第5章 基础保障环境规划

5.1 基础保障环境规划的目标

在根据用户的需求完成软件开发后，信息系统需要部署到计算机机房内的服务器上运行，才能给用户提供信息服务。机房、网络、服务器、存储等硬件设施以及系统软件、中间件等软件平台都是信息系统运行的基础，通过合理的整体规划和设计，将这些组成部分完美地结合在一起，为信息系统的运行服务提供良好的基础保障环境支撑，通过良好的运维管理实现信息系统安全、稳定、高效地运行，确保对机构的业务连续运营的支持。伴随着信息系统的运行，机构的关键信息数据也一起存放在计算机机房内，通常将机房环境以及机房内的公共基础软件和硬件设施一起统称为数据中心。基础保障环境的规划也就是数据中心的规划。

1. 基础保障环境组成

基础保障环境主要由硬件基础设施、软件公共平台、安全保障体系、运维服务体系四个部分组成。

硬件基础设施包括网络、服务器、存储、机房环境等部分，通过分类分组的服务器群、统一的存储和网络架构、统一的机房基础设施来支撑各信息系统及相应基础软件的运行。

软件公共平台包括基础平台软件和公共中间件，软件公共平台为所有信息系统提供操作系统、数据库、Web 应用服务、门户、认证、数据交换等公共基础服务。

安全保障体系是针对信息系统和数据的各种安全风险，在物理安全、网络安全、系统安全、数据安全、应用安全、终端安全等不同层次上采取可靠的安全防范技术手段，同时，建立机构的信息安全管理制度和流程规范，实现严密、多渠道的安全控制，从而确保信息系统安全可靠，提高用户对信息系统的信赖度。限于篇幅，本书只对网络安全部分进行简单的介绍，有关安全保障体系的详细内容可以参考相关专业书籍。

运维服务体系是按照 IT 服务领域的通用标准和方法，设计 IT 服务，制定运行维护管理流程和规范，设计运行维护管理组织结构和运行维护队伍，最终通过人员、技术和流程的有机结合，有效实现 IT 运行维护管理标准化和规范化，有效提高 IT 运营的整体水平。

基础保障环境总体框架如图 5.1 所示。

2. 基础保障环境规划的目标

基础设施是信息系统运行的物质基础，为信息系统提供资源充足的运行支撑是其核心任务。由于任何设备和系统都不是完全可靠的，任何系统都可能出现故障，而且系统出现故

障的原因也很复杂，既包括产品设计缺陷、生产质量不过关、运行环境恶劣和人为操作失误等因素，也有系统配置不合理、系统可维护性差等因素。基础保障环境规划的目标就是进行合理的整体规划和设计，在提供资源充足的运行支撑的同时，关注系统的可靠性和可维护性，为信息系统的运行服务提供可靠的支撑，最终实现信息系统安全、稳定、高效地运行。

