[报价文件]

项目名称：温州理工学院信息化建设设备采购项目

项目编号：WZHC-20220615

投标文件

投标人全称：（公章或 CA 章）浙江怡联网络科技股份有限公司

时　　间：2022 年 08 月 01 日

http://www.yilian.com.cn
联系人：吴欣
Zhejiang Yilian Network Technology Co.,Ltd
Email：1090683177@qq.com
Tel：0577-56555317　Mobile：18072197909
ADD：温州市车站大道金鳞花苑二幢七楼

目 录

第一章 报价一览表

项目编号： WZHC-20220615 标段：标项一温州理工学院信息化建设设备采购项目

（价格单位：人民币元）

项目名称	完工期（日历天）	项目负责人	备注
温州理工学院信息化建设设备采购项目	服务期限为 30 日历天	潘奕	无
总价（大写）： （小写）：￥	贰佰壹拾陆万玖仟贰佰壹拾元整 2169210.00		

附注：1. **▲此栏内总价应与“分项报价表”中合计总价相一致。**

2. **▲此表不得自行增减内容，不提供此表格将被视为没有满足招标文件的实质性要求**。

3. **▲本次报价包含运输、安装、辅材、调试、税等相关费用，报价时因充分考虑材料变化，如有增加则视为对采购人的优惠，后期金额不做调整，此项目为交钥匙工程。**

投标人全称（公章或 CA 章）：浙江怡联网络科技股份有限公司

日期： 2022 年 08 月 01 日

第二章 分项报价表

项目编号： WZHC-20220615 标段：标项一温州理工学院信息化建设设备采购项目

（价格单位：人民币元）

序号	产品名称	品牌	规格型号	单位及数量	性能及指标	产地	单价
1	24 口千兆交换机	H3C	MS4024P-HPWR-EITC	16 台	完全响应招标文件	杭州	3800
2	汇聚交换机	H3C	LS-5500V2-34S-EITC	3 台	完全响应招标文件	杭州	18000
3	汇聚交换机	H3C	LS-5120V2-28P-LITC	1 台	完全响应招标文件	杭州	6800
4	光模块	H3C	SFP-XG-LX-SM1310-D	4 个	完全响应招标文件	杭州	1000
5	千兆光纤收发器	海康威视	DS-5D301R/T-3E(SC)	16 个	完全响应招标文件	杭州	485
6	高清解码器	海康威视	DS-6916TC-YSD	3 台	完全响应招标文件	杭州	26000
7	机柜	星弘达	HG6612	3 套	完全响应招标文件	浙江	2950
8	核心交换机	H3C	S7506X	2 台	完全响应招标文件	杭州	110000
9	48 口楼宇接入交换机	H3C	S5130S-52S-EI	20 台	完全响应招标文件	杭州	4800
10	24 口楼宇接入交换机	H3C	S5130S-28S-EI	60 台	完全响应招标文件	杭州	3200
11	24 口 POE 交换机	H3C	S5130S-28S-PWR-EI	60 台	完全响应招标文件	杭州	4500
12	48 口 POE 交换机	H3C	E552C-X-PWR	25 台	完全响应招标文件	杭州	7000
13	AC 无线控制器（含 1024 授权）	H3C	WX5540X	1 台	完全响应招标文件	杭州	140000
14	光模块	H3C	SFP-XG-LX-SM1310-D	60 块	完全响应招标文件	杭州	1000
15	云桌面 VDI 授权（1 套/130 个授权）	深信服	深信服 VDI 授权	1 套	完全响应招标文件	深圳	208000
16	云桌面瘦终端	深信服	aDesk-STD-320(VGA+HDMI)	20 个	完全响应招标文件	深圳	1750

17	Web 应用防火墙	安恒	WAF-2600AG	1 台	完全响应招标文件	杭州	288000
18	数据库审计与风险控制系统	安恒	DAS-A1800	1 台	完全响应招标文件	杭州	265000
设备总价			2169210.00				
运杂及保险费（含卸货）			含				
安装调试费（包括设备的测试、调试、验收等费用）			含				
培训费			含				
售后服务			含				
税金			含				
其他相关费用			含				
合计总价（应与报价一览表中总价相一致）			2169210.00				

附注：1. **▲不提供分项报价表将视为没有实质性响应投标文件。货物名称按设备清单内容。**

2. **▲此表的合计总价应与附件二“报价一览表”总价相一致。**

3. 如果免费请在该备注栏内注明“免”，如果含在产品价格中则填“含”，如无此项内容则填“无”，不留空白。

4. “设备总价”不应包含：运杂及保险费及其他相关费用。

5. **根据《中华人民共和国政府采购法实施条例 》第四十三条规定，在中标或者成交公告的内容中公开本表，请各投标人认真填写，确保报价数据的真实性、完整性和合理性。**

