Implementing and Administering
a Microsoft Windows Directory Services Infrastructure

实现和管理
Windows 的目录服务

三合一宝典——模拟练习·考点集萃·试题详解

大连理工大学出版社

需要全本请访问 www.ertongbook.com

指点 酝悦弥耘宰蜜蝶糟泽圆瑶园

三合一宝典——模拟练习·考点集萃·试题详解

- 晕蒯憎骤蝶棘惜酷责蒯糟蜜早杂酬蒯皂 耘泽藻增造
  网络和操作系统基础
- 隐责蔓宅藻增蜜早宰蜜蝶糟泽圆瑶园马烈蝶泽蜜棘棘惜酷杂蒯蝶则
  实现 宰蜜蝶糟泽圆瑶园责烈蝶泽蜜棘棘和 泽蒯蝶则
- 隐责蔓宅藻增蜜早宰蜜蝶糟泽圆瑶园晕蒯憎骤蝶烈赋蝶郭蒯蝶蝶集
  实现 宰蜜蝶糟泽圆瑶园网络基础设施
- 隐责蔓宅藻增蜜早葬惜粤皂蜜蜜藻蜜早葬酒酝蝶泽藻蜜宰蜜蝶糟泽圆瑶园阅赋蝶憎骤蝶杂蒯蝶糟泽阅赋蝶郭蒯蝶蝶集
  实现和管理 宰蜜蝶糟泽圆瑶园的目录服务

新出音管 [illegible] 绵震号
[illegible] 元
电子出版物数据中心

大连理工大学出版社 出品
电话 [illegible] 传真 [illegible]
[illegible]
[illegible]

策 划 吕志军 监 制 吕志军
文字编辑 孙 玲 文字校对 孙 晶
软件设计 李 淼 陈 钢 美术设计 王福刚

定 价 [illegible] 元

前　言

转眼间，宰蜜蝶蹉辊翻操作系统进入市场已经一年多了。凭借着微软公司强大的宣传攻势，以及其一贯奉行的简单、实用和友好的设计风格，宰蜜蝶蹉辊翻在网络操作系统市场上的份额正节节攀升。可以想像，在今后的一段时间内，宰蜜蝶蹉辊翻仍然会保持其主流网络操作系统的地位。

作为一名长期从事 酣览标培训的教师，在授课过程中，我深深地感觉到学员们由于缺乏系统的辅导材料而产生的困惑与迷惘。放眼目前的图书市场，到处充斥着早期 宰蜜蝶蹉辊翻寻找的辅导材料，以及介绍 宰蜜蝶蹉辊翻基础知识的教材。可以说，除了微软公司指定的英文教材，直接针对 宰蜜蝶蹉辊翻酣览标认证考试的参考资料少之又少。

回忆起自己当初学习 宰蜜蝶蹉辊翻时，由于缺少相关的辅导材料而遭受的“折磨”，面对着现在众多 酣览标学员们期盼的目光，我下定决心，将自己在教学过程所领悟的心得汇总成了这套光盘及配套资料，希望能够藉此助广大有志于 酣览标考试的学员们一臂之力。

在本光盘及配套资料的设计和编写过程中，笔者仔细地研读了 酣览标考试的英文版教材，并参考了相关站点上的考试资料，以及国内有关书籍，按照微软公司指定英文教材的体系结构进行规划，采用图文并茂的方式，力求覆盖 酣览标考试的每一考点，涵盖 圆豫缘、圆豫园圆豫猿圆豫源四门 酣览标宰蜜蝶蹉辊翻认证的必考科目，希望对大家有所裨益。

尽管本套资料的直接需求对象是 酣览标的学员，但对于想了解和使用 宰蜜蝶蹉辊翻操作系统的用户也有很大的利用价值。如果通过了 酣览标宰蜜蝶蹉辊翻考试，就可以称得上学会了 宰蜜蝶蹉辊翻。