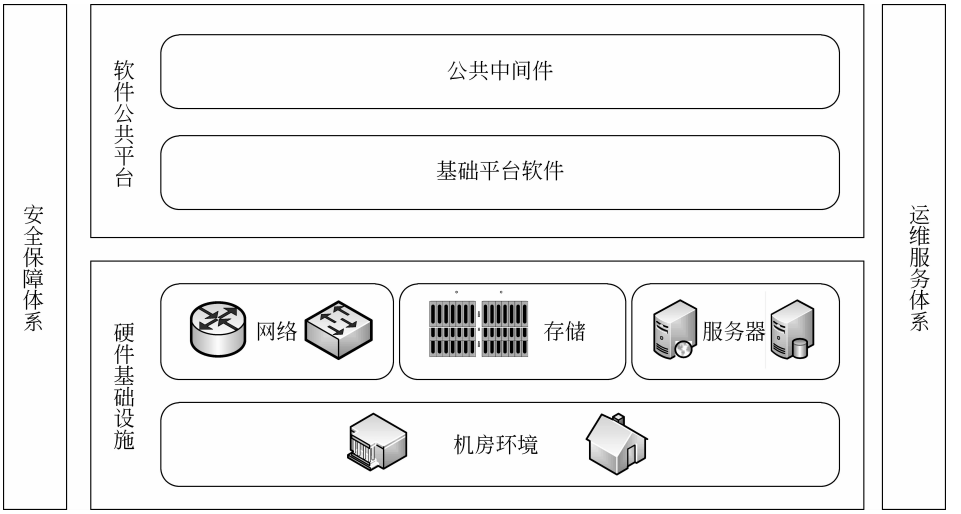

图 5.1 基础保障环境总体框架

具体地，基础保障环境规划的目标包括以下几个。

(1) 提供资源充足的运行支撑。

- 统一的硬件基础设施。建设专业的机房、高效的网络、集中的存储和柔性的服务器架构，提供资源充足的硬件支撑。
- 丰富的基础服务软件。配备支持各种虚拟化和硬件平台的操作系统、成熟高效的数据库系统软件、通用的应用服务器软件以及其他丰富的基础服务软件，提供丰富的软件公共平台支撑。
- 集成的数据支撑环境。建立完善的数据备份与容灾体系，按业务需求建设主题数据库和归档数据库，实现对决策支持应用的良好支持。

(2) 具备良好的扩展能力。

- 基础设施对业务的需求变化应具有良好的适应能力，以加快新系统和应用的部署。
- 基础设施至少能满足未来 5 年内业务变化对资源的增长需求。

(3) 实现全面的安全保障与高可用。

- 从硬件基础设施到数据环境，从应用开发到应用运行，建立全面的安全保障机制，确保信息化总体的安全有效。
- 遵循高可用性的原则，建设可靠的基础保障环境，应尽可能避免因基础设施故障而造成业务无法正常进行。系统可用性的两个主要衡量指标是设备平均无故障时间(Mean Time Between Failure，MTBF)和平均修复时间(Mean Time To Repair，MTTR)。

(4) 达到专业化的运维服务。

- 建立完善的运行管理流程，为应用运行提供专业化、流程化服务。
- 建立统一的基础设施管理平台，清晰地定义 IT 管理人员的角色和职责，明确运维流

程和规范，提高管理和运维效率。

5.2　基础保障环境规划的步骤

基础保障环境规划的基本步骤如图 5.2 所示。

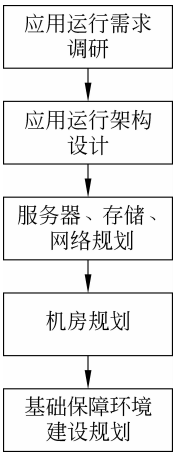

图 5.2　基础保障环境规划步骤

1. 应用运行需求调研

了解一个机构的信息系统的建设和运行情况，可以通过设计如下所示的《信息系统运行环境需求调查表》来收集各信息系统的运行需求（每个信息系统一份调查表），调查表主要包括以下一些方面的内容：

- 信息系统数量和技术平台。
- 对计算资源（CPU/RAM）、存储、负载均衡的需求。
- 对操作系统和公共平台软件的需求。
- 容灾和备份需求。
- 网络访问和安全管理的需求。
- 用户的行为习惯。

信息系统运行环境需求调查表

信息系统名称：_____

系统负责部门：_____

系统开发商：_____

联系人：_____

联系电话：_____

电子邮件：_____

1　信息系统总体情况

1.1　部署方式

□ A：集中部署在机构的中央机房　　□ B：部署在各自部门内部

□ C：托管在机构外面

1.2　运行架构

□ A：浏览器/服务器（B/S）　　□ B：客户端/服务器（C/S）

1.3　技术开发平台

□ A：Java　　□ B：.NET

□ C：其他（请注明）_____

1.4　是否需要集中部署在机构的中央机房

□ A：需要　　□ B：不需要

1.5 是否需要与机构的应用集成运行环境(统一门户、统一用户、数据交换)集成

□ A：需要　　□ B：不需要

2 信息系统对基础运行环境的需求

2.1 正常负载运行时,对服务器的需求

服务器功能	数量(台)	服务器配置需求
示例：Web 服务器	1	CPU 2 * 4core,内存 4GB,硬盘 50GB(其他无)