投标人全称（公章）：浙江怡联网络科技股份有限公司

法定代表人或授权代表（签字或盖章）：

日期：2022 年 08 月 01 日

附：详细配置

序号	设备名称	参数要求	
1	24 口千兆交换机【H3C、MS4024P-HPWR-EITC】	24 个 10/100/1000Base-T 电口;2 个 1000Base-X SFP 端口;转发能力:38.7Mpps;交换容量:52Gbps;支持 PoE+;双风扇	
2	汇聚交换机【H3C、LS-5500V2-34S-EITC】	交换容量 598Gbps；转发性能 216Mpps；性能指标 MAC 地址表 32K；路由表容量 32K；24 个 GE 端口，4 个万兆 SFP+口，2 个 40G QSFP+口，所有端口均固化，万兆端口支持千兆自适应；最大堆叠台数 9 台；最大堆叠带宽 60G；可要求堆叠带宽 80G，并要求实配接口的基础额外满配堆叠带宽所需的接口和互联模块；支持跨设备链路聚合，单一 IP 管理，分布式弹性路由；支持通过标准以太端口进行堆叠；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预；支持远程堆叠；VLAN 特性 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN；提供配套的 SDN controller。	
3	汇聚交换机【H3C、LS-5120V2-28P-LITC】	24 个 10/100/1000TX+4 个 SFP;转发能力:51Mpps;交换容量:336Gbps	
4	光模块【H3C、SFP-XG-LX-SM1310-D】	原厂千兆单模光模块	
5	千兆光纤收发器【海康威视、DS-5D301R/T-3E(SC)】	接口数量：2 个；接口类型：1 个 10/100/1000Mbps 的自适应 RJ45 口，1 个 1000Mbps 的 SC 光纤口；供电电源：5VDC，0.6A；功耗：3W；电源输入：220VAC，50Hz，0.3A；RJ45 端口防雷：6 kV；光纤类型：单模光纤；传输距离：3 km；工作波长：发送：1310nm，接收：1550nm。	
6	高清解码器【海康威视、DS-6916TC-YSD】	高清视音频解码器，嵌入式架构，专用 Linux 系统，使用 DSP 解码。为了设备稳定可靠运行，不得采用工控机或者 PC 机的 X86 架构。支持 YUV422 上墙显示；输出接口：支持 8 路 HDMI 和 4 路 BNC 输出，HDMI（可以转 DVI-D）（奇数口）输出分辨率最高支持 4K（3840*2160@30HZ）编码格式：支持 H.265、H.264、MPEG4、MJPEG 等主流的编码格式；封装格式：支持 PS、RTP、TS、ES 等主流的封装格式；音频解码：支持 G.722、G.711A、G.726、G.711U、MPEG2-L2、AAC 音频格式的解码；解码能力：支持 8 路 1200W，或 16 路 800W，或 24 路 500W，或 40 路 300W，或 64 路 1080P 及以下分辨率同时实时解码；画面分割：支持 1、2、4、6、8、9、10、12、16、25、36 画面分割显示。网络接口：2 光口，2 电口；支持黑白名单功能，可设置 256 个黑白名单；当设置白名单时，只允许白名单 IP 访问设备；当设置黑名单时，黑名单内 IP 无法访问设备。音频接口：支持 8 路音频输出，1 路对讲输入，1 路对讲输出；串行接口：一个标准 232 接口（RJ45）、一个标准 485 接口；报警接口：8 路报警输入，8 路报警输出。	
7	机柜【星弘达、HG6612】	壁挂 12U 机柜，600*440*635mm（宽深高），符合 GB/T3047.2-92 标准，采用 SPCC 冷轧钢板制作，承重额定静载 1000kg，表面处理采用脱脂、水洗、磷化、喷涂（含 PDU 电源、模块等）	
8	核心交换机【H3C、S7506X】	功能及技术指标	参数要求
		设备性能	交换容量 336Tbps、包转发率 57600Mpps，提供官网清晰截图证明；
		槽位数量	支持业务槽位数量 6；
		关键部件热插拔	主控交换卡、电源、接口模块、风扇等关键部件可热插拔
		★接口要求	单槽位可提供 24 端口 1G/2.5G/5G/10G 自适应以太网电接口，提供产品官网选配信息截图证明；

			支持 40G 跟 100G 端口切换，切换后流量正常转发，无丢包
			单槽位可提供 40G 端口密度 24，100G 端口密度 4，提供产品官网选配信息截图证明；
			支持 10G EPON 功能，支持 10G 对称和非对称 ONU
		Qos	每端口支持 8 个优先级队列，3 个丢弃优先级，支持 SP、WRR、SP+WRR 三种队列调度算法，支持精细化的流量监管，粒度可达 8K，支持流量整形 Shapping，支持 WRED 拥塞避免
			支持 802.1p、TOS、DSCP、EXP 优先级映射
			支持 HQoS（支持五级 HQoS 调度）
		可靠性	双引擎快速倒换，主备切换时候板内转发无丢包
		IPv6	支持RIPng、OSPFv3、BGP4+、IS-ISv6协议 支持IPv6策略路由； 支持DHCPv6功能、IPv6 portal功能、IPv6管理功能； 支持基于IPv6的VXLAN二三层互通； 支持基于IPv6的VRRP功能
		★虚拟化技术	支持多虚一技术(N:1)，支持 4 框虚拟化技术：可将 4 台物理设备虚拟化，实现流量负载分担功能；支持一虚多技术（1:N）；支持多虚一技术和一虚多技术的配合使用；（提供第三方权威检测报告证明）
			支持二级 PE 端口扩展设备级联：CB（Controlling Bridge）控制设备能够支持二级 PE（Port Extender）端口扩展设备级联，即一级 PE 端口扩展设备下挂二级 PE 端口扩展设备，虚拟化后的设备支持基于 IPv4\IPv6 的 VXLAN 的二三层互通；
			支持基于IRF3.1的有线无线统一管理功能
		★网络安全一体化	支持扩展硬件防火墙业务板、IPS 入侵防御系统业务板、负载均衡业务板、应用控制网关业务板、SSL VPN 业务板、EPON 业务板，提供生产厂商官网选配信息截图；
		可视化功能	支持 Telemetry 流量可视化功能
		无线功能	支持融合 AC 功能：无需额外配置单独硬件，能再交换机上对所有上线的 AP 进行管理与配置
			支持有线无线一体化的终端准入认证
		智能网管功能	内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级，无需配置额外网管平台
		终端管理及网络安全	支持融合终端安全管理板卡，实现对摄像头等物联终端统一识别、认证和管理 支持 PC 终端、哑终端、网络设备等连接元素的准入控制和权限划分，确保网络的可信可控 支持设备识别、归类、类型定义，可以对全网资产进行梳理，识别异常终端链接，确保网络的安全性 提供官网清晰截图证明；
		多业务融合	支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 Windows Server 及 SDN 控制器，实现方案与设备一体化部署，提供官网清晰截图证明；
		★兼容性要求	要求本次所配置核心交换机满足无缝对接校园 SDN 控制器，作为控制器子节点，通过 SDN 控制器实现全流程自动化、故障替换即插即用、用户移动，

