



中华人民共和国国家标准

GB/T 16264.4—2008/ISO/IEC 9594-4:2005
代替 GB/T 16264.4—1996

信息技术 开放系统互连 目录 第 4 部分：分布式操作规程

Information technology—Open Systems Interconnection—The Directory—
Part 4: Procedures for distributed operation

(ISO/IEC 9594-1:2005 Information technology—Open Systems
Interconnection—The Directory:Procedures for distributed operation,IDT)

2008-08-06 发布

2009-01-01 实施



中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会

发布

中 华 人 民 共 和 国
国 家 标 准
信息技术 开放系统互连 目录
第 4 部分：分布式操作规程

GB/T 16264.4—2008/ISO/IEC 9594-4:2005

*

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

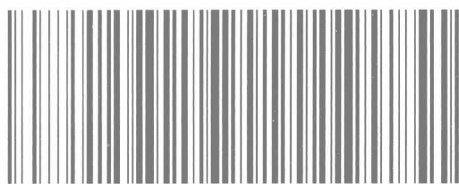
*

开本 880×1230 1/16 印张 7.5 字数 227 千字
2008 年 12 月第一版 2008 年 12 月第一次印刷

*

书号: 155066 • 1-34754 定价 68.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533



GB/T 16264.4-2008

前 言

GB/T 16264 在《信息技术 开放系统互连 目录》总标题下,包括以下 10 个部分:

- 第 1 部分:概念、模型和服务的概述;
- 第 2 部分:模型;
- 第 3 部分:抽象服务定义;
- 第 4 部分:分布式操作规程;
- 第 5 部分:协议规范;
- 第 6 部分:选定的属性类型;
- 第 7 部分:选定的客体类;
- 第 8 部分:公钥和属性证书框架;
- 第 9 部分:复制(待发布);
- 第 10 部分:公用目录管理机构的系统管理用法(待发布)。

本部分是 GB/T 16264 的第 4 部分。

本部分等同采用国际标准 ISO/IEC 9594-4:2005《信息技术 开放系统互连 目录 分布式操作规程》,仅有编辑性修改。

本部分代替 GB/T 16264.4—1996。

本部分与 GB/T 16264.4—1996 的差异在于:

- 增加知识管理;
- 扩展了各章条内容。

本部分的附录 A 和附录 D 是规范性附录,附录 B、附录 C 和附录 E 是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息技术标准化技术委员会归口。

本部分起草单位:中国电子技术标准化研究所。

本部分主要起草人:徐冬梅、张翠、冯惠、胡顺、刘文治。

本部分于 1996 年首次发布,本次为第一次修订。

引 言

GB/T 16264 的本部分连同本标准其他部分是方便信息处理系统之间的互连以提供目录服务而制定的。所有这些系统的集合,连同它们所拥有的目录信息可被视为一个整体,被称为“目录”。目录所拥有的信息,总称为目录信息库(DIB),典型地被用于方便客体之间的通信、与客体的通信或有关客体的通信等,这些客体如应用实体、个人、终端和分布列表等。

目录在开放系统互连中扮演了重要角色,其目标是,在它们自身的互连标准之外做最少的技术约定的情况下,允许下述各种信息处理系统之间的互连:

- 来自不同生产厂商;
- 具有不同的管理;
- 具有不同的复杂程度,以及
- 有不同的年代。

本部分规定了目录各组件进行交互工作所遵循的规程,以便为用户提供一致的服务。

本部分提供了一些基础框架,在此框架基础上,其他标准化组织和业界论坛可以定义工业配置集。在这些框架中定义为可选的许多特性,可通过配置集的说明,在某种环境下作为必选特性来使用。ISO/IEC 9594 的第 5 版是原有国际标准第 4 版的修订和增强,但不是替代。在系统实现时仍可以声明为符合第 4 版。然而,在某些方面,将不再支持第 4 版(即不再消除一些报告上来的差错)。建议在系统实现时尽快符合第 5 版。

第 5 版详细定义了目录协议的第 1 版和第 2 版。

第 1 版和第 2 版仅定义了协议第 1 版。本版本(第 5 版)中定义的许多服务和协议被设计为可运行在第 1 版下。然而,一些增强的服务和协议,如署名差错,只有包含在操作中的所有的目录条目都协商支持协议第 2 版时才可运行。无论协商的是哪一版,第 5 版中所定义的服务之间的差异和协议之间的差异,除了那些特别分配给第 2 版的外,都可以使用 GB/T 16264.5—2008 中定义的扩展规则调节。

本部分使用术语“第 1 版系统”来指遵循国际标准第 1 版的所有系统,即 ISO/IEC 9594:1990 版本;本部分使用术语“第 2 版系统”来指遵循国际标准第 2 版本的所有系统,即 ISO/IEC 9594:1995 版本;本部分使用术语“第 3 版系统”来指遵循国际标准第 3 版的所有系统,即 ISO/IEC 9594:1998 版本;本部分使用术语“第 4 版系统”来指遵循国际标准第 4 版的所有系统,即 ISO/IEC 9594:2001 版本的第 1 部分到第 10 部分;本部分使用术语“第 5 版系统”来指遵循国际标准第 5 版的所有系统,即 ISO/IEC 9594:2005 版本。

