网络操作系统的目录服务

摘要：以Windows 2000操作系统的重要组件活动目录为例，介绍网络操作系统的目录服务特性。目录服务作为当今分布式网络系统的重要管理工具，实现了网络的集中管理，对各种网络资源提供一种统一的命名、定位及访问的方法，提供单一且一致的管理点，同时结合操作系统的管理和安全机制，提供实现网络的完整性和保密性，使各种资源能协调有效地工作。

关键词：目录服务 活动目录

齐幼菊 （杭州 浙江广播电视大学计算机教研室 310012）

1 引 言

早期的网络操作系统一般只提供简单的文件服务和打印服务，然而现代网络由各种相互依赖的资源所组成，解决网络中各种分散资源的管理问题变得相当复杂，提供简单透明的中心化管理及强大的安全服务已成为相当重要。Novell 在其网络操作系统NetWare 4.0中提出了目录服务（NetWare Directory Service）的概念，Microsoft 也在Windows 2000中提出了活动目录（Active Directory）和集成化目录服务的概念，从而隐蔽了错综复杂的网络物理拓扑结构，实现了网络的透明管理，提供了强大、统一的网络安全服务及开放式同步机制，为多种技术的协同运行提供条件。随着网络中各种资源数量的急剧增加，目录服务作为网络系统的管理工具变得越来越重要，已成为大型分布系统的轴心，理解目录服务对于理解网络操作系统的整体价值是十分重要的，它为现代商务企业组织机构提供关键的商务技术。本文以作为Windows 2000操作系统的重要组件活动目录为例，初步探析网络操作系统的目录服务特性。

2 什么是目录服务

目录服务作为网络操作系统的关键部分，提供在分布式网络环境中实现集中管理的机制，管理分布式资源之间关系的认证和代理，使各种资源能协调工作。

目录服务的主要特性有：存储作为目录对象的网络资源信息；定义这些对象的类和属性以及描述和访问控制方法；全局目录信息的更新及时复制到域中所有域控制器；提供一个准确的查询和索引机制；加强网络登录安全控制以及对目录数据的访问控制。

目录服务简化了网络管理，对各种网络资源提供一种单一的、一致的管理点。为用户提供单一注册机制，即用户一次登录就可获得各种网络服务，同时也加强了网络安全性。

3 Windows 2000 操作系统的活动目录

Windows 2000的活动目录概念包括目录和与目录相关的服务两方面。目录是存储各种对象的一个容器，目录服务是使目录中所有信息和资源协调工作的各种服务。活动目录是一个分布式的目录服务，包含用户和资源管理、基于目录的网络服务、基于网络的应用管理三个方面的内容，是一套改进了网络管理和系统互操作性、加强了安全服务的一个集成的目录服务，是一个使用Internet标准的企业级的可扩展可伸缩的目录服务，能满足商业ISP的需要和企业内部网及外联网的需要。活动目录集成了关键服务，如DNS、MSMQ（消息队列服务）；集成了关键应用，如电子邮件、网管、ERP等；集成了关键数据访问，如ADSI、OLE DB等；还集成了关键的安全性，如Kerberos和公开密钥基础设施等。

3.1 目录对象

活动目录使用对象代表网络资源，系统提供了大量的标准对象类型如域、组织单元、用户、组、计算机、卷、打印队列等。同时管理者或开发者也可以建立自己的目录对象类型或用新属性扩展现有的对象。如用户对象已有姓名、职业、电话号码、E_mial地址等属性，若需要添加身份证号码这一属性，则可以方便地扩充。如需要增加新的对象类型可以通过定义或举例的方式加入，从而实现了对象类的扩展。

3.2 目录结构

活动目录采用层次化可扩展的域结构，将域中的对象组成包容结构（Container）即组织单元（Organizational Unit，OU）结构，可以把反应企业组织结构的组织单元

嵌入域中以建立组织模型构成域树，并对各个组织单元视其现实组织关系授予不同的管理权限。并可把多个域组合起来构成域森林，形成广域网模式。活动目录分层结构可灵活配置，集中的组织机构可更合理地组织资源，以优化其可用性和可管理性。这种域树与域森林的方法，使活动目录用容器层次来模拟一个企业的组织结构。组织中的不同部门可以成为不同的域，或者一个域中有层次结构的组织结构，从而采用层次化的命名方法来反映组织结构和进行管理授权。Windows2000 Server 采用静态访问权继承（Create Time 继承）可获得很好的访问控制验证性能，在容器上定义的访问控制信息可以向下流动到容器的子对象。在创建子对象时，从容器继承的权限将与新对象的默认访问权合并。目录按组织结构进行管理授权，在加强集中管理的同时，增加了充分的机动灵活性，可以解决很多管理上错综复杂的问题。

例如某企业的域树下，可建立一个本土的总部组织单元（OU）和多个国外分部组织单元（OU）。在本土的总部组织单元（OU）可建立各种下一级组织单元（OU），如人事、财务、开发、维护等组织单元，同样在国外分部组织单元（OU）可建立诸如销售、技术支持、培训等组织单元，并把特定组织单元的管理权授予指定的用户或组。如该企业兼并了某公司，则可以加入该公司域，构成域森林。域与域之间可以通过双向、传递的委托关系建立符合企业要求的管理关系。活动目录支持集中化、分散化或既有集中又有分散的业务模型，建立符合业务组织环境中的各种复杂的管理关系，并可非常灵活地调整其组织结构。

