CA Access Control

参考指南

12.6

第三方通知

示例脚本和示例 SDK 代码

CA Access Control 产品随附的示例脚本和示例 SDK 代码均“按原样”提供，仅供参考之用。 在特定环境下，可能需要对它们进行调整，而且在生产系统中部署它们之前，未经事先测试和验证不应将其用于生产。

CA Technologies 不向这些示例提供支持，而且对于这些脚本可能会引起的任何错误概不负责。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control 企业版
- CA Access Control
- CA Single Sign-On (CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM，以前为 Unicenter NSM 和 Unicenter TNG）
- CA Software Delivery（以前为 Unicenter Software Delivery）
- CA Service Desk（以前为 Unicenter Service Desk）
- CA User Activity Reporting Module（以前是 CA Enterprise Log Manager）
- CA Identity Manager

文档约定

CA Access Control 文档使用以下约定：

格式	含义
等宽字体	代码或程序输出
斜体	重点或新术语
粗体	必须完全按照显示内容键入的文本
正斜杠 (/)	用于描述 UNIX 和 Windows 路径的独立于平台的目录分隔符

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

格式	含义
斜体	您必须提供的信息
用方括号括起来 ([])	可选运算符

格式	含义
用大括号括起来 ({})	强制运算符集
用管道符 (|) 分隔的选项。	分隔可选运算符（选择一项）。 例如：下面的示例*既*可以表示用户名，*也*可以表示组名： `{username|groupname}`
…	指明前面的项或项组可以重复
下划线	默认值
前面带空格的行尾反斜杠 (\)	有时，在本指南中，一行无法容纳一个命令。 在这些情况下，行结尾处的空格加上反斜杠 (\) 就表示该命令延续到下一行。 **注意：**请勿复制反斜杠字符，并且请省略换行符。 这些不是实际命令语法的一部分。

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

在该示例中：

- 命令名称 (ruler) 以常规等宽字体显示，必须按照显示内容键入。
- *className* 选项以斜体显示，因为它是一个类名（例如 USER）的占位符。
- 即使不带有方括号中的第二部分，您也可以运行该命令，方括号表示该运算符是可选的。
- 使用可选参数 (props) 时，可以选择关键字 *all*，也可以指定一个或多个属性名（以逗号分隔）。

文件位置约定

CA Access Control 文档使用以下文件位置约定：

- *ACInstallDir*—默认 CA Access Control 安装目录。
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/CA/AccessControl/
- *ACSharedDir*—CA Access Control for UNIX 使用的默认目录。
  - UNIX—/opt/CA/AccessControlShared

- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—默认分发服务器安装目录。
  - /opt/CA/DistributionServer
- *JBoss_HOME*—默认 JBoss 安装目录。
  - /opt/jboss-4.2.3.GA

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

文档更改

从上一版本以来对该文档进行了以下更新：

- 实用程序－在此更新章节中更新了以下实用程序、服务和后台进程：
  - acuchkey
  - seaudit
  - sepmd
  - uxconsole -verify
- 配置文件－在此更新章节中添加或更改了以下部分：
  - seos.ini－seosd
  - 审核日志路由配置文件 selogrd.cfg
  - uxauth.ini－ad
  - uxauth.ini－agent
  - uxauth.ini－map

目录

附录 A： 审核日志记录 525

第 1 章： 简介

此部分包含以下主题：

关于本指南

本指南提供了有关 CA Access Control 实用程序、配置文件、状态代码和消息等的信息。 本指南也随 CA Access Control 企业版 提供，CA Access Control 企业版 提供企业管理和报告功能，以及高级策略管理功能。

为了简化术语，在本指南中我们将此产品称为 CA Access Control。

使用本指南的用户

本指南是为执行命令或维护和配置受 CA Access Control 保护的环境的安全和系统管理员编写的。

第 2 章： 实用程序

CA Access Control 具有多个实用程序。 为便于参考，本章按字母顺序对它们进行了说明。

acpwd 实用程序—签入和签出特权帐户密码

可使用 特权用户密码管理 代理从 CA Access Control 端点获得特权帐户密码。 通过使用命令行运行 特权用户密码管理 代理，您可以连接 CA Access Control 企业管理 以签入、签出和检索特权帐户密码。

此命令格式如下：

```
acpwd {-checkin | -checkout | -get} -account name -ep name -eptype type -container name -[timeout <timeout>] [-nologo] [-help]
```

-checkin

执行特权帐户密码签入过程。

-checkout

执行特权帐户密码签出过程。

-get

检索特权帐户密码，而不执行签出过程。

-account *name*

定义要签出或签入的特权帐户密码。

-ep *name*

定义特权帐户所在端点的名称。

-eptype *type*

指定端点的类型。

示例：Windows Agentless

-container *name*

定义帐户所在容器的名称。

-nologo

指定输出中仅显示密码而没有任何其他信息。

-timeout *timeout*

指定等待服务器响应的超时期间（秒）。

-help

显示帮助文件。

acuxchkey 实用程序－更改加密密钥设置

可使用 acuxchkey 实用程序来更改加密密钥和消息队列设置。 此命令格式如下：

```
acuxchkey -t -pwd password
```

-t

指定消息队列更改选项。

-pwd *password*

定义消息队列密码。

示例：更改消息队列密码

该命令在数据库中保存更改的消息队列加密密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
acuxchkey -t -pwd "secret"
```

示例：更改分发服务器通讯设置

此示例展示了如何将分发服务器设置更改为使用 SSL：

```
env config
editres CONFIG accommon.ini section (communication) token (Distribution_Server)
value ("ssl://DS_host:7243")
```

更多信息：

sechkey 实用程序－更改消息队列密码 (p. 116)

ChangeEncryptionMethod 实用程序－更改加密方法

在 UNIX 上有效

ChangeEncryptionMethod 实用程序可更改加密方法。

注意：此实用程序以脚本文件形式提供，位于 lbin 目录中。

运行此实用程序时，可以选取以下加密方法之一：

- DEFAULT
- AES（128 位、192 位、或 256 位）
- DES
- TRIPLEDES
- SCRAMBLE

如果未指定加密方法，此实用程序将提示您进行指定。 此实用程序会在系统中搜索现有的策略模型，通过运行“sepmd -de pmd_name”将策略模型解密，然后通过将 libcrypt 链接到新的共享库（libaes128、libaes192、libaes256、libdes、libtripledes 或 libscramble）更改加密方法。

注意：要运行此实用程序，CA Access Control 必须正在运行。 为更改加密方法，脚本会询问您是否可以暂时关闭 CA Access Control。

重要说明！ 确定在 CA Access Control 企业管理 服务器和 CA Access Control 端点上使用相同的加密方法。 如果选择更改现有 CA Access Control 端点的加密方法，则所有密码历史记录将丢失。

此命令格式如下：

```
ChangeEncryptionMethod.sh [DES|TRIPLEDES|SCRAMBLE|AES128|AES192|AES256]
```

更多信息：

sechkey 实用程序－更改对称加密方法 (p. 111)

dbmgr 实用程序

通过 dbmgr 实用程序，您可以创建、管理和维护 CA Access Control 数据库文件。

注意：此实用程序替换了先前版本中的以下实用程序：dbdump、rdbdump、dbutil、secredb、sedb2scr 和 semigrate。

重要说明！ 问题解析过程中，只有在支持人员指导下才能使用此实用程序。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

要运行 dbmgr 实用程序，必须具有 ADMIN、AUDITOR 或 SERVER 属性。

该实用程序可处理多个任务，并具有以下关联函数：

任务	函数
创建数据库 (p. 32)	`dbmgr -create`
显示数据库信息 (p. 35)	`dbmgr -dump`
创建可定义数据库的脚本 (p. 37)	`dbmgr -export`
将数据库复制到平面文件 (p. 38)	`dbmgr -migrate`
管理现有的数据库 (p. 40)	`dbmgr -util`
备份数据库 (p. 41)	`dbmgr -backup`
还原数据库 (p. 42)	`dbmgr -restore`

dbmgr -create 函数—创建数据库

dbmgr -create 函数可生成一个新的空数据库。 仅在安装时或要创建数据库或 PMDB 时使用此函数。 CA Access Control 可在当前目录中创建数据库。

注意：如果要将用户定义的类添加到新数据库中，请在创建新的数据库之后先运行 seclassadm 实用程序。-

此命令格式如下：

```
dbmgr {-create|-c} {-c[q]|-h} [-d] [-f filename] \
    [-n] [-o] [-t terminalNames] \
    [-u userName [,userName...]] [-ux userName [,userName...]]\
    [-v] [-w] [-k] [-n pathName]
```

-create|-c

执行 dbmgr 实用程序的数据库创建函数。

-c

提示您是否要创建一个新数据库。

-cq

在不事先提示的情况下创建一个新数据库。

-h

显示此函数的帮助。

-d

打印数据库布局文档。 输出包括在数据库中使用的结构和属性格式的完整说明。

-f *filename*

定义可直接输出至的文件，而非标准输出设备。

-k

数据库创建完成后，指定运行共存实用程序。

-n *pathName*

（仅限 UNIX）。 定义要备份的 CA Access Control 数据库的完整路径名。

创建新数据库时，将生成一个基本类方案。 使用 seclassadm 实用程序将新类添加到数据库时，类信息将存储在数据库目录下的文件中。要使用其类方案备份特定数据库（例如策略模型数据库），请使用 -n 选项指定其位置。将从该位置提取用户定义的类信息。如果未指定 -n 选项，则将在要创建数据库的本地目录中搜索类信息文件。 如果从该处未找到，则将从活动 CA Access Control 安全数据库目录中提取该文件。

--o

将 Unicenter TNG 类添加到现有数据库中。

-t *terminalName*

定义用逗号分隔的终端的列表（从该列表中，超级用户可管理本地数据库）以在数据库中创建该列表。

-u *userName [,userName...]*

定义用逗号分隔的用户列表以在数据库中创建该列表。 这些用户被定义为 CA Access Control 安全管理员。

如果指定 -t 选项，这些用户将有权从已定义的终端管理本地数据库。

另请参阅 -ux 参数。

-xu *userName [,userName...]*

定义用逗号分隔的企业用户列表，这些用户将被定义为 CA Access Control 安全管理员。

如果指定 -t 选项，这些用户将有权从已定义的终端管理本地数据库。

如果未创建任何用户，则 dbmgr -create 将在数据库中创建一个具有 ADMIN、AUDITOR 和 IGN_HOL 属性的用户，该用户与 UNIX 中的 *root 用户*或 Windows 中的管理员对应。

--v

禁用进程消息。

--w

创建包括 Unicenter TNG 类的新数据库。

注意：-v 和 -d 选项不能同时使用。

示例：在 Windows 上创建新数据库

如果在系统提示符 c:\temp 下，请输入以下命令：

```
dbmgr -c -c -u user1 -t myterminal.company.com
```

如果确认要创建数据库，此实用程序将在 c:\temp 目录中创建一个新数据库。 此实用程序将在数据库中创建用户 *user1*，该用户具有 ADMIN、AUDITOR 和 IGN_HOL 属性，并可从终端 *myterminal.company.com* 管理该数据库。

示例：在 UNIX 上创建新数据库

如果在 \tmp\db 目录下，请输入以下命令：

```
dbmgr -c -cq -d -f dbLayout
```

此实用程序将在 \tmp\db 目录中创建一个新数据库。 还将创建一个包含数据库布局文档的文件 (dbLayout)。 默认情况下，将在数据库中创建用户 *root*，并指定其 ADMIN、AUDITOR 和 IGN_HOL 属性。

更多信息：

seclassadm 实用程序－管理 CA Access Control 类 (p. 116)
eACoexist 实用程序－检测并注册共存的受托程序 (p. 52)

dbmgr -dump 函数－显示数据库信息

dbmgr -dump 函数可生成有关数据库中记录的报告。 使用此函数可执行以下操作：

- 显示某个指定类的记录的信息
- 显示某个指定类的单个记录的信息
- 显示某个类的所有记录的信息（除某个指定记录外）
- 生成类和属性定义的列表
- 生成用户所属组的列表
- 生成特定类的记录列表

此函数假定 CA Access Control 后台进程未运行；您必须从数据库所在的目录调用它。 如果使用 -r 开关参数，CA Access Control 后台进程必须正在运行，且您必须具有 ADMIN、AUDITOR 或 SERVER 属性。 要执行此函数，您还必须具有对数据库文件的读写权限。

此命令格式如下：

```
dbmgr {-dump|-d} [-h] [-r] [-f fileName] \
    [c] [fc] [g user] [l class] [p class] [fp class] \
    [d class [props|@fileName] \
    [dn class [props|@fileName] \
    [e class record [props|@fileName] \
    [en class record [props|@fileName] \
    [o class record [props|@fileName] \
    [on class record [props|@fileName]
```

-dump|-d

执行 dbmgr 实用程序的数据库转储函数。

-f *fileName*

将输出定向到指定文件，而不是标准输出设备。

-h

显示此函数的帮助。

--r

显示有关授权后台进程当前正在使用的数据库的信息。

如果忽略此选项，dbmgr 会显示有关当前目录中的数据库的信息。

c

列出在数据库中定义的所有类的名称。

d *class* [*props*|*@fileName*]

显示某个类的所有记录的选定属性的值。 *class* 参数用于指定类。 *props* 参数用于定义您希望显示值的属性（用空格分隔）的列表。

要从文件读取属性列表，请在“at”符号 (@) 之后指定文件的完整路径名。 文件中列出的每个属性必须以单独的一行显示。

如果没有指定任何属性，则列出所有属性值。

dn *class* [*props*|*@fileName*]

与 *d* 选项相同，只是不显示具有未知值的属性。

e *class record* [*props*|*@fileName*]

显示某个类所有记录（*除*单个指定记录外）的选定属性的值。*class* 参数用于指定类。 *record* 参数用于指定要从列表中忽略的记录的名称。 *props* 参数用于定义您希望显示值的属性（用空格分隔）的列表。

要从文件读取属性列表，请在“at”符号 (@) 之后指定文件的完整路径名。 文件中列出的每个属性必须以单独的一行显示。

如果没有指定任何属性，则列出所有属性值。

en *class record* [*props*|*@fileName*]

与 *e* 选项相同，只是不显示具有未知值的属性。

fc

列出数据库中所有类的全部类信息。

fp *class*

列出指定类的属性的全部属性信息。

g *user*

列出指定用户所属的组。

l *class*

列出指定类中的所有记录。

o *class record property* / on *class record property*

显示某个类的一个记录的选定属性的值。 *class* 参数用于指定类。 *record* 参数用于指定记录。 *props* 参数用于定义您希望显示值的属性（用空格分隔）的列表。

要从文件读取属性列表，请在“at”符号 (@) 之后指定文件的完整路径名。 文件中列出的每个属性必须以单独的一行显示。

如果没有指定任何属性，则列出所有属性值。

o *class record property* / on *class record property*

与 *o* 选项相同，只是不显示具有未知值的属性。

p *class*

列出指定类的属性的名称。

注意：除 -r 和 -f 之外，只能再指定一个其他选项。

dbmgr -export 函数－创建可定义数据库的脚本

dbmgr -export 函数可复制其他站上的数据库。 它可生成一个由定义现有数据库所需的 selang 命令组成的脚本。

注意：使用本地命令（例如：UNIX 上的 cp 或 tar，或 Windows 上的 copy）时，如果数据库文件不使用相同的字节顺序，则无法将数据库文件从一种体系结构复制到另一种体系结构。 例如：您无法将数据库从基于 Sparc 的计算机复制到基于 Intel 的计算机，因为这两种计算机使用的字节顺序不同。

重要说明！ 首先查看一下脚本，然后再执行。

此命令格式如下：

```
dbmgr {-export|-e} {-l|-r} [-c className] [-f fileName]
```

-export|-e

执行 dbmgr 实用程序的数据库导出函数。

-h

显示此函数的帮助。

-l

导出当前目录中的数据库。

注意：此选项假定 CA Access Control 后台进程未运行。 如果此后台进程正在运行，那么它将假定您正在与该后台进程所使用的数据库不同的数据库中执行操作。

--r

导出 CA Access Control 当前正在使用的数据库。 您必须具有 ADMIN 或 SERVER 属性，且 CA Access Control 后台进程必须正在运行。

-c *className*

定义要从数据库中导出的类（用空格分隔）的列表。

-f *fileName*

将输出定向到指定文件，而不是标准输出设备。 然后可通过该文件创建一个新的数据库，方法是指示 selang 从该文件中读取命令。

dbmgr -migrate 函数—将数据复制到平面文件

dbmgr -migrate 函数可以将现有数据库中用户和程序记录的数据复制到平面文件（二进制格式）。 也可以将数据从平面文件复制到新的数据库。 从中导入数据的数据库必须是 1.21 版本或更高版本。

将平面文件复制到新数据库时，请使用创建该平面文件时所用的该函数的同一版本。 如果您有多个版本，强烈建议您使用最新的版本。

注意：为了更好地保证安全，在将数据从旧数据库复制到新数据库以后，请删除旧数据库、用于生成新数据库的脚本，以及此函数创建的平面文件。

重要说明！ 在使用该函数前，务必创建数据库的备份。

此命令格式如下：

```
dbmgr {migrate|-m} {-r|-w|-h} [-s] filename \
    [-v versionNumber] [-f fileName]
```

-migrate|-m

执行 dbmgr 实用程序的数据库迁移函数。

filename

定义要从中复制数据或将数据复制到其中的平面文件。

-f *filename*

将输出定向到指定文件，而不是标准输出设备。

-h

显示此函数的帮助。

--r

读取当前目录中的数据库，并将某些数据复制到平面文件 *filename* 中。

-s

使用 CA Access Control 服务器从数据库读取信息，而不直接读取数据库。 此选项仅在与 -r 开关参数一起使用时有效。

您必须具有管理员权限以及对终端的 R（读取）和 W（写入）权限才能使用此选项。

如果您未指定此选项，该函数将从当前目录中的数据库进行读取或写入到此数据库。

-v *versionNumber*

读取由先前版本创建的平面文件。该选项仅对 -w 命令有效。在文件名后输入此选项，并提供版本号。

--w

读取平面文件 *filename*，并将数据复制到当前目录中的数据库。

示例：将现有数据库中的数据复制到新数据库

下列步骤说明如何将当前数据库中的数据复制到新数据库。 假定旧数据库位于目录 /tmp/old_db 中。 假定新数据库位于目录 *ACInstallDir*/seosdb（其中 *ACInstallDir* 是 CA Access Control 的安装目录）。

注意：此步骤是使用 UNIX 路径名编写的，不过通过修改这些路径名（根据需要）也可在 Windows 上执行。

1. 作为超级用户登录。
2. 如果 CA Access Control 后台进程正在运行，请使用以下命令将其关闭：

   ```
   secons -s
   ```

3. 将旧数据库复制到其他位置或备份介质，从而为其创建备份。
4. 将数据库复制到 /tmp/old_db 中，然后针对旧数据库运行 dbmgr 实用程序，从而创建复制旧数据库的脚本：

   ```
   cd /tmp/old_db
   /opt/CA/AccessControl//bin/dbmgr -export -l -f lang_script
   ```

5. 新建数据库：

   ```
   cd /opt/CA/AccessControl//seosdb
   /opt/CA/AccessControl//bin/dbmgr -c -cq
   ```

6. 执行在上一步生成的脚本，并新建数据库：

   ```
   cd /opt/CA/AccessControl//seosdb
   /opt/CA/AccessControl//bin/selang -l /tmp/old_db/lang_script
   ```

7. 执行 dbmgr 实用程序以创建包含旧数据库中数据的平面文件：

   ```
   cd /tmp/old_db
   /opt/CA/AccessControl//bin/dbmgr -migrate -r flat_file
   ```

8. 将平面文件中的数据装入到新数据库中：

   ```
   cd /opt/CA/AccessControl//seosdb
   /opt/CA/AccessControl//bin/dbmgr -migrate -w /tmp/old_db/flat_file
   ```

dbmgr -util 函数—管理现有数据库

dbmgr -util 函数可在数据库上执行管理和维护操作。 它假定 CA Access Control 当前未运行。 从数据库所在的目录中调用此函数。

-util 选项用于管理和操作由参数 *filename* 指定的本地数据库。 数据库文件具有扩展名 .dat 并且必须是 DBIO 文件。 对于数据库索引文件（扩展名为 .001 的文件），不能使用 -util 选项。

此命令格式如下：

```
dbmgr {-util|-u} [-h] \
    [-all filename] \
    [-build filename] \
    [-check] \
    [-close] \
    [-dump filename] \
    [-dup src dst] \
    [-fast] \
    [-free filename] \
    [-index filename] \
    [-key filename] \
    [-load db ascii \
    [-scan filename] \
    [-scana filename] \
    [-stat filename] \
    [-verify] \
    [-f fileName]
```

-util-u

执行 dbmgr 实用程序的数据库管理和维护函数。

-all *filename*

执行所有索引检查；与指定 *-index* 和 *-free* 选项相同。

-build *filename*

基于数据记录生成 DBIO 的索引。

-check

（仅限 UNIX）。 对所有数据库文件的所有索引条目执行快速完整性和一致性检查。

--close

如果数据库处于打开状态，则将其关闭。

-dump *filename*

将数据文件以 ASCII 格式转储在标准输出设备上。

-dup *src dst*

基于文件标头复制 DBIO 文件。

-f *fileName*

将输出定向到指定文件，而不是标准输出设备。

--fast

对所有数据库文件的所有索引条目执行快速完整性检查。

-free *filename*

检查自由索引。

-index *filename*

检查索引的一致性。

-key *filename*

按顺序扫描索引文件。

-load *db* ascii

加载 ASCII 文件并将其转换为 DBIO 文件。

-scan *filename*

按顺序扫描数据库。

-scana *filename*

按顺序扫描数据库，包括已删除的记录。

-stat *filename*

列出数据库文件的标头信息。

-verify

（仅限于 UNIX）。验证某些预定义对象是否存在于数据库中，例如：所有类的 SEOS、ADMIN 和 UACC。

dbmgr -backup 函数—备份数据库

dbmgr -backup 函数可在指定目录中创建 CA Access Control 数据库的联机备份。 无论 CA Access Control 后台进程是否正在运行，此函数均可用。

此命令格式如下：

```
dbmgr {-backup|-b} backup_directory
```

-backup|-b

执行 dbmgr 实用程序的数据库备份函数。

backup_directory

定义备份目录。 无法在远程计算机上找到此目录；如果此目录不存在，则此函数可创建此目录。

dbmgr -restore 函数—还原数据库

在 UNIX 上有效

dbmgr -restore 函数可在指定目录中为 CA Access Control 数据库执行联机还原。 无论 CA Access Control 后台进程是否正在运行，此函数均可用。

此命令格式如下：

```
dbmgr {-restore|-r} restore_directory
```

-restore|-r

执行 dbmgr 实用程序的数据库还原函数。

restore_directory

定义要还原的数据库所在的目录。

defclass 实用程序—将用户定义的资产类型定义为类

CA Access Control 在每个 CA Access Control 数据库以及每个已定义的新 PMDB 中定义基本的 Unicenter TNG 资产类型。 defclass 脚本可将用户定义的安全资产类型定义为 CA Access Control 数据库中的 CA Access Control 类。-

注意：选择 Unicenter 集成时，安装程序会自动执行此脚本。 无论何时新建 PMDB，都可以（并且应该）手工调用该脚本。

此命令格式如下：

```
defclass
```

注意：在 UNIX 上，此实用程序作为脚本文件提供；您需要指定 .sh 扩展才能运行此程序。 只有启用 Unicenter 集成（默认情况下，处于禁用状态），才能使用此实用程序。

DictImport 实用程序－导入字典文件

DictImport 实用程序可准备字典文件并将其导入到 CA Access Control 数据库中。 安装 CA Access Control 后，必须将字典文件导入到 CA Access Control 数据库中，然后将其激活，以便可以设置密码保护。

DictImport 实用程序将 use_dbdict 密码规则设置为 *db*，并激活 DICTIONARY 类和 PASSWORD 类。

注意：如果 PASSWORD 类不活动，则禁用集中字典。

此命令格式如下：

```
DictImport [-h] [-o selangFilename] [-f dictionaryFilename]
```

注意：此实用程序以脚本文件形式提供，位于 lbin 目录中。

-f *dictionaryFilename*

生成从指定文件导入所有字典单词的 selang 命令。如果忽略此选项，则将通过配置设置中的值定义字典文件。

-h

显示该实用程序的帮助。

-o *selangFilename*

将 selang 命令写入到指定文件。 如果忽略此选项，selang 命令将写入到标准输出设备。

dmsmgr 实用程序

通过 dmsmgr 实用程序，您可以管理高级策略管理基础结构。 基础结构组件包括 CA Access Control 端点、部署映射服务器 (DMS) 和分发主机 (DH)。

该实用程序可处理多个任务，并具有以下关联函数：

任务	函数
创建 DMS 或 DH (p. 44)	`dmsmgr -create`
删除 DMS 或 DH (p. 45)	`dmsmgr -remove`

任务	函数
删除 DMS 数据库中过时节点 (p. 46)	`dmsmgr -cleanup`
配置高级策略管理 (p. 46)	`dmsmgr -config`
还原 DMS 或 DH (p. 47)	`dmsmgr -restore`

dmsmgr -create 函数能—创建 DMS 或 DH

dmsmgr -create 函数可在安装了 CA Access Control 的计算机上创建部署映射服务器 (DMS) 或分发主机 (DH)。

注意：也可以在安装过程中创建 DMS 或 DH。

注意：将始终授予运行此实用程序的用户管理创建的 DMS 或 DH 的权限。

此命令格式如下：

