



系统管理指南：卷 1

Adaptive Server® Enterprise

15.5

文档 ID: DC38757-01-1550-01

最后修订日期: 2009 年 11 月

版权所有 © 2010 Sybase, Inc. 保留所有权利。

除非在新版本或技术声明中另有说明, 否则本出版物适用于 Sybase 软件 and 任何后续版本。此文档中的信息如有更改, 恕不另行通知。此处说明的软件按许可协议提供, 其使用和复制必须符合该协议的条款。

若要订购附加文档, 美国和加拿大的客户请拨打客户服务部门电话 (800) 685-8225 或发传真至 (617) 229-9845。

持有美国许可协议的其它国家 / 地区的客户可通过上述传真号码与客户服务部门联系。所有其它国际客户请与 Sybase 子公司或当地分销商联系。仅在定期安排的软件发布日期提供升级。未经 Sybase, Inc. 的事先书面许可, 不得以任何形式、任何手段 (电子的、机械的、手动、光学的或其它手段) 复制、传播或翻译本出版物的任何部分。

可在位于 <http://www.sybase.com/detail?id=1011207> 的 “Sybase 商标页” (Sybase trademarks page) 查看 Sybase 商标。Sybase 和列出的标记均是 Sybase, Inc. 的商标。® 表示已在美国注册。

Java 和所有基于 Java 的标记都是 Sun Microsystems, Inc. 在美国和其它国家 / 地区的商标或注册商标。

Unicode 和 Unicode 徽标是 Unicode, Inc. 的注册商标。

IBM 和 Tivoli 是 International Business Machines Corporation 在美国和 / 或其它国家 / 地区的注册商标。

提到的所有其它公司和产品名均可能是与之相关的相应公司的商标。

Use, duplication, or disclosure by the government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of DFARS 52.227-7013 for the DOD and as set forth in FAR 52.227-19(a)-(d) for civilian agencies.

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

目录

关于本手册	xv
第 1 部分	系统管理基础知识
第 1 章	系统管理概述 3
	Adaptive Server 管理任务 3
	系统管理任务所需的角色 4
	使用 isql 执行系统管理任务 7
	将 Sybase Central 用于系统管理任务 8
	系统表 9
	查询系统表 9
	系统表中的键 10
	更新系统表 10
	系统过程 11
	使用系统过程 11
	系统过程表 12
	创建系统过程 12
	系统扩展存储过程 13
	创建系统 ESP 13
	记录错误消息 14
	连接到 Adaptive Server 14
	interfaces 文件 14
	目录服务 15
	LDAP 作为一个目录服务 16
	Adaptive Server 中可用的安全性功能 18
第 2 章	系统及可选数据库 21
	系统数据库概述 21
	master 数据库 23
	控制 master 数据库中的对象创建 24
	备份 master 数据库并保留系统表的副本 24
	model 数据库 25
	sybsystemprocs 数据库 26

tempdb 数据库	26
创建临时表	27
sybsecurity 数据库	27
sybssystemdb 数据库	28
sybmgmtdb 数据库	28
pubs2 和 pubs3 样本数据库	28
维护样本数据库	29
pubs2 image 数据	29
dbccdb 数据库	29
sybdiag 数据库	29
确定安装脚本的版本	30

第 3 章

系统管理入门	31
逻辑页大小	31
使用“测试”服务器	32
计划资源	32
达到性能目标	32
安装 Sybase 产品时的注意事项	33
检查产品的兼容性	33
安装或升级 Adaptive Server	33
安装其它第三方软件	33
配置并测试客户端连接	34
分配物理资源	34
专用服务器与共享服务器	34
决策支持和 OLTP 应用程序	35
预先的资源计划	35
操作系统配置	35
备份和恢复	36
保留 master 的最新备份	36
自动备份过程	37
备份数据库前检验数据一致性	38
监控日志大小	38
即时维护和故障排除	39
启动和停止 Adaptive Server	39
查看和清理错误日志	39
保留记录	39
联系信息	40
配置信息	40
维护日程表	40
系统信息	41
灾难性事故恢复计划	41
其它资源	41

第 4 章	用于 Sybase Central 的 Adaptive Server 插件简介	43
	Adaptive Server Sybase Central 插件概述	43
	Adaptive Server 插件和命令行更新	44
	使用 Adaptive Server 插件	45
	启动和停止 Sybase Central	46
	注册 Adaptive Server 插件	46
	执行常见任务	47
	使用 Interactive SQL	53
	启动 Interactive SQL	54
第 5 章	设置配置参数	55
	概述	55
	Adaptive Server 配置文件	56
	修改配置参数	56
	用于修改配置参数的必需角色	56
	使用 sp_configure 的单位规范	58
	获取有关配置参数的帮助信息	58
	使用 sp_configure	59
	语法元素	60
	使用 sp_configure 及配置文件	60
	参数层次	64
	用户定义的参数层次子集：显示级别	66
	使用 sp_configure 和 sp_sysmon 进行性能调优	67
	在集群环境中使用配置参数	67
	sp_configure 输出	68
	命名高速缓存配置参数	70
	sysconfigures 和 syscurconfigs 表	71
	查询 syscurconfigs 和 sysconfigures：一个示例	71
	配置参数	71
	按字母顺序排列的配置参数列表	72
第 6 章	磁盘资源问题概述	245
	设备分配和对象放置	245
	用于管理磁盘资源的命令	246
	存储管理决策中需要考虑的事项	247
	恢复	248
	性能	248
	安装时的状态和缺省值	249
	用于管理存储的系统表	250
	sysdevices 表	251
	sysusages 表	251
	syssegments 表	252
	sysindexes 表	252
	syspartitions 表	252

第 7 章	初始化数据库设备	253
	数据库设备	253
	使用 disk init 命令	254
	disk init 语法	254
	指定逻辑设备名	254
	指定物理设备名	255
	选择设备号	255
	指定设备大小	256
	指定 dsync 设置（可选）	257
	使用 directio 绕过操作系统缓冲区	259
	disk init 的其它可选参数	260
	获取有关设备的信息	260
	删除设备	262
	指派缺省设备	262
	选择缺省设备和非缺省设备	263
	使用 disk resize 增加设备大小	263
	磁盘空间不足	265
第 8 章	设置数据库选项	267
	使用 sp_dboption 过程	267
	数据库选项说明	268
	查看数据库的选项	269
第 9 章	配置字符集、排序顺序和语言	271
	了解国际化和本地化	271
	国际化系统的优点	272
	国际化系统示例	273
	国际化系统的元素	275
	为服务器选择字符集	275
	Unicode	277
	选择服务器缺省字符集	281
	选择排序顺序	283
	使用排序顺序	283
	不同类型的排序顺序	283
	选择缺省排序顺序	284
	为系统消息选择语言	290
	设置服务器：示例	291
	西班牙语版服务器	291
	总部在美国的日本公司	292
	具有多国客户端的日本公司	292

更改字符集、排序顺序或消息语言	293
更改缺省字符集	293
用资源文件更改排序顺序	294
更改缺省排序顺序	295
重新配置字符集、排序顺序或消息语言	295
Unicode 示例	296
预备步骤	297
设置用户的缺省语言	298
重新配置后的恢复	299
处理可疑分区	302
安装不支持语言的日期字符串	303
服务器与客户端之间的日期解释	303
国际化和本地化文件	304
国际化文件的类型	304
字符集目录结构	305
本地化文件的类型	306
软件消息目录结构	306
消息语言和全局变量	307

第 10 章	配置客户端 / 服务器字符集转换	309
	字符集转换	309
	支持的字符集转换	310
	本地字符集的转换	310
	Unicode 系统中的转换	311
	Adaptive Server 直接转换	312
	Unicode 转换	312
	选择转换类型	312
	非 Unicode 客户端 / 服务器系统	312
	Unicode 客户端 / 服务器系统	313
	配置服务器	314
	启用和禁用字符集转换	314
	无法转换的字符	315
	字符集转换中的错误处理	316
	转换和数据长度的变化	316
	配置系统和应用程序	317
	为实用程序指定字符集	318
	显示和文件字符集的命令行选项	318

第 11 章	诊断系统问题	321
	Adaptive Server 如何使用错误消息	321
	错误消息和消息号	322
	错误消息文本中的变量	323
	Adaptive Server 错误记录	324
	错误日志格式	324
	严重级	325
	严重级 10-18	326
	严重级 19-26	329
	报告错误	331
	Backup Server 错误记录	331
	注销进程	332
	仅将注销用于状态	335
	使用 sp_lock 检查阻塞进程	335
	管家功能	336
	管家清洗	336
	管家杂事	337
	管家碎片收集	337
	配置 enable housekeeper GC	338
	将 Adaptive Server 配置为保存 SQL 批处理文本	339
	为批处理文本分配内存	339
	不以文本表示的 SQL 命令	340
	查看 SQL 语句的查询计划	341
	查看嵌套的过程	342
	关闭服务器	343
	关闭 Adaptive Server	343
	关闭 Backup Server	344
	了解已知的问题	345
 第 2 部分	 安全性管理	
 第 12 章	 安全性简介	 349
	安全性简介	349
	什么是“信息安全性”？	349
	信息安全性标准	350
	公共标准配置评估	351
	FIPS 140-2 验证的加密模块	352

第 13 章	Adaptive Server 中的安全性管理快速入门	353
	安全性管理的一般过程	353
	设置安全性的建议	354
	设置安全性的示例	355
	Adaptive Server 中的安全性功能	357
	标识和鉴定	357
	自由选择访问控制	358
	角色分离	359
	责任审计	360
	数据保密性	361
第 14 章	管理远程服务器	363
	概述	363
	管理远程服务器	365
	添加远程服务器	365
	管理远程服务器名	367
	设置服务器连接选项	367
	获取有关服务器的信息	369
	删除远程服务器	369
	添加远程登录名	369
	映射用户的服务器 ID	370
	将远程登录名映射为特定的本地名	370
	将所有的远程登录名映射到一个本地名	371
	在本地服务器中保留远程登录名	372
	远程用户登录映射的示例	372
	远程用户的口令检查	374
	使用 untrusted 模式的效果	374
	获取有关远程登录的信息	375
	远程登录的配置参数	375
第 15 章	管理 Adaptive Server 登录名、数据库用户和客户端连接	377
	选择和创建口令	378
	将登录添加到 Adaptive Server	379
	登录失败	380
	创建组	381
	向数据库添加用户	381
	将 “guest” 用户添加到数据库	383
	将 guest 用户添加到服务器	384
	添加远程用户	385
	用户数和登录 ID 数	385
	ID 号的限制和范围	385
	登录连接限制	386
	为用户创建和指派角色	387

系统定义角色	388
系统管理员特权	388
系统安全员特权	389
操作员特权	390
Sybase 技术支持部门	390
“复制”角色	390
分布式事务管理器角色	391
高可用性角色	391
监控和诊断	391
Job Scheduler 角色	391
实时消息传送角色	391
Web 服务角色	392
密钥管理者角色	392
用户定义角色	392
添加和删除角色口令	393
角色层次和互斥性	394
角色层次和互斥性	394
设置登录时的缺省激活角色	397
激活和停用角色	398
设置组和添加用户	399
删除用户、组和用户定义角色	399
删除用户	399
删除组	400
删除用户定义角色	400
锁定或删除 Adaptive Server 登录帐户	400
锁定和解锁登录帐户	401
删除登录帐户	402
锁定拥有阈值的登录名	402
更改用户信息	402
更改口令	403
更改用户缺省值	404
更改用户组成员资格	405
更改用户进程信息	406
在数据库中使用别名	407
添加别名	407
删除别名	408
获取有关别名的信息	408
获取有关用户的信息	409
有关用户和进程的报告	409
获取有关登录帐户的信息	410
获取有关数据库用户的信息	411
查找用户名和 ID	411
显示有关角色的信息	413

建立口令和登录策略	415
设置和更改最大登录尝试次数	416
在丢失口令后登录	418
锁定和解锁登录和角色	418
显示口令信息	419
检查口令中是否至少包含一个数字	420
设置和更改 minimum password length	421
口令复杂程度检查	422
启用自定义口令检查	428
为口令设置登录名和角色有效期	430
保护磁盘上和内存中存储的登录口令	435
仅使用 SHA-256 算法	435
口令的字符集注意事项	438
升级和降级行为	439
当 allow password downgrade 设置为 0 时，口令会到期	443
上次登录和锁定不活动帐户	445
在高可用性环境中使用口令	446
监控许可证的使用状况	447
如何计算许可证数	448
配置许可证使用监控器	448
通过管家任务监控许可证使用状况	448
记录用户许可证数	449
获取有关使用情况的信息：收费退回式会计	449
报告当前使用状况统计信息	450
指定添加会计统计信息的间隔	450

第 16 章	外部鉴定	451
	配置 Adaptive Server 以实现基于网络的安全性	452
	安全服务和 Adaptive Server	453
	管理基于网络的安全性	453
	为安全性设置配置文件	454
	向安全性机制标识用户和服务器	460
	配置 Adaptive Server 的安全性	460
	添加登录以支持统一登录	464
	建立远程过程的安全性	465
	连接到服务器并使用安全服务	470
	获取有关可用安全服务的信息	472
	使用 Kerberos	474
	使用主管名	479
	并发 Kerberos 鉴定	484

为 LDAP 用户鉴定配置 Adaptive Server	485
组合型 DN 算法	486
搜索型 DN 算法	486
配置 LDAP	487
LDAP 用户鉴定管理	488
Adaptive Server 登录和 LDAP 用户帐户	491
辅助查找服务器支持	491
LDAP 服务器状态转换	493
LDAP 用户鉴定调优	495
对登录映射增加更严格的控制	496
LDAP 用户鉴定错误的故障排除	498
配置 LDAP 服务器	499
LDAP 用户鉴定改进	500
自动 LDAP 用户鉴定和故障恢复	501
设置 LDAP 故障恢复时间间隔	501
外部鉴定的登录映射	503
为使用 PAM 的鉴定配置 Adaptive Server	504
在 Adaptive Server 上启用 PAM	505
增强的登录控制	507
强制鉴定	507
使用 sp_maplogin 映射登录	508

第 17 章

管理用户权限	511
概述	511
创建数据库的权限	513
更改数据库所有权	513
数据库所有者特权	514
数据库对象所有者特权	515
其他数据库用户的特权	515
系统过程的权限	516
授予和撤消权限	516
对象访问权限	517
授予函数的权限	524
授予和撤消执行命令的权限	525
授予 dbcc 命令的权限	528
系统表的权限	529
组合 grant 和 revoke 语句	532
了解权限顺序及层次	533
Grant dbcc 和 set proxy 发出针对 fipslogger 的警告	534
授予和撤消角色	534
授予角色	534
了解 grant 和角色	535
撤消角色	536

获取另一用户的权限	536
使用 setuser	536
使用代理授权	537
权限报告	541
查询代理授权的 sysprotects 表	542
显示有关用户和进程的信息	542
报告数据库对象或用户的权限	543
报告特定表的权限	544
报告特定列的权限	545
使用视图和存储过程作为安全性机制	545
使用视图作为安全性机制	546
使用存储过程作为安全机制	548
了解所有权链	549
触发器的权限	553
使用行级访问控制	553
访问规则	554
使用应用程序环境功能	563
创建和使用应用程序环境	565
SYS_SESSION 系统应用程序环境	569
使用访问规则和 ACF 解决问题	570
使用登录触发器	572
从登录触发器导出 set 选项	580
设置全局登录触发器	581

第 18 章

审计	583
Adaptive Server 中的审计简介	583
将 Adaptive Server 与操作系统的审计记录相关联	584
审计系统	584
安装和设置审计	588
安装审计系统	588
设置审计追踪管理	592
设置事务日志管理	598
启用和禁用审计	599
单表审计	599
重新启动审计	602
设置全局审计选项	603
审计选项：类型和要求	603
隐藏系统存储过程和命令口令参数	610
确定当前审计设置	610
向审计追踪中添加用户指定的记录	611
查询审计追踪	612
了解审计表	613
读取 extrainfo 列	614
监控失败登录尝试次数	623
审计登录失败	624

第 19 章	数据的保密性	627
	Adaptive Server 中的安全套接字层 (SSL)	627
	因特网通信概述	628
	Adaptive Server 中的 SSL	630
	启用 SSL	633
	性能	639
	密码成套程序	639
	设置 SSL 密码成套程序优先选项	640
	使用 SSL 指定公用名	645
	使用 sp_listener 指定公用名	645
	存储过程 sp_addserver 已更改	645
	Kerberos 保密性	646
	转储和装载数据库时使用口令保护	646
	口令与 Adaptive Server 的早期版本	647
	口令和字符集	647
索引		649

关于本手册

读者

如何使用本手册

本手册（《系统管理指南：卷 1》）介绍如何在不借助任何特定数据库应用程序的情况下管理和控制 Sybase® Adaptive Server® Enterprise 数据库。

本手册的目标读者是 Sybase 系统管理员和数据库所有者。

本指南由两部分组成：第 1 部分介绍有关系统管理的基础概念，并包括以下各章：

- 第 1 章 “系统管理概述”，介绍 Sybase 系统的结构。
- 第 2 章 “系统及可选数据库”，讨论 Adaptive Server 系统数据库的内容和功能。
- 第 3 章 “系统管理入门”，概要介绍没有经验的系统管理员必须执行的重要任务。
- 第 4 章 “用于 Sybase Central 的 Adaptive Server 插件简介”，介绍如何启动和使用 Sybase Central（一个用于管理 Adaptive Server 的图形用户界面）。
- 第 5 章 “设置配置参数”，概要介绍用 `sp_configure` 设置的配置参数，这些参数控制 Adaptive Server 行为的许多方面。
- 第 6 章 “磁盘资源问题概述”，讨论 Adaptive Server 和 Backup Server™ 错误处理，并说明如何关闭服务器和注销用户进程。
- 第 7 章 “初始化数据库设备”，介绍如何初始化数据库设备以及如何将设备指派到设备的缺省缓冲池。
- 第 8 章 “设置数据库选项”，说明如何设置数据库选项。
- 第 9 章 “配置字符集、排序顺序和语言”，讨论国际问题，如语言模块中包含的文件和如何配置 Adaptive Server 的语言、排序顺序和字符集。
- 第 10 章 “配置客户端 / 服务器字符集转换”，讨论异构环境中 Adaptive Server 和客户端之间的字符集转换。
- 第 11 章 “诊断系统问题”，讨论 Adaptive Server 和 Backup Server 错误处理，并说明如何关闭服务器和注销用户进程。

第 2 部分讨论安全性管理，包括以下各章：

- [第 12 章 “安全性简介”](#)，介绍安全性概念。
- [第 13 章 “Adaptive Server 中的安全性管理快速入门”](#)，概述 Adaptive Server 中可用的安全性功能。
- [第 15 章 “管理 Adaptive Server 登录名、数据库用户和客户端连接”](#)，介绍如何管理 Adaptive Server 登录帐户和数据库用户。
- [第 14 章 “管理远程服务器”](#)，讨论在启用远程过程调用 (RPC) 时，每个 Adaptive Server 系统管理员和系统安全员必须执行的步骤。
- [第 16 章 “外部鉴定”](#)，说明基于网络的安全服务。这些服务用于鉴定用户和保护在网络上的计算机之间传输的数据。
- [第 17 章 “管理用户权限”](#)，说明用户权限的使用和实施。
- [第 18 章 “审计”](#) 说明如何为安装设置审计。
- [第 19 章 “数据的保密性”](#)，介绍如何配置 Adaptive Server 以确保所有数据的安全性和保密性。

相关文档

Adaptive Server[®] Enterprise 文档集包括：

- 针对所用平台的发行公告 — 包含未能及时写入手册的最新信息。
最新版本的发行公告可能已提供。若要了解本产品 CD 发行以后增加的重要产品或文档信息，请使用 Sybase[®] Product Manuals 网站。
- 针对所用平台的安装指南 — 介绍所有 Adaptive Server 产品及相关 Sybase 产品的安装、升级和一些配置过程。
- New Feature Summary (《新增功能摘要》) — 介绍 Adaptive Server 中的新增功能，为支持这些功能所添加的系统更改，以及可能会影响现有应用程序的更改。
- Active Messaging Users Guide (《Active Messaging 用户指南》) — 介绍如何使用 Active Messaging 功能捕获 Adaptive Server Enterprise 数据库中的事务 (数据更改)，并将它们作为事件实时发送给外部应用程序。
- 《组件集成服务用户指南》 — 说明如何使用组件集成服务功能来连接远程 Sybase 和非 Sybase 数据库。
- 针对所用平台的《配置指南》 — 提供执行特定配置任务的操作说明。
- 《词汇表》 — 定义 Adaptive Server 文档中使用的技术术语。
- 《Historical Server 用户指南》 — 介绍如何使用 Historical Server 从 Adaptive Server 获取性能信息。

- 《Adaptive Server Enterprise 中的 Java》— 介绍在 Adaptive Server 数据库中如何安装 Java 类，如何将它们用作数据类型、函数及存储过程。
- 《Job Scheduler 用户指南》— 提供有关如何使用命令行或图形用户界面 (GUI) 在本地或远程 Adaptive Server 上安装、配置、创建和调度作业的操作说明。
- 《迁移技术指南》— 介绍用于迁移到不同版本 Adaptive Server 的策略和工具。
- 《Monitor Client Library 程序员指南》— 介绍如何编写访问 Adaptive Server 性能数据的 Monitor Client Library 应用程序。
- 《Monitor Server 用户指南》— 介绍如何使用 Monitor Server 从 Adaptive Server 获取性能统计信息。
- Monitoring Tables Diagram (《监控表框图》) — 以张贴画的形式阐明监控表及其实体关系。实际大小的图只提供印刷品；缩略图采用 PDF 格式提供。
- Performance and Tuning Series 《性能和调优系列》— 是一系列丛书，介绍如何调整 Adaptive Server 以获得最优性能：
 - Basics (《基础知识》) — 通晓和研究 Adaptive Server 的性能问题需具备的基础知识。
 - Improving Performance with Statistical Analysis (《利用统计分析改进性能》) — 介绍 Adaptive Server 如何存储和显示统计信息，及如何使用 `set statistics` 命令分析服务器统计信息。
 - Locking and Concurrency Control (《锁定和并发控制》) — 介绍如何使用锁定方案改进性能，及如何选择索引以最大限度地降低并发操作次数。
 - Monitoring Adaptive Server with sp_sysmon (《使用 sp_sysmon 监控 Adaptive Server》) — 讨论如何使用 sp_sysmon 监控性能。
 - Monitoring Tables (《监控表》) — 介绍如何从 Adaptive Server 的监控表中查询统计信息和诊断信息。
 - Physical Database Tuning (《物理数据库调优》) — 介绍如何管理物理数据放置、为数据分配的空间及临时数据库。
 - Query Processing and Abstract Plans (《查询处理和抽象计划》) — 介绍优化程序如何处理查询以及如何使用抽象计划更改某些优化程序计划。

-
- 《快速参考指南》 — 这是一本袖珍手册，完整地列出了各种命令、函数、系统过程、扩展系统过程、数据类型和实用程序的名称和语法（该手册在用 PDF 格式阅读时采用正常大小）。
 - 《参考手册》 — 是一系列丛书，包含详细的 Transact-SQL[®] 信息：
 - 《构件块》 — 讨论数据类型、函数、全局变量、表达式、标识符、通配符和保留字。
 - 《命令》 — 介绍各种命令。
 - 《过程》 — 介绍系统过程、目录存储过程、系统扩展存储过程及 dbcc 存储过程。
 - 《表》 — 讨论系统表、监控表及 dbcc 表。
 - 《系统管理指南》 —
 - 《卷 1》 — 介绍了系统管理的基本知识，包括配置参数说明、资源问题、字符集、排序顺序及诊断系统问题的操作说明。《卷 1》的第二部分深入讨论了安全性管理。
 - 《卷 2》 — 包括管理物理资源、镜像设备、配置内存和数据高速缓存、管理多处理器服务器和用户数据库、装入和卸下数据库、创建和使用段、使用 reorg 命令及检查数据库一致性的操作说明和指导。《卷 2》的后半部分介绍了如何备份和恢复系统数据库和用户数据库。
 - System Tables Diagram（《系统表框图》） — 以张贴画的形式阐明系统表及其实体关系。实际大小的图只提供印刷品；缩略图采用 PDF 格式提供。
 - 《Transact-SQL 用户指南》 — 提供有关 Transact-SQL 这一 Sybase 关系数据库语言增强版的文档资料。此指南可作为数据库管理系统入门用户的教科书，还包括 pubs2 和 pubs3 示例数据库的详细说明。
 - Troubleshooting: Error Messages Advanced Resolutions（《故障排除：错误消息高级解析》） — 包括您可能遇到的问题的故障排除步骤。此处讨论的问题是 Sybase 技术支持人员最常听到的问题。
 - 《加密列用户指南》 — 介绍了如何利用 Adaptive Server 配置和使用加密列。
 - 《内存数据库用户指南》 — 介绍如何配置和使用内存数据库。
 - Using Adaptive Server Distributed Transaction Management Features（《使用 Adaptive Server 分布式事务管理功能》） — 介绍如何在分布式事务处理环境中配置、使用 Adaptive Server DTM 功能以及如何排除其中的故障。

- 《将 Backup Server 与 IBM® Tivoli® Storage Manager 配合使用》——介绍如何设置和使用 IBM Tivoli Storage Manager 以创建 Adaptive Server 备份。
- 《在高可用性系统中使用 Sybase 故障切换》——提供有关使用 Sybase 的故障切换功能将 Adaptive Server 配置为高可用性系统中的协同服务器的操作说明。
- Unified Agent and Agent Management Console（《Unified Agent 和 Agent Management Console》）——介绍用于提供管理、监控和控制分布式 Sybase 资源的运行期服务的 Unified Agent。
- 《实用程序指南》——提供有关在操作系统级别执行的 Adaptive Server 实用程序（例如 isql 和 bcp）的文档资料。
- 《Web 服务用户指南》——介绍如何配置、使用 Adaptive Server Web 服务以及如何排除其中的故障。
- 《适用于 CICS、Encina 和 TUXEDO 的 XA 接口集成指南》——提供有关将 Sybase DTM XA 接口与 X/Open XA 事务管理器配合使用的说明。
- 《Adaptive Server Enterprise 中的 XML 服务》——介绍了 Sybase 本机 XML 处理器、Sybase 基于 Java 的 XML 支持及数据库中的 XML，并提供了 XML 服务中可用的查询和映射函数的文档资料。

其它信息来源

使用 Sybase Getting Started CD、SyBooks™ CD 和 Sybase Product Manuals 网站可以了解有关产品的更多信息：

- Getting Started CD 包含 PDF 格式的发行公告和安装指南，还可能包含 SyBooks CD 中未收纳的其它文档或更新信息。它随软件一起提供。若要阅读或打印 Getting Started CD 上的文档，需要使用 Adobe Acrobat Reader，该软件可以使用 CD 上提供的链接从 Adobe 网站免费下载。
- SyBooks CD 含有产品手册，它随软件一起提供。基于 Eclipse 的 SyBooks 浏览器使您能够以易于使用的、基于 HTML 的格式阅读手册。

有些文档可能是以 PDF 格式提供的，您可以通过 SyBooks CD 上的 PDF 目录访问这些文档。若要阅读或打印 PDF 文件，您需要使用 Adobe Acrobat Reader。

有关安装和启动 SyBooks 的说明，请参见 Getting Started CD 上的《SyBooks 安装指南》或 SyBooks CD 上的 *README.txt* 文件。

-
- Sybase Product Manuals 网站是 SyBooks CD 的联机版本，您可以使用一种标准 Web 浏览器来访问它。除了产品手册之外，还可以找到有关 EBFs/Maintenance（EBF/维护）、Technical Documents（技术文档）、Case Management（案例管理）、Solved Cases（解决的案例）、Newsgroups（新闻组）和 Sybase Developer Network（Sybase 开发员网络）的链接。

要访问 Sybase Product Manuals 网站，请转到位于

<http://www.sybase.com/support/manuals/> 的“产品手册” (Product Manuals)。

Web 上的 Sybase 认证

Sybase 网站上的技术文档会不断更新。

❖ 查找有关产品认证的最新信息

- 1 将 Web 浏览器定位到位于 <http://www.sybase.com/support/techdocs/> 的“技术文档” (Technical Documents)。
- 2 单击“认证报告” (Certification Report)。
- 3 在“认证报告” (Certification Report) 过滤器中选择相应的产品、平台和时间范围，然后单击“查找” (Go)。
- 4 单击“认证报告” (Certification Report) 标题显示此报告。

❖ 查找有关组件认证的最新信息

- 1 将 Web 浏览器定位到位于 <http://certification.sybase.com/> 的“可用性和认证报告” (Availability and Certification Reports)。
- 2 在“按基本产品搜索” (Search by Base Product) 下选择产品系列和产品，或在“按平台搜索” (Search by Platform) 下选择平台和产品。
- 3 选择“搜索” (Search) 以显示所选项目的可用性和认证报告。

❖ 创建 Sybase 网站（包括支持页）的个人化视图

建立 MySybase 配置文件。MySybase 是一项免费服务，它允许您创建 Sybase Web 页的个人化视图。

- 1 将 Web 浏览器定位到位于 <http://www.sybase.com/support/techdocs/> 的“技术文档” (Technical Documents)。
- 2 单击“我的 Sybase” (MySybase) 并创建 MySybase 配置文件。

Sybase EBF 和软件维护

❖ 查找有关 EBF 和软件维护的最新信息

- 1 将 Web 浏览器定位到位于 <http://www.sybase.com/support> 的“Sybase 支持页” (Sybase Support Page)。
- 2 选择 “EBF/ 维护” (EBFs/Maintenance)。如果出现提示信息，请输入您的 MySybase 用户名和口令。
- 3 选择一个产品。
- 4 指定时间范围并单击 “查找” (Go)。即会显示 EBF/ 维护版本的列表。

锁形图标表示因为您没有注册为 “技术支持联系人” (Technical Support Contact)，因此您没有某些 EBF/ 维护版本的下载授权。如果您尚未注册，但拥有 Sybase 代表提供的或通过支持合同获得的有效信息，请单击 “编辑角色” (Edit Roles) 将 “技术支持联系人” (Technical Support Contact) 角色添加到 MySybase 配置文件中。

- 5 单击信息图标可显示 EBF/ 维护报告，单击产品说明可下载软件。

约定

以下各部分将说明在本手册中使用的约定。

SQL 是一种形式自由的语言。没有规定每一行中的单词数量或者必须折行的地方。然而，为便于阅读，本手册中所有示例和大多数语法语句都经过了格式设置，以便语句的每个子句都在一个新行上开始。有多个成分的子句会扩展到其它行，这些行会有缩进。复杂命令使用已修改的 Backus Naur Form (BNF) 符号进行了格式处理。

表 1 说明本手册中出现的语法语句的约定：

表 1：本手册的字体和语法定义

元素	示例
命令名、过程名、实用程序名和其它关键字用 sans serif 字体显示。	<code>select</code> <code>sp_configure</code>
数据库名和数据库类型用 sans serif 字体显示。	<code>master</code> 数据库
书名采用正常字体并加书名号；文件名、变量和路径名用斜体显示。	《系统管理指南》 <code>sql.ini</code> 文件 <code>column_name</code> <code>\$SYBASE/ASE</code> 目录
变量（即代表您要填充的值的词语）作为查询或语句的一部分出现时用斜体的 Courier 字体显示。	<code>select column_name</code> <code>from table_name</code> <code>where search_conditions</code>
键入小括号作为命令的一部分。	<code>compute row_aggregate (column_name)</code>

元素	示例
双冒号加等号表示语法是用 BNF 符号编写的。请勿输入此符号。表示“被定义为”。	::=
大括号表示至少必须选择括号中的一个选项。不要输入大括号。	{cash, check, credit}
方括号表示可以选择括号中的一个或多个选项，也可不选。不要输入方括号。	[cash check credit]
逗号表示可以选择任意多个显示的选项。可用逗号作为命令的一部分来分隔选项。	cash, check, credit
竖线 () 表示只可选择所显示的选项中的一个。	cash check credit
省略号 (...) 表示可以将最后一个单元重复任意多次。	buy thing = price [cash check credit] [, thing = price [cash check credit]]... 您必须至少购买一件产品，并给出其价格。可以选择一种付款方式：方括号中的选项之一。还可选择购买其它物品：可根据需要购买任意数量的物品。对于要买的每种产品，给出其名称、价格和付款方式（可选）。

- 语法语句（显示命令的语法和所有选项）显示如下：

`sp_dropdevice [device_name]`

对于具有多个选项的命令：

`select column_name
from table_name
where search_conditions`

在语法语句中，关键字（命令）采用常规字体，而标识符为小写。斜体表示用户提供的内容。

- 说明 Transact-SQL 命令用法的示例如下：

`select * from publishers`

- 计算机输出的示例如下：

pub_id	pub_name	city	state
0736	New Age Books	Boston	MA
0877	Binnet & Hardley	Washington	DC
1389	Algodata Infosystems	Berkeley	CA

(3 rows affected)

本手册中的大多数示例都用小写显示。不过，输入 Transact-SQL 关键字时可以忽略大小写。例如，`SELECT`、`Select` 和 `select` 是相同的。

Adaptive Server 是否区分数据库对象（如表名）的大小写，取决于安装在 Adaptive Server 上的排序顺序。通过重新配置 Adaptive Server 的排序顺序，可改变单字节字符集的区别大小写设置。有关详细信息，请参见《系统管理指南》。

辅助功能特性

本文档具有针对辅助功能进行了专门设计的 HTML 版本。可以利用适应性技术（如屏幕阅读器）浏览 HTML 文档，也可以用屏幕放大器进行查看。

Adaptive Server HTML 文档已经过测试，符合美国政府“第 508 节辅助功能”的要求。符合“第 508 节”的文档一般也符合非美国的辅助功能原则，如针对网站的 World Wide Web 协会 (W3C) 原则。

注释 您可能需要对辅助功能工具进行配置以获得最佳使用效果。某些屏幕阅读器按照大小写来辨别文本，例如将“ALL UPPERCASE TEXT”看作首字母缩写，而将“MixedCase Text”看作单词。对工具进行配置，规定语法规则，您可能会感觉更方便。有关工具的信息，请查阅文档。

有关 Sybase 如何支持辅助功能的信息，请参见位于 <http://www.sybase.com/accessibility> 的“Sybase 辅助功能” (Sybase Accessibility)。Sybase Accessibility 站点包括指向“第 508 节”和 W3C 标准相关信息的链接。

如果需要帮助

对于购买了支持合同的客户安装的每一个 Sybase 产品，都会有一位或多位指定人员获得与 Sybase 技术支持部门联系的授权。如果使用手册或联机帮助不能解决问题，可让指定人员与 Sybase 技术支持部门联系或与所在区域的 Sybase 子公司联系。

系统管理基础知识

以下各章介绍 Adaptive Server 中系统管理的概念：

- [第 1 章 “系统管理概述”](#)，介绍 Sybase 系统的结构。
- [第 2 章 “系统及可选数据库”](#)，讨论 Adaptive Server 系统数据库的内容和功能。
- [第 3 章 “系统管理入门”](#)，概要介绍没有经验的系统管理员必须执行的重要任务。
- [第 4 章 “用于 Sybase Central 的 Adaptive Server 插件简介”](#)，介绍如何启动和使用 Sybase Central（一个用于管理 Adaptive Server 的图形用户界面）。
- [第 5 章 “设置配置参数”](#)，概要介绍用 sp_configure 设置的配置参数，这些参数控制 Adaptive Server 行为的许多方面。
- [第 6 章 “磁盘资源问题概述”](#)，介绍与磁盘上数据库、表和索引的物理放置相关的问题。
- [第 7 章 “初始化数据库设备”](#)，介绍如何初始化数据库设备和如何将设备指派到设备的缺省缓冲池。
- [第 8 章 “设置数据库选项”](#)，说明如何设置数据库选项。
- [第 9 章 “配置字符集、排序顺序和语言”](#)，讨论国际问题，如语言模块中包含的文件和如何配置 Adaptive Server 的语言、排序顺序和字符集。
- [第 10 章 “配置客户端 / 服务器字符集转换”](#)，讨论异构环境中 Adaptive Server 和客户端之间的字符集转换。
- [第 11 章 “诊断系统问题”](#)，讨论 Adaptive Server 和 Backup Server™ 错误处理，并说明如何关闭服务器和注销用户进程。

系统管理概述

本章介绍 Adaptive Server 系统管理的基本主题。

主题	页码
Adaptive Server 管理任务	3
系统表	9
系统过程	11
系统扩展存储过程	13
记录错误消息	14
连接到 Adaptive Server	14
Adaptive Server 中可用的安全性功能	18

Adaptive Server 管理任务

Adaptive Server 管理任务包括：

- 安装 Adaptive Server 和 Backup Server
- 创建和管理 Adaptive Server 登录帐户
- 为 Adaptive Server 用户授予角色和权限
- 管理和监控磁盘空间、内存和连接的使用情况
- 备份和恢复数据库
- 诊断系统问题
- 配置 Adaptive Server 以获取最佳性能

此外，系统管理员还可以协助完成某些数据库设计任务，这些任务与应用程序设计者的工作（例如强制执行完整性标准）重叠。

虽然一般而言系统管理员主要是执行与 Adaptive Server 上运行的应用程序无关的任务，但系统管理员可能对所有应用程序的概况最为了解。因此，系统管理员可以就 Adaptive Server 中已存在的数据向应用程序设计者提出建议，并推荐在应用程序之间使数据定义标准化的方法等。

不过，具体应用程序对应的任务会有所区别，而实际的不同之处有时会有些“模糊”。用户数据库的所有者可参考本手册的某些章节。同样，系统管理员和数据库所有者还可以使用《Transact-SQL 用户指南》（特别是有关数据定义、存储过程和触发器的章节）。系统管理员和应用程序设计者都需要使用 Performance and Tuning Series（《性能和调优系列》）。

系统管理任务所需的角色

本手册中讨论的许多命令和过程都需要系统管理员或系统安全员角色。本手册中的其它各节与数据库所有者相关。

各种与安全性有关的任务、管理任务和操作任务经过分组分配到以下用户角色中：

- **系统管理员** — 缺省情况下，为系统管理员 (sa) 分配了以下角色：
 - sa_role
 - sso_role
 - oper_role
 - sybase_ts_role

系统管理员的任务包括：

- 管理磁盘存储
- 监控 Adaptive Server 自动恢复过程
- 通过更改可配置的系统参数来调整 Adaptive Server
- 诊断和报告系统问题
- 备份和装载数据库
- 修改和删除服务器登录帐户
- 授予和撤消系统管理员角色
- 为 Adaptive Server 用户授予权限
- 创建用户数据库并授予数据库的所有权
- 建立可用于授予和撤消权限的组

- **系统安全员** — 执行与安全性相关的任务，例如：
 - 创建服务器登录帐户，包括指派初始口令
 - 更改任何帐号的口令
 - 授予和撤消系统安全员和操作员角色
 - 创建、授予和撤消用户定义角色
 - 授予模拟服务器中另一个用户的能力
 - 设置口令有效期间隔
 - 设置 Adaptive Server 以使用基于网络的安全服务
 - 管理审计系统
- **操作员** — 在全服务器范围内备份和装载数据库。操作员角色允许单个用户使用 `dump database`、`dump transaction`、`load database` 和 `load transaction` 命令备份和恢复服务器上的所有数据库，而不必是每个数据库的所有者。这些操作可以由数据库所有者或系统管理员为单个数据库执行。但是，操作员可以为所有数据库执行这些操作。

这些角色为执行操作任务和管理任务的用户指定了个人职责。用户的操作可以被审计并归属于这些用户。系统管理员的操作不受自由选择访问控制 (DAC) 保护系统的限制，也就是说，当系统管理员访问对象时，Adaptive Server 不会检查 DAC 权限。

此外，有两种类型的对象所有者因其所拥有对象的不同而具有特殊的状态。这些所有权类型为：

- 数据库所有者
- 数据库对象所有者

数据库所有者

数据库所有者是数据库的创建者或接受移交的数据库所有权的用户。系统管理员可使用 `grant` 命令授予用户创建数据库的权限。

数据库所有者使用分配给自己的登录名和口令登录到 Adaptive Server，并具有“dbo”帐户。当此用户登录到不是由他们创建的数据库时，此用户由其常规用户名来标识。

数据库所有者可以：

- 运行系统过程 `sp_adduser` 以允许其他 Adaptive Server 用户访问数据库
- 使用 `grant` 命令授予其他用户在数据库内创建对象和执行命令的权限

向数据库中增加用户将在第 15 章 “管理 Adaptive Server 登录名、数据库用户和客户端连接” 中进行讨论。授予用户权限将在第 17 章 “管理用户权限” 中进行讨论。

数据库所有者不会自动获得对其他用户所拥有的对象的权限。但是，数据库所有者可以随时通过使用 `setuser` 命令临时获得数据库中其他用户的权限。通过组合使用 `setuser` 和 `grant` 命令，数据库所有者可以获得对数据库中任何对象的权限。

注释 由于数据库所有者角色的权限比较强大，因此系统管理员应该仔细规划应拥有服务器中数据库的人员。系统安全员应该考虑审计所有数据库所有者的数据库活动。

数据库对象所有者

数据库对象所有者是创建数据库对象的用户。**数据库对象**包括表、索引、视图、缺省值、触发器、规则、约束和过程。在用户可以创建数据库对象之前，数据库所有者必须先授予该用户创建特定类型对象的权限。数据库对象所有者没有特殊的登录名或口令。

数据库对象所有者可使用适当的 `create` 语句创建对象，然后为其他用户授予权限。

数据库对象的创建者将被自动授予对该对象的所有权限。系统管理员也拥有对该对象的所有权限。对象所有者必须其他用户可以访问该对象之前明确地将权限授予这些用户。即使是数据库所有者也无法直接使用对象，除非对象所有者授予其相应的权限。但是，数据库所有者总是可以使用 `setuser` 命令模拟数据库中的任何其他用户，包括对象所有者。

注释 如果拥有数据库对象的用户不是数据库所有者，则该用户（包括系统管理员）必须使用对象所有者的名称来限定该对象的名称 (`ownername.objectname`) 才能访问该对象。如果有非常多的用户必须访问某个对象或过程（尤其是在即席查询中），则让 “dbo” 拥有这些对象可极大地简化访问。

使用 *isql* 执行系统管理任务

本手册假定您使用命令行实用程序 *isql* 来执行本指南中描述的系统管理任务。本节提供有关使用 *isql* 的一些基本信息。有关完整信息，请参见《实用程序指南》。

也可以使用图形化工具 Sybase Central™ 执行本手册中描述的许多任务，如第 8 页的“将 Sybase Central 用于系统管理任务”中所述。

启动 *isql*

在大多数平台上，若要启动 *isql*，请在操作系统提示符下键入以下命令，其中 *username* 为系统管理员：

```
isql -Uusername
```

Adaptive Server 将提示输入口令。

注释 不要使用 *isql* 的 *-P* 选项来指定口令；其他用户随后可能会看到您的口令。

可以在命令行模式下使用 *isql* 来输入本手册中的许多 Transact-SQL 示例。

输入语句

在 *isql* 中输入的语句可以占多行。只有在您另起一行键入了“go”时，*isql* 才会处理语句。例如：

```
1> select *
2> from sysobjects
3> where type = "TR"
4> go
```

本手册中的示例在各语句间不包含 *go* 命令。在您键入示例时，必须输入 *go* 命令才可以查看输出样本。

保存和重用语句

本手册经常建议您保存用于创建或修改用户数据库和数据库对象的 Transact-SQL 语句。最简便的方法就是创建一个 ASCII 格式的文件，或将这些语句复制到一个 ASCII 格式的文件中。以后如果需要重新创建数据库或数据库对象，则可以使用该文件为 *isql* 提供语句。

在 *isql* 中使用 ASCII 格式文件的语法如下，其中 *filename* 是包含 Transact-SQL 语句的文件的完整路径和文件名：

```
isql -Uusername -ifilename
```

在 UNIX 和其它平台中，使用 “小于” 符号 (<) 重定向该文件。

ASCII 文件中的 Transact-SQL 语句必须使用有效的语法和 go 命令。

读取来自文件的命令时，必须：

- 在命令行中提供 **-Ppassword** 选项，或
- 在输入文件的第一行上包括指定用户的口令。

将 Sybase Central 用于系统管理任务

使用 Adaptive Server 所带的图形化工具 Sybase Central，可以执行许多系统管理任务。

- 初始化数据库设备
- 设置配置参数
- 查看数据库中可用日志空间的数量
- 生成数据定义语言 (DDL)
- 创建登录
- 增加远程服务器
- 创建数据库
- 创建存储过程
- 定义角色
- 增加数据高速缓存
- 设置数据库选项
- 备份和恢复数据库

使用 Sybase Central 的 Monitor Viewer 功能来访问 Adaptive Server Monitor™。Sybase Central 包括大量的联机帮助。

使用 Sybase Central 的 DDL 生成功能记录对 Transact-SQL 脚本的处理。利用 DDL 生成功能，可将整个服务器中或特定数据库内执行的操作保存到脚本中。

系统表

master 数据库包含跟踪有关 Adaptive Server 信息的**系统表**。此外，每个数据库（包括 **master** 数据库）都包含可跟踪特定于该数据库的信息的系统表。

master 数据库（Adaptive Server 控制数据库）中 Adaptive Server 提供的所有表都被视为系统表。每个用户数据库都是使用这些系统表的子集创建的。还可以将系统表称为**数据字典**或系统目录。

master 数据库及其表是在安装 Adaptive Server 时自动创建的。用户数据库中的系统表是在发出 **create database** 命令后创建的。所有系统表的名称均以 “sys” 开头。不能在用户数据库中创建与系统表同名的表。请参见《参考手册：表》，了解系统表及其列的详细说明。

查询系统表

采用查询任何其它表一样的方式来查询系统表。例如，以下语句将返回数据库中所有触发器的名称：

```
select name
from sysobjects
where type = "TR"
```

此外，Adaptive Server 还提供了**存储过程**（称为**系统过程**），许多存储过程都提供查询系统表的快捷方式。

以下系统过程可提供系统表中的信息：

• sp_commonkey	• sp_helpremotelogin
• sp_configure	• sp_help_resource_limit
• sp_countmedatada	• sp_helpprotect
• sp_dboption	• sp_helpsegment
• sp_estspace	• sp_helpserver
• sp_help	• sp_helpsort
• sp_helppartition	• sp_helptext
• sp_helpcache	• sp_helpthreshold
• sp_helpconfig	• sp_helpuser
• sp_helpconstraint	• sp_lock
• sp_helppdb	• sp_monitor
• sp_helpdevice	• sp_monitorconfig
• sp_helpgroup	• sp_showcontrolinfo
• sp_helpindex	• sp_showexeclass
• sp_helpjava	• sp_showplan

• sp_helpjoins	• sp_spaceused
• sp_helpkey	• sp_who
• sp_helplanguage	• sp_help_resource_limit
• sp_helplog	

有关系统过程的完整信息，请参见 《参考手册：过程》。

系统表中的键

系统表的主键、外键和公用键是在 `master` 和 `model` 数据库中定义的。通过执行 `sp_helpkey`，可以生成关于已定义的键的报告。若要获得两个可能是连接候选者的系统表中各列的报告，请执行 `sp_helpjoins`。

Adaptive Server System Tables Diagram （《Adaptive Server 系统表框图》）显示了系统表中各列之间的关系。

更新系统表

Adaptive Server 系统表包含对数据库操作非常重要的信息。通常情况下，不必对系统表直接进行数据修改。

只能在 Sybase 技术支持部门指导下或按照 `Error Messaging and Troubleshooting Guide` （《错误消息和故障排除指南》）或本手册中的指导来更新系统表。

更新系统表之前，必须发出启用系统表更新的 `sp_configure` 命令。此命令生效时，任何具有相应权限的用户都可以修改系统表。要直接修改系统表，还有一些其它要求：

- 仅在事务内部修改系统表。在发出数据修改命令之前先发出 `begin transaction` 命令。
- 验证是否只有希望更改的行受此命令的影响，且数据已正确更改。
- 如果命令不正确，则发出 `rollback transaction` 命令。如果命令正确，则发出 `commit transaction` 命令。

警告！ 某些系统表在任何情况下均不得由任何用户进行改变。某些系统表由系统过程动态建立，包含编码信息，或在查询时仅显示一部分数据。轻率地即席更新某些系统表会导致 Adaptive Server 无法运行、数据库对象不可访问、对象权限混乱或用户会话终止。此外，绝不要尝试以任何方式改变系统表的定义。例如，不要将系统表变为包含约束。系统表中不允许包含触发器、缺省值和规则。如果创建触发器、绑定规则或为系统表使用缺省值，您将看到一条错误消息。

系统过程

所有系统过程的名称均以“sp_”开头。系统过程位于 `sybsystemprocs` 数据库中，但是，通过从数据库中执行存储过程或使用数据库名限定过程名，可以在任何数据库中运行多个系统过程。

Sybase 提供的系统过程（例如 `sp_who`）是使用 *installmaster* 安装脚本创建的。使用 `sp_version` 可确定最近执行的 *installmaster* 的版本。请参见《参考手册：过程》，了解有关 `sp_version` 的详细信息。

如果执行的系统过程并非在 `sybsystemprocs` 数据库中，则该过程会在执行它的数据库中的系统表上运行。例如，如果 `pubs2` 的数据库所有者从 `pubs2` 中运行 `sp_adduser`，或发出命令 `pubs2..sp_adduser`，则会将新用户添加到 `pubs2..sysusers` 中。但是，这不适用于只更新 `master` 数据库表的系统过程。

对系统过程的权限在《参考手册：过程》。

使用系统过程

参数是存储过程或系统过程的变量。如果系统过程的参数值包含保留字、标点符号或嵌入的空格，则必须将其括在单引号或双引号中。如果参数是对象名，并且对象名用数据库名或所有者名加以限定，则必须用单引号或双引号将整个名称括起来。

可以在会话过程中使用链式事务模式或非链式事务模式来调用系统过程。链式模式在执行任何数据检索或修改语句之前会隐式开始一项事务。非链式模式要求显式用与 `commit transaction` 或 `rollback transaction` 语句成对出现的 `begin transaction` 语句来开始事务。请参见《Transact-SQL 用户指南》中的第 21 章“事务：维护数据一致性和恢复”。

修改 `master` 数据库系统表中的数据的系统过程不能在事务内部执行，因为这可能会损害恢复过程。创建临时工作表的系统过程不能从事务中运行。

如果执行系统过程时没有活动的事务，`Adaptive Server` 将关闭链式模式并在过程执行期间设置 `transaction isolation level 1`。返回之前，会话的链接模式和隔离级别将重置为其原始设置。请参见《Transact-SQL 用户指南》中的第 21 章“事务：维护数据一致性和恢复”。

所有系统过程都会报告返回状态。例如，以下返回状态表示该过程已成功执行：

```
return status = 0
```

如果系统过程未成功执行，则返回状态为非 0 数字。

系统过程表

系统过程使用 **master** 和 **sybsystemdb** 数据库中的多个**系统过程表**，将内部系统值（如状态位）转换为用户可以理解的格式。其中的 **spt_values** 表可以由许多系统过程使用，包括：

• sp_configure	• sp_helpdevice
• sp_dboption	• sp_helpindex
• sp_depends	• sp_helpkey
• sp_help	• sp_helpprotect
• sp_helpdb	• sp_lock

spt_values 表只能通过升级进行更新；您不能修改该表。若要了解该表如何使用，请执行 **sp_helptext** 并查看引用该表的其中一个系统过程的文本。

其它系统过程表包括 **spt_monitor**、**spt_committab** 和目录存储过程所需的表。（**spt_committab** 表位于 **sybsystemdb** 数据库中。）

此外，某些系统过程会先创建临时表，然后再删除它们。例如，**sp_helpdb** 创建 **#spdbdesc**，**sp_helpdevice** 创建 **#spdevtab**，而 **sp_helpindex** 创建 **#spindtab**。

创建系统过程

本手册的相关章节中解释了很多系统过程。有关详细的参考信息，请参见《参考手册：过程》。

系统管理员可编写能够在任何数据库中执行的系统过程。在 **sybsystemprocs** 中创建一个存储过程，并为其指派一个以 “sp_” 开头的名称。存储过程的 **uid** 必须为 1，即数据库所有者的 **uid**。

创建的大多数系统过程都会查询系统表。Sybase 建议您不要创建修改系统表的存储过程。

若要创建修改系统表的存储过程，系统安全员必须先启用 **allow updates to system tables** 配置参数。此参数设置为启用时创建的任何存储过程始终可以更新系统表，即使当 **allow updates to system tables** 处于禁用状态时也是如此。创建更新系统表的存储过程：

- 1 使用 **sp_configure** 将 **allow updates to system tables** 设置为启用。
- 2 使用 **create procedure** 创建存储过程。

- 3 使用 `sp_configure` 将 `allow updates to system tables` 设置为禁用。

警告！ 在修改系统表时要小心。请始终在开发或测试数据库中测试修改系统表的过程，而不是在生产数据库中进行测试。

系统扩展存储过程

利用扩展存储过程 (ESP)，您可以从 Adaptive Server 内调用外部语言函数。Adaptive Server 包括一组预定义 ESP；用户也可以创建自己的扩展存储过程。所有系统扩展存储过程的名称均以 “xp_” 开头，并位于 `sybsystemprocs` 数据库中。

`xp_cmdshell` 是一个非常有用的系统 ESP，它可以在运行 Adaptive Server 的系统上执行操作系统命令。

就像调用系统过程那样调用系统 ESP。不同之处在于系统 ESP 执行过程语言代码，而不是 Transact-SQL 语句。所有 ESP 均由名为 XP Server™ 的 Open Server™ 应用程序实现，该应用程序与 Adaptive Server 运行在同一台计算机上。XP Server 在第一次调用 ESP 时自动启动。

有关 Adaptive Server 附带的系统 ESP 的信息，请参见《参考手册：过程》。

创建系统 ESP

使用 `create procedure` 在 `sybsystemprocs` 数据库中创建系统 ESP。系统过程将自动包括在 `sybsystemprocs` 数据库中。ESP 的名称及其过程语言函数必须以 “xp_” 开头。存储过程的 `uid` 必须为 1，即数据库所有者的 `uid`。

有关创建 ESP 的一般信息，请参见《Transact-SQL 用户指南》中的第 17 章 “使用扩展存储过程”。

记录错误消息

每次启动时，Adaptive Server 都会将启动信息写入一个本地错误日志文件。在配置新的 Adaptive Server 时，安装程序会自动设置错误日志的位置。请参见所用平台的《配置指南》，以了解错误日志的缺省位置和文件名。

Adaptive Server 中的许多错误消息只会写入用户的终端。不过，Adaptive Server 的致命错误消息（严重级为 19 及以上）、内核错误消息或信息性消息将会记录在错误日志文件中。

Adaptive Server 会使错误日志文件保持打开状态，直至您停止服务器进程为止。在删除旧消息以减小错误日志的大小之前，请停止 Adaptive Server 进程。

注释 在某些平台（例如 Windows 上），Adaptive Server 还会将错误消息记录在操作系统事件日志中。请参见所用平台的安装指南和配置指南。

连接到 Adaptive Server

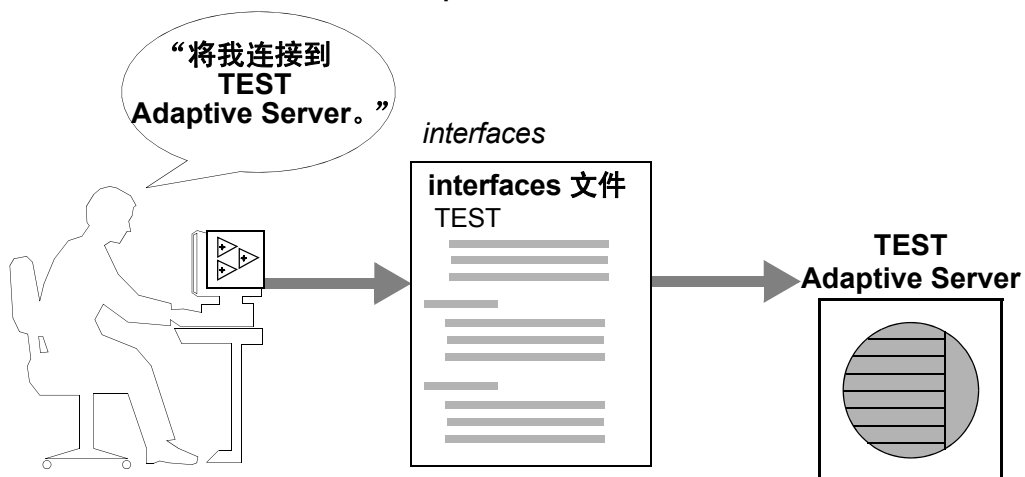
Adaptive Server 可以与网络上的其它 Adaptive Server、Open Server 应用程序和客户端软件进行通信。使用远程过程调用，客户端可以与一台或多台服务器进行对话，服务器也可以与其它服务器进行通信。为了使产品之间能够进行交互，每种产品都必须知道其它产品在网络中的位置。此网络服务信息存储在 *interfaces* 文件中。

interfaces 文件

根据操作系统的不同，*interfaces* 文件通常命名为 *interfaces*、*interface* 或 *sql.ini*。

interfaces 文件列出每个已知服务器的名称和地址。当您使用客户端程序连接到服务器时，该程序将在 *interfaces* 文件中查找服务器名，然后使用相应的地址连接到该服务器，如 [图 1-1](#) 所示。

图 1-1: 连接到 Adaptive Server



interfaces 文件的名称、位置和内容因操作系统而异。此外，*interfaces* 文件中的 Adaptive Server 地址的格式也会因网络协议而异。

Adaptive Server 安装程序将创建一个简单的 *interfaces* 文件，您可以使用该文件通过一个或多个网络协议实现与 Adaptive Server 的本地连接。系统管理员负责修改 *interfaces* 文件并将其分发给用户，使用户可以通过网络连接连接到 Adaptive Server。有关 *interfaces* 文件的信息，请参见所用平台的《配置指南》。

请参见 Performance and Tuning Series: Basics 《性能和调优系列：基础知识》中的第 2 章 “Networks and Performance”（网络 and 性能），了解有关 *interfaces* 文件和网络监听器的详细信息。

目录服务

目录服务管理网络服务信息的创建、修改和检索。目录服务由平台或第三方供应商提供，必须单独购买，且必须与 Adaptive Server 分开安装。注册表和分布式计算环境 (DCE) 就是目录服务的两个示例。

`$SYBASE/$SYBASE_OCS/config/libtcl.cfg` 文件是 Sybase 提供的配置文件，服务器和客户端使用该文件来确定：

- 要使用的目录服务。
- 指定目录服务的驱动程序的位置。

如果目录服务未安装或未在 *libtcl.cfg* 文件中列出，Adaptive Server 将缺省使用 *interfaces* 文件来获取网络服务信息。

系统管理员必须根据操作环境对 *libtcl.cfg* 文件进行相应的修改。

某些目录服务是针对于给定平台的，而其它目录服务则可以在多种不同的平台上使用。由于目录服务因平台而异的特点，因此请参见所用平台的配置文档来了解有关配置目录服务的详细信息。

LDAP 作为一个目录服务

轻量目录访问协议 (LDAP) 是访问目录服务的行业标准。目录服务允许组件通过区分名 (DN)，从存储并管理整个企业或网络所使用的服务器、用户和软件信息的 LDAP 服务器上查找信息。

LDAP 服务器所在的平台可能与运行 Adaptive Server 或客户端的平台不同。LDAP 用于定义通信协议以及客户端与服务器之间交换的消息内容。消息是各种操作码，例如客户端读、写和查询请求以及服务器响应等，其中包括元数据（与数据本身有关的数据）。

LDAP 服务器可以存储和检索与以下各项相关的信息：

- Adaptive Server，例如 IP 地址、端口号和网络协议
- 安全性机制和过滤器
- 高可用性协同服务器名
- 供用户访问 Adaptive Server 的鉴定信息

可以通过存储在 *syslogins* 目录中的信息或通过集中的 LDAP 服务器（能够在企业范围内实现单一登录名和口令），对登录到 Adaptive Server 的用户进行鉴定。请参见第 15 章“[管理 Adaptive Server 登录名、数据库用户和客户端连接](#)”。

可以配置 LDAP 服务器以使用以下访问限制：

- 匿名验证 — 所有数据对任何用户均可见。
- 用户名和口令鉴定 — Adaptive Server 使用相应文件中的缺省用户名和口令：
 - UNIX，32 位 — `$SYBASE/$SYBASE_OCS/config/libtcl.cfg`
 - UNIX，64 位 — `$SYBASE/$SYBASE_OCS/config/libtcl64.cfg`
 - Windows — `%SYBASE%\%SYBASE_OCS%\ini\libtcl.cfg`

用户名和口令鉴定属性可建立和结束与 LDAP 服务器的会话连接。

注释 存储在 *libtcl.cfg* 中并传递给 LDAP 服务器用于鉴定的缺省用户名和口令与用于访问 Adaptive Server 的用户名和口令不同。缺省用户名和口令允许访问 LDAP 服务器以执行管理任务。

如果在 *libtcl.cfg* 或 *libtcl64.cfg* 文件（统称为 *libtcl*.cfg* 文件）中指定了 LDAP 服务器，则只能从该 LDAP 服务器中访问服务器信息；Adaptive Server 将忽略 *interfaces* 文件。

如果服务器中支持多个目录服务，则搜索这些服务所采用的顺序是在 *libtcl*.cfg* 中指定的。您不能使用 *dataserver* 命令行选项来指定搜索顺序。

多个目录服务

任何类型的 LDAP 服务（无论是实际的服务器还是其它 LDAP 服务的网关）都称为 LDAP 服务器。

可以在 *libtcl*.cfg* 中为高可用性故障切换保护指定多个目录服务。并非列表中的每个目录服务都必须是 LDAP 服务器。

在以下示例中，如果与 *test:389* 的连接失败，则该连接将故障切换转到具有指定目录信息树 (DIT) 基址的 DCE 驱动程序。如果此操作也失败，则尝试连接 *huey:11389* 上的 LDAP 服务器。不同的供应商采用不同的 DIT 基址格式。

[DIRECTORY]

```
ldap=libdldap.so ldap://test:389/dc=sybase,dc=com
dce=libddce.so ditbase=../subsys/sybase/dataservers
ldap=libdldap.so ldap://huey:11389/dc=sybase,dc=com
```

请参见 Open Client Client-Library/C Programmer's Guide（《Open Client Client-Library/C 程序员指南》）和《Open Client Client-Library/C 参考手册》。

LDAP 目录服务与 Sybase interfaces 文件

LDAP 驱动程序实现目录服务以与 LDAP 服务器一起使用。LDAP 基础结构提供：

- 传统 Sybase interfaces 文件基于网络的替代形式
- 信息的单一层次视图，包括用户、软件、资源、网络、文件等

表 1-1 重点介绍了 Sybase interfaces 文件与 LDAP 服务器的差别。

表 1-1: interfaces 文件与 LDAP 目录服务

interfaces 文件	目录服务
因平台而异	与平台无关
每次 Sybase 安装各不相同	集中式和层次化
包含单独的主条目和查询条目	每个服务器对应有一个条目，客户端和服务器均可访问
无法存储有关服务器的元数据	可存储有关服务器的元数据

性能

使用 LDAP 服务器时的执行速度可能比使用 interfaces 文件时的执行速度慢，这是因为 LDAP 服务器需要花一些时间来建立网络连接和检索数据。由于这种连接在启动 Adaptive Server 时进行，因此无论如何也能在登录时间上体现出性能的差别。在常规系统负载期间，延迟并不明显。而当系统负载很大、且有很多连接时，尤其是在有持续时间很短的重复连接时，使用 LDAP 服务器与使用传统 interfaces 文件在整体性能上的差异就会非常明显。

Adaptive Server 中可用的安全性功能

表 1-2 总结了可用于 Adaptive Server 的主要安全性功能。有关配置 Adaptive Server 以获得安全性的信息，请参见本手册的第 2 部分。

表 1-2: 主要安全性功能

安全性功能	说明	位置
标识和认证控制	确保只有经过授权的用户才能登录到系统。除了基于口令的登录鉴定外， Adaptive Server 还支持使用 Kerberos、 LDAP 或可插入鉴定模块 (PAM) 的外部鉴定。	第 357 页的 “标识和鉴定”
自由选择访问控制 (DAC)	通常使用 grant 和 revoke 命令提供访问控制，使对象所有者能够限制对对象的访问。这种类型的控制取决于对象所有者的选择。	第 358 页的 “自由选择访问控制”

安全性功能	说明	位置
角色分离	允许管理员将特权角色授予指定用户，以便只有指定的用户才能执行某些任务。Adaptive Server 包含一些预定义角色（称为“系统角色”），例如系统管理员和系统安全员。此外，Adaptive Server 允许系统安全员定义其它角色（称为“用户定义角色”）。	第 359 页的“角色分离”
责任	提供了审计事件（例如登录、注销、服务器启动操作、远程过程调用、对数据库对象的访问，以及由特定用户或具有特定活动角色的用户执行的所有操作）的能力。Adaptive Server 还提供了单个选项，用于审计全服务器范围内与安全性相关的一组事件。	第 360 页的“责任审计”
数据保密性	对客户端 / 服务器通信使用加密来维护数据的保密性，利用 Kerberos 或安全套接字层 (SSL) 实现。不活动数据的保密性是通过口令保护的数据库备份保持的。	第 361 页的“数据保密性”

系统及可选数据库

本章描述所有 Adaptive Server 系统中的系统数据库。本章还描述 Sybase 提供的可选择安装的数据库，以及 Sybase 技术支持部门可能为诊断目的安装的 sybdiag 数据库。

主题	页码
系统数据库概述	21
master 数据库	23
model 数据库	25
sybssystemprocs 数据库	26
tempdb 数据库	26
sybsecurity 数据库	27
sybssystemdb 数据库	28
sybmgmtdb 数据库	28
pubs2 和 pubs3 样本数据库	28
dbccdb 数据库	29
sybdiag 数据库	29

系统数据库概述

Adaptive Server 的缺省安装包括以下系统数据库：

- master 数据库
- model 数据库
- 系统过程数据库 sybssystemprocs
- 两阶段提交事务数据库 sybssystemdb
- 临时数据库 tempdb

还可以选择安装：

- 审计数据库 `sybsecurity`
- 样本数据库 `pubs2` 和 `pubs3`
- `dbcc` 数据库 `dbccdb`
- Job Scheduler 数据库 `sybmgtmtdb`

有关安装 `master`、`model`、`sybssystemprocs`、`tempdb` 和 `sybmgtmtdb` 数据库的信息，请参见所用平台的安装指南。有关安装 `dbccdb` 的信息，请参见《系统管理指南：卷 2》中的第 10 章“检查数据库一致性”。有关使用 Job Scheduler 的信息，请参见《Job Scheduler 用户指南》。

`master`、`model`、`sybssystemdb` 和临时数据库位于在安装期间指定的主设备上。`master` 数据库完全包含在主设备上，不能将其扩展到任何其它设备上。在其它设备上创建所有其它数据库和用户对象。

警告！ 不要将用户数据库存储在主设备上；这样做将导致很难恢复存储在主设备上的系统数据库和任何用户数据库。

请将 `sybsecurity` 和 `sybmgtmtdb` 数据库安装在它们自己的设备和段上。请参见所用平台的安装文档。

将 `sybssystemprocs` 数据库安装在您选择的设备上。可能需要修改 `pubs2` 和 `pubs3` 的安装脚本，以共享用户为 `sybssystemprocs` 创建的设备。

使用 `installjsdb` 脚本（位于 `$SYBASE/ASE-15_0/scripts` 中）来安装 `sybmgtmtdb` 数据库。`installjsdb` 将查找名为 `sybmgtmtdb` 的设备，将在该设备上创建 `sybmgtmtdb` 数据库及其相应的表和存储过程。如果 `sybmgtmtdb` 数据库已存在，则 `installjsdb` 会在现有数据库中创建 Job Scheduler 表和存储过程。如果 `installjsdb` 找不到 `sybmgtmtdb` 设备或 `sybmgtmtdb` 数据库，则会在主设备上创建 `sybmgtmtdb`。但是，Sybase 强烈建议您从主设备中删除 `sybmgtmtdb` 数据库。

`installpubs2` 和 `installpubs3` 脚本并没有在其 `create database` 语句中指定设备，因此将在缺省设备上创建这些脚本。在安装过程中，主设备为缺省设备。若要更改这一点，请编辑脚本，或按第 7 章“初始化数据库设备”中的说明进行操作。

master 数据库

master 数据库控制 Adaptive Server 的操作，并存储有关所有用户数据库及其相关数据库设备的信息。表 2-1 描述了 master 数据库存储的信息。

表 2-1: master 数据库存储的信息

信息	系统表
用户帐户	syslogins
远程用户帐户	sysremotelogins
此服务器可以交互的远程服务器	syssservers
正在执行的进程	sysprocesses
可配置的环境变量	sysconfigures
系统错误消息	sysmessages
Adaptive Server 上的数据库	sysdatabases
分配到每个数据库的存储空间	sysusages
装入系统的磁带和磁盘	sysdevices
活动的锁	syslocks
字符集	syscharsets
语言	syslanguages
拥有全服务器范围内各种角色的用户	sysloginroles
服务器角色	sysssrvroles
联机的 Adaptive Server 引擎	sysengines

因为 master 数据库存储有关用户数据库和设备的信息，所以您必须位于 master 数据库中，才能执行 create database、alter database、disk init、disk refit、disk reinit 及磁盘镜像命令。

master 数据库的最小大小取决于所用服务器的逻辑页的大小。由于 master 数据库必须至少包含 6656 个逻辑页，因此该数据库相对于各逻辑页大小的实际最小容量为：

- 2K 页 — 13MB
- 4K 页 — 26MB
- 8K 页 — 52MB
- 16K 页 — 104MB

控制 master 数据库中的对象创建

安装 Adaptive Server 时，只有系统管理员可以在 master 数据库中创建对象，因为系统管理员已隐式成为其所用任何数据库的 “dbo”。在 master 数据库上创建的任何对象应只用于系统管理。在 master 中设置权限，以使大多数用户无法在该处创建对象。

警告！ 不要将用户对象放在 master 中。在 master 数据库中存储用户对象会导致事务日志很快填满。如果事务日志空间已用完，则无法使用 `dump transaction` 命令来释放 master 中的空间。

您可能还需要使用 `sp_modifylogin` 更改用户的缺省数据库（用户在登录时所连接的数据库）。请参见第 381 页的“向数据库添加用户”。

在 `sybsystemprocs` 数据库（而不是 master）中创建任何系统过程。

备份 master 数据库并保留系统表的副本

为了防止 Adaptive Server 出现硬件或软件故障，请执行以下操作：

- 经常备份 master 数据库和所有用户数据库。请参见第 36 页的“保留 master 的最新备份”以及《系统管理指南：卷 2》中的第 13 章“恢复系统数据库”。
- 保留以下系统表的副本（最好为脱机副本）：`sysusages`、`sysdatabases`、`sysdevices`、`sysloginroles` 和 `syslogins`。请参见第 37 页的“保留系统表的脱机副本”。如果有这些脚本的副本，并且硬盘故障或其它灾难导致数据库无法使用，您可以使用《系统管理指南：卷 2》的第 13 章“恢复系统数据库”中所述的恢复过程。如果没有这些脚本的最新副本，则在 master 数据库损坏时恢复 Adaptive Server 就难很多。

model 数据库

Adaptive Server 包括 model 数据库，此数据库为新用户数据库提供了模板或原型。用户每次输入 `create database` 命令时，Adaptive Server 就会制作 model 数据库的副本并将这个新数据库扩展到 `create database` 命令所指定的大小。

注释 新数据库至少必须与 model 数据库一样大。

model 数据库包含每个用户数据库所需的系统表。可以修改 model 来自定义新创建的数据库的结构，而对 model 执行的所有操作都将反映在每个新数据库中。系统管理员通常会对 model 进行以下一些更改：

- 添加用户定义的数据类型、规则或缺省值。
- 添加需要访问 Adaptive Server 上所有数据库的用户。
- 授予缺省特权，特别是 “guest” 帐户的缺省特权。
- 设置数据库选项，例如 `select into/bulkcopy/pllsort`。这些设置将反映在所有新数据库中。model 中这些选项的缺省设置为 `off`。请参见第 8 章 “设置数据库选项”。

通常，大多数用户没有修改 model 数据库的权限。也没有必要授予读取权限，因为 Adaptive Server 会将它的全部内容复制到每个新用户数据库中。

model 数据库的大小不能超过 `tempdb`。缺省情况下，model 的大小为 6 个分配单元（一个分配单元为 256 个逻辑页）。如果增加 model 数据库的大小而没有将 `tempdb` 数据库至少增加到相同大小，您将看到错误消息。

注释 请保留 model 数据库的备份副本，并在每次更改 model 时使用 `dump database` 对其进行备份。在发生介质故障的情况下，要像恢复用户数据库一样恢复 model 数据库。

sybssystemprocs 数据库

Sybase 系统过程存储在 sybssystemprocs 数据库中。当任意数据库中的用户执行系统存储过程（即名称以 `sp_` 开头的过程）时，Adaptive Server 将首先在用户的当前数据库中查找该过程。如果没有与该名称相符的过程，Adaptive Server 将在 sybssystemprocs 数据库中进行查找。如果 sybssystemprocs 中没有过程，Adaptive Server 将在 master 中查找该过程。

如果过程修改了系统表（例如，`sp_adduser` 修改了 `sysusers` 表），则会在执行该过程的数据库中进行更改。

若要更改对系统过程的缺省权限，请在 sybssystemprocs 数据库中修改这些权限。

注释 任何时候对 sybssystemprocs 进行更改时，都要备份该数据库。

tempdb 数据库

Adaptive Server 具有一个**临时数据库 tempdb**，该数据库可为临时表及其它临时工作存储提供所需的存储区域。服务器上所有数据库的所有用户都共享 tempdb 的空间。

tempdb 的缺省大小取决于所用服务器的逻辑页大小（2K、4K、8K 或 16K）。某些活动可能要求增大 tempdb 的大小：

- 大型临时表。
- 临时表上有许多活动，这些活动将填满 tempdb 日志。
- 大量的排序或许多同时进行的排序。包含 `group by` 的子查询和集合也会导致某种 tempdb 活动。

使用 `alter database` 来增大 tempdb 的大小。tempdb 数据库最初创建于主设备上。可以从主设备或任何其它数据库设备中向 tempdb 添加空间。

如果对大型表运行 `update index statistics`，则在 tempdb 不够大的情况下，该命令将失败，并出现错误号 1105。

除了系统临时数据库 tempdb 外，您还可以创建和管理多个临时数据库。多个临时数据库可减少对系统目录和 tempdb 中日志的争用。

创建临时表

在创建临时表或执行可能需要临时数据库中的存储空间的命令时，并不需要特殊权限。

创建临时表有两种途径，既可以通过在 `create table` 语句中的表名前使用井号 (#)，也可以指定名称前缀 “`tempdb..`”。

只有当前 Adaptive Server 会话可以访问用井号 (#) 创建的临时表：其它会话中的用户不能访问它们。在每个会话结束时，将销毁这些非共享的临时表。表名的前 13 个字节，包括 (#) 号，必须是唯一的。Adaptive Server 会给这些表名指派一个 17 字节的数字后缀。（通过查询 `tempdb..sysobjects` 可以看到该后缀。）

使用 “`tempdb..`” 前缀创建的临时表存储在 `tempdb` 数据库中而且可以由 Adaptive Server 的会话共享。Adaptive Server 不改变以此方式创建的临时表名。这种表将一直存在，除非重新启动 Adaptive Server 或者表所有者使用 `drop table` 将其删除。

只有在 `tempdb` 中使用系统过程时，它们才在临时表上运行。

如果存储过程创建了临时表，则在该过程退出时将删除这些表。也可以在会话结束前显式删除临时表。

警告！ 除非打算在其他用户和会话之间共享这些表，否则请不要使用 “`tempdb..`” 前缀从存储过程内部创建临时表。

每次重新启动 Adaptive Server 时，都会将 `model` 复制到 `tempdb`，这样做可清除该数据库。您无法恢复临时表。

sybsecurity 数据库

sybsecurity 数据库（包含 Adaptive Server 的审计系统）包括：

- 系统表 `sysaudits_01`、`sysaudits_02` ... `sysaudits_08`，这些表包含审计追踪
- `sysauditoptions` 表包含描述全局审计选项的行
- 派生自 `model` 的所有其它缺省系统表

请参见第 18 章 “审计”。

sybsystemdb 数据库

sybsystemdb 数据库存储有关分布式事务的信息。Adaptive Server 版本 12.0 和更高版本可以为使用远程过程调用 (RPC) 或组件集成系统 (CIS) 传播到远程服务器的事务提供事务协调服务。参与分布式事务的远程服务器的有关信息存储在 `syscoordinations` 表中。

注释 Adaptive Server 12.0 版及更高版本中的分布式事务管理 (DTM) 服务是需要单独进行许可的功能。必须先购买并安装分布式事务管理许可证，然后才能使用 DTM 服务。请参见《使用 Adaptive Server 分布式事务管理功能》和安装指南。

sybsystemdb 数据库还存储使用 Sybase 两阶段提交协议的 SYB2PC 事务的有关信息。用于存储有关每个两阶段提交事务的信息并跟踪其完成状态的 `spt_committab` 表存储在 sybsystemdb 数据库中。

有关两阶段提交事务以及如何创建 sybsystemdb 数据库的信息，请参见所用平台的《配置指南》。

sybmgmtadb 数据库

sybmgmtadb 数据库存储内部 Job Scheduler 任务进行处理所需的作业、日程表、预定作业信息和数据。sybmgmtadb 还保留这些已执行任务的输出和结果。请参见《Job Scheduler 用户指南》。

pubs2 和 pubs3 样本数据库

pubs2 和 pubs3 样本数据库的安装是可选的。这些数据库是用户学习 Adaptive Server 的工具。Adaptive Server 文档的大部分示例都使用 pubs2 样本数据库，已特别注明的示例使用 pubs3 数据库。有关安装 pubs2 和 pubs3 的信息，请参见所用平台的安装指南。有关这些样本数据库的内容的信息，请参见《Transact-SQL 用户指南》。

维护样本数据库

样本数据库包括一个“guest”用户登录名，该登录名允许任何已授权的 Adaptive Server 用户访问该数据库。“guest”登录名对 pubs2 和 pubs3 拥有广泛的特权，包括选择、插入、更新和删除用户表的权限。请参见第 15 章“管理 Adaptive Server 登录名、数据库用户和客户端连接”。

pubs2 和 pubs3 数据库的大小由服务器的逻辑页大小（2K、4K、8K 或 16K）确定。如果可能，请为每个新用户提供一个 pubs2 和 pubs3 的原始副本，这样该用户就不会混淆其他用户所做的更改。若要将 pubs2 或 pubs3 置于特定的数据库设备上，请在安装数据库之前编辑安装脚本。

如果空间不足，可指导用户在更新样本数据库之前执行 `begin transaction` 命令。用户完成对某个样本数据库的更新后，可以发出 `rollback transaction` 命令来撤消更改。

pubs2 image 数据

Adaptive Server 提供用于在 pubs2 数据库中安装 image 数据的脚本（pubs3 不使用 image 数据）。image 数据由六幅图像组成，PICT、TIF 和 Sun 光栅文件格式各占两个。Sybase 没有提供显示 image 数据的工具。从数据库抽取此类数据后，必须使用相应的屏幕图形工具来显示图像。

有关在 pubs2 中安装 image 数据的信息，请参见所用平台的安装文档。

dbccdb 数据库

dbcc checkstorage 记录目标数据库的配置信息、操作活动以及 dbccdb 数据库中操作的结果。在此数据库中存储的是 dbcc 存储过程，用于创建和维护 dbccdb，并生成有关 dbcc checkstorage 操作结果的报告。请参见《系统管理指南：卷 2》中的第 10 章“检查数据库一致性”。

sybdiag 数据库

Sybase 技术支持部门可能会为调试目的而在系统中创建 sybdiag 数据库。此数据库保存诊断配置数据，而且客户不应使用该数据库。

确定安装脚本的版本

通过 `sp_version` 可以确定在 Adaptive Server 上安装的脚本（*installmaster*、*installdbccdb* 等）的当前版本、脚本运行是否成功，以及脚本完成所花费的时间。

`sp_version` 的语法为：

```
sp_version [script_file [, "all"]]
```

其中：

- *script_file* 是安装脚本的名称（缺省值为 NULL）。
- **all** 报告有关每个脚本的详细信息，例如执行日期以及执行所花费的时间。

如果不带任何参数运行 `sp_version`，它将报告有关所有脚本的信息。

以下示例介绍了所运行的安装脚本、这些脚本的运行时间以及完成运行的时间：

```
sp_version null, 'all'
Script          Version
Status
-----
installmaster   15.0/EBF XXXXX/B/Sun_svr4/OS 5.8/asemain/1/32-bit/OPT/Thu Sep
23 22:12:12 2004
Complete [Started=Sep 24 2004  3:39PM]-[Completed=Sep 24 2004  3:45PM]
```

系统管理入门

本章内容如下：

- 向没有经验的系统管理员介绍一些重要主题
- 帮助系统管理员在 Sybase 文档中查找信息

有经验的管理员也可能会发现本章对组织日常维护活动很有帮助。

主题	页码
逻辑页大小	31
使用“测试”服务器	32
安装 Sybase 产品时的注意事项	33
分配物理资源	34
备份和恢复	36
即时维护和故障排除	39
保留记录	39
其它资源	41

逻辑页大小

数据库对象是使用逻辑页构建的。数据库及其任何相关对象必须使用相同的逻辑页大小。也就是说，您创建的服务器所使用的逻辑页大小不能大于一个逻辑页。Adaptive Server 允许创建逻辑页大小为 2K、4K、8K 或 16K 的主设备和数据库，但一个给定服务器安装只能使用以上四个逻辑页大小之一。服务器中的所有数据库（以及每个数据库中的所有对象）都使用相同的逻辑页大小。例如，在一台逻辑页大小为 4K 的服务器上，所有页大小均必须为 4K，即使某些页只会用到最初的 2K。

创建主设备时，可使用 `dataserver -z` 来选择页大小。

有关 `dataserver` 命令（该命令用于创建主设备）的详细信息，请参见《实用程序指南》。有关逻辑页大小的详细信息，请参见《系统管理指南：卷 2》中的第 3 章“配置内存”。

使用“测试”服务器

Sybase 建议您先安装并使用一台测试或开发 Adaptive Server，然后在创建生产服务器之前将其删除。使用测试服务器可更轻松地区计划和测试不同的配置，并且从错误中恢复时也较为容易。在没有必须重新启动生产服务器或重新创建生产数据库的风险时，学习如何安装和管理新功能就变得较为容易。

如果使用测试服务器，Sybase 建议您从安装或升级 Adaptive Server 开始，直到完成服务器配置过程为止。正是在这些步骤中，您需要做出一些有关最终生产系统的重要决定。以下各节介绍使用测试服务器如何能够为系统管理员提供帮助。

计划资源

使用测试服务器有助于计划系统的最终资源要求，并有助于发现可能未预料到的资源不足情况。

特别是，磁盘资源可能会对生产系统的最终设计产生深刻的影响。例如，您可能会决定在出现介质故障时，需要对特定数据库进行不间断恢复。这意味着，您必须配置一台或多台其它的数据库设备对关键数据库进行镜像。了解测试服务器的资源要求，使您可以更改数据库和表的物理布局，而不影响数据库用户。

使用测试服务器，可采用不同的硬件配置对 Adaptive Server 和应用程序进行基准测试。这允许您在将整个系统联机（以供常规使用）之前，在 Adaptive Server 级别和操作系统级别确定物理资源的最佳设置。

达到性能目标

大多数性能目标只有通过仔细规划数据库的设计和配置才能达到。例如，您可能会发现特定表的插入和 I/O 性能导致了瓶颈。这种情况下，最好的办法是在一个专门的段上重新创建该表并将该表分区。这种性质的改变会中断生产系统；即使是更改某个配置参数，也可能需要重新启动 Adaptive Server。

安装 Sybase 产品时的注意事项

有时需由系统管理员来负责安装 Adaptive Server 和其它 Sybase 产品。如果需要由您负责安装，请使用以下指导来帮助您完成该过程。

检查产品的兼容性

安装新产品或对已有产品进行升级之前，需要阅读产品所包含的发行公告，以了解可能影响系统性能的所有兼容性问题。兼容性问题发生在硬件和软件之间或同一软件的不同版本之间。事先阅读发行公告，可以免掉对已知兼容性问题进行故障排除而进行的猜测工作并节省时间。请特别注意发行公告中包括的已知问题列表。

安装或升级 Adaptive Server

在进行新的安装或升级之前，请通读所用平台的安装指南。可能还需要向操作系统管理员咨询，讨论 Adaptive Server 对操作系统的要求。这些要求可能包括对内存、裸设备、异步 I/O 以及其它功能的配置，具体情况取决于您所使用的平台。其中的多数任务必须在开始安装之前完成。

如果要升级服务器，请在开始之前脱机备份所有数据（包括 master 数据库、用户数据库、触发器和系统过程）。升级完成后，特别是在旧的转储文件和新版本不兼容的情况下，立即为数据创建一个单独的完全备份。

安装其它第三方软件

Adaptive Server 通常支持硬件平台常用的网络协议。如果网络支持其它协议，请安装所需的协议支持。

除了使用 Sybase *interfaces* 文件之外，还可以使用目录服务获取服务器的地址和其它网络信息。目录服务由平台或第三方供应商提供，必须单独购买，且必须与 Adaptive Server 分开安装。有关 Adaptive Server 当前支持的目录服务的列表，另请参见第 15 页的“目录服务”和所用平台的《配置指南》。

配置并测试客户端连接

成功的客户端连接依赖于 Adaptive Server、客户端软件和网络产品之间的协调。如果使用的是随 Adaptive Server 一起安装的网络协议，有关测试网络连接的信息，请参见所用平台的《配置指南》。如果使用不同的网络协议，按该网络产品所包括的说明进行操作。还可以使用 Sybase 连接性产品附带的“ping”实用程序来测试客户端与 Adaptive Server 的连接。有关客户端如何连接至 Adaptive Server 的一般说明，请参见第 14 页的“[连接到 Adaptive Server](#)”。有关 *interfaces* 文件的名称和内容的详细信息，请参见所用平台的《配置指南》。

分配物理资源

物理资源分配是指为 Adaptive Server 提供达到性能和恢复目标所需的内存、磁盘空间、工作进程及 CPU 处理能力。安装新服务器时，每位系统管理员都必须做出有关资源利用方面的决定。如果升级所用平台，或者数据库系统的设计发生变化，您也必须通过添加新的内存、磁盘控制器或 CPU 来重新分配 Adaptive Server 资源。及早对 Adaptive Server 和应用程序进行基准测试可帮助您确定造成性能瓶颈的硬件资源缺乏情况。

请参见《系统管理指南：卷 2》中的第 16 章“磁盘资源概述”，了解 Adaptive Server 所需的各种磁盘资源。另请参见《系统管理指南：卷 2》中的第 3 章“配置内存”和《系统管理指南：卷 2》中的第 5 章“管理多处理器服务器”，了解有关内存和 CPU 资源的信息。

以下各节提供确定物理资源要求的帮助性指导。

专用服务器与共享服务器

规划 Adaptive Server 资源的第一步是了解运行在同一计算机上的其它应用程序所需的资源。通常，系统管理员会将整台计算机专供 Adaptive Server 使用，这意味着只有操作系统和网络软件才会消耗可能为 Adaptive Server 保留的资源。在共享系统中，其它应用程序（例如 Adaptive Server 客户端程序或打印服务器）与 Adaptive Server 在同一台计算机上运行。在共享系统中，计算可供 Adaptive Server 使用的资源可能很困难，因为应用程序类型及其使用方式会随时间而改变。

为 Adaptive Server 配置资源时，系统管理员应考虑操作系统、客户端程序以及基于窗口的系统等所使用的资源。将 Adaptive Server 配置为只使用可供它使用的资源。否则，服务器的性能会大大降低或者无法启动。

决策支持和 OLTP 应用程序

Adaptive Server 包含许多功能，这些功能都可针对 OLTP、决策支持和混合工作负载环境优化性能。但是，若要以最佳方式使用这些功能，请事先确定系统应用程序的要求。

对于混合工作负载系统，列出预计各种应用程序频繁使用的各个表；这有助于使应用程序获得最优性能。

预先的资源计划

预先了解和计划资源的使用极其重要。以磁盘资源为例，在初始化某设备并将其分配给 Adaptive Server 后，即使 Adaptive Server 从未向该设备填入数据，也不能将其挪作它用。同样，Adaptive Server 会自动保留为其配置的内存，任何其它应用程序都不能使用这部分内存。

在规划资源使用时：

- 为了便于恢复，请始终将数据库的事务日志放在与存放数据的设备不同的物理设备上。请参见《系统管理指南：卷 2》中的第 6 章“创建和管理用户数据库”。
- 考虑对存储关键数据的设备进行镜像处理。请参见《系统管理指南：卷 2》。如果操作系统支持这些功能，请考虑为 Adaptive Server 数据使用磁盘阵列和磁盘镜像。
- 如果使用的是测试 Adaptive Server，为方便起见，您可能会发现，将数据库设备初始化为操作系统文件而不是裸设备会更容易。Adaptive Server 支持其设备使用裸分区或经认证的文件系统。
- 更改配置选项可能会影响 Adaptive Server 消耗物理资源（特别是内存）的方式。有关各个参数使用的内存量的详细信息，请参见第 5 章“设置配置参数”。

操作系统配置

确定了可供 Adaptive Server 使用的资源和您所需的资源后，请在操作系统级别配置这些物理资源：

- 如果使用的是裸分区，请将裸设备初始化为 Adaptive Server 需要的大小。如果为 Adaptive Server 初始化裸设备，则无法将该设备用于任何其它用途（例如，存储操作系统文件）。请操作系统管理员协助初始化裸设备，并配置成所需的大小。

- 配置网络连接数。确保运行 Adaptive Server 的计算机确实能支持所配置的连接数。请参见操作系统文档。
- 操作系统和所使用的应用程序可能需要其它配置。请阅读所用平台的安装指南。另请阅读客户端软件文档或咨询工程师，以了解应用程序的操作系统要求。

备份和恢复

定期对数据库进行备份对维护数据库系统的完整性是至关重要的。尽管 Adaptive Server 能自动从系统崩溃（例如，电源断电）或服务器故障中恢复，但只有您才能从介质故障导致的数据丢失中恢复。

《系统管理指南：卷 2》中的以下各章介绍如何制订和实施备份和恢复计划：

- 第 11 章 “开发备份和恢复计划”
- 第 12 章 “备份和恢复用户数据库”
- 第 13 章 “恢复系统数据库”
- 第 16 章 “使用阈值管理可用空间”

保留 master 的最新备份

备份 master 数据库是任何备份和恢复计划的最重要因素。master 数据库包含有关整个数据库系统结构的详细信息。它存储有关 Adaptive Server 数据库、设备及组成这些数据库的设备段的信息。由于 Adaptive Server 需要为恢复使用该信息，因此始终要保留一份 master 数据库的最新备份副本，这一点至关重要。

为确保 master 备份始终为最新，请在执行了影响磁盘、存储、数据库或段的每个命令或过程后备份数据库，这些命令或过程包括：

- 创建或删除数据库
- 初始化新数据库设备
- 增加新转储设备
- 使用任何设备镜像命令
- 创建或删除系统的存储过程（如果它们存储在 master 中）

- 创建、删除或修改段
- 添加新的 Adaptive Server 登录名

若要将 master 备份到磁带设备，请启动 isql 并输入以下命令：

```
dump database master to "tape_device"
```

其中，*tape_device* 是磁带设备的名称（例如，*/dev/rmt0*）。

保留系统表的脱机副本

除了定期备份 master 外，还要保留以下系统表的脱机副本：

sysdatabases、**sysdevices**、**sysusages**、**sysloginroles** 和 **syslogins**。使用《实用程序指南》中描述的 **bcp** 实用程序，并存储每个系统表的内容的打印副本。通过打印以下命令的输出来创建打印副本：

```
select * from sysusages order by vstart
select * from sysdatabases
select * from sysdevices
select * from sysloginroles
select * from syslogins
```

如果有这些表的副本，并且硬盘故障或其它灾难导致数据库无法使用，您可以使用《系统管理指南：卷 2》的第 13 章“恢复系统数据库”中所述的恢复过程。

还要保留用户对象的所有数据定义语言 (DDL) 脚本的副本，如第 39 页的“保留记录”中所述。

自动备份过程

通过创建自动备份过程，将能更方便、更快速地执行流程。自动备份非常简单，如同使用操作系统脚本或实用程序（例如，UNIX **cron** 实用程序）执行必要的备份命令一样。或者，可以通过使用阈值来进一步提高该过程的自动化程度，《系统管理指南：卷 2》中的第 16 章“使用阈值管理可用空间”中讨论了阈值。

❖ 创建自动备份过程

尽管创建自动备份脚本所需的命令因所使用的操作系统而异，但所有的脚本都应该完成相同的基本步骤：

- 1 启动 **isql** 并将事务日志转储到存放区域（例如，某个临时文件）。
- 2 将转储文件重命名为包含转储日期、时间和数据库名的名称。

- 3 在历史文件中，记录有关新备份的信息。
- 4 将在转储过程中出现的任何错误记录到单独的文件中。
- 5 对任何错误情况，自动向系统管理员发送邮件。

备份数据库前检验数据一致性

数据库备份必须一致而准确，对于 **master** 尤其如此。如果备份包含内部错误的数据库，则在数据库的恢复版本中，错误仍然存在。

使用 **dbcc** 命令，在备份数据库之前检查数据库中是否存在错误。在转储数据库之前，请始终使用 **dbcc** 命令来检验其完整性。如果 **dbcc** 检测到错误，请在转储数据库之前纠正这些错误。

经过一段时间后，如果在运行 **dbcc** 时发现错误很少或没有错误，则可以确定数据库损坏的风险很小，只需偶尔运行 **dbcc** 即可。如果丢失数据的后果极其严重，请在每次备份数据库时都继续运行 **dbcc** 命令。

注释 出于性能方面的考虑，许多节点选择在非高峰时间段或单独的服务器上运行 **dbcc** 检查。

请参见《系统管理指南：卷 2》中的第 10 章“检查数据库一致性”。

监控日志大小

当事务日志将满时，可能无法使用标准过程来转储事务并回收空间。系统管理员应监控日志大小，并定期执行事务日志转储（除定期执行数据库转储之外），以确保避免这种情况。设置一个阈值存储过程，当日志大小达到某一容量时，该过程将会通知您（或转储日志）。请参见《系统管理指南：卷 2》中的第 16 章“使用阈值管理可用空间”。Sybase 还建议：为了缩短转储和装载数据库所需的时间，请在执行完整数据库转储之前立即转储事务日志。

也可以使用 **sp_helpsegment** 手动监控日志段中使用的空间，如《系统管理指南：卷 2》的第 8 章“创建和使用段”中所述。

即时维护和故障排除

除了定期安排备份之外，系统管理员还会在本节中论述的服务器正常运行期间执行维护活动。

启动和停止 Adaptive Server

大多数系统管理员会将启动 Adaptive Server 的过程自动化，以便与服务器的启动保持一致。可通过编辑操作系统的启动脚本或使用其它操作系统过程来完成此操作。请参见所用平台的配置文档以确定如何启动和停止 Adaptive Server。

查看和清理错误日志

定期检查错误日志的内容，以便确定是否发生了严重错误。还可以使用操作系统脚本扫描错误日志，以查看是否有特定消息，并在特定错误发生时自动通知系统管理员。定期检查错误日志可帮助确定是否连续出现了同一性质的错误，或者某个特定的数据库设备是否有可能出现故障。有关错误消息及其严重性的详细信息，请参见第 11 章“[诊断系统问题](#)”。

错误日志文件会随着时间的推移而越来越大，因为 Adaptive Server 每次启动时都会向其中附加信息性消息和状态消息。可通过打开日志文件并删除旧记录来定期“清理”日志文件。将日志文件的大小保持在一个便于管理的水平可节省磁盘空间，并能更容易地定位当前错误。

保留记录

作为系统管理员，保留有关 Adaptive Server 系统的记录是您工作的一个重要部分。当您与 Sybase 技术支持部门联系或者恢复数据库时，对所遇到的问题和变动进行的准确记录是颇有价值的参考。在您不在时，这些记录还可以为负责管理 Adaptive Server 系统的管理员提供重要信息。

联系信息

在您的系统中，为您自己以及系统安全员、操作员和数据库所有者保留一份联系信息列表。另外，为每个角色记录辅助联系方式。将此信息提供给所有 Adaptive Server 用户，以便相应的联系人能够收到有关增强功能的请求和问题报告。

配置信息

理想情况下，请创建数据库和数据库对象，然后使用存储在安全位置的脚本文件配置 Adaptive Server。通过存储脚本文件，可以在发生灾难时重新创建整个系统。您还可以使用脚本文件在新的硬件平台上快速重新创建数据库系统，以做评估之用。如果使用第三方工具来执行系统管理，请记住在执行管理任务之后生成等效的脚本。

考虑记录以下信息种类：

- 用于创建数据库和数据库对象（DDL 脚本）的命令
- 用于添加新的 Adaptive Server 登录名和数据库用户的命令
- 当前 Adaptive Server 配置文件，如第 60 页的“[使用 sp_configure 及 配置文件](#)”中所述
- 所有文件和被初始化为数据库设备的裸设备的名称、位置及大小

保留一个带有日期的日志，在其中记录对 Adaptive Server 配置所做的所有更改。用简要说明标记每一改变，描述所做改变发生的时间和原因，以及最终结果的摘要信息。

维护日程表

保留一份记录安排好的定期维护活动的日历；列出在您的节点执行的任何过程。

- 使用 dbcc 来检查数据库的一致性
- 备份用户和系统数据库
- 监控事务日志中的剩余空间（如果该过程不能自动执行的话）
- 转储事务日志
- 检查 Adaptive Server、Backup Server 和 Adaptive Server Monitor 的错误日志内容

- 运行 `update statistics` 命令（请参见 Performance and Tuning Series: Improving Performance with Statistical Analysis（《性能和调优系统：利用统计分析改进性能》）中的第1章“Using the set statistics Commands”（使用 `set statistics` 命令））
- 检查审计信息（如果已安装审计选项）
- 重新编译存储过程
- 监控服务器主机的资源使用情况

系统信息

记录有关运行 Adaptive Server 的硬件和操作系统的信息，其中包括：

- 操作系统配置文件或启动文件的副本
- 网络配置文件（例如，`hosts` 和 `services` 文件）的副本
- Adaptive Server 库文件和数据库设备的名称及权限
- 用于备份的磁带设备的名称和位置
- 用于进行自动备份、启动 Adaptive Server 或执行其它管理活动的操作系统脚本或程序的副本

灾难性事故恢复计划

将基本备份和恢复过程、第36页的“备份和恢复”中的准则和您在进行数据恢复时获得的个人经验综合起来，形成一个针对您的系统定制的简明恢复步骤列表。对于您自己和需要在紧急情况下恢复生产系统的其他系统管理员，这种做法可能非常有用。

其它资源

系统管理员要了解的信息量似乎非常大。可以使用几个软件工具，帮助您学习和利用基本的管理任务。这些工具包括 Adaptive Server Monitor，用于监控服务器性能和其它活动；以及 Sybase Central，它简化了许多管理任务。另外，还有很多为帮助系统管理员管理日常维护活动而设计的第三方软件包。

用于 Sybase Central 的 Adaptive Server 插件简介

本章介绍了如何使用 Sybase Central 来管理 Adaptive Server，并概要介绍了 Sybase Central。有关 Adaptive Server 插件功能的完整说明，请参见 Sybase Central 联机帮助。

主题	页码
Adaptive Server Sybase Central 插件概述	43
使用 Adaptive Server 插件	45
启动和停止 Sybase Central	46
注册 Adaptive Server 插件	46
执行常见任务	47
使用 Interactive SQL	53

Adaptive Server Sybase Central 插件概述

Sybase Central 是一种图形用户界面 (GUI) 管理工具。Sybase Central 支持可用于管理特定 Sybase 产品的各种“插件”。使用 Adaptive Server 插件可以管理 Adaptive Server，并帮助您执行复杂的管理任务，而无需记住 Transact-SQL 命令或系统存储过程的语法。可以使用 Adaptive Server 插件执行以下操作：

- 从一个主控台管理多台服务器 — 可以从 Sybase Central 主窗口中管理所有 Adaptive Server 安装。
- 生成数据库定义语言 (DDL) — 可以为 Adaptive Server 中的对象生成 DDL。
- 直观地表示对象 — 可以查看每个 Adaptive Server 中的数据库和登录名以及每个数据库中的对象，并可以展开和折叠窗口以显示有关数据库和登录名的信息。Adaptive Server 插件可扩展以显示许多项的相关信息，其中包括：
 - 数据库和表
 - 磁盘设备

- 活动进程和锁
- 登录名和用户
- 数据高速缓存
- ASE Replicator、Job Scheduler 和消息传送服务
- 访问其它实用程序，例如 Interactive SQL（用于发送查询和显示查询结果）。
- 在相关对象之间导航 — 若要获得有关数据库对象（与要显示其属性表的对象相关）的详细信息，可通过所显示对象的对话框直接导航到相关对象。
- 创建集群 — 如果购买了 Adaptive Server Cluster Edition，您可以利用 Adaptive Server 插件来创建集群。请参见联机帮助和《集群用户指南》。

Adaptive Server 插件和命令行更新

用于 Sybase Central 的 Adaptive Server 插件可管理各种 Adaptive Server Enterprise 产品。在 15.0.3 之前的版本中，Adaptive Server 插件基于 Sybase Central 4.3 运行。在 15.0.3 中，Adaptive Server 插件基于 Sybase Central 6.00 运行。15.0.3 版、Sybase Central 6.00 新增了以下功能：

- 搜索工具可帮助您查找插件显示的对象。选择“视图”(View) | “搜索窗格”(Search Pane) 以依据对象所属的插件来选择对象。
- “连接配置文件说明”(Connection Profile Description)、“导入”(Import) 和 “导出”(Export) 选项允许您向配置文件连接中添加文本说明。您也可以将连接配置文件导入文件和从文件中导出连接配置文件，从而能够在用户之间共享这些配置文件。
- 更好地支持 Windows Vista。

15.0.3 版 Adaptive Server 插件新增了以下功能。

- 通过从上下文相关工具栏（位于 Sybase Central 上下文栏下方，后者又位于标准工具栏中）选择“添加”图标来创建对象。
- 存储过程和 SQLJ 过程位于 Procedures 文件夹中。
- 现在支持标量函数或用户定义函数，并且这些函数与 SQLJ 函数一起位于 Functions 文件夹中。Adaptive Server 插件帮助中也介绍了这些函数。
- 现在可从上下文相关工具栏或标准工具栏下方的上下文栏上的菜单中访问实用程序项。

之前作为 Adaptive Server 插件的一部分提供的 DBISQL11 现在为独立产品（版本为 11.0），并包括以下增强功能：

- 多个结果集的数量不再限制为 10。
- Adaptive Server 的登录对话框现在保留并显示最后五个连接的服务器名称。
- DBISQL11（或 Interactive SQL）现在支持类似于连接配置文件的连接收藏夹。
- SQL 语句窗格现在包含行号。
- “结果”窗格现在显示使用 `select all`、`insert/update/delete` SQL 语句的情况，以及选定行中的排序和生成情况。

使用 Adaptive Server 插件

用于 Sybase Central 的 Adaptive Server 插件可提供一种管理 Adaptive Server Enterprise 的直观而简便的方法。Sybase Central 在其左窗格中显示 Adaptive Server 插件。此窗格中包括一个文件夹分层列表，表示插件可管理的不同对象，其中包括：

- 查看和更改对象的特性
- 创建其它对象
- 生成用于创建对象的 SQL 文本（使用该文本可对 Adaptive Server 对象进行反向工程）
- 删除对象
- 配置 Adaptive Server
- 管理：
 - 数据库设备
 - 代理数据库和临时数据库
 - 索引
 - 分区
 - 段
 - 触发器
 - 登录名和角色

- 视图
- ASE Replicator
- 使用 Job Scheduler 配置 Adaptive Server 作业
- 启动和停止 Adaptive Server
- 执行查询
- 根据用户的操作，记录由插件生成的 SQL 语句

启动和停止 Sybase Central

启动 Sybase Central:

- 在 UNIX 上，移动到 `$SYBASE/shared/sybccentral600` 目录，并运行 `scjview.sh` 脚本。
- 在 Windows 上，从“开始”菜单中选择“程序” | “Sybase” | “Sybase Central v6”，或者
在 Windows 上，移动到 `%SYBASE%\Shared\Sybase Central 6.0.0\` 目录，并运行 `scjview.bat` 脚本。

若要停止 Sybase Central，请选择“文件” | “退出”

注册 Adaptive Server 插件

在 Sybase Central 中，将在安装服务器时对 Adaptive Server 插件进行注册。不过，如果 Adaptive Server 插件未正确注册，您可以手动注册 Adaptive Server 插件:

- 在 Unix 上，运行 `$SYBASE/ASEP/bin/registerASEP`。
- 在 Windows 上，运行 `%SYBASE%\ASEP\bin\registerASEP.bat`
- 可通过以下方式手动注册 Adaptive Server 插件:
 - a 从“工具”(Tools) | “插件”(Plug-ins) 中选择“注册”(Register)。将出现注册向导。
 - b 选择“注册”(Register)

- c 选择“通过指定插件注册文件来注册插件”(Register a plug-in by specifying a plug-in registration file)。
- d 单击“浏览”(Browse)。
- e 导航到 `$SYBASE/ASEP/bin` (在 Windows 上为 `%SYBASE%\ASEP\bin`)，并选择 `ASEPlugin.jpr`。按照向导中的说明注册 Adaptive Server 插件。

执行常见任务

下面是一些用户可使用 Adaptive Server 插件执行的常见任务。

有关以下所有任务的详细信息，请参见 Adaptive Server 插件联机帮助。

启动和停止 Adaptive Server

如果统一代理正在监控 Adaptive Server，则可以通过右键单击服务器然后选择“关闭”(Shutdown)、“启动”(Start)或“重新启动”(Restart)，来停止、启动或重新启动服务器。

如果统一代理未监控 Adaptive Server，则可以通过选择“关闭”(Shutdown)来关闭服务器。

连接到 Adaptive Server

可通过以下任一方式连接到 Adaptive Server：

- 从工具栏中选择“连接”图标。
- 右键单击“Adaptive Server Enterprise”，然后从菜单中选择“连接”。
- 右键单击任何服务器组，然后从菜单中选择“连接”。

如果连接是从 Adaptive Server Enterprise 文件夹或连接图标启动的，则已连接的服务器将显示在缺省服务器组中。如果连接是从服务器组启动的，则插件会在对应的服务器组中显示“已连接到服务器”(Connected to server)。

还可以通过以下任一方式指定要连接到的服务器：

- 在“连接”对话框中指定服务器的主机名和端口号。
- 从服务器名下拉列表选择一个预定义的 Adaptive Server。此下拉列表包含在 `interfaces` 文件 (UNIX) 和 `sql.ini` 文件 (Windows) 中列出的服务器以及 LDAP 服务器。
- 可通过单击“连接”对话框中的“查找”(Find)，来发现可用的 Adaptive Server。在使用此方法之前，必须首先在 Adaptive Server Enterprise 属性页的“服务器发现”(Server Discovery) 选项卡中定义发现服务器。

创建数据库

创建数据库之前，您计划使用的数据库设备上一定要有足够的可用空间。
创建数据库：

- 右键单击右面板中的“添加数据库”图标，或者
- 1 选择“数据库”(Databases)文件夹，
 - 2 在“数据库”(Database)文件夹中，选择“文件”(File)|“新建”(New)|“数据库”(Database)，或者单击“添加数据库”选项。将打开“新建数据库”向导。“新建数据库”向导会要求您提供以下信息：

表 4-1：“新建数据库”向导要求提供的输入信息

输入	说明
数据库名	输入数据库的名称
数据库设备	指定要在其上分配新数据库的数据库设备
数据库设备大小	指定每台数据库设备的大小
数据或日志	指定数据库设备是存储数据还是存储事务日志。
使用覆盖	如果要将数据和日志存储在上一设备上，请指定“进行替换”(With override)。
用于装载	如果您要创建数据库以便能够从备份中恢复它，请选中“用于装载”(For Load)复选框。只有在您要从介质故障中恢复，或者您要将数据库从一个位置移到另一个位置时，才需要这样做。
访客帐户	指定是否在数据库中创建 guest 用户。

如果未输入大小，则 Adaptive Server 会分配 database size 配置变量的值或 model 数据库的大小（取两者中较大的值）。

如果存储空间有限且必须将事务日志和数据存储到同一逻辑设备上，则指定“使用覆盖”可允许 Adaptive Server 将日志和数据保存在不同的设备段上。

创建数据库后，不能删除或更改数据库设备，除非首先删除该数据库。

警告！ 删除数据库时也会删除该数据库的所有对象。

删除数据库

只有数据库的所有者才能删除数据库。

删除数据库：

- 1 选择数据库图标。
- 2 选择 “编辑” (Edit) | “删除” (Delete)。
- 3 在确认对话框中确认删除。

注释 Sybase 建议您在删除某个用户数据库之后备份 master 数据库。

添加用户

数据库所有者可以在他们拥有的数据库中添加和删除用户。

创建用户：

- 1 展开数据库文件夹（选择 “+” 图标），然后选择 “用户” (Users) 文件夹。
- 2 选择 “文件” (File) | “新建” (New) | “用户” (User)。

将打开 “添加新用户” (Add a New User) 向导并要求提供以下信息：

表 4-2: “添加新用户” (Add a New User) 向导要求提供的输入信息

输入	说明
名称	用户的名称。该名称不必与登录名相同。
登录名	为此用户指派的登录名。
组	（可选）为用户指派组。缺省值： public

注释 用户可以是某一指派组或缺省 “public” 组的成员。

还可以选择 “用户” (Users) 文件夹，然后在右窗格中双击 “添加用户” (Add User) 图标。

删除用户

不能删除拥有对象的用户。由于没有用于移交对象所有权的命令，所以您必须先删除用户拥有的对象，然后才能删除用户。此外，对于已向其他用户授予权限的用户，如果不先用 cascade 撤消权限，也无法将其删除。如果需要，请向其他用户重新授予权限。

锁定登录名是删除用户的简单替代选项。

删除用户：

- 1 选择用户图标。
- 2 选择 “编辑” (Edit) | “删除” (Delete)。
- 3 在确认对话框中确认删除。

也可以右键单击用户图标并选择用户文件夹，然后选择“删除”(Delete)。
删除用户之前：

- 1 使用 **cascade** 撤消用户的命令权限和对象权限。
- 2 如果合适，重新授予其他用户权限。
- 3 删除用户的对象。

创建表

只有数据库所有者或具有 **create table** 权限的用户才可以创建表。

创建表：

- 1 在您使用的数据库中，选择“用户表”(User Tables) 文件夹。
- 2 在“用户表”(User Tables) 文件夹中，选择“文件”(File) | “新建”(New) | “表”(Table)，或者单击“添加表”图标。
“表编辑器”(Table Editor) 即会打开。
- 3 在“名称”(Name) 框中，输入名称。
- 4 从“所有者”(Owner) 列表中，选择所有者。缺省值为“dbo”。

也可以选择“用户表”(User Tables) 文件夹，然后在右窗格中双击“添加表”(Add Table) 图标。

删除表

删除表之前，一定要确保没有任何其它对象引用它。如果有任何对象引用它，请编辑那些对象以避免出错。若要弄清楚是否有其它对象引用表，请检查它的依赖性。

注释 在删除表时，Adaptive Server 会删除与该表关联的索引和触发器，并解除对绑定到该表的列的规则或缺省值的绑定。

只有表的所有者才可以删除表。

删除表：

- 请按照以下步骤进行操作：
 - 选择表图标。
 - 选择“编辑”(Edit) | “删除”(Delete)。
 - 在确认对话框中确认删除，或者，
- 也可以右键单击表图标并选择表，然后选择“删除”(Delete)。

创建服务器组

要创建服务器组，请执行以下操作：

- 1 选择 Adaptive Server Enterprise
- 2 选择“文件”(File)|“新建”(New)|“服务器组”(Server Group)
- 3 按照“新建服务器组”(New Server Group)向导提供的步骤进行操作。

也可以通过双击右窗格中的“添加服务器组”(Add Server Group)，来添加服务器组。

获取服务器状态

如果统一代理正在监控 Adaptive Server，则可通过以下任一方式检查服务器状态：

- 单击服务器所属的服务器组。选中服务器组“详细信息”(Details)窗格中的“状态”列。
- 单击在 Sybase Central 下列出的 Adaptive Server Enterprise，然后单击右侧面板中的“服务器”(Servers)选项卡。“状态”列中即会显示服务器状态。
- 服务器图标右下方的绿色三角表明 Adaptive Server 正在运行。红色正方形表明 Adaptive Server 已停止。

注释 缺省情况下，Adaptive Server 插件未启用“检查服务器状态”(Check Server Status)。使统一代理能够监控 Adaptive Server：

- 右键单击 Adaptive Server Enterprise，然后选择“属性”。
 - 选择“优先选项”，然后选中“启用与统一代理(UA)相关的功能”(Enable Unified Agent (UA) related features)。
-

获取服务器日志

如果统一代理正在监控 Adaptive Server，则通过选择服务器然后单击右窗格中的“服务器日志”选项卡，可以检索服务器日志。

对服务器日志的检索基于服务器日志过滤器的配置方式。要配置服务器日志过滤，请右键单击服务器，然后选择“服务器日志过滤器”(Server Log Filter)。缺省情况下，Adaptive Server 插件会检索服务器日志中的最后 1000 行。可以将服务器过滤器配置为检索以下内容：

- 整个日志文件。
- 最后 n 行。
- 最近 n 天的日志。
- 与正则表达式匹配的行

记录 SQL 语句

记录通过 Adaptive Server 插件执行的所有 SQL 语句：

- 右键单击服务器，然后选择 “记录 SQL 语句” (Log SQL Statement)。
- 选择是将 SQL 语句直接记录到窗口还是记录到文件。

执行 SQL 语句

可以使用 Interactive SQL 查询工具从 Adaptive Server 插件内执行 SQL 语句。若要启动 Interactive SQL 工具，您可以：

- 右键单击要在其中执行 SQL 语句的服务器，然后从菜单中选择 “打开 Interactive SQL” (Open Interactive SQL)，或者
 - 1 单击 “Adaptive Server Enterprise”。
 - 2 单击右窗格中的 “实用程序” 选项卡，然后选择 “Interactive SQL”。

在属于某一服务器组的一组服务器上同时执行 SQL 语句：

- 1 右键单击该服务器组，然后选择 “执行 SQL” (Execute SQL)。
- 2 选择要在其中执行 SQL 语句的服务器。
- 3 单击 “执行” (Execute)。

每台服务器的结果集都列在 “SQL 执行” (SQL Execution) 对话框的 “结果集” (Result Set) 窗格中。

查看 SQL 执行计划和成本信息

使用 Adaptive Server 插件查看单个查询的 SQL 执行计划的 GUI 版本（与 showplan 的 GUI 版本非常类似），以及某个存储过程中所有查询的执行计划的 GUI 版本。此 GUI 显示的内容包括执行计划的各个运算符的节点。

要获取 GUI 计划，请执行以下操作：

- 1 启动 Interactive SQL。
- 2 执行查询或存储过程。
- 3 单击 Interactive SQL 的 “结果” 窗格中的计划选项卡。
- 4 从查询下拉列表中选择查询。
- 5 单击 “详细信息” (Details) 选项卡可查看选定查询的 GUI 计划。单击运算符节点可查看该节点的详细统计信息。
- 6 单击 “XML” 选项卡可查看选定查询的执行计划的 XML 表示形式。
- 7 单击 “文本” (Text) 选项卡可查看已提交查询的文本格式的执行计划。

有关 Interactive SQL 的详细信息，请参见第 54 页的 “启动 Interactive SQL”。

查看和更新对象属性

使用“属性”对话框查看和修改 Adaptive Server 插件中呈现的任何对象的配置。

打开“属性”对话框：

- 1 单击要查看或修改的对象。
- 2 右键单击该对象，然后选择“属性”。
- 3 选择适当的选项卡以执行任务。
- 4 在“属性”对话框中进行任意修改。
- 5 单击“应用”、“确定”或“取消”。

生成用于创建对象的 SQL 文本

生成创建对象所需的 SQL 文本，使用该文本可对对象进行反向工程。若要生成 SQL 文本，请右键单击对象，然后选择“生成 DDL”。

查看和更新 Adaptive Server 配置参数

使用“服务器属性”对话框查看和更新 Adaptive Server 配置参数。

- 1 右键单击服务器，然后从菜单中选择“配置”
- 2 从“显示配置参数”的下拉列表中选择功能组
- 3 找到并选择要查看或更新的参数
- 4 如果需要更新，请在值列中输入新值
- 5 根据需要，单击“应用” / “确定” / “取消”

使用 Interactive SQL

使用 Interactive SQL，可以对服务器执行 SQL 语句、建立脚本和显示数据库数据。可以使用它来：

- 浏览数据库中的信息。
- 对计划包含到应用程序中的 SQL 语句进行测试。
- 将查询结果保存到文件中。
- 在结果集中编辑数据。
- 将数据装载到数据库中并执行管理任务。

此外，Interactive SQL 还可运行命令文件或脚本文件。例如，可以建立要对数据库运行的可重复执行的脚本，然后使用 Interactive SQL 以批处理形式执行这些脚本。

启动 Interactive SQL

从 Sybase Central 启动 Interactive SQL

若要启动 Interactive SQL，请执行以下任一操作：

- 选择 Sybase Central 中的某一数据库，然后选择“文件”(File)|“打开 Interactive SQL”(Open Interactive SQL)。Interactive SQL 即会连接到该数据库。也可以右键单击该数据库，然后选择“打开 Interactive SQL”(Open Interactive SQL)。

“打开 Interactive SQL”(Open Interactive SQL) 菜单项会打开与服务器的连接。不过，在为某一服务器选择该菜单项后，Interactive SQL 会打开与该服务器的缺省数据库的连接。在从“打开 Interactive SQL”(Open Interactive SQL) 菜单中选择了特定数据库后，Interactive SQL 会打开选定数据库。
- 若要启动 Interactive SQL 而不连接到服务器，请选择“工具”(Tools)|“Adaptive Server Enterprise”|“打开 Interactive SQL”(Open Interactive SQL)。将显示“连接”对话框。

从命令行启动 Interactive SQL

从命令行启动 Interactive SQL 的方式取决于所用操作系统。

如果独立启动 Interactive SQL，那么就像在 Sybase Central 中那样，会出现用于连接到数据库的“连接”对话框。

- 对于 UNIX，请切换到 `$SYBROOT/DBISQL/bin` 目录并输入：

```
dbisql
```

在 Windows 上，切换到 `%SYBROOT%\DBISQL\bin` 目录并输入：

```
dbisql.bat
```

- 在“连接”对话框中，输入信息以便连接到“连接”对话框中的数据库，并单击“确定”(OK)。

打开一个新的 Interactive SQL 窗口：

- 1 选择“窗口”(Window)|“新建窗口”(New Window)。将显示“连接”对话框。
- 2 在“连接”对话框中，输入连接选项，然后单击“确定”(OK)即可连接。

连接信息（包括数据库名称、用户 ID 和数据库服务器）会出现在“SQL 语句”窗格上方的标题栏中。

使用 SQL 菜单中的“连接”和“断开连接”命令，或者在“SQL 语句”窗格中执行 `connect` 或 `disconnect` 语句，也可以连接到数据库或断开与数据库的连接。

设置配置参数

本章介绍 Adaptive Server 配置参数，这些参数在此处按字母顺序列出。

配置参数是可由用户定义的设置，是通过 `sp_configure` 来设置的。配置参数可用于包含基本服务器操作到特定服务器操作在内的广泛的服务领域，还可用于性能调优。

主题	页码
概述	55
使用 sp_configure	59
sp_configure 输出	68
命名高速缓存配置参数	70
sysconfigures 和 syscurconfigs 表	71
配置参数	71

概述

配置参数是用于控制 Adaptive Server 行为的各个方面的可由用户定义的设置。Adaptive Server 为所有配置参数都提供了缺省值。使用配置参数来针对安装的特定需求定制 Adaptive Server。

仔细阅读本章，确定应重置哪些配置参数以便优化服务器性能。

警告！ 更改配置参数时要谨慎。任意更改配置参数值可能会对 Adaptive Server 的性能产生负面影响，还可能影响服务器操作的其它方面。

Adaptive Server 配置文件

Adaptive Server 将配置参数的值存储在一个 ASCII 文本文件类型的配置文件中。安装新的 Adaptive Server 时，这些参数将设置为缺省配置；文件的缺省名称为 *server_name.cfg*，文件的缺省位置为 Sybase Adaptive Server 主目录 (\$SYBASE_ASE)。每次您修改配置参数时，Adaptive Server 都会使用以下命名约定创建过期配置文件的副本：*server_name.001*、*server_name.002*、*server_name.003*...*server_name.999*。Adaptive Server 将新值写入文件 *server_name.cfg*，或写入您在启动时指定的文件名。

修改配置参数

按以下方式之一设置或更改配置参数：

- 使用适当的参数和值执行 `sp_configure` ；
- 通过编辑配置文件然后使用 `configuration file` 选项来调用 `sp_configure` ；
或者
- 通过在启动时指定配置文件的名称。

配置参数可以是动态的，也可以是静态的。一旦您执行 `sp_configure`，动态参数就立即生效。静态参数则要求重新分配内存，因此它们只会在您重新启动 Adaptive Server 后生效。本章中每个参数的说明都指明了它是静态的还是动态的。

在更改值后，Adaptive Server 会将新值写入系统表 `sysconfigures` 和配置文件。当前配置文件和 `sysconfigures` 反映的是配置值，而不是运行值。系统表 `syscurconfigs` 反映配置参数的当前运行值。

用于修改配置参数的必需角色

使用 `sp_configure` 所必需的角色：

- 任何用户都可以执行 `sp_configure` 以显示有关参数及其当前值的信息。
- 只有系统管理员或系统安全员才能执行 `sp_configure` 来修改配置参数。
- 只有系统安全员才能执行 `sp_configure` 来修改以下参数的值：
 - `allow procedure grouping`
 - `allow remote access`
 - `allow sendmsg`

- allow updates to system tables
- auditing
- audit queue size
- check password for digit
- current audit table
- enable ldap user auth
- enable pam user auth
- enable ssl
- log audit logon failure
- log audit logon success
- maximum failed logins
- minimum password length
- msg confidentiality reqd
- msg integrity reqd
- secure default login
- select on syscomments.text
- SQL Perfmon Integration
- syb_sendmsg port number
- suspended audit when device full
- systemwide password expiration
- unified login required
- use security services

使用 `sp_configure` 的单位规范

`sp_configure` 允许在指定配置参数的值时指定单位指示符。单位指示符用 `p` 或 `P` 代表页，用 `m` 或 `M` 代表兆字节，用 `g` 或 `G` 代表千兆字节。如果不指定单位，并且配置了控制内存的参数，则 Adaptive Server 使用逻辑页大小作为基本单位。

注释 在配置与内存相关的参数时，应只对单位规范使用 `P`（页大小）参数。如果使用任何其它参数来配置与内存相关的参数，则 Adaptive Server 可能会发出算术溢出错误消息。

指示特定单位规范的语法为：

```
sp_configure "parameter name", 0, "p|P|k|K|m|M|g|G"
```

必须包括 “0” 作为占位符。

可使用此单位规范配置任何参数。例如，如果将 `number of locks` 设置为 1024，则可输入：

```
sp_configure "number of locks", 1024
```

或：

```
sp_configure "number of locks", 0, "1K"
```

此功能不改变 Adaptive Server 报告 `sp_configure` 输出的方式。

获取有关配置参数的帮助信息

使用 `sp_helpconfig` 或 `sp_configure` 可显示特定配置参数的信息。例如：

```
sp_helpconfig "number of open"
```

Configuration option is not unique.

option_name	config_value	run_value
number of open databases	12	12
number of open indexes	500	500
number of open objects	500	500

```
sp_helpconfig "number of open indexes"
```

number of open indexes sets the maximum number of indexes that can be open at one time on SQL Server. The default value is 500.

Minimum Value	Maximum Value	Default Value	Current Value	Memory Used
-----	-----	-----	-----	-----

100 2147483647 500 500 208

```
sp_configure "number of open indexes"
```

Parameter Name	Default	Memory Used	Config Value	Run Value
number of open indexes	500	208	500	500

请参见《系统管理指南：卷2》中的第3章“配置内存”。

使用 *sp_configure*

sp_configure 可显示并重置配置参数。可以限制 *sp_configure* 显示的参数数量，方法是使用 *sp_displaylevel* 将显示级别设置为以下值之一：

- Basic
- Intermediate
- Comprehensive

有关显示级别的信息，请参见第 66 页的“用户定义的参数层次子集：显示级别”。有关 *sp_displaylevel* 的信息，请参见《参考手册：过程》。

表 5-1 介绍了 *sp_configure* 的语法。“作用”列中的信息假定显示级别设置为“Comprehensive”。

表 5-1: *sp_configure* 语法

命令	作用
<code>sp_configure</code>	按组显示所有配置参数、其当前值、缺省值、最近被设置的值以及这种特定设置所使用的内存量。
<code>sp_configure "parameter"</code>	显示指定参数使用的当前值、缺省值、最近更改的值以及内存量。
<code>sp_configure "parameter" , value</code>	将 <i>parameter</i> 重置为 <i>value</i> 。
<code>sp_configure "parameter" , 0, "default"</code>	将指定参数重置为其缺省值。
<code>sp_configure "group_name"</code>	显示 <i>group_name</i> 中的所有配置参数、其当前值、缺省值、最近被设置的值以及每个设置所使用的内存量。
<code>sp_configure "configuration file" , 0, "sub_command" , "file_name"</code>	设置配置文件中的配置参数。有关这些参数的说明，请参见第 60 页的“使用 <i>sp_configure</i> 及配置文件”。

语法元素

表 5-1 中的命令使用以下变量：

- *parameter* — 是任何有效的 Adaptive Server 配置参数或参数子串。
- *value* — 是参数有效取值范围内的任一整数。（关于参数有效取值范围的信息，请参见各个参数的说明。）起切换作用的参数只有两个有效值：1（打开）和 0（关闭）。
- *group_name* — 是参数层次中任何组的名称。

参数语法分析

`sp_configure` 将每个参数（和参数名片段）分析为 “%*parameter*%”。如果字符串不能唯一标识特定参数，则它返回与该字符串匹配的所有参数的值。

以下示例返回包含 “lock” 的所有配置参数的值，这些配置参数有 lock shared memory、number of locks、lock promotion HWM、server clock tick length、print deadlock information 和 deadlock retries：

```
sp_configure "lock"
```

注释 如果尝试设置的参数值的参数名片段不唯一，`sp_configure` 会返回与该片段匹配的所有参数的当前值，并要求您指定唯一的参数名。

使用 `sp_configure` 及配置文件

按上文所述使用 `sp_configure` 以交互方式配置 Adaptive Server；也可通过指示 Adaptive Server 从已编辑或恢复的配置文件版本中读取值，以非交互方式配置 Adaptive Server。

通过从配置文件中进行更改，您可以：

- 通过使用同一配置文件，在多台服务器之间复制特定配置。
- 使用某个配置文件作为基准来测试服务器上的配置值。
- 在实际设置参数值之前，先使用配置文件对参数值进行验证检查。
- 创建多个配置文件，以便需要更改资源时在它们之间切换。

有关编辑该文件的信息，请参见第 62 页的“编辑配置文件”。有关在启动时指定配置文件名称的信息，请参见第 63 页的“通过配置文件启动 Adaptive Server”。

配置文件的命名技巧

若要使用其名称不是缺省名称的配置文件，请保留文件名的 *server_name* 部分，并在扩展名中至少包括一个字母字符（例如 *my_server.A001*）。或者，您可以更改文件名的 *server_name* 部分（例如，*A_my_server.001*）。这样做可以避免与修改参数时由 Adaptive Server 生成的备份配置文件混淆。

使用 *sp_configure* 读取或写入配置文件

使用带有 *configuration file* 选项的 *sp_configure* 的语法如下：

```
sp_configure "configuration file", 0, "subcommand", "file_name"
```

其中：

- “configuration file” — （包括引号）指定此命令使用配置文件。
- 0 — 在 *configuration file* 参数后是必需的，以便向后兼容。
- “subcommand” — 为以下值之一：
 - **write** — 使用当前配置创建名为 *file_name* 的文件。如果 *file_name* 已存在，则向错误日志中写入一条消息；将使用约定 *server_name.001*、*server_name.002* 等重命名现有文件。如果更改静态参数后没有重新启动服务器，则 **write** 会显示该参数当前运行的值。如果未使用 *file_name* 指定目录，则会将该文件写入 Adaptive Server 的启动目录。
 - **read** — 对包含在 *file_name* 中的值执行验证检查，并且将通过验证检查的值读入到服务器中。如果 *file_name* 遗漏了任何参数，则使用那些参数的当前值。

如果 *file_name* 中的静态参数值与其当前运行值不同，则 **read** 命令失败，并显示一条消息。但是，对 *file_name* 中值的验证仍会进行。
 - **verify** — 对 *file_name* 中的值执行验证检查。如果已编辑过配置文件，这将大有益处，因为它可以防止您试图用无效的配置文件配置服务器。
 - **restore** — 用最近配置的值创建 *file_name*。如果静态参数已配置为新值，该子命令会将配置的值而非当前运行的值写入该文件。如果丢失了配置文件的所有副本，而又必须生成新副本，它就非常有用。如果未使用 *file_name* 指定目录，则会将该文件写入 Adaptive Server 的启动目录。
- *file_name* — 指定要与 *subcommand* 一起使用的配置文件。如果未指定目录作为文件名的一部分，则使用 Adaptive Server 的启动目录。

示例

示例 1 对 `srv.config` 文件中的值执行验证检查，并将通过验证的参数读入到服务器中。当前的运行值会替代没有通过验证检查的值：

```
sp_configure "configuration file", 0, "read", "srv.config"
```

示例 2 创建文件 `my_server.config`，并将服务器正在使用的当前配置值写入该文件：

```
sp_configure "configuration file", 0, "write", "my_server.config"
```

编辑配置文件

配置文件是 ASCII 文件，可以使用任何能够以 ASCII 格式保存文件的文本编辑器对其进行编辑。每个参数的语法为：

`parameter_name={value | DEFAULT}`

其中：

- `parameter_name` — 是您要指定的参数的名称。
- `value` — 是所设置 `parameter_name` 的数字值。
- “DEFAULT” — 指定要为 `parameter_name` 使用缺省值。

示例

示例 1 此示例指定了在索引页拆分或聚合期间发生死锁时，事务能够重试一次以获取锁：

```
deadlock retries = 1
```

示例 2 此示例指定应使用 `cpu accounting flush interval` 参数的缺省值：

```
cpu accounting flush interval=DEFAULT
```

编辑配置文件时，所做的编辑在执行以下操作后才会生效：使用 `verify` 选项检查该文件、通过 `read` 选项读取该文件，或使用该配置文件重新启动 Adaptive Server。

如果所有配置文件丢失或损坏，您可以在正在运行的服务器上重新创建一个配置文件，方法是使用子命令 `restore`，再为这个新文件指定一个名称。新文件中的参数被设置为服务器当前运行所使用的值。

配置文件的权限

配置文件是不加密的 ASCII 文本文件。缺省情况下，创建这些文件后，文件所有者对文件拥有读写权限，而所有其他用户只有读权限。在操作系统级创建配置文件的用户是文件所有者；如果从 Adaptive Server 使用 `write` 或 `restore` 参数创建配置文件，则文件所有者是启动 Adaptive Server 的用户。一般情况下，就是用户 “sybase”。若要限制对配置文件的访问，应使用操作系统的文件权限命令设置适当的读、写和执行权限。

注释 必须相应地为所创建的每个配置文件设置权限。

备份配置文件

备份 master 数据库时不会自动备份配置文件。因为它们是操作系统的文件，因此请按备份其它操作系统文件的方式备份它们。

检查当前使用的配置文件的名称

由于空间限制，`sp_configure` 的输出截断了配置文件的名称。若要查看配置文件的完整名称，请使用：

```
select s1.value2
from syscurconfigs s1, sysconfigures s2
where s1.config = s2.config
and s2.name = "configuration file"
```

通过配置文件启动 Adaptive Server

缺省情况下，Adaptive Server 在启动时读取启动目录中的配置文件 `server_name.cfg`。如果该文件不存在，则将创建一个新的文件并将所有值设置为 Adaptive Server 的缺省值。

您可以用指定的配置文件启动 Adaptive Server。有关详细信息，请参见《实用程序指南》。

如果指定的配置文件不存在，Adaptive Server 则会显示一条错误消息而不会启动。

如果命令执行成功，则创建文件 `server_name.bak`。该文件包含 `sysconfigures` 中存储的配置值，它们是在使用从指定配置文件中读取的值更新 `sysconfigures` 之前存储的值。以后每次启动时，都会覆盖该文件。

配置文件错误

配置文件中存在错误时， Adaptive Server 可能不会启动，或者可能使用缺省值。

如果存在以下情况， Adaptive Server 将使用缺省值：

- 存在非法值。例如，如果一个参数要求使用数值，而配置文件包含的是字符串，则 Adaptive Server 将使用缺省值。
- 存在低于所允许的最小值的值。

参数层次

配置参数根据它们影响 Adaptive Server 行为的不同方面进行分组。这样就可以更加轻松地识别为改善 Adaptive Server 性能的特定方面而需要调整的所有参数。

虽然每个参数都有一个所属的主组，但许多参数也同时属于某些从组。例如， `number of remote connections` 首先属于网络通信组，其次还属于内存使用组。这反映出某些参数会影响 Adaptive Server 多方面的行为。`sp_configure` 可以将参数显示在其所属的所有组中。

表 5-2 列出了配置参数组。

表 5-2: 配置组

参数组	将 Adaptive Server 配置用于
备份 / 恢复	备份和恢复数据
高速缓存管理器	数据和过程高速缓存
组件集成服务管理	组件集成服务
DTM 管理	分布式事务管理 (DTM) 功能
诊断	诊断原则
磁盘 I/O	磁盘 I/O
错误日志	错误日志，以及将 Adaptive Server 事件记录到 Windows 事件日志
扩展存储过程	扩展存储过程 (ESP) 的行为。
一般信息	基本系统管理
Java 服务	Adaptive Server 中用于 Java 的内存 有关数据库中 Java 的完整信息，请参见《Adaptive Server Enterprise 中的 Java》手册。 如果使用方法调用 JDBC，则需要增加用户的可用执行堆栈的大小。请参见第 224 页的 “stack size”。
语言	语言、排序顺序和字符集
锁管理程序	锁定

参数组	将 Adaptive Server 配置用于
内存使用	内存消耗
元数据高速缓存	针对频繁使用的系统目录信息，设置元数据高速缓存大小。元数据高速缓存是一块保留的内存区域，用于跟踪有关数据库、索引或对象的信息。打开的数据库、索引或对象的数量越多，元数据高速缓存的大小就会越大。有关内存使用上下文中元数据高速缓存的论述，请参见《系统管理指南，卷2》中的第3章“配置内存”。
监控	收集监控信息。缺省情况下，Adaptive Server 不会收集监控信息。请参见 Performance and Tuning Guide: Monitoring and Analyzing（《性能和调优指南：监控和分析》）中的第2章“Monitoring Table”（监控表）。
网络通信	Adaptive Server 与远程服务器之间的通信，以及 Adaptive Server 与客户端程序之间的通信
操作系统资源	使用操作系统资源
物理内存	计算机的物理内存资源
处理器	SMP 环境中的处理器
查询调优	查询优化
RepAgent 线程管理	通过 Replication Server 进行复制
SQL Server 管理	常规 Adaptive Server 管理。
与安全性相关的参数	与安全性相关的功能
Unicode	与 Unicode 相关的功能
用户环境	用户环境

显示所有组和其关联参数以及这些参数的当前值的语法是：

```
sp_configure
```

注释 sp_configure 返回的参数数目取决于设置的显示级别的值。请参见第 66 页的“用户定义的参数层次子集：显示级别”。

下面是用于显示特定组及其关联参数的语法：

```
sp_configure "group_name"
```

例如，若要显示磁盘 I/O 组，请输入：

```
sp_configure "Disk I/O"

Group: Disk I/O
Parameter Name      Default Memory Used Config Value Run Value
unit                type
-----
allow sql server async i/o      1          0          1          1
switch                    static
```

diabile disk mirroring	1	0	1	1
switch static				
disk i/o structures	256	0	256	256
number dynamic				
number of devices	10	0	10	10
number dynamic				
number of large I/O buffers	6	12352	6	6
number dynamic				
page utilization percent	95	0	95	95
percent dynamic				

注释 如果服务器使用的是不区分大小写的排序顺序，则不带参数的 `sp_configure` 会按字母顺序返回所有配置参数和组的列表，而不分组显示。

用户定义的参数层次子集：显示级别

根据使用 Adaptive Server 的方式，您可能需要经常调整某些参数。使用参数子集可能更加简便。

缺省显示级别为 `comprehensive`。设置了显示级别后，该设置将适用于多个会话。不过，您可以随时重置该显示级别。

- **Basic** — 只显示最基本的参数，适用于常规的服务器调整操作。
- **Intermediate** — 除了 `basic` 参数外，还包括复杂度稍高的参数。
- **Comprehensive** — 包括最复杂参数在内的所有参数。该级别适于对服务器进行高精度调优的用户。

用于显示当前显示级别的语法是：

`sp_displaylevel`

若要设置显示级别，请使用：

`sp_displaylevel user_name[, basic | intermediate | comprehensive]`

其中 `user_name` 为您的 Adaptive Server 登录名。

显示级别对 `sp_configure` 输出的影响

如果显示级别设置为 `basic` 或 `intermediate`，`sp_configure` 将只返回显示级别设置为 `comprehensive` 时返回的参数的子集。例如，如果显示级别设置为 `intermediate`，并且要查看 `languages` 组中的参数，请输入：

```
sp_configure "Languages"
```

输出结果如下：

```
sp_configure
Group: language
```

Parameter Name	Default	Memory Used	Config Value	Run Value	Unit	Type
default character set	1	0	1	1	id	static
default language id	0	0	0	0	id	dyna
...						

