Microsoft

Active Directory 服务实用教程

[美] Daniel Blum著
天宏工作室 译

清 华 大 学 出 版 社
http:www.tup.tsinghua.edu.cn

Active Directory 服务实用教程

[美] Daniel Blum 著
天宏工作室 译

清华大学出版社

(京) 新登字 158 号

Active Directory 服务实用教程
Daniel Blum: **Understanding Active Directory Services**
EISBN: 1-57231-721-3

北京市版权局著作权合同登记号 图字 01-2002-1117 号

图书在版编目 (CIP) 数据

Active Directory 服务实用教程/ (美) 布拉姆著; 天宏工作室译 .—北京: 清华大学出版社, 2002.12
书名原文: Understanding Active Directory Services
ISBN 7-302-05991-8
Ⅰ. A... Ⅱ. ①布 ... ②天 ... Ⅲ. 互连网络－软件工具, Active Directory Ⅳ. TP393.4
中国版本图书馆 CIP 数据核字 (2002) 第 080195 号

出 版 者: 清华大学出版社 (北京清华大学学研大厦, 邮编 100084)
http://www.tup.tsinghua.edu.cn
http://www.tup.com.cn
责任编辑: 林庆嘉
印 刷 者: 清华大学印刷厂
发 行 者: 新华书店总店北京发行所
开 本: 787 × 960 1/16 **印张**: 15.25 **字数**: 325 千字
版 次: 2002 年 12 月第 1 版 2002 年 12 月第 1 次印刷
书 号: ISBN 7-302-05991-8/TP·3573
印 数: 0001 ~ 2000
定 价: 29.00 元

作者简介

Daniel Blum 是 Burton 集团的资深副总裁和首席咨询师，是目录服务、公钥构架（PKI）以及电子商务安全咨询方面的专家。他一直为世界上一些最大的公司提供咨询，并与 Electronic Messaging Association（EMA）、Network Applications Consortium（NAC）、National Institute of Standards（NIST）以及 Corporation for Open Systems（COS）这样的贸易协会和标准委员会合作。他出版过书籍、行业报告并发表过文章。他在北美和欧洲各地发表讲演，作为分析家出现在公共电视上，主持行业会议，他的文章内容被大量引用。他还在 Network World 上定期主持专栏，在 http://www.tbg.com 上可以找到有关他与 Burton 集团的咨询业务的更多信息。

目录

第 1 章

Active Directory 服务简介

目录是分布式计算所必需的。

在我们这个时代，信息技术（IT）的最重要目标是部署分布式软件对象、分布式计算机文件系统、单一登录和公钥安全性以及如何进行集中管理。不过，具有讽刺意味的是，这些伟大目标的成功与否在很大程度上取决于一个微不足道的网络组件——电子网络目录，而许多开发商和大多数企业多年来都忽略了这一组件。本书将介绍 Microsoft Windows 2000 Active Directory（活动目录）服务，这是一个通用的目录产品，它将有助于把目录迁移到它们在用户网络、安全和应用程序环境中的适当位置。

1.1 目录的基础知识

本章描述了基本的目录概念并指出了适合使用 Active Directory 服务的情况。

网络目录（或简称为目录）是一个文件或数据库，用户或应用程序可以从中获得网络对象的参考信息。有一些专用目录，只有一种用途或只为一种应用程序服务，而通用目录可以执行许多功能。本章定义了专用目录和通用目录，并说明了它们之间的区别，从而为本书其余各章做好了准备。本章回顾了目录波澜起伏的过去，揭示了目前目录改进与合并的机遇，并解释了企业级目录对于开发和管理支持目录的应用程序及支持目录的网络至关重要的原因。本章还详细描述了 Active Directory 技术的适用环境，阐明了为什么这项技术如此重要的原因，并为读者介绍了各章的内容。