```
dmsmgr -create -auto [-osgroups] [-admin user [,user...]] [-xadmin user [,user...]]
\
[-desktop hosts]

dmsmgr -create -dms name \
[-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts] [-subscriber dh-names]

dmsmgr -create -dh name [-parent dms_name@hostname] \
[-admin user [,user...]] [-xadmin user [,user...]] \
[-desktop hosts]
```

-admin *user* [,*user*...]]

（可选）将内部用户定义为创建的 DMS 或 DH 的管理员。

-auto

使用默认名称（DMS__、DH__ 和 DH__WRITER）创建 DMS 和 DH。

使用此选项可轻松创建 DMS 和 DH 以及它们之间所需的关联。

-osgroups

（可选）指定在创建 DMS 时创建预定义的主机组。

-desktop *hosts*

（可选）定义对附带创建的 DMS 或 DH 的计算机具有 TERMINAL 访问权限的计算机列表（用逗号分隔）。

注意：无论指定与否，运行此实用程序的终端都将始终被授予对创建的 DMS 或 DH 的管理权限。

-dh *name*

使用在本地主机上 *name* 所指定的名称创建 DH。

注意：如果使用此选项创建 DH，则 CA Access Control 将使您了解到此时需要同步 DMS 和 DH，即使已订阅 DH 且之前未发送任何策略。此消息是对您需要采取的步骤的提醒，可能不会指示实际情况。 如果您完成了所有所需的步骤，则可以安全地忽略此消息。

-dms *name*

使用在本地主机上 *name* 所指定的名称创建 DMS。

-parent *dms_name@hostname*

（可选）定义创建的 DH 要将端点通知发送到的 DMS。指定以下格式的 DMS：*DMS_name@hostname*。

-subscriber *dh_names*

（可选）定义创建的 DMS 要将策略更新到的 DH PMDB 的列表（用逗号分隔）。 指定以下格式的 DH：*DH_name@hostname*。

-xadmin *user* [*,user...*]]

（可选）将企业用户定义为创建的 DMS 或 DH 的管理员。

dmsmgr -remove 函数—删除 DMS 或 DH

dmsmgr -remove 函数可删除安装了 CA Access Control 的计算机上的 DMS 或 DH。

此命令格式如下：

```
dmsmgr -remove {-dms|dh} name
```

```
dmsmgr -remove -auto
```

-auto

删除本地主机上的默认 DMS 和 DH。

这些是默认情况下，在安装过程中或使用 dmsmgr -create -auto 时创建的 DMS 和 DH 数据库。

-dh *name*

从本地主机上删除 *name* 所指定名称的 DH。

-dms *name*

从本地主机上删除 *name* 所指定名称的 DMS。

dmsmgr -cleanup 函数—删除过时节点

dmsmgr -cleanup 函数可从 DMS 或 DH 数据库中删除过时节点。 这些是表示在指定的时间内已不可用的 CA Access Control 节点的 HNODE 对象。

注意：作为例行维护程序，您应从 DMS 和 DH 中清理这些过时节点。

此命令具有以下格式：

```
dmsmgr -cleanup {-hnode|-deployment} -days number {-dms|-dh} name
```

```
dmsmgr -cleanup -policy name -vcount number {-dms|dh} name
```

-hnode

删除代表已超过 *number* 天不可用的 CA Access Control 节点的 HNODE 对象。

-deployment

删除早于 *number* 天的 DEPLOYMENT 对象。

-policy *name*

删除属于指定策略且早于 *number* 版本的 POLICY 对象（策略版本）。

-dh *name*

定义要从中删除过时节点的 DH 的名称。

-dms *name*

定义要从中删除过时节点的 DMS 的名称。

-vcount

定义要保持的版本号。

dmsmgr -config 函数—配置高级策略管理

dmsmgr -config 函数可配置高级策略管理。

此命令格式如下：

```
dmsmgr -config[-] [host_name] {-endpoint|-dhname names|-drname names}
```

```
dmsmgr -config -osgroups [-dms name]
```

-config[-]

配置或删除高级策略管理的配置。

-dhname *names*

配置要与分发主机列表（用逗号分隔）一起使用的端点。

-dms *name*

定义在其上创建自动主机组的 DMS 的名称。

-drname *names*

配置要与灾难恢复分发主机列表（用逗号分隔）一起使用的端点。

-endpoint

为高级策略管理配置端点。

host_name

执行 *host_name* 中的配置。 如果未指定主机，则执行本地计算机中的配置。

-osgroups

将自动主机组添加到 DMS 中。

注意：有关自动主机组的详细信息，请参阅*《企业管理指南》*。

dmsmgr -restore 函数—还原 DMS 或 DH

dmsmgr -restore 函数可从备份文件中还原 DMS 或 DH。 您可以在 CA Access Control 正在运行或已停止时，以覆盖现有 DMS 的方式还原 DMS 或 DH，也可以将 DMS 或 DH 还原至新目录。

此命令格式如下：

```
dmsmgr -restore -dms name -source path\
[-replica name|-parent name] [-subscriber dhname[,dhname...]]\
[-admin user[,user...]] [-xadmin user[,user...]]

dmsmgr -restore -dh name -source path\
[-parent name] [-admin user[,user...]]\
[-xadmin user[,user...]] [-desktop host[,host...]]
```

-admin *user*[,*user*...]

(UNIX) 将内部用户定义为还原的 DMS 或 DH 的管理员。

-desktop *host*[, *host*...]

（可选）定义对附带已还原 DH 的计算机具有 TERMINAL 访问权限的计算机列表。

注意：无论指定与否，运行此实用程序的终端将始终被授予对已还原 DH 的管理权限。

-dh *name*

定义在本地主机上还原的 DH 的名称。

-dms *name*

定义在本地主机上还原的 DMS 的名称。

-parent *name*

（可选）定义订户父项的名称。如果在灾难恢复部署方面对 CA Access Control 进行了设置，并且要还原灾难恢复 DMS 或 DH，则可使用此参数。 如果要还原灾难恢复 DMS，请指定生产 DMS 的名称；如果要还原 DH，请指定父 DMS 的名称。 请按以下格式指定父 DMS：*name@hostname*。

-replica *name*

（可选）定义灾难恢复 DMS 的名称。如果在灾难恢复部署方面对 CA Access Control 进行了设置，并且要还原生产 DMS，可使用此参数。请按以下格式指定灾难恢复 DMS 的名称：*DMS_name@hostname*。

-source *path*

定义包含要还原的备份文件的目录。

-subscriber *dh_name*[, *dh_name*...]

（可选）定义还原的 DMS 要将策略更新发送到的 DH 的列表（以逗号分隔）。 指定以下格式的 DH：*DH_name@hostname*。

-xadmin *user*[,*user*...]

(UNIX) 将企业用户定义为还原的 DMS 或 DH 的管理员。

eacpg_gen 实用程序－定义最佳实践策略

在 Linux 上有效

eacpg_gen 也称为策略生成器。 此菜单驱动的实用程序提供了一种为 CA Access Control 应用程序定义策略的快捷方法。 策略生成器可在不具有任何 CA Access Control 规则的测试系统上使用。 其目的是通过对那些重要的电子资产应用最佳安全操作，保护企业应用程序和（或）操作系统及其机密数据。

使用“default-deny”模式创建应用程序单元。 这些策略类似于 UNIX chroot() jail 的概念。 为面向 Internet 的应用程序生成此类策略时，使用该应用程序对主机的安全所造成的风险可大大降低。

应用程序单元是阻止应用程序的 Access Control 列表 (ACL) 规则。 对于每个应用程序，eacpg_gen 均可生成许多应用程序单元。 应用程序单元只强制访问特定资源。 受单元策略保护的任何进程在策略中都不能访问没有明确为该进程授予访问权限的资源。 这样就阻止了可能的攻击者向未经授权的磁盘区域中写入信息，或执行未经授权的二进制文件。

注意：请确认在运行此实用程序之前，数据库中存在 secadmin 和 组 secadmin。

策略生成包括几个关键步骤：

- 初始化
- 应用程序检查
- 应用程序测试
- 策略生成
- 应用策略
- 测试策略

此命令格式如下：

```
eacpg_gen \
    [-u user] \
    [-g group] \
    [-p path] \
    [-o owner] \
    [-w wheel] \
    [-m machine] \
    [-a] \
    [-s file] \
    [-# step] \
    [-x]
```

-u *user*

指定运行该进程的用户。

-g *group*

指定将拥有该进程的组名。

-p *path*

指定程序的完整路径。

-o *owner*

指定策略所有者。

-w *wheel*

设置为“secadmins”组（建议）。

-m *machine*

指定计算机名称。

-a

设置是否应用生成的规则。

-s *file*

指定存储策略规则的完整路径和文件名。

-# *step 1-2*

应设置为 2。

-x

在警告模式与失败模式之间切换。

示例：运行策略生成器

1. （初始化）。 执行策略生成器：

   ```
   eacpg_gen
   ```

2. 在提示下键入 **y**，将系统置于警告模式。
3. 通过可执行文件的完整路径提供策略生成器，例如：

   ```
   /work/WebServers/apache_1.3.26/bin/htppd
   ```

4. 接受默认用户名。
5. 接受默认组名。
6. 在提示下键入 **y**，验证信息是否正确。

   （应用程序检查）。 策略生成器开始在要为其创建策略的进程中收集数据。

7. 确认屏幕上的信息，然后按 Enter 键。
8. （应用程序测试）。 启动应用程序。 例如：

   ```
   ./apachectl start
   ```

9. 停止应用程序。 例如：

   ```
   ./apachectl stop
   ```

   注意：此时您已经启动了应用程序，然后又将其停止。 最好重新启动它并允许收集正常使用情况的数据。 您可以让该检查运行任意长的时间；运行时间越长，策略生成器收集的数据越多，生成的策略越准确。 当认为已收集到足够的数据时，请继续下一步。

10. （策略生成）。 将该策略存储为一个文件（输入 *filename*.txt，然后按 Enter 键）。

11. （策略应用）。 键入 **y** 应用策略。

12. 键入 **y** 将系统置于*失败*模式，然后开始开始策略实施。

13. （策略测试）。 测试该策略。

    下面的示例屏幕显示了对一个名为 evil.html 的文件进行的策略测试。

    ```
    Linux:/srv/www/htdocs: #telnet localhost 80
    Trying ::1...
    telnet: connect to address ::1: Connection refused
    Trying 127.0.0.1...
    Connected to localhost.
    Escape character is '^]'.
    GET /evil.html
    <!DOCTYPE HTML PUBLIC “-//IETF//DTD HTML 2.0//EN”>
    <HTML><HEAD>
    <TITLE>403 Forbidden</TITLE>
    <HEAD><BODY>
    <H1>Forbidden</H1>
    You don't have permission to access /evil.html
    on the server. <P>
    <HR>
    <ADDRESS>Apache/1.3.26 Server at linux.local Port 80</ADDRESS>
    </BODY></HTML>
    Connection closed by foreign host.
    Linux:/srv/www/htdocs# []
    ```

    由于该策略已应用，因此不能再使用文件 evil.html。 原因是它超出了正常使用情况的配置范围。

eACoexist 实用程序－检测并注册共存的受托程序

在 Windows 上有效

eACoexist 实用程序将检测在本地系统中共存的所有程序（例如：CA Anti-Virus）。 如果检测到的程序已受托，CA Access Control 将使用 SPECIALPGM 规则注册该程序。 特殊程序规则可定义该程序的访问类型并确保 CA Access Control 授予访问权限时跳过它。

此命令格式如下：

```
eACoexist [plug-in-path]
```

plug-in-path

（可选）定义您希望共存程序使用的共存插件所在的文件夹路径。

如果您未定义路径，程序将使用存储共存插件的默认路径 (*ACInstallDir*/Coexistence)。

更多信息：

共存实用程序的工作方式 (p. 53)
response.ini — 配置共存实用程序 (p. 67)

共存实用程序的工作方式

通过 CA Access Control 提供的共存实用程序 (eACoexist)，您可以解决与本地计算机上其他程序的潜在冲突。 要了解 CA Access Control 以何种方式解决这些潜在的冲突，以及怎样才能够影响解决冲突的方式，您需要了解实用程序的工作方式。

共存实用程序运行时，将执行以下操作：

1. 检查是否符合以下条件之一：
   a. CA Access Control 未运行。
   b. 您具有 ADMIN 属性。

   如果未应用任一条件，则退出实用程序。
2. 查找 response.ini 文件，如下所示：
   - 如果实用程序在安装期间运行，将使用路径 *media_drive*:\Coexistence_*architecture*
   - 如果 CA Access Control 已安装在计算机上，将使用以下注册表键值：

     HKLM\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SeOSD\ResponseFile

   如果文件不存在，则退出实用程序。
3. 查找共存插件目录，如下所示：
   - 如果运行实用程序并通过命令行传递参数，它将把此路径作为插件的路径。
   - 如果实用程序在安装期间运行，将使用路径 *media_drive*:\Coexistence_*architecture*
   - 如果不使用参数运行实用程序，它会将字符串“\Coexistence”连接到以下注册表键值：

     HKLM\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SeOSPath

   如果该目录不存在，或该目录中没有共存插件，则退出实用程序。
4. 执行搜索过程。

   要执行此过程，将枚举共存插件目录中的可执行文件并逐一执行这些文件，如下所示：
   a. 将插件执行结果存储在 %windir%\EACDiscovery.ini

      注意：实用程序成功完成插件搜索过程后，将自动删除此文件。
   b. 请检查是否存在输出文件 EACDiscovery.ini。

      如果不存在该文件，实用程序将继续执行下一个插件。

c. 对于 EACDiscovery.ini 中的每个产品部分，将部分（产品）名称和版本值连接起来，并检查响应文件是否包含匹配的部分。

注意：response.ini 文件包含每个共存程序的一部分。 如果一个部分名称出现版本号（例如：eTrust Audit-1.5），实用程序将仅对指定版本执行操作。

d. 如果响应文件中存在匹配的部分，将执行由该部分中的 Act-Utility-0 值所设置的操作，如下所示：

- **1**－发出搜索到的产品与 CA Access Control 不兼容的警告。
- **2**－停止搜索产品的服务。

  实用程序将在 EACDiscovery.ini 文件中检索搜索到的产品的服务。
- **3**－与 2 相同，但是在安装 CA Access Control 期间。
- **4**－启动搜索到的产品的服务。

  实用程序将在 EACDiscovery.ini 文件中检索搜索到的产品的服务。
- **5**－为搜索到的产品的进程创建受托程序规则 (SPECIALPGM) 并启动 CA Access Control。

  实用程序将在 EACDiscovery.ini 文件中检索搜索到的产品的进程。 它还将在此文件中检索各自的程序类型 (pgmtype)。 然后它将创建一个临时脚本文件 (*ACInstallDir*\Data\discoveryscp)，启动 CA Access Control 时将执行该文件。
- **6**－与 2 相同，但是在卸载 CA Access Control 期间。

注意：每个部分可以包含多个操作。 例如：可以按 Act-Utility-0、Act-Utility-1 和 Act-Utility-2 的顺序执行。

更多信息：

策略管理器插件的工作方式

开始安装 CA Access Control 之前，共存实用程序会运行策略管理器插件以扫描计算机的策略管理器注册表键和可执行文件，如下所示：

- 查询是否存在以下注册表键：

  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\SeAM.Exe

  如果存在该注册表键，插件将：

  - 读取 Path 条目的值
  - 返回以下可执行文件的路径名：

    FilePathFromRegistry\Bin\SeAM.exe
  - 在安装 CA Access Control 过程中发出兼容警告

    这是响应文件中所定义的默认操作。 默认情况下，策略管理器插件不添加受托程序 (SPECIALPGM) 规则。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。 此外，策略管理器应用程序不再随 CA Access Control 提供。

BrightStor 插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 BrightStor 插件以扫描计算机中的 CA BrightStor 注册表键和可执行文件，如下所示：

1. 查询是否存在以下注册表键：

   HKLM\SOFTWARE\ComputerAssociates\BrightStor ARCserve Backup\UniversalClientAgent\Common
   HKLM\SOFTWARE\ComputerAssociates\Cheetah\UniversalClientAgent\Common
   HKLM\SOFTWARE\ComputerAssociates\BrightStor Enterprise Backup\UniversalClientAgent\Common

   存在第一个注册表键时，该插件将：

   - 读取 Path 条目的值
   - 返回以下可执行文件的路径名：

     FilePathFromRegistry\UnivAgent.exe

   - 创建 DCM 类型的 SPECIALPGM 资源

     这是响应文件中所定义的默认操作。

2. 如果插件在步骤 1 中无法找到任何注册表键，将查询是否存在以下注册表键：

   HKLM\SOFTWARE\ComputerAssociates\BrightStor ARCserve Backup\Base\Path
   HKLM\SOFTWARE\ComputerAssociates\Cheetah\Base\Path
   HKLM\SOFTWARE\ComputerAssociates\BrightStor Enterprise Backup\Base\Path

   存在第一个注册表键时，该插件将：

   - 读取 HOME 条目的值
   - 返回以下可执行文件的路径名：

     FilePathFromRegistry\carunjob.exe

   - 创建 DCM 类型的 SPECIALPGM 资源

     这是响应文件中所定义的默认操作。

3. 如果插件在步骤 2 中也无法找到任何注册表键，查询是否存在以下注册表键：

   HKLM\SOFTWARE\ComputerAssociates\ARCserveIT\Base\Path

   如果存在该注册表键，插件将：

   - 读取 HOME 条目的值
   - 返回以下可执行文件的路径名：

     FilePathFromRegistry\ASRunJob.exe

   - 创建 DCM 类型的 SPECIALPGM 资源

     这是响应文件中所定义的默认操作。

4. 查询是否存在以下注册表键：

   ```
   HKLM\SOFTWARE\ComputerAssociates\CA BAOF\CurrentVersion
   HKLM\SOFTWARE\ComputerAssociates\BrightStor Backup Agent for Open
   Files\CurrentVersion
   ```

   存在第一个注册表键时，该插件将：

   - 读取 ServicePath 条目的值
   - 为 *ServicePathFromRegistry* 创建 DCM 类型的 SPECIALPGM 资源

     这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

Dr. Watson 插件的工作方式

在 CA Access Control 安装结束时 以及每次运行实用程序时，共存实用程序将运行 Dr.Watson 插件以扫描计算机中的 Dr.Watson 可执行文件，如下所示：

- 查询是否存在以下路径名：

  ```
  %windir%\system32\drwtsn32.exe
  ```

  如果存在该文件，插件将创建 DCM 类型的 SPECIALPGM 资源。

  这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

eTrust AV 插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 eTrust AV 插件以扫描计算机中的 CA Antivirus 注册表键和可执行文件，如下所示：

1. 读取以下注册表键条目值：

   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\InocIT.Exe\Path
   HKLM\SOFTWARE\ComputerAssociates\eTrustITM\CurrentVersion\Path\Home

   如果其中一个条目返回值，插件将创建 DCM 类型的以下 SPECIALPGM 资源：

   - *FilePathFromRegistry*\InoRT.exe
   - *FilePathFromRegistry*\InoTask.exe
   - *FilePathFromRegistry*\InocIT.exe
   - *FilePathFromRegistry*\ShellScn.exe

   这是响应文件中所定义的默认操作。

2. 读取以下注册表键条目值：

   HKLM\SOFTWARE\ComputerAssociates\ScanEngine\Path\Engine

   如果条目返回值，插件将创建 DCM 类型的以下 SPECIALPGM 资源：

   FilePathFromRegistry\InoCmd32.exe

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

Scout 插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 Scout 插件以扫描计算机中的 SurfControl Web Filter for Windows 注册表键和可执行文件，如下所示：

- 查询是否存在以下注册表键：

  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Scscout.Exe

  如果存在该注册表键，插件将：

  - 读取 Path 条目的值
  - 返回以下可执行文件的路径名：

    FilePathFromRegistry\scoutsvc.exe
  - 创建 DCM 类型的 SPECIALPGM 资源

    这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

Unicenter 插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 Unicenter 插件以扫描计算机中的 CA Unicenter 注册表键和可执行文件，如下所示：

1. 使用 CAUENV.dll 检索 CA Unicenter 目录 (*UniPath*) 的路径
2. 创建 DCM 类型的以下 SPECIALPGM 资源：
   - *UniPath*\Bin\sfauditd.exe
   - *UniPath*\Bin\secdos2.exe
   - *UniPath*\Bin\caulgnd.exe
   - *UniPath*\Bin\sccommit.exe
   - *UniPath*\Bin\dsbulist.exe
   - *UniPath*\Bin\fmpost.exe
   - *UniPath*\Bin\catlbl.exe
   - *UniPath*\Bin\caanal.exe
   - *UniPath*\Bin\cascan.exe
   - *UniPath*\Bin\causamd.exe
   - *UniPath*\Bin\acbrows.exe

- *UniPath*\Bin\secadmin.exe
- *UniPath*\Bin\dsbufcrt.exe
- *UniPath*\Bin\cnvpwd.exe
- *UniPath*\Bin\fmeng.exe
- *UniPath*\Bin\fmmscan.exe
- *UniPath*\Bin\cadevscn.exe
- *UniPath*\AGENTS\Bin\prfagent.exe
- *UniPath*\AGENTS\Bin\msexchagnt.exe

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

资产管理插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行资产管理插件以扫描计算机中的 Unicenter DSM 服务，如下所示：

1. 提取“CA Unicenter NSM Systems Performance Agent for UAM”服务的可执行文件的目录路径 (*ServicePath*)
2. 创建 REGISTRY 类型的以下 SPECIALPGM 资源：

   ServicePath\agents\bin\hpacbcol.exe
3. 提取“caf”服务的可执行文件的目录路径 (*ServicePath*)
4. 创建 REGISTRY 类型的以下 SPECIALPGM 资源：
   ServicePath\PMAgent\agents\bin\hpacbcol.exe

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序还将运行资产管理插件以扫描计算机中的 Unicenter Asset Management version 4 服务，如下所示：

1. 提取“CA Unicenter NSM Systems Performance Agent for UAM”服务的可执行文件的目录路径 (*ServicePath*)
2. 创建 REGISTRY 类型的以下 SPECIALPGM 资源：

   ServicePath\agents\bin\hpacbcol.exe

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序还将运行资产管理插件以扫描计算机中的 Unicenter DSM r11 服务，如下所示：

1. 提取“caf”服务的可执行文件的目录路径 (*ServicePath*)
2. 创建 REGISTRY 类型的以下 SPECIALPGM 资源：

   ServicePath\PMAgent\agents\bin\hpacbcol.exe

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

Windows 插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 Windows 插件以扫描计算机中的 Windows 服务和注册表键，如下所示：

1. 提取“WinMgmt”服务的可执行文件的目录路径 (*ServicePath*)
2. 创建 REGISTRY 类型的以下 SPECIALPGM 资源：

   ServicePath

   这是响应文件中所定义的默认操作。
3. 创建 PBF 类型的以下 SPECIALPGM 资源：

   %windir%\System32\cidaemon.exe

   这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

eTrust Audit 插件的工作方式

CA Access Control 安装开始前，共存实用程序将运行 eTrust Audit 插件以扫描计算机中的 eTrust Audit Version 1.5 注册表键和文件，如下所示：

1. 查询是否存在以下注册表键：

   HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\acdistagn.exe

   如果成功，它将提取“Path”值指定的 %PathFromRegistry%。

   如果存在该注册表键，插件将：

   - 读取 Path 条目的值
   - 返回以下可执行文件的路径名：

     FilePathFromRegistry\bin\acactmgr.exe
     FilePathFromRegistry\bin\SeLogRcd.exe
     FilePathFromRegistry\bin\acdistagn.exe
     FilePathFromRegistry\acdistsrv.exe
     FilePathFromRegistry\acfwrecd.exe
     FilePathFromRegistry\acrecorderd.exe
     FilePathFromRegistry\aclogrd.exe
     FilePathFromRegistry\portmap.exe
     FilePathFromRegistry\SeLogRec.exe
     FilePathFromRegistry\SeLogRd.exe
     FilePathFromRegistry\snmprec.exe

     这是响应文件中所定义的默认操作。 默认情况下 eTrust Audit 插件不添加受托程序 (SPECIALPGM) 规则。

2. 停止以下服务：

   - “eAudit Action Manager”
   - “eAudit Distribution Agent”
   - “eAudit Log Router”
   - “eAudit Recorder”
   - “eAudit Redirector”
   - “eAudit Portmap”

   如果安装了较新版本的 eTrust Audit，它将停止以下服务：

   - “eTrust Audit Action Manager”
   - “eTrust Audit Collector”
   - “eTrust Audit Distribution Agent”
   - “eTrust Audit Distribution Server”
   - “eTrust Audit FW-1 Recorder”
   - “eTrust Audit Generic Recorder”

- “eTrust Audit Log Router”
- “eTrust Audit Portmap”
- “eTrust Audit Recorder”
- “eTrust Audit Redirector”
- “eTrust Audit SNMP Recorder”

3. CA Access Control 安装完成时，它将重新启动以上服务。

共存实用程序还将运行 eTrust Audit 插件以执行以下操作：

- 卸载 CA Access Control 时停止 eTrust Audit 服务
- 卸载 CA Access Control 完成后，启动 eTrust Audit 服务

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

eTrust Audit80 插件的工作方式

共存实用程序运行 eTrust Audit80 插件以扫描计算的 eTrust Audit r8 注册表键以及 CA Access Control 安装结束时和实用程序运行时所需的文件，如下所示：

- 查询是否存在以下注册表键：

  HKLM\SOFTWARE\ComputerAssociates\eTrust Audit\Paths

  如果成功，它将提取“Path”值指定的 %PathFromRegistry%。

  如果存在该注册表键，插件将：

  - 读取 RootPath 条目的值
  - 创建 DCM 类型的以下 SPECIALPGM 资源：

    FilePathFromRegistry\bin\acactmgr.exe
    FilePathFromRegistry\bin\SeLogRcd.exe
    FilePathFromRegistry\bin\acdistagn.exe
    FilePathFromRegistry\acdistsrv.exe
    FilePathFromRegistry\acfwrecd.exe
    FilePathFromRegistry\acrecorderd.exe
    FilePathFromRegistry\aclogrd.exe
    FilePathFromRegistry\portmap.exe
    FilePathFromRegistry\SeLogRec.exe

FilePathFromRegistry\SeLogRd.exe
FilePathFromRegistry\snmprec.exe

这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

F-Secure Antivirus 插件的工作方式

共存实用程序将运行 F-Secure Antivirus 插件以扫描计算机中的 F-Secure Anti-Virus 注册表键和文件，如下所示：

- 在开始安装 CA Access Control 前，该插件将停止 F-Secure Anti-Virus 服务。
- CA Access Control 安装完成时，该插件将查询是否存在以下注册表键：

  HKLM\SOFTWARE\Data Fellows\F-Secure\Anti-Virus

  如果成功，它将提取“Path”值指定的 %PathFromRegistry%。

  如果存在该注册表键，插件将：

  - 读取 Path 条目的值
  - 创建 DCM 类型的以下 SPECIALPGM 资源：

    FilePathFromRegistry\fssm32.exe
    FilePathFromRegistry\fsgk32st.exe

    这是响应文件中所定义的默认操作。 默认情况下 eTrust Audit 插件不添加受托程序 (SPECIALPGM) 规则。
- 每次运行共存实用程序时，该插件将执行以下操作：

  a. 停止 F-Secure Anti-Virus 服务

  b. 创建与 CA Access Control 安装完成时所创建的 SPECIALPGM 资源相同的 SPECIALPGM 资源（按照之前该主题中的说明）

  c. 重新启动 F-Secure Anti-Virus 服务

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

McAfee Antivirus 插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 McAfee VirusScan 插件以扫描计算机中的 McAfee VirusScan 服务，如下所示：

1. 提取“McShield”服务的可执行文件的目录路径 (*ServicePath*)
2. 创建 DCM 类型的以下 SPECIALPGM 资源：

   ServicePath

   这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

Windows 模块安装程序插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行 Windows 模块安装程序插件以扫描计算机中的 Windows Modules Install 服务，如下所示：

1. 提取“TrusterInstaller”服务的可执行文件的目录路径 (*ServicePath*)
2. 创建 PBF 类型的以下 SPECIALPGM 资源：

   ServicePath

   这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

服务和控制器插件的工作方式

CA Access Control 安装结束时以及每次运行实用程序时，共存实用程序将运行服务和控制器插件以扫描计算机中的 Windows 服务管理可执行文件，如下所示：

1. 检查操作系统的版本是否为 Windows Vista 或更高版本

   如果操作系统是早期的 Windows 版本，插件将终止。

2. 创建 KILL 类型的以下 SPECIALPGM 资源：

   ```
   %windir%\system32\services.exe
   ```

   这是响应文件中所定义的默认操作。

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

资源承载子系统插件如何工作

在安装 CA Access Control 过程中，CA Access Control 安装进程将会运行资源承载子系统插件，而且此共存实用程序在客户执行实用程序时会运行资源承载子系统。 资源承载子系统插件会如下扫描计算机查找 Cluster Service Element：

1. 检查操作系统是否为 Windows Server 2008 或更高版本。

   如果操作系统是早期的 Windows 版本，插件将终止。

2. 检查 Cluster Service Element 是否安装在计算机中。

   如果没有安装 Cluster Service Element，插件将终止。

3. 创建 PBF 类型的以下 SPECIALPGM 资源：

   system_drive:\Windows\Cluster\rhs.exe

注意：响应文件决定共存实用程序在规定阶段执行的默认操作（安装 CA Access Control 之前和安装 CA Access Control 之后要执行的操作，等等）。

response.ini – 配置共存实用程序

在 Windows 上有效

响应文件可指示共存实用程序 (eACoexist) 运行时要执行的操作。 响应文件包含为共存实用程序运行的每款插件预定义的一组操作。 可以编辑响应文件以更改默认的插件操作。

注意：响应文件路径名在 SeOSD 部分的 ResponseFile 配置设置中指定。默认情况下，此文件为 *ACInstallDir*\Data\response.ini。

此文件格式如下：

[*部分名*]
Act-*Stage*-*#*=*Action*
...

部分名

定义与并存插件匹配部分的名称。

共存实用程序根据在此部分中定义的操作运行插件。

Act-*Stage*-*#*=*Action#*

定义希望插件在规定阶段执行的操作。

Stage

指定希望插件执行该操作的规定阶段，如下所示：

- **BeginInstall**－插件在 CA Access Control 开始安装之前执行指定的操作。
- **EndInstall**－插件在 CA Access Control 安装完成之后执行指定的操作。
- **Utility**－插件在执行共存实用程序时执行指定的操作。
- **BeginUninstall**－插件在 CA Access Control 开始卸载之前执行指定的操作。
- **EndInstall**－插件在 CA Access Control 卸载完成之后执行指定的操作。

#

指定插件在此阶段执行操作的顺序。

Action

指定用于定义插件应执行的操作的编号，如下所示：

- **1**－警告 CA Access Control 与发现的产品不兼容。
- **2**－CA Access Control 安装过程中停止提供服务。

- **3**—停止提供服务。
- **4**—开始提供服务。
- **5**—创建 SPECIALPGM 规则。
- **6**—CA Access Control 卸载过程中停止提供服务。

示例：Dr. Watson 插件操作

此示例显示了在计算机中发现 Dr. Watson 程序后，Dr. Watson 并存插件在默认情况下执行的默认操作。

