中国华能
CHINA HUANENG

华能山东石岛湾核电厂

服务器虚拟化项目技术规格书

批准：　张　勇

审核：　侯曰永

校对：　翟晓飞

编写：　胡　镇

华能石岛湾核电开发有限公司

二〇二一年十月

一、 概述

1.1 项目建设背景

华能山东石岛湾核电厂（简称石岛湾核电厂）由华能集团公司牵头开发，厂址位于山东半岛东海岸威海市所辖荣成市境内，地处石岛管理区宁津所街道办事处东南海滨，东部濒临黄海。工程建设一台 20 万千瓦级高温气冷堆核电机组。

2012 年，石岛湾公司完成服务器虚拟化建设，上线运行 9 年，维保于 2016 年 6 月过期，无法进行系统升级和补丁更新。目前，公司共有服务器环境 169 台套，其中虚拟化服务器 147 台套，物理机 22 台套，虚拟化率占 87%，承载了公司绝大多数应用服务，是公司核心 IT 基础设施及平台。虚拟化系统使用时间已超出设计使用时间，且已超出质保期，基于现状，石岛湾公司现提出服务器虚拟化项目，为公司各个应用系统提供稳定可靠的存储环境和运行环境。

1.2 项目建设目标

随着公司信息化建设的开展，应用系统的不断增多，特别是工程管理、OA、统一认证等重要应用系统对服务器与的计算性能和读写性能有着较高的要求。因此，本项目升级原服务器虚拟化系统，以支持新版的操作系统和新版虚拟服务器；同时部署针对虚拟化服务器的网络安全系统，提高虚化服务器的安全性，更好的支持应用系统的运行。

1.3 投标文件技术要求

本次招标要求投标单位提供产品报价、安装调试计划与实施方案、虚级化产品相关资料，以及招标单位认为需要的其他文件等。至少包括但不限于以下内容:

1、 投标文件中必须提供产品厂商针对本项目的授权文件。

2、 产品报价应针对四部分进行说明，分别是服务器虚拟化产品价格、虚拟化安全产品价格、安装调试报价、其他费用（请说明价格的来源）。

3、 对有利于完善和提高虚拟化系统质量，但本技术要求中未能尽述的有关内容，投标单位应根据自己的经验进行补充。

4、 服务响应和服务承诺，投标人需说明分时间阶段提供的服务内容及费用计划。

5、 合同签订后及竣工后的工作计划，包括技术支持方案和服务承诺。

1.4 其他配合要求

本项目承包单位应根据石岛湾核电厂的虚拟化产品的使用需求和本标书技术要求，制定详细的虚拟化系统安装调试计划。

本项目合同生效后，在执行合同过程中，本项目承包单位在 30 天内交付产品。如发生争议，由招标人裁决，各方都应遵守，并不得籍此要求增加费用或延长工期。

投标人必须保证所提供的产品或产品的任何一部分，招标人在中华人民共和国使用时，免受第三方提出的侵犯其专利权，商标权，著作权或其它知识产权的起诉。

二、 软件的技术参数要求

2.1 总体建设内容

根据石岛湾核电厂虚拟化何海虚拟化安全部署情况,采购相应的虚拟化产品和虚拟化安全产品。

2.2 规格与型号

1、备份软件（数量：1套）

	指标项	指标要求
★	配置要求	配置16颗服务器物理CPU的备份许可,不限制备份虚拟机的数量,支持EMC的DD6300;
★	品牌要求	企业级备份软件，国际知名品牌；非OEM贴牌产品；成熟稳定,与存储及虚拟带库统一品牌，以便统一管理;
	操作系统支持	备份软件支持多种操作系统，至少支持AIX、Linux， Windows等操作系统
	支持多种数据库	支持多种数据库系统，支持多种数据库在线备份，包括SQL Server、Oracle等的在线备份。支持简体中文的界面操作
	文件备份支持	支持文件服务器上小文件的块级备份，提高备份速度。且支持按文件颗粒度进行恢复
	虚拟合成	支持虚拟合成全备份，即通过与备份设备结合，通过增量备份或差异备份与最近一次全备份，即可生成新的全备份，降低全备份频率。
		支持与重复数据删除功能设备VTL/CIFS/NFS/Boost功能相结合，实现备份架构的灵活扩展。
	Client directly 功能	备份数据可以直接从应用服务器备份到 备份设备,无需安装介质服务器插件，降低网络流量，且提升备份速度。
	虚拟化备份支持	支持VMWARE VMDK映像备份，与VMWARE自带的VDP备份可以实现平滑迁移，支持CBT备份与恢复，支持虚拟机立即启动服务。支持TCP/IP网络环