			地址和权限动态跟随、配置自动下发等功能，需提供相关兼容性证明材料。
		配置要求	配置主控引擎模块 2，满足 1+1 冗余；配置 650W 冗余电源，万兆光口 24（支持 VXLAN 功能）；
9	48 口楼宇接入交换机【H3C、S5130S-52S-EI】	功能及技术指标	参数要求
		设备性能	交换容量 432Gbps，转发性能 144Mpps，（以官网低指标为准，官网参数若标注为交换容量“A/B”，以 A/B 中更小值为准）；
		接口要求	48 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口；
		ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间 50ms
		路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3
		纵向虚拟化	连接到主设备就可以自动化上线，可以被管理设备统一管理，实现自动配置功能，要求提供权威机构颁发的第三方测试报告；
		★堆叠	支持 IRF 本地负载分担，流量可以均匀负载分担到各个堆叠链路；
			IRF 单点管理功能测试，可以通过任意一台设备的 Console 口对整个堆叠进行管理
			最大堆叠台数 9 台
			支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预；
			支持通过标准以太端口进行堆叠（万兆或千兆均支持）
		可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms
			支持 Smartlink，收敛时间 50m s
		SDN/OPENFLOW	支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换；
			支持多表流水线
			支持 Group table
			支持 Meter
		管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
			支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
		绿色节能	符合 IEEE 802.3az（EEE）节能标准
			端口定时 down 功能（Schedule job）
			支持端口休眠，关闭没有应用的端口，节省能源
		★兼容性要求	要求本次所配置接入交换机满足无缝对接校园 SDN 控制器，作为控制器子节点，通过 SDN 控制器实现开流程自动化、故障替换即插即用、用户移动，地址和权限动态跟随、配置自动下发等功能，需提供相关兼容性证明材料。
10	24 口楼宇接入交换机【H3C、S5130S-28S-EI】	功能及技术指标	参数要求
		设备性能	交换容量 336Gbps，转发性能 108Mpps，（以官网低指标为准，官网参数若标注为交换容量“A/B”，以 A/B 中更小值为准）；
		接口要求	24 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口；
		ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间 50ms
		路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3
		纵向虚拟化	连接到主设备就可以自动化上线，可以被管理设备统一管理，实现自动配

			置功能
		★堆叠	支持 IRF 本地负载分担，流量可以均匀负载分担到各个堆叠链路；
			IRF 单点管理功能测试，可以通过任意一台设备的 Console 口对整个堆叠进行管理
			最大堆叠台数 9 台
			支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预；
			支持通过标准以太端口进行堆叠（万兆或千兆均支持）
		可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms
			支持 Smartlink，收敛时间 50ms
		SDN/OPENFLOW	支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换；
			支持多表流水线
			支持 Group table
			支持 Meter
		管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
			支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
		绿色节能	符合 IEEE 802.3az（EEE）节能标准
			端口定时 down 功能（Schedule job）
			支持端口休眠，关闭没有应用的端口，节省能源
		★兼容性要求	要求本次所配置接入交换机满足无缝对接校园 SDN 控制器，作为控制器子节点，通过 SDN 控制器实现全流程自动化、故障替换即插即用、用户移动，地址和权限动态跟随、配置自动下发等功能，需提供相关兼容性证明材料。
11	24 口 POE 交换机【H3C、S5130S-28S-PWR-EI】	功能及技术指标	参数要求
		设备性能	交换容量 336Gbps，转发性能 108Mpps，（以官网低指标为准，官网参数若标注为交换容量“A/B”，以 A/B 中更小值为准）；
		接口要求	24 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口；
		POE 功能	支持 POE 供电功能，整机提供 170W POR 供电功率；
		ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间 50ms
		路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3
		纵向虚拟化	连接到主设备就可以自动化立线，可以被管理设备统一管理，实现自动配置功能，
		★堆叠	支持 IRF 本地负载分担，流量可以均匀负载分担到各个堆叠链路；
			IRF 单点管理功能测试，可以通过任意一台设备的 Console 口对整个堆叠进行管理
			最大堆叠台数 9 台
			支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预；
			支持通过标准以太端口进行堆叠（万兆或千兆均支持）
		可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms

			支持 Smartlink，收敛时间 50ms
		SDN/OPENFLOW	支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换；
			支持多表流水线
			支持 Group table
			支持 Meter
		管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
			支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
		绿色节能	符合 IEEE 802.3az（EEE）节能标准
			端口定时 down 功能（Schedule job）
			支持端口休眠，关闭没有应用的端口，节省能源
		★兼容性要求	要求本次所配置接入交换机满足无缝对接校园 SDN 控制器，作为控制器子节点，通过 SDN 控制器实现全流程自动化、故障替换即插即用、用户移动，地址和权限动态跟随、配置自动下发等功能，需提供相关兼容性证明材料。
12	48 口 POE 交换机【H3C、E552C-X-PWR】	功能及技术指标	参数要求
		设备性能	交换容量 432Gbps，转发性能 144Mpps，（以官网低指标为准，官网参数若标注为交换容量“A/B”，以 A/B 中更小值为准）；
		接口要求	48 个 10/100/1000Base-T 自适应以太网端口，4 个千兆 SFP 口；
		POE 功能	支持 POE 供电功能，整机提供 370W POR 供电功率；
		ERPS	实现 ERPS 功能，能够快速阻断环路，链路收敛时间 50ms
		路由协议	支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng、OSPF v3
		纵向虚拟化	连接到主设备就可以自动化上线，可以被管理设备统一管理，实现自动配置功能
		★堆叠	支持 IRF 本地负载分担，流量可以均匀负载分担到各个堆叠链路；
			IRF 单点管理功能测试，可以通过任意一台设备的 Console 口对整个堆叠进行管理
			最大堆叠台数>=9 台
			支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预；
			支持通过标准以太端口进行堆叠（万兆或千兆均支持）
		可靠性	支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms
			支持 Smartlink，收敛时间 50ms
		SDN/OPENFLOW	支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换；
			支持多表流水线
			支持 Group table
			支持 Meter
		管理和维护	支持 SNMP V1/V2/V3、RMON、SSHV2
			支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准
		绿色节能	符合 IEEE 802.3az（EEE）节能标准
			端口定时 down 功能（Schedule job）
			支持端口休眠，关闭没有应用的端口，节省能源