1.1.1 专用目录

目录是包含最少属性集的任何一个或多个项目列表。

大多数用户都部署了数十个(可能是数百个)目录作为在企业内的不同分公司、部门和工作组中使用的应用程序和网络的一部分。包含最少的属性集(名称、位置、地址和型号等)的任何项目(人员、打印机和服务器等)列表都可以是一个目录。每一个网络应用程序都有某种类型的目录以及哪些人可以在哪些时候访问目录的规则。

专用目录嵌在产品中。

顾名思义，专用目录只适用于一个物理设备（如文件服务器）或一个应用程序（如 Mricrosoft Exchange Server 这样的电子邮件系统)。这些专用目录经常被嵌在产品中，起到了地址簿或管理工具的作用。

1.1.2 通用目录

对通用目录的兴趣正在增加。

近来，随着企业越来越意识到管理多个目录所产生的隐含成本，对可以为多个应用程序提供服务的目录——换句话说，就是 Novell 的 Novell Directory Service（NDS）或 Netscape 的 Directory Server 这样的通用目录——的兴趣增加了。

通用目录可以支持许多应用程序和网络服务。

正如在我公司关于支持目录的计算的报告中讨论的[①]，通用的功能性目录是分布式计算基础结构的重要组成部分。目录服务将与消息服务、安全服务以及组件软件架构一起在创建一种使用网络的新方式方面起到重要作用。而过去的专用目录无论如何也无法支持这种巨大的变化。

通用目录改进了网络的可管理性。

通用目录使用户可以在企业一级上有效地部署和管理不同的应用程序、安全性和网络基础结构组件，它是定义下一代网络服务和应用程序的重要部分。来自多个开发商的应用程序和组件会反复使用这种目录。这些目录为网络用户、资源和对象提供了企业级的可视性、管理能力和安全性。在大型企业中，不会只依赖于一台单独的服务器，并且通常会联合使用多种产品。

---

① 《Directory-Enabled Computing: The Directory's Expanding Role》，作者是 Larry Gauthier 和 Jamie Lewis，Burton Group，1998 年 9 月，Web 地址为 http://www.tbg.com ——原著者注。

在大多数情况下，通用目录产品必须不仅能与多种应用程序和用户交互，还将与其他开发商的目录服务一起工作。这意味着通用目录产品必须灵活且基于标准化。通用目录不仅仅是一个单独的产品，它们其实是包含多个产品的集成目录环境。在本章中，我们将注意到通用目录可以充当三个或更多角色：在网络操作系统（Network Operating System，NOS）一级上、作为企业级目录以及作为电子商务级目录操作的一部分。我们还将揭示 Active Directory 适用的位置及其原因。不过，首先我们将回顾目录的简短历史，并介绍通用目录的一个商业案例或经济理由。

通用目录必须是基于标准的。

1.1.3　目录的历史：波澜起伏的过去

在目录策略文档中，Microsoft 曾经将目录描述为在网络上组织、管理或定位对象的工具。网络对象是用户（以及应用程序）完成其工作所需要了解的项目，如用户、打印机、文档、电子邮件地址、数据库、分布式组件以及其他资源。目录的最简单形式是提供电话簿白页这样的服务。例如，在输入一个人的姓名后返回一个地址和电话号码。目录服务还可以充当黄页，例如提供建筑物内的所有打印机的列表。用户、管理员以及他们使用的应用程序总是需要目录。为了满足这种需求，人们建立了专用目录，现在的问题是专用目录太多了。

目录一直是在网络上定位信息所必需的。

在 60 年代和 70 年代网络计算的初期，网络对象及其定位器直接在它们自己的程序中被编码或者存储在主机或工作站上的参数文件中。例如，用户曾经维护了一个名为 hosts 的文件，其中包含了因特网上所有主机的名称和地址。当计算机的地址改变后，用户更新这个文件，应用程序将继续运行。用户将 hosts 文件复制到各个位置，以保持它们之间的同步。不过 hosts 文件最终会变得太大，而更改也太频繁了。因特网转向了一种更加动态的、基于服务器的目录，称为域名服务（Domain Name Service，DNS），如果给出一个包括主机域（如 www.rapport.com）的主机名，它就会返回该主机的 IP 地址。DNS 是第一个标准化的目录，也是最成功的一个。