		境的数据备份，可以升级到 SAN 环境下的 LANFree 备份，并升级到 ServerFree 备份;
★	虚拟化连续数据保护	对 VMware 环境，支持指定 VM 的 CDP 连续数据保护，直接可以与 VMware vCenter 集成，可以通过 vCenter 管理配置整个 CDP 过程; 实现对 VMware 虚拟机数据逻辑故障的保护与恢复，逻辑故障包括: 数据库逻辑错误、人为误操作和病毒等引起的数据库数据丢失、人为或病毒引起的数据库崩溃等故障; 实现任意时间点恢复功能: 可以捕获并记录每一个写 I/O 操作，当数据需要恢复时，用户可从时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复; 本次配置 16 个 CPU 授权许可。
	服务	原厂 3 年软件 7*24 服务

2、虚拟化软件（1 套）

	指标项	**指标要求**
★	基本要求	采用裸金属架构，无需绑定操作系统即可搭建虚拟化平台。Hypervisor 结构精简，部署后所占用的存储空间在 200M 以下，配置 16 颗 CPU 使用许可;
		虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。
		虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址、MAC 地址等。
		能够提供性能监控功能，可以对资源中的 CPU、网络、磁盘使用率等指标进行实时统计，并能反映目前物理机、虚拟机的资源瓶颈。
★	兼容性要求	支持现有市场上的主流 x86 服务器，具有双方认可的官方服务器硬件兼容性列表，包括 IBM、HP、DELL、Cisco、NEC 以及国内自主品牌服务器等。
★		兼容现有市场上主流的存储阵列产品，具有双方认可的官方存储阵列兼容性列表，存储阵列类型包括 SAN、NAS 和 iSCSI 等，存储阵列品牌

		包括 EMC、IBM、HP、HDS、NetApp、Dell 等。
★		兼容现有市场上主流厂商的多款不同型号的服务器配件、网卡和 HBA 卡产品。
★		兼容现有市场上 x86 服务器上能够运行的主流操作系统，具有双方认可的官方客户操作系统兼容性列表， 尤其包括以下操作系统: Windows XP、Windows Vista、Windows 2000、Windows 2003、Windows 2008、Windows 8、Redhat Linux、Suse linux、Solaris x86、FreeBSD、Ubuntu、Debian、Mac OS 等，虚拟机上的操作系统不进行任何修改即可运行。
	功能性要求	提供 HA 功能，当集群中的主机硬件或虚拟化软件发生故障时，该主机上的虚拟机可以在集群之内的其它主机上自动重启。当虚拟机的客户操作系统出现故障时，可以自动重启该虚拟机客户操作系统，保障业务连续性。
★		提供容错机制，可以保证运行虚拟机的主机发生故障时，虚拟机会自动触发透明故障切换，同时不会引起任何数据丢失或停机。支持不少于 2 个虚拟 CPU 的工作负载容错功能。
★		支持虚拟机的在线迁移功能，无论有无共享存储，都可以在不中断用户使用和不丢失服务的情况下在服务器之间实时迁移虚拟机，保障业务连续性。
★		提供虚拟机的备份功能，能够利用重复数据删除技术对整个虚拟机或虚拟机单个磁盘快速进行无代理备份(全备份或增量备份)和恢复。同时提供备份接口，能够与第三方备份软件无缝兼容对虚拟机进行集中备份。还支持诸如 Microsoft Exchange、SQL Server 和 SharePoint 应用级的备份
		虚拟机支持多路虚拟 CPU(vSMP)技术，以满足高负载应用环境的要求。
		可以为虚拟机创建一个或多个快照来保存虚拟机的基于时间点的运行状况和数据。
		提供专用的 P2V 工具，实现在线物理机至虚拟机的无间断平滑转换。
		虚拟化平台可以内建标准虚拟交换机，实现虚拟机之间或虚拟机与物

