Exchange 信息交换系统的结构与安全分析

汪成义　（武汉计算机外部设备研究所　430050）

摘要：本文总结了 Exchange Server 信息交换系统的基本构成；通过 Exchange 的内在层次关系，将各种结构归纳为三种结构类型，分析了各类型的特点及其适用对象；总结了相关安全措施，分析了它们的特点，并初步探讨了它们的适用场合或对象。

关键词：企业网　信息交换系统　电子邮件　Exchange　结构　安全

一、引言

MS Exchange 系统是美国微软公司的一个基于电子邮件服务的群件产品，它适于企业网络内部使用，并与因特网等有较好的连接。它是一个模块化的、采用客户机/服务器结构的、集成式系统监控和管理的电子信息交换系统。它的服务器端运行于 Windows NT Server，并与之紧密集成，具有一致的安全模型，多台 Exchange 服务器可协同工作，并支持广泛的客户平台，如 DOS、Windows3.x、WFW、Windows95、Windows NT 和 Macintosh 等。在功能上，Exchange 超越了传统的电子邮件系统，能更方便地收发电子邮件、进行小组讨论、安排小组日程、访问公告栏，能更方便有效地管理和维护系统，并与 Web、浏览器紧密相联。

作为微软 Backlffice 产品的组成成员，Exchange 与 IIS 相辅相成，是建设全面的企业新型网络或 Intranet 的基础之一。在具体策划、实施信息交换系统的建设时，须对系统的组成，可实现的结构类型及其相关特点、差别和适用对象有较全面的认识，才能组建合理、实用的系统，另一方面，只有对安全手段有较全面的了解，才能采取可信、有效、方便的安全措施。

二、Exchange 的基本组成

Exchange 系统由一系列组件组成，这些组件分别安装于 NT 服务器上作为 Exchange 服务器和各种操作系统平台上作为 Exchange 的客户端，具体为：

1. Exchange Server（信息交换服务器）

用于传递消息，存放邮件/数据信息，提供目录服务，提供一组消息传输代理，以及日程安排和密钥管理服务等。其核心组件包括系统助手(System Attendant)、目录服务(Directory Service)、消息传输代理(Message Transfer Agent)和信息仓库(Information Store)。另外，还有一组增强系统性能和连通性的组件，如 Internet 新闻服务(Internet News Service)、目录同步(Directory Synchronization)、密钥管理服务器(Key Management Server)等。

2. Exchange Client(客户端)

其核心组件是"浏览器"，用于对用户邮箱、公共文件夹和个人文件夹的各种管理以及阅读、编辑、修改和传送各种邮件；Schedule + 是另一组件，用于管理、协调个人的日程安排、工作安排和群组的活动安排；Forms Designer 是 Exchange 给用户提供的表格设计工具。

Exchange Client 可运行于 MS DOS、Windows 3. x(包括 WFW3.11)、Windows 95、Windows NT 和 Apple Macintosh System7。

3. Outlook(微软另一个能与 Exchange 紧密集成的客户端)

将电子邮件、个人组织和工作组软件与 Microsoft office 应用程序集成在一起，并以 Office 为基础，使组织可以开发和推广工作组应用程序。

三、Exchange 的层次结构及其特点

总的来说，Exchange 系统是一个具有可分为四层的总体结构，并通过各种连接器相互连接并对外交换信息的系统。具体来说，它分为组织(organization)、节点(site)、服务器(Server)、客户端(Client)四层，并通过 Site Connector 将组织中的两个节点相连，通过 MS Mail Connector 与 MS Mail(pc)和 MS Mail(Apple Talk)相连，通过 Interent Mail Connector 与 Internet 网相连，通过 X.400 Connector 与外界的 X.400 系统相连等。根据此四层的相互关系，以及企业网络规模、地域分布和组织结构的不同，可分别采用如下几种结构形式：

1. 单一节点单一服务器结构

该结构简单，易于安装、管理，适用于网络规模小，单一部门负责管理的网络。如机器不多的一般中小企业计算中心。对已建邮局(MS Mail postoffice)，可通过 Mail connector 与之相连，从而保留原有系统。通过 Internet connector 还可以与因特网相连，既收发企业内邮件，又能与外界进行邮件传递。