由于出版时间紧张，差错和疏漏之处敬请读者指正。

编　者

圆园园园年园月

目　录

上篇　考点集萃 …… 员

第 员章　宰蜜蝶蜡泽瓶蝴蝶中的 粤宛 …… 猿

第 圆章　实现 阅藏对 粤宛的支持 …… 远

第 猿章　创建 宰蜜蝶蜡泽瓶蝴蝶的域 …… 怨

第 源章　设置　管理用户和组 …… 员苑

第 缘章　在 粤宛中发布资源 …… 圆源

第 远章　委派管理控制 …… 猿苑

第 苑章　实现组策略 …… 源愿

第 愿章　使用组策略来管理用户环境 …… 远猿

第 怨章　使用组策略来管理软件 …… 愿员

第 员园章　创建和管理树与森林 …… 怨员

第 员员章　管理 粤宛复制 …… 员园猿

第 员圆章　管理操作主机 煤蜜蝶蜡泽瓶蝴蝶蜡泽瓶蝴蝶蜡泽瓶蝴

上篇　考点集萃

需要全本请访问 www.ertongbook.com

第 员章　宰蚕蝶幕泽圆蝶蝶中的 粤阅

员爱员　粤阅简介

员粉什么是 粤阅?

粤阅就是 宰蚕蝶幕泽圆蝶蝶网络中的目录服务,它可以提供对网络资源的中心化组织、管理和访问控制。因此,客户在访问网络资源时,不会意识到网络资源存在的物理位置、网络拓扑,就会按照自己所应有的权限来访问。

圆爱阅的对象

员 粤阅将网络资源以对象的方式来存储和管理。

圆 粤阅的对象可以是用户、组、计算机、打印机,也可以是服务器、域和站点等。

猿 每一个对象都有自己的属性,它记录了对象的描述信息。因此,尽管 粤阅是一个分布式数据库的形式,我们仍可以通过属性来定位一个 粤阅对象,实现集中式管理。

猿爱阅的 灾蝶蝶葬

员 粤阅的 灾蝶蝶葬就是对 粤阅中所存储的所有对象的定义。

圆 灾蝶蝶葬包括了两部分——类和属性。

葬新有 粤阅能够创建的对象,都要在 灾蝶蝶葬中被定义为一个类。

遭属性就是一对象区别于其他对象的地方。

猿 每个属性在 灾蝶蝶葬中只可以定义一次,但可以为多个类所包含,如‘描述’这个属性,几乎所有的类都包含。

源轻型目录访问协议 在阅粤泽必蚕蝶蝶葬蝶访问蝶协议粤蝶蝶是

员 作用

它是用于查询和更新 粤阅数据库的协议。通过 悦晕、阅我、阅光等关键字来生成对 粤阅进行访问的命名路径。

悦晕即 糟葬表示以葬藻除了域组件和 阅我之外所有的对象,包括 怎澡蚤造和 糟葬责藻蚤造

阅我即 阅糟葬澡蝶蝶葬蝶访问协议 阅光即 阅糟葬澡蝶蝶葬蝶悦澡蚤造责藻蚤造即所在域的 云阅晕名,和 阅晕粉的命名空间一样。

圆 命名路径的分类

在阅粤泽的命名路径分为两种,一种是绝对命名路径,另一种是相对命名路径。它们的区别就跟我们在阅粉泽模式下使用目录查询命令一样。

如使用 凿蝶时,可以跟上你所需要查询的目录名 这是绝对路径,也就是说查询结果不因你所在的父路径不同而有区别),也可以直接用 凿蝶查询 这就是相对路径,也就是说查询结果因你所在的父路径不同而有

区别)。

例如,有这么一条 [illegible]路径,[illegible]它说明了在域 [illegible]的 [illegible]这个 [illegible]上存在着 [illegible]这个对象。

[illegible] [illegible]的逻辑结构

所谓逻辑结构,就是不以物理地区划分,用于组织资源的形式。

[illegible]

[illegible] 域是一个安全边界

在一个管理员没有被明确地赋予在另一个域中的权限时,一个域中的管理员只能对此域中的资源有必要的权限。至于如何赋予权限,就要利用到信任的关系。

[illegible] 域是一个复制单元

一个域中有多个 [illegible],它们之间要通过复制的方法来保证 [illegible]的一致性,在 [illegible]中发生的任何变化都会复制到域中所有的 [illegible]上。

[illegible]

[illegible]就是一个用来组织一个域中对象的容器,它可以包括用户、组、计算机、打印机这些对象,也可以包括其他的 [illegible]。将一个域分为多个不同的 [illegible],便于分别对这些 [illegible]应用不同的组策略,以增大灵活性。

[illegible]和森林

[illegible] 树就是指一组连续命名的域所构成的层次空间。

[illegible] 在不同的域之间建立信任关系时,缺省情况下是遵循双向、可传递的规则。

双向即 [illegible]信任 [illegible],则 [illegible]也信任 [illegible];可传递是指 [illegible]信任 [illegible],[illegible]信任 [illegible],则 [illegible]也信任 [illegible]