这只代表 `languages` 组中参数的一个子集；某些语言参数仅在显示级别为 `comprehensive` 时显示。

使用 `sp_configure` 和 `sp_sysmon` 进行性能调优

`sp_sysmon` 可以监控 Adaptive Server 的性能并生成各种统计信息，用以描述 Adaptive Server 系统的行为。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

可以在使用 `sp_configure` 调整配置参数之前和之后运行 `sp_sysmon`。输出不仅提供了性能调优依据，还能让用户了解配置更改的结果。

在集群环境中使用配置参数

对于 Cluster Edition，Sybase 支持集群范围内的配置和特定于实例的配置。集群范围内的配置参数将应用于集群中的所有实例。本地配置参数则仅应用于指定的实例。

- 本地配置优先于集群范围内的配置。
- 如果尚未应用特定于实例的配置，则应用集群范围内的配置。
- 某些参数（例如 `default character set id`）无法应用于特定实例。只能在整个集群上使用这些参数。

集群配置文件包括特定于实例的配置块。特定于实例的块中的参数设置优先于集群范围内的设置。例如：

```
max online engines = DEFAULT

[Instance:ase1]
max online engines = 5
[Instance:ase2]
max online engines = 3
```

请参见 《集群用户指南》。

sp_configure 输出

下面的输出示例显示，在显示级别为 **comprehensive**，并且不带参数执行 **sp_configure** 的情况下，**sp_configure** 所输出信息的类型。它输出的值将因所在的平台和更改的值而异。

```
sp_configure
Group: Configuration Options

Group: Backup/Recovery
```

Parameter Name	Default	Memory Used	Config Value	Run Value	Unit	Type
allow remote access	1	0	1	1	switch	dyn
print recovery info	0	0	0	0	switch	dyn
recovery interval in m	5	0	5	5	minutes	dyn
...						

注释 如果显示级别设置为 “comprehensive”，则所有配置组和参数都将出现在输出中。

其中：

- “Default” 列显示缺省值。如果没有明确重新配置参数，该参数将保留其缺省值。
- “Memory Used” 显示参数使用当前值时所占用的内存量（以 KB 为单位）。某些相关参数占用的内存来自同一内存池。例如，**stack size** 和 **stack guard size** 占用的内存已被计入 **number of user connections** 占用的内存。如果将这些参数使用的内存一一相加，则总值会大于实际使用的内存量。与其它参数 “共享” 内存的参数标有井号 (#)。

- “Config Value” 显示配置参数最近被设置的值。执行 `sp_configure` 以修改动态参数时：
 - 将更新配置值和运行值。
 - 将更新配置文件。
 - 更改会立即生效。
- 修改静态参数时：
 - 将更新配置值。
 - 将更新配置文件。
 - 只有当重新启动 Adaptive Server 后更改才会生效。
- “Run Value” 显示 Adaptive Server 当前正使用的值。若修改动态参数的值，该列将立即发生变化；若修改静态参数的值，该列在重新启动 Adaptive Server 后才显示出变化。
- “Unit” 显示配置参数的单位值。Adaptive Server 使用以下单位显示信息：

单位名称	单位说明
数字	项数。
时钟周期	时钟周期数。
微秒	微秒数。
毫秒	毫秒数。
秒	秒数。
分钟	分钟数。
小时	小时数。
字节	字节数。
天	天数。
千字节	千字节数。
兆字节	兆字节数。
内存页 (2K)	2K 内存页数。
虚拟页 (2K)	2K 虚拟页数。
逻辑页	逻辑页数。该值取决于服务器正使用的逻辑页大小：2、4、8 或 16K。
百分比	配置的参数的值（百分比形式）。
比率	配置的参数的值（比率形式）。
开关	参数的值为 TRUE（启用参数）或 FALSE。
id	所调查的配置参数的 ID。
名称	分配给参数的运行值或配置值的字符串名称。例如，对于 <code>sp_configure</code> "lock scheme" 的输出，“binary” 出现在 “Run Value” 或 “Config Value” 列的下方。
行	行数

- “Type” 列显示配置选项是静态的还是动态的。对静态参数进行更改要求重新启动 Adaptive Server 以使更改生效。动态参数的更改可立即生效，不必重新启动 Adaptive Server。

命名高速缓存配置参数

命名高速缓存配置参数组提供命名高速缓存的详细信息：

- **cache size** — 高速缓存的大小。缺省情况下，Adaptive Server 创建 8MB 高速缓存。使用 **sp_cacheconfig** 动态更改此参数，或更改服务器配置文件中的值以使更改在下次服务器重新启动后生效。
- **cache status** — 高速缓存的状态。default data cache、log only、mixed 或 in-memory storage 其中的一个值。缺省数据高速缓存的高速缓存状态必须为 default data cache，并且不能更改。命名高速缓存的 **cache status** 可以为 log only、mixed 或对于内存中数据库可以为 in-memory storage（对于内存数据库，您不能更改 **cache status**）。

在其它实例使用不同 **cache status** 的情况下，您不能在集群环境中动态地将 **cache status** 从本地高速缓存上的 log only 更改为其它值。

- **cache replacement** — 描述高速缓存替换策略。对于命名高速缓存和缺省数据高速缓存，替换策略为 strict LRU 或 relaxed LRU。使用 **sp_cacheconfig** 动态更改此参数，或更改服务器配置文件中的值以使更改在下次服务器重新启动后生效。对于内存中数据库，高速缓存替换策略必须为 none，因为内存数据库不使用缓冲区或页替换。
- **local cache partition number** — 高速缓存分区数。您可以将命名高速缓存划分为多个高速缓存分区。可接受的值为 0、2、4、8、16、32、64 或 128。您无法动态更改高速缓存分区数；必须重新启动 Adaptive Server 以使更改生效。

sysconfigures 和 syscurconfigs 表

sp_configure 显示的报告主要根据 master..sysconfigures 和 master..syscurconfigs 系统表构建而成，sysattributes、sysdevices 和其它系统表提供附加信息。

sysconfigures 表的 value 列中记录 sp_configure 或配置文件最后一次设置的值；syscurconfigs 的 value 列中存储当前使用的值。对于动态参数，这两个值是一致的；而对于静态参数，由于只有在重新启动服务器后才能使更改值生效，因此如果 Adaptive Server 最近一次启动后更改了这些值，这两个值就会不同。如果使用缺省值，这些值也可能不同。在这种情况下，sysconfigures 存储的值为 0，syscurconfigs 存储 Adaptive Server 计算和使用的值。

sp_configure 将对 sysconfigures 和 syscurconfigs 执行连接以显示 sp_configure 报告的值。

查询 syscurconfigs 和 sysconfigures：一个示例

可能需要查询 sysconfigures 和 syscurconfigs 以按所需组织方式组织信息。例如，在不带任何参数的情况下执行 sp_configure，会列出配置参数占用的内存，但不会列出最小值和最大值。使用此查询来获取当前内存使用量的完整列表，以及最小值、最大值和缺省值：

```
select b.name, memory_used, minimum_value,
       maximum_value, defvalue
from master.dbo.sysconfigures b,
     master.dbo.syscurconfigs c
where b.config *= c.config and parent != 19
and b.config > 100
```

配置参数

许多情况下，配置参数的最大可允许值通常受可用内存所限，而不是受 sp_configure 限制所限。

注释 若要查找所用平台和 Adaptive Server 版本的最大支持的值，请参见适用于您的平台的《安装指南》中的“Adaptive Server 规范”。

按字母顺序排列的配置参数列表

以下各部分包括每个配置参数的摘要信息和详细信息。

abstract plan cache

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

`abstract plan cache` 启用抽象计划散列键的高速缓存。请参见 Performance and Tuning Series: Query Processing and Abstract Plans （《性能和调优系列：查询处理和抽象计划》）中的第 12 章 “Creating and Using Abstract Plans”（创建和使用抽象计划）。必须启用 `abstract plan load` 才能使计划高速缓存生效。

abstract plan dump

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

`abstract plan dump` 使抽象计划能够保存到 `ap_stdout` 抽象计划组中。请参见 Performance and Tuning Series: Query Processing and Abstract Plans （《性能和调优系列：查询处理和抽象计划》）中的第 12 章 “Creating and Using Abstract Plans”（创建和使用抽象计划）。

abstract plan load

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

abstract plan load 启用查询与 **ap_stdin** 抽象计划组中的抽象计划的关联。请参见 Performance and Tuning Series: Query Processing and Abstract Plans（《性能和调优系列：查询处理和抽象计划》）中的第 12 章 “Creating and Using Abstract Plans”（创建和使用抽象计划）。

abstract plan replace

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

abstract plan replace 启用对 **ap_stdout** 抽象计划组中的抽象计划的计划替换。请参见 Performance and Tuning Series: Query Processing and Abstract Plans（《性能和调优系列：查询处理和抽象计划》）中的第 12 章 “Creating and Using Abstract Plans”（创建和使用抽象计划）。必须启用 **abstract plan load** 以使替换模式生效。

additional network memory

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、网络通信、物理内存

additional network memory 设置额外内存的最大大小，这些额外内存可以用于比缺省包大小更大的网络包。Adaptive Server 将输入的值向下舍入到最近的 2K 值。缺省值表示没有额外空间可供分配给较大的包。

当一个登录操作请求的包大小比较大时，Adaptive Server 首先会检查它是否具有足够的内存来满足该请求。如果没有，Adaptive Server 则会寻找最大可用内存块，然后尝试分配比最大内存块小的适当内存（其大小为 **default network packet size** 的倍数）。如果尝试失败，Adaptive Server 则会减少请求的值，减少量等于 **default network packet size** 的字节数（如果有）。Adaptive Server 最多会连续尝试 10 次，直到该大小等于 **default network packet size** 的值为止。在进行第十次尝试时，Adaptive Server 会使用 **default network packet size** 的值作为包大小。

如果增大 **max network packet size**，您必须增大 **additional network memory**，因为所有留给用户使用的已分配网络内存都等于缺省大小。Adaptive Server 确保每个用户连接都能够以缺省包大小进行登录。

如果增大 **max network packet size** 而不增大 **additional network memory**，则 Adaptive Server 不保证请求的网络包大于缺省大小的客户端能够按请求的包大小登录。

增大 **additional network memory** 可提高传输大量数据的应用程序的性能。应用程序使用较大的包大小时，要确定 **additional network memory** 的值：

- 1 估计同时请求较大的包的用户数目和他们的应用程序请求的大小；
- 2 将该总和乘以 3，因为每个连接需要 3 个缓冲区；
- 3 为服务器增加用于开销的内存：32 位服务器增加 2%，64 位服务器增加 4%；
- 4 将该值取整到 2048 的最近倍数。

例如，估计较大包大小的所有这些需求：

应用程序	包大小	开销
bcp	8192	
Client-Library	8192	
Client-Library	4096	
Client-Library	4096	
总计	24576	
乘以 3 个缓冲区 / 用户	* 3=73728	
计算 2% 的开销		* .02=1474
增加开销	+ 1474	
额外的网络内存	75202	
向上舍入到 2048 的倍数	75776	

将 **additional network memory** 设置为 75,776 字节。

allocate max shared memory

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、物理内存

`allocate max shared memory` 确定 Adaptive Server 是分配在启动时 `max memory` 指定的所有内存，还是只分配配置参数需要的内存量。

通过将 `allocate max shared memory` 设置为 0，可确保 Adaptive Server 只使用当前配置所需的共享内存量，并在启动时只分配配置参数所需的内存量，它比 `max memory` 值要小。

如果将 `allocate max shared memory` 设置为 1，则 Adaptive Server 在启动时分配 `max memory` 指定的所有内存。如果将 `allocate max shared memory` 设置为 1，并且增大 `max memory`，则 Adaptive Server 将尝试立即分配内存。如果内存分配失败，Adaptive Server 会向错误日志中写入消息。检查错误日志以验证是否未发生错误。

成功的内存分配意味着 Adaptive Server 对任何内存配置的更改总有所需的内存，并且服务器在因附加的内存而重新调整时性能不会降低。但是，如果不能精确地估计出内存的增长量，并将 `max memory` 设置为较大的值，则可能浪费总的物理内存。

allow backward scans

摘要信息	
缺省值	1（打开）
有效值	0（关闭）， 1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	查询调优

allow backward scans 控制优化程序如何执行包含 `order by...desc` 命令的 `select` 查询：

- 该值设置为 1 时，优化程序可按页链以递减索引顺序访问索引或表行。
- 该值设置为 0 时，优化程序通过按索引页指针以升序将这些行选入工作表，然后按降序对该工作表进行排序。

第一种方法（执行向后扫描）能够加快访问表的速度，这些表需要结果按列值的降序排序。但是，某些应用程序可能由于执行了向后扫描而出现死锁。特别地，如果存在一个包含 `delete` 或 `update` 的查询，它向前扫描了相同的索引，则会增加死锁。也可能由于索引中的页面拆分而产生死锁。

使用 `print deadlock information` 将有关死锁的消息发送到错误日志。请参见第 201 页的“[print deadlock information](#)”。或者，可以使用 `sp_sysmon` 检查死锁。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon`（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

allow nested triggers

摘要信息	
缺省值	1（打开）
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

allow nested triggers 控制嵌套触发器的使用。将值设置为 1 时，由触发器所做的数据修改可能会引发其它触发器。如果将 `allow nested triggers` 设置为 0，则可禁用嵌套触发器。`set` 选项 `self_recursion` 控制由触发器所做的修改是否可使该触发器再次触发。

allow procedure grouping

摘要信息	
缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	与安全性相关的参数

allow procedure grouping 控制对同名的存储过程进行分组的能力，从而使用单个 **drop procedure** 语句就可删除一组存储过程。

allow remote access

摘要信息	
缺省值	1（打开）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	备份 / 恢复、网络通信

allow remote access 控制从远程 Adaptive Server 的登录。缺省值为 1，允许 Adaptive Server 与 Backup Server 通信。

注释 如果设置为 0，则将禁止服务器到服务器的 RPC。因为 Adaptive Server 通过 RPC 与 Backup Server 进行通信，所以将该参数设置为 0 就不可能进行数据库备份。

因为执行 RPC 需要其它系统管理操作来启用远程服务器而不是 Backup Server，所以将该选项设置为 1 不会产生安全风险。

allow resource limits

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、SQL Server 管理

`allow resource limits` 控制资源限制的使用。在将值设置为 1 时，服务器为时间范围、资源限制和服务器内部报警分配内部内存。服务器还将可应用的范围和限制内部分配给用户会话。`showplan` 和 `statistics io` 的输出将显示优化程序对查询的开销估计。将 `allow resource limits` 设置为 0 可禁用所有资源限制。

allow sendmsg

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	网络通信

`allow sendmsg` 允许或禁止将消息从 Adaptive Server 发送到用户数据报协议 (UDP) 端口。当 `allow sendmsg` 设置为 1 时，任何用户都可使用 `sp_sendmsg` 或 `syb_sendmsg` 发送消息。若要设置 Adaptive Server 所使用的端口号，请参见第 230 页的 “[syb_sendmsg port number](#)”。

注释 Windows 不支持将消息发送到 UDP 端口。

allow sql server async i/o

摘要信息	
缺省值	1（打开）
有效值	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	磁盘 I/O

`allow sql server async i/o` 使 Adaptive Server 能够以异步磁盘 I/O 方式运行。若要使用异步磁盘 I/O，请同时在 Adaptive Server 和操作系统上启用该参数。有关在操作系统级启用异步 I/O 的信息，请参见操作系统文档。

异步运行磁盘 I/O 都比同步运行快。这是因为当 Adaptive Server 发出异步 I/O 时，它不必等待响应即可发出随后的 I/O。

allow updates to system tables

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`allow updates to system tables` 使具有系统管理员角色的用户能够更改系统表并创建可修改系统表的存储过程。如果启用 `allow updates to system tables`，则数据库管理员可以在其拥有的任何表中更新系统表。

系统表包括：

- master 数据库中所有 Sybase 提供的表
- 用户数据库中所有以 “sys” 开始的表和在 sysobjects 表中其 ID 值小于或等于 100 的表

警告！ 如果对系统表进行不正确的变更，则可能会导致数据库破坏和数据丢失。若要防止可能损坏数据库的错误，请在修改系统表时始终使用 `begin transaction`。完成修改后，请立即禁用 `allow updates to system tables`。

allow updates to system tables 设为打开状态时所创建的存储过程和触发器可以更新系统表，即便在此参数被设置为关闭后也是如此。在将 **allow updates to system tables** 设置为打开状态时，就会产生一段“脆弱时间段”，即在此段时间内用户可以变更系统表或创建将来可能会变更系统表的存储过程。

由于系统表非常重要，Sybase 建议您仅在严格控制的情况下将此参数设置为打开。若要确保当系统表可被直接更新时没有其他用户可以访问 Adaptive Server，应以单用户模式重新启动 Adaptive Server。有关详细信息，请参见《实用程序指南》中的 **startserver** 和 **dataserver**。

注释 全服务器范围内的配置选项 **allow updates to system tables** 优先于 **allow updates to system tables** 的存储过程设置。如果未在服务器级启用 **allow updates to system tables**，单个存储过程设置将确定是否可以修改系统目录。

average cap size

摘要信息	
缺省值	200
值的范围	100 - 10000
状态	静态
显示级别	
要求的角色	
配置组	诊断

留作将来使用。

audit queue size

摘要信息	
缺省值	100
值的范围	1 - 65535
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	内存使用、与安全性相关的参数

由用户进程生成的审计记录一直保存在内存中的审计队列，直到可以对这些记录进行处理并写入审计追踪时为止。若要更改审计队列的大小，系统安全员可以使用 `audit queue size`。配置队列大小时，要对性能和风险加以权衡。如果队列太大，记录可在其中保留一段时间。如果系统失败，记录只要在队列中，就有可能丢失。但是，如果队列太小，就会经常处于充满状态，从而影响系统的总体性能；如果审计队列处于充满状态，生成审计记录的用户进程就会进入休眠状态。

以下是确定审计队列大小的几个原则。此外，还必须考虑要在您的节点上执行的审计量。

- 单个审计记录需要的内存是 424 字节；但是，当一条记录被写入数据页时，可以只有 22 字节。
- 在系统失败时可能丢失的审计记录的最大数目是审计队列的大小（记录的数目）加上 20。记录离开审计队列后将驻留在缓冲页上，直到将其写入磁盘上的当前审计表为止。每次最多只能将页中的 20 条记录刷新到磁盘（如果审计进程不是一直很忙，则可能更少）。
- 在系统审计表中，`extrainfo` 字段和包含名称的字段的可变的，所以包含完整名称信息的审计记录通常更大。

一页可容纳的审计记录的数目最少为 4，并可多达 80 以上。缺省审计队列大小为 100 条审计记录，所需内存大约为 42K。

审计

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

auditing 启用或禁用对 Adaptive Server 的审计。

automatic cluster takeover

摘要信息	
缺省值	1
有效值	0（启用），1（禁用）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

如果将 `automatic cluster takeover` 设置为 1，将允许启动的实例自动从突发总体集群故障中恢复。如果将 `automatic cluster takeover` 设置为 0，那么，除非包括 `--cluster_takeover` 参数，否则集群可能无法从突发集群故障切换恢复。

Cluster Edition 使用定额心跳和集群接管算法来确定应在何时执行集群接管。此算法使启动的实例能够区分以下两种情况：由于集群崩溃（在这种情况下适合于接管）而无法加入集群的情况，以及由于启动的实例未连接网络（这种情况下不适合于接管）而无法加入集群的情况。

如果禁用 `automatic cluster takeover`（将其设置为 0），则 Cluster Edition 会以建议消息的形式将该算法的结果写入错误日志，然后退出。

如果启用 `automatic cluster takeover`（将其设置为 1），则 Cluster Edition 将作为集群协调器启动，并恢复数据库。在启用了 I/O 防护的环境中，可确保此操作是安全操作。

在没有 I/O 防护的环境中，算法故障可能会导致数据损坏，因此您可以将该配置参数设置为 0 以禁用此算法。但是，没有 I/O 防护的环境存在数据损坏的风险，而禁用自动集群接管并不能减轻所有这些风险。

builtin date strings

摘要信息	
缺省值	0
值的范围	0 - 1
状态	动态
显示级别	
要求的角色	
配置组	查询调优

如果给定的字符串作为参数代替按时间顺序的值，则服务器会将其解释为 `datetime` 值（而不考虑其外观精度）。通过设置配置参数 `builtin date strings` 或设置 `builtin_date_strings` 选项，可以更改此默认行为。当设置这些选项时，服务器会将为按时间顺序的 `builtin` 指定的字符串解释为 `bigdatetime`。

caps per ccb

摘要信息	
缺省值	50
值的范围	5 - 50
状态	静态
显示级别	
要求的角色	
配置组	诊断

留作将来使用。

check password for digit

摘要信息	
缺省值	0（关闭）
值的范围	1（打开），0（关闭）
状态	动态
显示级别	10
要求的角色	系统安全员
配置组	与安全性相关的参数

系统安全员可以通知服务器使用全服务器范围内的配置参数 `check password for digit` 检查口令中是否至少包含一个字符或数字。如果设置了此参数，并不会影响现有的口令。

CIPC large message pool size

摘要信息	
缺省值	512
有效值	512 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

CIPC large message pool size 指定 CIPC 在启动时分配的大型消息缓冲区的数目。

CIPC regular message pool size

摘要信息	
缺省值	8192
有效值	2048 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

CIPC regular message pool size 指定 CIPC 在启动时分配的常规消息缓冲区的数目。

cis bulk insert array size

摘要信息	
缺省值	50
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

当执行从一个 Adaptive Server 到另一个 Adaptive Server 的数据批量传输时，CIS 会在内部将数据行放入缓冲区，然后要求 Open Client 批量库将它们作为一个块进行传输。数组的大小由 *cis bulk insert array size* 控制。

cis bulk insert batch size

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

`cis bulk insert batch size` 确定使用 `select into` 从源表向目标表进行批量复制时，一批可包含多少行。

如果将 `cis bulk insert batch size` 保留为 0，则会在一批中复制所有行。否则，按该参数指定的行数将行复制到目标表中后，服务器向目标服务器提出批量提交，从而提交该批处理。

如果收到正常客户端生成的批量复制操作（例如由 `bcp` 实用程序生成的操作），则该客户端预期将控制批量处理的大小，服务器将忽略该配置参数的值。

cis connect timeout

摘要信息	
缺省值	0
值的范围	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

`cis connect timeout` 确定成功建立 Client-Library 连接所等待的时间（以秒为单位）。

cis cursor rows

摘要信息	
缺省值	50
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

cis cursor rows 指定用于 cursor open 和 cursor fetch 操作的游标行数。增加该值意味着，在一次操作中可以获取更多的行。这会加快速度，但要求使用更多的内存。

cis idle connection timeout

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

cis idle connection timeout 将 Adaptive Server 配置为检查未使用的时间超过指定秒数的任何远程服务器 CIS 连接。Adaptive Server 将删除未使用的连接并重新分配其资源。

虽然指定的数字以秒为单位，管家任务至多每分钟唤醒一次，因此，空闲连接处于空闲状态的时间可能比配置的值长得多。如果空闲连接上的事务处于活动状态，则 Adaptive Server 不会删除这些连接；如果用户执行任何访问此连接的命令，则会自动重新建立连接。

cis packet size

摘要信息	
缺省值	512
值的范围	512 - 32768
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

cis packet size 指定 Tabular Data Stream™ (TDS) 包的大小，连接启动后，将在服务器和远程服务器之间交换这些包。

大多数系统上的缺省包大小为 512 字节，这对于大多数应用程序是足够的。但是，如果包大小更大些，或许能显著提高查询性能；当涉及 **text**、**unitext**、**image** 或批量数据时，效果尤其明显。

如果指定的包大小大于缺省值，则必须使用以下各项配置目标服务器，以允许可变长度的包大小：

- additional netmem
- maximum network packet size

cis rpc handling

摘要信息	
缺省值	0（关闭），缺省值为 1（用于 Cluster Edition）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

cis rpc handling 为远程过程调用 (RPC) 处理指定缺省方法。将 **cis rpc handling** 设置为 0 表示将 Adaptive Server 节点处理器设置为缺省的 RPC 处理机制。将该参数设置为 1 将强制 RPC 处理使用组件集成服务访问方法。请参见《组件集成服务用户指南》中的 **set cis rpc handling**。

cluster heartbeat interval

摘要信息	
缺省值	10
有效值	1 - 127
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

cluster heartbeat interval 控制集群实例用于发送和检查心跳状态的间隔。

如果为 cluster heartbeat interval 使用较低的值，将会缩短故障检测时间，但会增加由于瞬时问题（例如过载的 CPU）而导致误报故障的风险。将 cluster heartbeat interval 调优为较大的值可以减小误报故障的风险，但会增加检测故障所需的时间。

cluster heartbeat retries

摘要信息	
缺省值	1
有效值	1 - 127
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

cluster heartbeat retries 控制实例在进入故障模式之前重试失败的集群心跳的次数。

将 cluster heartbeat retries 调优为较低的值可缩短检测故障的时间，但会增加由于瞬时问题（例如过载的 CPU）而导致误报故障的风险。将 cluster heartbeat retries 调优为较大的值可以减小误报故障的风险，但会增加检测故障所需的时间。

cluster vote timeout

摘要信息	
缺省值	60
有效值	1 - 127
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

cluster vote timeout 控制某个实例在投票期间等待其它实例投票的最大时间量。实例只会等待它认为正在运行的实例。

将 **cluster vote timeout** 调优为较低的值可缩短故障切换时间，但会增加正在运行的实例被排除在新集群视图之外的风险。将 **cluster vote timeout** 调优为较大的值可减小正在运行的实例被排除在新集群视图之外的风险，但可能会增加故障切换时间。

compression memory size

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	物理内存

在将压缩转储装载到存档数据库中时使用。**compression memory size** 确定 Adaptive Server 用于解压缩压缩转储的内存池的大小（以 2KB 页为单位）。如果将 **compression memory size** 设置为 0，则不会创建池，并且无法装载压缩转储。

请参见《系统管理指南：卷 2》第 14 章“存档数据库访问”中的“创建压缩内存池”。

配置文件

摘要信息	
缺省值	0（关闭）
值的范围	以下值之一：0, verify、read、write 或 restore
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	一般信息

configuration file 指定当前使用的配置文件的位置。有关配置文件的完整说明，请参见第 60 页的“使用 sp_configure 及配置文件”。

在 sp_configure 输出中，“Run Value”列仅显示 10 个字符，因此输出可能无法显示配置文件的整个路径和名称。

cost of a logical io

摘要信息	
缺省值	2
值的范围	0 - 254
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

cost of a logical io 指定单个逻辑 I/O 的开销。

cost of a physical io

摘要信息	
缺省值	25
值的范围	0 - 254
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

cost of a physical io 指定单个物理 I/O 的开销。

cost of a cpu unit

摘要信息	
缺省值	1000
值的范围	1 - 65534
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

cost of a cpu unit 指定单个 CPU 操作的开销。

优化程序中串行计划的开销采用以下公式描述：

$$\text{Cost} = \text{PIO} \times \text{estimated\_pio} + \text{LIO} \times \text{estimated\_lio} + 100 \times \text{estimated\_cpu} / \text{CPU}$$

其中的各个缺省值为：

- *estimated_pio* = 25
- *estimated_lio* = 2
- *estimated_cpu* = 1000

如果您的 Adaptive Server 有足够的内存，则所有表都将存在于内存中，则且可以将 **cost of a physical io** 的值设置为 0。

如果您的 CPU 速度足够快，因此 **cost of a cpu unit** 的值不是问题，请使用此公式来确定 CPU 的开销，该开销组合了 2 个 LIO 和 25 个 PIO（缺省值）：

$$\text{CPU} \times 100 / \text{configuration\_value}$$

configuration_value 的缺省值为 1000。

当您增加 **cost of a cpu unit** 的值时，此公式将减少 CPU 对开销的影响。

cpu accounting flush interval

摘要信息	
缺省值	200
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`cpu accounting flush interval` 以计算机时钟周期（非 Adaptive Server 时钟周期）为单位，指定 Adaptive Server 等待多长时间后，才将每个用户的 CPU 使用率统计信息从 `sysprocesses` 刷新到 `syslogins`（用于收费退回式会计的一个过程）。

用户登录到 Adaptive Server 后，服务器开始累计 `sysprocesses` 中此用户进程的 CPU 使用率。当用户从 Adaptive Server 注销，或超过 `cpu accounting flush interval` 的值时，累计的 CPU 使用率统计信息从 `sysprocesses` 刷新到 `syslogins`。这些统计信息不断在 `syslogins` 中累计，直至您清除总计为止。使用 `sp_reportstats` 显示 `syslogins` 中的当前总计。

报告运行类型决定了 `cpu accounting flush interval` 的设置值。如果报告每月运行一次，则将 `cpu accounting flush interval` 设置为一个相对高的值。如果报告运行频率很低，`syslogins` 中的数据是否经常更新并不重要。

但是，如果对 `syslogins` 中的 `totcpu` 列执行定期即席选择以确定进程的 CPU 使用率，请将 `cpu accounting flush interval` 设置为较低的值，以增加 `syslogins` 中的数据在您执行选择时保持最新的可能性。

如果将 `cpu accounting flush interval` 设置为较低的值，将可能导致锁管理程序错误地将进程识别为潜在死锁牺牲品。当锁管理程序检测到一个死锁时，它将检查每个争用进程所累积的 CPU 时间。将选择具有较少时间的进程作为死锁牺牲品，并且锁管理程序终止运行该进程。此外，如果将 `cpu accounting flush interval` 设置为较小的值，则会更频繁地初始化存储进程 CPU 使用率信息的任务处理程序，由此使进程累计的 CPU 时间看起来比实际少。这样，锁管理程序可能选择某个进程作为死锁牺牲品，但该进程实际上累积的 CPU 时间比争用进程多。

如果根本不希望报告 CPU 使用率，请将 `cpu accounting flush interval` 设置为其最大值。这样就减少了 `syslogins` 的更新次数，并减少了必须将其页面写入磁盘的次数。

cpu grace time

摘要信息	
缺省值	500
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

cpu grace time 和 time slice 参数一起使用时可指定：用户进程在被 Adaptive Server 抢占，并因时间片错误而被终止之前，在不放弃 CPU 的情况下可以运行的最长时间。cpu grace time 的单位是 sql server clock tick length 所定义的时间周期。请参见第 221 页的“sql server clock tick length”。

当一个进程超过 cpu grace time 时， Adaptive Server 通过将此进程从内部队列删除来“影响”它。该进程即被注销，而 Adaptive Server 不受影响。这样可防止失去控制的进程独占 CPU。如果任何用户进程受到影响，可以通过增加 cpu grace time 的值临时修复此问题。但应确保问题的症结在于，某个进程的完成时间超过了 cpu grace time 的当前值，而不是某个进程失去了控制。

临时增大 cpu grace time 的值只是一种变通手段，并非永久性解决方案，因为它可能会导致新的问题；请参见第 233 页的“time slice”。有关任务调度的更详细论述，另请参见 Performance and Tuning Series: Basics（《性能和调优系列：基础知识》）中的第 4 章“Using Engines and CPUs”（使用引擎和 CPU）。

current audit table

摘要信息	
缺省值	1
值的范围	0 - 8
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

current audit table 创建 Adaptive Server 将审计行写入其中的表。系统安全员可以使用以下语法更改当前审计表：

```
sp_configure "current audit table", n
[, "with truncate"]
```

其中 n 是确定当前新审计表的一个整数，如下所示：

- 1 表示 sysaudits_01， 2 表示 sysaudits_02，依此类推，最大可为 8。
- 0 通知 Adaptive Server 将当前审计表设置为下一个表。例如，如果系统中有三个审计表， sysaudits_01、 sysaudits_02 和 sysaudits_03， 则 Adaptive Server 会将当前审计表设置为：
 - 2， 如果当前审计表是 sysaudits_01
 - 3， 如果当前审计表是 sysaudits_02
 - 1， 如果当前审计表是 sysaudits_03

"with truncate" 指定 Adaptive Server 应截断尚不为空的新表。如果没有指定该选项而表又不为空，sp_configure 将失败。

注释 如果 Adaptive Server 截断了当前的审计表，而且您没有将数据存档，则该表中的审计记录将丢失。确保在使用 with truncate 选项之前将审计数据存档。

若要执行 sp_configure 以更改当前的审计表，ssso_role 必须为活动状态。可以编写一个阈值过程来自动更改当前审计表。

deadlock checking period

摘要信息	
缺省值	500
值的范围	0 - 2147483
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序

deadlock checking period 指定了在 Adaptive Server 对等待释放一个锁的进程开始进行死锁检查之前的最小的时间量（以毫秒为单位）。对于没有遇到死锁或遇到的死锁很少的应用程序，死锁检查是消耗时间的开销；随着必须等待一个锁的锁请求百分比的增加，这种开销还会增加。

如果将 deadlock checking period 设置为非零值 (n)，则在进程等待至少 n 毫秒后，Adaptive Server 会启动死锁检查。例如，输入如下命令，即可让进程在执行每一次死锁检查前，至少要针对一个锁等待 700 毫秒：

```
sp_configure "deadlock checking period", 700
```

如果将 deadlock checking period 设置为 0，则当每个进程开始等待锁时，Adaptive Server 都会启动死锁检查。任何比一个时钟周期中的毫秒数小的值都被视为 0。请参见第 221 页的“sql server clock tick length”。

如果将 deadlock checking period 配置为较大值，则会导致在检测出死锁前更长的延迟。但是，因为在这段时间过去之前 Adaptive Server 会同意大多数锁请求，所以可以避免对这些锁请求进行开销很高的死锁检查。如果应用程序死锁不频繁，请将 deadlock checking period 设置为较高的值。否则，缺省值 500 应已足够。

可以使用 sp_sysmon 来确定系统中死锁的频率，以及 deadlock checking period 的最佳设置。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

deadlock pipe active

摘要信息	
缺省值	0
值的范围	0 - 1
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

`deadlock pipe active` 控制 Adaptive Server 是否收集死锁消息。如果同时启用了 `deadlock pipe active` 和 `deadlock pipe max messages`，则 Adaptive Server 将收集每个死锁的文本。使用 `monDeadLock` 来检索这些死锁消息。

deadlock pipe max messages

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

`deadlock pipe max messages` 确定 Adaptive Server 存储的每个引擎的死锁消息数。`monSQLText` 表中的消息总数等于 `sql text pipe max messages` 的值与正在运行的引擎数的乘积。

deadlock retries

摘要信息	
缺省值	5
值的范围	0 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

deadlock retries 指定了在索引页拆分或聚合期间发生死锁时事务能够尝试获得锁的次数。

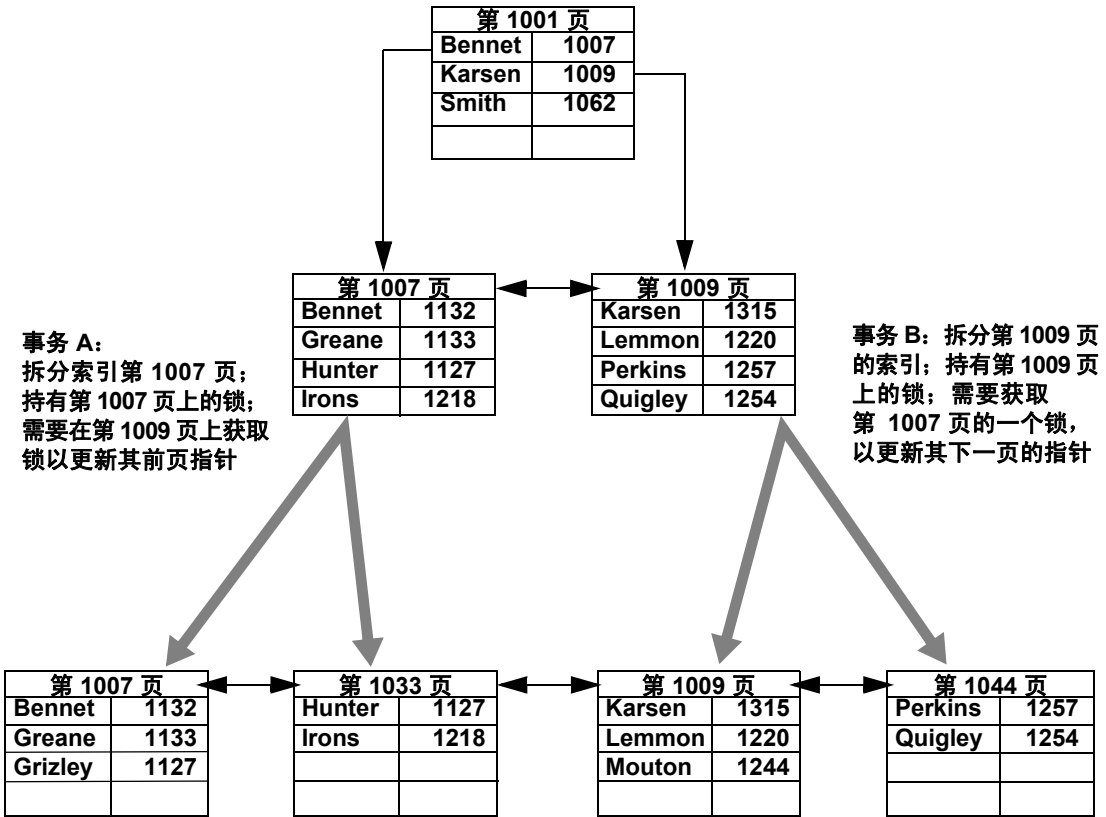
例如，图 5-1 阐释了以下情形：

- 事务 A 锁定了 1007 页，并且需要在 1009 页上获取一个锁以便为页面拆分更新页面指针。
- 事务 B 也正在插入一个索引行，该索引行造成页面拆分、持有 1009 页上的锁和需要在 1007 页上获得锁。

在这种情况下，Adaptive Server 并不立刻选择一个进程作为死锁牺牲品，而是放弃某一事务的索引锁。这样做常常使其它事务完成和释放它的锁。

对于放弃锁定尝试的事务，将从根页起重新扫描索引，然后重新尝试页拆分操作直到达到 deadlock retries 指定的次数为止。

图 5-1：聚簇索引中页拆分期间的死锁



`sp_sysmon` 报告有关死锁和重试的信息。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

default character set id

摘要信息	
缺省值	1
值的范围	0 - 255
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	语言

`default character set id` 指定服务器所使用的缺省字符集的编号。缺省值是在安装时设置的，以后可以使用 Sybase 安装实用程序进行更改。请参见第9章“配置字符集、排序顺序和语言”。

default database size

摘要信息	
缺省值	3MB
值的范围	2 ^a - 10000 a. 是由服务器逻辑页大小确定的最小值。
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

`default database size` 设置在没有任何大小参数的情况下发出 `create database` 后，在缺省情况下分配给一个新的用户数据库的空间（以兆字节为单位）。`create database` 语句给定的数据库大小优先于此配置参数设置的值。

如果 Adaptive Server 上大部分的新数据库要求的大小都大于一个逻辑页，则最好增加缺省值。

注释 如果更改 `model` 数据库，您还必须增加 `default database size`，因为 `create database` 命令将复制 `model` 来创建新的用户数据库。

default exp_row_size percent

摘要信息	
缺省值	5
值的范围	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

default exp_row_size percent 保留的空间用于 DOL 锁定表中的扩展更新，目的是减少行转移。“扩展更新”指对数据行进行的增加行长度的任何更新。允许空值的数据行或包含可变长度列的数据行可能会进行扩展更新。在 DOL 锁定表中，如果增加数据行的大小以致该页无法继续容纳，扩展更新会要求行转移。

缺省值将留出 5% 的可用数据页大小以用于扩展更新。由于 DOL 锁定表的页上有 2002 字节可用于数据存储，所以将为扩展保留 100 字节。该值仅应用于具有长度可变列的表中的页。

将 **default exp_row_size percent** 设置为 0 意味着所有的页都完全填满，没有剩余空间可用于扩展更新。

如果没有使用 **create table** 来明确提供 **exp_row_size** 或使用 **sp_chgattribute** 进行设置，则将 **default exp_row_size percent** 应用于带有可变长度列的 DOL 锁定表。如果使用 **create table** 提供了一个值，则该值将优先于配置参数的设置。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

default fill factor percent

摘要信息	
缺省值	0
值的范围	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

default fill factor percent 确定当 Adaptive Server 对已有数据创建新索引时每个索引页的充满度，除非 **create index** 语句中已指定了填充因子。

fillfactor 百分比仅在创建了索引后才有意义。随着数据变化，页的填充程度不会维持任何特定水平。

default fill factor percent 影响：

- 数据使用的存储空间量 — Adaptive Server 创建聚簇索引时重新分配数据。
- 性能 — 拆分页使用 Adaptive Server 的资源。

通常不要更改 **default fill factor percent**，因为可在 **create index** 命令中替换其值。请参见《参考手册：命令》中的 **create index**。

default language id

摘要信息	
缺省值	0
值的范围	0 - 32767
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	语言

default language id 是用于显示系统消息的语言（除非用户已选择了服务器上的其它可用语言）的编号。**us_english** 的 ID 始终为 NULL。其它语言在添加时都指派了唯一的号码。

default network packet size

摘要信息	
缺省值	2048
值的范围	512 - 65024
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、网络通信、用户环境

`default network packet size` 为所有 Adaptive Server 用户配置缺省包大小。可以将 `default network packet size` 的值设置为 512 字节的任何倍数；但不是 512 偶数倍的值将向下舍入。

使用缺省包大小登录的所有用户的内存都是从 Adaptive Server 内存池分配的，内存池使用 `total logical memory` 进行设置。Adaptive Server 启动时分配该内存以用于网络包。

每个 Adaptive Server 用户连接都使用：

- 一个读缓冲
- 一个消息缓冲
- 一个写缓冲

其中的每个缓冲区都需要 `default network packet size` 字节。分配给网络包的内存总量是：

$(\text{用户连接数} + \text{工作进程数}) * 3 * \text{缺省网络包大小}$

例如，如果将 `default network packet size` 设置为 1024 字节，并且有 50 个用户连接和 20 个工作进程，则要求的网络内存是：

$(50 + 20) * 3 * 1024 = 215040$ 字节

如果增加 `default network packet size`，则还必须将 `max network packet size` 增加到至少与前者一样大。如果 `max network packet size` 的值大于 `default network packet size` 的值，则应增大 `additional network memory` 的值。请参见第 73 页的“[additional network memory](#)”。

可以使用 `sp_sysmon`，了解 `default network packet size` 参数的更改如何影响网络 I/O 管理和任务切换。例如，尝试增加 `default network packet size`，然后检查 `sp_sysmon` 输出，了解这样的更改如何影响较大批处理的 `bcp`。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

在登录时请求较大的包大小

大多数客户端程序（如 `bcp` 和 `isql`）的缺省包大小都设置为 512 字节。如果更改了缺省包大小，客户端必须在它们连接时请求较大的包大小。使用 Adaptive Server 客户端程序的 `-A` 标志请求较大的包大小。例如：

```
isql -A2048
```


default sortorder id

摘要信息	
缺省值	50
值的范围	0 - 255
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	语言

default sortorder id 是在服务器上作为缺省值安装的排序顺序号。若要更改缺省排序顺序，请参见第9章“配置字符集、排序顺序和语言”。

default unicode sortorder

摘要信息	
缺省值	binary
值的范围	当前未使用
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Unicode

default unicode sortorder 是一个字符串参数，该参数唯一定义服务器上安装的缺省 Unicode 排序顺序。若要更改 Unicode 缺省排序顺序，请参见第9章“配置字符集、排序顺序和语言”。

default XML sortorder

摘要信息	
缺省值	binary
值的范围	(当前未使用)
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Unicode

default XML sortorder 是一个字符串参数，该参数定义 XML 引擎使用的排序顺序。之所以使用字符串参数而非数字参数，目的是为了确保 ID 的唯一性。请参见《Adaptive Server Enterprise 中的 XML 服务》中的第6章“i18N 的 XML 支持”。

deferred name resolution

摘要信息	
缺省值	0（禁用）
值的范围	0 到 1
状态	动态
要求的角色	系统管理员
配置组	查询调优

如果 deferred name resolution 处于活动状态 (1)，则会将延迟名称解析以全局方式应用于所有服务器连接；将使用延迟名称解析创建您在服务器中创建的所有过程。

因此，将会在不解析存储过程内引用的对象的情况下创建存储过程，从而将对象解析处理推迟到执行时进行。请参见 《Transact-SQL 用户指南》中的第 17 章 “使用存储过程”

disable character set conversions

摘要信息	
缺省值	0（启用）
有效值	0（启用）， 1（禁用）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	语言

将 disable character set conversions 更改为 1 会关闭用于客户端和 Adaptive Server 间进行数据移动的字符集转换功能。缺省情况下，对于使用与服务器不同的字符集的客户端，Adaptive Server 会对移入、移出的数据执行转换。例如，如果有些客户端使用 Latin-1 (iso_1)，而 Adaptive Server 使用 Roman-8 (roman8) 作为其缺省字符集，则来自这些客户端的数据在被装载到 Adaptive Server 时，会被转换为 Roman-8。对于使用 Latin-1 的客户端，数据被发送到客户端时被重新转换；如果客户端使用的字符集与 Adaptive Server 使用的字符集相同，则不转换数据。

通过设置 disable character set conversions，可以请求不进行转换。例如，如果所有客户端都使用某个给定字符集，而您希望 Adaptive Server 采用该字符集存储所有数据，请将 disable character set conversions 设置为 1，这时就不会发生任何转换。

disable disk mirroring

摘要信息	
缺省值	1
有效值	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	磁盘 I/O

disable disk mirroring 启用或禁用 Adaptive Server 的磁盘镜像。这是一个全局变量；Adaptive Server 在该配置参数设置为 1 并重新启动 Adaptive Server 后将不执行任何磁盘镜像操作。如果将 disable disk mirroring 设置为 0，则会启用磁盘镜像。

注释 如果针对故障切换配置了 Adaptive Server，则必须禁用磁盘镜像。

disk i/o structures

摘要信息	
缺省值	256
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	磁盘 I/O、内存使用

disk i/o structures 指定 Adaptive Server 在启动时分配的磁盘 I/O 控制块的初始数目。

在 Adaptive Server 可以启动进程的 I/O 请求之前，用户进程需要一个磁盘 I/O 控制块。在 Adaptive Server 启动时，预分配用于磁盘 I/O 控制块的内存。为了最大程度地减少出现磁盘 I/O 结构不够用的情况，您应将 disk i/o structures 配置为操作系统允许的最高值。关于并行磁盘 I/O 的信息，请参见操作系统文档。

使用 sp_sysmon 确定是否要分配更多的磁盘 I/O 结构。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。可以将 max async i/os per server 配置参数的值设置为与 disk i/o structures 相同的值。请参见第 144 页的“max async i/os per server”。

DMA object pool size

摘要信息	
缺省值	4096
有效值	2048 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

DMA object pool size 指定 CIPC 在启动时分配的 DMA（直接内存访问）对象的数目。

dtm detach timeout period

摘要信息	
缺省值	0（分钟）
有效值	0 - 2147483647（分钟）
状态	动态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理

dtm detach timeout period 设置分布式事务分支可以处于分离状态的时间（以分钟为单位）。在一些 X/Open XA 环境中，事务可能与它的控制线程分离（通常会附加到另一个控制线程）。Adaptive Server 允许事务保留在分离状态的时间长度是由 dtm detach timeout period 指定的。如果超过此时间，Adaptive Server 将回退分离的事务。

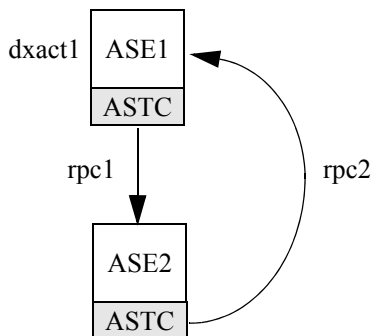
dtm lock timeout period

摘要信息	
缺省值	300（秒）
有效值	1 - 2147483647（秒）
状态	动态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理

`dtm lock timeout period` 用于设置：在等待锁定资源变为可用时，一个分布式事务分支等待的最长时间（以秒为单位）。这段时间过去后，Adaptive Server 认为该事务处于死锁状态，于是回退那些触发了死锁的事务分支。最终会回退整个分布式事务。

如果分布式事务将事务传播给远程服务器，或远程服务器将事务传播回源服务器，分布式事务就可能潜在死锁它们本身。图 5-2 中显示了这种情况。分布式事务 “dxact1” 的工作通过 “rpc1” 传播到 Adaptive Server 2。然后，Adaptive Server 2 通过 “rpc2” 将该事务传回协调服务器。“rpc2” 和 “dxact1” 虽共享相同的 `gtrid`，但具有不同的分支限定符，因此，它们不能共享相同的事务资源。如果 “rpc2” 正在等待 “dxact1” 持有的锁，则会发生死锁的情况。

图 5-2：分布式事务死锁



Adaptive Server 无法检测服务器之间的死锁。相反，它依赖于 `dtm lock timeout period`。在图 5-2 中，当 `dtm lock timeout period` 到期后，为 “rpc2” 创建的事务即会中止。这会使 Adaptive Server 2 报告其工作失败，并且 “dxact1” 最终也会被完全中止。

`dtm lock timeout period` 的值仅适用于分布式事务。本地事务可以使用通过全服务器范围内的 `lock wait period` 参数设置的锁定超时期限。

注释 Adaptive Server 不使用 `dtm lock timeout period` 来检测系统表上的死锁。

dump on conditions

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	组诊断

dump on conditions 确定 Adaptive Server 在符合 maximum dump conditions 中指定的条件时是否在共享内存中生成数据的转储。

注释 dump on conditions 参数仅供 Sybase 技术支持部门使用。除非有 Sybase 技术支持部门的指导，否则不要修改此参数。

dynamic allocation on demand

摘要信息	
缺省值	1（打开）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、物理内存

dynamic allocation on demand 确定何时针对动态内存配置参数的更改分配内存。

如果 dynamic allocation on demand 设置为 1，内存只根据其所需进行分配。这意味着，如果将 number of user connections 的配置从 100 更改为 200，则只在用户连接到服务器时才为每一用户增加内存。Adaptive Server 持续增加内存，直到达到用于用户连接的新的最大值。

如果 dynamic allocation on demand 设置为 0，则立即分配任何动态配置更改所需的所有内存。即，如果将用户连接数从 100 更改为 200，则立即分配这额外 100 个用户连接所需的内存。

enable backupserver HA

摘要信息	
缺省值	1
有效值	0（启用），1（禁用）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

如果将 **enable backupserver HA** 设置为 1，将会为集群启动高可用性 Backup Server。如果将 **enable backupserver HA** 设置为 0，则会在集群上禁用高可用性 Backup Server。

enable cis

摘要信息	
缺省值	1（打开）
有效值	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

enable cis 启用或禁用组件集成服务。

enable DTM

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	静态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理、SQL Server 管理

`enable DTM` 启用或禁用 Adaptive Server 分布式事务管理 (DTM) 功能。如果启用了 DTM，则可以使用 Adaptive Server 作为 X/Open XA 和 MSDTC 系统中的资源管理器。必须重新启动服务器以使此参数生效。有关在 X/Open XA 环境中使用 Adaptive Server 的详细信息，请参见《适用于 CICS、Encina 和 TUXEDO 的 XA 接口集成指南》。有关在 MSDTC 环境中的事务的信息以及有关 Adaptive Server 本地事务协调服务的信息，请参见 `Using Adaptive Server Distributed Transaction Management Features`（《使用 Adaptive Server 分布式事务管理功能》）。

注释 `enable DTM` 的许可证信息和运行值是相互独立的。无论您是否具有 DTM 许可证，在重新启动 Adaptive Server 后，运行值和配置值都会设置为 1。除非安装有效的许可证，否则不能运行 DTM。如果您没有安装有效的许可证，则 Adaptive Server 将记录一条错误消息，并且不会激活该功能。有关安装许可证密钥的信息，请参见所用平台的安装指南。

enable encrypted columns

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	与安全性相关的参数

`enable encrypted columns` 启用加密列。

除非您购买并在服务器上安装和注册了 ASE_ENCRYPTION 许可证，否则将无法设置 `enable encrypted columns`。任何尝试在没有此类许可的情况下设置该参数的行为都将导致出现消息 10834：

```
Configuration parameter 'enable encrypted columns'
cannot be enabled without license 'ASE_ENCRYPTION'
```

注释 使用加密列会将使用的逻辑内存增加 8198 千字节。

enable enterprise java beans

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Java 服务

enable enterprise java beans 启用和禁用 Adaptive Server 数据库中的 EJB Server。除非 Adaptive Server 启用 EJB 服务器，否则不能使用 EJB 服务器。

注释 **enable java beans** 的许可证信息和运行值是相互独立的。无论是否有 Java 许可证，在重新启动 Adaptive Server 后，运行值和配置值都设置为 1。除非有许可证，否则不能运行 EJB Server。如果您没有安装有效的许可证，则 Adaptive Server 将记录一条错误消息，并且不会激活该功能。有关安装许可证密钥的信息，请参见所用平台的安装指南。

enable file access

摘要信息	
缺省值	1（打开）
有效值	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

enable file access 启用通过代理表访问外部文件系统。需要 ASE_XFS 的许可证。

enable full-text search

摘要信息	
缺省值	1
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	组件集成服务

enable full-text search 启用增强型全文本搜索服务。需要 ASE_EFTS 的许可证。

enable HA

摘要信息	
缺省值	0（关闭）
值的范围	0 - 2
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

将 **enable HA** 设置为 1，以将 Adaptive Server 配置为主动 - 主动高可用性子系统 中的协同服务器。将 **enable HA** 设置为 2，以将 Adaptive Server 配置为主动 - 被动高可用性子系统 中的协同服务器。

Adaptive Server 使用 Sybase 故障切换与高可用性子系统进行交互。将 **enable HA** 设置为 1 后，才能运行 *installhasvss* 脚本（Windows 上为 *insthasv*），此脚本会安装用于 Sybase 故障切换的系统过程。

注释 **enable HA** 的许可证信息和运行值是相互独立的。无论是否有 Sybase 故障切换许可证，在重新启动 Adaptive Server 后，运行值和配置值都将设置为 1。除非有许可证，否则无法运行 Sybase 故障切换。如果您没有安装有效的许可证，则 Adaptive Server 将记录一条错误消息，并且不会激活该功能。有关安装许可证密钥的信息，请参见所用平台的安装指南。

将 enable HA 设置为 1 或 2 并不意味着 Adaptive Server 已配置为可在高可用性系统中工作。必须执行《在高可用性系统中使用 Sybase 故障切换》中所述的步骤，才可将 Adaptive Server 配置为高可用性系统中的协同服务器。

当 enable HA 设置为 0 时，不能进行 Sybase 故障切换配置，也不能运行 *installhasvss*（Windows 上为 *insthasv*）。

enable housekeeper GC

摘要信息	
缺省值	1（打开）
值的范围	0 - 5
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

管家碎片收集任务在仅数据锁定表上执行空间回收操作。如果用户任务将行从 DOL 锁定表中删除，则为管家安排一个任务以检查数据和索引页上提交的删除。

管家碎片收集任务由 enable housekeeper GC 控制。请参见 Performance and Tuning Series: Basics（《性能和调优系列：基础知识》）中的第 3 章“Using Engines and CPUs”（使用引擎和 CPU）。

enable housekeeper GC 的有效值如下：

- 0 — 禁用管家碎片收集任务，但启用 delete 命令的消极碎片收集。必须使用 reorg reclaim_space 释放空白页。这是消耗最少的选项，而且对性能的影响也最小，但如果出现许多空白页累计的情况，则可能会导致性能问题。Sybase 建议您不要使用此值。
- 1 — 为管家碎片收集任务和 delete 命令启用消极碎片收集。如果累计的空白页数超过了应用程序所允许的数量，应考虑使用选项 4 或 5。可以使用 optdiag 实用程序获取空白页统计信息。
- 2 — 留作将来使用。
- 3 — 留作将来使用。
- 4 — 为管家碎片收集任务和 delete 命令启用积极碎片收集。此选项效率最高，但 delete 命令会消耗很多资源。如果 DOL 锁定表上的删除操作在一个批处理中，此选项最为理想。

- 5 — 为管家启用积极碎片收集，并为 `delete` 命令启用消极碎片收集。对于删除操作，此选项比选项 4 消耗的资源少。此选项适用于并行事务导致删除操作的情况。

`sp_sysmon` 报告管家碎片收集任务执行空间回收的频率以及回收的页数。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

enable i/o fencing

摘要信息	
缺省值	0
有效值	0（启用）， 1（禁用）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

如果将 `enable i/o fencing` 设置为 1，则会为支持 SCSI-3 持久组保留 (PGR) 标准的每个数据库设备启用 I/O 防护。

enable java

摘要信息	
缺省值	0（禁用）
值的范围	0（禁用）， 1（启用）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Java 服务

`enable java` 在 Adaptive Server 数据库启用和禁用 Java。只有服务器启用了 Java 才能安装 Java 类或执行任何 Java 操作。

注释 `enable java` 的许可证信息和运行值是相互独立的。无论是否有 java 许可证，在重新启动 Adaptive Server 后，运行值和配置值都设置为 1。除非有许可证，否则不能运行 Java。如果您没有安装有效的许可证，则 Adaptive Server 将记录一条错误消息，并且不会激活该功能。有关安装许可证密钥的信息，请参见所用平台的安装指南。

enable job scheduler

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

enable job scheduler 确定当 Adaptive Server 启动时，是否启动 Job Scheduler。

enable ldap user auth

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）— 只允许 syslogins 鉴定。 1（打开）— 允许 LDAP 和 syslogins 鉴定。 2（打开）— 只允许 LDAP 鉴定。
状态	动态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	与安全性相关的参数

当 enable ldap user auth 为 1 时，Adaptive Server 将搜索 LDAP 服务器以对每个用户进行鉴定。如果 LDAP 鉴定失败，Adaptive Server 将会搜索 syslogins 来鉴定用户。当您将用户从 Adaptive Server 鉴定迁移到 LDAP 鉴定时，请使用级别 1。

enable literal autoparam

摘要信息	
缺省值	0
值的范围	0（启用），1（禁用）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	查询调优

enable literal autoparam 在全服务器范围内启用和禁用文字参数化。

enable logins during recovery

摘要信息	
缺省值	1
值的范围	0（启用）， 1（禁用）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	与安全性相关的参数

enable logins during recovery 确定在数据库恢复过程中是否允许使用非系统管理员登录名。值 1 表示在恢复过程中允许使用这些登录名，值 0 表示在恢复过程中不允许使用这些登录名（也就是说，只有系统管理员才能登录到 Adaptive Server）。

enable merge join

摘要信息	
缺省值	2
值的范围	0 — 在服务器级禁用合并连接。 1 — 在服务器级启用合并连接。 2 — 在服务器级将合并连接设置为其缺省值。
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

enable merge join 可在服务器级启用或禁用合并连接。
合并连接的缺省值取决于 optimization goal 配置参数的当前值：

optimization goal 的值	合并连接的缺省值
allrows_mix	打开
allrows_dss	打开
allrows_oltp	关闭

enable metrics capture

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

enable metrics capture 使 Adaptive Server 能够在服务器级捕获指标。即席语句的指标会被捕获到系统目录中；存储过程中的语句的指标则保存在过程高速缓存中。

enable monitoring

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

enable monitoring 控制 Adaptive Server 是否收集监控表数据。**enable monitoring** 充当主开关，用于确定是否启用任何监控配置参数。

enable pam user auth

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）— 只允许 syslogins 鉴定。 1（打开）— 允许 PAM 和 syslogins 鉴定。 2（打开）— 只允许 PAM 鉴定。
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

`enable pam user auth` 控制使用可插入鉴定模块 (PAM) 鉴定用户的能力。

当 `enable pam user auth` 设置为 1 时，Adaptive Server 使用 PAM 提供程序鉴定每一个用户。如果 PAM 鉴定失败，Adaptive Server 则会搜索 `syslogins` 来鉴定用户。当您从 Adaptive Server 鉴定迁移到 PAM 鉴定时，请使用级别 1。

enable pci

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）， 1（打开）， 2（打开，但操作系统设置优先）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	用户环境

`enable pci` 为 Adaptive Server 启用或禁用 Java PCI Bridge。

注释 除非有 Sybase 技术支持部门的指示，否则不使用设置 “2”（打开，但操作系统设置优先）。此设置将在可能不完全或正确支持 PCI 功能的操作系统版本上启用 PCI Bridge。

enable query tuning mem limit

摘要信息	
缺省值	1（打开）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	查询调优

`enable query tuning mem limit` 启用查询调优内存限制。

enable query tuning time limit

摘要信息	
缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	Intermediate
显示级别	Intermediate
要求的角色	系统管理员
配置组	查询调优

enable query tuning time limit 启用查询调优时间限制。

enable real time messaging

摘要信息	
缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

enable real time messaging 启用实时消息传送服务。

enable rep agent threads

摘要信息	
缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、RepAgent 线程管理

enable rep agent threads 启用 Adaptive Server 内的 RepAgent 线程。

其它步骤也要求启用复制。有关详细信息，请参见 Replication Server 文档。

enable row level access control

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	与安全性相关的参数

`enable row level access control` 启用行级访问控制。启用安全服务许可证密钥后，才能配置 `enable row level access control`。

enable semantic partitioning

摘要信息	
缺省值	0
值的范围	0（启用）， 1（禁用）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`enable semantic partitioning` 在 Adaptive Server 中启用非循环分区（如列表分区、散列分区和域分区）。要想使用这些分区方案，必须首先获得相应的许可证。

enable sort-merge join and JTC

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

在 Adaptive Server 处于兼容模式时使用。启用之后，当 Adaptive Server 在兼容模式下编译查询时， enable sort-merge join and JTC 允许查询处理器选择 sort merge 或 nested loop join。enable sort-merge join and JTC 启用连接传递闭包 (JTC)，从而使 15.0 之前的版本的查询处理器能够使用其它连接子句。

有关兼容模式的详细信息，请参见 《迁移技术指南》。

enable sql debugger

摘要信息	
缺省值	1（打开）
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

启用和禁用使您能够逐步调试 T-SQL 代码的 Adaptive Server SQL 调试程序。

enable ssl

摘要信息	
缺省值	0（关闭）
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	与安全性相关的参数

enable ssl 启用或禁用基于安全套接字层会话的安全性。

enable stmt cache monitoring

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理
配置组	监控

enable stmt cache monitoring 允许或禁止 Adaptive Server 收集有关语句高速缓存的监控信息。启用之后，monStatementCache 和 monCachedStatement 将显示有效数据。

enable surrogate processing

摘要信息	
缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Unicode

激活处理并保持 Unicode 数据中代理对的完整性。如果禁用 enable surrogate processing，服务器将忽略 Unicode 数据中存在的代理对，并且所有保持代理对完整性的代码都将被忽略。这可提高性能，但会限制可在数据中出现的 Unicode 字符范围。

enable unicode conversion

摘要信息	
缺省值	1
值的范围	0 — 仅使用内置字符集转换。 1 — 使用内置转换。如果找不到内置转换，Adaptive Server 将使用 Unilib 字符转换。 2 — 使用适当的 Unilib 转换。
状态	动态
显示级别	Comprehensive

摘要信息

要求的角色	系统管理员
配置组	语言、Unicode

enable unicode conversion 为 char、varchar 和 text 数据类型激活使用 Unilib 的字符转换。

enable unicode normalization**摘要信息**

缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Unicode

激活 Unilib 字符规范化。规范化进程修改数据，以使得对于给定顺序的抽象字符，在数据库中只有唯一的表示方法。一般情况下，后跟组合读音符的字符会被预组合形式所取代。

将 enable unicode normalization 设置为 1 以使用可增强所有引入 Unicode 数据规范性的内置进程。如果该参数被禁用（设置为 0），规范化步骤将被忽略，并由客户端代码而不是服务器负责规范化。如果禁用规范化，所有客户端必须都使用相同的表示方法向服务器提供 Unicode 数据，性能才会有所提高。

注释 规范化禁用后，可重新启用。这样可防止非规范化数据进入数据库。

enable webservices**摘要信息**

缺省值	0
值的范围	0（启用），1（禁用）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

启用 Web 服务。

enable xact coordination

摘要信息	
缺省值	1（打开）
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理

enable xact coordination 启用或禁用 Adaptive Server 事务协调服务。此参数设置为 1（打开）时就启用了协调服务，服务器能够将事务传播到其它 Adaptive Server。在事务执行远程过程调用 (RPC) 以更新另一个服务器中的数据时，或者事务使用组件集成服务 (CIS) 更新另一个服务器中的数据时，就可能发生此情况。事务协调服务确保对远程 Adaptive Server 数据的更新能够随原始事务提交或通过原始事务回退。

如果该参数设置为 0（关闭）， Adaptive Server 就不调整远程服务器的工作。虽然事务仍然能够使用 CIS 执行 RPC 和更新数据，但是 Adaptive Server 不能确保在远程服务器发生系统故障时，远程事务还能通过原始事务进行回退或远程工作能够和原始事务一起提交。这与 Adaptive Server 12.x 之前的版本的行为一致。

enable xml

摘要信息	
缺省值	0
值的范围	0（启用）， 1（禁用）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

启用 XML 服务。

engine memory log size

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	
要求的角色	
配置组	物理内存

engine memory log size 只用于诊断目的，在生产环境中没有用。除非 Sybase 技术支持部门另有要求，否则应将此参数保留为缺省设置。

errorlog pipe active

摘要信息	
缺省值	0
值的范围	0 - 1
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

errorlog pipe active 控制 Adaptive Server 是否收集错误日志消息。如果同时启用 **errorlog pipe active** 和 **errorlog pipe max messages**，则 Adaptive Server 将收集发送到错误日志的所有消息。使用 **monErrorLog** 来检索这些错误日志消息。

errorlog pipe max messages

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

errorlog pipe max messages 确定 Adaptive Server 存储的每个引擎的错误日志消息数。monSQLText 表中的消息总数等于 sql text pipe max messages 的值与正在运行的引擎数的乘积。

esp execution priority

摘要信息	
缺省值	8
值的范围	0 - 15
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	扩展存储过程

esp execution priority 设置执行 ESP 的 XP Server 线程的优先级。ESP 会长时间大量占用 CPU。此外，因为 XP Server 与 Adaptive Server 位于同一计算机上，所以 XP Server 可能会影响 Adaptive Server 的性能。

有关安排 Open Server 线程的信息，请参见 Open Server Server-Library/C Reference Manual （《Open Server Server-Library/C 参考手册》）。

esp execution stacksize

摘要信息	
缺省值	34816
值的范围	$34816 - 2^{14}$
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	扩展存储过程

esp execution stacksize 设置要为 ESP 执行分配的堆栈的大小（以字节为单位）。

如果有自己的 ESP 函数并且要求的堆栈尺寸比缺省值 34816 大，则可以使用该参数。

esp unload dll

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	扩展存储过程

esp unload dll 指定在 ESP 调用完成后，是否应从 XP Server 内存中自动卸载支持 ESP 的 DLL。

如果将 **esp unload dll** 设置为 0，则不会自动卸载 DLL。如果设置为 1，则自动进行卸载。

如果将 **esp unload dll** 设置为 0，仍然可以在运行期间使用 **sp_freedll** 明确卸载单个 DLL。

event buffers per engine

摘要信息	
缺省值	100
值的范围	1 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、SQL Server 管理

event buffers per engine 指定 Adaptive Server Monitor 可同时监控的各 Adaptive Server 引擎上的事件数。Adaptive Server Monitor 用事件来观测 Adaptive Server 的性能；如果未使用 Adaptive Server Monitor，将此设置参数为 1。

配置中的引擎数、Adaptive Server 上的活动级别以及正在运行的应用程序的类型，决定了 **event buffers per engine** 的值应设置为多少。

将 **event buffers per engine** 设置为较小的值可能导致事件信息丢失。缺省值对于大多数节点而言可能太低。对于常规监控，设置为 2000 或更大的值可能更合理。但是，请进行试验以确定对自己节点合适的值。

一般情况下，将 **event buffers per engine** 设置为较大的值可减少 Adaptive Server Monitor 引起的 Adaptive Server 性能下降。

每个事件缓冲区使用 100 字节的内存空间。若要确定由 `event buffers per engine` 的特定值使用的总内存量，请将配置中的 Adaptive Server 引擎数乘以此参数的值。

event log computer name（仅限 Windows）

摘要信息	
缺省值	LocalSystem
有效值	- 网络中配置为记录 Adaptive Server 消息的 Windows 计算机的名称 - LocalSystem - NULL
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	错误日志

`event log computer name` 指定在其 Windows 事件日志中记录 Adaptive Server 消息的 Windows PC 的名称。仅 Windows 服务器提供该功能。

值 `LocalSystem` 或 `NULL` 指定缺省本地系统。

还可以使用 `Server Config` 实用程序来设置 `event log computer name` 参数，方法是指定“事件记录”下的“事件日志计算机名”。

通过 `sp_configure` 设置 `event log computer name` 参数或指定“事件记录”下的“事件日志计算机名”，则会覆盖命令行 `-G` 选项的作用（如果指定了该选项）。如果 Adaptive Server 是使用 `-G` 选项启动的，则可以通过设置 `event log computer name` 来更改目标远程计算机。

有关将 Adaptive Server 消息记入远程节点的详细信息，请参见 *Configuration Guide for Windows*（《适用于 Windows 的配置指南》）。

event logging（仅限 Windows）

摘要信息	
缺省值	1
有效值	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	错误日志

event logging 可以控制是否允许将 Adaptive Server 消息记录到 Windows 事件日志中。

缺省值为 1，表示允许将 Adaptive Server 消息记录到 Windows 事件日志中；值为 0 时，表示不允许这样做。

使用 Server Config 实用程序来设置 event logging 参数，方法是选择“事件记录”下的“使用 Windows 事件记录”。

如果设置 event logging 参数或选择“使用 Windows 事件记录”，会覆盖命令行选项 -G 的作用（如果指定了该选项）。

executable codesize + overhead

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	已计算
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用

executable codesize + overhead 报告 Adaptive Server 可执行代码与开销的组合大小（以千字节为单位）。此值是通过计算得出的，用户无法对其进行配置。

extended cache size

摘要信息	
缺省值	0
值的范围	0 - 31457280
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	高速缓存管理器

extended cache size 指定辅助高速缓存的大小。

FIPS login password encryption

摘要信息	
缺省值	0
值的范围	0 - 1
状态	静态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	与安全性相关的参数

需要安全和目录服务许可证才能启用 FIPS login password encryption。此参数提供 FIPS 140-2 加密模块支持，用于对传输中、内存中和磁盘上的口令进行加密。

Adaptive Server 使用 FIPS 140-2 认证的 Certicom 安全提供程序进行登录加密。如果未启用此配置，Adaptive Server 将使用 OpenSSL 安全提供程序来执行登录口令加密。

global async prefetch limit

摘要信息	
缺省值	10
值的范围	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	高速缓存管理器

global async prefetch limit 指定一个可以容纳由异步预取引入且尚未被读取的页的缓冲池百分比。由于没有使用 sp_poolconfig 明确给池规定限制，因此该参数将为所有高速缓存中的所有池设置限制。

如果超过了池的限制，则异步预取暂停使用，直到未读取页的百分比下降到限制值以下。请参见 Performance and Tuning Series: Basics （《性能和调优系列：基础知识》）中的第 3 章 “Using Engines and CPUs”（使用引擎和 CPU）。

global cache partition number

摘要信息	
缺省值	1
值的范围	1 - 64, 2 的乘方
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	高速缓存管理器

global cache partition number 为所有数据高速缓存设置缺省的高速缓存分区数值。可以使用 **sp_cacheconfig** 为特定高速缓存设置分区数目；本地值优先于全局值。

使用高速缓存分区来减少高速缓存螺旋锁争用；一般来说，如果螺旋锁争用超过 10%，则对高速缓存进行分区应会改善性能。如果分区数增加一倍，则使螺旋锁争用减少大约一半。

请参见《系统管理指南：卷 2》中的第 4 章“配置数据高速缓存”。另请参见 *Performance and Tuning Series: Basics*（《性能和调优系列：基础知识》）中的第 3 章“Using Engines and CPUs”（使用引擎和 CPU）。

heap memory per user

摘要信息	
缺省值	4K
有效值	0 - 2147483647 字节
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、物理内存

heap memory per user 配置每个用户的堆内存量。堆内存池是启动时创建的内部内存，任务根据需要用它来动态分配内存。如果运行使用宽列的任务，它需要使用堆栈中的大量内存，此时内存池就显得非常重要。堆内存分配临时缓冲区，以使这些宽列任务顺利完成。任务结束后，任务所用的堆内存返回堆内存池中。

内存池的大小取决于用户的连接数。Sybase 建议将 **heap memory per user** 设置为逻辑页大小的三倍。

histogram tuning factor

摘要信息	
缺省值	20
值的范围	1 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

histogram tuning factor 控制 Adaptive Server 分析 update statistics、update index statistics、update all statistics 和 create index 的每个直方图的梯级数。如果值为 1，则禁用该参数。

注释 对于 Adaptive Server 版本 15.0.2 ESD #2 和更高版本，如果将 histogram tuning factor 设置为缺省值 20，并且为直方图请求大量梯级数，则用于直方图的实际梯级计数限制为可减少过程高速缓存使用量的值：

```
min (max (400, requested_steps),
      histogram_tuning_factor X requested_steps)
```

在下例中，Adaptive Server 用 30 个值生成了一个中等 20 梯级的直方图：

```
sp_configure 'histogram tuning factor',20
update statistics tab using 30 values
```

Adaptive Server 分析此直方图并根据以下参数将其压缩到最终生成的直方图中：

- 第一梯级原样复制。
- 高频率梯级原样复制。
- 连续范围梯级被折叠到最终生成的梯级中，从而折叠梯级的总权值不会超过值的三十分之一。

sysstatistics 中的最终直方图：

- 用类似于 30 梯级 update statistics 的方式生成范围梯级，并且高频率范围被隔离（如同直方图是用 600 梯级创建的一样）。
- 最终生成的直方图中的梯级总数可能从 30 到 600 个值不等。
- 对于等量分布的数据，该值应该很接近 30。
- 表中的“高频”值越多，表示直方图中的梯级越多。
- 如果某一行上不同的值很少，则所有这些值可能都显示为高频率单元。

可通过将 `number of histogram steps` 增加到 600 来实现相同的效果，但这样做会使用缓冲区和过程高速缓存中的更多资源。

`histogram tuning factor` 最大限度地降低直方图所消耗的资源，仅当最有利于优化时才增加资源的使用量。例如，某列中存在数据的不一致分布，或某列中包含高重复值时。在这种情况下，最多可使用 600 个直方图梯度。但是，在大多数情况下，`histogram tuning factor` 使用缺省值（上例中为 30）。

housekeeper free write percent

摘要信息	
缺省值	1
值的范围	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

`housekeeper free write percent` 指定管家清洗任务可以增加数据库写入的最大百分比。

例如，若要在数据库写入的频率达到正常以上 5% 时停止运行管家任务，可将 `housekeeper free write percent` 设置为 5。

当 Adaptive Server 没有要处理的用户任务时，管家清洗任务会自动开始将高速缓存中已更改的页写入磁盘。这种写入可提高 CPU 的利用率，降低事务处理期间缓冲区冲洗的需要，并可缩短检查点。

在反复更新同一数据库页的应用程序中，管家清洗可能会启动一些不必要的数据库写入。尽管这些写入操作只发生在服务器空闲周期，但在有过载磁盘的系统上可能不会被接受。

用于优化查询的表和索引的统计信息在查询处理期间保留在内存结构中。当这些统计信息更改时，这些更改不会立即被写到 `systabstats` 表中，以减少 I/O 争用并改善性能。而是由管家杂事任务定期将统计信息刷新到磁盘。

此缺省值允许管家清洗任务增加最大为 1% 的磁盘 I/O。这可使大多数系统性能提高，恢复速度加快。

若要禁用管家清洗任务，请将 `housekeeper free write percent` 的值设置为 0。

仅当系统的磁盘争用很严重，并且系统无法容纳管家清洗任务所产生的额外 I/O 时，才能将此值设置为 0。

如果禁用管家任务，则应让统计信息保持最新状态。向磁盘中写入统计信息的命令为：

- `update statistics`
- `dbcc checkdb` （用于数据库中的所有表）或 `dbcc checktable` （用于单个表）
- `sp_flushstats`

请在以下时间，在自上次将统计信息写入磁盘后更新的所有表上，运行上述命令之一：

- 转储数据库之前
- 按顺序关闭之前
- 在失败 （或按顺序关闭）并重新启动之后 （在这些情况下就不能使用 `sp_flushstats`，而必须使用 `update statistics` 或 `dbcc` 命令）
- 对表进行重大更改 （例如大批量复制操作、变更锁定方案、删除或插入大量行或执行 `truncate table` 命令）之后

若要允许管家清洗任务连续工作，而不考虑附加数据库写入的百分比，可将 `housekeeper free write percent` 设置为 100。

可使用 `sp_sysmon` 监控管家程序的性能。请参见 [Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon](#) （《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

您或许还想查看由管家任务启动的自由检查点的数目。[Performance and Tuning Series: Basics](#) （《性能和调优系列：基础知识》）描述了此输出。

i/o accounting flush interval

摘要信息	
缺省值	1000
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`i/o accounting flush interval` 以计算机时钟周期为单位，指定 Adaptive Server 等待多长时间后，才将每个用户的 I/O 统计信息从 `sysprocesses` 刷新到 `syslogins`。此参数用于收费退回式会计。

用户登录到 Adaptive Server 后，服务器在 sysprocesses 中开始累计此用户进程的 I/O 统计信息。在超过 i/o accounting statistics interval 的值或用户从 Adaptive Server 注销时，此用户的累计 I/O 统计信息将从 sysprocesses 刷新到 syslogins。这些统计信息不断在 syslogins 中累计，直到使用 sp_clearstats 将总和清除为止。可以使用 sp_reportstats 命令来显示 syslogins 的当前总和值。

报告运行类型决定了 i/o accounting flush interval 的设置值。如果报告每月运行一次，则将 i/o accounting flush interval 设置为一个相对高的值。如果报告运行频率很低，syslogins 中的数据是否经常更新并不重要。

如果对 syslogins 的 totio 列定期进行特定选择，以确定进程的 I/O 量，可将 i/o accounting flush interval 设置为一个较小的值。这样做增加了 syslogins 中的数据在您执行选择时保持最新的可能性。

如果根本不报告 I/O 统计信息，则将 i/o accounting flush interval 设置为最大值。这样就减少了 syslogins 的更新次数，以及将其页面写入磁盘的必要次数。

i/o batch size

摘要信息	
缺省值	100
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

i/o batch size 设置任务在开始休眠前，一个批处理发出的写操作数。一旦该批处理完成，任务便会苏醒过来，然后就发出下一批写操作，这样就能确保 I/O 子系统不会被大量同时进行的写操作充满。将 i/o batch size 设置为适当的值，可以提高操作（如 checkpoint、dump database、select into 等等）的性能。

i/o polling process count

摘要信息	
缺省值	10
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

i/o polling process count 指定在调度程序检查磁盘和网络 I/O 的完成情况之前，Adaptive Server 可以运行的最多进程数。调整 i/o polling process count 的值既会影响响应时间，又会影响 Adaptive Server 的吞吐量。

Adaptive Server 检查磁盘或网络 I/O 的完成情况：

- 如果自从上次 Adaptive Server 检查 I/O 的完成情况以后运行的任务数与 i/o polling process count 的值相等，且
- 在每一 Adaptive Server 时钟周期。

一般情况下，如果增大 i/o polling process count 的值，就会增加那些生成大量磁盘和网络 I/O 的应用程序的吞吐量。相反，如果降低该值，则会改善这些应用程序的进程响应时间，但可能会导致吞吐量降低。

如果应用程序既创建 I/O 密集型任务，又创建 CPU 密集型任务，则将 i/o polling process count 调整为较小的值 (1-2) 可确保 I/O 密集型任务可访问 CPU 周期。

对于 OLTP 应用程序（或任何有用户连接和短事务的 I/O 密集型应用程序），则将 i/o polling process count 调整为一个 20-30 范围内的值可以增加吞吐量，但这样也可能会延长响应时间。

在调优 i/o polling process count 时，还应考虑其它三个参数：

- [sql server clock tick length](#)，用来指定 Adaptive Server 的时钟周期的持续时间（以微秒为单位）。请参见第 221 页的“[sql server clock tick length](#)”。
- [time slice](#)，用来指定 Adaptive Server 调度程序允许一个用户进程运行的时钟周期数。请参见第 233 页的“[time slice](#)”。
- [cpu grace time](#)，用来指定用户进程在被 Adaptive Server 抢占，并因时间片错误而被终止之前，在不放弃 CPU 的情况下可以运行的最长时间（以时钟周期为单位）。请参见第 92 页的“[cpu grace time](#)”。

使用 `sp_sysmon` 来确定更改 i/o polling process count 所产生的效果。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon`（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

identity burning set factor

摘要信息	
缺省值	5000
值的范围	1 - 9999999
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

IDENTITY 列的类型为 **numeric**，标度为零，其值由 Adaptive Server 生成。列值介于最小值 1 和列精度确定的值之间。

对于每个带有 IDENTITY 列的表，Adaptive Server 将可能的列值组分成数值连续的几块，并在内存中一次使一块可用。每次向表中插入一行时，Adaptive Server 从块中将下一个可用值分配给 IDENTITY 列。当一个块中的所有数值都已被使用时，下一块变得可用。

这种选择 IDENTITY 列值的方法可提高服务器性能。当 Adaptive Server 分配一个新列值时，它从内存中读取当前最大值，然后加 1。仅当块中的所有值都已被使用后，才需要访问磁盘。由于在服务器故障（或 **shutdown with nowait**）时块中的所有剩余数值全被丢弃，此方法可能导致 IDENTITY 列值出现中断。

可使用 **identity burning set factor** 更改每个块中可用潜在列值的百分比。为保证良好的性能，此值应足够高，但又不应高到使列值的中断大到不可接受的地步。此参数的缺省值为 5000，即每次释放 0.05% 的可能 IDENTITY 列值以供使用。

若要得到 **sp_configure** 的正确值，请以小数形式表示此百分比，然后乘以 10^7 (10,000,000)。例如，若要每次释放 15% (.15) 的可能 IDENTITY 列值，在 **sp_configure** 中指定的值应为 .15 乘以 10^7 （或 1,500,000）。

identity grab size

摘要信息	
缺省值	1
值的范围	1 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

`identity grab size` 允许每个 Adaptive Server 进程保留一个 IDENTITY 列值块，用来插入到具有 IDENTITY 列的表中。

如果您正在执行插入操作，并且想让所有插入的数据具有连续的 IDENTITY 号，它就很有用。例如，如果正在输入 payroll 的数据，并希望特定部门的所有记录的行都在同一块中，则可将 `identity grab size` 设置为该部门的记录数。

`identity grab size` 适用于 Adaptive Server 上的所有用户。如果设置较大的 `identity grab size` 值，在许多用户向具有 IDENTITY 列的表中插入数据时，会导致 IDENTITY 列中出现较大的中断。

Sybase 建议您将 `identity grab size` 值设置得足够大，以便能够容纳要插入连续行的最大记录组。

identity reservation size

摘要信息	
缺省值	1
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`identity reservation size` 设置对标识值数量的限制。

idle migration timeout

摘要信息	
缺省值	60
有效值	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

`idle migration timeout` 指定一段时间，空闲连接将在这一段时间后关闭，而不会使发送到客户端的迁移请求失效，从而允许您在指定的时间段后停止实例，而无需等待空闲客户端连接迁移。

如果将 `idle migration timeout` 设置为较高的值，将会减慢正常关闭的速度，原因是对于发出迁移请求而没有已启动迁移的客户端的所有空闲连接，实例都必须等待指定的一段时间。

job scheduler interval

摘要信息	
缺省值	1（分钟）
值的范围	1 - 600
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`job scheduler interval` 设置 Job Scheduler 以多长的时间间隔检查哪些预定作业达到了执行时间。

job scheduler tasks

摘要信息	
缺省值	32
值的范围	1 - 640
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`job scheduler tasks` 设置可通过 Job Scheduler 同时运行的作业的最大数量。

license information

摘要信息	
缺省值	25
有效值	0 - 2 ³¹
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

license information 允许 Sybase 系统管理员监控 Adaptive Server 中使用的用户许可证的数目。启用该参数只监控发出的许可证数；但不强制执行许可协议。

如果将 license information 设置为 0，则 Adaptive Server 不会监控许可证使用。如果将 license information 设置为大于 0 的数值，则管家杂事任务将监控 Adaptive Server 空闲周期中使用的许可证的数目。将 license information 设置为许可协议中指定的许可证数目。

如果使用的许可证的数目大于为 license information 设置的数目，则 Adaptive Server 会将此消息写入错误日志：

```
WARNING: Exceeded configured number of user licenses
```

每过 24 小时，在此段时间内使用的最大许可证数就被加入到 syblicenseslog 表中。如果 Adaptive Server 重新启动，则重新开始 24 小时周期。

请参见第 447 页的“[监控许可证的使用状况](#)”。

lock address spinlock ratio

摘要信息	
缺省值	100
值的范围	1 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序

对于运行多个引擎的 Adaptive Server，address lock spinlock ratio 设置由一个螺旋锁保护的内部地址锁散列表中的行数。

Adaptive Server 使用带有 1031 行的内部散列表（通称为散列桶）来管理地址锁的获取和释放。该散列表可以使用一个或多个螺旋锁，使运行在不同引擎上的进程之间的访问串行化。

address lock spinlock ratio 缺省值为地址锁散列表定义了 11 个螺旋锁。前 10 个螺旋锁每一个可以保护 100 行，第十一个螺旋锁保护剩余的 31 行。如果为 address lock spinlock ratio 指定的值为 1031 或更大，则 Adaptive Server 将只为整个表使用一个螺旋锁。

lock hashtable size

摘要信息	
缺省值	2048
值的范围	1 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序、内存使用

lock hashtable size 指定锁散列表中散列桶的数目。该表管理所有行锁、页锁、表锁，以及所有锁请求。每当一个任务获取一个锁时，即会将该锁指派到一个散列桶，此后，对该锁的每个锁请求都将检查同一散列桶。将该值设得太小将导致每个散列桶中容纳大量的锁，并减慢搜索的速度。在具有多个引擎的 **Adaptive Server** 中，将该值设得太小还可能导致螺旋锁争用的增加。设置该值不得小于缺省值 2048。

lock hashtable size 必须是 2 的幂。如果指定的值不是 2 的幂，**sp_configure** 将该值取整为 2 的下一个最高次幂，并显示信息性消息。

最佳的散列表大小是一个与可并发锁定的不同对象（页、表和行）的数目相关的函数。最佳散列表大小至少应为需要并发锁定的不同对象的数目的 20%。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

lock scheme

摘要信息	
缺省值	allpages
值的范围	allpages、datapages、datarows
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序

lock scheme 用于设置当命令中未指定锁定方案时，由 **create table** 和 **select into** 命令使用的缺省锁定方案。

锁定方案的值是字符数据，因此必须使用 0 作为第二个参数（必须为数字）的占位符，并指定 **allpages**、**datapages** 或 **datarows** 作为第三个参数：

```
sp_configure "lock scheme", 0, datapages
```

lock shared memory

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	物理内存

lock shared memory 不允许 Adaptive Server 页到磁盘的交换，并允许操作系统内核避开服务器的内部页锁定代码。这可以减少开销较大的磁盘读取。

并非所有平台都支持共享内存的锁定。即使平台支持它，但由于设置权限不正确、物理内存不足或其它原因，lock shared memory 也可能会失败。有关共享内存锁定的信息，请参见所使用平台的操作系统文档。

lock spinlock ratio

摘要信息	
缺省值	85
值的范围	1 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序、内存使用

Adaptive Server 使用带有可配置散列桶个数的内部散列表来管理锁的获取和释放。在 SMP 系统上，该散列表可以使用一个或多个螺旋锁，使运行在不同引擎上的进程之间的访问串行化。若要设置散列桶的数目，请使用 lock hashtable size。

对于运行多个引擎的 Adaptive Server，lock spinlock ratio 会设置一个比率，用来确定一个螺旋锁保护的锁散列桶的数量。如果增加 lock hashtable size，螺旋锁的数目也会增加，这样，一个螺旋锁保护的散列桶的数量将保持不变。

Adaptive Server 的 lock spinlock ratio 缺省值为 85。如果将 lock hashtable size 设置为缺省值 2048，则缺省的螺旋锁比率会为锁散列表定义 26 个螺旋锁。请参见《系统管理指南：卷 2》中的第 5 章“管理多处理器服务器”。

sp_sysmon 报告有关锁散列表中散列链的平均长度。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon （《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

lock table spinlock ratio

摘要信息	
缺省值	20
值的范围	1 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序

对于运行多个引擎的 Adaptive Server，table lock spinlock ratio 设置由一个螺旋锁保护的内部表锁散列表中的行数。

Adaptive Server 使用有 101 行的内部散列表（通称为散列桶）来管理表锁的获取和释放。该散列表可以使用一个或多个螺旋锁，使运行在不同引擎上的进程之间的访问串行化。

Adaptive Server 的 table lock spinlock ratio 缺省值为 20，该值为表锁散列表定义了 6 个螺旋锁。前 5 个螺旋锁每个螺旋锁保护 20 行；第 6 个螺旋锁保护最后一行。如果为 table lock spinlock ratio 指定的值为 101 或更高，则 Adaptive Server 只使用一个螺旋锁保护整个表。

lock wait period

摘要信息	
缺省值	2147483647
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序

lock wait period 限制任务等待获取表、数据页或数据行中的锁的秒数。如果任务不能在指定的时间段内获取锁，Adaptive Server 将向用户返回错误消息 12205 并回退事务。

set 命令的 lock wait 选项设置任务等待锁时的会话级等待时间（秒）。该值将替换此会话的服务器级设置。

lock wait period 与会话级设置 set lock wait nnn 一起使用，仅应用于用户定义的表。这些设置对系统表毫无影响。

对于缺省值，所有进程都等待不确定的时间以获取锁。若要恢复缺省值，请将该值重置为 2147483647，或输入：

```
sp_configure "lock wait period", 0, "default"
```

log audit logon failure

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	错误日志

log audit logon failure 指定是否将不成功的 Adaptive Server 登录记入 Adaptive Server 错误日志；在 Windows 服务器上，则是是否记入 Windows 事件日志（如果启用了事件记录）。

log audit logon success

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	错误日志

log audit logon success 指定是否将成功的 Adaptive Server 登录记入 Adaptive Server 错误日志；在 Windows 服务器上，则是是否记入 Windows 事件日志（如果启用了事件记录）。

max async i/os per engine

摘要信息	
缺省值	因平台而异
值的范围	1 - 因平台而异的值
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	操作系统资源

`max async i/os per engine` 指定单个引擎一次能够进行的未完成异步磁盘 I/O 请求的最大数目。

在 Linux 平台上

在 Linux 平台上，`max async i/os per engine` 控制每个引擎在计算机启动时从操作系统中保留的异步 IO 数。当使用的数字大于缺省值时，系统会从中受益。

可以使用 `sp_sysmon` 来帮助调优 `max async i/os per engine`。`sp_sysmon` 的 `disk i/o section` 包含有关采样期间每个引擎的未完成 IO 的最大数量以及因引擎或操作系统限制延迟的 I/O 数量的信息。通常，因引擎限制延迟的任何 I/O 均表示应增大 `max async i/os per engine` 的值。

Adaptive Server 是否能对设备执行异步 IO 操作取决于此设备是否支持内核异步 I/O (KAIO)。Linux 内核要求在文件系统级别实现内核异步 I/O 支持。大多数主流文件系统都支持内核异步 I/O，其中包括 `ext3`、`xf`s、`jfs` 和裸设备。`tmpfs` 文件系统不支持内核异步 I/O。如果设备不支持内核异步 I/O，**Adaptive Server** 将不能对该设备执行异步 IO 操作，而是将对该设备的所有读取和写入都恢复为标准同步 IO。**Adaptive Server** 将在错误日志中输出类似如下的消息，指出设备已切换到同步 IO：

```
00:00000:00001:2006/12/15 11:47:17.98 kernel Virtual device
'/dev/shm/tempdb.dat' does not support kernel asynchronous i/o. Synchronous i/o
will be used for this device.
```

max async i/os per server

摘要信息	
缺省值	因平台而异
值的范围	1 - 因平台而异的值
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	操作系统资源

max async i/os per server 参数指定：对 Adaptive Server 而言，允许同时存在的、未完成异步磁盘 I/O 请求的最大数量。该限制不受每个 Adaptive Server 的联机引擎数影响；max async i/os per engine 限制每个引擎未完成 I/O 的数目。

大多数操作系统限制同时处理的异步磁盘 I/O 的数目；一些操作系统限制每个操作系统进程能够处理的数目，而另一些操作系统限制每个系统能够处理的数目，还有一些操作系统则对两者都进行限制。如果应用程序超过这些限制，则操作系统返回一个错误消息。因为操作系统调用的开销相对较大，所以 Adaptive Server 尝试执行已被操作系统拒绝的异步 I/O 的效率较低。

为了避免这种情况，Adaptive Server 维护每个引擎和每个服务器的未完成异步 I/O 的数量；如果一个引擎发出的异步 I/O 超过 max async i/os per engine 或 max async i/os per server，则 Adaptive Server 将延迟 I/O 直到有足够多的未完成异步 I/O 完成，使异步 I/O 降到超过的限制以下为止。

例如，假设操作系统限制每个系统有 200 个异步 I/O 及每个进程有 75 个异步 I/O，同时一个 Adaptive Server 带有 3 个联机引擎。这些引擎当前总共有 200 个待执行的异步 I/O，按照下表进行分配：

引擎	待执行的 I/O 数目	结果
0	60	引擎 0 延迟执行任何后面的异步 I/O，直到该服务器的异步 I/O 总数降到操作系统对每个系统的限制以下，然后继续发出异步 I/O。
1	75	引擎 1 延迟执行任何后面的异步 I/O，直到每个引擎的异步 I/O 总数降到操作系统对每个进程的限制以下，然后继续发出异步 I/O。
2	65	引擎 2 延迟执行任何后面的异步 I/O，直到该服务器的异步 I/O 总数降到操作系统对每个系统的限制以下，然后继续发出异步 I/O。

所有的 I/O（包括同步和异步）都需要磁盘 I/O 结构，因此 `disk i/o structures` 值限制了未完成的磁盘 I/O 的总数。与因为 I/O 请求超过 `max i/os per server` 而延迟 I/O 相比，Adaptive Server 因为它不能得到磁盘 I/O 结构而延迟 I/O 的效率稍高一些。将 `max async i/os per server` 设置为与 `disk i/o structures` 的值相等。请参见第 103 页的“`disk i/o structures`”。

如果在操作系统能够调优异步 I/O 限制，则确保为 Adaptive Server 设置足够高的异步 I/O 限制。根据需要设置较高的限制，并不会对性能产生任何影响。

使用 `sp_sysmon` 查看每个服务器或每个引擎的限制是否延迟系统的 I/O。如果 `sp_sysmon` 显示 Adaptive Server 超出了每个引擎或每个服务器未完成请求的限制，则提高相应参数的值。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon`（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

max cis remote connections

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	组件集成服务

`max cis remote connections` 指定能够通过组件集成服务与远程服务器同时进行 Client-Library 连接的最大数目。

缺省情况下，组件集成服务允许每个用户同时与远程服务器进行的连接最多为四个。如果将最多用户数设置为 25，则组件集成服务最多允许同时建立 100 个 Client-Library 连接。

如果此数目没有满足安装需要，则可以明确指定服务器一次能够建立的对外 Client-Library 连接的数目来替换原设置。

max concurrently recovered db

摘要信息	
缺省值	0
有效值	1 - 启动时的引擎数减 1
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	备份 / 恢复

`max concurrently recovered db` 确定并行度。最小值为 1（即使用串行恢复），但您也可以使用它的缺省值 0，以使用自调优方法。最大值等于启动时的引擎数减 1。`max concurrently recovered db` 还受配置参数 `number of open databases` 的值的限制。

max memory

摘要信息	
缺省值	因平台而异
值的范围	因平台而异的最小值 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、物理内存

`max memory` 指定可配置 Adaptive Server 分配的最大物理内存总量。`max memory` 必须大于 Adaptive Server 的当前配置所消耗的总逻辑内存量。

对于配置 Adaptive Server 以便使用计算机上最大的可用内存，并不会对性能产生任何影响。不过，应估计系统上的其它内存需求，否则 Adaptive Server 可能无法获得足够的内存来启动。

请参见《系统管理指南：卷 2》中的第 3 章“配置内存”。

如果 Adaptive Server 不能启动

在 `allocate max shared memory` 设置为 1 时，Adaptive Server 必须具有 `max memory` 指定的可用内存量。如果内存不足，Adaptive Server 就不会启动。如果发生这种情况，可手动更改服务器配置文件中 `max memory` 的值，以减少 Adaptive Server 的内存需求。也可将 `allocate max shared memory` 更改为 0，以便在启动时不需要 `max memory` 所要求的全部内存。

还可能减少其它需要大量内存的配置参数的值。然后重新启动 Adaptive Server 以使用新值所指定的内存。如果因其它配置参数值的总和大于 `max memory` 的值，而导致 Adaptive Server 启动失败，请参见《系统管理指南：卷 2》中的第 3 章“配置内存”，了解有关使用内存的配置参数的信息。

max native threads per engine

摘要信息	
缺省值	50
最大值	50 - 1000
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	用户环境

`max native threads per engine` 定义服务器生成的每个引擎的本地线程最大数。达到本地线程的数量限制时，请求本地线程的 Adaptive Server 会话进入休眠状态，直到其它会话释放本地线程为止。

`max nesting level`

在 Adaptive Server 15.0.3 及更高版本中，最大嵌套级别已增加到 100，并将缺省值增加到 50。

摘要信息	
缺省值	50
值的范围	16 - 100
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	用户环境

`maximum nesting level` 设置存储过程和触发器的最大嵌套级别。每增加一个嵌套级别都需要约 160 字节的额外内存。例如，如果将嵌套级别从 16 增加到 26，则 Adaptive Server 需要 1600 字节的额外内存。

max network packet size

摘要信息	
缺省值	512
值的范围	512 - 65024
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	网络通信

max network packet size 指定与 Adaptive Server 通信的客户端能够请求的最大网络包大小。

如果某些应用程序通过网络发送或接收大量数据，并且这些应用程序使用较大的包大小，则可以显著地改善性能。大批量复制操作以及读取或写入大量 text、unitext 和 image 值的应用程序，便是两个示例。

通常情况下，您希望：

- 对于执行小规模查询的用户，将 default network packet size 设置为较小的值，并且
- 将 max network packet size 设置为较大的值，以使发送或接收大量数据的用户能够请求较大的包大小。

max network packet size 值必须保持与 default network packet size 值同样大小或比它更大。不是 512 偶数倍的值将被向下舍入。

对于显式请求较大网络包大小以接收网络包的客户端应用程序，还必须配置 additional network memory。请参见第 73 页的 “additional network memory”。

Open Client Server 不能接受超过 64K 的网络包大小。

有关使用这些程序的较大包大小的信息，请参见 《实用程序指南》中的 bcp 和 isql。Open Client Client-Library 文档包括关于使用可变包大小的信息。

选择包大小

为了获得最佳性能，选择一个可充分使用网络上基础包大小的服务器包大小。目标是：

- 减少服务器读取和写入网络的次数
- 减少网络包中的未使用空间 （增加网络吞吐量）

例如，如果网络包大小支持 1500 字节的数据，则将 Adaptive Server 的包大小设置为 1024（即 512×2 ）可能比设置为 1536（即 512×3 ）会获得更好的性能。图 5-3 显示了在这一方案中四个不同的包大小配置的执行情况。

图 5-3：确定包大小的因子

基础网络包：去掉开销后有 1500 字节

包大小为 512

已使用 1024 字节
未使用 476 字节
使用百分比：68%
2 次服务器读取



根据数据量，网络包可能有 1 或 2 个

包大小为 1024

已使用 1024 字节
未使用 476 字节
使用百分比：68%
1 次服务器读取



应该比缺省值 512 时的性能有所改善

包大小为 2560

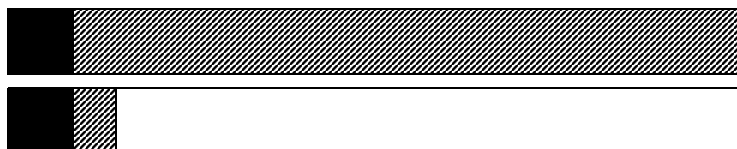
已使用 2560 字节
未使用 440 字节
使用百分比 85%
2 次服务器读取



可能是图示选择中的最佳选项

包大小为 1536

已使用 1536 字节
未使用 1464 字节
使用百分比 51%
2 次服务器读取



可能是图示选择中的最差选项

关键字：

开销

数据

未使用



确定网络上基础包的可用数据空间后，执行自己的基准测试以确定配置的最优大小。

可以使用 `sp_sysmon`，了解 `max network packet size` 的更改如何影响网络 I/O 管理和任务切换。例如，尝试增加 `max network packet size` 的值，然后检查 `sp_sysmon` 输出，了解这样的更改如何影响较大批次的 `bcp`。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

max number network listeners

摘要信息	
缺省值	5
值的范围	0 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、网络通信

`max number network listeners` 指定 Adaptive Server 一次允许使用的网络监听器的最大数目。

每个主端口都有一个网络监听器。一般情况下，无需拥有多个主端口，除非 Adaptive Server 必须通过多种网络类型进行通信。某些平台支持套接字和 TLI（传送层接口）网络接口。有关支持的网络类型的信息，请参见所使用平台的《配置指南》。

max online engines

摘要信息	
缺省值	1
值的范围	1 - 128
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、处理器

`max online engines` 的作用是：设置在 SMP 环境中任何时刻能够同时联机的引擎的最大数目。其不考虑启动时可用的 CPU 数量，并允许用户日后增加 CPU 数。

max engines online 指定在 SMP 环境中任何时刻能够同时联机的 Adaptive Server 引擎的最大数目。请参见《系统管理指南：卷 2》中的第 5 章“管理多处理器服务器”，了解有关如何为 SMP 环境设置此参数的详细论述。

在启动时，Adaptive Server 以单个引擎启动并完成其初始化操作，包括所有数据库的恢复。它最终任务是分配额外的服务器引擎。每个引擎访问共享内存中的通用数据结构。

调优 max engines online 参数时：

- 绝不能使联机引擎数大于 CPU 的数目。
- 根据整个系统的负载（包括除了 Adaptive Server 的应用程序），可以通过保留一些可用的 CPU 来运行非 Adaptive Server 进程，获得最佳吞吐量。
- 可以通过减少所运行引擎的数量，提高 CPU 使用率，获得较好的吞吐量。
- 可伸缩性与应用程序有关。对应用程序做全面的基准测试，以确定联机引擎的最佳配置。
- 可以使用 sp_engine 使引擎脱机或联机。可以使除引擎 0 以外的所有引擎脱机。

请参见 Performance and Tuning Series: Basics（《性能和调优系列：基础知识》）中的第 3 章“Using Engines and CPUs”（使用引擎和 CPU）。

max online Q engines

摘要信息	
缺省值	0
值的范围	0 - 127
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	

MQ 所需的 max online Q engines。指定可联机使用的最大 Q 引擎数。您可能需要增加 max online engines 以适合 max online Q engines 数。

max parallel degree

摘要信息	
缺省值	1
值的范围	1 - 255
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	查询调优

max parallel degree 指定在全服务器范围内每个查询允许使用的工作进程的最大数目。这称为“最大并行度”。

如果 max parallel degree 太低，则给定查询的性能提高可能不很明显；如果 max parallel degree 太高，则服务器编译的计划所要求的进程可能比执行时实际使用的进程多，或者系统可能变得饱和而导致吞吐量下降。若要启用并行分区扫描，请将该参数的值设置为等于或大于所查询的表中的分区数。

此参数的值必须小于或等于 number of worker processes 的当前值。

如果将 max parallel degree 设置为 1：

- Adaptive Server 将以串行方式扫描所有表或索引。
- Adaptive Server 将强制实施串行查询执行，优化程序可以选择并行度比禁用此参数时更高的计划。

如果更改 max parallel degree，则会导致过程高速缓存中的所有查询计划失效，并且在下一次执行存储过程或触发时需要编译新的计划。

请参见 Performance and Tuning Series: Query Processing and Abstract Plans（《性能和调优系列：查询处理和抽象计划》）中的第 9 章“Parallel Sorting”（并行排序）。

max pci slots

摘要信息	
缺省值	0
值的范围	0 - 30
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	用户环境

设置 Adaptive Server 允许的最大 PCI 插槽数。其值为：

- 0、1 — 带有一个 PCA 的缺省桥。

注释 JVM 只支持一个插槽。不要增加插槽数量。

- 2–30 — 为将来的版本分配。

有关 PCI 插槽的详细信息，请参见《Adaptive Server Enterprise 中的 Java》。

max query parallel degree

摘要信息	
缺省值	1
值的范围	1 - 255
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

在 Adaptive Server 处于兼容模式时使用。定义要用于给定查询的工作进程数。只有当您不需要以全局方式启用并行时，此参数才适用。number of worker process 的值不能小于 max query parallel degree 的值。

请参见 Performance and Tuning Series: Query Processing and Abstract Plans（《性能和调优系列：查询处理和抽象计划》）中的第 10 章 “Using Statistics to Improve Performance”（利用统计信息来提高性能）。

有关兼容模式的详细信息，请参见《迁移技术指南》。

max repartition degree

摘要信息	
缺省值	1
值的范围	1 - max parallel degree 的值
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

max repartition degree 配置 Adaptive Server 要求的动态重新分区数，这可使 Adaptive Server 能够使用水平并行度。但是，如果分区数过高，系统会被争用资源的工作进程所占用，并导致性能下降。max repartition degree 的值强行限定了这些资源可以创建的最大分区数。如果所有表和索引均未分区， Adaptive Server 将在对数据重新分区后使用 max repartition degree 的值来提供要创建的分区数。

max resource granularity

摘要信息	
缺省值	10
值的范围	1 - 100
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

max resource granularity 表示一个查询可使用的系统资源的最大百分比。此参数不在执行时间强制使用，而是仅供查询优化程序参考，并且不阻止查询处理器并行运行查询。查询引擎以 max resource granularity 作为参考，可避免一些内存密集型策略。

max scan parallel degree

摘要信息	
缺省值	1
值的范围	1 - 255
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	查询调优

max scan parallel degree 为可用于以下访问方法的基于散列的扫描指定全服务器范围内的最大并行度：

- 用于分区和不分区的表的并行索引扫描
- 用于不分区的表的并行表扫描

max scan parallel degree 应用于每个表或索引；也就是说，如果 max scan parallel degree 为 3，则使用基于散列的表扫描来扫描连接查询中的一个表，第二个表则可通过基于散列的索引扫描进行最佳访问，该查询可以使用 9 个工作进程（只要 max scan parallel degree 设置为 9 或更高值）。

当优化程序选择用于并行的、基于不分区扫描操作的进程数时，它将使用 max scan parallel degree 作为指导。它不适用于并行排序。因为没有分区用来在设备间传播数据，所以并行进程可能在扫描期间访问同一个设备。这可能导致额外的磁盘争用和磁头移动，从而可能使性能下降。若要防止多个磁盘访问出现问题，请使用 max scan parallel degree 减少能够并行访问该表的进程的最大数目。

如果该值太低，给定查询的性能提高就不很明显；而如果该值太高，服务器就可能编译一些计划，它们会使用大量进程，导致磁盘访问效率降低。一般的规则是：将该参数的值设置为不大于 2 或 3，因为只要 2 到 3 个工作进程就可以充分使用给定物理设备的 I/O。

将 max scan parallel degree 的值设置为小于或等于 max parallel degree 的当前值。如果您指定的数值大于 max parallel degree 值，则 Adaptive Server 返回一个错误。

如果将 max scan parallel degree 设置为 1，则 Adaptive Server 将不会执行基于散列的扫描。

如果更改 max scan parallel degree，则会导致过程高速缓存中的所有查询计划失效，并且在下一次执行存储过程或触发时需要编译新的计划。

max SQL text monitored

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

max SQL text monitored 指定了为将 SQL 文本保存到与 Adaptive Server Monitor 共享的内存而给每个用户连接分配的内存量。

如果没有为批处理语句分配足够的内存，则要查看的文本可能会被截断。Sybase 推荐使用的每个用户连接的内存初始值为 1024 字节。

从共享内存中分配给 SQL 文本的总内存量为：max SQL text monitored 与当前配置的用户连接数的乘积。

请参见第 339 页的“将 Adaptive Server 配置为保存 SQL 批处理文本”。

max transfer history

摘要信息	
缺省值	10
值的范围	1 - 255
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Adaptive Server 管理

max transfer history 控制 Adaptive Server 在每个数据库的 spt_TableTransfer 表中保留多少传输历史记录条目。对于跟踪的每个表，spt_TableTransfer 保留：

(*N* 个成功条目数) + (*N* 个未成功条目数)

其中 *N* 是 max transfer history 的值。

降低此参数不会自动从 spt_TableTransfer 中删除任何条目。下一次您为该表启动传输时，将会为给定的传输表删除条目。如果传输成功，则会清除该表的成功传输条目。如果传输未成功，则将清除其失败的传输条目。

例如，如果某个表在 spt_configure 中有 12 个成功和 9 个未成功的历史记录条目，并且您将 max transfer history 更改为 5，则下一次成功传输该表时，会将 5 个成功的条目放入 spt_configure，但 spt_configure 仍保留之前的 9 个失败条目。

maximum dump conditions

摘要信息	
缺省值	10
值的范围	10 - 100
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	组诊断

maximum dump conditions 设置：针对 Adaptive Server 在共享内存中生成数据转储这一情况，可以指定的约束条件的最大数目。

注释 此参数仅供 Sybase 技术支持部门使用。除非有 Sybase 技术支持部门的指导，否则不要修改此参数。

max buffers per lava operator

摘要信息	
缺省值	2048
值的范围	500 - 65535
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

maximum buffers per lava operator 设置执行排序或散列处理（会占用大量处理资源）的 Lava 运算符使用的缓冲区数量的上限。Lava 运算符使用会话的 **tempdb** 数据高速缓存池中的缓冲区作为处理行的工作区。

Lava 运算符通常在其输入流中递归。排序将需要后续的合并轮次，直至有足够的缓冲区可用于合并所有其余运行为止。散列处理需要后续轮次基于任何溢出的集合建立散列表，直至所有其余数据都能放入内存中的散列表中为止。某些查询在您增加 **max buffers per lava operator** 的情况下需要较少的 I/O。对于使用 **HASH DISTINCT**、**HASH VECTOR AGGREGATE** 和 **HASH UNION** 运算符的查询，情况尤为如此。

在为具有多个并发用户的服务器增加 **maximum buffers per lava operator** 的缺省值时，一定要小心。Adaptive Server 可能会为高开销的运算符单独分配更多缓冲区，从而减少了可用于高速缓存用户的表和其它会话的工作表的缓冲区数。使用 **sp_sysmon** 来分析 **tempdb** 的数据高速缓存效率。

maximum buffers per lava operator 使用 **max resource granularity** 来限制使用的缓冲区数。限制设置为以下各项中的最小值：

- **maximum buffers per lava operator** 的值，或
- $(\text{max resource granularity}) \times (\text{tempdb 的页大小池中的数据缓冲区数})$

有关设置为排序缓冲区分配的内存量的信息，请参见第 185 页的“**number of sort buffers**”。

maximum failed logins

摘要信息	
缺省值	0
值的范围	-1 - 32767
状态	动态
显示级别	10

摘要信息	
要求的角色	系统安全员
配置组	与安全性相关的参数

maximum failed logins 允许为登录名和角色设置全服务器范围内的最大登录尝试失败次数。

值 -1 指示：每当鉴定失败时 **syslogins** 列 **logincount** 中的失败登录计数都会更新，但不会锁定帐户。与之相比较，值 0（零）不允许为每次失败鉴定递增该列，并且不允许因鉴定失败锁定帐户。

请参见《参考手册：过程》，了解有关使用 **sp_modifylogin** 更改特定角色的最大失败登录数的信息。请参见《参考手册：命令》，了解有关使用 **alter role** 更改最大失败登录数的信息。

maximum job output

摘要信息	
缺省值	32768
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

maximum job output 对单个作业可产生的最大输出设置限制（以字节为单位）。如果一个作业产生的输出超过了 **maximum job output** 中指定的值，则超过所输入值的所有返回数据都将被丢弃。

memory alignment boundary

摘要信息	
缺省值	逻辑页大小
值的范围	2048 ^a - 16384 a 是由服务器逻辑页大小确定的最小值
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	高速缓存管理器

memory alignment boundary 确定数据高速缓存联接处的内存地址边界。

如果内存结构沿某个地址界限对齐，一些计算机执行 I/O 的效率可以更高。若要保持这种对齐方式，**memory alignment boundary** 的值应当始终是介于逻辑页大小和 2048K 之间 2 的乘方。

注释 **memory alignment boundary** 参数可用来支持一些硬件平台。除非有 Sybase 技术支持部门的指导，否则不要修改此参数。

memory per worker process

摘要信息	
缺省值	1024
值的范围	1024 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用

memory per worker process 指定工作进程使用的内存量（以字节为单位）。每个工作进程在查询处理期间都需要内存以用于消息发布。该内存是从一个共享的内存池中分配的；该内存池的大小是 **memory per worker process** 与 **number of worker processes** 的乘积。对大多数查询处理，缺省大小已经足够了。如果使用 **dbcc checkstorage** 并将 **number of worker processes** 设置为 1，则可能需要将 **memory per worker process** 增加到 1792 字节。

请参见《系统管理指南：卷 2》中的第 3 章“配置内存”。

messaging memory

摘要信息	
缺省值	400
值的范围	60 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、物理内存

配置可用于 Sybase 消息传送的内存量。

metrics elap max

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

metrics elap max 配置 QP 指标的最长经历时间和阈值。

metrics exec max

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

metrics exec max 配置 QP 指标的最长执行时间和阈值。

metrics lio max

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

metrics lio max 配置 QP 指标的最大逻辑 I/O 和阈值。

metrics pio max

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	

metrics pio max 配置 QP 指标的最大物理 I/O 和阈值。

min pages for parallel scan

摘要信息	
缺省值	200
值的范围	20 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

min pages for parallel scan 控制 Adaptive Server 可并行访问的表和索引的数目。如果表中的页数低于您设置的值，则以串行方式访问表。min pages for parallel scan 不考虑页大小。如果 Adaptive Server 访问索引和表，Adaptive Server 将尝试在适合的情况下对数据进行重新分区，并在适合的情况下以并行方式进行扫描。

minimum password length

摘要信息	
缺省值	6
值的范围	0 - 30
状态	动态
显示级别	10
要求的角色	系统安全员
配置组	与安全性相关的参数

`minimum password length` 允许自定义全服务器范围内的口令值或者每个登录名或每个角色口令值的长度。每个登录名或每个角色的 `minimum password length` 值将替换全服务器范围内的值。设置 `minimum password length` 只影响设置此值以后创建的口令；现有口令长度不变。

使用 `minimum password length` 为登录名和角色指定 `minimum password length` 的全服务器范围内的值。例如，若要将所有登录名和角色的 `minimum password length` 都设置为 4 个字符，请输入：

```
sp_configure "minimum password length", 4
```

若要在创建特定登录名时设置 `minimum password length`，请使用 `sp_addlogin`。例如，若要创建口令为 “Djdiek3” 的新登录名 “joe”，并将 “joe” 的 `minimum password length` 设置为 4，请输入：

```
sp_addlogin joe, "Djdiek3", minimum password length=4
```

若要在创建特定角色时设置 `minimum password length`，请使用 `create role`。若要创建口令为 “temp244” 的新角色 “intern_role”，并将 “intern_role” 的 `minimum password length` 设置为 0，请输入：

```
create role intern_role with passwd "temp244", minimum password length 0
```

原口令是 7 个字符，但由于最小口令长度设置为 0，因此该口令可更改为任意长度。

使用 `sp_modifylogin` 设置或更改现有登录名的 `minimum password length`。`sp_modifylogin` 只影响用户角色，并不影响系统角色。例如，若要将登录名 “joe” 的 `minimum password length` 更改为 8 个字符，请输入：

```
sp_modifylogin "joe", @option="minimum password length", @value="8"
```

注释 `value` 参数的数据类型为 `character`；因此数字值必须用引号引起来。

若要将所有登录名的 `minimum password length` 的替换值都更改为两个字符，请输入：

```
sp_modifylogin "all overrides", "minimum password length", @value="2"
```

若要删除所有登录名的 `minimum password length` 的替换值，请输入：

```
sp_modifylogin "all overrides", @option="minimum password length", @value="-1"
```

使用 `alter role` 设置或更改现有角色的 `minimum password length`。例如，若要将现有角色 “physician_role” 的 `minimum password length` 设置为 5 个字符，请输入：

```
alter role physician_role set minimum password length 5
```

若要替换所有角色的 `minimum password length`，请输入：

```
alter role "all overrides" set minimum password length -1
```

mnc_full_index_filter

摘要信息	
缺省值	2
值的范围	0 - 2 0 — 禁用。 1 — 启用。 2 — 根据优化目标设置来设置。
状态	动态
显示级别	Comprehensive
所需的角色	系统管理员
配置组	查询调优

如果存在以下各项，则 `mnc_full_index_filter` 将防止 Adaptive Server 考虑在服务器级没有限制搜索参数的非覆盖索引：

- 索引中的列
- 没有直方图的谓词

可以对其中有智能索引扫描的 DOL 锁定表使用 `mnc_full_index_filter`，即使智能索引扫描生成搜索参数也是如此。

更改 `mnc_full_index_filter` 的值不会增加 Adaptive Server 使用的内存量。

没有为任何特定可选目标启用 `mnc_full_index_filter`；获得该行为的唯一方式是显式启用该参数。

msg_confidentiality reqd

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

`msg_confidentiality reqd` 要求对所有进出 Adaptive Server 的消息进行加密。若要对消息进行加密，`use security services` 参数必须是 1。

msg integrity reqd

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

msg integrity reqd 要求检查所有消息的数据完整性。要检查消息的完整性，use security services 必须是 1。如果 msg integrity reqd 设置为 1，Adaptive Server 就允许客户端成功连接，除非客户端在使用下面的某个安全服务：message integrity、replay detection、origin checks 或 out-of-seq checks。

net password encryption required

摘要信息	
缺省值	0
值的范围	0 - 2
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

net password encryption reqd 将登录鉴定限定为仅使用 RSA 加密算法或 Sybase 专有算法。表 5-3 介绍了 net password encryption reqd 的有效值。

表 5-3: net password encryption reqd 的值及说明

值	说明
0	允许客户端选择用于网络登录口令的加密算法，包括无口令加密。
1	限制客户端使用 RSA 或 Sybase 专有加密算法对网络上的登录口令进行加密。此值提供限制性更强的设置，允许以前连接的客户端使用 Sybase 专有算法重新连接，而新客户端使用更强大的 RSA 算法连接。客户端尝试不使用口令加密进行连接会失败。
2	限制客户端仅使用 RSA 加密算法对网络上的登录口令进行加密。这样可提供口令的强 RSA 加密。客户端尝试不使用 RSA 加密进行连接会失败。

当连接因为要求网络口令加密被拒绝时，客户端会收到以下消息：

```
Msg 1640, Level 16, State 2:
Adaptive Server requires encryption of the login
password on the network.
```


number of alarms

摘要信息	
缺省值	40
值的范围	40 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、SQL Server 管理

`number of alarms` 指定由 Adaptive Server 分配的警报结构数量。

Transact-SQL 命令 `waitfor` 为语句块、存储过程或事务的执行定义特定时间、时间间隔或事件。Adaptive Server 使用警报来正确地执行 `waitfor` 命令。其它内部进程也需要警报。

当 Adaptive Server 需要比当前分配的更多警报时，如下消息将写入错误日志中：

```
uasetalarm:no more alarms available
```

每个警报结构所需的内存字节数很少。如果显著地增加 `number of alarms value`，请相应地调整 `max memory`。

number of aux scan descriptors

摘要信息	
缺省值	200
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、SQL Server 管理

`number of aux scan descriptors` 设置在由服务器上的所有用户共享的缓冲池中，可用的辅助扫描描述符的数量。

每个用户连接和每个工作进程都有专门分配给其的 48 个扫描描述符。其中，16 个留给用户表，12 个留给工作表，还有 20 个留给系统表（其中有 4 个留给回退条件）。当查询直接或间接地引用表时，要用到每个表的描述符。对于用户表，表引用包括：

- 在查询的 `from` 子句中引用的所有表
- 在查询指定的视图中引用的所有表（视图本身不算在内）

- 子查询中引用的所有表
- 用于检查参照完整性的所有表（这些表只用于插入、更新和删除）
- 使用 `select...into` 创建的表
- 所有为查询创建的工作表

如果某个表被引用一次以上（例如，在自连接中、在多个视图中或在多个子查询中），每次都应对该表进行计数。如果查询包括 `union`，则 `union` 查询中的每个 `select` 语句都是单独的扫描。如果查询以并行方式运行，协调进程和每个工作进程时都需要扫描描述符以用于引用每个表。

由查询扫描引用的用户表的数量超过 16，或工作表的数量超过 12 时，将从共享缓冲池中分配扫描描述符。通过表扫描访问的每个 DOL 锁定表（而不是通过索引扫描访问的表）也需要系统表描述符。如果在一次查询中使用表扫描方式扫描了 16 个以上的 DOL 锁定表，将为它们分配辅助扫描描述符。

如果扫描在已用完所分配数目的描述符后需要辅助扫描描述符，但在共享的缓冲池中没有可用的描述符，`Adaptive Server` 将显示一条错误消息并回退用户事务。

如果查询均不需要额外的扫描描述符，最好仍将 `number of aux scan descriptors` 的设置保持为缺省值，以防增加系统要求。只有在确保系统中的用户运行查询的表的数目绝不超过 16，并且您的表将始终只有很少（或根本没有）参照完整性约束的情况下，才能将该参数设置为 0。请参见第 167 页的“[监控扫描描述符的使用](#)”。

如果查询需要更多的扫描描述符，可使用以下方法之一进行补救：

- 重写查询，或使用临时表将它分为几个步骤。对于 DOL 锁定表，如果有许多表扫描，可以考虑增加索引。
- 如果表使用大量的参照完整性约束，可重新设计表的模式以使其使用较少的扫描描述符。可通过在执行查询前启用 `set showplan on`、`set noexec on`，来了解查询将使用多少扫描描述符。
- 增加 `number of aux scan descriptors` 的设置值。

以下各节说明如何使用 `sp_monitorconfig` 监视当前和高水印时的使用情况，以避免用完描述符；以及如何估计所需扫描描述符的数量。

监控扫描描述符的使用

sp_monitorconfig 报告未使用（可用）的扫描描述符的数量、当前正在使用的辅助扫描描述符数量、处于活动状态的百分比以及自从服务器上上次启动后所使用的扫描描述符的最大值。在高峰期定时运行该命令以监控扫描描述符的使用情况。

此示例显示配置了 500 个描述符的扫描描述符的使用情况：

```
sp_monitorconfig "aux scan descriptors"

Usage information at date and time:Apr 22 2002  2:49PM.
Name                num_free   num_active pct_act      Max_Used Reused
-----
number of aux              260           240  48.00          427  NA
```

只有 240 个辅助扫描描述符正被使用，留下 260 个没有使用。但是，自最近一次启动 Adaptive Server 后任意时刻使用的扫描描述符的最大数量为 427，留下大约 20% 以备使用增长和非常繁忙的高峰使用时所需。“Re-used” 不适用于扫描描述符。

估计和配置辅助扫描描述符

若要估计扫描描述符，请使用：

- 1 通过运行启用 set showplan 和 set noexec 的查询，为引用超过 16 个用户表的任何查询或有大量参照约束的任何查询确定表引用的数量。如果需要辅助扫描描述符，用 showplan 报告所需的数量：

```
Auxiliary scan descriptors required: 17
```

报告的数量包括查询所需的所有辅助扫描描述符，包括所有用于工作进程的描述符。如果查询只包括参照约束，也可以使用 sp_helpconstraint，它可显示每个表参照约束的计数。
- 2 对于每个使用辅助扫描描述符的查询，可估计同时运行查询的用户数量并相乘。如果预计有 10 个用户要运行需要 8 个辅助描述符的查询，则一次需要的总数为 80。
- 3 对每个查询的结果求和以计算所需辅助扫描描述符的数量。

number of backup connections

摘要信息	
缺省值	0
值的范围	1 - 32768
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	用户环境

number of backup connections 设置 Backup Server 建立的用于转储或装载内存中数据库的用户连接的最大数量。由于 Backup Server 在您运行 dump 或 load database 时需要为每个设备使用一个用户连接，并且需要额外的连接来运行 dump database 命令，因此 number of backup connections 的值限制存档数据库的设备数。

number of backup connections 是一个限制，并且不会消耗任何资源。将 number of backup connections 设置为 0 意味着 Backup Server 可使用最大数量的用户连接。

number of ccbs

摘要信息	
缺省值	0
值的范围	0 - 100
状态	静态
显示级别	
要求的角色	
配置组	诊断

留作将来使用。

number of checkpoint tasks

摘要信息	
缺省值	1
有效值	1 - 8
状态	动态
显示级别	Comprehensive

摘要信息

要求的角色	系统管理员
配置组	备份 / 恢复

number of checkpoint tasks 配置并行检查点。**number of checkpoint tasks** 的值必须小于或等于启动时的引擎数。该参数的最大值受到配置参数 **number of engines online at startup** 和 **number of open databases** 的值的限制，最大值为 8。

缺省值将串行检查点设置为缺省行为。

number of devices**摘要信息**

缺省值	10
值的范围	1 - 2,147,483,647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	磁盘 I/O、内存使用

number of devices 控制 Adaptive Server 可使用的数据库设备数。它不包括用于数据库或事务日志转储的设备。

在执行 **disk init** 时，尽管虚拟设备号 (**vdevno**) 是可选的，但您也可以分配此值。如果不分配 **vdevno**，Adaptive Server 则会分配下一个可用虚拟设备号。

如果分配了虚拟设备号，在 Adaptive Server 所使用的设备号当中，每个设备号都必须具有唯一性。数字 0 是专为主设备保留的。您可以输入处于有效值范围内的任意未使用的设备号。

若要确定当前正在使用哪些号码，请输入：

```
select vdevno from master..sysdevices
       where status & 2 = 2
```

其中，“status 2”指定物理磁盘。

注释 UNIX 平台：如果您正在使用大量设备，Sybase 建议您首先在配置文件中设置适当数量的设备和用户连接，然后重新启动 Adaptive Server。尝试用 **sp_configure** 动态配置大量设备可能会失败。

number of dtx participants

摘要信息	
缺省值	500
有效值	100 - 2147483647
状态	动态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理、内存使用

`number of dtx participants` 设置 Adaptive Server 事务协调服务可以同时传播和协调的远程事务的总数。DTX 参与者是协调服务用于管理远程事务分支的内部内存结构。当事务被传播到远程服务器时，协调服务必须获得新的 DTX 参与者来管理这些分支。

将 `number of dtx participants` 设置为小于缺省值的数字会减少服务器能够管理的远程事务的数量。如果没有可用的 DTX 参与者，就无法启动新的分布式事务。如果没有可用的 DTX 参与者传播新的远程事务，则正在进行的分布式事务可能会中止。

将 `number of dtx participants` 设置为大于缺省值的数字会增加 Adaptive Server 能够处理的远程事务分支的数量，但占用的内存也更多。

针对系统优化 DTX 参与者的数量

在高峰期间，可使用 `sp_monitorconfig` 检查 DTX 参与者的使用情况：

```
sp_monitorconfig "number of dtx participants"

Usage information at date and time: Apr 22 2002 2:49PM.
Name                num_free  num_active  pct_act    Max_Used   Reused
-----
number of dtx       80        20          4.00      210        NA
```

如果 `num_free` 值为零或非常低，则新的分布式事务可能会由于缺少 DTX 参与者而无法启动。可考虑增加 `number of dtx participants` 的值。

较低的 `Max_used` 值可能表示未使用的 DTX 参与者会占用可供其它服务器功能使用的内存。可考虑减少 `number of dtx participants` 的值。

number of dump threads

摘要信息	
缺省值	禁用
值的范围	1（禁用，无并行）- 8（完全并行）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	组诊断

number of dump threads 控制 Adaptive Server 为执行内存转储而产生的线程数。使用合适的 **number of dump threads** 值可以减少内存转储过程中引擎停止的时间。

在确定内存的线程数时：

- 如果计算机有足够的可用内存供文件系统高速缓存来保存整个内存转储，则使用值 8。
- 如果不知道计算机是否有足够的可用内存，**number of dump threads** 的值取决于许多因素，包括 I/O 系统的速度、磁盘速度、控制器的高速缓存、转储文件是否存在于在几个磁盘上创建的逻辑卷管理器中等。
- 在执行内存转储时如果不停止引擎，则禁用并行处理（通过分配值 1），如下所述。

当 Adaptive Server 执行内存转储时，所创建的文件数等于所分配的内存段数的总和乘以已配置的线程数。Adaptive Server 使用独立的线程写入独立的文件。此作业完成后，引擎重新启动，并且文件被合并到目标转储文件中。因此，以并行方式转储共享内存所用的时间大于以串行方式转储共享内存所用的时间。

- 如果在内存转储过程中停止引擎，则使用除 1 以外的其它值可能会减少转储内存时引擎停止的时间。

number of engines at startup

摘要信息	
缺省值	1
值的范围	1 — 计算机上的 CPU 数
状态	静态
显示级别	Basic

摘要信息	
要求的角色	系统管理员
配置组	Java 服务、内存使用、处理器

Adaptive Server 允许用户使所有引擎脱机，引擎 0 除外。

number of engines at startup 专门用于启动时设置要联机的引擎数。它在设置联机的引擎数方面提供了非常大的灵活性，但也受一定的约束，即不能将 **number of engines at startup** 的值设置为大于计算机上的 CPU 数，或大于 **max online engines** 的配置。如果不希望启动后使引擎联机，应将 **max online engines** 和 **number of engines at startup** 设置为相同的值。如果 **number of engines at startup** 和 **max online engines** 的值不同，则每个引擎大约浪费 1.8 MB 内存。

number of histogram steps

摘要信息	
缺省值	20
值的范围	3 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

number of histogram steps 指定直方图中的梯级数。

number of index trips

摘要信息	
缺省值	0
值的范围	0 - 65535
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	高速缓存管理器

number of index trips 指定在考虑将一个旧索引页换出前，该页遍历最近使用最多的 / 最近使用最少的 (MRU/LRU) 链的次数。如果增加了 **number of index trips** 的值，则索引页在高速缓存中将保留更长的时间。

数据高速缓存将被作为 MRU/LRU 链执行。当用户线程访问数据和索引页时，这些页被放置在高速缓存的 MRU/LRU 链的 MRU 末端。在一些事务密集环境（和基准值）中，您可能需要将索引页保留在高速缓存中，因为很可能不久需要再次使用它们。如果设置较高的 **number of index trips** 参数值，则使索引页在高速缓存中保留的时间更长；而如果设置较低的值，则可以将索引页立即换出高速缓存。

无法为宽松的 LRU 页设置 **number of index trips**。请参见《系统管理指南：卷 2》中的第 4 章“配置数据高速缓存”。

注释 如果索引使用的高速缓存相对较小（特别是如果它与其它对象共享空间），而事务量很大，则不要将 **number of index trips** 设置得太高。高速缓存可能会被大量没有过期的页占用，这可能会导致等待高速缓存空间的进程超时。

在将 **number of index trips** 的值更改为非零数字之前，请确保应用程序有足够的高速缓存来存储所有索引、OAM 和数据页。在更改 **number of index trips** 的值之前，请咨询 Sybase 技术支持部门。

number of java sockets

摘要信息	
缺省值	0
有效值	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Java 服务、内存使用

number of java sockets 实现 Java VM 和 java.net 类 Sybase 支持。

number of large i/o buffers

摘要信息	
缺省值	6
有效值	1 - 256
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	磁盘 I/O、内存使用、SQL Server 管理

number of large i/o buffers 设置分配单元大小的缓冲区的数目，这些缓冲区是预留给某些 Adaptive Server 实用程序的，用于执行大 I/O。这些大 I/O 缓冲区主要由 **load database** 命令使用，该数据库使用一个缓冲区来装载数据库，而坏考虑它指定的设备数。**load database** 然后使用最多 32 个缓冲区来清除它装载的数据库页。**load transaction** 不使用这些缓冲区。若需同时执行六个以上 **load database** 命令，请为每个 **load database** 命令配置一个大 I/O 缓冲区。

create database 和 **alter database** 在清除数据库页时，会将这些缓冲区用于大 I/O。**create database** 或 **load database** 的每个实例可使用最多 32 个大 I/O 缓冲区。

磁盘镜像和一些 **dbcc** 命令也使用这些缓冲区。

注释 在 Adaptive Server 12.5.0.3 版和更高版本中，大 I/O 缓冲区的大小是一个分配（256 页），而不是一个扩充（8 页）。因此服务器需要对大缓冲区分配更多内存。例如，早期版本中需要 8 页的内存的磁盘缓冲区现在需要 256 页内存。

number of locks

摘要信息	
缺省值	5000
值的范围	1000 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	锁管理程序、内存使用

number of locks 设置可供 Adaptive Server 上所有用户使用锁的总数。Adaptive Server 需要的锁的数目取决于并发和并行的进程数目，以及事务所执行的操作的类型。若要查看在某个特定时间正在使用的锁的数目，请使用 **sp_lock**。

对于串行操作，Sybase 建议开始时为每个活动的并发连接分配 20 个锁。并行执行的操作要求的锁比串行执行要多。例如，如果发现查询平均使用五个工作进程，则尝试将为串行操作配置的 **number of locks** 增加三分之一。

如果系统用尽了所有锁， Adaptive Server 会显示一个服务器级的错误消息。如果用户收到报告锁错误，则您可能需要增加 number of locks ；但要记住锁会占用内存。请参见 《系统管理指南，卷 2》中的第 3 章“配置内存”。

注释 数据行锁定可能要求更改 number of locks 的值。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon （《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

number of mailboxes

摘要信息	
缺省值	30
值的范围	30 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、 SQL Server 管理

number of mailboxes 指定 Adaptive Server 所分配的邮箱结构数。与邮件一起使用的邮箱是由 Adaptive Server 内部使用的，用于在内核服务进程之间进行通信和同步。用户进程不使用邮箱。除非有 Sybase 技术支持部门的指导，否则不要修改此参数。

number of messages

摘要信息	
缺省值	64
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、 SQL Server 管理

number of messages 指定由 Adaptive Server 分配的消息结构数。与邮箱一起使用的邮件是由 Adaptive Server 内部使用的，用于在内核服务进程之间进行通信和同步。消息也用于在并行处理中进程系列之间进行协调。除非有 Sybase 技术支持部门的指导，否则不要修改此参数。

number of oam trips

摘要信息	
缺省值	0
值的范围	0 - 65535
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员

`number of oam trips` 指定在考虑将对象分配映射 (OAM) 页换出前, 该页遍历 MRU/LRU 链的次数。 `number of oam trips` 的值越高, 旧 OAM 页保留在高速缓存中的时间就会越长。

每个表、表上的每个索引都有一个 OAM 页, 其中包含分配给该表或索引的页的有关信息; 当该索引或表需要新的页时, 就会检查该页 (请参见第 195 页的“[page utilization percent](#)”。) 单个 OAM 页可以保存 2,000 到 63,750 个数据页或索引页的分配映射。

OAM 页指向每个分配单元的分配页, 对象使用这些分配单元中的空间。而分配页又跟踪分配单元中有关扩充和页使用情况的信息。

在某些涉及重要的空间分配 (即大批量复制操作) 的环境和基准中, 将 OAM 页较长时间地保留在高速缓存中会提高性能。如果将 `number of oam trips` 设置为较高的值, 则会将 OAM 页保留在高速缓存中。

注释 如果高速缓存相对较小并被大量的对象使用, 则不要将 `number of oam trips` 设置得太高。这样做可能导致高速缓存被大量没有过期的 OAM 页占用, 并且用户线程可能开始超时。

在将 `number of oam trips` 的值更改为非零数字之前, 请确保应用程序有足够的`高速缓存`来存储所有索引、OAM 和数据页。在更改 `number of oam trips` 的值之前, 请咨询 Sybase 技术支持部门。

number of open databases

摘要信息	
缺省值	12
值的范围	6 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存、SQL Server 管理

`number of open databases` 设置在 Adaptive Server 上能够同时打开的数据库的最大数量。

计算一个值时，应包括 `master`、`model`、`sybssystemprocs` 和 `tempdb` 系统数据库。如果已经安装了审计，则还包括 `sybsecurity` 数据库。计算还会包括样本数据库 `pubs2` 和 `pubs3`、语法数据库 `sybsyntax` 以及 `dbcc` 数据库 `dbccdb`（如果已经安装这些数据库）。

如果计划进行重大改动，例如从另一个服务器装载一个大数据库，请使用 `sp_helpconfig` 来估算元数据高速缓存大小。`sp_helpconfig` 显示给定数量的元数据描述符所需的内存量，以及给定内存能够容纳的描述符的数量。数据库元数据描述符代表了数据库的状态，即该数据库是正在使用还是在使用间隔被高速缓存。

❖ 优化 `number of open databases`

如果 Adaptive Server 显示一条消息，指出超出了允许的打开数据库的数目，则应调整该值。

- 1 使用 `sp_countmetadata` 查找数据库元数据描述符的总数：

```
sp_countmetadata "open databases"
```

运行 `sp_countmetadata` 的最佳时间是在服务器几乎没有活动的时候。在高峰期运行 `sp_countmetadata` 会导致该系统过程与其它进程的争用。

假设 Adaptive Server 报告以下信息：

```
There are 50 databases, requiring 1719 Kbytes of
memory.The 'open databases' configuration parameter
is currently set to 500.
```

- 2 将 `number of open databases` 的值配置为 50：

```
sp_configure "number of open databases", 50
```

这个新的配置数仅仅是一个起点，请根据活动的元数据数据库高速缓存描述符数（而非数据库总数）来确定理想大小。

- 3 在高峰期间查找活动的元数据描述符的数目：

```
sp_monitorconfig "open databases"
```

```
Usage information at date and time: Apr 22 2002 2:49PM.
```

Name	num_free	num_active	pct_act	Max_Used	Reused
-----	-----	-----	-----	-----	-----
number of open	50	20	40.00	26	No

在此示例中，有 20 个元数据数据库描述符处于活动状态；自服务器上次启动以来一直处于活动状态的描述符最多有 26 个。

请参见《参考手册：过程》中的 `sp_monitorconfig` 了解详细信息。

- 4 将 `number of open databases` 配置为 26，再加上 10% 的额外空间（大约是 3），则总共为 29:

```
sp_configure "number of open databases", 29
```

如果服务器上有许多活动，例如正在增加或减少数据库，则要定期运行 `sp_monitorconfig`。当活动描述符数发生变化时，请重置高速缓存大小。

number of open indexes

摘要信息	
缺省值	500
值的范围	100 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存

`number of open indexes` 设置可在 Adaptive Server 上同时使用的索引的最大数量。

如果计划进行大量更改，例如从其它服务器装载一个具有大量索引的数据库，请使用 `sp_helpconfig` 估算元数据高速缓存的大小。`sp_helpconfig` 显示了给定数量的元数据描述符所要求的内存量，以及可以被给定内存容量容纳的描述符的数量。索引元数据描述符代表索引的状态，即该索引是正在使用还是在使用间隔被高速缓存。

❖ **优化 `number of open indexes`**

如果 `number of open indexes` 的缺省值不够，则 Adaptive Server 在尝试重新使用活动索引描述符后将显示一条消息，并且您必须调整此值。

- 1 使用 `sp_countmetadata` 查找索引元数据描述符的总数:

```
sp_countmetadata "open indexes"
```

运行 `sp_countmetadata` 的最佳时间是在服务器几乎没有活动的时候。在高峰期运行 `sp_countmetadata` 会导致该系统过程与其它进程的争用。

假设 Adaptive Server 报告以下信息:

```
There are 698 user indexes in all database(s),
requiring 286.289 Kbytes of memory.The 'open
indexes' configuration parameter is currently set to
500.
```

- 2 将 `number of open indexes` 参数配置为 698:

```
sp_configure "number of open indexes", 698
```

这个新配置只是一个起点，请根据活动的索引元数据高速缓存描述符数（而不是索引总数）来确定理想大小。

- 3 在高峰期间查找活动的索引元数据描述符的数目:

```
sp_monitorconfig "open indexes"
```

Usage information at date and time: Apr 22 2002 2:49PM.

