 访问。（Level3）

6.2 电源和热管理

电源和热管理的要求包括：
a) 应支持服务器整机实时功率查询和显示；（Level1）
b) 应支持历史功率曲线图；（Level2）
c) 应支持功率统计功能，包括不限于系统峰值功率统计、系统平均功率统计、系统累计耗电量统计；（Level3）
d) 应提供电源模式配置功能，包括负载均衡模式、主备模式；（Level3）
e) 应支持实时温度查询，包括不限于 CPU 温度、内存温度、进风口温度；（Level2）
f) 应支持进风口历史温度曲线图；（Level2）
g) 应提供功率封顶功能，功率封顶功能通过设置系统的功率预期上限，当系统功率超过此上限值后，引导特定动作发生，从而保证机箱整体功率的合理分配；（Level3）
h) 应支持风扇智能调速。（Level3）

6.3 告警监控

告警监控的要求包括：
a) 应支持传感器的状态显示，传感器包括门限传感器和离散传感器；（Level1）
b) 应支持告警事件自定义查找，通过告警级别、主体类型、产生时间或事件描述等条件查询指定告警；（Level1）
c) 应支持功率告警门限自定义；（Level1）
d) 应提供告警通知功能，包括 Trap 报文通知、系统日志通知；支持邮件报文通知；（level2）
e) 应支持部件的监控，包括不限于风扇监控、电源监控、内存监控、CPU 监控。（Level2）

6.4 升级

升级的要求包括：
a) 应提供固件升级和版本查询功能；（Level1）
b) 应支持升级的固件，如 BMC 固件、BIOS、电源固件；（Level1）
c) 应支持固件的升级生效分离，允许先升级，后生效；（Level3）
d) 支持升级接口，如 Web GUI/Redfish；（Level2）
e) 应支持 BMC 固件双镜像或双 flash；（Level3）
f) 应支持升级包防篡改校验，要求使用签名校验；（Level2）
g) 更换 FRU 场景下主板 FRU 的刷新。（Level2）

6.5 部署和配置

部署和配置的要求包括：
a) 应支持通过 BMC 对 BIOS 配置，包括系统启动项，电源策略；（level2）
b) 应支持通过远程挂镜像的方式进行 OS 部署；（Level2）
c) 应支持图形化配置界面；（Level2）

d) 应支持机机交互配置接口；（Level2）
e) 应支持配置导入导出功能，可以导入和导出 BMC/BIOS 的主流配置；（Level2）
f) 应支持通过 DHCP 下发 NTP 配置。（Level3）

6.6 维护诊断

维护诊断的要求包括：
a) 应支持服务器可识别部件更换时记录日志信息；（Level3）
b) 应支持通过配置导出功能对服务器配置备份；（Level2）
c) 应支持通过配置导入功能对服务器配置恢复；（Level2）
d) 应提供恢复出厂配置功能；（Level1）
e) 应支持健康状态指示灯；（Level1）
f) 应支持手动截屏，获取当前系统屏幕快照；（Level2）
g) 应支持宕机截屏功能，BMC 在检测到宕机发生时将系统临终时刻的屏幕以指定的格式保存在 BMC 的存储空间内；（Level2）
h) 应支持系统串口数据记录；（Level3）
i) 应支持对 BMC 的复位操作，包括手动近端复位 BMC 和远程复位 BMC；（Level3）
j) 应提供 OS 看门狗功能，默认该功能关闭；（Level3）
k) 宜支持 X86 平台的诊断中断，向 OS 触发一个诊断中断；（Level3）
l) 应支持系统记录事件类、审计类和相关的日志内容；（Level3）
m) 应支持历史故障数据收集；（Level2）
n) 应支持故障诊断，包括故障检测、诊断、上报以及诊断辅助功能；（Level2）
o) 应支持 SEL 记录 OS 重启、关机、开机的详细原因，包括 Power Button、主板电源故障、AC 掉电、IPMI 命令控制和看门狗。（Level1）

7 硬件管理接口

7.1 电源管理

电源管理的要求包括：
a) 应支持电源状态的显示；（Level1）
b) 支持查询输入功率；（Level1）
c) 支持电源温度告警；（Level1）
d) 支持电源异常检测功能；（Level1）
e) 电源资产信息；（Level1）
f) 支持查询电源实时数据；（Level1）
g) 支持电源拔出告警；（Level2）
h) 支持 PMBUS 协议；（Level1）
i) 支持电源固件升级；（Level3）
j) 电源风扇状态监控。（Level1）

7.2 风扇管理

风扇管理的要求包括：
a) 应支持设置风扇模式，包括手动模式和自动模式；（Level1）

b) 应支持设置风扇转速，在风扇模式为手动模式时，支持设置风扇转速。（Level1）

7.3 硬盘背板

硬盘背板管理的要求包括：

a) 应支持查询硬件标识，包括 board ID；（Level3）
b) 应支持硬盘背板在位检测；（Level3）
c) 应支持硬盘背板上 CPLD 或 pSoC 固件状态检查。（Level3）