DNS 用来使 Internet 上的资源位置更易于管理和扩展。

单有 DNS 还不够，很快又发展了其他许多基于网络的目录。

不过，Internet 和 DNS 经历了数十年才成为行业中的重要力量。随着时间的推移，人们还为 Novell NetWare、Microsoft LAN Manager、Banyan VINES、DECnet、IBM 的 SNA 以及其他许多专用网络开发了目录。这些系统都不使用 DNS，因为 DNS 和 Internet 的情况仍然不明朗。但是开发商确实遵循了构造基于服务器的目录的 DNS 方式。

DNS 缺少关于人员和其他对象的详细信息，这促使人们开发了其他不太成功的目录标准。

虽然 DNS 和其他早期网络目录比较先进，但是它们只包含有关主机、域和地址的信息。在包含大量信息的网络计算环境中，用户还需要存储有关人员、组织、服务、资源和应用程序等的信息。基于这种认识，国际标准组织于 80 年代中期尝试创建一个丰富的、面向对象的目录标准，称为 X.500。正如我们将会看到的，X.500 的继承者轻量级目录访问协议（Lightweight Directory Access Protocol，LDAP）过了多年才得到广泛应用。

由于缺少目录标准，通用目录没有继续发展下去，而目录的种类却在激增。

与此同时，因为不能在友好的邻居目录中找到丰富的信息仓库，所以无数应用程序开发人员和用户开始创建专用目录，如电子邮件目录、人力资源目录、电话目录以及能想像到的其他任何专用目录。更糟糕的是，其他开发商继续依赖基于工作站的目录，如 Windows 注册表及类似目录。在典型的企业中，用户要面对数十个孤立的目录，与图 1-1 所示的窘境相似。

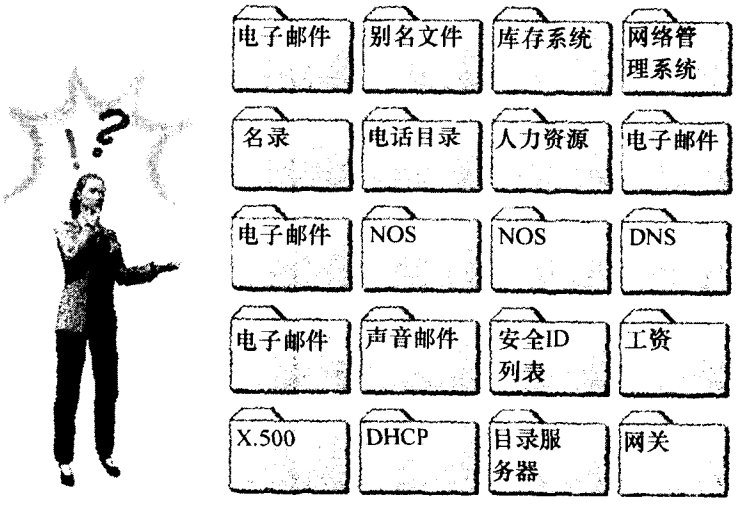

图 1-1　过多的目录

1.1.4　成本的现状

独立的目录产生了庞大的隐含成本。

对于目录繁多造成的后果，可以用一个词来表示：成本。不幸的是，目录成本是隐含的，公司通常会忽略它们。目录几乎总是与它们的上一级应用程序捆绑在一起的。如果没有目录，那么电子邮件系统、网络操作系统（NOS）以及人力资源（HR）系统就不能运行，因此开发人员通常不对它们另行收费。但是这并不意味着目录是免费的。

成本是隐藏在重复的支持需要和损失的生产力中的。

一些隐含的目录成本源于支持包含相同信息的重复系统。这些隐含的成本主要是人力成本，包括培训、安装、配置以及管理。例如，在电子邮件数据库（Daniel.Blum）、NOS 目录（dblum）、人力资源数据库（Daniel J. Blum）以及图 1-1 所示的其他所有目录中，都可以找到企业网络上的各个用户的项目。在每次必须更改用户项目（如聘请、终止、结构重组、站点移动、网络升级或其他一些操作）时，都必须更新部分或全部目录。