		★兼容性要求	要求本次所配置接入交换机满足无缝对接校园 SDN 控制器，作为控制器子节点，通过 SDN 控制器实现全流程自动化、故障替换即插即用、用户移动，地址和权限动态跟随、配置自动下发等功能，需提供相关兼容性证明材料。
13	AC 无线控制器（含 1024 授权）【H3C、WX5540X】	功能及技术指标	参数要求
		管理 AP 数	支持常规 AP 最大数量 5120，本次配置无线 AP 管理 License1024
		转发性能	要求所投产品数据转发性能 120Gbps，提供官网截图
		端口要求	要求所投产品提供 8 个千兆 GE 端口，8 个 SFP+端口，以及 2 个 QSFP+端口
		电源	支持双电源备份，并支持交流或直流两种供电方式。支持电源模块热插拔
		组网能力	支持标准 IETF 5415 CAPWAP 协议，AP 和 AC 之间支持 L2/L3 层网络拓扑，为提高网络安全，AP 与控制器之间能够支持 DTLS 对 CAPWAP 隧道进行加密处理
		认证加密	支持 MAC 地址认证、802.1x 认证（EAP-PAP、EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS）、Portal 认证、MAC+Portal 混合认证； 支持 WPA 标准、WEP(WEP64/WEP128)、TKIP、CCMP； 支持内置 portal、dot1x 服务器；
			支持 Private PSK 方式的动态密码功能，可以为每终端分配独立秘钥；
			支持防 PSK 暴力破解，当用户密码错误超过预设的阈值之后，能够将该用户加入动态黑名单，一段时间内禁止其接入网络，要求提供工信部或下属实验室出具的第三方测试报告
		无线漫游	支持 AC 内漫游，支持跨 AC 间漫游，支持跨 VLAN 的三层漫游
			支持基于 802.11k/802.11v/802.11r 协议的智能漫游
		可靠性	支持 IRF1+1 热备，对外呈现一个 IP 地址，简化网络拓扑；对外统一管理界面，简化运维；
			支持雷达检测 SSID 逃生功能：AC、AP 支持 SSID 自主逃生，当 AP 射频检测到雷达信号时，会将本射频的 SSID 迁移到其他射频，保障关键业务正常通信。要求提供工信部或下属实验室出具的第三方测试报告
		认证功能	支持 Portal 在线用户与 DHCP 租约联动功能：AC 支持根据 DHCP 租约信息联动 Portal 用户自动下线，可以提高 DHCP 地址池的利用率，降低 Portal 重复认证开销。
		IPv6 能力	为保障 IPV4 网络过渡到 IPV6 网络的安全性，设备需支持 IPV6 SAVI 功能。
			支持 AC 之间漫游同步 IPv6 SAVI 信息
			支持 RFC8106 在 IPv6 RA 报文选项中填充 DNS 相关信息
		无线网络优化	为实现 AC 的全面运维，所投产品需要支持：AC CPU、内存使用率以及历史信息，AC 整机广播、组播、单播流量成分以及历史信息，AC 仿真面板端口图以及每端口广播、组播、单播流量成分以及历史信息，同时可以识别最近一分钟端口入方向广播组播占比过高、最近一分钟端口流量过大等异常事件。
			为分析无线网络中 IP 地址的异常改变造成的上网体验差的原因，所投产品需要支持对异常终端的 IP 地址变更时间、MAC 地址、IP 地址、接入 SSID