7.4 PCIE 卡管理

PCIE卡管理的要求包括：

a) 应支持 PCIE 卡信息显示；（Level1）
b) 应支持 PCIE 卡状态监控；（Level3）
c) 应支持获取 PCIE 卡归属 CPU 信息，显示该 PCIE 卡属于哪个 CPU；（Level2）
d) 应支持 PCIE 链路错误指示。（Level3）

7.5 灯板管理

灯板管理的要求包括：

a) 应支持面板指示灯的管理；（Level1）
b) 应支持面板按钮的管理，包括不限于电源按钮(Power Button)，定位指示灯按钮(UID Button)。（Level1）

8 软件管理接口

8.1 IPMI 管理接口

IPMI管理接口要求包括：

a) 应支持 IPMI 2.0 规范；（Level1）
b) 用户管理(新增用户/修改密码/修改权限/删除用户)；（Level1）
c) 服务启停及端口修改；（Level1）
d) 管理网络配置(IP/掩码/网关、DNS)；（Level1）
e) 系统启动(系统启动设备)；（Level1）
f) SEL 查看；（Level1）
g) 传感器查询（温度、电压等查询）；（Level1）
h) 电源控制(上下电、重启)；（Level1）
i) 查看主板 FRU 信息(资产标签/产品名称/产品序列号等)；（Level1）
j) SOL 功能；（Level2）
k) BMC、BIOS、电源 FW 等固件升级；（Level2）
l) 功率封顶配置。（Level3）

8.2 SNMP 管理接口

SNMP管理接口要求包括：

a) 应支持 SNMP Get/Set/Trap 操作；（Level1）
b) SNMP 代理应支持 V1/V2C/V3 版本；（Level1）

c) 系统启动(系统启动设备)；（Level1）
d) 查看当前系统健康状态；（Level2）
e) 温度、电压查询；（Level1）
f) 电源控制(上下电、重启)；（Level1）
g) 查看整机系统信息(资产标签/产品名称/产品序列号等)；（Level1）
h) 查看系统电源、风扇信息；（Level1）
i) 查看网卡及网口信息。（Level2）

8.3 Redfish 管理接口

Redfish管理接口要求包括：
a) BMC、BIOS、电源 FW 等固件升级；（Level2）
b) 用户管理(新增用户/修改密码/修改权限/删除用户)；（Level2）
c) 软件资源列表查看；（Level2）
d) 服务启停及端口修改；（Level2）
e) 管理网络配置(IP/掩码/网关、DNS)；（Level2）
f) 系统启动(系统启动设备、是否单次生效)；（Level2）
g) 系统信息(主机名称、域名称)；（Level2）
h) 查看当前健康事件/历史事件/系统健康状态；（Level2）
i) 事件订阅；（Level2）
j) 远程虚拟媒体(属性查看、挂载、断开)；（Level2）
k) NTP 配置/时区配置；（Level2）
l) LDAP 配置；（Level2）
m) 温度、电压查询；（Level2）
n) 电源控制(上下电、重启)；（Level2）
o) 查看整机系统信息(资产标签/产品名称/产品序列号等)；（Level2）
p) 查看 CPU/内存信息；（Level2）
q) 查看系统电源、风扇信息；（Level2）
r) 查看网卡及网口信息；（Level2）
s) SNMP TRAP 配置；（Level2）
t) BMC 和 BIOS 配置的导入导出；（Level3）
u) BIOS 菜单项查看及配置；（Level2）
v) 功率封顶配置；（Level3）
w) 电源主备配置。（Level3）

8.4 Web 管理接口

Web管理接口的要求包括：
a) 支持通过界面操作完成设置和查询任务；（Level1）
b) 支持 TLS 1.2/1.3；（Level1）
c) BMC、BIOS 等固件升级；（Level1）
d) 用户管理(新增用户/修改密码/修改权限/删除用户)；（Level1）
e) 服务启停及端口修改；（Level1）
f) 管理网络配置(IP 地址/掩码/网关、DNS 服务器)；（Level1）
g) 系统启动项配置(系统启动设备、是否单次生效)；（Level1）

h) 查看当前健康事件/历史事件/系统健康状态、清除事件；（Level1）
i) 远程虚拟媒体及配置(属性查看、挂载、断开)；（Level2）
j) 远程 KVM；（Level2）
k) NTP 配置/时区配置；（Level1）
l) LDAP 配置；（Level2）
m) 温度、电压查询；（Level1）
n) 电源控制(上下电、重启)；（Level2）
o) 查看整机系统信息(资产标签/产品名称/产品序列号等)；（Level1）
p) 查看 CPU/内存信息；（Level1）
q) 查看系统电源、风扇信息；（Level1）
r) 查看网卡及网口信息；（Level1）
s) SNMP TRAP 配置；（Level1）
t) E-mail 上报配置；（Level2）
u) BMC 和 BIOS 配置；
v) 功率封顶配置；（Level3）
w) 证书管理(查看、CSR 生成和导出、证书/证书链导入)；（Level2）
x) 电源主备配置。（Level2）