GB/T 16264—1996 是参照 ISO/IEC 9594:1990 而制定的。我国没有制定与国际标准第 2 版、第 3 版、第 4 版对应的国家标准。本部分提到的版本号是指国际标准的版本号。

附录 A 是规范性附录,提供了目录分布式操作的 ASN.1 模块定义。

附录 B 是资料性附录,描述了分布式名(称)解析的一个示例。

附录 C 是资料性附录,描述了分布式操作环境中的鉴别。

附录 D 是规范性附录,提供了本目录规范中引入的 ASN.1 信息客体类的定义。

附录 E 是资料性附录,举例说明了知识的维护。

目 次

前言	I
引言	II
第一篇:综述	1
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 缩略语	6
5 约定	6
第二篇:概述	6
6 概述	6
第三篇:分布式目录模型	7
7 分布式目录系统模型	7
8 DSA 交互模型	8
第四篇:DSA 抽象服务	11
9 DSA 抽象服务概述	11
10 信息类型	11
11 绑定和解绑定	20
12 链接操作	21
13 链接差错	22
第五篇:分布式规程	23
14 概述	23
15 分布式目录行为	24
16 操作调度程序	29
17 请求有效性验证规程	35
18 名(称)解析规程	38
19 操作赋值(evaluation)	47
20 连续引用规程	67
21 结果合并规程	79
22 分布式鉴别规程	81
第六篇:知识管理	82
23 知识管理概述	82
24 分等级操作绑定	85
25 非特定分等级操作绑定	93
附录 A (规范性附录) 分布式操作的 ASN.1 定义	97
附录 B (资料性附录) 分布式名(称)解析的示例	102
附录 C (资料性附录) 鉴别的分布式使用	104
附录 D (规范性附录) 分等级和非特定分等级操作绑定类型的规范	110
附录 E (资料性附录) 知识维护示例	113

信息技术 开放系统互连 目录

第4部分：分布式操作规程

第一篇：综 述

1 范围

GB/T 16264 的本部分规定涉及分布式目录应用的 DSA 行为。对于跨越许多 DSA 的广域 DIB, 已经设计了允许的行为以确保提供一致的服务。

虽然目录可以建立在某种通用的数据库系统之上, 但它本身并不属于这样一种通用的数据库系统。目录是在假定查询操作远比更新操作频繁的情况下建立的。

2 规范性引用文件

下列文件中的条款通过 GB/T 16264 的本部分的引用而成为本部分的条款。凡是注日期的引用文件, 其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分, 然而, 鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件, 其最新版本适用于本部分。

GB/T 9387.1—1998 信息技术 开放系统互连 基本参考模型 第1部分: 基本模型(idt ISO/IEC 7498-1:1994)

GB/T 16262.1—2006 信息技术 抽象语法记法一(ASN.1) 第1部分: 基本记法规范(ISO/IEC 8824-1:2002, IDT)

GB/T 16262.2—2006 信息技术 抽象语法记法一(ASN.1) 第2部分: 信息客体规范(ISO/IEC 8824-2:2002, IDT)

GB/T 16262.3—2006 信息技术 抽象语法记法一(ASN.1) 第3部分: 约束规范(ISO/IEC 8824-3:2002, IDT)

GB/T 16262.4—2006 信息技术 抽象语法记法一(ASN.1) 第4部分: ASN.1 规范的参数化(ISO/IEC 8824-4:2002, IDT)

GB/T 16264.1—2008 信息技术 开放系统互连 目录 第1部分: 概念、模型和服务的概述(ISO/IEC 9594-1:2005, IDT)

GB/T 16264.2—2008 信息技术 开放系统互连 目录 第2部分: 模型(ISO/IEC 9594-2:2005, IDT)

GB/T 16264.3—2008 信息技术 开放系统互连 目录 第3部分: 抽象服务定义(ISO/IEC 9594-3:2005, IDT)

GB/T 16264.5—2008 信息技术 开放系统互连 目录 第5部分: 协议规范(ISO/IEC 9594-5:2005, IDT)

GB/T 16264.6—2008 信息技术 开放系统互连 目录 第6部分: 选定的属性类型(ISO/IEC 9594-6:2005, IDT)

GB/T 16264.7—2008 信息技术 开放系统互连 目录 第7部分: 选定的客体类(ISO/IEC 9594-7:2005, IDT)

ISO/IEC 9594-8:2005 信息技术 开放系统互连 目录: 公钥和属性证书框架

ISO/IEC 9594-9:2005 信息技术 开放系统互连 目录: 复制

ISO/IEC 9594-10:2005 信息技术 开放系统互连 目录: 公用目录管理机构的系统管理用法

IETF RFC 2251:1997 轻量级目录访问协议(v3)

IETF RFC 3377:2002 轻量级目录访问协议(v3):技术规范

3 术语和定义

下列术语和定义适用于 GB/T 16264 的本部分。

3.1 通信模型定义

本部分使用 GB/T 16264.5—2008 中定义的下列术语：

应用实体名称 *application-entity-title*;