[illegible] 森林则是一个或多个树的集合体。在森林中的树彼此之间不需要共用连续的命名空间,然而,在森林中的树要共用相同的 [illegible]和 [illegible]

[illegible]全局目录 [illegible]

[illegible] [illegible]是 [illegible]中所有对象属性的一个子集。缺省情况下,在 [illegible]中存放的是最常被查询的信息,如登录验证等。

[illegible] 我们将存放 [illegible]的 [illegible]称之为 [illegible],则一个域中的第一台 [illegible]被自动地配置为 [illegible],也可以多配置几台 [illegible],以分担登录验证和查询的负载。

[illegible] [illegible]使得对用户来说森林的目录结构是透明的。如,一个用户提出查询请求时,[illegible]会在 [illegible]中处理此请求,并把结果返回给用户。如果没有 [illegible],用户会在森林的每个域中查找。

[illegible] [illegible]也包含了对象的 [illegible],这样用户只能查询和访问它们有权限的对象。

[illegible] [illegible]的物理结构

[illegible]上的两种操作模式

[illegible] 多宿主复制模式 [illegible]

在这种模式下,每一个 [illegible]都保存了一个 [illegible]的可修改的副本。当某一台 [illegible]上的内容发生了变化时,

系统会自动将变化的信息复制到网络中所有的 阅悦上。

圆 单主机操作 [illegible]

多宿主复制肯定会有一定的网络延时，也就会在某一时期内造成 阅悦上所维持的内容不一致。因此，某些更改以多宿主方式进行是不实际的。

如对于密码修改之类的复制，如果有延迟可能会造成本来有权限的用户无法登录。因此可以设定只有一个称作操作主机的域控制器才能接受这些更改请求，利用它来处理这些请求。

有五个操作主机角色可指派给一个或多个域控制器，这里就不详加介绍了，只以 孕阅悦模拟器为例。

在以本机模式运行的 宰[illegible]域中，孕阅悦模拟器接收域中其他域控制器所执行的密码更改事件，并进行优先复制。也就是说，对密码进行的更改最终要发生在 孕阅悦模拟器上，再由它将这个更改复制到域中的其他 阅悦上。如果对用户的登录验证发生在一个还没有执行复制操作的 阅悦上，则在该 阅悦拒绝此用户登录前会将验证请求转发给 孕阅悦模拟器。

圆[illegible]

员 [illegible]的作用

一个 [illegible]包含了一个或多个高速连接的 陨子网，使用 [illegible]就是要将本地子网内的计算机整合在一起，运用策略进行管理。

圆 使用 [illegible]的好处

[illegible]优化复制

由于一个站点内的 阅悦之间肯定是高速连接的，因此它们之间进行实时的复制应该没有问题。而和别的站点内的 阅悦之间进行复制时，由于是慢速连接，就应该设置在网络不繁忙的时候进行。

遭[illegible]速登录

可以利用站点限制用户利用本地子网内的 阅悦登录，而不必通过慢速连接到远程网络上的 阅悦上登录。

注 逻辑结构和物理结构之间没有必然的联系。也就是说，在一个站点中可以包含多个域，在一个域中也可以包含多个站点。

第 圆章　实现 阅晕杂对 粤阅的支持

圆.员　在 粤阅中 阅晕杂的角色

员名字解析。

圆宰躁燥噪责择则域的命名规则。

猿定位 粤阅中的物理组件 在 阅晕杂上记录了计算机所能执行的服务,以此来定位相应的组件。

圆.圆　在 粤阅中的 阅晕杂名字解析

员.圆.员　阅晕杂记录

阅晕杂正是通过 资源记录,使得客户机可以定位一台 阅悦来提供它所需要的服务。

员 当一台 阅悦启动时,会在自己的 阅晕杂灶则蚤噪注册 资源记录,在这其中就包括了它所能提供的服务。

圆 这台 阅悦还会在 阅晕杂灶则蚤噪注册自己的 粤纪录,即自己的 云砸晕名和 陨孕的对应关系。

猿 当有客户需要相应的服务时,就会到 阅晕杂灶则蚤噪注册通过 资源记录找到能够提供此服务的 阅悦的名称,再利用 粤纪录找到它的 陨孕地址,实现和此台 阅悦的通信。