			以及接入 AP 信息予以记录及显示，需要提供第三方报告证明
		★兼容性要求	要求本次所配置无线控制器满足无缝对接校园 SDN 控制器，作为控制器子节点，通过 SDN 控制器实现全流程自动化、故障替换即插即用、用户移动，地址和权限动态跟随、配置自动下发等功能，需提供相关兼容性证明材料。
14	光模块【H3C、SFP-XG-LX-SM1310-D】	功能及技术指标	参数要求
		万兆单模光模块	SFP+ 万兆模块(1310nm,10km,LC)
15	云桌面 VDI 授权（1 套/130 个授权）【深信服 VDI 授权】	功能项	功能要求说明
		配置要求	★本项目要求提供 1 套/130 个虚拟桌面用户授权，提供发布专有桌面、还原桌面、池化桌面、共享桌面、远程应用至少 5 种桌面资源的授权，满足不同场景的应用需求。本次平台要求具备管控原超融合虚拟化平台的能力，本次云桌面控制平台无需重新配置，通过原有控制平台数据同步即可实现配置同步。
		部署模式	为了简化部署，本项目要求桌面云控制平台所有组件完全集成化，不需要过多的安装调试步骤，后台导入一个镜像就可以完成部署，提升上线效率。
			桌面云控制平台自带高可用性技术方案，在不增加第三方负载均衡工具的情况下，支持集群（主主）模式，支持桌面云控制平台宕机切换会话不中断。
			★支持将桌面云控制平台直接映射到互联网，要求自带 SSL VPN 功能，不要借助第三方设备，并且能够用于固定 IP 线路和动态 IP 线路 2 种方式，其中动态 IP 不依赖第三方插件，降低部署复杂度。（需提供产品截图证明）
		用户体验	支持 PC、笔记本（含 Windows 操作系统和 MAC 笔记本）、云终端（含 ARM 和 X86）、iPad、iPhone、Android 移动终端等设备接入访问虚拟桌面。
			在多应用办公场景下，可针对当下使用频率较高的软件做进程加速，管理员也可自定义需做进程加速应用，以保障应用使用体验。
			支持 PC 磁盘映射，即 PC 本地硬盘可直接映射到虚拟桌面上使用，并可根据策略进行文件读写权限设置和数据读写审计。（需提供产品截图证明）
			为了提高桌面使用稳定性，所投产品客户端连接虚拟桌面无需依赖虚拟机 IP，具体表现为禁用虚机网卡或者随意更改 IP，桌面会话不会中断，用户可以正常办公和播放视频，避免因误操作而导致业务中断。
			支持设置终端流量、支持设置 USB 设备、磁盘映射和剪切板的上下行带宽，以避免带宽被抢占。
			支持自助快照恢复，当用户自己误操作导致云桌面卡慢、蓝屏、死机或者中病毒的时候，用户通过导航条按钮，可以自助进行系统盘快照还原操作，支持安卓瘦终端、PC 客户端。
			要求支持配置压缩质量、帧率等，降低流量、提升体验。
		运维功能	为了满足日常维护需求，需支持虚拟机热迁移技术，可在桌面业务不中断的情况将虚拟机运行位置更改至其他虚拟机节点。
			支持软件分发，通过创建软件库并关联给虚拟机，实现应用软件、驱动程序的增量式更新，不需要在每个虚拟机执行安装过程，整个分发过程秒级完成，且分发后不会覆盖原虚拟机的个性化配置和自主安装的软件，本项

			目要求支持应用软件、办公文件的分发。
			支持设置主题，管理员可以在主题商城中下载主题，并将主题应用到包括瘦终端（ARM、X86）、PC 客户端。
		安全管理	支持在管理组件中内置应用管控技术，实现全方位云桌面管控，在禁止名单中可以通过配置规则禁止指定应用或进程在云桌面中运行；在允许名单中通过配置规则只允许规则中的应用或进程在云桌面中运行。
			支持多种认证方式随需组合，包括本地账号密码、usb-key 认证、短信认证、硬件特征绑定、动态口令、ldap 认证、raduis 认证、AD 域认证、瘦终端客户机认证、802.1x 等多种方式，满足不同级别用户的安全接入需求。（需提供产品截图证明）
			支持个人盘加密技术，对云桌面个人数据进行加密保存，保障个人隐私安全。
			支持虚拟机快照技术，当数据误删或系统故障时可实现回滚，快照只保存增量数据，节省存储空间。
			★桌面云控制器内置防火墙，包括设置过滤规则、NAT 设置、访问监控、防 DOS 攻击、QOS 上传下载规则等。（需提供产品截图证明）
			★支持文件导出内容审计，开启文件安全导出后，虚拟机通过剪切板、PC 设备和 USB 设备外发文件的操作将被禁止，用户可以使用虚拟机内部的文件导出工具实现文件外发，所有外发的文件内容都可以加密备份到数据中心，以备后续审计使用，可疑的导出行为会产生告警。
16	云桌面瘦终端【深信服、aDesk-STD-320(VGA+HDMI)】	功能项	功能要求说明
		要求	保证与原桌面云超融合平台兼容性。
		硬件规格	硬件参数：CPU A55 1.8GHz，内存 2GB，硬盘容量 8GB（板载），接口：支持不低于 1 千兆电口，接口类型：1*VGA + 1*HDMI，USB：4*USB2.0+2*USB3.0
		平台兼容	★要求本次采购的云终端，能够通过自带的系统，登陆到本次建设的云桌面环境平台并具备调取原有云桌面虚拟机的能力。
		管理运维	采用嵌入式操作系统，若使用 windows 操作系统作为云终端底层操作系统，则需提供正版授权。
			★云终端易用性管理：支持配置自定义开机画面、支持云终端分组管理、支持配置云终端定时开关机计划、支持开启“云终端加电自启”功能、支持配置是否自动下载并安装更新、支持批量移动/删除/关闭云终端、支持配置是否允许自动登录和保存密码。（需提供产品截图证明）
			在瘦终端的管理方面，需支持分组管理、批量移动、删除、关闭瘦终端，支持配置定时开关机计划及加电自启动功能，支持自定义开机画面、配置自动登录和保存密码。
		用户体验	支持联动关机，用户可以跟使用 PC 一样，打开操作系统“开始”菜单、点击“关机”按钮，云终端和操作系统将会一体化关闭，没有多余的操作步骤。
17	Web 应用防火墙【安恒、WAF-2600AG】	技术指标	技术要求
		★规格要求	机箱高度：2U 标配网口：2 千兆电口管理口， 千兆业务电口*4（含 2 组硬件 BYPASS 模块），千兆业务光口*4，万兆业务光口*2；