```
[DrWatson]
Act-EndInstall-0=5
Act-Utility-0=5
```

此部分指定，插件在 CA Access Control 安装完成之后运行时，应为程序创建 SPECIALPGM 规则。 此部分还指定，执行实用程序时，插件应执行相同的操作。

eACSigUpdate 实用程序—替换 STOP 签名文件

在 Windows 上有效

eACSigUpdate 实用程序可使用您在其他计算机上更新的文件替换本地堆栈溢出保护 (STOP) 签名文件。

注意：eACSigUpdate 实用程序可在启动 CA Access Control 时自动运行，然后定期运行（如果定义了签名文件中介或父策略模型）。

此命令格式如下：

```
eACSigUpdate hostname target_file
```

hostname

定义具有要复制到此计算机的更新 STOP 签名文件的主机的名称。

注意：要运行命令，您必须在远程主机上具有管理权限。

target_file

定义新签名文件的完整路径和路径名称。 这是从指定主机检索到的签名的位置和名称。

eACSyncLockout 实用程序－同步帐户注销

在 Windows 上有效

eACSyncLockout 实用程序可将帐户的注销与 CA Access Control 数据库同步。（即，帐户注销时，CA Access Control 数据库中相应用户的记录将挂起。）此实用程序仅在密码同步处于打开状态*且*正在运行此实用程序的用户具有 ADMIN 属性时才有效。

此命令格式如下：

```
eACSyncLockout -start [-u username] [-p password]

eACSyncLockout -stop|-remove|-debug
```

-p *password*

为要安装并启动的服务定义用户密码。 如果未指定 -p，则此实用程序将假定用户没有密码。

-remove

导致服务停止和卸载。（在计算机下一次引导时，服务不会出现在服务控制管理器中。）

-start

导致服务安装和启动。 如果未指定 -u，则此实用程序将在当前用户上下文中安装并启动服务。

-stop

停止服务。

-u *user*

为安装和启动服务定义用户上下文。

exporttngdb 实用程序—迁移 Unicenter Security 数据

exporttngdb 程序可将当前的 Unicenter Security 数据迁移到本地 CA Access Control 数据库或 PMDB 中。

注意：在 UNIX 上，两个脚本 uni_migrate_master.sh 和 uni_migrate_node.sh 将自动执行此程序。 即使这两个脚本都在主机上运行，uni_migrate_master.sh 脚本首先调用此程序以将全局 Unicenter Security 数据迁移到全局 PMDB 中。 uni_migrate_node.sh 脚本可调用此程序以将本地 Unicenter Security 数据迁移到本地 SeOS 数据库中。

此命令格式如下：

```
exporttngdb
```

issec 实用程序—显示 CA Access Control 后台进程状态

在 UNIX 上有效

issec 实用程序可显示 CA Access Control 安全后台进程的状态。 如果未指定任何选项，则将显示以下信息：

- CA Access Control 版本和安装目录
- CA Access Control 内核扩展的状态
- 以下三个主要的 CA Access Control 后台进程的状态：seosd、agent 和 watchdog
- CA Access Control 后台进程的状态：serevu、selogrd、selogrcd、eacws、ReportAgent、policyfetcher、KBLAudMgr
- PMDB 后台进程的状态和名称
- 在 seos.ini 的 [daemons] 部分指定的后台进程的状态

此命令格式如下：

```
issec [-b] [-k] [-h]
```

--b

显示主要的后台进程（seosd、agent 和 watchdog）的状态和 pid。

-k

检查是否已加载 CA Access Control 内核扩展。

-h

显示该实用程序的帮助。

ldap2seos 脚本—从 LDAP 中提取用户以添加到 CA Access Control 中

在 UNIX 上有效

ldap2seos 实用程序从位于服务器主机上的 LDAP 数据库提取用户，并将他们添加到 CA Access Control 数据库中。

重要说明！ 如果操作系统使用 LDAP 用户存储（即 LDAP 用户存储是企业用户存储），则通过 CA Access Control，您可以直接使用 LDAP 用户而无需导入用户。 考虑使用 CA Access Control 的此功能代替 ldap2seos 实用程序。

ldap2seos 实用程序从 LDAP 服务器提取有关已定义的用户的信息。 提取的信息将自动用于执行 selang 命令，从而将用户添加至数据库。 生成的命令还将打印到标准输出，并自动存储到名为 /tmp/ldap2seos.tcl.log 的文件中。

此实用程序需要访问 TCL shell 环境。 ldap2seos 脚本假定 TCL shell 路径为 /usr/local/bin/tclsh。 如果 TCL shell 放置在别处，请更改脚本中的第一行。

要使该实用程序能够正常工作，CA Access Control 必须处于运行状态。此实用程序将更新数据库，因此它必须由具有 ADMIN 权限的用户运行。 还必须在 LDAP 数据库设置中授予该用户执行搜索查询的权限。

此脚本有以下格式：

```
ldap2seos [options]
```

-accfld *account-field*

指定包含 CA Access Control 的用户 ID 的 LDAP 字段名称。

如果 UNIX 用户 ID 在 LDAP userid 字段中，则该选项并不是必需的。

如果 UNIX 用户 ID 分配给了 LDAP 字段而不是 userid 字段，请将 LDAP 字段指定为 *account-field*，LDAP userid 字段将被忽略。

注意：如果脚本找不到 userid，用户将不上传到 CA Access Control 数据库。

-b *base-entry*

指定从中提取用户的 LDAP 数据库中的基本条目。 该条目在 LDAP 数据库内必须有效。 如果忽略基本条目，LDAP 将使用默认基本条目提供用户。

-d *dn*

指定要与 *-w* 开关参数结合使用的条目名称，以作为另一个用户在 LDAP 中进行身份验证；通常在以 admin 用户身份登录到 LDAP 时使用。

-f *filename*

定义可以在其中临时存储从 LDAP 服务器检索到的数据的文件。

-h

显示此实用程序的帮助。屏幕包含 ldap2seos 用法和选项的列表和说明。

-h *ldap-host*

指定 LDAP 数据库所在的主机的名称。 默认为本地主机。

-l *ldap-dir*

指定包含假设位于 bin 子目录的命令行实用程序的目录。 默认值为 /usr/local/ldap。

-p *port*

指定 LDAP 用于连接的端口。 默认值为端口 389。

-u

等同于 -h，可显示帮助。屏幕包含 ldap2seos 用法和选项的列表和说明。

-w *bindpasswd*

指定用户密码。 与 -d 选项结合使用，在需要进行身份验证才能访问 LDAP 数据库时使用。

示例：提取用户信息

以下命令可从主机 myhost.mysite.com 上的 LDAP 数据库中提取有关用户的信息，并尝试将他们添加到 CA Access Control 数据库中。

```
ldap2seos -h myhost.mysite.com
```

seos2ldap 脚本—将 CA Access Control 用户导出到 LDAP

seos2ldap 可将 CA Access Control 用户从数据库导出到服务器主机上的 LDAP 数据库。 它从 CA Access Control 数据库中提取有关用户的适当信息。 然后将信息传输到所选服务器的 LDAP 数据库。 提取的信息将用于生成 LDIF 文件。 指定用户将添加到 LDAP 数据库。 响应将自动存储到名为 /tmp/seos2ldap.tcl.log 的文件。

此实用程序需要访问 TCL shell 环境。 ldap2seos 假定 TCL shell 路径为 /usr/local/bin/tclsh。 如果 TCL shell 放置在别处，请更改脚本中的第一行。

要使该实用程序能够正常工作，CA Access Control 必须处于运行状态。此实用程序将从数据库进行读取，因此它必须由具有 ADMIN 权限的用户运行。 还必须在 LDAP 数据库设置中授予该用户进行修改的权限。

LDAP 数据库的条目架构（如果您选择使用一个）应类似于 Netscape 服务器的架构。 如果您已更改 Netscape 架构，或使用的是其他类型的 LDAP 服务器，则可能需要相应编辑 seos2ldap 示例脚本。

如果 CA Access Control 数据库用户已显示在 LDAP 数据库中，则不添加用户。 将生成一条错误消息，但导出过程将继续。

此脚本有以下格式：

```
seos2ldap [options]
```

-b *base-entry*

指定用于存储用户信息的 LDAP 数据库中的基本条目。 该条目在 LDAP 数据库内必须有效。如果忽略基本条目，LDAP 将提示用户提供。

-d *dn*

指定要与 *-w* 开关参数结合使用的条目名称，以作为另一个用户在 LDAP 中进行身份验证。 以 admin 用户身份登录到 LDAP 时需要使用该选项。

-f *filename*

定义可以在其中临时存储从 LDAP 服务器检索到的数据的文件。

-h

显示此实用程序的帮助。屏幕包含 ldap2seos 用法和选项的列表和说明。

-h *ldap-host*

指定 LDAP 数据库所在的主机的名称。 默认为本地主机。

-l *ldap-dir*

指定包含假设位于 bin 子目录的命令行实用程序的目录。 默认值为 /usr/local/ldap。

-noprompt

取消基本条目提示。 如果没有使用 -b *base-entry* 标志来指定基础 LDAP 条目，默认情况下 seos2ldap 会提示您输入基础条目。 此标志可抑制提示。

-p *port*

定义 LDAP 用于连接的端口。 默认值为端口 389。

-u

等同于 -h，可显示帮助。 屏幕包含 ldap2seos 用法和选项的列表和说明。

-w *bindpasswd*

定义用户密码。 此选项与 -d 选项结合使用，在需要进行身份验证才能访问 LDAP 数据库时使用。

示例：导出用户信息

以下命令可从 CA Access Control 数据库中提取有关用户的信息，并创建名为 SeOS_user_dump 的 LDIF 文件。 此命令可将记录添加至主机 myhost.mysite.com 上的 LDAP 数据库。 以后您可以编辑 LDIF 文件，并手动更新 LDAP。

```
seos2ldap -h myhost.mysite.com
```

migopts 实用程序—转换 Unicenter Security 设置

将当前的 Unicenter Security 环境设置转换为本地 CA Access Control 数据库或 PMDB 的全局设置。

注意：选择 Unicenter 集成时，安装程序会自动执行此脚本。 无论何时新建 PMDB，都可以（并且应该）手工调用该脚本。

此命令格式如下：

```
migopts [options]
```

-d *pmdName*

在运行任意 selang 命令以更新导入的 PMDB（而非默认的本地 CA Access Control 数据库）之前，发出 CA Access Control **hosts** 命令。

-f *fileName*

在可执行的脚本文件中生成任意 **selang -c** 命令。

-l *logfileName*

将日志消息写入完全指定的文件名中。

ntimport 实用程序－导入 Windows 用户和组

在 Windows 上有效

ntimport 实用程序从 Windows 操作系统数据库提取 Windows 用户和组以便导入本地数据库。 ntimport 实用程序可创建将用户和组添加到本地 CA Access Control 数据库所需的 Windows 命令。

重要说明。 通过 CA Access Control，可以直接使用 Windows 用户和组，而无需将其导入数据库。 考虑使用 CA Access Control 的此功能代替 ntimport 实用程序，这是在 CA Access Control 可以直接使用 Windows 用户和组之前开发出来的。

在标准输出中显示生成的命令。 如果希望创建一个文件作为 selang 实用程序的输入，请使用 -f 选项。

此命令格式如下：

```
ntimport {-a|{[-u] [-g] [-c]}} [-d] [-U] \
    [-D] [-f filename] [-o owner] [-p pmdb] \
    [-pa pmdb] [-r remote-host] [-v]
```

-a

执行 -c、-g 和 -u 开关参数的所有操作。

-c

生成将用户加入它们的默认组所需的 selang 命令。

-d

导入用户和组，使用其域作为前缀。

-D

从第一个可用的域控制器中检索用户和组信息。

-f *filename*

将输出重定向到指定的文件。

--g

生成将组从 Windows 导入本地数据库所需的 selang 命令。

-o *owner*

为每个导入的记录设置所有权规则。 使用这个标志，以防止*管理员*自动变为所有记录的所有者。 *Owner* 是被分配具有由 ntimport 定义的所有记录的所有权的用户或组的名称。

-p *pmdb*

生成用于将用户和组导入 PMDB 的 AC 环境中的命令。

-pa *pmdb*

生成用于将用户和组导入到 PMDB 的 AC 环境和本地环境中的命令。

-pn *pmdb*

生成用于将用户和组导入到 PMDB 的本地环境中的命令。

-r *remote-host*

从指定的远程主机检索用户和组信息。

-u

生成将用户从 Windows 数据库导入本地数据库所需的 selang 命令。超过 40 个字符的名称将会被截短。

-U

生成导入用户的 surrogate 规则所需的 selang 命令。

--v

为用户提供进度信息。 使用这个标志，在具有很多用户或组时验证程序的进度。

policydeploy 实用程序—管理企业策略部署

policydeploy 实用程序可管理多规则策略（高级策略管理）。 通过此实用程序，您可以在 DMS 节点上存储策略版本、将策略分配给主机和主机组、取消分配这些策略、直接部署已存储的策略或取消部署，或者将部署的策略升级到最新版本。

该实用程序可处理多个任务，并具有以下函数：

任务	函数
分配策略或取消对策略的分配 (p. 77)	`policydeploy -assign`
删除策略 (p. 79)	`policydeploy -delete`
部署策略 (p. 80)	`policydeploy -deploy`
取消部署策略 (p. 80)	`policydeploy -undeploy`
重新执行部署任务 (p. 81)	`policydeploy -fix`
查看部署脚本 (p. 82)	`policydeploy -getrules`
将主机加入主机组或从主机组删除主机 (p. 83)	`policydeploy -join`

任务	函数
将 PMD 迁移到高级策略管理 (p. 84)	`policydeploy -migrate`
重置策略部署 (p. 86)	`policydeploy -reset`
还原所有策略 (p. 87)	`policydeploy -restore`
存储策略 (p. 88)	`policydeploy -store`
升级策略版本 (p. 90)	`policydeploy -upgrade`
降级策略版本 (p. 90)	`policydeploy -downgrade`

policydeploy -assign 函数—分配策略或取消对策略的分配

此函数可将指定策略分配到一个或多个主机或主机组，或者从一个或多个主机或主机组取消对指定策略的分配。

此函数的格式如下：

`policydeploy -assign[-] name -hnode|-ghnode list [-dms list]`

-assign *name*

将指定策略分配到一个或多个主机或主机组。

-assign- *name*

从一个或多个主机或主机组取消对指定策略的分配。

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

`so dms+(new_dms_name)`

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-ghnode *list*

定义要将策略分配至的主机组（GHNODE 对象）的列表（用逗号分隔）。

-hnode *list*

定义要将策略分配至的主机（HNODE 对象）的列表（用逗号分隔）。

示例：分配 IIS 5 保护策略

以下示例展示了如何分配用于保护 Internet 信息服务 (IIS) 5 Web 服务器安全的策略。 我们将复查该策略和 IIS5 策略的最新（第四）版本，然后将该策略分配至名为 IIS5Servers 的主机组。 IIS5 策略存储在 crDMS@cr_host.company.com DMS 节点上。

1. 通过 selang 连接到 DMS：

   ```
   hosts crDMS@cr_host.company.com
   ```

   您可以通过 selang 查询 DMS。

2. 如果您无法确定哪个才是经过最终确定的最新策略版本，请运行以下 selang 命令查找该策略的所有版本：

   ```
   sr GPOLICY IIS5
   ```

   selang 窗口将列出 IIS5 策略的属性，包括“最终策略”，该“最终策略”即为可以分配（经过最终确定）的最新策略版本。

3. 发出以下 selang 命令查看策略部署和取消部署脚本：

   ```
   sr RULESET IIS5#04
   ```

   selang 窗口显示 IIS5#04 RULESET 对象，包括与第四版的 IIS5 策略相关的部署和取消部署规则。

4. 在命令提示符窗口中，运行 policydeploy 实用程序：

   ```
   policydeploy -assign IIS5 -ghnode IIS5Servers
   ```

   此操作将把 IIS5 策略分配至 IIS5Servers 逻辑主机组中的所有主机，然后依次将 IIS5 策略的第四版本部署在这些主机上。

示例：取消对 IIS 5 保护策略的分配

以下示例展示了如何从在上个示例中为其分配了 IIS 5 策略的 Web 服务器取消对该策略的分配。

在命令提示符窗口中，运行 policydeploy 实用程序：

```
policydeploy -assign IIS5 -ghnode IIS5Servers
```

此操作将把 IIS5 策略从 IIS5Servers 逻辑主机组中的所有主机上取消分配，然后对部署在这些主机上的 IIS5 策略版本依次进行取消部署。

policydeploy -delete 函数—删除策略

此函数可删除指定策略或策略版本。

注意：您无法删除已分配给主机或主机组、已部署到主机或主机组、状态为“取消部署，但存在失败”或在 DMS 上有状态的策略或策略版本。请确保在删除策略或策略版本之前，从所有主机和主机组取消对该策略或策略版本的部署或分配。 此外，您无法删除作为其他策略先决条件的策略。 在删除策略之前，请先删除此策略的所有依存关系。

此函数的格式如下：

```
policydeploy -delete name[#xx] [-dms list]
```

-delete *name*[#*xx*]

删除指定策略或策略版本。

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

示例：删除已取消分配的 IIS 5 保护策略

以下示例展示了如何从 DMS 删除已取消分配的 IIS 5 策略。 在本例中，策略 IIS5 未分配给任何主机或主机组，它存储在 crDMS@cr_host.company.com DMS 节点上。

要删除 IIS 5 保护策略，请打开命令提示符窗口并运行 policydeploy 实用程序：

```
policydeploy -delete IIS5
```

策略 IIS5 将从 crDMS@cr_host.company.com DMS 节点删除。

示例：删除 IIS 5 保护策略版本

以下示例展示了如何从 DMS 中删除未分配的策略版本 IIS5#05。 在本例中，策略版本 IIS5#05 未分配给任何主机或主机组，并存储在 crDMS@cr_host.company.com DMS 节点上。

要删除 IIS 5 保护策略版本，请打开命令提示符窗口并运行 policydeploy 实用程序：

```
policydeploy -delete IIS5#05
```

将从 crDMS@cr_host.company.com DMS 节点删除策略版本 IIS5#05。

policydeploy -delete 函数－部署策略或取消对策略的部署

此函数可在指定端点上部署策略或取消对策略的部署，而不会将策略分配给主机，也不会从主机取消对策略的分配。

此函数的格式如下：

```
policydeploy { -deploy name[#xx] | -undeploy name[#xx] } {-nodelist hnode_list
| -root dbs} [-dms list]
```

-deploy *name*[#*xx*]

提示您是否要在定义的端点上直接部署指定的已存储策略版本（而不将策略分配给主机）。 要部署策略最新的已存储版本，请忽略策略版本号。

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-nodelist *hnode_list*

定义要为其执行操作的主机（HNODE 对象）的列表（用逗号分隔）。

-root *dbs*

定义应在其中部署或取消部署策略的数据库的列表（用逗号分隔）。

注意：如果根数据库为父策略模型，则将在整个订阅数据库中部署或取消部署策略。 如果根数据库为 CA Access Control 端点，则将仅在指定数据库上部署或取消部署策略。 此选项用于实现与 r8 SP1 数据库和 PMDB 的后向兼容。

-undeploy *name*[#*xx*]

提示您是否需要直接从定义的端点取消部署指定策略版本 *name#xx*（不取消分配该策略）。

要取消部署策略最新的已存储版本，请忽略策略版本号。

policydeploy -fix 函数—重新执行部署任务

此函数可修复并重新部署指定的部署任务或程序包。

此函数的格式如下：

