NHJC-05-2018

重点用能单位能耗在线监测系统技术规范

第 5 部分 省级平台机房与硬件配置规范

（试行）

2018 年 5 月发布

目 次

前　言

为贯彻落实《国家发展改革委 质检总局关于印发重点用能单位能耗在线监测系统推广建设工作方案的通知》（发改环资〔2017〕1711 号），规范和指导重点用能单位能耗在线监测系统建设，按照统一标准、互联互通、信息共享的建设原则，特制定《重点用能单位能耗在线监测系统技术规范》。

本部分为《重点用能单位能耗在线监测系统技术规范》的第 5 部分。

本部分参照 GB/T1.1-2009 给出的规则起草。

本部分起草指导单位为国家发展改革委环资司、市场监管总局计量司。

本部分主要起草单位：国家节能中心、中通服咨询设计研究院有限公司、国家信息中心、太极计算机有限公司、北京节能环保中心、浙江省能源监察总队、云南省计量测试技术研究院、湖北万洲电气集团有限公司。

重点用能单位能耗在线监测系统技术规范

第 5 部分 省级平台机房与硬件配置规范

1 适用范围

本规范中规定了省级平台机房、服务器、存储、网络硬件的配置标准及性能参数等内容，各级节能主管部门、质监部门建设省级平台时，可遵循本规范的相关要求

本规范用于指导不具备使用政务云资源条件的地方自建机房环境及硬件资源开展能耗在线监测系统建设。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本适用于本文件：

GB 50174 电子信息系统机房设计规范

GB/T 2887 电子计算机场地通用规范

GB 9361 电子计算站场地安全要求

GB 6650 电子计算机机房用活动地板技术条件

SJ/T 30003 电子计算机机房施工及验收规范

GB 50052 供配电系统设计规范

GB 50054 低压配电设计规范

GB 14050 系统接地的形式及安全技术要求

JGJ/T 16 民用建筑电气设计规范

GB 50311 综合布线系统工程设计规范

YD/T 1099 以太网交换机技术要求

3 机房建设要求

省级平台机房建设应满足等保二级要求，参照《电子信息系统机房设计规范》及相关规范及标准建设。机房电气、环境、空调、消防、安防等配套设施参照 B 级机房要求建设。

机房关键设备按冗余要求配置，在设备冗余能力范围内，不会因为设备故障和维护需要，而导致数据中心信息系统运行中断。机房基本参数列举如下：

1) 供配电系统：N+1；

2) 机房环境温度：18~27℃（冷通道）；

3) 机房湿度：35%~60%；

4) 空调制冷系统：N+1；

5) 接地：采用联合接地系统，接地电阻<1Ω；

6) 安保系统：设置视频监控及出入口控制系统；

7) 机房设洁净气体灭火系统；

8) 零地电压小于 2V。

4 服务器配置要求

1) 服务器应选用当前国内先进的、主流的机型，要具有较高的性能价格比，同时系统必须符合标准化，开放式系统互连的原则，易于开发维护，还要具有较强的网络通信和数据库管理功能和较强的扩充能力；

