NECC-NHJC-05-2014

重点用能单位能耗在线监测系统
省级节点机房与硬件配置规范
（试行）

国家节能中心

2014 年 8 月发布

前　言

为贯彻落实国务院《“十二五”节能减排规划》（国发[2012]40 号）和《2014-2015 年节能减排低碳发展行动方案》（国办发[2014]23 号）的有关要求，指导重点用能单位能耗在线监测系统建设，国家节能中心组织制定了重点用能单位能耗在线监测总体架构规范、基础数据定义规范、国家节点与省级节点通信规范、能耗监测端设备与系统平台通信规范、省级节点机房与硬件配置规范、能耗监测端设备功能规范、能源品种数据采集规范、系统安全规范等 8 项技术规范（试行），以及部分行业能耗在线监测数据采集技术指南（试行）。本规范主要用于指导重点用能单位能耗在线监测系统省级数据中心建设工作，规范省级节点电子信息系统硬件的建设标准，确保电子信息系统设备安全、可靠地运行，做到技术先进、经济合理、安全适用、节能环保。

本指南主要起草单位：国家节能中心、中国电子工程设计院。参加起草单位：煤炭工业太原设计研究院。

本指南由国家节能中心发布，自 2014 年 8 月 1 日起试行。

目 录

1 适用范围 1
2 规范性引用文件 1
3 机房建设要求 1
4 服务器配置要求 2
5 存储配置要求 2
6 网络配置要求 2
6.1 DMZ 区-接入交换机 3
6.2 核心业务区-核心交换机 3
6.3 核心业务区-接入交换机 3
7 安全设备配置要求 4
7.1 防火墙 4
7.2 堡垒主机 4
7.3 网络安全审计系统 4
7.4 漏洞扫描 5
7.5 入侵检测系统（IDS） 5
7.6 身份认证网关 5
7.7 WEB 防火墙（WAF ）设备 6
7.8 SSL VPN 网关 6

重点用能单位能耗在线监测系统
省级节点机房与硬件配置规范
（试行）

1 适用范围

本规范规定了省级数据中心服务器、存储、网络硬件的配置标准及性能参数等几方面内容，适用于重点用能单位能耗在线监测系统中省级数据中心机房电子信息系统服务器、存储、网络硬件建设。

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

省级节点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》(GB50174-2008)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际上先进的、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 8Gb/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、防火墙宜为同一品牌。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

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。

8) 要求设备配置 6 个千兆电接口；

9) 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，模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 身份认证网关

1) 最大并发连接数 400；

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

3) 最大流量不小于 50Mbps；

4) 系统可以设置是否需要用户提交用户证书；

5) 系统可以自动更新黑名单、动态更新，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；

6) 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；

7) 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；

8) 支持格尔、CFCA、SHECA 及多数省级 CA 中心数字证书；

9) 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；

10) 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）；

11) 系统将真正应用服务的地址隐藏，用户仅知道网关地址；

12) 在有防火墙 NAT 映射的情况下正常访问有重定向的网站；

13) 不少于 4*GE 电口。

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 SSL VPN 网关

1) SSL/IPSec 一体化设备，支持第三方数字证书认证，支持硬件加速，能够同时运行 SSL 和 IPSec 两种 VPN 业务，提供 C\S 应用支持；

2) 支持 SSL VPN 加密速度≥200Mbps；

3) SSL VPN 并发用户数≥800；

4) SSL VPN 每秒新建用户数≥90；

5) IPSec VPN 加密速度≥280Mbps；

6) IPSec VPN 隧道数≥4000；

7) IPSec VPN 并发客户端数≥4000；

8) 支持虚拟化远程应用发布

9) 支持单点登录功能（SSO）；

10) 网络接口≥4 个千兆电口。