低质量的目录信息内容降低了用户的生产效率。

无效或过时的目录信息会产生额外的隐含成本。用户不能在网络上彼此找到对方，从而无法进行通信。邮件会丢失，导致出现误会。新员工不能访问他们需要使用的系统。用户必须使用多个密码登录到多个系统，这是很难管理的。当员工离开公司而没有删除登录 ID 时，用户就会面临安全风险。

在目录的当前状态中隐藏着很高的机会成本。

还有一些机会成本。当企业或业务单位需要新的应用程序时，该应用程序很可能需要使用目录来管理用户、路由、安全性、组以及其他信息。然而，支持应用程序目录的人员会干扰应用程序的部署。需要做的工作很多，而所用的时间又很少，因此很可能没有足够的资源或预算来部署该应用程序。在部署应用程序时，缺少目录基础结构可能会限制其管理、安全性以及所有一体化功能在企业网络中的使用。

1.1.5　通用目录的商业分析

一旦集成的目录基础结构取代了孤立的目

如果企业可以将孤立的目录合并成一个集成的通用目录基础结构，允许从一个位置管理大多数应用程序，那么情况会怎样

录，企业就将获得增值并节省大量成本。

呢？这种理想的目录环境会减少培训、安装、配置以及管理的成本。使新的应用程序支持目录也更容易，信息会更快地更新。随着每一个新应用程序利用目录基础结构，成本的节省将会增加。这些想法形成了通用目录服务的经济合理性或商业分析的核心。图 1-2 显示了多个应用程序和服务共享一个通用目录基础结构的概念。

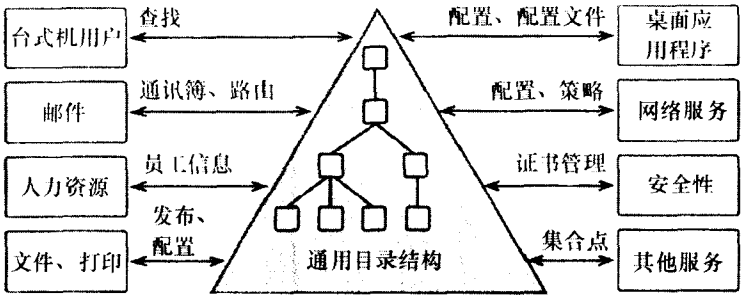

图 1-2　多个应用程序使用的通用目录基础结构

通用目录基础结构会降低 PC 的所有者成本。

可管理的通用目录基础结构为企业提供了降低工作站或 PC 维护费用（估计目前每台 PC 每年大约需要数千美元）的机会。目录可以集中存储桌面设置和其他配置项目，否则就需要在基于工作站的文件、脚本或注册表中保存这些项目。如果信息位于工作站中，那么进行更改就需要在每一台工作站上进行，而当信息转移到网络目录上时，只需进行一次改动即可。支持目录的早期服务（如 Novell 的 Z.E.N.works 以及 Netscape Mission Control Desktop）都证明了这个概念，Microsoft 也在其 Zero Administration Initiative for Windows（ZAW）中采用了这个概念。

通用目录可以支持许多应用程序并使安全系统更易于管理。

桌面用户将可以通过容易使用的白页视图、黄页视图甚至简单的桌面快捷方式来查找目录中的信息。电子邮件系统可以从目录系统中获得通讯簿和路由信息。合并到通用目录中后，就更容易管理安全系统的证书，也更容易查找共享文件和打印系统的信息。用户可以很容易地在网络上查找对象，服务可以在企业范围内发布和配置信息，还可以将安全权限灵活地扩展到外联网或贸易伙伴群体中。

电子商务、VPN 以及外联网需要通用目录支持。

目录还使企业可以将它们的内联网扩展到虚拟专用网络（Virtual Private Network，VPN）或外联网，为外出员工、贸易伙伴、用户以及供应商提供安全的数据库访问、消息传递、协作