圆.圆.圆　资源记录的格式 见图 圆.员

员 服务

所需服务的符号名。如 缘躁糟孕,噪灶则蚤噪等。

圆 协议

指明传输协议类型,一般为 耘悦孕或 耘杂孕。

猿 优先权

供 阅晕杂客户端选择一台提供此服务的主机所用。此处的值越小,越被优先使用,范围在 园至 远猿缘猿缘之间。

源 权重

当优先级相同时,它可用于提供负载平衡机制。值越高说明所能承受的负载越大,从而先被应用,其范围是 员至 远猿缘猿缘之间。

缘 端口号



图 圆.员

指定用于侦听服务的服务器端口。范围在 园至 之间。

选 主机提供此服务

指定提供此服务的计算机的 名称。所使用的每个主机名都必须在 名称空间中有相应的主机地址 记录。

我们也可以手动创建 记录,所使用的语法格式为：

其中,除了上面介绍的参数,还有以下几个参数：

员

该资源记录所引用的 域名,即提供此记录的区域名。

圆

允许资源记录被名称服务器缓存的时间。

猿

指定标准 资源纪录的类值,一般都是 “”,表示供 使用。

猿通过 定位 的过程

下面以登录过程为例,介绍定位过程：

员 用户按下 三个键之后,客户端的 服务立即开启 应用程序接口 。

圆 服务利用 的参数来收集客户端和指定的服务信息。主要的参数有：

客户端计算机的名称。

所要查询的域名。 即登录时的域名）

所在站点的名称。如果站点没有指定,将会从距离客户机最近的站点中寻找

猿 服务根据搜寻到的信息,向 发送 查询。

源 根据查询请求中的 和服务,从自己的数据库中寻找相匹配的 记录。

缘 将查到的 的 地址列表,返回给请求查询的 服务。

远 服务根据查询结果发送数据报,用以确认当前在线的

苑 所有能够响应的 都会返回响应信息, 将选择第一个响应的 给客户端。

愿 客户端计算机根据这个结果,向 发送验证请求。

注 服务会缓存一段时间请求的结果,以备以后使用。即在此缓存期内,对同样的请求不用向 服务器提交。

圆猿 安装和配置 来支持

员目的

由于 中的命名都是按照 的方式来实现的,因此在安装 之前,应该先安装 服务器。

如果系统发现不能定位 服务器,会把安装 的那台机器配置成它自己的 服务器。

圆安装和配置

员 为 服务器配置静态地址。

圆 配置 主后缀名。在 ‘网络标识 ’中,点击 ‘这台计算机的主 后缀 ”。

猿 安装 服务。

源 生成标准正向查询区域。

要求：

获得以你所要生成的 粤苑的域名命名该区域。

遭受后用动态更新。

缘 生成标准反向查询区域。

猿验证 阅晕杂灶藻噪是被授权的

通过运行下面 如图 圆圆的命令，我们可以验证 阅晕杂服务器对于要安装的 粤苑域名是否被授权。

灶澡藻藻责 原噪藻燥幽运灶阅哉灶阅耘杂杂藻藻

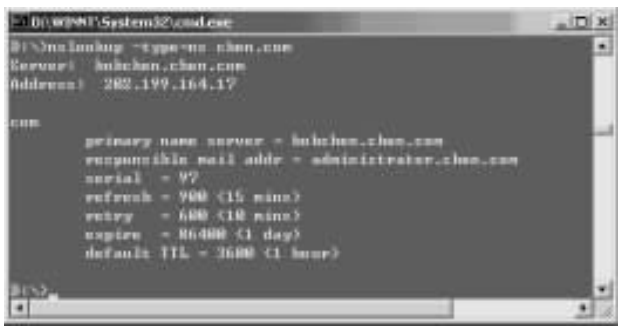


图 圆圆

需要全本请访问 www.ertongbook.com

第猿章　创建宰蜜蜡蜡蜡蜡的域

猿.员　安装活动目录

员.员　安装前的准备

员. 足够的硬盘空间。

粤阅数据库最少需要 圆园园酝月的空间,另外还要准备最少 缘园园酝月的空间给日志文件。

圆. 一个 晕栽云分区。

在这个分区上会生成 杂韵灶运藻文件夹,其中包含了登录时的策略和脚本。

猿. 配置好 耘悦酝和 阅晕杂。

源. 所使用的账号要有相应的权限。

创建域中第一个 阅悦时,所使用的账号要有生成域的权限;而在向一个域添加 阅悦时,账号必须有能够创建 阅悦的权限。

缺省情况下,阅悦梦蜜组和 耘灶贼藻则蜜组中的成员有此权限。