2.2 对操作系统及版本的需求

□ A：Linux 版本：_____　　□ B：Windows Server 版本：_____

□ C：其他(请注明)：_____

2.3 对数据库系统及版本的需求

□ A：Oracle 版本：_____　　□ B：SQL Server 版本：_____

□ C：其他(请注明)：_____

2.4 对网络运营商及带宽的需求(可多选)

□ A：教育科研网_____MB 带宽　　□ B：中国电信_____MB 带宽

□ C：中国联通_____MB 带宽　　□ D：其他(请注明)：_____

2.5 对应用服务器中间件及版本的需求

□ A：WebLogic 版本：_____　　□ B：Resin 版本：_____

□ C：Tomcat 版本：_____　　□ D：其他(请注明)：_____

3 信息系统数据情况

3.1 数据采集周期

□ A：每年一次　　□ B：每季度一次

□ C：每月一次　　□ D：实时采集

□ E：不定期　　□ F：不需要数据采集

3.2 每次采集的最大数据量

□ A：约_____MB　　□ B：不需要数据采集

3.3 信息系统产生的结构化数据量(请填写所有选项)

□ A：约_____GB/年　　□ B：约_____条记录/年

□ C：最大总量约_____GB　　□ D：最大总量约_____条记录

3.4 信息系统产生的非结构化数据量(请填写所有选项)

□ A：约_____GB/年　　□ B：约_____个/年

□ C：最大总量约_____GB　　□ D：最大总量约_____个

3.5 信息系统数据备份数据量(请填写所有选项)

□ A：周期约每_____一次　　□ B：数据量约_____GB/次

□ C：最多保留_____次备份数据

4　信息系统用户和网络访问情况

4.1　是否提供面向互联网用户的服务

□ A：是　　□ B：否

4.2　是否有系统内用户从外部进行应用访问或网络连接的需求

□ A：否

□ B：是。请注明用户访问的详细情况：_____

_____

4.3　日常使用并发用户数

□ 约_____并发数

4.4　高峰使用并发用户数

□ 约_____并发数

4.5　用户高峰访问时段

□ _____

5　信息系统对安全的需求

5.1　等级保护定级情况

□ A：定为等级保护_____级　　□ B：未定级

5.2　是否需要数字证书进行用户身份认证

□ A：是　　□ B：否

5.3　是否需要使用电子签章和数字签名

□ A：是　　□ B：否

5.4　是否需要对分级部署的系统间传输的数据进行加密

□ A：是　　□ B：否

5.5　对安全方面的其他需求

□ _____

6　信息系统建设进度情况

6.1　目前的建设阶段

□ A：已经正式运行　　□ B：正在开发和测试阶段

□ C：还未正式启动

6.2　信息系统运行预计开始时间

□ A：_____年　　□ B：没有明确计划

7　信息系统统一门户集成需求

7.1　是否有面向公众的门户页面

□ A：有　　□ B：没有

7.2 哪些信息和功能需要在机构统一门户中展现

□ A：无

□ B：若有请填写：_____

_____

8 信息系统统一用户集成需求

8.1 是否已实现单点登录(SSO)功能

□ A：是 □ B：否

8.2 若已实现单点登录(SSO)功能，是如何实现的

□ A：未实现 SSO 功能 □ B：本系统定制开发的 SSO 功能

□ C：使用_____(第三方软件厂商)产品实现 SSO 功能

8.3 用户口令是否加密存储

□ A：未加密 □ B：自定义加密算法

□ C：使用第三方标准算法加密

9 信息系统公共软件平台需求

9.1 对公共基础服务软件的需求(可多选)