```
policydeploy -fix {-task list | -package list} [-dms list]
```

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-fix

修复并重新部署指定的部署任务或程序包。

-package *list*

定义部署软件包 (GDEPLOYMENT) 的列表（用逗号分隔）。

-task *list*

定义用逗号分隔的部署任务的列表。

policydeploy -getrules 函数—查看部署脚本

此函数允许您查看指定策略版本的 selang 部署和取消部署脚本。

```
policydeploy -getrules name[#xx] -ds file1 -uds file2 [-dms list]
```

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-ds *file1*

指定包含部署规则的文件的路径名。这些是构建策略所必需的命令。使用 -getrules 选项时，实用程序会创建此文件。

重要说明！ 策略部署不支持设置用户密码的命令。 不要将这类命令包含在您的部署脚本文件中。 本地 selang 命令虽然受支持，但这些命令不会在偏差报告中出现。

-getrules *name*[*#xx*]

检索指定的策略版本的 selang 部署和取消部署脚本。 如果未指定策略版本，该命令将应用于最新的策略版本。

-uds *file2*

定义包含取消部署策略所需规则的文件的路径名。 这些是取消部署该策略所必需的命令。 使用 -getrules 选项时，实用程序会创建此文件。

CA Access Control 取消部署策略时，如果未存储任何策略取消部署脚本，CA Access Control 将计算删除该策略所需的命令。

示例：查看与 IIS 5 保护策略关联的部署脚本

以下示例展示了如何查看与部署用于保护 Internet 信息服务 (IIS) 5 Web 服务器的策略以及取消对此策略的部署相关联的 selang 脚本。 策略名称为 myPolicy。

要查看 selang 脚本，请运行以下命令：

```
policydeploy -getrules myPolicy -ds c:\folder\deployRules.txt -uds
undeployRules.txt
```

policydeploy -join 函数—将主机加入主机组或从主机组删除主机

此函数可将主机加入主机组或者从主机组删除主机。

此函数的格式如下：

```
policydeploy -join[-] hnode_name -ghnode name [-dms list]
```

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-ghnode *name*

为要执行的操作定义主机组的名称。

-join *hnode_name*

将指定主机添加到主机组中。

-join- *hnode_name*

从主机组删除指定主机。

policydeploy -migrate 函数—将 PMD 迁移到高级策略管理

此函数可将 PMD 迁移到高级策略管理环境。 将 PMD 迁移到高级策略管理时，将根据 PMD 中的规则创建策略，在 DMS 中创建主机组和主机，并将策略分配到主机组。

此函数的格式如下：

```
policydeploy -migrate pmdName@hostName [-dms name] [-policydir directory] \
[-exportfilter "class, class..."] [-hgcreate] [-pcreate name] [-addpmdfilter]\
[-unsubs] [-delete] [-auto]
```

pmdName@hostName

定义要迁移的 PMD 的名称。

-dms *name*

（可选）定义 PMD 中的规则将迁移到的 DMS 的名称。如果没有指定 DMS 名称，将从本地主机上的 CA Access Control 数据库检索 DMS 名称。

注意：如果没有指定 DMS 名称，并且本地主机上的 CA Access Control 数据库中指定了多个 DMS 名称，则 PMD 中的规则将迁移到所有指定的 DMS。

-policydir *directory*

（可选）定义在其中存储策略文件的目录。 如果没有指定目录，策略文件将存储到当前工作目录中。

策略文件的名称为 *pmdName_hostName*_policy。

-exportfilter "*class, class...*"

（可选）指定要从 PMD 数据库导出的 CA Access Control 类。 如果没有指定任何类，将导出 PMD 数据库中的所有类。

-exportfilter 参数具有以下特点：

- 如果您导出修改特定类中资源的规则，并且该类具有相应的资源组，则 CA Access Control 还会导出修改该资源组中资源的规则。
- 如果您导出修改特定资源组中资源的规则，则 CA Access Control 还会导出修改资源组的成员资源的规则。
- 如果您导出修改特定类中资源的规则，并且该类具有 PACL，则 CA Access Control 还会导出修改 PROGRAM 类中资源的规则。

- 如果您导出修改特定类中资源的规则，并且该类具有 CALACL，则 CA Access Control 还会导出修改 CALENDAR 类中资源的规则。
- 如果您导出修改特定类中资源的规则，并且该类中的其中一个资源是 CONTAINER 资源组的成员，则 CA Access Control 会导出修改 CONTAINER 类中资源的规则，并导出修改作为每个 CONTAINER 资源组成员的资源的规则。

-hgcreate

（可选）在 DMS 上创建与 *pmdName* 对应的主机组（GHNODE 对象），在 DMS 上创建与 *pmdName* 的端点订户对应的主机（HNODE 对象），并将这些主机加到主机组中。

-pcreate *name*

（可选）在 DMS 上创建一个 POLICY 对象，其中包含从 *pmdName* 导出的策略文件中的规则，并将此 POLICY 对象分配到 DMS 上与 *pmdName* 对应的主机组。 如果指定 *name*，则所创建的 POLICY 对象的名称为 *name*_POLICY#01；如果没有指定名称，则所创建的 POLICY 对象的名称为 *pmdName*_POLICY#01。

-addpmdfilter

（可选）将筛选文件应用于 *pmdName*。 筛选文件名为 filter.flt，与 *pmdName* 位于同一目录中。

注意：您将使用筛选文件来创建密码 PMD。 筛选文件仅允许将用户密码命令发送给 *pmdName* 的订户。

-unsubs

（可选）取消端点订户对 *pmdName* 的订阅。

-delete

（可选）在 policydeploy -migrate 函数执行完之后删除 *pmdName*。

-auto

（可选）指定执行 -hgcreate 和 -pcreate 选项。此选项执行以下操作：

- 导出 pmdName 中的规则
- 在 DMS 上创建与 *pmdName* 对应的主机组（GHNODE 对象）
- 在 DMS 上创建与 *pmdName* 的端点订户对应的主机（HNODE 对象）
- 将这些主机加到主机组中
- 在 DMS 上创建一个 POLICY 对象，其中包含从 *pmdName* 导出的策略文件中的规则
- 将此 POLICY 对象分配到 DMS 上与 *pmdName* 对应的主机组

示例：迁移规则并创建主机组

本例将规则从主机 A 上的主 PMD 迁移到主机 B 上的 DMS__，将策略文件保存到 C:\Data\policies_MasterPMD_hostA 目录，在 DMS__ 上创建名为“MasterPMD”的主机组，在 DMS__ 上创建与主 PMD 的端点订户对应的主机，并将主机加到 MasterPMD 主机组中：

```
policydeploy -migrate MasterPMD@hostA -dms DMS__@hostB -policydir
"C:\Data\policies_MasterPMD_hostA" -hgcreate
```

policydeploy -reset 函数－重置策略部署

此函数可重置端点上的策略部署。 CA Access Control 可取消部署端点上的所有有效策略、检测所有高级策略管理属性，以及重置主机状态。

此函数的格式如下：

```
policydeploy -reset hnode_name [-dms list]
```

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-reset *hnode_name*

重置指定端点上的策略部署。

policydeploy -restore 函数—还原所有策略

此函数可取消对指定主机上任何策略的部署，然后还原（直接重新部署）所有策略，应通过将所有部署任务重新发送到主机以供执行来部署这些策略。

重要说明！ 如果主机具有某些已应用的策略，还原将失败，因为它在执行之前未重置主机状态。 应使用 policydeploy -reset 函数。

此函数的格式如下：

```
policydeploy -restore hnode_name [-dms list]
```

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意： 如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-restore *hnode_name*

还原（直接重新部署）应在指定主机上进行部署的所有策略。

policydeploy -store 函数—存储策略

此函数可将指定策略存储在该命令指定的 DMS 节点上或本地 CA Access Control 数据库中。 除非使用 -silent 选项，否则您需要在提示下确认此操作。

如果 DMS 上未存储任何指定策略的先前版本，则将创建该策略的版本 1 (*name*#01)。 如果存在该策略的先前版本，则将创建该策略的新版本 (*name#last_version+1*)。 您存储的策略版本是自动确定的。 需要更新某个策略时，必须存储该策略的新版本，其中包含已进行必要修改的策略部署和取消部署规则。

此函数的格式如下：

```
policydeploy -store name -ds file1 [-uds file2] [-dms list] [-desc description]
[-prereq list] [-silent]
```

-desc *description*

（可选）定义策略的业务说明。

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-ds *file1*

指定包含部署规则的文件的路径名。这些是构建策略所必需的命令。使用 -getrules 选项时，实用程序会创建此文件。

重要说明！ 策略部署不支持设置用户密码的命令。 不要将这类命令包含在您的部署脚本文件中。 本地 selang 命令虽然受支持，但这些命令不会在偏差报告中出现。

-prereq *list*

（可选）定义在可以部署此策略之前必须部署的策略的列表（用逗号分隔）。

重要说明！ 如果尝试部署从属策略时未部署先决条件策略，则部署任务的状态将更改为*挂起先决条件*，且该部署将在部署所有先决条件策略后恢复。 同样，如果您尝试取消部署作为另一个已部署策略的先决条件的策略，则部署任务的状态将更改为*挂起从属*，且该部署将在取消部署所有从属策略后恢复。

-silent

（可选）不显示所请求操作的确认提示。

-store *name*

将指定策略存储在指定 DMS 节点上或本地 CA Access Control 数据库中。

注意：策略名称不能包含 #（井号）字符，该字符已保留用于表示策略版本号而保留，并自动进行添加。

-uds *file2*

定义包含取消部署策略所需规则的文件的路径名。 这些是取消部署该策略所必需的命令。 使用 -getrules 选项时，实用程序会创建此文件。

CA Access Control 取消部署策略时，如果未存储任何策略取消部署脚本，CA Access Control 将计算删除该策略所需的命令。

示例：存储 IIS 5 保护策略

以下示例展示了如何存储用于保护 Internet 信息服务 (IIS) 5 Web 服务器安全的策略。 这是我们在 DMS 上第一次存储此策略。

注意：在此示例中，selang 命令是针对 Windows 操作系统上的资源的，不过此步骤在 UNIX 中同样适用。

1. 使用以下 IIS 脚本保存名为 IIS5.selang 的文件：

```
# IIS5 deployment script
eu inet_pers owner(nobody)
er FILE c:\InetPub\wwwroot\* defaccess(none) owner(nobody)
authorize FILE c:\InetPub\wwwroot\* uid(inet_pers) access(all)
er FILE c:\InetPub\wwwroot\scripts defaccess(none) owner(nobody)
er FILE *.asp defaccess(none) owner(nobody)
authorize FILE *.asp uid(inet_pers) via(pgm(inetinfo.exe)) access(read,
execute)
```

这些是部署 IIS 5 保护策略必需的命令。

2. 使用以下脚本保存名为 IIS5_rm.selang 的文件：

```
# IIS5 undeployment script
ru inet_pers
rr FILE c:\InetPub\wwwroot\*
rr FILE c:\InetPub\wwwroot\scripts
rr FILE *.asp
```

以上是取消对在步骤 1 中创建的 IIS 5 保护策略的部署所需的命令。

3. 打开命令提示符窗口，运行 policydeploy 实用程序：

```
policydeploy -store IIS5 -ds IIS5.selang -uds IIS5_rm.selang -desc "IIS5 web server security policy" -silent
```

此操作将通过在 IIS5.selang 和 IIS5_rm.selang 中定义的脚本，将策略 IIS5（GPOLICY 对象）和该策略的第一个版本（IIS5#01 POLICY 对象）存储在 DMS 上。

policydeploy -upgrade 函数—升级或降级策略版本

此函数可在已定义主机上将策略升级到其最新的已确定版本，或在已定义主机上将策略降级到指定策略版本。

此函数的格式如下：

```
policydeploy {-upgrade name | -downgrade name#xx} [-nodelist hnode_list|-ghnode name] [-list] [-dms name]
```

-dms *list*

（可选）指定要使用的 DMS 节点的列表（用逗号分隔）。 部署或取消部署策略时，这些是要将操作报告至的 DMS 节点。 存储策略时，这些是存储策略的 DMS 节点。

如果未使用此选项指定 DMS 节点，则此实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。 要指定数据库中 DMS 节点的列表，您需要在使用 dmsmgr 创建新 DMS 后发出以下 selang 命令：

```
so dms+(new_dms_name)
```

注意：如果您在安装过程中没有指定 DMS 节点，或您希望在端点替换或添加已注册的 DMS，则需要发出同样的命令。 但是，如果指定在安装过程中创建高级策略管理服务器，则 DMS 将添加到数据库，无需手动运行以上命令。

-downgrade *name#xx*

将策略降级到定义的主机上指定的策略版本。

-ghnode *name*

为要执行的操作定义主机组的名称。

-list

（可选）列出已部署某版本指定策略（而非指定版本）的主机。 如果使用 -upgrade，则隐性指定的版本是最新的可用版本。

-nodelist *hnode_list*

定义要为其执行操作的主机（HNODE 对象）的列表（用逗号分隔）。

-upgrade *name*

将已定义的主机上的指定策略升级到其最终确定的版本。

示例：升级 IIS 5 保护策略

以下示例展示了如何升级策略。 我们将先复查部署，以确定哪些主机未部署此策略的最新版本。

1. 在命令提示符窗口中，运行 policydeploy 实用程序：

   ```
   policydeploy -upgrade IIS5 -list
   ```

   此操作将列出已部署旧版本 IIS5 策略的主机。

2. 为这些主机全部升级至该策略的最新版本：

   ```
   policydeploy -upgrade IIS5
   ```

示例：降级 IIS 5 保护策略

以下示例展示了如何降级策略。 我们将先复查部署，以确定哪些主机已部署旧版本策略。

1. 在命令提示符窗口中，运行 policydeploy 实用程序：

   ```
   policydeploy -downgrade IIS5#3 -list
   ```

   此操作将列出已部署高于版本 3 的 IIS5 策略的主机。

2. 为这些主机全部降级至该策略的第三版本：

   ```
   policydeploy -downgrade IIS5#3
   ```

pwextractor 实用程序－提取特权帐户密码

pwextractor 实用程序可从数据库提取特权帐户密码。 如果要备份特权帐户密码，或者 特权用户密码管理 不可用且您无法签出特权帐户，则可以使用 pwextractor。

要使用 pwextractor，您必须：

- 有权使用数据库表
- 知道 特权用户密码管理 用来访问数据库的帐户的用户名和密码

  注意：在安装企业管理服务器时需提供这些凭据。

如果使用的是 Microsoft SQL Server 数据库且数据库身份验证模式为 Windows 身份验证，则在使用 pwextractor 时必须：

- 确定 sqljdbc_auth.dll 文件位于 JAVA_HOME\bin 目录
- 使用 pwextractor -url 格式
- 在 JDBC URL 字符串中指定 integratedSecurity=true

注意：仅当您在 Windows 计算机上安装企业管理服务器并使用 Microsoft SQL Server 数据库时，才能使用 pwextractor -url 格式。 有关 sqljdbc_auth.dll 文件的详细信息，请参阅 Microsoft SQL Server 文档。

pwextractor 位于以下目录中：

ACServerInstallDir/IAM Suite/Access Control/tools/pwextractor

此命令格式如下：

```
pwextractor -h hostname [-r port] -d {database | schema} -t {mssql | oracle} -l
login -p password -f filename [-k key_file]
```

对于 JDBC 数据库，此命令有以下格式。 仅当您在 Windows 计算机上安装了企业管理服务器并使用 Microsoft SQL Server 数据库时，此格式才有效：

```
pwextractor -url url -f filename [-k key_file]
```

-h *hostname*

定义数据库主机的名称。

-r *port*

定义数据库用来进行通讯的端口号。

-d {*database* | *schema*}

定义以下内容：

- (MS SQL) 定义数据库名称。
- (Oracle) 定义架构名称。

-t {mssql | oracle}

指定数据库类型。

值：mssql、oracle

-l *login*

定义 特权用户密码管理 用来访问数据库的帐户的用户名。

-p *password*

定义 特权用户密码管理 用来访问数据库的帐户的密码。

-f *filename*

定义输出文件的目录路径和文件名。如果指定现有文件，pwextractor 会用新输出替换现有文件。

-k *key_file*

定义用于对密码进行加密的加密文件的完整路径和名称。

-url *url*

定义用来访问数据库的 JDBC URL 字符串。

格式：jdbc:sqlserver://*servername*:*port*[;*property*=*value*]

示例：
jdbc:sqlserver://localhost:1433;selectMethod=cursor;DatabaseName=mydb;user=sa;password=mypwd;

示例：从 Microsoft SQL Server 数据库提取 特权用户密码管理 密码

以下示例将从 myhost.example.com 主机上名为 mydb 的 Microsoft SQL Server 数据库提取 特权用户密码管理 密码。 企业管理服务器位于 Windows 计算机上，加密文件位于 C:\FIPSkey.dat。 pwextractor 将输出写入 C:\accounts.txt 文件。

- 下面的示例在数据库身份验证模式为 SQL Server 身份验证时提取密码：

```
pwextractor.bat -h myhost.example.com – r 1433 -d mydb -t mssql -l sa -p mypwd
-f C:\accounts.txt -k "C:\FIPSkey.dat"
```

- 下面的示例在数据库身份验证模式为 Windows 身份验证时提取密码：

```
pwextractor.bat -url
jdbc:sqlserver://myhost.example.com:1433;selectMethod=cursor;DatabaseName
=mydb;user=sa;password=mypwd;integratedSecurity=true; -f C:\accounts.txt -k
"C:\FIPSkey.dat"
```

ReportAgent 实用程序－发送报告快照和审核事件

ReportAgent 将报告快照和审核事件发送到分发服务器，以包含在 CA Access Control、UNIX 身份验证代理 和 CA Enterprise Log Manager 报告中。

在运行 ReportAgent 之前，必须先针对报告操作配置端点。 在针对报告操作配置端点时，可指定与 ReportAgent 通讯的分发服务器及 ReportAgent 运行的日程。 在针对报告操作配置端点后，ReportAgent 将作为后台进程或服务运行，并在排定的时间发送快照。 但是，如果想立即将报告快照或审核事件发送到分发服务器，可以按照需要运行 ReportAgent。

注意：有关如何针对报告操作配置端点的详细信息，请参阅 *《实施指南》*。 在 UNIX 计算机上，还可以使用 report_agent.sh 脚本来配置、启动和停止 ReportAgent。

在 UNIX 计算机上，从 UNIX 计算机 *ACSharedDir*/bin 目录运行 ReportAgent 实用程序，其中 *ACSharedDir* 是默认目录 /opt/CA/AccessControlShared。 您还可能需要设置库路径环境变量。

此命令使用以下语法：

```
ReportAgent -debug {0 | 1 | 2} -task {0 | 1 | 2 | 3 | 4} [-now]
ReportAgent -report snapshot
```

-debug {0 | 1 | 2}

指定以调试模式运行 ReportAgent。 必须停止 ReportAgent 服务或后台进程才能使用此选项。

限制：0－将调试信息输出到控制台。

1－将调试信息输出到日志文件。

2－不输出调试信息（无输出）。

-task {0 | 1 | 2 | 3 | 4}

指定 ReportAgent 发送给分发服务器的信息。

限制：0－将 CA Access Control 数据库和任何本地 PMDB 的快照发送到分发服务器上的 queue/snapshots 队列。

1－将端点审核事件发送到分发服务器上的 queue/audit 队列。

2－(UNIX) 将 UNIX 身份验证代理 数据库的快照发送到分发服务器上的 ac_endpoint_to_server 队列。

3－(UNIX) 将 UNIX 身份验证代理 审核事件发送到分发服务器上的 queue/audit 队列。

4－(UNIX) 将键盘记录器审核事件发送到分发服务器上的 queue/audit 队列。

-now

指定立即运行 ReportAgent。

如果不指定此选项，ReportAgent 将在下一个排定的时间运行。

-report snapshot

指定立即将 CA Access Control 数据库和任何本地 PMDB 的快照发送到分发服务器上的 queue/snapshots 队列。 必须运行 ReportAgent 服务或后台进程才能使用此选项。

示例：查看 ReportAgent 调试信息

以下示例将在 Linux 计算机上设置库路径环境变量，然后指定立即以调试模式运行 ReportAgent，将调试信息输出到控制台，并将审核事件发送到分发服务器：

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/AccessControlShared/lib
export LD_LIBRARY_PATH
cd /opt/CA/AccessControlShared/bin
./ReportAgent -debug 0 -task 1 -now
```

更多信息：

ReportAgent (p. 268)
ReportAgent 键—注册表设置 (p. 507)

ReportAgent 日志文件

下表列出了在运行 ReportAgent -debug 1 命令时 ReportAgent 用来写入调试信息的日志文件。 在此表中，*ACSharedDir* 是默认目录 /opt/CA/AccessControlShared，*ACInstallDir* 是 CA Access Control 的安装目录：

ReportAgent 选件	UNIX 日志文件	Windows 日志文件
-task 0	*ACSharedDir*/log/ac2xml.log	*ACInstallDir*\log\ac2xml.log
-task 1	*ACSharedDir*/log/ac2elm.log	*ACInstallDir*\log\ac2elm.log
-task 2	*ACSharedDir*/log/unab2xml.log	-
-task 3	*ACSharedDir*/log/unab2elm.log	-
-task 4	*ACSharedDir*/log/kbl2elm.log	-

report_agent.sh 脚本—配置报告代理

在 UNIX 上有效

通过 report_agent.sh 脚本，可以在安装之后配置报告代理后台进程。 如果需要更改在安装 CA Access Control 时设置的报告代理配置设置，请使用 report_agent.sh 脚本。

report_agent.sh 脚本位于 *ACSharedDir*/lbin 中。 默认情况下，此目录为 /opt/CA/AccessControlShared/lbin。

此命令格式如下：

```
report_agent.sh start
report_agent.sh stop
report_agent.sh config -server hostname [-proto {ssl|tcp}] [-port port_number]
[-rqueue queue_name] \
[-schedule <time@day[,day2,...]>] [-audit] [-bak] [-silent]
```

config

指定其余参数配置报告代理后台进程。

start

启动报告代理。

stop

停止报告代理。

-server *hostname*

定义分发服务器主机的名称。脚本将结合 -port 选项的输入来构建分发服务器 URL，并设置 ReportAgent 部分中的 report_server 配置设置。

-audit

指定是否要将端点审核数据发送到分发服务器。 这可以设置 ReportAgent 部分中的 reportagent_enabled 配置设置。

-bak

指定保留审核文件的时间戳备份。 这可以将 logmgr 部分配置设置 Backup_Date 设置为 yes，并将 audit_max_files 设置为 50。

-port *port_number*

定义要用于与分发服务器通讯的端口号。 脚本将结合 -server 选项的输入来构建分发服务器 URL，并设置 ReportAgent 部分中的 report_server 配置设置。

-proto

指定连接协议（是 TCP 还是 SSL）。 这可以设置 ReportAgent 部分中的 use_ssl 配置设置

-rqueue *queue_name*

定义报告代理将本地数据库的快照和所有 PMDB 发送到的队列的名称。 这样便可以设置 ReportAgent 部分中的 send_queue 配置设置。

-schedule <*time@day*[,*day2*,...]>

定义何时生成报告以及何时将报告发送到分发服务器。

-silent

指定不要求确认。

示例：配置报告代理

此示例将报告代理设置为通过 SSL 使用端口 7243 和 queue/snapshots 队列将数据库快照发送到 rscomp.com 上的分发服务器中。 它还允许将审核数据发送到分发服务器，并为审核日志文件设置备份设置：

```
report_agent.sh config -server rscomp.com -proto ssl -port 7243 -rqueue
queue/snapshots -audit
```

配置报告代理后，应使用分发服务器所需的正确密码（共享密钥）更新 +reportagent 用户。 要执行此操作，请输入以下内容：

```
eu +reportagent epassword(共享密码) nonnative
```

更多信息：

ReportAgent (p. 268)

seaudit 实用程序－显示审核日志记录

seaudit 实用程序可显示 CA Access Control 审核日志文件中的记录。 要在 Windows 上执行 seaudit 实用程序，必须具有 AUDITOR 属性。 要在 UNIX 上执行 seaudit 实用程序，您必须属于 seos.ini 的 audir_group。 显示包括密码的审核记录时，seaudit 通过将密码文本替换为一系列星号 (***) 来保护密码识别。

注意：您可以在命令开关参数和选项中使用字符串匹配。 某些 UNIX shell 自动展开掩码参数；因此，当从此类 shell 调用 seaudit 时，应在星号或问号前键入反斜杠 (\)，以防止 shell 处理掩码。

注意：seaudit 实用程序按用户名（而不是用户 ID）显示跟踪记录。

此命令格式如下：

```
seaudit switch [options]
```

switch

定义实用程序的操作模式。 可以是以下各项之一：

--a | -all

显示除跟踪工具发送到审核日志的用户跟踪记录以外的所有记录。

注意：同样无法显示已连接的 TCP 记录（UNIX 中可显示）。 您还需要指定 -c 选项以显示这些记录。

-h | -help

显示该实用程序的帮助。

{-i | -inet} ***host service***

显示从指定服务的指定主机收到的 TCP 请求的 INET 审核记录。 *host* 和 *service* 都是标识 seaudit 所搜索的主机和服务集的掩码。

在 UNIX 上，要列出具有已建立连接的网络 ID（端口号）的 TCP 记录，请添加 -c 标志。 例如：

```
seaudit -i -c myhost telnet
```

{-l | -login} ***user1, user2, ... terminal***

显示指定终端上用逗号分隔的指定用户的 LOGIN 记录。

user 和 *terminal* 均为掩码。

在 UNIX 上，这还将列出 serevu 在启用和禁用用户时所创建的记录，以及验证后台进程在您输入了无效密码后所创建的记录。

{-r | -resource} ***class resource user1, user2, ...***

显示指定用户（用逗号分隔）的指定资源上指定类的常规资源审核。

- *class* 是标识所访问的资源所属的类的掩码。
- *resource* 是标识所访问的资源的名称的掩码。
- *user* 是访问资源的用户的名称的掩码。

-s | -start

显示 CA Access Control 启动和关闭消息。

-St | -Stat ***message_number***

（仅限于 UNIX）。 显示 Watchdog 消息编号的描述。

-t | -table

显示日志代码表。

-tr

tr 显示跟踪其活动的所有用户的跟踪记录。

注意：跟踪记录默认显示登录会话 ID 列。 如果您不想显示该列，请使用 -format 选项。

-trr *resource*

显示指定资源的跟踪记录。

-tru {*uid1*|*user1*}, {*uid1*|*user2*}, ...