				硬盘容量：2T 内存：16G USB2.0 口*2 串口：RJ45 口*1 电源：1+1 热插拔冗余电源 保护站点：无限制
		性能要求		硬件性能： 网络吞吐量 8Gbps HTTP 应用吞吐量 6Gbps HTTP 最大并发数 35 万 HTTP 最大新建数 3.2 万 HTTPS 应用吞吐量 1.5Gbps HTTPS 最大并发数 6.5 万 HTTPS 最大新建数 6500
		基本功能	部署模式	支持透明串接、反向代理、旁路镜像等多种部署模式部署，支持链路聚合
			高可用	支持集群模式、主-主模式、主备模式、硬件 BYPASS、软件 BYPASS
			SSL 加速卡	★内置 SSL 硬件加速卡，实现对 HTTPS 的加解密，提供设备对 HTTPS 的处理性能（需提供相关截图）
			保护对象	支持多条链路数据的防护，防护网段数量不限
				支持 ipv4/ipv6 双协议栈
				可通过设置数据缓存、页面压缩进行 web 加速
				支持保护站点快速向导配置部署
				可以设置后端 TCP 连接模式，可根据业务特点设置长连接和短连接，并且可以通过设置连接复用，减轻后端服务器压力（需提供相关截图）
			Web 服务自发现	支持自动发现网络环境中存在的 Web 业务系统，记录服务器的 IP、Port、域名等信息
			HTTPS 防护	支持 HTTPS 协议的选择可以选择 SSL/TLS 协议版本，可选 SSLv3、TLS1.0、TLS1.1、TLS1.2
				★支持 HTTPS 站点 SSL 算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果（需提供相关截图证明）
				支持透明串接和旁路反向代理下的 HTTPS 业务的安全防护
				支持源地址识别，部署在 SSL 网关后面，能够解析到真实的访问者 IP，并能对真实的 IP 进行防护和阻断
				支持证书批量管理，并且支持证书有效性检测
				在单个服务器通过相同的 IP 地址为多个 HTTPS 域名提供服务时，WAF 可以通过启用 SNI 来准确确定域名与证书的对应关系（需提供相关截图）
			攻击检测	支持对跨站脚本（XSS）和注入式攻击（包括 SQL 注入、命令注入 、代码注入、文件注入、LDAP 注入、SSI 注入等）的检测防护
				支持对 HTTP 请求关键字段进行合规性的检测（包括 Host 字段、User-Agent、Content-type 字段等）
				支持 HTTP 请求走私，防止 HTTP 请求分割攻击，防 Content-Length 与 Transfer-Encoding 分割
				支持 HTTP 响应分割，防止提交 HTTP 响应报文截断攻击
				支持防护 Session-Fixation 攻击，防止提交过期会话进行攻击

				支持防护 Java 反序列化及基于 Java 的通用攻击
				支持 XML 防护，XML 攻击行为包括 XML Ddos
				支持对 HTTP 头部各字段内容长度进行限制并可以自定义调整限制大小，包括参数名长度、参数值长度、HTTP 请求头部长度、URI 长度、cookie 长度、User-Agent 长度、Content-type 长度、Host 长度等，提供界面截图
				支持识别 HTTP 报文常见的编码和编码攻击：URL 解码、Base64 解码、HTML 解码、16 进制转换、JSON 解析、XML 解析、PHP 反序列解析、UTF-7 解码等
			HTTP 协议规范性检查	检查 HTTP 报文合法性
				检查 HTTP 报头是否有缺失或为空
				检查允许提交的 HTTP 方法
				检查请求报文是否畸形
				通过检查上传和下载的文件类型，防止下载敏感文件和上传 webshell 文件
				检查 HTTP 报头长度，防止缓冲区攻击
			Webshell 检测（语义分析）	内置 Webshell 检测规则，可以对上传的文件内容进行检查，防止恶意 Webshell 文件上传，对已经上传的 webshell 发起请求的行为进行拦截阻断
			敏感信息泄露检测	内置身份证、银行卡、手机号、社保号等个人敏感信息数据，对服务器返回的敏感个人信息数据通过星号进行隐藏，并支持用户自定义敏感词
				能够检测防止服务器导致的信息泄露行为，包括：目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等信息泄露行为
				支持禁止防敏感词发布，防止提交政治敏感、违反法规相关的言论信息，保障网站的内容健康呈现
				支持服务器信息隐藏，可配置删除服务器响应头信息
			应用层安全防护	支持对服务器响应安全设置，可通过选择不同的操作策略对响应头内容进行增删改。在修改响应头时，要保证触发条件的准确性，不得随意修改。
				★支持客户端安全防护，插入特殊的 HTTP 报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受 Clickjacking 攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到 XSS 攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的 XSS 风险和数据注入攻击）(需提供相关截图证明)
			爬虫、扫描器等自动化工具的安全检测	内置安全规则库有效识别 Acunetix、nessus 、WebScan、Webdump、AppScan 、等扫描器的扫描行为。
				内置安全规则可有效识别 baidu、google、yahoo 等常见网络爬虫的访问行为
			第三方组件漏洞防护	支持防护 WEB 容器漏洞，防止 Nginx、IIS、Tomcat 等 WEB 服务器漏洞
				支持防护 Kuwebs、phpcms、TRS WCM、JBR-CMS、DeDeCMS 内容管理系统等开源 CMS 漏洞
				支持防护 WEB 服务器插件漏洞，防止 Apache Struts2 漏洞
			盗链攻击	支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据