□ A：LDAP □ B：电子邮件

□ C：GIS □ D：电子签章

□ E：报表/BI □ F：非结构化数据内容管理

□ G：数据传输/交换 □ H：数据采集

□ I：其他(请注明)_____

2. 应用运行架构设计

根据收集和了解的应用运行环境需求，按照顶层设计的分析，在技术架构设计的指导下，对信息系统按运行环境进行分类和归并，再进行统一的运行架构设计，包括服务器架构(小型机/X86、虚拟化)、存储架构(SAN/NAS)、网络架构(网络出口、网络子网、网络安全区域)、容灾和备份架构(本地备份、异地容灾)等，并选择合适的公共平台软件，同时根据信息安全等级保护要求制定出完善的安全规划。

3. 服务器、存储、网络规划

根据统一设计的运行架构，结合各应用的运行环境需求，综合考虑可靠性需求和可扩展性需求，计算出服务器、存储和网络需求，包括服务器规格型号和数量(含操作系统、虚拟化软件等)、存储设备的规格型号和存储容量、网络设备的规格型号和数量需求。上述需求一方面作为设备采购的依据，另一方面也是机房规划的依据。

4. 机房规划

服务器、存储和网络规划完成后，就可以计算出基础保障环境总体电源和空间需求，从而进行机房电源和空间规划，包括电源功率、UPS 容量等。然后根据机构的实际情况规划机房的面积和位置，同时，根据应用的部署、服务器及存储等硬件设备和空间的情况合理设计机房的布局和机房内网络的综合布线。

机房规划可参照美国 TIA-942《数据中心通信网络基础设施标准》和中国国家标准 GB 50174—2008《电子信息系统机房设计规范》。

5. 建设和运维规划

最后，根据机构的信息化建设整体规划和投资规划，综合考虑最新的技术与成熟技术的平衡、最高性能与最优价格的平衡，制定一个近期的和一个中长期的基础保障环境建设规划，并设计出合理的运行维护方案，作为各年度信息化基础保障环境建设实施的依据和指南。

5.3　硬件基础设施规划

硬件基础设施规划包括网络环境、服务器环境、存储和备份环境以及机房环境的规划。

5.3.1　网络环境

数据中心的网络首先要有足够的端口和带宽，以满足大量服务器的网络接入需求，通常以千兆接入为主，存储以及虚拟机主机则尽量使用万兆接入；其次，应配置互联网链路负载均衡、应用负载均衡以及冗余的网络设备及网络连接，以确保数据中心网络无单点故障；此外，还应配备防火墙、入侵检测、安全审计等各项安全设施，以满足国家信息安全等级保护的要求。

数据中心的网络设计应遵循以下基本原则：

(1) 扁平化。为适应大规模虚拟化及云计算环境下业务需求，网络架构宜采用“大二层”方式，构建一个可扩展的扁平拓扑结构，从而实现虚拟机的无缝迁移。

(2) 虚拟化。数据中心核心网络设备除考虑高可用设计(如冗余引擎、冗余电源、冗余风扇等)外，更要支持虚拟化特性，将多台物理设备虚拟成一台逻辑设备，实现统一配置和管理，解决传统二层启用 STP 协议带来的计算复杂、收敛过慢导致业务中断的问题，也解决传统三层启用 VRRP/HSRP 协议带来主设备和备用设备切换对业务的影响及交换节点链路带宽浪费的问题。

(3) 可扩展。数据中心虚拟化以及 iSCSI、FC over IP 的应用都带来了数据中心流量模型的改变，核心网络设备的模块化设计和可扩展性就变得尤为重要。

(4) 高安全。网络设备应具有诸如路由协议加密、MAC 地址过滤、动态 ARP 检测、ACL 等一系列安全特性，能按业务进行分区，实现各个业务区域网络相互独立、互相隔离，确保业务安全。