3.2 基本目录定义

本部分使用 GB/T 16264.1—2008 中定义的下列术语：

a) 目录 (*the*) *Directory*

b) 目录信息库 *Directory Information Base*

3.3 目录模型定义

本部分使用 GB/T 16264.2—2008 中定义的下列术语：

a) 访问点 *access point*;

b) 别名 *alias*;

c) 可辨别名 *distinguished name*;

d) 目录信息树(DIT) *Directory Information Tree(DIT)*;

e) 目录系统代理(DSA) *Directory System Agent (DSA)*;

f) 目录用户代理(DUA) *Directory User Agent (DUA)*;

g) 相关可辨别名 *relative distinguished name*。

3.4 DSA 信息模型定义

本部分使用 GB/T 16264.2—2008 中定义的下列术语：

a) 种类 *category*;

b) 公共可用的 *commonly usable*;

c) 上下文前缀 *context prefix*;

d) 交叉引用 *cross reference*;

e) DIB 片段 *DIB fragment*;

f) DSA 信息树 *DSA information tree*;

g) DSA 特定条目(DSE) *DSA-Specific Entry (DSE)*;

h) DSE 类型 *DSE type*;

i) 直接上级引用 *immediate superior reference*;

j) 知识信息 *knowledge information*;

k) 知识引用种类 *knowledge reference category*;

l) 知识引用类型 *knowledge reference type*;

m) 命名上下文 *naming context*;

n) 非特定知识 *non-specific knowledge*;

o) 非特定下级引用 *non-specific subordinate reference*;

p) 操作属性 *operational attribute*;

q) 引用路径 *reference path*;

r) 特定知识 *specific knowledge*;

s) 下级引用 *subordinate reference*;

t) 上级引用 *superior reference*。

3.5 抽象服务定义

本部分使用 GB/T 16264.3—2008 中定义的下列术语：

- a) 流结果 *streamed result*;

3.6 目录复制定义

本部分使用 ISO/IEC 9594-9:2005 中定义的下列术语：

- a) 属性完备性 *attribute completeness*;
- b) 影像操作绑定 *shadowing operational binding*;
- c) 下级完备性 *subordinate completeness*;
- d) 复制单元 *unit of replication*。

3.7 分布式操作定义

下列术语和定义适用于本部分。

3.7.1

基本客体 *base object*

一个客体或别名条目，是发起者所发起的某个操作的目标。

3.7.2

绑定的 DSA *bound DSA*

一个 DSA，发起请求的 DUA 通过与该 DSA 执行一个绑定操作而与之绑定起来。

3.7.3

绑定的 DSA 的分页结果 *bound-DSA paged results*

分页完全由 DUA 所绑定的 DSA 来执行。

注：这是遵循第 5 版之前的系统所支持的唯一一种分页模式。

3.7.4

链接 *chaining*

单链接或多链接的通用术语。

3.7.5

上下文前缀信息 *context prefix information*

上级 DSA 在一个 RHOB 中向下级 DSA 所提供的关于下级上下文前缀的上级 DIT 顶点的操作信息和用户信息。

3.7.6

分布式名(称)解析 *distributed name resolution*

在多于一个的 DSA 中执行名(称)解析的过程。

3.7.7

DSP 分页结果 *DSP paged results*

当执行的 DSA 与绑定的 DSA 不相同且由初始执行者完成的分页结果，依据 DSP 协议提供。

3.7.8

差错 *error*

由执行者向请求者发送的信息，信息中携带了一个对之前接收到的请求的否定结果。

3.7.9

硬差错 *hard error*

一个明确的差错，该差错指示如果没有外部的干预，则操作目前不能被执行。

3.7.10

分等级操作绑定 *hierarchical operational binding; HOB*

指两个拥有命名上下文的主 DSA 之间的关系，其中一个是另一个的直接下级，在该关系中，上级 DSA 拥有一个指向下级 DSA 的下级引用。

3.7.11

初始执行者 initial performer

开始执行某个操作的第一个 DSA,即进入操作赋值阶段的第一个 DSA。

3.7.12

修改操作 modification operations

指目录修改操作,即修改条目、增加条目、移除条目和修改 DN 等。

3.7.13

多链接 multi-chaining

一种交互模式,在该模式中,自身执行某个请求的 DSA 向其他 DSA 的集合发出多个请求,或者是并列的,或者是顺序的。

3.7.14

多条目查询操作 multiple entry interrogation operations

指目录搜索操作,即列表和搜索。

3.7.15

名(称)解析 name resolution

定位某个条目的过程,该过程是通过对声称名(称)的每个 RDN 与 DIT 的顶点进行顺序匹配而完成的。

3.7.16

非特定分等级操作绑定 non-specific hierarchical operational binding; NHOB

指两个拥有命名上下文的主 DSA 之间的关系,其中一个是另一个的直接下级,在该关系中,上级 DSA 拥有一个指向下级 DSA 的非特定下级引用。

3.7.17

分解 NSSR decomposition NSSR

将非特定知识引用分解为多个子请求以便于其他 DSA 能够继续执行;这些子请求可以被执行该分解的 DSA 链接到其他 DSA;或者可以将标识了其他 DSA 的一个连续引用返回给请求者,由请求者来继续执行;或者执行分解的 DSA 可以继续执行某些子请求,而留下其他子请求交给请求者来继续执行。