Name	num_free	num_active	pct_act	Max_Used	Reused
number of open	182	516	73.92	590	No

在这个示例中，自从上一次启动服务器后已经使用的索引描述符的最大数量是 590。

请参见《参考手册：过程》中的 `sp_monitorconfig`。

- 4 将 `number of open indexes` 配置参数配置为 590，再加上 10% 的额外空间 (59)，则总共为 649:

```
sp_configure "number of open indexes", 649
```

如果服务器上有许多活动，例如正在增加或删除表，则要定期运行 `sp_monitorconfig`。当活动描述符数发生变化时，请重置高速缓存大小。

number of open objects

摘要信息	
缺省值	500
值的范围	100 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存、SQL Server 管理

`number of open objects` 设置在 Adaptive Server 上能够同时打开的对象的 maximum 数量。

如果计划进行大量更改，例如从其它服务器装载一个具有大量对象的数据库，请使用 `sp_helpconfig` 重新估算元数据高速缓存的大小。`sp_helpconfig` 显示了给定数量的元数据描述符所要求的内存量，以及可以被给定内存量容纳的描述符的数量。对象元数据描述符代表对象的状态，即该对象是正在使用还是在用间隔被高速缓存。

❖ **优化 `number of open objects`**

如果缺省的 `number of open objects` 不够，则 Adaptive Server 在尝试重新使用活动的对象描述符后将显示一条消息。

- 1 使用 `sp_countmetadata` 查找对象元数据高速缓存描述符的总数：

```
sp_countmetadata "open objects"
```

运行 `sp_countmetadata` 的最佳时间是在服务器几乎没有活动的时候。在高峰期运行 `sp_countmetadata` 会导致该系统过程与其它进程的争用。

假设 Adaptive Server 报告此信息：

```
There are 1340 user objects in all database(s),
requiring 1443 Kbytes of memory.The 'open objects'
configuration parameter is currently set to 500.
```

- 2 将 `number of open objects` 配置为适合打开的对象数：

```
sp_configure "number of open objects", 1407
```

1407 包含临时表容纳的 1340 个用户对象加上其 5% 的用户对象。

这个新配置只是一个起点；请根据活动的对象元数据高速缓存描述符数（而不是对象总数）来确定理想大小。

- 3 在高峰期间查找活动的元数据高速缓存描述符的数目：

```
sp_monitorconfig "open objects"

Usage information at date and time: Aug 20 2007 1:32PM..
Name                               Num_free   Num_active  Pct_act     Max_Used
Num_reuse
-----
number of open objects             560         847         71.40       1497
0
```

在这个示例中，自从上一次启动服务器后已经使用的对象描述符的最大数量是 1497。

- 4 将 number of open objects 配置 1397，再加上 10% (140)，则总共为 1537：

```
sp_configure "number of open objects", 1537
```

如果服务器上有许多活动，例如正在增加或删除表，则要定期运行 `sp_monitorconfig`。当活动描述符数发生变化时，请重置高速缓存大小。请参见《参考手册：过程》中的 `sp_monitorconfig`。

number of open partitions

摘要信息	
缺省值	500
值的范围	100 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存

指定 Adaptive Server 可同时访问的分区数。

为系统优化 *number of open partitions* 参数

如果 number of open partitions 的缺省值不足，则 Adaptive Server 在尝试重新使用活动分区描述符后将显示一条消息。该值必须调整。

- 1 使用 `sp_countmetadata` 查找打开的分区总数。例如：

```
sp_countmetadata "open partitions"
```

运行 `sp_countmetadata` 的最佳时间是在服务器几乎没有活动的时候。在高峰期运行 `sp_countmetadata` 会导致该系统过程与其它进程的争用。

假设 Adaptive Server 报告以下信息：

```
There are 42 user partitions in all database(s),
requiring 109 Kbytes of memory.The 'open
partitions' configuration parameter is currently set
to 110.
```

- 2 将 number of open partitions 配置为 110，与 `sp_countmetadata` 报告的值相同：

```
sp_configure "number of open partitions", 110
```

3 在高峰期查找活动的元数据高速缓存描述符的数目，例如：

```
sp_monitorconfig "open partitions"
Usage information at date and time: Jun 30 2008 3:15PM.
```

Name	Num_free	Num_active	Pct_act
Max_Used			
Reuse_cnt			
-----	-----	-----	-----
number of open partitions	27	57	51.8
83			
0			

在本例中，83 为自上次启动服务器后，已经使用的分区描述符的数量最大值。

4 将 number of open partitions 配置为 83，再加上 10% (8)，则总共为 91：

```
sp_configure "number of open partitions", 91
```

如果服务器上有许多活动，例如正在增加或删除表，则要定期运行 `sp_monitorconfig`。当活动描述符数发生变化时，请重置高速缓存大小。请参见《参考手册：过程》中的 `sp_monitorconfig`。

number of pre-allocated extents

摘要信息	
缺省值	2
值的范围	1 - 32
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`number of pre-allocated extents` 指定在到页管理器的单个行程中分配的扩充（八页）数。目前，该参数仅被 `bcp` 用来在进行大量数据复制时提高性能。缺省情况下，`bcp` 一次分配两个扩充，并且每次都向日志中写入分配记录。

设置 `number of pre-allocated extents` 意味着 `bcp` 每次需要更多空间时，将分配指定数量的扩充，并为该事件写一条日志记录。

为对象分配的页有可能比实际需要的多，因此，在小批查询中使用 `bcp` 时，`number of pre-allocated extents` 的值应较低。如果在较大的批查询中使用 `bcp`，可增加 `number of pre-allocated extents` 的值，以减少分配页时的总开销并减少日志记录的数量。

为预先分配的扩充数使用值 32

为 number of pre-allocated extents 使用值 32 对于配置有特殊意义，并且会影响 Adaptive Server 内部执行的空间分配。如果您将 number of pre-allocated extents 设置为 32，则 Adaptive Server 会为实用程序操作（如 bcp-in 和 select into，两者均使用大规模的空间保留分配方案）保留值得扩充的整个分配单元。这将大大提升这些实用程序的性能，特别是当您在多个节点上同时运行这些实用程序时，情况尤为如此。因此，使用值 32 可保证集群的每个节点都能够在其自己的分配单元上独立工作，而不会相互干扰。

在 Adaptive Server 的早期版本中，number of pre-allocated extents 参数指定为所有大小的表保留在单个分配调用中的扩充数。

在 Adaptive Server 的此版本中，对于包含 240 页或更多页的大型表，将只会为以下命令忽略 number of pre-allocated extents 的值：

- alter table *table_name* add *column_name* ...
- alter table *table_name* modify *column_name* ...
- alter table *table_name* drop *column_name* ...
- alter table lock ...
- reorg rebuild

当在超过 240 页的表运行这些命令时，Adaptive Server 将保留整个分配单元（32 个扩充），从而大大提升了性能，特别是当您在多个节点上同时运行这些命令时，情况尤为如此。

对于少于 240 页的表，将继续为上述命令观察 number of pre-allocated extents 的值，而对于所有大小的表，将继续为所有命令（例如 select into、bcp、alter table partition）继续观察该值。

number of Q engines at startup

摘要信息	
缺省值	0
值的范围	0 - 127
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	处理器

number of Q engines at startu 是 MQ 所必需的，用于指定服务器在启动时可以联机的 Q 引擎数。您可能需要增加 max online engines 以适合 max online Q engines 数。

number of remote connections

摘要信息	
缺省值	20
值的范围	5 - 32767
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、网络通信

`number of remote connections` 指定向 Adaptive Server 同时可以互相开放的逻辑连接的数目。执行 ESP 时，每个同时连到 XP 服务器的连接都使用一个远程连接。请参见第 14 章 “管理远程服务器”。

number of remote logins

摘要信息	
缺省值	20
值的范围	0 - 32767
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、网络通信

`number of remote logins` 控制从 Adaptive Server 到远程服务器的活动用户连接的数目。执行 ESP 时，每个到 XP 服务器的同时连接最多使用一个远程登录。将该参数设置为等于或小于 `number of remote connections` 的值。请参见第 14 章 “管理远程服务器”。

number of remote sites

摘要信息	
缺省值	10
值的范围	0 - 32767
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、网络通信

number of remote sites 确定能够同时访问 Adaptive Server 的远程节点的最大数目。每个 Adaptive Server 到 XP Server 的连接都使用一个远程节点连接。

number of remote sites 在内部确定能够随时被激活的节点处理器的数目；所有从单个节点进行的服务器访问均通过单个节点处理器来管理。例如，如果将 number of remote sites 设置为 5，并且每个节点发出三个远程过程调用，则 sp_who 会显示处理这 15 个过程的 5 个节点处理器。请参见第 14 章 “管理远程服务器”。

number of sort buffers

摘要信息	
缺省值	500
值的范围	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

number of sort buffers 指定为用于在排序期间容纳从输入表中读取的页和执行索引合并的缓冲区分配的内存量。number of sort buffers 仅用于并行排序。当您执行以下操作时，将使用并行排序：

- 运行 updates statistics
- 创建索引

请参见 Performance and Tuning Series: Query Processing and Abstract Plans（《性能和调优系列：查询处理和抽象计划》）中的第 10 章 “Using Statistics to Improve Performance”（利用统计信息来提高性能）。

用于 number of sort buffers 的值取决于服务器的页大小。

Sybase 建议您将此参数的设置保持为缺省值，以并行方式创建索引时除外。

如将此值设置太高，会阻碍非排序进程访问用于执行排序进程的高速缓存中的缓冲池。

如果配置了很多排序缓冲区，则对大表进行排序时，可能需要更多的过程高速缓存。如果表中的行都比较短，效果就特别明显，因为每页的行数会很多。

可通过以下公式估算所需的过程高速缓存量（以字节为单位）：

(排序缓冲区数) X (每页行数) X 100

如果没有针对排序缓冲区数配置足够的过程高速缓存，排序可能会失败，同时出现错误消息 701。发生这种情况时，重新为 Adaptive Server 配置一个较小的排序缓冲区数，然后重试排序。

有关为运算符使用的缓冲区数设置上限的信息，请参见第 157 页的“max buffers per lava operator”。

number of user connections

摘要信息	
缺省值	25
值的范围	5 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、用户环境

number of user connections 设置可同时连接到 Adaptive Server 的最大用户连接数。它不是指最大进程数；最大进程数不仅仅取决于此参数的值，还取决于其它系统活动。

每个进程中允许的最大文件描述符数取决于操作系统；请参见所用平台的配置文档。

可用于 Adaptive Server 连接的文件描述符数目存储在全局变量 @@max_connections 中。可以使用以下语法报告系统可用文件描述符的最大数目：

```
select @@max_connections
```

返回值表示系统允许用于进程的文件描述符的最大数目，再减去开销。开销随引擎数的增加而增加。有关多重处理如何影响可用于 Adaptive Server 连接的文件描述符数的详细信息，请参见《系统管理指南：卷 2》中的第 5 章“管理多处理器服务器”。

另外，必须为以下各项保留一定的连接数（也可使用配置参数进行设置）：

- 数据库设备，包括镜像设备
- 节点处理器
- 网络监听器

number of user connections + (number of devices * max online engines * 2) + number of remote sites + max number network listeners 不能大于 @@max_connections 的值。

maximum number of user connections 的上限

保留的连接

在配置的这些连接中，有一个是专门保留用于临时管理任务，目的是为了确保数据库管理员可以连接到 Adaptive Server。保留的连接的总登录时间为 15 分钟，并且只能分配给具有 `sa_role` 的用户。15 分钟后，Adaptive Server 会终止连接，以确保有多个数据库管理员进行安装时该保留的连接的可可用性。

Adaptive Server 在客户端使用最后的资源连接到 Adaptive Server 时也会自动使用这一保留的连接。

如果 Adaptive Server 正在使用保留的连接，则当用户登录 Adaptive Server 时，会出现以下信息性消息：

```
There are not enough user connections available; you are being connected
using a temporary administrative connection which will time out after '15'
minutes. Increase the value of the 'number of user connections' parameter
```

当 Adaptive Server 上的最后一个连接因超时而终止时，Adaptive Server 还将在错误日志中记录类似如下内容的消息：

```
00:00000:00008:2003/03/14 11:25:31.36 server Process '16' has been
terminated as it exceeded the maximum login time allowed for such processes.
This process used a connection reserved for system administrators and has a
maximum login period of '15' minutes
```

优化 *max number of user connections*

没有用于确定每个用户允许的连接数的公式。必须根据系统和用户要求来估计此数目。还必须考虑到在多用户系统上，通常可在用户之间共享偶尔或暂时需要的连接。下面的进程需要用户连接：

- 运行 `isql` 的每个用户需要一个连接。
- 应用程序开发人员为每个编辑会话使用一个连接。
- 运行应用程序的用户需要的连接数取决于如何编写应用程序。执行 Open Client 程序的用户使用每个开放的 DB-Library dbprocess 或 Client-Library™ `cs_connection` 时都需要一个连接。

注释 Sybase 建议您在系统中增加物理设备或用户时，先估计 Adaptive Server 使用的最多连接数，并更新 `number of user connections`。定期使用 `sp_who` 来确定 Adaptive Server 上的活动用户连接数。

某些其它配置参数（包括 `stack size` 和 `default network packet size`）会影响用于每个用户连接的内存量。

共享内存的用户连接数 — EJB Server

Adaptive Server 使用 number of user connections 的值为 EJB Server 建立共享内存连接数。因此，如果 number of user connections 为 30，则 Adaptive Server 为 EJB Server 建立 10 个共享内存连接。共享内存连接不是用户连接的子集，也不能从用户连接数中减去。

若要增加共享内存的用户连接数，必须：

- 1 将 number of user connections 的值增加到所需共享内存连接数的三倍。
- 2 重新启动 Adaptive Server。

虽然 number of user connections 是一个动态配置参数，但是要更改共享内存用户连接数，还必须重新启动服务器。请参见 EJB Server Users Guide（《EJB Server 用户指南》）。

在 Adaptive Server 版本 12.5.3 ESD #2 中，不会自动为 EJB 保留套接字。但是，可以启动跟踪标志 1642，以还原早期版本的功能，从而为 EJB 保留三分之一的套接字。启用跟踪标志 1642 以设置 EJB Server。对于 Adaptive Server 的此版本，如果未配置 EJB Server，则可以忽略错误日志中的此消息：“hbc_ninit:No sockets available for HBC”。

在 Adaptive Server 12.5.3 版及更高版本中，如果 EJB 服务器已启用，且 HBC 套接字不可用，将报告以下消息：“hbc_ninit:No sockets available for HBC”。如果未启用跟踪标志 1642，请设置该标志，并重新启动 Adaptive Server。如果 EJB Server 未启用，则不报告任何消息，并且 Adaptive Server 将自动禁用为 EJB Server 保留的套接字。

number of worker processes

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、查询调优

number of worker processes 为所有同时运行的并行查询指定 Adaptive Server 可以随时使用的工作进程的最大数目。

如果没有足够的内存创建指定数目的工作进程，则 Adaptive Server 在启动时会发出警告消息。memory per worker process 控制分配给每个工作进程的内存。

如果尚未为工作线程池中足够多数量的线程配置 `number of worker processes`，Adaptive Server 将在运行时调整查询计划以使用较少的工作线程。如果 Adaptive Server 在运行时无法调整查询，则查询将依次重新编译。但是，如果 `alter table` 和 `execute immediate` 命令没有足够多的工作线程，将会中止这些命令。

o/s file descriptors

摘要信息	
缺省值	0
值的范围	节点特定
状态	只读
显示级别	Comprehensive
要求的角色	系统管理员
配置组	操作系统资源

`o/s file descriptors` 指示为操作系统配置的文件描述符的每个进程的最大数目。该参数是只读的，并且不能通过 Adaptive Server 进行配置。

许多操作系统允许配置每个进程的可用文件描述符数。请参见操作系统文档。

可用于 Adaptive Server 连接的文件描述符数（小于 `o/s file descriptors` 的值）存储在变量 `@@max_connections` 中。请参见第 186 页的“[maximum number of user connections 的上限](#)”。

object lockwait timing

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

`object lockwait timing` 控制 Adaptive Server 是否收集请求对象上的锁的计时统计信息。

open index hash spinlock ratio

摘要信息	
缺省值	100
值的范围	1 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存

`open index hash spinlock ratio` 设置由一个**螺旋锁**保护的索引元数据描述符散列表的数目。该参数只用于多重处理系统。

可通过散列表访问属于该表的所有索引描述符。在对该表执行查询时，Adaptive Server 使用散列表在它的 `sysindexes` 行中查找必要的索引信息。散列表是 Adaptive Server 用来快速检索信息的内部机制。

通常，不需要更改该参数。但在极少情况下，如果 Adaptive Server 出现争用散列螺旋锁的情况，则可能需要重置该参数。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon` （《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

有关配置螺旋锁比率的详细信息，请参见 《系统管理指南：卷 2》中的第 5 章 “管理多处理器服务器”。

open index spinlock ratio

摘要信息	
缺省值	100
值的范围	1 - 214748364
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存

`open index spinlock ratio` 指定由一个**螺旋锁**保护的索引元数据描述符的数目。

Adaptive Server 使用螺旋锁保护索引描述符，因为多个进程可以访问该索引描述符的内容。`open index spinlock ratio` 只用于多重处理系统。

为该参数指定的值定义每个螺旋锁的索引描述符比率。

如果太多的索引描述符共享一个螺旋锁，则可能会导致螺旋锁争用。使用 `sp_sysmon` 获取有关螺旋锁争用的报告。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon* （《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

如果 `sp_sysmon` 输出指示一个索引描述符螺旋锁争用大于 3%，请尝试减小 `open index spinlock ratio` 的值。

请参见 《系统管理指南：卷 2》中的第 5 章 “管理多处理器服务器”。

open object spinlock ratio

摘要信息	
缺省值	100
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	元数据高速缓存

`open object spinlock ratio` 指定由一个**螺旋锁**保护的**对象描述符**的数目。Adaptive Server 使用螺旋锁保护对象描述符，因为多个进程可以访问该对象描述符的内容。`open object spinlock ratio` 只用于多重处理系统。

该参数的缺省值是 100；服务器上每 100 个对象描述符配置 1 个螺旋锁。如果服务器只配置了一个引擎，则不管有多少个对象描述符，Adaptive Server 只设置一个对象描述符螺旋锁。

如果太多的对象描述符共享一个螺旋锁，则会导致螺旋锁争用。使用 `sp_sysmon` 获取有关螺旋锁争用的报告。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon* （《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

如果 `sp_sysmon` 输出指示一个对象描述符螺旋锁争用大于 3%，请尝试减小 `open object spinlock ratio` 参数的值。

请参见 《系统管理指南：卷 2》中的第 5 章 “管理多处理器服务器”。

optimization goal

摘要信息	
缺省值	allrows_mix
值的范围	allrows_oltp、 allrows_dss
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

优化的目标在于，通过一种便利方式使查询需求与最佳优化技术相称，从而确保最好地利用优化程序的时间和资源。 Adaptive Server 允许用户配置两个优化目标，可以指定三个级别：服务器级、会话级和查询级。

查询级高于会话级，会话级又高于服务器级。

利用这些优化目标可以选择一种最适合自己的查询环境的优化策略：

- allrows_oltp — 对于纯粹 OLTP 查询最有用的目标
- allrows_dss — 对于中等到高复杂性的可操作 DSS 查询最有用的目标

optimization timeout limit

摘要信息	
缺省值	10
值的范围	0 - 1000
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

optimization timeout limit 指定 Adaptive Server 在优化查询时可以花费的时间，该时间仅占估计的查询执行时间的一小部分。

值 0 表示没有优化超时。

page lock promotion HWM

摘要信息	
缺省值	200
值的范围	2 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

page lock promotion HWM（高位值）及 page lock promotion LWM（低位值）与 page lock promotion PCT（百分比）共同指定 Adaptive Server 尝试将页锁升级到表锁之前，在页锁定表或索引的单次扫描会话期间所允许的页锁数目。

当扫描会话期间需要的页锁数目上超出 page lock promotion HWM 时，Adaptive Server 将尝试获取表锁。page lock promotion HWM 值不能高于 number of locks。

有关扫描会话和设置页锁升级限制的更详细信息，请参见 Performance and Tuning Series: Locking and Concurrency Control（《性能和调优系列：锁定和并发控制》）。

page lock promotion HWM 的缺省值适用于大多数应用程序。若要避免表锁定，您可能需要增加该值。例如，如果您知道含有数千行的所有页锁定表和数据页锁定表中有 500 行要进行定期更新，则可以将 page lock promotion HWM 设置为 500，从而提高表的并发性。

也可以在对象级配置页锁定表和视图的锁升级。请参见《参考手册：过程》中的 sp_setrowlockpromote。

可使用 sp_sysmon，了解 page lock promotion HWM 参数的更改如何影响锁升级的数目。sp_sysmon 报告排它页锁升级到排它表锁的比例和共享页锁升级到共享表锁的比例。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

page lock promotion LWM

摘要信息	
缺省值	200
值的范围	2 - page lock promotion HWM 的值
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

page lock promotion LWM （低位值）及 page lock promotion HWM （高位值）与 page lock promotion PCT 指定 Adaptive Server 尝试将页锁升级到表锁之前，在页锁定表或索引的单次扫描会话期间所允许的页锁数目。

page lock promotion LWM 设置页锁定数目，如果低于该数目， Adaptive Server 将不会尝试向对象发出表锁。page lock promotion LWM 必须小于或等于 page lock promotion HWM。

page lock promotion LWM 的缺省值对于大多数应用程序而言已足够。如果 Adaptive Server 已用完所有的锁 （除了隔离事件），则应增加 number of locks。

请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon （《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。也可以在对象级别配置页锁升级。请参见 《参考手册：过程》中的 sp_setpglockpromote。

page lock promotion PCT

摘要信息	
缺省值	100
值的范围	1 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

如果对象持有锁的数目介于 page lock promotion LWM （低位值）和 page lock promotion HWM （高位值）之间， page lock promotion PCT 将基于表大小设置页锁的百分比，高于该值时， Adaptive Server 将尝试获取表锁。

请参见 Performance and Tuning Series: Locking and Concurrency Control（《性能和调优系列：锁定和并发控制》）。

page lock promotion PCT 的缺省值对于大多数应用程序而言已足够。
也可以在对象级别为页锁定对象配置锁升级。请参见《参考手册：过程》中的 sp_setpglockpromote。

page utilization percent

摘要信息	
缺省值	95
值的范围	1 - 100
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	磁盘 I/O

page utilization percent 用于在页分配期间控制 Adaptive Server 是否要扫描表的对象分配映射 (OAM)，以便查找未使用的页，或只是为表分配新的扩充。有关 OAM 的详细信息，请参见第 176 页的“[number of oam trips](#)”。可使用 page utilization percent 参数对包含非常大的表的服务器进行性能优化；它减少了增加新空间所需要的时间。

如果将 page utilization percent 设置为 100，Adaptive Server 首先会将所有 OAM 页扫描一遍，以查找分配给对象的未使用页，然后再分配新扩充。如果为此参数设置的值低于 100，则 Adaptive Server 将 page utilization percent 设置与分配给表的已使用页和未使用页的比率进行比较，如下所示：

$$100 * \text{used pages} / (\text{used pages} + \text{unused pages})$$

如果 page utilization percent 低于该比率，则 Adaptive Server 将分配新的扩充而不再搜索未使用的页。

例如，将数据插入一个 10GB 的表，该表具有 120 个 OAM 页，且仅有一个未使用数据页：

- page utilization percent 设置为 100 将指示 Adaptive Server 扫描全部 120 个 OAM 页以查找未使用的数据页。
- 如果 page utilization percent 设置为 95，则允许 Adaptive Server 给对象分配一个新的扩充，因为 95 低于已使用的页与已使用和未使用页的比率。

如果 `page utilization percent` 值较低，将会产生更多未使用的页。`page utilization percent` 值较高会减慢在非常大的表中分配页的速度，因为 Adaptive Server 在分配一个新的扩充前要执行 OAM 扫描以查找每个未使用的页。这样做会增加逻辑和物理 I/O。

如果页分配速度很慢（特别是在大量插入时），请降低 `page utilization percent` 的值，但应在插入数据后重置它。较低的设置会影响服务器上的所有表，并在所有表中产生未使用的页。

快速批量复制忽略 `page utilization percent` 设置，并且将一直分配新的扩充直到数据库中没有可用扩充时为止。

partition groups

摘要信息	
缺省值	1024
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存

`partition groups` 指定可由 Adaptive Server 分配的分区组的最大数目。分区组是 Adaptive Server 用于控制对表的单独分区的访问的内部结构。在升级的同时或在 `load database` 升级期间，使用分区组来取消 Adaptive Server 12.5.x 版及早期版本的分区。

缺省值允许最多打开 1024 个分区组和最多打开 2147483647 个分区。分区的实际数量可能会稍少一些，取决于分区的分组情况。

partition spinlock ratio

摘要信息	
缺省值	10
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、元数据高速缓存

对于运行有多个引擎的 Adaptive Server，`partition spinlock ratio` 设置由一个螺旋锁保护的分区描述符内的行数。

Adaptive Server 使用分区描述符管理对表分区的访问。每个分区描述符都存有一个分区的信息（例如，分区的最后一页），进程在访问该分区时必须使用这些信息。使用 **number of open partitions** 配置分区描述符。

partition spinlock ratio 的缺省值为每 10 个分区高速缓存设置 1 个螺旋锁。减少 **partition spinlock ratio** 的值对 Adaptive Server 的性能影响不大。默认设置对大多数服务器都是较为合适的。

请参见《系统管理指南：卷 2》中的第 5 章“管理多处理器服务器”。

pci memory size

摘要信息	
缺省值	64MB
有效值	0 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	用户环境

pci memory size 设置可插入组件接口 (PCI) 内存池的大小。在 PCI 桥下运行的所有可插入组件适配器 (PCA) 和 JVM 插件均共享一个专用的 PCI 内存池。如果将 **pci memory size** 设置为小于缺省值，则 Adaptive Server 将使用缺省大小。

此内存池完全专用于 PCI 桥和任何运行的可插入组件。与所有其它内存池相同，Adaptive Server 控制此内存池。但是，与其它内存池不同的是，PCI 内存池是在您初始化 PCI 桥时分配的，并且之后将不会增大。

per object statistics active

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

per object statistic active 控制 Adaptive Server 是否收集每个对象的统计信息。

percent database for history

摘要信息	
缺省值	20
有效值	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

`percent database for history` 指定总可用空间在为 `js_history` 表保留的 `sybmgmtldb` 中所占的百分比。如果有更多作业正在运行，或要存储已执行作业的历史记录以便将来查询，请增加 `percent database for history`。

percent database for output

摘要信息	
缺省值	30
有效值	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

`percent database for output` 指定总可用空间在为作业输出保留的 `sybmgmtldb` 中所占的百分比。如果有更多作业正在运行，而这些作业生成的大量输出必须加以存储以供将来查询，请增加缺省值。

percent history free

摘要信息	
缺省值	30
有效值	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

percent history free 指定保留的空间在应保持可用的 **sybmgmtdb** 中所占的百分比。例如，如果您使用缺省值，则 **Adaptive Server** 将在填充了 **sybmgmtdb** 的 70% 时开始清除最早的历史记录，以便为新记录腾出空间。

percent output free

摘要信息	
缺省值	50
有效值	0 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

指定保持可用的保留空间在为 **Job Scheduler** 输出保留的 **sybmgmtdb** 中所占的百分比。例如，如果使用缺省值，则 **Adaptive Server** 将在填充了 **sybmgmtdb** 的 50% 时开始清除最早的历史记录，以便为新记录腾出空间。

performance monitoring option

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

performance monitoring option 为 **BMC DBXray** 图形性能监控和诊断工具启用许可证。

permission cache entries

摘要信息	
缺省值	15
值的范围	1 - 2147483647
状态	动态
显示级别	Comprehensive

摘要信息	
要求的角色	系统管理员
配置组	内存使用、用户环境

permission cache entries 确定每个任务的高速缓存保护器的数目，会增加用于每个用户连接和工作进程的内存量。

关于用户权限的信息保存在权限高速缓存中。Adaptive Server 检查权限时，首先在许可高速缓存中查找；如果没有发现所需的权限，则在 **sysprotects** 表中查找。如果 Adaptive Server 在权限高速缓存中查找所需信息，并且无需读取 **sysprotects**，则该进程的速度会明显加快。

但是，仅当 Adaptive Server 检查用户权限而不是授予或撤销权限时，才在许可高速缓存中查找。授予或撤销权限时，整个许可高速缓存都被刷新。这是因为授予新权限或撤销权限时，现有权限的时间戳已过时。

如果 Adaptive Server 上的用户频繁执行需要检查用户权限的操作，则增加 **permission cache entries** 的值后，性能只能略有提高。这种效果不可能明显到足以保证广泛调优。

如果 Adaptive Server 上的用户频繁授予或撤销权限，则不要将 **permission cache entries** 的值设置得很大。用于权限高速缓存的空间会被浪费，因为高速缓存被每一 **grant** 和 **revoke** 命令刷新。

plan text pipe active

摘要信息	
缺省值	0
值的范围	0 - 1
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

plan text pipe active 确定 Adaptive Server 是否收集查询计划文本。如果同时启用 **plan text pipe active** 和 **plan text pipe max messages**，则 Adaptive Server 收集每个查询的计划文本。可以使用 **monSysPlanText** 针对所有用户任务检索查询计划文本。

plan text pipe max messages

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

`plan text pipe max messages` 确定 Adaptive Server 存储的每个引擎的查询计划文本消息数。monSQLText 表中的消息总数等于 `sql text pipe max messages` 的值与正在运行的引擎数的乘积。

print deadlock information

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开），2（打开，输出摘要）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

`print deadlock information` 将死锁信息输出到错误日志。

如果遇到循环死锁，可将 `print deadlock information` 设置为 1，以在错误日志中提供用于跟踪死锁起因的详细信息。然而，将 `print deadlock information` 设置为 1 可能会降低 Adaptive Server 的性能。因此，只有在尝试确定死锁的原因是才将 `print deadlock information` 设置为打开。

可使用 `sp_sysmon` 的输出结果，确定是否在应用程序中产生了死锁。如果发生死锁，可将 `print deadlock information` 设置为 1 以深入了解起因。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon`（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

如果值为 2，您可将死锁信息的摘要输出到错误日志（与值 1 提供的详细信息相对）。例如：

```
Deadlock Id 34:Process (Familyid 0, Spid 70) was waiting for a 'exclusive page'
lock on page 10858346 of the 'equineline_job' table in database 18 but process
(Familyid 0, Spid 88) already held a 'exclusive page' lock on it.
Deadlock Id 34:Process (Familyid 0, Spid 88) was waiting for a 'exclusive page'
lock on page 11540986 of the 'equineline_job' table in database 18 but process
(Familyid 0, Spid 70) already held a 'update page' lock on it.
```

print recovery information

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	备份 / 恢复

print recovery information 确定在恢复期间， Adaptive Server 在主控台上显示的信息。在 Adaptive Server 启动和装载数据库转储时，会对每个数据库执行恢复）。缺省值表示 Adaptive Server 只显示数据库名以及一条表明恢复正在进行中的消息。值 1 表示 Adaptive Server 会显示在恢复期间处理的每一单独事务的有关信息，包括该事务是被中止还是已被提交。

procedure cache size

摘要信息	
缺省值	7000
值的范围	7000 - 2147483647
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	内存使用、SQL Server 管理

指定过程高速缓存的大小（以 2K 页为单位）。 Adaptive Server 在运行存储过程时使用过程高速缓存。如果服务器发现高速缓存中已经有了一个过程的副本，则它就不需要从磁盘上读取该过程。 Adaptive Server 在创建存储过程时还使用过程高速缓存中的空间来编译查询。

由于不同应用程序的 `procedure cache size` 最优值不同，因此重置最优值可能会提高 Adaptive Server 的性能。例如，如果运行了许多不同的过程或即席查询，应用程序则使用大量的过程高速缓存，因此可能需要增加该参数的值。

警告！ 如果 `procedure cache size` 太小，Adaptive Server 性能将降低。

如果您正在升级，`procedure cache size` 则被设置为升级时原始过程高速缓存的大小。

procedure deferred compilation

摘要信息	
缺省值	1（启用）
值的范围	0 - 1
状态	动态
显示级别	
要求的角色	系统管理员
配置组	查询调优

如果启用此参数，对于引用本地变量或存储过程中的临时变量的语句而言，编译这些语句的操作将推迟到执行时进行，因此在优化这些语句时可能会使用运行时值，而不是估计值或幻数。

process wait events

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

`process wait events` 控制 Adaptive Server 是否收集每个任务的每个等待事件的统计信息。您可以使用 `monProcessWaits` 获取特定任务的等待信息。

请参见《Transact-SQL 用户指南》中的第 17 章“使用存储过程”。

prod-consumer overlap factor

摘要信息	
缺省值	20
值的范围	
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	

prod-consumer overlap factor 会影响优化。Adaptive Server 更改了 group by 算法，因此不能将 set statistics I/O 与并行计划一起使用。

quorum heartbeat interval

摘要信息	
缺省值	5
有效值	1 - 60
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

quorum heartbeat interval 指定仲裁心跳间隔的秒数。将 quorum heartbeat interval 设置为较低的值会增加心跳开销，但可加快检测丢失的磁盘链接的速度，从而对于已设置 I/O 防护或已丢失其 SAN 链接的实例而言，将能够更快地终止。将 quorum heartbeat interval 设置为较高的数字可减少心跳开销，但会延迟丢失的磁盘链接的检测。

quorum heartbeat retries

摘要信息	
缺省值	2
有效值	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

read committed with lock

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	锁管理程序

read committed with lock 确定在 **select** 查询期间，使用事务隔离级别 1（读提交）的 Adaptive Server，持有的是仅数据锁定表的行共享锁还是页共享锁。对于游标，**read committed with lock** 只适用于声明的只读游标。

对于事务隔离级别 1，所有页锁定表上的 **select** 查询继续在当前位置持有页上的锁。DOL 锁定表上的所有可更新的游标也在当前页或行上持有锁。请参见 Performance and Tuning Series: Monitoring Adaptive Server with **sp_sysmon**（《性能和调优系列：用 **sp_sysmon** 监控 Adaptive Server》）中的第 3 章“Using Engines and CPUs”（使用引擎和 CPU）。

recovery interval in minutes

摘要信息	
缺省值	5
值的范围	1 - 32767
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	备份 / 恢复

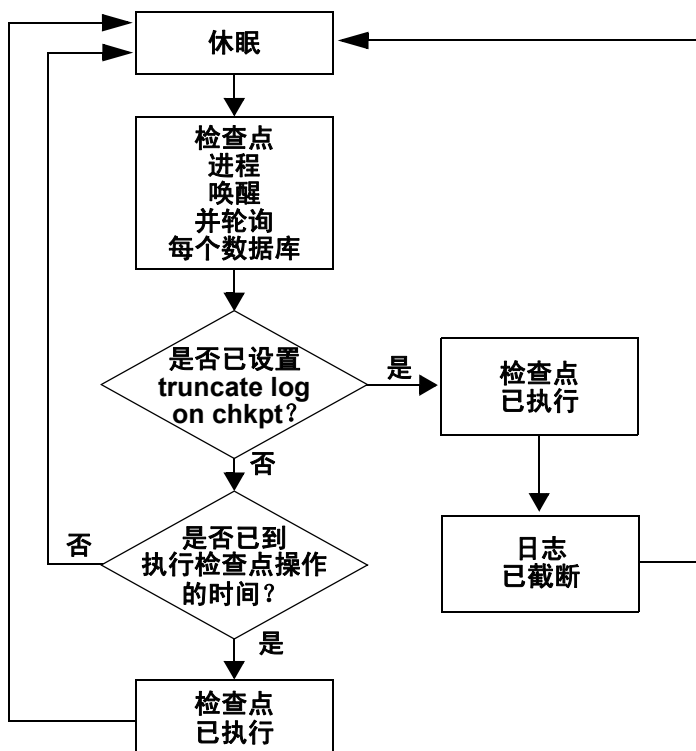
recovery interval in minutes 设置每个数据库所需时间的最大值（以分钟为单位），当出现系统故障时，Adaptive Server 将使用该值完成其恢复过程。恢复过程会以正向或反向滚动处理事务，从检查点进程指明的最早的活动事务开始。**recovery interval in minutes** 的值决定恢复过程的工作量大小。

Adaptive Server 估计恢复事务日志中 6000 行的时间需要 1 分钟的时间。但是，不同类型的日志记录所需的恢复时间会有所不同。如果将 `recovery interval in minutes` 设置为 3，则只有当 `syslogs` 从上一个检查点算起包含的行多于 18,000 行时检查点进程才将发生更改的页写入磁盘。

注释 恢复间隔对以下事务没有影响：在 Adaptive Server 发生故障时处于活动状态、长期运行且记入日志内容很少的事务（例如 `create index`）。恢复这些事务所花费的时间可能与运行它们所花费的时间相等。为了避免长时间的延迟，在索引维护操作之后转储每个数据库。

Adaptive Server 使用 `recovery interval in minutes` 设置以及每个数据库的活动量来决定何时对每个数据库执行检查点操作。当 Adaptive Server 对数据库执行检查点操作时，它将所有的脏页（在高速缓存中已被修改的数据页）写入磁盘。这可能会导致在很短时间内产生大量 I/O，称为“检查点测试信号”。检查点还执行其它维护任务，其中包括设置了 `truncate log on chkpt` 选项的数据库的事务日志截断。休眠的检查点进程大约每分钟“唤醒”一次，检查 `truncate log on chkpt` 设置和恢复间隔，以确定是否需要执行检查点操作。图 5-4 显示了 Adaptive Server 在该进程中所用的逻辑。

图 5-4：检查点进程



如果应用程序和其用途改变，最好更改恢复间隔。例如，当 Adaptive Server 上的更新活动增加时，您最好缩短恢复间隔。缩短恢复间隔会导致更频繁地执行检查点进程，检查点测试信号也会随之减弱但更频繁，同时系统速度略微减慢。但是，如果将恢复间隔设置得太高，则可能会导致恢复时间过长而不可接受。可通过重新配置 `housekeeper freewrite percent` 参数来减少由检查点操作产生的测试信号。请参见第 131 页的“[housekeeper free write percent](#)”。有关 `recovery interval in minutes` 对性能的影响的详细信息，请参见 Performance and Tuning Series: Basics（《性能和调优系列：基础知识》）中的第 3 章“Using Engines and CPUs”（使用引擎和 CPU）。

使用 `sp_sysmon` 以确定特定恢复间隔对系统的影响。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon`（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

remote server pre-read packets

摘要信息	
缺省值	3
值的范围	3 - 255
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、网络通信

remote server pre-read packets 确定在连接远程服务器期间，一个节点处理器 “预读” 的包的数目。

为了减少所需的连接数，两台服务器之间的通信是通过单个节点处理器管理的。在接收进程准备接收用户进程的数据包之前，节点处理器可以预读取并跟踪这些数据包。

remote server pre-read packets 的缺省值对大多数服务器都是合适的。增加该值会占用更多内存；减少该值则可能会减慢服务器之间网络通信的速度。请参见第 14 章 “管理远程服务器”。

restricted decrypt permission

摘要信息	
缺省值	0
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Basic
要求的角色	系统安全员
配置组	与安全性相关的参数

restricted decrypt permission 在所有数据库中启用或禁用受限制的解密权限。您必须让 sso_role 来设置此参数。

restricted decrypt permission 设置为 0（关闭）时，对加密列的解密权限与 15.0.2 以前的版本中的作用相同：

- 表所有者或 SSO 会显式授予解密权限。但是，支持解密权限的 with grant 选项。

- 解密权限会通过所有权链隐式授予表所有者和 SSO，并授予任何用户。例如，如果用户 Fred 拥有 proc1 存储过程，该过程会从加密列 fred.table1.col1 选择数据，如果 Fred 将对 proc1 的 exec 权限授予 Harry，则 Harry 将拥有对 fred.table1.col1 的隐式解密权限。
- alter table decrypt 不需要解密权限。原因是表所有者拥有对加密列的隐式解密权限。

当 restricted decrypt permission 设置为 1（开启）时：

- 只会将解密权限隐式授予 SSO。
- SSO 可以使用 with grant option 参数授予解密权限。这允许 SSO 决定系统中谁可授予解密权限。例如，如果 SSO 希望 user1 能够授予对 user3.user3_tab 的 decrypt permission，则该 SSO 会发出：

```
grant decrypt on user3.user3_tab to user1
with grant option
```

如果使用系统加密口令，则 Sybase 建议您不要对 DBO 授予解密权限，以保护数据的隐私。通过用户口令访问密钥可防止 DBO 和其他方访问数据，除非他们具有密钥口令，然而，这对于 DBO 而言，决定哪些用户应该看到解密数据也十分方便。如果您不使用用户指定口令来保护密钥和数据，则 SSO 应该保留角色职责以授予解密权限。

- 表所有权不会给予用户隐式解密权限。也就是说，如果使用加密列创建表，则您对这些列没有解密权限，除非已显式授予您这些权限。
- 不会通过所有权链隐式授予用户解密权限。例如，如果 Fred 拥有 proc1 存储过程，该过程会从加密列 fred.table1.col1 选择数据，如果 Fred 将对 proc1 的 exec 权限授予 Harry，则 Harry 还必须拥有对 fred.table1.col1 的显式解密权限才能看到数据。
- 具有别名的用户会假定他们对其具有别名的用户的权限。同样，如果具有 sa_role 的用户对任何数据库中的 DBO 具有隐式别名，则会继承已显式授予 DBO 的任何解密权限。
- alter table decrypt 语句需要解密权限，因为表所有者不具有对表的隐式解密权限。

如果将 restricted decrypt permission 从 0 更改为 1，则使用隐式解密权限的当前正在运行的语句将完成；但是，后面的任何使用隐式解密权限的语句将因以下错误而失败，直至 SSO 授予用户必要列的解密权限为止：

```
Msg 10330 "DECRYPT permission denied on object object_name, database
database_name, owner owner_name."
```

如果将 `restricted decrypt permission` 从 1 更改为 0，则反应显式授予的行会保留在 `sysprotects` 系统表中。然而，这些行对于隐式授予的解密权限没有影响，因为 Adaptive Server 不会检查 `sysprotects` 以确保解密权限可以隐式授予。`sp_helprotect` 只为以下用户显示误导信息：在重新配置系统之前被授予或撤消显式解密权限的用户，以及现在具有隐式解密权限的用户。

Sybase 建议您在启用或禁用 `restricted decrypt permission` 之间切换之前，撤消授予用户的任何显式解密权限，以保持系统一致性。

有关解密权限的详细信息，请参见 《加密列用户指南》。

row lock promotion HWM

摘要信息	
缺省值	200
值的范围	2 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

`row lock promotion HWM`（高位值）与 `row lock promotion LWM`（低位值）以及 `row lock promotion PCT` 指定: Adaptive Server 尝试将行锁升级到表锁之前，在表或索引的单次扫描会话期间所允许的最大行锁数目。

如果扫描会话期间获取的锁数目超过了 `row lock promotion HWM`，Adaptive Server 将试图获取表锁。`lock promotion HWM` 值不能高于 `number of locks` 值。

请参见 Performance and Tuning Series: Locking and Concurrency Control（《性能和调优系列：锁定和并发控制》）。

`row lock promotion HWM` 的缺省值适用于大多数应用程序。若要避免表锁定，您可能需要增加 “`row lock promotion HWM`” 的值。例如，如果含有数千行的表中有 500 行要进行定期更新，则可以将 `row lock promotion HWM` 设置为 500 左右，从而提高表的并发性。

也可以在对象级别配置行锁升级。请参见 《参考手册：过程》中的 `sp_setpglockpromote`。

row lock promotion LWM

摘要信息	
缺省值	200
值的范围	2 - row lock promotion HWM 的值
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

row lock promotion LWM（低位值）与 row lock promotion HWM（高位值）以及 row lock promotion PCT 指定：Adaptive Server 尝试将行锁升级到表锁之前，在表或索引的单个扫描会话期间所允许的行锁数目。

row lock promotion LWM 设置锁的数目，低于该数值时 Adaptive Server 不会尝试在对象上获取表锁。row lock promotion LWM 必须小于或等于 row lock promotion HWM。

row lock promotion LWM 的缺省值适用于大多数应用程序。如果 Adaptive Server 已用完所有的锁（除了隔离事件），则应增加 number of locks。

请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

也可以在对象级别配置锁升级。请参见《参考手册：过程》中的 sp_setpglockpromote。

row lock promotion PCT

摘要信息	
缺省值	100
值的范围	1 - 100
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	锁管理程序、SQL Server 管理

如果对象持有锁的数目介于 row lock promotion LWM（低位值）和 row lock promotion HWM（高位值）之间，row lock promotion PCT 将基于表中的行数设置行锁的百分比，高于该值时，Adaptive Server 将尝试获取表锁。

row lock promotion PCT 的缺省值适用于大多数应用程序。

有关设置锁升级限制的详细信息，请参见 Performance and Tuning Series: Locking and Concurrency Control （《性能和调优系列：锁定和并发控制》）。

也可以在每个对象级别配置行锁升级。请参见 《参考手册：过程》 中的 sp_sterowlockpromote。

rtm thread idle wait period

摘要信息	
缺省值	600
值的范围	600 - 4026531839
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

rtm thread idle wait period 定义 Adaptive Server 使用的本机线程在没有任何工作时等待的时间（以秒为单位）。达到为本机线程设置的等待时间后，该线程自动消失。

runnable process search count

摘要信息	
缺省值	2000（缺省值为 3，用于 Cluster Edition）
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

runnable process search count 指定引擎在查找可运行的任务时，循环多少次后才将 CPU 交还操作系统。

只要引擎上的某个任务完成或超过其分配的时间， Adaptive Server 引擎就会检查运行队列中的可运行任务。有时，运行队列中会没有任务。这时，引擎可以将 CPU 归还操作系统或继续检查是否有要运行的任务。将 runnable process search count 设置为较高值，将导致引擎循环更多次，因此也就占用更长的 CPU 时间。将 runnable process search count 设置为较低值，将使引擎早些交还 CPU。

如果计算机是依靠辅助线程执行 I/O 的单处理器，通过设置 `runnable process search` 执行网络 I/O、磁盘 I/O 或其它操作系统任务，可在一定程度上提高性能。如果客户端（如批量复制操作）运行在使用辅助线程的单 CPU 服务器上，则您可能需要允许服务器和客户端访问 CPU。

注释 如果遇到性能问题，请尝试将 `runnable process search count` 设置为 3。

对于运行在不使用辅助线程的单处理器计算机以及多处理器计算机上的 Adaptive Server，使用缺省值就可提供良好的性能。

当 `runnable process search count` 的值为 3 时，Cluster Edition 能够更好地与同一计算机上运行的其它进程共享系统 CPU。但是，如果 `runnable process search count` 为 3，并且 Adaptive Server 正在以独立进程方式运行，用户在服务器响应时可能会遇到延迟情况。在这种情况下，请将 `runnable process search count` 重置为 2000。

使用 `sp_sysmon` 可确定 `runnable process search count` 参数如何影响 Adaptive Server 对 CPU 周期的使用，如何影响引擎将 CPU 移交给操作系统，以及如何影响对网络检查的阻塞。请参见 Performance and Tuning Series: Monitoring Adaptive Server with `sp_sysmon`（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

sampling percent

摘要信息	
缺省值	0
值的范围	0 - 100%
状态	动态
显示级别	Comprehensive
要求的角色	系统或数据库管理员
配置组	查询调优

`sampling percent` 是采样百分比的数值，例如 5 表示 5%，10 表示 10%，依此类推。

若要减少 I/O 争用和资源，请运行使用采样方法的 `update statistics` 命令，在维护窗口较小但数据集较大的情况下，它可以减少 I/O 和时间。如果正在更新的是处于连续使用状态、被截断并重新填充的大型数据集或表，则需要执行一次统计采样，以减少时间和 I/O 的大小。

请谨慎使用采样，因为结果并非完全准确。请针对 I/O 的节省来平衡对直方图值的更改。

尽管数据集的采样可能不完全精确，但通常情况下，直方图和密度值还是在合理的可接受范围内。

在确定是否使用采样时，请考虑数据集的大小、所面临的时间约束以及直方图生成的结果是否达到需要的精度。

采样时使用的百分比取决于您的需要。请测试不同的百分比，直到得到一个反映特定数据集的最精确信息的结果。

这些统计信息保存在系统表（`systabstats` 和 `sysstatistics`）中。

安全缺省登录

摘要信息	
缺省值	0
值的范围	0（后接另一参数，指定缺省登录）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

`secure default login` 为预先进行过鉴定而在 `master.syslogins` 中没有登录名的所有用户指定缺省登录名。

可使用以下语法来设置缺省安全登录名：

```
sp_configure "secure default login", 0, default_login_name
```

其中：

- `secure default login` 为参数名。
- 由于 `sp_configure` 的第二个参数必须是数值，因此 0 为必需参数。
- `default_login_name` 是 Adaptive Server 不知道但已通过安全性机制鉴定的用户的缺省登录名。该登录名必须是 `master.syslogins` 中的有效登录名。

select on syscomments.text

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统安全员
配置组	与安全性相关的参数

select on syscomments.text 通过限制 **syscomments** 表中 **text** 列上的 **select** 权限，启用数据库对象的文本保护。缺省值将 **select** 权限设置为 “public”。将值设置为 0，以将 **select** 权限限于对象所有者和系统管理员。

send doneinproc tokens

摘要信息	
缺省值	1（打开）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	网络通信

send doneinproc tokens 允许或禁止 Adaptive Server 发送 **doneinproc** 包（在存储过程中执行的每个 **select** 语句之后发送的 TDS 消息）。**send doneinproc tokens** 替换 **dbcc tune 'doneinproc'** 和跟踪标志 292。当前运行的查询将立即记下选项中的任何更改。

大多数情况下，将 **send doneinproc tokens** 设置为 1 是安全的。但是，某些存储过程是使用 CT-Lib 中的异步命令运行的，使用值 0 可能会导致某些 CT-Lib 应用程序中出现状态机错误。

session migration timeout

摘要信息	
缺省值	600
有效值	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

session migration timeout 指定客户端可用于通过连接到目标实例完成迁移的时间量。如果客户端未在分配的时间内迁移到目标实例，则 Adaptive Server 将连接失败。

session tempdb log cache size

摘要信息	
缺省值	逻辑页大小
值的范围	逻辑页大小最大为 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	用户环境

session tempdb log cache size 配置用户日志高速缓存 (ULC) 的大小，从而有助于确定其所需的刷新频率。

shared memory starting address

摘要信息	
缺省值	0
值的范围	因平台而异
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	物理内存

shared memory starting address 确定 Adaptive Server 启动其共享内存区域的虚拟地址。

通常不需要重新配置 shared memory starting address。只有在咨询 Sybase 技术支持部门后才能执行此操作。

number of worker processes、max parallel degree 和 max scan parallel degree 控制服务器级的并行查询处理。使用 set 命令的 parallel_degree、process_limit_action 和 scan_parallel_degree 选项可以限制会话级的并行优化，使用 select 命令的 parallel 关键字能够限制特定查询的并行优化。

size of auto identity column

摘要信息	
缺省值	10
值的范围	1 - 38
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

size of auto identity column 设置 IDENTITY 列的精度，IDENTITY 列用 sp_dboption auto identity 和 unique auto_identity index 选项自动创建的。

可插入到 IDENTITY 列的最大值为 10 精度 1。IDENTITY 列达到最大值后，所有进一步的 insert 语句将返回错误消息并终止当前事务。

如果达到了 IDENTITY 列的最大值，可通过用 alter table 命令执行修改操作增加该值。有关示例，请参见《Transact-SQL 用户指南》。

您还可以使用 create table 命令创建一个与旧表相同的新表，但新表中的 IDENTITY 列应该具有更高的精度。新表创建完后，可使用 insert 命令或 bcp 将数据从旧表复制到新表。

size of global fixed heap

摘要信息	
缺省值	150 页（32 位版本）
	300 页（64 位版本）
最小值	10 页（32 位版本）
	20 页（64 位版本）
状态	动态

摘要信息	
显示级别	Comprehensive
要求的角色	系统管理员
配置组	Java 服务、内存使用

size of global fixed heap 指定用于内部数据结构和满足其它需要的内存空间。

如果更改 size of the global fixed heap，请对总逻辑内存进行相同的更改。

size of process object heap

摘要信息	
缺省值	1500 页（32 位版本）
	3000 页（64 位版本）
最小值	45 页（32 位版本）
	90 页（64 位版本）
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	Java 服务、内存使用

size of process object fixed heap 指定使用 Java VM 的所有进程的总内存空间。

如果更改 size of process object fixed heap，请将 total logical memory 更改同样的数量。

size of shared class heap

摘要信息	
缺省值	1536 页（32 位版本）
	3072 页（64 位版本）
最小值	650 页（32 位版本）
	1300 页（64 位版本）
状态	动态
显示级别	Basic
要求的角色	系统管理员
配置组	Java 服务、内存使用

size of shared class heap 指定调入 Java VM 的所有 Java 类的共享内存空间。Adaptive Server 在全服务器范围内为用户定义的和系统提供的 Java 类保留共享的类堆。

如果更改 **size of shared class heap**，请将 **total logical memory** 更改同样的数量。

size of unilib cache

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、Unicode

size of unilib cache 指定除最小开销之外的已使用内存（以字节计算，向上舍入到最接近的 1K），它足以装载一份最大 Unilib 转换表与最大 Unilib 排序表。亚洲客户如果想通过基于 Unicode 的转换支持其它字符集，就需要增加 **size of unilib cache**；每增加一个字符集，该参数就需要增加 100K。

sproc optimize timeout limit

摘要信息	
缺省值	40
值的范围	0 - 4000
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

sproc optimize timeout limit 可将 Adaptive Server 在优化存储过程方面花费的时间指定为估计的执行时间的一部分。

SQL batch capture

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

SQL batch capture 控制 Adaptive Server 是否收集 SQL 文本。如果同时启用 SQL batch capture 和 max SQL text monitored，则 Adaptive Server 会针对每个用户任务收集每个批处理的 SQL 文本。

SQL Perfmon Integration（仅限 Windows）

摘要信息	
缺省值	1（打开）
有效值	0（关闭）， 1（打开）
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

SQL Perfmon Integration 启用或禁用从 Windows 性能监视器监控 Adaptive Server 统计信息的能力。

Adaptive Server 必须注册为 Windows 服务，才能支持监控器集成。下列情况下将自动注册：

- 使用 Sybase for Windows 程序组中的服务管理器启动 Adaptive Server。
- 使用“控制面板”中的“服务”选项。
- 已将 Windows 配置为让 Adaptive Server 作为自动服务启动。

有关可监控的 Adaptive Server 计数器列表，请参见《适用于 Windows 的配置指南》。

sql server clock tick length

摘要信息	
缺省值	因平台而异
值的范围	最小值（因平台而异） — 1000000；缺省值的若干倍
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

sql server clock tick length 指定服务器的时钟周期的持续时间（以微秒为单位）。缺省值和最小值都随平台而定。Adaptive Server 将值向上舍入到 *n* 的偶数倍，其中 *n* 是因平台而异的时钟周期缺省值。使用 sp_helpconfig 或 sp_configure 查找 sql server clock tick length 的当前值。

在和某些 CPU 密集型任务混合使用的应用程序中，将 sql server clock tick length 的值减少为：

- 对 I/O 密集性任务有所帮助 — 此时值为 20000 是较为合理的。如果缩短时钟周期长度，在单位时间内，CPU 密集型任务超过引擎上的分配时间的频率将增加，这样，其它任务便有更多的机会访问 CPU
- 会少量地增加响应次数 — Adaptive Server 在每个时钟周期运行一次其服务任务。缩短时钟周期长度意味着，服务任务在单位时间内的运行频率将增加。

增加 sql server clock tick length 对 CPU 密集型任务有利，因为它们的环境切换之间可运行更长时间。对主要为 CPU 密集型的应用程序来说，最大值 1,000,000 可能是合适的。但对所有 I/O 密集型任务却不适合。可通过调优 cpu grace time（请参见第 92 页的“cpu grace time”）和 time slice（请参见第 233 页的“time slice”）来改善这种情况。

注释 更改 sql server clock tick length 的值可能会对 Adaptive Server 性能产生极大影响。重置此值前，请先咨询 Sybase 技术支持部门。

sql text pipe active

摘要信息	
缺省值	0
值的范围	0 - 1
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

sql text pipe active 控制 Adaptive Server 是否收集 SQL 文本。如果启用此选项并设置 sql text pipe max messages，则 Adaptive Server 收集每个查询的 SQL 文本。使用 monSysSQLText 为所有用户任务检索 SQL 文本。

sql text pipe max messages

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

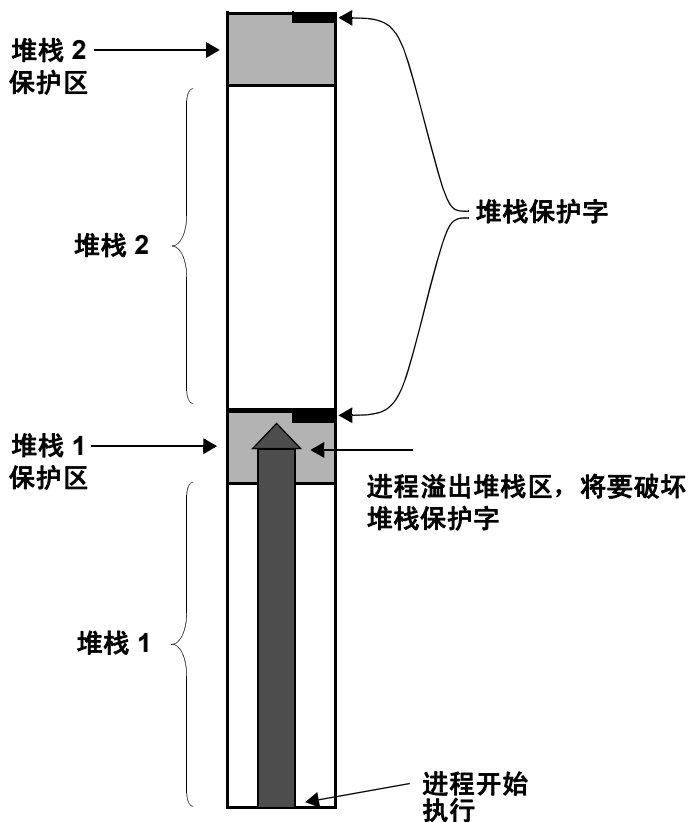
sql text pipe max messages 指定 Adaptive Server 存储的每个引擎的 SQL 文本消息数。monSQLText 表中的消息总数等于 sql text pipe max messages 的值与正在运行的引擎数的乘积。

stack guard size

摘要信息	
缺省值	4096
值的范围	0 - 2147483647
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、用户环境

stack guard size 设置堆栈保护区的大小（以字节为单位），堆栈保护区是每个堆栈末尾可配置大小的溢出堆栈。Adaptive Server 在启动时为每个用户连接和工作进程分配一个堆栈。这些堆栈紧挨着位于同一内存区域中，在每个堆栈的末端有一保护区。每个堆栈保护区的末尾是保护字，它是一个具有已知模式的 4 字节结构。图 5-5 阐释了进程如何破坏堆栈保护字。

图 5-5：将破坏堆栈保护字的进程



Adaptive Server 进行定期检查，查看用户连接的堆栈指针是否进入了和该用户连接的堆栈相关联的堆栈保护区。如果已经进入，Adaptive Server 则会中止事务，将控制权返回生成该事务的应用程序，并生成错误 3626:

```
The transaction was aborted because it used too much
stack space. Either use sp_configure to increase the
stack size, or break the query into smaller pieces.
spid: %d, suid: %d, hostname: %.*s, application name:
%.*s
```

Adaptive Server 还定期检查保护字模式，查看它是否发生了更改；如果已更改，这说明进程已溢出堆栈界限。发生这种情况时， Adaptive Server 将以下消息输出到错误日志中，然后关闭：

```
kernel: *** Stack overflow detected: limit: 0x%lx sp: 0x%lx
kernel: *** Stack Guardword corrupted
kernel: *** Stack corrupted, server aborting
```

在第一个消息中，“limit”是堆栈保护区末端的地址，“sp”是堆栈指针的当前值。

另外， Adaptive Server 还定期检查堆栈指针，查看它是否完全位于指针进程的堆栈和堆栈保护区之外。如果在堆栈和堆栈保护区之外，则即使保护字没有被破坏， Adaptive Server 也会关闭。发生这种情况时， Adaptive Server 将以下消息输出到错误日志中：

```
kernel: *** Stack overflow detected: limit: 0x%lx sp: 0x%lx
kernel: *** Stack corrupted, server aborting
```

stack guard size 的缺省值适用于大多数应用程序。但是，如果发生了由于堆栈保护字破坏或堆栈溢出而导致服务器关闭这一情况，则将 stack guard size 的值增加 2K。每个已配置的用户连接和工作进程都有一个堆栈保护区；因此，如果增加 stack guard size，就会消耗该值乘以已配置的用户连接数和工作进程数所得的内存量。

不要通过增大 stack guard size 来避免堆栈溢出问题，应考虑增大 stack size（请参见第 224 页的“stack size”）。堆栈保护区用作溢出区，而不是对常规堆栈的扩充。

Adaptive Server 通过增加 stack size 和 stack guard size 参数的值，为每个任务分配堆栈空间。stack guard size 的值必须配置为 2K 的倍数。如果指定的值不是 2K 的倍数，则 sp_configure 验证例程将此值取整到下一个最高倍数。

stack size

摘要信息	
缺省值	因平台而异
值的范围	最小值（因平台而异） — 2147483647
状态	静态
显示级别	Basic
要求的角色	系统管理员
配置组	用户环境

`stack size` 指定 Adaptive Server 上每个用户进程使用的执行堆栈的大小（以字节为单位）。要查找所用平台的 `stack size` 值，请使用 `sp_helpconfig` 或 `sp_configure`。`stack size` 必须配置为 2K 的倍数。如果指定的值不是 2K 的倍数，则 `sp_configure` 验证例程将此值取整到下一个最高倍数。

执行堆栈是 Adaptive Server 内存区域。在此区域中，用户进程跟踪其进程环境并存储本地数据。

某些查询可能会导致堆栈溢出。例如，具有相当长的 `where` 子句、较长的选择列表、深层嵌套的存储过程以及使用 `holdlock` 进行的多次选择和更新的查询。发生堆栈溢出时，Adaptive Server 将输出错误消息并回退事务。有关特定错误消息的详细信息，请参见第 222 页的“[stack guard size](#)”和 *Troubleshooting and Error Messages Guide*（《故障排除和错误消息指南》）。

用来解决堆栈溢出问题的两种方法是，将较大查询分成若干较小查询和增加 `stack size`。更改 `stack size` 会影响每个已配置用户连接和工作进程所需的内存量。请参见第 235 页的“[total logical memory](#)”。

如果某些查询超过了执行堆栈的大小，最好将它们重写为一系列较小查询，如果此类查询的数量很少或很少运行，则更应如此。

如果不实际运行查询，则无法确定该查询所需堆栈空间的大小。启动时对每个用户连接和工作进程所需的堆栈空间进行预分配。

因此，确定相应的 `stack size` 值只能根据经验进行。使用 `stack size` 的缺省值测试一下最大且最复杂的查询。如果运行后没有生成错误消息，则缺省值大概就可以使用了。如果生成了错误消息，则首先应将 `stack size` 稍微增大 (2K)。重新运行查询，看看增加的量是否足够。如果不够，则继续增加 `stack size`，直到运行查询后不生成错误消息时为止。

如果使用 CIS，或数据库中启用了 Java，而且要使用调用 JDBC 的方法，Sybase 推荐增加 50% 的缺省值。如果当前未使用 JDBC 或 CIS，标准缺省值通常就足够了。

start mail session（仅限 Windows）

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	扩展存储过程

start mail session 启用或禁用 Adaptive Server 启动时 Adaptive Server 邮件会话的自动启动。

如果参数值为 1，则在下一次 Adaptive Server 启动时 Adaptive Server 将启动一个邮件会话。如果参数值为 0，则下一次重新启动时 Adaptive Server 将不会启动一个邮件会话。

如果 start mail session 为 0，则可以使用 xp_startmail 系统 ESP 来明确启动 Adaptive Server 邮件会话。

设置 start mail session 之前，必须在 Windows 系统中为 Adaptive Server 创建一个邮箱和邮件配置文件。然后，创建用于 Sybmail 的 Adaptive Server 帐户。请参见 《适用于 Windows 的配置指南》。

start xp server during boot

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	静态
显示级别	
要求的角色	
配置组	扩展存储过程

start xp server during boot 确定当 Adaptive Server 启动时，是否启动 XP Server。

如果设置为 1，则在 Adaptive Server 启动时，将启动 XP Server。如果将 start xp server during boot 设置为 0，则在您运行 xp_cmdshell 之前，XP Server 将不会启动。

startup delay

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭）， 1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	查询调优

`startup delay` 控制在服务器启动过程中何时启动 RepAgent。缺省情况下，RepAgent 与 Adaptive Server 同时启动。Adaptive Server 将在错误日志中写入一条消息以说明等待时间。

statement cache size

摘要信息

缺省值	0
有效值	高速缓存大小（以 2K 页为单位）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、SQL Server 管理

`statement cache size` 可增加服务器分配的过程高速缓存内存，并限制过程高速缓存池中用于高速缓存的语句的内存数量。

注释 如果启用语句高速缓存，您必须在其自身的批处理中配置 `set chained on/off`。

由于高速缓存的语句将转换为轻量存储过程，因此进行语句高速缓存需要额外的可用对象描述符。

statement pipe active

摘要信息

缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

`statement pipe active` 控制 Adaptive Server 是否收集语句级别统计信息。如果同时启用 `statement pipe active` 和 `statement pipe max messages`，则 Adaptive Server 收集每个查询的语句级别统计信息。使用 `monSysStatement` 来检索所有已执行语句的统计信息。

statement pipe max messages

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

statement pipe max messages 确定 Adaptive Server 存储的每个引擎的语句统计消息数。**monSQLText** 表中的消息总数等于 **sql text pipe max messages** 的值与正在运行的引擎数的乘积。

statement statistics active

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	监控

statement statistic active 控制 Adaptive Server 是否收集监控表语句级别统计信息。使用 **monProcessStatement** 来获取特定任务的语句统计信息。

strict dtm enforcement

摘要信息	
缺省值	0（关闭）
有效值	0（关闭），1（打开）
状态	静态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理

strict dtm enforcement 决定 Adaptive Server 事务协调服务是否严格执行分布式事务的 ACID 属性。

在 Adaptive Server 只应为其它支持事务协调的 Adaptive Server 传播和协调事务的环境中，将 **strict dtm enforcement** 设置为打开。如果事务试图更新不支持事务协调服务的服务器中的数据，Adaptive Server 将中止该事务。

在异构环境中，可能需要使用不支持事务协调的服务器，包括早期版本的 Adaptive Server 和使用 CIS 配置的非 Sybase 数据库存储。在这些情况下，请将 **strict dtm enforcement** 设置为关闭，以允许 Adaptive Server 将事务传播到遗留 Adaptive Server 和其它数据存储。但是，这样并不能确保这些服务器的远程工作随原始事务回退或提交。

suspend audit when device full

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

suspend audit when device full 确定审计设备完全充满时 Adaptive Server 的行为。

注释 如果有两个或多个审计表，每个表都位于非主设备的单独设备上，而且每个审计表段都有阈值过程，则审计设备应绝不会充满。仅当阈值过程运行不正常时，才会发生“充满”情况。

选择以下值之一：

- 0 — 表示当前审计表充满时，将截断下一个审计表，并开始将其用作当前审计表。如果将 **suspend audit when device full** 设置为 0，则可确保审计进程绝不会挂起。但是，如果旧的审计记录没有存档，就有可能丢失。
- 1 — 将导致审计事件的审计进程和所有用户进程挂起。若要恢复正常操作，系统安全员必须登录并将一个空表设置为当前审计表。在此期间，系统安全员不能进行正常审计。如果系统安全员的操作在正常情况下会生成审计记录，Adaptive Server 会将一条错误消息和有关事件的信息发送到错误日志。

syb_sendmsg port number

摘要信息	
缺省值	0
有效值	0、1024 - 65535 或系统限制
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	网络通信

`syb_sendmsg port number` 指定 Adaptive Server 使用 `sp_sendmsg` 或 `syb_sendmsg` 将消息发送到 UDP（用户数据报协议）端口时所用端口号。

如果配置了多个引擎，则每个引擎使用一个端口号，从指定的端口号开始依次连续编号。如果端口号设置为缺省值 0，那么 Adaptive Server 指派端口号。

注释 Windows 不支持将消息发送到 UDP 端口。

系统安全员必须将 `allow sendmsg` 配置参数设置为 1，才能允许将消息发送到 UDP 端口。若要启用 UDP 消息传送，系统管理员必须将 `allow sendmsg` 设置为 1。请参见第 78 页的“`allow sendmsg`”。有关 UDP 消息传送的详细信息，请参见《参考手册：过程》中的 `sp_sendmsg`。

sysstatistics flush interval

摘要信息	
缺省值	0
有效值	0 - 32767
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

`sysstatistics flush interval` 确定刷新 `sysstatistics` 的时间间隔长度（以分钟为单位）。

Adaptive Server 通过任何 DML 语句，动态维护表中修改的行数和列数统计信息，并依据 `sysstatistics flush interval` 的值刷新它们。

由于这些统计信息较为准确，因此 Adaptive Server 将它们用于查询优化。**datachange** 功能确定：自上一次执行 **update statistics** 以来，在表级、列级或分区级更改的数据的量，并启动对象的统计信息更新。

在服务器正常关闭期间，这些内存中的统计信息始终都会刷新到磁盘上。可以配置 **sysstatistics flush interval**，通过管家任务定期将这些内存中的统计信息刷新到磁盘。将 **sysstatistics flush interval** 设置为 0，会禁用此管家任务。

systemwide password expiration

摘要信息	
缺省值	0
值的范围	0 - 32767
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

systemwide password expiration 设置口令在更改后保持有效的天数。如果将 **systemwide password expiration** 设置为 0，则口令不会过期。

口令将在经过指定的天数后过期。例如，如果您在 2007 年 8 月 1 日上午 10:30 创建一个新登录名，其口令有效期为 30 天，那么该口令将在 2007 年 8 月 31 日上午 10:30 过期。

如果最后一次更改某帐户的口令到现在的时间间隔已大于 *number_of_days*，则认为该帐户的口令已过期。

如果过期前的剩余天数小于 **systemwide password expiration** 值的 25% 或小于 7 天（以较大的为准），则每次用户登录时都会显示一条消息，说明过期前的剩余天数。在到期之前的任何时候，用户都可以更改自己的口令。

某一帐户的口令过期后，用户仍然可以登录到 Adaptive Server。但在使用 **sp_password** 更改其口令之前，该用户无法执行任何命令。如果系统安全员更改用户口令时帐户处于仅 **sp_password** 模式，则在指派新口令后，帐户将恢复正常。

此限制仅适用于口令到期后建立的登录会话。口令到期时登录的用户在下次登录之前不会受到影响。

tape retention in days

摘要信息	
缺省值	0
值的范围	0 - 365
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	备份 / 恢复

tape retention in days 指定每个磁带在用于数据库或事务日志转储后要保留的天数。设置此参数可防止意外覆盖转储磁带。

例如，如果将 **tape retention in days** 设置为 7 天，当您试图在距离上次磁带转储事件不到 7 天的时间使用磁带时，Backup Server 会发出一条警告消息。

执行转储命令时，可以使用 **with init** 选项撤消警告。此操作将导致磁带被覆盖，磁带上的全部数据都将丢失。

dump database 和 **dump transaction** 命令都提供 **retaindays** 选项，该选项可针对特定转储覆盖 **tape retention in days** 值。请参见 《系统管理指南：卷 2》中的第 12 章 “备份和恢复用户数据库”。

tcp no delay

摘要信息	
缺省值	1（打开）
有效值	0（关闭），1（打开）
状态	静态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	网络通信、操作系统资源

tcp no delay 控制 TCP（传输控制协议）包批处理。缺省值为表示不对 TCP 包进行批处理。

TCP 通常将小的逻辑包成批放入单个较大的物理包，并用尽可能多的数据填充物理网络框架，这样可以提高终端模拟环境中的网络吞吐量，在该环境中，用户通常通过网络发送键击。

但是，禁用 TCP 包批处理，可能对使用小 TDS (Tabular Data Stream) 包的应用程序有益。

注释 禁用 TCP 包批处理意味着不管包的大小如何都会被发送出去；这样就增加了网络通信量。

text prefetch size

摘要信息	
缺省值	16
有效值	0 - 65535
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	网络通信

text prefetch size 限制可被预取到现有缓冲池中的 **text**、**unitext** 和 **image** 数据的页数。Adaptive Server 只预取由 Adaptive Server 12.x 创建的或用 **dbcc rebuild_text** 更新的 **text**、**unitext** 和 **image** 数据。

time slice

摘要信息	
缺省值	100
值的范围	50 - 1000
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

time slice 设置 Adaptive Server 调度程序允许任务运行的毫秒数。如果 **time slice** 设置得太低，Adaptive Server 将消耗太多时间用于任务间的切换，这将增加响应时间。如果设置得太高，CPU 密集型任务则可能独占引擎，进而延长响应时间。缺省值允许每个任务运行 1/10 秒，然后将 CPU 让给另一任务。

请参见 **Performance and Tuning Series: Basics**（《性能和调优系列：基础知识》）中的第 3 章 “Using Engines and CPUs”（使用引擎和 CPU）。

使用 `sp_sysmon` 以确定 `time slice` 如何影响 Adaptive Server 引擎的主动放弃。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon*（《性能和调优系列：用 `sp_sysmon` 监控 Adaptive Server》）。

total data cache size

摘要信息	
缺省值	0
值的范围	0 - 2147483647
状态	已计算
显示级别	Basic
要求的角色	系统管理员
配置组	高速缓存管理器、内存使用

`total data cache size` 报告当前可供数据、索引和日志页使用的内存量（以千字节为单位）。该参数不是由用户直接配置的，而是通过计算得来的。

可供数据高速缓存使用的内存量会受一些因素的影响，包括：

- 计算机实际可用内存量的大小
- 要对其设置以下参数的值：
 - `total logical memory`
 - `number of user connections`
 - `total procedure cache percent`
 - `number of open databases`
 - `number of open objects`
 - `number of open indexes`
 - `number of devices`

其它参数也会影响可用内存量，但影响的程度会小一些。

有关 Adaptive Server 如何分配内存以及数据高速缓存的信息，请参见第 71 页的“配置参数”。

total logical memory

摘要信息	
缺省值	不适用
值的范围	不适用
状态	只读
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、物理内存

total logical memory 显示 Adaptive Server 当前配置的总逻辑内存。总逻辑内存是 Adaptive Server 当前配置所使用的内存量。**total logical memory** 显示可供使用所必需的内存，但该内存不一定在任何给定时刻都被使用。有关给定时刻使用的内存量的信息，请参见 **total physical memory**。不能使用 **total logical memory** 设置任何内存配置参数。

total physical memory

摘要信息	
缺省值	不适用
值的范围	不适用
状态	只读
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用

total physical memory 是只读配置参数，它显示 Adaptive Server 当前配置的总物理内存。总物理内存是 Adaptive Server 在给定时刻使用的内存量。对 Adaptive Server 进行适当配置，使 **max memory** 的值大于 **total logical memory** 的值，**total logical memory** 的值大于 **total physical memory** 的值。

transfer utility memory size

摘要信息	
缺省值	4096
值的范围	0 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	SQL Server 管理

Adaptive Server 为 **transfer table** 命令和标记为增量传输的表保留内存池。此池提供了用于保留有关当前和过去的传输的状态信息的内存，以及用于写入传输文件和从传输文件中进行读取的内存。 **transfer utility memory size** 确定此内存池的大小。

此池的单元位于内存页（大小为 2048 字节的一些块）中。缺省大小已足够大，可容纳超过 100 个标记为增量传输的表（所有表均同时传输）。

如果您的安装未包括标记为增量传输的表，并且未使用 **transfer table** 命令，则可将此内存池的大小设置为零以回收此内存。

txn to pss ratio

摘要信息	
缺省值	16
有效值	1 - 2147483647
状态	静态
显示级别	1
要求的角色	系统管理员
配置组	DTM 管理、内存使用

Adaptive Server 管理作为可配置服务器资源的事务。每次开始一个新事务时， Adaptive Server 都必须从服务器启动时所创建的全局缓冲池中获得一个可用的**事务描述符**。事务描述符是 Adaptive Server 用来表示活动事务的内部内存结构。

Adaptive Server 需要将一个可用事务描述符用于：

- 各服务器事务的外部块。事务的外部块可能在客户端执行新的 **begin transaction** 命令时就已经明确创建了。当客户端使用 Transact-SQL 修改数据而没有使用 **begin transaction** 定义该事务时， Adaptive Server 也可能隐式创建了外部事务块。

注释 使用另外的 **begin transaction** 命令创建的后继嵌套事务块不要要求额外的事务描述符。

- 在**多数据库事务**中访问的每个数据库。每次事务使用或修改新数据库中的数据时， Adaptive Server 都必须获得新的事务描述符。

txn to pss ratio 决定了服务器可以使用的事务描述符的总数。在启动时，将该比率乘以 PSS 结构的数目以创建事务描述符缓冲池：

of transaction descriptors = PSS structures * txn to pss ratio

缺省值 16 可确定与 12.x 之前的 Adaptive Server 早期版本兼容，这些版本也为每个用户连接分配 16 个事务描述符。在版本 12 和更高版本中，同时发生的事务数量仅受到服务器中可用事务描述符数量的限制。

注释 您在用户事务中具有的数据库的数目可以与 Adaptive Server 安装后具有的数据库数目一样多。例如，如果 Adaptive Server 具有 25 个数据库，则您可以在用户事务中包括 25 个数据库。

优化系统的 txn 与 pss 的比率

在高峰期间，使用 `sp_monitorconfig` 检查事务描述符的使用情况：

```
sp_monitorconfig "txn to pss ratio"
```

Usage information at date and time: Apr 22 2002 2:49PM.

Name	num_free	num_active	pct_act	Max_Used	Reused
-----	-----	-----	-----	-----	-----
txn to pss ratio	784	80	10.20	523	NA

如果 `num_used` 值为零或过低，则事务可能会延迟，因为 Adaptive Server 需要等待服务器中的事务描述符变为可用的。在这种情况下，应考虑增大 `txn to pss ratio` 的值。

如果 `Max_Used` 值太低，则未使用的事务描述符可能会消耗其它服务器功能可使用的内存。请考虑减少 `txn to pss ratio` 的值。

unified login required

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	动态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

`unified login required` 要求通过某种安全机制对登录到 Adaptive Server 的所有用户进行鉴定。若要使用统一登录安全服务，则必须将 `use security services` 参数设置为 1。

upgrade version

摘要信息	
缺省值	1100
值的范围	0 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	SQL Server 管理

upgrade version 报告升级主设备的升级实用程序版本。更新实用程序在更新期间检查并修改此参数。

警告！ 不要重置 upgrade version。否则可能会导致 Adaptive Server 出现严重问题。

通过在不指定值的情况下使用 upgrade version，可确定是否已对主设备进行了升级：

```
sp_configure "upgrade version"
```

use security services

摘要信息	
缺省值	0（关闭）
值的范围	0（关闭），1（打开）
状态	静态
显示级别	Intermediate
要求的角色	系统安全员
配置组	与安全性相关的参数

use security services 指定 Adaptive Server 使用基于网络的安全服务。如果该参数设置为 0，则无法使用任何基于网络的安全服务。

user log cache size

摘要信息	
缺省值	逻辑页大小
值的范围	2048 ^a - 2147483647
	a. 是由服务器逻辑页大小确定的最小值
状态	静态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、用户环境

user log cache size 指定每个用户的日志高速缓存的大小（以字节为单位）。其大小由服务器的逻辑页大小决定。每个已配置用户连接和工作进程都有一个用户日志高速缓存。Adaptive Server 使用这些高速缓存缓冲用户事务日志记录，这可缓解在事务日志末端的争用。

当用户日志高速缓存变满或发生了另一事件时（如事务完成时），Adaptive Server 将所有日志记录从用户日志高速缓存“刷新”到数据库事务日志。通过首先整合每个用户日志高速缓存中的日志记录，而不是立即将每条记录添加到数据库事务日志中，Adaptive Server 可以减少写入日志的进程的争用，特别是配置了多个引擎的 SMP 系统。

注释 对于使用了混合数据和日志段的数据库的事务，在每个日志记录之后将用户日志高速缓存刷新到事务日志。不会发生缓冲。如果数据库没有专用的日志段，则不要增加用户日志高速缓存的大小。

不要将 user log cache size 配置为大于由应用程序的事务写入的最大日志信息量。由于 Adaptive Server 在事务完成时刷新用户日志高速缓存，因此就浪费了分配给用户日志高速缓存的额外内存。如果服务器中事务生成的事务日志记录没有一个多于 4000 字节，则设置的 user log cache size 值不要高于该值。例如：

```
sp_configure "user log cache size", 4000
```

将 user log cache size 设置得太高会浪费内存。将其设置得太低，则可能导致用户日志高速缓存充满，且每个事务不止刷新一次。这将会增加事务日志的争用。如果事务量较少，事务日志的争用量可能不会很明显。

使用 sp_sysmon 了解此参数如何影响高速缓存的行为。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon（《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

user log cache spinlock ratio

摘要信息	
缺省值	20
值的范围	1 - 2147483647
状态	动态
显示级别	Intermediate
要求的角色	系统管理员
配置组	内存使用、用户环境

对于运行了多个引擎的 Adaptive Server， user log cache spinlock ratio 指定用户日志高速缓存与用户日志高速缓存螺旋锁的比率。每个已配置用户连接都有一个用户日志高速缓存。

缺省值针对为服务器配置的每 20 个用户连接指定 1 个螺旋锁。

使用 sp_sysmon 了解此参数如何影响高速缓存行为。请参见 Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon （《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》）。

wait event timing

摘要信息	
缺省值	0
值的范围	0 - 1
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	内存使用、监控

wait event timing 控制 Adaptive Server 是否收集各个等待事件的统计信息。任务可能会因各种原因而必须等待（例如，等待缓冲区读取完成）。monSysWaits 表包含每个等待事件的统计信息。monWaitEventInfo 表包含等待事件的完整列表。

workload manager cache size

摘要信息	
缺省值	80
有效值	80 - 2147483647
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	共享磁盘集群

workload manager cache size 以 2K 页为单位指定工作负荷管理器可以使用的最大内存量。请参见 *Cluster Users Guide* （《集群用户指南》）中的第 6 章 “Managing the Workload”（管理工作负荷）。

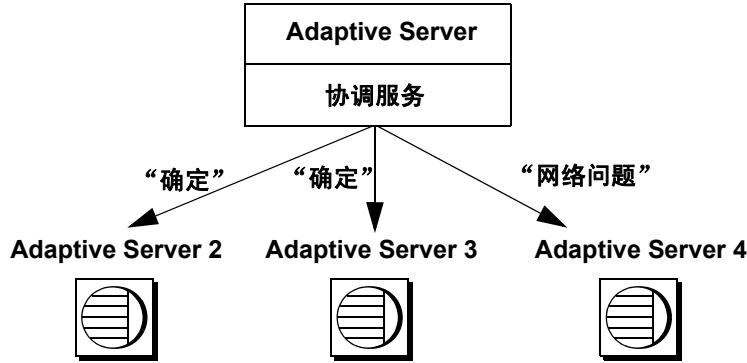
xact coordination interval

摘要信息	
缺省值	60（秒）
有效值	1 - 2147483647（秒）
状态	动态
显示级别	10
要求的角色	系统管理员
配置组	DTM 管理

xact coordination interval 定义了解析远程事务分支（已传播到远程服务器）的两次尝试之间的时间间隔。

协调 Adaptive Server 定期尝试解析那些参与分布式事务的远程服务器的工作。协调服务器将依次联系每个参与分布式事务的远程服务器，如图 5-6 中所示。协调服务可能会由于各种原因而不能解析事务分支。例如，如果由于网络问题无法联系到远程服务器，协调服务器在 **xact coordination level** 指定的时间过后重新尝试连接。

图 5-6：解决远程事务分支



xact coordination interval 的缺省值为 60 秒，Adaptive Server 每分钟尝试解析一次远程事务。减少该值可能会加速分布式事务的完成，但只限于可在一分钟之内完成解析的事务。在正常情况下，减少 xact coordination interval 的值不会对性能产生任何影响。

将 xact coordination interval 的值设得太高会减慢分布式事务完成的速度，并且会导致事务分支占用资源的时间过长。正常情况下，不要使 xact coordination interval 的值超过其缺省值。

xp_cmdshell context

摘要信息	
缺省值	1
有效值	0, 1, 2
状态	动态
显示级别	Comprehensive
要求的角色	系统管理员
配置组	扩展存储过程

xp_cmdshell context 为要使用 xp_cmdshell 系统 ESP 执行的操作系统命令设置安全上下文。该上下文的值确定命令采用哪个帐户运行：

- 0 — 命令采用 XP Server 的帐户运行。
- 1 — 命令采用用户的帐户运行。
- 2 — 只有当用户拥有系统管理员权限时，命令才采用 XP Server 的帐户运行。

如果将 `xp_cmdshell context` 设置为 1，则将 `xp_cmdshell` 安全上下文限制为在操作系统级别拥有帐户的用户。它的行为因平台而异。如果 `xp_cmdshell context` 设置为 1，要使用 `xp_cmdshell ESP`，对于 Adaptive Server 用户名必须有一个操作系统用户帐户。例如，名为 “sa” 的 Adaptive Server 用户无法使用 `xp_cmdshell`，除非其拥有一个名为 “sa” 的操作系统级别用户帐户。

在 Windows 上，如果 `xp_cmdshell context` 设置为 1，则仅当登录 Adaptive Server 的用户的用户名是有效的 Windows 用户名（在运行 Adaptive Server 的系统上具有 Windows 系统管理权限）时，`xp_cmdshell` 才能成功。

在其它平台上，如果 `xp_cmdshell context` 设置为 1，那么只有当启动 Adaptive Server 的用户在操作系统级具有 “超级用户” 权限时，`xp_cmdshell` 才能成功。当 Adaptive Server 得到执行 `xp_cmdshell` 的请求时，它将核对该 ESP 请求者的用户名的 uid，并根据该 uid 的许可权限运行操作系统命令。

如果 `xp_cmdshell context` 设置为 0，则运行 Adaptive Server 的操作系统的帐户权限可以用来从 `xp_cmdshell` 执行操作系统命令。这就使用户能够执行操作系统命令，这些命令是用户在其操作系统帐户的安全性环境下通常不能执行的命令。

磁盘资源问题概述

主题	页码
设备分配和对象放置	245
用于管理磁盘资源的命令	246
存储管理决策中需要考虑的事项	247
安装时的状态和缺省值	249
用于管理存储的系统表	250

Adaptive Server 中设置的许多缺省值都是存储管理方面的合理值，例如数据库、表和索引位置，以及为每一项分配多少空间。存储分配和管理的责任通常是集中的。通常，系统管理员能够完全控制 Adaptive Server 的磁盘资源分配和数据库、表以及索引在那些资源上的物理位置。

设备分配和对象放置

当配置新系统时，系统管理员必须考虑对所需的磁盘资源的数量和大小有直接影响的几个问题。这些设备分配问题是指向 Adaptive Server 增加磁盘资源的命令和过程。

表 6-1：设备分配主题

任务	章节
初始化和分配数据库设备的缺省缓冲池	第 7 章 “初始化数据库设备”
镜像数据库设备以用于恢复	《系统管理指南：卷 2》中的第 2 章 “镜像数据库设备”

在为 Adaptive Server 分配完初始磁盘资源之后，系统管理员、数据库所有者和对象所有者应考虑如何在特定数据库设备上放置数据库和数据库对象。这些对象放置问题决定数据库对象驻留在系统上的什么位置，或者对象是否共享设备。本手册中的很多地方（包括表 6-2 中所示的章节）论述了对象放置任务。

表 6-2：对象放置主题

任务	章节
在特定数据库设备上放置数据库	《系统管理指南：卷 2》中的第 6 章 “创建和管理用户数据库”
在特定数据库设备上放置表和索引	《系统管理指南：卷 2》中的第 6 章 “创建和管理用户数据库”

不要将分配设备与对象放置分开考虑。例如，如果决定某个特定表必须驻留在一对专用设备上，请先为 Adaptive Server 分配那些设备。本章中的其它部分概述了跨两个设备分配和对象放置问题，并给出了相应章节的位置指示。

用于管理磁盘资源的命令

表 6-3 列出了系统管理员用来为 Adaptive Server 分配磁盘资源的主要命令，并提供了对讨论那些命令的章节的引用。

表 6-3：用于分配磁盘资源的命令

命令	任务	请参见
disk init name = "dev_name" physname = "phys_name"...	使某个物理设备可供特定的 Adaptive Server 使用。指派数据库设备名称 (dev_name)，用于在其它 Adaptive Server 命令中标识该设备。	第 7 章 “初始化数据库设备”
sp_deviceattr logicalname, optname, optvalue	更改现有数据库设备文件的 dsync 设置。	第 7 章 “初始化数据库设备”
sp_diskdefault "dev_name"...	向缺省数据库空间的常规缓冲池中添加 dev_name。	第 7 章 “初始化数据库设备”
disk resize name = "device_name" , size = additional_space	动态增加数据库设备的大小。	第 7 章 “初始化数据库设备”
disk mirror name = "dev_name" mirror = "phys_name"...	在特定物理设备上镜像数据库设备。	《系统管理指南：卷 2》中的第 2 章 “镜像数据库设备”

表 6-4 列出了对象放置中使用的命令。有关对象放置如何影响性能的信息，请参见 Performance and Tuning Series: Physical Database Tuning（《性能和调优系列：物理数据库调优》）中的第 1 章 “Controlling Physical Data Placement”（控制物理数据放置）。

表 6-4：用于在磁盘资源上放置对象的命令

命令	任务	请参见
create database...on dev_name 或者 alter database...on dev_name	使数据库设备可供特定 Adaptive Server 数据库使用。create database 的 log on 子句将数据库日志放在特定数据库设备上。	《系统管理指南：卷 2》中的第 6 章“创建和管理用户数据库”
create database... 或者 alter database...	当不带 on dev_name 子句使用时，这些命令将在缺省数据库设备上分配空间。	《系统管理指南：卷 2》中的第 6 章“创建和管理用户数据库”
sp_addsegment seg_name, dbname, devname 和 sp_extendsegment seg_name, dbname, devname	从可用于特定数据库的设备中创建段（指定的空间集合）。	《系统管理指南：卷 2》中的第 8 章“创建和使用段”
create table...on seg_name 或者 create index...on seg_name	创建数据库对象，同时将其放在数据库的已指派磁盘空间的特定段上。	《系统管理指南：卷 2》中的第 8 章“创建和使用段”
create table... 或者 create index...	当不带 on seg_name 使用时，表和索引将占据分配给数据库的空间的常规缓冲池（缺省设备）。	《系统管理指南：卷 2》中的第 8 章“创建和使用段”

存储管理决策中需要考虑的事项

系统管理员必须做出有关 Adaptive Server 数据库的物理空间分配的多项决定。做出这些选择时需要考虑的主要事项包括：

- 恢复 — 在单独的物理设备上对磁盘镜像和日志维护时，将提供两种恢复机制，可在发生物理磁盘故障时完全恢复。
- 性能 — 对于磁盘读写速度非常重要的表或数据库，在物理设备上适当放置数据库对象可提高性能。磁盘镜像将减慢磁盘写入的速度。

恢复

恢复是使用多个磁盘设备的主要原因。您可以对数据库设备进行镜像来实现不间断的恢复。也可以通过将数据库日志存储在单独的物理设备上上来确保完全恢复。

在单独的设备上保留日志

除非数据库设备已被镜像，否则完全恢复要求数据库的事务日志存储在不同于数据库实际数据（包括索引）所在的设备上。在硬盘出现故障的情况下，可以通过装载数据库的转储，然后应用已安全存储在另一设备上的日志记录，从而创建最新的数据库。请参见《系统管理指南：卷 2》中的第 6 章“创建和管理用户数据库”，了解有关 `create database` 的 `log on` 子句的信息。

镜像

通过将所有 Adaptive Server 设备都镜像到单独的物理磁盘上，可以确保在发生硬盘故障时能够不间断地进行恢复。请参见《系统管理指南：卷 2》中的第 2 章“镜像数据库设备”。

性能

通过将日志和数据库对象放到单独的设备上可以提高系统性能：

- 把表和非聚簇索引放在不同的硬盘上能提高物理读写速度，因为工作被分给两个不同的磁盘驱动器。
- 将大型表拆分到两个磁盘上可提高性能，尤其对于多用户应用程序。
- 当日志和数据共享设备时，用户日志高速缓存将事务日志记录放入缓冲区被禁用。
- 分区为堆表提供多个插入点，提高配置为执行并行查询处理的系统的并行度，并使其可以跨多个数据库设备分配表的 I/O。

请参见 Performance and Tuning Series: Physical Database Tuning（《性能和调优系列：物理数据库调优》）中的第 1 章“Controlling Physical Data Placement”（控制物理数据放置），了解对象放置如何影响性能的详细论述。

安装时的状态和缺省值

安装程序和脚本将初始化主设备并为您设置 `master`、`model`、`sybssystemprocs`、`sybsecurity` 和临时数据库。

安装 Adaptive Server 时，请按下面的方式组织系统数据库、系统定义的段和数据库设备：

- `master`、`model` 和 `tempdb` 数据库安装在主设备上。
- `sybssystemprocs` 数据库安装在指定的设备上。
- 每个数据库中创建三个段：`system`、`default` 和 `logsegment`。
- 主设备是所有用户创建的数据库的缺省存储设备。

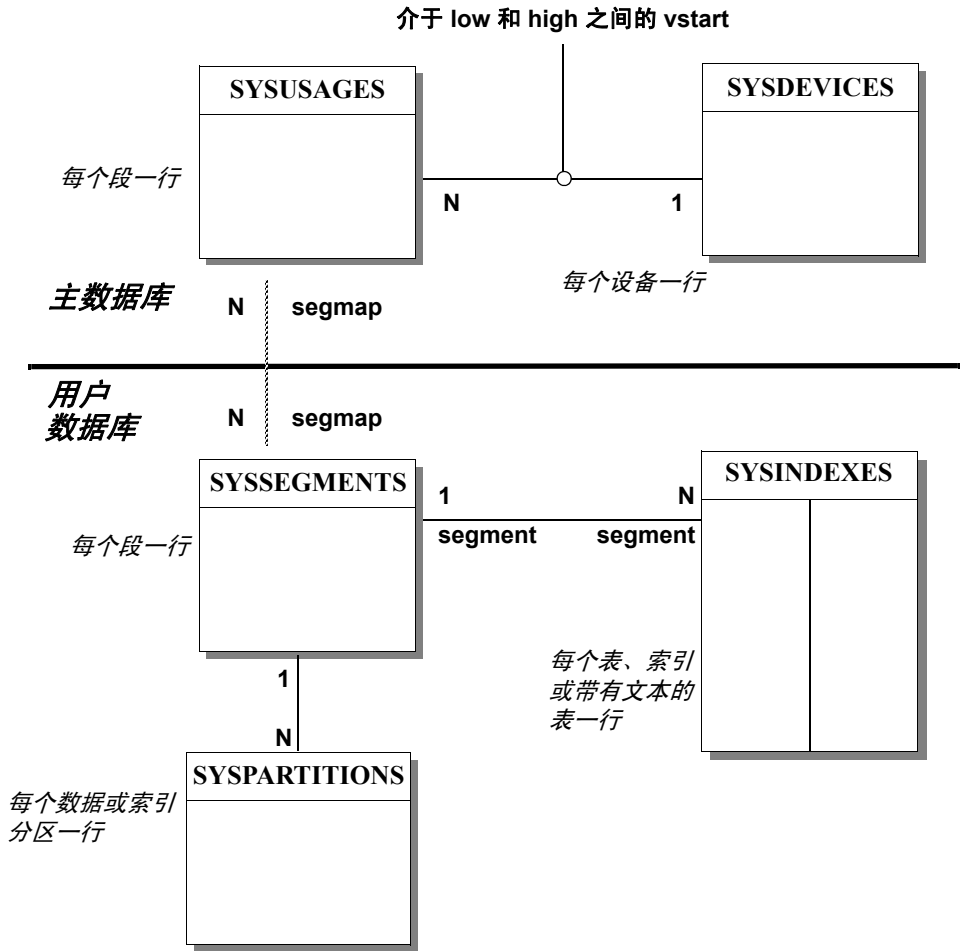
注释 在初始化缺省存储的新设备后，使用 `sp_diskdefault` 从缺省存储区域删除主设备。在主设备上不要存储用户数据库和对象。请参见第 262 页的“指派缺省设备”。

- 如果安装审计数据库 `sybsecurity`，该数据库将位于它自己的设备上。

用于管理存储的系统表

master 数据库中的两个系统表（sysusages 和 sysdevices）以及每个用户数据库中三个其它系统表（syssegments、sysindexes 和 syspartitions）跟踪数据库、表（包括事务日志表 syslogs）和索引的放置。表间的关系如图 6-1 中所示。

图 6-1：用于管理存储的系统表



sysdevices 表

在 master 数据库中的 sysdevices 表中，每个数据库设备都有相应的一行，而且可供 Adaptive Server 使用的每个转储设备（磁带、磁盘或操作系统文件）也可能有相应的一行。

disk init 命令向 master..sysdevices 中添加数据库设备的条目。使用 sp_addumpdevice 添加的转储设备，请参见《系统管理指南：卷 2》的第 11 章“开发备份和恢复计划”

sysdevices 为每个设备存储两个名称：

- **逻辑名或设备名**，此类名称用于所有后续存储管理命令中，存储在 sysdevices 中的 name 列中。通常，这是个好记的名称，可能指示设备的计划用途，例如“logdev”或“userdbdev”。
- **物理名**是设备的实际操作系统名称。只有 disk init 命令中使用此名称；除此之外，所有 Adaptive Server 数据存储命令均使用逻辑名。

通过在 create database 或 alter database 语句中指定设备的逻辑名，可将数据库或事务日志放置在一个或多个设备上。create database 的 log on 子句将数据库的事务日志放到单独的设备上，以确保可完全恢复。日志设备还必须在 sysdevices 中有相应条目，才能使用 log on。

数据库可驻留在一个或多个设备上，一个设备可存储一个或多个数据库。请参见《系统管理指南：卷 2》中的第 6 章“创建和管理用户数据库”，了解有关在特定数据库设备上创建数据库的信息。

sysusages 表

master 数据库中的 sysusages 表跟踪分配给所有 Adaptive Server 数据库的空间。

create database 和 alter database 通过为每个数据库设备或设备片段在 sysusages 中添加一行，为数据库分配新的空间。当使用 create 或 alter database 在设备上只分配一部分空间时，该部分称为**片段**。

sp_addsegment、sp_dropsegment 和 sp_extendsegment 为已映射或未映射到段的设备更改 sysusages 中的 segmap 列。请参见《系统管理指南：卷 2》中的第 8 章“创建和使用段”。

syssegments 表

syssegments 表（每个数据库中都有一个）列出了数据库中的段。段是可用于特定数据库的数据库设备和片段的集合。表和索引可被指派给特定的段（因此可被指派给特定的物理设备），也可以跨一组物理设备。

create database 在 **syssegments** 中生成缺省条目。**sp_addsegment** 和 **sp_dropsegment** 在 **syssegments** 中添加和删除条目。

sysindexes 表

sysindexes 表列出了每个表和索引以及存储每个表、聚簇索引、非聚簇索引和文本页链的段。它还列出了其它信息，如表或索引的 **max_rows_per_page** 设置。

create table、**create index** 和 **alter table** 命令在 **sysindexes** 中创建新行。对表进行分区将会更改表的 **sysindexes** 条目的功能。

syspartitions 表

syspartitions 表列出了每个表和索引分区，以及存储分区的段。**syspartitions** 维护主要存储管理信息，例如数据或索引页链的第一页、堆的最后一页、索引分区的根页等。

使用 **create table**、**create index** 和 **alter table** 在 **syspartitions** 中创建新行。

初始化数据库设备

主题	页码
数据库设备	253
使用 disk init 命令	254
disk init 语法	254
获取有关设备的信息	260
删除设备	262
指派缺省设备	262
使用 disk resize 增加设备大小	263

数据库设备

数据库设备存储组成数据库的对象。术语**设备**不一定是指一个确切的物理设备：它可以指磁盘上的任何一块区域（例如一个磁盘分区），也可以指文件系统中用来存储数据库及其对象的一个文件。

每个数据库设备或文件在用于数据库存储之前，必须已准备好而且能够被 Adaptive Server 识别。这一过程称为**初始化**。

数据库设备初始化后就可以用来：

- 分配给用于 create 和 alter database 命令的设备缺省缓冲池
- 指派到用户数据库可用空间的缓冲池
- 指派到用户数据库并用于存储一个或多个数据库对象
- 指派用于存储数据库的事务日志

使用 *disk init* 命令

系统管理员使用 *disk init* 命令初始化新数据库设备，该命令：

- 将指定的物理磁盘设备或操作系统文件映射到数据库设备名
- 在 *master.sysdevices* 中列出新设备
- 为数据库存储准备设备

注释 在运行 *disk init* 之前，请查看所用平台的安装文档，了解有关选择数据库设备和对设备进行准备以便用于 Adaptive Server 的信息。可能要对计算机的磁盘进行重新分区以提供 Sybase 数据库的最佳性能。

disk init 将数据库设备分成多个分配单元，即一些包含 256 个逻辑页的组。分配单元的大小取决于为服务器所配置的逻辑页大小（2、4、8 或 16K）。在每个分配单元中，*disk init* 命令将第一页初始化为分配页，该页包含有关驻留在分配单元中的数据库（如果有）的信息。

警告！ 运行 *disk init* 命令后，请转储 *master* 数据库。这样做使得在 *master* 损坏的情况下能够更容易和安全地进行恢复。请参见《系统管理指南：卷 2》中的“恢复系统数据库”。

disk init 语法

请参见《参考手册：命令》，了解 *disk init* 语法。

指定逻辑设备名

device_name 必须为有效的标识符。此名称在 *create database* 和 *alter database* 命令以及管理段的系统过程中使用。只有 Adaptive Server 可识别逻辑设备名，而运行服务器的操作系统无法识别逻辑设备名。

指定物理设备名

数据库设备的 *physname* 给出了原始磁盘分区 (UNIX) 名称、外部设备的名称或操作系统文件名。在 PC 平台上，通常使用操作系统文件名作为 *physname*。

选择设备号

Adaptive Server 接受（但不要求）`disk init vdevno` 参数。如果指定了 `vdevno`，则可以选择 1 到 2,147,483,647（虚拟设备 ID 0 由 master 设备使用）之间的、当前未使用的任意标识符。例如，如果指定 `vdevno = 33`，则会为设备指派虚拟设备 ID 33。如果未指定 `vdevno`，则 Adaptive Server 会选择比在 `sysdevices` 中当前列出的最高 `vdevno` 还要高的数字。

可创建的数据库设备数受 `number of devices` 配置参数的限制。Adaptive Server 的初始配置为 10 个设备。使用 `sp_configure` 更改 `number of devices` 的值。

所用操作系统可能还会限制您的安装可以同时使用的设备数。对于操作系统，每个 Sybase 设备计为一个打开的文件。

Adaptive Server 自动指定数据库设备的下一个可用标识号。此标识号是虚拟设备号 (`vdevno`)。发出 `disk init` 命令时，无需指定此标识号。

如果手动选择 `vdevno`，它在 Adaptive Server 所使用的设备中必须唯一。设备号 0 代表主设备。合法设备号为 1 – 2,147,483,647。可以选择该范围内任何未使用的 `vdevno`。

若要查看已用于 `vdevno` 的设备号，请查看 `sp_helpdevice` 的报告中的 `vdevno` 列，或使用以下查询列出当前使用的所有设备号：

```
select vdevno from master..sysdevices
where status & 2=2
```

此处 `status & 2=2` 指定物理磁盘。

指定设备大小

若要指示设备的大小，请使用“k”或“K”表示千字节，使用“m”或“M”表示兆字节，使用“g”或“G”表示千兆字节，并使用“t”或“T”表示太字节。为了避免在已分配的实际页数中造成混淆，Sybase 建议您始终在 `disk init` 和 `create database` 命令中都包括单位指示符。请用单引号或双引号或者方括号将单位指示符括起来。

从理论上说，您可以创建多达 2,147,483,647 个磁盘设备，其中每个磁盘设备的大小都可达 2,147,483,648 个 2K 块。最大安装大小取决于数据库大小、硬件和操作系统限制。

下面的准则适用于 `disk init` 的语法：

- 如果没有为 `disk init` 或 `disk reinit` 的 `size` 参数包括单位指示符，则缺省情况下将按虚拟页数来计算 `size`。因此，如果输入 `size = 15000`，则 Adaptive Server 将假定有 15,000 个虚拟页。每个虚拟页为 2048 个字节。
- 可使用 `disk resize` 命令增加（但不能减小）现有数据库设备的大小。
- 如果计划使用新设备来创建新数据库，则最小 `size` 取决于服务器所用的逻辑页大小，如表 7-1 所示：

表 7-1：最小数据库大小

逻辑页大小	最小数据库大小
2K	3MB
4K	6MB
8K	12MB
16K	24MB

数据库不能小于 `model` 数据库。大于上面列出的最小值的 `model` 数据库确定最小数据库大小。

Adaptive Server 在分配单元（包含 256 个逻辑页的组）中分配和管理数据库空间。可（使用 `create database`）创建的最小数据库为 1MB；因此，最小可用数据库设备的大小是 1MB 或 256 个逻辑页中的较大者（对于 2K 或 4K 逻辑页大小，此值为 1 MB；对于 8K 逻辑页大小，此值为 2MB；对于 16K 逻辑页大小，此值为 4MB）。

在确定设备多大才能不浪费空间时，请记住这种 256 页的分组。例如，如果安装使用 16k 的逻辑页大小，则将设备指定为 `size = '31M'` 将会导致设备末端浪费 3MB，因为分配单元为 4MB。

如果要初始化裸设备，请从操作系统确定设备的大小，如所用平台的安装指南中所述。使用可用的总大小，直到平台允许的最大值。初始化磁盘以供 Adaptive Server 使用后，就不能再将该原始磁盘上的空间用于任何其它用途。

`disk init` 使用 `size` 来计算 `sysdevices.high` 中高虚拟页码的值。`sysdevices.high` 和 `sysdevices.low` 的值是以 2K 字节块为单位的虚拟页码，这种块是 Adaptive Server 物理磁盘管理单元。这可能与安装的逻辑页大小有所不同。

注释 如果物理设备不包含 `size` 参数所指定的块数，则 `disk init` 将失败。如果使用可选的 `vstart` 参数，则物理设备必须包含 `vstart` 和 `size` 参数指定的块的总和，否则命令将失败。

指定 `dsync` 设置（可选）

对于在 UNIX 操作系统文件上初始化的设备，`dsync` 设置控制是否将对那些文件的写入放入缓冲区。如果启用 `dsync` 设置，则 Adaptive Server 将使用 UNIX `dsync` 标志打开数据库设备文件，这样可确保在物理存储介质上直接进行对设备文件的写入，并且 Adaptive Server 能够在系统出现故障时恢复设备上的数据。

如果禁用 `dsync` 设置，则对设备文件的写入可能会被 UNIX 文件系统放入缓冲区，并且无法确保恢复设备上的数据。只有在不要求数据完整性时才禁用 `dsync`。

注释 对于在裸分区上初始化的设备，将忽略 `dsync` 设置。相反，对数据库设备的写入操作直接在物理介质上进行。

dsync 的性能影响

对数据库设备文件使用 **dsync** 设置将产生若干性能权衡问题：

- 对于 HP-UX， Adaptive Server 不支持操作系统文件上的异步 I/O。
- 如果数据库设备文件使用 **dsync** 选项，则写入设备文件的 Adaptive Server 引擎将会等待，直至写入操作完成为止。这可能会导致更新操作过程中的性能下降。
- 如果启用 **dsync**，则对数据库设备文件的写入操作可能比早期版本的 Adaptive Server（不支持 **dsync**）要慢。这是因为 Adaptive Server 必须将数据写到磁盘上，而不是只将高速缓存数据复制到 UNIX 文件系统缓冲区。

在要求最高写入性能（但不要求系统发生故障之后的数据完整性）的情况下，禁用 **dsync** 可获得与 Adaptive Server 早期版本相似的设备文件性能。例如，如果使用 **dsync** 时性能不可接受，则可以考虑将 **tempdb** 存储在一个禁用 **dsync** 的专门设备文件中。

- 与存储在裸分区上的设备相比，存储在 UNIX 操作系统文件中设备的读操作的响应时间通常要快一些。设备文件中的数据可以受益于 UNIX 文件系统高速缓存和 Adaptive Server 高速缓存，而且不需要物理磁盘访问就可以执行更多的读取操作。

dsync 的限制和约束

以下限制和约束适用于使用 **dsync** 的情况：

- 对于主设备， **dsync** 始终设置为 **true**，并且您无法更改该设置。
- 如果使用 **sp_deviceattr** 过程更改设备文件的 **dsync** 设置，请重新启动 Adaptive Server 以使更改生效。
- 从 12.x 版以前的 Adaptive Server 升级时，只会为主设备文件将 **dsync** 设置为 **true**。使用 **sp_deviceattr** 来更改任何其它设备文件的 **dsync** 设置。
- 对于存储在裸分区上的数据库设备， Adaptive Server 将忽略 **dsync** 设置。对存储在裸分区上的设备的写入操作始终直接写入物理介质。
- **directio** 和 **dsync** 参数是互斥的。如果设备的 **dsync** 设置为 **true**，则无法为同一设备将 **directio** 设置为 **true**。若要为设备启用 **directio**，您必须先将 **dsync** 重置为 **false**。

使用 *directio* 绕过操作系统缓冲区

利用 `disk init`、`disk reinit` 和 `sp_deviceattr` 的 `directio` 参数，您可以配置 Adaptive Server 以将数据直接传输到磁盘，而绕过操作系统缓冲区高速缓存。`directio` 采用与裸设备相同的方式执行 I/O，并提供与裸设备相同的性能优势，但它可以轻松地使用和管理文件系统设备。无法为主设备设置 `directio`。`directio` 是静态参数；请重新启动 Adaptive Server 以使其生效。

注释 `directio` 并非在所有平台上都可用。如果在不支持该参数的平台上发出带有 `directio` 参数的 `disk init`，Adaptive Server 将发出消息 `No such parameter: 'directio'`。

缺省情况下，`directio` 选项对于所有平台都设置为 `false`（关闭）。

注释 如果恢复对于某些数据库（例如 `tempdb`）并不重要，则用于这些数据库的设备缺省情况下可将 `dsync` 设置为 `false`。对于这些设备，启用 `directio` 可能会对性能产生负面影响，因此在启用 `directio` 之前请仔细查看设备使用情况。

以下示例将创建一个名为 “`user_disk`” 的设备，该设备使用 `directio` 将数据直接写入磁盘：

```
disk init
name = "user_disk",
physname = "/usr/u/sybase/data/userfile1.dat",
size = 5120, directio = true
```

若要在 UNIX 操作系统文件上初始化 10MB 的磁盘，请输入：

```
disk reinit
name = "user_disk",
physname = "/usr/u/sybase/data/userfile1.dat",
size = 5120, directio = true
```

缺省情况下，`directio` 对于所有现有设备均处于禁用状态；请使用 `sp_deviceattr` 将其启用：

```
sp_deviceattr device_name, directio, [true | false]
```

例如，以下命令将为 “`user_disk`” 设备启用 `directio` 磁盘写入：

```
sp_deviceattr user_disk, directio, true
```

disk init 的其它可选参数

vstart 是 Adaptive Server 开始使用数据库设备的起始虚拟地址或偏移量。vstart 接受以下可选单位指示符：“k”或“K”（千字节）、“m”或“M”（兆字节）、“g”或“G”（千兆字节）以及“t”或“T”（太字节）。偏移的大小取决于输入 vstart 值的方式：

- 如果未指定单位大小，则 vstart 将使用 2K 页作为其起始地址。例如，如果指定 vstart = 13，则 Adaptive Server 使用 13 * 2K 页作为起始地址的偏移量。
- 如果指定单位值，则 vstart 将使用您输入的值作为起始地址。例如，如果指定 vstart = "13M"，则 Adaptive Server 将起始地址的偏移量设置为 13MB。

vstart 的缺省值（通常为首选值）为 0。如果指定设备中的块数达不到 vstart + size 的块数之和，则 disk init 命令将失败。

可选的 cntrltype 关键字用于指定磁盘控制器。其缺省值为 0。除非有系统管理员的指导，否则不要重置此值。

注释 若要执行磁盘初始化，启动 Adaptive Server 的用户必须对要初始化的设备拥有适当的操作系统权限。

获取有关设备的信息

sp_helpdevice 提供了有关 sysdevices 表中设备的信息。

使用时如果不指定设备名，sp_helpdevice 将列出 Adaptive Server 上的所有可用设备。具有设备名时，它将列出所有关于此设备的信息。此处 sp_helpdevice 用于报告有关主设备的信息：

sp_helpdevice master				
device_name	physical_name	description		
-----	-----	-----		
master	d_master	special, default disk, physical disk, 30 MB		
status	cntrltype	vdevno	vpn_low	vpn_high
-----	-----	-----	-----	-----
3	0	0	0	10239

`master.sysdevices` 中的每一行描述：

- 用来备份数据库的转储设备（磁带、磁盘或文件），或
- 用于数据库存储的数据库设备。

`sysdevices` 的初始内容取决于操作系统。`sysdevices` 条目通常包括：

- 关于主设备的一个条目
- 关于 `sybsystemprocs` 数据库（使用该数据库可以存储其它的数据
库，例如 `pubs2` 和 `sybsyntax`）的一个条目，或者关于用户数据库和
日志的一个条目
- 关于磁带转储设备的两个条目

如果安装了审计功能，将会有有一个用于 `sybsecurity` 的独立设备。

`vpn_low` 和 `vpn_high` 列表示已指派给设备的页码。对于转储设备，这些
列表示设备的介质容量。

`status` 字段指示设备的类型、当用户发出 `create` 或 `alter database` 命令而未
指定数据库设备时是否将磁盘设备用作缺省存储设备、磁盘镜像信息以
及 `dsync` 设置。

表 7-2: `sysdevices` 中的状态位

位	含义
1	缺省磁盘（可由任何未指定位置的 <code>create</code> 或 <code>alter database</code> 命令使用）
2	物理磁盘
4	逻辑磁盘（未使用）
8	跳过标头（与磁带转储设备一起使用）
16	转储设备
32	串行写
64	设备已镜像
128	读取已镜像
256	仅辅助镜像端
512	已启用镜像
2048	内部使用；在 <code>disk unmirror, side = retain</code> 之后设置
4096	主设备需要被解除镜像（内部使用）
8192	辅助设备需要被解除镜像（内部使用）
16384	UNIX 文件设备使用 <code>dsync</code> 设置（直接写入物理介质）

有关转储设备和 `sp_addumpdevice` 的详细信息，请参见《系统管理指南：
卷 2》中的第 11 章“开发备份和恢复计划”。

删除设备

若要删除数据库和转储设备，请使用 `sp_dropdevice`：

```
sp_dropdevice logicalname
```

不能删除数据库正在使用的设备。必须首先删除数据库。

`sp_dropdevice` 从 `sysdevices` 中删除设备名。`sp_dropdevice` 不会删除操作系统文件；它只会使 Adaptive Server 无法访问该文件。请在使用 `sp_dropdevice` 之后使用操作系统命令来删除文件。

指派缺省设备

若要创建一个缺省数据库设备缓冲池以供所有 Adaptive Server 用户创建数据库时使用，可在设备初始化之后使用 `sp_diskdefault`。`sp_diskdefault` 在 `sysdevices` 中将设备标记为缺省设备。只要用户创建（或更改）数据库而未指定数据库设备，就从缺省磁盘空间的缓冲池分配新的磁盘空间。

`sp_diskdefault` 的语法为：

```
sp_diskdefault logicalname, {defaulton | defaultoff}
```

添加用户设备后，请使用 `defaultoff` 选项从缺省空间缓冲池中删除主设备：

```
sp_diskdefault master, defaultoff
```

以下命令指定 `sprocdev`（存放 `sybsystemprocs` 数据库的设备）为缺省设备：

```
sp_diskdefault sprocdev, defaulton
```

Adaptive Server 可以有多个缺省设备。将按照这些设备出现在 `sysdevices` 表中的顺序（即字母顺序）来使用它们。当第一个缺省设备填满后，将使用第二个缺省设备，依此类推。

注释 初始化一组数据库设备后，您可能需要将它们指派到特定的数据库或数据库对象，而不是将它们添加到设备的缺省缓冲池。例如，最好确保一个表的增长永远不超过特定设备的大小。

选择缺省设备和非缺省设备

通过 `sp_diskdefault`，您将能够针对性能和恢复规划空间使用，同时允许用户创建或更改数据库。

不要使用以下设备作为缺省设备：

- 主设备
- 用于 `sybsecurity` 的设备
- 供日志单独使用的任何设备
- 高性能数据库驻留的设备

可以为其它用户数据库使用存放 `sybsystemprocs` 的设备。

注释 如果在使用磁盘镜像或段，在决定将哪些设备添加到缺省列表时要谨慎。在大多数情况下，要被镜像的设备或包含放在段上的对象的数据库应专门分配设备，而不是使之成为缺省存储的一部分。

使用 `disk resize` 增加设备大小

使用 `disk resize` 命令可以动态增加数据库设备的大小，而不是初始化一个新设备。例如，如果 `/sybase/testdev.dat` 需要额外的 10MB 空间，则可以运行 `disk resize` 为该设备分配这一空间。`create` 和 `alter database` 命令可以使用这一增加的空间。

使用 `disk resize` 来增加裸分区上的设备以及文件系统的大小。可为设备增加的最小空间量为 1MB 或一个分配单元，两者相比取较大者。

页大小	分配单元大小	最小增量
2K	0.5MB	1MB
4K	1MB	1MB
8K	2MB	2MB
16K	4MB	4MB

不能对转储或装载设备使用 `disk resize`。

当增加设备大小后，在设备上设置的任何属性将继续保持设置状态。也就是说，如果设备在增加大小前已经设置了 `dsync`，则之后 `dsync` 仍处于已设置状态。同样，在增加设备大小前所设置的任何访问权限也仍将保持。

具有 `sa_role` 的用户可执行 `disk resize` 命令，该命令可以：

- 更新 `master....sysdevices` 中的高值，并
- 为数据库存储准备额外空间。

对 `disk resize` 使用审计追踪来跟踪调整设备大小的次数。调整操作期间，调整大小的设备始终处于联机状态并可供用户使用。

调整磁盘大小时，将要求：

- 您已使用 `disk init` 初始化了该设备。
- `device_name` 必须引用有效的逻辑设备名。
- 您在大小调整操作的过程中禁用镜像。您可以在大小调整操作完成时重新建立镜像。

在此示例中，设备 `testdev` 的配置为：

```
sp_helpdevice testdev
device_name  physical_name      description
status  cntrltype  vdevno      vpn_low      vpn_high
-----  -
testdev      /sybase/dev/testdev.dat    special, dsync on, directio off,
physical disk, 10.00MB
16386      0          1          0          5119
```

若要使用 `disk resize` 将 `testdev` 的大小增加 4MB，请输入：

```
disk resize
name = "test_dev",
size = "4M"
```

`testdev.dat` 现在为 14MB：

```
sp_helpdevice testdev
device_name  physical_name      description
status  cntrltype  vdevno      vpn_low      vpn_high
-----  -
testdev      /sybase/dev/testdev.dat    special, dsync on, directio off,
physical disk, 14.00MB
16386      0          1          0          7167
```

请参见《参考手册：命令》，了解 `disk resize` 语法。

磁盘空间不足

在磁盘物理初始化期间，如果由于磁盘空间不足发生错误，则 `disk resize` 会将数据库设备扩展到发生错误前的最大可能大小。

例如，在一台使用 4K 逻辑页的服务器上，如果尝试将设备的大小增加 40MB，但是只有 39.5MB 可用，则只能将设备扩展 39.5MB。

不能使用 `disk resize` 减小设备大小。

设置数据库选项

主题	页码
使用 sp_dboption 过程	267
数据库选项说明	268
查看数据库的选项	269

数据库选项控制：

- 事务行为
- 表列的缺省值
- 用户访问权限的限制
- 恢复操作和 bcp 操作的性能
- 日志行为

系统管理员和数据库所有者可以使用数据库选项来配置整个数据库的设置。数据库选项与 `sp_configure` 参数（影响整个服务器）和 `set` 选项（只影响当前会话或存储过程）不同。

使用 `sp_dboption` 过程

可以使用 `sp_dboption` 更改整个数据库的设置。选项在更改之前一直有效。`sp_dboption`：

- 不带参数使用时，将显示数据库选项的完整列表
- 带参数使用时，将更改某个数据库选项

只能更改用户数据库的选项。不能更改 `master` 数据库的选项。若要更改用户数据库中的数据库选项（或显示数据库选项的列表），可在使用 `master` 数据库时执行 `sp_dboption`。

语法为：

```
sp_dboption [dbname, optname, {true | false}]
```

注释 当您重新启动 Adaptive Server 时，对 **model** 的数据库选项所做的更改不会影响 **tempdb** 或当前用户定义的多个临时数据库。这些更改只会出现在您在更改 **model** 数据库之后创建的数据库中。重新启动 Adaptive Server 将会清除包含在临时数据库中的对象和数据，但不会重置数据库选项。

数据库选项说明

对 **master** 数据库具有访问权限的所有用户都可以执行不带参数的 **sp_dboption** 来显示数据库选项列表。**sp_dboption** 生成的报告类似于：

```
sp_dboption
Settable database options.
-----
abort tran on log full
allow nulls by default
async log service
auto identity
dbo use only
ddl in tran
delayed commit
identity in nonunique index
no chkpt on recovery
no free space acctg
read only
select into/bulkcopy/pllsort
single user
trunc log on chkpt
trunc. log on chkpt.
unique auto_identity index
```

若要获取有关特定数据库中设置了哪些选项的报告，请在该数据库中执行 **sp_helpdb**。

请参见 **Commands Reference: Procedures**（《命令参考：过程》），详细了解有关每个数据库选项的信息。

查看数据库的选项

使用 `sp_helpdb` 可以确定为特定数据库设置的选项。`sp_helpdb` 在其输出的“status”列中列出各个活动选项。

下面的示例显示在 `mydb` 中启用了 `read only` 选项：

```

sp_helpdb mydb

name          db_size  owner  dbid   created          status
-----
mydb          20.0 MB   sa     5      Mar 05, 2005    read only

device_fragments  size      usage          created          free kbytes
-----
master            10.0 MB   data and log   Mar 05 2005     1792

device          segment
-----
master          default
master          logsegment
master          system

```

若要显示所有数据库的选项摘要，请使用 `sp_helpdb` 而不指定数据库：

```

sp_helpdb

name          db_size  owner  dbid   created          status
-----
master        48.0 MB   sa     1      Apr 12, 2005    mixed log and data
model         8.0 MB   sa     3      Apr 12, 2005    mixed log and data
pubs2         20.0 MB   sa     6      Apr 12, 2005    select into/
               bulkcopy/pllsort, trunc log on chkpt, mixed log and data
sybssystemdb  8.0 MB   sa     5      Apr 12, 2005    mixed log and data
sybssystemprocs 112.0 MB sa     4      Apr 12, 2005    trunc log on chkpt,
               mixed log and data
tempdb        8.0 MB   sa     2      Apr 12, 2005    select into/
               bulkcopy/pllsort, trunc log on chkpt, mixed log and data

```


配置字符集、排序顺序和语言

本章讨论了 Adaptive Server 国际化和本地化支持的问题。

主题	页码
了解国际化和本地化	271
国际化系统的优点	272
国际化系统示例	273
国际化系统的元素	275
为服务器选择字符集	275
选择排序顺序	283
为系统消息选择语言	290
设置服务器：示例	291
更改字符集、排序顺序或消息语言	293
安装不支持语言的日期字符串	303
国际化和本地化文件	304

了解国际化和本地化

国际化是使应用程序支持多语言和文化习惯的过程。

国际化的应用程序使用外部文件在运行时提供特定语言的信息。因为不包含特定的语言代码，所以国际化的应用程序可在任何本地语言环境中配置而无需更改代码。单一版本的软件产品可适应不同语言和地区，无需工程方面的更改即可符合当地要求和习惯。这种软件开发方法在应用程序的整个寿命周期内节省了大量的时间和金钱。

本地化是使国际化的产品适合特定语言（如西班牙语）或地区要求的过程，包括提供已翻译的系统信息、用户界面及正确的日期、时间和货币格式。软件产品的一个版本可能有多个本地化版本。

Sybase 提供国际化和本地化支持。Adaptive Server 包括字符集定义文件和排序顺序定义文件，这些文件是支持西欧、东欧、中东、拉丁美洲和亚洲各种主要商务语言的数据处理所必需的。

Sybase 语言模块提供已翻译的系统信息和中文（简体）、法语、德语、日语、朝鲜语、巴西葡萄牙语和西班牙语版本。缺省情况下， Adaptive Server 使用美国英语的消息文件。

本章介绍了可用字符集和语言模块，并总结了更改 Adaptive Server 的缺省字符集、排序顺序或消息语言所需的步骤。

国际化系统的优点

设计一个能在本国以外工作的应用程序，这一任务看起来是令人望而生畏的。通常，程序员认为国际化意味着基于对一个国家 / 地区文化和语言习惯的硬编码依赖性。

更好的方法是编写国际化的应用程序：这样的应用程序会检查本地计算环境来确定使用何种语言，并在运行时装载包含特定语言信息的文件。

当使用国际化应用程序时，单个应用程序可在所有国家 / 地区配置。这种方法具有以下优点：

- 编写和维护一个应用程序。
- 如果需要，这个应用程序不用做任何更改就可以在其它国家 / 地区配置，只须提供正确的本地化文件即可。
- 所有节点都具有标准的功能和行为。

国际化系统示例

国际化系统可能包括运行于不同本地语言环境的不同平台上的国际化的客户端应用程序、网关和服务端。

例如，国际化系统可能包括以下组件：

- 位于纽约、墨西哥城和巴黎的订单处理应用程序（Client-Library 应用程序）
- 位于德国的库存控制服务器（Adaptive Server）
- 位于法国的订单完成服务器（Adaptive Server）
- 位于日本的中央会计应用程序（与 Adaptive Server 一同工作的 Open Server 应用程序）

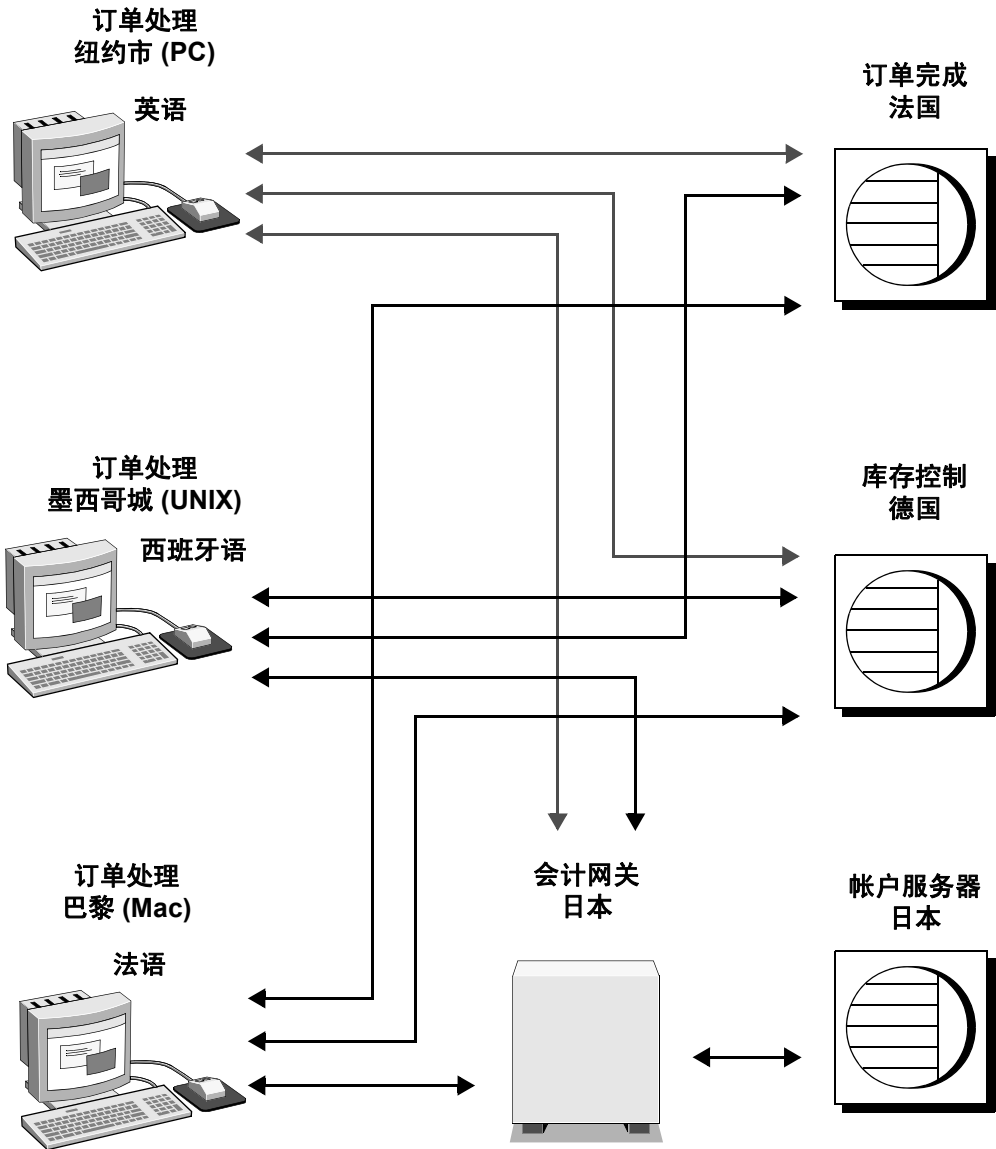
在此系统中，订单处理应用程序：

- 查询库存控制服务器，以确定库存中是否有请求的物品
- 通过订单完成服务器下订单
- 向会计应用程序发送财务信息

库存控制服务器和订单完成服务器对查询作出响应，会计应用程序收集财务数据并生成报告。

这个系统类似于：

图 9-1：国际化系统的示例



在此示例中，所有应用程序和服务使用本地语言和字符集来接受输入并输出消息。

国际化系统的元素

有三种元素，可用来在国际化环境中配置服务器语言。Sybase 建议查看这三种元素并仔细计划要创建的客户端 / 服务器网络。

- 字符集 — 服务器用于与客户端服务器交换数据的语言。应在仔细计划和分析所有客户端服务器的语言需要之后，对字符集进行选择。
- 排序顺序 — 排序顺序选项取决于所选的语言和字符集。
- 系统消息 — 用 Sybase 提供的几种语言之一显示的消息。如果服务器语言不是所提供的语言之一，则以英语（缺省语言）显示系统消息。

下节提供了每种元素的详细信息。

为服务器选择字符集

服务器中的所有数据都用特殊代码进行编码。例如，将字母“a”编码为十进制的“97”。**字符集**是字符（包括字母和数字字符、符号和非打印控制字符）及为其指派的数字值或代码的特定集合。字符集通常包含一个字母表中的字符，例如，英语中使用拉丁字母表，而诸如俄语、塞尔维亚语和保加利亚语等语言使用古斯拉夫语之类的脚本。平台专用并支持一组语言（如西欧语言）子集的字符集称为**本地或国家字符集**。除了 Unicode UTF-8 之外，Adaptive Server 使用的所有字符集都是本地字符集。