		理机之间的网络调度，支持同一物理机上虚拟机之间的网络隔离(支持VLAN)。
		支持 16 Gb 端到端光纤通道。
★		提供防病毒和防恶意软件解决方案，可以与第三方杀毒软件或安全软件融合，无需在虚拟机内安装代理即可保护虚拟机，实现虚拟化环境下的安全防范。
★		提供物理主机级别的无状态防火墙，无需使用 IPTABLES，管理员可以用命令行和图形化界面配置防火墙。
		虚拟机支持直接访问裸设备，将虚拟机数据直接存储在 LUN 上。
★		具有存储精简配置能力，可以超额分配存储容量，提高存储的利用率，减少存储容量的需求。
★		提供虚拟机的存储在线迁移功能，无需中断或停机即可将正在运行的虚拟机从一个存储位置实时迁移到另一个存储位置。支持跨不同存储类型以及不同厂商存储产品之间进行在线迁移。
		提供热添加 CPU，磁盘和内存的功能，无需中断或停机即可根据需要向虚拟机添加 CPU，磁盘和内存。
		提供具有存储识别功能的 API，使第三方存储厂商可以将存储软件与虚拟化平台更好的整合，使虚拟化平台能够识别特定磁盘阵列的功能特性以及状态信息。
★		虚拟机可以被外部存储阵列识别，实现基于存储策略的管理(SPBM)，可允许跨存储层实现通用管理以及动态存储类服务自动化，可实现按虚拟机级别的数据服务(快照、克隆、远程复制、重复数据消除等)
		支持跨多个 LUN 的共享数据文件系统，可以聚合至少 32 个异构逻辑卷（LUN），支持在线实时添加 LUN 以实现集群卷容量动态增长，可支持至少 64TB 容量集群卷。虚拟机文件系统也支持主流存储厂商的存储自动分层功能。
★	扩展性要求	每台虚拟化主机至少支持 768 颗逻辑 CPU，要求提供官网链接。
		每台虚拟化主机至少支持 4096 颗虚拟 CPU(vCPU)。
★		每台虚拟化主机至少支持 16TB 内存，要求提供官网链接。

★		每台虚拟化主机至少支持 12TBr 持久内存(Persistent Memory)，要求提供官网链接。
		每台虚拟化主机至少支持单个存储卷 64TB 大小。
		每台虚拟化主机至少支持 1024 个虚拟机。
		每个集群至少支持 64 个主机，至少支持 8000 个虚拟机
		可以内建分布式虚拟交换机，每个分布式虚拟交换机可以管理至少 1000 台虚拟主机。每台主机的虚拟网络交换机的端口总数至少可以达到 4096 个。
		每个虚拟机至少支持 62TB 的虚拟磁盘容量。
		每个虚拟机至少支持 256 个 vCPU,要求提供官网链接。
★		每个虚拟机的内存至少可以达到 6128GB，要求提供官网链接。
★		每台虚拟化服务器的虚拟机在线迁移并发数量至少可以达到 8 个，要求提供官网链接。
★		官方公布虚拟机至少支持 150 种以上的客户操作系统，要求提供官网链接。
		控制台自身具备备份和还原机制，可以对数据进行备份和还原。
		控制台自身具备高可用机制，不依赖于任何外部共享存储或数据库，可以在 5 分钟内完成服务切换。
		每个控制台可管理至少 2500 台物理服务器、40000 台已打开电源的虚拟机，45000 台已注册的虚拟机；并可以通过链接至少 15 个控制台实例，跨 15 个实例管理 15000 台物理服务器，135000 个已打开电源的虚拟机和 150000 个已注册的虚拟机。
		使用服务器主机远程管理应用程序来远程交互式安装和脚本式安装虚拟化软件
★		支持对包括虚拟机模板、ISO 映像和脚本在内的内容进行存储库统一存储。用户可以从集中化位置存储和管理内容,以及通过发 / 订阅模型共享内容。