3.7.18

操作进展 operation progress

一系列的值,指示了名(称)解析所完成的程度。

3.7.19

发起者 originator

发起一个特定的(分布式)操作的 DUA。

3.7.20

分页 paging

以一页或多页的分段方式返回的搜索或列表操作的结果,每页都由有限数量的条目组成。

3.7.21

执行者 performer

接收了某个请求的 DSA(即将执行某个操作)。

注:执行者也是初始执行者,除非对于可以包括多个 DSA 进行赋值的操作。

3.7.22

规程 procedure

关于 DSA 如何将给定的输入变元集及其 DSA 信息树映射为一个结果的一个(非正式)规范。

注:输入变元和结果可以对应为从一个被请求的操作中接收到的信息和在一个答复中发送的信息,或者它们可以表示根据一个被请求的操作而对答复进行计算的中间阶段。在 14.2,前面一种输入变元和结果类型被称为是外部的。

3.7.23

相关的分等级操作绑定 relevant hierarchical operational binding; RHOB

或者是指一个 HOB, 或者是指一个 NHOB, 依赖于上下文。

3.7.24

转向推荐 referral

自己不能执行某个操作的 DSA 返回的一种结果, 标识了一个或多个可以执行此操作的其他 DSA。

3.7.25

答复 reply

一个结果或一个差错。

3.7.26

请求 request

由一个操作代码和相关变元所组成的信息, 表示从请求者向执行者所发起的一个目录操作。

3.7.27

请求分解 request decomposition

将一个请求分解为多个子请求以便于其他 DSA 能够继续执行; 这些子请求可以被执行分解的 DSA 链接到其他 DSA; 或者可以将标识了其他 DSA 的连续引用返回给请求者, 由请求者来继续执行; 或者执行分解的 DSA 可以继续执行某些子请求, 而留下其他子请求交给请求者来继续执行。

3.7.28

请求者 requester

发送一个请求以便执行(即调用)某个操作的一个 DUA 或 DSA。

3.7.29

单条目查询操作 single entry interrogation operations

指目录阅读操作, 即阅读和比较操作。

3.7.30

软差错 soft error

一个差错, 可以是瞬时的, 也可以指示了一个局部的问题, 在这种情况下, 使用一个不同的知识引用或访问点可获得一个结果或一个硬差错。

3.7.31

下级 DSA subordinate DSA

共享一个 HOB 或一个 NHOB 的两个 DSA 中, 其中拥有下级命名上下文的那个 DSA。

3.7.32

子请求 subrequest

通过请求分解而产生的一个请求。

3.7.33

上级 DSA superior DSA

共享一个 HOB 或一个 NHOB 的两个 DSA 中, 其中拥有上级命名上下文的那个 DSA。

3.7.34

上级、下级 DSA superior, subordinate DSA

两个拥有命名上下文的主 DSA, 其中一个是另一个的直接下级; 这两个 DSA 之间的关系可以通过一个 HOB(或 NHOB)来显式地管理, 或者依靠上级 DSA 来隐含存在, 该上级 DSA 拥有一个指向下级 DSA 的下级引用(或非特定下级引用)。

3.7.35

目标客体名 target object name

一个条目的名(称),该条目或者是操作在名(称)解析的某个特定阶段所指向的客体,或者是包含在操作赋值中。

3.7.36

单链接 uni-chaining

某个自身不能直接执行操作的 DSA 可选使用的一种交互模式。DSA 的链接是通过调用另一个 DSA 的某个操作,并且将结果再转发给初始请求者来完成的。

4 缩略语

下列缩略语适用于 GB/T 16264 的本部分:

ASN.1	抽象语法标记一
DISP	目录信息影像协议
DMD	目录管理域
DOP	目录操作绑定管理协议
DSE	DSA 特定条目
HOB	分等级操作绑定
NHOB	非特定的分等级操作绑定
NSSR	非特定下级引用
RHOB	相关的分等级操作绑定

5 约定

术语“目录规范(或本目录规范)”指的是 GB/T 16264.4。术语“系列目录规范”指的是 GB/T 16264 (或者 ISO/IEC 9594)的所有部分。

本目录规范使用术语“第 1 版系统”来指遵循系列目录规范第 1 版的所有系统,即 GB/T 16264—1996 版本。本目录规范使用术语“第 2 版系统”来指遵循系列目录规范第 2 版本的所有系统,即 ISO/IEC 9594:1995 版本。本目录规范使用术语“第 3 版系统”来指遵循系列目录规范第 3 版的所有系统,即 ISO/IEC 9594:1998 版本。本目录规范使用术语“第 4 版系统”来指遵循系列目录规范第 4 版的所有系统,即 ISO/IEC 9594:2001 版本的第 1 部分到第 10 部分。

本目录规范使用术语“第 5 版系统”来指遵循系列目录规范第 5 版的所有系统,即 GB/T 16264—2008 版本的第 1 部分到第 7 部分以及 ISO/IEC 9594-8:2005、ISO/IEC 9594-9:2005 和 ISO/IEC 9594-10:2005。