2) 服务器支持 SMP 对称多处理方式和 Cluster 方式；

3) 服务器的设计必须确保其高效、可靠及安全性(如带 ECC 校验，对数据的奇偶校验，热切换等)，同时又能大大简化维护工作；

4) 服务器要具有良好的性能，具有较高的 TPS 值；

5) 服务器在设计上最好采用模块化及通用件设计，易于扩充，以胜任网络及应用的扩展；

6) 服务器厂商具有良好的售后服务和技术支持；

7) 虚拟化宿主机每台服务器内存应不低于 128G，CPU 不低于 2 颗，每颗 CPU 不少于 6 核。

5 存储配置要求

1) 存储阵列控制器，需配置 RISC 架构双活控制器，需具有独立的 RAID 校验芯片；

2) 前端主机接口，配置≥8 个 16Gb/s FC 端口，支持扩展≥4 个 1Gb 的 iSCSI 端口；

3) 磁盘列阵配置容量应满足监测数据需求及未来 10 年内的扩展性要求。

4) 磁盘扩展能力，最大可扩展磁盘数量 ≥110 块；

5) RAID 级别支持，支持 RAID 0/ 1/ 1+0/ 3/ 5/ 6；

6) 支持磁盘类型，支持 SAS，NL_SAS 及 SSD（固态硬盘）等类型；

7) 需配置后备锂电池，支持 BBU、flash、控制器缓存镜像等三重数据保护；

8) 需支持后台介质扫描、RAID 级别在线迁移、LUN 在线扩容，需支持卷快照、卷复制、卷远程镜像功能，需支持自动精简功能；

9) 需配置相应数量的路径冗余软件，并支持 I/O 通道故障切换和链路负载均衡

（Windows/Linux）；

10) 需配置冗余电源,风扇；

11) 需支持 Windows、Linux、UNIX 等操作系统。

6 网络配置要求

交换机、防火墙不为同一品牌。所有需要的设备均应从设备性能、可靠性、协议、安全性、服务质量、易管理性、可扩展性等方面考虑。

6.1 DMZ 区-接入交换机

1) 支持堆叠的三层交换机，全部端口支持千兆，支持 10GE 扩展模块；

2) 整机 10/100/1000M 电接口≥48，10GE 光纤接口≥2；

3) 单台支持可扩展插槽≥1 个，扩展模块支持在线热拔插；

4) 交换容量不低于 160Gbps；

5) 转发性能不低于 120Mpps，要求实现端口全线速交换转发；

6) MAC 地址表不低于 32K，支持 MAC 地址自动学习和老化；

7) 支持 4K 个 VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN；

8) 支持静态路由、RIP V1/2、OSPF、IS-IS、BGP；

9) 双电源，可插拔，交流供电；

10) 端口配置：48 个 10/100/1000BASE-T 端口。

6.2 核心业务区-核心交换机

1) 要求为框式交换机，业务插槽不少于 3 个；

2) 交换容量不低于 540Gbps；

3) 转发性能不低于 360Mpps，要求实现端口全线速交换转发；

4) 支持 VLAN 交换，支持 QinQ、增强型灵活 QinQ；

5) 支持 MAC 地址自动学习和老化；

6) 支持 RIP、OSPF、ISIS、BGP 等 Ipv4 动态路由协议；

7) 支持 RIPng、OSPFv3、ISISv6、BGP4+等 Ipv6 动态路由协议；

8) 支持组播、MPLS、QoS 功能；

9) 一体化总装机箱,双主控板,双交流电源；

10) 端口配置：48 个 GE 电口。

6.3 核心业务区-接入交换机

1) 支持堆叠的三层交换机，全部端口支持千兆，支持 10GE 扩展模块整机；

2) 10/100/1000M 电接口≥48，10GE 光纤接口≥2；

3) 单台支持可扩展插槽≥1个，扩展模块支持在线热拔插交换容量不低于 160Gbps 转发性能不低于120Mpps，要求实现端口全线速交换转发 MAC 地址表不低于 32K；