脚本是一个书写系统，是具有某种人类语言（例如拉丁语、日语或阿拉伯语）书写格式特征的所有元素的集合。根据字母表或脚本所支持语言的不同，字符集可支持一种或多种语言。例如，拉丁字母表支持西欧语言（请参见第 276 页的表 9-1 中的第 1 组）。另一方面，日语脚本仅支持日语这一种语言。因此，组 1 中的字符集支持多种语言，而许多字符集，如组 101 中的字符集，仅支持一种语言。

字符集所包含的一种或多种语言称为**语言组**。语言组可包含多种语言或仅一种语言，本地字符集是特定语言组的一种或多种语言字符的特定平台编码。

在客户端 / 服务器网络中，如果所有语言都属于同一语言组（请参见第 276 页的表 9-1），则您可以支持采用多种语言的数据处理。例如，如果服务器中的数据用组 1 中的字符集编码，则同一数据库中可以有法语、德语和意大利语数据以及任何其它在组 1 中的语言。然而，在同一数据库中不可以存储来自其它语言组的数据。例如，不可以将日语数据和法语或德语数据一起存储。

与刚刚介绍的本地字符集不同， **Unicode** 是支持世界上 650 多种语言（例如日语、中文、俄语、法语和德语）的国际字符集。Unicode 允许在同一服务器上混合使用不同语言组的不同语言，并与平台无关。有关详细信息，请参见第 277 页的“Unicode”。

由于所有字符集都支持拉丁语脚本，并且因而支持英语，所以一个字符集总是至少支持两种语言，即英语和另外一种语言。

许多语言由超过一种的字符集所支持。为某种语言安装的字符集取决于客户端平台和操作系统。

Adaptive Server 支持以下语言和字符集：

表 9-1: 支持的语言和字符集

语言组	语言	字符集
组 1	西欧： 阿尔巴尼亚语、加泰罗尼亚语、丹麦语、荷兰语、英语、法罗语、芬兰语、法语、加利西亚语、德语、冰岛语、爱尔兰语、意大利语、挪威语、葡萄牙语、西班牙语、瑞典语	ASCII 8、CP 437、CP 850、CP 860、CP 863、CP 1252 ^a 、ISO 8859-1、ISO 8859-15、Macintosh Roman、ROMAN8、ROMAN9、ISO-15、CP 858
组 2	东欧： 克罗地亚语、捷克语、爱沙尼亚语、匈牙利语、拉脱维亚语、立陶宛语、波兰语、罗马尼亚语、斯洛伐克语、斯洛文尼亚语（和英语）	CP 852、CP 1250、ISO 8859-2、Macintosh Central European
组 4	波罗的语（和英语）	CP 1257
组 5	古斯拉夫语： 保加利亚语、白俄罗斯语、马其顿语、俄语、塞尔维亚语、乌克兰语（和英语）	CP 855、CP 866、CP 1251、ISO 8859-5、Koi8、Macintosh Cyrillic
组 6	阿拉伯语（和英语）	CP 864、CP 1256、ISO 8859-6
组 7	希腊语（和英语）	CP 869、CP 1253、GREEK8、ISO 8859-7、Macintosh Greek
组 8	希伯来语（和英语）	CP 1255、ISO 8859-8
组 9	土耳其语（和英语）	CP 857、CP 1254、ISO 8859-9、Macintosh Turkish、TURKISH8
组 101	日语（和英语）	CP 932 DEC Kanji、EUC-JIS、Shift-JIS
组 102	简体中文（中华人民共和国）（和英语）	CP 936、EUC-GB、GB18030
组 103	繁体中文（台湾地区）（和英语）	Big 5、CP 950 ^b 、EUC-CNS、Big 5 HKSCS
组 104	朝鲜语（和英语）	EUC-KSC、cp949
组 105	泰语（和英语）	CP 874、TIS 620
组 106	越南语（和英语）	CP 1258
Unicode	超过 650 种语言	UTF-8

a. 除了 0x80-0x9F 码点在 CP 1252 中映射为字符以外，CP 1252 与 ISO 8859-1 完全相同。

b. CP 950 与 Big 5 相同。

注释 由于任何字符集的前 128（十进制）个字符都包含拉丁字母表（定义为“ASCII-7”），因此所有字符集都支持英语。各字符集中前 128 个字符之外的字符各不相同，用于支持不同的本地语言字符。例如，CP 932 和 CP 874 中的码点 0-127 都支持英语和拉丁字母表。但是，码点 128-255 在 CP 932 中支持日语字符，而在 CP 874 中支持泰语字符。

以下字符集支持欧洲货币符号“欧元”：CP 1252（西欧）、CP 1250（东欧）、CP 1251（古斯拉夫语）、CP 1256（阿拉伯语）、CP 1253（希腊语）、CP 1255（希伯来语）、CP 1254（土耳其语）、CP 874（泰语）、iso15、roman9 和 CP858。Unicode UTF-8 还支持：

- Windows 和 Solaris 平台上的繁体中文
- Linux 平台上的阿拉伯语、希伯来语、泰语和俄语

注释 iso_1 和 ISO 8859-1 是同一字符集的不同名称。

若要混合使用不同语言组中的语言，您必须使用 Unicode。如果服务器字符集是 Unicode，则可在单一服务器上支持超过 650 种的语言，并且可混合不同语言组中的语言。

Unicode

Unicode 是第一个支持使用同一数据集对世界上的所有语言进行编码的字符集。在引入 Unicode 之前，例如，如果要以中文存储数据，则必须选择适合该语言的字符集，这样就将其余大多数语言排除在外。将不同的字符集混合在一起，从而在同一数据集中使用多种语言是不可能或不切实际的。

Sybase 支持以下三种数据类型的 Unicode：unichar、univarchar 和 unitext。这些数据类型以 Unicode 的 UTF-16 编码方式存储数据。

在 UTF-16 编码方式中，Unicode 标量值用一个 16 位值表示（或者，在少数情况下，用一对 16 位值表示）。这三种编码方式中的任一种都可用于表示所有 Unicode 字符，从这方面来说，它们是等价的。之所以选择使用 UTF-16 数据类型，而不使用 UTF-8 服务器缺省字符集，是为了实现对现有数据库应用程序的简单、分步迁移。

Adaptive Server 支持在 SQL 查询中使用 Unicode 文字，并且支持 UTF-8 的多种排序顺序。

Adaptive Server 使用的字符集模型基于单个、可配置的全服务器范围内的字符集。使用任一种“字符”数据类型（`char`、`varchar`、`nchar`、`nvarchar` 和 `text`）存储在 Adaptive Server 中的所有数据都被解释为在此字符集中。排序顺序是用此字符集定义的，语言模型（翻译为本地语言的服务器消息集合）也是。

在连接对话框期间，客户端应用程序声明其本地字符集和语言。如果配置正确，服务器之后会尝试在自己的字符集和客户端的字符集之间转换任何字符数据（字符数据包括存储在数据库中的任何数据，以及采用客户端本机语言的服务器消息）。只要服务器和客户端的字符集兼容，这就没有问题。但是，如果字符在另一字符集中未定义，就会出现错误。例如，用于日语的字符集 SJIS、用于俄语的 KOI8 和其它古斯拉夫语言。这种不兼容性就是引入 Unicode 的原因。我们可将 Unicode 看作一个超字符集，它包括其它所有字符集中的字符的定义。

Unicode 数据类型 `unichar`、`univarchar` 和 `unitext` 完全独立于传统的字符集模型。客户端单独发送和接收 Unicode 数据，与其发送和接收的任何其它字符数据无关。

安装字符集

Adaptive Server 版本 12.5.1 和更高版本支持 4 个字节格式的 UTF-8，这种格式用于表示在 UTF-16 中用 16 位值对（“代理对”）表示的少数特殊 Unicode 字符。在 Adaptive Server 版本 12.5.1 之前，只支持 3 个字节格式的 UTF-8。如果在早于版本 12.5.1 的 Adaptive Server 服务器上安装了 UTF-8 字符集，则应重新安装该字符集，以便能够使用 4 个字节格式的 UTF-8。

配置参数

Unicode 的 UTF-16 编码包括“代理对”，这些代理对表示很少使用的字符。Adaptive Server 中内置了额外的检查机制，以确保代理对的完整性。可以通过将配置参数“`enable surrogate processing`”设置为 0 来关闭此检查机制。尽管这样做将不再确保代理对的完整性，但可以使性能得到略微提高。

Unicode 还定义了“规范化”过程，通过这一过程，一个字符的所有可能表示形式都将被转换为单一的表示形式。许多后面跟有混合变音标记的基本字符与预先构成的字符等同，虽然它们的位模式并不相同。例如，以下两个序列等同：

```
0x00E9  -- é (LATIN SMALL LETTER E WITH ACUTE)
0x00650301  -- e (LATIN SMALL LETTER E), ´ (COMBINING ACUTE ACCENT)
```

`enable unicode normalization` 配置参数控制 Adaptive Server 是否对传入的 Unicode 数据进行规范化。

如果将 `default Unicode sortorder` 设置为 “binary”，并且 `enable Unicode normalization` 配置参数设置为 1，则可以大大提高性能。这个组合允许 Adaptive Server 对 Unicode 数据的性质进行几种假设，而且已实现了代码来利用这些假设。

函数

所有接受 `char` 参数的函数均经过了过载设计，也可接受 `unichar`。对于具有多个参数的函数，在使用至少一个 `unichar` 参数调用时，这些函数会隐式地将所有非 `unichar` 参数转换为 `unichar`。

在 `enable surrogate processing` 设置为 1（缺省值）时，为确保代理对的完整性，字符串函数不允许拆分代理对。位置会被调整到代理对的开头处。

添加了几个函数以完善对 `unichar` 的支持。其中包括 `to_unichar()` 和 `uscalar()`，这两个函数类似于 `char()` 和 `ascii()`。函数 `uhighsurr()` 和 `ulowsurr()` 可用于对用户代码中的代理对进行显式处理。

使用包含函数的 `unitext` 时，会有一些限制。有关信息，请参见每个函数“用法”部分下的限制说明。

使用 unichar 列

使用 `isql` 或 `bcp` 实用程序时，Unicode 值将显示为十六进制形式，除非使用 `-Jutf8` 标志，表明客户端的字符集为 UTF-8。在这种情况下，实用程序会将它从服务器接收到的任何 Unicode 数据都转换为 UTF-8。例如：

```
% isql -Usa -P -Jiso_1
1> select unicode_name from people where unicode_name = 'Jones'
2> go

unicode_name
-----
0x004a006f006e00650073
(1 row affected)
```

但是：

```
% isql -Usa -P -Jutf8
1> select unicode_name from people where unicode_name = 'Jones'
2> go

unicode_name
-----
Jones
(1 row affected)
```

这简化了即席查询。并非所有终端窗口都能显示全部的 Unicode 字符，但涉及 ASCII 字符的简单测试得到了大大地简化。

使用 `unitext`

可变长度的 `unitext` 数据类型最多可容纳 1,073,741,823 个 Unicode 字符（2,147,483,646 字节）。可以在使用 `text` 数据类型的任何位置，使用具有相同语义的 `unitext`。无论 Adaptive Server 的缺省字符集是什么，`unitext` 列都采用 UTF-16 编码存储。

Open Client 互用性

Open Client 库支持数据类型 `cs_unichar`，该数据类型可以绑定到声明为短整型数组的用户变量。此 Open Client 数据类型直接与服务器的 `unichar`、`unitext` 和 `univarchar` 交互。

Java 互用性

内部 JDBC 驱动程序可有效地在 SQL 和 Java 环境之间传送 `unichar` 数据。

从 SQL 向 Java 传送数据时，`java.sql.ResultSet` 类提供了大量“获取”方法用于从结果集的列中检索数据。其中的任何一种获取方法都可使用定义为 `unichar`、`unitext` 或 `univarchar` 的列。`getString()` 方法的效率特别高，原因是无需执行任何转换。

使用 `java.sql.PreparedStatement` 类的 `setString()` 方法从 Java 向 SQL 传送数据。内部 JDBC 驱动程序会将 Java 字符串数据直接复制到定义为 `unichar`、`unitext` 或 `univarchar` 的 SQL 参数中。

外部 JDBC 驱动程序 (jConnect) 已进行了修改，可支持与内部驱动程序相同的无缝接口。

限制

由于 Adaptive Server 的早期版本未包括基于 Unicode 的语言分析程序，因此使用新的 Unicode 数据类型会受到限制。若要使用新的数据类型，需要将服务器的缺省字符集配置为 UTF-8。Adaptive Server 12.5.1 版及更高版本中已经没有这个限制。无论服务器的缺省字符集是什么，都可以使用 Unicode 数据类型。

选择服务器缺省字符集

配置服务器时，必须为服务器指定缺省字符集。缺省字符集是服务器用来存储和处理数据的字符集。每个服务器只能有一个缺省字符集。

缺省情况下，安装工具假定平台操作系统的本地字符集是服务器的缺省字符集。但是，您可以选择任何 Adaptive Server 支持的字符集作为服务器上的缺省字符集（请参见第 276 页的表 9-1）。

例如，如果在运行 AIX 的 IBM RS/6000 上安装服务器，并选择安装一种西欧语言，则安装工具假定缺省字符集为 ISO 8859-1。

如果要安装 Unicode 服务器，请选择 UTF-8 作为缺省字符集。

对于非 Unicode 服务器，请确定大多数客户端系统使用的平台，并使用此平台的字符集作为服务器的缺省字符集。

这有两个优点：

- 字符集间不可映射字符数量得到减少。

由于通常在两个字符集的字符间没有完全一对一的映射，因此有可能造成部分数据丢失。这通常很少发生，因为大多数的未转换字符是不常用的特殊符号，或是某一平台专有的。

- 这将所需的字符集转换减至最少。

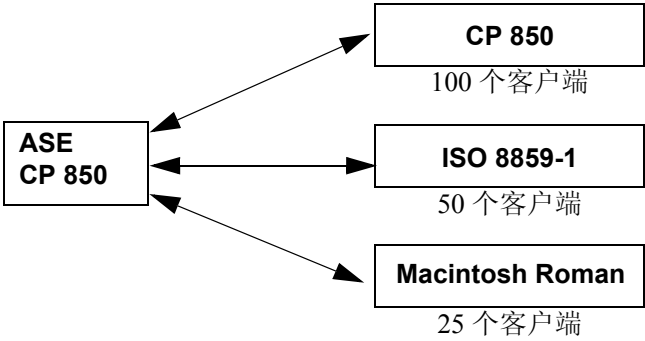
当客户端系统的字符集与服务器缺省字符集不同时，必须转换数据以确保数据完整性。虽然字符集转换所导致的性能降低是微不足道的，但最好选择引起转换最少的字符集。

例如，如果大多数客户端使用 CP 850，就应在服务器上指定 CP 850 为缺省字符集。即使服务器是在 HP-UX 系统（其组 1 的语言的本地字符集是 ROMAN8）上也可这样做。

注释 Sybase 强烈建议在创建任何数据库或对 Sybase 所提供的数据库进行任何更改之前决定要使用何种字符集作为缺省字符集。

在下面的示例（图 9-2）中，175 个客户端都访问同一个 Adaptive Server。客户端在不同的平台上，并使用不同的字符集。允许这些客户端一起运行的关键因素是，客户端 / 服务器系统中的所有字符集都属于同一语言组（请参见第 276 页的表 9-1）。Adaptive Server 的缺省语言是 CP 850，它是大多数客户端使用的字符集。这使得服务器最有效地工作，所需字符集转换也最少。

图 9-2：使用同一语言组中不同字符集的客户端



为帮助选择服务器缺省字符集，下表按平台和语言列出了最常用的字符集。

表 9-2：流行的西欧语言客户端平台

平台	语言	字符集
Win 95、 98	美国英语、西欧	CP 1252
Win NT 4.0	美国英语、西欧	CP 1252
Win 2000	美国英语、西欧	CP 1252
Sun Solaris	美国英语、西欧	ISO 8859-1
HP-UX 10、 11	美国英语、西欧	ROMAN8
IBM AIX 4.x	美国英语、西欧	ISO 8859-1

表 9-3：流行的日语客户端平台

平台	语言	字符集
Win 95、 98	日语	CP 932 for Windows
Win NT 4.0	日语	CP 932 for Windows
Win 2000	日语	CP 932 for Windows
Sun Solaris	日语	EUC-JIS
HP-UX 10、 11	日语	EUC-JIS
IBM AIX 4.x	日语	EUC-JIS

表 9-4：流行的中文客户端平台

平台	语言	字符集
Win 95、 98	中文（简体）	CP 936 for Windows
Win NT 4.0	中文（简体）	CP 936 for Windows
Win 2000	中文（简体）	CP 936 for Windows
Sun Solaris	中文（简体）	EUC-GB
HP-UX 10、 11	中文（简体）	EUC-GBS
IBM AIX 4.x	中文（简体）	EUC-GB

选择排序顺序

不同语言对同样字符的排序是不同的。例如，在英语中，*Cho* 排在 *Co* 之前，而在西班牙语中则相反。在德语中，*ß* 是个单字符，而在字典中将其视为双字符 *ss* 并相应进行排序。变音字符按特定顺序排序，因此，*aménité* 排在 *amène* 之前，而如果忽略变音，排序顺序则相反。因此，需要使用语言特定的排序顺序，以便正确地对字符进行排序。

每种字符集都有一种或多种排序顺序，*Adaptive Server* 使用它们来收集数据。排序顺序与特定语言或语言组及特定的字符集联系密切。由于英语、法语和德语采用相同方式对相同的字符进行排序，因此，它们可以使用同样的排序顺序，例如，*A*、*a*、*B*、*b*，等等。或者，字符是特定于其中一种语言的——例如，法语中使用变音字符 *é*、*à* 和 *á*，但英语或德语中不使用这些字符——因此，这些字符的排序方式没有冲突。然而，对于西班牙语却不是这样，在西班牙语中，双字母 *ch* 和 *ll* 的排序是不同的。因此，虽然相同的字符集支持所有四种语言，但英语、法语和德语有一组排序顺序，而西班牙语有一组不同的排序顺序。

另外，排序顺序与特定字符集密切相关。因此，在 *ISO 8859-1* 字符集中有一组英语、法语和德语的排序顺序，在 *CP 850* 字符集中有另外的一组，等等。特定字符集的可用排序顺序位于字符集目录的排序顺序定义文件（**.srt* 文件）中。有关字符集及其可用排序顺序的列表，请参见第 285 页的表 9-5。

使用排序顺序

排序顺序用于：

- 创建索引
- 将数据存入按索引排序的表
- 指定 *order by* 子句

不同类型的排序顺序

为所有字符集都至少提供了一个二进制排序顺序，这种排序顺序对数据进行摸索式的排序，即排序仅基于字符集中分配给代表每个字符的代码（“二进制”代码）的算术值。二进制排序顺序适用于每个字符集的前 128 个字符（*ASCII* 英语）和亚洲语言。如果字符集支持多种语言（例如，组 1 或 *Unicode*），二进制排序顺序很可能会得出不正确的结果，并且您应选择其它排序顺序。

字符集也可以有以下一种或多种字典排序顺序：

- **字典顺序，区分大小写，区分变音**— 分别对大写和小写字母进行排序。字典排序顺序识别字母的各种变音形式，并将它们排在相关的非变音字母之后。
- **字典顺序，不区分大小写，区分变音**— 按字典顺序对数据排序，但不区分大小写。大写字母与相应的小写字母等同，在排序结果中大小写字母混合在一起。对于避免名称表中的重复条目是很有用的。
- **字典顺序，不区分大小写，区分变音，按优先级排序**— 在确定条目是否相同时不区分大小写。同一单词的大小写形式是同等的。在所有其它条件相同时，大写字母具有高的优先级（它们先出现）。

当 `order by` 子句中指定的列与表的聚簇索引的键相匹配时，使用这种具有优先级的不区分大小写的排序顺序可能导致大型表的性能降低。不要选择具有优先级的不区分大小写的排序顺序，除非安装要求在 `order by` 子句的其它同等字符串中，大写字母排在小写字母之前。

- **字典顺序，不区分大小写，不区分变音**— 将变音形式的字母与不加变音的关联字母视为相同。它在排序结果中混合了变音字符。

选择缺省排序顺序

Sybase 服务器每次只能支持一种缺省排序顺序。如果用户使用同一语言或他们的语言使用同样的排序顺序，那么就选择所需要的排序顺序。例如，如果用户使用法语，并希望使用法语排序，那么就可选用一种法语字典排序顺序。或者，如果用户使用多语言的数据，并且这些语言使用同样的排序顺序，例如，英语、法语和德语，那么就可选用一种排序顺序，它可用于所有使用各种语言的用户。

然而，如果用户使用不同语言（需要不同的排序顺序），例如，法语和西班牙语，那么，必须在排序顺序中选择一种作为缺省排序顺序。举例而言，如果选用了法语排序顺序，那么，对于使用西班牙语的用户，*ch* 和 *ll* 这样的双字符的排序就不会像他们所期望的那样。在缺省状态下，安装过程用二进制排序顺序配置服务器。

可使用 `sortkey` 函数为数据设置定制的替代排序顺序（每种语言设置一种排序顺序）。可动态选择这些排序顺序来满足不同用户的需求。`sortkey` 函数是从缺省排序顺序中分离出来的，但它们可共存于同一服务器中。`sortkey` 函数所提供的排序顺序比缺省排序顺序机制所提供的排序顺序在广度和深度上要好。有关详细信息，请参见《参考手册：构件块》中的 `sortkey` 和 `compare`。

表 9-5：可用的排序顺序

语言或脚本	字符集	排序顺序
所有语言	UTF-8	多种排序顺序，请参见表 9-7 以获取列表
古斯拉夫语： 保加利亚语、白俄罗斯语、马其顿语、俄语、塞尔维亚语、乌克兰语	CP 855、CP 866、CP 1251、ISO 8859-5、Koi8、Macintosh Cyrillic	字典顺序，区分大小写，区分变音
东欧： 捷克语、斯洛伐克语	CP 852、ISO 8859-2、CP 1250	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，区分变音 字典顺序，区分大小写，区分变音，具有优先级字典顺序，不区分大小写，不区分变音
英语、法语、德语	ASCII 8、CP 437、CP850、CP 860、CP 863、CP 1252a、ISO 8859-1、ISO 8859-15、Macintosh Roman、ROMAN8、ROMAN9、ISO 15	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，区分变音 字典顺序，区分大小写，区分变音，具有优先级 字典顺序，不区分大小写，不区分变音
英语、法语、德语	CP 850、CP 858	替代字典顺序，区分大小写 替代字典顺序，区分大小写，不区分变音 替代字典顺序，区分大小写，具有优先级
希腊语	ISO 8859-7	字典顺序，区分大小写，区分变音
匈牙利语	ISO 8859-2	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，区分变音 字典顺序，不区分大小写，不区分变音
日语	EUCJIS、SJIS、DECKANJI	不区分大小写的通用字典顺序
哈萨克语	87	50
俄语	CP 866、CP 1251、ISO 8859-5、Koi8、Macintosh Cyrillic	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，区分变音
斯堪的纳维亚语	CP 850	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，具有优先级
简体中文	EUC-GB、GB-18030、CP936	不区分大小写的通用字典顺序
西班牙语	ASCII 8、CP 437、CP850、CP 860、CP 863、CP 1252、ISO 8859-1、ISO 8859-15、Macintosh Roman、ROMAN8	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，区分变音 字典顺序，不区分大小写，不区分变音
泰语	CP 874、TIS 620	字典顺序
土耳其语	ISO 8859-9	字典顺序，区分大小写，区分变音 字典顺序，不区分大小写，不区分变音 字典顺序，不区分大小写，区分变音

语言或脚本	字符集	排序顺序
西欧语言	CP 1252	字典顺序，不区分大小写，区分变音，具有优先级，不区分变音，西班牙语字典，不区分大小写的西班牙语，不区分变音的西班牙语

对于在此未列出的语言，没有该语言的特定语言排序顺序。选择二进制排序顺序，然后研究 `sortkey` 函数是否满足要求。如此表所示，许多语言有多种排序顺序。

中文拼音排序顺序

拼音（更正式的名称为“汉语拼音”）使用罗马字母来表示标准中文发音系统。拼音包含一个转写为罗马字母的转写系统，用于不使用中文字符阅读和书写普通话。拼音使用变音来表示普通话的四个音调。

Adaptive Server 的早期版本使用简体中文 (GB) 排序顺序（`gbpinyin` 和 `gbpinyinocs`），同时使用 `Unilib` 字符集，从而会对使用 GB 字符集的数据库的性能产生很大影响。

Adaptive Server 15.0.3 版自动使用 `gbpinyin` 和 `gbpinyinocs` 排序顺序，从而避免了处理步骤，并显著改善了性能。

在早期版本中，缺省 `size of unilib cache` 配置参数为 268 KB。在 15.0.3 版中，缺省值已增加到 302 KB。

在访问 ASCII 和 `gbpinyin` 数据的查询中，性能得到了改善。但是，如果数据集混用了其它字符，您可能看不到任何性能改善。

有关配置 Adaptive Server 以使用 `gbpinyin` 和 `gbpinyinocs` 排序顺序的信息，请参见《系统管理指南》中的第 9 章“配置字符集、排序顺序和语言”。

选择用于中文和日文字符集的不区分大小写的排序顺序

使用两个存储过程来选择不区分大小写的排序顺序：

- `sp_helpsort`
- `sp_configure`

`sp_helpsort`

`sp_helpsort` 列出了不区分大小写的可用排序顺序。

```
sp_helpsort
-----
Name                                ID
-----
nocase_eucgb                        52
nocase_cp936                        52
nocase_gb18030                      52
nocase_eucjis                       52
nocase_sjis                         52
nocase_deckanji                     52
```

`sp_configure`

若要切换到不区分大小写的排序顺序，请输入：

```
sp_configure 'default sortorder id', 52
```

选择缺省 Unicode 排序顺序

缺省的 Unicode 排序顺序明显不同于服务器缺省字符集的排序顺序。这个单独的配置参数是静态参数，如果它发生了变化，就需要重新启动服务器并重新建立 `unichar` 数据的索引。此排序顺序使用字符串参数，而不是数字参数，以确保排序顺序是唯一的。

表 9-6 列出了可用的缺省 Unicode 排序顺序。

表 9-6：缺省的 Unicode 排序顺序

名称	ID	说明
defaultml	20	缺省的 Unicode 多语言排序
thaidict	21	泰语字典顺序
iso14651	22	按照每个 ISO14651 标准进行排序
utf8bin	24	为与 UTF-8 二进制相匹配的 UTF-16 排序
binary	25	二进制排序
altnoacc	39	替代不区分变音

名称	ID	说明
altdict	45	替代字典排序
altnocsp	46	替代不区分大小写且具有优先级
scandict	47	斯堪的纳维亚语字典排序
scannocp	48	斯堪的纳维亚语不区分大小写且具有优先级
bin_utf8	50	UTF-8 二进制排序顺序
dict	51	通用字典顺序
nocase	52	不区分大小写的通用字典顺序
nocasep	53	通用的不区分大小写且具有优先级
noaccent	54	通用的不区分变音的字典顺序
espdict	55	西班牙语字典顺序
espnocs	56	不区分大小写的西班牙语字典顺序
espnocac	57	不区分变音的西班牙语字典顺序
rusnocs	59	不区分大小写的俄语字典顺序
cyrnocs	64	不区分大小写的古斯拉夫语字典顺序
elldict	65	希腊语字典顺序
hundict	69	匈牙利语字典顺序
hunnocac	70	不区分变音的匈牙利语字典顺序
hunnocs	71	不区分大小写的匈牙利语字典顺序
turknocac	73	不区分变音的土耳其语字典顺序

表 9-7 列出了可装载的排序顺序。

表 9-7：可装载的排序顺序

名称	ID	说明
cp932bin	129	与 CP932 的二进制排序相匹配的顺序
dynix	130	中文拼音排序
gb3213bn	137	与 GB2312 的二进制排序相匹配的顺序
cyrdict	140	通用古斯拉夫语字典顺序
turdict	155	土耳其语字典顺序
euckscbn	161	与 EUCKSC 的二进制排序相匹配的顺序
gbpinyin	163	中文拼音排序
rusdict	165	俄语字典顺序
sjisbin	179	与 SJIS 的二进制排序相匹配的顺序
eucjisbn	192	与 EUCJIS 的二进制排序相匹配的顺序
big5bin	194	与 BIG5 的二进制排序相匹配的顺序

若要在 Adaptive Server 中查看此排序顺序列表，请使用 `sp_helpsort`。请参见《参考手册：过程》。

可使用 `$$SYBASE/collate/Unicode` 目录中的外部文件来添加排序顺序。名称与归类 ID 存储在 `syscharsets` 中。在设置缺省 Unicode 排序顺序之前，外部 Unicode 排序顺序名称不必在 `syscharsets` 中。

注释 外部 Unicode 排序顺序由 Sybase 提供。不要尝试创建外部 Unicode 排序顺序。

与 Unicode 数据相关联的排序顺序完全独立于与传统字符数据相关联的排序顺序。所有涉及 Unicode 数据类型的关系表达式都将使用 Unicode 排序顺序执行。这包括涉及 Unicode 和非 Unicode 数据的混合模式表达式。例如，在下面的查询中，`varchar` 字符常量 “Mü” 将隐式转换为 `unichar`，并且将依据 Unicode 排序顺序执行比较：

```
select * from authors where unicode_name > 'Mü'
```

对于所有其它比较运算符以及并置运算符 “+”、运算符 “in” 和运算符 “between” 也都一样。同样，其目的是为了保持与现有数据库应用程序的兼容性。

基于等同性的表连接（等同连接）需要特别说明。服务器通常会优化这些连接以利用在参与列上定义的索引。连接 `unichar` 列和 `char` 列时，后者需要进行转换，并且由于字符排序顺序和 Unicode 排序顺序不同，因此优化程序将忽略 `char` 列上的索引。

在 Adaptive Server 12.5.1 版及更高版本中，如果服务器的缺省字符集配置为 UTF-8，则可将服务器的缺省排序顺序（对于 char 数据）配置为以上的任意排序顺序。在此前的版本中，二进制排序顺序 “bin_utf8” (ID=50) 是唯一适用于 UTF-8 的良好排序顺序。虽然没有要求这样做，但可以为 UTF-8 中的 char 数据选择一种排序顺序，使其与 unichar 数据的排序顺序相对应。

在为 Unicode 选择哪种二进制排序顺序的问题上，存在潜在的混淆。名为 “binary” 的排序顺序对 unichar 数据 (UTF-16) 的效率最高，因此它是缺省排序顺序。该顺序基于 Unicode 标量值，意味着所有 32 位代理对都放在所有 16 位 Unicode 值之后。名为 “utf8bin” 的排序顺序用于匹配 UTF-8 char 数据的缺省（效率最高）二进制顺序，也就是 “bin_utf8”。因此，建议使用的匹配组合为：unichar 使用 “binary”，UTF-8 char 也使用 “binary”；或 unichar 使用 “utf8bin”，UTF-8 char 使用 “bin_utf8”。前一种组合偏向于优化 unichar 的效率，而后一种组合偏向于优化 char 的效率。避免对 UTF-8 char 使用 “utf8bin”，因为它与 “bin_utf8” 等同，但效率较低。

为系统消息选择语言

任何 Adaptive Server 安装都可以使用包含不同语言消息文件的语言模块。Adaptive Server 提供以下语言的消息语言模块：英语、简体中文、法语、德语、日语、朝鲜语、巴西葡萄牙语和西班牙语。如果客户端语言不是这些语言之一，则系统消息将以缺省语言英语显示。

每个客户端可以同时选择用自己的语言从同一服务器查看消息，例如，一个客户端用法语查看系统消息，一个用西班牙语，另一个用德语。但是，这要求所有选择的语言必须在同一语言组中。例如，法语、西班牙语和德语都在语言组 1 中。另一方面，日语在语言组 101 中，该组不包含其它语言。因此，如果服务器语言是日语，则只能以日语或英语显示系统消息。应记住所有语言组都可以用英语显示消息。还有一个服务器范围的缺省语言，在用户未选择特定语言时使用这种缺省语言。如果使用 Unicode，就可用任何一种支持的语言查看系统消息。

可以用以下两种方法中的一种来为系统消息选择语言：

- 选择作为用户配置文件一部分的语言
- 在 *locales.dat* 文件中输入一种语言

表 9-8 显示所支持的系统消息语言及其语言组。每个用户在每个会话中只可为系统消息选择一种语言。

表 9-8：支持的系统消息

语言组	系统消息语言	字符集
组 1	法语、德语、西班牙语、巴西葡萄牙语	ASCII 8、CP 437、CP 850、CP 860、CP 863、CP 1252、ISO 8859-1、ISO 8859-15、Macintosh Roman、ROMAN8
组 2	波兰语	Cp 1250、CP 852、ISO 8859-2
组 101	日语	CP 932、DEC Kanji、EUC-JIS、Shift-JIS
组 102	简体中文 (PRC)	CP 936、EUC-GB、GB18030
组 104	朝鲜语	EUC-KSC、CP 949
组 105	泰语	CP 874、TIS 620
Unicode	法语、德语、西班牙语、巴西葡萄牙语、日语、简体中文、朝鲜语	UTF-8
所有其它语言组	英语	

为客户端用来接收消息的所有语言安装语言模块。这些语言模块（位于 Adaptive Server 安装目录的 *locales* 子目录中）是称为本地化文件的一组文件中的一部分。有关本地化文件和软件消息目录结构的信息，请参见第 306 页的“本地化文件的类型”。

设置服务器：示例

这一节讨论设置选项及其执行的必要步骤。这只是个示例，它对您自己的设置过程提供一些建议和方法。

西班牙语版服务器

本示例显示了在所有客户端使用同一语言时，如何设置新的服务器。若要执行此操作：

- 1 选择服务器语言，在此例中是西班牙语。通过查看第 276 页的表 9-1，可以获知西班牙语在语言组 1 中。根据使用的平台，从第 1 组中选择一种字符集。Sybase 建议选择大多数客户端所使用的字符集。或者，如果认为您的公司有一天会发展到其它国家 / 地区，并会用到其它语言，就应该考虑安装 Unicode（请参见第 275 页的“为服务器选择字符集”）。

- 2 在服务器中安装西班牙语语言模块。这允许客户端使用西班牙语查看系统消息。
- 3 选择缺省排序顺序。通过参考第 285 页的表 9-5，可以获知除了二进制排序顺序外，西班牙语还有 3 种可能的排序顺序。选择一种排序顺序。
- 4 重新启动服务器。

总部在美国的日本公司

该示例涉及在日本的客户端将使用日语输入数据、排序数据并用日语查看系统消息，而将数据提交给只使用英语的用户访问的服务器：

- 1 为服务器选择缺省字符集。如果安装了语言组 101（日语）中的字符集，则可在同一服务器中支持日语和英语。
- 2 安装日语语言模块，使系统消息可使用日语。
- 3 选择排序顺序。通过参考第 285 页的表 9-5，可以获知二进制排序顺序是日语的唯一一种可用排序顺序。因此，英语和日语客户端都使用缺省的二进制排序顺序。考虑使用 `sortkey` 函数为两方用户提供解决方案。
- 4 确保缺省情况下，每个日语用户请求日语消息。由于正在使用语言组 101 中的字符集，并已安装了日语语言模块，所以在日本的客户端将用日语查看消息，而在美国的客户端可选择用英语或日语查看消息。

具有多国客户端的日本公司

这个公司在日本，并且在法国、德国和西班牙有客户端。您需要在同一服务器中混用欧洲和亚洲语言。

- 1 选择缺省服务器语言和字符集。由于公司在日本，并且大多数客户端在日本，所以缺省服务器语言应该是日语。但还想让在法国、德国和西班牙的客户端能够用他们的本地语言收发数据。通过查看第 276 页的表 9-1，可以获知日语在语言组 101 中，而法语、德语和西班牙语在语言组 1 中。由于所需的语言不在同一语言组中，因此只有选择 `Unicode` 作为缺省字符集才能在同一服务器上使用所有这些语言。
- 2 为日语、法语、德语和西班牙语安装语言模块。

- 3 选择二进制排序顺序，因为它是 Unicode 字符集可用的唯一排序顺序。（但是，可以考虑在应用程序代码内使用 `sortkey` 函数来提供依据每个用户的优先选项进行排序的数据。）
- 4 选择日语作为系统消息的缺省语言。其它国家 / 地区的客户可为消息选择他们自己的本地语言。

更改字符集、排序顺序或消息语言

即使在您配置了服务器之后，系统管理员也可更改 Adaptive Server 使用的缺省字符集、排序顺序或消息语言。因为排序顺序建立在特定字符集的基础上，所以改变字符集总是伴随着排序顺序的改变。不过，您可以更改排序顺序而不更改字符集，因为一种字符集可以使用多种排序顺序。

若要显示 Adaptive Server 的缺省排序顺序、字符集及其主要排序顺序表，请输入：

```
sp_helpsort
```

更改缺省字符集

Adaptive Server 只能有一个缺省字符集，数据使用此字符集存储在数据库中。安装 Adaptive Server 时，请指定缺省字符集。

警告！ 请仔细阅读以下内容，并且在更改 Adaptive Server 中的缺省字符集时要小心。Sybase 强烈建议在更改缺省字符集之前执行备份。

更改 Adaptive Server 中的缺省字符集时，需要将所有已有数据转换到新的缺省字符集。只有在以下情况下，才不需要转换：

- 服务器中没有用户数据。
- 对服务器中用户数据的损坏是可接受的。
- 您确信服务器中的数据仅使用 ASCII-7。在这种情况下，您可以更改缺省值而无需首先将数据复制出服务器。

在其它情况下，必须转换已有数据，如下所示：

- 1 使用 **bcp** 将数据复制出来。
- 2 更改缺省字符集
- 3 使用带有适当数据转换标志的 **bcp** 将数据复制回服务器。

有关使用 **bcp** 复制数据的详细信息，请参见《实用工具指南》。

警告！ 在将数据转换到不同的字符集（特别是 UTF-8）后，对于分配的列大小，数据可能会太大。使用大一点的列大小重新创建受影响的列。

必须支持现有数据的字符集与新的缺省字符集之间的代码转换。如果不支持，将会出现转换错误，并且不会正确地转换数据。有关支持的字符集转换的详细信息，请参见第 10 章“配置客户端/服务器字符集转换”。

即使支持字符集之间的转换，由于在字符集之间存在一些细小的差别，或者因为某些字符在其它字符集中没有等价的字符，仍可能会出现一些错误。包含有问题数据的行不能复制回数据库，否则数据可能包含不完整的字符或无效的字符。

用资源文件更改排序顺序

可使用资源文件更改 Adaptive Server 字符集。样本资源文件 *sqlloc.rs* 位于 *\$\$SYBASE/ASE-12_5/init/sample_resource_files/* 中。

来自 Adaptive Server 12.5.1 安装的资源文件与以下内容相似：

```
sybinit.release_directory: USE_DEFAULT
sqlsrv.server_name: PUT_YOUR_SERVER_NAME_HERE
sqlsrv.sa_login: sa
sqlsrv.sa_password:
sqlsrv.default_language: USE_DEFAULT
sqlsrv.language_install_list: USE_DEFAULT
sqlsrv.language_remove_list: USE_DEFAULT
sqlsrv.default_character_set: USE_DEFAULT
sqlsrv.character_set_install_list: USE_DEFAULT
sqlsrv.character_set_remove_list: USE_DEFAULT
sqlsrv.sort_order: USE_DEFAULT
# An example sqlloc resource file...
# sybinit.release_directory: USE_DEFAULT
# sqlsrv.server_name: PUT_YOUR_SERVER_NAME_HERE
# sqlsrv.sa_login: sa
```

```
# sqlsrv.sa_password:
# sqlsrv.default_language: french
# sqlsrv.language_install_list: spanish,german
# sqlsrv.language_remove_list: USE_DEFAULT
# sqlsrv.default_characterset: cp437
# sqlsrv.characterset_install_list: mac,cp850
# sqlsrv.characterset_remove_list: USE_DEFAULT
# sqlsrv.sort_order: dictionary
```

更改缺省排序顺序

Adaptive Server 只能有一种缺省排序顺序，即 Adaptive Server 用于对数据进行排序的归类序列。考虑在特定的 Adaptive Server 上更改字符数据的排序顺序时，请记住：组织中的所有 Adaptive Server 应具有相同的排序顺序。单一的排序顺序可以增进一致性并使分布式处理更易于管理。

在更改缺省排序顺序后，可能要重建索引。有关详细信息，请参见第 295 页的“重新配置字符集、排序顺序或消息语言”。

重新配置字符集、排序顺序或消息语言

本节总结在更改 Adaptive Server 的缺省字符集、排序顺序或消息语言前后需要执行的步骤。有关如何为新服务器配置字符集、排序顺序或消息语言的过程，请参见所用平台的配置文档。

在更改字符集或排序顺序的前后，请备份 Adaptive Server 中的所有数据库。备份数据库之后，如果满足以下条件，请使用 `bcp` 将数据复制入或复制出数据库：

- 数据库包含字符数据，并且您希望将数据转换到新的字符集。不要将数据的数据库转储装载到使用新缺省字符集的服务器中。Adaptive Server 假定装载的数据采用新的字符集，并且会损坏数据。
- 您只更改缺省排序顺序，而不更改缺省字符集。您无法从在更改排序顺序之前执行的转储中装载数据库，如果尝试这样做，则会出现错误消息，并且 Adaptive Server 将中止装载。
- 您更改缺省字符集，并且旧排序顺序或新排序顺序不是二进制的。无法装载更改字符集之前进行的数据库转储。

一旦重新配置了缺省字符集和排序顺序之后，您将无法从数据库转储中重新装载数据（除非旧字符集和新字符集均使用二进制排序顺序，并且无需在旧字符集和新字符集之间进行转换）。有关详细信息，请参见第 293 页的“更改缺省字符集”。

Unicode 示例

在以下示例中，将对名为 **xpubs** 的虚拟数据库进行修改以使用 **univarchar** 列。

模式

假定在一台具有所有缺省安装设置（即字符集 “iso_1”，缺省排序顺序 ID 50 “binary_iso_1”）的服务器上使用以下脚本创建了一个数据库。

```
> create database xpubs
> go
> use xpubs
> go
> create table authors (au_id int, au_lname
varchar(255), au_fname varchar(255))
> go
> create index au_idx on authors(au_lname, au_fname)
> go
```

然后使用一系列插入和更新操作将数据装载到该服务器中。

转换到 UTF-8

转为使用 Unicode 的第一步是提取数据，并将其转换为 UTF-8 格式。

```
% bcp xpubs..authors out authors.utf8.bcp -c -Jutf8 -Usa -P
```

下一步是安装 UTF-8 作为服务器中的缺省字符集：

```
% charset -Usa -P binary.srt utf8
% isql -Usa -P
> sp_configure 'default sortorder id', 50, 'utf8'
> go
> shutdown
> go
```

重新启动服务器以修改缺省字符集并在系统表上重新创建索引。再次重新启动服务器，然后重新装载数据：

```
% isql -Usa -P
> sp_dboption xpubs, 'select into', true
> go
> use xpubs
> go
> checkpoint
> go
> delete from authors
```

```
> go
> quit

% bcp xpubs..authors in authors.utf8.bcp -c -Jutf8 -Usa -P
```

将所选列迁移到 unichar

对于一个使用 UTF-8 作为缺省字符集运行的工作数据库，将所选列转换为 `univarchar` 非常简单：

```
% isql -Usa -P
> use xpubs
> go
> alter table authors modify au_lname univarchar(255),
au_fname univarchar(255)
> go
```

这些列将被修改为新的数据类型，数据将进行相应的转换，并且将重新创建索引。

迁移到 unitext 或从 unitext 迁移

目前，`alter table modify` 命令不支持 `text`、`image` 或 `unitext` 列。若要从 `text` 迁移到 `unitext` 列，必须首先使用 `bcp` 创建带有 `unitext` 列的表，然后再次使用 `bcp` 将数据放入新表中。只有用 `-Jutf8` 选项调用 `bcp` 时，此迁移路径才有效。

预备步骤

在运行安装程序对 Adaptive Server 进行重新配置之前：

- 1 转储所有用户数据库和 `master` 数据库。如果更改了 `model` 或 `sybssystemprocs`，也要对其进行转储。
- 2 如果尚未装载语言模块，则进行装载（有关完整的说明，请参见所用平台的配置文档）。
- 3 如果要更改 Adaptive Server 缺省字符集，并且当前数据库包含非 ASCII-7 数据，请使用 `bcp` 将现有数据从数据库中复制出来。

装载了语言模块之后，即可运行 Adaptive Server 安装程序来完成以下操作：

- 安装或删除 Adaptive Server 包含的消息语言和字符集
- 更改缺省消息语言或字符集
- 选择另一种排序顺序

有关使用安装程序的说明，请参见所用平台的配置文档。

注释 更改字符集或排序顺序前，Adaptive Server 打开的数据库必须与由服务器管理的数据库的数量相同。如果更改 Adaptive Server 排序顺序后重新启动时没有打开足够数量的数据库，则 Adaptive Server 就会将此消息输出到错误日志，并且服务器将还原为其先前的排序顺序：

```
The configuration parameter 'number of open databases'
must be at least as large as the number of databases,
in order to change the character set or sort order."Re-
start Adaptive Server, use sp_configure to increase
'number of open databases' to at least %d, then re-
configure the character set or sort order
```

若要重新配置语言、字符集或排序顺序，请使用《实用程序指南》中介绍的 `sqlloc` 实用程序。如果在使用 Windows，请使用《配置指南》的第 3 章“Adaptive Server 缺省配置”中介绍的 `Server Config` 实用程序。

如果安装了其它语言，但没有更改 Adaptive Server 字符集或排序顺序，则已完成了重新配置过程。

如果更改了 Adaptive Server 的缺省字符集，而当前数据库中包含非 ASCII-7 数据，则应使用带有启用转换所需标志的 `bcp` 将数据复制回数据库中。

如果更改了 Adaptive Server 缺省排序顺序或字符集，请参见第 295 页的“重新配置字符集、排序顺序或消息语言”。

设置用户的缺省语言

如果安装了其它语言，运行客户端程序的用户可以运行 `sp_modifylogin` 将该语言设置为缺省语言，或使用 `locales.dat` 中的相应条目在客户端计算机上设置 `LANG` 变量。

重新配置后的恢复

每次停止和重新启动 Adaptive Server 时，都将自动对每个数据库执行恢复。《系统管理指南：卷 2》的第 11 章“制订备份和恢复计划”中详细论述了自动恢复。

完成恢复后，将装载新的排序顺序和字符集定义。

如果更改了排序顺序，Adaptive Server 将切换到单用户模式，以便允许对系统表进行必要的更新并防止其他用户使用该服务器。将自动检查每个包含基于字符的索引的表，以查看索引是否由于排序顺序的更改而损坏。如有必要，使用新的排序顺序定义自动重建表中基于字符的索引。

重建系统索引之后，将在 `sysindexes` 系统表中将基于字符的用户索引标记为“可疑”。在 `sysobjects` 中会将包含可疑索引的用户表标记为“只读”，以防止对这些表进行更新或使用“可疑”索引，直到经过检查或重建（如果需要）。

将在域分区用户表中检查是否有基于字符的分区键，并且，如果排序顺序更改或字符集更改可能导致分区损坏，则将这些表标记为“可疑”。

接着，新的排序顺序信息将替换磁盘上存放配置信息的区域中的旧信息。然后，Adaptive Server 将关闭，以便使用一组完整、准确的系统信息启动下一个会话。

使用 `sp_indsuspect` 查找损坏的索引

在 Adaptive Server 关闭之后重新启动它，并使用 `sp_indsuspect` 查找需要重建索引的用户表。

```
sp_indsuspect [tab_name]
```

其中 `tab_name` 是您正调查的表的名称。如果缺少 `tab_name`，`sp_indsuspect` 会创建一个列表，其中包含当前数据库中在排序顺序更改时将索引标记为“可疑”的所有表。

以下示例显示，在 `mydb` 数据库中运行 `sp_indsuspect` 将产生一个可疑索引：

```
sp_indsuspect

Suspect indexes in database mydb
Own.Tab.Ind (Obj_ID, Ind_ID) =
dbo.holdings.h_name_ix(160048003, 2)
```

更改排序顺序后重建索引

`dbcc reindex` 通过运行“快速”版本的 `dbcc checktable` 来检查用户表上索引的完整性。有关详细信息，请参见《系统管理指南：卷 2》中的第 10 章“检查数据库一致性”。`dbcc reindex` 将删除并重建那些所用排序顺序与新排序顺序不一致的索引。当 `dbcc reindex` 发现第一个与索引相关的错误时，它将显示一条消息，然后重建不一致的索引。更改了 Adaptive Server 中的排序顺序之后，系统管理员或表所有者应运行 `dbcc reindex`。

```
dbcc reindex ({table_name | table_id})
```

对 `sp_indsuspect` 列出的所有包含可疑索引的表运行此命令。例如：

```
dbcc reindex (titles)
```

```
One or more indexes are corrupt.They will be rebuilt.
```

在前面的示例中，`dbcc reindex` 在表 `titles` 中发现一个或多个可疑索引；它将删除并重建相应的索引。

如果表的索引已经是正确的，或者表没有索引，则 `dbcc reindex` 不会重建任何索引。而是显示一条消息。如果怀疑表中包含损坏的数据，则命令中止。如果发生这种情况，就会显示错误消息，指示用户运行 `dbcc checktable`。

当 `dbcc reindex` 成功完成后，将删除表索引上的所有“可疑”标记。表上的“只读”标记也将被删除，而且可以对表进行更新。无论是否必须重建任何索引，这些标记都将删除。

`dbcc reindex` 不会为系统表重建索引。如果有必要，在排序顺序更改后重新启动 Adaptive Server，然后作为恢复操作的一个自动执行的部分检查并重建系统索引。

更改字符集之后升级 `text` 数据

如果已将 Adaptive Server 字符集更改为多字节字符集，请使用 `dbcc fix_text` 升级 `text` 值。

`text` 值可以大到占据多页；因此，Adaptive Server 必须能够处理跨越页边界的字符。为此，Adaptive Server 需要有关每个 `text` 页的额外信息。系统管理员或表所有者必须在每个包含 `text` 数据的表上运行 `dbcc fix_text`，以计算所需的新值。

若要查看所有包含 `text` 数据的表的名称，请使用：

```
select sysobjects.name
from sysobjects, syscolumns
where syscolumns.type = 35
and sysobjects.id = syscolumns.id
```


系统管理员或表所有者必须运行 `dbcc fix_text` 来计算所需的新值。

`dbcc fix_text` 命令的语法是：

```
dbcc fix_text (table_name | table_id)
```

命名的表必须在当前数据库中。

`dbcc fix_text` 打开指定的表，计算每个 `text` 值所需的字符统计信息，并将这些统计信息添加到相应的页标头字段中。此过程可能需要很长的时间，具体情况取决于表中 `text` 值的数量和大小。`dbcc fix_text` 可能会生成大量的日志记录，这些记录可能会填满事务日志。`dbcc fix_text` 以一系列小事务进行更新，这样，如果日志已满，则只会丢失少量的工作。

如果日志空间已用完，请清理日志（请参见《系统管理指南：卷2》中的第12章“备份和恢复用户数据库”）。然后，重新启动 `dbcc fix_text`，使用原来的 `dbcc fix_text` 停止时所升级的同一个表。每个多字节文本值均包含表示其是否已升级的信息，所以 `dbcc fix_text` 只升级在以前的处理过程中未处理的 `text` 值。

如果数据库将其日志存储在单独的段上，可以使用阈值来管理日志的清除。请参见《系统管理指南：卷2》中的第16章“使用阈值管理可用空间”。

如果 `dbcc fix_text` 无法在文本页上获得所需的锁，它将报告问题并继续工作，如下所示：

```
Unable to acquire an exclusive lock on text page 408.
This text value has not been recalculated. In order to
recalculate those TEXT pages you must release the lock
and reissue the dbcc fix_text command.
```

在更改字符集后检索 `text` 值

如果尝试在更改为多字节字符集后检索 `text` 值，且尚未运行 `dbcc fix_text`，则命令将失败并出现以下错误消息：

```
Adaptive Server is now running a multi-byte character
set, and this TEXT column's character counts have not
been recalculated using this character set. Use dbcc
fix_text before running this query again.
```

如果更改了排序顺序或字符集，并出现了错误，请参见 *Adaptive Server Enterprise Troubleshooting and Error Messages Guide*（《Adaptive Server Enterprise 故障排除和错误消息指南》）中的“*How to Manually Change Sort Order or Default Character Set*”（如何手动更改排序顺序或缺省字符集）。

处理可疑分区

将出现以下两个原因将分区标记为可疑：

- 域分区表上的排序顺序或字符集更改
- 包含散列分区表的跨平台转储和装载

如果表标记为具有可疑分区：

- 此表上的所有更新和游标活动将挂起。
- 不允许使用 `alter table` 命令（`partition by` 除外）。不允许对具有可疑分区的表使用 `create index` 和 `drop index`。
- 允许对包含可疑分区的表使用 `select` 命令。但是，优化程序将此类表视为循环分区表，以避免使用可能损坏的分区条件。

修复具有可疑分区的表

- 如果分区条件需要在排序顺序更改后修复，则可以使用带 `partition by` 选项的 `alter table` 对具有可疑分区的表重新分区。
- 如果分区条件不需要修复，则可以使用 `reorg rebuild table` 命令重建该表，同时仅在分区之间重新分配数据行。
- 如果表上的索引以及分区均标记为可疑，请使用 `partition by` 或 `reorg rebuild` 同时修复可疑索引和可疑分区。

在跨平台转储和装载操作中处理可疑分区

- 在跨两个规模类型不同的平台执行 `load database` 后，首次执行 `online database` 命令的过程中，散列分区被标记为可疑分区。
- 循环分区（已使用 `unichar` 或 `varchar` 分区键在内部生成分区条件）上的任何全局聚簇索引都会被标记为可疑索引。
- 数据库联机后，使用 `sp_post_xpload` 修复可疑分区和索引。

安装不支持语言的日期字符串

对于没有语言模块的语言，请使用 `sp_addlanguage` 来安装一周中每一天的名称和一年中每个月份的名称。使用 `sp_addlanguage` 可以定义：

- 语言名称和（可选）名称的别名
- 月份全名的列表及月份名称缩写的列表
- 一周中每天的全名的列表
- 输入日期时使用的日期格式（例如月 / 日 / 年）
- 一周中第一天的编号

例如，若要添加意大利语的信息：

```
sp_addlanguage italian, italiano,
"gennaio, febbraio, marzo, aprile, maggio, giugno, luglio, agosto, settembre, ottobre,
novembre, dicembre",
"genn, feb, mar, apr, mag, giu, lug, ago, sett, ott, nov, dic",
"lunedì, martedì, mercoledì, giovedì, venerdì, sabato, domenica",
dmy, 1
```

`sp_addlanguage` 强制执行严格的数据输入规则。月份名称、月份缩写和一周中每天的名称的列表必须用逗号分隔，不能包含空格或换行符（回车符）。此外，还必须包含正确的元素数目（月份字符串为 12 个，一周中每天的字符串为 7 个）。

日期格式的有效值为：`mdy`、`dmy`、`ymd`、`ydm`、`myd` 和 `dym`。`dmy` 值表明日期的顺序是日 / 月 / 年，这种格式只影响数据输入；要更改输出格式，必须使用 `convert` 函数。

服务器与客户端之间的日期解释

通常在客户端上解析日期值。当用户选择日期值时，Adaptive Server 将采用内部格式将它们发送到客户端。客户端使用客户端上 `locales` 目录的缺省语言子目录中的 `common.loc` 文件和其它本地化文件将内部格式转换为字符数据。例如，如果用户的缺省语言为西班牙语，则 Adaptive Server 在 `/locales/spanish/char_set` 中查找 `common.loc` 文件。它使用该文件中的信息进行显示，例如，12 febrero 2007。

假定用户的缺省语言设置为意大利语，而 Adaptive Server 没有提供该语言的语言模块，并且已添加了意大利语的日期值。当客户端连接到服务器并查找用于意大利语的 *common.loc* 文件时，将找不到该文件。客户端输出一条错误消息并连接到服务器。如果用户随后选择了日期值，则日期以美国英语的格式显示。要使用 `sp_addlanguage` 显示添加的日期值，可使用 `convert` 函数强制将日期转换为服务器上的字符数据。

以下查询生成的结果集包含使用美国英语格式的日期：

```
select pubdate from titles
```

但是，下面的查询返回的日期包含意大利语的月份名称：

```
select convert(char(19),pubdate) from titles
```

国际化和本地化文件

国际化文件的类型

支持采用特定语言进行数据处理的文件称为国际化文件。Adaptive Server 提供了几种类型的国际化文件。

表 9-9：国际化文件

文件	位置	目的和内容
<i>charset.loc</i>	在 <i>charsets</i> 目录的每个字符集子目录中	字符集定义文件，用来定义每个字符的词法属性，如字母数字、标点符号、操作数和大写或小写。供 Adaptive Server 用于正确处理数据。
<i>*.srt</i>	在 <i>charsets</i> 目录的每个字符集子目录中	定义字母数字和特殊字符（包括连字符、读音符和其它语言特定元素）的排序顺序。
<i>*.xlt</i>	在 <i>charsets</i> 目录的每个字符集子目录中	供实用程序（如 <code>bcp</code> 和 <code>isql</code> ）使用的终端特定字符转换文件。有关如何使用 <i>.xlt</i> 文件的详细信息，请参见第 10 章“配置客户端 / 服务器字符集转换”和《实用程序指南》。

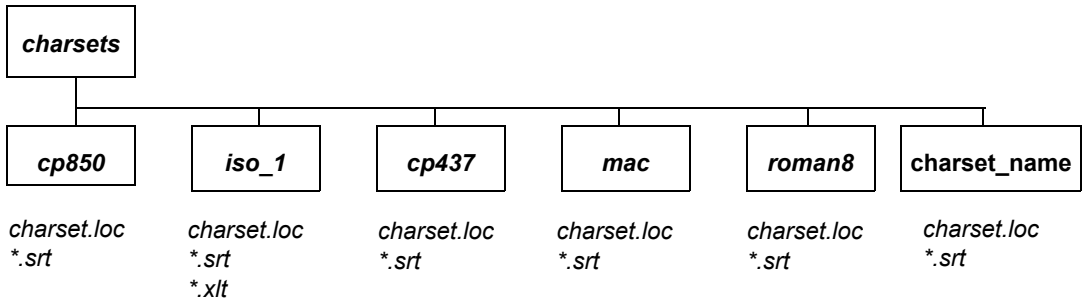
警告！ 不要更改任何国际化文件。如果需要安装新的终端定义或排序顺序，请与当地 Sybase 机构或分销商联系。

字符集目录结构

图 9-3 显示了 Adaptive Server 附带的西欧字符集的目录结构。每个字符集在 *charsets* 目录中都有一个单独的子目录。对应于每个字符集（例如，*cp850*）的子目录中包含字符集和排序顺序定义文件以及终端特定文件。

如果装载了其它字符集，它们也将出现在 *charsets* 目录中：

图 9-3: *charsets* 目录的结构



以下全局变量包含有关字符集的信息：

表 9-10: 用于字符集的全局变量

全局变量	说明
<code>@@char_convert</code>	如果字符集转换无效，则包含 0。如果字符集转换有效，则包含 1。
<code>@@client_csname</code>	客户端字符集名称。如果客户端的字符集从未初始化，则设置为 NULL；否则，将包含用于连接的字符集的名称。
<code>@@client_csid</code>	客户端字符集 ID。如果客户端的字符集从未初始化，则设置为 -1；否则，将包含 <code>syscharsets</code> 用于连接的客户端字符集 ID。
<code>@@client_csexpansion</code>	返回从服务器字符集转换为客户端字符集时使用的扩展因子。
<code>@@maxcharlen</code>	Adaptive Server 的缺省字符集中字符的最大长度（以字节为单位）。
<code>@@ncharsize</code>	当前服务器的缺省字符集中字符的最大长度（以字节为单位）。
<code>@@unicharsize</code>	等于 2。

本地化文件的类型

对于各个语言模块， Adaptive Server 均提供了几个本地化文件，如表 9-11 所示。

表 9-11：本地化文件

文件	位置	目的和内容
<i>locales.dat</i>	在 <i>locales</i> 目录中	客户端应用程序使用该文件来标识缺省的消息语言和字符集。
<i>server.loc</i>	在 <i>\$SYBASE/\$SYBASE_ASE/locales</i> 目录的每个语言子目录下的字符集子目录中	已转换为本地语言的软件消息。 Sybase 产品有产品特定的 *.loc 文件。如果某个条目没有转换，则该软件消息或字符串将以美国英语（而不是本地语言）显示。
<i>common.loc</i>	在 <i>locales</i> 目录的每个语言和字符集目录中	包含一年中各月的本地名称及其缩写，以及有关本地日期、时间和货币格式的信息。

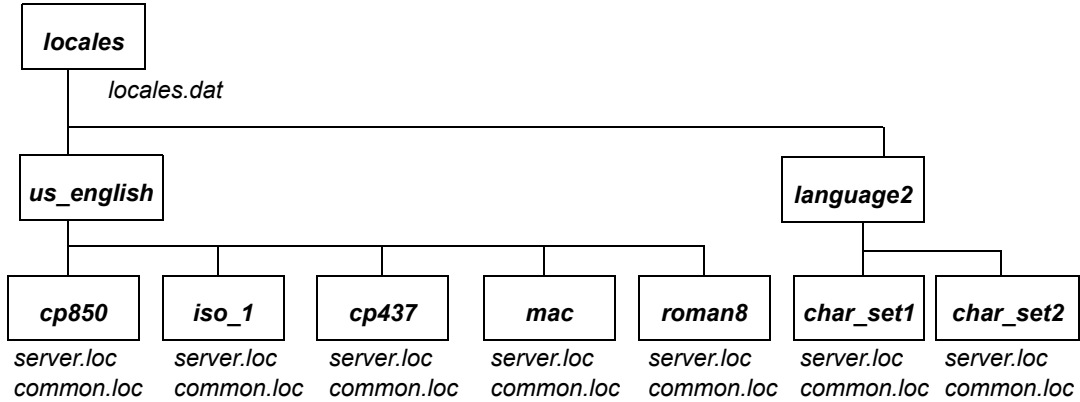
所有 Adaptive Server 相关区域设置文件（由 *dataserver*、*sqlloc*、*syconfig* 等使用）均位于 *\$SYBASE/\$SYBASE_ASE/locales* 中。所有 Open Client/Server 相关区域设置文件（*ctlib*、*ctisql*、*ctbcp*、*optdiag*、*installjava* 等）均位于 *\$SYBASE/locales* 中。

警告！ 不要改变任何本地化文件。如果需要改变这些文件中的任何信息，请与当地 Sybase 机构或分销商联系。

软件消息目录结构

图 9-4 显示本地化文件的排列方式。*locales* 目录中有所安装的每种语言的子目录，其中总有一个 *us_english* 子目录。（在 PC 平台上，此目录名为 *english*。）在安装过程中，当提示选择要在 Adaptive Server 上安装的语言时，安装程序将列出支持的软件消息语言。如果安装其它语言的语言模块，您将看到那些语言的子目录。每个语言子目录内都有所支持的字符集的子目录；例如，*cp850* 是 *us_english* 支持的字符集。每种 Sybase 产品的软件消息文件均在字符集的子目录中。

图 9-4：消息目录结构



消息语言和全局变量

以下的全局变量包含有关语言的信息：

<code>@@langid</code>	包含当前使用的语言的本地语言 ID（在 <code>syslanguages.langid</code> 中指定）
<code>@@language</code>	包含当前使用的语言的名称（在 <code>syslanguages.name</code> 中指定）

主题	页码
字符集转换	309
支持的字符集转换	310
选择转换类型	312
启用和禁用字符集转换	314
字符集转换中的错误处理	316
转换和数据长度的变化	316
为实用程序指定字符集	318
显示和文件字符集的命令行选项	318

字符集转换

在异构环境中， Adaptive Server 可能需要与运行在使用不同字符集的不同平台上的客户端通信。尽管不同的字符集可以支持同一语言组（例如， ISO 8858-1 和 CP 850 都支持第 1 组语言），但它们对相同的字符可能有不同的编码。例如，在 ISO 8859-1 中，字符 à 的十六进制编码为 0xE0。但在 CP 850 中，同样字符的十六进制编码却为 0x85。

为保持客户端与服务器之间的数据完整性，数据必须在字符集之间进行转换。其目的是为了确保在跨计算机和字符集使用时，“a”仍保持为 “a”。此过程就称为**字符集转换**。

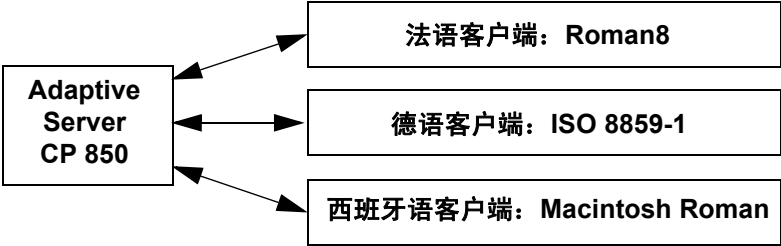
支持的字符集转换

字符集转换发生在字符集对之间。任何特定的客户端 / 服务器系统所支持的转换都取决于服务器和它的客户端所使用的字符集。如果服务器使用本地字符集作为缺省值，则会进行某种类型的字符集转换。如果服务器缺省使用 Unicode UTF-8，就会使用另一种类型的字符集转换。

本地字符集转换

Adaptive Server 支持属于同一语言组的本地字符集之间的转换。如果服务器将一种本地字符集作为其缺省字符集，则客户端字符集必须属于同一语言组。[图 10-1](#) 是西欧客户端 / 服务器系统的一个示例。在此示例中，客户端字符集和 Adaptive Server 缺省字符集都属于语言组 1。数据可在客户端字符集和服务器缺省字符集之间正确转换。由于它们都属于同一语言组，客户端可以在服务器上浏览所有客户端提交的数据。

图 10-1：服务器和客户端字符集属于同一语言组时的字符集转换

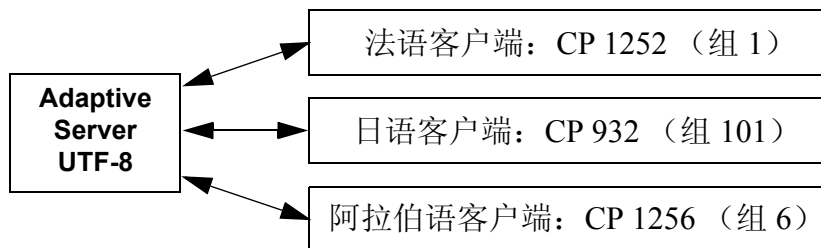


有关语言组和所支持的字符集的列表，请参见[第 276 页的表 9-1](#)。

Unicode 系统中的转换

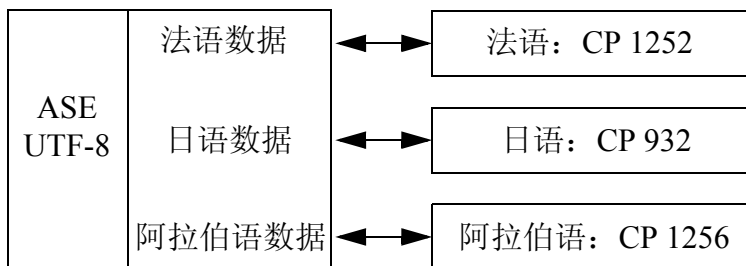
Adaptive Server 还支持 UTF-8 与 Sybase 支持的任何本地字符集之间的字符集转换。在 Unicode 系统中，由于服务器缺省字符集为 UTF-8，所以客户端字符集可以是任何语言组中的一种本地字符集。因此，日语客户端（第 101 组）、法语客户端（第 1 组）和阿拉伯语客户端（第 6 组）都可以向同一服务器发送数据，并从同一服务器接收数据。来自每个客户端的数据在每个客户端和服务器之间传递时都可得到正确转换。

图 10-2: Unicode 系统中的字符集转换



每个客户端只能查看其字符集所支持语言的数据。因此，日语客户端可以查看服务器上的所有日语数据，但不能查看阿拉伯语或法语数据。同样，法语客户端可以查看其字符集所支持的法语或任何其它西欧语言，但不能查看日语和阿拉伯语。

图 10-3: 查看 Unicode 数据



附加的字符集 ASCII-7 是 *every* 字符集（包括 Unicode）的子集，因此它与 **all** 语言组中的 **all** 字符集兼容。如果 Adaptive Server 或客户端的字符集设置为 ASCII-7，则任何 7 位的 ASCII 字符均可在客户端与服务器之间未经改变地传递而无需转换。

Sybase 建议您不要针对 ASCII-7 配置服务器。您可以通过限制每个客户端只使用每个本地字符集的前 128 个字符，从而获得同样的兼容性优点。

Adaptive Server 直接转换

Adaptive Server 直接转换是同一语言组的两种本地字符集之间的转换。例如，Adaptive Server 支持 CP 437 和 CP 850 之间的转换，因为它们都属于语言组 1。属于同一语言组的许多（但不是全部）本地字符集之间均可进行 Adaptive Server 直接转换（请参见第 313 页的表 10-1）。

Unicode 转换

Unicode 转换可应用于所有本地字符集。在两种本地字符集之间进行转换时，Unicode 转换方式将 Unicode 作为中间字符集。例如，在服务器缺省字符集（CP 437）和客户端字符集（CP 860）之间进行转换时，首先将 CP 437 转换成 Unicode，然后再将 Unicode 转换成 CP 860。

Unicode 转换既可以用于服务器缺省字符集 UTF-8，又可以用于本地字符集。必须专门将服务器配置为使用 Unicode 转换（除非服务器的缺省字符集为 UTF-8）。

Adaptive Server 的早期版本使用直接转换，它也是字符集转换的缺省方法。然而，Unicode 转换使字符集转换变得更加简单和方便。尽管仍然支持 Adaptive Server 直接转换，但 Sybase 现在也使用 Unicode 转换为所有字符集提供完整的转换支持，并且没有添加新的直接转换的计划。

选择转换类型

若要确定您的客户端 / 服务器系统的可用转换选项，请参见第 313 页的表 10-1。

非 Unicode 客户端 / 服务器系统

非 Unicode 系统中，服务器和客户端的字符集为本地字符集；因而，您可以使用 Adaptive Server 直接转换。

然而，一些字符集没有 Adaptive Server 直接转换；在这种情况下，必须使用 Unicode 转换。

- 如果您的客户端 / 服务器系统中的所有字符集都在表 10-1 的第 1 列中，请使用 Adaptive Server 直接转换。所有的字符集必须属于同一语言组。

- 如果您的客户端 / 服务器系统中的字符集位于表 10-1 的第 2 列中，或有些在第 1 列，有些在第 2 列，请将服务器配置为使用 Unicode 转换。同样，所有的字符集必须属于同一语言组。

例如，假定服务器缺省字符集为 CP 850 且客户端字符集为 ISO 8859-1 或 ROMAN 8。表 10-1 显示在 CP 850 与客户端字符集之间可以进行直接转换。现在，假设您使用 CP 1252 添加客户端。由于 CP 1252 和 CP 850（缺省服务器字符集）之间没有直接转换，因此您必须使用 Unicode 转换在 CP 1252 和 CP 850 之间进行转换。如果您的字符集为混合型，有一些您可以使用 Adaptive Server 直接转换，其它的必须使用 Unicode 转换，您可以指定使用 Adaptive Server 直接转换和 Unicode 转换的组合。

Unicode 客户端 / 服务器系统

如果您的服务器缺省值为 Unicode UTF-8，那么所有转换都将在 UTF-8 与客户端系统上所使用的本地字符集之间进行。在 Unicode 系统中，将以独占方式使用 Unicode 转换。

表 10-1: 字符集转换方法

语言组	第 1 列 — Adaptive Server 直接转换和 Unicode 转换	第 2 列 — 仅 Unicode 转换
组 1	CP 437、CP 850、ISO 8859-1、Macintosh Roman	CP 860、CP 1252、ISO 8859-15、CP 863
组 2	CP 852、CP 1250、CP 8859-1、Macintosh Central European	ISO 8859-2
组 4	无需转换（仅支持一个字符集）	
组 5	CP 855、CP 866、CP 1251、ISO 8859-5、Koi8、Macintosh Cyrillic	
组 6		CP 864、CP 1256、ISO 8859-6
组 7	CP 869、CP 1253、GREEK8、ISO 8859-7、Macintosh Greek	
组 8		CP 1255、ISO 8859-8
组 9	CP 857、CP 1254、ISO 8859-9、Macintosh Turkish、TURKISH8	
组 101	DEC Kanjii、EUC-JIS、Shift-JIS	CP 932
组 102		CP 936、EUC-GB、GB18303
组 103		Big 5、CP 950、EUC-CNS
组 104		EUCKSC、CP 949
组 105		CP 874、TIS 620
组 106	无需转换（仅支持一个字符集）	
Unicode	无需转换（仅支持一个字符集）	

配置服务器

缺省情况下，Adaptive Server 使用直接转换在不同的字符集之间转换数据。若要使用 Unicode 转换，请使用 `sp_configure` 将 `enable unicode conversions` 选项设置为 1 或 2。

- 如果将 `sp_configure` “`enable unicode conversions`” 设置为 1：
此设置使用 Adaptive Server 直接转换或 Unicode 转换。Adaptive Server 首先检查服务器和客户端字符集是否能够进行 Adaptive Server 直接转换。如果可以，将使用直接转换；如果不可以，将使用 Unicode 转换。

如果您的客户端 / 服务器系统中的字符集在表 10-1 的第 1 列和第 2 列中都有，请使用此设置。

- 如果将 `sp_configure` “`enable unicode conversions`” 设置为 2：
此设置只使用 Unicode 转换。Adaptive Server 使用 Unicode 转换，而不试图去查找 Adaptive Server 直接转换。

如果客户端 / 服务器转换导致数据长度发生变化（请参见第 316 页的“转换和数据长度的变化”），请使用此设置

如果所有字符集都在表 10-1 的第 2 列中，将 `enable unicode conversions` 设置为 2 可以始终使用 Unicode 转换。

对于 Adaptive Server 15.0 版及更高版本，`enable unicode conversions` 的缺省值为 1。

如果服务器缺省字符集为 UTF-8，服务器会自动仅使用 Unicode 转换。

启用和禁用字符集转换

请求连接的客户端会向 Adaptive Server 标识其字符集。Adaptive Server 将客户端字符集与缺省字符集比较，如果两个名称相同则无需转换。如果名称不同，Adaptive Server 将确定其是否支持缺省字符集与客户端字符集之间的转换。如果不支持，则它将向客户端发送错误消息并继续执行登录过程。如果支持，则自动启用字符集转换。如果服务器的缺省字符集为 UTF-8，则自动使用 Unicode 转换。如果缺省字符集为本地字符集，则服务器将使用 Adaptive Server 直接转换，除非用户请求 Unicode 转换。

可以在服务器级禁止字符集转换。如果满足下列情况，您可能会禁止转换：

- 所有客户端都使用与服务器缺省字符集相同的字符集，因此无需转换。
- 不支持客户端字符集与服务器缺省值之间的转换。
- 您希望在不更改编码的情况下将数据存储在服务器中。

若要在服务器级启用字符集转换，请将 `disable character set conversion` 参数设置为 1。

可以从客户端会话内使用 `set char_convert` 命令控制连接级别的字符集转换。`set char_convert off` 会关闭特定客户端和服务器之间的转换。如果客户端和服务器使用同一字符集，从而不必进行转换，则您可能需要使用 `set char_convert off`。`set char_convert on` 可再次打开转换。

无法转换的字符

如果出现以下情况，则可能无法转换某些字符：

- 字符存在（被编码）于源字符集中，但在目标字符集中不存在。例如，OE 连字是 Macintosh 字符集的一部分（码点 0xCE）。此字符在 ISO 8859-1 字符集中不存在。如果在从 Macintosh 字符集转换为 ISO 8859-1 字符集的数据中存在 OE 连字，则会导致一个转换错误。
- 字符在源字符集和目标字符集中都存在，但在目标字符集中，该字符与源字符集中用不同的字节数表示。

例如，占 1 个字节的变音字符（例如 á、è）在 UTF-8 中为占 2 个字节的字符；占 2 个字节的泰语字符在 UTF-8 中为占 3 个字节的字符。通过将 `enable unicode conversion` 选项配置为 1 或 2 可避免此限制。

字符集转换中的错误处理

如果客户端字符集中有某个字符，而服务器字符集中没有该字符（反之亦然），则 Adaptive Server 字符集转换将报告错误。对于在输入到服务器时成功转换的数据，Adaptive Server 必须确保在客户端检索这些数据时，还能将其成功转换回客户端字符集。为了有效地做到这一点，Adaptive Server 必须避免将可疑的数据输入到数据库中。

如果 Adaptive Server 在输入的数据中遇到转换错误，它会生成下面的错误消息：

```
Msg 2402, Severity 16 (EX_USER):
Error converting client characters into server's
character set.Some character(s) could not be converted.
```

转换错误会阻止查询插入与更新语句。如果发生此情况，请检查数据中有问题的字符并替换它们。

如果 Adaptive Server 在将数据发送到客户端时遇到转换错误，它会用 ASCII 码的问号 (?) 替换可疑字符所占字节。查询批处理继续进行直到完成为止。语句执行完成后，Adaptive Server 将发送以下消息：

```
Msg 2403, Severity 16 (EX_INFO):
WARNING!Some character(s) could not be converted into
client's character set.Unconverted bytes were changed
to question marks ('?').
```

转换和数据长度的变化

某些情况下，在服务器字符集和客户端字符集之间转换数据会导致数据长度发生变化，例如，当一个系统上的字符集使用 1 个字节代表每个字符，而另一个系统上的字符集每个字符要求 2 个字节时，就会出现这种情况。

字符集转换引起数据长度的改变有两种可能：

- 数据长度减少，如下例所示：
 - 多字节 UTF-8 希腊语或俄语转换到单字节希腊语或俄语字符集
 - EUC-JIS 中的双字节 Hankaku-Katakana 日语字符集到 Shift-JIS 中的单字节字符集的转换

- 数据长度增加，如下例所示：
 - 单字节泰语到 UTF-8 中多字节泰语的转换
 - Shift-JIS 中的单字节日语字符集到 EUC-JIS 中的双字节 Hankaku-Katakana 字符集的转换

配置系统和应用程序

如果您在客户端 / 服务器系统的任何位置使用 UTF-8 或日语字符集，在字符集转换时，可能遇到数据长度变化的情况。必须对您的服务器进行配置来处理数据长度的变化。还可能需要对您的客户端进行设置来处理数据长度的变化。

- 1 把服务器配置为使用 Unicode 转换。请参见第 314 页的“配置服务器”。如果服务器和客户端之间的数据长度增加，您还必须完成步骤 2 和 3。
- 2 客户端必须使用 Open Client 11.1 或更高版本。它必须使用 Open Client `ct_capability` 函数来通知服务器它能够在连接时处理 `CS_LONGCHAR` 数据。

`capability` 参数必须设置为 `CS_DATA_LCHAR`，并且 `value` 参数必须设置为 `CS_TRUE`，其中 `connection` 是指向 `CS_CONNECTION` 结构的指针：

```
CS_INT capval = CS_TRUE
ct_capability(connection, CS_SET, CS_CAP_RESPONS,
              CS_DATA_LCHAR, &capval)
```

- 3 当转换导致数据长度增加时，`char` 和 `varchar` 数据将转换为客户端字符集，并作为 `CS_LONGCHAR` 数据发送到客户端。客户端应用程序必须能够提取 `CS_LONGCHAR` 数据。

为实用程序指定字符集

Sybase 实用程序假定客户端平台的缺省字符集与客户端正在使用的字符集相同。然而，有些情况下客户端字符集与平台的字符集不同。因此，可能需要在命令行指定客户端字符集。isql、bcp 和 defncopy 实用程序的命令行选项指定客户端字符集，并暂时覆盖 LANG 变量的设置或 *locales.dat* 中的设置。

-J *charset_name* (UNIX 和 PC) 将客户端字符集设置为 *charset_name*。
如果省略客户端字符集的命令行标志，则使用平台的缺省字符集。请参见《实用程序指南》。

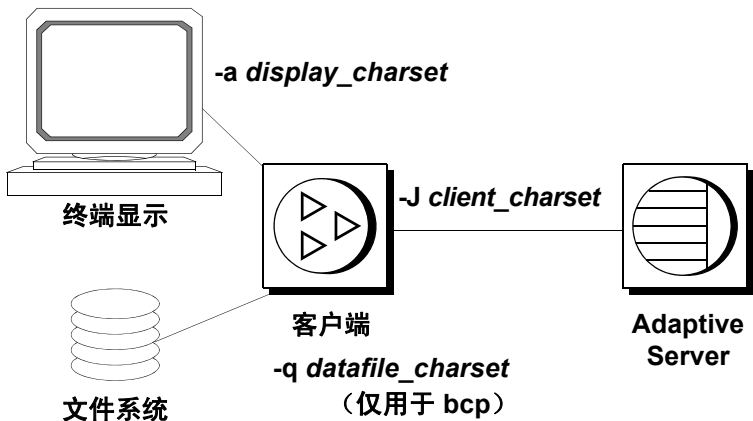
显示和文件字符集的命令行选项

尽管本章重点讨论客户端与 Adaptive Server 之间的字符集转换，但还有另外两个地方也可能需要进行字符集转换：

- 客户端与终端之间
- 客户端与文件系统之间

图 10-4 说明了独立实用程序 isql、bcp 和 defncopy 中提供的路径和命令行选项。

图 10-4：可能需要进行字符集转换的位置



-J 或 /clientcharset 命令行选项指定客户端在向 Adaptive Server 发送字符数据或从 Adaptive Server 接收字符数据时使用的字符集。

设置显示字符集

要从具有与客户端不同的字符集的终端运行客户端，则需使用 `-a` 命令行选项。在图 10-4 中，使用了 `-a` 选项和 `-J` 选项一起标识转换所需的字符集转换文件（*.xlt* 文件）。

只有在客户端字符集与缺省字符集相同时，才单独使用 `-a`，而不用 `-J`。

设置文件字符集

如果您正在运行 `bcp` 在客户端和文件系统之间复制字符数据，而文件系统使用的字符集与客户端不同，则应使用 `-q` 命令行选项。在图 10-4 中，使用了 `-q` 或 `/filecharset` 选项和 `-J` 或 `/clientcharset` 选项一起标识转换所需的字符集转换文件（*.xlt* 文件）。

诊断系统问题

本章讨论诊断及修复系统问题。

主题	页码
Adaptive Server 如何使用错误消息	321
Adaptive Server 错误记录	324
Backup Server 错误记录	331
注销进程	332
管家功能	336
将 Adaptive Server 配置为保存 SQL 批处理文本	339
关闭服务器	343
了解已知的问题	345

Adaptive Server 如何使用错误消息

Adaptive Server 遇到问题时将会显示包括以下内容的错误消息：

- 唯一标识错误消息的**消息号**
- 指示问题的类型和严重程度的**严重级号**（介于 10 和 24 之间）
- **错误状态号**，用于唯一标识引发错误的 Adaptive Server 代码行
- **错误消息**，告知问题是什么，并可能建议如何解决

例如，如果尝试访问不存在的表，您将看到：

```
select * from publisher

Msg 208, Level 16, State 1:
publisher not found. Specify owner. objectname or
use sp_help to check whether the object exists
(sp_help may produce lots of output).
```

一个查询可能有多条错误消息。如果批处理或查询中有多个错误，Adaptive Server 通常只报告第一个错误。您下次执行该批处理或查询时，将报告后续错误。

错误消息存储在 `master..sysmessages` 中，每次发布 Adaptive Server 的新版本时，都会对其进行更新。以下是前几行错误消息（来自使用 `us_english` 作为缺省语言的 Adaptive Server）：

```
select error, severity, description
from sysmessages
where error >=101 and error <=106
and langid is null

error severity description
-----
101      15 Line %d: SQL syntax error.
102      15 Incorrect syntax near '%.*s'.
103      15 The %S_MSG that starts with '%.*s' is too long.
           Maximum length is %d.
104      15 Order-by items must appear in the select-list if
           the statement contains set operators.
105      15 Unclosed quote before the character string '%.*s'.
106      16 Too many table names in the query. The maximum
           allowable is %d.

(6 rows affected)
```

您可以查询 `sysmessages` 以生成错误消息的自定义列表：

- 如果服务器支持多种语言，则 `sysmessages` 存储将采用每种语言存储各条消息。`langid` 列对于 `us_english` 为 `NULL`，对于服务器上安装的其它语言，则与 `syslanguages.langid` 匹配。
- `sysmessages` 中的 `dlevel` 列当前未使用。
- `sqlstate` 列存储在 ANSI SQL92 中定义的错误情况和异常的 `SQLSTATE` 值。
- 大于或等于 17000 的消息号表示系统过程错误消息和消息字符串。

错误消息和消息号

消息号 (`error`) 和语言 ID (`langid`) 的组合唯一地标识每条错误消息。消息号相同但语言 ID 不同的消息表示翻译。

```
select error, description, langid
from sysmessages
where error = 101

error description                                langid
-----
101 Line %d: SQL syntax error.                    NULL
```

```
101 Ligne %1!: erreur de syntaxe SQL. 1
101 Zeile %1!: SQL Syntaxfehler. 2

(3 rows affected)
```

错误消息文本描述问题。该描述通常包括行号、对某类数据库对象（表、列、存储过程等等）的引用或特定数据库对象的名称。

在 `sysmessages` 的 `description` 字段中，后面跟一个字符或字符串的百分比符号 (%) 是各种数据的占位符。Adaptive Server 遇到问题并生成错误消息时，会提供这些数据。“%d” 是数字的占位符；“%S_MSG” 是数据库对象类型的占位符；“%.*s”（引号中的所有内容）是特定数据库对象的名称的占位符。第 323 页的表 11-1 列出了占位符及其表示的数据。

例如，消息号 103 的 `description` 字段内容为：

```
The %S_MSG that starts with '%.*s' is too long. Maximum
length is %d.
```

向用户显示的实际错误消息可能是：

```
The column that starts with 'title' is too long. Maximum
length is 80.
```

对于向技术支持部门报告的错误，请包括编号、对象类型和对象名称。（请参见第 331 页的“报告错误”。）

错误消息文本中的变量

表 11-1 说明每条错误消息解释文本中的符号的含义：

表 11-1： 错误文本符号的含义

符号	表示
%d,%D	十进制数
%x,%X,%.*x,%lx,%04x,%08lx	十六进制数
%s	以空值终止的字符串
%.*s,%*s,%*.s	字符串，通常是特定数据库对象的名称
%S_type	Adaptive Server 定义的结构
%c	单字符
%f	浮点数
%ld	长型十进制数
%lf	双精度浮点数

Adaptive Server 错误记录

来自 Adaptive Server 的错误消息将只发送到用户的屏幕。

来自致命错误消息（严重级为 19 或更高）的堆栈跟踪以及来自内核的错误消息将发送到错误日志文件。该文件的名称会有所不同；请参见所用平台的配置文档或《实用程序指南》。

注释 错误日志文件的所有者是安装 Adaptive Server 的用户（或在删除错误日志后启动 Adaptive Server 的人员）。有关操作系统级的错误日志的权限或所有权问题会导致无法成功启动 Adaptive Server。

如果还没有错误日志，Adaptive Server 会创建一个。在启动时，使用 `runserver` 文件或命令行中的 `errorlogfile` 参数指定错误日志的位置。如果没有选择替代位置，则 Sybase 安装程序实用程序将使用 `$SYBASE/install` 作为错误日志的位置来配置 `runserver` 文件。如果未在 `runserver` 文件中或命令行上指定位置，则错误日志的位置就是启动 Adaptive Server 的目录。有关指定错误日志位置的详细信息，请参见《实用程序指南》中的 `dataserver`。

注释 应始终从同一目录启动 Adaptive Server（或使用 `runserver` 文件或错误日志标志）以便于找到错误日志。

每次启动服务器时，错误日志中的消息给出服务器上每个数据库启动和恢复成功（或失败）的信息。后续的致命错误消息及所有内核错误消息被添加到错误日志文件中。若要通过删除旧消息或不需要的消息来减小错误日志的大小，则必须在 Adaptive Server 关闭时“清理”日志。

错误日志格式

错误日志中的条目包括：

- 每个日志条目涉及的引擎。引擎号由两位数的数字表示。如果只有一个引擎处于联机状态，则显示为“00”。
- 起始线程的系列 ID：
 - 在串行处理中，显示为“00000”。
 - 在并行处理中，显示为起始线程的父线程的服务器进程 ID 号。

- 起始线程的服务器进程 ID：
 - 在串行处理中，它是生成消息线程的服务器进程 ID 号。如果该线程是系统任务，则显示为 “00000”。
 - 在并行处理中，它是起始线程的服务器进程 ID 号。
- 以 yyyy/mm/dd 格式显示的日期，可用于按日期对错误消息进行排序。
- 以 24 小时格式显示的时间，含秒数和厘秒数。
- 单词 “server” 或 “kernel”。此条目仅供 Sybase 技术支持部门使用。
- 错误消息本身。

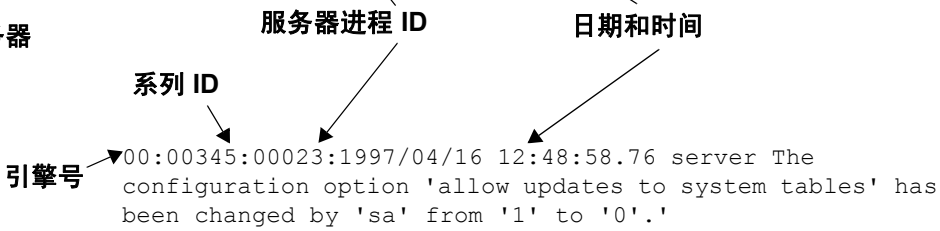
图 11-1 显示了错误日志中某一行两个示例：

图 11-1：错误日志格式

单引擎服务器

00:00000:00008:1997/05/16 15:11:46.58 server Process id 9
killed by Hostname danish, Host process id 3507.

多引擎服务器



严重级

消息的严重级指示有关 Adaptive Server 遇到的问题的类型及严重性。为了获得最大限度的完整性，Adaptive Server 应答错误情况时，显示来自 sysmessages 的消息，但根据内部表采取措施。某些对应的消息在严重级上会有所差异，因此，如果您在开发引用 Adaptive Server 消息和严重级的应用程序或过程，将会偶尔发现不同于预期的行为。

警告！ 可以在 Adaptive Server 错误号的基础上创建自己的错误号和消息。例如，在 Adaptive Server 的值上加上 20,000。但是，不能变更 sysmessages 系统表中由 Adaptive Server 提供的系统消息。

可以使用 `sysusermessages` 将用户定义的错误消息加到 `sp_addmessage` 中。请参见《参考手册：过程》。

每当出现了生成等于或高于 17 严重级的问题时，用户应通知系统管理员。系统管理员负责解决这些问题并跟踪其出现频率。

如果问题已影响了整个数据库，则系统管理员可能必须使用数据库一致性检查程序 (`dbcc`) 来确定损坏程度。`dbcc` 可以标识出一些必须予以删除的对象，并能够修复一些损坏，但可能还是需要重新装载数据库。

有关详细信息，请参见《系统管理指南：卷 2》中的以下各章：

- 《系统管理指南：卷 2》的第 10 章“检查数据库一致性”中论述了 `dbcc`。
- 《系统管理指南：卷 2》的第 12 章“备份和恢复用户数据库”中“开发备份和恢复计划”
- 《系统管理指南：卷 2》的第 13 章“恢复系统数据库”中论述了装载系统数据库。

严重级 10-18

严重级为 10-16 的错误消息由用户错误引起的问题生成。这些问题可由用户解决。严重级 17 和 18 不会终止用户会话。

应将严重级为 17 或更高的错误消息报告给系统管理员或数据库所有者。

级别 10：状态信息

严重级 10 的消息根本不是错误。执行某些命令后，这些消息能提供附加信息，并且通常不显示消息号或严重级。例如，在 `create database` 命令之后，Adaptive Server 将显示一条消息，告知用户已将请求的多少空间分配给了新数据库。

级别 11：未找到指定的数据库对象

严重级为 11 的消息指示 Adaptive Server 找不到命令中引用的对象。

之所以发生这种情况，原因通常是用户在键入数据库对象名称时出错、用户未指定对象所有者的名字，或对哪个数据库是当前数据库产生了混淆。检查对象名称的拼写，如果用户或“`dbo`”不是对象的所有者，请使用所有者的名称，并确保正在使用正确的数据库。

级别 12: 遇到错误的数据类型

严重级 12 的消息表示数据类型问题。例如，用户可能试图在列中输入为错误数据类型的值，或者比较数据类型不同并且不兼容的列。

为了解决比较引起的问题，请将 `convert` 函数与 `select` 一起使用。请参见《参考手册：构件块》或《Transact-SQL 用户指南》。

级别 13: 用户事务语法错误

严重级为 13 的消息表示当前用户定义的事务中有错误。例如，用户可能在尚未发出 `begin transaction` 时发出了 `commit transaction` 命令，或者可能已尝试将事务回退到未定义的保存点（有时保存点名称中可能有键入或拼写错误）。

严重级 13 还可能表示出现死锁，在这种情况下，将回退死锁牺牲品的进程。用户必须重新启动其命令。

级别 14: 权限不足，无法执行命令

严重级为 14 的消息表示用户没有执行命令或访问数据库对象的必要权限。他们可以要求数据库对象所有者、数据库所有者或系统管理员为其授予使用上述命令或对象的权限。

级别 15: SQL 语句中的语法错误

严重级 15 的消息表明用户命令的语法有错。这些错误消息文本包括发生错误的行号以及离出错位置最近的特定词。

级别 16: 杂类用户错误

大多数严重级 16 的错误消息表明用户犯了非致命错误，而该错误无法归入其它错误种类。严重级 16 或更高的严重级还可能指出软件错误或硬件错误。

例如，用户可能试图以违反限制的方式更新视图。可归入此类错误的另一种错误是，在包含多个具有相同列名的表的命令中没有对列名进行限定。Adaptive Server 无法确定用户所指的是哪个表。检查命令语法及工作数据库环境。

通常由 `dbcc checktable` 或 `dbcc checkalloc` 引起且严重级大于 16 的消息只显示为严重级 16，以便能够继续检查下一个对象。如果正在运行 `dbcc` 实用程序，请检查《错误消息和故障排除指南》，了解有关 2500 和 2599 之间严重级为 16 的错误消息的信息。

注释 错误日志中通常不报告级别 17 和级别 18。当出现级别 17 和级别 18 错误时，应指示用户通知系统管理员。

级别 17：资源不足

严重级为 17 的错误消息表示命令已导致 Adaptive Server 资源用尽或超出了由系统管理员设置的某个限制。用户可以继续执行其工作，但可能无法执行某条特定命令。

这些系统限制包括可同时打开的数据库数以及允许与 Adaptive Server 建立的连接数。这些限制存储在系统表中，并可以使用 `sp_configure` 进行检查。有关更改配置变量的详细信息，请参见第 5 章“[设置配置参数](#)”。

数据库所有者可纠正表示用户已用尽空间的级别 17 错误消息。其它的级别 17 的错误消息应该由系统管理员纠正。

级别 18：检测到非致命内部错误

严重级为 18 的错误消息表示内部软件错误。不过，命令可运行完成，且保持与 Adaptive Server 的连接。用户可以继续其正在进行的工作，但可能无法执行特定命令。例如，一种会生成严重级为 18 的错误消息的示例为：Adaptive Server 检测到在没有有效理由时做出了关于特定查询访问路径的决定。

由于生成这种消息的问题不会打断用户的工作，因此用户倾向于不报告这些问题。但是，应指示用户每次遇到此严重级（或更高严重级）的错误消息时，都要通知系统管理员，以便系统管理员能够报告这些错误。

严重级 19-26

致命问题生成严重级 19 和严重级更高的错误消息。这些错误会断开户户与 Adaptive Server 的连接（某些严重级更高的错误还会关闭 Adaptive Server）。若要继续工作，用户必须重新启动客户端程序。

发生致命错误时，进程在停止之前冻结其状态，并记录有关所发生情况的信息。然后，该进程被注销并消失。

当用户连接中断时，用户或许能够或许不能重新连接并继续工作。严重级在此范围内的某些问题只影响一个用户和一个进程。其它问题则影响数据库中的所有进程。在某些情况下，系统管理员必须重新启动 Adaptive Server。这些问题不一定（但有可能）会损坏数据库或数据库对象。这些问题还可能由数据库或其对象以前的损坏引起。其它问题由硬件故障引起。

从内核返回的错误消息将定向到错误日志文件。

级别 19：资源中的 Adaptive Server 致命错误

严重级为 19 的错误消息表示已超出一些不可配置的内部限制，且 Adaptive Server 无法正常恢复。必须重新连接到 Adaptive Server。

级别 20：当前进程中的 Adaptive Server 致命错误

严重级为 20 的错误消息表明 Adaptive Server 在命令中遇到错误。该问题只影响了当前进程，数据库不太可能已损坏。请运行 dbcc 诊断。用户必须重新连接到 Adaptive Server。

级别 21：数据库进程中的 Adaptive Server 致命错误

严重级为 21 的错误消息表明遇到了影响当前数据库中的所有进程的错误。然而，数据库本身不太可能已被损坏。请重新启动 Adaptive Server 并运行 dbcc 诊断。用户必须重新连接到 Adaptive Server。

级别 22: Adaptive Server 致命错误: 表完整性可疑

严重级为 22 的错误消息表明消息中指定的表或索引以前已被软件问题或硬件问题损坏。

第一步应重新启动 Adaptive Server 并运行 `dbcc` 以确定数据库中的其它对象是否也已损坏。无论 `dbcc` 的报告如何, 问题可能只出现在高速缓存中, 而不在磁盘本身上。如果是这样, 重新启动 Adaptive Server 就可以解决问题。

如果重新启动无效, 则问题出在磁盘上。有时, 删除错误消息中指定的对象便能解决问题。例如, 如果消息显示 Adaptive Server 在非聚簇索引中找到长度为 0 的行, 则表所有者可以删除该索引并重新创建索引。

Adaptive Server 会将其在恢复过程中找到的所有可疑页或索引脱机。使用 `sp_setsuspect_granularity` 确定恢复是将整个数据库标记为可疑, 还是仅将个别页标记为可疑。请参见《参考手册: 过程》中的 `sp_setsuspect_granularity`。

用户必须重新连接到 Adaptive Server。

级别 23: 致命错误: 数据库完整性可疑

严重级 23 的错误消息指出, 由于软件问题或硬件问题引起数据库早期的损坏, 使整个数据库的完整性可疑。请重新启动 Adaptive Server 并运行 `dbcc` 诊断。

即使严重级 23 的错误指出整个数据库可疑, 损坏也可能局限于高速缓存, 而磁盘本身没有问题。如果是这样, 请使用 `startserver` 重新启动 Adaptive Server 即可解决问题。

级别 24: 硬件错误或系统表损坏

严重级为 24 的错误消息反映介质故障或 (在极少情况下) `sysusages` 损坏。系统管理员可能必须重新装载数据库。可能需要与硬件供应商联系。

级别 25: Adaptive Server 内部错误

用户不会看到级别 25 错误; 这一级别仅用于 Adaptive Server 内部错误。

级别 26: 规则错误

严重级为 26 的错误消息反映内部锁定或同步规则已破坏。必须关闭并重新启动 Adaptive Server。

报告错误

向 Sybase 技术支持部门报告错误时，请包括：

- 消息号、级别号和状态号。
- 错误消息中包括的任何编号、数据库对象类型或数据库对象名称。
- 生成消息的上下文，即当时正在运行的命令。若能提供错误日志的书面副本也会有所帮助。

Backup Server 错误记录

如同 Adaptive Server 一样，Backup Server 会在错误日志不存在的情况下创建一个错误日志。在启动时，使用 `runserver` 文件或命令行中的 `error_log_file` 参数指定错误日志的位置。如果在安装过程中未选择替代位置，则 Sybase 安装程序将使用 `$SYBASE/install` 作为错误日志的位置来配置 `runserver` 文件。如果在 `runserver` 文件或命令行中没有指定位置，错误日志的位置就是启动 Backup Server 的目录。使用 `backupserver -V` 选项（在 Windows NT 上为 `bcksvr -V`）限制输出到错误日志的消息。请参见《实用程序指南》中描述 Backup Server 的各节。

Backup Server 错误消息的格式如下：

```
MMM DD YY:Backup Server:N.N.N.N:Message Text
```

Backup Server 消息号由四位整数组成，各整数之间用句点分隔，格式为 N.N.N.N。格式为 N.N.N.N 的消息由 Open Server 发送。

Backup Server 错误消息的四个组成部分为 *major.minor.severity.state*：

- *major* 部分通常表示发生错误的 Backup Server 代码的功能区域：
 - 1 — 系统错误。
 - 2 — Open Server 事件错误。
 - 3 — Backup Server 远程过程调用错误。
 - 4 — I/O 服务层错误。
 - 5 — 网络数据传输错误。
 - 6 — 卷处理错误。
 - 7 — 选项分析错误。

错误类型为 1-6 的大部分错误可能起因于 Backup Server 内部错误或各种系统问题。类型 7 的大部分错误几乎总是起因于转储命令或装载命令中指定的选项的问题。

- *minor* 编号是在主类中按顺序指派的。
- *severity* 为：
 - 1 — 信息性，不需用户采取措施。
 - 2、3 — 发生了可能对会话有致命影响的意外情况。该错误可能由使用因素、环境因素、内部逻辑因素或这些因素的任何组合而引起。
 - 4 — 发生了可能对 Backup Server 的执行有致命影响的意外情况。Backup Server 必须立即退出。
- *state* 代码与代码中的错误报告的实例一一对应。如果需要就 Backup Server 错误与技术支持部门联络，状态代码将有助于确定错误的确切起因。

注销进程

进程是 Adaptive Server 的执行单元。每个进程在启动时都会被指派一个唯一的进程标识号，该标识号称作 *spid*。这些标识号与每个进程的其它信息一起存储在 *master..sysprocesses* 中。在并行处理环境中运行的进程可创建子进程，每个子进程都有其自己的 *spid*。有几个进程可创建并指派 *spids*：启动 Adaptive Server、登录任务、检查点、管家任务，等等。可通过运行 *sp_who*，获取大多数信息。

在单引擎服务器上运行 *sp_who* 将显示正在运行的 *sp_who* 进程和所有其它处于“可运行”状态或休眠状态之一的进程。在多引擎服务器中，每个引擎都可有一个正在运行的进程。

kill 命令注销正在进行的进程。注销进程最常见的原因是，该进程与其他用户冲突并且找不到负责运行该进程的用户。这种进程可能持有阻止访问数据库对象的锁，或者有许多休眠的进程占据了可用的用户连接。系统管理员可以注销大多数正在运行或“可运行”的进程，其中包括正在等待以下各项的进程：

- 报警（例如 *waitfor* 命令）
- 网络发送或接收
- 锁定
- 来自系列中另一进程的同步消息

仅当 Adaptive Server 能够完全回退所有未完成的事务，并释放进程所用的全部系统资源时，才允许注销进程。对于作为系列一部分的进程，如果注销任何一个子进程，则还会注销该系列中的所有其它进程。不过，注销父进程最容易。对于一系列进程，如果子进程的状态为 sync sleep，则可以更快速地检测到 kill 命令：

表 11-2 显示了 sp_who 报告的状态值，以及 kill 命令生效的时间。

表 11-2: sp_who 报告的状态值

状态	表示	kill 命令的效果
recv sleep	等待网络读取。	立即。
send sleep	等待网络发送。	立即。
alarm sleep	等待警报，例如： waitfor delay "10:00"	立即。
lock sleep	等待获取锁。	立即。
sync sleep	等待来自系列中另一进程的同步消息。	立即。系列中的其它进程也必须变为可注销的状态。
sleeping	等待磁盘 I/O 或某种其它资源。可能表示正在运行的进程，但该进程正在执行大量的磁盘 I/O	当该进程“苏醒”后将其注销，通常立即注销；少数休眠进程不能苏醒，因而需要服务器重新启动以将其清除。
runnable	在可运行进程的队列中。	立即。
running	活跃地运行在一个服务器引擎中。	立即。
infected	服务器已检测到严重的错误情况；极其少见。	不建议使用 kill 命令。可能需要重新启动服务器以清除进程。
background	由 Adaptive Server 而不是用户运行的进程，例如阈值进程。	立即；使用 kill 时必须格外小心。建议在注销后台进程之前，仔细检查 sysprocesses。
log suspend	到达日志的最后机会阈值时挂起进程。	立即。

只有系统管理员才能发出 kill 命令；不能移交使用该命令的权限。

语法为：

kill spid

一次只能注销一个进程，但可以在批处理中执行一系列注销命令。例如：

```
1> kill 7
2> kill 8
3> kill 9
4> go
```

kill 命令不可逆，且不能包含在用户定义的事务中。spid 必须为数字常量；不能使用变量。下面是 sp_who 的输出样本：

```
fid spid status      loginame origname  hostname  blk  dbname cmd
--- ---
0 1 recv sleep howard howard svr30eng 0 master AWAITING COMMAND
0 2 sleeping NULL NULL 0 master NETWORK HANDLER
0 3 sleeping NULL NULL 0 master DEADLOCK TUNE
0 4 sleeping NULL NULL 0 master MIRROR HANDLER
0 5 sleeping NULL NULL 0 master CHECKPOINT SLEEP
0 6 sleeping NULL NULL 0 master HOUSEKEEPER
0 7 recv sleep bill bill bigblue 0 master AWAITING COMMAND
0 8 recv sleep wilbur wilbur hazel 0 master AWAITING COMMAND
0 9 recv sleep joan joan luv2work 0 master AWAITING COMMAND
0 10 running foote foote svr47hum 0 master SELECT
(10 rows affected, return status = 0)
```

在上面的示例中，不能注销进程 2-6：它们是系统进程。如果使用登录名 NULL 且主机名空缺，则将这些进程标识为系统进程。NETWORK HANDLER、MIRROR HANDLER、HOUSEKEEPER 和 CHECKPOINT SLEEP（极少情况下为 CHECKPOINT）始终出现在 sp_who 输出中。如果审计可用，则 AUDIT PROCESS 将出现。

可以注销进程 1、8、9 和 10，因为它们的状态值分别为 “recv sleep”、“send sleep”、“alarm sleep” 和 “lock sleep”。

在 sp_who 输出中，您无法判断状态为 “recv sleep” 的进程是否属于正在使用 Adaptive Server，但可能正在暂停该进程以检查命令执行结果的用户；也无法判断该进程是否表明用户已重新启动了 PC 或其它终端，并留下了被搁置的进程。请查询 sysprocesses 表以了解有关可疑进程的详细信息。例如，以下查询显示进程 8 使用的主机进程 ID 和客户端软件。

```
select hostprocess, program_name
      from sysprocesses
 where spid = 8

hostprocess program_name
-----
3993        isql
```

此查询以及 sp_who 结果中的用户及主机相关信息，为从操作系统级跟踪进程提供了附加信息。

仅将注销用于状态

`kill ...statusonly` 命令报告处于回退状态的服务器进程 ID (`spid`) 的进度。它不终止 `spid`。`statusonly` 报告显示已完成回退的百分比以及距离回退完成的估计时间长度（以秒为单位）。若要跟踪回退的进度，您必须运行 `kill...with statusonly` 多次：

`kill spid with statusonly`

其中 `spid` 是您正在终止的进程号。

例如，以下内容报告了 `spid` 号为 13 的回退的进程：

```
kill 13 with statusonly
spid: 13 Transaction rollback in progress. Estimated rollback completion:17%
Estimated time left: 13 seconds
```

如果在发出 `kill...statusonly` 时 `spid` 的回退已经完成，或者 Adaptive Server 无法回退指定的 `spid`，则 `kill...statusonly` 将返回以下消息：

```
Status report cannot be obtained. KILL spid:nn is not
in progress.
```

使用 `sp_lock` 检查阻塞进程

除 `sp_who` 外，`sp_lock` 可帮助确定正在阻塞其它进程的进程。如果 `sp_who` 报告中的 `blk_spid` 列指出另一进程在等待获取锁时已被阻塞，则 `sp_lock` 可以显示关于阻塞进程的信息。例如，上述 `sp_who` 输出中的进程 10 被进程 7 阻塞。若要查看有关进程 7 的信息，请执行：

```
sp_lock 7
```

有关 Adaptive Server 中的锁定的详细信息，请参见 Performance and Tuning Series: Locking and Concurrency Control（《性能和调优系列：锁定和并发控制》）。

管家功能

管家任务提供了以下重要功能：

- 管家由以下三个任务组成：管家清洗、管家碎片收集和管家杂事。
sp_who 可识别所有三个任务，如以下输出所示：

fid	spid	status	loginame	origname	hostname	blk_sp
	id	dbname	cmd	block_xloid		
0	5	sleeping	henry	NULL	luv2work	0
master		tempdb	select	0		
0	6	sleeping	joe	NULL	NULL	0
master		tempdb	HK GC	0		
0	7	sleeping	NULL	NULL	NULL	0
master		tempdb	HK CHORES	0		

(11 rows affected, return status = 0)

- 与管家相关的系统任务的常规自动重新启动：如果这些系统任务异常退出，您无需重新启动服务器。
- 系统管理员可以更改所有管家任务优先级。

sp_showpsexec 和 sp_who 都识别所有三个管家名称。

有关 sp_who 和 sp_showpsexec 的详细信息，请参见 《参考手册：过程》。

管家清洗

清洗缓冲区是一个可选任务，该任务在启用的情况下只在空闲时间运行。使用配置参数 housekeeper free write percent 可以禁用此任务。此配置参数只能用于管家清洗任务。

管家杂事

管家杂事任务只在空闲时间运行，并且不使用公共配置参数。它管理各种杂务，例如：

- 刷新表统计信息。
- 刷新帐号统计信息。
- 处理分离事务的超时。使用配置参数 `dtm detach timeout period` 可以禁用此任务。
- 检查许可证使用情况。使用配置参数 `license information` 可以禁用此任务。

管家碎片收集

有两种形式的碎片收集：消极和积极。这些术语描述两种不同的查找空白页测试。

- 消极碎片收集是指耗费较少的查找空白页测试。对于运行时间较长的事务，这种测试可能不太有效，会出现空白页累计的情况。使用消极碎片收集的耗费较少，但可能会降低性能，性能会受到已分配表空间的分段的影响，并且会受到在查询期间必须计算的空白页累计的影响。
- 积极碎片收集是指一种复杂的空白页测试。这种测试要比消极碎片收集的耗费高，因为它会检查页中被删除的每一行以确定删除的事务是否已提交。

使用 `enable housekeeper GC` 配置参数来配置 `delete` 命令，并将管家碎片收集任务配置为积极或消极碎片收集。

积极管家碎片收集会自己调优管家碎片收集任务检查管家列表的频率，使检查频率与应用程序生成空白页的速率匹配。

在用户优先级上运行

管家碎片收集任务在普通用户的优先级上工作，与普通用户任务争用 CPU 时间。这一行为可以防止空白页列表的增长速度超过管家删除空白页的速度。

配置 enable housekeeper GC

若要针对碎片收集任务配置 Adaptive Server，请使用：

```
sp_configure "enable housekeeper GC", value
```

例如，输入：

```
sp_configure "enable housekeeper GC", 4
```

enable housekeeper GC 配置参数的有效值为：

- 0 — 禁用管家碎片收集任务，但为 **delete** 命令启用消极碎片收集。必须使用 **reorg reclaim_space** 释放空白页。这是消耗最少的选项，而且对性能的影响也最小，但如果出现许多空白页累计的情况，则可能会导致性能问题。Sybase 建议您不要使用此值。
- 1 — 为管家碎片收集任务和 **delete** 命令都启用消极碎片收集。该值为缺省值。如果累计的空白页数超过了应用程序所允许的数量，应考虑使用选项 4 或 5。可以使用 **optdiag** 实用程序获取空白页统计信息。
- 2 — 留作将来使用。
- 3 — 留作将来使用。
- 4 — 为管家碎片收集任务和 **delete** 命令都启用积极碎片收集。此选项效率最高，但 **delete** 命令消耗的资源也最多。如果仅数据锁定表上的删除操作在一个批处理中，则此选项很理想。
- 5 — 为管家启用积极碎片收集，为 **delete** 启用消极碎片收集。对于删除操作，此选项比选项 4 消耗的资源要少。此选项适用于并行事务导致删除操作的情况。

使用 reorg 命令

将 **enable housekeeper GC** 设置为 4 或 5 时，碎片收集的效率最高。Sybase 建议将该参数设置为 5。但是，如果出于性能方面的考虑不能将该参数设置为 4 或 5，而且出现空白页累计的情况，请对受影响的表运行 **reorg**。通过 **optdiag** 实用程序可以获得有关空白页的统计信息。

在服务器关闭或崩溃时，释放管家碎片收集任务尚未处理的页的请求将会丢失。这些页（虽然已空但尚未由管家碎片收集任务释放）将保持已分配状态，直到通过运行 **reorg** 将其删除为止。

请参见《系统管理指南：卷 2》中的第 9 章“使用 **reorg** 命令”。

将 Adaptive Server 配置为保存 SQL 批处理文本

有时，查询或过程会导致 Adaptive Server Monitor 停止响应。具有系统管理员角色的用户可以对 Adaptive Server 进行配置，使 Adaptive Server Monitor 能够访问当前正在执行的 SQL 批处理文本。查看运行时间长的批处理的 SQL 文本可帮助您调试“阻塞的”进程或调整大量消耗资源的长语句。

必须将 Adaptive Server 配置为收集 SQL 批处理文本并将其写入共享内存，Adaptive Server Monitor Server（Adaptive Server Monitor 的服务器组件）可以读取共享内存中的这些文本。客户请求可能来自 Monitor Viewer（Sybase Central 的插件），或来自其它 Adaptive Server Monitor Server 应用程序。

如果将 Adaptive Server 配置为保存 SQL 批处理文本，还可以按照 showplan 格式查看当前查询计划（与启用 showplan 后的结果一样）。可以在 Adaptive Server 内查看当前查询计划；请参见第 341 页的“查看 SQL 语句的查询计划”。但只能通过 Adaptive Server Monitor Server 查看 SQL 批处理。有关显示批处理文本的详细信息，请参见 Adaptive Server Monitor Server 文档。

由于所查看的查询或过程可能嵌套在 SQL 文本的批处理内，因此 sysprocesses 表包括已停止响应的语句的行号、语句号及 spid 号等列，以便可对该语句的查询计划进行分析。

缺省情况下，Adaptive Server 不保存 SQL 批处理文本，因此必须对 Adaptive Server 进行配置，为此功能分配内存。如果未配置任何内存来保存 SQL 批处理，则 Adaptive Server Monitor 访问 SQL 对性能没有任何影响。

为批处理文本分配内存

配置要保存的 SQL 文本批处理的数量。启用文本保存时，Adaptive Server 会将后续的 SQL 文本批处理复制到与 SQL Server Monitor 共享的内存中。因为每个新的批处理清除用于连接的内存并覆盖上一个批处理，所以只能查看当前正在执行的 SQL 语句。

❖ 保存 SQL 文本

- 1 配置内存中保留的 SQL 文本的数量（请参见第 340 页的“配置保留在内存中的 SQL 文本的数量”）。
- 2 启用 Adaptive Server，开始保存 SQL 文本（请参见第 340 页的“使 Adaptive Server 开始保存 SQL 文本”）。

注释 您必须具有系统管理特权才能配置和保存 SQL 文本批处理。

配置保留在内存中的 SQL 文本的数量

安装后，必须决定可复制到共享内存的 SQL 文本的最大数量。若要确定为每个用户分配多少内存，请考虑：

- 超出了分配的内存量的 SQL 批处理将被截断，且不出现警告。如果没有为批处理语句分配足够的内存，则要查看的文本可能在被截断的批处理中。
- 从共享内存分配给 SQL 文本的内存越多，从复制到共享内存的批处理文本中截断问题语句的可能性就越小。但是，Adaptive Server 会直接拒绝非常大的值，因为非常大的值没有为数据和过程高速缓存留出足够的内存。

Sybase 建议使用的每个用户连接的初始值为 1024 字节。

使用 `sp_configure` 和 `max SQL text monitored` 配置参数可以分配共享内存，其中，`bytes_per_connection`（为每个客户端连接保存的最大字节数）在 0（缺省值）和 2,147,483,647（理论极限值）之间：

```
sp_configure "max SQL text monitored", bytes_per_connection
```

必须重新启动 Adaptive Server 以使此参数生效。

从共享内存中分配给的 SQL 文本的总内存为 `bytes_per_connection` 与用户连接数的乘积。

使 Adaptive Server 开始保存 SQL 文本

为 SQL 文本分配了共享内存后，只要启用包括 SQL 批处理的 Adaptive Server Monitor 事件摘要，Adaptive Server 就会保存每个 SQL 批处理一个副本。

可能还必须为 SQL 文本重新配置 Adaptive Server Monitor 的事件缓冲区扫描间隔。请参见 Adaptive Server Monitor 文档。

不以文本表示的 SQL 命令

如果使用不以文本表示的 Client-Library 函数（例如，`ct_cursor` 或 `ct_dynamic`）来发出 SQL 命令，Client-Library 为提高效率会对信息进行编码，而 Adaptive Server 通常会解码并显示关键的命令信息。例如，如果使用 `ct_cursor` 打开游标且该命令正在运行，Adaptive Server Monitor 事件摘要将显示游标名称和游标声明语句。

表 11-3 列出了不以文本表示的 Client-Library 函数：

表 11-3：不以文本表示的 SQL 命令

Client-Library 例程	DB-Library 例程	表示的名称	表示的数据
ct_cursor	不适用	CLOSE_CURSOR	游标名称、语句
ct_cursor	不适用	DECLARE_CURSOR	游标名称、语句
ct_cursor	不适用	DELETE_AT_CURSOR	游标名称、语句
ct_cursor	不适用	FETCH_CURSOR	游标名称、语句
ct_fetch（正在处理 ct_cursor 的结果时）	不适用	FETCH_CURSOR	游标名称、语句
ct_cursor CURSOR_ROWS，或 ct_cancel（当连接具有 Client- Library 游标时）	不适用	CURSOR_INFO	游标名称、语句
ct_cursor	不适用	OPEN_CURSOR	游标名称、语句
ct_cursor	不适用	UPDATE_AT_CURSOR	游标名称、语句
ct_command (CS_RPC_CMD) （缺省行为）	dbrpcinit（仅在版本 10.0.1 或更高版本中）	DBLIB_RPC	RPC 名称
ct_dynamic	不适用	DYNAMIC_SQL	动态语句名称、 语句
ct_command (CS_MSG_CMD)	不适用	MESSAGE	无
ct_param	dbrpcparam	PARAM_FORMAT	无
ct_param	dbrpcparam	PARAMS	无
ct_command (CS_RPC_CMD) （仅当使用 5.0 之前的 TDS 版本时）	dbrpcparam（位于 10.0.1 之前的 DB-Library 版本中）	RPC	RPC 名称

关于不以文本表示的 SQL 命令的详细信息，请参见 Open Client 文档。

查看 SQL 语句的查询计划

使用 `sp_showplan` 和所讨论用户连接的 `spid` 可以检索该连接上当前正在运行的语句的查询计划。还可以使用 `sp_showplan` 查看相同批处理中的上一条语句的查询计划。

```
declare @batch int
declare @context int
declare @statement int
execute sp_showplan <spid_value>, @batch_id= @batch output,
@context_id= @context output, @stmt_num=@statement output
```

其中：

- *batch_id* — 是批处理的唯一编号。
- *context_id* — 是该批处理中执行的每个过程（或触发器）的唯一编号。
- *stmt_num* — 是当前语句在批处理内的编号。

Adaptive Server 使用唯一的批处理 ID 使查询计划与批处理文本和由 Adaptive Server Monitor 检索到的其它数据同步。

注释 您必须是系统管理员才能执行 `sp_showplan`。

例如，若要查看 `spid 99` 的当前语句的查询计划，请输入：

```
declare @batch int
declare @context int
declare @statement int
exec sp_showplan 99, @batch output, @context output, @statement output
```

不论 Adaptive Server 是否为 SQL 文本分配了共享内存，都可以独立于 Adaptive Server Monitor 运行查询计划过程。

查看以前的语句

若要查看相同批处理中上一条语句的查询计划，请使用与原始查询相同的值发出 `sp_showplan`，但语句号减 1。使用这种方法，可以向前查看语句批处理中的所有语句，直到查询编号 1 为止。

查看嵌套的过程

尽管使用 `sp_showplan` 可以查看当前语句的查询计划，但当前正在运行的实际语句却可能位于从初始 SQL 批处理调用的过程（或嵌套的过程链）中。[表 11-4](#) 显示了 `sysprocesses` 中包含嵌套语句信息的列。

表 11-4：嵌套语句的 sysprocesses 列

列	数据类型	详细说明
id	Integer	正在运行的过程的对象 ID（如果没有运行任何过程，则为 0）
stmtnum	Integer	正在运行的过程中的当前语句号（如果没有运行任何过程，则为 SQL 批处理语句号）
linenum	Integer	正在运行的存储过程中当前语句的行号（如果没有运行任何过程，则为当前 SQL 批处理语句的行号）

此信息保存在 `sysprocesses` 中，不论是启用了 SQL 文本还是为 SQL 文本分配了任何内存均是如此。

若要显示 `id`、`stmtnum` 和 `linenum` 列，请输入：

```
select id, stmtnum, linenum
from sysprocesses
where spid = spid_of_hung_session
```

注释 无需 `sa_role` 即可运行此 `select` 语句。

关闭服务器

系统管理员可以使用以下命令关闭 Adaptive Server 或 Backup Server：

```
shutdown [backup_server_name] [with {wait|nowait}]
```

`shutdown` 命令的缺省选项是 `with wait`。这就是说，`shutdown` 和 `shutdown with wait` 执行完全相同的任务。

关闭 Adaptive Server

如果未提供服务器名，则 `shutdown` 将关闭您正在使用的 Adaptive Server。发出 `shutdown` 命令后，Adaptive Server 将执行以下任务：

- 1 禁止登录（系统管理员除外）
- 2 在每个数据库中执行检查点操作，并将已更改的页从内存刷新到磁盘
- 3 等待结束当前正在执行的 SQL 语句或过程

这样，`shutdown` 将重新启动 Adaptive Server 时自动恢复必须做的工作量降到最少。

`with nowait` 选项将立即关闭 Adaptive Server。用户过程被中止，并且在执行 `shutdown with nowait` 后恢复可能耗时较长。在发出 `shutdown with nowait` 命令之前发出 `checkpoint` 命令，可将恢复时间降至最少。

关闭 Backup Server

若要关闭 Backup Server，请包括 Backup Server 名称：

```
shutdown SYB_BACKUP
```

缺省值为 `with wait`，因此，在 Backup Server 进程停止之前，任何正在进行的转储和装载将完成。发出 `shutdown` 命令后，将不能在 Backup Server 上启动任何新的转储会话和装载会话。

若要查看可从 Adaptive Server 中访问的 Backup Server 的名称，请执行 `sp_helpserver`。请使用 `shutdown` 命令中 `name` 列的值。可以关闭 Backup Server，只要 Backup Server：

- 在 Adaptive Server 上的 `syssservers` 中列出，并且
- 在本地 `interfaces` 文件中列出。

使用 `sp_addserver` 将 Backup Server 添加到 `syssservers` 中。

检查活动的转储和装载

若要在执行 `shutdown` 命令之前查看 Backup Server 上的活动，请在 Backup Server 上运行 `sp_who`：

```
SYB_BACKUP...sp_who

spid   status  loginame  hostname  blk cmd
-----
1  sleeping NULL      NULL      0  CONNECT HANDLER
2  sleeping NULL      NULL      0  DEFERRED HANDLER
3  runnable NULL      NULL      0  SCHEDULER
4  runnable NULL      NULL      0  SITE HANDLER
5  running  sa        heliotrope 0  NULL
```

在 Backup Server 上使用 *nowait*

无论当前正在进行什么活动，`shutdown backup_server with nowait` 命令都将关闭 Backup Server。仅在紧急情况下使用该命令。该命令可使转储或装载变为未完成的状态或不一致的状态。

如果在日志转储或数据库转储中使用 `shutdown with nowait`，应检查是否有说明转储已完成的消息。如果未收到该消息，或者不能确信转储是否完成，下一个转储应该是 `dump database`，而不能是事务转储。这将确保您不会使用可能不一致的转储。

如果在任何种类的装载过程中使用了 `shutdown with nowait`，且未出现表明装载已完成的消息，则可能无法在数据库上发出其它 `load transaction` 命令。在使用数据库之前，确保对其进行充分的数据库一致性检查 (`dbcc`)。可能必须从 `load database` 开始重新发出整套装载命令。

了解已知的问题

发行公告是了解已知问题或与 Adaptive Server 和 Backup Server 不兼容的问题的有用资源。事先阅读发行公告，可以免去对如何排除已知问题的猜测，并节省时间。

安全性管理

以下各章讨论了 Adaptive Server 中的安全性管理：

- [第 13 章 “Adaptive Server 中的安全性管理快速入门”](#)，概述 Adaptive Server 中可用的安全性功能。
- [第 15 章 “管理 Adaptive Server 登录名、数据库用户和客户端连接”](#)，介绍管理 Adaptive Server 登录帐户和数据库用户的方法。
- [第 14 章 “管理远程服务器”](#)，讨论在启用远程过程调用 (RPC) 时，每个 Adaptive Server 系统管理员和系统安全员必须执行的步骤。
- [第 16 章 “外部鉴定”](#)，说明基于网络的安全服务。这些服务用于鉴定用户和保护在网络上的计算机之间传输的数据。
- [第 17 章 “管理用户权限”](#)，说明用户权限的使用和实施。
- [第 18 章 “审计”](#)，说明如何为安装设置审计。
- [第 19 章 “数据的保密性”](#)，介绍如何配置 Adaptive Server 以确保所有数据的安全性和保密性

主题	页码
安全性简介	349
什么是“信息安全性”？	349
信息安全性标准	350

安全性简介

信息可能是公司的最重要资产。信息与其它资产一样，也需要保护。系统管理员应确定如何以最佳方式保护公司数据库中包含的信息，以及谁可访问该信息。单个数据库服务器需要功能强大而灵活的安全性支持。

用户和用户所访问的数据可能位于世界各地，由非受托网络连接。确保这种环境中的敏感数据和事务的机密性和完整性至关重要。

只有需要信息的人在需要时可以获得信息，信息才是有用的。由于商业关系复杂多变，因此只允许经过授权的用户访问信息至关重要。

什么是“信息安全性”？

在考虑企业的安全性时，应遵循以下一些一般原则：

- 敏感的信息应保持机密性 — 请确定哪些用户应能访问哪些信息。
- 系统应强制实施完整性保护 — 服务器应强制执行规则和约束以确保信息准确和完整。
- 信息应保持可用 — 即使已实施了所有安全保护措施，任何需要访问信息的人在需要信息时也应该能够访问到此信息。

明确公司要保护的内容，以及外部有关各方对公司有何要求：

- 明确信息资产以及当它们易受攻击或受到损害时会有哪些安全风险。
- 明确并了解适用于公司和信息资产的所有法律、法令、规章以及合约协议。
- 明确公司的业务流程及其对信息资产的要求，以兼顾实际业务需要和安全风险。

安全要求会随着时间的推移而改变。请定期重新评估安全要求，确保它们仍能体现出公司的需要。

接着，设置一系列满足公司安全性目标的控制和策略，这样做可以建立一个信息安全策略文档，该文档阐明了为信息安全性所做的决策。

Adaptive Server 包含了一组安全性功能，可帮助您强制实施公司的安全策略。有关 Adaptive Server 中安全性功能的详细信息，请参见第 13 章“[Adaptive Server 中的安全性管理快速入门](#)”。

信息安全性标准

已依照公共标准评估和验证方案的条款对 Adaptive Server 进行了评估和验证。Adaptive Server 还使用 FIPS 140-2 认证模块实现加密功能。

本节将介绍这些认证。

公共标准配置评估

信息技术安全性评估公共标准是计算机安全性认证的一项国际标准 (ISO/IEC 15408)。公共标准由加拿大、法国、德国、荷兰、英国和美国的政府制定。

Adaptive Server 15.0.1 版于 2007 年 9 月完成了公共标准验证。“已评估的配置”包括具有安全性和目录服务选项的 Adaptive Server 15.0.1 版。Adaptive Server 安全性评估是依照公共标准评估和验证方案 (CCEVS) 的过程和方案来实施的。在信息技术安全性评估的公共标准 2.3 版和 2005 年 8 月生效的国际解释中介绍了判定 Adaptive Server Enterprise 所依据的标准。如果按照 Supplement for Installing Adaptive Server for Common Criteria Configuration (《安装用于公共标准配置的 Adaptive Server 的补充说明》) 中的说明来配置 Adaptive Server, 则 Adaptive Server 符合 Sybase Adaptive Server Enterprise 安全性目标 (1.5 版) 中规定的所有安全性功能要求。

Adaptive Server 支持八种安全性功能:

- 加密支持 — Adaptive Server 支持列级的透明数据加密。SQL 语句和扩展提供了安全的密钥管理。
- 安全性审计 — 检查访问、鉴定尝试和管理员功能的审计机制。该安全性审计功能记录了日期、时间、负责人和在审计追踪中描述事件的其它详细信息。
- 用户数据保护 — Adaptive Server 对相应的数据库对象执行自由选择访问控制策略: 数据库、表、视图、存储过程和加密密钥。
- 识别和鉴定 — 除了基础操作系统机制以外, Adaptive Server 还提供它自己的识别和鉴定机制。
- 安全性管理 — 允许您管理用户和相关特权、访问权限的功能以及其它安全性功能 (例如审计追踪)。这些功能受到自由选择访问控制策略规则 (包括角色限制) 的限制。
- 保护 TOE 安全性功能 (TSF) — Adaptive Server 将其环境与其用户的环境分离并使用操作系统机制, 可确保 Adaptive Server 使用的内存和文件具有适当的访问设置。Adaptive Server 通过定义明确的界面与用户进行交互, 旨在确保强制执行其安全性策略。
- 资源利用 — Adaptive Server 提供资源限制, 以防止查询和事务独占服务器资源。
- 评估目标 (TOE) 访问 — Adaptive Server 允许经过授权的管理员构造登录触发器, 以限制登录到特定数量的会话, 并基于时间限制访问。经过授权的管理员还可以基于用户身份限制访问。

FIPS 140-2 验证的加密模块

SSL 是一种用于保护通过 Internet 传输敏感信息（例如信用卡号、股票交易和银行交易）的标准。Adaptive Server 的 SSL 使用 Certicom Security Builder GSE（一种 FIPS 140-2 级别 1 验证的加密模块。请参见 NIST 网站 <http://csrc.nist.gov> 上的验证证书 #542（日期为 2005 年 6 月 2 日）。

如果启用了 FIPS login password encryption 配置参数，FIPS 140-2 认证的 Certicom Security Builder GSE 还用于对传输的登录包中、内存中和磁盘上的登录口令进行加密。

注释 需要安全和目录服务许可证才能使用 SSL 和启用 FIPS login password encryption 参数。如果未启用该参数，则使用 OpenSSL 安全提供程序来执行登录口令加密。

Adaptive Server 加密列功能依赖于对称密钥密码术，并使用相同的 FIPS 140-2 验证的加密模块作为 SSL。请参见《加密列用户指南》。

注释 您必须有加密列许可证才能使用 Adaptive Server 加密列功能。

Adaptive Server 中的安全性管理快速入门

主题	页码
安全性管理的一般过程	353
设置安全性的建议	354
设置安全性的示例	355
自由选择访问控制	358
Adaptive Server 中的安全性功能	357
标识和鉴定	357
外部鉴定	358
管理远程服务器	358
自由选择访问控制	358
角色分离	359
责任审计	360
数据保密性	361

安全性管理的一般过程

表 13-1 介绍了以安全方式管理 Adaptive Server 所需执行的主要任务，并介绍了包含用于执行每个任务的说明的文档。

表 13-1: 安全性管理的一般过程

任务	说明	请参见
1. 安装 Adaptive Server，包括审计。	此任务包括准备安装；从发行介质中装载文件；执行实际的安装；以及管理所需的物理资源。	所用平台的安装文档和 第 18 章“审计”
2. 建立安全的管理环境。	这包括启用审计、为单个用户授予角色以确保个人责任、为系统管理员和系统安全人员指派登录名，以及建立口令和登录策略。	第 15 章“管理 Adaptive Server 登录名、数据库用户和客户端连接”

任务	说明	请参见
3. 为服务器添加用户登录名；为数据库添加用户；建立组和角色；设置代理授权。	添加登录；创建组；为数据库增加用户；删除和锁定登录；以及分配初始口令。为用户指派角色，创建用户定义角色以及定义角色层次和角色的互斥性。	第 15 章 “管理 Adaptive Server 登录名、数据库用户和客户端连接”
4. 管理用户、组和角色的权限。	授予和撤消某些 SQL 命令、执行某些系统过程以及访问数据库、表、特定表列和视图的权限。创建访问规则以强制实施精细访问控制。	第 17 章 “管理用户权限”
5. 在数据库中配置加密以对表中的敏感数据进行加密。对敏感数据进行加密。	配置 Adaptive Server 以使用列级加密，决定要对哪些列数据进行加密，执行一次性密钥创建操作，并使用 <code>alter table</code> 执行初始数据加密。	《加密列用户指南》
6. 建立对数据的完整性控制。	添加检查约束、域角色和参照约束以验证传入数据。	《Transact-SQL 用户指南》和《参考手册：命令》
7. 设置和维护审计。	确定审计对象，审计 Adaptive Server 的使用情况以及使用审计追踪检测系统渗透和资源误用情况。	第 18 章 “审计” 和所用平台的 Adaptive Server 安装和配置文档
8. 设置安装以使用高级鉴定机制和网络安全性。	配置服务器以使用诸如基于 LDAP、PAM 或 Kerberos 的用户鉴定、通过加密实现数据保密性以及数据完整性等服务。	第 16 章 “外部鉴定” 和第 19 章 “数据的保密性”

设置安全性的建议

以下内容介绍了登录名以及登录名与安全性之间的关系。

- 使用 “sa” 登录名 — 当您安装 Adaptive Server 时，将使用系统管理员和系统安全员角色配置一个名为 “sa” 的单一登录名，这意味着 “sa” 登录名对数据库中进行的操作具有无限制的控制。

只在初始设置时使用 “sa” 登录名。不要允许几个用户使用 “sa” 帐户，而是要通过将特定角色指派给个别管理员来建立个人责任。
- 更改 “sa” 登录口令 — “sa” 登录名配置为最初使用 “NULL” 口令登录。请在安装后立即使用 `sp_password` 命令更改口令。

警告！ 登录到 Adaptive Server 时，不要使用 `isql` 命令的 `-P` 选项来指定口令，因为其他用户可能有机会看到该口令。

- 启用审计 — 在管理过程中尽早启用审计，以便记录由系统安全员和系统管理员执行的特权命令。可能还需要审计由具有其它特殊角色的成员执行的命令，例如操作员在转储和装载数据库时
- 指派登录名 — 指派与各自操作系统的登录名相同的 Adaptive Server 登录名。这将使登录到 Adaptive Server 更加容易，简化了服务器和操作系统登录帐号的管理，同时也使关联 Adaptive Server 生成的审计数据和操作系统生成的审计数据更加容易。

设置安全性的示例

此示例使用指派给表 13-2 所列用户的特殊角色。

表 13-2: 将为其指派角色的用户

名称	特权	操作系统登录名
Rajnish Smith	sso_role	rsmith
Catherine Macar-Swan	sa_role	cmacar
Soshi Ikedo	sa_role	sikedo
Julio Rozanski	oper_role	jrozan
Alan Johnson	dbo	ajohnson

表 13-3 根据表 13-2 所示的角色指派，显示了为 Adaptive Server 设置安全操作环境可能使用的命令序列。登录到操作系统后，使用初始 “sa” 帐号发出这些命令。

表 13-3: 用于设置安全性的命令示例

命令	结果
• isql -Usa	以 “sa” 身份登录到 Adaptive Server。sa_role 和 sso_role 均处于活动状态。
• sp_audit “security”, “all”, “all”, “on”	为全服务器范围内与安全性相关的事件以及对激活了 sa_role 或 sso_role 的所有操作的审计设置审计选项。
• sp_audit “all”, “sa_role”, “all”, “on”	
• sp_audit “all”, “sso_role”, “all”, “on”	
• sp_configure “auditing”, 1	启用审计。