显示具有指定的数字 uid 或用户名的用户的跟踪记录。

-u *command class record user*

显示数据库更新审核记录：

- *command* 是标识要搜索的 selang 命令集的掩码。
- *class* 是标识要搜索的类的掩码。
- *record* 是标识要搜索的记录的掩码。
- *user* 是标识执行命令的用户的掩码。

--w

显示 Watchdog 审核记录。

options

定义可更改实用程序显示其信息的方式的可选修改符。 可以是以下一项或多项：

-c

（仅限于 UNIX）。 显示*已连接的* INET 记录。这些是为会话 ID 跟踪而生成的记录，列出了成功的 TCP 连接的端口号。

例如：某位用户 (user1) 打开了从 comp1 到 comp2 的 Telnet 会话，comp1 和 comp2 均安装了 CA Access Control。可以将 comp2 上安装的 CA Access Control 配置（logconnected 配置设置）为向 comp1 发送声明以及通过 Telnet 会话登录的用户的凭据（可能是 user1 以外的其他用户）。 comp1 收到此声明后，将创建一条 TCP-CONNECTED 记录（会话建立记录），之后可使用 -c 选项显示此记录。

-detail

显示有关每条记录的详细信息。

-delim *delimiter*

定义在第一个字段之前和其余字段之间所使用的分隔符。 例如：以下命令可使字段显示在用逗号分隔的引号中。

seaudit -a -delim \",\"

-delim2 *delimiter*

除了第一个字段前面没有分隔符之外，与 -delim 选项相同。

-delim3 *delimiter*

除了年、月和日之间有分隔符之外，与 -delim 选项相同。

-delim4 *delimiter*

与 -delim2 选项相同。

-ed *date*

指定结束日期。 *不*显示此日期之后的记录。

您可以用两种方式之一指定 *date*：

- 使用格式 *dd-mm-yyyy*。
- 使用字符串 *today* 将日期设置为今天。

也可以使用字符串 *today*，后跟（减号）和一个数字。- 这样可以将日期定义为今天之前的指定天数。 例如：*today-3* 表示日期为三天前。

-et *time*

指定结束时间。 *不*显示此时间之后的记录。

您可以用两种方式之一指定 *time*：

- 使用 24 小时格式 *hh:mm*
- 使用字符串 *now* 将时间设为当前时间。

  也可以使用字符串 *now*，后跟 -（减号）和一个数字。 这可以将时间定义为现在之前的指定分钟数。 例如：now-*60* 表示时间是六十分钟（一小时）前。 要描述某特定日内的时间范围，请将此选项与 -sd 和/或 -ed 结合使用。

-f | -failure

指定 *不*显示失败的访问。

{-fn | -file} *fileName*

指定要搜索的审核日志文件的名称。

-format *release*

指定输出格式与用于 CA Access Control *版本*的一样。

release－定义版本号。 有效值包括：

- **80sp1**－r8 SP1 中的输出不包括较新的版本中有效的 UID 列。
- **12**－r12.0 中的输出无法显示密码更改记录。 对于跟踪记录，r12.0 中的输出也不包括登录会话 ID 信息。

-g | -grant

指定*不*显示成功（授权）的访问。

-gn | -grantnotify

指定*不*显示成功（授权）的访问，但通知记录除外。

-kbl -a -sid *sid* {-rp | -pr | -cmd | -exe | -disp}

（仅限 UNIX）指定显示键盘日志记录审核文件 (kbl.audit) 的内容。

-a

显示审核文件中记录的所有会话。

-sid *sid*

指定键盘记录会话 ID。

-rp

重放整个键盘记录会话。

-pr

显示整个键盘记录会话，不包括控制字符。

-cmd

（仅限 UNIX）显示用户在命令行记录会话期间输入的命令。

-exe

显示用户在 shell 中执行的命令的 EXECARGS 详细信息。

-disp

指定此选项时，将显示记录的会话时间。

注意：可以在以下 shell 中运行此命令：bash、tcsh、csh、ksh、jsh、rsh、ash、zsh

-logout

（仅限 UNIX）指定*不*显示注销记录。

-millennium

（仅限 UNIX）指定应该显示四位数年份而不是两位数年份。

-n | -netaddr

指定应在 TCP/IP 记录中显示 Internet 地址而不是主机名。

-notify

指定*不*显示 NOTIFY 审核记录。

{-o | -origin} *host*

指定仅显示来源于指定主机的记录。

仅当从 selogrcd 日志路由收集后台进程所创建的合并审核文件浏览记录时，此选项才适用。-

-pwa

（仅限 UNIX）指定*不*显示密码尝试记录。

-sd *date*

指定开始日期。 *不*显示此日期之前的记录。

您可以用两种方式之一指定 *date*：

- 使用格式 *dd-mm-yyyy*。
- 使用字符串 *today* 将日期设置为今天。

也可以使用字符串 *today*，后跟（减号）和一个数字。- 这样可以将日期定义为今天之前的指定天数。 例如：*today-3* 表示日期为三天前。

sessionid

指定以显示包含用户登录会话 ID 信息的列。 默认情况下该列将隐藏。

注意：该选项仅对配备 r12.0 SP1 及更高版本的端点有效。

-st *time*

指定开始时间。 *不*显示此时间之前的记录。

您可以用两种方式之一指定 *time*：

- 使用 24 小时格式 *hh:mm*
- 使用字符串 *now* 将时间设为当前时间。

也可以使用字符串 *now*，后跟 -（减号）和一个数字。 这可以将时间定义为现在之前的指定分钟数。 例如：now-*60* 表示时间是六十分钟（一小时）前。 要描述某特定日内的时间范围，请将此选项与 -sd 和/或 -ed 结合使用。

-v | -servnum

指定显示端口号，而不是服务名。

-warn

指定*不*显示警告记录。

示例

- 要列出自 2004 年 1 月 3 日以来的所有审核记录，请使用以下命令：

  ```
  seaudit -a -sd 04-Jan-2004
  ```

- 要列出用户 root 在 2004 年 1 月 3 日从任意终端进行的失败登录，请使用以下命令：

  ```
  seaudit -sd 04-Jan-2004 -ed 04-Jan-2004 -l root * -g
  ```

- 要列出用户 John 对类 FILE 的每个资源的所有访问，请使用以下*命令：*

  ```
  seaudit -r FILE * John
  ```

- 要为所有日期列出在 17:00（第一天）到 08:00（随后一天）之间记录的所有审核记录，请使用以下命令：

  ```
  seaudit -a -st 17:00 -et 08:00
  ```

- 要列出在 08:00 到 17:00 之间记录的所有审核记录，请使用以下命令：

  ```
  seaudit -a -st 08:00 -et 17:00
  ```

- 要列出一名用户的登录和资源访问的所有警告记录，请使用以下命令：

  ```
  seaudit -login * * -resource * * * -grant -failure -logout -pwa
  ```

- 要列出两名用户的所有登录记录，请使用以下命令：

  ```
  seaudit -login "user1, user2"
  ```

- 要列出昨天的所有审核记录，请使用以下命令：

  ```
  seaudit -a -sd today-1 -ed today-1
  ```

- 要列出 kbl.audit 日志文件的所有审核记录，请使用以下命令：

  ```
  seaudit -kbl
  ```

- 要重放用户会话，请使用以下命令：

  ```
  seaudit -kbl -sid 22316 -rp
  ```

- 要显示用户在会话中输入的所有命令，请使用以下命令：

  ```
  seaudit -kbl -sid 22316 -cmd
  ```

- 要列出跟踪一名 UID 为 244 的用户尝试访问文件的活动的所有审核记录，请使用以下命令：

  ```
  seaudit -tru 244 -trr FILE
  ```

- 要列出跟踪两名用户的活动的所有审核记录，请使用以下命令：

  ```
  seaudit -tru "user1, 244"
  ```

更多信息：

如何识别审核记录的事件类型 (p. 525)
审核事件类型 (p. 528)

sebuildla 实用程序—创建后备数据库

在 UNIX 上有效

sebuildla 实用程序创建后备数据库以供 CA Access Control 后台进程 seosd 使用。 seosd 后台进程使用该数据库将 UNIX UID 转换为用户名，将 GID 转换为组名，将主机 IP 地址转换为主机名，将服务端口转换为端口名。 该数据库只包含数字到名称的转换。 通过 sebuildla，您还可以将 LDAP 目录信息树 (DIT) 的信息添加到用户后备数据库。

重要说明！ 要设置 sebuildla 和所需的 LDAP 配置设置，您必须熟悉 LDAP 并能够执行 ldapsearch 命令。 建议您阅读 ldap(1)、ldapsearch(1) 的说明页面以及 LDAP 客户端文档中关于设置的信息。 此外，在使用 sebuildla 构建后备数据库以前，请在 lookaside_path 配置设置中指定后备数据库的完整路径。

第一次生成 lookaside 数据库时，请使用以下命令：

```
sebuildla -a
```

这将创建它的*所有*组件。 以后，可使用相关的开关参数更新数据库的单个文件。

如果在 NIS、NIS+ 或 DNS 服务器上安装了 CA Access Control，则应该在相关 makefile 中调用 sebuildla 实用程序。

注意：默认情况下，除使用 sebuildla 程序执行的访问外，禁止所有用户访问后备数据库文件（groupdb.la、hostdb.la、servdb.la 和 userdb.la）。

sebuildla 实用程序扫描系统中的解析机制（如 /etc 文件和 NIS）以生成 lookaside 数据库。

- sebuildla 读取 /etc/resolv.conf 以获取所使用的域名。

  注意：要使 CA Access Control 将主机名解析为完全限定名，resolv.conf 文件必须具有已定义的域或搜索配置选项。 有关 resolv.conf 文件的详细信息，请参阅此文件的手册页。

- sebuildla 使用系统解析选项创建后备数据库。 （这通常是网络缓存后台进程。）
- CA Access Control 使用 /etc/nsswitch.conf 文件（用于网络缓存后台进程或任何其他系统解析选项）确定数据的检索位置。

例如：如果 /etc/nsswitch.conf 文件包含如下主机行，则首先从本地计算机的文件 (/etc/hosts) 检索信息；然后再依次从 DNS 和 NIS 检索信息：

```
hosts:      files dns nis
```

如果该文件包含以下行，则仅从本地计算机的文件检索信息。 后备数据库将只包含 /etc/hosts 中的主机：

```
hosts:      files
```

注意：如果主机具有完全限定名，则 sebuildla 将使用它。

计算机配置的变化可能会导致出现 sebuildla 不列出本地环境的所有名称的情况。 在这种情况下，可以使用 sebuildla 从某列表文件加载所有必需项。 为此，请创建一个列表文件，使每个对象名在单独的一行。 该实用程序将读取该列表文件，并确保将列表文件中的所有对象添加到相关的后备数据库（如有必要）。 sebuildla 将忽略重复的对象。

下表列出了 sebuildla 用来生成每个 lookaside 数据库的文件。

以下位置的对象	被添加到以下位置
ACInstallDir/ladb/userlist	用户 lookaside 数据库
ACInstallDir/ladb/grouplist	组 lookaside 数据库
ACInstallDir/ladb/hostlist	主机 lookaside 数据库
ACInstallDir/ladb/servlist	服务 lookaside 数据库

在 *ACInstallDir*/ladb 目录中的文件格式中：

- sebuildla 忽略空行或以惊叹号 (!)、数字符号 (#) 或分号 (;) 开头的行。
- 其他行表示 sebuildla 必须添加到相应 lookaside 数据库的项（如果可以解析这些项）。
- 用户、组、主机或服务的名称必须出现在行的第一个位置。

可以使用 dbmgr -dump -r 创建列表文件。 例如：要创建在本地数据库的 HOST 类中定义的主机的列表，请输入：

```
dbmgr -dump -r l HOST > /opt/CA/AccessControl//ladb/hostlist
```

-l 开关参数将从 DNS 发出单个请求，请求默认域中所有主机的列表，而不是在 DNS 服务器中查询所获取的每个主机条目的 FQDN。 只有在安装了 DNS 的情况下，快速加载选项才有效。 只有默认域中的主机名才是完全限定的。 完全限定名按原样保留。 从系统机制中扫描到的非完全限定主机名（且在默认域中未找到）保留非限定形式。 从 hostlist 文件加载的非完全限定主机名将被放弃。

此命令格式如下：

```
sebuildla switch [options]
```

switch

指定实用程序的操作模式。 可以是以下各项之一：

-a

创建*所有*后备数据库文件。

-e

创建不包括 DNS 的主机后备数据库文件。

--g

创建组后备数据库文件。

-h

创建具有 DNS 的主机后备数据库文件。

-help

显示该实用程序的帮助。

-n

收集 LDAP 目录信息树 (DIT) 的信息并将其附加到从主用户数据源（-u 开关参数）创建的用户后备数据库。 仅可以将此开关参数与 -u 开关参数或 -a 开关参数一起使用，以使其在 LDAP DIT 提供其他用户数据且未用作系统的命名服务时最有用。

使用此开关参数之前，请执行以下步骤：

a. 为 CA Access Control 设置以下 seos.ini 文件标记以查找 LDAP 服务：ldap_base、ldap_hostname 和 ldap_userdn。

b. 运行 seldapcred 实用程序以存储加密的 LDAP 密码。

c. （可选）根据环境的需要设置 ldap_port 和 ldap_timeout 标记。

从 LDAP 服务检索信息所需的时间取决于 LDAP 服务的速度以及存储在 DIT 中的用户数据量。 可以将 seos.ini 文件的 [seos] 部分中的 ldap_timeout 标记调整为负责这些方面。

d. （可选）如果您使用的是非标准架构，请设置 ldap_uid_attr、ldap_uidNumber_attr 和 ldap_user_class 标记。

-s

创建服务后备数据库文件。

-u

创建用户后备数据库文件。

注意：可以指定 -n 开关参数与 -u 开关参数一起使用，以添加从 LDAP 服务收集的用户数据。

-G

列出组后备数据库文件的内容。

-H [IPv4 | IPv6]

列出主机后备数据库文件的内容。

-S

列出服务后备数据库文件的内容。

-U

列出用户后备数据库文件的内容。

options

指定可更改实用程序显示其信息的方式的可选修改符。 可以是以下一项或多项：

-l

加载仅使用列表文件的后备数据库。 这排除了系统的解析机制。

-f

使用 -h 开关参数时，快速加载后备数据库（仅限主机）。

更多信息：

seos.ini 初始化文件 (p. 275)

sechkey 实用程序

使用 sechkey 实用程序管理 CA Access Control 加密，并因此保护 CA Access Control 管理通讯。 必须具有 ADMIN 属性才能使用 sechkey。

可以使用它来为对称加密设置加密密钥，或者进行 SSL (PKI) 加密。

如果使用的是对称密钥，建议更改默认密钥。 如果使用的是 SSL，建议更改默认证书和关联的默认私钥。

无论使用哪种加密方法，都应在安装或升级 CA Access Control 后更改站点中所有计算机的密钥。 这可阻止未授权用户访问系统。

此实用程序处理以下任务：

- 更改对称加密密钥 (p. 110)
- 更改对称加密方法 (p. 111)
- 配置 X.509 证书 (p. 113)
- 更改消息队列密码 (p. 116)

sechkey 实用程序—更改对称加密密钥

sechkey 实用程序可更改 CA Access Control 程序的 CA Access Control 对称加密密钥。

可以在交互模式或非交互模式下运行 sechkey。 在交互模式下运行 sechkey 时，sechkey 会提示您输入旧加密密钥和新加密密钥。

在使用 sechkey 更改对称加密密钥之前，必须先停止 CA Access Control。 必须具有 ADMIN 属性才能使用 sechkey。

重要说明！ 为避免通讯问题，请在所有运行 CA Access Control 组件的计算机上使用相同的加密密钥。

在交互模式下，此实用程序具有以下格式：

```
sechkey
```

在非交互模式下，此实用程序具有以下格式：

```
sechkey {oldkey | -d} {newkey | -d} [-s registry_path]
```

sechkey 还有一些仅在 UNIX 计算机上有效的其他开关参数。 对于 UNIX 计算机，此实用程序具有以下格式：

```
sechkey {oldkey | -d} {newkey | -d | -n} [-nopmd | -r hostname]

sechkey -k newkey

sechkey -c
```

-c

(UNIX) 清除 selogrd 加密密钥。 默认密钥存储在密钥文件中。

注意：保存的密钥本身是使用默认加密方法加密的。

-d

指定默认 CA Access Control 密钥。

-k

(UNIX) 指定更改后的 selogrd 新加密密钥。 该加密密钥存储在新文件中，或在旧文件中进行更新。

-n

(UNIX) 列出正在使用当前密钥的程序，但不更改为其他密钥。

newkey

指定新的加密密钥。

-nopmd

(UNIX) 更改密钥，但不使用新密钥更新策略模型更新文件。

oldkey

指定要更改的（当前）加密密钥。

-r *hostname*

(UNIX) 指定要更改加密密钥的远程计算机的名称。

要使用此选项，CA Access Control 必须同时在本地和远程计算机上运行。 此参数实际上并不更改密钥；而是存储信息以便下次启动远程计算机上的 CA Access Control（使用 seload -c）时更改密钥。

-s *registry_path*

(Windows) 指定用来存储 CA Access Control 程序加密密钥的注册表根路径。 此开关参数仅适用于使用 CA Access Control SDK 的第三方程序。

示例：检查 UNIX 计算机是否使用默认加密密钥

以下命令检查 UNIX 计算机是否使用默认 CA Access Control 加密密钥：

```
sechkey -d -n
```

sechkey 实用程序—更改对称加密方法

sechkey 实用程序可更改 CA Access Control 程序的对称加密方法。 更改对称加密方法后，sechkey 会对 CA Access Control 数据库中的每个加密密码进行解密，然后再使用新的加密方法加密每个密码。

注意：当 CA Access Control 以仅 FIPS 模式运行时，将无法更改对称加密方法。 crypto 部分中 fips_only 配置标记的值为 1 时，CA Access Control 以仅 FIPS 模式运行。 此项限制可防止您将加密方法更改为不遵从 FIPS 的方法。

在使用 sechkey 来更改对称加密方法之前，必须先停止 CA Access Control。 必须具有 ADMIN 属性才能使用 sechkey。

重要说明！ 为避免通讯问题，请在所有运行 CA Access Control 组件的计算机上使用相同的加密方法。

该实用程序格式如下：

```
sechkey -m -sym {aes128 | aes192 | aes256 | des | tripledes | default} [-s
registry_path]
```

-m

指定更改加密方法。

-s *registry_path*

(Windows) 指定用来存储 CA Access Control 程序加密密钥的注册表根路径。 此开关参数仅适用于使用 CA Access Control SDK 的第三方程序。

-sym

指定要使用的新加密方法。

aes128

指定使用以下加密方法：

(Windows)：aes128enc.dll

(UNIX)：libaes128.so

aes192

指定使用以下加密方法：

(Windows)：aes192enc.dll

(UNIX)：libaes192.so

aes256

指定使用以下加密方法：

(Windows)：aes256enc.dll

(UNIX)：libaes256.so

des

指定使用以下加密方法：

(Windows)：desenc.dll

(UNIX)：libdes.so

tripledes

指定使用以下加密方法：

(Windows)：tripledesenc.dll

(UNIX)：libtripledes.so

default

指定使用以下专有 CA Access Control 加密方法：

(Windows)：defenc.dll

(UNIX)：libscramble.so

示例：将对称加密方法更改为 AES256

以下命令可将对称加密方法更改为 AES256：

```
sechkey -m -sym aes256
```

更多信息：

ChangeEncryptionMethod 实用程序－更改加密方法 (p. 31)

sechkey 实用程序－配置 X.509 证书

sechkey 实用程序可配置 CA Access Control 用来验证组件之间通讯的根证书和服务器证书。

可以使用 sechkey 实用程序执行以下任务：

- 将 CA Access Control 配置为使用第三方根证书和服务器证书，包括 OU 密码保护的证书
- 从第三方根证书创建服务器证书
- 将受密码保护的证书的密码保存在计算机上

在使用 sechkey 配置 X.509 证书之前，必须先停止 CA Access Control。 必须具有 ADMIN 属性才能使用 sechkey。

注意：如果 CA Access Control 正以仅 FIPS 模式运行，则您无法使用受密码保护的证书。 crypto 部分中 fips_only 配置标记的值为 1 时，CA Access Control 以仅 FIPS 模式运行。 此限制将阻止您使用不符合 FIPS 的方法在证书内对密码进行加密。

此命令采用以下格式来创建 X.509 根证书或服务器证书：

```
sechkey -e {-ca|-sub [-priv privfilepath]} [-in infilepath] [-out outfilepath]
[-capwd password] [-subpwd password]
```

此命令采用以下格式来使用 OU 密码保护的服务器证书：

```
sechkey -g {-subpwd password | -verify}
```

-ca

指定 sechkey 创建用作 CA（根）证书的自签名证书。

sechkey 将证书和私钥存储在由 crypto 部分中的 ca_certificate 配置设置所定义的 PEM 文件中。

-capwd *password*

指定 sechkey 用来生成服务器（主题）证书的根证书的私钥密码。

-e

指定 sechkey 创建 X.509 证书。

-g

指定 CA Access Control 使用第三方服务器证书。将第三方服务器证书保存在 crypto 部分中的 subject_certificate 配置设置所指定的位置，或者编辑 crypto 部分中 subject_certificate 配置设置的值，以指定第三方服务器证书的完整路径。

注意：如果在新目录中安装服务器证书，请写入 CA Access Control FILE 规则以保护新目录。

-in *infilepath*

指定包含证书信息的输入文件。 如果未指定 -in，则 sechkey 将从标准输入中读取信息。

sechkey 需要使用以下信息来创建证书：

- 序号
- 主题
- 开始日期（证书的第一个有效日）
- 结束日期（证书的最后一个有效日）

sechkey 可以使用以下信息，但是该信息并不是必需的：

- Email
- URI（通常称为 URL）
- DNS 名称
- IP 地址

-out *outfilepath*

指定要将证书信息放入到的输出文件。输出文件是输入信息的副本。如果未指定 -out，则 sechkey 将不复制输入信息。

-priv *privfilepath*

指定用于保留与证书相关的私钥的文件。 此选项仅在与 -sub 选项一起使用时有效。

-sub

指定 sechkey 创建服务器（主题）证书。

sechkey 将证书和私钥存储在由 crypto 部分中的 subject_certificate 配置设置所定义的 PEM 文件中。

如果不指定 -priv，crypto 部分中的 private_key 配置设置将定义用于保存与证书相关联的私钥的文件。

如果创建受密码保护的服务器证书，sechkey 不会对证书进行加密。如果创建不受密码保护的服务器证书，sechkey 将使用 AES256 和 CA Access Control 加密密钥对证书进行加密。

-subpwd *password*

指定服务器（主题）证书的私钥的密码。 sechkey 将密码存储在 *ACInstallDir*/Data/crypto 目录下的 crypto.dat 文件中，其中 *ACInstallDir* 是 CA Access Control 的安装目录。 crypto.dat 文件为隐藏、加密、只读文件，且受 CA Access Control 保护。如果 CA Access Control 已停止，则只有超级用户可以访问密码。

-verify

验证 CA Access Control 是否可以使用存储的密码打开受密码保护的服务器密钥。

示例：从 OU 密码保护的第三方根证书创建服务器证书

以下命令将使用以下值从 OU 密码保护的第三方根证书创建服务器证书：

- 包含证书信息的输入文件的路径是 C:\Program Files\CA\AccessControl\data\crypto\sub_cert_info
- 根证书私钥的路径是 C:\Program Files\CA\AccessControl\data\crypto\ca.key
- 根证书私钥的密码是 P@ssw0rd

```
sechkey -e -sub -in "C:\Program
Files\CA\AccessControl\data\crypto\sub_cert_info" -priv "C:\Program
Files\CA\AccessControl\data\crypto\ca.key" -capwd P@ssw0rd
```

示例：输入文件

下面是包含证书信息的输入文件的示例：

```
SERIAL: 00-15-58-C3-5E-4B
SUBJECT: CN=192.168.0.1
NOTBEFORE: “12/31/08”
NOTAFTER: "12/31/09"
E-MAIL: john.smith@example.com
URI: http://www.example.com
DNS: 168.192.0.100
IP:  168.192.0.1
```

sechkey 实用程序—更改消息队列密码

可以使用 sechkey 实用程序更改消息队列密码。 您可以更改客户端或服务器的消息队列密码。

必须具有 ADMIN 属性才能使用 sechkey。

此命令格式如下：

```
sechkey -t [-server] -pwd password
```

-t

指定更改消息队列密码。

-server

指定更改服务器消息队列密码。

注意：如果不指定此参数，sechkey 将更改客户端消息队列密码。

-pwd *password*

定义新密码。

更多信息：

acuxchkey 实用程序—更改加密密钥设置 (p. 30)

seclassadm 实用程序—管理 CA Access Control 类

seclassadm 实用程序可管理 CA Access Control 类。 seclassadm 可将用户定义的新类添加到本地数据库。 在 CA Access Control *未*运行的情况下，从数据库所在的目录中调用 seclassadm（或使用 -p 选项）。