活动目录为网络提供一种统一的组织模型，不管网络资源信息处在什么地方，用户无论从什么地方访问，系统对用户都将提供一个统一的逻辑视图，屏蔽了实际的网络物理结构，为用户和管理员提供了极大的方便。活动目录支持现有标准和协议，与域名系统（DNS）紧密集成。使用DNS作为定位服务，实现整个网络资源的单点管理。

3.3 目录复制

在活动目录中只有域控制器，且所有域控制器是对等的。同时为了提供分布式环境的高性能、高可用性和灵活性.。目录信息分散在多台域控制器中，保证了网络快速响应及其容错性。活动目录采用多主复制技术，采用“更新序列号（USN）”技术，随对象的创建或修改使所在服务器立即自动更新一个64位序列号，所有服务器都跟踪其复制伙伴收到的最新USN，复制与本域相关的对象和元数据、域树中所有域的列表和全局目录服务器的位置等信息的更新部分，以避免复制大量数据。多主复制技术保证信息的有效性、容错性，提供网络的负载平衡。在一个域中的多个域控制器，如果其中一个域控制器减速或停止或甚至失败，同域中的其他域控制器则可及时提供必要的目录访问。这种完全同步的目录拷贝技术使得在广域网（WAN）中可利用本地目录服务即可定位资源，实现本地与远程管理。

3.4 互操作性

为支持多操作系统及其目录同步和互操作性，活动目录为各种不同的系统、应用程序集成和公开同步机制提供一套标准的接口（如LDAP、ADSI、JADSI、MAPI），以便企业合并现有的目录，并确保 Windows 与更大范围的应用程序和设备的互操作性。可将多个应用程序目录的管理合并在一起，使用开放的接口、连接器和同步机制，组织机构可对多个目录（如Novell的NDS 、LDAP、ERP、Email以及其他关键任务的应用程序）进行合并。避免了用户以不同的帐号和密码登录不同的系统，以及必须正确定位网络资源位置的麻烦。也避免了网络管理员及应用程序开发人员对不同目录的管理和开发任务。活动目录服务接口（ADSI）允许应用程序开发人员将基于COM的业务规则与存储在活动目录中的对象进行关联，使开发人员和管理人员可以通过这种一致和简单的方式与应用程序及其对象进行交互。ADSI是开放目录服务接口（ODSI）的一部分，抽象了来自不同网络提供者的目录服务能力以便为管理网络资源提供一组目录服务接口。Windows NT Server 4.x 、Novell NetWare 3.x 和4.x 以及活动目录和任何其他支持LDAP(Lightweight Directory Access Protocol)协议的目录服务都可以使用ADSI对象。同时简化了分布式应用程序的开发和分布式系统的管理。

3.5 安全性

活动目录和安全服务之间存在的基本关系已经集成到 Windows 2000 操作系统中，活动目录安全系统的域安全策略信息。对象及其属性的安全性能准确地对访问存储目录进行控制，在没有授权的情况下不能更改帐号限制或组成员资格。域之间默认的传递信任可简化域之间信任帐号的管理。给对象的所有属性授予统一的读、写访问权是对象创建者的默认访问权限，从而减轻了网络管理员的管理工作。

活动目录改进了密码安全性和管理，提供对最终用

（下转第 33 页）

（上接第 30 页）

户透明的、集成的和高性能的安全服务。嵌入了对Internet安全协议、多种身份验证机制（如Kerberos、x.509证书以及智能卡SmartCard等），公共密钥基础设施（PKI，Public Key Infrastructure）以及SSL上LDAP协议的支持，加快了网络应用服务验证速度，允许多层次的各户/服务器代理验证和跨域验证建立可传递的信任关系。为开展电子商务提供了条件，组织机构能将所选目录信息安全地扩展到防火墙之外即内部网络之外的用户和电子商务客户。活动目录通过允许管理员使用相同的工具和过程，来管理访问控制内部用户、远程拨号用户和外部电子商务客户的用户权限。

管理代理使组织可将安全管理限制在整个组织域的某个子集，如在责任区域内授予更改属性、增删某类型对象等的权限，使基于职责的安全性与组织的商务过程保持一致。活动目录提供用Directory Service Administration用户接口可以方便地查看代理信息。

4 结论

在各种网络资源不断增长、扩散的网络系统中，要充分发挥网络资源的作用，目录服务已经成为网络操作系统的关键部分。目录服务所提供的在分布式网络环境中的管理机制，使日益错综复杂的网络系统能协调地工作，无论是网络管理员，还是网络应用开发人员或用户都避免了各种复杂的处理，提高了网络的易用性、可扩展性、安全性和可靠性，降低了网络的运行成本，提高了网络的整体性能。■

参考文献

1 www.microsoft.com/windows/server