本目录规范使用粗体字来表示 ASN.1 符号。若在常规文本中要表示 ASN.1 的类型和值时,为了区别于常规文本,使用了粗体字表示。为了表示过程的语义而引用过程名时,为了区别于常规文本,使用了粗体字表示。访问控制许可使用斜体字表示。

第二篇:概 述

6 概述

目录抽象服务允许对 DIB 中的目录信息进行查询、获取和修改。该服务按照 GB/T 16424.3 中规定的抽象目录客体来进行描述。类似的,轻量级目录访问协议(LDAP)允许对 DIB 中的目录信息进行查询、获取和修改。该协议以及它所允许的服务在 RFC 3377 中规定。

必要地,抽象目录客体的规范没有以任何方式指定目录的物理实现:尤其是它没有指定目录系统代理(DSA)的规范,这些 DSA 存储了 DIB 并对 DIB 进行管理,并且通过 DSA 提供服务。另外,它没有考

考虑 DIB 是否是分布式的,即 DIB 是包含在一个单独的 DSA 内,还是分布在多个 DSA 内。因此,为了在一个分布式环境中支持抽象服务,需要 DSA 具有其他 DSA 的知识,能够导航到其他 DSA,并且与其他 DSA 进行合作等,这些需求也没有涵盖在服务描述中。

本目录规范对抽象目录客体进行了细化,这种细化通过一个或多个 DSA 客体集来表示,这些 DSA 客体共同构成了分布的目录服务。

另外,本目录规范规定了 DIB 可被分布到一个或多个 DSA 内的允许的方式。对于某种受限情况,即 DIB 包含在一个单独的 DSA 内,这种情况下目录实际上是集中式的;对于 DIB 分布在两个或多个 DSA 内的情况,则规定了知识和导航机制以确保所有的拥有组成条目的 DSA 能够潜在地访问到整个 DIB。

DIB 的一部分内容也可在多个 DSA 内被复制。本目录规范中描述的协议允许使用复制信息来提高分布式目录服务的可用性、性能和效率。复制信息的使用在某种程度上是在用户的控制之下的,通过使用服务控制选项来实现。本目录规范中描述的规程也指示了在使用复制信息时进行设计最优化的某些时机。

另外,也规定了请求处理的交互,使得特定的目录操作特性能够被它的用户所控制。尤其是当 DSA 要响应一个与其他 DSA 中拥有的信息相关的目录请求时,用户能够控制一个 DSA 是否拥有直接查询其他 DSA 的权力(即链接),或者它是否应当在响应中提供其他能够继续处理请求的 DSA 的信息(即转向推荐)。

一般来说,一个 DSA 是进行链接还是转向推荐的决定是根据用户所设置的服务控制,以及 DSA 的自身管理、操作或技术环境来决定的。

应当意识到的是,一般来说,目录将是分布式的,因此目录请求将由任意数量的合作 DSA 来满足,这些 DSA 根据上述的条件可以是任意地进行链接或转向推荐,本目录规范规定了 DSA 在响应分布式目录请求时所采用的适当的规程。这些规程将确保分布式目录服务的用户能够感觉到规程既是用户友好的,又是协调一致的。

第三篇:分布式目录模型

7 分布式目录系统模型

目录抽象服务,如在 GB/T 16264.3 中定义的那样,将目录建模为一个客体,该客体向其用户提供了一系列的目录服务。目录用户通过一个访问点来访问它所提供的服务。目录可以拥有一个或多个访问点,且每个访问点都通过它所提供的服务以及提供这些服务的交互模式来描述其特性。

图 1 举例说明了分布式目录模型,该模型将作为规定目录分布特性的基础。它举例说明了由一个或多个 DSA 的集合所组成的目录。

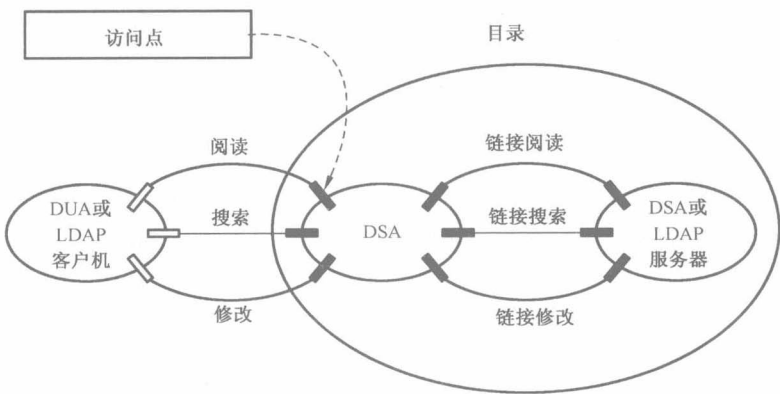


图 1 分布式目录模型中的客体

在本目录规范的后续章条中将详细规定 DSA。本章仅仅陈述一些它们的特性作为介绍性引言,同时建立本目录规范和其他目录规范之间的关系。

DSA 的定义是为了能够适应 DIB 的分布,且一系列的在物理上分布的 DSA 能够以一种预定义的、合作的方式进行交互来向目录用户(DUA 或 LDAP 客户机)提供目录服务。