5.3.1.1 网络拓扑结构设计

数据中心的网络一般分为边界层、核心层和接入层。接入层在物理上可以出现二到三级的架构，比如“独立接入交换机＋刀片服务器的交换机＋VMware 虚拟交换机”的架构。

- 边界层。机构对外的网络出口一般都放在数据中心，采用双出口或多出口连接到不同的 ISP，以实现链路负载均衡和网络出口的可靠。网络出口通常采用静态路由协议，以确保出口路由稳定。同时，应在网络边界部署防火墙以抵御来自外网的网络攻击。边界防火墙的访问控制规则往往比较粗粒度，主要防止 DoS 攻击、端口扫描等，对单个服务器的细粒度的保护通常由数据中心内部应用入口防火墙解决。
- 核心层。核心层实现数据中心多个区的接入互联，并提供与网络出口的路由。核心层要求具有高可靠性、高交换能力和突发流量适应能力，同时核心层还应支撑 VLAN 以及 ACL 访问控制列表，以实现网络安全域的划分和管理。核心交换机可以采用两台物理设备虚拟成一台逻辑的、统一管理的虚拟设备，以实现高可靠性；接入交换机可通过多台堆叠后采用双链路分别上连到两个核心交换机上以实现冗余。
- 接入层。数据中心的接入交换机要求支持高密度千兆和万兆接入，以实现大量的服务器接入需求。综合考虑性价比，接入交换机的接入总带宽和上行带宽可以存在收敛比，也可以全线速无阻塞模式。接入层交换机要求具有良好的扩展性、关键部件冗余设计等功能。

在网络安全域的划分上，数据中心的网络可以分为信息服务域、数据中心内部域、网络服务和运维管理域等安全区域。通过设置严格的安全策略，实现不同安全区域之间的安全隔离。

- 信息服务域。包括各个业务系统的服务器和数据资源，实现机构信息服务资源的集中管理。信息服务域又可分为面向不特定公众的信息服务域、面向特定公众的信息服务域以及面向内部用户的信息服务域，还可以根据不同的业务进一步细分，以实现业务的区分和隔离。
- 数据中心内部域。此安全域内的资源仅限于数据中心内部的访问，包括各种数据库、存储设备等，根据业务需要，数据中心内部域也可以细分为多个不同的安全区域，相互之间实行逻辑隔离。
- 网络服务和运维管理域。网络服务主要包括 AD 域服务、DNS（域名解析）服务、DHCP 服务、邮件服务、对时服务（NTP）、代理服务、负载均衡服务等；运维管理则包括网管监控、服务器系统监控、机房监控等。根据服务的对象不同，可以进一步细分为外部访问和内部访问的安全区域。

5.3.1.2 路由策略和 IP 地址规划

在网络的路由策略上，所有服务器宜采用静态 IP 分配模式，各个子网的网关统一设在核心交换机上，出口路由采用静态路由模式，对于多出口采用链路负载均衡设备。防火墙则根据网络拓扑的具体结构采用网关模式或透明模式部署。

IP 地址的规划要与网络拓扑层次结构相适应。既要有效地利用地址空间，又要体现出

网络的可扩展性和灵活性，同时还能满足路由协议的要求，以便于网络中的路由聚类，减少路由器中路由表的长度，减少对路由器 CPU、内存的消耗。此外，还要考虑到网络地址的可管理性，对同一类业务应尽量分配连续的 IP 地址空间，以利于路由聚合以及安全控制，并为将来业务扩展后仍保持 IP 地址的连续性预留一定的地址空间。

5.3.1.3　网络服务

网络服务一般包括 Windows 域服务(AD)、DNS 服务、代理服务、邮件服务、NTP 服务、负载均衡服务等。

1. Windows 域服务

Windows 域服务是 Windows 系列的基本服务之一，它实现了全域 Windows 机器的统一用户管理、统一策略配置等功能。

2. DNS 服务

DNS 服务是网络的基本服务之一，它建立了主机名到 IP 地址的映射关系，是 WWW、FTP、电子邮件及其他互联网服务的基础。若机构网络采用的是私有 IP，则域名服务器通常会采用内外网分别部署或者是统一部署分区解析的方式。