注释 在启用审计前，请为审计追踪设置一个阈值过程并确定如何处理 sybsecurity 中的事务日志。请参见第 18 章 “审计”。

- sp_addlogin rsmith, js&2P3d, @fullname = "Rajnish Smith" 为 Rajnish、Catherine、Soshi 和 Julio 添加登录名和口令。

命令	结果
• sp_addlogin cmacar, Fr3ds#1, @fullname = "Catherine Macar-Swan" • sp_addlogin sikedo, mi5pd1s, @fullname = "Soshi Ikedo" • sp_addlogin jrozan, w1seCrkr, @fullname = "Julio Rozanski"	因为没有为任何用户指定缺省数据库，所以这些用户的缺省数据库是 master。
• grant role sso_role to rsmith • grant role sa_role to sikedo • grant role sa_role to cmacar • grant role oper_role to jrozan	为 Rajnish 授予 sso_role，为 Soshi 和 Catherine 授予 sa_role，为 Julio 授予 oper_role。
• use sybsecurity • sp_changedbowner rsmith	通过使系统安全员 Rajnish 成为数据库所有者，授予访问审计数据库 sybsecurity 的权限。未授予 Alan 任何系统定义角色。
<pre>use master sp_addlogin ajohnson, j06n50n, @fullname = "Alan Johnson" create database sales_summary use sales_summary sp_changedbowner ajohnson sp_modifylogin ajohnson, 'defdb', sales_summary</pre>	创建一个新数据库 sales_summary，并使 Alan 成为该数据库的所有者。由于 Alan 是数据库的所有者，因此他现在可以创建用户、创建新数据库对象，以及为此数据库中的其他用户授予权限。
<pre>sp_locklogin sa,"lock"</pre>	锁定 “sa” 登录名，以便没有人能够以 “sa” 身份登录。个人只能使用为他们配置的角色。

注释 在为个别用户授予 sa_role 和 sso_role 角色并已证实这些角色可成功操作之前，请不要锁定 “sa” 登录名。

Adaptive Server 中的安全性功能

表 13-4 介绍了 Adaptive Server 中的安全性功能。

表 13-4：主要安全性功能

安全性功能	说明
标识和认证控制	确保只有经过授权的用户才能登录到系统。除了基于口令的登录鉴定外， Adaptive Server 还支持使用 Kerberos、 LDAP 或 PAM 的外部鉴定。
自由选择访问控制 (DAC)	通常使用 grant 和 revoke 命令提供访问控制，使对象所有者能够限制对对象的访问。此类控制取决于对象所有者的选择。
角色分离	允许管理员将特权角色授予指定用户，以便只有指定的用户才能执行某些任务。 Adaptive Server 包含一些预定义角色（称为“系统角色”），例如系统管理员和系统安全员。此外， Adaptive Server 允许系统安全员定义其它角色（称为“用户定义角色”）。
责任审计	提供了审计事件（例如登录、注销、服务器启动操作、远程过程调用、对数据库对象的访问，以及由特定用户或具有特定活动角色的用户执行的所有操作）的能力。 Adaptive Server 还提供了单个选项，用于审计全服务器范围内与安全性相关的一组事件。
数据保密性	对客户端 / 服务器通信使用加密来维持数据的保密性，可用 Kerberos 或 SSL 实现。列级加密可保持数据库中所存储数据的保密性。不活动数据的保密性是通过口令保护的数据库备份保持的。

标识和鉴定

Adaptive Server 使用服务器用户标识 (SUID) 来唯一地标识具有登录帐户名的用户。此标识链接到每个数据库中的特定用户标识 (UID)。访问控制使用此标识确定是否允许具有此 SUID 的用户访问对象。鉴定会检验某个用户实际上是否是其所称的用户。 Adaptive Server 允许同时使用内部和外部鉴定机制。

标识和鉴定控制将在第 15 章“管理 Adaptive Server 登录名、数据库用户和客户端连接”中讨论。此外，另请参见第 537 页的“使用代理授权”和第 14 章“管理远程服务器”。

外部鉴定

通过使用中央存储库鉴定登录名，通常可以增强大型异构应用程序的安全性。Adaptive Server 支持多种外部鉴定方法：

- **Kerberos** — 在包括 Kerberos 基本结构的企业环境中，提供一种集中且安全的鉴定机制。使用一台名为密钥分发中心的第三方受托服务器进行鉴定，以同时检验客户端和服务端。
- **LDAP 用户鉴定** — 轻量目录访问协议 (LDAP) 可根据用户的登录名和口令，提供一种集中式鉴定机制。
- **PAM 用户鉴定** — 可插入鉴定模块 (PAM) 提供一种集中式鉴定机制，该鉴定机制为管理和运行时应用程序操作使用操作系统界面。

有关每个外部鉴定方法的详细信息，请参见第 16 章 “外部鉴定”。

管理远程服务器

第 14 章 “管理远程服务器” 中介绍了用于管理 Adaptive Server 之间的登录名和用户的内部机制。

自由选择访问控制

对象所有者可将他们拥有的对象访问权限授予其他用户。数据库所有者还可以授予其他用户将访问权限转交给其他用户的权限。通过 Adaptive Server 自由选择访问控制，可以使用 **grant** 命令授予用户、组和角色各种权限。使用 **revoke** 命令撤消这些权限。**grant** 和 **revoke** 命令授予用户执行指定命令和访问指定表、过程、视图、加密密钥和列的权限。

某些命令可由任何用户随时使用，而不需要任何权限。其它命令则只能由具有某种身份的用户（例如系统管理员）使用，并且不可转交。

是否能够指派可被授予或撤消的命令的权限由每个用户的身份（系统管理员、系统安全员、数据库所有者或数据库对象所有者）以及是否授予特定用户可将该权限授予其他用户的权限来决定。

自由选择访问控制在第 17 章 “管理用户权限” 中讨论。

行级访问控制

行级访问控制提供了一种功能强大而灵活的保护数据（直到行级别）的方式。管理员定义的访问规则基于单个数据元素的值，而服务器会透明地强制执行这些规则。管理员定义访问规则后，只要通过应用程序、即席查询、存储过程、视图等查询受影响的数据，就会自动调用该规则。

使用基于规则的访问控制可简化 Adaptive Server 安装的安全性管理和应用程序开发过程，因为是服务器而不是应用程序强制执行安全性。利用以下功能，可以实现行级访问控制：

- 访问规则
- 应用程序环境功能
- 登录触发器
- 域完整性规则

请参见第 553 页的“使用行级访问控制”。

角色分离

Adaptive Server 支持的角色允许您强制执行并维护个人责任。Adaptive Server 提供了系统角色（例如系统管理员和系统安全员），以及由系统安全员创建的用户定义角色。

角色为执行操作和管理任务的用户提供个人责任，并允许您审计操作并将操作归于这些用户。

角色层次

系统安全员可以定义角色层次，以便如果用户拥有一个角色，则将自动拥有层次中较低的角色。例如，“chief_financial_officer”角色可以包含“financial_analyst”和“salary_administrator”两个角色。首席财务官可以执行所有任务，并查看工资管理员和财务分析员可以查看的所有数据。

互斥性

可在成员资格级别或激活级别将角色定义为互斥。例如：

- 您可能不希望将 “payment_requestor” 和 “payment_approver” 这两个角色授予同一用户。
- 可以授予一个用户 “senior_auditor” 和 “equipment_buyer” 角色，但您可能不希望允许用户同时启用这两个角色。

可将系统角色以及用户定义角色定义为位于一个角色层次中，或定义为互斥。例如，您可能希望有一个 “super_user” 角色包含系统管理员角色、操作员角色和技术支持部门角色。另外，您可能希望将系统管理员和系统安全员角色定义为在成员资格级别互斥；即一个用户不能被同时授予这两个角色。

请参见第 387 页的 “为用户创建和指派角色”。

责任审计

Adaptive Server 包括全面的审计系统。审计系统包括：

- sybsecurity 数据库
- 用于管理审计的配置参数
- sp_audit （用于设置所有审计选项）
- sp_addauditrecord （用于将用户定义记录添加到审计追踪）

安装审计后，可以指定 Adaptive Server 用于审计追踪的审计表的数量。如果使用两个或多个表来存储审计追踪，可以建立一个可以平稳运行而且无须手动干涉又不会丢失记录的审计系统。

系统安全员管理审计系统，且只有系统安全员可以启动和停止审计、设置审计选项以及处理审计数据。作为系统安全员，您可以为诸如以下事件建立审计：

- 全服务器范围内的与安全性相关的事件
- 创建、删除和修改数据库对象
- 特定用户执行的所有操作或具有特定活动角色的用户执行的所有操作
- 授予或撤消数据库访问权限
- 导入或导出数据
- 登录和注销
- 与加密密钥相关的所有操作

审计功能在第 18 章 “审计” 中讨论。

数据保密性

Adaptive server 通过使用安全套接字层 (SSL) 标准或 Kerberos 来加密客户端 / 服务器通信，以便您可以保持数据的保密性。通过在数据库中使用列级加密和对脱机数据的备份进行加密，您可以保护数据的保密性。

有关详细信息，请参见：

- SSL — [第 19 章 “数据的保密性”](#)
- Kerberos — [第 16 章 “外部鉴定”](#)
- 加密列 — 《加密列用户指南》

口令保护的数据库备份

`dump` 和 `load database` 命令包括一个 *password* 参数，该参数允许您为数据库转储提供口令保护。请参见《参考手册：命令》和《系统管理指南：卷 2》中的第 12 章 “备份和恢复用户数据库”。

管理远程服务器

本章讨论在启用[远程过程调用 \(RPC\)](#) 时，每个 Adaptive Server 的系统管理员和系统安全员所必须执行的步骤。

主题	页码
概述	363
管理远程服务器	365
添加远程登录名	369
远程用户的口令检查	374
获取有关远程登录的信息	375
远程登录的配置参数	375

概述

本地 Adaptive Server 的用户可以执行远程 Adaptive Server 上的存储过程。执行 RPC 会将远程过程的结果发送给调用过程，通常显示在用户的屏幕上。

若要启用 RPC，每个 Adaptive Server 的系统管理员和系统安全员必须执行以下步骤：

- 在本地服务器上：
 - 系统安全员 — 使用 `sp_addserver` 在系统表 `master..sys.servers` 中列出本地服务器和远程服务器。
 - 在本地服务器的 `interfaces` 文件或目录服务中列出远程服务器。
 - 重新启动本地服务器以将全局变量 `@@servername` 设置为本地服务器的名称。如果此变量未正确设置，则用户无法从本地服务器对任何远程服务器执行 RPC。

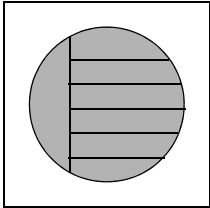
- 在远程服务器上：
 - 系统安全员 — 使用 `sp_addserver` 在系统表 `master..sys.servers` 中列出引发 RPC 的服务器。
 - 若要允许引发远程过程的用户访问服务器，系统安全员需使用 `sp_addlogin`，系统管理员需使用 `sp_addremotelogin`。
 - 添加远程登录名作为相应数据库的用户，并授予其执行此过程的登录权限。（如果已将 `execute` 权限授予 “public”，则无需为用户授予特定权限。）

图 14-1 显示了如何设置服务器以进行远程访问。

图 14-1：设置服务器以允许远程过程调用

ROSE 上的用户 “joe” 需要访问 ZINNIA 上的存储过程

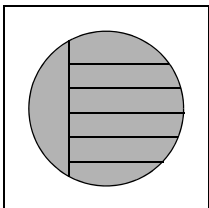
ROSE



`sp_addserver` ROSE, local
`sp_addserver` ZINNIA

`interfaces` 文件必须有用
于 ZINNIA 的条目

ZINNIA



`sp_addserver` ROSE
`sp_addlogin` joe
`sp_addremotelogin` ROSE, joe

`sp_adduser` joe （在相应的数据库
中）
`grant execute` on `procedure_name` to joe

有关处理远程服务器的特定于操作系统的信息，请参见所用平台的安装文档。

管理远程服务器

表 14-1 列出了与管理远程服务器相关的任务，以及用于执行这些任务的系统过程。

表 14-1：与管理远程服务器相关的任务

目的	使用	请参见
添加远程服务器	sp_addserver	第 365 页的 “添加远程服务器”
管理远程服务器名	sp_addserver	第 367 页的 “管理远程服务器名”
更改服务器连接选项	sp_serveroption	第 367 页的 “设置服务器连接选项”
显示有关服务器的信息	sp_helpserver	第 369 页的 “获取有关服务器的信息”
删除服务器	sp_dropserver	第 369 页的 “删除远程服务器”

添加远程服务器

系统安全员使用 `sp_addserver` 将条目添加到 `sys.servers` 表中。在发起调用的服务器上，必须为本地服务器和其所调用的每个远程服务器添加一个条目。

创建远程服务器的条目时，可以输入：

- 使用在 `interfaces` 文件中列出的名称，或
- 为远程服务器提供本地名。例如，如果 `interfaces` 文件中的名称是 “MAIN_PRODUCTION”，您可能需要将其称为 “main”。

语法为：

```
sp_addserver lname [{, local | null}
[, pname]]
```

其中：

- `lname` — 为远程服务器提供本地的 “调用名称”。如果此名称与 `interfaces` 文件中的远程服务器名称不同，请提供该名称作为第三个参数 `pname`。

远程服务器必须列在本地计算机上的 `interfaces` 文件中。如果没有列出，应从远程服务器中复制 `interfaces` 文件条目，并将其附加到现有 `interfaces` 文件中。请保持端口号相同。

- **local** — 将所添加的服务器标识为本地服务器。**local** 值只在启动或重新启动后使用，以标识本地服务器名，使其能够出现在 Adaptive Server 显示的消息中。**null** 指定此服务器是远程服务器。

注释 要使用户能够从本地服务器中成功运行 RPC，请使用 **local** 选项添加本地服务器，并重新启动该服务器。设置全局变量 @@servername 要求重新启动。

- **pname** — 是名为 *lname* 的服务器的 *interfaces* 文件中列出的远程服务器。此可选的参数允许您为任何其它需要与之通信的 Adaptive Server、Open Server 或 Backup Server 建立本地别名。如果不指定 **pname**，则缺省值为 *lname*。

添加远程服务器的示例

此示例为名为 DOCS 的本地服务器创建一个条目：

```
sp_addserver DOCS, local
```

此示例为名为 GATEWAY 的远程服务器创建条目：

```
sp_addserver GATEWAY
```

若要在 GATEWAY 服务器上运行诸如 **sp_who** 等远程过程，请执行以下命令：

```
GATEWAY.sybsystemprocs.dbo.sp_who
```

或：

```
GATEWAY...sp_who
```

此示例为名为 MAIN_PRODUCTION 的远程服务器创建一个本地别名“main”：

```
sp_addserver main, null, MAIN_PRODUCTION
```

然后，用户可以输入：

```
main...sp_who
```

管理远程服务器名

`master.dbo.sys.servers` 表包含两个服务器名称列：

- `srvname` 是用户执行远程过程调用时必须提供的唯一服务器名。
- `srvnetname` 是服务器的网络名，该名称必须与 `interfaces` 文件中的名称相匹配。

要在网络中添加或删除服务器，请使用 `sp_addserver` 更新服务器在 `srvnetname` 中的网络名。

例如，若要从网络中删除服务器 `MAIN`，并将远程应用程序移到名为 `TEMP` 的服务器，请使用以下语句更改网络名，同时保留本地别名：

```
sp_addserver MAIN, null, TEMP
```

`sp_addserver` 将显示消息来说明它正在更改现有服务器条目的网络名。

设置服务器连接选项

`sp_serveroption` 设置服务器选项 `timeouts`、`net password encryption`、`rpc security model A` 以及 `rpc security model B`，这些设置将影响与远程服务器的连接。此外，如果已将远程过程安全模式设置为 `rpc security model B`，则可以使用 `sp_serveroption` 设置以下选项：`security mechanism`、`mutual authentication`、`use message confidentiality` 和 `use message integrity`。

为 `sp_serveroption` 指定的选项不影响 `Adaptive Server` 和 `Backup Server` 之间的通信。

以下各部分介绍 `timeouts`、`net password encryption`、`rpc security model A` 和 `rpc security model B`。有关在 `rpc security model B` 打开时可以指定的其它选项的信息，请参见第 465 页的“建立远程过程的安全性”。

使用 `timeouts` 选项

系统管理员可以使用 `timeouts` 选项来禁用和启用本地服务器使用的常规超时代码。

缺省情况下，`timeouts` 设置为 `true`，如果在一分钟内没有远程用户的活动，管理远程登录的节点处理器进程将超时。通过将远程过程调用中涉及的两个服务器上的 `timeouts` 设置为 `false`，可禁用自动超时。若要将 `timeouts` 更改为 `false`，请使用：

```
sp_serveroption GATEWAY, "timeouts", false
```

在两台服务器中将 `timeouts` 都设置为 `false` 后，无论用户从任一方向执行 RPC，每台计算机上的节点处理器都将运行，直到其中一台服务器关闭为止。服务器再次启动后，该选项会保持为 `false`，并在下次用户执行 RPC 时重建节点处理器。如果用户频繁地执行 RPC，那么就系统资源而言，将此选项设置为 `false` 可能效率较高，因为在建立物理连接时会有一些系统开销。

使用 *net password encryption* 选项

系统安全员可以使用 `net password encryption` 指定开始与远程服务器连接时，是使用客户端口令加密握手还是使用常规未加密口令握手序列。缺省值是 `false`。

如果 `net password encryption` 设置为 `true`：

- 1 不用口令，发送初始登录包。
- 2 客户端向远程服务器指示需要加密。
- 3 远程服务器返回加密密钥，客户端可以用该密钥对其纯文本口令进行加密。
- 4 然后，客户端对其自己的口令进行加密，当这些口令到达远程服务器后，远程服务器使用该密钥来对口令进行鉴定。

此示例将 `net password encryption` 设置为 `true`：

```
sp_serveroption GATEWAY, "net password encryption",  
true
```

使用 *rpc security model* 选项

`rpc security model A` 和 `rpc security model B` 选项指定可用于 RPC 的安全类型。如果使用模式 A（缺省值），则 Adaptive Server 不支持安全服务，例如两台服务器间通过加密实现消息保密的服务。

对于安全模式 B，本地 Adaptive Server 从安全性机制获得认证并使用该认证建立与远程 Adaptive Server 的安全物理连接。使用此模式，可以选择以下一项或多项安全服务：相互鉴定、通过加密实现消息保密性或消息完整性。

若要为服务器 GATEWAY 设置安全模式 A，请执行：

```
sp_serveroption GATEWAY, "rpc security model A",  
true
```

有关如何将服务器设置为安全模式 B 的信息，请参见第 465 页的“[建立远程过程的安全性](#)”。

获取有关服务器的信息

`sp_helpserver` 报告有关服务器的信息。如果没有参数，`sp_helpserver` 将提供有关 `sys.servers` 中列出的所有服务器的信息。如果包括服务器名称，`sp_helpserver` 将仅提供有关该服务器的信息：

```
sp_helpserver [server]
```

`sp_helpserver` 在 `master.sysremotelogins` 表中检查 `srvname` 和 `srvnetname`。

有关设置远程服务器的特定于操作系统的信息，请参见所用平台的安装文档。

删除远程服务器

系统安全员可以使用 `sp_dropserver` 从 `sys.servers` 中删除服务器。

```
sp_dropserver server [, droplogins]
```

其中：

- `server` — 是要删除的服务器的名称。
- `droplogins` — 允许您删除远程服务器及该服务器的所有远程登录信息。如果不使用 `droplogins`，则无法删除带有与之关联的远程登录信息的服务器。

以下语句删除 `GATEWAY` 服务器及与之关联的所有远程登录信息：

```
sp_dropserver GATEWAY, droplogins
```

不必使用 `droplogins` 来删除本地服务器；该条目不包含与其关联的远程登录信息。

添加远程登录名

任何 Adaptive Server 的系统安全员和系统管理员都共享以下控制：哪些远程用户可以访问服务器，以及远程用户使用什么标识。系统管理员可使用 `sp_addremotelogin` 添加远程登录名，使用 `sp_dropremotelogin` 删除远程登录名。系统安全员可使用 `sp_remoteoption` 来控制是否需要检查口令。

映射用户的服务器 ID

远程服务器上的登录名可以用三种方法映射到本地服务器：

- 特定远程登录名可被映射为特定的本地登录名。例如，远程服务器上的用户 “joe” 可能被映射为 “joesmith”。
- 来自一个远程服务器的所有登录名都可被映射为一个本地名。例如，从 MAIN 服务器发送远程过程调用命令的所有用户都可被映射为 “remusers”。
- 来自一个远程服务器的所有登录名都可使用其远程名。

第一个选项可与其它两个选项组合使用，它的特定映射优先于其它两种较为普通的映射。第二个和第三个选项是互斥的；可以使用两者中的一个，但不能一起使用。

更改映射选项

使用 `sp_dropremotelogin` 删除旧的映射。

使用 `sp_addremotelogin` 添加远程登录名：

```
sp_addremotelogin remoteserver [, loginame
                                [, remotename]]
```

如果本地名未列在 `master.syslogins` 中，请在添加远程登录名之前，使用 `sp_addlogin` 添加本地名作为 Adaptive Server 登录名。

只有系统管理员才能执行 `sp_addremotelogin`。请参见 《参考手册：过程》。

将远程登录名映射为特定的本地名

以下示例将远程系统中的登录名 “pogo” 映射为本地登录名 “bob”。用户以 “pogo” 的身份登录到远程系统。当 “pogo” 从 GATEWAY 执行远程过程调用时，本地系统将远程登录名映射为 “bob”。

```
sp_addlogin bob
sp_addremotelogin GATEWAY, bob, pogo
```

将所有的远程登录名映射到一个本地名

以下示例创建一个条目，它将所有远程登录名映射为本地名“albert”。除了特定映射的名称，所有名称都映射为“albert”，如上节所述。例如，如果将“pogo”映射为“bob”然后将其余的登录名映射为“albert”，则“pogo”仍映射为“bob”。

```
sp_addlogin albert
sp_addremotelogin GATEWAY, albert
```

如果使用 `sp_addremotelogin` 将远程服务器中的所有用户映射为相同的本地名，请使用 `sp_remoteoption` 为这些用户指定“trusted”选项。例如，若要使服务器 GATEWAY 中所有映射为“albert”的用户获得信任，请指定：

```
sp_remoteoption GATEWAY, albert, NULL, trusted, true
```

如果未将登录名指定为受托，则这些登录名无法在本地服务器上执行 RPC，除非在他们登录到远程服务器时，为本地服务器指定了口令。用户在使用 Open Client Client-Library 时可以运行 `ct_remote_pwd` 为服务器到服务器的连接指定口令。`isql` 和 `bcp` 不允许用户为 RPC 连接指定口令。有关 `sp_remoteoption` 的详细信息，请参见第 374 页的“远程用户的口令检查”。

警告！ 不要将多个远程登录名映射为单个本地登录名，因为这样做减少了服务器上的个人责任。被审计的操作只能追踪到本地服务器的登录名，无法追踪到远程服务器上的各个登录名。

如果正在使用的是基于网络的安全性

如果用户使用“统一登录”登录到远程服务器，则必须在本地服务器上将这些登录名指定为受托，或者用户在登录到远程服务器时必须指定服务器口令。

警告！ 使用 `sp_remoteoption` 的 `trusted` 模式降低了服务器的安全性，因为不会对这些“trusted”用户给出的口令进行验证。

在本地服务器中保留远程登录名

若要允许远程用户在使用本地服务器时保留各自的远程登录名，请执行下述操作：

- 1 使用 `sp_addlogin` 为来自远程服务器的每个登录创建登录名。
- 2 为服务器使用 `sp_addremotelogin`，以便在 `master..sysremotelogins` 中创建一个条目，其远程登录名为空值，且 `suid` 的值为 `-1`。例如：

```
sp_addremotelogin GATEWAY
```

远程用户登录映射的示例

以下语句将显示记录在 `master..sys.servers` 中的本地和远程服务器信息：

```
select srvid, srvname from sys.servers
srvid  srvname
-----
0      SALES
1      CORPORATE
2      MARKETING
3      PUBLICATIONS
4      ENGINEERING
```

SALES 服务器是本地的，其它服务器都是远程的。

以下语句将显示有关存储在 `master..sysremotelogins` 中的远程服务器和用户的信息：

```
select remoteserverid, remoteusername, suid
from sysremotelogins
remoteserverid  remoteusername  suid
-----
1               joe             1
1               nancy           2
1               NULL            3
3               NULL            4
4               NULL            -1
```

通过比较此结果中的 `remoteserverid` 值和前一个结果中 `srvid` 的值，可以找到 `remoteusername` 在其上为有效的服务器的名称。例如，在第一个结果中，`srvid 1` 指示 `CORPORATE` 服务器；在第二个结果中，`remoteserverid 1` 指示同一服务器。因此，远程用户登录名“joe”和“nancy”在 `CORPORATE` 服务器上是有用的。

以下语句可显示 `master..syslogins` 中的条目：

```
select suid, name from syslogins
suid    name
-----
1       sa
2       vp
3       admin
4       writer
```

以上三个查询结果合在一起显示如下：

- 远程 CORPORATE 服务器（`srvid` 和 `remoteserverid` 1）上的远程用户名 “joe”（`suid` 1）被映射为 “sa” 登录名（`suid` 1）。
- 远程 CORPORATE 服务器（`srvid` 和 `remoteserverid` 1）上的远程用户名 “nancy”（`suid` 2）被映射为 “vp” 登录名（`suid` 2）。
- CORPORATE 服务器上的其它登录名（`remoteusername` “NULL”）被映射为 “admin” 登录名（`suid` 3）。
- PUBLICATIONS 服务器（`srvid` 和 `remoteserverid` 3）上的所有登录名被映射为 “writer” 登录名（`suid` 4）。
- ENGINEERING 服务器（`srvid` 和 `remoteserverid` 4）上的所有登录名将按其远程用户名（`suid` -1）在 `master..syslogins` 中进行查找。
- `sysremotelogins` 中没有 MARKETING 服务器的 `remoteserverid` 条目。因此，登录到 MARKETING 服务器的用户不能从该服务器运行远程过程调用。

使用远程用户映射过程和为单个存储过程设置权限的能力可以控制能够访问本地过程的用户。例如，可以允许 CORPORATE 服务器上的 “vp” 登录名执行某些本地过程，并且允许 CORPORATE 上的所有其它登录名执行 “admin” 登录名具有执行权限的过程。

注释 通常，远程服务器上的用户口令必须与本地服务器上的口令相匹配。

远程用户的口令检查

系统安全员可以使用 `sp_remotoption` 确定在远程用户登录到本地服务器时是否检查口令。缺省情况下，将验证口令（此模式为“untrusted”模式）。在 `trusted` 模式中，本地服务器接受来自其它服务器和前端应用程序的远程登录，而不对特定登录名进行用户访问验证。

带参数使用 `sp_remotoption` 时，它将更改指定用户的模式：

```
sp_remotoption [remoteserver, loginame, remotename,  
               optname, {true | false}]
```

例如，若要为用户“bob”设置 `trusted` 模式，请输入

```
sp_remotoption GATEWAY, pogo, bob, trusted,  
               true
```

使用 untrusted 模式的效果

“untrusted”模式的效果取决于用户的客户端程序。`isql` 和一些用户应用程序要求登录名在远程服务器和本地服务器具有相同的口令。可编写 `Open Client` 应用程序以允许本地登录名在不同的服务器上具有不同的口令。

若要在“untrusted”模式中更改口令，必须先在所有访问的远程系统中更改，然后才能在本地服务器上更改。如果首先在本地上更改口令，则在发出远程过程调用以在远程服务器上执行 `sp_password` 时，口令将不再匹配。

在远程服务器上更改口令的语法为：

```
remote_server...sp_password caller_passwd, new_passwd
```

在本地服务器上，语法为：

```
sp_password caller_passwd, new_passwd
```

请参见第 403 页的“更改口令”。

获取有关远程登录的信息

`sp_helpremotelogin` 在服务器上显示有关远程登录名的信息。以下示例显示将远程登录名 “pogo” 以本地方式映射为登录名 “bob”，而所有其它远程登录名则保持其远程名称：

```

      sp_helpremotelogin
server      remote_user_name      local_user_name      options
-----
GATEWAY     **mapped locally**      **use local name**   untrusted
GATEWAY     pogo                    bob                   untrusted

```

远程登录的配置参数

表 14-2 显示了影响 RPC 的配置参数。所有这些配置参数都是使用 `sp_configure` 设置的，并且在重新启动 Adaptive Server 前这些参数不会生效。

表 14-2: 影响 RPC 的配置参数

配置参数	缺省值
allow remote access	1
number of remote logins	20
number of remote sites	10
number of remote connections	20
remote server pre-read packets	3

请参见第 5 章 “设置配置参数” 中各配置参数的说明。

管理 Adaptive Server 登录名、数据库用户和客户端连接

主题	页码
选择和创建口令	378
将登录添加到 Adaptive Server	379
登录失败	380
创建组	381
向数据库添加用户	381
用户数和登录 ID 数	385
为用户创建和指派角色	387
删除用户、组和用户定义角色	399
锁定或删除 Adaptive Server 登录帐户	400
更改用户信息	402
在数据库中使用别名	407
获取有关用户的信息	409
建立口令和登录策略	415
监控许可证的使用状况	447
获取有关使用情况的信息：收费退回式会计	449

向 Adaptive Server 中添加新的登录名，向数据库中添加用户，以及授予用户使用命令和数据库对象的**权限**的职责由系统安全员、系统管理员和数据库所有者分担完成。

这些步骤使用 `sp_addlogin` 为特定服务器创建登录帐户，并在该服务器的 `syslogins` 表中存储帐户信息。也可以在 LDAP 服务器上创建并存储登录帐户：

- 1 系统安全员使用 `sp_addlogin` 为新用户创建服务器登录帐户。
- 2 系统管理员或数据库所有者使用 `sp_adduser` 向数据库中添加用户或为组分配用户。请参见第 381 页的“创建组”。可以使用别名为用户授予数据库访问权限。请参见第 407 页的“添加别名”。
- 3 系统安全员授予用户特定的角色。

- 4 系统管理员、数据库所有者或对象所有者授予用户或组对特定命令和数据库对象的特定权限。还可以授予用户或组为其他用户或组授予特定对象权限的权限。请参见第 17 章 “管理用户权限”。

表 15-1 汇总了用于所述任务的系统过程和命令。

表 15-1: 将用户添加到 Adaptive Server 和数据库

任务	要求的角色	命令或过程	数据库
创建新的登录；指派口令、缺省数据库、缺省语言和全名	系统安全员	sp_addlogin	任何数据库
创建组	数据库所有者或系统管理员	sp_addgroup	用户数据库
创建并指派角色	系统安全员	create role、 grant role	主数据库
向数据库中添加用户和指派组	数据库所有者或系统管理员	sp_adduser	用户数据库
为用户授予其他数据库用户的别名	数据库所有者或系统管理员	sp_addalias	用户数据库
为组、用户或角色授予创建或访问数据库对象以及运行命令的权限	数据库所有者、系统管理员、 系统安全员或对象所有者	grant	用户数据库

选择和创建口令

在添加用户作为 Adaptive Server 的登录名时，系统安全员将为每个用户分配一个口令。用户可使用 sp_password 随时修改其口令。请参见第 403 页的 “更改口令”。

创建口令时：

- 不要使用诸如生日、街道名或其它任何与个人生活有关的单词或数字。
- 不要使用宠物或爱人的名字。
- 不要使用字典中出现的单词或反向拼写的单词。

最难猜的口令是那些组合了大小写字母和数字的口令。绝不要将口令泄露给他人或记录在别人能看到的地方。

口令必须满足以下条件：

- 长度至少为 6 个字符。
- 包含任意可打印字母、数字或符号。

- 如果存在以下情况，则口令在 `sp_addlogin` 中必须放在引号内：
 - 口令中包含 A - Z、a - z、0 - 9、_、#、有效的单字节或多字节字母字符、变音字母字符以外的任何字符
 - 以数字 0 - 9 开头

请参见第 422 页的“口令复杂程度检查”。

将登录添加到 Adaptive Server

可使用 `sp_addlogin` 命令将新登录名添加到 Adaptive Server。（使用 `sp_adduser` 授予访问用户数据库的权限。）只有系统安全员才能执行 `sp_addlogin`。

请参见《参考手册：过程》了解完整的 `sp_addlogin` 语法。

下面的语句为用户 “maryd” 建立一个帐户，口令为 “100cents”，使用缺省数据库 (master)、缺省语言，且没有全名：

```
sp_addlogin "maryd", "100cents"
```

由于口令以 1 开头，因此要用双引号引起来。

执行完此语句后，“maryd” 就可以登录到 Adaptive Server。除非特别授予该用户对 master 的访问权限，否则系统会自动将其作为 master 数据库的 “guest” 用户对待，只具有有限的权限。

下面的语句设置一个登录帐户（“omar_khayyam”）和口令（“rubaiyat”），并使 pubs2 成为此用户的缺省数据库：

```
sp_addlogin omar_khayyam, rubaiyat, pubs2
```

要为用户指定全名并使用缺省数据库和语言，请指定 `null` 来代替 `defdb` 和 `deflanguage` 参数。例如：

```
sp_addlogin omar, rubaiyat, null, null,
"Omar Khayyam"
```

另外，也可以指定一个参数名，这样就不必指定所有参数。例如：

```
sp_addlogin omar, rubaiyat,
@fullname = "Omar Khayyam"
```

当您执行 `sp_addlogin` 时，Adaptive Server 将向 `master.dbo.syslogins` 中添加一行，为新用户指派唯一的系统用户 ID (suid)，并填入其它信息。用户登录时，Adaptive Server 在 `syslogins` 中查找用户提供的名称和口令。`password` 列使用单向算法加密，因此不可读。

创建登录时，syslogins 的 crdate 列设置为当前时间。

syslogins 中的 suid 列在 Adaptive Server 中唯一地标识每个用户。不论用户正在使用什么数据库，用户的 suid 都保持不变。总是将 suid 1 指派给安装 Adaptive Server 时创建的缺省 “sa” 帐户。其他用户的服务器用户 ID 是由 Adaptive Server 在每次执行 sp_addlogin 时连续指派的整数。

登录失败

Adaptive Server 必须成功对用户进行鉴定，该用户才能够访问 Adaptive Server 中的数据。如果鉴定尝试失败，Adaptive Server 将返回以下消息且网络连接将终止：

```
isql -U bob -P badpass
Msg 4002, Level 14, State 1:
Server 'ACCOUNTING'
Login failed.
CT-LIBRARY error:
ct_connect(): protocol specific layer:external error:
The attempt to connect to the server failed
```

此消息是常规登录失败消息，它不会通知进行连接的用户失败是由错误的用户名还是由错误的口令导致。

尽管客户端显示登录失败常规消息的目的是为了避免向恶意用户提供信息，但系统管理员可能会发现，失败的原因对于检测入侵尝试和诊断用户鉴定问题十分重要。

Adaptive Server 在 sysaudits.extrainfo 列的 Other Information 部分的 Errornumber.Severity.State 中提供了登录失败原因。登录失败审计具有事件编号 45 和 eventmod 2。

将 sp_audit login 参数设置为 on 或 fail 以启用登录失败审计：

```
sp_audit "login", "all", "all", "fail"
sp_audit "login", "all", "all", "on"
```

请参见 [“审计登录失败”](#)。

创建组

组使您只需通过一个语句即可为多个用户授予或撤消权限，并允许您为一组用户提供一个总称。在管理拥有大量用户的 Adaptive Server 安装时，组非常有用。

请在向数据库中添加用户之前创建组，因为 `sp_adduser` 既可以将用户指派到组中，也可以将用户添加到数据库中。

您必须具有系统管理员或系统安全员角色或是数据库所有者，才能使用 `sp_addgroup` 创建组。语法为：

```
sp_addgroup grpname
```

组名（必需参数）必须遵循标识符规则。系统管理员、系统安全员或数据库所有者可以使用 `sp_changegroup` 将用户指派或重新指派给组。

例如，若要创建 Senior Engineering 组，请在使用要添加该组的数据库时使用此命令：

```
sp_addgroup senioreng
```

`sp_addgroup` 将在当前数据库的 `sysusers` 中添加一行。因此，数据库中的每个组以及每个用户在 `sysusers` 中都有一个条目。

向数据库添加用户

数据库所有者或系统管理员可以使用 `sp_adduser` 向特定数据库中添加用户。但用户必须已经拥有 Adaptive Server 登录帐户。语法为：

```
sp_adduser loginame [, name_in_db [, grpname]]
```

其中：

- *loginame* — 是现有用户的登录名。
- *name_in_db* — 指定一个与登录名不同的名称，将采用该名称在数据库中标识用户。

使用 *name_in_db* 来适应用户的优先选项。例如，如果有五个名为 Mary 的 Adaptive Server 用户，则每个用户都必须有一个不同的登录名。Mary Doe 可能以 “maryd” 登录，而 Mary Jones 以 “maryj” 登录，依此类推。但是，如果这些用户没有使用同一数据库，则每个人可能都希望在特定数据库中只以 “mary” 作为登录名。

如果未提供 *name_in_db* 参数，则数据库中的名称与 *loginame* 相同。

注释 此功能与第 407 页的“在数据库中使用别名”中描述的别名机制不同，后者将一个用户的标识和权限映射到另一个用户的标识和权限。

- *grpname* — 是数据库中现有组的名称。如果不指定组名称，则用户将成为缺省组 “public” 的成员。即使用户是其它组的成员，也仍属于 “public” 组。请参见第 405 页的“更改用户组成员资格”。

sp_adduser 命令将在当前数据库的 **sysusers** 系统表中添加一行。当用户在数据库的 **sysusers** 表中已有一个条目时，用户：

- 可以发出 **use database_name** 命令来访问此数据库
- 将缺省使用此数据库，条件是 **sp_addlogin** 指定了缺省数据库参数
- 可以使用 **sp_modifylogin** 使该数据库成为缺省数据库

该示例显示数据库所有者如何授予已存在的工程组 “eng” 中的 “maryh” 访问权限：

```
sp_adduser maryh, mary, eng
```

下面的示例显示如何授予 “maryd” 访问数据库的权限，并保持其在数据库中的名称与登录名相同：

```
sp_adduser maryd
```

此示例显示如何通过使用 **null** 替代新的用户名，向现有组 “eng” 中添加 “maryj”，并保持其在数据库中的名称与登录名相同：

```
sp_adduser maryj, null, eng
```

可以访问数据库的用户仍需要读取数据、修改数据和使用特定命令的权限。这些权限使用第 17 章“管理用户权限”中讨论的 **grant** 和 **revoke** 命令来授予。

将 “guest” 用户添加到数据库

如果数据库中创建一个名为 “guest” 的用户，就能够使任何拥有 Adaptive Server 帐户的用户作为 **guest** 用户访问该数据库。如果未作为用户或别名用户添加到数据库的用户发出 `use database_name` 命令，Adaptive Server 将查找 **guest** 用户。如果有，就允许用户以 **guest** 用户的权限访问数据库。

数据库所有者可以使用 `sp_adduser` 向数据库的 `sysusers` 表中添加 **guest** 条目：

```
sp_adduser guest
```

可以使用第 399 页的 “删除用户” 中论述的 `sp_dropuser` 删除 **guest** 用户。

如果从 **master** 数据库中删除 **guest** 用户，则尚未添加到任何数据库中的服务器用户将无法登录到 Adaptive Server。

注释 尽管可以有多个用户是数据库的 **guest** 用户，但 Adaptive Server 仍然可以使用用户在服务器内唯一的服务器用户 ID 来审计每个用户的活动。请参见第 18 章 “审计”。

“guest” 用户权限

“**guest**” 继承 “**public**” 的特权。数据库所有者和数据库对象的所有者可以使用 `grant` 和 `revoke` 使 “**guest**” 的特权大于或小于 “**public**” 的特权。请参见第 17 章 “管理用户权限”。

安装 Adaptive Server 时，`master..sysusers` 中包含一个 **guest** 条目。

用户数据库中的 “guest” 用户

在用户数据库中，数据库所有者可添加一个允许所有 Adaptive Server 用户使用该数据库的 **guest** 用户，从而使所有者不必使用 `sp_adduser` 将每个用户显式命名为数据库用户。

在允许访问数据库时，可以利用 **guest** 机制限制对数据库对象的访问。

例如，`titles` 表的所有者可通过执行以下命令，授予除 “**guest**” 外的所有数据库用户对 `titles` 的 `select` 权限：

```
grant select on titles to public
sp_adduser guest
revoke all on titles from guest
```

已安装系统数据库中的“guest”用户

Adaptive Server 使用 guest 用户创建系统 tempdb 数据库和用户创建的临时数据库。“guest”用户自动拥有在 tempdb 中创建的临时对象和其他对象。sybsystemprocs、sybsystemdb 和 sybsyntax 数据库自动包括“guest”用户。

pubs2 和 pubs3 中的“guest”用户

样本数据库中的“guest”用户条目允许新的 Adaptive Server 用户按照《Transac-SQL 用户指南》中的示例进行操作。可授予 guest 用户许多特权，包括：

- 对所有用户表的 select 权限与数据修改权限
- 对所有过程的 execute 权限
- create table、create view、create rule、create default 和 create procedure 权限

将 guest 用户添加到服务器

系统安全员可以使用 sp_addlogin 输入登录名和口令，将指示访问用户使用该登录名和口令。通常只授予这些用户有限的权限。可以指定一个缺省数据库。

警告！ 访问者用户帐户与“guest”用户帐户不是一回事。所有具有访问者帐户的用户均使用相同的服务器用户 ID；因此不能审计单个用户的活动。每个“guest”用户都有一个唯一的服务器 ID，因此可审记个人活动并分清个人责任。Sybase 建议您不要创建一个访问者帐户供多个用户使用，因为这样会无法分清个人责任。

可以使用 sp_login 将名为“guest”的访问者用户帐户添加到 master..syslogins。此“guest”用户帐户优先于系统的“guest”用户帐户。如果用 sp_adduser 添加名为“guest”的访问者用户，则会影响诸如 sybsystemprocs 和 sybsystemdb 等系统数据库，这些数据库需与数据库中的系统“guest”用户配合使用。

添加远程用户

可以通过启用远程访问，允许另一个 Adaptive Server 上的用户执行本地服务器上的存储过程。使用远程服务器的系统管理员身份，您还可以允许服务器上的用户执行对远程服务器的[远程过程调用](#)。

若要启用远程过程调用，您必须对本地服务器和远程服务器均进行重新配置。请参见[第 14 章 “管理远程服务器”](#)。

用户数和登录 ID 数

Adaptive Server 支持每个服务器有超过 2,000,000,000 个登录名，每个数据库有超过 2,000,000,000 个用户。Adaptive Server 可使用负数和正数增加可用 ID 的范围。

ID 号的限制和范围

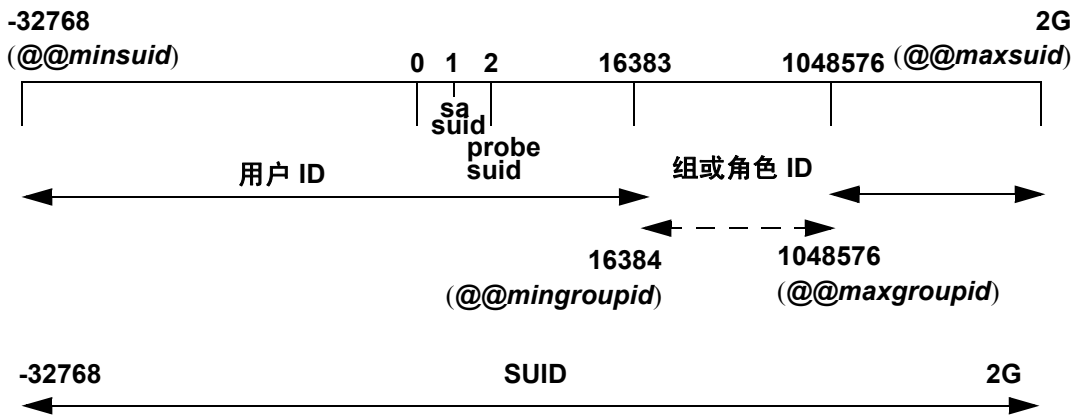
[表 15-2](#) 说明了 ID 类型的有效范围。

表 15-2: ID 类型的范围

ID 类型	服务器限制
每个服务器的登录数 (<i>suid</i>)	2G 加上 32K
每个数据库的用户数 (<i>uid</i>)	2G 减去 1032193
每个数据库的组数或角色数 (<i>gid</i>)	16,384 到 1,048,576

图 15-1 说明了登录名、用户和组的限制和范围。

图 15-1: Adaptive Server 中可用的用户、组和登录名



可以为用户 ID (*uid*) 使用负值。

与 *sysusers* 中一个组或角色关联的服务器用户 ID (*suid*) 不等于其用户 ID (*uid*) 的负值。在 *sysusers* 中，将每个与组或角色相关联的 *suid* 设置为 -2 (*INVALID_SUID*)。

登录连接限制

尽管 Adaptive Server 允许为每个服务器定义超过 2,000,000,000 个登录名，但可以同时连接到 Adaptive Server 的实际用户数受以下因素限制：

- *number of user connections* 配置参数的值和
- 可用于 Adaptive Server 的文件描述符数。每个登录都使用一个文件描述符用于连接。

注释 服务器上运行的最大并发任务数为 32,000。

❖ 允许登录和同时连接的最大值

- 1 为运行 Adaptive Server 的操作系统配置至少 32,000 个文件描述符。
- 2 将 number of user connections 的值至少设置为 32,000。

注释 在 Adaptive Server 可以处理数量超过 64K 的登录和同时连接之前，必须先将操作系统配置为可以使用 64K 以上的文件描述符。有关增加文件描述符数的信息，请参见操作系统文档。

表 15-3 列出了登录、用户和组的服务器限制的全局变量：

表 15-3：登录、用户和组的全局变量

变量名称	显示内容	值
<code>@@invaliduserid</code>	无效用户 ID	-1
<code>@@minuserid</code>	最小的用户 ID	-32768
<code>@@guestuserid</code>	Guest 用户 ID	2
<code>@@mingroupid</code>	最小的组或角色用户 ID	16384
<code>@@maxgroupid</code>	最大的组或角色用户 ID	1048576
<code>@@maxuserid</code>	最大的用户 ID	2147483647
<code>@@minsuid</code>	最小的服务器用户 ID	-32768
<code>@@probesuid</code>	Probe 服务器用户 ID	2
<code>@@maxsuid</code>	最大的服务器用户 ID	2147483647

若要发出全局变量，请输入：

```
select variable_name
```

例如：

```
select @@minuserid
-----
-32768
```

为用户创建和指派角色

添加数据库用户的最后步骤是，为用户指派特定的角色并根据需要授予权限。有关权限的详细信息，请参见第 17 章“管理用户权限”。

Adaptive Server 支持的角色使您可以强化个人责任。Adaptive Server 提供了系统角色（如系统管理员和系统安全员）和由系统安全员创建并授予用户或其他角色的用户定义角色。对象所有者可以为每个角色授予适当的数据库访问权限。

系统定义角色

表 15-4 列出了系统角色、grant role 或 revoke role 命令的 *role_granted* 选项使用的值以及具有此角色的用户通常执行的任务。

表 15-4: 系统角色和相关任务

角色	<i>role_granted</i> 的值	说明
系统管理员	sa_role	管理和维护 Adaptive Server 数据库和磁盘存储
系统安全员	sso_role	执行与安全性相关的任务
操作员	oper_role	备份和装载全服务器范围内的数据库
Sybase 技术支持部门	sybase_ts_role	数据库结构的分析和修复
复制	replication_role	复制用户数据
分布式事务管理器	dtm_tm_role	跨服务器协调事务
高可用性	ha_role	管理和执行故障切换
监控和诊断	mon_role	管理和执行性能及诊断监控
Job Scheduler 管理	js_admin_role	管理 Job Scheduler
Job Scheduler 用户	js_user_role、 js_client_role	通过 Job Scheduler 创建和运行作业
实时消息传送	messaging_role	管理和执行实时消息传送
Web 服务	webservices_role	管理 Web 服务
密钥管理者	keycustodian_role	创建和管理加密密钥

系统管理员特权

系统管理员:

- 处理非特定于应用程序的任务
- 在 Adaptive Server 的自由选择访问控制系统之外操作

通常将系统管理员角色授予个别 Adaptive Server 登录名。该用户执行的所有操作均可根据他 / 她各自的服务器用户 ID 进行跟踪。如果节点上的服务器管理任务由一个人执行, 则可以改用随 Adaptive Server 一起安装的 “sa” 帐户。安装时, “sa” 帐户的用户可充当系统管理员、系统安全员或操作员角色。知道 “sa” 口令的任何用户都可登录到此帐户并充当这些角色中的任何角色或所有角色。

让系统管理员在保护系统之外操作是一种安全预防措施。例如，如果数据库所有者意外删除了 `sysusers` 表中的所有条目，系统管理员可以恢复此表（只要备份存在）。有几个命令只能由系统管理员发出。这些命令包括 `disk init`、`disk refit`、`disk reinit`、`shutdown`、`kill`、`disk mirror`、`mount`、`unmount` 及若干监控命令。

授予权限时，系统管理员被视作对象所有者。如果系统管理员授予操作另一用户的对象的权限，则相应的所有者名称将作为授权者在 `sysprotects` 和 `sp_helprotect` 输出中显示。

系统管理员在登录到数据库时自动充当数据库所有者的身份，并使用所有数据库所有者特权。无论为用户指派了任何别名，都会进行这种自动映射。系统管理员可执行通常为数据库所有者保留的任务，例如 `dbcc` 命令、诊断功能、读取数据页，以及恢复数据或索引。

系统安全员特权

系统安全员在 Adaptive Server 中执行与安全性相关的任务，其中包括：

- 授予系统安全员、操作员和密钥管理者角色
- 管理审计系统
- 更改口令
- 添加新登录名
- 删除登录名
- 锁定和解锁登录帐户
- 创建和授予用户定义的角色
- 管理基于网络的安全性
- 授予 `set proxy` 或 `set session authorization` 命令的使用权限

系统安全员可以访问任何数据库以启用审计，但通常情况下，系统安全员没有针对数据库对象的特殊权限（除了加密密钥和针对加密列的解密权限外。请参见《加密列用户指南》）。不过，`sybsecurity` 数据库除外，因为只有系统安全员才可以访问 `sysaudits` 表。还有几个只能由系统安全员执行的系统过程。

系统安全员可以修复用户对保护系统所进行的任何意外更改。例如，如果数据库所有者忘记了自己的口令，系统安全员可以更改口令，让数据库所有者登录。

系统安全员与系统管理员一起负责登录管理。系统安全员负责添加、锁定和解锁登录名。

系统安全员还可以创建用户定义角色并将相应角色授予用户、其它角色或组。请参见第 387 页的“为用户创建和指派角色”。

操作员特权

授予了操作员角色的用户可以在全服务器范围内备份和恢复数据库，而不必是每个数据库的所有者。操作员角色允许用户对任何数据库使用以下命令：

- dump database
- dump transaction
- load database
- load transaction
- checkpoint
- online database

系统安全员授予操作员角色。

Sybase 技术支持部门

使用技术支持角色，Sybase 技术支持部门的工程师就可以通过跟踪输出、一致性检查和修补数据结构，来显示内部内存结构和磁盘数据结构。此角色用于分析问题和手动恢复数据。解决这些问题所需的某些操作可能需要其它系统角色才能访问。Sybase 建议只有在执行此类分析或修复时，系统安全员才将此角色授予知识渊博的 Sybase 工程师。

“复制”角色

维护 Replication Server 和 ASE Replicator 的用户需要“复制”角色。有关此角色的信息，请参见 Replication Server Administration Guide（《Replication Server 管理指南》）和 ASE Replicator Users Guide（《ASE Replicator 用户指南》）。

分布式事务管理器角色

分布式事务管理器 (DTM) 事务协调器使用此角色允许系统存储过程跨服务器管理事务。使用 DTM XA 接口的客户端需要此角色。请参见 *Using Adaptive Server Distributed Transaction Management Features* (《使用 Adaptive Server 分布式事务管理功能》)。

高可用性角色

必须具有高可用性角色才能将高可用性子系统配置为通过命令和存储过程管理主服务器和协同服务器。请参见 《在高可用性系统中使用 Sybase 故障切换》。

监控和诊断

管理 Adaptive Server 监控表需要此角色。必须具有此角色才能执行监控表远程过程调用和管理监控数据集合。请参见 *Performance and Tuning Series: Monitoring Adaptive Server with sp_sysmon* (《性能和调优系列：用 sp_sysmon 监控 Adaptive Server》)。

Job Scheduler 角色

Job Scheduler 具有三种用于管理其操作权限的系统角色：

- `js_admin_role` — 使用此角色可管理 Job Scheduler、访问存储过程，以及修改、删除和执行 Job Scheduler 管理操作。
- `js_user_role` — 用户需要使用此角色通过 Job Scheduler 存储过程来创建、修改、删除和运行预定作业。
- `js_client_role` — 允许用户使用预定义的作业，但不允许创建或更改作业。

有关详细信息，请参见 《Job Scheduler 用户指南》。

实时消息传送角色

实时消息子系统 (RTMS) 使用此角色执行 `msgsend`、`msgrecv` 和某些 `sp_msgadmin` 命令。有关详细信息，请参见 *Messaging Services User's Guide* (《消息传送服务用户指南》)。

Web 服务角色

Web 服务子系统使用此角色执行 `create service`、`create existing service`、`drop service` 和 `alter service` 命令。请参见《Web 服务用户指南》。

密钥管理者角色

密钥管理者角色负责密钥管理：创建和更改加密密钥、设置系统加密口令、为用户设置密钥副本等。请参见《加密列用户指南》。

用户定义角色

规划用户定义角色

在实现用户定义角色之前，请确定：

- 希望创建的角色
- 每种角色的责任
- 每种角色在角色层次中的位置
- 层次中的哪些角色互斥，如果互斥，是在成员资格级还是在激活级互斥

遵循某种命名约定，以避免在创建用户定义角色时出现名称冲突。例如，可以在角色名中使用 “_role” 后缀。Adaptive Server 不会检查此类限制。

用户定义角色名不能与用户名重名。如果角色必须与用户同名，为了避免冲突，可以创建一个新角色，并将原角色包含在新角色中，然后将这个新角色授予用户。

规划了要创建的角色及各角色之间的成员关系后，请确定如何根据用户的业务要求和责任来分配角色。

每个用户会话用户可激活的最大角色数为 127。

最小角色数 15 包括 Adaptive Server 附带的系统角色。

全服务器范围内可以激活的最大用户定义角色数是 992。前 32 个角色保留给 Sybase 系统角色使用。

创建用户定义角色

使用 `create role` 命令创建一个角色。语法为：

```
create role role_name [with passwd "password"
[, {passwd expiration | min passwd length |
max failed_logins } option_value ]]
```

其中：

- *role_name* — 新角色的名称。
- *password* — 可选口令。必须由使用该角色的任何用户指定。
- *passwd expiration* — 指定口令的有效期（以天为单位）。可以是介于 0 和 32767 之间的任何值（包括 0 和 32767）。
- *min passwd length* — 指定特定角色需要的最短口令长度。
- *max failed_logins* — 指定允许所指定登录名登录失败的尝试次数。
- *option_value* — 指定 *passwd expiration*、*min passwd length* 或 *max failed_logins* 的值。

例如，若要不使用口令创建 `intern_role`，请输入：

```
create role intern_role
```

若要创建 `doctor_role` 并分配口令 “physician”，请输入：

```
create role doctor_role with passwd "physician"
```

只有系统安全员才能创建用户定义角色。

添加和删除角色口令

只有系统安全员才能添加或删除角色的口令。

使用 `alter role` 命令为系统角色或用户定义角色添加或删除口令：

```
alter role role_name
[add passwd password | drop passwd]
```

例如，若要为 `oper_role` 添加口令 “oper8x”，请输入：

```
alter role oper_role add passwd oper8x
```

若要删除角色口令，请输入：

```
alter role oper_role drop passwd
```

角色层次和互斥性

系统安全员可以定义角色层次，以便用户拥有某个角色时，也会拥有层次中较低级别的角色。例如，“chief_financial_officer”角色可以包含“financial_analyst”和“salary_administrator”两个角色。

首席财务官可以执行所有任务，并查看工资管理员和财务分析员可以查看的所有数据。

此外，可以定义角色的互斥性，以强制实施职责的静态或动态分离策略。在以下情形时可以将角色定义为互斥：

- 成员资格 — 一个用户不能被授予两个不同的角色。例如，您也许不希望将“payment_requestor”和“payment_approver”这两个角色授予同一用户。
- 激活 — 一个用户不能激活（或启用）两个不同的角色。例如，用户可被授予“senior_auditor”和“equipment_buyer”角色，但不允许同时启用这两个角色。

系统角色和用户定义角色既可以按角色层次定义，也可以定义为互斥角色。例如，您可能希望有一个“super_user”角色包含系统管理员角色、操作员角色和技术支持部门角色。若要强制实施角色分离，您可能希望将系统管理员和系统安全员角色定义为在成员资格级互斥；即一个用户不能被同时授予这两个角色。

角色层次和互斥性

本节介绍如何设置角色层次和强制实施角色分离。

定义和更改角色互斥性

若要定义两个角色间的互斥性，请使用：

```
alter role role1 { add | drop } exclusive { membership | activation } role2
```

例如，若要定义 intern_role 和 specialist_role 在成员资格级互斥，请输入：

```
alter role intern_role add exclusive membership
specialist_role
```

上面的示例限制在 intern_role 中具有成员资格的用户同时成为 specialist_role 的成员。

若要将 sso_role 和 sa_role 定义为在激活级别互斥，请输入以下命令，该命令禁止作为 sso_role 和 sa_role 成员的用户同时充当这两个角色：

```
alter role sso_role add exclusive activation sa_role
```

定义和更改角色层次

定义角色层次包括选择层次类型和角色，然后通过为其它角色授予角色来设计层次。

例如：

```
grant role intern_role to specialist_role
grant role doctor_role to specialist_role
```

这会为 “specialist” 授予 “doctor” 和 “intern” 的所有特权。

若要建立一个层次，其中的 “super_user” 角色包括 sa_role 和 oper_role 系统角色，请指定：

```
grant role sa_role to super_user
grant role oper_role to super_user
```

注释 如果某个角色要求口令包含在其它角色中，则具有该角色（包含其它角色）的用户不必使用已包含角色的口令。例如，在上例中，假定 “doctor” 角色通常需要口令。具有 “specialist” 角色的用户不必输入 “doctor” 口令，因为 “doctor” 已包含在 “specialist” 中。只有最高级别的角色需要角色口令。

创建角色层次时：

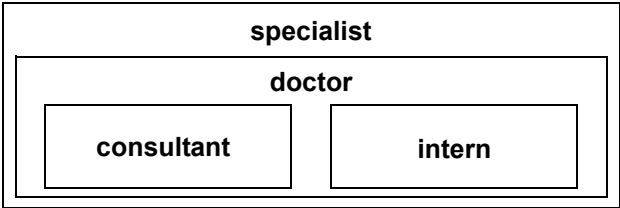
- 不能将一个角色授予直接包含该角色的角色。这样可以防止重名。
在上例中，由于 “specialist” 已经包含 “doctor”，因此不能将 “doctor” 授予 “specialist”。
- 可以将一个角色授予不是直接包含该角色的另一个角色。

例如，在图 15-2 中，即使 “specialist” 角色已经包含 “doctor” 角色，而 “doctor” 角色包含 “intern”，也可以将 “intern” 角色授予 “specialist” 角色。如果随后从 “specialist” 中删除了 “doctor”，则 “specialist” 仍包含 “intern”。

在图 15-2 中，由于已将 “consultant” 授予 “doctor”，因此 “doctor” 具有 “consultant” 角色权限。“specialist” 角色也具有 “consultant” 角色权限，这是因为 “specialist” 包含 “doctor” 角色，而 “doctor” 角色又包含 “consultant”。

但 “intern” 没有 “consultant” 角色的特权，这是因为 “intern” 不包含 “consultant” 角色（不论是直接还是间接的）。

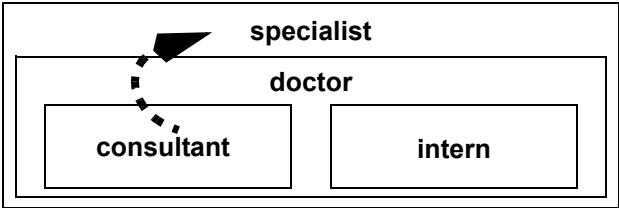
图 15-2：显式或隐式授予的特权



- 不能将一个角色授予该角色包含的另外一个角色。这可防止在角色层次中出现“连环套”。

例如，在图 15-3 中，不能将“specialist”角色授予“consultant”角色；“consultant”已包含在“specialist”中。

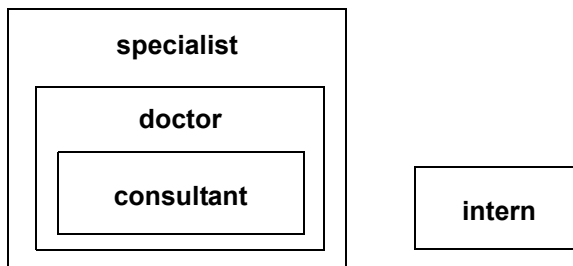
图 15-3：将角色授予授权者包含的角色
不允许



- 当系统安全员为用户授予一个包含其它角色的角色时，该用户将隐式获得该角色包含的所有角色的成员资格。但是，只有当用户在角色中拥有显式成员资格时，才能直接激活或停用该角色。
- 系统安全员不能将一个角色授予另一个在成员资格级显式或隐式与该角色互斥的角色。

例如，在图 15-4 中，如果将“intern”角色定义为在成员资格级与“consultant”角色互斥，则系统安全员不可将“intern”授予“doctor”。

图 15-4: 成员资格级的互斥性



- 用户只能直接激活或停用被授予的角色。

例如，在图 15-4 所示的层次中，假定已经授予您 “specialist” 角色。您拥有 “specialist” 角色的所有权限，并且因为层次关系，您还隐式地拥有 “doctor” 和 “consultant” 角色的所有权限。然而，您只可激活 “specialist” 角色。您不能激活 “doctor” 或 “consultant” 角色，这是因为并没有直接将它们授予您。请参见第 398 页的“激活和停用角色”。

从其它角色撤消角色与将角色授予其它角色类似。此操作删除了包含关系，且包含关系必须是直接包含。

例如：

- 如果系统安全员从 “specialist” 撤消 “doctor” 角色，则 “specialist” 不再包含 “consultant” 角色或 “intern” 角色。
- 系统安全员不能从 “specialist” 撤消 “intern” 角色，这是因为 “intern” 没有直接包含在 “specialist” 中。

设置登录时的缺省激活角色

系统安全员可以更改任何用户的缺省角色。单个用户只能更改自己的缺省设置。

当用户登录到 Adaptive Server 时，其角色不一定处于活动状态，具体取决于将该角色设置为缺省角色的方式。如果该角色带有关联的口令，用户必须使用 `set role` 命令激活该角色。

系统安全员或用户可以决定在缺省情况下，是否在登录时激活任何被授予的角色。`sp_modifylogin` 命令为每个用户单独设置用户角色的缺省状态。`sp_modifylogin` 只影响用户角色，不影响系统角色。

缺省情况下，授予的用户定义角色在登录时不激活，而授予的系统角色如果不带有与其关联的口令，则将自动激活。

若要将角色设置为在登录时激活：

```
sp_modifylogin loginname, "add default role", role_name
```

若要将多个缺省角色指派给用户，请使用多个 `sp_modifylogin` 命令。

若要确保角色在登录时停用：

```
sp_modifylogin loginname, "drop default role", role_name
```

例如，若要将 Ralph 的 `intern_role` 缺省设置更改为在登录时自动激活，请执行：

```
sp_modifylogin ralph, "add default role", intern_role
```

激活和停用角色

角色必须激活才拥有每个角色的访问特权。缺省角色在登录时不能激活。如果角色带有口令，则在登录时始终不会激活该角色。

立即激活或停用角色：

```
set role role_name [on|off]
```

若要激活或停用一个带有口令的角色，请使用：

```
set role role_name with passwd "password" [on|off]
```

例如，若要用口令 “sailing19” 激活 “financial_analyst” 角色，请输入：

```
set role financial_analyst with passwd "sailing19" on
```

仅在需要时激活角色，并在不需要时关闭角色。例如，当 `sa_role` 激活时，用户将在任何所使用的数据库中承担数据库所有者的职责。若要关闭系统管理员角色并使用 “真实” 的用户标识，请使用：

```
set role sa_role off
```

如果在会话中被授予一个角色，并希望立即激活此角色，可使用 `set role` 命令启用该角色。

设置组和添加用户

系统安全员、系统管理员或数据库管理员使用 `sp_addgroup group_name` 来创建组。

可以在组级授予和撤消权限。组权限将自动传递到组成员。每个数据库在创建后都有一个名为 “public” 的组，所有用户均将自动从属于该组。使用 `sp_adduser` 向组中添加用户，并使用 `sp_changegroup` 更改用户所在的组。请参见第 405 页的 “更改用户组成员资格”。

组由 `sysusers` 表中的一个条目表示。您不能使用相同的名称在数据库中创建组和用户（例如，不能将某个组和用户同时命名为 “shirley”）。

删除用户、组和用户定义角色

系统管理员、系统安全员或数据库所有者可以使用 `sp_dropuser` 或 `sp_dropgroup` 从数据库中删除用户和组。

删除用户

数据库所有者、系统安全员或系统管理员可以使用 `sp_dropuser`，拒绝 Adaptive Server 用户访问执行 `sp_dropuser` 的数据库。（如果在此数据库中定义了 “guest” 用户，则该用户仍可以作为 “guest” 访问该数据库。）

以下是语法，其中 `name_in_db` 通常是登录名，除非使用 `sp_adduser` 指派了另一个名称：

```
sp_dropuser name_in_db
```

不能删除拥有对象的用户。由于没有用来转移对象所有权的命令，因此在删除用户之前，必须先删除用户所拥有的对象。若要拒绝对拥有对象的用户进行访问，请使用 `sp_locklogin` 锁定其帐户。

也不能删除已授予其他用户权限的用户。可使用 `revoke with cascade` 命令先撤消所有由要删除的用户授予了权限的用户的权限，然后删除该用户。如果需要，必须再次为这些用户授予权限。

删除组

系统安全员、系统管理员或数据库管理员使用 `sp_dropgroup` 来删除组。语法为：

```
sp_dropgroup grpname
```

不能删除包含成员的组。如果试图这样做，错误报告将显示试图删除的组中的成员列表。若要从组中删除用户，请使用[第 405 页的“更改用户组成员资格”](#)中讨论的 `sp_changegroup`。

删除用户定义角色

为了删除角色，系统安全员将使用以下语法，其中 `role_name` 是用户定义角色的名称：

```
drop role role_name [with override]
```

`with override` 可撤消在每个数据库服务器范围内授予角色的所有访问特权。

如果不使用 `override` 选项，您必须撤消在所有数据库中授予角色的所有特权，然后才能删除该角色。如果没有这样做，删除命令将失败。若要撤消特权，请使用 `revoke` 命令

删除角色前不必先删除成员资格。删除一个角色将自动删除具有此角色的任何用户的成员资格，无论是否使用了 `with override` 选项。

锁定或删除 Adaptive Server 登录帐户

若要防止某个用户登录到 Adaptive Server，可以锁定或删除其 Adaptive Server 登录帐户。锁定登录帐户可以保留 `suid` 以使其无法重新使用。

警告！ Adaptive Server 可能在创建下一个登录帐户时重新使用已删除的登录帐户的服务器用户 ID (`suid`)。这种情况只有在所删除的登录帐户持有 `syslogins` 中最大的 `suid` 的情况下才会出现；不过，如果不对 `sp_droplogin` 的执行情况进行审计，则会造成无法分清责任。此外，带有重新使用的 `suid` 的用户有可能可以访问授权给旧 `suid` 的数据库对象。

不能在以下情况下删除登录：

- 用户位于任何数据库中。
- 登录是最后一个保留下来的用户，该用户拥有系统安全员或系统管理员角色。

系统安全员可以使用 `sp_locklogin` 或 `sp_droplogin` 锁定或删除登录。如果为复制记录了系统过程，则系统安全员在发出命令时必须位于主数据库中。

锁定和解锁登录帐户

使用 `sp_locklogin` 锁定和解锁帐户或显示锁定帐户的列表。您必须是系统安全员才能使用 `sp_locklogin`。

语法为：

```
sp_locklogin [ {login_name | "all"}, { "lock" | "unlock" } ]
```

其中：

- *login_name* 是要锁定或解锁的帐户的名称。登录名必须是一个已存在的有效帐户。
- **all** 表示锁定或解锁 Adaptive Server 上的所有登录帐户，具有 **sa_role** 的帐户除外。
- **lock | unlock** 指定是否要锁定或解锁帐户。

若要显示所有锁定登录的列表，请使用不带参数的 `sp_locklogin`。

可以锁定当前登录的帐户，但用户在注销之前不会受帐户锁定的影响。可以锁定数据库所有者的帐户，并且锁定的帐户也可以拥有数据库中的对象。此外，可以使用 `sp_changedbowner`，将某个锁定帐户指定为数据库所有者。

Adaptive Server 确保至少总是有一个未锁定的系统安全员帐户和一个未锁定的系统管理员帐户。

删除登录帐户

系统安全员可以使用 `sp_droplogin` 拒绝用户访问 Adaptive Server。语法为：

```
sp_droplogin login_name
```

如果 `login_name` 标识的用户在任何数据库中以数据库用户或别名的形式存在，则 `sp_droplogin` 将失败。使用 `sp_dropuser` 删除某个数据库的用户。请参见第 399 页的“删除用户”。

锁定拥有阈值的登录名

本节讨论阈值及其如何受锁定的用户登录影响。

- 作为一项安全性措施，可使用帐户名和创建此过程的登录角色来执行阈值存储过程。
 - 不能删除拥有阈值的用户登录。
 - 如果锁定拥有阈值的用户登录，则用户不能执行存储过程。
- 最后机会阈值和使用“sa”登录创建的阈值不受 `sp_locklogin` 影响。如果锁定“sa”登录，则由“sa”用户创建或修改的最后机会阈值仍会引发。

更改用户信息

表 15-5 列出了可用于更改口令、缺省数据库、缺省语言、全名或组指派的系统过程。

表 15-5：用于更改用户信息的系统过程

任务	要求的角色	系统过程	数据库
更改用户口令	无	sp_password	任何数据库
更改其他用户的口令	系统安全员	sp_password	任何数据库
更改鉴定机制	系统安全员	sp_modifylogin	任何数据库
更改缺省数据库、缺省语言或全名	无	sp_modifylogin	任何数据库
更改登录帐户的缺省数据库、缺省语言或全名	系统管理员或系统安全员	sp_modifylogin	任何数据库
更改用户的组指派	系统管理员、数据库所有者或系统安全员	sp_changegroup	用户数据库

更改口令

所有用户都使用 `sp_password` 随时更改其口令。系统安全员可以使用 `sp_password` 更改任何用户的口令。

请参见《参考手册：过程》了解 `sp_password` 语法。

例如，一个用户可以使用以下命令将其口令从 “3blindmice” 更改为 “2mediumhot”：

```
sp_password "3blindmice", "2mediumhot"
```

因为这些口令是以数字开始，所以都用双引号引起来。

在下面的示例中，系统安全员的口令是 “2tomato”，系统安全员将 Victoria 的口令更改为 “sesame1”：

```
sp_password "2tomato", sesame1, victoria
```

要求新口令

可以选择使用 `systemwide password expiration` 配置参数设定口令有效期，这将强制所有 Adaptive Server 用户定期更改口令。请参见第 5 章 “[设置配置参数](#)” 即使不使用 `systemwide password expiration`，但出于安全原因，用户定期更改口令也是非常重要的。

口令策略设置取代该配置参数。

`password expiration interval` 指定口令的有效期（以天为单位）。可以是介于 0 和 32767 之间的任何值（包括 0 和 32767）。例如，如果您在 2007 年 8 月 1 日上午 10:30 创建一个新登录名，其口令有效期为 30 天，那么该口令将在 2007 年 8 月 31 日上午 10:30 过期。

`syslogins` 表中的 `pwdate` 列记录上次更改口令的日期。下面的查询选择自 2007 年 9 月 15 日以来口令未更改的所有登录名：

```
select name, pwdate
from syslogins
where pwdate < "Sep 15 2007"
```

空口令

不要指定一个空口令。安装了 Adaptive Server 之后，缺省 “sa” 帐户具有一个空口令。下面的示例显示如何将空口令更改为一个有效口令：

```
sp_password null, "8M4LNCH"
```

注释 在语句中不要将 “null” 用引号引起。

丢失口令后登录

如果您的站点遇到以下任意情况，您可以使用 `dataserver -plogin_name`:

- 所有系统管理员登录帐户均被锁定。
- 所有系统安全员登录帐户均被锁定。
- `sa_role` 或 `sso_role` 的口令已丢失。

利用带 `-p` 参数的 `dataserver` 参数，您可以为这些帐户和角色设置新口令。`login_name` 是必须为其重置口令的用户或角色（`sa_role` 或 `sso_role`）的名称。

使用 `-p` 参数启动时，Adaptive Server 会生成一个随机口令，接着显示并加密该口令，然后将其作为该帐户或角色的新口令保存在 `master.syslogins` 或 `master.syssrvroles` 中。

Sybase 强烈建议您在重新启动服务器时更改口令。例如，要为具有 `sa_role` 的用户 `rsmith` 重新设置口令，请输入：

```
dataserver -prsmith
```

重置 `sso_role` 的口令：

```
dataserver -psso_role
```

更改用户缺省值

任何用户都可使用 `sp_modifylogin` 更改其全名、缺省鉴定方法、缺省数据库、缺省语言和缺省角色。使用 `sp_modifylogin` 来设置口令长度和有效期、限制失败登录尝试次数，以及指定登录脚本在用户登录时自动运行。系统管理员可为任何用户更改这些设置。语法为：

```
sp_modifylogin login_name, option, value
```

其中：

- `login_name` — 是要修改其帐户的用户的名称。
- `option` — 指定所更改的选项。有关可用选项的列表，请参见《参考手册：过程》中的 `sp_modifylogin`。
- `value` — 是指定选项的新值。

执行 `sp_modifylogin` 命令更改缺省数据库后，用户将在下次登录时连接到新的缺省数据库。但 `sp_modifylogin` 不会自动授予用户访问此数据库的权限。除非数据库所有者使用 `sp_adduser`、`sp_addalias` 或 `guest` 用户机制设置访问权限，否则即使其缺省数据库已经更改，用户也将被连接到 `master` 数据库。

此示例将 “anna” 的缺省数据库更改为 pubs2:

```
sp_modifylogin anna, defdb, pubs2
```

此示例将 “claire” 的缺省语言更改为法语:

```
sp_modifylogin claire, deflanguage, french
```

此示例将 “mtwain” 的全名更改为 “Samuel Clemens”。

```
sp_modifylogin mtwain, fullname, "Samuel Clemens"
```

更改用户组成员资格

系统管理员、系统安全员或数据库所有者可以使用 `sp_changegroup` 更改用户的组从属关系。每个用户都可以只从属于一个不是 “public” 的组，但所有用户通常都是 “public” 的成员。

在执行 `sp_changegroup` 之前:

- 组必须存在。
- 用户必须有访问当前数据库的权限（必须在 `sysusers` 中列出）。

`sp_changegroup` 的语法为:

```
sp_changegroup grpname, username
```

例如，若要将用户 “jim” 从当前组更改到 “management” 组，请使用:

```
sp_changegroup management, jim
```

若要从组中删除一个用户而不将其指派到另一组，必须将其组的从属关系更改为 “public”:

```
sp_changegroup "public", jim
```

名称 “public” 必须用双引号引起，因为它是一个保留字。此命令将 Jim 的组从属关系简化为只属于 “public”。

当某个用户从一个组更改到另一个组时，该用户将失去在旧组中拥有的所有权限，而获得向新组授予的权限。

可随时更改用户的组指派。

更改用户进程信息

`set` 命令包括的选项可为每个客户端指派各自的名称、主机名和应用程序名。在一个系统中，当多个客户端使用相同的名称、主机名或应用程序名与 Adaptive Server 连接时，该命令对区别这些客户端很有用。

`set` 命令的部分语法是：

```
set [clientname client_name | clienthostname host_name |  
clientappliance application_name]
```

其中 *client_name* 是指派给客户端的名称，*host_name* 是客户端所连接主机的名称，而 *application_name* 是连接到 Adaptive Server 的应用程序。这些参数存储在 `sysprocesses` 表的 `clientname`、`clienthostname` 和 `clientappliance` 列中。

例如，如果用户以 “client1” 登录到 Adaptive Server，则可以使用类似下面的命令为其指派客户端名、主机名和应用程序名：

```
set clientname 'alison'  
set clienthostname 'money1'  
set clientappliance 'webserver2'
```

此用户此时作为用户 “alison” 从主机 “money1” 登录并使用 “webserver2” 应用程序，显示在 `sysprocesses` 表中。然而，尽管新名称出现在 `sysprocesses` 中，但它们并没有用于权限检查，且 `sp_who` 仍将客户端连接显示为属于初始登录（在上述情况中为 `client1`）。`set clientname` 不执行与 `set proxy` 相同的功能，后者允许用户使用另一个用户的权限、登录名和 `suid`。

可以为唯一当前客户端会话设置客户端名、主机名或应用程序名（尽管可以查看任何客户端连接的连接信息）。此外，此信息在用户注销时将丢失。每次用户登录时，这些参数必须都要重新指定。例如，用户 “alison” 不能为任何其它客户端连接设置客户端名、主机名或应用程序名。

使用客户端的系统进程 ID 可以查看其连接信息。例如，如果上面提到的用户 “alison” 使用 `spid` 13 进行连接，则发出下面的命令可查看此用户的所有连接信息：

```
select * from sysprocesses where spid = 13
```

若要查看当前客户端连接的连接信息（例如，如果用户 “alison” 要查看自己的连接信息），请输入：

```
select * from sysprocesses where spid = @@spid
```

在数据库中使用别名

别名机制允许在数据库中把两个或多个用户当作同一用户对待，因此所有这些用户都具有相同的特权。此机制经常用于使多个用户充当数据库所有者的角色。数据库所有者可以使用 `setuser` 命令模拟数据库中的另一个用户。也可以使用别名机制设置一个集合用户标识。

例如，假设有几个副总裁要以相同的特权和所有权使用同一个数据库。如果将登录“vp”添加到 Adaptive Server 和数据库中，并且让每个副总裁都以“vp”登录时，则无法区分各个用户。反之，若为每个副总裁指定一个数据库用户名“vp”的别名，每个人都可以有自己的 Adaptive Server 帐户。

注释 尽管在一个数据库中可能有多人使用别名，但仍可通过审计每个用户所执行的数据库操作来维护个人责任。请参见第 18 章“审计”。

使用别名过程中的集合用户标识意味着数据库对象的集合所有权。例如，如果用户“loginA”在数据库 db1 中的别名为 dbo，则“loginA”在 db1 中创建的所有对象由 dbo 拥有。但是，Adaptive Server 将按照登录名和创建者的数据库用户 ID 具体地记录对象的所有权。请参见第 520 页的“具体标识”。如果别名具体地拥有数据库中的任何对象，则不能将其从该数据库删除。

注释 如果某个登录在数据库中创建了对象，则不能删除该登录的别名。在大多数情况下，只对不拥有表、过程、视图或触发器的用户使用别名。

添加别名

若要为用户添加别名，请使用 `sp_addalias`：

```
sp_addalias loginame, name_in_db
```

其中：

- *loginame* — 是在当前数据库中需要别名的用户的名称。此用户必须在 Adaptive Server 中有一个帐户且不能是当前数据库的用户。
- *name_in_db* — 是数据库用户的名称，由 *loginame* 指定的用户将被链接到此数据库用户。*name_in_db* 必须存在于当前数据库的 `sysusers` 中。

执行 `sp_addalias` 可将由 *loginame* 指定的用户名映射到由 *name_in_db* 指定的用户名。此功能是通过在系统表 `sysalternates` 中添加一行实现的。

用户试图使用数据库时， Adaptive Server 将在 *sysusers* 中检查用户的服务器用户 ID 号 (*suid*)。如果未发现， Adaptive Server 随后将检查 *sysalternates*。如果在此发现用户的 *suid*，并且它已被映射到数据库用户的 *suid*，则第一个用户在使用数据库时将被看作是第二个用户。

例如，假定 Mary 拥有一个数据库。她希望允许 Jane 和 Sarah 都可以使用此数据库，就像他们是数据库所有者一样。Jane 和 Sarah 在 Adaptive Server 上有相应的登录名，但未获授权使用 Mary 的数据库。Mary 执行以下命令：

```
sp_addalias jane, dbo
exec sp_addalias sarah, dbo
```

警告！ 对于讨论中的数据库，具有数据库所有者别名的用户拥有所有权限，并可执行可由数据库所有者执行的所有操作。数据库所有者应仔细考虑授予其他用户数据库全部访问权限可能带来的后果。

删除别名

使用 *sp_dropalias* 可删除替代 *suid* 与用户 ID 的映射关系。此操作将从 *sysalternates* 中删除相应的行。语法如下，其中 *loginame* 是在使用 *sp_addalias* 映射用户名称时由 *loginame* 指定的名称：

```
sp_dropalias loginame
```

用户的别名被删除后，该用户不再具有访问数据库的权限。

如果别名登录创建了任何对象或阈值，则不能删除此别名。在使用 *sp_dropalias* 删除已经执行这些操作的别名之前，删除对象或过程。如果删除别名以后仍然要使用它们，应使用不同的所有者来重新创建它们。

获取有关别名的信息

若要显示有关别名的信息，请使用 *sp_helpuser*。例如，若要找到 “dbo” 的别名，请执行：

```
sp_helpuser dbo

Users_name      ID_in_db      Group_name      Login_name
-----
dbo             1             public         sa

(1 row affected)
```

```
Users aliased to user.  
Login_name  
-----  
andy  
christa  
howard  
linda
```

获取有关用户的信息

表 15-6 列出了可以用于获取用户、组和当前 Adaptive Server 使用状况相关信息的过程。

表 15-6：报告有关 Adaptive Server 用户和组的信息

任务	过程
报告当前的 Adaptive Server 用户和进程	sp_who
显示有关登录帐户的信息	sp_displaylogin
报告数据库中的用户和别名	sp_helpuser
报告数据库中的组	sp_helpgroup

有关用户和进程的报告

使用 sp_who 报告有关 Adaptive Server 上当前用户和进程的信息：

```
sp_who [loginame | "spid"]
```

其中：

- *loginame* — 是用户的 Adaptive Server 登录名。如果您提供登录名，则 sp_who 报告有关此用户正在运行的进程的信息。
- *spid* — 是特定进程的编号。

对于每个进程运行，sp_who 会报告服务器进程 ID 的安全相关信息、其状态、进程用户的登录名、真实的登录名（如果 *login_name* 为别名）、主机计算机的名称、阻塞此进程的进程（如果存在）的服务器进程 ID、数据库名和正在运行的命令。

如果不提供登录名或 *spid*，sp_who 将报告所有用户正在运行的进程。

下面的示例显示了执行未带参数的 `sp_who` 命令的安全相关结果：

spid	status	loginame	origname	hostname	blk	dbname	cmd
1	running	sa	sa	sunbird	0	pubs2	SELECT
2	sleeping	NULL	NULL		0	master	NETWORK HANDLER
3	sleeping	NULL	NULL		0	master	MIRROR HANDLER
4	sleeping	NULL	NULL		0	master	AUDIT PROCESS
5	sleeping	NULL	NULL		0	master	CHECKPOINT SLEEP

(5 rows affected, return status = 0)

`sp_who` 将所有系统进程的 `loginame` 报告为 NULL。

获取有关登录帐户的信息

使用 `sp_displaylogin` 可显示有关指定登录帐户或与通配符模式匹配的登录名（包括授予此帐户的任何角色）的信息，其中 `loginame`（或通配符匹配模式）是要获取其有关信息的用户登录名模式：

`sp_displaylogin [loginame | wildcard]`

如果您不是系统安全员或系统管理员，则只能显示有关自己的帐户的信息。如果是系统安全员或系统管理员，则可以使用 `loginame | wildcard` 参数访问有关任何帐户的信息。

`sp_displaylogin` 显示您的服务器用户 ID、登录名、全名、授予您的任何角色、上次更改口令的日期、缺省数据库、缺省语言、帐户是否被锁定、任何自动登录脚本、口令有效期、口令是否已经到期、使用的登录口令加密版本，以及为登录指定的鉴定机制。

`sp_displaylogin` 显示授予用户的所有角色，因此，即使使用 `set` 命令使某个角色失效时，此角色也将出现。例如，此示例显示 `sa` 的角色：

```
sp_displaylogin 'sa'

Suid: 121
Loginame: mylogin
Fullname:
Default Database: master
Default Language:
Auto Login Script:
Configured Authorization:
    sa_role (default ON)
    sso_role (default ON)
    oper_role (default ON)
    sybase_ts_role (default ON)
```

```

Locked: NO
Date of Last Password Change: Aug 10 2006 11:17AM
Password expiration interval: 0
Password expired: NO
Minimum password length: 6
Maximum failed logins: 0
Current failed login attempts:
Authenticate with: NONE
Login password encryption: SYB-PROP, SHA-256
Last login date : Aug 17 2006 5: 55PM
(return status = 0)

```

获取有关数据库用户的信息

使用 `sp_helpuser` 可报告有关当前数据库的授权用户的信息，其中 `name_in_db` 是当前数据库中的用户名：

```
sp_helpuser [name_in_db]
```

如果您提供用户名，则 `sp_helpuser` 将报告有关该用户的信息。如果不提供名称，此命令报告所有用户的有关信息。

下面的示例显示在 `pubs2` 数据库中不带参数执行 `sp_helpuser` 的结果：

```

sp_helpuser
Users_name  ID_in_db  Group_name Login_name
-----
dbo         1         public    sa
marcy       4         public    marcy
sandy       3         public    sandy
judy        5         public    judy
linda       6         public    linda
anne        2         public    anne
jim         7         senioreng jim

```

查找用户名和 ID

若要查找用户的服务器用户 ID 或登录名，请使用 `suser_id` 和 `suser_name`。

表 15-7: 系统函数 `suser_id` 和 `suser_name`

查找	使用	参数
服务器用户 ID	<code>suser_id</code>	<code>(["server_user_name"])</code>
服务器用户名（登录名）	<code>suser_name</code>	<code>([server_user_ID])</code>

这些系统函数的参数都是可选的。如果不提供参数，则 Adaptive Server 显示有关当前用户的信息。

下面的示例显示了如何查找用户 “sandy” 的服务器用户 ID:

```
select suser_id("sandy")
-----
3
```

下面的示例显示登录名为 “mary” 的系统管理员如何发出不带参数的命令:

```
select suser_name(), suser_id()
-----
mary                                     4
```

若要在数据库内查找用户的 ID 号或名称，请使用 `user_id` 和 `user_name`。

表 15-8: 系统函数 `user_id` 和 `user_name`

查找	使用	参数
用户 ID	<code>user_id</code>	<code>(["db_user_name"])</code>
用户名	<code>user_name</code>	<code>([db_user_ID])</code>

这些函数的参数都是可选的。如果不提供参数，则 Adaptive Server 显示有关当前用户的信息。例如:

```
select user_name(10)
-----
NULL
(1 row affected)

select user_name( )
-----
dbo
(1 row affected)

select user_id("joe")
-----
NULL
(1 row affected)
```


显示有关角色的信息

表 15-9 列出了要用于查找有关角色的信息的系统过程和函数。

表 15-9: 查找有关角色的信息

显示有关信息	使用	请参见
角色名的角色 ID	<code>role_id</code> 系统函数	第 413 页的“查找角色 ID 和名称”
角色 ID 的角色名	<code>role_name</code> 系统函数	第 413 页的“查找角色 ID 和名称”
系统角色	<code>show_role</code> 系统函数	第 413 页的“查看活动的系统角色”
角色层次和授予用户的角色	<code>sp_displayroles</code> 系统过程	第 414 页的“显示角色层次”
角色在角色层次中是否包含其它角色	<code>role_contain</code> 系统函数	第 414 页的“查看层次中的用户角色”
两个角色是否为互斥	<code>mut_excl_roles</code> 系统函数	第 414 页的“确定互斥性”
为当前会话激活的角色	<code>sp_activeroles</code> 系统过程	第 414 页的“确定角色激活”
是否已激活正确角色以执行过程	<code>proc_role</code> 系统函数	第 415 页的“检查存储过程中的角色”
登录（包括授予的角色）	<code>sp_displaylogin</code> 系统过程	第 410 页的“获取有关登录帐户的信息”
用户、组或角色权限	<code>sp_helprotect</code> 系统过程	第 541 页的“权限报告”

查找角色 ID 和名称

在已知角色名时查找角色 ID:

```
role_id(role_name)
```

任何用户都可以执行 `role_id`。如果角色有效，则 `role_id` 返回角色在全服务器范围内的 ID (`srid`)。`sysssrvroles` 系统表包含一个含有角色 ID 的 `srid` 列和一个含有角色名的 `name` 列。如果角色无效，则 `role_id` 返回 NULL。

若要在已知角色 ID 时查找角色名，请使用 `role_name`:

```
role_name(role_id)
```

任何用户都可以执行 `role_name`。

查看活动的系统角色

使用 `show_role` 为指定登录显示当前活动的系统角色:

```
show_role()
```

如果没有激活任何系统角色，则 `show_role` 返回 NULL。如果用户是数据库所有者，并且在使用 `setuser` 模拟其他用户后执行 `show_role`，则 `show_role` 返回用户自己的活动系统角色，而不是所模拟用户的角色。

任何用户都可以执行 `show_role`。

注释 `show_role` 函数不提供有关用户定义角色的信息。

显示角色层次

您可以使用 `sp_displayroles` 查看授予您的登录名的所有角色，或查看以表格格式显示的整个角色层次树：

```
sp_displayroles {login_name | rolename [, expand_up | expand_down]}
```

任何用户都可以执行 `sp_displayroles` 来查看自己的角色。只有系统安全员可以查看有关授予其他用户的角色信息。

查看层次中的用户角色

可以使用 `role_contain` 确定任何指定角色是否包括其它指定角色：

```
role_contain (["role1", "role2"])
```

如果 `role2` 包含 `role1`，则 `role_contain` 返回 1。

任何用户都可以执行 `role_contain`。

确定互斥性

可以使用 `mut_excl_roles` 函数，确定为用户指派的任意两个角色是否互斥以及它们的互斥级别：

```
mut_excl_roles(role1, role2, {membership | activation})
```

任何用户都可以执行 `mut_excl_roles`。如果指定的角色或任何被指定角色包含的角色是互斥的，则 `mut_excl_roles` 返回 1；如果角色不互斥，则 `mut_excl_roles` 返回 0。

确定角色激活

若要查找 Adaptive Server 的当前登录会话的所有活动角色，请使用：

```
sp_activeroles [expand_down]
```

`expand_down` 显示任何授予用户的角色所包含的所有角色的层次。

任何用户都可以执行 `sp_activeroles`。

检查存储过程中的角色

可以在存储过程中使用 `proc_role` 来保证仅具有特定角色的用户可以执行此过程。只有 `proc_role` 可提供一种可靠方法，帮助防止对特定存储过程的不适当访问。

可以使用 `grant execute`，授予所有被授予指定角色的用户执行存储过程的权限。类似地，可使用 `revoke execute` 撤消这种权限。

然而，`grant execute` 权限不会阻止为没有指定角色的用户授予存储过程的执行权限。例如，若要确保绝不会为不是系统管理员的所有用户授予执行存储过程的权限，请在存储过程本身内使用 `proc_role`，检查调用用户是否有执行该过程的正确角色。

`proc_role` 为所需角色带一个字符串并在调用者拥有它时返回 1，否则返回 0。

例如，下面是一个使用 `proc_role` 来查看用户是否有 `sa_role` 角色的过程：

```
create proc test_proc
as
if (proc_role("sa_role") = 0)
begin
    print "You don't have the right role"
    return -1
end
else
    print "You have System Administrator role"
    return 0
```

建立口令和登录策略

Adaptive Server 包括几个控件，可用来设置登录、角色和口令的策略以进行内部鉴定。

在 Adaptive Server 中，系统安全员可以：

- 指定在某个登录名或角色被自动锁定前，为该登录名或角色键入无效口令的最大允许次数
- 在丢失口令后登录
- 手动记录和解锁登录名和角色
- 显示登录口令信息

- 指定服务器范围或特定登录或角色所需的 `minimum password length`。
- 检查登录名的口令复杂程度
- 启用登录名的自定义口令检查
- 设置口令有效期
- 保护磁盘上和内存中存储的登录口令
- 仅使用 SHA-256 算法将口令存储在磁盘上
- 考虑登录口令字符集
- 执行升级和降级行为
- 锁定不活动的登录帐户
- 在高可用性环境中使用口令

设置和更改最大登录尝试次数

设置允许的最大登录尝试次数可以防止“强制侵入”或以基于字典猜口令的方式尝试登录。系统安全员可以指定允许的最大连续登录尝试次数，尝试指定次数后，登录名或角色将被自动锁定。允许的失败登录尝试次数可以设置为适用于整个服务器或个别登录名和角色。个别设置优先于服务器范围的设置。

失败的登录次数存储在 `master..syslogins` 的 `logincount` 列中。成功的登录可以将失败登录次数重置为 0。

❖ 设置全服务器范围的 *maximum failed logins*

- 缺省情况下，`maximum failed logins` 处于禁用状态，不对口令应用此项检查。使用 `sp_passwordpolicy` 为登录名和角色设置全服务器范围的最大登录失败次数。

若要设置允许的失败登录次数，请输入：

```
sp_passwordpolicy 'set', 'maximum failed logins', number
```

请参见《参考手册：过程》中的 `sp_passwordpolicy`。

❖ 为特定登录名设置 *maximum failed logins*

- 若要在创建特定登录名时设置 *maximum failed logins*，请使用 `sp_addlogin`。

此示例新建口令为 “Djdiek3” 的登录名 “joe”，并将登录名 “joe” 的最大尝试登录失败次数设置为 2：

```
sp_addlogin joe, "Djdiek3", pubs2, null, null, null,
null, 2
```

请参见《参考手册：过程》中的 `sp_addlogin`。

❖ 为特定登录名设置 *maximum failed logins*

- 若要在创建特定角色时设置 *maximum failed logins*，请使用 `create role`。

此示例创建口令为 “temp244” 的 `intern_role` 角色，并将 `intern_role` 的 *maximum failed logins* 设置为 20：

```
create role intern_role with passwd "temp244",
maximum failed logins 20
```

请参见《参考手册：命令》中的 `create role`。

❖ 更改特定登录名的 *maximum failed logins*

- 使用 `sp_modifylogin` 设置或更改现有登录名的 *maximum failed logins*。

将登录名 “joe” 的 *maximum failed logins* 更改为 40：

```
sp_modifylogin "joe", "max failed_logins", "40"
```

注释 *value* 参数的数据类型为 `character`；因此数字值必须用引号引起来。

`sp_modifylogin` 只影响用户角色，不影响系统角色。有关语法和规则的详细信息，请参见 `sp_modifylogin`。

请参见《参考手册：过程》中的 `sp_modifylogin`。

❖ 更改特定角色的 *maximum failed logins*

- 使用 `alter role` 设置或更改现有角色的 *maximum failed logins*。

示例 1 将 `physician_role` 允许的 *maximum failed logins* 更改为 5：

```
alter role "all overrides" set maximum failed logins -1
```

示例 2 删除所有角色的 *maximum failed logins* 的替换值：

```
alter role physician_role set maximum failed logins 5
```

有关使用 *maximum failed logins* 的语法和规则的详细信息，请参见 `alter role`。

在丢失口令后登录

使用 `dataserver -plogin_name` 参数可以在服务器启动时指定系统安全员或系统管理员的名称。如果无法恢复丢失的口令，则使用这种方法可以为这些帐户设置新口令。

使用 `-p` 参数启动时，Adaptive Server 会生成一个随机口令，接着显示并加密该口令，然后将其作为该帐户的新口令保存在 `master.syslogins` 中。

可以使用 `dataserver -p` 重新设置 `sa_role` 和 `sso_role` 的口令。如果丢失了这些角色中任一角色的口令，而这些角色需要口令才能变为活动状态，请使用 `dataserver -p`。

例如，如果使用以下命令启动服务器：

```
dataserver -psa_role
```

Adaptive Server 会显示以下消息：

```
New password for role 'sa_role' : qjcdyrbfkxgyc0
```

如果 `sa_role` 没有口令，且使用 `-psa_role` 启动，则 Adaptive Server 会在错误日志中显示一条错误消息。

Sybase 强烈建议您在重新启动服务器时更改登录名或角色的口令。

锁定和解锁登录和角色

以下情况中将锁定登录名或角色：

- 口令到期，或
- 达到最大登录尝试失败次数，或
- 系统安全员手动将其将锁定。

❖ 锁定和解锁登录名

- 系统安全员可使用 `sp_locklogin` 手动锁定或解锁登录名。

例如：

```
sp_locklogin "joe" , "lock"  
sp_locklogin "joe" , "unlock"
```

有关登录名锁定状态的信息存储在 `syslogins` 的 `status` 列中。

请参见《参考手册：过程》中的 `sp_locklogin`。

❖ 锁定和解锁角色

- 系统安全员可使用 `alter role` 手动锁定或解锁角色。

例如：

```
alter role physician_role lock
alter role physician_role unlock
```

有关角色锁定状态的信息存储在 `sysssrvroles` 的 `status` 列中。

请参见《参考手册：命令》中的 `alter role`。

❖ 在服务器启动时解锁登录名和角色

- 如果所有能够解锁登录名的帐户（系统管理员和系统安全员）均已锁定，则自动登录名锁定可能会使节点停止。请在启动 Adaptive Server 时，在 `dataserver` 实用程序中使用 `-u` 标志来解锁特定的登录名或角色。

请参见《实用程序指南》中的 `dataserver`。

显示口令信息

本节论述如何显示登录名和角色的口令信息。

❖ 显示特定登录名的口令信息

- 使用 `sp_displaylogin` 显示登录名的口令设置。

此示例显示有关登录名 `joe` 的信息：

```
sp_displaylogin joe

Suid: 3
Loginame: joe
Fullname:
Default Database: master
Default Language:
Auto Login Script:
Configured Authorization:
Locked: NO
Date of Last Password Change: Sep 22 2008  3:50PM
Password expiration interval: 0
Password expired: NO
Minimum password length: 6
Maximum failed logins: 1
Current failed login attempts: 2
Authenticate with: ANY
```

```
Login Password Encryption: SHA-256
Last login date: Sep 18 2008 10:48PM
```

请参见《参考手册：过程》中的 `sp_displaylogin`。

❖ **显示特定角色的口令信息**

- 使用 `sp_displayroles` 显示角色的口令设置。

此示例显示有关 `physician_role` 角色的信息：

```
sp_displayroles physician_role, "display_info"
Role name = physician_role
Locked : NO
Date of Last Password Change: Nov 24 1997 3:35PM
Password expiration interval = 5
Password expired : NO
Minimum password length = 4
Maximum failed logins = 10
Current failed logins = 3
```

请参见《参考手册：过程》中的 `sp_displayroles`。

检查口令中是否至少包含一个数字

系统安全员可以指示服务器使用全服务器范围的配置参数 `check password for digit`，来检查口令中是否至少包含一个数字。如果设置了此参数，并不会影响现有的口令。缺省情况下，数字检查是关闭的。

此示例激活检查口令功能：

```
sp_configure "check password for digit", 1
```

这将停用检查口令功能：

```
sp_configure "check password for digit", 0
```

请参见《参考手册：过程》中的 `sp_configure`。

设置和更改 *minimum password length*

可配置的口令允许自定义口令来适应需要，例如使用四位个人标识号 (PIN) 或口令为空值的匿名登录名。

注释 Adaptive Server 为 *minimum password length* 使用缺省值 6。Sybase 建议您对此参数使用 6 个或更多字符。

系统安全员可指定：

- 全局强制的 *minimum password length*
- 每个登录名或角色的 *minimum password length*

每个登录名或每个角色的值将替换全服务器范围的值。设置 *minimum password length* 只会影响设置该值后创建的新口令。

❖ 为特定登录名设置 *minimum password length*

- 若要在创建特定登录名时设置 *minimum password length*，请使用 `sp_addlogin`。

此示例创建一个口令为 “Djdiek3” 的新登录名 “joe”，并将 “joe” 的 *minimum password length* 设置为 8：

```
sp_addlogin joe, "Djdiek3", @minpwdlen=8
```

有关使用 *minimum password length* 的语法和规则的详细信息，请参见《参考手册：过程》中的 `sp_addlogin`。

❖ 为特定角色设置 *minimum password length*

- 若要在创建特定角色时设置 *minimum password length*，请使用 `create role`。

此示例创建一个口令为 “temp244” 的新角色 `intern_role`，并将 `intern_role` 的 *minimum password length* 设置为 0：

```
create role intern_role with passwd "temp244", min  
passwd length 0
```

原口令为 7 个字符，但由于 *minimum password length* 设置为 0，因此该口令可更改为任意长度。

请参见《参考手册：命令》中的 `create role`。

❖ 更改特定登录名的 *minimum password length*

- 使用 `sp_modifylogin` 设置或更改现有登录名的 *minimum password length*。`sp_modifylogin` 只影响用户角色，并不影响系统角色。

示例 1 将登录名 “joe” 的 *minimum password length* 更改为 8 个字符。

```
sp_modifylogin "joe", @option="min passwd length",
@value="8"
```

注释 *value* 参数的数据类型为 `character`；因此数字值必须用引号引起来。

示例 2 将所有登录名的 *minimum password length* 的替换值更改为八个字符。

```
sp_modifylogin "all overrides", @option="min passwd
length", @value="8"
```

示例 3 删除所有登录名的 *minimum password length* 的替换值。

```
sp_modifylogin "all overrides", "min passwd length",
@value="-2"
```

请参见《参考手册：过程》中的 `sp_modifylogin`。

❖ 更改特定角色的 *minimum password length*

- 使用 `alter role` 设置或更改现有角色的 *minimum password length*。

示例 1 将现有角色 `physician_role` 的最短长度设置为 5 个字符：

```
alter role physician_role set min passwd length 5
```

示例 2 替换所有角色的 *minimum password length*：

```
alter role "all overrides" set min passwd length -1
```

请参见《参考手册：命令》中的 `alter role`。

口令复杂程度检查

可以在存储过程接口中使用这些支持口令复杂程度检查的选项；它们的值存储在 `master.dbo.sysattributes` 表中。

若要禁用某个单独选项，请输入：

```
sp_passwordpolicy 'clear', option
```

若要禁用所有口令策略选项，请输入：

```
sp_passwordpolicy 'clear'
```

请参见《参考手册：过程》了解完整的 `sp_passwordpolicy` 语法。

不允许使用简单口令

`disallow simple password` 检查口令中是否包含了作为子字符串的登录名。可对其进行设置以便：

- 0 — （缺省值）禁用该选项，并允许简单口令。
- 1 — 启用该选项，并不允许使用简单口令。

要设置该选项，可输入：

```
sp_passwordpolicy 'set', 'disallow simple passwords', 1
```

不允许使用简单口令时，则不能让登录名作为口令的子字符串出现在口令中。必须将口令设置得复杂一些。例如：

```
sp_password 'old_complex_password', BHotAcha789, johnd
```

登录名 `johnd` 现在的口令为 `BHotAcha789`，其中不包含登录名作为子字符串。

然而，如果您通过输入以下内容来更改登录口令，则登录名 `johnd` 现在是新口令 `johnd123` 的子字符串，并且该命令将失败：

```
sp_password 'old_complex_password', johnd123, johnd
```

自定义口令复杂程度检查

Adaptive Server 允许您使用 `sp_extrapwdchecks` 和 `sp_cleanpwdchecks` 自定义配置口令检查规则。

这两个存储过程在 `master` 数据库中定义并位于该数据库中，分别在进行 Adaptive Server 口令复杂程度检查期间和删除登录名时自动调用。有关如何创建这两个自定义存储过程的示例，请参见第 428 页的“启用自定义口令检查”。

指定口令中的字符

使用这些 `sp_passwordpolicy` 参数来指定口令中字符（数字、大小写字母等）的最小数目：

- `min digits in password` — 口令中数字的最小数目。缺省为禁用。有效值包括：
 - 0 到 16 — 口令中至少必须包含的数字位数。
 - -1 — 口令中不能包含数字。

- **min alpha in password** — 口令中允许使用的字母字符的最小数目。该值不得小于大写字母最小数目与小写字母最小数目的和。缺省为禁用。有效值包括：
 - 0 到 16 — 口令中需要包含的特殊字符的最小数目。
 - -1 — 口令中不能包含特殊字符。
- **min special char in password** — 口令中特殊字符的最小数目。有效值包括：
 - 0 到 16 — 口令中需要包含的特殊字符的最小数目。
 - -1 — 口令中不能包含特殊字符。
- **min upper char in password** — 口令中大写字母的最小数目。缺省为禁用。有效值包括：
 - 0 到 16 — 口令中需要包含的大写字母的数目。
 - -1 — 口令中不能包含大写字母。
- **min lower char in password** — 口令中小写字母的最小数目。有效值包括：
 - 0 到 16 — 口令中需要包含的大写字母的数目。
 - -1 — 口令中不能包含大写字母。
- **minimum password length** — 口令的最小长度。可以将口令的最小长度设置在 0 - 30 之间。指定的值不得小于所有其它最小要求值的和。例如，如果已经进行了如下设置，则必须至少将 **minimum password length** 设置为 10：
 - **minimum digits in password** 设置为 3
 - **minimum special characters in password** 设置为 2
 - **minimum uppercase characters in password** 设置为 2
 - **minimum lowercase characters in password** 设置为 3
- **password expiration** — 口令到期之前可以使用多少天。指定的值将在全局范围内生效。缺省为禁用。有效值包括：
 - 0 — 口令永不过期。
 - 1 到 32767 — 口令到期之前可以使用的天数。

- **password exp warn interval** — 系统将在口令到期之前多少天显示口令有效期警告消息。这些消息将在每次成功登录时显示，直到更改了口令或口令到期。该值必须小于或等于口令有效期天数。缺省为禁用。

有效值为 0 到 365。

- **maximum failed logins** — 指定失败登录的最大次数，在此次数之后登录名将被锁定。在全局范围内指定此值。缺省为禁用。有效值包括：
 - 0 — 无论登录失败多少次，始终不锁定登录名。
 - 1 到 32767 — 允许的失败登录次数，在此次数之后登录名将被锁定。
- **expire login** 用于在系统安全员创建或重置登录名时将登录名状态更改为已到期。这样，在首次登录时即需要为登录名更改口令。缺省为禁用。有效值包括：
 - 0 — 新登录名或重置的登录名将不到期。
 - 1 — 新登录名或重置的登录名到期；您必须在首次登录时重置口令。

请参见《参考手册：过程》中的 `sp_passwordpolicy`。

口令复杂程度选项交叉检查

某些口令复杂程度选项相互影响：

- **minimum password length** 不得小于 **min digits in password**、**min alpha in password** 及 **min special characters in password** 的和。
- **min alpha in password** 不得小于 **min upper char in password** 与 **min lower char in password** 的和。
- **systemwide password expiration** 必须大于 **password exp warn interval**。

为了进行上述交叉检查，如果 Adaptive Server 遇到的口令复杂程度选项值为 -1，则它会将该选项的值解释为 0。如果未设置某个选项，Adaptive Server 也会将该选项的值解释为 0。

Adaptive Server 将对每个不满足交叉检查的新口令复杂程度选项输出警告消息。不过，选项的设置仍然是成功的。

设置口令复杂程度检查

表 15-10: 口令复杂程度检查

用于 Adaptive Server 鉴定的口令检查和策略	使用 sp_configure 指定的配置参数	使用 sp_passwordpolicy 指定的口令复杂程度选项	使用 sp_modifylogin 指定的逐登录名替换项
口令有效期	system-wide password expiration	system-wide password expiration	password expiration
口令中包含的数字	check password for digit	min digits in password	不适用
口令中包含的字母字符	不适用	min alpha in password	不适用
口令长度	minimum password length	minimum password length	min passwd length
失败登录的锁定	maximum failed logins	maximum failed logins	max failed_logins
不允许使用简单口令	不适用	disallow simple passwords	不适用
口令中包含的特殊字符	不适用	min special char in password	不适用
口令中包含的大写字母	不适用	min upper char in password	不适用
口令中包含的小写字母	不适用	min lower char in password	不适用
口令有效期警告间隔	不适用	password exp warn interval	不适用
首次登录时重置口令	不适用	expire login	不适用
自定义口令复杂程度检查	不适用	不适用	不适用

在以下级别设置口令复杂程度选项：

- 登录名级别，使用 sp_addlogin 或 sp_modifylogin。
- 全局级别，使用新的 sp_passwordpolicy 或 sp_configure。

由于设置的口令配置选项既可能是全局范围的，也可能是特定于每个登录名的，而且既可能使用旧参数，也可能使用新参数，因此将应用的口令选项的优先级顺序非常重要。

应用口令选项时，优先级顺序为：

- 1 每个登录名的现有参数
- 2 口令复杂程度选项
- 3 现有全局口令选项

示例

示例 1 此示例将 “johnd” 的最小口令长度设置为 6:

```
sp_addlogin @login_name = 'johnd',
           @passwd = 'complex_password',
           @minpwdlen = 6
```

登录名 “johnd” 的这些全局选项为登录名 “johnd” 创建两个最小口令长度要求，并设置有关口令中的数字的限制:

```
sp_configure 'minimum password length', 8
sp_configure 'check password for digit', 'true'
sp_passwordpolicy 'set', 'min digits in password', 2
```

如果之后尝试为登录名 “johnd” 创建口令:

```
sp_password @caller_password = 'old_complex_password',
           @new_password = 'abcd123', @login_name = 'johnd'
```

Adaptive Server 将按如下顺序检查口令:

- 1 特定于每个登录名的现有选项检查: 口令的最小长度必须大于 6。由于情况的确如此，因此通过检查。
- 2 新选项: 口令中包含数字的最小数目必须大于 2。由于情况的确如此，因此通过检查。
- 3 现有全局选项: 不检查此处指定的最小口令长度，因为已经对登录名 “johnd” 进行了特定于每个登录名的检查。
- 4 check password for digit 选项是冗余的，因为在打开数字的最小数目选项并设为 2 时，即已经对 check password for digit 选项进行了检查。

Adaptive Server 按指定顺序执行完这些检查之后，登录名 “johnd” 的新口令通过了这些检查，从而成功创建了这个新口令。

示例 2 如果为用户 “johnd” 输入了以下内容，则 Adaptive Server 首先会检查每个登录名的现有选项，确定最小口令长度设置为 6，而您尝试创建仅有 4 个字符的口令:

```
sp_password @caller_password = 'old_complex_password',
           @new_password = 'abcd', @login_name = 'johnd'
```

检查失败，Adaptive Server 输出一条错误消息。在一个口令复杂程度检查失败后，将不再对其它选项进行检查。

示例 3 此示例将尝试使用以下口令配置选项创建新登录名，并将登录名 johnd 的最小口令长度设置为 4:

```
sp_addlogin @login_name = 'johnd', @passwd =
'complex_password', @minpwdlen = 4
```

这是每个登录名的现有选项。如果添加以下内容，则会创建口令中必须至少包含 1 个数字的全局要求：

```
sp_passwordpolicy 'set', 'min digits in password', 1
```

如果之后尝试为登录名 johnd 创建口令，如下所示：

```
sp_password @caller_password = 'old_complex_password',
@ new_password = 'abcde', @login_name = 'johnd'
```

Adaptive Server 将按如下顺序进行检查：

- 1 特定于每个登录名的现有选项检查：新口令的最小长度为 4。口令“abcde”的长度大于 4，因此通过检查。
- 2 新的全局要求检查：口令中所包含数字的最小数目被全局性地设为 1。该检查失败。

Adaptive Server 不创建新的口令，并输出一条错误消息。

若想创建新的口令，必须通过所有检查。

启用自定义口令检查

Adaptive Server 允许系统安全员编写启用自定义口令检查的用户定义存储过程。

例如，为实现口令历史记录检查，可以创建一个新的用户表来存储口令历史：

```
create table pwdhistory
(
    name varchar(30)not null, -- Login name.
    password varbinary(30)not null, -- old password.
    pwdate datetime not null, -- datetime changed.
    changedby varchar(30)not null -- Who changed.
)
go
```

指定新的口令时可以调用此用户定义存储过程 (sp_extrapwdchecks)，将口令以加密形式保存在 pwdhistory 表中：

```
create proc sp_extrapwdchecks
(
@caller_password varchar(30), -- the current password of caller
@new_password    varchar(30), -- the new password of the target acct
@loginname       varchar(30), -- user to change password on
)
as
```



```

begin
declare @current_time      datetime,
        @encrypted_pwd     varbinary(30),
        @changedby         varchar(30),
        @cutoffdate        datetime

select @changedby = suser_name()

-- Change this line according to your installation.
-- This keeps history of 12 months only.
select @current_time = getdate(),
       @cutoffdate = dateadd(month,-12,getdate())
select @encrypted_pwd = internal_encrypt(@new_password)

delete master..pwdhistory
       where name = @loginame
       and    pwdate < @cutoffdate

if not exists ( select 1 from master..pwdhistory
               where name = @loginame
               and    password = @encrypted_pwd )
begin
    insert master..pwdhistory
    select @loginame, internal_encrypt(@new_password),
           @current_time, @changedby
    return(0)
end
else
begin
    raiserror 22001 -- user defined error message
end
end

```

使用 `sp_addmessage` 添加用户定义的消息 22001。`raiserror 22001` 指示自定义口令复杂程度检查错误，并因此导致 `sp_addlogin` 或 `sp_password` 失败。

可以使用以下用户定义的存储过程 (`sp_cleanpwdchecks`)，通过 `sp_extrapwdchecks` 来清除口令历史记录。

```

create proc sp_cleanpwdchecks
(
    @loginame          varchar(30)
    -- user to change password on
)
as

```

```
begin

delete master..pwdhistory
where name = @loginame
end

go
```

定义了上述两个过程并将它们安装在 **master** 数据库中之后，系统就会在口令复杂程度检查期间动态调用它们。

为口令设置登录名和角色有效期

系统管理员和系统安全员可以：

使用	目的
sp_addlogin	在创建登录口令时指定其有效期。
sp_modifylogin	更改登录口令的有效期。 sp_modifylogin 只影响用户角色，并不影响系统角色。
create role	在创建角色口令时指定其有效期（只有系统安全员才能发出 create role）。
alter role	在创建角色口令时更改其有效期（只有系统安全员才能发出 alter role）。

以下规则适用于登录名和角色的口令有效期：

- 指派给个别登录帐户或角色的口令有效期将替换全局口令有效期的值。这使您可以为敏感的帐户或角色（例如系统安全员口令）指定较短的有效期，而为不敏感的帐户（例如匿名登录名）指定较为宽松的间隔。
- 口令到期的登录名或角色不能直接激活。
- 口令将在经过 password expiration interval 指定的天数后上次更改口令的时间到期。

有关命令和系统过程的语法和规则的详细信息，请参见相应的 《参考手册》。

12.x 版本以前的口令取消有效期限制

口令有效期不影响 Adaptive Server 12.x 之前版本中的角色。在 Adaptive Server 12.x 及更高版本中，任何现有用户定义角色的口令均取消口令有效期限制。

回避口令保护

在自动登录系统中，回避口令保护机制是必要的。可以创建不用口令即可访问其它角色的角色。

系统安全员可通过将口令保护的角色授予另一个角色来为某些用户回避口令机制，并将口令保护的角色授予一个或多个用户。激活此角色将会自动激活口令保护的角色，而不必提供口令。

例如：

Jane 是 ABC Inc. 的系统安全员，该公司使用自动登录系统。Jane 创建如下角色：

- `financial_assistant`
`create role financial_assistant with passwd "L54K3j"`
- `accounts_officer`
`create role accounts_officer with passwd "9sF6ae"`
- `chief_financial_officer`
`create role chief_financial_officer`

Jane 将 `financial_assistant` 和 `accounts_officer` 的角色授予 `chief_financial_officer` 角色：

```
grant role financial_assistant, accounts_officer to
chief_financial_officer
```

然后，Jane 将 `chief_financial_officer` 角色授予 Bob：

```
grant role chief_financial_officer to bob
```

Bob 登录到 Adaptive Server 并激活 `chief_financial_officer` 角色：

```
set role chief_financial_officer on
```

`financial_assistant` 和 `accounts_officer` 的角色将自动激活，无须 Bob 提供口令。现在，Bob 可以访问 `financial_assistant` 和 `accounts_officer` 角色下的所有内容，而无须输入这些角色的口令。

为新登录名创建口令有效期

使用 `sp_addlogin` 为新登录名设置口令有效期。

此示例创建口令为 “Djdiek3” 的新登录名 “joe”，并将 “joe” 的口令有效期设置为 2 天：

```
sp_addlogin joe, "Djdiek3", null, null, null, 2
```

“joe”的口令在创建登录帐户之日起 2 天后或自上次更改口令起 2 天后过期。

请参见《参考手册：过程》中的 `sp_addlogin`。

为新角色创建口令有效期

使用 `create role` 为新角色设置口令有效期。

此示例创建口令为 “temp244” 的新角色 `intern_role`，并将 `intern_role` 的口令有效期设置为 7 天：

```
create role intern_role with passwd "temp244", passwd expiration 7
```

`intern_role` 的口令将在您创建该角色之日起 7 天后或自上次更改口令起 2 天后过期。

请参见《参考手册：命令》中的 `create role`。

为口令添加的创建日期

口令使用创建日期标记，该日期等于给定服务器的升级日期。登录口令的创建日期存储在 `syslogins` 的 `pwdate` 列中。角色口令的创建日期存储在 `sysrvroles` 的 `pwdate` 列中。

更改或删除登录名或角色的口令有效期

使用 `sp_modifylogin` 更改已存在登录的口令有效期，为没有口令有效期的登录增加口令有效期，或删除口令有效期。`sp_modifylogin` 只影响登录口令，并不影响角色口令。

此示例将登录名 “joe” 的口令有效期更改为 5 天：

```
sp_modifylogin "joe", @option="passwd expiration", @value="5"
```

口令将在您实施口令到期之日起 5 天后到期。

注释 `value` 参数的数据类型为 `character`；因此数字值必须用引号引起来。

请参见《参考手册：过程》中的 `sp_modifylogin`。

保护网络上的登录口令

Adaptive Server 允许使用非对称加密，以采用 RSA 公用密钥加密算法将口令从客户端安全地传输到服务器。Adaptive Server 生成非对称密钥对，并将公用密钥发送给使用登录协议的客户端。例如，在将用户登录口令发送到服务器之前，客户端将使用公用密钥对该口令进行加密。服务器则使用私有密钥将口令解密，以开始对客户端连接进行鉴定。

您可以将 Adaptive Server 配置为要求客户端使用登录协议。将 Adaptive Server 配置参数 `net password encryption reqd` 设置为要求所有基于用户名和口令的鉴定请求使用 RSA 非对称加密。请参见第 164 页的“[net password encryption required](#)”。

生成非对称密钥对

在以下情况下，Adaptive Server 生成新的密钥对：

- 服务器每次启动时，
- 使用 Adaptive Server 管家机制每隔 24 小时自动生成一次，
- 具有 `sso_role` 的管理员请求重新生成密钥对时。

密钥对保存在内存中。重新生成密钥对时，错误日志和审计追踪中会记录一条消息。

要在需要时生成密钥对，请使用：

```
sp_passwordpolicy "regenerate keypair"
```

注释 根据系统负载，此命令执行的时间与密钥对实际生成的时间之间可能有一段延迟。这是因为管家任务以低优先级运行，且可能由于更高优先级的任务而被延迟。

要在具体时间生成密钥对，请使用：

```
sp_passwordpolicy "regenerate keypair", "datetime string"
```

例如，日期时间字符串“Jan 16, 2007 11:00PM”会在该指定时间生成密钥对。日期字符串也可以只是一天中的某个时间，例如“4:07AM”。如果仅指定了一天中的某个时间，重新生成密钥对会安排在 24 小时之后的该时间点。

服务器选项 “net password encryption”

建立远程过程调用 (RPC) 时，Adaptive Server 也充当客户端。

当连接到远程服务器时，Adaptive Server 使用 net password encryption 选项来确定是否使用口令加密。

当此服务器选项设置为 true 时，Adaptive Server 使用 RSA 或 Sybase 专有算法。用于启用 net password encryption 的命令为：

```
sp_serveroption server, "net password encryption",  
"true"
```

此设置存储在 master.sys.servers 中，可以使用 sp_helpserver 存储过程显示服务器选项的值。

对于使用 sp_addserver 添加的任何新服务器，net password encryption 的缺省值为 true。在升级过程中，对于含有 ASEnterprise 类值的 sys.servers 条目，Adaptive Server 将 net password encryption 设置为 true。不对其它服务器类进行修改。这样可以提高两个通信的 Adaptive Server 之间的口令安全性。

注释 如果您在与服务器建立连接时遇到问题，管理员可以选择将 net password encryption 重置为 false。但是，如果该选项设置为 false，口令就会在网络中以明文传输。

向后兼容性

- Sybase 建议您使用 RSA 算法保护网络上的口令。
- 若要使用 RSA 算法，必须有 Adaptive Server 15.0.2 版和新的 Connectivity SDK 客户端（15.0 ESD#7 版及更高版本）。Sybase 提供 net password encryption reqd 配置参数和 net password encryption 服务器选项，以允许使用等效于 15.0.2 之前的版本设置，并保持与旧客户端和服务器的向后兼容性。
- 不支持 RSA 算法的旧客户端可将此属性设置为使用 Sybase 专有算法进行口令加密，此算法已在 12.0 版中提供。然后，Adaptive Server 会使用 Sybase 专有算法。
- 支持 RSA 和 Sybase 专有算法的新客户端可以为这两种算法设置属性。与此类客户端通信时，Adaptive Server 15.0.2 使用 RSA 算法。15.0.2 之前版本的 Adaptive Server 使用 Sybase 专有算法。

保护磁盘上和内存中存储的登录口令

Adaptive Server 用于鉴定客户端连接的登录口令以 SHA-256 散列摘要的形式安全地存储在磁盘上。SHA-256 算法是一种单向加密算法，它生成的摘要不能被解密，确保了存储在磁盘上的安全性。为了鉴定用户的连接，会对客户端发送的口令应用 SHA-256 算法，然后将结果与磁盘上存储的值进行比较。

为了防止对磁盘上存储的登录口令进行基于字典的攻击，在使用 SHA-256 算法之前，将一个 salt 与口令混合。salt 与 SHA-256 散列存储在一起，且在登录鉴定过程中使用。

为了简化在从 15.0.2 之前版本迁移时向新的磁盘上加密算法的过渡，Adaptive Server 包括了口令策略 `allow password downgrade`。从 15.0.2 之前版本升级后，该策略的值为 1，表示口令既会以早期版本使用的 Sybase 专有算法存储，也会以 Adaptive Server 15.0.2 中使用的新的 SHA-256 算法存储。

只要口令以新旧两种形式存储，则无需重置用户口令，就可以将 Adaptive Server 降级到 Adaptive Server 15.0 或 15.0.1。如果将策略 `allow password downgrade` 设置为 0，则口令只会以新的 SHA-256 形式存储，此形式与旧版本不兼容。当降级到先前版本时，只有以 SHA-256 存储的口令会被重新设置为随机口令，并会以与旧版本兼容的旧形式存储。请参见第 434 页的“向后兼容性”。

Sybase 建议：只要您确保将不会降级到早期版本，即仅使用 SHA-256。在进行决策时请考虑权衡；如果需要降级到 15.0.2 之前的版本，则该算法需要管理员的干预才能将用户登录口令解锁。

仅使用 SHA-256 算法

要不再允许口令降级，请执行：

```
sp_passwordpolicy set, "allow password downgrade", 0
```

在执行此命令前，请使用 `sp_displaylogin` 检查登录帐户，以确定登录帐户是否已使用，以及口令是否以 SHA-256 编码存储。否则，将会自动锁定该帐户，并用生成的口令重置帐户。若要再次使用该帐户，您必须对该帐户进行解锁，并为用户提供新生成的口令。

您可能需要保存此命令的输出，因为其中可能包含有关被锁定的登录帐户及这些帐户的生成口令的信息。

口令降级阶段结束时：

- 口令降级阶段结束时的 `datetime` 记录在 `master.dbo.sysattributes` 中。
- `syslogins` 中的每个 `password` 列的值都会被重写，以仅使用磁盘上结构的新口令。
- 如果登录名尚未过渡到新算法，则其口令会被重置为服务器生成的、SHA-256 格式的新口令，并且该登录名将被锁定。生成的口令仅显示给执行上述 `sp_passwordpolicy` 过程的管理员。锁定原因设置为 3（“未过渡到 SHA-256 的登录名或角色”）。

`sp_passwordpolicy` 过程完成后：

- 登录鉴定仅使用 SHA-256。
- 仅为 `password` 列使用磁盘上结构的新口令。
- 尝试使用锁定的登录名不会通过鉴定。若要使用锁定的登录名，您必须使用 `sp_locklogin` 解锁该登录名，且用户必须使用 `sp_passwordpolicy` 生成的口令。或者，您可能更愿意为锁定的登录帐户指定新的口令，而不是使用生成的口令。

示例 1

本示例准备了一个仅使用 SHA-256 的升级服务器。使用 `sp_displaylogin` 检查登录帐户以确定该帐户使用的是哪种加密。

```
1> sp_displaylogin login993
2> go
Suid: 70
Loginame: login933
Fullname:
Default Database: master
Default Language:
Auto Login Script:
Configured Authorization:
Locked: NO
Date of Last Password Change: Apr 20 2007 2:55PM
Password expiration interval: 0
Password expired: NO
Minimum password length: 0
Maximum failed logins: 3
Current failed login attempts:
Authenticate with: ANY
Login Password Encryption: SYB-PROP
Last login date:
(return status = 0)
```


Login Password Encryption: SYB-PROP 行中的 SYB-PROP 值指示为此帐户仅使用 Sybase 专有加密。此登录名在升级到 Adaptive Server 15.0.2 版之前尚未使用过，并且，如果执行了 `sp_passwordpolicy 'set', 'allow password downgrade', 0`，此登录名会被锁定，且其口令将被重置。

升级到 Adaptive Server 15.0.2 后首次登录到帐户之后，此行会发生更改，显示同时使用了新旧两种加密：

```
Login Password Encryption: SYB-PROP,SHA-256
```

这是所有活动的登录帐户的预期状态，因此执行 `sp_passwordpolicy 'set', 'allow password downgrade', 0` 不会锁定帐户和重置帐户的口令。

执行 `sp_passwordpolicy 'set', 'allow password downgrade', 0` 之后，将只会使用 SHA-256 加密，并且您将看到：

```
Login Password Encryption: SHA-256
```

显示此值的登录帐户现在使用更强大的磁盘上加密算法。

当所有口令都更改为使用新的算法时，重新执行 `sp_passwordpolicy` 将不会显示重置或锁定的帐户：

```
1> sp_passwordpolicy 'set', 'allow password downgrade', 0
2> go
```

```
Old password encryption algorithm usage eliminated from 0 login accounts,
changes are committed.
(return status = 0)
```

示例 2 此示例中，1000 个登录帐户中有 990 个都已过渡到 SHA-256 算法，但有 10 个帐户仍在使用 SYB-PROP 算法：

```
1> sp_passwordpolicy 'set', 'allow password downgrade', 0
2> go

Old password encryption algorithm found for login name login1000, suid 3,
ver1 =5, ver2 = 0, resetting password to EcJxKmMvOrDsC4
Old password encryption algorithm found for login name login999, suid 4,
ver1 =5, ver2 = 0, resetting password to MdZcUaFpXkFtM1
Old password encryption algorithm found for login name login998, suid 5,
ver1 =5, ver2 = 0, resetting password to ZePiZdSeMqBdE6
Old password encryption algorithm found for login name login997, suid 6,
ver1 =5, ver2 = 0, resetting password to IfWpXvGlBgDgW7
Old password encryption algorithm found for login name login996, suid 7,
ver1 =5, ver2 = 0, resetting password to JhDjYnGcXwObI8
Old password encryption algorithm found for login name login995, suid 8,
ver1 =5, ver2 = 0, resetting password to QaXlRuJlCrFaE6
Old password encryption algorithm found for login name login994, suid 9,
ver1 =5, ver2 = 0, resetting password to HlHcZdRrYcKyB2
```

```
Old password encryption algorithm found for login name login993, suid 10,
ver1 =5, ver2 = 0, resetting password to UvMrXoVqKmZvU6
Old password encryption algorithm found for login name login992, suid 11,
ver1 =5, ver2 = 0, resetting password to IxIwZqHxEePbX5
Old password encryption algorithm found for login name login991, suid 12,
ver1 =5, ver2 = 0, resetting password to HxYrPyQbLzPmJ3
Old password encryption algorithm usage eliminated from 10 login accounts,
changes are committed.
(return status = 1)
```

注释 登录名、suid 和生成的口令将向执行过程的管理员显示。此命令的输出表明所有 10 个未过渡的帐户都被重新设置（并锁定）。

口令的字符集注意事项

被加密的口令和其它敏感数据必须确定明文字符集，才能准确地解释鉴定过程中解密的结果或者散列值的比较结果。

例如，客户端使用 isql 连接到 Adaptive Server 并建立新的口令。无论客户端使用的是什么字符集，字符通常都会转换为服务器的缺省字符集，以用于在 Adaptive Server 中进行处理。假设 Adaptive Server 的缺省字符集为 “iso_1”，考虑过程调用：

`sp_password old_passwd, new_passwd`

该参数为 `varchar`，以带引号的字符串表示，在加密前以 “iso_1” 编码存储。如果 Adaptive Server 的缺省字符集以后进行更改，则加密的口令仍为以原始缺省字符集编码的加密字符串。由于不匹配的字符映射，这可能导致鉴定失败。尽管缺省字符集很少更改，但在平台间进行迁移时变得尤为重要。

Adaptive Server 在加密前将明文口令转换为规范形式，以便可跨平台、芯片体系结构和字符集使用口令。

为 `syslogins` 中的存储使用规范形式：

- 1 将明文口令字符串转换为 UTF-16。
- 2 将 UTF-16 字符串转换为网络字节顺序。
- 3 将具有随机字节的小缓冲区 (salt) 附加到口令。
- 4 应用 SHA-256 散列算法。
- 5 在 `password` 列中存储摘要、salt 和版本。

在鉴定时：

- 1 将明文口令字符串转换为 UTF-16。
- 2 将 UTF-16 字符串转换为网络字节顺序。
- 3 将 `syslogins` 中的 `password` 列中的 `salt` 附加到口令。
- 4 应用散列算法。
- 5 将结果与 `syslogins` 中的口令列进行比较，如果两者匹配，则鉴定成功。

升级和降级行为

本节包含有关在各版本之间升级和降级 Adaptive Server 的信息。

升级的 *master* 数据库中的行为更改

当您升级 *master* 数据库时，Adaptive Server 将使用 `password` 列中 Adaptive Server 早期或升级版本中的算法保留 `syslogins` 目录中的加密口令。

用户可以调用 `sp_displaylogin` 来确定某次登录使用哪种 “Login password encryption”。

在升级后进行首次登录鉴定时：

- 用户使用 `password` 列的内容和旧算法进行鉴定。
- Adaptive Server 会先后使用旧的加密算法和新的加密算法更新 `password` 列。

在升级后进行后续登录鉴定时，在 “allow password downgrade” 设置为 0 之前，用户使用新的算法鉴定。

新的 *master* 数据库中的行为更改

在新的 Adaptive Server *master* 数据库中，或者在 `allow password downgrade` 设置为 0 之后的升级 *master* 数据库中，服务器仅使用 `password` 列中的新算法保留 `syslogins` 中的加密口令。只有 SHA-256 算法才会鉴定连接请求和在磁盘上存储口令。

发出 `sp_passwordpolicy`，以确定服务器是否已升级（例如，从 15.0 版升级到 15.0.2 版），并使用升级前或升级后的服务器中的算法保留口令，或者，确定是否新安装了服务器，并且服务器是否包括使用（15.0.2 版中的）最新算法的 *master* 数据库：

```
sp_passwordpolicy "list", "allow password downgrade"
```

在升级并随之降级后保留口令加密

如果升级到 Adaptive Server 15.0.2 或更高版本，然后降级到某个早期版本，请使用 `sp_downgrade` 以保留并使用 15.0.2 及更高版本服务器中的口令加密功能。缺省情况下，Adaptive Server 允许您在升级之后降级口令，直到结束口令降级阶段为止。

注释 如果运行 `sp_downgrade`，关闭服务器，然后重新启动您从其降级的 Adaptive Server 的同一版本，则会删除 `sp_downgrade` 所做的更改。必须重新运行 `sp_downgrade` 以重复更改。有关运行 `sp_downgrade` 的信息，请参见《安装指南》。

在升级之前增加空间

Adaptive Server 要求 `master` 数据库和事务日志中有额外的空间。使用 `alter database` 为 `master` 数据库和事务日志增加额外的空间。

加密算法和口令策略：

- 将 `syslogins` 所需的空间增加大约 30%。
- 将每个登录帐户的最大行长度增加 135 个字节。
- 在 Adaptive Server 15.0.1 版和 15.0.2 版之间，将每页行数的比率从每 2K 页 16 行降低到每 2K 页 12 行。在升级过程中有一段时间 `allow password downgrade` 的值为 1（此时同时使用了新旧两种口令加密算法）；该比率会进一步降低到每 2K 页大约 10 行。

例如，如果 Adaptive Server 15.0.1 有 1,000 个登录帐户，数据适合 59 页，则同样数目的登录帐户在 Adaptive Server 15.0.2 新的 `master` 数据库上可能另外需要大约 19 页；或者，如果从 15.0.1 升级（`allow password downgrade` 设置为 1），则另外需要 33 页。

对于更新的 `password` 列，事务日志需要额外的空间。用户第一次登录时，Adaptive Server 需要每 1,000 个登录大约 829 个 2K 页，而对于用户在升级和降级过程中进行的口令更改，则需要每 1,000 个登录大约 343 页。若要确保有足够的日志空间，在开始口令升级或降低之前，以及在用户第一次登录到 Adaptive Server 15.0.2 版及更高版本时，请验证每个登录有大约一个 2K 页的可用日志空间。

降级

Adaptive Server 支持从 15.0.2 版或更高版本降级到 15.0 版或 15.0.1 版。如果要降级到 Adaptive Server 的某个早期版本，您可能需要执行额外操作。

如果 `allow password downgrade` 为 0 或 NULL，或者，如果口令已仅使用 SHA-256 算法存储在 `syslogins` 中，请对登录帐户使用 `sp_displaylogin` 以确定使用了哪种算法，或使用 `sp_downgrade "prepare"` 以确定重置了哪些帐户。

`prepare` 选项报告服务器是否已准备好降级。如果 `prepare` 选项失败，它将报告必须修复的错误。如果在修复错误之前在服务器上执行降级，则降级将失败。对于登录口令，`prepare` 将报告在降级过程中重置了哪些口令。

运行 `sp_downgrade "prepare"`，验证您是否应运行 `sp_downgrade`：

```
sp_downgrade 'prepare','15.0.1',1
Checking databases for downgrade readiness.

There are no errors which involve encrypted columns.

Allow password downgrade is set to 0. Login passwords
may be reset, if old encryption version of password is
not present.

Warning: New password encryption algorithm found for
login name user103, suid 103.

Password will be reset during the downgrade phase.

sp_downgrade 'prepare' completed.
(return status = 0)

sp_droplogin 'probe'
```

如果该登录名在数据库中有用户条目，请从 `master` 数据库中删除用户，然后删除该登录名：

```
use master
sp_dropuser 'probe'
```

对降级的服务器运行 `installmaster` 时，会重新创建 `probe` 登录名。

执行 `sp_downgrade` 之前，Sybase 建议删除 `syslogins` 和 `sysssrvroles` 的统计信息。这样做可避免在降级过程记录 `sysstatistics` 中的无效列信息，例如口令列的长度。

若要删除 `syslogins` 和 `sysssrvroles` 的统计信息，请输入：

```
delete statistics master..syslogins
delete statistics master..sysssrvroles
```

在此示例中，执行 `sp_downgrade` 将会锁定并重置 `user103` 的登录口令。
Adaptive Server 生成的随机口令仅对执行 `sp_downgrade` 的客户端显示。
 管理员可以将此输出重定向到文件，以便保留这些口令；管理员也可以在降级完成并且服务器重新启动后手动重置这些口令。

```
sp_downgrade 'downgrade','15.0.1',1

Checking databases for downgrade readiness.
There are no errors which involve encrypted columns.

Allow password downgrade is set to 0. Login passwords
may be reset, if old encryption
version of password is not present.
Warning:New password encryption algorithm found for
login name user103, suid 103 .
Password is reset during the downgrade phase.

Executing downgrade step 1 [sp_passwordpolicy
'downgrade'] for :
- Database: master (dbid:1)

New password encryption algorithm found for login name
user103, suid 103.
Resetting password to 'ZdSuFpNkBxAbW9'.

Total number of passwords reset during downgrade = 1

[ ... output from other downgrade steps ...]
(return status = 0)
```

错误日志中将出现其他消息，标识在 `sp_downgrade` 过程中进行的步骤：

```
00:00000:00006:2007/05/21 05:34:07.81 server  Preparing ASE downgrade from 1502
to 1501.
00:00000:00006:2007/05/21 05:35:59.09 server  Preparing ASE downgrade from 1502
to 1501.
00:00000:00006:2007/05/21 05:35:59.19 server  Starting downgrading ASE.
00:00000:00006:2007/05/21 05:35:59.20 server  Downgrade : Downgrading login
passwords.
00:00000:00006:2007/05/21 05:35:59.22 server  Downgrade : Starting password
downgrade.
00:00000:00006:2007/05/21 05:35:59.23 server  Downgrade : Removed sysattributes
rows.
00:00000:00006:2007/05/21 05:35:59.23 server  Downgrade : Updated 1 passwords.
```

```

00:00000:00006:2007/05/21 05:35:59.24 server Downgrade : Removed columns in
syslogins -
lastlogindate, crdate, locksuid, lockreason, lockdate are removed.
00:00000:00006:2007/05/21 05:35:59.26 server Downgrade : Truncated password
lengths.
00:00000:00006:2007/05/21 05:35:59.28 server Downgrade : Successfully
completed password
downgrade.
00:00000:00006:2007/05/21 05:35:59.28 server Downgrade : Marking stored
procedures to
be recreated from text.
00:00000:00006:2007/05/21 05:36:03.69 server Downgrade : Dropping Sysoptions
system
table.
00:00000:00006:2007/05/21 05:36:03.81 server Downgrade : Setting master
database minor
upgrade version.
00:00000:00006:2007/05/21 05:36:03.83 server Downgrade : Setting user
databases minor
upgrade version.
00:00000:00006:2007/05/21 05:36:03.90 server ASE downgrade completed.