图 1 举例说明了目录抽象服务和 DSA 抽象服务之间的关系。目录抽象服务在 GB/T 16264.3 中定义,是通过一系列的目录操作来提供的。为了实现该服务,组成目录的各 DSA 之间需要相互交互。

这种交互的自然特性是根据一个 DSA 可以向另一个 DSA 所提供的服务来定义的,即 DSA 抽象服务。DSA 抽象服务是通过一系列的操作来提供的,这些操作被称为链接操作,每个操作都在目录抽象服务中拥有一个对应操作。

因此,在目录抽象服务中给定的一个操作,如阅读,可要求提供服务的 DSA 通过使用链接操作来与其他的一个或多个 DSA 进行交互,如链接阅读。

注:对于作为 LDAP 请求者的 DSA 来说,进行链接操作也是可能的,例如,使用 LDAP 控制或扩展操作;然而,完成这些的规程和协议不在本目录规范的定义范围之内。

8 DSA 交互模型

目录的一个基本特性是,给定一个分布式 DIB,一个用户应当潜在地能够被满足任何服务请求(在符合安全性、访问控制和管理策略等的前提下),而不论请求所发起的访问点。为了适应此需求,必要的是任何一个与满足某个特定服务请求相关的 DSA 都应拥有被请求的信息位于何处的知识(在 GB/T 16264.2—2008 中指定),并且,或者将这些知识返回给请求者,或者试图自己来满足此请求(请求者可以是一个 DUA、一个 LDAP 客户机或其他的 DSA;在后一种情况下,两个 DSA 都应支持 DSP)。

定义了三种 DSA 交互模式以便符合这些需求,这三种模式被称为“单链接”,“多链接”和“转向推荐”。在本目录规范的后续部分,使用通用术语“链接”在适当的上下文中来表示单链接和/或多链接。“链接”指的是 DSA 为了满足某个请求,而向另一个 DSA 发送一个或多个链接操作;“转向推荐”指的是向请求者返回知识信息,于是请求者自身可以再与知识信息中所标识的 DSA 进行交互。

单链接或转向推荐交互可源于一个单独的请求。可选的,请求可以在交互之前被分解为多个子请求。多链接或多转向推荐交互,或两者的混合,可能源自分解后的请求。定义了两种分解类型:NSSR 分解和请求分解。

8.1 一个请求的分解

8.1.1 NSSR 分解

NSSR 分解是将同样的请求准备成便于传送到(或者是顺序的,或者是并行的)多个下级 DSA 中去的过程,这是在名(称)解析的过程中遇到一个 NSSR 的结果。非特定下级引用中不包含被引用的下级命名上下文的 RDN,因此,引用的 DSA 不能够区分哪个下级 DSA 拥有哪个下级命名上下文。因此,在名(称)解析过程中,一个遇到 NSSR 的 DSA 应向每个下级 DSA(在没有影像的情况下)发送一个同样的请求。这可以是顺序执行的,也可以是并行执行的。典型地,仅有一个 DSA 能够继续执行名(称)解析;而其余 DSA 将返回一个问题为 `unableToProceed` 的 `serviceError`。在某种(很少)情况下,有可能有多个 DSA 将继续进行名(称)解析,由此导致了双重结果。

注:NSSR 不能引用 LDAP 服务器。

8.1.2 请求分解

请求分解,另一种分解请求的方式,是在 DSA 与其他一个或多个 DSA 和/或 LDAP 服务器通信之前,由 DSA 内部执行的一个过程。一个请求被分解为多个可能不同的子请求,因此每个子请求完成原始任务的一部分。请求分解能够仅被用于列表或搜索操作的操作赋值过程中。在请求分解完成后,每个子请求可以被链接到其他 DSA 和/或 LDAP 服务器以便继续任务的执行,或者可有一个局部结果(一个内嵌的转向推荐)返回给请求者。同一个子请求被产生到不同的 DSA 和/或 LDAP 服务器中的一个示例为:某个条目具有下级引用和/或 NSSR,且共同引用了多个 DSA 或 LDAP 服务器。不同的子请求被产生到相同的或不同的 DSA 和/或 LDAP 服务器中的一个示例为:两个不同的条目在某个搜索

(子树)的操作中相遇,且每个都拥有一个下级引用。

8.2 单链接

当一个 DSA 具有另一个 DSA 所拥有的命名上下文的知识时,第一个 DSA 可使用这种交互模式(图 2 中显示)将请求传递给第二个 DSA。单链接可用于与某个单独的 DSA 联系,该 DSA 是在交叉引用、下级引用、上级引用、提供者引用或主引用中被指向的 DSA。