			检测	恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问，
			Cookie 安全	支持 Cookie 自学习 支持 Cookie 防篡改、防劫持
			自定义规则	支持对 HTTP 请求中 URI、HOST、参数、参数名、请求头、Cookie、版本号、方法和请求体及 HTTP 响应的响应体等条件进行自定义正则 支持多种组合条件，并且对于编写的正则表达式需要支持在 WAF 的管理界面上在线验证合规性。
			防护动作	支持阻断、重定向、智能加黑名单、丢弃、告警、仅检测等动作。不同的防护规则，可以选择不同的防护动作及返回码，也可针对不同规则设置专属 URL 白名单。
		高可靠性	链路聚合	支持链路聚合，提升网络带宽、增加容错性和链路负载均衡
			VLAN 子接口	支持 VLAN 子接口，业务口可承载多个 VLAN 通道
			HA	支持集群模式、主-主模式、主备模式
			运行模式	透明代理部署下，可支持对全局设置物理直通、网桥直通、纯代理、正常防护模式，也可针对单个保护站点设置不同的运行模式。反向代理部署下，可支持对全局设置纯代理或正常防护模式，也可针对单个设置不同的运行模式。
		高级功能	智能语义分析	★内置对 SQL 注入、XSS 攻击检测的语义分析规则（需提供相关截图证明）
			机器学习	1、具有机器学习安全引擎，可以对用户 web 业务系统建立安全的访问模型 ，学习的内容包括 URL 地址、URL 请求参数等信息 2、支持设定学习的周期，域名信息，可信任的客户端 IP，不可信的客户端 IP 以及不学习的 URL 信息 3、模型数据可以显示学习中的 URL 数量，学习完成的 URL 数量、检测中 URL 数量、学习失败的 URL 数量，同时可以显示各个阶段的占比情况 4、具有通用的机器学习模型，数据模型可实现在线更新
			智能攻击者锁定	支持智能识别攻击者，对网站连接发起攻击的 IP 地址进行自动锁定禁止访问被攻击的网站，可配置攻击者锁定时间，可配置将攻击者直接加入网络黑名单
			CC 防护功能	支持根据细粒度条件对 CC 攻击进行检测和防护；匹配条件由 URL 参数、请求头部字段、目的 IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由 IP、IP+URL、IP+User_Agent 等参数组成；支持从请求头字段获取真实源 IP 地址
			区域态势分析和阻断	按地理区域对攻击次数等进行统计，并通过地图展示；支持在地图上对某一地理区域设置阻断此区域 IP 的访问
			威胁情报	支持威胁情报库在线同步，可主动发现恶意 IP 发起的访问行为，并进行告警和拦截，威胁情报库支持离线更新，须提供第三方测评机构的检测报告
			云端高防联动	★WAF 与云端高防中心联动，通过 WAF 一键开启防护，实现 3-7 的 DDOS 安全防护，可提供 1T 的抗 D 能力（需提供相关截图证明）
			安全审计	能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容

				能详细记录服务器响应头信息，服务器响应内容
		日志报表管理	日志分析	★根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率（需提供相关截图证明）
			日志记录	支持记录应用防护日志、网络防护日志、CC 防护日志、访问审计日志、防篡改日志、操作日志、系统日志、升级日志
			访问审计	具备审计网站正常访问流量的能力，提供按小时，天、月份生成生成报表，需提供第三方测评机构的检测报告
				能记录、查询所有用户对网站的访问情况，包括访问的 URL、客户端 IP、服务器返回的状态码
				能够统计分析出用户所访问 URL/IP TOP10 数据
				能够统计分析访问流量最大的文件类型
				能够统计分析出搜索引擎的 TOP10 数据
				能够统计分析出客户端所使用操作系统的 TOP10 数据
			报表	支持报表导出为 Word、pdf、html 等多种格式
				支持定时报表，并发送到管理员邮箱
				支持攻击事件、告警等级、被攻击服务器 IP、攻击者 IP、攻击入口等不同报表模板
				支持对不同报表模板进行组合生成多维度报表
				支持根据 PCI DSS 标准对网站进行扫描评估并导出 PCI DSS 合规报表
		设备管理	管理方式	支持 HTTPS 方式进行设备管理
			账户管理	设备管理采用管理员与审计员分离
			SNMP 管理	支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2c
			NTP	支持 NTP 时间同步
			Console 管理	通过 Console 口进行本地配置
			分权管理	设备管理采用管理员与审计员分离
			风险趋势	支持防护站点风险趋势查看
			设备状态	支持设备自身状态查看：系统负载、业务流量、接口状态等信息，并可查看历史数据
			系统升级	支持系统升级并可查看升级日志
			告警方式	支持 Syslog、手机短信、邮件等多种告警方式
			规则升级	规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保 WAF 能够针对新型的、突发型的 Web 攻击进行防护
			认证	支持 LDAP
18	数据库审计与风险控制系统【安恒、DAS-A1800】	技术指标		技术要求
		★规格要求		硬件类型：工控机； 硬件尺寸：标准 2U； CPU 规格：4 核； 内存容量：8GB*2； 硬盘容量：4TB*2（Raid 1）； 硬盘接口：企业级 SATA； 网口：1 管理口+1HA 口+8 审计口（4 个千兆电+4 个千兆光）；

			网口类型：1000M 电口*6，1000M 光口*4（多模，标配 2 个 SFP 模块、3 米 LC-LC 跳线 2 根）； 电源配置：双电源； 空余拓展板卡位：2 个； 总网络吞吐量：3000Mbps； 双向审计最大数据库流量：300Mbps； 峰值事务处理能力 TPS：20000 条/秒； 日志数量存储：20 亿条； 功能描述：全功能开放； 数据库实例授权许可数量：无限个数据库授权； 硬件是否可扩容：是
		性能要求	审计性能：峰值 SQL 处理能力 20000 条/秒； 硬件最大吞吐量 3000Mbps，最大纯数据库流量 300Mbps，标配日志存储数 20 亿条； 审计日志检索能力 1500 万条/秒
		部署方式	为适应各种复杂的部署环境，产品部署模式应满足以下要求：
			旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计；
			可在云环境操作系统中安装软件代理；
			在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；
			★支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询、一键批量升级所有节点；提供证明材料
			管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；
			支持 IPv4/IPv6 双栈审计；
			支持和 ES 平台对接，将审计日志和告警日志存储在 ES 系统中，并支持通过页面查询日志
		协议支持	支持 Oracle、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ 等主流数据库的审计；
			支持 GuassDB、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、K-DB 等国产数据库的审计；
			★支持 MongoDB、Hbase、Hive、Impala、Elastic Search、HDFS、Cassandra、greenplum、LibrA、Grashbase、Cache、Redis、HANA、ArangoDB、Neo4j、OrientDB 等非关系型数据库的审计；（需提供截图证明）
			支持主流业务协议 HTTP、HTTPS、Telnet、FTP 的审计；
			可以通过导入证书的方式实现审计和防护，支持对 SQL Server（2005 及以上版本）数据库；
			可以通过导入证书的方式实现 MySQL 5.7 及以上版本采用了加密协议通讯的审计（需提供相关截图证明）；
			支持对各种协议自动识别编码及在 web 界面手工配置特定编码。
		审计功能	支持数据库操作表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
			审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集(需