8.5 管理网口

管理网口的要求包括：
a) 应支持专用管理网口或边带共享网口，通过该网口可以对 BMC 进行远程管理；（Level1）
b) 管理网口应支持 VLAN、IPv4；（Level1）
c) 管理网口应支持静态 IP 模式；（Level1）
d) 应支持 DDNS；（Level3）
e) 可支持专用/边带网口自适应，根据网口 link 状态，自动将逻辑网口与其中一个物理网口适配；（Level3）
f) 管理网口应支持 IPv6；（Level2）
g) 管理网口应支持 DHCP 模式。（Level2）

9 安全

9.1 口令安全

口令安全的要求包括：
a) 应支持密码复杂度检查，密码复杂度要求：长度要求至少为 8 位字符；字符类型要求包含数字、小写字母、大写字母、标点符号、特殊符号中的至少两类；口令不能和账号一样；（Level1）
b) 应支持禁用历史密码，设置的新密码不允许和保留的历史密码相同；（Level1）
c) 应支持用户配置密码有效期时间，密码到达有效期后，系统会提示用户修改密码；（Level2）
d) 应支持管理密码最短使用期,防止频繁修改密码而重复使用历史密码,确保密码安全;(Level2)
e) 应支持账号防暴力破解；（Level1）
f) 应保证用户身份标识具有唯一性；（Level1）
g) 应禁止预留任何的未公开账号，所有账号都必须可被系统管理，并在资料中提供所有账号及管理操作说明。（Level1）

9.2 认证管理

认证管理的要求包括：

a) 应支持公钥认证，SSH 支持用户名、密码和公钥方式认证；（Level1）
b) 应支持二次认证，对于重要的管理操作，如用户配置、权限配置、公钥导入会对已登录用户进行二次认证，认证通过后才能执行重要操作，防止用户登录后没有断开链接，被其它非法用户执行恶意操作；（Level1）
c) 支持通过目录服务进行远程认证。（Level1）

9.3 授权管理

授权管理的要求包括：

a) 应支持本地用户管理，分为管理员，操作员，普通用户，为不同用户分配不同权限；（Level1）
b) 应支持自定义用户权限。（Level1）

9.4 证书管理

证书管理的要求包括：

a) 应支持证书的查看；（Level1）
b) 应支持证书导入；（Level1）
c) 应支持证书有效期检测；（Level2）
d) 应支持证书吊销检测（level3）。

9.5 会话管理

会话管理的要求包括：

a) 应支持会话有效期检测；（Level1）
b) 应支持自动会话注销；（Level1）
c) 应支持手动会话注销。（Level2）

9.6 安全协议

安全协议的要求包括：

a) 应默认使用安全的通信协议，包括 SFTP、SSH、HTTPS、SNMPv3、RMCP+(IPMILAN)；（Level1）
b) 应默认关闭不安全协议，打开时需要提示安全风险。（Level1）

9.7 数据保护

数据保护的要求包括：

a) 应支持敏感数据(包括密码、证书、密钥)加密保存，防止敏感信息泄露；（Level1）
b) 应支持备份数据的完整性保护和权限控制，防止未经授权的访问；（Level1）
c) 应支持数据备份恢复机制，防止系统异常掉电导致的数据文件丢失。（Level2）

9.8 访问策略

访问策略的要求包括：

a) 支持登录规则限制，基于时间段、IP、MAC 的访问控制策略，通过配置登入时间段、登入 IP 网段、登入 MAC 地址白名单；（Level2）
b) 支持客户配制安全警示信息；（Level3）
c) 支持带外管理系统锁定功能，系统锁定功能开启后，系统中的用户配置、常规配置、虚拟控制台配置、安全配置都处于锁定状态不能配置。（Level2）

9.9 日志审计

日志审计的要求包括：
a) 日志信息中应包含用户名、用户 IP 地址、操作时间、操作内容等信息；（Level1）
b) 应支持日志转储，防止本地日志满后被覆盖丢失；（Level1）
c) 应支持对日志转储服务器进行验证。（Level2）

9.10 固件韧性

固件韧性的要求包括：
a) 支持 BMC 固件自动恢复机制,在检测到固件被篡改后,可以采取相应的自动恢复措施;(Level2)
b) 基于物理可信根，对待启动的 BIOS 和 BMC 固件进行签名校验，保证关键固件的完整性和真实性；（Level3）
c) 基于物理可信根，对待升级的 BIOS 和 BMC 固件进行签名校验，校验通过后才能执行升级操作；（Level3）
d) 基于物理可信根，对待恢复的 BIOS 和 BMC 固件进行签名校验，校验通过后才能执行恢复操作。（Level3）

10 性能

10.1 Web GUI 加载时间

Web GUI采用BMC端口直连，加载时间低于5s。（Level2）

10.2 BMC 快速启动时间

BMC启动时间不超过180s，实现功能包括网络、IPMI、散热、传感器服务可用。（Level3）

参 考 文 献

[1] Arm Server Base Boot Requirements 1.2, Platform Design Document, arm, 2019年9月