4) 支持 MAC 地址自动学习和老化；

5) 支持 4K 个 VLAN；

6) 支持基于 MAC/协议/IP 子网/策略/端口的 VLAN 支持静态路由、RIP V1/2、OSPF、IS-IS、BGP 双电源，可插拔，交流供电；

7) 端口配置：48 个 10/100/1000BASE-T 端口。

7 安全设备配置要求

不同种类安全设备不采用同一厂家产品。

7.1 防火墙

1) 百兆防火墙，采用专用设计的硬件平台，支持冗余电源；

2) 每秒新建会话能力不少于 35k；

3) 最大并发连接数不少于 30 万；

4) 最大吞吐量不低于 4G；

5) 最大 IPS 吞吐量不少于 1G；

6) 最大访问控制策略不少于 20000 条；

7) 具有访问控制，IPS 防护，应用层攻击保护功能；

8) 支持远程管理，维护。

9) 要求设备配置 6 个千兆电接口；

10) 配置内存>=2GB。

7.2 堡垒主机

1) 含单交流电源，2*USB 接口，1*RJ45 串口，1*GE 管理口，4*GE 电口，不小于 2T SATA 硬盘。缺省授权管理 100 台设备；

2) 支持证书、口令、短信、动态字符等多种认证方式，可基于角色和安全等级的动态授权；

3) 支持虚拟网关和虚拟防火墙；

4) 可支持不少于 500 个并发用户。

7.3 网络安全审计系统

1) 含交流冗余电源，标准配置提供一路监听，支持对未注册的用户终端实施自动阻断

网络的功能；

2) 支持对用户的进程审计、服务审计、主机资源审计、主机端口审计、主机账号审计、主机文件操作审计；

3) 支持客户端媒体介质控制，并进行日志记录与审计；

4) 支持客户端 IP 与 MAC 绑定控制管理；

5) 支持吞吐量≥1.0Gbps；

6) 并发会话数≥80 万；

7) 并发用户数≥2000；

8) 设备接口≥4 个千兆电口；

9) 磁盘容量不小于 500G。

7.4 漏洞扫描

1) 含交流单电源，1*RJ45 串口，1*GE 管理口，4 个 10M/100M/1000M 自适应以太网电口扫描口，标准配置提供 1 路授权扫描端口，IP 点授权，授权可扫描总数量不多于 512 个无限制范围的 IP 地址或域名，支持能对扫描目标的安全脆弱性进行全面检查，检查内容包括缺少的安全补丁、暴露的危害信息、不安全的服务配置等；

2) 漏洞库的数量应不低于 2000 条，支持国际 CVE 标准；应支持对主流数据库包括：Sybase、SQLServer、Oracle、MySql、DB2 等的扫描检测功能；

3) 支持的最大并发扫描 IP 应不少于 30 个，单个 IP 的最大并发扫描线程应不少于 30 个，单个 IP 的平均扫描时间不大于 30 秒，扫描 IP 数量 500 以上。

7.5 入侵检测系统（IDS）

1) 百兆入侵检测系统，>4 个 10/100M 以太网口，1 个异步控制口；

2) 含交流冗余电源模块，2*USB 接口，1*RJ45 串口，2*GE 管理口；

3) 漏洞特征库能够自动或者手动升级；

4) IPS 防护对像包括了防护服务器和防护客户端两种，防护的类型包括了蠕虫、木马、后门、DoS、DDoS 攻击探测、扫描、间谍软件、利用漏洞的攻击、缓冲区溢出攻击、协议异常、 IPS 逃逸攻击等；IPS 能够对应用服务器信息进行隐藏，并且能够对服务器进行扫描，从而评估服务器对漏洞的防护能力。

7.6 安全认证网关

1) 支持基于 Linux、Windows 等操作系统的企业端设备 CA 数字证书的身份认证和传

输加密，满足国家信息中心的数字证书信任链验证及证书黑名单验证，符合相关接入要求。

2) 最大并发连接数 400；

3) 最大新建连接数 60 次/秒；每秒完成交易数(TPS)1000 次/秒；

4) 最大流量不小于 50Mbps；

5) 系统可以设置是否需要用户提交用户证书；

6) 系统可以自动、动态更新黑名单，不需要重新启动服务，支持 LDAP、HTTP 等多种方式更新，支持 B64、DER 等多种格式；

7) 系统可以拥有多个站点证书，不同的服务可以拥有不同的站点证书；

8) 一个 SSL 服务中可同时配置多条证书链，验证不同 CA 的用户证书；

9) 要求支持主流数字证书认证体系，并支持接入国家电子政务外网信息体系中；

10) 系统可以将用户证书信息包括扩展项信息传送给应用系统；

11) 支持 B/S 应用；支持 FTP、telnet、远程桌面以及通用的 C/S 应用，系统可以创建多个 SSL 服务，保护不同的应用服务，也可以采用同一个 SSL 服务保护多个应用服务（需客户端）；

12) 系统将真正应用服务的地址隐藏，用户仅知道网关地址；

13) 在有防火墙 NAT 映射的情况下正常访问有重定向的网站；

14) 可以独自完成基于数字证书的身份认证；

15) 国密算法支持：支持 RSA1024 及 2048 位算法；支持商用密码非对称算法 SM2；支持商用密码杂凑算法 SM3；支持商用密码对称算法 SM4；支持扩展国密对称加密算法 SM1；

16) 能够提供浏览、下载等日志管理功能，且可与第三方审计系统进行关联功能；

17) 支持串联、并联等多种部署方式，适用不同的网络环境和应用需求；

18) 拥有公安部销售许可证。

7.7 WEB 防火墙（WAF ）设备

1) 标准配置含 SQL 注入/XSS 防护、WEB 常规攻击防护、扫描防护、Cookie 安全防护、URL ACL、CSRF 防护、HTTP 协议防护、ARP 欺骗防护、非法下载防护、非法上传防护、Web 内容安全防护、网页盗链、爬虫防护等功能。