			提供相关截图证明，并提供权威检测机构检测报告证明)；
			支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小
			支持跨语句、跨多包的绑定变量名及绑定变量值审计；
			支持超长 SQL 语句（最长 4M）审计。
		智能发现	支持自动发现流量中的数据库信息，简化配置。
		安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义；
			产品具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警；
			★内置安全特征库不少于 900 条，如 SQL 注入、缓冲区溢出等；（需提供截图证明）
			可自定义审计规则，审计规则至少支持 18 个条件；
			规则各条件之间支持与或非逻辑关系；
			支持内置安全规则单独升级；
			支持信任规则，信任规则至少支持 18 个匹配条件。
		查询分析	为满足审计追踪溯源、分析安全问题等需求，数据库审计应满足以下查询需求：
			具有高效的查询性能，后台采用全文检索引擎检索；
			查询条件易于使用，审计查询条件均为非正则表达式形式进行；
			支持基于数据库访问日期、时间、源/目的 IP、来源、数据库名、数据库表名、字段值、数据库登录账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询；
			★支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单（需提供截图证明）
			设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源 IP、目的 IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想；
			★支持告警分析功能，告警支持按照源 IP 和数据库账号对 SQL 模板维度进行排行，支持在页面一键删除规则、添加规则白名单。（需提供截图证明）
		统计报表	系统内置多种报表模板库，报表不少于 20 种；
			报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
			支持按照时间曲线统计流量、在线用户数、并发会话、DDL 操作数、DML 操作数、执行量最多的 SQL 语句等报表；
			支持性能分析，准确提炼出 SQL 语句执行频率和执行时间异常的报表；
			支持基于表维度的报表分析，表分析报表支持通过桑基图展示对该表的访问情况；
			支持 HTML、PDF、PNG、Word 等格式的报表导出；
			支持报表页面信息钻取。

		模型分析	★可依据客户端工具名、数据库用户名、客户端 IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器 IP 等配置行为模型，并可查看相应告警日志；
			可通过桑基图展示访问数据库的路径，路径包括数据库账号、IP 地址、客户端工具、数据库名、表明等；
		数据管理	为满足数据备份保留的需求，产品需要具备以下功能：
			支持根据在线数据最小保留天数和在线数据的磁盘空间占比自动清理早期数据；
			支持对在线数据的备份，支持调整备份压缩级别，支持展示数据备份进度；
			支持将审计日志通过 FTP/SFTP 的方式外送，支持自定义在线数据备份时间周期，支持从 FTP/SFTP 上恢复数据，恢复数据支持进度展示；
			提供审计策略和系统配置信息的单独导入、导出功能。
		系统管理	★支持用户界面告警、邮件、短信、钉钉、SYSLOG、微信方式告警；（需提供相关截图证明）
			采用 B/S 架构管理；
			支持系统安全配置（登录超时、用户登录失败锁定策略、密码强弱策略、密码有效时间）；
			支持 NTP 时间同步，客户端浏览器时间同步、SNMP（V1、V2、V3）网络管理协议；
			支持系统资源使用率超阈值、agent 状态异常、长时间无审计日志时触发系统告警，且告警支持通过页面、SYSLOG、邮件、短信、钉钉、微信方式输出。
		Agent 管理	支持在审计管理端批量安装、卸载、重新安装审计代理；
			支持在审计管理端启动、停止、挂起 Agent；
			Agent 支持设置 CPU 亲和性、最大资源使用率限制（CPU、内存）
			可监控 Agent 的转发速率，以及 Agent 所在数据库服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上线阈值，超阈值时 Agent 将自动停止转发数据（需提供相关截图证明）；
			支持根据系统 CPU 使用率、系统内存使用率、系统 I/O 使用率自动熔断；
			Agent 支持按照客户端工具、数据库账号过滤审计日志；
			Agent 支持在 RDP 或 SSH 登录数据库服务器运维时，审计原始登录人员的 IP 地址；
			Agent 支持设置抓包过滤器，回放网口抓包；
			支持在审计页面直接升级或回退已安装在数据库服务器上的 Agent，且升级或回退不需要输入数据库服务器的账号、密码
		分布式	支持在管理节点上管理数据库资产、审计规则、报表订阅、告警通知等；
			支持在管理节点查询所有审计节点的日志信息；
			支持在管理节点上监控所有审计节点的状态信息，包括 CPU 使用率、内存使用率、数据库流量、磁盘使用率、审计日志数、告警日志数等信息；
			支持管理中心和审计节点手工同步配置信息；
			支持在管理中心直接升级审计节点；
			管理中心和审计节点统一 license。（需提供相关截图证明）
		三层关联	可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句

			关联功能；
			支持通过部署 agent 实现 java web 环境 100%准确关联
		易用性	支持对 SQL 语句进行业务化翻译
			支持资产组管理；
			支持分组管理，分组管理包含 IP 组、应用用户组、对象组、时间组、数据库账号组；
			支持一键取证；
			支持区分历史会话和在线会话；
			支持 LADP 用户认证；
			支持配置过滤规则，过滤规则包含 IP 过滤、SQL 模板过滤和自定义过滤，自定义过滤条件不少于 28 个条件；
			在页面支持 ping、traceroute、nc 命令测试连通性；
			支持路由配置。
			支持英文界面
		可维护性	内置排错平台，支持一键检测系统的关键信息
			★内置运维终端，可实现日志查看、设备状态检查、执行 SQL 语句、执行常用命令、特权运维等能力（需提供相关截图证明）
			支持系统引擎管理，调整系统运行参数
		租户化管理	支持租户化管理，针对租户的账户只授权租户可查看租户内的数据库产生的审计日志、告警信息。