		提供统一的图形界面管理软件，可以在一个地点完成所有虚拟机的日常管理工作，包括控制管理、CPU 内存管理、用户管理、存储管理、网络管理、日志收集、性能分析、故障诊断、权限管理、在线维护等工作。同时能够直接配置、管理存储阵列，具有对存储阵列的多路径管理功能。支持 QoS 能力，支持基于应用程序的服务级别自动管理功能。
★		可以支持 Web Client 和命令行管理功能。支持与主机管理软件集成，并通过管理软件获取主机硬件监控信息。
★		支持单点登录，用户只需登录一次，无需进一步的身份验证即可访问控制台并对集群进行监控与管理。
		支持自定义角色和权限，可以限制用户对资源的访问，实现分级管理并增强安全性和灵活性。
★		支持 AD 域整合，域用户可以访问控制台，由 AD 来处理用户身份验证。
		管理软件可实现多管理软件级别互通功能，支持多管理中心架构，并可实现分布式管理。
		可以记录重大配置更改以及发起这些更改的管理员的记录，可以导出报告以进行事件跟踪。
		提供自动报警功能，能够提供物理服务器或虚拟机的 CPU、网络、 磁盘使用率等指标的实时数据统计，并能反映目前各物理服务器、虚拟机的资源瓶颈。
★	服务及其它要求	虚拟化软件的所有功能必须为同一家厂商提供，禁止借用第三方软件的整合，以保证功能的可靠性和安全性。
★		厂商在中国有独立的软件研发中心，可以提供产品本地化优化与深度问题本地研发支持。
		虚拟化管理平台提供 API、SDK 等接口，可以与第三方管理软件结合或二次开发。
★		为市场成熟产品，被五百强企业广泛采用，在本地区内具有广泛的应用案例。
		提供 3 年原厂商 5*12 软件升级服务、在线支持服务、800 电话支持服务。

3、虚拟化防护产品

	功能明细	功能描述
	数量要求	提供 16 个物理 CPU 的原厂授权许可和统一的集中控管平台。
★	服务器安全防护管理中心	1.虚拟化服务器、物理服务器安全防护使用同一管理中心，对全网的物理服务器及虚拟化服务器进行统一管理; 2.支持所有虚拟化平台在统一安全管理平台管理，包括 VMware、H3C 和华为等（提供截图证明并加盖原厂公章）。
	服务器安全防护支持平台	1.物理服务器要求提供轻代理客户端部署方式，支持目前主流的操作系统平台，针对 Linux 操作系统的部署支持，提供官方公开查询网址及查询说明; 2.虚拟化平台提供轻代理和无代理两种部署模式，无代理部署模式支持 VMware、华为 Fusion、华三 CAS、品高云、Citrix Xen Server、微软 Hyper-v 等虚拟化平台，支持 IPv6 的部署和应用，提供相关证明材料; 3.为保证后续信息化基础设施的扩容和发展，要求服务器安全防护支持公有云平台的部署，包括：AWS、Azure、阿里云，提供相关证明材料。
★	产品成熟度 要求	投标产品有公安部的安全产品销售许可证，必须是自主开发，拥有自主知识产权，市场主流的，非 OEM 产品，具有先进性，并成熟可靠，至少已在市场销售五年以上，以首次取得销售许可证为准（提供相应证书并盖原厂公章）。
	产品授权要求	提供三年期限的版本升级、病毒库升级、维保、原厂技术经理服务、提供产品安装介质、使用手册、产品使用授权书和技术培训。
	数据库支持	产品自身使用的数据库应该支持外挂企业级数据库，例如：SQL Server，Oracle;
	病毒库更新	1.产品需要支持更新的多级部署，分流冗余节省带宽，更新速度快; 2.产品安全升级需要支持 Pattern 回退; 3.产品需要支持设置定时任务检查软件升级和安全升级; 4.产品需要支持自定义升级某一个或者某一些客户端的病毒码，而不是只能