注意：运行 seclassadm 将使用新类信息在 seosdb 目录中创建一个文件。 使用 dbmgr -c 创建新数据库时，如果 CreateNewClasses 配置设置被设为 yes（默认值），则将在新数据库中创建用户定义的类。-

此命令格式如下：

```
seclassadm -add className [-a access] [{-|+}c] [-d access] \
    [-f] [-g] [-o] [-p db_pathname] [-t]

seclassadm -del className

seclassadm -upd className {-|+}c [-p db_pathname]
```

-add *class-name*

将新的资源类添加到现有数据库中，其中 *class-name* 是新类的名称。

CA Access Control 将保留字符大写的类名称。 在添加类时，请至少使用一个小写字符。 类名最长可以为 79 个字符。

在创建新类后，您必须使用 selang setoptions 命令来启用该类。

-del *class-name*

从数据库中删除指定的资源类。

-upd *class-name*

更新数据库中指定的资源类。

-a *access*

为类指定访问模式。 字符串 *access* 表示允许的访问。 每种访问模式都由以任意顺序列出的单个字符代码表示。 此字符串不能包含任何空格或其他非字母字符。- 有效的访问模式包括：

缩写	说明
C	control
D	delete
E	create
F	filescan
M	chmod
O	chown
R	read
S	security
T	utime
U	update

缩写	说明
V	rename
W	write
x	execute

-d *access*

指定类的默认访问模式。 这是在您未指定访问权限的情况下执行授权命令时，CA Access Control 分配给用户的访问模式。 授权命令所使用的这种隐含访问权限与分配给资源的默认访问权限不同。 可能的访问模式在 -a 选项中列出。

-f

指定 CA Access Control 将接受新类名，即使该名称包含的字母全部大写也是如此。

注意：默认情况下，seclassadm 实用程序不允许您创建字母全部大写的类名。 CA Access Control 大写名称是为预定义的 CA Access Control 类保留的。

--g

指定新类为将现有类成员分组的资源。 现有类与新组类之间的关系与数据库中任意类及其组类之间的关系相同（例如：TERMINAL 和 GTERMINAL）。对现有类成员分组的资源必须以大写字母 G 开始。也就是说，它具有与现有类相同的名称，但以前缀 *G* 开始。

--o

为新类创建 *_default* 记录并设置其默认访问。

-p *db_pathname*

指定本地数据库的完整路径名。

默认情况下，此实用程序在当前目录中的数据库中运行。 使用此选项可定义数据库所在的其他目录。

-t

指定该类为 Unicenter TNG 类。

示例：向数据库中添加新类

以下示例演示了您可以如何使用 seclassadm 实用程序向数据库中添加类：

- 要添加名为 *dbfield* 的资源类，请使用以下命令：

  ```
  seclassadm -add dbfield
  ```

- 要添加名为 *report* 且仅具有 READ 访问权的资源类，请使用以下命令：

  ```
  seclassadm -add report -d R -a R
  ```

- 要添加名为 *batch_jobs*、具有 READ、WRITE 和 MODIFY 权限且在未指定权限的情况下将 READ 访问权作为默认权限的资源类，请使用以下命令：

  ```
  seclassadm -add batch_jobs -d R -a RWM
  ```

- 要添加其对象是类 DEPTA 中的资源组且具有访问执行权限和隐式访问执行权限的新类，请使用以下命令：

  ```
  seclassadm -add DEPTA -d X -a X -g -f
  ```

secompas 实用程序—比较密码

在 UNIX 上有效

secompas 实用程序可将 CA Access Control 数据库中的密码与 UNIX 密码文件中的密码进行比较。

对于 CA Access Control 数据库中的每个用户，此实用程序均可输出一行（包含用户名）和一条消息，该消息将指明该用户是否已在 UNIX 中定义、是否在 CA Access Control 中没有密码或者密码是否相配。 此实用程序还显示它比较过的用户总数以及密码不匹配的用户数。 仅在密码存在于这两种环境中且不相同的情况下，才将其添加到此总数。 如果某个用户未在某种环境中定义，或者密码从某种环境中丢失，则 secompas 不会将其添加到不匹配密码的计数器中。

要比较密码，secompas 实用程序将使用 /etc/passwd 文件、shadow 密码文件以及 NIS/NIS+ 密码映射。

注意：您必须具有 ADMIN 属性，才能使用此实用程序。

此命令格式如下：

```
secompas [-db] [-ok] [-ux]
```

-db

指定不显示在 CA Access Control 数据库中没有密码的用户。

-h

显示该实用程序的帮助。

-ok

指定不显示在 CA Access Control 数据库和 UNIX 中具有相同密码（密码匹配）的用户。

-ux

指定不显示 UNIX 中不存在的用户。

示例：实用程序输出

以下示例显示了此实用程序的示例输出：

```
检查 root           : 在 Access Control 数据库中无密码。
检查 tst_001        : 未在 UNIX 中定义。
检查 tst_002        : UNIX 密码文件中无密码
检查 tst_003        : *** 密码不匹配。 ***
检查 tst_004        : *** 不匹配 - UNIX 已禁用 ***
检查 tst_005        : 正常

数据库中共找到 6 个用户。
发现 2 个不匹配的密码。 （1 UNIX 已禁用）。
```

以下是对上述输出中每一行的说明：

```
检查 root           : 在 Access Control 数据库中无密码。
```

未在 CA Access Control 数据库中定义用户 *root*，或者在数据库中定义了该用户，但数据库中没有密码。

```
检查 tst_001        : 未在 UNIX 中定义。
```

在 CA Access Control 数据库中定义了用户 tst_001，但是未在 UNIX 中定义。

```
检查 tst_002        : UNIX 密码文件中无密码
```

在 UNIX 中定义了用户 tst_002，但没有密码。

```
检查 tst_003        : *** 密码不匹配。 ***
```

用户 tst_003 的 CA Access Control 密码与 UNIX 密码不匹配。

```
检查 tst_004        : *** 不匹配 - UNIX 已禁用 ***
```

tst_004 用户帐户在 UNIX 环境中被禁用。 secompas 可通过 /etc/passwd 文件中密码前面的星号 (*) 来识别禁用的用户帐户。

```
检查 tst_005        : 正常
```

用户 tst_005 的 CA Access Control 密码与 UNIX 密码相匹配。

secons 实用程序

secons 实用程序是 CA Access Control 安全控制台。 通过它可以执行下列任务：

- 在 UNIX 上：
  - 显示运行时统计信息 (p. 135)
  - 管理并发登录选项 (p. 126)
  - 管理 CA Access Control 跟踪 (p. 125)
  - 管理资源缓存 (p. 127)
  - 管理 CA Access Control 关闭 (p. 122)
  - 重新加载配置设置 (p. 149)
  - 删除 XUSER 对象 (p. 132)
  - 显示内核表 (p. 139)
  - 清理、启用或禁用内核缓存表 (p. 148)

- 在 Windows 上：
  - 控制检测运行时设置 (p. 150)
  - 显示运行时统计信息 (p. 137)
  - 显示 ACEE 记录 (p. 133)
  - 管理并发登录选项 (p. 126)
  - 管理 CA Access Control 跟踪 (p. 125)
  - 刷新网络资源的 IP 地址 (p. 149)
  - 删除 XUSER 对象 (p. 132)
  - 解析循环帐户 (p. 134)
  - 关闭 CA Access Control (p. 132)
  - 显示用户名和安全凭据 (p. 153)

secons 实用程序适用于安全管理员和其他用户。 但是，只有某些选项适用于不具有 ADMIN 属性的用户。 这些选项包括：

-m（跟踪管理）、-d-、-d+、-ds（登录管理）和 -whoami（用户的凭据）。

secons 实用程序—管理 UNIX 中 CA Access Control 的关闭

在 UNIX 上有效

secons 实用程序可关闭 CA Access Control 及相关的后台进程。 您也可以使用此实用程序查找哪个进程仍在执行 CA Access Control 代码。

只有定义为 ADMIN 或 OPERATOR 的用户可以关闭 CA Access Control。 要关闭远程计算机上的 CA Access Control，您必须定义为这些远程计算机上的 ADMIN 或 OPERATOR。

此命令格式如下：

```
secons [-s [hosts | ghosts]] \
    [-S [{selogrd | selogrcd | serevu}]] \
    [-sc] [-scl] [-sk]
```

-s [*hosts* | *ghosts*]

关闭已定义的远程主机列表（用空格分隔）中的 CA Access Control 后台进程。 如果不指定任何主机，将关闭本地主机上的 CA Access Control。

您可以输入 *ghost* 记录的名称来定义一组主机。如果从远程终端使用此选项，此实用程序会请求进行密码验证。 您还需要具有远程和本地计算机的管理权限，以及对远程主机数据库中的本地计算机的写入权限。

-S [{selogrd | selogrcd | serevu}]

如果您未定义后台进程，则请终止 CA Access Control 后台进程并尝试终止活动的后台进程 selogrd、selogrcd 和 serevu。 如果将 seos.ini 文件的 [daemons] 部分中的 selogrd、selogrcd 或 serevu 标记设置为 *yes*，则请将终止请求发送到正在运行的 CA Access Control 主后台进程，或者如果 CA Access Control 已关闭，则请将此终止信号发送到指定后台进程。

如果您定义了后台进程，则 secons 将不终止 CA Access Control 后台进程。 如果将 seos.ini 文件的 [daemons] 部分中的相应标记设置为 *yes*，则会将终止请求发送到正在运行的 CA Access Control 主后台进程，或者如果 <eAC 已关闭，则会将此终止信号发送到该后台进程。

-sc[l]

显示仍在执行 CA Access Control 代码的进程。

如果在 CA Access Control 顶部加载的应用程序有一个被 CA Access Control 挂钩的公开系统调用，您就无法卸载 CA Access Control。得知哪些进程仍在执行 CA Access Control 代码后，您可以关闭这些进程并卸载 CA Access Control 内核模块。 然后，可以使用 UNIX 退出命令在卸载内核前自动关闭这些进程，并在内核卸载后重新启动。

-sc 输出为具有两列的表格，其中第一列中显示系统调用号，第二列中显示进程标识符。

-scl 选项还显示仍在执行 CA Access Control 代码的进程的父进程 ID (PPID)、UID、时间和程序名称信息。 通过时间信息，您可以查看该进程已钩住 CA Access Control 的时间。如果时间相对较短，则该挂钩可能是临时性的。

也可以在运行 CA Access Control 时运行此项，以帮助您提前预知可能导致卸载问题的原因。 但是，在某些情况下（例如接受命令），CA Access Control 代码会在卸载时删除挂钩。 这表示在运行 CA Access Control 时您看到的某些处于活动状态的挂钩实际上可能不会影响卸载。

注意：默认情况下，CA Access Control 会监控被 CA Access Control 拦截的系统调用。 如果您*不*希望 CA Access Control 监控系统调用，则必须将 seos.ini 文件中的 syscall_monitor 标记设置为 0（禁用）。

-sk

关闭所有 CA Access Control 后台进程并准备好要卸载的 CA Access Control 内核扩展。

示例：关闭 CA Access Control

- 要关闭 CA Access Control 后台进程，请输入：

```
secons -s
```

- 要关闭远程主机 HOST1 和 HOST2 上的 CA Access Control 后台进程，请输入：

```
secons -s HOST1 HOST2
```

示例：显示仍在执行 CA Access Control 代码的进程的信息

- 显示仍在执行 CA Access Control 代码的进程的基本信息：

```
secons -sc
```

显示的输出如下所示：

```
CA Access Control secons vX.X.X.xxx－控制台实用程序
版权所有 (c) YYYY CA。 保留所有权利。
活动系统调用:

syscall    5 - PID:  27477
```

- 显示有关仍在执行 CA Access Control 代码的进程的详细信息：

```
secons -scl
```

显示的输出如下所示：

```
CA Access Control secons vX.X.X.xxx－控制台实用程序
版权所有 (c) YYYY CA。 保留所有权利。
活动系统调用:

-Syscall  102 - PID:   2105  PPID:      1 UID:      0 TIME:    4d-4h PROGRAM
NAME: /usr/sbin/vsftpd
 Syscall    5 - PID:  24269  PPID:   4289 UID:      0 TIME:   2d-21h PROGRAM
NAME: /bin/bash
```

输出行开头的破折号 (-) 表示 CA Access Control 通过评估认定此挂钩不可能在卸载时引发问题。 使用此命令时，CA Access Control 还会向审核日志中添加行，以记录 CA Access Control 卸载是否可能成功。 例如：当运行 secons -scl 时，如果至少有一个阻止系统调用可能会阻止 CA Access Control 卸载，将创建以下审核记录：

```
10 Nov 2008 05:47:22 F CHECK       root       Scan      339  0 SEOS_syscall
unload
```

secons 实用程序—管理 CA Access Control 跟踪

secons 实用程序可管理 CA Access Control 跟踪。 通过跟踪可以监控操作系统事件。 CA Access Control 可累积报告操作系统事件的消息文件，然后显示出来。

此命令格式如下：

```
secons [-t+] [-t-] [-tt] [-ts] [-tc] [-tv [size] [-file fileName]]

secons -m message

secons -pupm trace {enable | disable | clear}
```

-m *message*

将文本消息添加至跟踪文件。

-t+

启用跟踪，使 CA Access Control 引擎 (seosd) 将指定其操作和活动的消息转储到跟踪文件中。

-t-

禁用跟踪，阻止 CA Access Control 引擎 seosd 将消息转储到跟踪文件中。

-tc

清除跟踪文件，删除其中的所有记录。

注意：无论 seosd 是否正在运行，均可使用此选项。

-ts

显示当前跟踪状态。

-tt

切换跟踪状态。

-tv [*size*] [-file *fileName*]

显示实时跟踪输出。 实用程序将显示跟踪文件的最后*大小* KB 数（默认情况下为 2 KB），并保持会话为打开状态，以便显示所有添加到文件中的新跟踪消息。 这与 UNIX tail -f 命令类似。

使用 Ctrl+C 组合键可停止此操作。

注意：无论 seosd 是否正在运行，均可使用此选项。 使用 full_year 配置设置可选择是以四位数（默认设置 yes）还是两位数显示年份。

大小

从最后开始，以千字节指定要显示的文件部分的大小。 指定 0 可显示整个跟踪文件。 如果未指定此选项，secons 将使用默认设置 2 KB。

-file *fileName*

读取 *fileName* 而非 *ACInstallDir*/log/seosd.trace。

-pupm trace {enable | disable | clear}

适用于 特权用户密码管理 代理

指定运行期间 特权用户密码管理 代理的跟踪选项。无需重新启动 CA Access Control 即可修改跟踪选项。

限制：enable（启用跟踪）；disable（禁用跟踪）；clear（清除跟踪文件）。

重要说明！ 指定的跟踪选项仅适用于当前会话。 在 CA Access Control 重新启动后，将根据 PUPMAgent 部分中的 OperationMode 标记设置跟踪选项。

secons 实用程序—管理并发登录选项

secons 实用程序可管理并发登录选项。 您可以将 CA Access Control 配置为阻止用户多次登录。 这可以防止入侵者登录到已经登录的用户的帐户。

此命令格式如下：

```
secons [-d+] [-d-] [-ds] [-l+] [-l-] [-ls] \
       [-u+ userName] [-u- userName] [-us userName]
```

-d+

为执行命令的用户启用并发登录。

-d-

为执行命令的用户禁用并发登录。 使用此命令将禁用该用户到本地计算机的任何并发登录。

注意：您也可以将此命令放在用户的 .login 或 .cshrc 文件中以禁用并发登录。

-ds

显示执行命令的用户的并发登录设置。

-l+

禁用系统范围的并发登录。

注意：默认情况下，CA Access Control 启用登录，但是，如果关闭系统以进行维护，则可以在特定时间段内禁用登录。

-l-

禁用系统范围的并发登录。

-ls

显示系统范围内的登录状态。-

-u+ ***userName***

为已定义的用户启用并发登录。

-u- ***userName***

为已定义的用户禁用并发登录。

-us ***userName***

显示已定义用户的并发登录设置。

secons 实用程序—在 UNIX 上管理资源缓存

在 UNIX 上有效

secons 实用程序可管理 UNIX 上的资源缓存（文件缓存）。 缓存（运行时表）会“记住”对 FILE 类中资源授权请求的上一次回答（允许或拒绝）。请求相同的权限时，会使用存储在缓存表中的最后一个响应来回答请求。

此命令格式如下：

```
secons [-C+] [-C-] [-CA value] [-CC interval] [-CD] \
    [-CF value] [-CI init_value] [-CP interval] -CU value]
```

-C+

启用文件授权的缓存。

-C-

禁用文件授权的缓存。

-CA *value*

指定表中授权记录的最大数。

默认值：80

限制：1 到 800 之间的数字

-CC *interval*

指定缓存清理间隔的时间（分钟）。

默认值：60

限制：大于 0 的数字

-CD

将缓存表显示为标准输出。

-CF *value*

指定表中文件记录的最大数。

默认值：20

限制：1 到 200 之间的数字

-CI *init_value*

指定缓存表中新记录的初始优先级值。

默认值：10

-CP *interval*

指定缓存优先级计算时间间隔。

默认值：1（一个记录）

限制：1 到 10 之间的数字

-CU *value*

指定表中用户记录的最大数。

默认值：50

限制：1 到 500 之间的数字

示例：更改缓存设置

以下示例展示了如何更改缓存设置，以将缓存中的文件、用户和授权记录的最大数设为 60：

```
secons -CF 60 -CU 60 -CA 60
```

示例：显示缓存表

以下示例展示了 secons -CD 命令的输出：

```
================================================================================
        FILE CACHE (配置、统计信息和调度进程数据)
--------------------------------------------------------------------------------
sizes(bytes)       tables:                | max records:      | intervals
缓存    头       文件     用户     授权   | 文件 用户 授权 |清除 优先级
--------------------------------------------------------------------------------
40244    44        5600     4200    30400 |  20    50    80   |   60   1
================================================================================
表   |统计信息         | 优先级     |最小 | 已用   | 平均       |优先级 |初始
name    |  hits misses (ok)| maxim  minim|ind | used | usage   life |fact|prio
--------------------------------------------------------------------------------
文件  |    5     1   83% |   0      0  |  0 |   1  |             |    |
用户  |    5     1   83% |  10      2  |  0 |   1  |  0       0   |  1 | 10
授权  |    4     2   66% |   2         |  0 |   2  |             |    |
================================================================================
文件表
--------------------------------------------------------------------------------
编号   类型     pid 优先级 用户                                  文件名
--------------------------------------------------------------------------------
0   显式    372      0    0                                    /etc/shadow
================================================================================
用户表
--------------------------------------------------------------------------------
编号    用户名      优先级    寿命    已用   UID  EUID  RUID 授权 上一(文件)下一
--------------------------------------------------------------------------------
0    root           2       2      7     0    0     0    0    50(   0)  50
================================================================================
授权结果表  (R - 结果: 'P'-允许, 'D'-拒绝 ...)
--------------------------------------------------------------------------------
编号   R ACEE acc  日志阶段 上一(用户)下一 时间        终端   程序
--------------------------------------------------------------------------------
0   P   6  read  0  00036 80(  0)  1   07:48:25            /usr/bin/login
================================================================================
```

以下内容对上述输出进行了说明：

输出包括五个部分：

- 缓存配置。 它包含以下字段：
  - 缓存大小（字节）
  - 缓存头的大小（字节）
  - 文件表的大小（字节）
  - 用户表的大小（字节）
  - 结果表的大小（字节）
  - 最大文件记录数
  - 最大用户记录数
  - 最大结果记录数
  - 统计信息：表中的匹配对象数
- 文件记录表。 它包含以下字段：
  - 记录的序号
  - 文件的类型（显式、隐式）
  - 进程 ID 号
  - 记录的优先级，是其用户优先级的总和
  - 用户表中相应的用户记录编号
  - 文件的名称
- 用户表。 它包含以下字段：
  - 记录的序号
  - 用户名
  - 记录的优先级
  - 记录寿命计数器
  - 记录使用计数器
  - 用户 ID；用户有效 ID；真正由安全性使用的 ID
  - 授权表中相应的授权记录编号
  - 用户链中上一个用户记录编号
  - 相应的文件记录编号
  - 用户链中下一个用户记录

- 授权结果表。 它包含以下字段：
  - 终端
  - 阶段
  - 授予阶段
  - 结果－授权结果（P 或 D）
  - ACEE 编号
  - 访问类型
  - 记录选项标志值
  - 所做决定的阶段编号
  - 记录链中的上一授权记录编号
- 相应的用户记录编号
  - 记录链中的下一授权记录编号
  - 统计信息：表中的不匹配记录数
  - 授权类
  - 程序名称（带有 via 参数）
  - 通知字符串
  - 更新时间 (GMT)
- 调度程序数据。 它包含以下字段：
  - 统计信息：表中的不匹配记录数
  - 统计信息：表中的匹配记录数
  - 表中的最高优先级
  - 表中的最低优先级
  - 具有最低优先级的项数
  - 已使用的记录数
  - 平均使用情况（仅适用于用户表）
  - 平均寿命（仅适用于用户表）
  - 优先级计算因子（仅限用户表）
  - 记录优先级的初始值（仅适用于用户表）

secons 实用程序—在 Windows 上关闭 CA Access Control

在 Windows 上有效

secons 实用程序可关闭 CA Access Control 引擎和本地工作站上或者一个或多个远程工作站上的所有其他 CA Access Control 服务。

只有定义为 ADMIN 或 OPERATOR 的用户可以关闭 CA Access Control。 要关闭远程计算机上的 CA Access Control，您必须定义为这些远程计算机上的 ADMIN 或 OPERATOR。

此命令格式如下：

```
secons -s [hosts | ghosts]
```

-s [*hosts* | *ghosts*]

在已定义的、以空格分隔的远程主机上关闭 CA Access Control 服务。 如果不指定任何主机，将关闭本地主机上的 CA Access Control。

您可以输入 ghost 记录的名称来定义一组主机。 如果从远程终端使用此选项，此实用程序会请求进行密码验证。 您还需要具有远程和本地计算机的管理权限，以及对远程主机数据库中的本地计算机的写入权限。

secons -dbclean—从 CA Access Control 数据库删除 XUSER 对象

secons 实用程序可从 CA Access Control 数据库中删除未解析为其本地安全标识符 (SID) 的 XUSER 对象。 使用 secons -dbclean 命令可以删除不再存在于本地环境中的 XUSER 对象。

此命令格式如下：

```
secons -dbclean <osuser>
```

-dbclean

指定从 CA Access Control 数据库中删除未解析的所有 XUSER 对象。

<osuser>

指定本地用户帐户名。

secons -acee 函数－在 Windows 上显示 ACEE 记录

在 Windows 上有效

通过 secons 实用程序可监控 Accessor Element Entry (ACEE) 表，该表将访问者缓存在授权引擎中。 ACEE 存储关于以下用户的信息：

- **登录用户**－已登录到操作系统的用户。 此类用户的特定 ACEE 属性为：
  - 登录会话 ID
  - 登录会话类型
- **管理用户**－已登录到 CA Access Control 管理应用程序（使用 LCA 连接）的用户。 例如：selang。
- **授权 API 用户**－在 SEOSROUTE_* API 中提及的用户。
- **SPECIALPGM 逻辑用户**－至少在一条 SPECIALPGM 记录中提及的用户。 此类用户的特定 ACEE 属性为：
  - 与 SPECIALPGM 记录的 ACEE 关联性
- **内置用户**－CA Access Control 中内置的用户。 例如：*_undefined*。

注意：仅 CA Access Control 管理员可使用此命令

此命令格式如下：

```
secons -acee [handle | all | list]
```

all

显示所有 ACEE 记录。

handle

定义要显示的 ACEE 句柄。

list

显示所有 ACEE 记录的摘要列表，而不显示完整的详细信息。

示例：显示 ACEE 记录

- 此示例将显示 ACEE 中句柄的列表：

  ```
  secons -acee list
  ```

  secons 输出类似为：

  ```
  ACEE handle '0' represents 'Logged on User': NT AUTHORITY\ANONYMOUS LOGON (OS
  User)
  ACEE handle '1' represents 'Logged on User': NT AUTHORITY\NETWORK SERVICE (OS
  User)
  ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86\John
  ACEE handle '3' represents 'Logged on User': NT AUTHORITY\LOCAL SERVICE (OS
  User)
  ACEE handle '4' represents 'Logged on User': NT AUTHORITY\SYSTEM (OS User)
  ACEE handle '5' represents 'Management User': COMP1-SRV-X86\John
  ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
  ```