```

`sp_downgrade` 更改目录并修改口令数据。服务器必须为单用户模式，才能成功执行 `sp_downgrade`。若要以单用户模式启动服务器并仅允许系统管理员登录，请使用 `-m` 命令行选项来启动服务器。

运行 `sp_downgrade` 之后，请关闭 15.0.2 服务器，以避免新的登录或者其它可能修改数据或系统目录的操作。如果在运行 `sp_downgrade` 之后重新启动 Adaptive Server 15.0.2 版，则早期版本将关闭，并且您将再次升级到 15.0.2 版或更高级别。

当 *allow password downgrade* 设置为 0 时，口令会到期

在口令降级阶段结束时使 `syslogins` 中的口令到期。

要将登录口令配置为到期，请使用：

```
sp_passwordpolicy "expire login passwords"[, "[loginame | wildcard]"]
```

若要将角色口令配置为到期，请使用：

```
sp_passwordpolicy "expire role passwords"[, "[rolename | wildcard]"]
```

要将旧登录名口令配置为到期，请使用：

```
sp_passwordpolicy "expire stale login passwords", "datetime"
```

要将旧角色口令配置为到期，请使用：

```
sp_passwordpolicy "expire stale role passwords", "datetime"
```

当您执行命令时，自 `sp_passwordpolicy "expire stale login passwords,"` 的 `datetime` 参数中所设置日期以来未更改的口令将到期。当口令降级阶段结束时，将自动要求用户更改其口令。

也可以锁定旧登录名或角色；但是，这将要求您手动重置口令，以使合法用户可以再次访问其登录帐户。

显示 *allow password downgrade* 的当前值

若要获取 `allow password downgrade` 的当前值，请输入：

```
sp_passwordpolicy list, "allow password downgrade"
```

结果集包括当前值及说明其意义的消息。

如果已升级 **master** 数据库，并且要采用新旧两种编码保留口令，则结果为：

```
sp_passwordpolicy list, "allow password downgrade"
go

value      message
-----
1 Password downgrade is allowed.
(1 row affected)
```

对于仅使用新口令加密的升级 **master** 数据库，此结果为：

```
sp_passwordpolicy list, "allow password downgrade"
go

value      message
-----
0 Last Password downgrade was allowed on <datetime>.
(1 row affected)
```

对于 Adaptive Server 15.0.2 上的仅使用新口令加密的新 **master** 数据库，此结果为：

```
sp_passwordpolicy list, "allow password downgrade"
go

value      message
-----
NULL New master database.
(1 row affected)
```


上次登录和锁定不活动帐户

Adaptive Server 通过以下方式为用户帐户提供安全性：

- 跟踪创建日期。
- 记录帐户的上次登录时间。
- 确定哪些帐户由于不活动而过时并被锁定。
- 记录锁定帐户的原因，以及锁定帐户的用户的标识。

使用 *syslogins* 跟踪帐户是否已锁定

syslogins 包括 *lastlogindate*、*crdate*、*locksuid*、*lockreason* 和 *lockdate* 列，以支持上次登录和锁定不活动的帐户，从而使帐户所有者或管理员能够了解帐户是否已锁定、帐户的锁定时间、锁定者以及锁定原因。

创建登录时，*crdate* 列设置为当前时间。

如果 *enable last login updates* 口令策略选项设置为 1，则 *lastlogindate* 列将设置为登录的 *datetime*，并且该列以前的值存储在登录会话的 PSS 中。每次登录到 Adaptive Server 时，可能会更新 *syslogins* 和 PSS。对于新的 *master* 数据库或升级的数据库，*enable last login updates* 的缺省值为 1。若要禁用此选项，请使用管理员权限执行此过程：

```
sp_passwordpolicy "set", "enable last login updates", 0
```

@@lastlogindate 特定于每次用户登录会话，该会话可以使用此变量来确定帐户上次登录的日期和时间。如果帐户之前未使用过，或 *enable last login updates* 为 0，则 *@@lastlogindate* 的值为 NULL。

事务日志不会记录对 *syslogins..lastlogindate* 的更新。

具有 *sso_role* 的管理员可以使用以下命令锁定在给定天数内处于非活动状态的登录帐户：

```
sp_locklogin 'all', 'lock', [ @except ], 'number of inactive days'
```

如果 *enable last login updates* 设置为 0，或 *lastlogindate* 列的值为 NULL，则此命令无效。*number of inactive days* 的值范围为 1 – 32767（天）。

lockreason 列指定锁定登录的原因。*lockdate* 列的值设置为当前 *datetime*。

如果帐户被解锁，列 *lockreason*、*lockdate* 和 *locksuid* 都会被重新设置为 NULL。

lockdate、locksuid 和 lockreason 列由 Adaptive Server 内部设置。表 15-11 介绍了锁定原因和 locksuid 值。

表 15-11: 原因和 locksuid 的值

lockreason 值	locksuid 值	lockreason 值说明
NULL	NULL	帐户未被锁定。
0	suid of caller of sp_locklogin	locksuid 通过手动执行 sp_locklogin 而锁定的帐户。
1	suid of caller of sp_locklogin	因帐户不活动而锁定的帐户， locksuid 已手动执行 sp_locklogin 'all', 'lock', 'ndays'。
2	suid of attempted login	因登录尝试失败次数达到了最大登录失败次数而由 Adaptive Server 锁定的帐户。
3	suid of caller of sp_passwordpolicy set, "allow password downgrade", 0	因口令降级阶段已结束、登录名或角色尚未过渡到 SHA-256 而由 locksuid 锁定的帐户。

在高可用性环境中使用口令

口令安全性影响高可用性的配置和 syslogins 中的口令在主服务器和协同服务器之间的行为。

高可用性配置

在您针对高可用性配置主服务器和协同服务器之前，这些服务器必须具有相同的 allow password downgrade 值。allow password downgrade 的 quorum 属性检查 allow password downgrade 的值在主服务器和辅助服务器上是否相同。

如果主服务器上的 allow password downgrade 为 1，在辅助服务器上为 0，则 sp_companion 的输出为：

```
1> sp_companion "primary_server",configure
2> go

Step: Access verified from Server:'secondary_server' to
Server:'primary_server'.
Step: Access verified from Server:'primary_server' to
Server:'secondary_server'.
Msg 18836, Level 16, State 1:
Server 'secondary_server', Procedure 'sp_companion', Line 392:
Configuration operation 'configure' can not proceed due to Quorum Advisory Check
failure. Please run 'do_advisory' command to find the incompatible attribute
and fix it.

Attribute Name      Attrib Type      Local Value      Remote Value      Advisory
-----
```

```

allow password downg    allow password                0                1                2

(1 row affected)
(return status = 1)

```

advisory 列中的值 2 表示：除非两个协同服务器上的值相同，否则用户不能进行集群操作。

sp_companion do_advisory 还会列出两个服务器上的 allow password downgrade 值的差异。

在主服务器和辅助服务器上单独运行 sp_passwordpolicy 'allow password downgrade' 以同步值，并确保服务器的状态相同。

升级后更新的口令

在针对高可用性升级和配置后第一次连接到主服务器时，在具有相同磁盘上加密格式的主服务器和协同服务器上，用户登录口令将同步。这样可避免在 allow password downgrade 阶段结束并且口令降级到 Adaptive Server 的早期版本时出现口令重置或锁定情况。无需被 sp_passwordpolicy 或 sp_downgrade 重置或锁定，就可以继续使用登录口令。

成功设置高可用性环境后，请分别在主服务器和协同服务器上结束 allow password downgrade 阶段。同样，降级到 Adaptive Server 的早期版本，分别主服务器和协同服务器上执行 sp_downgrade。

监控许可证的使用状况

系统管理员可以通过许可证使用监控器监控在 Adaptive Server 中使用的用户许可证数，同时安全地管理许可协议数据。这就是说，可以确保 Adaptive Server 中使用的许可证数没有超过许可协议中指定的数量。

许可证使用监控器追踪执行的许可证数；但不强制执行许可协议。如果许可证使用监控器报告正在使用的用户许可证数超出了许可协议中指定的数量，请咨询 Sybase 销售代表。

您必须具有系统管理员特权才能配置许可证使用监控器；缺省情况下，在安装或升级 Adaptive Server 时，该监控器处于禁用状态。

请参见下面的“配置许可证使用监控器”。

如何计算许可证数

许可证是指主机名和用户名的组合。如果用户从同一主机多次登录到 Adaptive Server，将使用一个许可证。然而，如果用户从主机 A 登录一次，从主机 B 登录一次，则使用两个许可证。如果多个用户以不同的用户名从同一主机登录到 Adaptive Server，则用户名与主机名的每个不同组合都使用一个许可证。

配置许可证使用监控器

使用 `sp_configure` 指定许可协议中的许可证数，其中 *number* 是许可证数：

```
sp_configure "license information" , number
```

此示例将用户许可证的最大数目设置为 300，如果许可证数目为 301，则报告出现了过度使用：

```
sp_configure "license information", 300
```

如果增加用户许可证的数目，还必须更改 `license information` 配置参数。

通过管家任务监控许可证使用状况

配置许可证使用监控器后，管家任务根据登录到 Adaptive Server 的每个用户的用户 ID 和主机名，来确定在使用中的用户许可证数。许可证使用监控器更新一个变量，该变量跟踪正在使用的用户许可证的最大数目：

- 如果使用中的许可证数自上次运行管家任务以来没有变化或已减少，许可证使用监控器将不进行任何操作。
- 如果在使用的许可证数自上次管家运行后已经添加，许可证使用监控器则将此数目设置为在使用的许可证最大数目。
- 如果在使用的许可证数大于许可协议允许的数目，则许可证使用监控器将此消息发送到错误日志：

超过许可证使用限制。请与 Sybase 销售部门联系以获取额外的许可证。

管家杂事任务在 Adaptive Server 空闲周期运行。`housekeeper free write percent` 和 `license information` 配置参数均必须设置为大于或等于 1 的值，以便许可证使用监控器跟踪许可证使用情况。

有关管家杂事任务的详细信息，请参见 Performance and Tuning Series: Basics（《性能和调优系列：基础知识》）中的第 3 章“Using Engines and CPUs”（使用引擎和 CPU）。

记录用户许可证数

syblicenseslog 系统表是在安装或升级 Adaptive Server 时在 master 数据库中创建的。许可证使用监控器在每个 24 小时周期结束时，更新 syblicenseslog 中的列，如表 15-12 所示。

表 15-12: syblicenseslog 表中的列

列	说明
status	-1 — 管家不能监控许可证。 0 — 没有超过许可证数量。 1 — 超过了许可证数量。
logtime	插入日志信息的日期和时间。
maxlicenses	在前 24 小时内使用的最大许可证数。

syblicenseslog 与以下内容类似：

status	logdate	maxlicenses
-----	-----	-----
0	Jul 17 1998 11:43AM	123
0	Jul 18 1998 11:47AM	147
1	Jul 19 1998 11:51AM	154
0	Jul 20 1998 11:55AM	142
0	Jul 21 1998 11:58AM	138
0	Jul 21 1998 3:14PM	133

在本例中，在 1998 年 7 月 19 日使用的用户许可证数超过了限制。

如果 Adaptive Server 关闭，则许可证使用监控器会以所用许可证当前的最大数目来更新 syblicenseslog。当 Adaptive Server 重新启动时，开始新的 24 小时监控周期。

1998 年 7 月 21 日记录的第二行是由于服务器的关机和重新启动引起。

获取有关使用情况的信息：收费退回式会计

用户登录到 Adaptive Server 时，服务器开始累计此用户的 CPU 和 I/O 使用状况。Adaptive Server 可以报告单个用户或所有用户的总体使用状况。每个用户的信息都存储在 master 数据库的 syslogins 系统表中。

报告当前使用状况统计信息

系统管理员可以使用 `sp_reportstats` 或 `sp_clearstats`，获取或清除有关 Adaptive Server 上单个用户或所有用户的当前总体使用状况的数据。

显示当前会计汇总

`sp_reportstats` 显示 Adaptive Server 用户的当前会计汇总。此命令报告全部 CPU 和 I/O 时间，以及使用这些资源的百分比。但不记录 “sa” 登录名 (`suid` 为 1 的进程)、检查点、网络和镜像处理程序的统计信息。

初始化新的会计间隔

Adaptive Server 将累计 CPU 和 I/O 统计信息，直到通过运行 `sp_clearstats` 从 `syslogins` 中清除汇总数据。`sp_clearstats` 为 Adaptive Server 用户初始化一个新的会计间隔，并执行 `sp_reportstats` 以显示上一时间段的统计信息。

通过确定如何在自己的节点使用统计信息来选择会计间隔的时间长度。例如，若要每月跨部门按 Adaptive Server 的 CPU 和 I/O 使用百分比收取费用，可每月运行一次 `sp_clearstats`。

有关这些存储过程的详细信息，请参见《参考手册：过程》。

指定添加会计统计信息的间隔

系统管理员可以使用配置参数确定将会计统计信息添加到 `syslogins` 的频率。

若要指定在会计统计信息被添加到 `syslogins` 之前计算机时钟累计的周期数，请使用 `cpu accounting flush interval` 配置参数。缺省值为 200。例如：

```
sp_configure "cpu accounting flush interval", 600
```

若要获取系统上一个时钟周期的微秒数，可在 Adaptive Server 中运行下面的查询：

```
select @@timeticks
```

若要指定在信息被添加（刷新）到 `syslogins` 之前读取或写入 I/O 的累计次数，请使用 `i/o accounting flush interval` 配置参数。缺省值为 1000。例如：

```
sp_configure "i/o accounting flush interval", 2000
```

I/O 和 CPU 统计信息在用户的累计 I/O 或 CPU 使用超过指定值时刷新。这些信息在用户退出 Adaptive Server 会话时也被刷新。

以上两个配置参数所允许的最小值为 1，最大值为 2,147,483,647。

外部鉴定

本章介绍了某些 Adaptive Server 功能，通过这些功能可以用存储在 Adaptive Server 外部存储库中的鉴定数据来鉴定用户。

主题	页码
配置 Adaptive Server 以实现基于网络的安全性	452
并发 Kerberos 鉴定	484
为 LDAP 用户鉴定配置 Adaptive Server	485
为使用 PAM 的鉴定配置 Adaptive Server	504
LDAP 用户鉴定改进	500
增强的登录控制	507

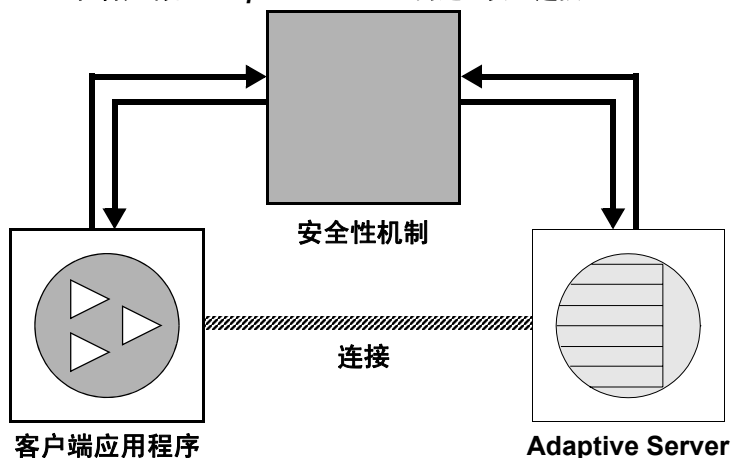
通过使用中央存储库鉴定登录名，可以增强大型异构应用程序的安全性。 Adaptive Server 支持以下外部鉴定方法：

- Kerberos — 可在使用 Kerberos 基础结构的企业环境中，提供一种集中且安全的鉴定机制。使用一台名为密钥分发中心 (KDC) 的第三方受托服务器进行鉴定，以同时验证客户端和服务器。
- LDAP 用户鉴定 — 轻量目录访问协议 (LDAP) 可根据用户的登录名和口令，提供一种集中式鉴定机制。
- PAM 用户鉴定 — 可插入鉴定模块 (PAM) 可以同时为管理和运行时应用程序界面，提供一种集中式鉴定机制，该机制可使用操作系统提供的界面。

配置 Adaptive Server 以实现基于网络的安全性

图 16-1 显示了一个使用安全性机制以确保与 Adaptive Server 的安全连接的客户端应用程序。

图 16-1: 在客户端和 Adaptive Server 之间建立安全连接



客户端和服务端之间的安全连接可用于登录鉴定和消息保护。

如果客户端请求验证服务：

- 1 客户端使用安全性机制验证登录。安全性机制返回一个包含安全性相关信息的认证。
- 2 客户端将认证发送到 Adaptive Server。
- 3 Adaptive Server 使用安全性机制鉴定客户端的认证。如果认证有效，在客户端和 Adaptive Server 之间建立安全连接。

如果客户端请求消息保护服务：

- 1 客户端使用安全性机制来准备将发送到 Adaptive Server 的数据包。
根据所请求的安全服务，安全性机制可能会加密数据或创建一个与数据关联的密码签名。
- 2 客户端将数据包发送到 Adaptive Server。
- 3 当收到数据包时，Adaptive Server 将使用安全性机制执行任何必需的解密和验证操作。
- 4 Adaptive Server 将结果返回给客户端，并使用安全性机制执行所请求安全性功能。例如，Adaptive Server 可能以加密的形式返回结果。

安全服务和 Adaptive Server

根据所选的安全性机制， Adaptive Server 允许您使用以下的一个或多个安全服务：

- 统一登录 — 一次性鉴定用户，而不要求用户每次登录到 Adaptive Server 时都提供用户名和口令。
- 消息保密性 — 加密网络上的数据。
- 相互鉴定 — 验证客户端和服务器的标识。相互鉴定只能由客户端请求；而不能由 Adaptive Server 要求。
- 消息完整性 — 验证数据通信是否未被修改。
- 重放检测 — 验证数据是否被入侵者截取。
- 顺序混乱检查 — 验证数据通信的顺序。
- 消息源检查 — 验证消息源。
- 远程过程安全性 — 为远程过程通信设置相互鉴定、消息保密性和消息完整性。

注释 正在使用的安全性机制可能无法使用上述所有服务。请参见第 472 页的“获取有关可用安全服务的信息”。

管理基于网络的安全性

表 16-1 提供了使用基于网络的安全性功能（由 Adaptive Server 提供）的全部过程。必须先安装 Adaptive Server，然后才能完成表 16-1 中的步骤。

表 16-1：管理基于网络的安全性

步骤	说明	请参见
1. 设置配置文件： • <i>libtcl.cfg</i> • <i>objectid.dat</i> • <i>interfaces</i> （或目录服务）	- 编辑 <i>libtcl.cfg</i> 文件。 - 编辑 <i>objectid.dat</i> 文件。 - 编辑 <i>interfaces</i> 文件或目录服务。	• 第 454 页的“为安全性设置配置文件” • 所用平台的 Open Client/Server Configuration Guide（《Open Client/Server 配置指南》）
2. 确保安全性机制的安全管理员已为每个用户及 Adaptive Server 和 Backup Server 创建了登录。	- 安全管理员必须为安全性机制中的用户和服务器添加名称和口令。 - 对于 DCE，安全管理员必须创建用于服务器条目的 <i>keytab</i> 文件。	• 随安全性机制提供的文档 • 第 460 页的“向安全性机制标识用户和服务器”

步骤	说明	请参见
3. 配置所安装产品的安全性。	使用 <code>sp_configure</code> 。	第 460 页的“配置 Adaptive Server 的安全性”
4. 重新启动 Adaptive Server。	激活 <code>use security services</code> 参数。	所用平台的《配置指南》
5. 将登录添加到 Adaptive Server 以支持企业范围的登录。	使用 <code>sp_addlogin</code> 添加用户。另外，还可以用 <code>sp_configure</code> 指定缺省安全登录。	第 464 页的“添加登录以支持统一登录”
6. 确定用于远程过程的安全模式并设置用于 RPC 安全性的本地和远程服务器。	使用 <code>sp_serveroption</code> 选择安全模式 A 或 B。	第 465 页的“建立远程过程的安全性”
7. 连接到服务器并使用安全服务。	使用 <code>isql_r</code> 或 Open Client Client-Library 连接到 Adaptive Server，并指定要使用的安全服务。	第 470 页的“连接到服务器并使用安全服务” - 所用平台的 Open Client/Server Configuration Guide (《Open Client/Server 配置指南》) 《Open Client Client-Library/C 参考手册》中的“安全性功能”
8. 检查可用的安全服务及安全性机制。	使用函数 <code>show_sec_services</code> 和 <code>is_sec_services_on</code> 检查哪种安全服务可用。 有关 Adaptive Server 所支持的一组安全性机制及其安全服务，可使用 <code>select</code> 来查询 <code>syssecmechs</code> 系统表。	第 472 页的“获取有关可用安全服务的信息”

为安全性设置配置文件

在安装过程中，会在 Sybase 目录结构的缺省位置创建配置文件。

表 16-2: 配置文件的名称和位置

文件名	说明	位置
<i>libtcl.cfg</i>	驱动程序配置文件包含有关目录、安全性和网络驱动程序的信息，还包含任何所需的初始化信息。	UNIX 平台: <code>\$SYBASE/\$SYBASE_OCS/config</code> Windows 平台: <code>%SYBASE%\%SYBASE_OCS%\ini</code>
<i>objectid.dat</i>	此对象标识符文件将全局对象标识符映射为字符集、归类序列和安全性机制的本地名。	UNIX 平台: <code>\$SYBASE/config</code> Windows 平台: <code>%SYBASE%\ini</code>

文件名	说明	位置
UNIX: <i>interfaces</i>	<i>interfaces</i> 文件包含关于文件中所列出的每个服务器的连接和安全性信息。	UNIX 平台: \$SYBASE 桌面平台: SYBASE_home\ini
桌面平台: <i>sql.ini</i>	注释 在 Adaptive Server 12.5.1 及更高版本中, 可以使用目录服务代替 <i>interfaces</i> 文件。	

有关配置文件的详细说明, 请参见所用平台的 Open Client/Server Configuration Guide (《Open Client/Server 配置指南》)。

指定服务器的安全信息

使用 *interfaces* 文件或目录服务, 以提供有关所安装服务器的信息。

interfaces 文件包含服务器的网络及安全性信息。若要使用安全服务, *interfaces* 文件必须包括 “secmech” 行, 该行指定全局标识符或计划使用的安全服务的标识符。

Adaptive Server 支持目录服务以跟踪有关服务器的信息。目录服务管理网络服务器信息的创建、修改和检索。使用目录服务的好处在于, 当网络上新添加服务器或者服务器移动到新地址时, 无须更新多个 *interfaces* 文件。若要将安全服务与目录服务一起使用, 您必须定义 secmech 安全属性, 以指向一个或多个计划使用的安全服务的全局标识符。

指定安全性机制的 UNIX 工具

要定义安全性机制, 请执行以下操作:

- 如果使用的是 *interfaces* 文件, 请使用 dsccp 实用程序。
- 如果使用的是目录服务, 请使用 dsccp_r 实用程序。

注释 UNIX 平台上提供了 dsedit 工具, 该工具可帮助创建 *interfaces* 文件或目录服务的条目。但是, 它不支持创建安全性机制的 secmech 条目。

有关 dsccp 的详细信息, 请参见 《用于 UNIX 的 Open Client/Server 配置指南》。

用于指定服务器属性的桌面工具

若要在 `sql.ini` 文件或目录服务中提供所安装的服务器的信息，请使用 `dsedit` 实用程序。此实用程序提供一个图形用户界面，用来指定服务器属性（如服务器版本、名称和安全性机制）。对于安全性机制属性，可以为计划使用的安全性机制指定一个或多个对象标识符。有关使用 `dsedit` 的信息，请参见 *Open Client/Server Configuration Guide for Desktop Platforms*（《用于桌面平台的 Open Client/Server 配置指南》）。

准备 `libtcl.cfg` 以使用基于网络的安全性

`libtcl.cfg` 和 `libtcl64.cfg`（用于 64 位应用程序）包含有关三种类型驱动程序的信息：

- 网络 (Net-Library)
- 目录服务
- 安全性

驱动程序是一个 Sybase 库，可提供到外部服务提供程序的接口。驱动程序可动态装载，因而，在更改某个应用程序使用的驱动程序时无需重新链接到该应用程序。

网络驱动程序条目

网络驱动程序条目的语法是：

driver=protocol description

其中：

- *driver* — 是网络驱动程序的名称。
- *protocol* — 是网络协议的名称。
- *description* — 是条目说明。此元素可选。

注释 如果不指定网络驱动程序，将自动使用适合您的应用程序和平台的驱动程序。例如，对于 UNIX 平台，在使用安全服务时，会自动选用可以处理线程的驱动程序。

目录服务条目

如果要使用目录服务而不是 *interfaces* 文件，则目录服务条目适用。请参见所用平台的配置文档，以及所用平台的 *Open Client/Server Configuration Guide*（《Open Client/Server 配置指南》）。

安全性驱动程序条目

安全性驱动程序条目的语法为：

provider=driver init-string

其中：

- *provider* — 是安全性机制的本地名。在 *objectid.dat* 中定义本地名到全局对象标识符的映射。

缺省本地名为：

- “dce” — DCE 的安全性机制。
- “csfkrb5” — CyberSAFE 或 MIT Kerberos 的安全性机制。
- “LIBSMSSP” — 用于 Windows NT 或 Windows 95 平台（仅适用于客户端）上的 Windows LAN Manager。

如果使用非缺省的本地机制名称，请在 *objectid.dat* 文件中更改相应的本地名（例如，请参见第 459 页的“*objectid.dat* 文件”）。

- *driver* — 是安全性驱动程序的名称。用于 UNIX 平台的所有驱动程序的缺省位置为 *\$\$SYBASE/\$\$SYBASE_OCS/lib*。驱动程序在 Windows 平台的缺省位置为 *%SYBASE%\%SYBASE_OCS%\dll*。
- *init-string* — 是驱动程序的初始化字符串。此元素可选。不同驱动程序的 *init-string* 值各不相同：
 - DCE 驱动程序 — 以下是 *init-string* 的语法，其中 *cell_name* 是 DCE 单元的名称：

secbase=../../cell_name
 - Kerberos 驱动程序 — 以下是 *init-string* 的语法，其中 *realm* 是缺省的 Kerberos 领域名：

secbase=@realm
 - Windows NT LAN Manager — *init-string* 不适用。

UNIX 平台信息

没有可用于编辑 *libtcl.cfg* 文件的特殊工具。使用您所喜欢的编辑器，注释掉那些在安装 Adaptive Server 后已经存在的条目，或撤消对这些条目的注释。

您在 UNIX 平台上安装 Adaptive Server 后，*libtcl.cfg* 文件已包含对应于文件以下三个部分的条目：

- [DRIVERS]
- [DIRECTORY]
- [SECURITY]

各部分无需依照特定顺序排列。

确保注释那些不想使用的条目（以 “;” 开头），而取消对那些要使用的条目的注释（不以 “;” 开头）。

有关详细信息，请参见 Open Client/Server Configuration Guide for UNIX（《用于 UNIX 的 Open Client/Server 配置指南》）

用于 Sun Solaris 的 *libtcl.cfg* 样本

```
[DRIVERS]
;libtli.so=tcp unused ; This is the non-threaded tli driver.
;libtli_r.so=tcp unused ; This is the threaded tli driver.

[DIRECTORY]
;dce=libsybddce.so ditbase=././subsys/sybase/dataservers
;dce=libsybddce.so ditbase=././users/cfrank

[SECURITY]
dce=libsybsdce.so secbase=./.../svrsole4_cell
```

此 *libtcl.cfg* 文件使用 DCE 安全服务。此文件不使用目录服务，因为所有 [DIRECTORY] 部分的条目均已被注释。

由于 [DRIVERS] 部分中的所有网络驱动程序条目也已被注释，因此系统会自动选择合适的驱动程序。当您使用安全服务时，Adaptive Server 会自动选择线程驱动程序，而对于那些不能使用线程驱动程序的应用程序，则会自动选择非线程驱动程序。例如，Backup Server 不支持安全服务，不使用线程驱动程序。

桌面平台信息

ocscfg 实用程序自动为 *libtcl.cfg* 文件创建节标题；您也可以使用 *ocscfg* 来编辑 *libtcl.cfg* 文件。

以下是用于桌面平台的 *libtcl.cfg* 样本文件：

```
[NT_DIRECTORY]
ntreg_dsa=LIBDREG  ditbase=software\sybase\serverdsa

[DRIVERS]
NLWNSCK=TCP  Winsock TCP/IP Net-Lib driver
NLMSNMP=NAMEPIPE  Named Pipe Net-Lib driver
NLNWLINK=SPX  NT NWLINK SPX/IPX Net-Lib driver
NLDECNET=DECNET  DecNET Net-Lib driver

[SECURITY]
NTLM=LIBSMSSP
```

请参见 *Open Client/Server Configuration Guide for Desktop Platforms*（《用于桌面平台的 Open Client/Server 配置指南》）。

objectid.dat 文件

objectid.dat 文件将全局对象标识符（例如用于 DCE 服务的某个标识符，举例来说，诸如 1.3.6.1.4.1.897.4.6.1 之类的标识符）映射到本地名（例如，“dce”）。*objectid.dat* 文件包括多个部分，例如用于字符集的 [CHARSET] 和用于安全服务的 [SECURITY]。以下是 *objectid.dat* 样本文件：

```
secmech]
    1.3.6.1.4.1.897.4.6.1    = dce
    1.3.6.1.4.1.897.4.6.3    = NTLM
    1.3.6.1.4.1.897.4.6.6    = csfkrb5
```

只有在更改了 *libtcl.cfg* 文件中安全服务的本地名后，才可使用文本编辑器更改此文件。

例如，如果将

```
[SECURITY]
dce=libsybsdce.so  secbase=/.../svrsole4_cell
```

更改为：

```
[SECURITY]
dce_group=libsybsdce.so  secbase=/.../svrsole4_cell
```

请更改 `libtcl.cfg` 中的 `objectid.dat` 反映更改。只需在 `objectid.dat` 中，更改 DCE 行的本地名即可：

```
1.3.6.1.4.1.897.4.6.1    = dce_group
```

注释 只能为每个安全性机制指定一个本地名。

向安全性机制标识用户和服务

安全性机制的安全管理员必须将主管（用户和服务）定义到安全性机制中。[表 16-3](#) 列出了可用于添加用户和服务的工具。

表 16-3：向安全性机制定义用户和服务

安全性机制	命令或工具
DCE	使用 <code>dcecp</code> 的 <code>user</code> 和 <code>create</code> 命令创建一个新主管（用户或服务）。此外，使用 <code>keytab create</code> 命令创建 DCE <code>keytab</code> 文件，此文件包含加密形式的主管口令。 在将服务器定义到 DCE 时，请使用指定新的主管可用作服务器的命令选项。
Kerberos	有关定义用户和服务器的信息，请参见 Kerberos 供应商特定的工具。有关 Kerberos 和 Adaptive Server 的详细信息，请参见 第 474 页的“使用 Kerberos” 。
Windows NT LAN Manager	运行用户管理工具将用户定义到 Windows NT LAN 管理器中。将 Adaptive Server 名称作为用户定义到 Windows NT LAN Manager 中，并将 Adaptive Server 显示为该用户名。

注释 在生产环境中，请控制对包含服务器和用户键的文件的访问。如果用户可以访问这些键，他们就能创建一个服务器来模拟您的服务器。

有关如何执行所需管理任务的详细信息，请参见第三方提供程序提供的安全性机制文档。

配置 Adaptive Server 的安全性

Adaptive Server 包括几个用于管理基于网络的安全性的配置参数。必须是系统安全员才能设置这些参数。用于基于网络的安全性的全部参数都是“安全性相关”配置参数组的一部分。

启用基于网络的安全性

若要启用或禁用基于网络的安全性，请使用 `sp_configure` 来设置 `use security services` 配置参数。

如果 `use security services` 设置为 1，则在以下两个条件同时成立时，Adaptive Server 支持安全性机制：

- `interfaces` 文件或目录服务中列出了安全性机制的全局标识符。
- 在 `objectid.dat` 中，全局标识符映射到 `libtcl.cfg` 中列出的本地名。

有关 Adaptive Server 如何确定用于特定客户端的安全性机制的信息，请参见第 472 页的“使用用于客户端的安全性机制”。

要求统一登录

若要要求安全性机制监控除系统安全员外的所有用户，请将 `unified login required` 配置参数设置为 1。设置了此配置参数后，只有具有 `sso_role` 的用户才能使用用户名和口令登录到服务器：

```
sp_configure "unified login required", [0|1]
```

例如，若要要求所有登录均经过安全性机制的鉴定，请执行：

```
sp_configure "unified login required", 1
```

建立安全缺省登录

当一个具有有效的安全性机制认证的用户登录到 Adaptive Server 时，服务器将检查在 `master.syslogins` 中是否存在该用户名。如果存在，则 Adaptive Server 使用该用户名。例如，如果用户以“ralph”身份登录到 DCE 安全性机制中，且“ralph”存在于 `master.syslogins` 中，则 Adaptive Server 将使用在服务器中为“ralph”定义的所有角色和授权。

但是，如果具有有效凭据的用户登录到 Adaptive Server，但该服务器却不知道该用户，则仅当使用 `sp_configure` 定义了安全缺省登录的情况下，才接受此登录名。Adaptive Server 对未在 `master.syslogins` 中定义但已预先通过安全性机制鉴定的所有用户使用缺省登录名。语法为：

```
sp_configure "secure default login", 0, login_name
```

`secure default login` 的缺省值为“guest”。

安全缺省登录必须是 `master.syslogins` 中的有效登录。例如，若要将“gen_auth”设置为缺省登录：

- 1 使用 `sp_addlogin` 添加该登录作为 Adaptive Server 中的有效用户：

```
sp_addlogin gen_auth, pwgenau
```

此过程将初始口令设置为“pwgenau”。

2 指定该登录作为安全缺省值：

```
sp_configure "secure default login", 0, gen_auth
```

Adaptive Server 对预先通过安全性机制鉴定但 Adaptive Server 不知道的用户使用此登录。

注释 多个用户可使用与安全缺省登录关联的 `suid`。因此，可能需要为缺省登录的全部活动激活审计。可能还要考虑使用 `sp_addlogin` 将所有用户添加到服务器。

请参见第 464 页的“添加登录以支持统一登录”和第 379 页的“将登录添加到 Adaptive Server”。

将安全性机制登录名映射到服务器名

某些安全性机制可能允许在 Adaptive Server 中无效的登录名。例如，长度超过 30 个字符的登录名或包含特殊字符（例如 `!`、`%`、`*` 和 `&`）的登录名在 Adaptive Server 中无效。Adaptive Server 中的所有登录名都必须有效标识符。请参见《参考手册》中的第 3 章“表达式、标识符和通配符”。

表 16-4 显示了 Adaptive Server 如何转换登录名中的无效字符：

表 16-4: 登录名中无效字符的转换

无效字符	转换为
与符号 <code>&</code>	下划线 <code>_</code>
撇号 <code>'</code>	
反斜杠 <code>\</code>	
冒号 <code>:</code>	
逗号 <code>,</code>	
等号 <code>=</code>	
左引号 <code>'</code>	
百分号 <code>%</code>	
右尖括号 <code>></code>	
右引号 <code>'</code>	
变音符号 <code>~</code>	
补注号 <code>^</code>	美元符号 <code>\$</code>
大括号 <code>{ }</code>	
感叹号 <code>!</code>	
左尖括号 <code><</code>	
小括号 <code>()</code>	
句号 <code>.</code>	
问号 <code>?</code>	

无效字符	转换为
星号 *	# 符号
减号 -	
竖线	
加号 +	
引号 "	
分号 ;	
斜杠 /	
方括号 []	

要求使用加密的消息保密性

若要要求对进出 Adaptive Server 的所有消息进行加密，请将 `msg confidentiality reqd` 配置参数设置为 1。如果此参数为 0（缺省值），则不要求消息的保密性，但客户端仍可以建立消息保密性。语法为：

```
sp_configure configuration_parameter, [0 | 1]
```

例如，若要要求对所有消息进行加密，请执行：

```
sp_configure "msg confidentiality reqd", 1
```

要求数据完整性

在 Adaptive Server 中，您可以使用 `msg integrity reqd` 配置参数，来要求检查所有消息中的一种或多种类型数据的完整性。将 `msg integrity reqd` 设置为 1，以要求检查所有消息的常规篡改。如果 `msg integrity reqd` 为 0（缺省值），则不要求消息完整性，但客户端可以建立消息完整性（如果安全性机制支持）。

基于网络的安全性的内存要求

为每个安全连接分配大约 2K 的附加内存。`max total_memory` 配置参数的值指定 Adaptive Server 启动时需要的内存量。例如，如果服务器使用 2K 逻辑页，且如果预计同时发生的安全连接最大数目是 150，请将 `max total_memory` 参数增加 150，这使得内存分配增加了 150 个 2K 块。

语法为：

```
sp_configure "max total_memory", value
```

例如，如果 Adaptive Server 要求 75,000 个 2K 的内存块（包括增加的用于基于网络安全性的内存），请执行：

```
sp_configure "max total_memory", 75000
```

请参见《系统管理指南：卷 2》中的第 3 章“配置内存”。

添加登录以支持统一登录

当用户使用预鉴定凭据登录到 Adaptive Server 时， Adaptive Server 将执行以下操作：

- 1 检查该用户是否为 master..syslogins 中的有效用户。如果用户被列在 master..syslogins 中，则 Adaptive Server 不需要口令就接受此登录。
- 2 如果用户名不在 master..syslogins 中，则 Adaptive Server 检查是否定义了缺省安全登录。如果定义了缺省登录，则该用户将使用缺省值成功登录。如果未定义缺省登录，则用户无法登录。

因此，需要考虑是只允许被定义为有效登录的用户使用 Adaptive Server，还是希望用户能够使用缺省登录进行登录。若要定义缺省值，请在 master..syslogins 中添加缺省登录，并使用 sp_configure。请参见第 461 页的“建立安全缺省登录”。

添加登录的常规过程

按照表 16-5 中介绍的常规过程将登录添加到服务器，并选择将具有相应角色和授权的用户添加到一个或多个数据库。

表 16-5： 添加登录并授权数据库访问

任务	要求的角色	命令或过程	请参见
1. 为用户添加一个登录。	系统安全员	sp_addlogin	第 379 页的“将登录添加到 Adaptive Server”
2. 将用户添加到一个或多个数据库。	系统管理员或数据库所有者	sp_adduser — 从数据库内部执行此过程。	第 381 页的“向数据库添加用户”
3. 将用户添加到数据库中的组。	系统管理员或数据库所有者	sp_changegroup — 从数据库内部执行此过程。	• 第 405 页的“更改用户组成员资格” • 《参考手册》中的 sp_changegroup
4. 为用户授予系统角色。	系统管理员或系统安全员	grant role	• 第 387 页的“为用户创建和指派角色” • 《参考手册》中的 grant
5. 创建用户定义角色并将角色授予用户。	系统安全员	create role grant role	• 《参考手册》中的 第 387 页的“为用户创建和指派角色” • 《参考手册》中的 grant • 《参考手册》中的 create role
6. 授予对数据库对象的访问权。	数据库对象所有者		第 17 章“管理用户权限”

建立远程过程的安全性

当 Adaptive Server 连接到另一台服务器以执行远程过程调用 (RPC) 时，它将充当客户端。

在两台服务器间建立了一个物理连接。服务器使用该物理连接建立一个或多个逻辑连接，每个 RPC 对应一个逻辑连接。

安全模式 A

在安全模式 A（缺省值）中，Adaptive Server 不支持安全服务，例如两台服务器间通过加密实现消息保密的服务。

安全模式 B

在安全模式 B 中，本地 Adaptive Server 从安全性机制接收认证，并使用该认证建立与远程 Adaptive Server 的安全物理连接。通过模式 B，可以使用以下一个或多个安全服务：

- 相互鉴定 — 本地服务器通过检索远程服务器的认证并用安全性机制对其进行验证的方式来鉴定远程服务器。两台服务器的认证都得到鉴定和验证。
- 通过加密获得消息保密性 — 消息在传送给远程服务器时被加密，从远程服务器传来的结果也被加密。
- 消息完整性 — 对服务器之间的消息进行检查以查看数据是否被篡改。

统一登录和远程过程模式

如果本地服务器和远程服务器均设置为使用安全服务，则可以使用以下两种方法中的一种，通过任一种模式在这两台服务器上使用统一登录：

- 系统安全员在远程服务器上使用 `sp_remoteoption` 来将用户定义为“trusted”。诸如 DCE 等安全性机制对用户和口令进行鉴定。用户使用“统一登录”获得对本地服务器的访问权，并执行远程服务器上的 RPC。此用户成为远程服务器的受托用户，不需提供口令。
- 当用户连接到本地服务器时，指定一个远程服务器口令。Open Client Client-Library/C 所附带的 `ct_remote_pwd` 例程提供了用于指定远程服务器口令的功能。请参见《Open Client Client-Library/C 参考手册》。

建立 RPC 安全模式

若要针对 RPC 为模式 A 和 B 建立安全模式，请使用 `sp_serveroption`。语法为：

```
sp_serveroption server, optname, [true | false]
```

若要建立安全模式，请将 `optname` 设置为 `rpc security model A` 或 `rpc security model B`。 `server` 是远程服务器名称。

例如，若要为远程服务器 TEST3 设置安全模式 B，请执行以下命令：

```
sp_serveroption test3, "rpc security model B", true
```

缺省模式为“A”。无需为模式 A 设置任何服务器选项。

请参见《参考手册：过程》。

为 RPC 设置安全模式 B 的规则

为 RPC 设置安全模式 B 时，请遵循以下规则：

- 两台服务器都必须使用安全模式 B。
- 两台服务器必须使用相同的安全性机制，且此安全性机制必须支持用 `sp_serveroption` 设置的安全服务。
- 本地服务器的系统安全员必须指定远程服务器所要求的所有安全服务。例如，如果远程服务器要求所有消息使用消息保密性安全服务，则系统安全员必须使用 `sp_serveroption` 来激活 `use message confidentiality`。
- 对于经过安全性机制鉴定并使用“统一登录”登录到 Adaptive Server 的登录名，将不允许其在远程过程上执行 RPC，除非这些登录名在远程服务器上被指定为“trusted”或者登录名指定了远程服务器口令。用户在使用 Open Client Client-Library 时，可使用例程 `ct_remote_pwd` 来指定服务器到服务器的连接口令。Adaptive Server 上的系统管理员可以使用 `sp_remoteoption` 来指定用户受托使用远程服务器，而无需指定口令。

准备为 RPC 使用安全模式 B

表 16-6 提供了使用安全模式 B 为 RPC 建立安全性的步骤。

表 16-6: 为 RPC 使用安全模式 B

任务、执行者及位置	命令、系统过程或工具	请参见
操作系统的系统管理员: 1. 确保 <i>interfaces</i> 文件或目录 服务包含对应于两台服务器的 条目和列出了安全性机制 的 <i>secmech</i> 行。	UNIX: <i>dscp</i> 桌面: <i>dsedit</i>	第 455 页的“指定服务器的安全 信息” 《用于 UNIX 的 Open Client/Server 配置指南》中的 <i>dscp</i> 《用于桌面平台的 Open Client/Server 配置指南》中的 <i>dsedit</i>
远程服务器上的系统安全员: 2. 将本地服务器添加到 <i>master.syssservers</i> 中。	<i>sp_addserver</i> 示例: <i>sp_addserver lcl_server</i>	第 365 页的“添加远程服务器” 《参考手册》中的 <i>sp_addserver</i> 。
远程服务器上的系统安全员: 3. 将登录添加到 <i>master.syslogins</i> 中。	<i>sp_addlogin</i> 示例: <i>sp_addlogin user1, "pwuser1"</i>	第 379 页的“将登录添加到 Adaptive Server” 《参考手册》中的 <i>sp_addlogin</i>
远程服务器上的系统安全员: 4. 将 <i>use security services</i> 设置为开, 并将 <i>rpc security model B</i> 设置为与本地服务器 进行连接的模式。	<i>sp_configure</i> — 用于设置 <i>use security services</i> 。 <i>sp_serveroption</i> — 用于设置 RPC 安全 模式。 示例: <i>sp_configure "use security services", 1</i> <i>sp_serveroption lcl_server, "rpc security model B", true</i>	第 466 页的“建立 RPC 安全模式” 第 461 页的“启用基于网络的 安全性” 第 5 章“设置配置参数”中的 <i>use security services</i> 《参考手册: 过程》中的 <i>sp_configure</i> 和 <i>sp_serveroption</i> 。
远程服务器上的系统管理员: 5. 或者, 指定某些用户为 “trusted”, 使其不必提供 口令就能从本地服务器登录 到远程服务器。	<i>sp_remoteoption</i> 示例: <i>sp_remoteoption lcl_server, user1, user1, trusted, true</i>	第 374 页的“远程用户的口令 检查” 《参考手册: 过程》中的 <i>sp_remoteoption</i> 。
本地服务器上的系统安全员: 6. 同时将本地服务器和远程 服务器添加到 <i>master.syssservers</i> 中。	<i>sp_addserver</i> 示例: <i>sp_addserver lcl_server, local</i> <i>sp_addserver rem_server</i>	第 365 页的“添加远程服务器” 《参考手册: 过程》中的 <i>sp_addserver</i> 。
本地服务器上的系统安全员: 7. 将登录添加到 <i>master.logins</i> 中。	<i>sp_addlogin</i> 示例: <i>sp_addlogin user1, "pwuser1"</i>	第 379 页的“将登录添加到 Adaptive Server” 《参考手册: 过程》中的 <i>sp_addlogin</i> 。

任务、执行者及位置	命令、系统过程或工具	请参见
本地服务器上的系统安全员： 8. 将 use security services 设置为开，并将 rpc security model B 设置为与远程服务器进行连接的模式。	<code>sp_configure</code> — 用于设置 use security services。 <code>sp_serveroption</code> — 用于设置 RPC 安全模式。 示例： <code>sp_configure "use security services", 1</code> <code>sp_serveroption rem_server, "rpc security model B", true</code>	第 466 页的“建立 RPC 安全模式” 第 461 页的“启用基于网络的安全性” 第 5 章“设置配置参数”中的 <code>use security services</code> 《参考手册：过程》中的 <code>sp_configure</code> 和 <code>sp_serveroption</code> 。
本地服务器上的系统安全员： 9. 指定与远程服务器进行连接时要使用的安全性机制和安全服务。	<code>sp_serveroption</code> 示例： <code>sp_serveroption rem_server, "security mechanism", dce</code> <code>sp_serveroption rem_server, "use message integrity", true</code>	第 367 页的“设置服务器连接选项” 《参考手册：过程》中的 <code>sp_serveroption</code> 。

为 RPC 设置安全模式 B 的示例

此示例假定：

- 本地服务器 “lcl_serv” 将在远程服务器 “rem_serv” 上运行 RPC。
- 两台服务器均使用安全模式 B 及 DCE 安全服务。
- 相互鉴定和消息完整性 RPC 安全服务有效。
- “User1” 和 “user2” 使用统一登录来登录到远程服务器 “lcl_serv”，然后在 “rem_serv” 上运行 RPC。这些用户在 “rem_serv” 上是受托用户，并且无需为远程服务器指定口令。
- “User3” 不使用统一登录，不是受托用户，并且在登录时必须向 Adaptive Server 提供口令。

为服务器之间的 RPC 设置安全性：

`interfaces` 文件或目录服务必须已包含对应于 “rem_serv” 和 “lcl_serv” 的条目。每个条目都应指定 “dce” 安全服务。例如，您可能有以下这些由 `dscp` 实用程序创建的 `interfaces` 条目：

```
## lcl_serv (3201)
lcl_serv
master tli tcp /dev/tcp \x00020c8182d655110000000000000000
query tli tcp /dev/tcp \x00020c8182d655110000000000000000
secmech 1.3.6.1.4.1.897.4.6.1
## rem_serv (3519)
```



```
rem_serv
master tli tcp /dev/tcp \x000214ad82d655110000000000000000
query tli tcp /dev/tcp \x000214ad82d655110000000000000000
secmech 1.3.6.1.4.1.897.4.6.1
```

远程服务器 “rem_serv” 上的系统安全员发出：

```
sp_addserver 'lcl_serv'
sp_addlogin user1, "eracg12"
sp_addlogin user2, "esirpret"
sp_addlogin user3, "drabmok"
sp_configure "use security services", 1
sp_serveroption lcl_serv, "rpc security model B", true
sp_serveroption lcl_serv, "security mechanism", dce
```

远程服务器 “rem_serv” 上的系统管理员发出：

```
sp_remoteoption lcl_serv, user1, user1, trusted, true
sp_remoteoption lcl_serv, user2, user2, trusted, true
```

本地服务器 “lcl_serv” 上的系统安全员发出：

```
sp_addserver lcl_serv, local
sp_addserver rem_serv
sp_addlogin user1, "eracg12"
sp_addlogin user2, "esirpret"
sp_addlogin user3, "drabmol"
sp_configure "use security services", 1
sp_configure rem_serv, "rpc security model B", true
sp_serveroption rem_serv, "security mechanism", dce
sp_serveroption rem_serv, "mutual authentication" true
sp_serveroption rem_serv, "use message integrity" true
```

注释 若要在任一服务器上使用安全性，您必须重新启动服务器，以使 `use security services` 静态参数生效。

获取关于远程服务器的信息

`sp_helpserver` 可显示服务器的有关信息。如果不带参数运行 `sp_helpserver`，它将提供 `sys.servers` 中列出的所有服务器的相关信息。可以指定某一特定服务器来接收有关该服务器的信息。语法为：

```
sp_helpserver [server]
```

例如，若要显示有关 GATEWAY 服务器的信息，请执行：

```
sp_helpserver GATEWAY
```

连接到服务器并使用安全服务

`isql` 和 `bcp` 实用程序包括以下命令行选项，用于对该连接启用基于网络的安全服务：

- `-K keytab_file`
- `-R remote_server_principal`
- `-V security_options`
- `-Z security_mechanism`

这些选项在以下段落中说明。

- `-K keytab_file` — 只能用于 DCE 安全性，并指定 DCE keytab 文件，该文件包含登录到服务器的用户的安全密钥。可以使用 DCE `dcecp` 实用程序创建 keytab 文件 — 请参见 DCE 文档。

如果未提供 `-K` 选项，则 `isql` 用户必须登录到 DCE。如果用户指定 `-U` 选项，则使用 `-U` 指定的名称必须与 DCE 中为用户定义的名称相匹配。

- `-R remote_server_principal` — 像为安全性机制定义那样指定服务器的主管名称。缺省情况下，服务器的主管名称与服务器的网络名（用 `-S` 选项或 `DSQUERY` 环境变量指定）相匹配。当服务器的主管名称和网络名不同时，必须使用 `-R` 选项。
- `-V security_options` — 指定基于网络的用户鉴定。使用此选项时，用户必须在运行实用程序之前登录到网络的安全系统。在这种情况下，如果用户指定了 `-U` 选项，用户必须提供安全性机制所知的网络用户名；使用 `-P` 选项提供的任何口令将被忽略。`-V` 后面可接 `security_options` 关键字字母字符串选项，以启用其它安全服务。这些关键字字母包括：
 - `c` — 启用数据保密性服务。
 - `i` — 启用数据完整性服务。
 - `m` — 启用用于建立连接的相互鉴定。
 - `o` — 启用数据源加戳服务。
 - `r` — 启用数据重放检测。
 - `q` — 启用顺序混乱检测。

- `-Z security_mechanism` — 指定要用于连接的安全性机制名称。

在 `libtcl.cfg` 配置文件中定义安全性机制名称。如果未提供 `security_mechanism` 名称，则使用缺省机制。请参见所用平台的 `Open Client/Server Configuration Guide`（《Open Client/Server 配置指南》）。

如果登录到安全性机制然后又登录到 Adaptive Server，则无需指定 `isql -U` 选项，因为 Adaptive Server 可从安全性机制中获得此用户名。例如，假定有以下会话：

```
svrsole4% dce_login user2
Enter Password:
svrsole4% $SYBASE/bin/isql_r -V
1> select suser_name()
2> go

-----
user2
```

对于此示例，“user2”使用 `dce_login` 登录到 DCE，然后登录到 Adaptive Server，而无需指定 `-U` 选项。不带参数的 `-V` 选项可隐式指定下面这项安全服务：统一登录。

有关 Adaptive Server 实用程序的详细信息，请参见《实用程序指南》。

如果使用 Client-Library 连接到 Adaptive Server，可以在连接到服务器之前定义安全性属性。例如，要检查消息序列，可设置 `CS_SEC_DETECTSEQ` 属性。有关通过 Client-Library 使用安全服务的信息，请参见《Open Client Client-Library/C 参考手册》。

使用安全服务的示例

此示例假定您的登录名为“mary”，并且希望使用实现了统一登录（当您指定 `isql` 或 `bcp` 的 `-V` 选项时，统一登录始终有效）、消息保密性以及用于远程过程的相互鉴定的安全性机制。您想连接到服务器 WOND 并通过相互鉴定的方式在 GATEWAY 上运行远程过程。假定系统安全人员已同时为 `rpc model B` 设置了 WOND 和 GATEWAY，已将您作为用户添加到这两台服务器上，并将您定义为 GATEWAY 上的远程“受托”用户，则您可以使用以下过程：

- 1 登录到 DCE 安全性机制并接收认证：

```
dce_login mary
```

- 2 使用 `isql` 登录到 Adaptive Server：

```
isql -SWOND -Vcm
```

3 运行:

```
GATEWAY...sp_who  
GATEWAY...mary_prc1  
GATEWAY...mary_prc2
```

现在，Mary 发送给服务器或从服务器接收的所有消息都将被加密（消息保密性），并且当她运行远程过程时，WOND 和 GATEWAY 服务器都将被鉴定。

使用用于客户端的安全性机制

Adaptive Server 在启动时确定它支持的一套安全性机制。请参见第 472 页的“[确定所支持的安全服务和机制](#)”。Adaptive Server 必须从支持的安全性机制列表中选择要用于特定客户端的一种机制。

如果客户端指定一种安全性机制（例如，使用 isql 的 -Z 选项指定），则 Adaptive Server 会使用该安全性机制。否则，它使用 *libtcl.cfg* 文件中列出的第一个安全性机制。

获取有关可用安全服务的信息

Adaptive Server 允许您确定：

- Adaptive Server 支持哪些安全性机制和服务
- 当前会话的哪些安全服务处于活动状态
- 是否为会话启用了特定安全服务

确定所支持的安全服务和机制

系统表 *syssecmechs* 提供有关 Adaptive Server 所支持的安全性机制和安全服务的信息。当您查询时，将动态地建立该表。它包含以下这些列：

- *sec_mech_name* — 是安全性机制名称；例如，安全性机制可能是“dce”或“NT LANMANAGER”。
- *available_service* — 是安全性机制所支持的安全服务的名称；例如，安全服务可能是“统一登录”。

有关某一安全性机制的信息可能会占据表的若干行：每行列出该机制所支持的一种安全服务。

若要列出 Adaptive Server 支持的所有安全性机制及服务，请运行：

```
select * from syssecmechs
```

结果可能类似以下内容：

sec_mech_name	available_service
dce	unifiedlogin
dce	mutualauth
dce	delegation
dce	integrity
dce	confidentiality
dce	detectreplay
dce	detectseq

确定活动的安全服务

若要确定当前会话的哪些安全服务处于活动状态，请使用函数 `show_sec_services`：

```
select show_sec_services()

-----
unifiedlogin mutualauth confidentiality
(1 row affected)
```

确定是否启用了某一安全服务

若要确定是否启用了某一特定的安全服务（例如 “mutualauth”），请使用函数 `is_sec_service_on`：

```
is_sec_service_on(security_service_nm)
```

其中 `security_service_nm` 是可用的安全服务：

使用在查询 `syssecmechs` 时返回的安全服务器。

例如，若要确定是否启用了 “mutualauth”，请执行：

```
select is_sec_service_on("mutualauth")

-----
1
(1 row affected)
```

结果为 1 表明已为会话启用了安全服务。结果为 0 表明未使用此服务。

使用 Kerberos

Kerberos 是一种网络鉴定协议，它使用密钥密码技术，以便客户端可以通过网络连接向服务器证明其身份。当用户登录到操作系统或执行鉴定程序时，将获得用户认证。各个应用程序将使用这些认证执行鉴定。用户只需登录一次，而不必登录到每个应用程序。

Kerberos 假设密钥分发中心 (KDC) 正在运行并针对您的领域进行了适当的配置，而且客户端库安装在领域中的每个客户端主机下或主机上。有关配置信息，请参见文档和 Kerberos 软件附带的参考页。

Adaptive Server 通过以下库来支持 Kerberos：

- CyberSafe Kerberos 库
- MIT Kerberos 库 1.3.1 版
- 本机库

注释 若要启用 Kerberos 安全性选项，您必须拥有 ASE_SECDIR，即“安全和目录服务”软件包。

Kerberos 兼容性

表 16-7 显示哪个平台支持哪一种 Kerberos。

表 16-7: Adaptive Server Kerberos 互操作性

硬件平台	KDC 服务器	通用安全标准 (GSS) 客户端
Solaris 32	CSF、AD 或 MIT	CSF、MIT 或本机
Solaris 64	CSF、AD 或 MIT	CSF、MIT 或本机
Linux 32	CSF、AD 或 MIT	MIT 或本机
Windows 32	CSF 或 AD	CSF
AIX 32	CSF	CSF

使用以下密钥读取互操作性矩阵：

- CSF — CyberSafe Ltd.
- AD — Microsoft Active Directory
- MIT — MIT 1.3.1 版

在 Kerberos 下启动 Adaptive Server

若要在 Kerberos 下启动 Adaptive Server，请将 Adaptive Server 名称添加到 KDC 中，并将服务键提取到键表文件。例如：

```
/krb5/bin/admin admin/ASE -k -t /krb5/v5srvtab -R"
addrn my_ase; mod
my_ase attr nopwchg; ext -n my_ase eytabfile.krb5"
Connecting as: admin/ASE
Connected to csfA5v01 in realm ASE.
Principal added.
Principal modified.
Key extracted.
Disconnected.
```

注释 也可以使用命令行上的口令鉴定管理员。在本例中，使用了 `-k` 选项，该选项指示管理员搜索 `/krb5/v5srvtab` 文件（使用 `-t` 选项指定）中是否有管理员和 Adaptive Server 键，而不是提示输入用于编写 shell 脚本的口令。

配置 Kerberos

不管使用哪一种 Kerberos，其配置过程都是相似的。

- 1 设置 Kerberos 第三方软件，并创建一个 Kerberos 管理用户。为此，必须执行以下操作：
 - a 在将要运行 Open Client Server 客户端或 Adaptive Server 的计算机上安装 Kerberos 客户端软件。以下客户端软件包已经过验证，可以运行：
 - CyberSafe TrustBroker 4.0
 - MIT Kerberos 1.3.1 版
 - b 在一台单独的专用计算机上安装 Kerberos KDC 服务器。

注释 CyberSafe TrustBroker 4.0、MIT Kerberos 1.3.1 版和 Microsoft Windows Active Directory 中的 KDC 已经通过验证，可与 Adaptive Server 一起使用。

- c 在 Kerberos 服务器上创建具有管理权限的管理员帐户。此帐户用于后续的客户端操作（例如从客户端计算机中创建主管）。

注释 在 Kerberos 客户端计算机上执行其余步骤。

- 2 为 Adaptive Server *ase120srv* 或 *ase120srv@MYREALM* 添加 Kerberos 主管。
- 3 为主管 *ase120srv@MYREALM* 提取 *keytab* 文件，并将其作为文件存储：

/krb5/v5srvtab

以下 UNIX 示例使用了可用于 CyberSafe 或 MIT Kerberos 的命令行工具 *kadmin*（此外还有 GUI 工具，可用于管理 Kerberos 及用户）：

```
CyberSafe Kadmin:
% kadmin aseadmin
Principal - aseadmin@MYREALM
Enter password:
Connected to csfA5v01 in realm ASE.
Command: add ase120srv
Enter password:
Re-enter password for verification:
Principal added.
Command: ext -n ase120srv
Service Key Table File Name (/krb5/v5srvtab):
Key extracted.
Command: quit
Disconnected.
```

在生产环境中，请控制对 *keytab* 文件的访问。如果用户可以读取 *keytab* 文件，则该用户就能创建一个服务器来模拟您的服务器。

使用 *chmod* 和 *chgrp* 命令，以使 */krb5/v5srvtab* 文件变为以下形式：

```
-rw-r----- 1 root sybase 45 Feb 27 15:42 /krb5/v5srvtab
```

在将 Active Directory 用作 KDC 时，请登录到域控制器以添加用户和 Adaptive Server 主管。可使用“Active Directory 用户和计算机向导”来引导您完成创建用户及主管的过程。

提取用于 Adaptive Server 的 *keytab* 文件需要一个名为 *ktpass* 的可选工具，该工具包含在 Microsoft 支持工具软件包中。

对于 Active Directory，使用 *ktpass* 提取 *keytab* 是独立于创建主管操作的一个步骤。在 Windows 上，用于 Adaptive Server 的 *keytab* 文件与 CyberSafe 程序文件放在一起。例如，如果将 CyberSafe 软件安装在驱动器 C: 上，则 *c:\Program Files\CyberSafe\v5srvtab* 就是 Adaptive Server *keytab* 文件的预期位置。

- 4 为用户“sybuser1”添加名为“sybuser1@MYREALM”的 Kerberos 主管。

- 5 启动 Adaptive Server，并使用 `isql` 命令以 “sa” 身份登录。以下步骤用于配置 Adaptive Server 参数，以便使用 Kerberos 安全服务，并创建用户登录帐户。以下步骤在 Windows 或 UNIX 计算机上都是相同的：

- 将配置参数 `use security services` 更改为 1：

```
sp_configure 'use security services', 1
```

- 为用户 “sybuser1” 添加新登录，然后添加用户：

```
sp_addlogin sybuser1, password
```

- 6 关闭 Adaptive Server，并修改管理文件和连接配置文件。

- 在 UNIX 平台上，`interfaces` 文件位于 `$$SYBASE/` 下，并包含一个类似于以下内容的条目：

```
ase120srv
    master tli tcp myhost 2524
    query tli tcp myhost 2524
    secmech 1.3.6.1.4.1.897.4.6.6
```

在 Windows 平台上，`sql.ini` 文件位于 `%SYBASE%\ini` 下，并包含一个类似于以下内容的等价的服务器条目：

```
[ase120srv]
master=TCP,myhost,2524
query=TCP,myhost,2524
secmech=1.3.6.1.4.1.897.4.6.6
```

- `libtcl.cfg` 或 `libtcl64.cfg` 文件位于 UNIX 平台上的 `$$SYBASE/$$SYBASE_OCS/config/` 中。“SECURITY” 部分应该包含一个用于 CyberSafe Kerberos 客户端库的条目，与以下内容相似：

```
[SECURITY]
csfkrb5=libsybskrb.so secbase=@MYREALM
libgss=/krb5/lib/libgss.so
```

以下是 64 位 CyberSafe Kerberos 客户端库条目：

```
[SECURITY]
csfkrb5=libsybskrb64.so secbase=@MYREALM libgss=
\
/krb5/appsec-rt/lib/64/libgss.so
```

对于使用 MIT Kerberos 客户端库的计算机，相应的条目与以下内容相似：

```
[SECURITY]
csfkrb5=libsybskrb.so
secbase=@MYREALM
libgss=/opt/mitkrb5/lib/libgssapi_krb5.so
```

对于使用本机操作系统（例如 Linux）提供的库的计算机，相应的条目与以下内容相似：

```
[SECURITY]
csfkrb5=libsybskrb.so secbase=@MYREALM
libgss=/usr/kerberos/lib/libgssapi_krb5.so
```

在 Windows 上，%SYBASE%\%SYBASE_OCS%\ini\libtcl.cfg 文件包含如下条目：

```
[SECURITY]
csfkrb5=libskrb secbase=@MYREALM
libgss=C:\WinNT\System32\gssapi32.dll
```

注释 libgss=<gss 共享对象路径> 指定要使用的 GSS API 库。您必须直接定位到正在使用的 Kerberos Client 库，特别是当一台计算机上安装了多个版本时更是如此。

- 还要检查 \$SYBASE/\$SYBASE_OCS/config/ 下的 objectid.dat，并确保 [secmech] 部分包含用于 csfkrb5 的条目：

```
[secmech]
1.3.6.1.4.1.897.4.6.6 = csfkrb5
```

- 7 可以使用环境变量来替换 keytab 文件、Kerberos 配置以及领域配置文件的缺省位置。这是 Kerberos 特有的行为，可能不会在所有平台上都能工作。

例如，在 CyberSafe UNIX 平台上使用 CSFC5KTNAME 环境变量来指定 keytab 文件：

```
% setenv CSFC5KTNAME /krb5/v5srvtab
```

对于 MIT Kerberos，等同的环境变量是 KRB5_KTNAME。

有关这些环境变量的信息，请参见供应商文档。

您可能需要为动态库搜索路径修改环境变量。在 UNIX 上，最常用的环境变量是 LD_LIBRARY_PATH；在 Windows 上，PATH 通常设置为包括 DLL 位置。可能需要修改这些环境变量，以使应用程序能够正确装载第三方对象。例如，在 C-shell 环境下，下面的命令将把 CyberSafe 32 位 *libgss.so* 共享对象的位置添加到搜索路径中：

```
% set path = ( /krb5/lib $path )
```

- 8 重新启动 Adaptive Server。您应会看到：

```
00:00000:00000:2001/07/25 11:43:09.91 server
Successfully initialized the security mechanism
'csfkrb5'.The SQL Server will support use of this
security mechanism.
```

- 9 以 UNIX 用户 “sybuser1” 的身份使用 isql（不带 -U 和 -P 参数）进行连接：

```
% $SYBASE/$SYBASE_OCS/bin/isql -Sase120srv -V
1>...
```

也可以使用加密选项：

```
$SYBASE/$SYBASE_OCS/bin/isql -Sase120srv -Vc
```

使用主管名

主管名是服务器向 Kerberos 密钥分发中心 (KDC) 进行鉴定时使用的名称。如果有多个正在运行的 Adaptive Server 实例，则必须为每个 Adaptive Server 使用不同的主管名。

指定 Adaptive Server 主管名

使用 DSLISTEN 和 DSQUERY 环境变量或 `dataserver -sserver_name` 命令行选项来指定 Adaptive Server 名称。

使用 `setenv` 命令或 `-k dataserver` 选项来设置主管名。

缺省情况下，主管名为 Adaptive Server 名称。若要指定不同的名称，请在启动 Adaptive Server 以使用 Kerberos 之前设置 SYBASE_PRINCIPAL：

```
setenv SYBASE_PRINCIPAL <name of principal>
```

一旦设置了 Adaptive Server 主管名，Adaptive Server 即使用此变量的值向 Kerberos 鉴定自身。

若要在启动 Adaptive Server 时指定 Adaptive Server 主管名，请使用：

```
-k <server principal name>
```

在启用了 Kerberos 安全性机制的情况下启动 Adaptive Server 时，Adaptive Server 首先会使用 `-k` 选项指定的主管名进行 Kerberos 鉴定。如果未指定 `-k` 选项，则 Adaptive Server 将在环境变量 `SYBASE_PRINCIPAL` 中查找主管名。如果两者均未指定，则 Adaptive Server 使用服务器名进行鉴定。

如果 `keytab` 文件中存在主管名条目，则 Adaptive Server 接受使用不同服务器主管名的 Kerberos Open Client 连接。允许使用不同主管名的连接：

- 传递一个空字符串作为 `-k` 选项的参数，或者
- 将 `SYBASE_PRINCIPAL` 环境变量设置为 ""。例如：

```
export SYBASE_PRINCIPAL=""
```

示例

在此示例中，Adaptive Server 名称是 “secure_ase”，领域名是 “MYREALM.COM”。Adaptive Server 名称是使用 `dataserver` 的 `-s` 参数在命令行上指定的。当前领域是在 `libtcl.cfg` 中由 `secbase` 属性值指定的：

```
[SECURITY]
csfkrb5=libskrb.so libgss=/krb5/lib/libgss.so
secbase=@MYREALM.COM
```

缺省 Adaptive Server 主管名为 “secure_ase@MYREALM.COM”。如果 Adaptive Server `keytab` 文件中定义的主管名为 “aseprincipal@MYREALM.COM”，您可以使用下面的选项 1 或 2 设置服务器主管名，从而覆盖缺省 Adaptive Server 主管名：

- 选项 1，指定 `-k`：

```
%
$SYBASE/$SYBASE_ASE/bin/dataserver -dmaster.dat
-s secure_ase -k aseprincipal@MYREALM.COM
```

通过 Kerberos 进行鉴定时使用的 Adaptive Server 主管名为 “aseprincipal@MYREALM.COM”。

- 选项 2，设置 `SYBASE_PRINCIPAL`：

```
setenv SYBASE_PRINCIPAL aseprincipal@MYREALM.COM
$SYBASE/$SYBASE_ASE/bin/dataserver -dmaster.dat
-s secure_ase
```

通过 Kerberos 进行鉴定时使用的 Adaptive Server 主管名为 “aseprincipal@MYREALM.COM”，即 `$SYBASE_PRINCIPAL` 的值。

- 选项 3，既不设置 `-k` 也不设置 `SYBASE_PRINCIPAL`：

```
% $SYBASE/$SYBASE_ASE/bin/dataserver -dmaster.dat
-s secure_ase
```

通过 Kerberos 进行鉴定时使用的 Adaptive Server 主管名为 “secure_ase@MYREALM.COM”。

使用 `sybmapname` 处理用户主管名

`sybmapname` 将 Kerberos 环境中使用的外部用户主管名转换为 Adaptive Server 用户登录名的命名空间。您可以自定义 `sybmapname` 共享对象，并将 Kerberos 输入缓冲区中指定的名称映射为适合于登录到 Adaptive Server 输出缓冲区的名称。

使用 `sybmapname` 共享对象来执行用户主管名和 Adaptive Server 登录名之间的自定义映射。可以选择在服务器启动时装载此共享对象，在成功完成 Kerberos 鉴定之后、用户主管名映射到 `syslogins` 表中的登录名之前，将调用此共享对象中包含的函数 `syb__map_name`。当要映射的用户主管名和登录名不同时，此函数很有用。

```
syb__map_name(NAMEMAPTYPE *protocol, char *orig,
              int origlen, char *mapped, int *mappedlen)
```

其中：

- `NAMEMAPTYPE *protocol` — 是为使用此函数而保留的结构。
- `char *orig` — 是输入缓冲区，该缓冲区不以 `null` 终止。
- `int origlen` — 是输入缓冲区长度，应小于或等于 255 个字符。
- `char *mapped` — 是输出缓冲区，该缓冲区不应以 `null` 终止。
- `int *mappedlen` — 是输出缓冲区长度，应小于或等于 30。

如果映射成功，`syb__map_name` 将返回大于 0 的值，或者，如果未发生映射，则返回值 0，而当 `syb__map_name` 中发生错误时则返回小于 0 的值。发生错误时，将向 Adaptive Server 错误日志中写入报告映射失败的内容。

例如，若要鉴定 Adaptive Server 上的 Kerberos 用户：

- 1 配置 Adaptive Server 以使用 Kerberos 安全性机制。请参见第 474 页的“使用 Kerberos”和 Open Client/Server 文档，以及 Sybase 网站 (<http://www.sybase.com/detail?id=1029260>) 上标题为“为 Sybase 配置 Kerberos” (Configuring Kerberos for Sybase) 的白皮书。

`$$SYBASE/$SYBASE_ASE/sample/server/sybmapname.c` 中有一个示例文件 `sybmapname.c`。

- 2 修改 `sybmapname.c` 以执行您的逻辑。请参见第 484 页的“使用 `sybmapname` 时的注意事项”。
- 3 使用提供的通用平台专用的 `makefile` 生成共享对象或 DLL。可能需要修改 `makefile` 以适合您的平台特定设置。

- 4 请将生成的共享对象放在 `$LD_LIBRARY_PATH`（UNIX 计算机）和 `PATH` 变量（Windows 计算机）中指定的位置。“sybase”用户应该具有该文件的读取和执行权限。

注释 Sybase 建议只赋予“sybase”用户读取和执行权限，并应当拒绝所有其它访问权限。

使用 Kerberos 鉴定来验证您的 Adaptive Server 登录

若要使用 Kerberos 鉴定来验证您的 Adaptive Server 登录，请假设：

- `$$SYBASE` 是指您的版本和安装目录。
- `$$SYBASE_ASE` 是指包含服务器二进制文件的 Adaptive Server 版本目录。
- `$$SYBASE_OCS` 是指 Open Client/Server 版本目录。

示例 1 如果客户端的主管名为 `user@REALM`，并且 `syslogins` 表中对应的条目为 `user_REALM`，则可以对 `sybmapname` 进行编码，以接受输入字符串 `user@realm`，并将输入字符串转换为输出字符串 `user_REALM`。

示例 2 如果客户端主管名为 `user`，并且 `syslogins` 表中的对应条目为 `USER`，则可以对 `sybmapname` 进行编码，以接受输入字符串 `user`，并将此字符串转换为大写字符串 `USER`。

`sybmapname` 由 Adaptive Server 在运行时装载并使用其逻辑进行必要的映射。

以下操作和输出阐释了示例 2 中描述的 `sybmapname` 函数。应将包含 `syb_map_name()` 的自定义定义的 `sybmapname.c` 文件作为共享对象（或 DLL）来编译和生成，并最终放在合适的路径位置。在启用了 Kerberos 安全性机制的情况下启动 Adaptive Server。

对提供标识的加密文件“票证授予票证 (TGT)”进行初始化：

```
$ /krb5/bin/kinit johnd@public
Password for johnd@public:
$
```

列出 TGT：

```
$ /krb5/bin/klist
Cache Type: Kerberos V5 credentials cache
Cache Name: /krb5/tmp/cc/krb5cc_9781
Default principal: johnd@public
```

以 “sa” 身份登录并验证 “johnd” 的用户登录名:

```
$ $SYBASE/$SYBASE_OCS/bin/isql -Usa -P  
-Ipwd\interfaces  
1>  
  
1> sp_displaylogin johnd  
2> go  
No login with the specified name exists.  
(return status = 1)  
  
1> sp_displaylogin JOHND  
2> go  
Suid: 4  
Loginame: JOHND  
Fullname:  
Default Database: master  
Default Language:  
Auto Login Script:  
Configured Authorization:  
Locked: NO  
Password expiration interval: 0  
Password expired: NO  
Minimum password length: 6  
Maximum failed logins: 0  
Current failed login attempts:  
Authenticate with: ANY  
(return status = 0)
```

Kerberos 鉴定成功, 使用 `sybmapname` 实用程序将小写的 johnd 映射到大写的 JOHND, 并允许用户 johnd 登录到 Adaptive Server:

```
$ $SYBASE/$SYBASE_OCS/bin/isql -V -I'pwd\interfaces  
1>
```

使用 `sybmapname` 时的注意事项

对 `sybmapname` 进行编码时：

- 修改 `sybmapname.c` 样本程序时要小心。避免使用可能生成分段错误、可能调用 `exit`、可能调用 `system calls`、可能更改 UNIX 信号或进行任何阻塞调用的代码。不正确的编码或调用可能会干扰 Adaptive Server 引擎。

注释 Sybase 不对 `sybmapname` 中的编码错误承担任何责任。

- 编码时应当小心，在不再引用指针之前请检查所有指针，并避免系统调用。您编写的函数必须为快速名称过滤函数。
- 不要使用 `goto` 语句，因为这些语句可能导致无法预料的副作用，具体取决于平台。
- 如果使用多个领域，在将用户主管名映射到合适的登录名以反映领域信息要小心。例如，如果您拥有的两个用户的用户主管名分别为 `userA@REALMONE` 和 `userB@REALMTWO`，请将它们映射到登录名 `userA_REALMONE` 和 `userB_REALMTWO`，而不是 `userA` 或 `userB`。这样可区别两个属于不同领域的用户。

并发 Kerberos 鉴定

Adaptive Server 15.0.3 版支持并发 Kerberos 鉴定，而早期版本则在 Kerberos 鉴定过程中使用锁定机制来保护内部数据结构。

如果存在使用 Kerberos 鉴定的并发登录，Adaptive Server 现在将建立多个 Kerberos 鉴定会话。

15.0.3 版还解决了并发登录会话在 Kerberos 鉴定过程中可能会被阻塞的问题。当您将 Adaptive Server 以前的版本与 MIT 1.3.x 版和 1.4.x Kerberos GSSAPI 库一起使用时，将发生此并发问题。

为 LDAP 用户鉴定配置 Adaptive Server

LDAP 用户鉴定允许客户端应用程序将用户名和口令信息发送到 Adaptive Server，以便通过 LDAP 服务器（而不是 `syslogins`）进行鉴定。通过 LDAP 服务器进行鉴定时，您可以使用全服务器范围的口令，而不使用 Adaptive Server 或特定于应用程序的口令。

如果希望对用户管理进行简化和集中，或者要避免用户管理不必要的复杂情况，则 LDAP 用户鉴定非常理想。

LDAP 用户鉴定可与符合 LDAP 协议标准版本 3 的目录服务器（包括 Active Directory、iPlanet 和 OpenLDAP Directory Server）一起使用。

为 LDAP 用户鉴定使用以下鉴定算法之一：

- 用于鉴定的组合型 DN，可用于 Adaptive Server 12.5.1 版或更高版本，或者
- 用于鉴定的搜索型 DN，可用于 Adaptive Server 12.5.2 版及更高版本。

这些算法在获取用户的区分名 (DN) 的方式上有所不同。

用于 LDAP 协议的主数据结构为 LDAP URL。

LDAP URL 会在 LDAP 服务器上指定一组对象或值。Adaptive Server 使用 LDAP URL 来指定用于鉴定登录请求的 LDAP 服务器和搜索条件。

LDAP URL 使用以下语法：

```
ldapurl::=ldap://host:port/node/attributes [base | one | sub] filter
```

其中：

- *host* — 是 LDAP 服务器的主机名。
- *port* — 是 LDAP 服务器的端口号。
- *node* — 指定对象层次中搜索开始处的节点。
- *attributes* — 是要返回到结果集中的属性列表。每个 LDAP 服务器都可能支持不同的属性列表。
- *base | one | sub* — 限定搜索条件。*base* 指定搜索基准节点；*one* 指定搜索基准节点以及基准节点下面的一个子级别；*sub* 指定搜索基准节点及所有节点子级别。
- *filter* — 指定要鉴定的一个或多个属性。过滤器可以是简单的，例如 `uid=*`；也可以是复合的，例如 `(uid=*) (ou=group)`。

组合型 DN 算法

这是在使用组合型 DN 算法时的登录顺序：

- 1 Open Client 连接到 Adaptive Server 监听器端口。
- 2 Adaptive Server 监听器接受连接。
- 3 Open Client 发送一个内部登录记录。
- 4 Adaptive Server 读取该登录记录。
- 5 Adaptive Server 使用由主 URL 组成的 DN 和登录记录中的登录名绑定到 LDAP 服务器。此绑定还使用登录记录中的口令。
- 6 LDAP 服务器对用户进行鉴定，并返回成功或失败消息。
- 7 如果主 URL 指定一个搜索，那么 Adaptive Server 会向 LDAP 服务器发送搜索请求。
- 8 LDAP 服务器返回搜索的结果。
- 9 Adaptive Server 根据搜索结果接受或拒绝登录。

搜索型 DN 算法

这是在使用搜索型 DN 算法时的登录顺序：

- 1 Open Client 连接到 Adaptive Server 监听器端口。
- 2 Adaptive Server 监听器接受连接。
- 3 Open Client 发送一个内部登录记录。
- 4 Adaptive Server 读取该登录记录。
- 5 Adaptive Server 使用目录服务器访问帐户绑定到 LDAP 服务器。
在步骤 5 和 6 中建立的连接可能会在来自 Adaptive Server 的鉴定尝试之间持续存在，以便重复使用这些连接进行 DN 搜索。
- 6 LDAP 服务器对用户进行鉴定，并返回成功或失败消息。
- 7 Adaptive Server 根据登录记录中的登录名和 DN 查找 URL 向 LDAP 服务器发送搜索请求。
- 8 LDAP 服务器返回搜索的结果。
- 9 Adaptive Server 读取结果以从 DN 查找 URL 中获取属性值。
- 10 Adaptive Server 将属性值用作登录记录中的 DN 和口令，以绑定到 LDAP 服务器。

- 11 LDAP 服务器对用户进行鉴定，并返回成功或失败消息。
- 12 如果主 URL 指定一个搜索，那么 Adaptive Server 会向 LDAP 服务器发送搜索请求。
- 13 LDAP 服务器返回搜索的结果。
- 14 Adaptive Server 根据搜索结果接受或拒绝登录。

如果不满足这些搜索条件中的任意一个，Adaptive Server 都会向客户端报告常规登录失败。

如果不在主 URL 字符串或辅助 URL 字符串中指定搜索条件，就可以跳过步骤 12 和 13。鉴定完成，并显示步骤 11 返回的成功或失败消息。

配置 LDAP

在新安装的 Adaptive Server 中配置 LDAP

以下是配置 Adaptive Server 以进行 LDAP 鉴定的步骤。

- 1 指定 Adaptive Server LDAP URL 搜索字符串和访问帐户值。
- 2 将 `enable ldap user auth` 设置为 2。
- 3 使用 LDAP 供应商提供的工具将用户添加到 LDAP 目录服务器中。
- 4 使用 `sp_addlogin` 将用户添加到 Adaptive Server。也可以使用 `sp_maplogin` 自动创建用于鉴定的登录帐户或应用其它登录控制。

将现有 Adaptive Server 迁移到 LDAP

若要避免在现有服务器安装中出现服务中断，请将 Adaptive Server 迁移到 LDAP：

- 指定一个针对 Adaptive Server 的 LDAP URL 搜索字符串。
- 将配置参数 `enable ldap user auth` 设置为 1。
- 将用户添加到 LDAP 目录服务器中。
- 将所有用户添加到 LDAP 服务器时，将 `enable ldap user auth` 设置为 2，以要求通过 LDAP 执行所有鉴定，或者使用 `sp_maplogin` 将配置参数替换为登录控制。

LDAP 用户鉴定管理

使用 `sp_ldapadmin` 创建或列出 LDAP URL 搜索字符串，验证 LDAP URL 搜索字符串或登录，并指定访问帐户以及可调优 LDAP 用户鉴定 (LDAPUA) 相关参数。必须具有 SSO 角色才能执行 `sp_ldapadmin`。

请参见《参考手册：命令》。

组合型 DN 示例

如果使用简单 LDAP 服务器拓扑和模式，则可以使用组合型 DN 算法进行用户鉴定。如果使用通过商业途径获得的模式（例如，iPlanet Directory Server 或 OpenLDAP Directory Server），则会将用户创建为 LDAP 服务器树上同一容器中的对象，并且 Adaptive Server 会根据对象的位置确定用户的 DN。但是，LDAP 服务器的模式有以下限制：

- 必须使用唯一地标识要鉴定用户的属性名指定过滤器。
- 必须将过滤器的属性指定为 `name=*`。星号为通配符。适合在过滤器中使用的属性名取决于 LDAP 服务器使用的模式。
- Adaptive Server 登录名与短用户名（如 UNIX 用户名）相同。
- DN 使用短用户名，而不使用嵌入空格或标点符号的全名。例如，`jqpublic` 符合 DN 的限制，而 “John Q. Public” 则不符合这一限制。

iPlanet 示例

LDAP 供应商所使用的对象名、模式和属性与以下示例中所用的对象名、模式和属性可能有所不同。可能存在许多 LDAP URL 搜索字符串，有效节点也可能会以本地方式扩展模式，或者以各不相同的方式使用它们：

- 此示例使用 `uid=*` 过滤器。为了组成 DN，Adaptive Server 会将通配符替换为要鉴定的 Adaptive Server 登录名，并在 LDAP URL 中将结果过滤器附加到节点参数中。得到的 DN 为：

```
uid=myloginname,ou=People,dc=mycompany,dc=com
```

- 成功完成绑定操作后，Adaptive Server 会使用连接来搜索等效于登录名的属性名（例如 `uid`）：

```
sp_ldapadmin set_primary_url,  
'ldap://myhost:389/ou=People,dc=mycompany,dc=com??sub?uid=*
```

- 此示例使用 OpenLDAP 2.0.25 中定义的模式，属性名为 `cn`。

组成的 DN 为 `cn=myloginname,dc=mycompany,dc=com`：

```
sp_ldapadmin set_primary_url,  
'ldap://myhost:389/dc=mycompany,dc=com??sub?cn=*
```

搜索型 DN 示例

通过搜索型 DN，可以使用不符合组合型 DN 算法使用限制的 Active Directory 服务器或其它 LDAP 服务器环境。

- 使用 Windows 2000 Server 中通过商业途径获得的用户模式，对 Active Directory 服务器执行以下步骤。

a 设置访问帐户信息：

```
sp_ldapadmin set_access_acct,
'cn=Admin Account, cn=Users, dc=mycompany, dc=com',
'Admin Account secret password'
```

b 设置主 URL：

```
sp_ldapadmin set_primary_url, 'ldap://hostname:389/'
```

c 设置 DN 查找 URL 搜索字符串：

```
sp_ldapadmin set_dn_lookup_url,
'ldap://hostname:389/cn=Users,dc=mycompany,dc=com?distinguishedName?one?samaccountname=*'
```

在 Windows 2000 上，短名称通常称为“用户登录名”，并在缺省模式下被赋予属性名 `samaccountname`。这是用于匹配 Adaptive Server 登录名的属性名。用户的 DN 中包含一个带有标点符号和嵌入空格的全名（例如，`cn=John Q. Public, cn=Users, dc=mycompany, dc=com`）。Windows 上的 DN 不使用短名称，因此对于将 Active Directory 模式（缺省值）用作 LDAP 服务器的节点而言，搜索型 DN 算法较合适。主 URL 不指定搜索，而是依赖于绑定操作进行鉴定。

使用搜索过滤器限制
Adaptive Server 访问
的示例

可以使用 LDAP URL 搜索字符串来限制对 LDAP 服务器上用户组的访问。例如，若要限制 `accounting` 组中用户的登录，可使用组合过滤器来限制对该用户组的访问，其中属性为 `group=accounting`。

- 以下 LDAP URL 字符串对 iPlanet 服务器使用组合型 DN 算法：

```
sp_ldapadmin set_primary_url,
'ldap://myhost:389/ou=People,dc=mycompany,
dc=com??sub?(&(uid=*)(group=accounting))'
```

Adaptive Server 与 DN

`uid=mylogin,ou=People,dc=mycompany,dc=com` 绑定在一起。成功绑定到此标识后，它会搜索以下内容：

```
"ou=People,dc=mycompany,dc=com??sub?(&(uid=mylogin)(group=accounting))"
```

如果此搜索返回任何对象，则表明鉴定成功。

- 以下示例将 LDAP URL 字符串用于组合过滤器：

```
sp_ldapadmin set_primary_url,
'ldap://myhost:389/ou=people,dc=mycompany,dc=com??s
ub?(&(uid=*)(ou=accounting) (l=Santa Clara))'

sp_ldapadmin, set_primary_url,
'ldap://myhost:389/ou=people,dc=mycompany,dc=com??s
ub?(&(uid=*)(ou=Human%20Resources))'
```

LDAP 用户鉴定口令信息的更改

有两种与 LDAP 用户鉴定相关的信息性消息，Adaptive Server 从 LDAP 服务器获取这些消息并传递到客户端：

- 在使用 LDAP 鉴定机制登录到 Adaptive Server 时，如果 LDAP 用户鉴定口令即将到期，您将看到：

```
Your password will expire in <number> days.
```

- 在 LDAP 服务器管理员重置了您的口令或者您的 LDAP 服务器口令已经到期之后，如果试图使用 LDAP 鉴定机制登录到 Adaptive Server，则会看到 4002 消息：

```
Login failed
```

如果启用了审计且打开了 **errors** 审计选项，则会将消息 4099 发送到审计日志：

```
Your LDAP password has expired.
```

注释 请配置 LDAP 服务器以提供此附加信息。此外，Adaptive Server 必须支持将 LDAP 口令控制传送到 LDAP 客户端。

故障切换支持

如果由主 URL 指定的 LDAP 目录服务器出现严重故障，并且该服务器不再对网络请求做出响应，则 Adaptive Server 会尝试连接到由辅助 URL 指定的辅助 LDAP 目录服务器。Adaptive Server 使用 LDAP 函数 `ldap_init` 确定它能否打开与 LDAP 目录服务器的连接。Null 或无效的主 URL 字符串会导致 Adaptive Server 尝试将故障切换到辅助 URL。LDAP 绑定或搜索操作返回的故障不会导致 Adaptive Server 将故障切换到辅助 URL。

Adaptive Server 登录和 LDAP 用户帐户

一旦启用了 LDAP 用户鉴定，选择并设置了鉴定算法和 URL 字符串，就必须配置用户帐户。LDAP 管理员在 LDAP 服务器中创建和维护帐户，数据库管理员在 Adaptive Server 中创建和维护帐户。或者，在将 Adaptive Server 与外部鉴定机制（如 LDAP 服务器）集成时，数据库管理员也可以选择允许灵活使用登录帐户的管理选项。数据库管理员可以继续使用传统命令和过程，来管理 Adaptive Server 帐户角色、缺省数据库、缺省语言及其它特定于登录的属性。

表 16-8 介绍了登录时 Adaptive Server 对 syslogins 表进行的更新。这些更新假定已配置 LDAP 用户鉴定，未限制登录使用 LDAP，并且您未设置 create login 映射。

表 16-8: 通过 LDAP 对 syslogins 进行的更新

syslogins 中是否存在行?	LDAP 服务器鉴定是否成功?	syslogins 中的更改
否	是	无更改，登录失败
否	否	无更改，登录失败
是	是	如果口令已更改，则更新行
是	否	无更改

辅助查找服务器支持

Adaptive Server 为 LDAP 服务器鉴定的 Adaptive Server 客户端提供不间断支持。您可以指定辅助 LDAP 查找服务器，当 LDAP 服务器发生故障或当计划的关机时间到来时可从主 LDAP 服务器故障切换到辅助服务器。

URL 的运行状况通过以下状态来监视：

- INITIAL（初始） — 表示未配置 LDAP 用户鉴定。
- RESET（重置） — 表示已通过 Adaptive Server 管理命令输入了 URL。
- READY（就绪） — 表示 URL 已准备好接受连接。
- ACTIVE（活动） — 表示 URL 已成功执行 LDAP 用户鉴定。
- FAILED（失败） — 表示连接 LDAP 服务器时出现问题。
- SUSPENDED（挂起） — 表示 URL 处于维护模式，并且不会再次使用它。

以下事件序列描述了故障切换和手动故障恢复：

- 1 主 URL 组和辅助 URL 组都已配置并且处于 READY 状态。
- 2 已使用主服务器基础结构鉴定了连接。
- 3 主服务器故障，并且其状态变为 FAILED。
- 4 通过辅助服务器基础结构，连接自动开始鉴定。
- 5 LDAP 管理员修复了主服务器并使其恢复到联机状态。Adaptive Server 管理员将主 LDAP 服务器状态更改为 READY。
- 6 已使用主服务器鉴定了新连接。

注释 一旦 Adaptive Server 进行故障切换并转移到辅助 LDAP 服务器，数据库管理员即必须手动激活主 LDAP 服务器，然后主服务器才能重新使用。

如果 Adaptive Server 在连接 LDAP 服务器时发生错误，则它会再尝试三次鉴定。如果错误仍然存在，则会将 LDAP 服务器标记为 FAILED。有关强制 Adaptive Server 进入重试循环的 LDAP 错误的信息，请参见第 498 页的“LDAP 用户鉴定错误的故障排除”。

使用 `sp_ldapadmin` 配置辅助查找 LDAP 服务器。

- 若要设置辅助 DN 查找 URL，请输入：

```
sp_ldapadmin set_secondary_dn_lookup_url, <URL>
```

- 若要设置辅助 DN 查找 URL 的管理访问帐户，请输入：

```
sp_ldapadmin set_secondary_access_acct, <DN>, <password>
```

- 若要暂停使用主 URL 鉴定或辅助 URL 鉴定，请输入：

```
sp_ldapadmin suspend, {primary | secondary}
```

- 若要激活主 URL 鉴定或辅助 URL 鉴定的设置，请输入：

```
sp_ldapadmin activate, {primary | secondary}
```

- 要显示有关主 / 辅 LDAP 服务器设置和状态的详细信息，请输入：

```
sp_ldapadmin list
```


`sp_ldapadmin list` 结合了 `list_access_acct` 和 `list_urls` 先前的输出。它具有以下关于主 / 辅服务器的所需输出：

- 搜索 URL
- 区分名查找 URL
- 访问帐户 DN
- 活动 [true | false]
- 状态 [ready | active | failed | suspended | reset]

Adaptive Server 12.5.4 版及更高版本包括以下支持辅助服务器的 `sp_ldapadmin` 选项。

- 若要显示辅助服务器的 DN 查找 URL，请输入：
`sp_ldapadmin list_urls`
- 要显示辅助 DN 查找 URL 的管理访问帐户，请输入：
`sp_ldapadmin list_access_acct`
- 若要显示子命令，请输入：
`sp_ldapadmin help`

LDAP 服务器状态转换

表 16-9 - 表 16-14 列出了执行每个 `sp_ldapadmin` 命令时 LDAP 服务器的状态转换。

表 16-9 显示了执行 `sp_ldapadmin set_URL` 时的状态转换，其中 `set_URL` 表示以下命令之一：

- `set_dn_lookup_url`
- `set_primary_url`
- `set_secondary_dn_lookup_url`
- `set_secondary_url`

表 16-9: 执行 `sp_ldapadmin set_URL` 时的状态转换

初始状态	最终状态
INITIAL	RESET
RESET	RESET
READY	READY
ACTIVE	RESET
FAILED	RESET
SUSPENDED	RESET

表 16-10 显示了执行 `sp_ldapadmin suspend` 时的状态转换。

表 16-10: 执行 `sp_ldapadmin suspend` 时的状态转换

初始状态	最终状态
INITIAL	Error
RESET	SUSPENDED
READY	SUSPENDED
ACTIVE	SUSPENDED
FAILED	SUSPENDED
SUSPENDED	SUSPENDED

表 16-11 显示了执行 `sp_ldapadmin activate` 时的状态转换。

表 16-11: 执行 `sp_ldapadmin activate` 时的状态转换

初始状态	最终状态
INITIAL	Error
RESET	READY
READY	READY
ACTIVE	ACTIVE
FAILED	READY
SUSPENDED	READY

以下表格显示了由 Adaptive Server 隐式执行的 LDAP 服务器状态转换。

表 16-12 显示了重新启动 Adaptive Server 时的状态转换：

表 16-12: 重新启动 Adaptive Server 时的状态转换

初始状态	最终状态
INITIAL	INITIAL
RESET	RESET
READY	READY
ACTIVE	READY
FAILED	FAILED
SUSPENDED	SUSPENDED

如果 LDAP 服务器处于 READY 或 ACTIVE 状态，则 Adaptive Server 只尝试 LDAP 登录。表 16-13 显示了状态转换：

表 16-13: LDAP 登录成功时的状态转换

初始状态	最终状态
READY	ACTIVE
ACTIVE	ACTIVE

表 16-14 显示了 LDAP 登录失败时的状态转换：

表 16-14: LDAP 登录失败时的状态转换

初始状态	最终状态
READY	FAILED
ACTIVE	FAILED

LDAP 用户鉴定调优

可根据传入连接和 Adaptive Server-LDAP 服务器基础结构的负载对 Adaptive Server 选项进行配置和调优。可根据并发传入请求的数量来配置这些选项：

- 使用 `sp_configure` 来设置 `max native threads`，它指示每个引擎的本机线程数。
- 使用 `sp_ldapadmin` 来配置 `max_ldapua_native_threads`，它指示每个引擎的 LDAP 用户鉴定本机线程数。

根据网络和 Adaptive Server/LDAP 服务器基础结构的运行状况配置 `set_timeout` 选项（该选项指示 LDAP 服务器绑定和搜索超时）。

配置 `set_abandon_ldapua_when_full` 选项，以指定当传入连接使用了 `max_ldapua_native_threads` 时的 Adaptive Server 行为：

使用这些 `sp_ldapadmin` 选项配置 LDAP 服务器以获得更好的性能：

- `set_max_ldapua_desc` — 管理 LDAPUA 连接请求的并发性。如果使用区分名算法，则将 `set_max_ldapua_desc` 设置为较大的数可加快 Adaptive Server 正在处理的 LDAPUA 连接。
- `set_num_retries` — 设置尝试次数。依据 Adaptive Server 和 LDAP 服务器之间的瞬时错误数调优此数值。可通过配置重试次数来取消瞬时错误。
- `set_log_interval` — 控制出于诊断目的发送到 Adaptive Server 错误日志的消息数。使用较低的数值会使错误日志杂乱，但有助于确定具体错误。如果使用较大的数值，则会减少发送到错误日志的消息数，但研究价值却不如前者。依据错误日志大小来调优 `set_log_interval`。

对登录映射增加更严格的控制

通过 `sp_maplogin` 将使用 LDAP 或 PAM 进行鉴定的用户映射到本地 Adaptive Server 登录。

注释 若要映射使用 Kerberos 进行鉴定的用户，请使用 `sybmapname`，而不是 `sp_maplogin`。

只有具有 `sso_role` 的用户才能使用 `sp_maplogin` 创建或修改登录映射。

Adaptive Server 避免了登录的鉴定机制设置和使用该登录的映射之间的冲突。潜在的映射冲突由存储过程 `sp_maplogin`、`sp_modifylogin` 或 `sp_addlogin` 进行检测。

这些控制不允许进行以下映射：

- 从一个 Adaptive Server 登录名映射到另一个登录名
- 从已经作为本地登录名存在的外部名称
- 映射到不存在的登录名

此外，如果鉴定机制是使用映射指定的，则该机制应与目标登录名中设定的鉴定机制相符。

如果目标登录的鉴定机制限制登录使用某个特定的鉴定机制，则使用映射指定的机制必须与为该登录指定的鉴定机制相匹配，或者与 “ANY” 鉴定机制相匹配。

当 `sp_maplogin` 检测到存在冲突时，`sp_maplogin` 将失败，并报告错误，指出所发生的冲突。

同样，`sp_modifylogin` 和 `sp_addlogin` 将检查是否存在某个可能与用户登录的 `authenticate with` 选项存在冲突的映射。

当 `sp_modifylogin` 或 `sp_addlogin` 检测到冲突时，则会报告错误，指出与登录映射存在的任何冲突。

示例

示例 1 将 LDAP 用户映射到 Adaptive Server “sa” 登录。某公司采用了 LDAP 作为其所有用户帐户的存储库，且其安全性策略要求对所有用户进行 LDAP 鉴定，包括可能管理数百台 Adaptive Server 的数据库管理员 “adminA” 和 “adminB”。已启用审计，并且登录事件记录在审计追踪中。

若要将这些管理员帐户映射到 “sa”，请输入：

```
sp_maplogin LDAP, 'adminA', 'sa'
go
sp_maplogin LDAP, 'adminB', 'sa'
go
```

要求所有用户使用 LDAP 鉴定进行鉴定：

```
sp_configure 'enable ldap user auth', 2
go
```

当 “adminA” 在登录到 Adaptive Server 期间进行鉴定时，将在登录审计事件中记录与 “adminA” 关联的区分名，而不是仅记录 “sa”。这可以让每个单独执行的操作在审计追踪中标识出来。

由于 “adminA” 和 “adminB” 的口令是在 LDAP 服务器中设置的，因此无需在所有管理的 Adaptive Server 中都保留 “sa” 的口令。

此示例还允许在鉴定时使用不同的外部标识和口令，尽管它们在 Adaptive Server 中的操作仍然需要与 “sa” 帐户关联的特殊权限。

示例 2 结合使用 PAM 和 LDAP 将用户映射到应用程序登录。某公司同时采用了 PAM 和 LDAP 鉴定，但分别用于不同的目的。公司的安全策略将 LDAP 定义为一般用户帐户的鉴定机制，将 PAM 定义为特殊用户（例如中间层应用程序）的鉴定机制。中间层应用程序可以建立一个到 Adaptive Server 的连接池，以处理代表中间层应用程序用户的请求。

为 LDAP 和 PAM 用户鉴定配置 Adaptive Server：

```
sp_configure 'enable ldap user auth', 2
go
sp_configure 'enable pam user auth', 2
go
```

在本地建立一个 Adaptive Server 登录名 appX，并使其具有与中间层应用程序相适应的权限：

```
sp_addlogin 'appX', password
go
sp_modifylogin appX, 'authenticate with', PAM
go
```

这种鉴定机制并不采用在 “appX” 中硬编码一个简单口令然后使该口令在几个不同的 Adaptive Server 中保持一致的方法，而是开发了一个自定义 PAM 模块，该模块使用其它事实来鉴定中央存储库中的应用程序，以验证中间层应用程序的身份。

客户端应用程序登录 “appY” 需要使用用户的 LDAP 标识和口令对用户进行 LDAP 鉴定。使用 sp_maplogin 将所有经过 LDAP 鉴定的用户映射到登录 “appY”，

```
sp_addlogin 'appY', password
go
sp_maplogin LDAP, NULL, 'appY'
go
```

“appY” 的用户将通过其公司标识和口令接受鉴定，然后被映射到一个本地的 Adaptive Server 登录 “appY”，以执行数据库操作。鉴定是使用记录在审计追踪中的 LDAP 用户标识来进行的，数据库操作则是通过与应用程序登录 “appY” 相适应的权限来执行的。

LDAP 用户鉴定错误的故障排除

Adaptive Server 在与 LDAP 服务器通信时可能会遇到以下瞬时错误。通常，重新尝试连接可解决这些错误。如果重新尝试三次后错误仍然存在，则 Adaptive Server 将该 LDAP 服务器标记为 FAILED。

- LDAP_BUSY — 服务器繁忙。
- LDAP_CONNECT_ERROR — 连接过程中发生错误。
- LDAP_LOCAL_ERROR — 客户端发生错误。
- LDAP_NO_MEMORY — 无法在客户端分配内存。
- LDAP_OPERATIONS_ERROR — 服务器端发生错误。
- LDAP_OTHER — 未知错误代码。
- LDAP_ADMINLIMIT_EXCEEDED — 搜索超出限制。
- LDAP_UNAVAILABLE — 服务器无法处理请求。

- LDAP_UNWILLING_TO_PERFORM — 服务器将不会处理请求。
- LDAP_LOOP_DETECT — 在引用过程中检测到循环。
- LDAP_SERVER_DOWN — 无法访问服务器（连接失败）。
- LDAP_TIMEOUT — LDAP API 因操作未在用户指定的时间内完成而失败。

瞬时错误和大量并发登录请求可能会导致错误日志中出现大量重复的错误消息。为提高日志的可读性，使用了以下错误消息记录算法：

- 1 如果是第一次记录某消息，则会记录它。
- 2 如果上次记录该消息的时间大于 3 分钟，则执行以下操作：
 - 记录该错误消息。
 - 记录自上次打印该消息以来该消息的重复次数。
 - 以分钟为单位记录自输出该消息以来经过的时间。

因以下问题而导致的鉴定失败不视为 LDAP 错误，并且此类鉴定失败也不是重新尝试鉴定请求的条件：

- 由于口令错误或区分名无效而导致的绑定失败。
- 在成功绑定后搜索所返回的结果集为 0 或未返回任何属性值。

分析 URL 时发现的语法错误是在设置 LDAP URL 时捕获的，因此不能归于上述任何类别。

配置 LDAP 服务器

轻量目录访问协议 (LDAP) 的用户鉴定支持安全套接字层 / 传送层安全性 (SSL/TLS) 协议，从而能够在 Adaptive Server 和 LDAP 服务器之间安全地传输数据。

❖ 配置与 LDAP 服务器的连接

- 1 确保所有受托根证书均位于同一文件中。

在您定义受托服务器之后，Adaptive Server 将配置安全连接，其中 *servername* 是当前 Adaptive Server 的名称。如果：

- 定义了 `$$SYBASE_CERTDIR`，Adaptive Server 将从 `$$SYBASE_CERTDIR/servername.txt` (UNIX) 或 `%SYBASE_CERTDIR%\servername.txt` (Windows) 装载证书。

- 未定义 `$SYBASE_CERTDIR`，则 Adaptive Server 将从 `$SYBASE/$SYBASE_ASE/certificates/servername.txt` (UNIX) 或 `%SYBASE%\%SYBASE_ASE%\certificates\servername.txt` (Windows) 中装载证书。
- 2 重新启动 Adaptive Server 以更改受托根证书文件。
- 3 使用 `sp_ldapadmin`（同时指定 `ldaps:// URL`，而不是 `ldap:// URL`）建立与 LDAP 服务器安全端口的安全连接。
- 4 通过简单的 TCP 连接建立 TLS 会话：

```
sp_ldapadmin 'starttls_on_primary', {true | false}
```

或者

```
sp_ldapadmin 'starttls_on_secondary', {true | false}
```

注释 LDAP 服务器连接没有 `connect timeout` 选项；如果 LDAP 服务器停止响应，则所有登录连接也将停止响应。

LDAP 用户鉴定改进

在 Adaptive Server 的早期版本中，如果需要修改证书颁发机构 (CA) 受托根文件，您必须重新启动 Adaptive Server 以使修改生效。Adaptive Server 15.0.3 版及更高版本支持修改受托根文件，因此不必重新启动服务器。一个新的子命令 `reinit_descriptors` 可解除绑定 LDAP 服务器描述符，并重新初始化用户鉴定子系统。有关此选项的语法，请参见《参考手册：过程》。

- 此命令需要系统安全员权限。
- 如果具有系统安全员权限的用户在未执行此命令的情况下修改了受托根文件，则管家实用程序杂事任务将使用新的杂事（设计为每隔 60 分钟重新初始化用户鉴定子系统一次）。

自动 LDAP 用户鉴定和故障恢复

Adaptive Server 15.0.3 提供了对辅助 LDAP 服务器的支持。在以前，在出现故障的主 LDAP 服务器联机后，若要鉴定新的 LDAP 登录并将它们转移到主 LDAP 服务器，必须要手动激活 LDAP 服务器。

在 15.0.3 版及更高版本中，Adaptive Server 的管家实用程序中增加了一项新的杂事，用于自动激活 LDAP 服务器：'set_failback_interval' – 有关语法，请参见第 501 页的“设置 LDAP 故障恢复时间间隔”。

sp_ldapadmin set_failback_interval 中的 set_failback_interval 选项设置激活出现故障的 LDAP 服务器的两次尝试之间的时间间隔；如果不设置此参数，则缺省值为 15 分钟。请参见《参考手册：过程》中的 sp_ldapadmin。

如果主 URL 标记为 FAILED，则管家任务将尝试使用主访问帐户区分名 (DN) 和口令将其激活。如果尚未配置主访问帐户，则管家任务将尝试使用匿名绑定。如果绑定操作在第一次尝试时失败，则管家任务将按配置的重试次数重试绑定操作。如果绑定操作成功，则将主 URL 标记为 READY。

如果辅助 URL 标记为 FAILED，则管家任务将尝试按类似的方式激活辅助 URL。

sp_ldapadmin 中的 reinit_descriptors 选项在修改证书文件时执行，在这种情况下，它将每隔 60 分钟重新初始化 LDAP 用户鉴定子系统一次。

设置故障恢复间隔之后，管家任务将在每次执行其各项杂事时检查是否存在出现故障的 LDAP 服务器。如果找到出现故障的 LDAP 服务器，它将尝试在故障恢复时间间隔到期时激活 LDAP 服务器。

设置 LDAP 故障恢复时间间隔

sp_ldapadmin set_failback_interval 的语法为：

```
sp_ldapadmin 'set_failback_interval', time_in_minutes
```

其中 time_in_minutes 为从 -1 到 1440 分钟（24 小时）的值。

- 值为 0 则表示手动进行故障恢复。也就是说，管家任务不会尝试自动对 LDAP 服务器进行故障恢复。您必须手动执行此任务。
- 如果值为 -1，则将故障切换时间间隔设置为 15 分钟（缺省值）。
- 如果您不带任何参数发出 sp_ldapadmin 'set_failback_interval'，则 sp_ldapadmin 将显示为故障恢复时间间隔设置的值。

- 如果您不带任何参数发出 `sp_ldapadmin`，则 `sp_ldapadmin` 将在输出中包括故障恢复时间间隔：

```
sp_ldapadmin
-----
Primary:
  URL:                ''
  DN Lookup URL:      ''
  Access Account:      ''
  Active:              'FALSE'
  Status:              'NOT SET'
  StartTLS on Primary LDAP URL: 'TRUE'
Secondary:
  URL:                ''
  DN Lookup URL:      ''
  Access Account:      ''
  Active:              'FALSE'
  Status:              'NOT SET'
  StartTLS on Secondary LDAP URL: 'FALSE'
Timeout value:        '-1'(10000) milliseconds
Log interval:         '3' minutes
Number of retries:     '3'
Maximum LDAPUA native threads per Engine: '49'
Maximum LDAPUA descriptors per Engine: '20'
Abandon LDAP user authentication when full: 'false'
Failback interval:    '-1'(15) minutes
(return status = 0)
```

示例

此示例将 LDAP 故障恢复时间间隔设置为 60 分钟：

```
sp_ldapadmin 'set_failback_interval' 60
```

此示例将 LDAP 故障恢复

时间间隔设置为缺省值 15 分钟：

```
sp_ldapadmin 'set_failback_interval' -1
```

此示例显示为故障恢复时间间隔设置的值：

```
sp_ldapadmin 'set_failback_interval'
The LDAP property 'set_failback_interval' is set to '15
minutes'.
```

外部鉴定的登录映射

当您配置外部鉴定机制时，如果恰好有一个外部用户到内部 Adaptive Server 登录的映射，并且已成功对其进行鉴定，则 Adaptive Server 将更新内部登录的口令以匹配外部用户的口令。例如，在以下情况下：

- 1 USER1 具有 Adaptive Server 登录名 `user_ase`，口令为 `user_password`。另一个用户具有 LDAP 登录名 `user_ldap`，口令为 `user_ldappasswd`
- 2 Adaptive Server 具有 `user_ldap` 到 `user_ase` 的一对一映射。
- 3 用户 `user_ldap` 使用口令 `user_ldappasswd` 登录到 Adaptive Server
- 4 Adaptive Server 将 `user_ase` 的口令更新为 `user_ldappasswd`。

在下面的示例中，如果您通过将外部用户映射到 Adaptive Server 内部登录来配置外部鉴定机制，并且鉴定故障切换到 Adaptive Server，则您可以使用外部用户名和正确的 Adaptive Server 口令登录。Adaptive Server 在内部使用映射的内部登录来鉴定外部用户：

- 1 用户具有 Adaptive Server 登录名 `user_ase`，口令为 `user_password`
- 2 另一个用户具有 LDAP 登录名 `user_ldap`
Adaptive Server 将 `user_ldap` 映射到 `user_ase`
- 3 如果启用 LDAP：

```
sp_configure 'enable ldap user auth', 1
```
- 4 如果 LDAP 服务器关闭或崩溃，`user_ldap` 可使用登录名 `user_ldap` 和口令 `user_password` 登录到 Adaptive Server。

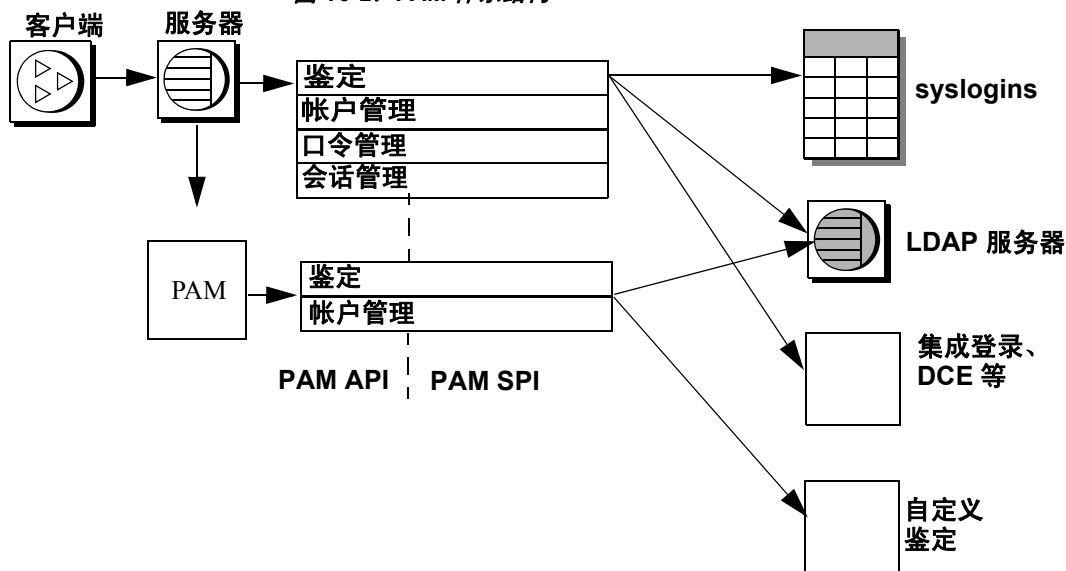
为使用 PAM 的鉴定配置 Adaptive Server

可插入鉴定模块 (PAM) 支持允许将多个鉴定服务模块叠加在一起，而无需修改需要鉴定的应用程序。

PAM 将 Adaptive Server 与 Solaris 和 Linux 操作系统集成在一起，并且简化了对用户帐户及鉴定机制的管理，从而降低了总拥有成本。用户可以自定义或编写他们自己的鉴定及授权模块。

注释 Linux 和 Solaris 平台上目前提供了 PAM 支持。有关 PAM 用户鉴定的详细信息，请参见操作系统文档。

图 16-2: PAM 体系结构



Adaptive Server 将登录名以及从登录包中获得的认证传递给 PAM API。PAM 装载在操作系统配置文件中指定的一个服务提供程序模块，并调用相应的函数来完成鉴定过程。

在 Adaptive Server 上启用 PAM

Linux 和 Solaris 中都包含预定义的 PAM 模块。可以使用这些模块之一，也可以创建自己的模块。在创建自己的模块时，请按照操作系统文档中有关创建 PAM 模块的指南进行操作。

注释 您创建的 PAM 模块应符合 RFC 86.0 “Unified Login With Pluggable Authentication Modules (PAM)”。Adaptive Server 支持 RFC 的鉴定管理模块。它不支持帐户管理模块、会话管理模块或口令管理模块。

配置操作系统

若要启用 PAM 支持，请按照下面的方法配置操作系统：

- 对于 Solaris，将以下行添加到 */etc/pam.conf*：

```
ase auth required /user/lib/security/$ISA/pam_unix.so.1
```

- 对于 Linux，创建一个名为 */etc/pam.d/ase* 的新文件，并添加：

```
auth requiried /lib/security/pam_unix.so
```

有关如何创建这些条目的详细信息，请参见操作系统文档。

在同一计算机上运行 32 位和 64 位服务器

\$ISA 是一个允许 32 位和 64 位库同时运行的环境变量。

在 Solaris 32 位计算机上，用一个空字符串替换 \$ISA；而在 64 位计算机上，则用字符串 “sparcv9” 替换 \$ISA。

若要同时运行 32 位和 64 位服务器，请将 32 位 PAM 模块放在一个目录中，然后将 64 位版本放到该目录的一个子目录中。

pam.conf 中的条目应该与以下内容类似：

```
$ ls /usr/lib/security/pam_sec.so.1
pam_sec.so.1 -> /SYBASE/pam_whatever_32bits.so.1

$ ls /usr/lib/security/sparcv9/pam_sec.so.1
pam_sec.so.1 -> /SYBASE/pam_sec_64bits.so.1

ase      auth      required
/usr/lib/security/$ISA/pam_sec.so.1
```

注释 \$ISA 是 *pam.conf* 中允许的唯一变量。

为 PAM 用户鉴定配置 Adaptive Server

enable pam user auth 启用 PAM 用户鉴定支持：

```
sp_configure "enable pam user auth", 0 | 1 | 2
```

其中：

- 0 — 禁用 PAM 鉴定。这是缺省值。
- 1 — 表示 Adaptive Server 将首先尝试进行 PAM 鉴定，如果 PAM 鉴定失败，则使用 syslogins 鉴定。
- 2 — 表示只能使用 PAM 鉴定。

注释 启用 PAM 后，口令管理将委派给 PAM 服务提供程序。

Adaptive Server 登录和 PAM 用户帐户

在设置了 enable PAM user authentication 并完成了对 Adaptive Server 和操作系统的 PAM 配置之后，必须配置用户帐户。操作系统或网络安全委员会在 PAM 服务提供程序中创建和维护用户帐户，数据库管理员会在 Adaptive Server 中创建和维护帐户。或者，在将 Adaptive Server 与外部鉴定机制（如 PAM）集成时，数据库管理员也可以选择允许灵活使用登录帐户的管理选项。数据库管理员可以继续使用传统命令和过程，来管理 Adaptive Server 帐户角色、缺省数据库、缺省语言及其它特定于登录的属性。

表 16-15 介绍了登录时对 syslogins 进行的更新。该表假定已配置 PAM 用户鉴定，允许使用 PAM 进行登录，并且没有设置 create login 映射。

Table 16-15: 通过 PAM 对 syslogins 进行的更新

syslogins 中是否存在行？	PAM 鉴定是否成功？	syslogins 中的更改
否	是	无更改，登录失败
否	否	无更改，登录失败
是	是	如果口令已更改，则更新行
是	否	无更改

增强的登录控制

根据前面 LDAP 和 PAM 部分中讨论的方法，将 Adaptive Server 配置为允许使用全服务器范围的鉴定机制。还可以使用如下所述的 Adaptive Server 增强登录控制，将 Adaptive Server 配置为对该服务器上每个单独的登录分别指定鉴定机制。

当服务器在两种鉴定机制之间转换时，特定于登录的控制会很有用；对于本地服务器管理可能需要的特定于服务器的登录，特定于登录的控制也可能很有用：它们不与集中管理的用户登录关联。

强制鉴定

通过将以下参数用于 `sp_modifylogin` 和 `sp_addlogin`，可以强制登录使用特定的鉴定过程：

- ASE — 通过 `syslogins` 表中的口令使用 Adaptive Server 内部鉴定。
- LDAP — 通过 LDAP 服务器使用外部鉴定。
- PAM — 通过 PAM 使用外部鉴定。
- ANY — 缺省情况下，使用此鉴定方法对用户进行鉴定。使用 ANY 鉴定的用户意味着 Adaptive Server 将检查是否已经定义了外部鉴定机制，如果有，则使用该外部鉴定机制。否则，它将使用 Adaptive Server 的鉴定机制。

Adaptive Server 按照以下顺序检查外部鉴定机制：

- 1 LDAP。
- 2 可插入鉴定模块 (PAM)。如果同时启用了 LDAP 和 PAM，则决不会尝试对用户进行 PAM 鉴定。
- 3 如果 PAM 或 LDAP 均未启用，则 Adaptive Server 使用 `syslogins` 对登录进行鉴定。

继续使用 `syslogins` 目录验证登录帐户（例如 “sa”）。只有 SSO 角色可以设置对登录的鉴定。

例如，以下命令使用 `sp_modifylogin` 对登录进行鉴定：

```
sp_modifylogin "nightlyjob", "authenticate with", "ASE"  
sp_displaylogin "nightlyjob"
```

显示类似以下内容的输出：

```
Suid: 1234
Loginname: nightlyjob
Fullname: Batch Login
Default Database: master
. . .
Date of Last Password Change: Oct 2 2003 7:38 PM
Password expiration interval: 0
Password expired: N
Minimum password length:
Maximum failed logins: 0
Current failed login attempts:
Authenticate with: ASE
```

使用 *sp_maplogin* 映射登录

使用 *sp_maplogin* 来映射登录：

```
sp_maplogin (authentication_mech | null),
            (client_username | null), (action | login_name | null)
```

其中：

- *authentication_mech* — 是为 *sp_modifylogin* 中的 *authenticate with* 选项指定的有效值之一。
- *client_username* — 是一个外部用户名，它可以是操作系统名、LDAP 服务器的用户名，也可以是 PAM 库可识别的任何其它名称。空值表示任何登录名都有效。
- *action* — 表示 *create login* 或 *drop*。使用 *create login* 时，将在通过鉴定后立即创建登录。使用 *drop* 可删除登录。
- *login_name* 是 *syslogins* 中已存在的 Adaptive Server 登录。

此示例将外部用户 “jsmith” 映射为 Adaptive Server 用户 “guest”。一旦通过鉴定，“jsmith” 就具有了 “guest” 的特权。审计登录记录会同时显示 *client_username* 和 Adaptive Server 用户名：

```
sp_maplogin NULL, "jsmith", "guest"
```

如果尚未创建登录，则此示例将告知 Adaptive Server 为所有使用 LDAP 鉴定过的外部用户新建一个登录：

```
sp_maplogin LDAP, NULL, "create login"
```


显示映射信息

sp_helpmaplogin 显示映射信息:

```
sp_helpmaplogin [ (authentication_mech | null), (client_username | null) ]
```

其中 *authentication_mech* 是为 *sp_modifylogin* 中的 *authenticate with* 选项指定的有效值之一, *client_username* 是外部用户名。

如果未包括任何参数, 则 *sp_helpmaplogin* 会显示有关当前登录到 Adaptive Server 的所有用户的登录信息。可以使用上面列出的参数, 将输出限制到客户端用户名或鉴定机制的特定集合。

以下显示了所有登录的相关信息:

sp_helpmaplogin		
authentication	client name	login name
-----	-----	-----
NULL	jsmith	guest
LDAP	NULL	create login

确定鉴定机制

使用 @@authmech 全局变量确定 Adaptive Server 使用的鉴定机制。

例如, 如果允许 Adaptive Server 使用具有故障切换功能的 LDAP 用户鉴定 (*enable ldap user auth* = 2), 并且用户 “Joe” 为外部用户且鉴定机制设置为 ANY, 则当 Joe 登录时, Adaptive Server 会尝试使用 LDAP 用户鉴定对 Joe 进行鉴定。如果 Joe 未能作为 LDAP 中的用户通过鉴定, 则 Adaptive Server 会使用 Adaptive Server 鉴定对 Joe 进行鉴定; 如果鉴定成功, 则 Joe 可以成功登录。

@@authmech 全局变量值为:

```
select @@authmech
-----
ase
```

如果配置 Adaptive Server 以进行严格的 LDAP 用户鉴定 (*enable ldap user auth* = 2), 并将 Joe 作为有效用户添加到 LDAP 中, 则当 Joe 登录时, @@authmech 的值为:

```
select @@authmech-----
ldap
```


管理用户权限

本章描述用户权限的使用和实施情况。

主题	页码
概述	511
系统过程的权限	516
数据库所有者特权	514
其他数据库用户的特权	515
数据库对象所有者特权	515
授予和撤消权限	516
授予和撤消角色	534
获取另一用户的权限	536
权限报告	541
使用视图和存储过程作为安全性机制	545
使用行级访问控制	553

概述

自由选择访问控制 (DAC) 允许基于用户标识、组成员资格和活动角色限制对对象和命令的访问。因为具有某种访问权限的用户，例如对象所有者，可以选择是否将这种访问权限传递给其他用户，所以此类控制是“自由选择”的。

Adaptive Server 的自由选择访问控制系统可识别以下用户类型：

- 拥有一个或多个系统定义角色的用户：系统管理员、系统安全
全员、操作员和其他角色
- 数据库所有者
- 数据库对象所有者
- 其他用户

系统管理员在 DAC 系统之外操作，并且在任何时候对所有数据库对象（加密密钥除外）都具有访问权限（请参见《加密列用户指南》）。系统安全员始终可访问 **sybsecurity** 数据库中的审计追踪表。

数据库所有者不能自动接受其他用户所拥有对象的权限；但可以：

- 通过 **setuser** 命令来假定数据库中某个用户的身份，可以临时获得此用户的所有权限。
- 通过 **setuser** 命令来假定某个对象所有者的身份，然后使用 **grant** 命令授予权限，可以永久获得此特定对象的权限。

有关通过假定另一用户的身份来获得某个数据库或对象的权限的详细信息，请参见第 536 页的“[获取另一用户的权限](#)”。

对象所有者可以将这些对象的访问权限授予其他用户，也可以授予其他用户将访问权限再传递给其他用户。可以使用 **grant** 命令授予用户、组和角色各种权限，并使用 **revoke** 命令撤消这些权限。使用 **grant** 和 **revoke** 授予用户权限以：

- 创建数据库
- 在数据库内创建对象
- 执行特定命令，例如 **dbcc** 和 **set proxy**
- 访问指定的表、视图、存储过程、加密密钥和列

grant 和 **revoke** 还可以用于设置系统表的权限。

对于“**Public**”的缺省权限，则不需要使用 **grant** 或 **revoke** 语句。

某些命令可由任何用户随时使用，而不需要任何权限。其它命令则只能由特定状态的用户使用，且不能移交给其他用户使用。

是否能为可授权和撤消的命令分配权限取决于各个用户的角色或状态（例如作为系统管理员、数据库所有者、系统安全员或数据库对象所有者）以及是否已授予用户一个角色，此角色有权将此权限授予其他用户。

还可以使用视图和存储过程作为安全性机制。请参见第 545 页的“[使用视图和存储过程作为安全性机制](#)”。

创建数据库的权限

只有系统管理员才能授权使用 `create database` 命令。接受 `create database` 权限的用户还必须是有有效的 `master` 数据库用户，因为所有数据库都是在使用 `master` 时被创建的。

在多数安装情况下，系统管理员保留对 `create database` 权限的独占，以便对数据库的放置和数据库设备空间分配进行集中控制。在这些情况下，系统管理员代表其他用户创建新的数据库，然后将所有权移交给相关用户。

若要为另一用户创建数据库：

- 1 在 `master` 数据库中发出 `create database` 命令。
- 2 使用 `use` 命令切换到新数据库。
- 3 执行 `sp_changedbowner`。

更改数据库所有权

使用 `sp_changedbowner` 更改数据库的所有权。通常，系统管理员先创建用户数据库，在完成某些初始工作后再将所有权授予另一用户。只有系统管理员才能执行 `sp_changedbowner`。

Sybase 建议您在用户尚未添加到数据库中，且用户还未开始在数据库中创建对象之时，移交所有权。新的所有者在 `Adaptive Server` 中必须已有一个登录名，但不能是该数据库的用户，也不能在该数据库中有别名。您可能必须使用 `sp_dropuser` 或 `sp_dropalias`，然后才能更改数据库的所有权，并且，您可能必须删除某些对象，然后才能删除用户。

在要更改所有权的数据库中发出 `sp_changedbowner`。语法为：

```
sp_changedbowner loginame [, true ]
```

以下示例使 “`albert`” 成为当前数据库的所有者，并删除作为旧的 “`dbo`” 的用户的别名：

```
sp_changedbowner albert
```

请包括 `true` 参数以将别名及其权限移交给新的 “`dbo`”。

注释 您不能更改 `master/model/tempdb` 或 `sybsystemprocs` 数据库的所有权，并且不应更改任何其它系统数据库的所有权。

数据库所有者特权

数据库所有者和系统管理员是唯一能够向其他用户授予对象创建权限（`create encryption key` 和 `create trigger` 权限除外，这两个权限只能由系统安全员授予）的用户。数据库所有者具有在该数据库内执行任何操作的全部特权，必须使用 `grant` 命令将权限显式授予其他用户。

以下命令的使用权限自动授予数据库所有者，不能移交给其他用户：

- `checkpoint`
- `dbcc`
- `alter database`
- `online database`
- `drop database`
- `dump database`
- `dump transaction`
- `grant`（对象创建权限）
- `load database`
- `load transaction`
- `revoke`（对象创建权限）
- `setuser`

数据库所有者可授予或撤消执行以下操作的权限：

- 使用以下命令：`create default`、`create procedure`、`create rule`、`create table`、`create view`。

如果数据库所有者拥有 `sa_role` 并处于 `master` 数据库中，则他们可授予使用 `create database`、`set tracing` 和 `connect` 的权限。

如果数据库所有者拥有 `sso_role`，则他们可授予使用 `set session authorization`、`create trigger` 和 `create encryption key` 的权限。

- `all` — 如果您是数据库所有者，则 `all` 会授予除 `create database`、`create trigger` 和 `create encryption key` 之外的所有 `create` 命令的权限。如果您拥有 `sa_role`，并在 `master` 数据库中发出 `grant` 命令，则 `all` 也会授予 `create database`、`set tracing` 和 `connect` 的权限。
- 系统表的缺省权限
- 使用 `dbcc` 命令：`checkalloc`、`checkcatalog`、`checkdb`、`checkindex`、`checkstorage`、`checktable`、`checkverify`、`fix_text`、`indexalloc`、`reindex`、`tablealloc`、`textalloc`、`tune`

数据库对象所有者特权

创建数据库对象（表、视图、加密密钥或存储过程）的用户拥有该对象，并自动授予所有对象访问权限。对于除对象所有者以外的用户（包括数据库所有者在内），不向他们自动授予此对象的所有权限，除非对象所有者或对此对象有 `grant` 权限的用户对其明确授权。

举例如下，假设 Mary 是 `pubs2` 数据库的所有者，并且已授予 Joe 在此数据库中创建表的权限。现在，Joe 创建了 `new_authors` 表，则他就是此数据库对象的所有者。

最初，只有 Joe 具有 `new_authors` 的对象访问权限。Joe 可以将此表的对象访问权限授予其他用户或撤消此权限。

以下对象更改权限缺省为表的所有者，并且不能移交给其他用户：

- `alter table`
- `drop table`
- `create index`

使用 `grant` 和 `revoke` 命令可授予特定用于对于特定数据库对象的 `select`、`insert`、`update`、`delete`、`references`、`decrypt`、`truncate table`、`update statistics`、`delete statistics` 和 `execute` 权限，可使用 `grant with grant option` 命令将这些权限移交给其他用户。

对对象（表、视图、索引、存储过程、规则、加密密钥、触发器或缺省值）执行 `drop` 命令的权限，在缺省情况下授予给对象所有者，且不能移交给其他用户。

其他数据库用户的特权

其他数据库用户位于层次底部。由对象所有者、数据库所有者、已授权的用户、系统管理员或系统安全员授予他们权限或撤消权限。这些用户由用户名、组名或关键字 `public` 指定。

系统过程的权限

在存储系统过程的 `sybsystemprocs` 数据库中设置系统过程的权限。

与安全性相关的系统过程只能由系统安全员运行。其它某些系统过程只能由系统管理员运行。

某些系统过程只能由数据库所有者运行。这些过程可以确保执行过程的用户是从中执行这些过程的数据库的所有者。

其它系统过程可由已授予权限的任何用户执行。用户在所有数据库中都必须具有执行系统过程的权限，或者在任一数据库中都不具有这一权限。

`sybsystemprocs..sysusers` 中未列出的用户在 `sybsystemprocs` 中被视为“`guest`”，并被自动授予多个系统过程的权限。若要拒绝向用户授予系统过程权限，系统管理员必须将此用户添加到 `sybsystemprocs..sysusers` 中，并发出适用于该过程的 `revoke` 语句。用户数据库的所有者不能从自己的数据库内部直接控制系统过程的权限。

授予和撤消权限

以下类型的权限由 `grant` 和 `revoke` 控制：

- 对象访问权限
- 选择函数的权限
- 执行命令的权限 (P)
- 执行 `dbcc` 命令的权限
- 执行某些 `set` 命令的权限
- 系统表的缺省权限

每个数据库都有自己独立的保护系统。在某个数据库中有权使用某一命令并不意味着也有权在其它数据库中使用同一命令。

对象访问权限

对象访问权限控制访问某些数据库对象的某些命令的使用。例如，必须明确授予用户在 `authors` 表上有使用 `select` 命令的权限。对象访问权限由对象所有者（以及系统管理员或系统安全员）授予和撤消，他们可以将这些权限授予其他用户。

表 17-1 列出了对象访问权限的类型及其适用对象。

表 17-1：权限及其适用对象

权限	对象
select	表、视图和列
update	表、视图和列
insert	表和视图
delete	表和视图
references	表和列
execute	存储过程
truncate table	表
delete statistics	表
update statistics	表
decrypt	表、视图和列
select	加密密钥

`references` 权限指可在 `alter table` 或 `create table` 命令中指定的参照完整性约束。`decrypt` 权限指对加密列进行解密所需的权限。加密密钥的 `select` 权限指在 `create table`、`alter table` 或 `select into` 命令中使用加密密钥对列进行加密所需的权限。其它权限参见 SQL 命令。对象访问权限缺省授予对象所有者，或授予系统管理员或系统安全员对于加密列的 `decrypt` 和对于加密密钥的 `select` 权限，并且可将对象访问权限授予其他用户。

使用 `grant` 命令授予对象访问权限。语法为：

```
grant {all [privileges]| permission_list}
on { table_name [(column_list)]
    | view_name [(column_list)]
    | stored_procedure_name}
to {public | name_list | role_name}
[with grant option]
```

使用 `revoke` 命令撤消对象访问权限。语法为：

```
revoke [grant option for]
{all [privileges] | permission_list}
on { table_name [(column_list)]
    | view_name [(column_list)]
    | stored_procedure_name}
from {public | name_list | role_name}
[cascade]
```

- **all** 或 **all privileges** 指定适用于特定对象的所有权限（解密权限除外）。所有对象所有者都可以使用含有对象名的 **all** 授予或撤消各自对象的权限。如果要授予或撤消存储过程的权限，则 **all** 与 **execute** 作用相同。

注释 **insert**、**update statistics**、**delete statistics**、**truncate table** 和 **delete** 权限不适用于列，因此，如果指定了列的列表，则不能将这些权限包括在权限列表中（或使用关键字 **all**）。

- *permission_list* 是要授予的权限的列表。如果指定多个权限，请用逗号将它们分隔开来。[表 17-2](#) 阐述了可针对每种对象类型授予的访问权限：

表 17-2: 对象访问权限

对象	permission_list 可包括
表或视图	select、insert、delete、update、references、truncate table、update statistics、decrypt、delete statistics references 适用于表，但不适用于视图；其它权限既适用于表，也适用于视图。update statistics、delete statistics 和 truncate table 适用于表，而不适用于视图。
列	select、update、references
存储过程	execute
加密密钥	select

可以在 *permission_list* 或 *column_list* 中指定列，但不能在两者中同时指定列。

- **on** 指定要授予或撤消其权限的对象。一次只能授予或撤消一个表、视图、加密密钥或存储过程对象的权限。一次可以授予或撤消多个列的权限，但所有列必须在同一表或视图中。只能授予或撤消当前数据库中对象的权限。
- **public** 指 “public” 组，其中包括所有 Adaptive Server 用户。对于 **grant** 和 **revoke**，**public** 的含义稍有不同：
 - 对于 **grant**，**public** 包括对象所有者。因此，如果您撤消了自己对于您的对象的权限，稍后再将 **grant** 权限授予 **public**，则您会和 “public” 的其余用户一同重新获得对该对象的权限。
 - 对于 **revoke**，**public** 不包括对象所有者。
- *name_list* 包括：
 - 组名
 - 用户名
 - 既有用户名又有组名，相邻名称之间以逗号分隔开来