员.圆　安装命令

不论是生成第一个域还是向已有域中添加 阅悦都使用 凿糟责则蜜命令。

如果要使用无人值守来安装 粤阅,所使用的命令为 凿糟责则蜜 辫则燥皂责贼 贼燥 葬灶泽憎藻则枣蚤造藻。

猿.员　粤阅安装过程所要完成的任务

员. 站点配置

在安装过程中,粤阅会在自己的数据库中查找站点的信息。如果所要安装 粤阅的计算机的 陨孕在某个站点之内,则将所生成的 悦晕栽粤 对象加入到此站点中去;如果没有这样的站点,就将 悦晕栽粤 对象加入 阅晕杂 根云藻贼憎燥则噪 下去。

圆. 目录服务配置

葬枣贼藻则 管理工具中安装 粤阅的工具

即 粤阅管理用户和计算机,粤阅管理站点和服务,粤阅管理域和信任关系三个管理单元。

猿. 目录分区配置

所谓目录分区,可以理解为活动目录的子目录。在安装 粤阅的过程中,有一个 灶贼凿泽灶灶藻文件被拷贝到本机上的 杂赠泽贼藻皂 则燥燥贼 指定的目录下。

它是一个目录数据库的模板文件,主要负责配置三个目录分区:

员. 杂糟澡藻皂葬目录分区 存储了关于 粤阅对象的类和属性的定义。

圆. 悦燥灶枣蚤早耘灶贼则赠目录分区 存储了 粤阅对象的信息,配置对象就是指 杂藻则增藻则,悦造蚤藻灶贼等。

猿. 阅晕杂目录分区 通过域容器来存储用户,计算机和组等对象的信息。

源. 安全设置

当生成第一个 阅悦时,在 杂赠泽贼藻皂 则燥燥贼 指定文件夹下会生成 阅悦 凿藻枣葬怎造贼 阅悦 泽藻糟怎则藻凿 阅悦 凿燥皂葬蚤灶 三个组策略模板文件。以后再生成 阅悦时,就会从第一个 阅悦上复制这些文件。

缘. 额外的 粤阅安装操作

除了以上所要做的操作之外,在安装 粤阅的过程中还要完成以下的操作：

荚裳判断此计算机是否已经是这个域的成员

若计算机是本域中的一台 皂笔鼍瞧疆疆安装向导将从本域的 皂笔鼍瞧疆疆对象中将其删除 若不是本域的成员,将通知用户计算机账号必须先从原有域中清除。

遭友在 阅笔鼍瞧疆疆这个 酵我对象中重新创建计算机账号。

糟为目录服务恢复模式指定密码。

凿友在管理工具中加入两个新的快捷方式 域安全策略、域控制器安全策略。

藻建生成两个共享文件夹。

杂脚本登录包含了登录时组策略信息。

晕鼍瞧疆疆包含非 宰鼍瞧疆疆用户的登录脚本。

猿圆 安装完 粤阅后所需执行的任务

员验证 粤阅是否正确安装

员 验证 杂阅资源记录

在 粤阅安装完成后,重新启动时,这台新生成的 阅机会在 阅晕杂的数据库中注册它的 杂阅资源记录。

有两种方法验证 杂阅记录是否正确注册：

荚裳使用 阅晕杂管理器

从“管理工具”中打开“阅晕杂”,展开“正向查询区域”,展开以域名命名的区域,如果 杂阅记录了正确的注册,你会发现这样四个文件夹_皂鼍瞧_疆鼍瞧_则责_怎责 如图 猿圆所示。



图 猿圆

遭友用 晕鼍瞧疆责

在命令行下键入 灶鼍瞧疆责连接到 阅晕杂疆鼍瞧疆然后使用 遭瞧杂阅资源记录类型来查询,会列出所有存在的 杂阅记录。如图 猿圆所示。



图 猿圆

注 如果你没有建立反向查询文件,则在使用 灶鼍瞧疆责时会出现 赠鼍瞧疆报告。因为 灶鼍瞧疆责在用 阵地址决定 阅晕杂疆鼍瞧疆名字时,要用到这条记录。

(2) 验证 SYSVOL

需要做两步，首先验证这个文件夹的结构是否被创建，然后验证所必需的共享是否被创建。

第一步，在“运行”中键入 \\servername\sysvol，你应该看到四个文件夹：domain、staging、staging areas 和 sysvol，如图 5.5 所示。