- 此示例将显示 ACEE 中的句柄 6：

  ```
  secons -acee 6
  ```

  secons 输出类似为：

  ```
  ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
  ACEE was created at: Wed Feb 20 17:35:52 2008
  ACEE was last accessed at: Wed Feb 20 17:35:52 2008
  ACEE user role is: Regular
  ACEE audit mode is: Failure, Login Success, Login Failure; Originated from
  User definition
  ACEE user is a member of 0 'CA Access Control' groups
  ACEE user is associated with 1 SPECIALPGM records
      1. C:\WINDOWS\system32\calc.exe
  ```

secons -checkSID 函数—在 Windows 上解析循环帐户

在 Windows 上有效

secons 实用程序可将每个企业帐户（XUSER 和 XGROUP 资源）的安全标识符 (SID) 与本地 Windows 帐户 SID 进行比较，并创建循环帐户的备份。 由于 CA Access Control 授权基于 SID，其中 CA Access Control 访问者资源的 SID 与本地帐户 SID（循环帐户）有所不同，因此实用程序将创建新的帐户（与旧帐户具有相同的名称）并使用以下命名约定备份过时资源：*SID* (*accountName*)

注意：有关循环企业存储帐户的详细信息，请参阅*《适用于 Windows 的端点管理指南》*。

此命令格式如下：

```
secons -checkSID {-groups | -users} [accountName [,accountName...]]
```

-groups

指定 secons 应检查企业组记录。

-users

指定 secons 应检查企业用户记录。

accountName

指定 secons 应搜索的用户或组的名称。 如果忽略 *accountName*，secons 将查找所有组和用户。

secons -i 函数－在 UNIX 上显示运行时统计信息

在 UNIX 上有效

secons 实用程序将显示有关系统行为的 CA Access Control 运行时统计信息。 使用该信息可了解网络连接请求、审核和错误日志队列的大小、缓存表的大小以及数据库大小和数据库每部分中的记录数。

此命令格式如下：

```
secons -i
```

-i

以格式化文本形式显示运行时统计信息。

示例：显示运行时数据

以下示例展示了 secons -i 命令的输出：

```
运行时统计信息:
            --------------------
            INet 统计信息:
                  已拒绝的请求    : 0
                  已授权的请求   : 17
                  找到的错误       : 0
            队列大小:
                  审核日志: 0
                  错误日志: 0
            缓存表信息:
                  ACEE 句柄       :       11
                  受保护客户端:        0
                  受托程序 :        77
                  未受托程序:         3
            数据库信息:（记录计数与第一个空闲 ID）
                  类      :     235 ( CID     0x00f0 )
                  属性   :    4829 ( PID     0x1346 )
                  对象      :     842 ( OID 0x0000035a )
                  PropVals    :    4109 ( N/A )
```

以下是对上述输出中每一行的说明：

```
INet 统计信息:
      已拒绝的请求    : 0
      已授权的请求   : 17
      找到的错误       : 0
```

显示由 CA Access Control 执行的网络访问授权的统计信息。 这些行汇总了授权网络请求期间拒绝、授予和错误的数量。

```
队列大小:
      审核日志: 0
      错误日志: 0
```

由于 CA Access Control 使用文件锁定创建记录，因此，稍后会将某些事件保存在内存中并写入日志文件。 如果这些值超过 10，则可能会发生干扰 CA Access Control 记录功能的错误。

```
缓存表信息:
      ACEE 句柄       :       11
      受保护客户端:       0
      受托程序 :       77
      未受托程序:       3
```

显示有关 CA Access Control 使用的缓存表大小的信息：

- Accessor Element Entry (*ACEE)* 是包含登录进程的表。-
- *受保护客户端*列出了缓存客户端的数量。 通常情况下，该值为 0。
- *Trusted Programs* 列出类 PROGRAM 中已缓存在内存中的条目数。 通常，应将所有程序缓存为可信任的程序。
- *Untrusted Programs* 显示所发现的未受托程序数。

```
数据库信息:（记录计数与第一个空闲 ID）
      类      :     235 ( CID     0x00f0 )
      属性   :    4829 ( PID     0x1346 )
      对象      :     842 ( OID 0x0000035a )
      PropVals    :    4109 ( N/A )
```

有关数据库大小和数据库每个部分中的记录数的常规信息。

secons -i 函数—在 Windows 上显示运行时统计信息

在 Windows 上有效

secons 实用程序可显示 CA Access Control 运行时统计信息和内部计数器。 使用此统计系统行为信息可了解以下内容：

- 为每个拦截类型触发了多少事件。
- 通过将缓存事件的数量与完全授权事件数量比较说明每个内核缓存的效果。

注意：正常情况下，审核队列在活动增加的时段会增大。 但是，当加载重新成为正常状态时则会减小队列大小。

此命令格式如下：

```
secons -i [-reset]
```

-i

以格式化文本形式显示运行时统计信息。

-reset

（可选）将运行时计数器重置为零。

示例：显示运行时数据

以下是在 secons -i 命令输出中需要加以说明的信息：

数据库运行时数据

显示 CA Access Control 数据库中类、对象及属性的数量，最后创建的类、对象和属性的 ID，以及属性值的数量。

通过此信息可评估数据库的大小。 使用的对象和属性越多，数据库就越大。

内核运行时数据

显示每个内核缓存（文件、注册表和代理）的创建时间、大小和效率。效率是指全部事件数量中审核事件所占数量。 剩下的拦截事件遵守授权流程。

通过此信息可评估每个内核缓存的需求和效率。

内核审核信息

显示当前内核审核队列大小及达到的最大大小及出现时间。

通过此信息可评估审核队列行为。 应确定审核队列没有超过分配的最大队列大小，此大小在 FsiDrv\MaxAuditRecordLimit CA Access Control 注册表项中设置。达到该限制时，CA Access Control 将会非常缓慢地生成审核事件以便解析队列。

用户模式强制执行运行时数据

显示拦截的文件、注册表、登录、终止和 Windows 服务事件（完全强制模式）的信息。 可以了解由授权引擎授权的事件数量以及授权流程完成每个类所花费的最长和平均时间。

通过此信息可对活动的生产系统中的问题进行疑难解答。 其可为您提供某些有价值的初始数据，而无需关闭 CA Access Control。

用户模式审核运行时数据

显示审核事件的信息（缓存的已拦截事件）。

通过此信息可监控用户模式审核队列行为。 如果最大审核队列持续增加，请确保 CA Access Control 可以写入审核日志文件。 如果系统的磁盘空间用尽或者对文件不具有本地访问权限，CA Access Control 可能无法写入文件。

注意：正常情况下，审核队列在活动增加的时段会增大。 但是，当加载重新成为正常状态时则会减小队列大小。

secons -kt 函数－在 UNIX 上显示内核表

在 UNIX 上有效

secons 实用程序显示内核表。

此命令格式如下：

```
secons -kt tableNumber
```

-kt

显示指定的内核表。

tableNumber

指定要显示的内核表。 *tableNumber* 必须为以下值之一：

1

指定显示 SpecPgm 内核表。

2

指定显示 TrustPg 内核表。

3

指定显示 LoginPg 内核表。

4

指定显示 DBfiles 内核表。

5

指定显示 FRegExp 内核表。

6

指定显示 DCMfile 内核表。

7

指定显示 AC pids 内核表。

8

指定显示 InoCach 内核表。

注意： 在 Linux 上无效。

9

指定显示 F cache 内核表。

10

指定显示 NetwDCM 内核表。

11

指定显示 MntDirs 内核表。

12

指定显示 F inode 内核表。

13

指定显示 STOPbyp 内核表。

注意：如果未启用 STOP，那么您无法显示此内核表。

14

指定显示 STOPexp 内核表。

注意：如果未启用 STOP，那么您无法显示此内核表。

15

指定显示 Family 内核表。

16

指定显示 DbgProt 内核表。

17

指定显示 TCPport 内核表。

18

指定显示 TCPoutp 内核表。

19

指定显示 ProcSrv 内核表。

示例：显示 DBfiles 内核表

以下示例为您显示当您显示 DBfiles 内核表时的输出示例：

```
secons -kt 4
DBfiles
file    ID      i-node  device  program name
1       29      280391  356515  /opt/CA/AccessControl/seosdb/seos_ids.dat
2       3       0       0       /opt/CA/AccessControl/etc/privpgms.init
```

内核表

内核表列出经常访问的信息以帮助提高 CA Access Control 性能。 内核表提高性能的原因是 CA Access Control 不需要检查数据库就可以允许、拒绝或解析列在内核表中的事件。

CA Access Control 包括以下类型的内核表：

- 缓存表－列出先前资源访问请求的结果、解析的 inode 号以及接受的传入 TCP 请求。
- 受保护资源表－列出请求访问资源对象和请求访问的时间，CA Access Control 总是将授权请求发送到 CA Access Control 引擎。
- 跳过表－列出请求访问资源对象和请求访问的时间，CA Access Control 在不将授权请求发送到 CA Access Control 引擎的情况下允许访问。
- 进程表－列出有关在系统中运行的所有进程的信息。

下表提供有关各内核表的信息：

表名	类型	列表	列名	配置设置
SpecPgm	受保护资源	SPECIALPGM 类中的所有对象	flags; user; oid; i-node; device; program	SPECIALPGM 类记录
TrustPg	受保护资源	PROGRAM 类中的所有对象	flags; i-node; device; program	PROGRAM 类记录
LoginPg	受保护资源	LOGINAPPL 类中的所有对象	flags; i-node; device; program	LOGINAPPL 类记录
DBfiles	受保护资源	FILE 类中的所有对象	file ID; i-node; device; program	FILE 类记录 **注意：**此表中的最大记录数由 seos.ini 文件的 SEOS_syscall 部分中的 max_regular_file_rules 定义。

表名	类型	列表	列名	配置设置
FRegExp	受保护资源	在 FILE 类中定义的一般文件访问规则	fid; expression	由 FILE 类记录中的一般规则定义 **注意：**此表中的最大记录数由 seos.ini 文件的 SEOS_syscall 部分中的 max_general_file_rules 定义。
DCMfile	跳过	使用 GAC 定义的 Do-not-call-me 文件	fid; user; type; access	GAC.init 文件
ACpids	跳过	CA Access Control 后台进程的进程 ID	pid; service; contractID	-
InoCach	缓存	缓存的 inode	i-node; device; priority; entry	seos.ini 文件的 SEOS_syscall 部分中的 cache_enabled
F cache	缓存	缓存的文件访问授权结果	file ID; access; acee; answer; phash; prio	-
NetwDCM	缓存	缓存已接受的传入 TCP 连接	peer; port; local port; flag; prio	seos.ini 文件的 seosd 部分中的 UseNetworkCache
MntDirs	受保护资源	CA Access Control 防止挂接的目录	dir ID; i-node; device; mount point	-
F inode	受保护资源	FILE 类中对象的 Inode 和设备号	file ID; i-node; device; links	-
STOPbyp	跳过	CA Access Control 不提供 STOP 保护的 PROGRAM 类中的对象	i-node; device; program	如果启用 STOP，此表中的对象有 SPECIALPGM 记录并带有属性 pgmtype(STOP)
STOPexp	跳过	定义 CA Access Control 不提供 STOP 保护的 PROGRAM 类中对象的正则表达式	priority; n-chars; expression	如果启用 STOP，此表中的对象由 SPECIALPGM 记录并带有属性 pgmtype(STOP) 中的一般规则定义

表名	类型	列表	列名	配置设置
Family	跳过	CA Access Control 后台进程	service; pid; contractID	-
DbgProt	受保护资源	CA Access Control 防止调试的 CA Access Control 二进制文件	pid; access; name in proc	-
TCPport	跳过	seos_syscall 不将事件传递到 seosd 的端口	TCP 端口	seos.ini 文件的 seosd 部分中的 bypass_TCPIP
TCPoutp	跳过	seos_syscall 不将传出连接事件传递到 seosd 的端口	TCP 端口	seos.ini 文件的 seosd 部分中的 bypass_outgoing_TCPIP
ProcServ	进程	列出有关在系统中运行的所有进程的信息	#n; pid; ppid; acee; flags; uid; euid; zone; arg0; ACuser **注意：**不由 secons 实用程序显示的此表中有许多内部列	-

内核表列名称

下表对内核表列名称进行说明：

#n

内核表中的条目数。

access

定义 CA Access Control 允许的访问类型或用户请求的访问类型。值为访问类型的总和：

1—read
2—write
4—chown
8—chmod
16—rename
32—unlink
64—utimes
128—chattr
256—link
512—chdir
1024—create

acee

定义发出访问请求用户的 ACEE。

ACuser

定义 CA Access Control 用户的用户名。

answer

定义 CA Access Control 对访问请求所做出的响应（允许或拒绝）。有效值包括：

0—拒绝

1—允许

arg0

定义程序名，与程序执行时在参数号 0 中定义的相同。

contractID

（仅 Solaris 10）定义合同进程 ID。

device

定义文件所在的逻辑磁盘。

dir ID

定义目录 ID。

entry

定义 inode 的字符串值。

euid

定义有效用户 ID。

expression

定义指定条目应用的资源的表达式（用于字符串匹配的文本模式）。

fid *or* file ID

定义 CA Access Control 用于识别文件的文件 ID。

flags

定义条目的位掩码标志。

i-node

定义 inode 号。

links

定义文件硬链接数量。

local port

定义接受传入 TCP 连接的本地主机上的端口。

mount point

定义防止挂接的目录中的位置。

n-chars

定义表达式中字符数。

name in proc

定义 /proc 文件系统中的进程名称。

注意：在 /proc 文件系统中，每个进程表示为一个文件，文件名是进程号。

oid

定义对象 ID。

peer

定义对等主机地址。

phash

定义路径字符串的哈希值。

pid

定义进程 ID。

port

定义传入 TCP 连接源于的端口。

ppid

定义父进程 ID。

prio *or* priority

定义内核表中条目的优先级。 当内核表充满时，在 CA Access Control 将新条目写入到内核表时最低优先级的条目将被删除。

program *or* program name

定义程序名称。

service

定义 CA Access Control 服务（后台进程）的名称。

TCP 端口

定义条目应用的 TCP 端口。

type

定义受保护的文件类型。

uid *or* user

定义用户 ID。

zone

（仅 Solaris 10）定义区域 ID。

注意：此列的值针对非 Solaris 10 的计算机总是为 0。

缓存表

有三种类型的内核缓存表：

- **F cache**－文件缓存表缓存先前授权请求的结果。

  当提出的授权请求相同时，CA Access Control 会针对存储在文件缓存表中最后响应的请求做出回答。

  注意：文件缓存表每 30 分钟进行清理且在以下类中记录发生更改时进行清理：CALENDAR、CONTAINER、FILE、GFILE、GROUP、HOLIDAY、PROGRAM、SECLABEL、SECLEVEL、SHIFT 和 USER。

- **InoCach**－inode 缓存表缓存解析的 inode 号。

  当 CA Access Control 需要将 inode 号解析为文件名称时，它会在检查文件系统之前检查 InoCach 表。

- **NetwDCM**－网络缓存表存储已接受的传入 TCP 请求。

  当 CA Access Control 接收与网络缓存中的请求相同的传入 TCP 请求时，CA Access Control 会自动允许该请求。

可以使用 secons 实用程序显示、清理、启用和禁用内核缓存表。

受保护资源表

当 CA Access Control 拦截授权请求时，会检查所请求访问的资源是否列在内核中受保护资源表中。

如果资源列在受保护资源表中，那么 CA Access Control 总是将授权请求发送到 CA Access Control 引擎。 如果资源未列在受保护资源表中，CA Access Control 不会将授权请求发送到引擎，反而会在内核中解析访问请求。

跳过表

当 CA Access Control 拦截授权请求时，会检查所请求访问的资源是否列在内核中跳过表中。

如果资源列在跳过表中，CA Access Control 允许访问请求。 如果资源未列在跳过表中，CA Access Control 会将请求传递到 CA Access Control 授权引擎进行进一步访问检查。

secons -ktc 函数 — 在 UNIX 上清理、启用或禁用内核缓存表

在 UNIX 上有效

secons 实用程序清理、启用或禁用内核缓存表。

此命令格式如下：

```
secons -ktc optionNumber
```

-ktc

指定清理、启用或禁用内核缓存表。

optionNumber

指定要执行的操作。 *optionNumber* 必须为以下数字之一：

1

清理 F cache 表。

2

启用 F cache 表。

3

禁用 F cache 表。

4

清理 NetwDCM 表。

5

启用 NetwDCM 表。

6

禁用 NetwDCM 表。

7

清理 F inode 表。

注意：在 Linux 上无效。

8

启用 F inode 表。

注意：在 Linux 上无效。

9

禁用 F inode 表。

注意：在 Linux 上无效。

示例：清理 F cache 表

以下示例清理 F cache 表：

```
secons -ktc 1
```

secons -refIP 函数—刷新网络资源的 IP 地址

在 Windows 上有效

secons 实用程序可刷新数据库网络资源的 IP 地址。 要刷新特定主机，则必须已在该主机上刷新 DNS。 使用以下 Windows 命令手动刷新 DNS：

```
ipconfig /flushdns
```

此命令格式如下：

```
secons -refIP [hosts]
```

-refIP [*hosts*]

（仅限于 Windows）定义以空格分隔的列表，列出了 CA Access Control 将刷新网络资源 IP 地址的主机。 如果未列出任何主机，将刷新本地网络资源。

使用此选项将以当前 IP 地址更新 CA Access Control 资源，在动态分配 IP 地址的 DHCP 环境中特别有用。

secons -rl 函数—在 UNIX 上重新加载配置设置

在 UNIX 上有效

secons 实用程序将重新加载 seos.ini 文件。 这样可以升级您的配置设置而无需关闭 CA Access Control。

此命令格式如下：

```
secons -rl
```

-rl

（仅限于 UNIX）重新加载 seos.ini 配置文件并更新设置，而无需关闭 CA Access Control。

secons -v 函数－在 Windows 上控制检测运行时设置

在 Windows 上有效

secons 实用程序可控制 CA Access Control 检测运行时设置。 可使用此实用程序将外部 DLL 库加载到活动的进程，并修改 CA Access Control 检测插件的运行时跟踪配置。 必须具有 ADMIN 或 OPERATOR 属性才能执行此命令。

此命令采用以下格式来加载 DLL 库：

```
secons -v target load "dll_name"
```

此命令采用以下格式来启用或禁用 CA Access Control 检测插件的跟踪：

```
secons -v target trace plugin_name
{trace:enable|trace:disable}:{file:"tracefile_path"|debug}
```

注意：只有正确配置跟踪之后，CA Access Control 才会开始跟踪。

此命令采用以下格式来配置 CA Access Control 检测插件的跟踪：

```
secons -v target trace plugin_name trace:option:{sources:{1 | 4} | filtering:value
| filecyclic:{0 | 1} | filelimit:value }
```

debug

指定此命令启用或禁用针对调试输出通道的跟踪。

file:"*tracefile_path*"

定义 CA Access Control 用来写入跟踪的文件的完整路径。

注意：如果指定 trace:disable 参数，CA Access Control 将忽略为 file:"*tracefile_path*" 参数指定的任何值。

filecyclic:{0 | 1}

指定是否启用循环文件跟踪。 如果启用循环文件跟踪，当跟踪文件的大小达到指定的最大大小时，CA Access Control 将返回到跟踪文件的开头并继续写入跟踪。

此参数具有以下值：

0－禁用循环文件跟踪

1－启用循环文件跟踪

filelimit:*value*

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小。

filtering:*value*

定义用来筛选指定检测插件的跟踪的位筛选掩码。 CA Access Control 不会将筛选出的事件写入跟踪文件。

注意：如果不指定筛选选项（即指定 CA Access Control 将所有事件写入跟踪），请使用值 0xFFFFFFFF。 此参数的所有其他值取决于指定的插件。

load "*dll_name*"

指定将指定的 DLL 加载到目标进程。DLL 操作环境和目标进程操作环境必须相同。 例如：如果指定 32 位进程作为目标过程，则 DLL 也必须是 32 位。

重要说明！ DLL 必须位于 *ACInstallDir*\bin 文件夹中。

sources:{1 | 4}

指定 CA Access Control 输出跟踪的位置。

此参数具有以下值：

1—输出到文件

4—输出到调试 API 跟踪

目标

定义一个或多个目标进程。 此参数具有下列值之一：

all_32bit

指定将命令发送到计算机上运行的所有 32 位进程。

all_64bit

指定将命令发送到计算机上运行的所有 64 位进程。

PID

定义目标进程的进程 ID。 目标进程必须正在计算机上运行。

process_name

定义用于标识目标进程的名称的掩码。目标进程必须正在计算机上运行。例如：如果为此参数指定 cmd.exe，并且有三个 cmd.exe 实例正在计算机上运行，CA Access Control 会将命令应用于全部三个进程。

trace *plugin_name*

指定修改名为 *module_name*（例如：cainstrm 或 stopplg）的 CA Access Control 检测插件的运行时跟踪配置。

注意：必须指定该插件的 DLL 名称。 如果升级检测插件，并更改该插件的 DLL 名称，必须在命令中指定新 DLL 的名称。 例如：如果升级 cainstrm 插件，并且该插件升级后的 DLL 名称是 cainstrm2.dll，则必须将 cainstrm2 指定为 *plugin_name*。

trace:disable

指定启用目标插件的跟踪。

trace:enable

指定禁用目标插件的跟踪。

注意：此参数将在运行时更改跟踪启用标志的状态。 只有正确配置跟踪之后，CA Access Control 才会开始跟踪。

trace:option

指定配置目标插件的跟踪。

示例：启用对调试输出通道的跟踪

以下命令将在运行时针对计算机上所运行的 32 位进程中的所有 stopplg 插件文件更改跟踪启用标志的状态。 只有正确配置跟踪之后，CA Access Control 才会开始跟踪：

```
secons -v all_32bit trace stopplg trace:enable:debug
```

示例：将跟踪筛选掩码应用于插件

以下命令将跟踪筛选掩码应用于 PID 为 362 的进程中的所有 cainstrm 插件文件：

```
secons -v 362 trace "cainstrm trace:option:filtering:4294967295"
```

secons -whoami 函数 — 显示您的用户名和安全凭据

在 Windows 上有效

secons 实用程序可显示已为 CA Access Control 授权引擎所知的用户名。这是其存储在 Accessor Element Entry (ACEE) 表中的信息。 ACEE 存储关于以下用户的信息：

- **登录用户** — 已登录到操作系统的用户。 此类用户的特定 ACEE 属性为：
  - 登录会话 ID
  - 登录会话类型
- **管理用户** — 已登录到 CA Access Control 管理应用程序（使用 LCA 连接）的用户。 例如：selang。
- **授权 API 用户** — 在 SEOSROUTE_* API 中提及的用户。
- **SPECIALPGM 逻辑用户** — 至少在一条 SPECIALPGM 记录中提及的用户。 此类用户的特定 ACEE 属性为：
  - 与 SPECIALPGM 记录的 ACEE 关联性
- **内置用户** — CA Access Control 中内置的用户。 例如：*_undefined*。

此命令格式如下：

```
secons -whoami
```

示例：显示您的用户名和安全凭据

此示例将显示 CA Access Control 授权引擎所知的您自己的用户名和安全凭据：

```
secons -whoami
```

secons 输出类似为：

```
ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86\John
ACEE was created at: Wed Feb 20 17:34:47 2008
ACEE was last accessed at: Wed Feb 20 17:36:49 2008
ACEE user role is: Auditor, Administrator
ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User
definition
ACEE user is a member of 0 'CA Access Control' groups
ACEE's Logon session ID is: 0:68737
ACEE's Logon session type is: Interactive
```

更多信息：

sewhoami 实用程序 — 在 UNIX 上显示您的 CA Access Control 用户名和安全凭据 (p. 217)

secrepsw 实用程序—创建策略模型和 Shadow 文件

在 UNIX 上有效

secrepsw 实用程序可为 /etc/passwd 文件中的每个用户创建密码记录。这对于管理由通过 UNIX 环境运行的 PMDB 定义的用户十分必要。 该实用程序还可以创建和删除 shadow 文件。

注意：此实用程序位于 lbin 目录中，只有 root 可以使用。 您必须在使用该实用程序之前将 pmd.ini 文件中的 shadow 标记更改为 *yes*。

此命令格式如下：

```
secrepsw [-h] [-c] [-r PolicyModel] [-s PolicyModel]
```

-c

从本地计算机上的 /etc/passwd 和 /etc/shadow 文件创建新的策略模型密码文件。

-h

显示该实用程序的帮助。

-r *PolicyModel*

将用户名和密码从策略模型的 shadow 文件传回原始策略模型密码文件 (passwd)。

-s *PolicyModel*

将用户名和密码从策略模型密码文件 (passwd) 传输到策略模型的 shadow 文件。

sedbpchk 实用程序－备份数据库

在 UNIX 上有效

sedbpchk 实用程序可创建数据库的备份副本。 它将运行时数据库复制到临时位置，对临时数据库执行各种数据库完整性检查，如果数据库通过检查，则将临时数据库复制到备份位置。

如果数据库未通过完整性测试，则 sedbpchk 会尝试确定是否在进行复制时向数据库应用了更新。 如果应用了更新，则数据库已损坏的结论可能并不准确。

如果复制数据库时没有应用任何更新，则数据库已损坏的推断可能是正确的。 在这种情况下，会向系统管理员发送一封邮件，系统管理员便可使用备份目录覆盖损坏的运行时数据库。

注意：此脚本并*非*完全可靠。 它可能会在数据库并未损坏的情况下得出数据库已损坏的结论。 不过，数据库正常的结论始终是准确的。

要运行此脚本，您必须具有 root 和 ADMIN 权限。 在使用 sedbpchk 之前，建议您复查该脚本（位于 *ACInstallDir*/lbin 中，名为 sedbpchk.sh），以确认下列字段的值是否符合您站点的需要