注:在图 2 中,交互的顺序由交互线上相关联的数字来定义。

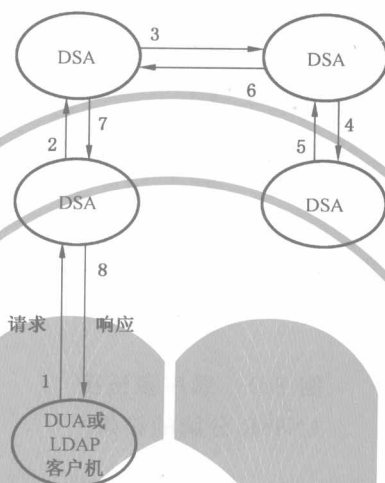


图 2 单链接模式

8.3 多链接

DSA 使用这种交互模式来传递多个出请求,这些出请求来自于同一个人请求,或者是请求分解的结果,或者是 NSSR 分解的结果。

8.3.1 并行多链接

在并行多链接情况下,DSA 将多个出请求同步进行传递(见图 3a))。并行多链接可带来性能的提高,但同时它也可以在某种环境下,如在影像存在时,导致接收到复制结果。

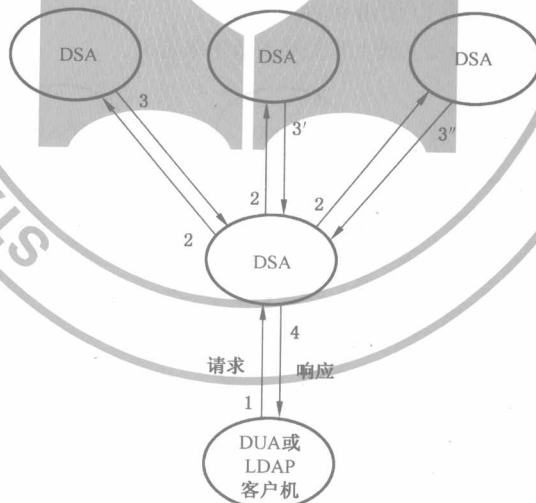
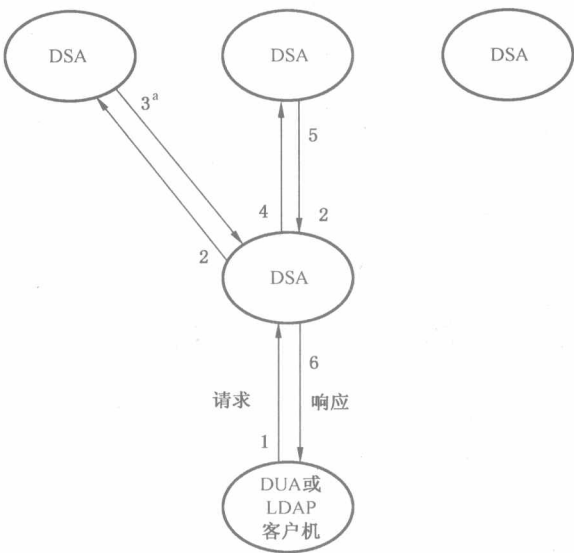


图 3a) 并行多链接

8.3.2 顺序多链接

在顺序多链接情况下,DSA 在一个时间点传递一个出请求,并且在发送下一个请求前等待此请求的结果或差错(见图 3b))。顺序多链接可以不是一种最快的交互模式,但同时它也不可以导致接收到复制结果。

注:一个 DSA 可以联合使用并行多链接和顺序多链接。



^a 不能继续。

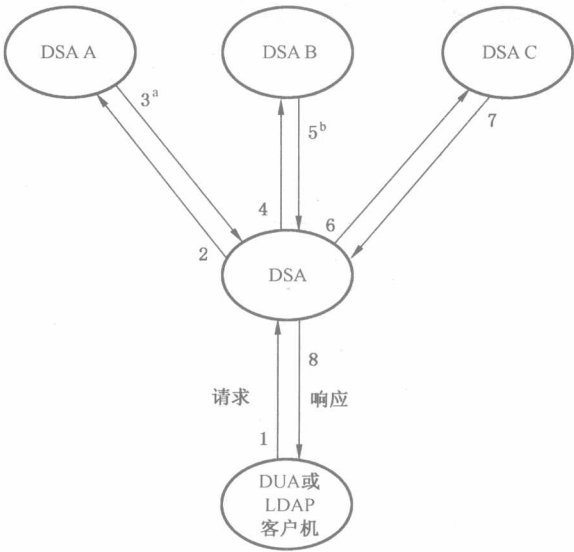
图 3b) 顺序多链接
(NSSR 分解的结果)

8.4 转向推荐

DSA 可以在响应从某个 DUA、LDAP 客户机或其他 DSA 发来的请求时,返回一个转向推荐(在图 4a)和图 4b)中描述)。转向推荐可构成整个响应(在这种情况下,它被分类为一种差错)或者仅仅是响应的一部分。转向推荐包含了知识引用,该知识引用可以是一个上级引用、下级引用、交叉引用、非特定下级引用,提供者引用或主引用等。