		一次升级所有客户端的病毒码。
	多租户支持	1.管理中心支持多租户; 2.支持不同租户 widget、事件、安全策略、管理、日志文件相互隔离; 3.支持不同租户计算机、终端、安全配置相互隔离。
	机器学习能力	机器学习能力，提供管理端及客户的的产品界面截屏（提供证明文件加盖原厂公章）。
	权限管理	支持管理用户角色，支持用户权限的灵活设定，可以让不同用户访问在管理界面上访问不同的客户端及配置管理界面（提供截图证明并加盖原厂公章）。
	加密访问	支持通过 HTTPs 方式登录管理控制台，管理控制台访问需进行加密访问（提供截图证明并加盖原厂公章）。
	集中管理	提供集中管控系统，集中管理各平台上部署的防毒系统，提供集中的监控界面、系统日志、产品更新、病毒警报等功能。
	VMware Operation Manager 集成	服务器安全防护系统可实现与 VMware Operation Manager 无缝集成，无需二次开发。
	外接沙箱能力	具备外接沙盒设备和威胁发现设备的联动能力，可自动提交可疑恶意文件，并可接收。
	APT 攻击防护联动能力	能够有效防御高级持续威胁（APT）的攻击，通过联动机制禁止客户机对命令与控制服务器的外联。
	基本防护功能	1.AV，防恶意程序; 2.Web 信誉，可以阻止用户访问恶意 Web 站点；支持设置 Web 信誉安全级别，包括高、中和低，支持配置阻止未经安全测试的页面，提供功能截图。 3.完整性监控，实时检测并报告对文件和系统注册表的恶意及意外更改; 4.防火墙，减少物理和虚拟服务器的攻击面;

		5.入侵防御（DPI），在已知漏洞修复之前，屏蔽漏洞以免遭受无限制的入侵； 6.日志审查，捕获和分析系统日志，为组织提供审计证据，可以将日志审计配置为将可疑事件转发到 SIEM 系统。
		产品要求提供完整的主机安全防护，同时支持实体服务器防御和虚拟服务器的主机防御，包括防火墙、防病毒、完整性监控、虚拟补丁技术、日志审计等功能；在虚拟化环境中，除日志审计模块，其余模块要求和虚拟化环境以无代理方式集成，不需要在每台虚拟机上安装客户端，以便减少对物理机的资源占用；主机整体资源与搭载虚拟机数量无直接关系；虚拟资源消耗不会随虚拟机数量成长（提供截图证明并加盖原厂公章）。
	主机防火墙功能	产品必须具有主机防火墙功能，不依赖分布式交换机可以无代理运行，并且可集中控管防火墙策略，策略定制可以针对 IP，Mac 地址或通讯端口，可保护所有基于 IP 通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等）（提供截图证明并加盖原厂公章）。
★	深度内容检测功能	产品必须具有深度内容检测功能，不依赖分布式交换机可以无代理运行，必须可以同时保护操作系统和应用服务（数据库，Web，DHCP 等）（提供截图证明并加盖原厂公章）。
★	虚拟补丁防护功能	产品必须具有操作系统虚拟补丁功能，不依赖分布式交换机可以无代理运行，通过漏洞防护规则，在机器不重启，没有补丁更新的情况下防护零日漏洞，阻止漏洞利用，在服务器尚无安装实体补丁前，提供针对此补丁攻击的防护能力。
		具备特征库更新功能，实时追踪并保护最新动态威胁：提供自动扫描功能，针对服务器弱点、漏洞进行安全检测并自动形成防护，产品必须能够防御应用层攻击、SQL Injection 及 Cross-site 跨网站程序代码改写的攻击。
		产品必须提供包含攻击来源、攻击时间及试图利用什么方式进行攻击等必要信息，并在事件发生时，立即自动通知管理员（提供截图证明并加盖原厂公章）。
	虚拟化平	产品必须可以和 VMSafe 集成并提供集成管理功能，支持无代理方式，不需