3. 代理服务

代理服务(proxy)通常被用来连接 Internet(国际互联网)和 Intranet(内网)，在实现机构内部员工访问互联网的同时，确保机构内网与国际互联网的逻辑隔离。代理服务又可分为 HTTP 代理、Socks 代理、VPN 代理、反向代理等。

4. 邮件服务

邮件服务(E-mail)是网络上应用最为广泛的基本服务之一，它实现了机构内部以及与机构外部人员之间的电子邮件收发服务。通常邮件服务还需要配置垃圾邮件过滤服务、归档服务等。

5. NTP 服务

NTP 是一个跨越广域网或局域网的复杂的同步时间协议，它通常可获得毫秒级的时间精度。数据中心内各服务器需要根据一个统一的 NTP 服务器进行系统时间同步，否则将会导致系统日志数据时间错误，同时还会影响各类依赖系统时间的应用正常运行。

6. 负载均衡服务

负载均衡(LB)服务分为链路负载均衡和服务器负载均衡。链路负载均衡通常部署在机构网络出口，实现网络出口流量的分担。服务器负载均衡则把大量的用户访问请求分配到不同的服务器节点上，以提高整体的响应速度，同时也间接实现了服务器的高可用性保障。

5.3.1.4 网络安全

对数据中心整体的安全设计，要综合考虑安全域的划分、外部攻击的防范、操作行为的审计、安全事件的管理、安全漏洞的发现与预防等方面。网络安全规划需从网络结构、访问控制、边界安全、入侵检测、恶意代码防范以及相应的设备安全配置等方面入手。

以下是一些常用的网络安全防范手段。

1. 安全域防护

通过防火墙可以将网络划分成不同的安全域并进行有效防护，防火墙可以基于简单的ACL规则来进行数据包过滤，也可基于连接方向和连接状态来进行复杂的规则过滤。针对安全域的扩展问题，可以通过在防火墙上增加接口板的方式来实现对新增类型接口的处理需求。

2. 数据库审计和日志审计系统

记录所有的网络日志、系统日志、应用日志、数据库日志，包括操作发生的URL、客户端的IP、请求报文等内容，通过应用层访问和数据库操作请求进行多层业务关联审计，更精确地定位事件发生前后所有层面的访问及操作请求，使管理人员对用户的行为一目了然，真正做到数据库操作行为可监控，违规操作可追溯。同时，在受到攻击时能快速进行定位和问题分析处理。

3. 入侵防护系统

入侵防护系统(Intrusion Prevention System，IPS)整合了防火墙技术和入侵检测技术，所有接收到的数据包都要经过入侵防护系统检查之后才决定是否放行，或者执行缓存、抛弃策略，发生攻击时及时发出警报，并将网络攻击事件及所采取的措施和结果进行记录。

4. Web应用防火墙(WAF)

WAF是基于应用层的安全过滤和控制设备，WAF具备审计、访问控制、Web应用加固能力。

- 审计功能：用来记录所有HTTP会话数据或者仅仅满足某些规则的HTTP会话数据。
- 访问控制：用来控制对Web应用的访问，既包括主动安全模式也包括被动安全模式。
- Web应用加固：该功能增强被保护Web应用的安全性，它不仅能够屏蔽Web应用固有弱点，而且能够保护Web应用的编程错误导致的安全隐患。

5. 网络版防病毒软件

网络版防病毒软件通过集成平台实现对全网的所有客户端计算机防病毒的统一管理，确保各客户端计算机采用统一的防病毒安全策略、集中统一的病毒库更新、病毒的统一收集和上报等，还可能通过管理员实现远程的病毒查杀等功能。