2) 提供网页篡改防护以及服务器侧恶意代码过滤功能。

3) 含交流单电源，1*RS232 串口，1*FE 管理口，4*100/1000M 自适应电口（Bypass）

标准配置提供 1 路电口 WAF 防护，支持 BYPASS。

7.8 VPN 网关

SSLVPN 与 IPSECVPN 均可以实现由互联网企业监测端到系统平台服务端的加密访问，实现证书的验证和传输加密，下面提供两类产品的要求及参数：

（1）SSLVPN：

1) SSLVPN 支持基于 CA 数字证书，实现互联网企业监测端到系统平台服务端的身份验证和加密通信。
2) SSLVPN 要求支持互联网企业监测端到系统平台服务端的传输加密；
3) SSLVPN 支持第三方数字证书认证，支持硬件加速，提供 C\S 应用支持；
4) 最大并发连接数≥400；
5) SSL VPN 并发客户端数≥2000；
6) 系统能够对用户连接数、应用访问情况，系统资源占用等信息进行详细统计，为更好了解应用及调节资源提供基础；
7) 系统实现客户端策略的统一下发，用户无需对客户端进行任何配置；
8) 对于特定应用，系统采用用户映射技术，将证书映射为原有系统中的账户，并进行自动登录，在后台应用无需修改的情况下实现单点登录；
9) 系统通过特有的 cookie 技术将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息；
10) 系统支持国密 SM1/SM2/SM3 算法，
11) 实现 URL 级别的访问控制，对于不同用户、不同角色实现不同的控制；
12) 支持单点登录功能（SSO）。

（2）IPSECVPN：

1）支持基于 CA 数字证书，实现互联网企业监测端到系统平台服务端的身份验证加密通信。

2）IPSec 支持第三方数字证书认证，支持硬件加速，提供 C\S 应用支持；

3）IPSec VPN 加密速度≥280Mbps；

4）IPSec VPN 隧道数≥2000；

5）IPSec VPN 并发客户端数≥2000；

6）支持虚拟化远程应用发布；

7）支持单点登录功能（SSO）；

8）系统对于认证错误可以重定向到用户指定页面，增强友好性

7.9 数据库安全审计系统

1) 电源硬件冗余，配置双交流电源；
2) 性能指标，检测能力≥1000Mbps；
3) 最大并发 TCP 连接数≥100 万；
4) 每秒新增 TCP 并发连接数≥30 万；
5) 支持对不少于 2000 在线用户进行审计；
6) 端口配置≥4 个 10/100/1000M 电口；
7) ≥4 个千兆光口（SFP）；
8) 系统要求，模块化设计，具有良好的可扩展性；
9) 旁路方式或透明方式接入网络；
10) 审计引擎支持不同的操作系统类型（Windows、Linux、Unix 等）；
11) 支持同时审计多种数据库及跨多种数据库平台操作；支持审计 ORALCE、SQL SERVER、MY SQL、DB2、Sybase、Postpresql 等各类主流数据库系；
12) 系统应支持基于 IP 地址、时间、用户/用户组、数据库用户名、数据库类型、数据库表名、字段名、关键字等组合数据库审计策略；
13) 应支持实时审计用户对数据库系统所有操作，如：登录、注销、插入、删除、执行存储过程、用户自定义操作等，支持分析、提取 SQL 语句中绑定变量，并可完全监测还原 SQL 操作语句包括源 IP 地址、目的 IP 地址、访问时间、MAC 地址、数据库用户名、客户端类型、数据库操作类型、数据库表名、字段名等；
14) 支持对邮件系统的审计，支持 SMTP、POP3、WEBMAIL 等协议，支持基于邮箱地址、邮件主题、邮件内容、附件名的关键字审计功能；
15) 日志管理，支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询；
16) 支持日志自动备份；
17) 支持日志归并；
18) 具备分级管理功能，满足分级管理的要求；
19) 支持对审计数据的多种查询方式；
20) 提供多种形式的审计报表，数据格式报表可以保存为 EXCEL、文本、WORD、HTML 等多种格式；

21) 具备对外接口，可将审计结果上报给安全管理平台或其它安全产品。