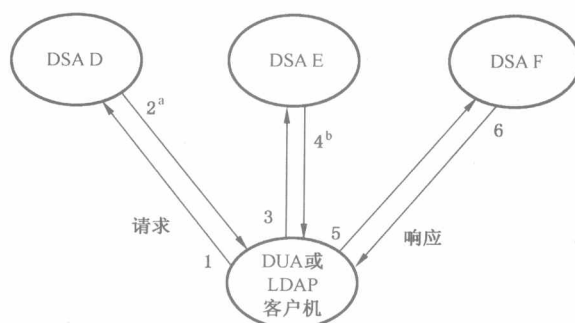
接收到转向推荐的 DSA(见图 4a))可使用包含在转向推荐中的知识引用来进行随后的链接或多播(依赖于引用的类型),将一个原始请求链接或多播到其他的 DSA。可选的,接收到转向推荐的 DSA,可在其响应中依次传递转向推荐。接收到转向推荐的一个 DUA 或 LDAP 客户机(见图 4b))可使用该转向推荐来与一个或多个其他 DSA 联系以便继续执行请求。

注:在图 4a)和图 4b)中,交互的顺序由交互线上相关联的数字来定义。



^a 转向推荐到 B。
^b 转向推荐到 C。

图 4a) 转向推荐模式(DSA 根据转向推荐执行动作)



^a 转向推荐到 E。

^b 转向推荐到 F。

图 4b) 转向推荐模式(DUA 根据转向推荐执行动作)

8.5 模式的决定

如果一个 DSA 自身不能完全地解决一个请求,则它应将该请求(或通过分解原始请求而形成的一个请求)链接到另一个 DSA,除非:

- 用户通过服务控制禁止链接,在这种情况下,DSA 应返回一个转向推荐或一个问题为 chaining Required 的 serviceError;或者
- DSA 由于管理、操作或技术等方面的原因倾向于不进行链接,在这种情况下,DSA 应返回一个转向推荐。

注 1:不进行链接的一个“技术原因”是在知识引用中标识的 DSA 不支持 DSP。

注 2:如果服务控制 localScope 被设置,则 DSA(或 DMD)应或者解决该请求,或者返回一个差错。

注 3:如果用户更希望转向推荐,则用户应设置 chainingProhibited。

第四篇:DSA 抽象服务

9 DSA 抽象服务概述

目录服务在 GB/T 16264.3—2008 中有全面描述。当这样的服务在分布式环境中提供时,如第 7 章中的建模,它可以被认为是通过一系列的 DSA 来提供的。如图 1 中所示。

对于目录服务中定义的每个操作,在 DSA 抽象服务中都定义了一个相应的“链接”操作,在完成目录服务操作中合作的 DSA 之间可以使用这些操作。这样,一个从 DUA 处接收到阅读操作的 DSA 可请求另一个 DSA 的协助(例如,另一个 DSA 中拥有目标条目或其拷贝)来满足此操作,因此会向此 DSA 发送一个链接阅读操作。

在 DSA 抽象服务中交互的信息类型在第 10 章定义。DSA 抽象服务的操作和差错在第 11 章到第 13 章定义。

10 信息类型

10.1 引言

本章标识,同时在某些情况下定义,在后续的 DSA 抽象服务的各种操作定义中所使用的一系列信息类型。

这些涉及到的信息类型包括:对于多个操作而言是通用的信息类型,或者将来可以是通用的信息类型,或者是足够复杂或自包含的信息,需要与使用它们的操作分别定义。

在 DSA 抽象服务的定义中使用的多个信息类型实际上是在别处定义的。10.2 标识了这些类型,并且指示了它们的定义来源。10.3 到 10.10 分别标识并定义了一个信息类型。

10.2 其他地方定义的信息类型

下列信息类型在 GB/T 16264.2—2008 中定义：

- aliasedEntryName;
- DistinguishedName;
- Name;
- RelativeDistinguishedName。

下列信息类型在 GB/T 16264.3—2008 中定义：

(绑定)

- DirectoryBind。

(操作)

- Abandon。

(差错)

- abandoned;
- attributeError;
- nameError;
- securityError;
- serviceError;
- updateError。

(信息客体类)

- OPTIONALLY-PROTECTED。

(数据类型)

- SecurityParameters。

下列信息类型在 GB/T 16264.6—2008 中定义：

- PresentationAddress。

10.3 链接变元

链接变元 ChainingArguments 出现在每个链接操作中,向某个 DSA 传递信息,这些信息是在该 DSA 成功执行全部任务中它需要完成的部分时所需的信息:

ChainingArguments ::= SET {

originator	[0]	DistinguishedName OPTIONAL,
targetObject	[1]	DistinguishedName OPTIONAL,
operationProgress	[2]	OperationProgress DEFAULT { nameResolutionPhase notStarted },
traceInformation	[3]	TraceInformation,
aliasDereferenced	[4]	BOOLEAN DEFAULT FALSE,
aliasedRDNs	[5]	INTEGER OPTIONAL,
——仅出现在第 1 版本系统中		
returnCrossRefs	[6]	BOOLEAN DEFAULT FALSE,
referenceType	[7]	ReferenceType DEFAULT superior,
info	[8]	DomainInfo OPTIONAL,
timeLimit	[9]	Time OPTIONAL,
securityParameters	[10]	SecurityParameters DEFAULT { },
entryOnly	[11]	BOOLEAN DEFAULT FALSE,
uniqueIdentifier	[12]	UniqueIdentifier OPTIONAL,