- *role_name* 是 Adaptive Server 系统定义角色或用户定义角色。可以创建和定义用户定义角色的层次，并根据授予的特定角色授予相应的特权。系统定义角色包括 **sa_role**（系统管理员）、**sso_role**（系统安全员）和 **oper_role**（操作员）。不能创建或修改系统定义角色。
- **grant** 语句中的 **with grant option** 允许 *name_list* 中指定的用户将指定的对象访问权限授予其他用户。如果某个用户具有某个对象的 **with grant option** 权限，则在撤消 **public** 或此用户所在组对此对象的权限时，不撤消此权限。
- **grant option for** 会撤消 **with grant option** 权限。因此，*name_list* 中指定的用户不能再将指定的权限授予其他用户。如果这些其他用户已将权限授予另一些用户，则必须使用 “**cascade**” 选项撤消其权限。*name_list* 中指定的用户保留对象访问权限，但不能再将访问权限授予其他用户。**grant option for** 仅适用于对象访问权限，而不适用于对象创建权限。
- **revoke** 语句中的 **cascade** 选项删除 *name_list* 中指定用户的指定对象访问权限，并且，如果他们将此访问权限转授给其他用户，则同时删除这些用户的指定对象访问权限。

只能授予和撤消当前数据库中对象的权限。

如果有多个用户授予某个特定用户访问某对象的权限，则在所有授权用户或系统管理员撤消该访问权限之前，该用户的访问权限将一直予以保留。也就是说，如果系统管理员撤消了访问权限，则即使其他用户已授予此用户访问权限，此用户仍然无权访问。

只有系统安全员才能授予或撤消创建加密密钥的权限。数据库所有者可在任何用户表中创建触发器。用户只能在其拥有的表中创建触发器。

在缺省情况下，发出 **create trigger** 命令的权限授予用户。

当系统安全员撤消用户创建触发器的权限时，会将撤消行添加到该用户的 **sysprotects** 表中。若要向该用户授予发出 **create trigger** 的权限，请发出两个 **grant** 命令：第一个命令从 **sysprotects** 中删除撤消行；第二个命令插入一个授权行。系统安全员必须授予创建触发器的权限。如果撤消创建触发器的权限，则用户不能创建触发器，即便是在自己的表上也不行。撤消用户创建触发器的权限只影响从中发出 **revoke** 命令的数据库。

具体标识

在会话期间 Adaptive Server 通过登录名来标识用户。此标识适用于服务器中的所有数据库。用户创建对象后，服务器会将所有者的数据库用户 ID (*uid*) 和创建者的登录名与 **sysobjects** 表中的该对象相关联。这些信息将对象具体标识为属于此用户，从而允许服务器在隐式授予对象权限时识别。

如果 Adaptive Server 用户创建了一个表，然后创建了一个访问该表的过程，则任何授予了执行此过程的权限的用户，将不再需要直接访问此对象的权限。例如，通过向用户 “mary” 授予 **proc1** 的权限，她虽然对于表 **table1** 没有显式的选择权限，但可以查看该表中的 **id** 和 **descr** 列：

```
create table table1 (id      int,
                    amount money,
                    descr   varchar(100))

create procedure proc1 as select id, descr from table1

grant execute on proc1 to mary
```

但是某些情况下，只有当对象被具体标识，隐式权限才有用。其一是涉及别名和跨数据库对象访问。

SQL92 标准一致性的特殊要求

如果已使用 **set** 命令来启用 **ansi_permissions**，则 **update** 和 **delete** 语句还需要其它权限。[表 17-3](#) 对所需权限进行了总结。

表 17-3：用于更新和删除的 ANSI 权限

所需权限：将 ansi_permissions 设置为 “关闭”		所需权限：将 ansi_permissions 设置为 “打开”	
update	针对要设置值的列的 update 权限	针对要设置值的列的 update 权限	和 针对出现在 where 子句中的所有列的 select 权限 set 子句右侧所有列的 select 权限
delete	表的 delete 权限	要删除其中的行的表的 delete 权限	和 针对出现在 where 子句中的所有列的 select 权限

如果 **ansi_permissions** 设置为打开状态，并试图在不具有其它 **select** 权限的情况下进行 **update** 或 **delete**，则此事务被回退，并且收到一条错误消息。如果发生这种情况，对象所有者必须授予所有相关列的 **select** 权限。

授予对象访问权限示例

以下语句授予 Mary 和 “sales” 组在 titles 表中执行插入和删除操作的权限：

```
grant insert, delete
on titles
to mary, sales
```

以下语句授予 Harold 使用存储过程 makelist 的权限：

```
grant execute
on makelist
to harold
```

以下语句将执行自定义存储过程 sa_only_proc 的权限授予具有系统管理员角色的用户：

```
grant execute
on sa_only_proc
to sa_role
```

以下语句授予 Aubrey 在 authors 表中选择、更新和删除的权限，并向其授权将相同权限授予其他用户：

```
grant select, update, delete
on authors
to aubrey
with grant option
```

撤消对象访问权限示例

以下两个语句都撤消所有用户（表所有者除外）对 titles 表中 price 列和 total_sales 列的更新权限：

```
revoke update
on titles (price, total_sales)
from public
```

以下语句撤消 Clare 更新 authors 表的权限。如果她将此权限转授给其他用户，则此语句同时撤消所有这些用户的该权限：

```
revoke update
on authors
from clare
cascade
```

以下语句撤消操作员执行自定义存储过程 new_sproc 的权限：

```
revoke execute
on new_sproc
from oper_role
```

授予和撤消 *update statistics*、*delete statistics* 和 *truncate table* 的权限

Adaptive Server 允许您授予和撤消用户、角色和组对 *update statistics*、*delete statistics* 和 *truncate table* 命令的权限。通过将 *update statistics*、*delete statistics* 和 *truncate table* 添加到一个存储过程，然后将此过程的执行权限授予用户或角色，表所有者也可以通过隐式 *grant* 提供权限。

不能在列级授予或撤消 *update statistics* 的权限。必须具有 *sso_role* 才能在 *sysroles*、*sysssrvroles* 和 *sysloginroles* 安全表上运行 *update statistics* 或 *delete statistics*。

缺省情况下，具有 *sa_role* 的用户有权在除 *sysroles*、*sysssrvroles* 和 *sysloginroles* 之外的系统表上运行 *update statistics* 和 *delete statistics*，并且可以将此特权转交给其他用户。

grant 和 *revoke* 的部分语法为：

```
grant [truncate table | update statistics | delete statistics] on table_name
to {user_name | role_name | group_name}

revoke [truncate table | update statistics | delete statistics] on
table_name from {user_name | role_name | group_name}
```

还可以发出 *grant all* 授予 *update statistics*、*delete statistics* 和 *truncate table* 的权限。

例如，以下语句允许用户 “harry” 对 *authors* 表使用 *truncate table* 和 *updates statistics*：

```
grant truncate table on authors to harry
grant update statistics on authors to harry
```

以下命令语句 “harry” 对 *authors* 表的 *truncate table* 和 *update statistics* 特权：

```
revoke truncate table on authors from harry
revoke update statistics on authors from harry
```

以下语句允许用户 “billy” 对 *authors* 表使用 *delete statistics* 命令：

```
grant delete statistics on authors to billy
```

以下语句撤消用户 “billy” 对 *authors* 表的 *delete statistics* 特权：

```
revoke delete statistics on authors from billy
```

以下语句授予所有具有 *oper_role* 的用户 *truncate table* 和 *update* 及 *delete statistics* 特权（如果用户 “billy” 和 “harry” 拥有 *oper_role*，则他们现在可对 *authors* 运行这些命令）：

```
grant truncate table on authors to oper_role
grant update statistics on authors to oper_role
grant delete statistics on authors to oper_role
```

以下语句撤消所有具有 `oper_role` 的用户的 `truncate table` 和 `update` 及 `delete statistics` 特权：

```
revoke truncate table on authors from oper_role
revoke update statistics on authors from oper_role
revoke delete statistics on authors from oper_role
```

用户 “billy” 和 “harry” 不再能对 `authors` 运行这些命令。

还可以通过一个存储过程来隐式授予 `truncate table`、`delete statistics` 和 `update statistics` 的权限。例如，假设 “billy” 拥有 `authors` 表，他可以运行以下命令授予 “harry” 对 `authors` 表运行 `truncate table` 和 `update statistics` 的特权：

```
create procedure sprocl
as
truncate table authors
update statistics authors
go
grant execute on sprocl to harry
go
```

也可以通过存储过程在列级隐式授予 `update statistics` 和 `delete statistics` 的权限。

注释 一旦授予用户执行 `update statistics` 的权限，他们也就具有执行此命令的各种变化形式的权限，例如 `update all statistics`、`update partition statistics`、`update index statistics`、`update statistics table` 等。例如，以下命令授予 “billy” 对 `authors` 表运行 `update statistics` 的各种变化形式的权限：

```
grant update statistics on authors to billy
```

如果撤消用户执行 `update statistics` 的权限，也就撤消了他们执行此命令的各种变化形式的能力。

不能单独授予 `update statistics` 的变化形式（例如，`update index statistics`）。也就是说，不能发出以下命令：

```
grant update all statistics to harry
```

但是，可以编写存储过程来控制谁执行这些命令。例如，以下命令授予 “billy” 在 `authors` 表上执行 `update index statistics` 的权限：

```
create proc sp_ups as
update index statistics on authors
go
revoke update statistics on authors from billy
go
grant execute on sp_ups to billy
```

不能在列级授予和撤销 `delete statistics` 权限。

尽管 Adaptive Server 将 `truncate table` 作为一个全局、杂类审计进行审计，但是它不审计 `update statistics`。为了使 `truncate table` 和 `update statistics` 的审计追踪保持清晰明了，Sybase 建议您在授予用户执行权限的存储过程中包括这两条命令，如上所述。

如果用户发出 `update statistics`、`delete statistics` 或 `truncate table` 并且他们符合下列条件之一，则命令将失败并生成错误号 10330：

- 不拥有此表。
- 不具有 `sa_role`。
- 不是数据库所有者，该所有者成功使用 `setuser` 成为此表的所有者。
- 尚未被授予 `update statistics`、`delete statistics` 或 `truncate table` 特权。

授予函数的权限

使用 `grant select on builtin function_name` 授予用户使用函数 `set_appcontext`、`get_appcontext`、`list_appcontext` 和 `rm_appcontext` 的权限。

语法为：

```
grant select on [builtin] function_name
to {name_list | role_list}
```

其中：

- `builtin` — 用于区分表和同名的可授予的函数。
- `function_name` — 您授予其权限的函数的名称。可以授予 `select` 权限的函数是 `set_appcontext`、`get_appcontext`、`list_appcontext` 和 `rm_appcontext`。
- `name_list` — 用户数据库名和组名的列表。
- `role_list` — 向其授予权限的系统定义角色或用户定义角色的名称列表，而且不能是变量。

以下语句授予 `public` 对 `get_appcontext` 函数的 `select` 权限：

```
grant select on builtin get_appcontext to public
```


授予和撤消执行命令的权限

本节介绍如何授予和撤消用户执行特定命令的权限。

授予执行命令的权限

对象创建权限控制对创建对象的命令的使用。除了用于创建对象的权限外，可以授予诸如 `connect` 和 `set session authorization` 等其它命令。这些权限只能由系统管理员或数据库所有者（除非另有说明）授予。

命令包括：

- `connect`
- `create database`
- `create default`
- `create procedure`
- `create rule`
- `create table`
- `create view`
- `set session authorization`
- `create encryption key`（只可由系统安全员授予）
- `create trigger`（只可由系统安全员授予）

命令权限的语法与对象访问权限的语法稍有不同。 `grant` 的语法为：

```
grant {all [privileges] | command_list}
to {public | name_list | role_name}
```

`revoke` 的语法为：

```
revoke {all [privileges] | command_list}
from {public | name_list | role_name}
```

其中：

- `all` 或 `all privileges` — 只能由系统管理员或数据库所有者使用。由系统管理员在 `master` 数据库中使用时，`grant all` 将指派所有 `create` 权限，其中包括 `create database`（`create encryption key` 和 `create trigger` 除外）。如果系统管理员从另一数据库中执行 `grant all`，则会授予除 `create database`、`create trigger` 和 `create encryption key` 外的所有 `create` 权限。当数据库所有者使用 `grant all` 时，Adaptive Server 将授予除 `create database`、`create trigger` 和 `create encryption key` 外的所有 `create` 权限，并显示信息性消息。

- *command_list* — 要授予或撤消的对象创建及其它命令权限。用逗号分隔各个命令。列表可包括 `create database`、`create default`、`create procedure`、`create rule`、`create table`、`connect`、`create encryption key`、`set session authorization`、`create view` 和 `create trigger`。`create database` 权限只能由系统管理员授予，且只能从 `master` 数据库内授予。您必须有系统安全员特权才能授予 `create encryption key`、`set session authorization` 和 `create trigger` 权限。
- *public* — 除数据库所有者（在数据库内“拥有”对象创建权限）之外的所有用户。
- *name_list* — 用户名或组名列表，各名称之间用逗号分隔。
- *role_name* — Adaptive Server 系统定义角色或用户定义角色的名称。可以创建和定义用户定义角色的层次，并根据授予的特定角色授予相应的特权。

授予命令权限示例

第一个示例授予 Mary 和 John 使用 `create database` 和 `create table` 的权限。因为正在授予 `create database` 权限，所以此命令只能由系统管理员在 `master` 数据库内执行。Mary 和 John 的 `create table` 权限仅适用于 `master` 数据库。

```
grant create table, create database
to mary, john
```

以下命令将在当前数据库中创建表和视图的权限授予所有用户：

```
grant create table, create view
to public
```

撤消命令权限示例

此示例撤消 “mary” 创建表和规则的权限：

```
revoke create table, create rule
from mary
```

授予代理授权

系统安全员使用 `grant set proxy` 或 `grant set session authorization` 命令授予用户模拟服务器中另一用户的权限。随后，具有此权限的用户可以执行 `set proxy` 或 `set session authorization` 以充当另一用户。

若要授予代理授权权限，您必须是系统安全员，并从 `master` 数据库中执行 `grant` 命令。语法为：

```
grant set proxy to user | role
    [restricted role role_list | all | system]
```

其中：

- *role_list* — 限制目标登录名的角色列表。如果被授者尚未拥有授予他们的 *role_list* 中的角色，并且目标登录名包含已授予的 *role_list* 中的角色，则对目标登录名进行 `set proxy` 将失败。
- *all* — 当用于将 `set proxy` 授予 *role_list* 时，限制在切换标识时为被授者授予任何新角色。
- *system* — 确保被授者与目标登录名具有相同的系统角色集。

示例 1

示例 1：此示例将 `set proxy` 授予用户 “joe”，但限制他将标识切换为任何具有 `sa_role`、`sso_role` 或 `admin_role` 角色的用户（但是，如果他已经有这些角色，则可以对具有这些角色的任何用户执行 `set proxy`）：

```
grant set proxy to joe
    restricted role sa_role, sso_role, admin_role
```

如果 “joe” 尝试将其标识切换为某个具有 `admin_role` 的用户（此示例中为 `Our_admin_role`）时，除非他已经具有 `admin_role`，否则命令将失败：

```
set proxy Our_admin_role
Msg 10368, Level 14, State 1:
Server 's', Line 2:Set session authorization permission
denied because the target login has a role that you do
not have and you have been restricted from using.
```

“joe” 被授予 `admin_role` 并重试此命令后，此命令成功：

```
grant role admin_role to joe
set proxy Our_admin_role
```

示例 2

示例 2：限制 “joe” 在切换标识时被授予任何新的角色：

```
grant set proxy to joe
restricted role all
```

“joe” 只能将 **set proxy** 授予具有与他相同角色（或角色子集）的用户。

示例 3

示例 3：限制 Joe 在使用 **set proxy** 时获得任何新的系统角色：

```
grant set proxy to joe
restricted role system
```

如果目标登录名具有 Joe 所没有的系统角色，则 **set proxy** 将失败。

授予 dbcc 命令的权限

系统管理员可以将执行 **dbcc** 命令的权限授予在 Adaptive Server 中不具有系统管理员级特权的用户和角色。这种**自由选择访问控制**使管理员能够控制对数据库对象或特定数据库级和服务级操作的访问。

请参见《参考手册：命令》了解完整的 **dbcc** 语法。

服务器范围的和特定于数据库的 dbcc 命令

dbcc 命令可以是以下两种情况之一：

- 特定于数据库 — 对特定目标数据库（例如，**checkalloc**、**checktable**、**checkindex**、**checkstorage**、**checkdb**、**checkcatalog**、**checkverify**、**fix_text**、**indexalloc**、**reindex**、**tablealloc** 和 **textalloc**）执行的 **dbcc** 命令。尽管这些命令特定于数据库，但只有系统管理员才能授予或撤销执行它们的权限。
- 服务器范围 — 有服务器范围内有效并且与任何特定数据库均无关联的 **dbcc** 命令（例如 **tune**）。缺省情况下，这些命令会在服务器范围内授予，并且与任何数据库都没有关联。

系统管理员可允许用户在所有数据库中执行 **dbcc** 命令，方法是使这些用户成为这些数据库中的有效用户。但是，向角色授予执行 **grant dbcc** 命令的权限比向单独用户授予该权限更加方便，因为这样可以使用户以 “guest” 用户的身份使用数据库，而不需要手动将每个用户添加到数据库中。

从安全管理的角度来看，系统管理员可能更希望在服务器范围内授权执行特定于数据库的 **dbcc** 命令。例如，可以针对名为 **storage_admin_role** 的用户定义角色对所有数据库执行 **grant dbcc checkstorage**，从而无需针对每个数据库中的 **storage_admin_role** 执行 **grant dbcc checkstorage**。

以下命令在服务器范围内有效，而不是特定于数据库的命令：

- 服务器范围的 `dbcc` 命令，例如 `tune`。
- 在服务器范围内授予的特定于数据库的 `dbcc` 命令，例如授予 `storage_admin_role` 的 `grant dbcc checkstorage`。

数据库中 `dbcc` 的被授者和用户

`grant dbcc` 和 `revoke dbcc` 可以用于数据库中的用户。

由于在数据库中第一次对角色执行 `grant` 时，角色即作为用户被自动添加到数据库中，因此，当角色被授予 `dbcc` 特权时，不会再有其它要求。登录名必须是在其中进行授权的数据库中的有效用户。有效用户包括“`guest`”。

对于服务器范围的 `dbcc` 命令，登录名必须是 `master` 中的有效用户，并且系统管理员必须在 `master` 中授予权限。

对于特定于数据库的 `dbcc` 命令，登录名应是目标数据库中的有效用户。

系统表的权限

如同任何其它表的权限一样，可以由数据库所有者来控制系统表的使用权限。创建数据库之后，某些系统表的 `select` 权限将授予 `public`，而某些系统表的 `select` 权限只有管理员才有。对于其它表，部分列的 `select` 权限对 `public` 有限制。

若要确定特定系统表的当前权限，请执行：

```
sp_helpprotect system_table_name
```

例如，若要检查 `master` 数据库中 `syssrvroles` 的权限，请执行：

```
use master
go
sp_helpprotect syssrvroles
go
```

缺省情况下，包括数据库所有者在内的任何一个用户都不能直接修改系统表，而是由 Adaptive Server 提供的 T-SQL 命令和系统过程来修改系统表。此种作法有助于保证完整性。

警告！ 虽然 Adaptive Server 提供了修改系统表的机制，Sybase 仍强烈建议不要进行修改。

授予系统表和存储过程缺省权限

grant 和 revoke 命令包括 default permissions 参数。installmodel 或 installmaster 不会授予任何系统表的缺省权限（请参见下表）。相反，Adaptive Server 在建立新的数据库时分配系统表的缺省权限。此命令的部分语法为：

```
grant default permissions on system tables
revoke default permissions on system tables
```

其中， default permissions on system tables 指定当您从任何数据库发出此命令时，都可以授予或撤消以下系统表的缺省权限：

sysalternates	sysjars	sysqueryplans	systypes
sysattributes	syskeys	sysreferences	sysusermessages
syscolumns	syslogs	sysroles	sysusers
syscomments	sysobjects	syssegments	sysxtypes
sysconstraints	syspartitions	sysstatistics	
sysdepends	sysprocedures	systabstats	
sysindexes	sysprotects	systhresholds	

default permissions on system tables 还进行以下更改：

- 撤消 public 的 syscolumns(encrkeyid) 的 select
- 撤消 public 的 select on syscolumns(encrkeydb)
- 将对 syscolumns 的 select 授予 sso_role
- 撤消 public 的 sysobjects(audflags) 权限
- 将 sysobjects 的权限授予 sso_role
- 撤消 public 对 sysencryptkeys 的所有列的 select
- 将对所有 sysencryptkeys 列的 select on 授予 sso_role

如果从 master 数据库运行此命令，则授予或撤消以下系统表的缺省权限：

syscharsets	syslanguages	sysremotelogins	systransactions
sysconfigures	syslocks	sysresourcelimits	sysusages
syscurconfigs	syslogins	syssservers	
sysdatabases	sysmessages	syssessions	
sysdevices	sysprocesses	systimeranges	

此命令还进行以下更改：

- 撤消 public 对 sysdatabases(audflags) 的 select
- 撤消 public 的 syscolumns(encrkeyid) 的 select
- 撤消 public 对 syscolumns(encrkeydb) 的 select
- 将对 syscolumns 的 select 授予 sso_role
- 撤消 public 对 sysdatabases(deftabaud) 的 select
- 撤消 public 对 sysdatabases(defvwaud) 的 select
- 撤消 public 对 sysdatabases(deffraud) 的 select
- 撤消 public 对 sysdatabases(audflags2) 的 select
- 将对 sysdatabases 的 select 授予 sso_role。
- 撤消 public 对 syslogins(password) 的 select
- 撤消 public 的 syslogins(audflags) 的 select
- 将对 syslogins 的 select 授予 sso_role
- 撤消 public 对 syslisteners(net_type) 的 select
- 撤消 public 对 syslisteners(address_info) 的 select
- 将对 syslisteners 的 select 授予 sso_role
- 撤消 public 对 sysssrvroles(srid) 的 select
- 撤消 public 对 sysssrvroles(name) 的 select
- 撤消 public 对 sysssrvroles(password) 的 select
- 撤消 public 对 sysssrvroles(pwdate) 的 select
- 撤消 public 对 sysssrvroles(status) 的 select
- 撤消 public 对 sysssrvroles(logincount) 的 select
- 将对 sysssrvroles 的 select 授予 sso_role
- 撤消 public 对 sysloginroles(suid) 的 select
- 撤消 public 对 sysloginroles(srid) 的 select
- 撤消 public 对 sysloginroles(status) 的 select
- 撤消 sso_role 对 sysloginroles 的 select

组合 *grant* 和 *revoke* 语句

可将特定权限分配给特定用户，或者，如果要将大多数特权授予大多数用户，则可先将所有权限分配给所有用户，然后再撤消特定用户的特定权限，这样做更为简便。

例如，数据库所有者可通过发出以下命令，将 **titles** 表的所有权限授予所有用户：

```
grant all
on titles
to public
```

数据库所有者随后可发出一系列 **revoke** 语句，例如：

```
revoke update
on titles (price, advance)
from public
revoke delete
on titles
from mary, sales, john
```

grant 和 **revoke** 语句须区分先后顺序：发生冲突时，最近发出的语句将取代所有其它语句。

注释 在 SQL 规则下，必须先使用 **grant** 命令，然后再使用 **revoke** 命令，而不能在同一事务中使用这两个命令。因此，如果先授予对某些对象的“public”访问权限，然后又撤消其中一个用户的访问权限，则在短暂时间内，此用户仍可以访问这些对象。若要防止这种情况发生，请使用 **create schema** 命令将 **grant** 和 **revoke** 子句并入同一事务中。

了解权限顺序及层次

`grant` 和 `revoke` 语句与其发出的先后次序有关。例如，如果先为 Jose 所在的组授予对 `titles` 表的 `select` 权限，然后撤消 Jose 对 `advance` 列的 `select` 权限，则 Jose 可以选择 (`select`) 除 `advance` 列之外的所有列，而组中的所有其他用户仍然可以选择 (`select`) 所有列。

适用于某个组或角色的 `grant` 或 `revoke` 语句可更改已指派给该组或角色中任何成员的所有相互冲突的权限。例如，如果 `titles` 表所有者已将不同权限授予 `sales` 组的各个成员，并希望标准化，则此所有者可以发出以下语句：

```
revoke all on titles from sales
grant select on titles(title, title_id, type,
                      pub_id)
to sales
```

同样，如果已向 `public` 发出 `grant` 或 `revoke` 语句，则所有用户以前发出的所有权限只要与新权限发生冲突都会更改。

相同的 `grant` 和 `revoke` 语句按不同顺序发出时会产生完全不同的情况。例如，下面一组语句将导致 `public` 组成员 Jose 对 `titles` 不具有任何 `select` 权限：

```
grant select on titles(title_id, title) to jose
revoke select on titles from public
```

相反，如颠倒顺序发出同一组语句，结果只有 Jose 才具有对 `title_id` 和 `title` 列的 `select` 权限：

```
revoke select on titles from public
grant select on titles(title_id, title) to jose
```

如果在 `grant` 命令中使用 `public` 关键字，则也包括自己在内。如果对对象创建权限执行 `revoke`，则除非您是数据库所有者，否则 `public` 也包括您自己在内。如果对对象访问权限执行 `revoke`，则除非您是对象所有者，否则 `public` 也包括您自己在内。您也许希望不具有自己所有的表的使用权限，而只具有基于此表的视图的访问权限。为此目的，必须发出 `grant` 和 `revoke` 语句，明确设置自己的权限。可以使用 `grant` 语句重新设置此权限。

Grant dbcc 和 set proxy 发出针对 fipsflagger 的警告

如果启用了 `set fipsflagger` 选项，在发出 `grant dbcc` 和 `set proxy` 命令时它们会发出以下警告：

```
SQL statement on line number 1 contains Non-ANSI
text.The error is caused due to the use of DBCC.
```

授予和撤消角色

定义了角色之后，可以将其授予服务器中的任何登录帐户或角色，只要不违反互斥性和层次规则即可。[表 17-4](#) 列出了与角色相关的任务、执行任务所要求的角色以及要使用的命令。

表 17-4：任务、要求的角色和所用命令

任务	要求的角色	命令
授予 sa_role 角色	系统管理员	grant role
授予 sso_role 角色	系统安全员	grant role
授予 oper_role 角色	系统安全员	grant role
授予用户定义角色	系统安全员	grant role
创建角色层次	系统安全员	grant role
修改角色层次	系统安全员	revoke role
撤消系统角色	系统安全员	revoke role
撤消用户定义角色	系统安全员	revoke role

授予角色

若要将角色授予用户或其他角色，请使用：

```
grant role role_granted [{, role_granted}...]
to grantee [{, grantee}...]
```

其中：

- `role_granted` — 是所授予的角色。可以指定任意多个要授予的角色。
- `grantee` — 是用户或角色的名称。可以指定任意多个被授者。

`grant` 语句中列出的所有角色都会授予所有被授者。如果将一个角色授予另一角色，则会创建一个角色层次。

例如，若要为 Susan、Mary 和 John 授予 “financial_analyst” 和 “payroll_specialist” 角色，请输入：

```
grant role financial_analyst, payroll_specialist
to susan, mary, john
```

了解 *grant* 和角色

可使用 **grant** 命令，为所有授予了某个角色的用户授予对象权限，这与授予的角色是系统定义角色还是用户定义角色无关。这样，就可以限制具有以下任何一个角色的用户对对象的使用情况：

- 任何系统定义角色
- 任何用户定义角色

只能将角色授予一个登录帐号或另一个角色。

但是，**grant** 权限不妨碍没有特定角色的用户被授予存储过程的 **execute** 权限。例如，若要确保只有系统管理员才能成功执行某个存储过程，请在该存储过程自身内使用 **proc_role** 系统函数。有关详细信息，请参见第 413 页的“显示有关角色的信息”。

授予角色的权限将替换授予用户或组的权限。例如，假定已授予 John 系统安全员角色，并且已授予 **sso_role** 对 **sales** 表的权限。如果撤消 John 对 **sales** 的个人权限，他仍能够在 **sso_role** 处于活动状态时访问 **sales**，因为其角色权限替换了其个人权限。

授予权限时，系统管理员被视作对象所有者。如果系统管理员授予操作另一用户的对象的权限，则相应的所有者名称将作为授权者在 **sysprotects** 和 **sp_helprotect** 输出中显示。

如果有多个用户授予某个特定用户访问某对象的权限，则在所有授权用户撤消该访问权限之前，该用户的访问权限将一直予以保留。如果系统管理员撤消了访问权限，则即使其他用户已授予此用户访问权限，此用户仍然无权访问。

撤消角色

使用 `revoke role` 撤消用户和其他角色的角色：

```
revoke role role_name [{, role_name}...][from grantee [{, grantee}...]
```

其中：

- *role_name* — 是所撤消的角色。可以指定任意多个要撤消的角色。
- *grantee* — 是用户或角色的名称。可以指定任意多个被授者。

`revoke` 语句中列出的所有角色都将从所有被授权者中撤消。

不能在用户登录时撤消该用户的角色。

获取另一用户的权限

Adaptive Server 提供两种方法来获取另一用户的标识和权限状态：

- 数据库所有者可以使用 `setuser` 命令来“模拟”当前数据库中另一用户的标识和权限状态。请参见第 536 页的“使用 `setuser`”。
- **代理授权** 允许一个用户在服务器范围内使用另一用户的标识。请参见第 537 页的“使用代理授权”。

使用 `setuser`

数据库所有者可使用 `setuser` 进行以下操作：

- 访问另一用户所属对象
- 授予他人另一用户所属对象的权限
- 创建将由另一用户拥有的对象
- 由于某些其它原因，临时假定另一用户的 DAC 权限

尽管 `setuser` 命令可使数据库所有者自动获得另一用户的 DAC 权限，但此命令不会影响已经授予的角色。

`setuser` 权限缺省授予数据库所有者，并且不能移交。被模拟的用户必须是数据库的授权用户。Adaptive Server 会检查被模拟用户的权限。

系统管理员可以使用 `setuser` 创建将由另一用户拥有的对象。但是，系统管理员在 DAC 权限系统之外操作，因此，他们不需要使用 `setuser` 来获取另一用户的权限。`setuser` 命令会一直有效，直到发出另一 `setuser` 命令、当前数据库更改或用户退出登录时为止。

语法为：

```
setuser ["user_name"]
```

其中，`user_name` 是数据库中要被模拟的有效用户。

若要重建原始标识，请在不为 `user_name` 赋值的情况下使用 `setuser`。

此示例演示数据库所有者如何授予 Joe 读取 Mary 拥有的 `authors` 表的权限：

```
setuser "mary"
grant select on authors to joe
setuser      /*reestablishes original identity*/
```

使用代理授权

利用 Adaptive Server 的代理授权功能，系统安全员可以将另一用户的安全环境的使用权限授予所选登录名，且应用程序可采用受控方式代表不同用户执行任务。如果某个登录名具有代理授权的使用权限，此登录名就可以模拟 Adaptive Server 中的任何其它登录名。

警告！ 使用另一用户标识的权限功能极强，应将其局限于受托的管理员和应用程序。可以使用 `grant set proxy ... restrict role` 来限制用户在切换标识时无法获取的角色。

执行 `set proxy` 或 `set session authorization` 的用户利用被模拟用户的登录名和服务器用户 ID 进行操作。登录名存储在 `master..syslogins` 的 `name` 列中，服务器用户 ID 存储在 `master..syslogins` 的 `suid` 列中。这些值在整个服务器上的所有数据库中都处于活动状态。

注释 `set proxy` 和 `set session authorization` 在功能上完全相同，可以互换使用。唯一的区别是 `set session authorization` 与 ANSI-SQL92 兼容，而 `set proxy` 是 Transact-SQL 扩展。

使用 set proxy 限制角色

授予 `set proxy...restrict role` 来限制在切换标识时无法获取的角色。

`set proxy` 的语法为：

```
grant set proxy to user | role
[restrict role role_list | all | system]
```

其中：

- *role_list* — 限制目标登录名的角色列表。被授者必须具有此列表上的所有角色，否则 `set proxy` 命令将失败。
- *all* — 确保被授者只能对与被授者具有相同角色（或角色子集）的用户运行 `set proxy`。
- *system* — 确保被授者与目标登录名具有相同的系统角色集。

例如，以下语句将 `set proxy` 授予用户 “joe”，但限制他将标识切换为具有 `sa`、`sso` 或 `admin` 角色的任何用户（但是，如果他已经具有这些角色，则他可以对具有这些角色的任何用户执行 `set proxy`）：

```
grant set proxy to joe
restrict role sa_role, sso_role, admin_role
```

如果 “joe” 尝试将其标识切换为某个具有 `admin_role` 的用户（此示例中为 `Our_admin_role`）时，除非他已经具有 `admin_role`，否则命令将失败：

```
set proxy Our_admin_role
Msg 10368, Level 14, State 1:
Server 's', Line 2:Set session authorization permission
denied because the target login has a role that you do
not have and you have been restricted from using.
```

“joe” 被授予 `admin_role` 并重试此命令后，此命令成功：

```
grant role admin_role to joe
set proxy Our_admin_role
```

有关 `set proxy` 命令的详细信息，请参见 《参考手册：命令》。

执行代理授权

执行 `set proxy` 或 `set session authorization` 时，请遵循以下规则：

- 不得在事务内执行 `set proxy` 或 `set session authorization`。
- 不能为另一用户的代理使用锁定的登录名。例如，如果 “joseph” 是一个锁定的登录名，则不允许执行以下命令：

```
set proxy "joseph"
```
- 可以在任何允许使用的数据库中执行 `set proxy` 或 `set session authorization`。但所指定的 `login_name` 必须是数据库中的有效用户，或者，数据库必须要有为其定义的 “guest” 用户。
- 只允许一个级别；若要模拟多个用户，则在模拟操作之间必须返回到原标识。
- 如果从某个过程内执行 `set proxy` 或 `set session authorization`，则原始标识会在退出该过程时自动恢复。

如果已授予某一登录名使用 `set proxy` 或 `set session authorization` 的权限，则可以设置代理来模拟另一用户。以下是语法，其中 `login_name` 是 `master..syslogins` 中的有效登录名。

```
set proxy login_name
```

或者

```
set session authorization login_name
```

为登录名加上引号。

例如，若要将代理设置为 “mary”，请执行：

```
set proxy "mary"
```

设置代理后，检查服务器中的登录名和数据库中的用户名。例如，假定登录名为 “ralph”，并具有 `set proxy` 授权权限。现在打算以 “sallyn” 和 “rudolph” 身份在 `pubs2` 数据库中执行某些命令。“sallyn” 在此数据库中有一个有效的名称 (“sally”)，而 `Ralph` 和 `Rudolph` 没有。但 `pubs2` 已定义了一个 “guest” 用户。则可以执行：

```
set proxy "sallyn"
go
use pubs2
go
select suser_name(), user_name()
go
-----
sallyn                                sally
```

若要更改为 **Rudolph**，必须首先恢复自己的标识。为此目的，请执行：

```
set proxy "ralph"
select suser_name(), user_name()
go
-----
ralph                                guest
```

注意：**Ralph** 是此数据库中的 “guest”。

然后执行：

```
set proxy "rudolph"
go
select suser_name(), user_name()
go
-----
rudolph                                guest
```

Rudolph 也是此数据库中的 **guest**，因为 **Rudolph** 不是此数据库中的有效用户。

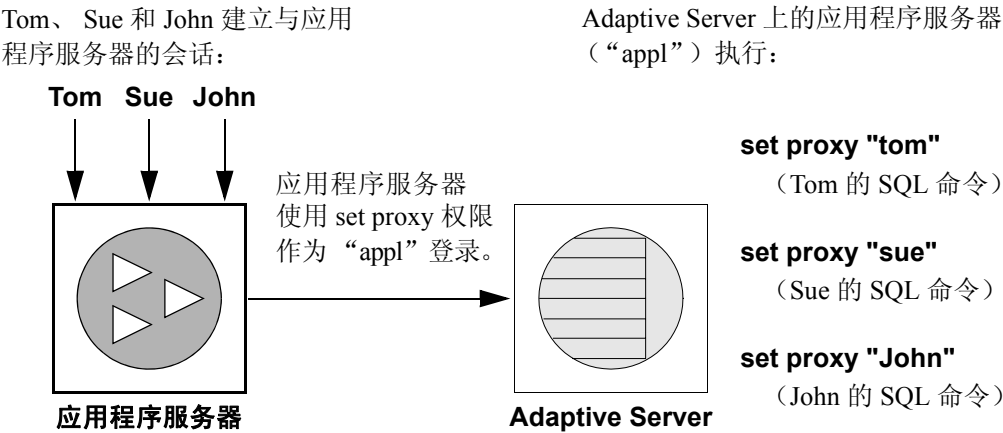
现在，模拟 “sa” 帐户。执行：

```
set proxy "ralph"
go
set proxy "sa"
go
select suser_name(), user_name()
go
-----
sa                                    dbo
```


应用程序的代理授权

图 17-1 显示使用通用登录名 “appl” 登录到 Adaptive Server 为多个用户执行过程和命令的应用程序服务器。一旦 “appl” 模拟 Tom，应用程序就有 Tom 的权限。同样，“appl” 分别模拟 Sue 和 John 时，应用程序便分别有 Sue 和 John 的权限。

图 17-1：应用程序和代理授权



权限报告

表 17-5 列出了用于报告有关代理、对象创建和对象访问权限信息的系统过程：

表 17-5：用于权限报告的系统过程

报告信息	使用
代理	系统表
用户和进程	sp_who
数据库对象或用户的权限	sp_helprotect
特定表的权限	sp_table_privileges
表中特定列的权限	sp_column_privileges

查询代理授权的 **sysprotects** 表

若要显示有关已授予（或撤销）用户、组和角色的权限的信息，请查询 **sysprotects** 表。**action** 列指定权限。例如，**set proxy** 或 **set session authorization** 的 **action** 值为 167。

可以执行以下查询：

```
select * from sysprotects where action = 167
```

结果将提供授予或撤销该权限用户的用户 ID（**grantor** 列）、具有权限的用户的用户 ID（**uid** 列）和保护类型（**protecttype** 列）。**protecttype** 列可包含以下值：

- **grant with grant** 的值为 0
- **grant** 的值为 1
- **revoke** 的值为 2

有关 **sysprotects** 表的详细信息，请参见《参考手册：构件块》。

显示有关用户和进程的信息

sp_who 显示有关当前所有 Adaptive Server 用户和进程的信息，或有关特定用户或进程的信息。**sp_who** 的结果包括 **loginame** 和 **origname**。如果用户正在某个代理下操作，则 **origname** 包含原始登录名的名称。例如，假设 “ralph” 执行以下命令，然后执行一些 SQL 命令：

```
set proxy susie
```

sp_who 为 **loginame** 返回 “susie”，并且为 **origname** 返回 “ralph”。

sp_who 查询 **master..sysprocesses** 系统表。该表包含服务器用户 ID (**suid**) 和原始服务器用户 ID (**origsuid**) 的列。

有关详细信息，请参见《参考手册：过程》中的 **sp_who**。

报告数据库对象或用户的权限

使用 `sp_helprotect` 报告数据库对象或用户的权限，以及用户的指定对象权限（可选）。任何用户都可以执行此过程。语法为：

```
sp_helprotect [name [, username [, "grant"
               [, "none"|"granted"|"enabled"|role_name]]]]
```

其中：

- *name* — 是表、视图或存储过程的名称，或者是当前数据库中用户、组或角色的名称。如果未提供名称，则 `sp_helprotect` 将报告数据库中的所有权限。
- *username* — 是当前数据库中的用户名。
如果指定 *username*，则只报告该用户对指定对象的权限。如果 *name* 不是对象，则 `sp_helprotect` 将检查 *name* 是否为用户、组或角色。如果是用户、组或角色，则列出其权限。如果指定关键字 `grant` 且 *name* 不是对象，则 `sp_helprotect` 将显示通过 `with grant option` 授予的所有权限。
- `grant` — 显示通过 `with grant option` 授予 *name* 的权限。
- `none` — 忽略授予用户的角色。
- `granted` — 包括有关授予用户的所有角色的信息。
- `enabled` — 包括有关被用户激活的所有角色的信息。
- *role_name* — 只显示指定角色的权限信息，而不管此角色是否已授予该用户。

例如，假设您已发出下面一系列 `grant` 和 `revoke` 语句：

```
grant select on titles to judy
grant update on titles to judy
revoke update on titles(contract) from judy
grant select on publishers to judy
with grant option
```

若要确定 `Judy` 现在对 `titles` 表中各列所具有的权限，请输入：

			sp_helprotect titles, judy			
grantor	grantee	type	action	object	column	grantable
-----	-----	-----	-----	-----	-----	-----
dbo	judy	Grant	Select	titles	All	FALSE
dbo	judy	Grant	Update	titles	advance	FALSE
dbo	judy	Grant	Update	titles	notes	FALSE
dbo	judy	Grant	Update	titles	price	FALSE
dbo	judy	Grant	Update	titles	pub_id	FALSE

dbo	judy	Grant	Update	titles	pubdate	FALSE
dbo	judy	Grant	Update	titles	title	FALSE
dbo	judy	Grant	Update	titles	title_id	FALSE
dbo	judy	Grant	Update	titles	total_sales	FALSE
dbo	judy	Grant	Update	titles	type	FALSE

第一行显示数据库所有者（“dbo”）授予 Judy 选择 **titles** 表中所有列的权限。其余各行指示她只能更新显示中出现的列。Judy 不能将 **select** 或 **update** 权限授予任何其他用户。

若要查看 Judy 对 **publishers** 表的权限，请输入：

```
sp_helpprotect publishers, judy
```

在此显示中，**grantable** 列显示为 **TRUE**，表示 Judy 可将权限授予其他用户。

grantor	grantee	type	action	object	column	grantable
-----	-----	-----	-----	-----	-----	-----
dbo	judy	Grant	Select	publishers	all	TRUE

报告特定表的权限

使用 **sp_table_privileges** 返回有关指定表的权限信息。语法为：

```
sp_table_privileges table_name [, table_owner  
[, table_qualifier]]
```

其中：

- *table_name* — 是表的名称，并且为必需。
- *table_owner* — 如果表所有者的名称不是 “dbo” 或执行 **sp_table_privileges** 的用户，则可用于指定表所有者的名称。
- *table_qualifier* — 是当前数据库的名称。

对要跳过的参数使用 **null**。

例如，此语句返回有关授予 **titles** 表的所有权限的信息：

```
sp_table_privileges titles
```

有关 **sp_table_privileges** 的输出的详细信息，请参见 《参考手册：过程》。

报告特定列的权限

使用 `sp_column_privileges` 可返回有关表中列的权限信息。语法为：

```
sp_column_privileges table_name [, table_owner  
[, table_qualifier [, column_name]]]
```

其中：

- *table_name* — 是表的名称。
- *table_owner* — 如果表所有者的名称不是 “dbo” 或执行 `sp_column_privileges` 的用户，则可用于指定表所有者的名称。
- *table_qualifier* — 是当前数据库的名称。
- *column_name* — 是要查看权限信息的列的名称。

对要跳过的参数使用 `null`。

例如，此语句返回有关 `publishers` 表的 `pub_id` 列的信息：

```
sp_column_privileges publishers, null, null, pub_id
```

有关 `sp_column_privileges` 的输出的详细信息，请参见《参考手册：过程》。

使用视图和存储过程作为安全性机制

视图和存储过程可以作为安全性机制。可以通过视图或存储过程授予用户对数据库对象受控制的访问权限，而不授予他们对数据的直接访问权限。例如，可以向操作人员授予对更新 `projects` 表中成本信息的过程的 `execute` 权限，而不让此用户查看此表中的机密数据。若要使用此功能，必须拥有此过程或视图及其基础对象。如果没有基础对象，用户必须具有对象访问权限。有关何时需要权限的详细信息，请参见第 549 页的“了解所有权链”。

Adaptive Server 使用视图或过程时，根据需要进行权限检查。创建视图或过程时，Adaptive Server 不对基础对象进行权限检查。

使用视图作为安全性机制

通过视图，用户只能查询和修改所看到的数据。数据库的其余部分既不可见也不可访问。

必须明确授予或撤消访问视图的权限，而不管视图的基础表的权限如何。如果视图和基础表的权限由同一用户拥有，则不需授予基础表权限。授权访问视图而非基础表的用户无法看到视图中没有的基础表数据。

通过定义不同的视图并有选择地授予它们的权限，可以把用户或用户组合限制到不同的数据子集上。访问权限可以限制到：

- 基表中行的子集（与值相关的子集）。例如，可以定义只包含商业与心理学书籍的视图，使某些用户无法看到其它类型书籍的信息。
- 基表中列的子集（与值不相关的子集）。例如，可以定义包含 **titles** 表中所有行但不包含 **price** 列与 **advance** 列的视图，因为这些信息是敏感的。
- 基表的行列子集。
- 限定多个基表连接的行。例如，可以定义连接 **titles**、**authors** 和 **titleauthor** 表的视图。此视图隐藏了作者的个人信息以及图书的价格信息。
- 基表中数据的统计信息。例如，可以只定义包含各类书籍平均价格的视图。
- 另一视图的子集，或视图和基表的某种组合的子集。

假设要阻止某些用户访问 **titles** 表中显示销售额和销售量的列。则可以创建 **titles** 表中不包括这些列的一个视图，然后将此视图的权限授予所有用户，而只将此表的访问权限授予销售部门：

```
grant all on bookview to public
grant all on titles to sales
```

如果不使用视图来设置这些特权条件的等效方法，则需使用下列语句：

```
grant all on titles to public
revoke select, update on titles (price, advance,
    total_sales)
from public
grant select, update on titles (price, advance,
    total_sales)
to sales
```

第二种解决方案可能遇到的一个问题是：如果用户不在 **sales** 组中而输入了 **select * from titles** 命令，则此用户可能会意外地看到包含以下短语的消息：

```
permission denied
```

Adaptive Server 将星号扩展到 **titles** 表中所有列的列表中，且由于已撤销非销售部门用户对某些列的权限，因此会拒绝对这些列的访问。错误消息列出了用户无权访问的所有列。

若要查看用户有权访问的所有列，非销售部门的用户必须要对它们进行明确指定。因此，较好的解决方法是创建视图并授予相应权限。

也可以使用视图进行**上下文相同的保护**。例如，可以创建一个视图，仅授予数据录入员访问自己添加或更新的那些行的权限。要完成上述操作，必须在表中添加一列。用户每输入一行在此列中就自动缺省记录此用户的 ID。可以在 **create table** 语句中定义此缺省值，如下所示：

```
create table testtable
    (empid          int,
     startdate      datetime,
     username       varchar(30) default user)
```

然后，定义一个包括表中所有行的视图，其中 **uid** 是当前用户：

```
create view context_view
as
    select *
    from testtable
    where username = user_name()
with check option
```

是否可以通过此视图检索行取决于在视图中发出 **select** 命令的用户的标识。将 **with check option** 添加到视图定义中之后，即可防止数据录入员在 **username** 列中伪造信息。

使用存储过程作为安全机制

如果同一个用户同时拥有存储过程与所有底层的对象，那么他可以授予其他用户使用存储过程的权限而不用授予对底层对象的权限。例如，可以授予用户执行存储过程（更新指定表上行列子集）的权限，尽管用户没有对此表的任何其它权限。

角色和存储过程

使用 `grant execute` 命令将存储过程的 `execute` 权限授予具有特定角色的所有用户。`revoke execute` 可删除此权限。但是，`grant execute` 权限不会妨碍对没有指定角色的用户授予存储过程的 `execute` 权限。

为进一步增加安全性，可以通过在存储过程中使用 `proc_role` 系统函数对此过程的使用予以限制，保证某一过程只能由具有给定角色的用户执行。如果用户具有特定角色（`sa_role`、`sso_role`、`oper_role` 或任何用户定义角色），则 `proc_role` 返回 1，如果用户不具有该角色，则返回 0。例如，下面是一个使用 `proc_role` 查看用户是否具有系统管理员角色的过程：

```
create proc test_proc
as
if (proc_role("sa_role") = 0)
begin
    print "You don't have the right role"
    return -1
end
else
    print "You have SA role"
    return 0
```

请参见《参考手册：构件块》中的“系统函数”，了解有关 `proc_role` 的详细信息。

了解所有权链

视图可依据其它视图或表而形成。过程可依据其它过程、视图或表而形成。这种依赖性可以看作是所有权链。

通常，视图所有者还拥有此视图的基础对象（其它视图和表），存储过程所有者拥有此过程引用的所有过程、表和视图。

同存储过程及其引用的所有对象一样，视图及其基础对象常常在同一数据库中；但并不要求必须在同一数据库中。如果对象在不同的数据库中，则要使用视图或存储过程的用户必须是所有包含这些对象的数据库的有效用户或 `guest` 用户。这样，除非数据库所有者已授权，否则用户无法访问数据库。

如果已授予某个用户对某一过程或视图的 `execute` 权限，则在该用户使用此视图或过程时，`Adaptive Server` 在下列情况下不检查任何基础对象的权限：

- 这些对象和视图或过程由同一用户拥有，并且
- 访问视图或过程的用户在每个包含基础对象的数据库中都是有效用户或 `guest` 用户。

但是，如果并非所有对象都由同一用户拥有，则 `Adaptive Server` 将在所有权链断开时检查对象权限。也就是说，如果对象 A 引用对象 B，而对象 B 不是由拥有对象 A 的用户拥有，则 `Adaptive Server` 会检查对象 B 的权限。使用这种方法，`Adaptive Server` 允许原始数据所有者对有权访问此数据的用户进行控制。

通常，创建视图的用户只需关注此视图的授权问题。例如，假设 Mary 已在其拥有的 `authors` 表中创建了名为 `auview1` 的视图。如果 Mary 将 `auview1` 的 `select` 权限授予 Sue，则 `Adaptive Server` 将允许 Sue 访问它，而不检查她对 `authors` 的权限。

但是，某个用户如果要依据另一用户所属对象创建一个视图或存储过程，则此用户必须知道自己的任何授权都取决于这些对象所有者允许的权限。

视图和所有权链的示例

假设 Joe 依据 Mary 的视图 auview1 创建了名为 auview2 的视图。然后，Joe 授予 Sue 对 auview2 的 select 权限。

图 17-2: 视图的所有权链和权限检查, 示例 1

Sue 的权限	对象	所有权	检查
select	auview2	Joe	Sue 不是所有者 检查权限
	↓		
select	auview1	Mary	所有者不同 检查权限
	↓		
无	authors	Mary	所有者相同 不进行权限检查

Adaptive Server 检查 auview2 和 auview1 的权限，发现 Sue 可以使用它们。Adaptive Server 检查 auview1 和 authors 的所有权，发现它们的所有者相同。因此，Sue 可以使用 auview2。

将此例进行一下扩展，假设 Joe 的视图 auview2 依据 auview1 而创建，而视图 auview1 又依据 authors 而创建。Mary 认为自己喜欢 Joe 的 auview2，因此以其为基础创建了 auview3。这样，auview1 和 authors 的所有者都为 Mary。

所有权链如下图所示：

图 17-3：视图的所有权链和权限检查，示例 2

Sue 的权限	对象	所有权	检查
select	auview3	Mary	Sue 不是所有者 检查权限
	↓		
select	auview2	Joe	所有者不同 检查权限
	↓		
select	auview1	Mary	所有者不同 检查权限
	↓		
无	authors	Mary	所有者相同 不进行权限检查

当 Sue 试图访问 auview3 时， Adaptive Server 检查 auview3、 auview2 和 auview1 的权限。如果 Joe 已授予 Sue auview2 的权限， Mary 也已授予她 auview3 和 auview1 的权限， 则 Adaptive Server 将允许进行访问。 Adaptive Server 仅在此链中某对象的前面一个对象具有不同所有者时（或者， 如果对象是此链中第一个对象时）才检查权限。例如， 它检查 auview2， 因为此视图的前一个对象 auview3 由不同的用户拥有。 它不检查 authors 的权限， 因为直接依赖于此视图的对象 auview1 由同一用户拥有。

过程和所有权链的示例

过程遵循的规则与视图相同。例如，假设所有权链如下所示：

图 17-4：存储过程的所有权链和权限检查

Sue 的权限	对象	所有权	检查
execute	proc4	Mary	Sue 不是所有者 检查权限
	↓		
无	proc3	Mary	所有者相同 不进行权限检查
	↓		
execute	proc2	Joe	所有者不同 检查权限
	↓		
execute	proc1	Mary	所有者不同 检查权限
	↓		
无	authors	Mary	所有者相同 不进行权限检查

若要执行 proc4，Sue 必须要有执行 proc4、proc2 和 proc1 的权限。而执行 proc3 的权限不是必需的，因为 proc3 和 proc4 的所有者相同。

Sue 每次执行 proc4 时，Adaptive Server 都会检查她对 proc4 及其引用的所有对象的权限。Adaptive Server 知道要检查哪些引用对象：在 Sue 首次执行 proc4 时，它就已经确定了要检查的引用对象，并将此信息同过程执行计划一同保存。除非此过程引用的对象中有一个对象被删除或重新定义，否则，Adaptive Server 不会更改初始确定的检查对象内容。

使用此保护层次，每个对象所有者都可完全控制对对象的访问。所有者可以控制对视图、存储过程和表的访问。

触发器的权限

触发器是一种特殊的存储过程，用于强制实现完整性，尤其是参照完整性。触发器从来都不能直接执行，而仅作为修改表的副作用。不得 **grant** 或 **revoke** 触发器的权限。

只有对象所有者才可创建触发器。但是，如果表中的触发器引用不同用户拥有的对象，则可能中断所有权链。适用于过程的保护层次规则也适用于触发器。

如果受触发器影响的对象通常由拥有此触发器的用户所有，则可以编写一个触发器，用来修改由另一用户拥有的对象。这种情况下，任何以激活此触发器的方法修改对象的用户都必须具有另一对象的权限。

如果 **Adaptive Server** 由于触发器影响用户对其没有权限的对象而拒绝授予对数据修改命令的权限，则整个数据修改事务会回滚。

请参见《Transact-SQL 用户指南》中的第 19 章“触发器：强制实施参照完整性”。

使用行级访问控制

行级访问控制可提供以下功能，使数据库所有者或表所有者能够自动创建安全数据访问环境：

- 更加细化的数据安全性：可针对个别的行设置权限，而不仅仅针对表和列
- 根据组、角色和应用程序进行的自动数据过滤
- 服务器中编码的数据级安全性

行级访问控制通过三项功能限制对表的个别行中数据的访问：

- 数据库所有者定义并绑定到表的访问规则
- 应用程序环境功能，可提供定义、存储和检索用户定义环境的内置函数
- 数据库所有者、**sa_role** 或用户可创建的登录触发器

Adaptive Server 为所有数据操纵语言 (DML) 实施了行级访问控制，从而可以防止用户绕过访问控制来获取数据。

配置系统实施行级访问控制的语法如下：

```
sp_configure "enable row level access", 1
```

此选项会稍微增加 Adaptive Server 使用的内存量，并且需要 ASE_RLAC 许可证选项。行级访问控制是一个动态选项，因此不需要重新启动 Adaptive Server。

访问规则

若要使用行级访问控制功能，请将 **access** 选项添加到现有的 **create rule** 语法中。访问规则将对任何可被查看或修改的行施加限制。

访问规则类似于域规则，域规则允许表所有者控制用户可以在某个列中插入或更新的值。域规则对添加的数据施加限制，对 **update** 和 **insert** 命令起作用。

访问规则对检索的数据施加限制，对 **select**、**update** 和 **delete** 操作起作用。Adaptive Server 将对查询所读取的所有列强制执行访问规则，即使 **select** 列表中不包括这些列。也就是说，在给定的查询中，Adaptive Server 将对更新的表强制执行域规则，并对所读取的所有表强制执行访问规则。

例如：

```
insert into orders_table  
select * from old_orders_table
```

在此查询中，如果 **orders_table** 上有域规则，**old_orders_table** 上有访问规则，则 Adaptive Server 将对 **orders_table** 强制执行域规则（原因是更新了该表），而对 **old_orders_table** 强制执行访问规则（原因是读取了该表）。

使用访问规则类似于使用视图或带有 **where** 子句的即席查询。查询是在附加访问规则之后才进行编译和优化的，因此它不会导致性能下降。访问规则提供表数据的虚拟视图，视图的内容取决于绑定到列的具体访问规则。

访问规则可以绑定到用 **sp_addtype** 定义的用户定义数据类型。Adaptive Server 在用户表上强制执行访问规则，这样，表所有者或数据库所有者在标准化方案中就无需执行将访问规则绑定到列的维护任务。例如，您可以创建一个名为 **username** 的用户定义类型，其基类型为 **varchar(30)**，并为该类型绑定一个访问规则。Adaptive Server 将对应用程序中任何具有 **username** 类型的列的表强制执行访问规则。

如第 560 页的“访问规则作为用户定义的 Java 函数”和第 563 页的“使用应用程序环境功能”所述，应用程序开发人员可以使用 Java 和应用程序环境编写灵活的访问规则。

访问规则的语法

在 `create rule` 语法中使用 `access` 参数创建访问规则。

```
create [or|and] access rule (access_rule_name)
as (condition)
```

创建带有访问规则的示例表

本节说明创建表并将访问规则绑定到该表的过程。

创建表

表所有者创建并填充表 T (`username char(30)`、`title char(30)`、`classified_data char(1024)`)：

```
AA, "Administrative Assistant", "Memo to President"
AA, "Administrative Assistant", "Tracking Stock
Movements"
VP1, "Vice President", "Meeting Schedule"
VP2, "Vice President", "Meeting Schedule"
```

创建并绑定访问规则

表所有者创建访问规则 `uname_acc_rule` 并将其绑定到表 T 上的 `username` 列。

```
create access rule uname_acc_rule
as @username = suser_name()
-----
sp_bindrule uname_acc_rule, "T.username"
```

查询表

当您发出以下查询时：

```
select * from T
```

Adaptive Server 将处理绑定到表 T 上 `username` 列的访问规则，并将其附加到查询树。然后优化查询树，并生成和执行查询计划，就好像用户执行带有访问规则中给定的过滤器子句一样。也就是说，Adaptive Server 按如下示例附加访问规则并执行查询：

```
select * from T where T.username = suser_name().
```

服务器强制执行条件 `where T.username = suser_name()`。用户不能绕过访问规则。

管理助手执行选择查询的结果是：

```
AA, "Administrative Assistant", "Memo to President"
AA, "Administrative Assistant", "Tracking Stock
Movements"
```

删除访问规则

在删除访问规则之前，必须使用 `sp_unbindrule` 取消它与任何列或数据类型的绑定，如下面的示例所示：

```
sp_unbindrule "T.username",  
NULL, "all"
```

`sp_unbindrule` 可取消绑定缺省情况下附加到列上的任何域规则。

在取消绑定规则之后，可以将其删除：

```
drop rule "rule_name"
```

例如：

```
drop rule "T.username"
```

扩展访问规则的语法

每个访问规则绑定到一个列，但一个表中可以具有多个访问规则。`create rule` 提供 **AND** 和 **OR** 参数来处理多个访问规则的计算。若要创建 **AND** 访问规则和 **OR** 访问规则，请使用扩展访问规则语法：

- **AND** 访问规则：
`create and access rule rule_name`
- **OR** 访问规则
`create or access rule rule_name as`

可以将 **AND** 访问规则和 **OR** 访问规则绑定到列或用户定义数据类型。虽然每个列只能绑定一个访问规则，但通过扩展访问规则语法，可以在表中绑定多个访问规则。当访问表时，这些访问规则就会生效，缺省情况下，先执行绑定的 **AND** 规则，然后执行 **OR** 访问规则。

如果在表中绑定多个访问规则但没有定义 **AND** 或 **OR** 访问，则缺省访问规则为 **AND**。

如果表中某行上只有一个访问规则，并且这一规则被定义为 **OR** 访问规则，则它与 **AND** 访问规则的行为相同。

使用访问规则和扩展访问规则

创建访问规则

以下步骤创建访问规则：

```
create access rule empidl_access
as @empid = 1

create access rule deptnol_access
as @deptid = 2
```

以下步骤创建 OR 访问规则：

```
create or access rule namel_access
as @name = "smith"

create or access rule phone_access
as @phone = "9999"
```

创建表

此步骤创建一个测试表：

```
create table testtab1 (empno int, deptno int, name
char(10), phone char(4))
```

将规则绑定到表

以下步骤将访问规则绑定到测试表中的列：

```
sp_bindrule empidl_access, "testtab1.empno"
/*Rule bound to table column.*/
(return status = 0)

sp_bindrule deptnol_access, "testtab1.deptno"
/*Rule bound to table column.*/
(return status = 0)

sp_bindrule namel_access, "testtab1.name"
/*Rule bound to table column.*/
(return status = 0)

sp_bindrule phone_access, "testtab1.phone"
/*Rule bound to table column.*/
(return status = 0)
```

将数据插入表中

以下步骤将值插入测试表中：

```
insert testtab1 values (1,1,"smith","3245")
(1 row affected)

insert testtab1 values (2,1,"jones","0283")
(1 row affected)

insert testtab1 values (1,2,"smith","8282") (1 row
affected)

insert testtab1 values (2,2,"smith","9999")
(1 row affected)
```

访问规则示例

以下示例说明访问规则如何返回包含访问规则限制的信息的特定行。

示例 1

此示例返回两行中的信息：

```
/* return rows when empno = 1 and deptno = 2
and ( name = "smith" or phone = "9999" )
*/

select * from testtab1

empno      deptno      name      phone
-----
          1          2 smith      8282
          1          2 jones      9999

(2 rows affected)

/* unbind access rule from specific column */
sp_unbindrule "testtab1.empno",NULL,"accessrule"
/*Rule unbound from table column.*/

(return status = 0)
```

示例 2

此示例返回四行中的信息：

```
/* return rows when deptno = 2 and ( name = "smith"
or phone = "9999" )*/

select * from testtab1

empno      deptno      name      phone
-----
          1          2 smith      8282
          2          2 smith      9999
          3          2 smith      8888
          1          2 jones      9999

(4 rows affected)

/* unbind all deptno rules from specific column */
```

```

sp_unbindrule "testtab1.deptno",NULL,"all"
/*Rule unbound from table column.*/

(return status = 0)

```

示例 3

此示例返回六行中的信息：

```

/* return the rows when name = "smith" or phone = "9999"
*/

select * from testtab1

```

empno	deptno	name	phone
1	1	smith	3245
2	1	smith	8282
3	2	smith	9999
4	3	smith	8888
5	1	jones	9999
6	2	jones	9999

访问规则和 alter table 命令

如果表所有者使用 **alter table** 命令，则在执行此命令期间，Adaptive Server 将禁用访问规则并在命令完成后启用它们。在执行 **alter table** 命令期间，禁用访问规则是为了避免过滤表数据。

访问规则和 bcp

使用 **bcp** 从表中向外复制数据时，Adaptive Server 将强制执行访问规则。由于对表具有选择权限的任何用户都可使用 **bcp**，因此 Adaptive Server 不能像对 **alter table** 那样禁用访问规则。

为了安全目的，批量向外复制期间，数据库所有者应以独占方式锁定表并禁用访问规则。禁用访问规则时，此锁定禁止其他用户访问。复制完数据之后，数据库所有者应绑定访问规则并将表解锁。

访问规则作为用户定义的 Java 函数

访问规则可以使用用户定义的 Java 函数。例如，可以使用 Java 函数编写复杂的规则，在规则中使用应用程序的配置文件、登录到应用程序的用户和当前分配给用户的应用程序的角色。

以下 Java 类使用 `GetSecVal` 方法来演示如何在访问规则中使用将 JDBC 用作用户定义函数的 Java 方法：

```
import java.sql.*;
import java.util.*;

public class sec_class {
    static String _url = "jdbc:sybase:asejdbc";
    public static int GetSecVal(int c1)
    {
        try
        {
            PreparedStatement pstmt;
            ResultSet rs = null;
            Connection con = null;
            int pno_val;

            pstmt = null;

            Class.forName("sybase.asejdbc.ASEDriver");
            con = DriverManager.getConnection(_url);

            if (con == null)
            {
                return (-1);
            }

            pstmt = con.prepareStatement("select classification
            from sec_tab where id = ?");

            if (pstmt == null)
            {
                return (-1);
            }

            pstmt.setInt(1, c1);

            rs = pstmt.executeQuery();

            rs.next();
```

```

pno_val = rs.getInt(1);

rs.close();

pstmt.close();

con.close();

return (pno_val);

}
catch (SQLException sqe)
{
return(sqe.getErrorCode());
}
catch (ClassNotFoundException e)
{

System.out.println("Unexpected exception : " +
e.toString());
System.out.println("\nThis error usually indicates that
" + "your Java CLASSPATH environment has not been set
properly.");
e.printStackTrace();

return (-1);
}
catch (Exception e)
{
System.out.println("Unexpected exception : " +
e.toString());
e.printStackTrace();
return (-1);
}
}
}

```

编译 Java 代码之后，您可从 isql 运行相同的程序，如下所示。

例如：

```

javac sec_class.java
jar cufo sec_class.jar sec_class.class
installjava -Usa -Password -
f/work/work/FGAC/sec_class.jar -
-D testdb

```

从 isql 中:

```
/*to create new user datatype class_level*/
sp_addtype class_level, int
/*to create the sample secure data table*/
create table sec_data (c1 varchar(30),
c2 varchar(30),
c3 varchar(30),
clevel class_level)
/*to create the classification table for each user*/
create table sec_tab (userid int, clevel class-level
int)

insert into sec_tab values (1,10)
insert into sec_tab values (2,9)
insert into sec_tab values (3,7)
insert into sec_tab values (4,7)
insert into sec_tab values (5,4)
insert into sec_tab values (6,4)
insert into sec_tab values (7,4)

declare @v1 int
select @v1 = 5
while @v1 > 0
begin
insert into sec_data values('8', 'aaaaaaaaaa',
'aaaaaaaaaa', 8)
insert into sec_data values('7', 'aaaaaaaaaa',
'aaaaaaaaaa', 7)
insert into sec_data values('5', 'aaaaaaaaaa',
'aaaaaaaaaa', 5)
insert into sec_data values('5', 'aaaaaaaaaa',
'aaaaaaaaaa', 5)
insert into sec_data values('2', 'aaaaaaaaaa',
'aaaaaaaaaa', 2)
insert into sec_data values('3', 'aaaaaaaaaa',
'aaaaaaaaaa', 3)
select @v1 = @v1 -1
end
go

create access rule clevel_rule
@clevel <= sec_class.GetSecVal(suser_id())
go

create default clevel_def as
sec_class.GetSecVal(suser_id())
```

```
go

sp_bindefault clevel_def, class_level
go

sp_bindrule clevel, class_level
go

grant all on sec_data to public
go
grant all on sec_tab to public
go
```

使用应用程序环境功能

数据库服务器上的应用程序必须限制对数据的访问。在编写应用程序代码时应仔细考虑用户的配置文件。例如，编写人力资源应用程序时需要了解应允许哪些用户更新工资信息。

实现这种编码方式的各种属性构成了应用程序环境。应用程序环境功能 (ACF) 由三个内置函数组成，通过允许访问规则与会话中分配给用户的固有值进行比较，它们可以提供安全的数据访问环境。

应用程序环境包括 `context_name`、`attribute_name` 和 `attribute_value`。用户为每个环境定义环境名、属性和值。可以使用 Sybase 提供的缺省只读应用程序环境 `SYS_SESSION` 来访问某些会话特定的信息。此应用程序环境在 [第 570 页的表 17-6](#) 中进行了介绍。也可以创建自己的应用程序环境，如 [第 565 页的“创建和使用应用程序环境”](#) 所述。

用户配置文件和应用程序配置文件一起提供了附加的和叠加的安全方案，应用程序配置文件在由系统管理员创建的表中定义。

ACF 允许用户定义、存储和检索：

- 用户配置文件（授权给用户的角色和用户所属的组）
- 当前使用的应用程序配置文件

每个会话可能会有任意数目的应用程序环境，任何环境都可以定义任意数目的属性 / 值对。ACF 环境行因不同的会话而异，不能在多个会话间保持；但是，与本地变量不同的是，它们可以用于不同的语句执行嵌套级别。ACF 提供了用于设置、获取、列出和删除这些环境行的内置函数。

设置使用应用程序环境函数的权限

可以在选择语句中执行应用程序环境函数。函数所有者是服务器的系统管理员。可以使用内置函数创建、设置、检索和删除应用程序环境。

函数中使用的数据是在包含所有表的所有登录的表中定义的，该表由系统管理员创建。有关此表的详细信息，请参见第 572 页的“使用登录触发器”。

- `set_appcontext()` 存储：


```
select set_appcontext ("titles", "rlac", "1")
```
- `get_appcontext()` 在会话中提供环境的两部分，并检索第三部分：

```
select get_appcontext ("titles", "rlac")
-----
1
```

有关这些函数、`list_appcontext` 和 `rm_appcontext` 的详细信息，请参见第 565 页的“创建和使用应用程序环境”。

授予和撤消

授予和撤消给定数据库中的用户、角色和组访问该数据库中对象的特权。但也有例外，如 `create database`、`set session authorization` 和 `connect`。授予了这些特权的用户应该是 `master` 数据库中的有效用户。若要使用其它特权，用户必须是对象所在的数据库中的有效用户。

函数的使用意味着，除非有特殊安排，否则任何登录用户都可以重置会话的配置文件。虽然 `Adaptive Server` 会审计内置函数，但在发现问题前还是会受到安全威胁。若要限制对这些内置函数的访问，请使用 `grant` 和 `revoke` 特权。只有具有 `sa_role` 的用户才能授予或撤消对这些内置函数的特权。作为这些函数执行的在服务器上强制实施的数据访问控制检查的一部分，将只检查 `select` 权限。

有效用户

函数没有对象 ID，也没有主数据库。因此，每个数据库所有者必须向适当的用户授予这些函数的选择权限。`Adaptive Server` 会查找用户的缺省数据库并检查对此数据库的权限。使用此方法，只有用户的缺省数据库的所有者才需要授予选择特权。如果要限制其它数据库，则相应数据库的所有者必须显式地撤消用户在这些数据库中的权限。

当授予和撤消对应用程序环境内置函数的特权时，只有这些函数会对用户执行数据访问控制检查。授予或撤消其它函数的特权在 `Adaptive Server` 中没有任何影响。

授予 `public` 的特权只影响在系统管理员创建的表中命名的用户。有关该表的信息，请参见第 572 页的“使用登录触发器”。只有在 `sa_role` 将 `Guest` 用户添加到表中明确授予某些特权后，`Guest` 用户才具有相应特权。

系统管理员可以执行以下命令，来授予或撤消对特定应用程序环境函数的 `select` 特权。

```
grant select on set_appcontext to user_role
```

```
grant select on set_appcontext to joe_user
```

```
revoke select on set_appcontext from joe_user
```

创建和使用应用程序环境

以下函数可用于创建和维护应用程序环境。有关详细信息，请参见《参考手册：构件块》。

- `set_appcontext`
- `get_appcontext`
- `list_appcontext`
- `rm_appcontext`

`set_appcontext`

为指定的用户会话设置由应用程序的属性定义的应用程序环境名、属性名和属性值。

```
set_appcontext ('context_name', 'attribute_name', 'attribute_value')
```

- *context_name* — 指定应用程序环境名的行，作为 `char(30)` 数据类型保存。
- *attribute_name* — 指定应用程序环境属性名的行，作为 `char(30)` 数据类型保存。
- *attribute_value* — 指定应用程序属性值的行，作为 `char(255)` 数据类型保存。

示例

此示例创建名为 CONTEXT1 的应用程序环境，其属性 ATTR1 的值为 VALUE1:

```
select set_appcontext("CONTEXT1", "ATTR1", "VALUE1")
-----
0
```

以下示例尝试替换现有的应用程序环境。尝试失败，返回 -1:

```
select set_appcontext("CONTEXT1", "ATTR1", "VALUE1")
-----
-1
```

以下示例显示 `set_appcontext` 如何在值中包括数据类型转换:

```
declare @val numeric
select @val = 20
select set_appcontext ("CONTEXT1", "ATTR2",
convert(char(20), @val))
-----
0
```

以下示例显示没有适当权限的用户试图设置应用程序环境的结果。尝试失败，返回 -1:

```
select set_appcontext("CONTEXT1", "ATTR2", "VALUE1")
-----
-1
```

用法

- `set_appcontext` 返回 0 表示成功，返回 -1 表示失败。
- 如果设置的值在当前会话中已存在，则 `set_appcontext` 返回 -1。
- `set_appcontext` 不能替换现有应用程序环境的值。若要为一个环境指定新值，应先删除该环境，然后使用新值重新创建一个环境。
- `set_appcontext` 将属性另存为 `char` 数据类型。如果您创建的访问规则必须将属性值与另一个数据类型进行比较，则该规则应该将 `char` 数据转换为适当的数据类型。
- 此函数中的所有参数都是必需的。

get_appcontext

返回指定环境中的属性值。

```
get_appcontext ("context_name", "attribute_name")
```

- *context_name* — 指定应用程序环境名的行，作为 char(30) 数据类型保存。
- *attribute_name* — 指定应用程序环境属性名的行，作为 char(30) 数据类型保存。

示例

此示例显示为 ATTR1 返回的 VALUE1：

```
select get_appcontext("CONTEXT1", "ATTR1")
-----
VALUE1
```

ATTR1 不存在于 CONTEXT2 中：

```
select get_appcontext("CONTEXT2", "ATTR1")
-----
NULL
```

以下示例显示没有适当权限的用户试图获取应用程序环境的结果：

```
select get_appcontext("CONTEXT1", "ATTR2")
select permission denied on built-in get_appcontext,
database dbid
-----
-1
```

用法

- `get_appcontext` 返回 0 表示成功，返回 -1 表示失败。
- 如果应用程序环境中不存在所需的属性，则 `get_appcontext` 返回“null”。
- `get_appcontext` 将属性保存为 char 数据类型。如果您创建的访问规则需将属性值与其它数据类型进行比较，则该规则应该将 char 数据转换为适当的数据类型。
- 此函数中的所有参数都是必需的。

list_appcontext

列出当前会话中所有环境的全部属性。

```
list_appcontext ("context_name")
```

- *context_name* — 命名会话中的所有应用程序环境属性。
list_appcontext 的数据类型为 char(30)。

示例

若要使用 list_appcontext，用户必须具有适当的权限。有关详细信息，请参见第 564 页的“[设置使用应用程序环境函数的权限](#)”。

本示例显示具有适当权限的用户列出应用程序环境的结果：

```
select list_appcontext ("*", "*")
Context Name: (CONTEXT1)
Attribute Name: (ATTR1) Value: (VALUE2)
Context Name: (CONTEXT2)
Attribute Name: (ATTR1) Value: (VALUE!)
-----
0
```

以下示例显示没有适当权限的用户试图列出应用程序环境的结果。尝试失败，返回 -1。

```
select list_appcontext()
Select permission denied on built-in
list_appcontext, database DBID
-----
-1
```

用法

- list_appcontext 返回 0 表示成功，返回 -1 表示失败。
- 由于内置函数不会返回多个结果集，因此客户端应用程序将收到 list_appcontext 以消息形式返回的结果。

rm_appcontext

删除特定应用程序环境或所有应用程序环境。

```
rm_appcontext ("context_name", "attribute_name")
```

- *context_name* — 指定应用程序环境名的行，作为 char(30) 数据类型保存。
- *attribute_name* — 指定应用程序环境属性名的行，作为 char(30) 数据类型保存。

示例

以下三个示例显示如何通过指定某些或全部属性来删除应用程序环境。使用星号 ("*") 可删除指定环境中的所有属性。

```
select rm_appcontext("CONTEXT1", "*")
-----
0
```

使用星号 ("*") 可删除所有环境和属性。

```
select rm_appcontext("?", "*")
-----
0
```

以下示例显示用户试图删除不存在的环境。尝试失败，返回 -1。

```
select rm_appcontext("NON_EXISTING_CTX", "ATTR2")
-----
-1
```

以下示例显示没有适当权限的用户试图删除应用程序环境的结果。

```
select rm_appcontext("CONTEXT1", "ATTR2")
-----
-1
```

用法

- `rm_appcontext` 返回 0 表示成功，返回 -1 表示失败。
- 此函数中的所有参数都是必需的。

SYS_SESSION 系统应用程序环境

`SYS_SESSION` 环境显示缺省的预定义应用程序环境，该环境提供特定于会话的属性 / 值对。使用该环境的语法是：

```
select list_appcontext ("SYS_SESSION", "*")
```

然后：

```
select get_appcontext ("SYS_SESSION", "<attribute>")
```

表 17-6: SYS_SESSION 属性和值

属性	值
username	登录名
hostname	客户端与其连接的主机的名称
applname	客户端设置的应用程序的名称
suserid	当前数据库中用户的用户 ID
groupid	当前数据库中用户的组 ID
dbid	用户的当前数据库的 ID
dbname	当前数据库
spid	服务器进程 ID
proxy_suserid	代理的服务器用户 ID
client_name	中间层应用程序使用 set client_name 命令设置的客户端名称
client_applname	中间层应用程序使用 set client_applname 命令设置的客户端应用程序名称
client_hostname	中间层应用程序使用 set client_hostname 命令设置的客户端主机名称
language	缺省情况下或使用 set language 命令设置后，客户端正在使用的当前语言 (@@language)
character_set	客户端正在使用的字符集 (@@client_csname)
dateformat	客户端需要的日期格式，使用 set dateformat 命令设置
is_showplan_on	如果 set showplan 处于启用状态，则返回 YES，如果处于禁用状态则返回 NO
is_noexec_on	如果 no exec 处于启用状态，则返回 YES，如果处于禁用状态则返回 NO

使用访问规则和 ACF 解决问题

本节将为如下问题提供一个解决方案：有 5 个用户处于不同的安全级别，每个用户应该只能看到相关值小于或等于该用户的安全级别的行。此解决方案使用访问规则，结合应用程序环境功能，只显示其中的一个用户 Dave 可看到的行。

有以下 5 个登录名：

- Anne 的安全级别为 1。
- Bob 的安全级别为 1。
- Cassie 的安全级别为 2。
- Dave 的安全级别为 2。
- Ellie 的安全级别为 4。

用户应该只能看到 **rlac** 中的值小于或等于各自的安全级别的行。若要实现此目的，可创建一个访问规则并应用 **ACF**。

rlac 列的类型为 **integer**，**appcontext** 参数的类型为 **char**。

```
create access rule rlac_rule as
    @value <= convert(int, get_appcontext("titles",
        "rlac"))
```

```
sp_bindrule rlac_rule, "titles.rlac"
```

```
/* log in as Dave and apply ACF value of 2*/
```

```
select set_appcontext("titles", "rlac", "2")
```

```
/*this value persists throughout the session*/
```

```
/*select all rows*/
```

```
select title_id, rlac from titles
```

```
-----
```

title_id	rlac
PC8888	1
BU1032	2
PS7777	1
PS3333	1
BU1111	2
PC1035	1
BU2075	2
PS2091	1
PS2106	1
BU7832	2
PS1372	1

```
(11 rows affected)
```

使用登录触发器

注释 本节中的一些信息摘自文章“Login Triggers in ASE 12.5”（ASE 12.5 中的登录触发器）。版权所有 1998–2002, Rob Verschoor/ Sypron B.V., 网址: <http://www.sypron.nl/logtrig.html>。

登录触发器在每次用户登录时执行指定的存储过程。登录触发器是普通的存储过程，只不过它在后台执行。它是成功登录过程的最后一个步骤，并为登录的用户设置应用程序环境。

只有系统安全员才能向服务器中的用户注册登录触发器。

若要提供安全的环境，系统管理员必须：

- 1 撤消对 `set_appcontext` 函数的 `select` 特权。登录触发器的所有者必须明确地具有使用 `set_appcontext` 的权限，即使该所有者具有 `sa_role` 也需要如此。
- 2 利用存储过程为每个用户配置登录触发器，然后向用户注册登录触发器。
- 3 向用户执行的登录触发器提供执行特权。

创建登录触发器

以存储过程的形式创建登录触发器。不要使用 `create trigger` 命令。下面的示例在 `pubs2` 数据库中创建一个登录触发器存储过程：

```
create loginproc as
    declare @appname varchar(20)
    declare @attr      varchar(20)
    declare @value      varchar(20)
    declare @retvalue   int
declare apctx cursor for
    select appname, attr, value from
    pubs2.dbo.lookup where login = suser_name()
open apctx
fetch apctx into @appname, @attr, @value

While (@@sqlstatus = 0)
    begin
        select f@retval =
            set_appcontext (rtrim (@appname),
                           rtrim(@attr),  rtrim(@value))
        fetch apctx into @appname, @attr, @value
    end
```



```

go

grant execute on loginproc to public
go

```

若要将特定用户与登录触发器关联，请在该用户的缺省数据库中运行 `sp_modifylogin`。

配置登录触发器

您必须启用 `sso_role` 才能设置、更改或删除登录触发器。登录触发器的对象 ID 存储在 `syslogins.procid` 列中。缺省情况下，登录触发器不存在。必须使用 `sp_modifylogin` 对它们进行注册。语法为：

```
sp_modifylogin <login_name>, "login script", <sproc_name >
```

- *login_name* — 用户的登录名。
- "login script" — 按显示的内容键入；"login script" 通知 `sp_modifylogin` 下一个参数 `"sproc_name"` 是登录触发器。
- *sproc_name* — 作为此用户的登录触发器进行配置的存储过程的名称。

在用户的缺省数据库中运行此过程。作为登录触发器注册的存储过程在用户的缺省数据库中必须可用，原因是 Adaptive Server 将在用户的缺省数据库中搜索 `sysobjects` 表，以查找登录触发器对象。

配置登录触发器

下面的示例将存储过程 `my_proc`（它必须存在于您要配置的数据库中）配置为 Adaptive Server 登录 `my_login` 的登录触发器：

```
sp_modifylogin my_login, "login script", my_proc
```

同样，必须在用户的缺省数据库中执行该命令。Adaptive Server 将检查登录名是否对存储过程具有 `execute` 权限，但只有在用户实际登录并执行登录触发器时才会发生。

删除和更改登录触发器

一旦将存储过程配置为登录触发器，就不能删除该存储过程了。必须先取消对它的配置，要么连登录触发器一起删除，要么将登录触发器更改为其它存储过程。若要删除登录触发器，请输入：

```
sp_modifylogin my_login, "login script", NULL
```

若要将登录触发器更改为其它存储过程，请输入：

```
sp_modifylogin my_login, "login script", diff_proc
```

显示登录触发器

若要显示当前登录触发器，请使用 `sp_displaylogin`：

```
sp_displaylogin my_login
go
(....)
Default Database:my_db
Default Language:
Auto Login Script: my_proc
....
```

执行登录触发器

登录触发器不同于普通的存储过程，原因在于它们一旦注册之后，便会在后台执行，而不需要活动的用户连接。在配置了登录触发器之后，只要用户一登录，**Adaptive Server** 就会在后台自动执行该登录触发器，并且执行登录触发器的过程会发生在服务器执行来自客户端应用程序的任何命令之前。

如果一个登录进行了多个并发连接，登录触发器会在每个会话中独立执行。同样，多个登录可以将同一个存储过程配置成登录触发器。

后台执行意味着您不能在配置为登录触发器的存储过程中使用存储过程的某些标准功能。例如，不能向该过程传送或从该过程接收任何没有缺省值的参数，该过程也不会传递回任何结果值。

这种特殊的执行模式会影响由登录触发器存储过程调用的任何存储过程，以及登录触发器存储过程本身生成的任何输出。

您还可以将登录触发器存储过程作为正常的存储过程执行，例如在 `isql` 命令中。该过程将正常地执行和发挥作用，像通常那样显示所有输出和错误消息。

了解登录触发器输出

将存储过程作为后台任务执行的主要影响是登录触发器的输出不会写入到客户端应用程序中，而是以一些（但不是全部）错误消息的形式写入 **Adaptive Server** 错误日志文件。

在错误日志中，来自 `print` 或 `raiserror` 消息的输出的前缀为 **background task message** 或 **background task error**。例如，在 **Adaptive Server** 错误日志中，登录触发器中的语句 `print "Hello!"` 和 `raiserror 123456` 显示为：

```
(....) background task message: Hello!
(....) background task error 123456: This is test
message 123456
```

但是，并非所有输出都会写入 Adaptive Server 错误日志：

- **select** 语句（通常被发送到客户端连接）的结果集不会出现在任何位置，甚至也不会出现在 Adaptive Server 错误日志中。此信息无处可寻。
- 通常执行以下语句：**insert...select** 和 **select...into** 语句，以及其它一些通常不将结果集发送到客户端应用程序的 DML 语句和存储过程中通常允许使用的 DDL 语句。

对其它应用程序使用登录触发器

登录触发器是作为 Adaptive Server 中行级访问控制功能的一部分设计的。在此环境中，一旦某个会话登录到 Adaptive Server 后，您就可以结合使用登录触发器与访问规则和应用程序环境的功能，设置行级访问控制。不过，还可以将登录触发器用于其它目的。

限制并发连接的数目

以下示例限制特定登录可与 Adaptive Server 建立的并发连接的数目。在需要被限制访问的用户的缺省数据库中执行示例中步骤 1 和 2 中描述的每个命令：

1 以系统管理员身份创建 **limit_user_sessions** 存储过程：

```
create procedure limit_user_sessions
as
declare @cnt int,
        @limit int,
        @loginname varchar(32)

select @limit = 2 -- max nr. of concurrent logins

/* determine current #sessions */
select @cnt = count(*)
from master.dbo.sysprocesses
where suid = suser_id()

/* check the limit */
if @cnt > @limit
begin
    select @loginname = suser_name()
    print "Aborting login [%1!]: exceeds session
          limit [%2!]",
          @loginname, @limit
    /* abort this session */
    select syb_quit()
end
```

```
go
```

```
grant exec on limit_user_sessions to public
go
```

- 2 以系统安全员身份将此存储过程配置为用户 “bob” 的登录触发器:

```
sp_modifylogin "bob", "login script",
"limit_user_sessions"
go
```

- 3 现在, 当用户 “bob” 创建 Adaptive Server 的第三个会话时, 登录触发器将调用 `syb_quit()` 函数终止该会话:

```
% isql -SASE125 -Ubob -Pbobpassword
1> select 1
2> go

CT-LIBRARY error:
ct_results(): network packet layer:internal net
library error: Net-Library operation terminated due
to disconnect
```

- 4 此消息将显示在 Adaptive Server 错误日志文件中:

```
(...) background task message: Aborting login [
my_login]: exceeds session limit [2]
```

强制执行基于时间的限制

此示例描述系统管理员如何通过创建登录触发器来对用户会话强制执行基于时间的限制。在需要被限制访问的用户的缺省数据库中执行步骤 1–4 中描述每个命令:

- 1 以系统管理员身份创建此表:

```
create table access_times (
suid int not null,
dayofweek tinyint,
shiftstart time,
shiftend time)
```

- 2 以系统管理员身份将以下行插入表 `access_times`。这些行指示允许用户 “bob” 在星期一上午 9 点到下午 5 点登录到 Adaptive Server, 并允许用户 “mark” 在星期二上午 9 点到下午 5 点登录到 Adaptive Server

```
insert into access_times
select suser_id('bob'), 1, '9:00', '17:00'
go
insert into access_times
select suser_id('mark'), 2, '9:00', '17:00'
go
```

- 3 以系统管理员身份创建 `limit_access_time` 存储过程，该存储过程引用 `access_time` 表来确定是否应授予登录访问权限：

```
create procedure limit_access_time as
declare @curdate date,
        @curdow tinyint,
        @curtime time,
        @cnt int,
        @loginname varchar(32)

-- setup variables for current day-of-week, time
select @curdate = current_date()
select @curdow = datepart(cdw,@curdate)
select @curtime = current_time()
select @cnt = 0

-- determine if current user is allowed access
select @cnt = count(*)
from access_times
where suid = suser_id()
and dayofweek = @curdow
and @curtime between shiftstart and shiftend

if @cnt = 0
begin
    select @loginname = suser_name()
    print "Aborting login [%!]: login attempt past
        normal working hours", @loginname

    -- abort this session
    return -4
end
go

grant exec on limit_access_time to public
go
```

- 4 以系统安全员身份将 `limit_access_time` 存储过程配置为用户 “bob” 和 “mark” 的登录触发器：

```
sp_modifylogin "bob", "login script",
"limit_access_time"
go
sp_modifylogin "mark", "login script",
"limit_access_time"
go
```

- 5 在星期一，用户 “bob” 可以成功创建一个会话：

```
isql -Ubob -Ppassword
1> select 1
2> go
-----
              1
(1 row affected)
```

但是，用户 “mark” 无权访问 Adaptive Server：

```
isql -Umark -Ppassword
1> select 1
2> go
CT-LIBRARY error:
ct_results(): network packet layer:internal net
library error: Net-Library operation terminated
due to disconnect
```

- 6 将在错误日志中记录以下消息：

```
(...) server back-ground task message: Aborting
login [mark]: login attempt past normal working
hours
```

上述示例显示了如何限制特定登录名的并发连接的数目，以及如何限制该登录名在特定的时间进行访问，但它有一个缺点：客户端应用程序无法方便地检测到会话被终止的原因。若要向用户显示一条消息（例如“现在用户太多 — 请稍后重试”），请使用其它方法。

您可以在存储过程中故意引发一个错误以中止登录触发器存储过程，而不是调用内置函数 `syb_quit()`，该函数将使服务器仅仅是终止当前会话。

例如，用零作除数可以中止登录触发器存储过程、终止会话并导致出现消息。

登录触发器限制

以下操作受到限制。

- 不能使用登录触发器设置特定于会话的选项，例如 `set nocount on`、`set rowcount on` 等。在任何存储过程中设置会话选项只在该存储过程中有效。
- 不能创建 `#temp` 表在会话中稍后使用。过程一旦完成，就将自动删除 `#temp` 表并恢复初始会话设置，就像在任何其它存储过程中一样。
- 不对 `sa` 登录名使用登录触发器；失败的登录触发器会将您锁定在 Adaptive Server 之外。
- 不要对任何执行时间超过几秒的操作或执行过程中可能存在问题的操作使用登录触发器。

发布和信息

- 如果不能访问 Adaptive Server 错误日志，请不要使用登录触发器。始终检查 Adaptive Server 错误日志中是否有错误消息。
- 对于 Adaptive Server 15.0.2 版及更高版本，当服务器启动时，在登录触发器中设置或取消设置的任何可导出选项将在登录过程中生效。

若要禁用此行为，请在登录触发器内执行 `set export_options off`。

Adaptive Server 15.0.1、12.5.4 版及早期版本要求您使用跟踪标志 4073 启动 Adaptive Server 来启用登录触发器选项。

- 客户端应用程序（如 `isql`）不知道登录触发器的存在或执行；它会在成功登录后立即显示命令提示符，尽管 Adaptive Server 在登录触发器成功执行前不会执行任何命令。即使登录触发器终止了用户连接，也会显示该 `isql` 提示符。
- 登录到 Adaptive Server 的用户必须具有 `execute` 权限才能使用登录触发器存储过程。如果未授予 `execute` 权限，则 Adaptive Server 错误日志中会显示一条错误消息并且用户连接将立即关闭（虽然 `isql` 仍显示命令提示符）。

Adaptive Server 错误日志显示类似于以下内容的消息：

```
EXECUTE permission denied on object my_proc,
database my_db, owner dbo
```

- 登录触发器存储过程不可以包含没有指定缺省值的参数。如果存储过程中出现不带缺省值的参数，则登录触发器将失败，并且 Adaptive Server 错误日志中出现类似于以下内容的错误：

```
Procedure my_proc expects parameter @param1, which
was not supplied...
```

禁用对登录触发器的执行特权

数据库所有者或管理员可以禁用对登录触发器的 `execute` 特权，或者对登录触发器进行编码，以便只允许特定时间内的访问。例如，您可能要禁止常规用户在数据库所有者或管理员更新表时使用数据库。

注释 如果登录触发器返回负数，则登录失败。

从登录触发器导出 **set** 选项

Adaptive Server 允许登录触发器内的 **set** 命令选项在整个用户会话期间保持有效。

将自动导出以下 **set** 选项：

- showplan
- arithabort [overflow | numeric_truncation]
- arithignore [overflow]
- colnames
- format
- statistics io
- procid
- rowcount
- altnames
- nocount
- quoted_identifier
- forceplan
- fmtonly
- close on endtran
- fipsflagger
- self_recursion
- ansinull
- dup_in_subquery
- or_strategy
- flushmessage
- ansi_permissions
- string_truncation
- prefetch
- triggers
- replication

- `sort_resources`
- `transactional_rpc`
- `cis_rpc_handling`
- `strict_dtm_enforcement`
- `raw_object_serialization`
- `textptr_parameters`
- `remote_indexes`
- `explicit_transaction_required`
- `statement_cache`
- `command_status_reporting`
- `proc_return_status`
- `proc_output_params`

设置全局登录触发器

使用 `sp_logintrigger` 设置在每个用户登录时执行的全局登录触发器。若要采取用户特定的操作，请使用 `sp_modifylogin` 或 `sp_addlogin` 设置用户特定的登录触发器。

注释 可通过设置跟踪标志 `-T4073` 来激活此选项。

审计

本章介绍如何为安装设置审计。

主题	页码
Adaptive Server 中的审计简介	583
安装和设置审计	588
设置全局审计选项	603
查询审计追踪	612
了解审计表	613

Adaptive Server 中的审计简介

一个安全系统的基本要素是责任。确保责任的一种方法是审计系统中的事件。 Adaptive Server 中发生的许多事件都可以记录。

审计是数据库管理系统中安全性的重要组成部分。可使用审计追踪来检测系统渗透和资源误用情况。通过检查审计追踪，系统安全员可以对数据库中对象的访问模式进行检测，并可监视特定用户的活动。可以跟踪特定用户的审计记录，这对于不正确使用系统的用户可起到威慑作用。

每个审计记录都可以记录事件的性质、日期和时间、对它负责的用户以及事件是否成功。可以审计的事件包括登录和注销、服务器的启动、数据访问命令的使用、访问特定对象的尝试以及特定用户的操作。**审计追踪**（即审计记录的日志）允许系统安全员重建系统上发生的事件并评估其影响。

只有系统安全员才能启动和停止审计、设置审计选项以及处理审计数据。作为系统安全员，您可以为诸如以下事件建立审计：

- 全服务器范围内的与安全性相关的事件
- 创建、删除和修改数据库对象
- 特定用户执行的所有操作或具有特定活动角色的用户执行的所有操作

- 授予或撤消数据库访问权限
- 导入或导出数据
- 登录和注销

将 Adaptive Server 与操作系统的审计记录相关联

链接 Adaptive Server 审计记录和操作系统记录的最简便方法是使 Adaptive Server 的登录名与操作系统的登录名相同。

或者，系统安全员可将用户的操作系统登录名映射为其 Adaptive Server 登录名。然而，这种方法要求进行即时维护，因为新用户的登录名必须手动记录。

审计系统

审计系统包括：

- **sybsecurity** 数据库，包括全局审计选项和审计追踪
- 内存中的审计队列；在审计记录被写入到审计追踪中之前，将其发送到队列中
- 用于管理审计的配置参数
- 用于管理审计的系统过程

sybsecurity 数据库

sybsecurity 数据库是在审计安装过程中创建的。除 model 数据库中的所有系统表外，它还包括用来跟踪整个服务器范围内审计选项的 sysauditoptions 系统表和用于审计追踪的系统表。

sysauditoptions 包含全局审计选项的当前设置，例如是否为磁盘命令、远程过程调用、用户定义的即席审计记录或所有安全性相关事件启用了审计。这些选项会影响整个 Adaptive Server。

审计追踪

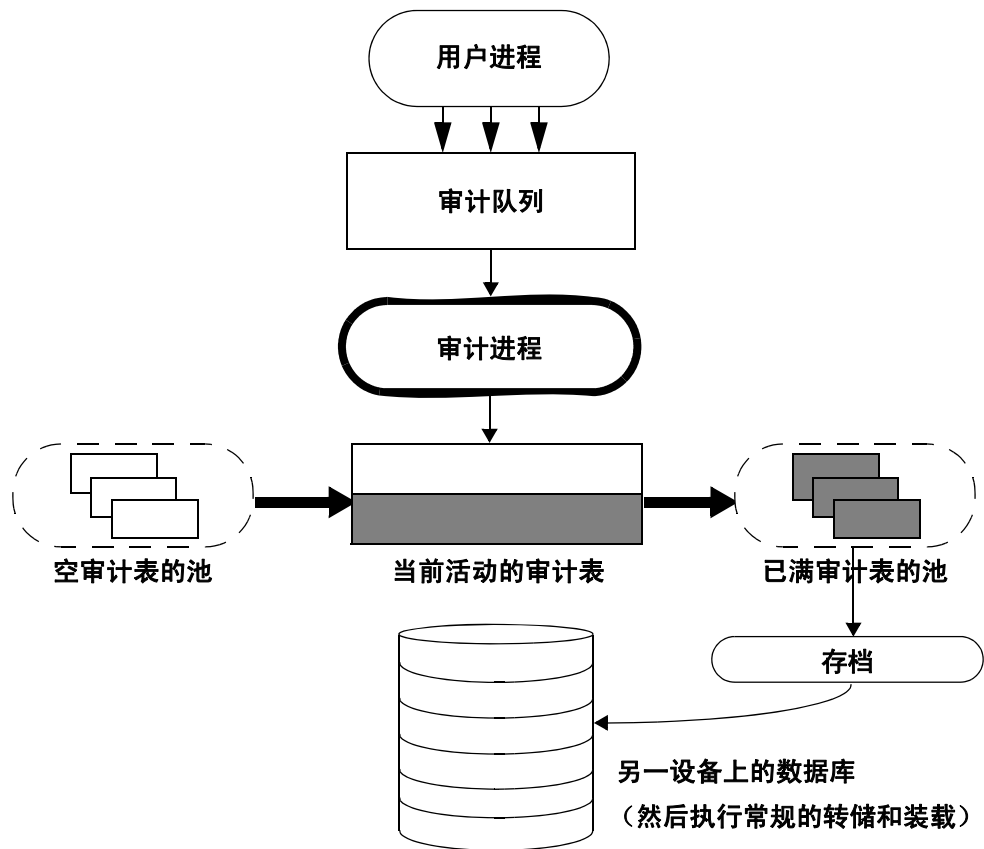
Adaptive Server 在名为 sysaudits_01 到 sysaudits_08 的系统表中存储审计追踪。安装审计时，需要确定要安装的审计表的数量。例如，如果选择使用两个审计表，其名称分别为 sysaudits_01 和 sysaudits_02。在任何给定时间，只有一个审计表是当前审计表。Adaptive Server 将所有审计数据都写入当前审计表中。系统安全员可以使用 sp_configure 来设置（或更改）哪个审计表为当前表。

Sybase 建议使用两个或两个以上的审计表，且每个表都位于单独的审计设备上。这样就可以建立一个稳定运行的审计过程来存档和处理审计表，而不会丢失审计记录并且不需要手动干预。

警告！ Sybase 强烈反对在生产系统中仅使用一个审计表。如果仅使用一个审计表，有可能丢失审计记录。如果由于系统资源有限而必须仅使用一个审计表，则请参见第 599 页的“单表审计”以获得有关说明。

图 18-1 显示了审计进程如何处理多个审计表。

图 18-1: 使用多个审计表进行审计



审计系统将来自内存中的审计队列的审计记录写入到当前审计表中。当前审计表将近充满时，一个阈值过程可自动将该表存档到另一数据库中。使用 `dump` 和 `load` 命令，可以对存档数据库进行备份和恢复。使用存档数据库访问权限以只读方式访问备份中的已存档审计表。请参见《系统管理指南：卷 2》中的第 14 章“存档数据库访问”。有关管理审计追踪的详细信息，请参见第 592 页的“设置审计追踪管理”。

审计队列

当被审计的事件发生时，首先向内存中的审计队列增加一条审计记录。该记录一直保留在内存中，直到被审计进程写入审计追踪。用户可使用 `sp_configure` 的 `audit queue size` 参数配置审计队列的大小。

配置审计队列的大小之前，应综合考虑在系统崩溃时丢失队列中的记录的风险以及队列充满时性能降低的风险。只要审计记录在队列中，如果系统崩溃，记录就有可能丢失。然而，如果队列频繁充满，则整个系统的性能都会受影响。如果在用户进程尝试生成一条审计记录时审计队列已满，则该进程将休眠，直至队列中有可用空间为止。

注释 由于不会将审计记录直接写入审计追踪，因此不能期望审计记录会立即被存储到当前审计表中。

审计配置参数

可以使用下面这些配置参数来管理审计进程：

- `auditing` 启用或禁用对整个 Adaptive Server 的审计。此参数在执行 `sp_configure` 后立即生效。只有在启用此参数后，审计才会发生。
- `audit queue size` 确定审计队列的大小。由于此参数会影响内存分配，所以需重新启动 Adaptive Server 后才会生效。
- `suspend audit when device full` 控制在审计设备充满时审计进程的行为。此参数在执行 `sp_configure` 后立即生效。
- `current audit table` 设置当前审计表。此参数在执行 `sp_configure` 后立即生效。

用于审计的系统过程

可以使用下面这些系统过程来管理审计进程：

- `sp_audit` 启用和禁用审计选项。这是建立待审计事件所需的唯一系统过程。
- `sp_displayaudit` 显示活动的审计选项。
- `sp_addauditrecord` 将用户定义的审计记录（注释）添加到审计追踪中。只有在系统安全员使用 `sp_audit` 启用即席审计后，用户才能添加这些记录。

安装和设置审计

表 18-1 提供了设置审计的一般过程。

表 18-1: 审计的常规步骤

操作	说明	请参见
1. 安装审计。	设置审计表的数量，并为审计追踪和 sybsecurity 数据库中的 syslogs 事务日志指派设备。	第 588 页的“安装审计系统”以及 Adaptive Server 安装和配置文档
2. 设置审计追踪管理。	编写和建立阈值过程，当前审计表将近充满时，由该过程接管。此过程将自动切换到新的审计表，并存档当前表的内容。 此外，该步骤还包括设置 audit queue size 和 suspend audit when device full 配置参数。	第 592 页的“设置审计追踪管理” 有关单个表审计的说明，请参见第 599 页的“单表审计”
3. 设置 sybsecurity 数据库中的事务日志管理。	确定如何处理 sybsecurity 数据库中的 syslogs 事务日志；如何设置 trunc log on chkpt 数据库选项；以及在 trunc log on chkpt 设置为禁用的情况下如何为 syslogs 建立一个最后机会阈值过程。	第 598 页的“设置事务日志管理”
4. 设置审计选项。	使用 sp_audit 建立要审计的事件。	第 603 页的“设置全局审计选项”
5. 启用审计。	使用 sp_configure 启用 auditing 配置参数。Adaptive Server 开始将审计记录写入当前审计表。	第 599 页的“启用和禁用审计”
6. 重新启动审计。	使用 sp_audit restart 重新启动审计（如果审计失败）。	第 602 页的“重新启动审计”

安装审计系统

通常使用 Sybase 安装程序 auditinit 来安装审计系统。或者，也可在不使用 auditinit 的情况下安装审计。有关详细信息，请参见第 589 页的“使用 installsecurity 安装审计”。所用平台的 Adaptive Server 安装和配置文档中论述了安装和 auditinit。

安装审计时，可以确定要用于审计追踪的系统表数量，用于每个审计系统表的设备以及用于 syslogs 事务日志的设备。

用于审计追踪的表和设备

最多可以指定八个系统表（sysaudits_01 到 sysaudits_08）。应计划至少使用两个表用于审计追踪。将每个表分别放在自己的设备上，不要放在主设备上。这样就可以使用一个阈值过程，在当前审计表快填满前自动存档当前审计表，然后为随后的审计记录切换到新的空审计表。

用于 *syslogs* 事务日志表的设备

安装审计时，必须为由 **syslogs** 系统表所组成的事务日志指定一个单独的设备。**syslogs** 表在每个数据库中都有，包含了数据库中执行的事务的日志。

使用 *installsecurity* 安装审计

\$SYBASE/ASE-15_0/scripts 目录包含一个用于安装审计的脚本 *installsecurity*。

注释 此示例假定服务器使用 2K 的逻辑页大小。

使用 *installsecurity* 安装审计：

- 1 使用 **disk init** 和 **create database** 命令创建审计设备和审计数据库。
例如：

```
disk init name = "auditdev",
    physname = "/dev/dsk/c2d0s4",
    size = "10M"
disk init name = "auditlogdev",
    physname = "/dev/dsk/c2d0s5",
    size = "2M"
create database sybsecurity on auditdev
log on auditlogdev
```

- 2 使用 **isql** 执行 *installsecurity* 脚本：

```
cd $SYBASE/ASE-12_5/scripts
setenv DSQUERY server_name
isql -Usa -Ppassword -Sserver_name < installsecurity
```

- 3 关闭并重新启动 Adaptive Server。

当您完成这些步骤后，**sybsecurity** 数据库已在自己的段中创建了一个审计表 (**sysaudits_01**)。这时可以启用审计，但应使用 **sp_addauditable** 添加更多的审计表。有关 **disk init**、**create database** 和 **sp_addauditable** 的信息，请参见《参考手册：过程》。

将审计数据库移动到多个设备

将 **sybsecurity** 数据库放在其自己的设备上，与 **master** 数据库分开。如果有多个审计表，将每个表放在各自的设备上。把每个表放在指向独立设备的独立的段上也会有所帮助。如果当前您将 **sybsecurity** 与 **master** 保存在同一设备上，或想将 **sybsecurity** 移动到另一设备上，则使用下面描述的过程之一来完成。移动数据库时，可以指定是否保存现有的全局审计设置。

移动 **sybsecurity** 而不保存全局审计设置

注释 这些步骤包括删除 **sybsecurity** 数据库，该步骤将销毁所有审计记录以及 **sybsecurity** 中以前记录的全局审计设置。在删除 **sybsecurity** 数据库之前，请确保使用备份或按照第 593 页的“存档审计表”中的说明将现有记录存档，以避免丢失保留在 **sybsecurity** 表中的任何历史数据。

移动 **sybsecurity** 数据库而不保存全局审计设置：

- 1 执行以下命令，从 **syslogins** 系统表中删除任何与登录相关的信息：

```
sp_audit "all","all","all","off"
```
- 2 删除 **sybsecurity** 数据库。
- 3 使用以下任意一项中描述的安装过程重新安装 **sybsecurity**：
 - 针对所用平台的配置文档，或
 - 第 589 页的“使用 **installsecurity** 安装审计”。
- 4 在安装过程中，将 **sybsecurity** 数据库放在独立于主设备的一个或多个设备上。

移动 **sybsecurity**，然后保存全局审计设置

❖ 移动 **sybsecurity** 数据库并保存全局审计设置

- 1 转储 **sybsecurity** 数据库：

```
dump database sybsecurity to "/remote/sec_file"
```
- 2 删除 **sybsecurity** 数据库：

```
drop database sybsecurity
```
- 3 初始化要在其中放置 **sybsecurity** 数据库的第一个设备：

```
disk init name = "auditdev",  
physname = "/dev/dsk/c2d0s4",  
size = "10M"
```

- 4 初始化要在其中放置安全性日志的设备:

```
disk init name = "auditlogdev",
physname = "/dev/dsk/c2d0s5",
size = "2M"
```

- 5 创建新的 **sybsecurity** 数据库:

```
create database sybsecurity on auditdev
log on auditlogdev
```

- 6 将旧 **sybsecurity** 数据库的内容装载到新数据库中。将保留全局审计设置:

```
load database sybsecurity from "/remote/sec_file"
```

- 7 运行 **online database**, 该命令将在必要时升级 **sysaudits** 和 **sysauditoptions**:

```
online database sybsecurity
```

- 8 使用所用平台的配置文档装载审计系统过程。

❖ 在 **sybsecurity** 中创建多个 **sysaudits** 表

- 1 初始化要在其中放置其它表的设备:

```
disk init name = "auditdev2",
physname = "/dev/dsk/c2d0s6",
size = "10M"
```

- 2 将 **sybsecurity** 数据库扩展到步骤 1 中初始化的设备上:

```
alter database sybsecurity on auditdev2 = "2M"
```

- 3 运行 **sp_addaudittable**, 在步骤 1 中初始化的设备上创建下一个 **sysaudits** 表:

```
sp_addaudittable auditdev2
```

- 4 对每个 **sysaudits** 表重复步骤 1-3。

设置审计追踪管理

若要有效地管理审计追踪：

- 1 确保审计安装后有两个或多个表，且每个表都在单独的设备上。如果不是，考虑添加审计表和设备。
- 2 编写一个阈值过程，并将其附加到每个审计表段。
- 3 为审计队列大小设置配置参数，并指明一旦当前审计表充满时应采取的相应措施。

以下各节假设您已安装的审计具有两个或更多个表，且每个表都位于单独的设备上。如果仅有一个设备用于审计表，可跳到[第 599 页的“单表审计”](#)。

设置阈值过程

启用审计之前，建立一个阈值过程，以在当前表充满时自动切换审计表。

用于审计设备段的阈值过程应该：

- 使用 `sp_configure` 设置 `current audit table` 配置参数，使下一个空审计表成为当前表。
- 使用 `insert...select` 命令存档接近全满的审计表。

更改当前审计表

`current audit table` 配置参数建立 Adaptive Server 向其中写入审计行的表。作为系统安全员，您可以使用 `sp_configure` 按照以下语法更改当前审计表，其中，`n` 是一个整数，用以确定新的当前审计表：

```
sp_configure "current audit table", n  
[, "with truncate"]
```

`n` 的有效值为：

- 1 表示 `sysaudits_01`，2 表示 `sysaudits_02`，依此类推。
- 值 0 将告知 Adaptive Server 自动将下一个表设置为当前审计表。例如，如果系统中有三个审计表，`sysaudits_01`、`sysaudits_02` 和 `sysaudits_03`，则 Adaptive Server 会将当前审计表设置为：
 - 2，如果当前审计表是 `sysaudits_01`
 - 3，如果当前审计表是 `sysaudits_02`
 - 1，如果当前审计表是 `sysaudits_03`

`with truncate` 选项指定如果新表不是空的，Adaptive Server 应截断该表。如果未指定此选项且新表不为空，则 `sp_configure` 将失败。

注释 如果 Adaptive Server 截断了当前的审计表，而且您没有将数据存档，则该表中的审计记录将丢失。因此，在使用 `with truncate` 选项之前，请将审计数据存档。

若要执行 `sp_configure` 以更改当前的审计表，`sso_role` 必须为活动状态。可以编写一个阈值过程来自动更改当前审计表。

存档审计表

可将 `insert` 与 `select` 一起使用，将审计数据复制到一个与 `sybsecurity` 中的审计表具有相同列的现有表中。

确保阈值过程可以成功将数据复制到另一数据库中的存档表中：

- 1 在不同于存放 `sybsecurity` 中审计表的另一设备上创建存档数据库。
- 2 创建一个存档表，表中的列与 `sybsecurity` 审计表中的列相同。如果还没有这样的表，可使用 `select into`，通过在 `where` 子句中设置一个 `false` 条件来创建空表。例如：

```
use aud_db
go
select *
    into audit_data
    from sybsecurity.dbo.sysaudits_01
    where 1 = 2
```

`where` 条件始终为 `false`，因此将创建 `sysaudits_01` 的空副本。

必须在存档数据库中启用 `select into/bulk copy` 数据库选项（使用 `sp_dboption`），然后才能使用 `select into`。

在使用 `sp_configure` 更改审计表之后，阈值过程可以使用 `insert` 和 `select` 将数据复制到存档数据库中的存档表。此过程可以执行类似如下的命令：

```
insert aud_db.sso_user.audit_data
select * from sybsecurity.dbo.sysaudits_01
```

审计段的阈值过程示例

此样本阈值过程假定已为审计配置了三个表：

```
declare @audit_table_number int
/*
** Select the value of the current audit table
*/
select @audit_table_number = scc.value
from master.dbo.syscurconfigs scc, master.dbo.sysconfigures sc
where sc.config=scc.config and sc.name = "current audit table"
/*
** Set the next audit table to be current.
** When the next audit table is specified as 0,
** the value is automatically set to the next one.
*/
exec sp_configure "current audit table" , 0, "with truncate"
/*
** Copy the audit records from the audit table
** that became full into another table.
*/
if @audit_table_number = 1
    begin
        insert aud_db.sso_user.sysaudits
            select * from sysaudits_01
        truncate table sysaudits_01
    end
else if @audit_table_number = 2
    begin
        insert aud_db.sso_user.sysaudits
            select * from sysaudits_02
        truncate table sysaudits_02
    end
return(0)
```

将阈值过程附加到每个审计段

若要将阈值过程附加到每个审计表段，请使用 `sp_addthreshold`。

执行 `sp_addthreshold` 之前：

- 确定为安装配置的审计表数目及其设备段名称
- 具有对阈值过程中所有命令执行 `sp_addthreshold` 所需的权限和角色

警告！ `sp_addthreshold` 和 `sp_modifythreshold` 将进行检查，以确保只有直接被授予 `sa_role` 的用户才能添加或修改阈值。增加或修改阈值时，所有活动的系统定义角色都将作为有效角色插入到用户所登录的 `systhresholds` 表中。然而，触发阈值过程时，仅激活直接授予的角色。

审计表及其审计段

安装审计时，`auditinit` 将显示每个审计表及其段的名称。`sysaudits_01` 的段名为“`aud_seg1`”，`sysaudits_02` 的段名为“`aud_seg2`”，依此类推。如果使用 `sybsecurity` 作为当前数据库来执行 `sp_helpsegment`，则可以找到有关 `sybsecurity` 数据库中的段的信息。查明用户安装中的审计表数目的一种方法是执行以下 SQL 命令：

```
use sybsecurity
go
select count(*) from sysobjects
       where name like "sysaudit%"
go
```

通过执行以下 SQL 命令，获取有关审计表和 `sybsecurity` 数据库的额外信息：

```
sp_helpdb sybsecurity
go
use sybsecurity
go
sp_help sysaudits_01
go
sp_help sysaudits_02
go
...
```

所需角色和权限

若要执行 `sp_addthreshold`，您必须是数据库所有者或系统管理员。系统安全员应是 `sybsecurity` 数据库的所有者，因此应该能够执行 `sp_addthreshold`。除了能执行 `sp_addthreshold`，您还应该具有执行阈值过程中的所有命令的权限。例如，要为 `current audit table` 执行 `sp_configure`，`sso_role` 必须为活动状态。当阈值过程触发时，Adaptive Server 会尝试打开在执行 `sp_addthreshold` 时有效的所有角色和权限。

将阈值过程 `audit_thresh` 附加到三个设备段：

```
use sybsecurity
go
sp_addthreshold sybsecurity, aud_seg_01, 250, audit_thresh
sp_addthreshold sybsecurity, aud_seg_02, 250, audit_thresh
sp_addthreshold sybsecurity, aud_seg_03, 250, audit_thresh
go
```

当前审计表中保留的可用页少于 250 页时，样本阈值过程 `audit_thresh` 会接管控制。

有关添加阈值过程的详细信息，请参见《系统管理指南：卷 2》中的第 16 章“使用阈值管理可用空间”。

在样本阈值过程就位的情况下进行审计

启用审计后，Adaptive Server 会将所有审计数据写入最初的当前审计表 `sysaudits_01`。当 `sysaudits_01` 还剩不到 250 页就将写满时，阈值过程 `audit_thresh` 将触发。该过程将当前审计表切换到 `sysaudits_02`，而 Adaptive Server 会立即开始将新的审计记录写入 `sysaudits_02`。该过程还会将所有审计数据从 `sysaudits_01` 复制到 `audit_db` 数据库中的 `audit_data` 存档表。审计表的轮换以这种方式继续下去，不需要手工干预。

设置审计配置参数

为审计安装设置以下配置参数：

- `audit queue size` 设置内存中的审计队列中的记录数目。
- `suspend audit when device full` 确定在当前审计表完全写满时 Adaptive Server 的行为。仅当附加到当前表段的阈值过程运行不正常时，才会发生完全充满的情况。

设置审计队列的大小

缺省审计队列大小为 100 字节。审计队列池所消耗的内存量在 `audit queue size` 参数中定义，并包括数据缓冲区和内存池的开销。但是，池中的内存量可能会因版本和芯片体系结构而异。

使用 `sp_configure` 设置审计队列的长度。语法为：

```
sp_configure "audit queue size", [value]
```

`value` 是审计队列可容纳的记录数。最小值为 1，最大值为 65,535。例如，若要将审计队列大小设置为 300，请执行：

```
sp_configure "audit queue size", 300
```

有关设置审计队列大小和其它配置参数的详细信息，请参见第 5 章“设置配置参数”。

设备已满时挂起审计

如果有两个或多个审计表，每个表都位于非主设备的单独设备上，而且每个审计表段都有阈值过程，则审计设备应绝不会充满。只有当阈值过程运行不正常时，才会发生“全满”情况。使用 `sp_configure` 设置 `suspend audit when device full` 参数，以确定设备确实充满时所发生的情况。选择下列选项之一：

- 将导致审计事件的审计进程和所有用户进程挂起。系统安全员清除当前审计表后，恢复正常操作。
- 截断下一个审计表并开始使用它。这样，就可以不需要系统安全员的干预而继续进行正常操作。

使用 `sp_configure to` 设置此配置参数。`sso_role` 必须为活动状态。语法为：

```
sp_configure "suspend audit when device full",  
[0|1]
```

- 0 — 每当当前审计表变满时，截断下一个审计表，并开始使用它作为当前审计表。如果将该参数设置为 0，审计进程将从不会挂起；但是，如果较旧的审计记录尚未存档则会丢失。
- 1（缺省值） — 挂起导致可审计事件的审计进程和所有用户进程。若要恢复正常操作，系统安全员必须登录并将一个空表设置为当前审计表。在此期间，系统安全员不能进行正常审计。如果系统安全员的操作在正常情况下会生成审计记录，Adaptive Server 会将一条错误消息和有关事件的信息发送到错误日志。

如果已将一个阈值过程附加到审计表段，则将 `suspend audit when device full` 设置为 1（开启）。如果设置为 0（关闭），则在阈值过程有机会存档审计记录之前，Adaptive Server 可能会截断已写满的审计表。

设置事务日志管理

本节描述有关管理 `sybsecurity` 中的事务日志的指导方针。

如果 `trunc log on chkpt` 数据库选项处于活动状态，则 Adaptive Server 每次执行自动 checkpoint 时，都将截断 `syslogs`。安装审计后，`trunc log on chkpt` 的值为 `on`，但可以使用 `sp_dboption` 来更改其值。

截断事务日志

如果为 `sybsecurity` 数据库启用了 `trunc log on chkpt` 选项，则不必担心事务日志会写满。Adaptive Server 每次执行 checkpoint 时都会截断日志。如果启用此选项，则无法使用 `dump transaction` 来转储事务日志，但可使用 `dump database` 来转储数据库。

如果按照第 592 页的“设置阈值过程”中的过程进行操作，审计表会自动存档到另一数据库的表中。可以对此存档数据库使用标准备份和恢复过程。

如果 `sybsecurity` 设备上出现故障，则可以重新装载数据库并继续进行审计。至多会丢失内存中的审计队列和当前审计表中的记录，因为存档数据库包含了所有其它审计数据。重新装载数据库后，使用 `sp_configure with truncate` 来设置和截断当前审计表。

如果转储数据库后没有改变过服务器范围的审计选项，则 `sysauditoptions` 中存储的所有审计选项在重新装载 `sybsecurity` 时都将自动恢复。如果没有恢复，可以运行脚本，以在重新开始审计前设置这些选项。

不截断的情况下管理的事务日志

如果使用 `db_option` 关闭 `trunc log on chkpt`，事务日志将会充满。您应计划将最后机会阈值过程附加到事务日志段。当段中剩余的空间小于 Adaptive Server 自动计算的阈值量时，该过程将接管控制。该阈值量是备份事务日志所需的可用日志页数的一个估计值。

最后机会阈值过程的缺省名是 `sp_thresholdaction`，但只要 `sa_role` 为活动状态，就可使用 `sp_modifythreshold` 指定其它名称。

注释 `sp_modifythreshold` 将进行检查以确保激活了“`sa_role`”。有关详细信息，请参见第 595 页的“将阈值过程附加到每个审计段”。

Adaptive Server 未提供缺省过程，但《系统管理指南：卷 2》中的第 16 章“使用阈值管理可用空间”包含了最后机会阈值过程的示例。该过程应该执行 `dump transaction` 命令，后者将截断日志。事务日志达到最后机会阈值点时，正在运行的任何事务都将被挂起，直到有空间可用为止。由于 `sybsecurity` 数据库的 `abort xact when log is full` 选项总是设置为 `false`，因此会发生挂起。您不能更改此选项。

当 `trunc log on chkpt` 选项处于禁用状态时，可以对 `sybsecurity` 数据库使用标准备份和恢复过程，但要注意，恢复的数据库中的审计表与其在设备出现故障时的状态可能不同步。

启用和禁用审计

将 `sp_configure` 与 `auditing` 配置参数一起使用以启用或禁用审计。语法为：

```
sp_configure "auditing", [0 | 1]
```

- 1 — 启用审计。
- 0 — 禁用审计。

例如，若要启用审计，请输入：

```
sp_configure "auditing", 1
```

注释 当您启用或禁用审计时，Adaptive Server 会自动生成审计记录。请参见第 614 页的表 18-5 中的事件代码 73 和 74。

单表审计

Sybase 极力建议您不要对生产系统使用单个设备进行审计。如果仅使用一个审计表，则在存档审计数据和截断审计表时会消耗一定时间，在此期间将丢失写入的审计记录。仅使用一个审计表时没有方法能避免这种情况发生。

如果仅使用一个审计表，则该审计表很可能会充满。其后果取决于您对 `suspend audit when device full` 的设置情况。如果已将 `suspend audit when device full` 设置为打开，则审计进程将被挂起，导致审计事件的所有用户进程也被挂起。如果 `suspend audit when device full` 为关闭，审计表将被截断，将丢失审计表中的所有审计记录。

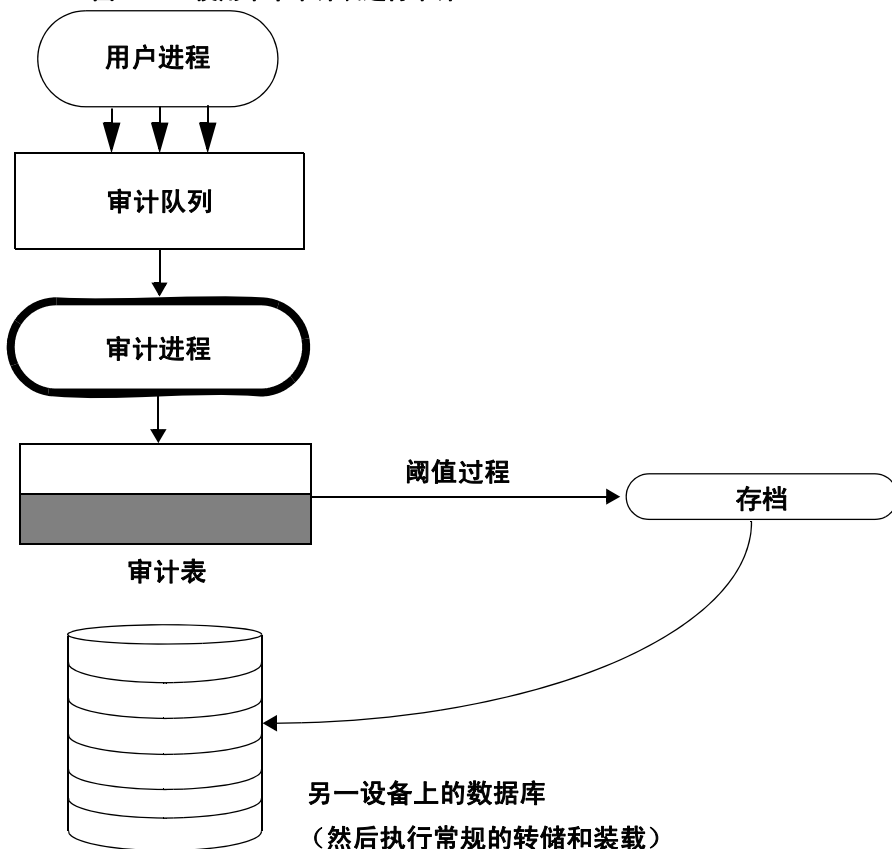
对于可接受少量审计记录丢失的非生产系统，如果不能腾出用于多个审计表的额外磁盘空间，或没有其它设备可用，您可以使用单个审计表审计。

使用单个审计表的过程与使用多个审计表的过程类似，不同之处如下所述：

- 安装时，仅指定一个系统表用于审计。
- 安装时，仅指定一个设备用于审计系统表。
- 为存档审计记录创建的阈值过程与使用多个审计表时创建的阈值过程不同。

图 18-2 显示审计进程如何处理单个审计表。

图 18-2: 使用单个审计表进行审计



建立和管理单表审计

单表审计与多表审计的配置步骤相同。有关详细信息，请参见[表 18-1](#)。

使用单表审计的审计进程

对于单表审计，其阈值过程应该：

- 用 `insert` 和 `select` 命令，将几乎充满的审计表存档到另一表中。
- 使用 `truncate table` 命令截断审计表以创建用于新审计记录的空间。

只有创建一个与审计表具有相同列的存档表之后，才可以存档审计记录。执行完这些步骤后，阈值过程就能使用 `insert` 和 `select` 将审计记录复制到存档表中。

下面是使用单个审计表的阈值过程样本：

```
create procedure audit_thresh as
/*
** copy the audit records from the audit table to
** the archive table
*/
insert aud_db.sso_user.audit_data
      select * from sysaudits_01
return(0)
go
/*
** truncate the audit table to make room for new
** audit records
*/
truncate table "sysaudits_01"
go
```

创建阈值过程后，将需要该过程附加到审计表段。有关说明，请参见[第 595 页的“将阈值过程附加到每个审计段”](#)。

警告！ 在多处理器上，即使有审计表充满之前触发的阈值过程，审计表也可能会充满。例如，如果阈值过程运行于负载很重的 CPU 上，而执行可审计事件的用户进程运行于负载较小的 CPU 上，则触发阈值过程之前，审计表有可能充满。配置参数 `suspend audit when device full` 确定审计表充满时所发生的情况。有关设置该参数的信息，请参见[第 597 页的“设备已满时挂起审计”](#)。

当前审计表充满时会发生什么？

当前审计表充满时：

- 1 审计进程试图将下一个审计记录插入该表中。此操作将失败，因此审计进程终止。将向错误日志中写入一条错误消息。
- 2 当用户尝试执行可审计事件时，由于审计无法继续，所以无法完成该事件。用户进程终止。没有试图执行可审计事件的用户不会受到影响。
- 3 如果启用了登录审计，则除了系统安全员外，其他人都不能登录到服务器。
- 4 如果在 `sso_role` 处于活动状态时审计执行的命令，则系统安全员将无法执行命令。

当前审计表充满时恢复

如果当前审计设备和审计队列都已满，则系统安全员不能执行审计。之后系统安全员执行的每个可审计事件都将向错误日志文件中发送一条警告消息。此消息指明日期和时间、说明审计已丢失的警告以及登录名、`event` 代码和通常存储在审计表的 `extrainfo` 列中的其它信息。

当前审计表已满时，系统安全员可以存档并截断审计表，如[第 593 页的“存档审计表”](#)中所述。系统管理员可以执行 `shutdown` 来停止服务器，然后重新启动服务器以重建审计。

如果审计系统异常终止，则系统安全员可在存档和截断当前审计表后关闭服务器。通常只有系统管理员才能执行 `shutdown`。

重新启动审计

如果审计进程因出现错误而强制终止，则可通过输入以下命令手动重新启动 `sp_audit`：

```
sp_audit restart
```

只要当前没有任何审计在运行，即可重新启动审计进程，但必须用 `sp_configure` “auditing” 1 启用审计进程。

设置全局审计选项

安装审计后，可使用 `sp_audit` 设置审计选项。`sp_audit` 的语法为：

```
sp_audit option, login_name, object_name [,setting]
```

如果不带参数运行 `sp_audit`，它将提供选项的完整列表。有关 `sp_audit` 的详细信息，请参见《参考手册：过程》。

注释 为服务器激活审计之前，不会进行审计。有关如何启动审计的信息，请参见第 599 页的“启用和禁用审计”。

审计选项：类型和要求

可为 `sp_audit` 参数的 `login_name` 和 `object_name` 参数指定的值取决于指定的审计选项类型：

- 全局选项应用于影响整个服务器的命令，例如启动服务器、磁盘操作命令和允许用户定义即席审计记录的命令。全局事件的选项设置存储在 `sybsecurity..sysauditoptions` 系统表中。
- 特定于数据库的选项应用于一个数据库。例如，更改数据库；将数据批量复制 (`bcp in`) 到数据库中；授予或撤消对数据库中对象的访问权；以及在数据库中创建对象，等等。特定于数据库的事件的选项设置存储在 `master..sysdatabases` 系统表中。
- 特定于对象的选项应用于一个对象。如选择、插入、更新或删除特定表或视图的行以及执行特定触发器或过程。特定于对象的事件的选项设置存储在相应数据库的 `sysobjects` 系统表中。
- 特定于用户的选项适用于特定的用户或系统角色。例如，特定用户对任何表或视图的访问，或当特定系统角色（例如 `sa_role`）为活动状态时执行的所有操作。单个用户的选项设置存储在 `master..syslogins` 中。系统角色的设置存储在 `master..sysauditoptions` 中。

表 18-2 显示：

- `option` 的有效值和每个选项的类型（全局、特定于数据库、特定于对象或特定于用户）
- 每个选项的 `login_name` 和 `object_name` 参数的有效值
- 您设置审计选项时所在的数据库
- 您设置选项时被审计的命令或权限
- 每个选项的一个示例

所有选项的缺省值都是 “off”。

表 18-2: 审计选项、要求和示例

选项 (选项类型)	login_name	object_name	设置选项时应 在的数据库	将被审计的命令或权限
adhoc (特定于用户)	all	all	任何	允许用户使用 sp_addauditrecord
	示例: sp_audit "adhoc", "all", "all", "on" (启用用户定义的即席审计记录。)			
all (特定于用户)	一个登录名 或角色	all	任何	特定用户或具有特殊角色的用户执行的 所有操作
	示例 sp_audit "all", "sa_role", "all", "on" (为 sa_role 处于活动状态的所有操作启用审计。)			
alter (特定于数据库)	all	要审计的 数据库	任何	alter database、alter table
	示例 sp_audit @option = "alter", @login_name = "all", @object_name = "master", @setting = "on" (为 master 数据库中所有 alter database 和 alter table 执行启用审计。)			
bcp (特定于数据库)	all	要审计的 数据库	任何	bcp in
	示例 sp_audit "bcp", "all", "pubs2" (返回 pubs2 数据库中 bcp 审计的状态。如果没有为 setting 指定值, Adaptive Server 将 返回指定选项的审计状态)			
bind (特定于数据库)	all	要审计的 数据库	任何	sp_bindefault、sp_bindmsg、 sp_bindrule
	示例 sp_audit "bind", "all", "planning", "off" (为 planning 数据库禁用绑定审计。)			
cmdtext (特定于用户)	要审计的用 户的登录名	all	任何	用户输入的 SQL 文本。 (不反映所涉及文本是否通过了权限 检查。eventmod 的值始终为 1。)
	示例 sp_audit "cmdtext", "sa", "all", "off" (为数据库所有者禁用文本审计。)			

选项 (选项类型)	login_name	object_name	设置选项时应 在的数据库	将被审计的命令或权限
create (特定于数据库)	all	要审计的 数据库	任何	create database、create table、create procedure、create trigger、create rule、 create default、sp_addmessage、 create view、create index、create function
注释 为 <i>object_name</i> 指定 master 以对 create database 进行审计。这样，还会对 master 中其它对象的创建进行审计。				
示例 <code>sp_audit "create", "all", "planning", "pass"</code> (启用对 planning 数据库中成功对象创建操作的审计。 create database 的当前审计状态不会受影响，因为没有指定 master 数据库。)				
dbaccess (特定于数据库)	all	要审计的 数据库	任何	另一数据库对该数据库的任何访问
示例 <code>sp_audit "dbaccess", "all", "project", "on"</code> (审计对 project 数据库的所有外部访问。)				
dbcc (全局)	all	all	任何	需要权限的所有 dbcc 命令
示例 <code>sp_audit "dbcc", "all", "all", "on"</code> (审计 dbcc 命令的所有执行。)				
delete (特定于对象)	all	要审计的表或 视图的名称， 或者 default view 或 default table	该表或视图的 数据库 (除 tempdb 之外)	从表中删除数据的 delete 命令、 从视图中删除数据的 delete 命令
示例 <code>sp_audit "delete", "all", "default table", "on"</code> (审计当前数据库中所有未来表的所有删除操作。)				
disk (全局)	all	all	任何	disk init、disk refit、disk reinit、disk mirror、disk unmirror、disk remirror、 disk resize
示例 <code>sp_audit "disk", "all", "all", "on"</code> (审计服务器的所有磁盘操作。)				
drop (特定于数据库)	all	要审计的 数据库	任何	drop database、drop table、drop procedure、drop index、drop trigger、 drop rule、drop default、 sp_dropmessage、drop view、drop function
示例 <code>sp_audit "drop", "all", "financial", "fail"</code> (审计 financial 数据库中所有未通过权限检查的删除命令。)				

选项 (选项类型)	login_name	object_name	设置选项时应 在的数据库	将被审计的命令或权限
dump (特定于数据库)	all	要审计的 数据库	任何	dump database、dump transaction
示例 sp_audit "dump", "all", "pubs2", "on" (审计 pubs2 数据库中的转储命令。)				
encryption_key (特定于数据库)	all	要审计的 数据库	任何	alter encryption key create encryption key drop encryption key sp_encryption
示例 审计 pubs2 数据库中的所有上述命令： sp_audit "encryption_key", "all", "pubs2", "on"				
errors (全局)	all	all	任何	致命错误、非致命错误
示例 sp_audit "errors", "all", "all", "on" (审计整个服务器上的错误。)				
errorlog	all	all	任何	sp_errorlog 或 errorlog_admin 函数
示例 sp_audit "errorlog", "all", "all", "on" (对尝试“更改日志”以转移到新 Adaptive Server 错误日志文件的操作进行审计。)				
exec_procedure (特定于对象)	all	要审计的过程 的名称或 default procedure	该过程的数据 库 (除 tempdb 之外)	execute
示例 sp_audit "exec_procedure", "all", "default procedure", "off" (禁用对当前数据库中新过程的自动审计。)				
exec_trigger (特定于对象)	all	要审计的触发 器的名称或 default trigger	该触发器的数 据库 (除 tempdb 之外)	任何引发触发器的命令
示例 sp_audit "exec_trigger", "all", "trig_fix_plan", "fail" (对当前数据库中 trig_fix_plan 触发器的所有失败的执行进行审计。)				
func_dbaccess (特定于数据库)	all	正在审计的数 据库的名称	任何	使用以下函数对数据库进行的访问： curunreserved_pgs、db_name、 db_id、lct_admin、setdbrepstat、 setrepstatus、setrepdefmode、 is_repagent_enabled、 rep_agent_config、rep_agent_admin
示例 sp_audit @option="func_dbaccess", @login_name="all", @object_name = "strategy", @setting = "on" (对通过内置函数对 strategy 数据库的访问进行审计。)				

选项 (选项类型)	login_name	object_name	设置选项时应 在的数据库	将被审计的命令或权限
func_obj_access (特定于对象)	all	任何在 sysobjects 中 具有一个条目 的对象的名称	任何	使用以下函数对对象进行的访问： schema_inc、col_length、col_name、 data_pgs、index_col、object_id、 object_name、reserved_pgs、rowcnt、 used_pgs、has_subquery
示例 sp_audit @option="func_obj_access", @login_name="all", @object_name = "customer", @setting = "on" (对通过内置函数对 customer 表的访问进行审计。)				
grant (特定于数据库)	all	要审计的数据 库的名称	任何	grant
示例 sp_audit @option="grant", @login_name="all", @object_name = "planning", @setting = "on" (审计 planning 数据库中的所有授权。)				
insert (特定于对象)	all	正在向其插入 行的视图或表 的名称, 或者 default view 或 default table	该对象的数据 库 (除 tempdb 之外)	将数据插入到表中的 insert 命令、 将数据插入到视图中的 insert 命令
示例 sp_audit "insert", "all", "dpt_101_view", "on" (对向当前数据库中的 dpt_101_view 视图插入数据的所有插入命令进行审计。)				
install (特定于数据库)	all	要审计的 数据库	任何	install java
示例 sp_audit "install", "all", "planning", "on" (审计数据库 planning 中 Java 类的安装)				
load (特定于数据库)	all	要审计的 数据库	任何	load database、load transaction
示例 sp_audit "load", "all", "projects_db", "fail" (对 projects_db 数据库中所有已失败的、数据库和事务装载的执行进行审计。)				
login (全局)	all	all	任何	到 Adaptive Server 的任何登录
示例 sp_audit "login", "all", "all", "fail" (对所有已失败的、到服务器的登录尝试进行审计。)				
login_locked (全局)	all	all	任何	
示例 sp_audit "login_locked", "all", "all", "on" (登录由于超过配置的失败登录尝试次数而被锁定。)				
logout	all	all	任何	任何从 Adaptive Server 注销的操作
示例 sp_audit "logout", "all", "all", "off" (禁用对服务器注销操作的审计。)				