	台集成功能	要在每台虚拟机上安装，只需在虚拟化环境底层安装即可，对每个虚拟机没有资源占用。
		产品可以通过在整个虚拟环境中安装单一拷贝来达到保护所有虚拟环境中 Guest OS 和应用的功能。
		产品必须和虚拟化环境的 WMotion，Storage VMotion 以及 HA 集成，能够自动感知和保护虚拟环境的变更和迁移。
	完整性监控功能	产品支持完整性监控，能够监控操作系统和关键应用包括注册表项、关键目录、特定目录变更，以防范恶意修改（提供截图证明并加盖原厂公章）。
	日志审计功能	产品支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件 ；协助遵循规范(PCI DSS 10.6) 优化识别埋在多个日志项下的重要安全事件； 将事件转至 SIEM 系统或中央日志服务器，做关联性分析、报告和归档； 侦测可疑行为、收集数据中心的安全事件和管理操作，并使用 OSSEC 语法来建立高级规则（提供截图证明并加盖原厂公章）。
	主机加固功能	产品支持主机加固功能，实现对服务器的系统及应用的弱口令、高危账号、配置缺陷、网页后门、反弹 shell 等检查，同时实现对业务系统资产进行等保定级跟踪，根据资产定级自动进行对应 级别的安全配置检查，对合规情况出具等保符合性报告，提供功能截图。
	EDR 功能	产品支持 EDR 功能，可以形成持续监测、主动检测、溯源分析、自动响应的完整闭环。端点植入探针，“高清摄像头”实时记录系统事件形成持续检测体系;资产管理，热点威胁检测，集成 ATT&CK 引擎的 IOA 入侵检测等模块不断进行主动检测，通过可视化的进程树和溯源分析模块追踪威胁事件的完整过程，提供功能截图。
★	日志集中分析功能	产品必须具有集中控管的功能，能够统一的管理和配置各类安全组件的日志信息，包括: 服务器安全防护日志、网络边界安全检测日志信息、APT 攻击事件日志信息、沙箱检测日志信息等，并且日志能够统一的在集中控管平台上呈现，可通过集中控管功能将日志信息同步给所有安全设备进行统一的防护，提升整体的安全基线（提供相关截图）。
	异常监控	产品需要支持不少于 100 种异常监控和告警规则。

	与告警	具有病毒日志查询与统计功能，可以随时对网络中病毒发生的情况进行查询统计，统计显示饼状图、柱状图等，能按时间（日、周或任意时间段）、按 IP 地址、机器名、按病毒名称、病毒类型进行统计查询，并能将查询统计结果打印或导出。
		支持服务器审计日志，针对服务器运行情况进行监控、报警，针对客户端防病毒感染情况进行监控、报警。报警支持邮件、syslog（提供截图证明并加盖原厂公章）。
	系统事件	1.产品应支持不少于 700 种系统事件，记录包括管理员、审计员、系统等所有审计日志; 2.系统事件支持 NSX 标记功能，根据条件自动标记事件，并可以根据标记展示和过滤时间，标记条件包括事件、事件 ID 和级别、目标、操作者、管理中心和事件起源。一旦检测到恶意威胁，DS 可将 NSX 安全标记应用于受保护的 VM。
	报表/报告	1.产品应提供至少 19 个报表模板，覆盖所有功能，包括数量排名、图形展示; 2.可指定任意虚拟机/终端、计算机组、策略、时间段和标记进行报表生成，支持定义报表保密级别，支持生成报表加密。
	快速服务支持	产品厂家在国内具有独立的病毒研发和响应中心，国家计算机病毒应急处理中心技术支持单位（提供证明文件并加盖原厂公章）。
★	质量保证	产品须通过 IPv6 Ready logo 认证，具备新华三 CAS、华为 Fusion、浪潮云海等平台兼容性测试认证；厂商具备信息安全管理体系认证、信息技术服务管理体系认证、CMMI5 认证及信息系统服务交付能力一级。

2.2.2 安装调试技术要求

项目承担单位需提供系统实施工作方案，在合同签订后，入场进行项目调研，制定项目总体实施计划和详细实施方案，实施方案包含但不限于虚拟化系统部署方案，虚拟化安全部署方案，数据迁移计划及