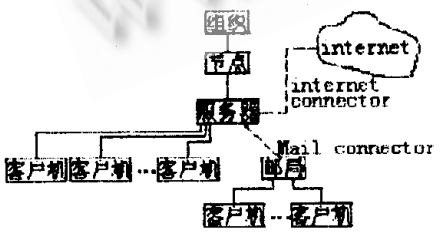

图 1　单一节点单一服务器结构

2. 单一节点多服务器结构

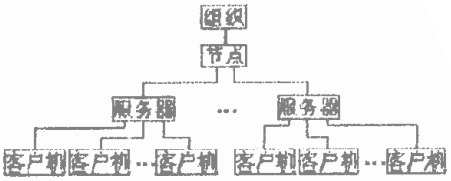

图 2　单一节点多服务器结构

该结构适用于地域相对集中、规模较大的网络。特别对于有多个备份域控制器协同服务的 NT 网络，以及有多个 NT 域，每个域的管理相对独立的网络，适合选用该结构。在该结构中，第一个安装的服务器是主服务器，其他服务器是从属服务器，它们共用同一全局地址簿。从属服务器拥有自己的邮箱，当主服务器出现故障或关机时，在该从属服务器上建有邮箱的客户可照常收发邮件。

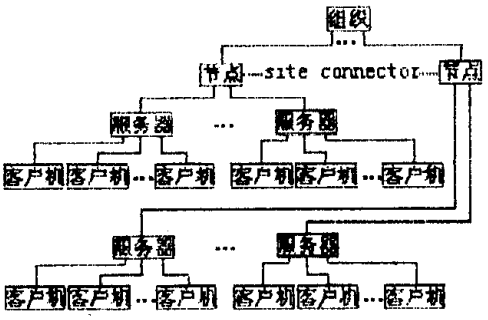

图 3　多节点多服务器结构

同样该结构通过 Mail connector 可与邮局共存，通过 Internet connctor 可接入因特网。

3. 多节点多服务器结构

该结构适用于规模大、地域分布广的大型网络，或者是部门间独立性、安全性强，联系较少的网络。如特大型企业，分布于不同城市的工商、税务之类政府职能部门等。在同一组织里有多个节点，每个节点可有一个或多个服务器，每个节点相对独立运作，并通过 site connector 与其他节点相连，构成一个整体。

同样该结构通过 Internet connector 可接入因特网，并可与 MS Mail Server、X.400、Lotus cc:Mail、DEC All-in-1 和 IBM PROFS 等邮件系统连接。

四、Exchange 信息交换系统的安全管理

Exchange 系统采用了多种安全措施对邮件进行安全保护，具体分为一般安全措施、帐户权限管理和高级安全管理。

1. 一般安全措施

(1)设定传输过程的加密状态，即在客户浏览器上的加密信息栏中选取“使用网络时”。

(2)设定脱机文件夹的加密状态，即可选为压缩加密、最佳加密或不加密。

(3)在“发送”选项中，将敏感度设为：

·私人：答复或转发邮件时，私人邮件将禁止任何收件人修改原始邮件。

·机密：根据管理员在服务器上设定的保密性策略来保密邮件。

2. 帐户权限管理

(1)用户帐户安全管理与 NT 帐户管理一致，Exchange 邮箱用户与 NT 域用户或 NT 域组对应。应在 NT 用户帐户管理和 NT 域间信任关系的基础上实现邮箱用户的权限管理。

(2)设定公共文件夹用户。这样，不同的公共文件夹只许可不同用户或不同组别用户访问。如实现小组讨论，部门公告栏、宣传栏等。

(3)授权代理访问，可让其他用户代理工作，访问其他用户文件夹或以委托人的名义发送邮件。如负责人授权秘书或助手代理工作。

3. 高级安全管理

通过 CAST 加密算法对邮件进行加密，在服务器管理员提供令牌并由用户设置成功后，可进入高级安全方式，具体体现在：

(1)将邮件内容与附件加密：密封发送的邮件及其附件，只能被发件人和由发件人指定的收件人阅读。如将企业主要负责人、技术骨干和销售主管人员的邮件授权可收发密封邮件，其他人员不能收发密封邮件。

(2)将数字式签名加到邮件中：为所有发送的邮件加上发件人的数字式签字，使收件人确认邮件的发送者。如企业领导发文。

由于美国出口政策的限制，在国内使用的 Exchange 系统，其加密算法为 CAST-40，而北美地区为 CAST-64 或 DES，故这里的安全性也是很有限的，对一般企业已足够，但对特殊单位或部门，还需作进一步的安全处理。

五、结束语

本文以典型信息交换系统 Exchange Server 为例，分析在规划电子邮件系统时，不同规模、类型的网络应采用的电子邮件总体结构类型，并总结、分析其相关安全措施，以便帮助进行企业内部网络或 Intranet 的建设，特别是电子邮件系统的建设。今天，电子邮件系统已不再孤立存在，已向群件发展，与 Web、浏览器混合并存，与数据库、办公软件相集成。文中缺点和不足之处，欢迎批评与探讨。

参考文献

[1] 微软. Microsoft Exchange Server Concepts and Planning Guide

[2] 微软. Microsoft Exchange Server Administrator Guide

[3] 微软. Microsoft Exchange Server Application Designer Guide

(来稿时间：1998 年 4 月)