选项 (选项类型)	login_name	object_name	设置选项时应 在的数据库	将被审计的命令或权限
mount (全局)	all	all	任何	mount database
	示例 sp_audit "mount", "all", "all", "on" (审计发出的所有 mount database 命令。)			
password	all	all	任何	全局口令和登录策略选项的设置
	示例 sp_audit "password", "all", "all", "on"			
quiesce (全局)	all	all	任何	quiesce database
	示例 sp_audit "quiesce", "all", "all", "on" (对 quiesce database 命令启用审计。)			
reference (特定于对象)	all	正在向其插入 行的视图或表 的名称, 或者 default view 或 default table	任何	create table、alter table
	示例 sp_audit "reference", "all", "titles", "off" (禁用对 titles 表的引用创建的审计。)			
remove (特定于数据库)	all	all	任何	审计 Java 类的删除
	示例 sp_audit "remove", "all", "planning", "on" (审计数据库 planning 中 Java 类的删除。)			
revoke (特定于数据库)	all	要审计的 数据库	任何	revoke
	示例 sp_audit "revoke", "all", "payments_db", "off" (禁用对 payments_db 数据库中 revoke 执行的审计。)			
rpc (全局)	all	all	任何	远程过程调用 (内部或外部)
	示例 sp_audit "rpc", "all", "all", "on" (审计对服务器外部或内部进行的所有远程过程调用。)			
security (全局)	all	all	任何	全服务器范围内与安全性相关的事件。请参见表 18-5 中的“安全性”选项。
	示例 sp_audit "security", "all", "all", "on" (对服务器中全服务器范围内的与安全性相关的事件进行审计。)			
select (特定于对象)	all	正在向其插入 行的视图或表 的名称, 或者 default view 或 default table	该对象的数据 库 (除 tempdb 之外)	从表中选择数据的 select 命令、从视 图中选择数据的 select 命令
	示例 sp_audit "select", "all", "customer", "fail" (对从当前数据库中的 customer 表选择数据但失败的所有选择命令进行审计。)			

选项 (选项类型)	<i>login_name</i>	<i>object_name</i>	设置选项时应 在的数据库	将被审计的命令或权限
setuser (特定于数据库)	all 示例 <code>sp_audit "setuser", "all", "projdb", "on"</code> (审计 projdb 数据库中 setuser 的所有执行。)	all	任何	setuser
table_access (特定于用户)	要审计的用 户的登录名。 示例 <code>sp_audit "table_access", "smithson", "all", "on"</code> (审计由登录名 “smithson” 执行的所有表访问。)	all	任何	表中的 select、delete、update 或 insert 访问
transfer_table (全局)	all 示例 <code>sp_audit "transfer_table", "tdbl.table1", "all", "on"</code> (对服务器中全服务器范围内的与传输相关的事件进行审计。)	all	任何	全服务器范围内的选项。不显示在 sysauditoptions 中。
truncate (特定于数据库)	all 示例 <code>sp_audit "truncate", "all", "customer", "on"</code> (审计 customer 数据库中的所有表截断。)	要审计的 数据库	任何	truncate table
unbind (特定于数据库)	all 示例 <code>sp_audit "unbind", "all", "master", "fail"</code> (对 master 数据库中所有失败的解除绑定尝试进行审计。)	要审计的 数据库	任何	sp_unbindefault、sp_unbindrule、 sp_unbindmsg
unmount (全局)	all 示例 <code>sp_audit "unmount", "all", "all", "on"</code> (对使用任何数据库卸载或创建清单文件的所有尝试进行审计。)	all	任何	unmount database
update (特定于对象)	all 示例 <code>sp_audit "update", "all", "projects", "on"</code> (对用户更新当前数据库中 projects 表的所有尝试进行审计。)	指定要审计的 对象的名称， default table 或 default view	该对象的数据 库（除 tempdb 之外）	对表执行的 update 命令、对视图执 行的 update 命令
view_access (特定于用户)	要审计的用 户的登录名 示例 <code>sp_audit "view_access", "joe", "all", "off"</code> (禁用用户 “joe” 的视图审计。)	all	任何	对视图执行的 select、delete、insert 或 update

设置审计选项的示例

假定您要对 `company_operations` 数据库中 `projects` 表和该数据库中所有新表上所有失败的删除进行审计。对 `projects` 表使用特定于对象的 `delete` 选项，对数据库中的所有未来表使用 `default table`。在执行 `sp_audit` 以设置特定于对象的审计选项之前，您必须处于对象的数据库中：

```
sp_audit "security", "all", "all", "fail"
```

对于此示例，请执行：

```
use company_operations
go
sp_audit "delete", "all", "projects", "fail"
go
sp_audit "delete", "all", "default table",
"fail"
go
```

隐藏系统存储过程和命令口令参数

如果配置并启用了审计，且设置了 `sp_audit` 选项 `'cmdtext'`，则会将系统存储过程和命令口令参数替换为审计日志中所含审计记录中固定长度的星号字符串。

例如，当启用审计并设置了 `sp_audit cmdtext` 时执行以下命令：

```
sp_password 'oldpassword', 'newpassword'
```

会产生类似以下内容的输出：

```
sp_password '*****', '*****'
```

这样做可以保护口令不会被可以访问审计日志的其他人看到。

确定当前审计设置

若要确定给定选项的当前审计设置，请使用 `sp_displayaudit`。语法为：

```
sp_displayaudit [procedure | object | login | database | global |
                default_object | default_procedure [, name]]
```

有关详细信息，请参见《参考手册：过程》中的 `sp_displayaudit`。

向审计追踪中添加用户指定的记录

`sp_addauditrecord` 允许用户向审计追踪中输入注释。语法为：

```
sp_addauditrecord [text] [, db_name] [, obj_name]
[, owner_name] [, dbid] [, objid]
```

所有参数均为可选：

- *text* — 是要添加到 `extrainfo` 审计表中的消息文本。
- *db_name* — 是记录中引用的数据库的名称，它将插入到当前审计表的 `dbname` 列中。
- *obj_name* — 是记录中引用的对象的名称，它将插入到当前审计表的 `objname` 列中。
- *owner_name* — 是记录中引用的对象的所有者，它将插入到当前审计表的 `objowner` 列中。
- *dbid* — 是一个整数值，表示 `db_name` 的数据库 ID 号，它将插入到当前审计表的 `dbid` 列中。不要将其置于引号中。
- *objid* — 是一个整数值，表示 `obj_name` 的对象 ID 号。不要将其置于引号中。*objid* 将插入到当前审计表的 `objid` 列中。

在下列情况下，可以使用 `sp_addauditrecord`：

- 对 `sp_addauditrecord` 具有执行权限。
- 使用 `sp_configure` 激活了审计配置参数。
- `adhoc` 审计选项通过 `sp_audit` 启用。

缺省情况下，只有系统安全员和 `sybsecurity` 的数据库所有者才能使用 `sp_addauditrecord`。可以将执行该命令的权限授予其他用户。

增加用户定义的审计记录的示例

下面的示例向当前审计表中增加一条记录。文本部分将输入到当前审计表的 `extrainfo` 列中；“corporate”将输入到 `dbname` 列中；“payroll”将输入到 `objname` 列中；“dbo”将输入到 `objowner` 列中；“10”将输入到 `dbid` 列中；“1004738270”将输入到 `objid` 列中：

```
sp_addauditrecord "I gave A. Smith permission to view
the payroll table in the corporate database. This
permission was in effect from 3:10 to 3:30 pm on
9/22/92.", "corporate", "payroll", "dbo", 10,
1004738270
```

以下示例仅将信息插入当前审计表的 **extrainfo** 和 **dbname** 列中：

```
sp_addauditrecord @text="I am disabling auditing
briefly while we reconfigure the system",
@db_name="corporate"
```

查询审计追踪

若要查询审计追踪，请使用 SQL 来选择和汇总审计数据。如果按照 [第 592 页](#) 的“[设置审计追踪管理](#)”中描述的过程进行操作，审计数据将被自动存档到另一数据库中的一个或多个表中。例如，假定审计数据位于 **audit_db** 数据库中名为 **audit_data** 的表中。若要选择由“bob”于 1993 年 7 月 5 日所执行任务的审计记录，请执行：

```
use audit_db
go
select * from audit_data
    where loginname = "bob"
    and eventtime like "Jul 5% 93"
go
```

以下命令请求激活了系统安全员角色的用户在 **pubs2** 数据库中所执行的命令的审计记录：

```
select * from audit_data
    where extrainfo like "%sso_role%"
    and dbname = "pubs2"
go
```

以下命令请求所有表截断（事件 64）的审计记录：

```
select * from audit_data
    where event = 64
go
```

若要使用审计事件的名称来查询审计追踪，请使用 **audit_event_name** 函数。例如，若要请求所有数据库创建事件的审计记录，请输入：

```
select * from audit_data where audit_event_name(event)
    = "Create Database"
go
```


了解审计表

只有系统安全员才能访问系统审计表，该用户可通过执行 SQL 命令来读取这些表。只允许对系统审计表执行 `select` 和 `truncate` 命令。

表 18-3 介绍了所有审计表中的列。

表 18-3：每个审计表中的列

列名	数据类型	说明
event	smallint	审计的事件的类型。请参见第 614 页的表 18-5。
eventmod	smallint	有关被审计的事件的详细信息。指示被审计的事件是否通过了权限检查。可能的值有： • 0 = 此事件无修饰符。 • 1 = 事件通过了权限检查。 • 2 = 事件未通过权限检查。
spid	smallint	引起写入审计记录的进程的 ID。
eventtime	datetime	审计事件发生的日期和时间。
sequence	smallint	单个事件中记录的序列号。某些事件需要多个审计记录。
suid	smallint	执行审计事件的用户的服务器登录 ID。
dbid	int null	被审计的事件发生时所在的数据库 ID，或者对象、存储过程或触发器（取决于事件的类型）所在的数据库 ID。
objid	int null	被访问的对象、存储过程或触发器的 ID。
xactid	binary(6) null	包含审计事件的事务的 ID。对于多数据库事务，这是该事务在其中启动的数据库中的事务 ID。
loginname	varchar(30) null	与 suid 相对应的登录名。
dbname	varchar(30) null	与 dbid 相对应的数据库名。
objname	varchar(30) null	与 objid 相对应的对象名。
objowner	varchar(30) null	objid 的所有者名。
extrainfo	varchar(255) null	有关审计事件的其它信息。该列包含一系列用分号分开的项。有关详细信息，请参见第 614 页的“读取 extrainfo 列”。
nodeid	tinyint	发生事件的集群中的服务器 nodeid。

读取 **extrainfo** 列

extrainfo 列包含一系列用分号分隔的数据。数据按以下种类组织。

表 18-4: extrainfo 列中的信息

位置	类别	说明
1	角色	由空格分开的活动角色列表。
2	关键字或选项	用于事件的关键字或选项的名称。例如，对于 alter table 命令，可能已经使用了 add column 或 drop constraint 选项。如果列出了多个关键字或选项，则用逗号分开。
3	以前值	如果事件导致了值的更新，则此项包含更新之前的值。
4	当前值	如果事件导致了值的更新，则此项包含新值。
5	其它信息	为事件记录的其它与安全性相关的信息。
6	代理信息	初始登录名（如果在 set proxy 有效时发生该事件）。
7	主要名称	来自基础安全性机制的主要名称（如果用户的登录名是安全缺省登录名，并且用户通过统一登录名登录到 Adaptive Server ）。如果没有使用安全缺省登录名，则此项的值为 NULL 。

以下示例显示更改审计配置参数事件的 **extrainfo** 列条目。

```
sso_role;suspend audit when device full;1;0;;ralph;
```

此条目表示系统安全员已将 **suspend audit when device full** 从 1 更改为 0。此条目没有“其它信息”。第 6 个类别指出用户“ralph”正在使用代理登录。没有提供主要名称。

此审计记录中的其它字段提供了其它有关信息。例如，该记录包含服务器用户 ID (suid) 和登录名 (loginname)。

表 18-5 列出了 **event** 列中显示的值（按 **sp_audit** 选项排列）。“**extrainfo** 中的信息”列按照表 18-4 描述中的类别介绍了可能显示在审计表的 **extrainfo** 列中的信息。

表 18-5: 事件和 extrainfo 列中的值

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
（不受选项控制的自动被审计的事件）	使用以下命令启用审计： sp_configure auditing	73	—
（不受选项控制的自动被审计的事件）	使用以下命令禁用审计： sp_configure auditing	74	—
解锁管理员的帐户	使用以下命令禁用审计： sp_configure auditing	74	—
adhoc	用户定义的审计记录	1	extrainfo 由 sp_addauditrecord 的 text 参数填充

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
alter	alter database	2	子命令关键字: alter maxhold alter size inmemory
	alter table	3	子命令关键字: add/drop/modify column replace columns replace decrypt default replace/add decrypt default add constraint drop constraint 如果添加了一个或多个加密列, 则 extrainfo 将包含: add/drop/modify column <i>column1/keyname1</i> , [<i>column2/keyname2</i>] 其中, <i>keyname</i> 是密钥的完全限定名。
bcp	bcp in	4	—
bind	sp_bindefault	6	其它信息: 缺省值的名称
	sp_bindmsg	7	其它信息: 消息 ID
	sp_bindrule	8	其它信息: 规则的名称
all、create cmdtext	create database	9	关键字或选项: inmemory
	所有命令	92	命令的全文本, 由客户端发送
create	create database	9	—
	create default	14	—
	create procedure	11	—
	create rule	13	—
	create table	10	对于加密列, extrainfo 包含列名和密钥名。 EK <i>column1/keyname1</i> [<i>column2 keyname2</i>] 其中, EK 为前缀, 用于指示后续信息将引用加密密钥; 而 <i>keyname</i> 则是密钥的完全限定名。
	create trigger	12	—
	create view	16	—
	create index	104	其它信息: 索引的名称
	create function	97	—
	sp_addmessage	15	其它信息: 消息号
dbaccess	任何用户对数据库进行的任何访问	17	关键字或选项: use cmd outside reference

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
dbcc	dbcc (所有关键字)	81	关键字或选项: 任意 dbcc 关键字 (例如 checkstorage) 及该关键字的选项。
delete	从表中删除数据的 delete 命令	18	关键字或选项: delete
	从视图中删除数据的 delete 命令	19	关键字或选项: delete
disk	disk init	20	关键字或选项: disk init 其它信息: 磁盘的名称
	disk mirror	23	关键字或选项: disk mirror 其它信息: 磁盘的名称
	disk refit	21	关键字或选项: disk refit 其它信息: 磁盘的名称
	disk reinit	22	关键字或选项: disk reinit 其它信息: 磁盘的名称
	disk release	87	关键字或选项: disk release 其它信息: 磁盘的名称
	disk remirror	25	关键字或选项: disk remirror 其它信息: 磁盘的名称
	disk unmirror	24	关键字或选项: disk unmirror 其它信息: 磁盘的名称
	disk resize	100	关键字或选项: disk resize 其它信息: 磁盘的名称
drop	drop database	26	—
	drop default	31	—
	drop procedure	28	—
	drop table	27	—
	drop trigger	29	—
	drop rule	30	—
	drop view	33	—
	drop index	105	其它信息: 索引名
	drop function	98	—
	sp_dropmessage	32	其它信息: 消息号
dump	dump database	34	—
	dump transaction	35	—

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
encryption_key	sp_encryption	106	如果第一次设置口令： ENCR_ADMIN system_encr_passwd password ***** 如果后来更改口令： ENCR_ADMIN system_encr_passwd password ***** *****
	create encryption key	107	关键字包含： algorithm name-bitlength/IV [random NULL]/pad [random NULL] user/system 例如： AES-128/IV RANDOM/PAD NULL USER
	alter encryption key	108	default/not default
	drop encryption key	109	
	AEK modify encryption	118	modify encryption with user passwd for user <i>username</i> {with login passwd with user passwd with <i>keyvalue</i>} [for recovery] 请注意，<i>keyvalue</i> 只会为 alter encryption key modify encryption 的重复项显示。例如，当用户“stephen”修改其密钥副本时，将保存以下信息： MODIFY ENCRYPTION for user stephen WITH USER PASSWD
	AEK add encryption	119	add encryption for user <i>user_name</i> for login association recovery with keyvalue] 请注意，<i>keyvalue</i> 只会为 alter encryption key add encryption 的重复项显示。
	alter encryption key drop encryption	120	drop encryption [for recovery for user <i>user_name</i> 请参见《加密列用户指南》。
	alter encryption key modify owner	121	modify owner [new owner <i>user_name</i>] 请参见《加密列用户指南》。
	alter encryption key recover key	122	recovery key [with <i>key_value</i>] with <i>keyvalue</i> 只会在 alter encryption key 的复制过程中使用 请参见《加密列用户指南》。

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
errorlog	errorlog 或 errorlog_admin 函数	127	将记录传递到 errorlog_admin 的参数以标识子命令: errorlog_admin (param1, param2,...)。
errors	致命错误	36	其它信息: 错误号 . 严重性 . 状态
	非致命错误	37	其它信息: 错误号 . 严重性 . 状态
exec_procedure	执行过程	38	其它信息: 所有输入参数
exec_trigger	执行触发器	39	—
func_obj_access、 func_dbaccess	通过 Transact-SQL 函数对对象和数据库的访问。(必须为 sa_role 启用审计才能审计函数)。	86	—
grant	grant	40	—
insert	向表中插入数据的 insert 命令	41	关键字或选项: • 如果使用 insert: insert • 如果使用 select into: insert into, 后跟完全限定对象名
	向视图中插入数据的 insert 命令	42	关键字或选项: insert
install	install	93	—
load	load database	43	—
	load transaction	44	—
login	到服务器的任何登录	45	其它信息: • 从中执行登录的计算机的主机名和 IP 地址。 • 错误号 . 严重性 . 状态 (对于失败的登录)。
login_locked	由于超过配置的失败登录尝试次数而被锁定的登录	112	
logout	服务器的任何注销	46	其它信息: 主机名
mount	mount database	101	—
password	sp_passwordpolicy 及其所有操作 (list 除外)	115	sp_passwordpolicy 的参数
quiesce	quiesce database	96	—
reference	表的引用的创建	91	关键字或选项: reference 其它信息: 引用表的名称
remove	remove java	94	—
revoke	revoke	47	—

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
rpc	来自另一台服务器的远程过程调用	48	关键字或选项: 客户端程序的名称 其它信息: 服务器名, 即从其执行 RPC 的计算机的主机名。
	到另一台服务器的远程过程调用	49	关键字或选项: 过程名称
security	connect to (仅限 CIS)	90	关键字或选项: connect to
	online database	83	—
	proc_role 函数 (从系统过程中执行)	80	其它信息: 所需的角色
	由 sso 重新生成口令	76	关键字或选项: 设置 SSO 口令 其它信息: 登录名
	角色切换	55	以前值: on 或 off 当前值: on 或 off 其它信息: 正在设置的角色名称
	服务器启动	50	其它信息: -dmasterdevicename -iinterfaces file path -Sservername -errorfilename
	sp_webservices	111	关键字或选项: deploy (如果配置一项 Web 服务)。deploy_all (如果配置所有 Web 服务)
	sp_webservices	111	关键字或选项: undeploy (如果取消配置一项 Web 服务)。undeploy_all (如果取消配置所有 Web 服务)
	服务器关闭	51	关键字或选项: shutdown
	set proxy 或 set session authorization	88	以前值: 以前的 suid 当前值: 新的 suid
	sp_configure	82	关键字或选项: SETCONFIG 其它信息: • 如果正在设置某一参数: 配置参数的数量 • 如果正在使用配置文件设置参数: 配置文件的名称
	sp_ssladmin (启用管理)	99	关键字包含 SSL_ADMIN addcert (如果添加认证)。
	审计表访问	61	—
	create login、drop login	103	关键字或选项: create login、drop login
	create、drop、alter、grant 或 revoke role	85	关键字或选项: create、drop、alter、grant 或 revoke role

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
	内置函数	86	关键字或选项: 函数的名称
	要审计的安全命令或访问, 尤其是使用 -u 选项启动 Adaptive Server 来解锁管理员帐户。	95	其它信息包含 “解锁管理员帐户”
	对 LDAP state changes 的更改	123	关键字或选项: 主 URL 状态和辅助 URL 状态 • 以前值 • 当前值 其它信息指示状态更改是自动发生还是由于手动输入的命令而发生的。
	系统或 sp_passwordpolicy 为网络口令加密进行的非对称密钥对重新生成	117	extrainfo 中的信息
select	从表中选择数据的 select 命令	62	关键字或选项: select into select readtext
	从视图中选择数据的 select 命令	63	关键字或选项: select into select readtext
setuser	setuser	84	其它信息: 正在设置的用户名称
table_access	delete	18	关键字或选项: delete
	insert	41	关键字或选项: insert
	select	62	关键字或选项: select into select readtext
	update	70	关键字或选项: update writetext
truncate	truncate table	64	—
transfer_table	transfer table	136	transfer table
unbind	sp_unbindefault	67	—
	sp_unbindmsg	69	—
	sp_unbindrule	68	—
unmount	unmount database	102	—
	create manifest file	116	extrainfo 中的信息

审计选项	将被审计的命令或权限	event	extrainfo 中的信息
update	对表执行的 update 命令	70	关键字或选项: update writetext
	对视图执行的 update 命令	71	关键字或选项: update writetext
view_access	delete	19	关键字或选项: delete
	insert	42	关键字或选项: insert
	select	63	关键字或选项: select into select readtext
	update	71	关键字或选项: update writetext

表 18-6 列出了 event 列中显示的值（按审计事件排列）。

表 18-6: 审计事件值

审计事件 ID	命令名	审计事件 ID	命令名
1	ad hoc audit record	62	select table
2	alter database	63	select view
3	alter table	64	truncate table
4	bcp in	65	保留
5	保留	66	保留
6	bind default	67	unbind default
7	bind message	68	unbind rule
8	bind rule	69	unbind message
9	create database	70	update table
10	create table	71	update view
11	create procedure	72	保留
12	create trigger	73	启用审计
13	create rule	74	禁用审计
14	create default	75	保留
15	create message	76	SSO 更改口令
16	create view	77	保留
17	access to database	78	保留
18	delete table	79	保留

审计事件 ID	命令名	审计事件 ID	命令名
19	delete view	80	执行的角色检查
20	disk init	81	dbcc
21	disk refit	82	配置
22	disk reinit	83	online database
23	disk mirror	84	setuser 命令
24	disk unmirror	85	UDR 命令
25	disk remirror	86	内置函数
26	drop database	87	磁盘释放
27	drop table	88	set SSA 命令
28	drop procedure	89	kill 或 terminate 命令
29	drop trigger	90	connect
30	drop rule	91	引用
31	drop default	92	命令文本
32	drop message	93	JCS install 命令
33	drop view	94	JCS remove 命令
34	dump database	95	解锁管理员帐户
35	dump transaction	96	quiesce database
36	致命错误	97	create SQLJ 函数
37	非致命错误	98	drop SQLJ 函数
38	存储过程的执行	99	SSL 管理
39	触发器的执行	100	disk resize
40	grant	101	mount database
41	insert table	102	unmount database
42	insert view	103	login 命令
43	load database	104	create index
44	load transaction	105	drop index
45	login	106	sp_encryption （加密列管理）
46	logout	107	create encryption key
47	revoke	108	Alter Encryption Key as/not default
48	rpc in	109	drop encryption key
49	rpc out	110 111	deploy user-defined web services undeploy user defined web services
50	server boot	112	登录已锁定

审计事件 ID	命令名	审计事件 ID	命令名
51	服务器关闭	113	quiesce hold security
52	保留	114	quiesce release
53	保留	115	口令管理
54	保留	116	create manifest file
55	角色切换	117	regenerate keypair
56	保留	118	alter encryptin key modify encryption
57	保留	119	alter encryption key add encryption
58	保留	120	alter encryption key drop encryption
59	保留	121	alter encryption key modify owner
60	保留	122	alter encryption key for key recovery
61	对审计表的访问	123	LDAP 状态更改
		127	错误日志管理
		136	transfer table

监控失败登录尝试次数

当登录帐户由于失败登录尝试次数超出配置次数而被锁定时，将记录审计选项 login_locked 和事件 Locked Login (value 112)。设置了审计选项 login_locked 即会启用此事件。若要设置 login_locked，请输入：

```
sp_audit "login_locked","all","all","ON"
```

如果审计表已满，并且无法记录事件，则会向错误日志发送包含相关信息的消息。

审计记录中包括主机名和网络 IP 地址。监控 Locked Login 事件（编号 112）的审计日志有助于确定对登录帐户的攻击。

审计登录失败

尽管客户端应用程序可能由于多种原因而登录失败，但 Adaptive Server 不会向这些应用程序提供任何有关登录失败的详细信息。这样可以避免将相关信息提供给企图破译口令或以其它方式违反 Adaptive Server 的鉴定机制的恶意用户。

但是，作为系统管理员，详细信息有助于诊断 Adaptive Server 的管理或配置问题，并可帮助安全员调查是否有人试图违反安全性机制。

以下命令可启用对所有登录失败的审计：

```
sp_audit "login", "all", "all", "fail"
```

为防止对信息的不适当的使用，只有被授予了 SSO 角色的用户才能访问包含此敏感信息的审计追踪信息。

Adaptive Server 将审计以下情况下的登录失败：

- 对于作为 Windows 服务启动的 Adaptive Server，如果 Sybase SQLServer 服务已暂停（例如，由 Microsoft Management Console for Services 暂停）。
- 如果远程服务器尝试建立服务器到服务器 RPC 的节点处理器，但资源不足（或此处列出的任何其它情况）导致节点处理器初始化失败。
- 对 Adaptive Server for Windows 使用“受托登录”或“统一登录”配置，但指定的用户不是受托管理员（即鉴定失败）。
- Adaptive Server 不支持客户端请求的 SQL 接口。
- 用户试图在单用户模式下登录到 Adaptive Server。在单用户模式下，只允许一个具有 sa_role 的用户登录到 Adaptive Server。其它登录会被阻止，即使用户具有 sa_role。
- 主数据库中的 syslogins 表无法打开，表明主数据库具有内部错误。
- 客户端试图远程登录，但 sysremotelogins 无法打开，或指定用户帐户没有任何条目且不存在任何 Guest 帐户。
- 客户端试图远程登录，虽然它在 sysremotelogins 中找到引用指定用户的本地帐户的条目，但引用的本地帐户不存在。
- 客户端程序请求安全会话（例如 Kerberos 鉴定），但由于以下原因无法建立安全会话：
 - Adaptive Server 安全子系统未在启动时初始化。
 - 没有足够的内存资源来存储分配的结构。
 - 鉴定协商失败。

- 未找到针对指定用户的鉴定机制。
- 指定的口令不正确。
- **syslogins** 不包含指定登录所需的条目。
- 登录帐户被锁定。
- **Adaptive Server** 已达到了它对用户连接数量的限制。
- 设置了配置参数 **unified login required**，但相应的安全子系统未鉴定登录。
- **Adaptive Server** 的网络缓冲区不可用，或请求的包大小无效。
- 客户端应用程序请求基于主机的通信套接字连接，但没有用于基于主机的通信缓冲区的内存资源。
- 正在关闭，但指定用户没有 **sa** 角色。
- **Adaptive Server** 无法打开缺省数据库进行登录，且此登录没有对 **master** 数据库的访问权限。
- 客户端发出了高可用性登录故障切换请求，但高可用性子系统没有对此登录的高可用性会话，或此登录无法等待故障切换完成。
- 客户端请求高可用性登录设置，但高可用性子系统无法创建会话，或无法完成对高可用性会话的 **TDS** 协议协商。
- **Adaptive Server** 无法设置 **tempdb** 进行登录。
- 检测到 **TDS** 登录协议错误。

数据的保密性

本章介绍如何配置 Adaptive Server 以确保所有数据都是安全和保密的。

主题	页码
Adaptive Server 中的安全套接字层 (SSL)	627
Kerberos 保密性	646
转储和装载数据库时使用口令保护	646

Adaptive Server 中的安全套接字层 (SSL)

Adaptive Server Enterprise 安全服务现在支持安全套接字层 (SSL) 的基于会话的安全性。SSL 是一种用于保护通过 Internet 传输敏感信息（例如信用卡号、股票交易和银行交易）的标准。

虽然全面讨论公开密钥密码术超出该文档的范围，但是基本的信息值得说明一下，以便您对 SSL 如何保护 Internet 通信信道有所了解。该文档不是一个关于公开密钥密码术的综合指南。

Adaptive Server SSL 功能的实现基于以下假定：有一名知识渊博的系统安全员，他熟悉安全性策略和您节点的需要，以及对 SSL 和公用密钥密码术有一般性的了解。

因特网通信概述

TCP/IP 是在客户端 / 服务器计算中用到的主要传输协议，也是管理因特网上数据传输的协议。**TCP/IP** 使用中间的计算机将数据从发送者传输到接收者。中间计算机将易于篡改、偷窃、偷听和模拟的不安全连接引入通信系统。

公开密钥密码术

现在人们已经开发出几种机制并用以保护通过 **Internet** 传输的敏感数据，这些机制统称为**公开密钥密码术**。公开密钥密码术由加密、键交换、数字签名和数字认证组成。

加密

加密是使用密码算法对信息进行编码的过程，以防指定接收者以外的人利用这些信息。用于加密的密钥类型有两种：

- **对称密钥加密** — 用相同算法（密钥）来对消息进行加密和解密。这种形式的加密安全性最差，由于密钥非常简单，因此也就容易解译。不过，因为这种形式加密和解密消息所需的计算最少，所以使用对称密钥加密的数据的传输速度很快。
- **公开 / 私有密钥加密** — 也称作非对称密钥，是由公开和私有组件组成、用来对消息进行加密和解密的一对密钥。虽说可能有所不同，但通常来说，消息都是由发送者使用私有密钥加密，而由接收者使用发送者的公开密钥解密。您可以使用接收者的公开密钥来对消息进行加密，然后接收者使用自己的私有密钥对消息进行解密。

用来创建公开和私有密钥的算法更复杂，因此更不容易破译。但是，公开 / 私有密钥加密需要更多的计算、需要通过连接发送更多的数据，因而数据传输速度会明显降低。

键交换

减少计算开销同时加快事务处理速度，而又不牺牲安全性的方案是：综合使用对称密钥和公开 / 私有密钥加密，即所谓的“键交换”。

对于大量数据，用对称密钥来加密原始消息。然后，发送者使用自己的私有密钥或接收者的公开密钥来加密对称密钥。加密消息和加密过的对称密钥都将发送给接收者。根据用于加密消息的密钥（公开或私有），接收者使用相应的策略来解密对称密钥。一旦键被交换，接收者使用对称密钥来解密消息。

数字签名

数字签名用于篡改检测和不否认功能。数字签名通过数学算法创建，从文本消息生成唯一的、固定长度的数字字符串；其结果称作散列或消息摘要。

为了确保消息完整性，将使用签名者的私有密钥对消息摘要进行加密，然后将消息摘要和有关散列算法的信息一起发送给接收者。接收者用签名者的公开密钥对该消息进行解密。此过程还会重新生成原始消息摘要。如果该摘要匹配，则该消息完整且没被篡改。如果不匹配，则数据在转接过程中被更改，或者是被冒名者签名。

此外，数字签名提供**不否认**功能 — 发送者不能拒绝或否认他们发送了消息，因为他们的私有密钥对消息进行了加密。很显然，如果私有密钥产生危险（被偷窃或解译），则对于“不否认”而言，数字签名将变得毫无价值。

数字认证

数字认证类似于护照：一旦分配给您一个认证，权威部门会有您在系统中的所有标识（身份）信息。与护照类似，认证可用来检验一个实体（服务器、路由器及 Web 站点等）对另一个实体的标识。

Adaptive Server 使用两种类型的认证：

- **服务器认证** — 服务器认证对持有该认证的服务器进行鉴定。认证由受托第三方证书发放机构 (CA) 发布。CA 验证拥有者的标识，将拥有者的公开密钥和其它鉴定信息嵌入到数字认证中。认证也包含发布 CA、验证所含数据的完整性，以及检验其使用状况的数字签名。
- **CA 认证**（也称为**受托根认证**） — 是服务器在启动时装载的受托 CA 的列表。当服务器作为客户端运行时，例如在远程过程调用 (RPC) 期间，服务器将使用 CA 认证。Adaptive Server 在启动时装载 CA 受托根认证。为 RPC 连接到远程服务器后，Adaptive Server 将验证签署远程服务器认证的 CA 是否为列在其自己的 CA 受托根文件中的“受托”CA。如果不是，则连接失败。

认证在一段时期内有效，CA 可以因为多种原因撤消该认证，例如当出现安全问题时。如果一个认证在会话期间被撤消，则会话连接继续。以后的登录尝试将失败。同样，当认证到期后，登录尝试将失败。

这些机制的联合使用保护了在因特网上传输的数据免遭窃取和篡改。这些机制也保护用户免受其他用户欺骗，即一个实体假装成另一个实体（电子欺骗），或者一个人或组织为了特定目的而充当别的用户，其真实企图是获得私有信息（误传）。

SSL 概述

SSL 是一个通过安全网络连接发送在线级 (wire-level) 或套接字级 (socket-level) 加密的数据的行业标准。

建立 SSL 连接之前，服务器和客户端交换一系列 I/O 往返，就安全性加密会话达成一致。该过程称为 “SSL 握手”。

SSL 握手

客户端请求一个连接时，在传输数据前，启用 SSL 的服务器提出认证以证实客户端的标识。“握手”主要由以下步骤组成：

- 客户端向服务器发送连接请求。该请求包括客户端所支持的 SSL（或传送层安全性，TLS）选项。
- 服务器返回其认证和所支持的密码成套程序列表，该列表包括 SSL/TLS 支持选项、键交换所用算法和数字签名。
- 当客户端和服务器就 CipherSuite 达成一致后，将建立一个安全、加密会话。

有关 **SSL 握手**和 SSL/TLS 协议的更详细信息，请参见位于 <http://www.ietf.org> 的“互联网工程任务组” (Internet Engineering Task Force) 网站。

有关 Adaptive Server 支持的密码成套程序的列表，请参见第 639 页的“**密码成套程序**”。

Adaptive Server 中的 SSL

Adaptive Server 的 SSL 实现提供了几种级别的安全性。

- 服务器鉴定自身 — 证实它是否是您所要联系的服务器，并在数据传输之前加密 SSL 会话。
- 一旦 SSL 会话建立后，要求连接的客户便可以通过此安全、加密的连接发送他的用户名和口令。
- 服务器认证时对数字签名进行比较，这样可以确定客户端所收到的数据在到达预期接收者之前是否被修改过。

在大多数平台上，Adaptive Server 使用 Certicom Corp. 提供的 SSL Plus(TM) library API。但是，对于 Windows Opteron X64，Adaptive Server 使用 OpenSSL 作为 SSL 提供程序。

SSL 过滤器

Adaptive Server 目录服务（例如 *interfaces* 文件、Windows 注册表或 LDAP 服务）定义了服务器地址和端口号，并且确定为客户端连接而强制执行的安全协议。Adaptive Server 将 SSL 协议作为过滤器来执行，附加到目录服务的 *master* 行和 *query* 行。

Adaptive Server 在其上接受连接的地址和端口号是可配置的，因此您可以为单服务器启用多网络和安全协议。服务器连接属性由目录服务（如 LDAP）指定，或者由传统 Sybase *interfaces* 文件指定。请参见第 636 页的“创建服务器目录条目”。

所有尝试到具有 **SSL 过滤器** 的 *interfaces* 文件中 *master* 或 *query* 条目的连接都必须支持 SSL 协议。服务器可以配置为接受 SSL 连接，并且可拥有其它接受明码通信报文（未加密的数据）或使用其它安全性机制的连接。

例如，UNIX 上的 *interfaces* 文件，它既支持基于 SSL 的连接，也支持与下面类似的明文连接：

```
SYBSRV1
master tcp ether myhostname myport1 ssl
query   tcp ether myhostname myport1 ssl
master tcp ether myhostname myport2
```

与使用 *interfaces* 文件（Windows 上为 *sql.ini*）中的 SECMECH（安全性机制）行定义的其它安全性机制（例如 DCE 和 Kerberos）相比，SSL 过滤器有所不同。

通过认证进行的鉴定

SSL 协议需要通过服务器认证的服务器鉴定来启用加密会话。同样，当 Adaptive Server 在 RPC 期间作为客户端运行时，必须有一个受托 CA 存储库，客户端连接可以访问该库以验证服务器认证。

服务器认证

每个 Adaptive Server 必须拥有自己的服务器认证文件，该文件在启动时装载。下面是认证文件的缺省位置，其中 *servername* 是启动过程中使用 *-s* 标志在命令行上指定或通过环境变量 *\$DSLISTEN* 指定的 Adaptive Server 的名称。

UNIX *\$SYBASE/\$SYBASE_ASE/certificates/servername.crt*

Windows *%SYBASE%\%SYBASE_ASE%\certificates\servername.crt*

服务器认证文件由编码数据组成，包含服务器的认证和服务器认证的加密私有密钥。

或者，可以在使用 `sp_ssladmin` 时指定服务器认证文件的位置。

注释 若要成功进行客户端连接，认证中的公用名必须与 `interfaces` 文件中的 Adaptive Server 名称匹配。

CA 受托根认证

Adaptive Server 在启动时从受托根文件装载受托 CA 列表。受托根文件在格式上与认证文件类似，只是受托根文件包含 Adaptive Server 所知的 CA 认证。本地 Adaptive Server 可在以下文件中访问受托根文件，其中 `servername` 是服务器的名称：

- UNIX — `$SYBASE/$SYBASE_ASE/certificates/servername.txt`
- Windows — `%SYBASE%\%SYBASE_ASE\certificates\servername.txt`

仅当 Adaptive Server 作为客户端运行时（例如 RPC 调用或组件集成服务 (CIS) 连接时），才会使用受托根文件。

系统安全员使用标准 ASCII 文本编辑器添加和删除 Adaptive Server 所要接受的 CA。

警告！ 使用 Adaptive Server 内的系统安全员角色 (`sso_role`) 来限制访问和执行安全性敏感的对象。

Adaptive Server 提供工具以产生认证请求和批准认证。请参见第 635 页的“使用 Adaptive Server 工具请求和授权认证”。

连接类型

该节说明不同的客户端到服务器和服务器到服务器连接。

客户机登录到
Adaptive Server

Open Client 应用程序建立与 Adaptive Server 的套接字连接，类似于建立现有的客户端连接的方式。在传输任何用户数据之前，当客户端完成网络传送级连接调用且服务器端完成接受调用时，在套接口上将产生“SSL 握手”。

服务器到服务器的远程
过程调用

Adaptive Server 为 RPC（远程过程调用）建立的到另一服务器的套接字连接的方式，与现有 RPC 建立的连接方式相同。在传输任何用户数据之前，当网络传送级连接调用完成时，在套接口上将产生“SSL 握手”。如果已经建立服务器到服务器套接字连接，那么现有套接字连接和安全性环境将被再次使用。

Adaptive Server 在 RPC 期间作为客户端运行时，它会在连接过程中请求远程服务器的认证。然后 Adaptive Server 验证签署远程服务器认证的 CA 是否受托；也就是说，验证该 CA 是否位于受托根文件中其自己受托 CA 的列表上。同时也验证服务器认证中的公用名是否与建立连接时使用的公用名匹配。

协同服务器和 SSL

可以使用协同服务器为故障切换配置 Adaptive Server。必须用相同的 SSL 和 RPC 配置参数来配置主服务器和辅助服务器。当连接进行故障切换或故障恢复时，连接将重新建立安全性会话。

Open Client 连接

组件集成服务、RepAgent、分布式事务管理和其它 Adaptive Server 中的模块，使用 Client-Library 来建立与服务器（除了 Adaptive Server 外）的连接。远程服务器由其自身的认证体系来进行鉴定。远程服务器使用用户名和口令鉴定用于 RPC（远程过程调用）的 Adaptive Server 客户端连接。

启用 SSL

Adaptive Server 确定对于基于接口文件（Windows 的 *sql.ini*）的端口将使用何种安全服务。

❖ 启用 SSL

- 1 生成服务器的认证。
- 2 创建受托根文件。
- 3 使用 `sp_configure` 启用 SSL。从命令提示符中输入：


```
sp_configure "enable ssl", 1
```

 - 1 — 在启动时启用 SSL 子系统，分配内存，SSL 在网络上对数据执行线级加密。
 - 0（缺省值） — 禁用 SSL。此值为缺省值。
- 4 将 SSL 过滤器添加到 *interfaces* 文件中。请参见第 636 页的“[创建服务器目录条目](#)”。
- 5 使用 `sp_ssladmin` 将认证添加到认证文件中。请参见第 637 页的“[管理认证](#)”。
- 6 关闭并重新启动 Adaptive Server。

注释 若要请求、授权和转换第三方认证，请参见《实用程序指南》了解有关 `certauth`、`certreq` 和 `certpk12` 工具的信息。

与其它安全服务（例如 DCE、Kerberos 和 NTLAN）不同，SSL 既不依赖于 Open Client/Open Server 配置文件 *libtcl.cfg* 的“Security”部分，也不依赖于 *objectid.dat* 中的对象。

系统管理员在规划总物理内存时应考虑 SSL 使用的内存。Adaptive Server 中的每个连接（连接包含用户连接、远程服务器和网络监听器）大概需要 40K 才能进行 SSL 连接。内存保留和预分配在内存池中，当需要时由 Adaptive Server 和 SSL Plus libraries 在内部使用。

获得认证

系统安全员通过以下方式为 Adaptive Server 安装服务器认证和私有密钥：

- 使用与已经配置在客户环境下的现有公开密钥基础结构一起提供的第三方工具。
- 将 Adaptive Server 认证请求工具与受托第三方 CA 一起使用。

要获得认证，您必须从 CA 请求认证。如果从第三方请求认证，而且认证的格式是 PKCS #12，请使用 `certpk12` 实用程序将认证转换为 Adaptive Server 理解的格式。

为测试 Adaptive Server 认证请求工具，以及验证鉴定方法是否可以工作于您的服务器上，Adaptive Server 提供了一个供测试用的工具，该工具允许用户服务器作为 CA 运行以及向本机发布 CA 签署的认证。

创建用于 Adaptive Server 认证的主要步骤为：

- 1 生成公开和私有密钥对。
- 2 将私有密钥存储在安全的地方。
- 3 生成认证请求。
- 4 向 CA 发送认证请求。
- 5 CA 签署和返回认证后，把认证存储在文件中，然后对认证附加私有密钥。
- 6 把认证存储在 Adaptive Server 安装目录下。

请求认证的第三方工具

大多数第三方 PKI 供应商和一些浏览器包含生成认证和私有密钥的实用程序。通常，这些实用程序的形式为图形向导，它通过一系列问题提示您来定义认证的区分名和公用名。

遵照向导提供的指导来创建认证请求。一旦收到已签署的 PKCS #12 格式的认证，请使用 `certpk12` 生成认证文件和私有密钥文件。将两个文件并置到 `servername.crt` 文件（其中 `servername` 是服务器名）中，然后将该文件放置在 `$$SYBASE/$$SYBASE_ASE` 下的 `certificates` 目录中。请参见《实用程序指南》。

使用 Adaptive Server 工具请求和授权认证

Adaptive Server 提供两个用于请求和授权认证的工具。`certreq` 生成公开和私有密钥对以及认证请求。`certauth` 将服务器认证请求转换为 CA 签署的认证。

警告！ 仅将 `certauth` 作为测试之用。Sybase 建议您使用商业 CA 的服务，因为它对根认证的完整性提供了保护，而且由普遍公认的 CA 签署的认证容易移植到使用鉴定的客户端认证环境下。

准备服务器受托根认证的过程包含五个步骤。执行前两个步骤来创建测试受托根认证，以便您可以验证用户是否能够创建服务器认证。获得测试 CA 认证（受托根认证）后，重复执行步骤 3 到步骤 5 以签署服务器认证。

- 1 使用 `certreq` 请求认证。
- 2 使用 `certauth` 将认证请求转换为 CA 自签的认证（受托根认证）。
- 3 使用 `certreq` 请求服务器认证和私有密钥。
- 4 使用 `certauth` 将认证请求转换为 CA 签署的服务器认证。
- 5 将私有密钥文本附加到服务器认证，并将该认证存储在服务器安装目录中。

注释 Adaptive Server 在 `$$SYBASE/$SYBASE_OCS/bin` 目录中包括 `openssl` 开放源代码实用程序。使用 `openssl` 可完成由 `certreq`、`certauth` 和 `certpk12` 实现的所有认证管理任务。Sybase 包含此二进制程序是为了方便起见，对该使用二进制程序所引致的任何问题概不负责。有关详细信息，请参见 www.openssl.org。

有关 Sybase 实用程序，即用于请求、授权和转换第三方认证的 `certauth`、`certreq` 和 `certpk12` 的信息，请参见《实用程序指南》。

注释 `certauth` 和 `certreq` 依赖于 RSA 和 DSA 算法。这些工具仅用于 `crypto` 模块，该模块使用 RSA 和 DSA 算法来构造认证请求。

创建服务器目录条目

Adaptive Server 接受客户端登录和服务器到服务器的 RPC。Adaptive Server 接受连接的地址和端口号是可配置的，因此可以指定多网络、不同的协议和替代端口。

在 *interfaces* 文件中，SSL 被指定为 master 和 query 行上的过滤器，而诸如 DCE 或 Kerberos 等安全性机制则使用 SECMECH 行标识。以下示例显示在 UNIX 环境下，使用 SSL 的 Adaptive Server 的，基于 TLI 的条目：

UNIX 上使用 SSL 和 DCE 安全性机制的 Adaptive Server 的条目可能类似于：

```
SYBSRV1
master tcp ether myhostname myport1 ssl
query   tcp ether myhostname myport1 ssl
master tcp ether myhostname myport2
SECMECH 1.3.6.1.4.897.4.6.1
```

Windows 上使用 SSL 和 Kerberos 安全性机制的 Adaptive Server 的条目可能类似于：

[SYBSRV2]

```
query=nlwmsck, 18.52.86.120,2748,ssl
master=nlwmsck 18.52.86.120,2748,ssl
master=nlwmsck 18.52.86.120,2749
secmech=1.3.6.1.4.897.4.6.6
```

示例中 SYBSRV1 和 SYBSRV2 的 SECMECH 行包含对象标识符 (OID)，它分别表示安全性机制 DCE 和 Kerberos。OID（对象标识符）的值在以下文件中定义：

- UNIX — *\$SYBASE/\$SYBASE_OCS/config/objectid.dat*
- Windows — *%SYBASE%\%SYBASE_OCS\ini\objectid.dat*

这些示例中，SSL 安全服务在端口号 2748(0x0abc) 上指定。

注释 同时使用 SSL 和 SECMECH 安全性机制的目的是便于从 SECMECH 迁移到 SSL 安全性。

管理认证

要管理 Adaptive Server 中的 SSL 和认证，请使用 `sp_ssladmin`。`sso_role` 是执行存储过程所必需的。

`sp_ssladmin` 用于：

- 增加本地服务器认证。可以添加认证和指定用于加密私有密钥的口令，或者在启动期间要求在命令行上输入口令。
- 删除本地服务器认证。
- 列出服务器认证。

`sp_ssladmin` 的语法为：

```
sp_ssladmin {[addcert, certificate_path [, password|NULL]]
             [dropcert, certificate_path]
             [lscert]
             [help]}
             [lsciphers]
             [setciphers, {"FIPS" | "Strong" | "Weak" | "All"
                           | quoted_list_of_ciphersuites}]
```

例如：

```
sp_ssladmin addcert, "/sybase/ASE-12_5/certificates/Server1.crt",
               "mypassword"
```

此示例为本地服务器添加一个条目，即 *Server1.crt*，该条目位于绝对路径 */sybase/ASE-12_5/certificates*（Windows 上为 *x:\sybase\ASE-12_5\certificates*）下的认证文件中。私有密钥用口令 “*mypassword*” 进行加密，加密口令应为在创建私有密钥时指定的口令。

接受认证之前，`sp_ssladmin` 验证：

- 可以使用提供的口令对私有密钥解密（被指定为 NULL 时除外）。
- 认证中的私有密钥和公开密钥匹配。
- 从根 CA 到服务器认证的认证链有效。
- 认证中的公用名与 *interfaces* 文件中的公用名匹配。

如果公用名不匹配，`sp_ssladmin` 发出警告。如果其它标准失败，则不会将认证添加到认证文件中。

警告！ Adaptive Server 将口令限制为 64 个字符。此外，某些平台在创建服务器认证时限制有效口令的长度。在以下限制范围内选择口令：

- Sun Solaris — 32 位和 64 位平台，256 个字符。
 - Linux — 128 个字符。
 - IBM — 32 位和 64 位平台，32 个字符。
 - HP — 32 位和 64 位平台，8 个字符。
 - Windows — 256 个字符。
-

使用 NULL 作为口令的目的是在 SSL 加密会话开始之前的初始配置 SSL 期间保护口令。因为还没有配置 SSL，所以连接过程中口令没有加密。第一次登录时，通过将口令指定为 NULL 可以避免上述情况。

口令为 NULL 时，您必须使用 `-y` 标志启动 `dataserver`，该标志在命令行提示系统管理员输入私有密钥口令。

在建立了 SSL 连接并且重新启动了 Adaptive Server 后，再次使用 `sp_ssladmin`，这一次使用实际口令。这时，Adaptive Server 将加密并存储口令。以后从命令行启动 Adaptive Server 都要使用加密的口令；启动期间不必在命令行指定口令。

第一次登录时使用 NULL 口令的另一种替代方法是，通过 `isql` 避免远程连接到 Adaptive Server。可以指定 “localhost” 作为 *interfaces* 文件（Windows 上为 *sql.ini*）中的 *hostname*，以防止客户端以远程方式连接。只能建立本地连接，并且口令绝不会通过网络连接传送。

注释 Adaptive Server 在其网络内存池中有足够的内存，从而允许 `sp_ssladmin addcert` 使用其缺省内存分配来设置认证和私有密钥口令。但是，如果另一网络内存消耗程序已被分配了缺省网络内存，则 `sp_ssladmin` 可能会失败并向客户端显示以下错误：

```
Msg 12823, Level 16, State 1:
Server 'servername', Procedure 'sp_ssladmin', Line 72:
Command 'addcert' failed to add certificate path
/work/REL125/ASE-12_5/certificates/servername.crt,
system error: ErrMemory.
(return status = 1)
```

或者可能在错误日志中显示以下消息：

```
... ssl_alloc: Cannot allocate using
ubfalloc(rnetmempool, 131072)
```

一种解决方法是：您可以增加 `additional network memory` 配置参数。Adaptive Server 需要大约 500K 字节的内存才能使 `sp_ssladmin addcert` 成功，因此将额外的网络内存增大到该数量可能会使其成功。网络内存池在需要时会重用该内存，或者您可以在 `sp_ssladmin` 成功完成后将 `additional network memory` 恢复为它以前的值。

性能

建立安全会话需要额外的开销，因为数据加密后数据的大小将增加，而且需要额外的计算加密或解密信息。SSL 的额外内存要求将使用于网络吞吐量或建立连接的开销增加 50%-60%。每个用户连接必须有大约 40K 或更多的内存。

密码成套程序

SSL 握手期间，客户端和服务器通过密码成套程序对安全性协议达成一致。**密码成套程序**是启用 SSL 的应用程序所使用的密钥交换算法、散列方法和加密方法的优先列表。有关密码成套程序的完整说明，请访问位于 <http://www.ietf.org/rfc/rfc2246.txt> 的“互联网工程任务组”（Internet Engineering Task Force, IETF）组织。

缺省情况下，客户端和服务器均支持的最强大密码成套程序是用于基于 SSL 会话的密码成套程序。

Adaptive Server 支持对 SSL Plus library API 和密码引擎 Security Builder™（均由 Certicom Corp. 提供）都可用的密码成套程序。

注释 列出的密码成套程序符合传送层规范 (TLS)。TLS 是 SSL 3.0 的增强版本，并且是 SSL 3.0 版密码成套程序的一个别名。

@@ssl_ciphersuite

通过 Transact-SQL 全局变量 @@ssl_ciphersuite, 用户可以了解 SSL 握手选择了哪个密码成套程序, 并验证建立的连接是否为 SSL 连接。

Adaptive Server 在 SSL 握手完成时设置 @@ssl_ciphersuite。其值可以是 NULL (表示非 SSL 连接), 或包含 SSL 握手选择的密码成套程序的名称的字符串。

例如, 使用 SSL 协议的 isql 连接会显示为其选择的密码成套程序。

```
1> select @@ssl_ciphersuite
2> go
```

输出:

```
-----
TLS_RSA_WITH_AES_128_CBC_SHA

(1 row affected)
```

设置 SSL 密码成套程序优先选项

在 Adaptive Server 中, sp_ssladmin 具有两个命令选项, 用于显示和设置密码成套程序优先选项: lsciphers 和 setciphers。使用这些选项, 可以限制 Adaptive Server 使用的密码成套程序集, 这样, 系统安全员便能够控制客户端到服务器的连接或 Adaptive Server 的出站连接可使用的加密算法的种类。在 Adaptive Server 中, 缺省根据内部定义的密码成套程序优先选项集来使用 SSL 密码成套程序, 这一点与早期版本中相同。

若要显示任何设置的密码成套程序优先选项的值, 请输入:

```
sp_ssladmin lsciphers
```

若要设置特定的密码成套程序优先选项, 请输入:

```
sp_ssladmin setciphers, {"FIPS" | "Strong" | "Weak" |
    "All" | quoted_list_of_ciphersuites }
```

其中:

- "FIPS" — 是符合 FIPS 的加密算法、散列算法和密钥交换算法的集合。此列表包括的算法有 AES、3DES、DES 和 SHA1。
- "Strong" — 是所用密钥长度大于 64 位的加密算法的集合。
- "Weak" — 是所有支持的密码成套程序集中未包括在 strong 集合内的加密算法的集合。

- "All" — 是缺省密码成套程序的集合。
- quoted_list_of_ciphersuites — 以逗号分隔的列表形式指定密码成套程序集（按优先顺序排序）。该列表首尾用引号（"）括起。此带引号的列表可以包含任何预定义集合以及单个密码成套程序名称。未知的密码成套程序名称将导致报告错误，但对优先选项无影响。

第 641 页的表 19-1 中包含预定义集合的详细内容。

sp_ssladmin setciphers 将密码成套程序优先选项设置为给定的有序列表。这样可将可用的 SSL 密码成套程序限制为 "FIPS"、"Strong"、"Weak"、"All" 的指定集合或带引号的密码成套程序列表。此设置会在下一个监听器启动时生效，并且需要您重新启动 Adaptive Server 以确保所有监听器都使用新设置。

您可以显示已经使用 sp_ssladmin lsciphers 设置的任何密码成套程序优先选项。如果没有设置任何优先选项，sp_ssladmin lsciphers 将返回 0 行，表示未设置任何优先选项，并且 Adaptive Server 将使用其缺省（内部）优先选项。

表 19-1: Adaptive Server 中的预定义密码成套程序

集名称	集中包含的密码成套程序名称
FIPS	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_DES_CBC_SHA
	TLS_DHE_DSS_WITH_DES_CBC_SHA
	TLS_DHE_RSA_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
Strong	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_RC4_128_MD5
	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
	TLS_DHE_DSS_WITH_RC4_128_SHA
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

集名称	集中包含的密码成套程序的名称
Weak	TLS_RSA_WITH_DES_CBC_SHA
	TLS_DHE_DSS_WITH_DES_CBC_SHA
	TLS_DHE_RSA_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
	TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA
	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT_WITH_RC4_40_MD5
	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
All	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_RC4_128_MD5
	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
	TLS_DHE_DSS_WITH_RC4_128_SHA
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_DES_CBC_SHA
	TLS_DHE_DSS_WITH_DES_CBC_SHA
	TLS_DHE_RSA_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
	TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA
	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
	TLS_RSA_EXPORT_WITH_RC4_40_MD5
	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

表 19-2 介绍了 Adaptive Server 15.0 和更高版本不再支持的密码成套程序。15.0. 如果尝试使用任何删除的密码成套程序，将导致 SSLHandshake 失败，并且无法连接到 Adaptive Server。

表 19-2: 删除的密码成套程序

集名称	集中删除的密码成套程序的名称
FIPS	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
Strong	未删除
Weak	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
其它	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 TLS_DH_anon_WITH_3DES_EDE_CBC_SHA TLS_DH_anon_WITH_DES_CBC_SHA TLS_DH_anon_WITH_RC4_128_MD5 TLS_RSA_WITH_NULL_MD5 TLS_RSA_WITH_NULL_SHA

sp_ssladmin 示例

初始启动时，在设置任何密码成套程序优先选项之前， sp_ssladmin lscipher 不会显示任何优先选项。

```
1> sp_ssladmin lscipher
2> go
```

输出:

```
Cipher Suite Name      Preference
-----
(0 rows affected)
(return status = 0)
```

以下示例指定使用 FIPS 算法的密码成套程序集。

```
1> sp_ssladmin setcipher, 'FIPS'
```

The following cipher suites and order of preference are set for SSL connections:

Cipher Suite Name	Preference
-----	-----
TLS_RSA_WITH_AES_256_CBC_SHA	1
TLS_RSA_WITH_AES_128_CBC_SHA	2
TLS_RSA_WITH_3DES_EDE_CBC_SHA	3
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	4
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	5
TLS_RSA_WITH_DES_CBC_SHA	6
TLS_DHE_DSS_WITH_DES_CBC_SHA	7
TLS_DHE_RSA_WITH_DES_CBC_SHA	8
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	9
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	10

sp_ssladmin 输出优先选项 0（零）表示 Adaptive Server 未使用密码成套程序。如果输出的是其它非零值，则该数值表示 Adaptive Server 在 SSL 握手过程中使用该算法的优先顺序。SSL 握手的客户端选择这些密码成套程序中与其接受的密码成套程序的列表匹配的一个密码成套程序。

此示例使用带引号的密码成套程序列表来设置 Adaptive Server 中的优先选项：

```
1> sp_ssladmin setcipher, 'TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA'
2> go
The following cipher suites and order of preference are set for SSL connections:
Cipher Suite Name                                     Preference
-----
TLS_RSA_WITH_AES_128_CBC_SHA                           1
TLS_RSA_WITH_AES_256_CBC_SHA                           2
```

其它注意事项

升级到 Adaptive Server 12.5.3 版及更高版本时，密码成套程序优先选项为服务器缺省值，并且 sp_ssladmin 选项 lscipher 不显示任何优先选项。服务器使用其缺省优先选项，这些优先选项由 "All" 定义。系统安全员应考虑在其节点使用的安全性策略以及可用的 SSL 密码成套程序，以决定是否限制密码成套程序，以及哪些密码成套程序适合于安全性策略。

如果从 Adaptive Server 12.5.3 版及更高版本升级，并且设置了密码成套程序优先选项，则这些优先选项会在升级后保留。升级完成后，查看具有当前安全性策略的服务器的密码成套程序优先选项，以及在表 19-1 中找到的受支持和不受支持的密码成套程序列表。忽略任何不受支持的密码成套程序。

如果已设置 SSL 密码成套程序优先选项，并且需要从服务器上删除所有优先选项并使用缺省优先选项，请使用下列命令，将优先选项从其在系统目录中的存储位置中删除：

```
1> sp_configure 'allow updates to system tables', 1
2> go

1> delete from master..sysattributes where class=24
2> go

1> sp_configure 'allow updates to system tables', 0
2> go
```

只有系统安全员或系统管理员才能执行这些命令。

使用 SSL 指定公用名

目录服务条目中指定的服务器名可与 SSL 服务器认证用于执行 SSL 握手的公用名不同。这样，您将能够为 SSL 认证公用名使用完全限定域名（例如，*server1.bigcompany.com*）。

若要将公用名添加到 *interfaces* 文件中，请使用：

```
ase1
master tcp ether host_name port_number ssl="CN='common_name'"
query tcp ether host_name port_number ssl="CN='common_name'"
```

当客户端使用 SSL 连接到同样使用 SSL 的 Adaptive Server 时，将在 *interfaces* 文件中的端口号后面放置 SSL 过滤器。目录服务包括您使用 *dsedit* 或文本编辑器添加的公用名。

使用 *sp_listener* 指定公用名

sp_listener 包括 *CN=common_name* 参数，从而使您能够为 SSL 认证指定公用名。语法为：

```
sp_listener 'command','[protocol:]machine_name:port_number.
"CN=common_name"', 'engine_number'
```

其中，只有当将 *ssltcp* 指定为协议时，才使用 *CN=common_name*。将依据 SSL 认证中的 *common_name* 对您在此处指定的 *common_name* 进行验证。如果未包括 *CN=common_name*，Adaptive Server 将使用 *server_name*，依据 SSL 认证中的公用名进行验证。如果在认证中包括完全限定域名，该名称必须与 *CN=common_name* 匹配。

属性名“CN”不区分大小写（可为“CN”、“cn”或“Cn”），但公用名的属性值区分大小写。

例如，若要指定公用名 *ase1.big server 1.com*：

```
sp_listener 'start','ssltcp:blade1:17251:"CN=ase1.big server 1.com"', '0'
```

请参见《参考手册：过程》，了解有关 *sp_listener* 的详细信息。

存储过程 *sp_addserver* 已更改

filter 参数得以增强，可以指定公用名。请参见《参考手册：过程》。

Kerberos 保密性

您还可以使用 **Adaptive Server** 确保所有消息的保密性。若要要求对进出 **Adaptive Server** 的所有消息进行加密，请将 **msg confidentiality reqd** 配置参数设置为 1。如果此参数为 0（缺省值），则不要求消息的保密性，但客户端仍可以建立消息保密性。

例如，若要要求对所有消息进行加密，请执行：

```
sp_configure "msg confidentiality reqd", 1
```

有关使用 **Message Confidentiality with Kerberos** 和其它受支持的安全服务的详细信息，请参见第 453 页的“[管理基于网络的安全性](#)”。

转储和装载数据库时使用口令保护

可以使用 **dump database** 命令的 **password** 参数保护数据库转储，使其免于未经授权的装载。如果在进行数据库转储时包括了 **password** 参数，则在装载该数据库时，也必须提供相同的口令。

口令保护的 **dump database** 和 **load database** 命令的部分语法为：

```
dump database database_name to file_name [ with passwd = password ]  
load database database_name from file_name [ with passwd = password ]
```

其中：

- *database_name* — 是所转储或装载的数据库的名称。
- *file_name* — 是转储文件的名称。
- *password* — 是您提供的口令，用于保护转储文件免于被未经授权的用户使用。

口令长度必须介于 6 到 30 个字符之间。如果提供的口令少于 6 个字符或多于 30 个字符，**Adaptive Server** 将发出错误消息。如果在尝试装载数据库时发出了不正确的口令，**Adaptive Server** 将发出错误消息，并且命令将失败。

例如，以下命令将使用口令“bluesky”来保护 pubs2 数据库的数据库转储：

```
dump database pubs2 to "\Syb_backup/mydb.db" with passwd = "bluesky"
```

必须使用相同的口令装载数据库转储：

```
load database pubs2 from "\Syb_backup/mydb.db" with passwd = "bluesky"
```

口令与 Adaptive Server 的早期版本

仅当使用 Adaptive Server 12.5.2 版及更高版本时，才能使用口令保护的 `dump` 和 `load` 命令。如果对 Adaptive Server 12.5.2 版的转储使用口令参数，则在尝试将此转储装载到 Adaptive Server 的早期版本上时，装载会失败。

口令和字符集

只能将转储装载到另一台具有相同字符集的服务器上。例如，如果试图将使用 ASCII 字符集的服务器中的转储装载到一台使用非 ASCII 字符集的服务器上，由于 ASCII 口令的值不同于非 ASCII 口令的值，装载会失败。

用户输入的口令会转换为 Adaptive Server 的本地字符集。由于 ASCII 字符通常在各字符集中使用相同的值表示形式，因此，如果用户的口令在 ASCII 字符集中，则 `dump` 和 `load` 的口令在所有字符集中都可得到识别。

Adaptive Server 15.0.2 版及更高版本允许您存储可移植口令。请参见 [第 438 页的“口令的字符集注意事项”](#)。

索引

符号

- := (BNF 符号)
 - SQL 语句中 xxii
- ' (撇号)
 - 登录名中转换为下划线 462
- ' (右引号)
 - 登录名中转换为下划线] 462
- ' (左引号)
 - 登录名中转换为下划线 462
- % (百分比符号)
 - 错误消息占位符 323
 - 登录名中转换为下划线 462
- { (大括号)
 - SQL 语句中 xxii
 - 在登录名中转换为 \$ (美元符号) 462
- = (等号)
 - 登录名中转换为下划线 462
- , (逗号)
 - SQL 语句中 xxii
 - 登录名中转换为下划线 462
- [] (方括号)
 - SQL 语句中 xxii
 - 登录名中转换为 # (井号) 463
- ; (分号) 在登录名中转换为 # (井号) 463
- ~ (否定符号)
 - 登录名中转换为下划线 462
- !! (感叹号)
 - 在登录名中转换为 \$ (美元符号) 462
- + (加号)
 - 在登录名中转换为 # (井号) 463
- ^ (尖号)
 - 在登录名中转换为 \$ (美元符号) 462
- (减号)
 - 在登录名中转换为 # (井号) 463
- . (句点)
 - 在登录名中转换为 \$ (美元符号) 462
- : (冒号)
 - 登录名中转换为下划线 462
- | (竖线)
 - 在登录名中转换为 # (井号) 463
- ?? (问号)
 - 用于可疑字符 316
- ? (问号)
 - 在登录名中转换为 \$ (美元符号) 462
- () (小括号)
 - SQL 语句中 xxi
 - 在登录名中转换为 \$ (美元符号) 462
- / (斜杠)
 - 登录名中转换为 # (井号) 463
- \ (反斜杠)
 - 登录名中转换为下划线 462
- * (星号)
 - select** 547
 - 在登录名中转换为 # (井号) 463
- " " (引号)
 - 将参数值括起来 11
 - 将值引起来 379
 - 引号 379
 - 在登录名中转换为 # (井号) 463
- > (右尖括号)
 - 登录名中转换为下划线 462
- & (与符号)
 - 登录名中转换为下划线 462
- < (左尖括号)
 - 在登录名中转换为 \$ (美元符号) 462
- \$ISA 505

数字

7 位 ASCII 字符数据, 字符集转换 311

英文

- abstract plan cache** 配置参数 72
- abstract plan dump** 配置参数 72
- abstract plan load** 配置参数 73
- abstract plan replace** 配置参数 73
- ACF (应用程序环境功能), 解决问题 570
- Adaptive Server 插件 (ASEP)
 - 15.0.3 的命令行更新 44
- Adaptive Server 主管名 479
- additional network memory** 配置参数 73
- all** 关键字
 - grant** 518, 525
 - revoke** 525
- allow backward scans** 配置参数 76
- allow nested triggers** 配置参数 76
- allow procedure grouping** 配置参数 77
- allow remote access** 配置参数 77
- allow resource limits** 配置参数 78
- allow sendmsg** 配置参数 78
- allow sql server async i/o** 配置参数 79
- allow updates to system tables** 配置参数 12, 79
- allow updates** 配置参数 (现在称为 **allow updates to system tables**) 12
- alter database** 命令
 - 忽略数据库设备 261, 262
 - 系统表 251
- alter role** 命令 393, 418, 419
- ansi_permissions** 选项, **set**
 - 权限 520
- ASCII 字符
 - 字符集转换 311
- ASEP (Adaptive Server 插件)
 - 15.0.3 的新增功能 44
 - “连接配置文件说明”, “导入” 44
 - 新搜索工具 44
 - 支持 Windows Vista 44
- audit queue size** 配置参数 80, 587, 597
- auditing** 配置参数 81, 599
- automatic cluster takeover** 配置参数 82
- average cap size** 配置参数 80
- Backup Server
 - tape retention in days** 配置参数 232
 - 错误消息 331
 - 关闭 344
- Backus Naur Form (BNF) 符号 xxi, xxii
- bcp** (批量复制实用程序)
 - 安全服务 470
 - 具有访问规则 559
 - 排序顺序更改 295
 - 字符集转换 318
- Big 5
 - 类似于 CP 950 276
- CA 认证 629
 - 受托根认证 629
 - 位置 632
- caps per ccb** 配置参数 83
- cascade** 选项, **revoke** 519
- @@char_convert** 全局变量 305
- charset.loc* 文件 304
- charsets* 目录 305
- checktable** 选项, **dbcc** 300
- CIPC large message pool size** 配置参数 84
- CIPC regular message pool size** 配置参数 84
- cis bulk insert batch size** 配置参数 84, 85
- cis connect timeout** 配置参数 85
- cis cursor rows** 配置参数 86
- cis idle connectin timeout** 配置参数 86
- cis packet size** 配置参数 87
- cis rpc handling** 配置参数 87
- @@client_csexpansion** 全局变量 305
- @@client_csid** 全局变量 305
- @@client_csname** 全局变量 305
- cluster heartbeat interval** 配置参数 88
- cluster heartbeat retries** 配置参数 88
- cluster vote timeout** 配置参数 89
- cntrlrtype** 选项
 - disk init** 260
- common.loc* 文件 306
- compression memory size** 配置参数 89
- configuration file** 配置参数 90, 109, 218, 219
- cost of a cpu unit** 配置参数 91
- cost of a logical io** 配置参数 90
- cost of a physical io** 配置参数 90
- CP 1252
 - 类似于 ISO 8859-1 276
- CP 950
 - 类似于 Big 5 276
- cp437 字符集 97
- cp850 字符集 97

- CPR 文件 345
- cpu accounting flush interval** 配置参数 91, 450
- cpu grace time** 配置参数 92
- CPU 使用率
 - 每个用户的 449
- create database** 命令
 - default database size** 配置参数 97
 - model* 数据库 25
 - 忽略数据库设备 261, 262
 - 使用权限 513
 - 系统表 9
- create index** 命令 247, 252
- create procedure** 命令 12
- create role** 命令 393
- create rule** 命令, 新功能 554
- create rule** 语法 554
- create rule**, 语法 555
- create table** 命令 247
- create trigger** 命令 519
- cs_connection** 命令, **number of user connections** 187
- current audit table** 配置参数 93, 592
- DAC。请参见 自由选择访问控制 (DAC)
- database size 配置变量 48
- dataserver** 命令
 - 用来解锁登录名和角色 419
- dbcc storage_admin_role** 命令 529
- dbcc** (数据库一致性检查程序) 38
 - grant dbcc checkstorage** 命令 529
 - grant dbcc** 和角色 529
 - grant dbcc** 和数据库中的用户 529
 - tune** 命令 529
 - 定义的 528
 - 服务器范围的命令 528, 529
 - 描述的 528
 - 使用时间 330
 - 数据库损坏 326, 330
 - 特定于数据库的命令 528, 529
 - 自由选择访问控制 528
- DBISQL11
 - 现在为独立产品 45
 - 增强功能 45
- DB-Library 程序
 - number of user connections** 187
 - “dbo” 用户名 4, 5
- dbprocess** 命令, **number of user connections** 187
- DCE (分布式计算环境) 安全性机制 460
- deadlock checking period** 配置参数 94
- deadlock pipe active** 配置参数 95
- deadlock pipe max messages** 配置参数 95
- deadlock retries** 配置参数 95
- deckanji 字符集 97
- default character set id** 配置参数 97
- default database size** 配置参数 97
- default exp_row_size percent** 配置参数 98
- default fill factor percent** 配置参数 98
- default language id** 配置参数 99
- default network packet size** 配置参数 99
- default sortorder id** 配置参数 101
- default XML sortorder** 配置参数 101
- defaulton | defaultoff** 选项, **sp_diskdefault** 262
- defncopy** 实用程序命令
 - 另请参见 实用程序手册
 - 字符集转换 318
- delete statistics** 语法 522
- delete** 命令 337
- disable character set conversions** 配置参数 102
- disable disk mirroring** 配置参数 103
- disk i/o structures** 配置参数 103
- disk init** 命令 246, 251, 254–260
- disk mirror** 命令 246
- disk reinit** 命令
 - 另请参见 **disk init** 命令
- disk resize** 246, 263
 - 磁盘空间不足 265
 - 镜像 264
 - 设备容量缩减 265
 - 使用 264
 - 语法 264
 - 最小大小 263
- DMA object pool size** 配置参数 104
- drop logins** 选项, **sp_dropserver** 369
- drop role** 命令 400
- dscp** 实用程序 (用于指定安全性机制) 455
- dsedit** 安全服务实用程序 456
- dsync** 选项
 - disk init** 261
- dtm detach timeout period** 配置参数 104, 337
- dtm lock timeout period** 配置参数 104

- dump database** 命令
 - disk init** 254
 - master* 数据库 37
 - model* 数据库 25
- dump on conditions** 配置参数 106
- dynamic allocation on demand** 配置参数 106
- enable backupserver HA** 配置参数 107
- enable cis** 配置参数 107, 109, 110, 119
- enable DTM** 配置参数 107
- enable encrypted columns** 配置参数 108
- enable housekeeper GC** 配置参数 111, 338
- enable i/o fencing** 配置参数 112
- enable java** 配置参数 109, 112
- enable job scheduler** 配置参数 113
- enable ldap user auth** 配置参数 113
- enable literal autoparam** 配置参数 113
- enable logins during recovery** 配置参数 114
- enable merge join** 配置参数 114
- enable metrics capture** 配置参数 115
- enable monitoring** 配置参数 115
- enable pam user auth** 配置参数 115
- enable query tuning mem limit** 配置参数 116, 117
- enable real time messaging** 配置参数 117
- enable rep agent threads** 配置参数 117
- enable row level access control** 配置参数 118
- enable semantic partitioning** 配置参数 118
- enable sort-merge join and JTC** 配置参数 119
- enable SQL debugger** 配置参数 119
- enable stmt cache monitoring** 配置参数 120
- enable surrogate processing** 配置参数 120
- enable unicode conversion** 配置参数 120
- enable unicode conversions** 配置参数 314
- enable unicode normalization** 配置参数 121
- enable webservice** 配置参数 121
- enable xact coordination** 配置参数 122
- enable xml** 配置参数 122
- engine memory log size** 配置参数 123
- errorlog pipe active** 配置参数 123
- errorlog pipe max messages** 配置参数 123
- esp execution priority** 配置参数 124
- esp execution stacksize** 配置参数 124
- esp unload dll** 配置参数 125
- eucjis* 字符集 97
- event buffers per engine** 配置参数 125
- event log computer name** 配置参数 126
- event logging** 配置参数 126
- executable code size + overhead** 配置参数 127
- expand_down** 参数
 - sp_activeroles** 414
- extended cache size** 配置参数 127
- filter** 参数, 在 **sp_addserver** 中 645
- FIPS login password encryption** 配置参数 128
- fix_text** 选项, **dbcc** 300–301
- french*
 - 字符集支持 276
- get_appcontext** 565, 567
- global async prefetch limit** 配置参数 128
- global cache partition number** 配置参数 129
- grant dbcc**
 - 角色 529
 - 数据库中的用户 529
- grant option for** 选项, **revoke** 519
- grant** 命令 512, 516–533
 - all** 关键字 525
 - public* 组 518
 - 角色 535
- grant** 选项
 - sp_helprotect** 543
- Guest* 用户
 - 创建 48
- guest* 用户 516
 - 创建 383
 - 权限 383
 - 数据库 48
 - 添加 383
 - 样本数据库 29, 384
- hash*
 - 定义的 629
 - 消息摘要 629
- heap memory per user** 配置参数 129
- histogram tuning factor** 配置参数 130
- housekeeper free write percent** 配置参数 131, 336
- I/O*
 - 使用状况统计信息 450
- i/o accounting flush interval** 配置参数 132, 450
- i/o batch sizet** 配置参数 133
- i/o polling process count** 配置参数 134
- IBM* 字符集 97
- ID*, 用户 388, 411
 - 系统过程 12
- identity burning set factor** 配置参数 135

- identity grab size** 配置参数 135
- identity reservation size** 配置参数 136
- idle migration timeout** 配置参数 136
- installhasvss* 脚本 110
- insthasv* 脚本 110
- interfaces* 文件 14, 455
- is_sec_service_on** 安全性函数 473
- ISO 8859-1
 - 类似于 CP 1252 276
- iso_1 字符集 97
- isql** 实用程序命令
 - number of user connections** 187
 - 安全服务 470
 - 口令 374
 - 系统管理 7
 - 状态消息和信息消息 326
 - 字符集转换 318
- Java 配置参数 219
- job scheduler interval** 配置参数 137
- job scheduler tasks** 配置参数 137
- k 选项 479
- kadmin 476
- kanji。请参见 日语字符集
- Kerberos 474
 - CyberSafe Kerberos 库 474
 - keytab 文件 476
 - MIT Kerberos 库 474
 - 本机库 474
 - 兼容性 474
 - 配置 475
 - 许可证 474
- Kerberos 鉴定 479
 - 并发 484
 - 验证 482
- keytab 文件
 - 为实用程序指定 470
- kill statusonly** 参数 335
- kill** 命令 332-335
- kill** 命令, 更改 335
- LAN Manager 的安全性机制 460
- @@*langid* 全局变量 307
- @@*language* 全局变量 307
- LDAP
 - 定义的 16
 - 多个目录服务 17
 - 访问限制 16
 - 改进 500
 - 设置故障恢复时间间隔 501
 - 与 *interfaces* 文件 18
 - 语法 501
 - 支持 491
 - 状态转换 493
- LDAP 用户鉴定 495
 - 对登录映射的控制更加严格 496
 - 故障排除 498
 - 口令更改 490
 - 调优 495
- LDAP 用户鉴定的超时设置 495
- LDAP 用户鉴定的故障排除 498
- LDAP 用户鉴定的口令更改 490
- LDAP 用户鉴定的最大本机线程数 495
- libtcl.cfg* 文件 15
 - 编辑工具 458
 - 示例 459
 - 为基于网络的安全性做准备 456
- libtcl.cfg* 文件中的目录服务 15, 456
- license information** 配置参数 137, 448
- license information**, 配置参数 337
- list_appcontext** 565, 568
- local** 选项, **sp_addserver** 366
- locales* 目录 291
- locales.dat* 文件 306
- lock address spinlock ratio** 配置参数 138
- lock hashtable size** 配置参数 139
- lock scheme
 - 全服务器范围内的缺省值 139
 - 缺省 139
- lock scheme** 配置参数 139
- lock shared memory** 配置参数 140
- lock spinlock ratio** 配置参数 140
- lock table spinlock ratio** 配置参数 141
- lock wait period** 配置参数 141
- log audit logon failure** 配置参数 142
- log audit logon success** 配置参数 142
- log on** 选项
 - create database** 251

- logsegment* 日志存储 249
- Macintosh 字符集 97, 315
- master* 数据库 9, 23–24, 36
 - guest 用户位于 383
 - sysdevices* 表 261
 - 备份 36, 49
 - 撤消系统表的缺省权限 530
 - 创建 249
 - 更改选项设置 267
 - 另请参见 磁盘镜像 245
 - 删除 guest 用户 383
 - 授予系统表的缺省权限 530
 - 所有权 513
 - 系统表的键 10
- max async i/os per engine** 配置参数 143
- max async i/os per server** 配置参数 144
- max cis remote connections** 配置参数 145
- max concurrently recovered db** 配置参数 146, 169
- max memory** 配置参数 146
- max native threads per engine** 配置参数 147
- max nesting level** 配置参数 147
- max network packet size** 配置参数 148
- max number network listeners** 配置参数 150
- max online engines** 配置参数 150
- max online Q engines 151
- max parallel degree** 配置参数 152
- max pci slots** 配置参数 152
- max repartition degree** 配置参数 154
- max resource granularity** 配置参数 154
- max roles enabled per user** 配置参数 163, 392
- max scan parallel degree** 配置参数 154
- max SQL text monitored** 配置参数 155
- max transfer history**, 配置参数 156
- @@max_connections** 全局变量 186
- @@maxcharlen** 全局变量 305
- maximum buffers per lava operator** 配置参数 157
- maximum dump conditions** 配置参数 156
- mci memory size** 配置参数 197
- membership** 关键字, *alter role* 394
- memory alignment boundary** 配置参数 159
- memory per worker process** 配置参数 159
- messaging memory** 配置参数 159
- metrics elap max** 配置参数 160
- metrics exec max** 配置参数 160
- metrics lio max** 配置参数 160
- metrics pio max** 配置参数 161
- Microsoft 字符集 97
- min pages for parallel scan 161
- minimum pages for a parallel scan** 配置参数 161
- minimum password length** 配置参数 162
- mnc_full_index_filter** 配置参数 163
- model 数据库 48
- model* 数据库 25
 - 创建 249
 - 大小 97, 256
 - 系统表的键 10
- MSDTC 108
- msg confidentiality reqd** 配置参数 163
- msg integrity reqd** 配置参数 164
- mut_excl_roles** 系统函数 414
- @@ncharsize** 全局变量 305
- nested trigger** 配置参数 (现在称为 **allow nested triggers**) 76
- net password encryption reqd** 配置参数 164
- net password encryption** 选项 368
- NT LAN Manager 的安全性机制 460
- null** 关键字
 - 在 *sp_addlogin* 中 379
- number of alarms** 配置参数 165
- number of aux scan descriptors** 配置参数 165
- number of backup connections** 配置参数 168
- number of ccbs** 配置参数 168
- number of devices** 配置参数 169
- number of dtx participants** 配置参数 170
- number of histogram steps** 配置参数 172
- number of index trips** 配置参数 172
- number of large i/o buffers** 配置参数 174
- number of locks** 配置参数 174
- number of mailboxes** 配置参数 175
- number of messages** 配置参数 175
- number of oam trips** 配置参数 176
- number of open databases** 配置参数 177
- number of open indexes** 配置参数 178
- number of open objects** 配置参数 179
- number of pre-allocated extents** 配置参数 182
- number of Q engines at startup 183
- number of remote connections** 配置参数 184
- number of remote logins** 配置参数 171, 184
- number of remote sites** 配置参数 185
- number of sort buffers** 配置参数 185
- number of user connections** 配置参数 68, 186–187

- number of worker processes** 配置参数 188
- o/s file descriptors** 配置参数 189
- object lockwait timing** 配置参数 189
- objectid.dat** 文件 459
 - 位置 636
- on** 关键字
 - grant** 518
 - revoke** 518
- open index hash spinlock ratio** 配置参数 190
- open index spinlock ratio** 配置参数 190
- open object spinlock ratio** 配置参数 191
- optimization timeout limit** 配置参数 192
- page lock promotion HWM** 配置参数 193
- page lock promotion LWM** 配置参数 194, 211
- page lock promotion PCT** 配置参数 194
- partition groups** 配置参数 196
- partition spinlock ratio** 配置参数 196
- per object statistics active** 配置参数 197
- per object statistics active** 配置参数 197
- performance monitoring option** 配置参数 199
- permission cache entries** 配置参数 200
- plan text pipe active** 配置参数 200
- plan text pipe max messages** 配置参数 200, 201
- print deadlock information** 配置参数 201
- print recovery information** 配置参数 202
- proc_role** 系统函数
 - 存储过程 415, 548
- process wait events** 配置参数 203
- prod-consumer overlap factor** 204
- public** 成员资格 49
- public** 关键字
 - grant** 526
- public** 组 381
 - 另请参见 组
 - grant** 518, 526
 - guest 用户权限 383
 - revoke** 518
 - sp_adduser** 382
 - sp_changegroup** 405
 - 权限 515, 533
- pubs2** 数据库
 - image** 信息 29
 - 管理 28
- pubs3** 数据库
 - 管理 28
- quorum heartbeat interval** 配置参数 204
- quorum heartbeat retries** 配置参数 204
- read committed with lock** 配置参数 205
- read only** 数据库选项 299
- reconfigure** 命令
- recovery interval in minutes** 配置参数 205–207
 - 长期运行的事务 206
- remote server pre-read packets** 配置参数 208
- reorg reclaim_space** 命令 337
- reorg** 命令
 - 手动运行 338
- restricted decrypt permission** 配置参数 208
- retaindays** 选项
 - dump database** 232
 - dump transaction** 232
- revoke** 命令 512, 516–533
 - public** 组 518
- RFC 86.0 505
- rm_appcontext** 565, 568
- role_contain** 系统函数 414
- roman8 字符集 97
- row lock promotion HWM** 配置参数 210
- row lock promotion LWM** 配置参数 211
- row lock promotion PCT** 配置参数 211
- RPC。请参见 远程过程调用
- rtm thread idle wait period** 配置参数 212
- runnable process search count** 配置参数 212
- “sa” 登录名 354
 - 安全性建议用于使用 354
 - 更改口令 354
 - 使用系统管理员和系统安全员角色配置 354
- scripts 275
- secmech** 规范 459
- secure default login** 配置参数 214
- segmap** 列, **sysusages** 表
 - 过程, 更改 251
- select *** 命令
 - 错误消息 547
- select into/bulkcopy/pllsort** 数据库选项
 - model** 数据库 25
- select on syscomments.text column** 配置参数 215
- select** 命令
- send doneinproc tokens 215
- server.loc** 文件 306
- server_name.cfg** (配置文件的缺省名称) 56
- session authorization** 选项, **set** 539

- session migration timeout** 配置参数 216
- set** 命令
 - 角色 398
- set** 选项
 - 可导出 580
- set_appcontext** 565
- setuser** 命令
 - show_role** 413
- setuser**, 使用 536
- shared memory starting address** 配置参数 216, 217
- show_role** 系统函数 413
- show_sec_services** 安全性函数 473
- shutdown** 命令 343–345
- size of auto identity column** 配置参数 217
- size of global fixed heap** 配置参数 217
- size of process object fixed heap** 配置参数 218
- size of shared class heap** 配置参数 218
- size of unilib cache** 配置参数 219
- sjis** (Shift-JIS) 字符集 *请参见* 日语字符集
- sp_activeroles** 系统过程 414
- sp_addalias** 系统过程 407
- sp_addauditrecord** 系统过程 611
- sp_addgroup** 系统过程 381
- sp_addlanguage** 系统过程 303
- sp_addlogin** 系统过程 379–380, 430, 431, 432
- sp_addremotelogin** 系统过程 370–372
- sp_addsegment** 系统过程
 - sysusages* 251
- sp_addserver**
 - 包括 **filter** 参数 645
- sp_addserver** 系统过程 365–367
- sp_adduser** 系统过程 25, 381–383
- sp_audit** 系统过程
 - 设置选项 603
- sp_changedbowner** 系统过程 513
- sp_changegroup** 系统过程 381, 405
- sp_column_privileges** 编目存储过程 545
- sp_configure** 系统过程 59
 - 还可参见各个配置参数名
 - 为安全服务配置服务器 460
 - 远程登录名 375
- sp_countmetadata** 系统过程 177, 178, 180, 181
- sp_dboption** 系统过程 267–269
- sp_deviceattr** 系统过程 246, 258
- sp_diskdefault** 系统过程 246, 262–263
- sp_displaylogin** 系统过程 410
- sp_displayroles** 系统过程 414
- sp_dropalias** 系统过程 408
- sp_dropdevice** 系统过程 262
- sp_dropgroup** 系统过程 400
- sp_droplogin** 系统过程 402
- sp_dropremotelogin** 系统过程 370
- sp_dropsegment** 系统过程
 - sysusages* 251
- sp_dropserver** 系统过程 369
- sp_dropuser** 系统过程 399
- sp_extendsegment** 系统过程
 - sysusages* 251
- sp_helpconfig** 系统过程 177, 178, 180
- sp_helpdb** 系统过程 12
 - 数据库选项信息 268
- sp_helpdevice** 系统过程 12, 260
- sp_helpindex** 系统过程 12
- sp_helpjoins** 系统过程 10
- sp_helpkey** 系统过程 10
- sp_helpremotelogin** 系统过程 375
- sp_helprotect** 系统过程 543–544
- sp_helpserver** 系统过程 369
- sp_helptext** 系统过程 12
- sp_helpuser** 系统过程 408
- sp_indsuspect** 系统过程 299, 300
- sp_ldapadmin** 492
- sp_listener**, 指定公用名 645
- sp_locklogin** 系统过程 401
- sp_logintrigger** 581
- sp_maplogin** 496
- sp_modifylogin** 系统过程 298, 404, 430, 432
- sp_monitorconfig** 系统过程
 - 配置 **number of open databases** 177
 - 配置 **number of open indexes** 179
 - 配置 **number of open objects** 180, 182
- sp_password** 系统过程 403
- sp_passwordpolicy** 语法 433
- sp_remotoption** 系统过程 374
- sp_reportstats** 系统过程 450
- sp_serveroption net password encryption** 说明 434
- sp_serveroption** 系统过程 367
- sp_showplan** 系统过程 341
- sp_showpsexec** 系统命令, 管家输出 336
- sp_table_privileges** 编目存储过程 544
- sp_who** 系统过程 409, 542
- sp_who**, 管家输出 336

- #spdevtab 临时表 12
- #spindtab 临时表 12
- SPR 文件 345
- sproc optimize timeout limit** 配置参数 219
- spt_committab 表 12
- spt_monitor 表 12
- spt_values 表 12
- SQL batch capture** 配置参数 220
- sql server clock tick length** 配置参数 221
- sql text pipe active** 配置参数 222
- sql text pipe max messages** 配置参数 222
- SQL 语句中的 BNF 符号 xxi, xxii
- SQL 语句中的大括号 ({}) xxii
- .srt 文件 304
- srvname 列, syssservers 表 367
- srvnetname 列, syssservers 表 367
- SSL
 - 定义的 630
 - 公用名, 指定 645
 - 过滤, 定义的 631
 - 启用 SSL 633
 - 握手 630
- SSL 连接
 - Open Client 632, 633
 - 协同服务器 633
 - 针对 RPC 632
- stack guard size** 配置参数 223
- stack size** 配置参数 225
- start mail session** 配置参数 225
- start xp server during reboot** 配置参数 226
- startup delay** 配置参数 227
- statement pipe active** 配置参数 227
- statement pipe max messages** 配置参数 228
- statement statistic active** 配置参数 228
- statement statistics active** 配置参数 228
- status
 - 信息消息 (级别 10) 326
- strict dtm enforcement** 配置参数 228
- suid (服务器用户 ID) 380
- Sun 字符集 97
- suser_id** 系统函数 411–412
- suser_name** 系统函数 411–412
- suspend audit when device full** 配置参数 229, 597
- syb_map_name 481
- syb_sendmsg port number** 配置参数 230
- Sybase Central, 用于系统管理任务 8
- SYBASE_PRINCIPAL 479
- syblicenseslog 表 449
- sybmapname 481
- sybsecurity 的 syslogs 事务日志 598
- sybsecurity 数据库 27, 585
- sybsystemdb 数据库 28
- sybsystemprocs 数据库 11, 13, 26
 - 另请参见 数据库
 - 权限 516
- sys_session** 应用程序环境表 569, 570
- sysalternates 表 407, 408
 - 另请参见 sysusers 表
- sysconfigures 表 71
- syscurconfigs 表 71
- sysdevices 表 251, 260
 - disk init 251
 - sp_dropdevice 262
 - sp_helpdevice 260
 - 状态位 261
- sysdevices 中的 status 位 261
- sysindexes 表 252, 299
- syslogins 表
 - sp_addlogin 影响 379
- syslogs 表
 - 修改 10
- sysmessages 表 322, 323
- sysobjects 表 299
- sysremotelogins 表 372
- syssegments 表 252
- syssservers 表 363, 364, 365, 369
 - sp_helpserver 369, 469
- srvname 列 367
- srvnetname 列 367
- systemwide password expiration** 配置参数 231
- sysusages 表 251
 - 损坏 330
- sysusers 表
 - sysalternates 表 408
 - 权限 516
- tape retention in days** 配置参数 232
- tcp no delay** 配置参数 232
- tempdb 数据库 26–27
 - 另请参见 数据库
 - 创建 249
 - 大小 26

text prefetch size 配置参数 233
text 数据类型
 多字节字符集 300
 更改字符集 300
time slice 配置参数 233
timeouts 选项, **sp_serveroption** 367
total data cache size 配置参数 234
transfer utility memory size 配置参数 236
trunc log on chkpt 数据库选项
 recovery interval in minutes 206
truncate table 语法 522
txn to pss ratio 配置参数 236
unichar 数据类型 277
 Unicode 276, 277–280
 unichar 数据类型 277
 univarchar 数据类型 277
 UTF-16 277
 字符集 276
unified login required 237
univarchar 数据类型 277
 UNIX 平台, 原始磁盘分区 255
 untrusted 模式, 远程登录 374
update statistics 语法 522
upgrade version 配置参数 238
 us_english 语言 99
use security services 配置参数。 238, 461
user log cache size 配置参数 239
user log cache spinlock ratio 配置参数 240
user_id 系统函数 412
user_name 系统函数 412
 UTF-16 277
vstart 选项
 disk init 260
wait event timing 配置参数 240
 Windows NT LAN Manager 的安全性机制 460
with grant option 选项, **grant** 519
with nowait 选项, **shutdown** 343, 345
workload manager size 配置参数 241
 X/Open XA 108
 xact 241
 .xlt 文件 304
 XP Server
 释放内存, 从 125
 优先级 124
xp_cmdshell context 配置参数 242
xp_cmdshell 系统扩展存储过程 13

A

阿拉伯语字符集支持 276
 安全服务
 示例 452
 由 Adaptive Server 支持 453
 安全和目录服务, 要求 128
 安全模式 465
 模式 B 466
 模式 B 的示例 468
 设置 RPC 安全模式 B 466
 针对 RPC 466
 安全缺省登录 461
 安全性
 Kerberos 474
 安装后建立 354–356
 标识和认证控制 357
 登录功能 415
 角色 359
 审计 360
 自由选择访问控制 358
 安全性管理
 快速入门 353–356
 示例 355
 指南 354
 安全性函数 473
 安全性机制 472
 安全性驱动程序
 libtcl.cfg 文件中的条目示例 459
 libtcl.cfg 文件中条目的语法 457
 安装
 样本数据库 28
 安装, 服务器
 interfaces 文件 15
 安装后状态 249
 审计系统 588
 之后建立安全性 354–356

B

百分比符号 (%)
 错误消息占位符 323
 登录名中转换为下划线 462

- 包, 网络
 - 大小, 配置 148-149
- 保存点
 - 错误 (级别 13) 327
- 保护机制。请参见 安全性函数 349, 353
- 保护网络上的登录口令 433
- 保护系统
 - 报告 541-544
 - 层次 (所有权链) 549
 - 上下文相关的 547
 - 摘要 511
- 报告
 - 另请参见 信息 (服务器)
 - 错误 326, 328, 331
 - 服务器使用状况 449
 - 使用状况统计信息 450
- 备份 36-38
 - master 数据库 49
 - 提示 36-38
- 本地服务器 366
- 本地服务器和远程服务器。请参见 远程服务器
- 本地化 271, 272
 - 另请参见 语言, 替代
- 文件 306
- 比较值
 - 数据类型问题 327
- 编码字符 309
- 错误消息中的变量 323
- 标识和鉴定
 - 另请参见 登录名
- 控件 357
- 表
 - 另请参见 数据库对象 9
 - dbcc checktable** 300
 - 拆分到两个磁盘上 248
 - 对象分配映射 176
 - 基础的 546
 - 具有可疑分区, 修复 302
 - 可疑, 修复 302
 - 临时 26
 - 没有索引 300
 - 权限 515, 518
 - 权限, 与视图比较 546

- 权限信息 544
- 上下文相关的保护 547
- 所有权链 549
- 完整性损坏 330
- 系统过程 12
- 只读 299
- 表编辑器 50
- 表所有者。请参见 数据库对象所有者
- 别名
 - 服务器 366
- 别名, 用户
 - 创建 407
 - 另请参见 登录名 407
 - 删除 408
 - 数据库所有权移交 513
 - 有关帮助 408
- 并发 Kerberos 鉴定 484
- 波罗的语字符集支持 276
- 不否认, 数字签名 629
- 不间断的恢复 248
- 不允许使用简单口令 423
- 步骤
 - 管理安全性 353

C

- 参数, 过程 379
- 操作系统命令
 - 执行 13
- 操作员角色 5
 - 权限 390
- 测试服务器 32
- 层次
 - 角色。请参见 角色层次
 - 权限。请参见 权限
- 查询
 - 转换错误, 阻止 316
- 查找
 - 数据库对象 326
 - 数据库中的用户 411
 - 用户 ID 411
 - 用户名 411

- 查找服务器
 - 辅助 491
- 拆分
 - 跨越两个磁盘的表 248
- 朝鲜语
 - 字符集支持 276
- 撤消
 - create trigger 权限 519
 - 使用 **revoke role** 撤消角色 536
 - 系统表的缺省权限 530
- 撤消 master 数据库系统表的缺省权限 530
- 重放检测 453
- 重新建立原标识 537
- 重新启动, 服务器
 - 重新配置后 299
 - 重新索引 299
 - 临时表 27
 - 从同一目录 324
 - 系统表 299
- 重新启动服务器
 - 请参见 重新启动, 服务器
- 重新设置配置
 - 请参见 配置参数 267
- 初始化
 - 数据库设备 253–260
- 触发器
 - 创建 519
 - 另请参见 数据库对象 6
 - 嵌套 76
 - 权限 553
- 存储过程
 - 处理可疑分区 302
- 创建
 - guest 用户 48, 383
 - master 数据库 249
 - model 数据库 249
 - sybsecurity 数据库 589
 - tempdb 数据库 249
 - 触发器 519
 - 存储过程 12
 - 段 249
 - 数据库 48, 513
 - 数据库对象 247
 - 系统表 9
 - 系统过程 12
 - 用户 49
 - 用户别名 407
 - 用户定义的错误消息 326
 - 组 381
- 磁盘 I/O
 - 配置参数 171
 - 数据库装载和磁盘 I/O 146, 169, 174
- 磁盘镜像
 - sysdevices 表中的状态 261
 - 恢复 248
 - 禁用 103
 - 启用 103
- 磁盘空间不足
 - disk resize 265
- 磁盘控制器 260
- 磁盘 请参见 数据库设备 245
- 磁盘设备
 - 另请参见 数据库设备 245
- 篡改检测, 数字签名 629
- 脆弱时间段 80
- 存储管理 245
 - 安装时的缺省值 249
 - 另请参见 空间 245
- 命令摘要 246
- 缺省数据库设备 262–263
- 数据库设备初始化 253–261
- 问题 34–35, 247
- 系统表 250–252
- 存储过程 11, 349, 353
 - 作为安全性机制 548
- 触发器。请参见 触发器
 - 创建 12
 - 过程高速缓存以及 202
 - 检查其中的角色 415
 - 角色 548
 - 另请参见 数据库对象 6
 - 权限 373, 515, 518
 - 授予的权限 518
 - 授予角色执行权限 415
 - 所有权链 549
 - 系统表更改 12
 - 远程用户访问 373

系统过程

- 错误 321, 325
 - 10-18 级 (用户错误) 326
 - Backup Server 332
 - 报告 331
 - 多个 321
 - 服务器应答 321-330
 - 级别 19 - 24 (致命) 329
 - 记录 324
 - 另请参见 错误日志 321
 - 所记录信息的类型 14
 - 用户 326, 326-328
 - 致命的 329-330
 - 状态号 321
 - 字符转换 315
- 错误消息
- 错误, 用户 请参见 错误 321
- 错误日志 39, 329
 - 创建和所有权 324
 - 格式 324
 - 清除 324
 - 位置 14
- 错误消息 322-331
 - 编号 322
 - 创建用户定义的 325
 - 改变服务器提供的 306, 325
 - 严重级 325-330
 - 用户定义的 326
 - 致命错误 329-331
 - 字符转换 316

D

- 大括号 ({})
 - 在登录名中转换为 \$ (美元符号) 462
- 大小
 - 另请参见 空间
 - dbcc fix_text** 事务 300
 - model* 数据库 97, 256
 - tempdb* 数据库 26
 - 错误日志 14
 - 新数据库 25

代理授权 536-545

- 概述 537
- 使用 537, 539
- 授予 527
- 授予权限 527
- 应用程序如何使用代理授权 541
- 用户如何使用代理授权 539
- 执行 539
- 单用户模式 80, 299
- 当前使用状况统计信息 450
- 当前数据库 326
- 当前用户
 - set proxy** 539
- 导出 set 选项 580
- “导出”选项 44
- 到期的口令 231
- 德语
 - 字符集支持 276
- 登录 377
- 登录 ID 数 385
- 登录 ID, 数目 385
- 登录触发器
 - 创建的语法 572
 - 发布和信息 579
 - 和 set 选项 580
 - 禁用执行特权 579
 - 了解输出 574
 - 配置 572
 - 配置的语法 573
 - 删除和更改 573
 - 使用 572
 - 输出 574
 - 问题 579
 - 显示 574
 - 限制 578
 - 用于其它应用程序 574
 - 执行 574
- 登录过程
 - 鉴定 452
- 登录口令加密 128
- 登录名 377
 - “dbo” 用户名 4, 5
 - “sa” 354

- 标识和鉴定 357
- 别名 407, 408
- 查找 411
- 解锁 400, 418
 - 另请参见 远程登录 377
- 删除 402
- 数据库对象所有者 6
- 锁定 49, 400, 416, 418
- 添加到服务器 379–380
- 无效名 462
- 显示口令信息 419
- 有关信息 411
- 指派名称 355
- 最大尝试次数, 更改 417
- 最大尝试次数, 设置 416
- 登录名。请参见 登录名
- 登录映射
 - 严格的控制 496
- 地址, 服务器 14
- 调用, 远程过程 363–375
 - 超时 367
- 东欧
 - 字符集支持 276
- 动态配置参数 56
- 逗号 (,)
- SQL 语句中 xxii
 - 登录名中转换为下划线 462
- 独立的实用程序和字符集 318
- 读
 - 物理 248
- 存储管理
- 段 245, 252
 - logsegment 249
 - syssegments 表 252
 - 创建 249
 - 另请参见 数据库设备 245
 - 缺省 249
 - 系统段 249
- 对称密钥加密 628
- 对象
 - 导航到 44
 - 请参见 数据库对象
 - 图标 43
 - 对象访问权限 请参见 权限
 - 对象权限
 - grant all 518, 525
 - 对象所有者。请参见 数据库对象所有者
 - 多个目录服务
 - LDAP 17
 - 多语种字符集 97
 - 多字节字符集 300
 - default character set id 配置参数 97
 - 不兼容的 315
 - 更改为 301

E

- 俄语
 - 字符集支持 276

F

- 繁体中文
 - 字符集支持 276
- 反馈错误。请参见 错误日志
- 返回状态
 - 系统过程 11
- 方括号 []
 - SQL 语句中 xxii
 - 登录名中转换为 # (井号) 463
- 访问 554
 - 限制 guest 用户 383
- 访问保护。请参见 权限 349, 353
- 访问规则
 - alter table 命令 559
 - bcp 559
 - 创建 557
 - 创建和绑定 555
 - 扩展 556
 - 删除 556
 - 示例 558
 - 示例表 555
- 访问控制, 行级 553
- 访问权限。请参见 对象访问权限
- 访问者帐户 384

- 非对称密钥对, 生成 433
- 分布式事务处理 (DTP) 28
- 分布式事务管理 (DTM) 28
- 分离的事务 104
- 分配
 - units 254
 - 单元 *另请参见* 大小 245
 - 页 254
- 分区
 - 磁盘 255
- 分区, 可疑, 处理 302
- 分区, 可疑, 修复表 302
- 符号
 - SQL 语句中 xxi
- 服务器
 - interfaces 文件 14
 - 安装 33, 249
 - 本地 366
 - 错误消息 324
 - 错误消息严重级 325–330
 - 单用户模式 80
 - 调度程序 233
 - 非致命内部错误 328
 - 关闭 343
 - 监控性能 67
 - 口令 368, 374
 - 连接 14
 - 另请参见* 进程 (服务器任务) 363
 - 名称 366, 367
 - 排序顺序一致性 295
 - 配置参数的值 55
 - 删除登录名 402
 - 添加新登录名到 379–380
 - 添加用户到 379–380
 - 停止 343
 - 用户连接 187
 - 用户信息 409–450
 - 语法错误 327
 - 远程 365–371
 - 在启动时解锁登录名和角色 419
 - 致命错误 329–330
- 服务器别名 366
- 服务器范围的 **dbcc**、**master** 529

- 服务器鉴定
 - 服务器认证 631
- 服务器认证 629
 - 服务器鉴定 631
 - 位置 631
- 服务器信息选项。 *请参见* 信息 (服务器)
- 服务器用户名和 ID 411
- 辅助
 - 查找服务器, 使用 **sp_ldapadmin** 492
 - 查找服务器支持 491
- 覆盖用户权限 49
- 复选定定的数据
 - 请参见* **insert** 命令 309

G

- 感叹号 (!)
 - 在登录名中转换为 \$ (美元符号) 462
- 高可用性
 - installhasvss** 脚本 110
 - insthasv** 脚本 110
 - 设置 **enable HA** 110
- 高可用性和口令 446
- 高速缓存, 过程 202
- 高速缓存, 数据
 - 数据库完整性错误 330
- 高速缓存分区
 - 配置 127, 129
- 格式
 - 区域设置, 不支持的 303–304
 - 日期, 时间和货币 306
- 个别过程名*
- 个人责任 354
- 更改
 - 另请参见* 更新
 - 登录帐户的口令 403
 - 服务器登录名 404
 - 配置参数 67, 375
 - 缺省数据库 404
 - 数据库所有者 513
 - 数据库选项 267–269
 - 系统表, 危险 10, 12
 - 用户标识 536

- 用户信息 402–405
 - 用户组 405
 - 更新
 - 另请参见 更改
 - allow updates to system tables** 配置参数 12
 - 系统过程 548
 - 字符集更改后的文本 300
 - 公开 / 私有密钥加密 628
 - 公开密钥密码术
 - 定义的 628
 - 加密 628
 - 认证 628
 - 数字签名 628
 - 公式
 - 用户要求 187
 - 公用名, 使用 SSL 指定 645
 - 古斯拉夫语字符集支持 276
 - 故障, 介质 330
 - 关闭服务器 343
 - 管家任务
 - 空间回收 111
 - 配置 131
 - 统计信息刷新 131
 - 许可证使用监控 448
 - 管家实用程序
 - 功能 336
 - 管家清洗, 管家碎片收集, 管家杂事 336
 - 清洗 336
 - 清洗任务 131
 - 三个任务 336
 - 管家碎片收集器 337
 - 管家杂事 337
 - 配置参数 **license information** 337
 - 管理, 空间。请参见 空间分配 245
 - 管理安全性, 快速入门 353–356
 - 管理用户。请参见 用户
 - 规则
 - 另请参见 数据库对象
 - 保护层次 552
 - 国际化
 - 定义 271
 - 示例系统 273
 - 文件 304
 - 优点 272
 - 字符集的目录结构 305
 - 国际语言支持。请参见 字符集 309
 - 过程调用。
 - 请参见 远程过程调用
 - 过程高速缓存 202, 330
 - 过程请参见 存储过程 11
- ## H
- 函数
 - 安全性 473
 - 行, 表
 - sysindexes* 252
 - 行级访问控制 553
 - 行锁升级阈值
 - 使用 **sp_configure** 设置 210, 212
 - 后缀名, 临时表 27
 - 环境变量
 - \$ISA 505
 - 恢复
 - master* 数据库 36, 254
 - 不间断 248
 - 重新配置后 295
 - 计划备份 25
 - 空间分配 248
 - 排序顺序更改 295
 - 配置参数 205–207
 - 装载数据库 295
 - 回退处理
 - 服务器堆栈容量 225
 - 恢复间隔 205
 - 货币
 - 本地格式 306
- ## J
- 基表。参见表
 - 基于网络的安全性 451–473
 - 安全性机制 460
 - 标识用户和服务器 460
 - 获得有关信息 469, 472

- 连接服务器 470
- 内存要求 463
- 配置服务器 460
- 设置配置文件 454
- 使用 470
- 为统一登录添加登录 464
- 用于管理的过程 453
- 远程过程调用 465
- 积极管家 337
- 积极碎片收集 337
 - 优先级 337
- 激活角色 398
- 级别, 严重。
 - 请参见 严重级, 错误
- 记录
 - Windows NT 事件日志 126, 127
 - 成功的登录 142
 - 登录失败 142
 - 登录映射 503
- 记录, 审计 587
- 记录保留 39-41
 - 联系 40
 - 配置 40
 - 维护 40
 - 系统 41
- 加号 (+)
 - 在登录名中转换为 # (井号) 463
- 加密
 - 对称密钥 628
 - 公开 / 私有密钥 628
 - 公开密钥密码术 628
 - 键交换 628
- 加密, 口令 128
- 监控
 - spt_monitor 表 12
 - SQL 文本 155
 - Windows NT 性能监视器 220
- 监控表
 - 配置选项 65
- 检查点进程 206
 - recovery interval 参数 207
 - trunc log on chkpt 数据库选项 206
- 检查口令中是否至少包含一个字符 420
- 简体中文
 - 字符集支持 276
- 减号 (-)
 - 在登录名中转换为 # (井号) 463
- 鉴定 452
 - 相互 453
- 键, 表
 - 在系统表中 10
- 键交换
 - 对称密钥 628
 - 公开 / 私有密钥 628
 - 加密 628
- 降序扫描
 - 死锁 76
- 角色
 - 在 grant 和 revoke 语句中 519, 526
 - 存储过程 535
 - 存储过程权限 415
 - 激活 398
 - 解锁 418, 419
 - 口令 430
 - 权限 535
 - 锁定 416, 418
 - 停用 398
 - 为 “sa” 登录名配置 354
 - 最大登录尝试次数, 更改 417
 - 最大登录尝试次数, 设置 417
- 角色, 系统
 - 操作员 5
 - 系统安全员 5
 - 系统管理员 4
- 角色, 用户定义的
 - 计划 392
- 角色层次 359
 - 创建 534
 - 使用 role_contain 显示 414
 - 使用 sp_displayroles 显示 414
 - 显示 414
- 角色的互斥性 360, 414
- 角色分离 359
- 结构
 - 本地化文件目录 306
 - 国际化文件目录 305

解锁

- 登录帐户 400, 419
- 角色 418, 419
- 进程 ID, 状态 335
- 进程 (服务器任务) 332, 335
 - 另请参见 服务器
 - 服务器上的当前 409
 - 管理 Adaptive Server 353
 - 有关信息 409
 - 注销 332–335
- 进行替换, 数据库选项 48
- 禁用审计 587
- 静态配置参数 56
- 旧的口令复杂程度检查和新的口令复杂程度检查 426
- 拒绝对用户的访问 400, 402
- 具体标识 520
- 句点 (.)
 - 在登录名中转换为 \$ (美元符号) 462
- 角色
 - 存储过程 548

K

- 开发服务器 32
- 可插入鉴定模块 (PAM) 504
 - \$ISA 505
 - enable pam user auth 506
 - RFC 86.0 505
 - 口令管理 506
 - 确定要使用的模块 505
 - 同一计算机上的 32 位和 64 位服务器 505
 - 统一登录 505
 - 为 PAM 配置 Adaptive Server 506
- 可疑分区, 跨平台转储和装载 302
- 客户端
 - 指定客户端名、主机名和应用程序名 406
 - 字符集转换 318
- 空白页, 累计 337
- 空间
 - 另请参见 大小 245
 - 用尽 328
- 空间分配
 - 空间不足。请参见 空间
 - 存储管理
 - 空间分配
 - sysusages 表 251
 - 恢复 / 性能 247
 - 另请参见 数据库设备 245
 - 命令摘要 246
- 空间回收
 - enable housekeeper GC 配置参数 111
- 空口令 403
- 口令 403
 - sp_password 403
 - 保护 378
 - 防止猜口令 416
 - 高可用性 446
 - 更改 403
 - 规则 378
 - 检查至少一个字符 420
 - 降级 435
 - 角色 398, 430
 - 截止 430
 - 空 403
 - 上次更改的日期 410
 - 忘记的 389
 - 显示信息 419
 - 向后兼容性 434
 - 选择 378
 - 选择安全的 378
 - 有效期 430
 - 有效期警告 425
 - 远程用户 368, 374
 - 在网络上加密 368
 - 最小长度 421
- 口令安全性 415–447
 - 保护网络上的登录口令 433
 - 生成非对称密钥对 433
 - 使用 sp_passwordpolicy 生成密钥对 433
- 口令保护的数据库转储 646
- 口令复杂程度
 - 交叉检查 425
 - 旧的和新的 426
 - 自定义口令检查 428

- 口令复杂程度检查 422
 - 不允许使用简单口令 423
- 口令有效期警告 425
- 指定口令中大写字母的最小数目 424
- 指定数字的最小数目 423
- 指定字母字符的最小数目 423
- 自定义口令复杂程度检查 423
- 口令有效期 430
- 跨平台转储和装载, 处理可疑分区 302
- 会计, 收费退回式 449
- 括号。请参见方括号 []
- 扩展 UNIX 字符集 97
- 扩展存储过程
 - 配置参数 124–243

L

- 拉丁字母表 277
- 垃圾收集器
 - 管家实用程序 337
 - 配置积极 338
- 连接
 - interfaces 文件 14
 - 目录服务 15
 - 视图 546
 - 最大用户数 186
- 连接到 Adaptive Server 14
- 链, 所有权 549
- 链接, 页
 - 另请参见 页, 数据
- 链接用户。请参见 别名, 用户
- 两阶段提交
 - 事务 28
- 列
 - 权限 518, 545
- 列表
 - 数据库选项 268
- 列名称
 - 不合格的 327
- 临时表 26
- 浏览
 - 到对象 44

- 螺旋锁
 - 锁散列表 140
- 逻辑
 - 页大小 31

M

- 密码成套程序
 - 定义的 639
 - 支持的 639
- 密钥对, 生成非对称 433
- 敏感信息, 视图 546
- 名称
 - 别名 407, 408, 536
 - 查找用户 411
 - 服务器 367
 - 列, 在命令中 327
 - 另请参见 信息 (服务器) 377
 - 为登录 355
 - 系统过程 11
 - 系统扩展存储过程 13
 - 映射远程用户 370
 - 用户 381, 411, 515, 518
 - 原标识 537
 - 远程服务器 365
 - 远程用户 370
 - 组 518
- 命令
 - delete 337
 - disk resize 263
 - reorg reclaim_space 337
- 命令顺序
 - grant 和 revoke 语句 516–536
- 命名
 - 服务器 366
 - 用户定义角色 392
 - 组 381
- 模拟一个用户。请参见 setuser 命令
- 目录结构
 - *.loc 文件 307
 - 本地化文件 307
 - 国际化文件 305
 - 字符集 305

目录驱动程序 456
libtcl.cfg 文件中的条目示例 459
 目录条目, 创建 636

N

内部错误, 非致命 328
 内存
 另请参见 空间分配
 number of open databases 177
 从 XP Server 释放 125
 基于网络的安全性 463
 审计记录 81, 597
 内核
 错误消息 324, 329
 内置函数
 安全性 473

O

欧洲货币符号
 字符集 277

P

排序顺序
 default sortorder id 101
 default XML sortorder 101
 安装新的 304
 定义文件 304
 服务器之间的一致性 295
 更改 295–298
 更改后重建索引 300
 数字 101
 配置
 Kerberos 475
 配置 (服务器)
 基于网络的安全性 454
 排序顺序 293–300
 消息语言 293–298
 字符集 293

配置参数 71–240
 dtm detach timeout period 337
 housekeeper free write percent 336
 max native threads per engine 147
 rtm thread idle wait period 212
 帮助信息 58
 更改 375
 列出值 59
 缺省设置 55
 审计相关的 587
 收费退回式会计 450
 远程登录名 77, 375
 配置参数, **max transfer history** 156
 配置文件
 存储配置值 56
 缺省名称和位置 56
 在启动时指定 60
 片段, 设备空间 251
 撇号在登录名中撇号转换为下划线 462
 拼音
 gbpinyin、**gbpinyinocs** 排序顺序 286
 size of **unilib cache** 配置参数 286
 size of unilib cache 配置参数 286
 使用变音 286
 转写普通话发音 286

Q

启用
 SSL 633
 审计 587
 清洗, 管家任务 131
 区分大小写
 在 SQL 中 xxiii
 权限
 另请参见 自由选择访问控制 (DAC)
 ansi_permissions 选项 520
 create database 513
 disk init 260
 guest 用户 383
 master 数据库 24
 model 数据库 25
 public 组 515, 518, 533

- tempdb* 数据库 27
- 表 515, 518
- 别名 407
- 不足（级别 14） 327
- 操作员 390
- 撤消 516–533
- 触发器 553
- 创建触发器 519
- 存储过程 373, 515, 518
- 代理授权 527
- 对象 6, 515
- 对象创建 525
- 对象访问 516, 517–521
- 获取其他用户的 536
- 拒绝 327
- 具体标识 520
- 缺省 25
- 使用 **setuser** 536
- 视图 546–547
- 视图而非列 547
- 授予 516–533
- 数据库对象所有者 6
- 数据库所有者 6, 512, 514
- 所有权链 549
- 替换 49
- 同视图比较的表 546
- 系统表 529
- 系统管理员 512–513
- 系统过程 516
- 选择性分配 532
- 移交 513
- 用户层次 535
- 由数据库所有者指派 525
- 有关信息 541–544
- 远程用户 373
- 摘要 511
- 指派 525
- 组 381
- 组与用户 49
- 权限不足 327
- 全局登录触发器 581
- 缺省段 249

- 缺省设置
 - 安装时的系统数据库 249
 - 更改排序顺序 295–300
 - 更改字符集 293–301
 - 排序顺序 101
 - 配置参数 55
 - 权限 25
 - 数据库 24, 379
 - 语言 99
 - 字符集 ID 号 97
- 缺省数据库
 - 更改用户的 404
- 缺省数据库设备
 - 指派 262
- 缺省语言 99
 - us_english 99
 - 更改用户的 298
- 缺省值
 - 另请参见 数据库对象

R

- 认证
 - CA 认证 629
 - 定义的 629
 - 服务器认证 629
 - 公开密钥密码术 629
 - 管理 637
 - 获得 634
 - 请求 635
 - 授权 635
 - 自签 CA 635
- 认证，安全性机制 452
- 日期
 - 错误消息中的格式 325
 - 替代语言 303
 - 添加日期分量 303
 - 显示格式 306
- 日期分量
 - 替代语言 303

日语字符集 97
 另请参见 语言, 替代
 sjis (Shift-JIS) 97
 支持 276
 日志文件。 *请参见* 错误日志

S

散列桶 (锁) 140
 扫描描述符 165–167
 删除
 master 的 *guest* 用户 383
 服务器 369
 服务器中的登录名 402
 服务器中的用户 402
 缺省空间缓冲池的主设备 262
 数据库设备 262
 数据库中的用户 399
 文件 262
 拥有数据库对象的用户 399
 用户 49
 用户别名 408
 用户定义角色 400
 远程登录名 369, 370
 转储设备 262
 组 400
 上下文相关的保护 547
 设备 245, 253
 number of user connections 186, 187
 初始化 253–260
 列出的信息 261
 另请参见 数据库设备 245
 删除 262
 审计系统 588
 使用单独的 248
 添加 254–260
 物理名 255
 设备名 254
 sysdevices 列表 251
 设备片段 251
 设备容量缩减, **disk resize** 265

身份
 代理 537
 会话授权 537
 替代 407
 审计 360, 583, 583–612
 另请参见 审计选项
 sybsecurity 数据库 27, 585
 sysaudits_01...sysaudits_08 表 613
 安装 588
 打开和关闭 599
 队列, 大小 80, 587
 概述 583
 管理审计追踪 592
 管理事务日志 598
 禁用 587
 配置参数 587
 启用 587
 启用和禁用 599
 设备 588
 系统过程 587
 显示选项 587
 向审计追踪中添加注释 587
 阈值过程 592
 审计队列 587, 597
 审计选项
 设置 603
 示例 604
 显示 587
 审计追踪 27, 583, 613
 查询 612
 错误消息的堆栈跟踪 324
 更改当前审计表 592
 管理 592
 具有多个审计表的图示 586
 添加注释 587, 611
 阈值过程 592
 生产服务器 32
 时间
 获取锁 141
 时间值
 显示格式 306
 实用程序, 管家, 积极 337

实用程序命令

请参见 *实用程序手册*

字符集 318

使用代理授权 537

事务

长期运行 206

错误在 327

恢复 206

两阶段提交 28

事务日志

alter database 251

create database 251

trunc log on chkpt 选项 206

清除 301

设备放置 248, 251

视图

另请参见 数据库对象

安全性 545

权限 518, 546–547

所有权链 549

相关 549

视图的基础表（基表） 546

收费退回式会计 449

手动运行 **reorg** 命令 338

授权。请参见 权限

授予

create trigger 权限 519

代理授权权限 527

对象创建权限 6

访问权限 6

角色（使用 **grant role**） 534

角色给角色 395

授予和撤消用户和角色的权限 522

授予系统表的缺省权限 529–531

受托根认证

CA 认证 629

位置 632

受托模式

远程登录名 374

数据

另请参见 权限

完整性 463

数据高速缓存

配置分区 127, 129

数据库完整性错误 330

数据库

guest 用户 48

备份 25, 36, 49

创建 48

创建权限 513

错误影响 330

打开的数量 177

大小 25

另请参见 数据库对象 6

排序顺序更改后装载 295

缺省 24, 379, 404

缺省存储 22, 262

删除用户 399

审计 589

所有权 513

添加用户 381–385

完整性关系到 330

系统 21

新 25

选项 267–269

转储 36

字符集更改后装载 295

数据库对象

另请参见 个别对象名

查找 326

触发器 553

创建 24, 247, 515

错误影响 330

打开的最大数目 179

访问权限 6, 517

控制用户创建 24

权限 515

删除 515

删除用户, 用户拥有 399

所有权 6, 399, 515

相关 549

指派到设备 248

数据库对象所有者 6

另请参见 数据库所有者

权限 6, 512, 537

任务 6

状态不可移交 399

- 数据库管理 3-7
- 数据库设备 253
 - 初始化 253-260
 - 放置对象于 248
 - 可用服务器数 169
 - 空间 *请参见* 段 245
 - 另请参见* 磁盘镜像 245
 - 名称 249, 255
 - 片段 251
 - 缺省 262-263
 - 删除 262
 - 添加 254-260
 - 信息 261
- 数据库所有者 5
 - 另请参见* 数据库对象所有者 511
 - setuser** 命令 536-537
 - 错误职责 326, 328
 - 登录名 4, 5
 - 对象没有移交在 399
 - 更改 513
 - 几个用户作为同一个 407
 - 权限 6, 512, 514
 - 任务 5
 - 授予的权限 525
 - 数据库内部的名称 399, 407
 - 忘记的口令 389
- 数据库选项 267-269
 - 列表 268
 - 设置 268
 - 显示设置 268
- 数据库转储
 - 口令保护 646
- 数据字典。 *参见* 系统表
- 数目 (数量)
 - open objects 179
 - user connections (@@max_connections) 186
 - 服务器上打开的数据库 177
 - 获取锁的秒数 141
 - 数据库设备 169
 - 锁 174
 - 引擎 150
- 数字
 - 错误消息 322
 - 排序顺序 101
 - 引擎 324
 - 状态位 (sysdevices) 261
- 数字签名
 - 不否认 629
 - 篡改检测 629
 - 定义的 629
 - 公开密钥密码术 629
- 顺序混乱检查 453
- 顺序检查 453
- 死锁 327
 - 降序扫描 76
- 速度 (服务器)
 - 系统性能 248
- 碎片收集
 - 积极测试 337
 - 消极测试 337
- 索引
 - default fill factor percent** 百分比 98
 - 重建 299
 - 对象分配映射 176
 - 基于字符的 299
 - 可疑 299, 330
 - 排序顺序更改 300
 - 字符集更改 300
- 索引描述符
 - 打开的最大数目 178
- 锁
 - 数量 174
- 锁超时
 - 配置全服务器范围 141
- 锁定 49
 - 由 **dbcc** 命令 301
 - 登录名 400, 416
- 锁定登录名 49
- 锁散列表
 - 配置大小 139
- 锁散列桶 140
- 锁升级阈值
 - 使用 **sp_configure** 设置 193-212
- 所有权链 549
- 所有者。 *请参见* 数据库对象所有者 525

T

泰语

字符集支持 276

特定于数据库的 **dbcc**、**master** 529

替代标识。请参见 别名, 用户

替代语言。请参见 语言, 替代

天

替代语言 303

添加

guest 用户 383

登录到服务器 379–380

日期字符串 303

审计追踪的注释 587

数据库设备 187, 254–260

一年中的月份 303

用户到数据库 187, 377

用户到组中 382

远程登录名 370–372, 385

远程服务器 365–369

组到数据库 381

填充因子

default fill factor percent 配置参数 98

调优

LDAP 用户鉴定 495

监控性能 67

停用角色 398

停止

Backup Server 344

服务器 343

统计信息

I/O 使用状况 449, 450

管家刷新 132

使用管家任务刷新 131

统一登录 453

安全缺省登录 461

要求 461

映射登录名 462

远程过程安全模式 465

图标 43

土耳其语

字符集支持 276

W

网络

interfaces 文件 14

连接 14

目录服务 15

软件 33

网络驱动程序 456

libtcl.cfg 文件中的条目示例 459**libtcl.cfg** 文件中的语法 456文本值, **dbcc fix_text** 升级 300

文件

interfaces 14

libtcl.cfg 文件 15

本地化 306

错误日志 14, 324

国际化 304

删除 262

系统问题报告 (SPR) 345

已解决的问题报告 (CPR) 345

字符集转换 (.xlr) 304

文件描述符 186

特定操作系统配置的每进程最大数 189

问号 (??)

用于可疑字符 316

物理资源, 管理。

请参见 存储管理

X

西班牙语

字符集支持 276

西欧

字符集支持 276

希伯来语

字符集支持 276

希腊语

字符集支持 276

系统段 249

系统安全员 5

系统表 9–10

另请参见 各表名

create database 9, 251

- dbcc reindex** 300
 - 查询 9, 12
 - 重新索引 300
 - 创建 9
 - 存储管理关系 250–252
 - 存储过程 9, 12
 - 服务器重新启动 299
 - 更改危及 13
 - 更新 10, 12
 - 键 10
 - 权限 529
 - 损坏 330
 - 用户数据库 25
 - 允许的更改 529
- 系统管理任务
 - 使用 Sybase Central 完成 8
- 系统管理员 3–7
 - 初学者的任务 31–41
 - 错误职责 326, 328–330
 - 解决系统问题 326, 328
 - 权限 512–513
- 系统管理员可以将执行 528
- 系统过程 11–13
 - 表 12
 - 创建 12
 - 用于更改用户信息 402–405
 - 管理远程服务器 365–369
 - 在临时表上 27
 - 另请参见 信息（服务器） 11
 - 权限 516
 - 使用 11
 - 用于添加用户 377
 - 用于删除别名 408
- 系统角色
 - max_roles_enabled** 配置参数 392
 - show_role** 413
 - 激活 398
 - 使用 **grant role** 授权 534
 - 停用 398
- 系统扩展存储过程 13
- 系统目录。参见 系统表
- 系统审计表 613
- 系统数据库 21–28
- 系统问题
 - 另请参见 错误
 - 服务器应答 321–330
 - 系统问题报告 (SPR) 345
 - 严重级 10 到严重级 18 326–328
 - 严重级 19 到严重级 24 329–330
- 系统消息。请参见 错误消息 321
- 相互冲突的权限 533
 - 另请参见 权限
- 响应时间 233
- 消极碎片收集 337
- 消息
 - 保护服务 452
 - 保密性 453, 463
 - 错误 14, 322–331
 - 来源检查 453
 - 启动 14
 - 完整性 453, 463
 - 系统 322–330
 - 用户定义的 326
 - 语言设置 272
 - 致命错误 14
- 消息摘要
 - hash 629
 - 定义的 629
- 小括号 ()
 - SQL 语句中 xxi
 - 在登录名中转换为 \$（美元符号） 462
- 写操作
 - 物理 248
- 信息（服务器）
 - 错误消息 322–330
 - 登录名 411
 - 更改用户 402–405
 - 配置参数 59
 - 权限 541–544
 - 设备 261
 - 数据库设备 261
 - 数据库选项 268
 - 锁定的登录 401
 - 问题 324
 - 用户，数据库 409–450
 - 用户别名 408

- 远程服务器 369
- 远程服务器登录 375
- 转储设备 261
- 信息消息（服务器）。参见错误消息 321
- 星号 (*)
 - select** 547
 - 在登录名中转换为 #（井号） 463
- 性能
 - audit queue size 80
 - default fill factor percent** 影响 99
 - ESP 和 XP Server 优先级 124
 - 磁盘镜像 247
 - 空间分配 248
 - 速度 248
- 修改
 - 服务器登录名 404
- 需要许可证安全和目录服务 128
- 虚拟
 - 地址 260
 - 页码 257
- 许可证使用状况
 - 错误日志消息 448
 - 监控 447
- 选项
 - 服务器 367
 - 数据库 267–269
 - 远程登录名 374
 - 远程服务器 367

Y

- 严重级 321, 325, 326, 329, 332
- 严重级, 错误
- 验证 Kerberos 鉴定 482
- 验证, 用户访问 368, 371
- 页, 数据 254
 - 脏 206
- 一致性
 - 检查数据库 38
- 移交所有权。
 - 请参见 数据库对象, 所有权
- 已解决的问题报告 345
- 已知故障 345

- 溢出错误
 - 服务器堆栈 224
- 溢出堆栈（**stack guard size** 配置参数） 223
- 异步 I/O
 - 限制服务器请求 143
- 异步预取
 - 配置 128
- 引号（“ ”）
 - 在登录名中转换为 #（井号） 463
- 引擎
 - 标识号 324
 - 数目 151
- 应用程序
 - 代理授权 541
- 应用程序环境
 - 内置函数 565
 - 使用 565
- 应用程序环境功能 563
 - 设置权限 564
 - 授予和撤销特权 564
 - 有效用户 564
- 应用程序设计 187
- 硬件
 - 错误 330
- 映射
 - 设备名到物理名 254
 - 远程用户 369–373
- 映射, 登录 503
- 用法
 - disk resize** 264
 - 统计信息 450
- 用户
 - guest 48, 383, 516
 - ID 388, 411
 - number of user connections** 187
 - 别名 407
 - 创建 49
 - 从服务器删除 402
 - 从数据库中删除 399
 - 错误 326, 326–328
 - 单用户模式 80
 - 访问 384
 - 服务器上的当前 409
 - 客户端名, 设置 406

- 客户端主机名, 设置 406
- 另请参见 别名 377
- 删除 49
- 数据库上当前用户 409
- 数目 385
- 所有或特定用户的权限 532, 547
- 特定视图 546
- 添加 377–381
- 许可证使用监控 447
- 应用程序名, 设置 406
- 由组删除 405
- 有关信息 409–450
- 远程 369–373
- 远程登录
- 用户 ID 388
 - 编号 1, 数据库所有者 12
 - 查找 411
 - 显示 410
- 用户, 对象。请参见 数据库对象所有者
- 用户错误 326, 326–328
- 用户错误。请参见 错误 321
- 用户的标识。请参见 别名 377
- 用户定义角色
 - 激活 398
 - 计划 392
 - 删除 400
 - 使用 **grant role** 授权 534
 - 数目 392
 - 停用 398
- 用户对象。请参见 数据库对象
- 用户鉴定改进 500
- 用户连接
 - 分配的内存 186–187
- 用户名 411, 515
 - 查找 411
 - 更改 404
 - 优先选项 381
- 用户数 385
- 用户数据库
 - master** 数据库控制 23
 - 另请参见 数据库 511
 - 系统表 25
 - 用户定义消息 326
- 用户组 请参见 组 521
- 用于高可用性的 **enable HA** 配置参数 110
- 用于内存转储的线程数, 确定 171
- 用于装载 48
- 优化目标和配置参数 192
- 优先级
 - XP Server 124
- 优先选项, 用户名 381
- 邮件会话, 启动 226
- 游标
 - 行计数, 设置 86
- 与 (&)
 - 登录名中转换为下划线 462
- 阈值过程
 - 审计追踪 592
- 语法
 - disk resize** 264
 - 出错于 327
 - 转储数据库 646
 - 装载数据库 646
- 语法约定, Transact-SQL xxi
- 语言
 - 在服务器上 275
 - 字符集支持的 275
- 语言, 替代 304
 - 本地化文件 290–307
 - 不支持的日期格式 303
 - 另请参见 字符集 304
 - 支持的语言 272
- 语言组 275, 276
- 元数据高速缓存配置参数 65–191
- 远程登录名
 - 超时 367
 - 配置参数 77, 375
 - 删除 369, 370
 - 受托模式或非受托模式 371
 - 添加 370–372
 - 选项 374
- 远程服务器 365–369
 - 名称 365
 - 删除 369
 - 添加 365–369
 - 选项 367
 - 有关信息 369

远程服务器用户。*请参见* 远程登录

远程过程调用 363–375

安全模式 466

安全模式 B 的全部过程 466

基于网络的安全性 465

配置参数 375

设置安全性示例 468

统一登录 465

远程用户。*请参见* 远程登录

约定

Transact-SQL 语法 xxi

另请参见 语法

在参考手册中使用 xxi

越南语

字符集支持 276

月份值

替代语言 303

Z

杂类用户错误 327

脏页 206

占位符

错误消息百分比符号 (%) 323

帐户, 服务器

请参见 登录名 377

直接更新

系统表 79

执行

ESP 和 XP Server 优先级 124

指南, 安全性 354

指派

登录名 355

致命错误

错误消息 329–330

来自内核的反馈 324, 329

严重级 19 和更高严重级 329–330

终端

安装新的定义 304

字符集转换 318

主管名

对于 Adaptive Server 479

使用 sybmapname 481

用 -k 选项 479

用 SYBASE_PRINCIPAL 479

主设备 22, 255, 261

另请参见 数据库设备

sp_diskdefault 262

从缺省空间缓冲池删除 262

注释

添加到审计追踪中 587, 611

转储, 数据库 36

转储设备 245

sysdevices 表 251

删除 262

信息 261

转储数据库语法 646

转换。

请参见 字符集

转移的行

使用 **default exp_row_size** 配置参数减少 98

装载, 数据库

number of large i/o buffers 配置参数 103, 146, 169, 174

装载数据库语法 646

状态转换

LDAP 服务器 493

资源不足错误 (级别 17) 328

资源限制

配置 78

自定义口令复杂程度检查 423

自定义口令检查 428

自动 LDAP 改进 501

自动操作

登录中的字符转换 462

自动用户鉴定改进 501

自由选择访问控制 (DAC) 511–553

另请参见 权限

dbcc 命令 528

存储过程 548

概述 358

视图 546

授予和撤销权限 516

系统管理员 512

用户别名 536

字符

不允许使用的登录名 462

无法转换 315

- 字符集 97
 - 另请参见 日语字符集
 - ID 号 97
 - Unicode 276
 - 阿拉伯语 276
 - 波罗的语 276
 - 不同字符集的编码 309
 - 朝鲜语 276
 - 定义 275
 - 定义文件 304
 - 东欧 276
 - 多字节 300
 - 多字节, 更改为 301
 - 俄语 276
 - 繁体中文 276
 - 改变后升级文本值 300
 - 更改 293
 - 古斯拉夫语脚本 276
 - 简体中文 276
 - 客户端与服务器之间的转换 310–311
 - 客户端与文件系统之间的转换 318
 - 客户端与终端之间的转换 318
 - 欧洲货币符号 277
 - 配置后重建索引 299–301
 - 缺省 281
 - 日语 276
 - 泰语 276
 - 土耳其语 276
 - 西欧语言 276
 - 希伯来语 276
 - 希腊语 276
 - 语言组的 276
 - 越南语 276
 - 支持的转换方式 310–315
 - 转换错误 315
 - 转换文件, 终端特定 304, 319
- 字符集的二进制排序顺序
 - 字符集更改和数据库转储 295
- 字符集和口令保护的转储 647
- 字符集转换 309, 316–317
- 字节
 - 字符 315
- 阻止碎片收集
 - 累计空白页 337
- 组 377
 - 另请参见 public 组
 - grant** 521
 - public** 49
 - revoke** 521
 - 创建 381
 - 更改 405
 - 命名 381
 - 删除 400
 - 相互冲突的权限 533
 - 语言 276
- 最小
 - 大小, **disk resize** 263
 - 口令中大写字母的数目 424
 - 口令中的数字数目 423
 - 口令中的字母字符 423