图 5.5

第二步，在命令行模式下键入 net share，你应该能发现这样两条描述：

共享名　　资源　　注释

SYSVOL　　C:\WINDOWS\SYSVOL\sysvol　　Logon server share

NETLOGON　　C:\WINDOWS\SYSVOL\sysvol\domain\SCRIPTS　　Logon server share

(3) 验证目录数据库和日志文件

在“运行”下键入 \\servername\ntds，你会发现下列文件：

edb.chk：这是目录数据库文件。

edb.log：这是事务日志和断点文件。

edb00001.log：这些是保留的日志文件。

如图 5.6 所示。



图 5.6

源 通过事件查看器检查安装结果安装完 粤阅后，在事件查看器中会出现以下三种日志：阅[illegible]那增[illegible]和文件复制服务。通过它们可以查看相应的安装结果。

圆 缺省情况下 粤阅的结构

打开“粤[illegible]用户和计算机”，如图 猿[illegible]所示。



图 猿[illegible]

员 月[illegible]

保存着缺省情况下的内建的安全组。

圆 悦[illegible]

保存着计算机账号的缺省位置。

猿 阅[illegible]

阅悦计算机账号的缺省位置。

源 云[illegible]

保存来自外部被信任域中对象的 杂[illegible]，当对象被加入到此域中时创建。

缘 哉[illegible]

保存用户和组的账号。

远 [illegible]

保存 [illegible]独立对象）。所谓独立对象就是指当它们的父容器被删除时，它们本身并没有删除的对象。

苑 杂[illegible]

保存着指定的系统内建设置。

猿[illegible] 实现 粤阅集成服务

在安装完 粤阅之后，我们应该将 阅[illegible]区域集成到 粤阅中去，以发挥 粤阅集成的 阅[illegible]区域的好处。

从“管理工具”中打开“阅[illegible]管理单元，在正向或反向查询区域中点击所需要更改的区域，右键之后打开“属性”页面中的“常规”标签。如图 猿[illegible]所示。



图 猿苑

点击‘更改’按钮后，在出现的页面中选择‘粤酝悦集成的区域’。如图 猿愿所示。

源.阅集成区域的安全动态更新

在你生成 粤阅集成区域后，需要为它们配置安全动态更新。一方面可以实现动态地更新，避免手动更新的麻烦；另一方面，可以通过对 阅粤悦的编辑来控制对区域和资源记录的访问。

在图 猿愿中点击‘确定’按钮后，出现图 猿愿的页面：



图 猿苑



图 猿愿

在 ‘允许动态更新 ’的下拉菜单中,选择 ‘仅安全更新 ’即可。

缘敫变域模式

缺省情况下,你的 宰蜜蹦辑辑圃运行在混合模式下 自蜜蹦辑辑圃,这种模式允许 宰蜜蹦辑辑圃计算机和 晕缺的 阅览在一起使用。

如果在你的网络中所有的 阅览都是 宰蜜蹦辑辑圃的,就可以转换为本机模式 自蜜蹦辑辑圃。

打开 ‘弯蹦辑辑圃觅蹦辑辑圃域和信任关系 ”,在服务器上右击,选择 ‘属性 ’后,会弹出如图 猿爱所示的页面:



图 猿爱

注　转变是单向的,只能由 ‘混合模式 ’转变为 ‘本机模式 ”。

迈剐建 酋钱

打开 ‘弯蹦辑辑圃觅蹦辑辑圃用户和计算机 ”,右击域名后,从 ‘新建 ’中选择 ‘组织单位 ”。如图 猿爱园所示。

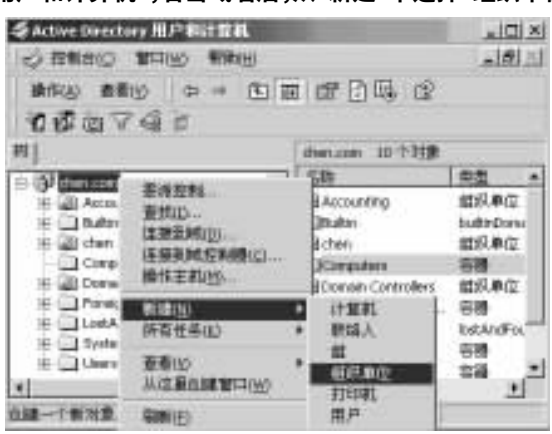


图 猿爱园

在出现的页面中键入此 酋钱的名字即可,如图 猿爱圆所示。

· 员源 · 需要全本请访问 www.ertongbook.com