回退方案等，确定系统测试方案，做好系统部署实施、调试工具的准备、安装调试环境的准备。

本项目中所有涉及到的虚拟化及安全系统的部署，全部由原厂工程师完成安装调试，用户参与整体的安装和调试，在部署过程中原厂工程师必须说明的安装步骤和注意的事项，安装的每一件产品必须做详细的安装记录，编制详细的系统实施报告。

三、 实施、调试和验收

3.1 实施和调试

1、卖方提供所采购软件的安装、调试和数据迁移服务；直至所有系统上线稳定运行，买方予以协助配合。

2、合同签订后，卖方在 10 天内在买方安排下进入现场调研，开展需求调研工作，形成双方签字确认的安装调试实施方案。

3、卖方必须提供买方规定的相关资质证明、授权文件等，保证提供的软件产品无质量问题与原厂保修权利问题。

4、系统安装调试由卖方在买方管理下进行，并制定出安装调试的计划与方案，经卖方审核后执行。安装调试必须进行详细记录，安装调试结束后，由卖方技术人员和项目负责人审核后签字交给买方验收。

3.2 验收

项目验收分两个阶段进行，即：到货安装验收与最终验收。到货安装验收之后进入系统试运行阶段，时间为三个月，试运行结束后进行最终测试，通过最终测试后完成最终验收。

到货安装验收与最终测试的依据是由卖方提供并经过买方认可的验收方案。

3.2.1 到货安装验收

卖方需邀请原厂工程师到场，协助买方清点软件型号等，查验所提供软件是否与招标要求相符。安装实施由原厂工程师实施。

软件安装完成后，进行系统实施和数据迁移，严格遵守买方生产管理的相关要求，制定数据迁移计划和方案并严格遵守，确保数据迁移零丢失。若产生数据损坏等意外情况影响业务系统运行，由卖方进行修复，买方将根据对业务的影响程度进行扣款。

由卖方负责制定测试内容、指标、方法和测试计划，经买方批准后进行现场测试。测试进行详细记录。测试内容至少包括：功能测试、性能测试、稳定性测试、故障测试和安全性测试等。

卖方提出到货安装验收申请，买方组织验收，测试合格后， 双方签署验收协议，完成到货验收，系统进入三个月的试运行阶段。

3.2.2 最终验收

试运行期间如虚拟化系统运行稳定可靠，所有功能及性能指标达、相关技术规范书及合同的要求，卖方可提出进行最终验收，并提供验收测试方案，经买方补充和修改确认后进行终验。在试运行期间，如发生由于软

件质量等因素造成某些指标达不到项目要求，允许卖方更换或进行修复，但试运行期顺延三个月，在全部指标达到要求时，双方签署最终验收文件。

验收主要内容:

1、 虚拟化及虚拟化安全系统已安装，经数据迁移和安全测试、进入稳定正常运行。

2、 此次项目实施的所有相关的技术资料（包括但不限于随机资料、安装报告，实施过程文档）中文文本，在验收前已经由卖方完整移交买方。

四、 售后服务要求

1、所有投标产品必须提供 3 年原厂商的技术支持、质量保证和免费上门售后服务。自双方最终验收签字之日起计算。

2、本项目售后技术支持服务人员应是参与该项目的实施人员，以便于出现问题时能够尽快解决。

3、如果系统发生故障，要及时查明故障原因并修复直至满足最终验收指标和性能的要求，查故障原因与修复的过程不收取额外费用。

4、卖方应提供多种途径的技术支持服务，包括 7x24 小时的电话支持、邮件支持及网上交流等；工作日内 2 小时响应，节假日内 4 小时响应。在保修期内服务响应完成时间不超过 24 小时。

5、卖方提供 3 年，每年不少于两次的巡检服务。

6、所有产品在质保期内须提供免费的驱动版本升级服务，以原厂商官方正式发布的最高版本为准。

7、根据最终客户要求，提供产品重新安装、特殊时段（公司重大活动、

政治任务等）现场支持、系统变更和迁移等服务。

8、如果由于维修服务失误或产品故障造成最终客户损失，卖方需要予以赔偿并提供处理办法。

9、卖方须认真理解上述质保要求，须详细说明原厂商及卖方随所投产品的售后支持与服务的项目，一经应答将作为合同的一部分。