MAIL_TO

指定向其发送数据库已损坏通知的用户的名称。

RETRIES

指定实用程序怀疑数据库损坏时，在发送通知前对数据库执行的检查次数。

ACInstallDir

指定 CA Access Control 安装目录的位置。

SE_BINDIR

指定 CA Access Control 二进制文件目录的位置。

SE_DB_DIR

指定 CA Access Control 运行时数据库目录的位置。

SE_BCKDIR

指定备份数据库目录的位置。

SE_TMPDIR

指定临时数据库目录的位置。

注意：此实用程序作为脚本文件提供；您需要指定 .sh 扩展名来运行该实用程序。

此命令格式如下：

```
sedbpchk
```

seerrlog 实用程序—显示错误日志记录

在 UNIX 上有效

seerrlog 工具可显示 CA Access Control 错误日志中的记录。 您必须具有读取错误日志文件的权限，或者是可以读取错误日志文件的组（在 error_group 配置设置中定义的组）的成员。

此命令格式如下：

```
seerrlog [-h] [-s date] [-e date] [-d] [-f filename]
```

-s *date*

指定列表的开始日期。 列出在定义的日期和之后写入的记录。

限制：日期格式应为 dd-mm-yyyy。

-e *date*

指定列表的结束日期。 列出直至定义的日期之前（包括定义的日期）写入的记录。
限制：日期格式应为 dd-mm-yyyy。

-d

指定*不*输出故障的详细信息。

-h

显示该实用程序的帮助。

-f *filename*

指定要读取的错误日志文件。

默认情况下，seerrlog 将读取 *ACInstallDir*/log/seos.error 文件。 您无法在数据库中定义此文件，只有 CA Access Control 才可以向该文件进行写入。

示例

- 要列出自 2006 年 1 月 3 日以来写入的所有错误记录，请指定：

  ```
  seerrlog -s 03-Jan-2006
  ```

- 要列出在 2006 年 1 月 3 日和 2007 年 1 月 1 日之间写入的所有错误记录，请指定：

  ```
  seerrlog -s 03-Jan-2006 -e 01-Jan-2007
  ```

segrace 实用程序－显示用户登录信息

segrace 命令行实用程序可显示用户的剩余宽限登录次数、用户的当前密码到期前剩余的天数，或者用户上次登录的日期和时间以及使用的终端。

注意：有关用户的宽限登录属性的详细信息，请参阅适用于您操作系统的*《端点管理指南》*。

系统管理员必须通过输入 selang 命令来激活 CA Access Control 密码检查，之后 segrace 才能正常工作：

```
setoptions class+(PASSWORD)
```

以后每次更改用户密码时，将根据数据库中设置的密码质量规则对新密码进行检查。

segrace 实用程序－在 UNIX 上显示用户登录设置

在 UNIX 上有效

segrace 实用程序可显示用户的登录设置。 建议每次用户登录时运行 segrace 命令。 要执行此操作，请将命令添加到 /etc/profile 和 /etc/csh.login（或者 Solaris 上的 /etc/.login）中。

要允许 segrace 为宽限登录计数，必须使用 sepass 实用程序更改密码。 如果用户没有剩余的宽限登录机会，segrace 会调用 sepass 实用程序，该实用程序会要求用户替换其密码。 您的站点可以在 seos.ini 文件 segrace 部分的 sepass_command 标记中指定其他实用程序来替代 sepass 实用程序，从而确定要执行的命令。

此命令格式如下：

```
segrace [-h] [-d days] [-l] [-p] [userName]
```

-d *days*

显示用户当前密码到期前剩余的天数。 只有在 *days* 参数中指定的天数大于或等于 CA Access Control 选项中的时间间隔值时，该数字才会显示。 如果忽略 *days* 参数，则 segrace 会使用七天的默认值。 此选项只适用于使用 sepass 更改了用户密码的情况。

-h

显示该实用程序的帮助。

-l

显示用户上次登录的日期和时间以及使用的终端。

-p

在用户密码到期后提示输入新密码。

userName

如果指定用户名，且请求者具有 ADMIN 属性，segrace 将为指定用户显示所需的登录信息。

如果不指定用户名，segrace 会显示当前用户的登录详细信息。

更多信息：

sepass 实用程序－设置或替换密码 (p. 180)

segrace 实用程序－在 Windows 上显示 用户登录设置

在 Windows 上有效

segrace 实用程序可显示用户的登录设置。 此实用程序可以作为独立模块，从远程计算机执行。

注意：如果在不使用任何参数的情况下调用 segrace，而找不到用户的宽限登录，则 segrace 不会显示任何内容。

此命令格式如下：

```
segrace [-h] [-d days] [-l] [-p] [-s host] [userName]
```

-d *days*

将 warning *days* 参数设置为与服务器中配置的默认参数不同的设置。

-h

显示该实用程序的帮助。

-l

显示用户上次登录的日期和时间以及使用的终端。

-p

如果密码将要在 *warning days* 时间内到期和（或）如果用户具有宽限计数，则会出现密码警告提示。

-s *host*

指定将使用 CA Access Control 数据库的远程服务器名称。

userName

如果您指定用户名且具有 ADMIN 属性，则 segrace 将为指定用户显示所需的数据。

如果不指定用户名，segrace 会显示当前用户的登录详细信息。

segracex 实用程序－在 UNIX 上检查密码到期

在 UNIX 上有效

segracex 实用程序可在 X-Windows 环境中设置新密码。 segracex 工具将检查用户的密码是否已到期。 如果已经到期，则 segracex 会显示一个窗口，用户可以在这个窗口中更换密码。

segracex 实用程序用于链接到用户初始化脚本，用户登录到桌面环境之后要调用这些脚本。

该实用程序将检查用户的 CA Access Control 宽限登录属性。 如果用户的剩余宽限登录次数为：

- 零，则 segracex 会强制用户更改密码。
- 正数但小于在用户宽限参数或全局宽限设置（如果有）中指定的值，则 segracex 会建议用户更改密码。
- 等于或大于在用户宽限参数或全局宽限设置（如果有）中指定的值，则 segracex 不会执行任何操作。

更改密码时，segracex 会提示用户输入旧密码。 然后再提示用户输入新密码。

- 如果已启用 CA Access Control 密码检查，segracex 将检查新密码是否符合在数据库中设置的密码规则。 如果新密码通过质量检查，将再次提示用户输入该新密码。
- 如果已禁用密码检查，则会立即再次提示用户输入新密码。-

  第二次输入新密码时，会将新密码的两个副本进行比较。 如果这两个副本不相同，则会再次提示用户输入新密码。

如果两个新密码相同，将以下列方式更新密码：

- 更新本地主机密码文件（/etc/passwd 和任何安全文件）及本地数据库。
- 如果在 seos.ini 文件 [seos] 部分的 passwd_pmd 或 parent_pmd 标记中定义了值，则会更新相应的 PMDB，之后 PMDB 会将更新传播给它在 UNIX 环境和数据库中的订户。 如果 seos.ini 文件 [passwd] 部分中的标记 nis_env 具有值（nis 或 nisplus），则会更新 NIS 或 NIS+ 服务器。 在主 NIS 服务器上设置密码时，会自动重建 NIS 密码映射。

可自定义的资源（如颜色和字体）在 segracex 文件中。 在 CA Access Control 的标准安装过程中，会将该文件放置在以下目录中：

- 对于除 Sun Solaris 以外的所有平台：

  ```
  /usr/lib/X11/app-defaults
  ```

- 对于 Sun Solaris 平台：

  ```
  /usr/lib/openwin/app-defaults
  ```

CA Access Control 商标的图标在 BigTradeMark_BW.xpm 文件中，您必须在安装之后将该文件放置在 *ACInstallDir*/data/segracex 目录中。

此命令格式如下：

```
segracex [-user userName]
```

userName

如果指定用户名，且请求者具有 ADMIN 属性，则 segracex 会针对指定用户进行操作。

如果不指定用户名，*segracex* 会针对当前用户进行操作。

SegraceW 实用程序－在 Windows 上检查密码到期

在 Windows 上有效

此 Windows GUI 宽限实用程序检查用户密码是否过期和（或）用户是否具有宽限登录计数。 如果有宽限登录计数，SegraceW 会显示用户可以替换密码的窗口。

SegraceW 可以在非 CA Access Control 环境中作为独立模块执行。 这使您可以将此实用程序应用在域中的任意工作站上。

首先，SegraceW 试图连接主域控制器（在 NT 4.0 环境中），只有尝试连接失败时，它才会搜索备份域控制器。 在 Windows 2000 或更高版本的环境中，SegraceW 将试图连接它所找到的第一个域控制器。

注意：如果在 SegraceW 执行选项中显式指定了远程主机，则 SegraceW 仅连接至远程主机。

经设计，可从位于域控制器 NETLOGON 共享的登录批文件中调用 SegraceW 实用程序。

SegraceW 实用程序检查用户密码是否过期和（或）用户是否具有宽限登录计数。

如果存在用户宽限登录计数属性，那么：

- 如果用户的剩余宽限登录次数为零，SegraceW 会强制用户更改密码。
- 如果用户的剩余宽限登录次数为正数，SegraceW 会建议用户更改密码。

如果用户没有宽限登录计数，SegraceW 会检查密码过期状态。

- 如果密码将要在大于在服务器端配置的 warning days 参数的时间范围内过期，则 SegraceW 不执行任何操作。
- 如果密码即将在等于或小于在服务器端配置的 *warning days* 参数值的时间范围内到期，则 SegraceW 会建议用户更改密码。
- 如果密码已经过期，SegraceW 强制用户更改密码。

更改密码时，SegraceW 显示“更改密码”消息，要求用户提供旧密码、新密码并确认新密码。

通过确认检查后，密码就会在域控制器的 SAM 数据库中更新。

此命令格式如下：

`segracew [d] [-s remoteHost]`

d

将 *warning days* 参数设置为与服务器中配置的默认参数不同的设置。

-s *remoteHost*

连接至指定的远程主机以检索信息。

注意：在连接远程主机之前，先将加密库从远程主机复制到本地主机，并将其重命名为 defence.dll。

seini 实用程序－管理配置文件

在 UNIX 上有效

seini 实用程序可管理任何主机的 CA Access Control 数据库和初始化文件。 对于任何主机，seini 实用程序可以执行下列操作：

- 显示 CA Access Control 数据库的路径
- 显示初始化 (.ini) 文件的路径
- 显示初始化文件中的内标识的内容
- 设置初始化文件的特定部分中的特定内标识的值
- 删除初始化文件的特定部分中的特定内标识

seini 实用程序还可显示其他任何 .ini 文件中的所有标记。 初始化文件的名称必须始终以 *.ini* 后缀结尾。 只要您具有 WRITE 和 ADMIN 权限，就可以从任意远程主机处理 .ini 文件。

如果不指定任何切换条件，则 seini 会显示数据库和 seos.ini 文件的路径。

注意：seini 实用程序只能在 seosd *未*运行或数据库中的规则明确允许时才能更新 seos.ini 文件。

seini 可以通过包括 seos.ini 文件中的某些标记来执行标记和部分的智能搜索。 此功能将每个标记或部分与您指定的标记或部分进行比较，直至找到完全匹配或部分匹配（在 25% 误差范围内）的项，以此来检查拼写错误。 如果找到相关的标记或部分，seini 会执行指定的操作；否则，它会显示一条错误消息。

注意：智能搜索功能只可在调用 seini 实用程序的主机上使用。

此命令格式如下：

```
seini [-d] [host]

seini [-i] [host]

seini [-H host] \
    {[-f [host.]section.token [ini_file]] | \
    [-r [host.]section.token [ini_file]] | \
    [-s [host.]section.token value [ini_file]] | \
    [-sn [host.]section.token value [ini_file]]}
```

-d [*host*]

显示远程主机上数据库的路径。 如果不指定主机，则 seini 将显示本地主机的路径。

-f [*host.*]*section.token* [*ini_file*]

显示指定主机上指定初始化文件的部分中标记的值。 如果 seini 找不到指定的部分或标记，则会显示一个空行。您必须用句点 (.) 将主机、部分和标记名称分隔开。 如果不指定 *ini_file*，CA Access Control 会在 seos.ini 文件中搜索该部分和标记。 要显示有关本地计算机的信息，请忽略 *host* 参数。

-g *section*

显示已定义部分中标记的列表。

-h

显示该实用程序的帮助。

-H [*host*]

指定要与 -f、-r、-s 和 -sn 标志配合使用的远程主机。

-i [*host*]

显示初始化文件 seos.ini 的路径名。如果不指定主机，则 seini 将显示本地主机的路径名。

-r [*host.*]*section.token* [*ini_file*]

从指定主机上 初始化文件的部分中删除标记。 如果未指定 *ini_file*，则 CA Access Control 将删除 seos.ini 文件中的标记。

要删除有关本地计算机的信息，请仅指定部分和标记的名称。

-s [*host.*]*section.token value* [*ini_file*]

设置指定主机上初始化文件的某部分中标记的值。 如果未指定 *ini_file* 参数，CA Access Control 将在 seos.ini 文件中设置该值。 如果该部分或标记不存在，并已指定远程主机，则 CA Access Control 会创建该部分或标记。

要在本地计算机上创建部分或标记，请使用 -sn 开关参数。

-sn [*host.*]*section.token newValue* [*ini_file*]

设置指定主机上初始化文件的某部分中标记的值。 如果未指定 *ini_file* 参数，CA Access Control 将在 seos.ini 文件中设置该值。 如果该部分或标记不存在，并已指定本地主机，则 CA Access Control 会创建该部分或标记。

要在远程计算机上创建部分或标记，请使用 -s 开关参数。

示例：使用 seini

- 要查找 seos.ini 初始化文件在本地计算机上的位置，请使用以下命令：

  ```
  seini -i
  ```

- 要在 [seosd] 部分中查找 *trace* 配置设置的值，请使用以下命令：

  ```
  seini -f seosd.trace_file
  ```

- 要在 [seosd] 部分中设置 *trace_to* 配置设置的值，请使用以下命令：

  ```
  seini -s seosd.trace_to file
  ```

  命令输出应如下所示：

  ```
  seosd.trace_to 内标识现设置为 file (先前是 file,stop)
  ```

selang 实用程序—运行 CA Access Control 命令行

selang 实用程序可以调用命令 shell，可提供对 CA Access Control 数据库和本地环境的访问权限。 通过在命令 shell 内执行 selang 命令，可以对数据库进行动态更新。

注意：命令的执行结果将发送到标准输出，除非包括 -o 选项。

在 UNIX 上，此命令格式如下：

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] \
[-u user pass]
selang [-l] [-o file] [-r file] [-s] [-u user pass]
```

在 Windows 上，此命令格式如下：

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] [-v]
selang [-l] [-o file] [-r file] [-s] [-v]
```

-c *command*

指定要执行的 selang 命令。 在 selang 执行完命令后将退出。

如果 *command* 包含空格，请用引号将整个字符串引起来。 例如：

```
selang -c "showusr rosa"
```

--d *path*

指定 selang 命令对定义路径中的数据库进行更新。

注意：您仅可以指定本地数据库。

--f *file*

指定从定义的文件而不是从终端的标准输入读取 selang 命令。

当 selang 执行输入文件中的命令时，所执行命令的行编号会显示在屏幕上。selang 提示不显示在屏幕上。在 selang 执行完 *file* 中的命令后将退出。

-h

显示该实用程序的帮助。

-l

指定 selang 更新默认的本地数据库，通常为 *ACInstallDir*/seosdb（其中 *ACInstallDir* 是安装 CA Access Control 的目录）。

您无需使用 -d 或 -p 指定此选项。

注意：此选项将替换 selang。 它仅在未运行 seosd 时有效，只有具有足够的更新数据库文件的本机权限的 CA Access Control 管理员才能执行此程序。

-o *file*

指定将 selang 输出写入指定的文件。 每次调用 selang 时，它都会创建一个新的空文件。如果指定当前文件的名称，selang 会覆盖该文件中的当前信息。

-p *pmdb*

指定 selang 命令更新已定义的 PMDB 的数据库，该数据库必须在本地工作站（这是 PMDB 子目录中的数据库）中。 对数据库所做的更改不会传播给订户。

注意：如果 sepmdd 或 seosd 在指定的 PMDB 上运行，则此选项无效，这与使用 *hosts* *命令*不同。

重要说明！ 请勿在此模式中进行需要传播的更改。 如果在进行更新时使用本地模式，则 CA Access Control 将仅更新本地主机文件（如 CA Access Control 配置选项中所定义的）。

-r *file*

指定 selang 从定义的文件中读取命令。 该文件应该由使用普通 selang 语法的命令组成，并且这些命令由分号或换行符分隔开。执行完 *file* 中的命令后，selang 会提示用户进行输入。

如果您没有为此选项定义文件，则 selang 将使用主目录中的 .selangrc 文件。

-s

指定在静默模式中打开 selang，而不显示版权消息。

-u *user pass*

（仅限于 UNIX）为正在运行的 selang 指定用户名和密码。

要使用此选项，必须将 seos.ini 文件中的 check_password 标记设置为 yes，这样当您运行 selang -u 时，CA Access Control 便会提示您“输入密码”。 您可以进行三次登录尝试。

seos.ini 文件 [lang] 部分中的标记 no_check_password_users 包含了登录 selang 期间绕过密码检查的用户的列表。

注意：如果 check_password 标记设置为 no（默认设置），则 selang 不要求任何密码。

-v

（仅限于 Windows）将命令行写入输出。

使用注意事项：

- 如果使用 -h，则所有其他选项都将被忽略。
- 您不能将 -c 选项与 -f 选项配合使用。
- 您不能将 -d 选项与 -p 选项配合使用。
- 如果指定 -d 或 -p，则无需指定 -l。

seldapcred 实用程序－加密和存储凭据

在 UNIX 上有效

seldapcred 实用程序可对您提供的凭据进行加密并存储。 启用 LDAP 的 CA Access Control 实用程序（例如：sebuildla）将使用此凭据从 LDAP 目录信息树 (DIT) 检索数据。 与 seos.ini 文件的 [seos] 部分中 ldap_userdn 标记的值配合使用，可使实用程序对 LDAP 服务进行身份验证。 对于简单的身份验证，凭据是与 ldap_userdn 值对应的密码。 对于 SASL 身份验证，凭据具有不同的语义。

seldapcred 实用程序会将加密凭据写入 *ACInstallDir*/etc/ldapcred.dat

此命令格式如下：

```
seldapcred [-h] [-w [credential]]
```

-h

显示该实用程序的帮助。

-w [*credential*]

指定希望 seldapcred 进行加密和存储的凭据。如果未向 seldapcred 实用程序提供输入，将提示您输入该值。 通过以这种方式使用交互模式，可以防止凭据被泄露给其他用户。

更多信息：

sebuildla 实用程序－创建后备数据库 (p. 105)

seload 实用程序—加载和启动 CA Access Control

在 UNIX 上有效

seload 实用程序可将 CA Access Control 扩展加载至 UNIX 内核并启动 CA Access Control 后台进程。 seload 实用程序可在本地和远程加载 CA Access Control 后台进程。 它还可确定是否在指定主机上加载了 UNIX 内核的 CA Access Control 扩展。 如果未运行 seosd，则 seload 会在指定主机上启动后台进程。 如果忽略 -r 开关参数和参数，seosd 后台进程将在本地主机上运行。

您可以指示 seload 在远程主机上加载以下后台进程之一：seosd、selogrd、selogrcd 或 serevu。 此进程取决于标记。

如果 CA Access Control 置于服务器工作站的引导序列中，请使用 seload。

注意：

- 安装 CA Access Control 时，CA Access Control 支持的每个操作系统的示例初始化文件放置在 *ACInstallDir*/samples/system.init 目录中。 如果系统初始化过程中需启动 CA Access Control，请使用这些文件。
- seload 实用程序要求可执行程序 se_loadtest 位于 *ACInstallDir*/lbin（其中 *ACInstallDir* 是安装目录）中。 此程序可确定是否加载了 UNIX 内核的 CA Access Control 扩展。
- 以远程方式工作时，seload 实用程序要求符合以下条件：
  - 可执行程序 rseloadd 位于 CA Access Control dir/lbin 中。 此程序将在远程主机上运行并激活 seload。
  - 文件 /etc/services 包含 seosload 服务。 应在安装 CA Access Control 期间添加此文件。
  - 文件 /etc/inetd.conf 包含 rseloadd 程序。 可在安装 CA Access Control 期间添加此程序。

此命令格式如下：

```
seload [-c] [-nopmd]  [-r host [daemon]]
```

-c

更改使用 sechkey -r 命令设置的加密密钥。

-nopmd

如果指定 -c 开关参数和 -nopmd 开关参数，seload 将不使用新密钥更新策略模型更新文件。

-r *host* [*daemon*]

加载 seosd 后台进程以及在 seos.ini 文件 [daemons] 部分中指定的任何其他后台进程。

如果指定 *daemon*，则 seload 只启动该后台进程；将忽略 seos.ini 标记。 您必须提供后台进程的完整路径。

[daemons] 部分中的 seos.ini 标记仅在指定值的情况下使用。 它没有默认值。 如果指定值，seload 会用指定实用程序或程序的标准值代替该标记的值。 例如：如果您指定值 selogrd=yes，seload 会在启动 seosd 后台进程后自动启动 selogrd 后台进程。

selock 实用程序—锁定 X 终端屏幕

在 UNIX 上有效

无论您何时离开办公区域，离开多长时间，selock 实用程序都会保护 X 终端或工作站。 selock 支持以下三种操作模式：

- 监控模式
- 保护程序模式
- 锁定模式

selock 的默认设置合并了保护程序模式和锁定模式。

注意：有关使用 selock 锁定 idle 工作站的详细信息，请参阅 *《适用于 UNIX 的端点管理指南》*。

此命令格式如下：

```
selock [-delay period] [-display hostname:display#.screen#] [-fodelay factor] \
    [-folevels levels] [-idelay seconds] [-lock-timeout minutes] \
    [-pixmapFile fileName] [-pw-timeout seconds]
```

-delay *period*

指定系统图标在屏幕上的一个位置显示多长时间后会隐去并移至屏幕其他位置。 这是标准屏幕保护程序活动，可防止烧屏。- 以微秒为单位输入时间。

如果您未定义该时间，实用程序将使用默认值 5000000（五百万）。

-display *hostname:display#.screen#*

指定要锁定哪个显示器。 可以在系统的 X 会话列表中找到显示器和屏幕编号。- 您必须从当前正在运行此处定义的备用显示器的用户处得到授权。

如果未定义此选项，实用程序将锁定您自己的显示器。

-fodelay *factor*

修改每个淡出级别在屏幕上显示的时间长度。 这样，用户便可延长在每一步中花费的时间，而无需增加级别数。 默认值为 10。

-folevels *levels*

指定系统图标淡出的步数。 增加淡出级别数会使淡出更加平滑，但是图标淡出的时间会更长。默认情况下，实用程序将使用 20 步淡出。

-help

显示说明各个 selock 选项的帮助屏幕。

-idelay *seconds*

指定自您登录后，开始监视之前过去的时间（秒）。 如果 selock 是 .login shell 的一部分，则在第一次登录后组织系统时需要这种延迟。 默认值是 30 秒。

-lock-timeout *minutes*

如果 transparent=off，则以分钟为单位指定 selock 在更改为锁定模式前处于保护程序模式的时间。

如果 transparent=on，则以分钟为单位指定 selock 在更改为锁定模式前处于监视器模式的时间。

默认值为 0，会立即调用锁定模式，并有效回避保护程序模式。

-pixmapFile *fileName*

指定屏幕锁定且 transparent=on 时 selock 在背景中显示的 XPM 文件。

-pw-timeout *seconds*

指定密码对话框在屏幕上保留的时间长度。默认值是 30 秒。请注意，数字过大可能会导致 X 服务器发生问题。- 如果未在指定时间内输入正确的密码，密码输入对话框将会关闭，而 selock 仍保持锁定模式。-

-segrace {on|off}

指定 selock 在识别用户和密码后调用 segracex。但是，如果用户 ID 和密码属于名称显示在 unlocking_user 标记（位于 seos.ini 的 [selock] 部分中）中的用户，则 selock 不会调用 segrace。 默认值为 off。

注意：segracex 实用程序将检查用户的密码是否到期；如果已经到期，则会显示一个对话框，用户可以在该对话框中选择新密码。 有关详细信息，请参阅“segrace 实用程序－在 UNIX 上显示用户登录设置”。

-timeout *minutes*

指定用户处于不活动状态的时间，此时间之后 selock 将从显示器模式切换到保护模式。 默认值为 10 分钟。

-transparent {on|off}

指定 selock 在处于锁定模式时是否使屏幕内容保持可见。 如果指定 *on*，则会继续显示并更新正在进行的进程。- selock 会显示通过 -pixmapFile 选项指定的文件的内容，来更改背景，以表明屏幕已锁定。
默认值为 *off*。

-user *user-name*

指定在锁定模式下检测到用户活动时，提示在密码对话框中输入其密码的用户。 默认值为当前用户名。 不管用户选项指定了哪个用户，都接受 root 密码。

-workhours (*hh*:*mm*-*hh*:*mm*)

指定用户可以解除锁定屏幕的时间段。 在指定时间段之前或之后，如果使用键盘或鼠标，则不会显示密码对话框。

默认值是 00:00-24:00；即，用户始终可以解锁屏幕。

-xmin *pixels*

指定系统图标每次移动所跳动的最小水平距离（像素）。 默认值为 100。

-xmax *pixels*

指定系统图标每次移动所跳动的最大水平距离（像素）。 默认值为 300。

-ymin pixels

指定系统图标每次移动所跳动的最小垂直距离（像素）。默认值为 80。

-ymax pixels

指定系统图标每次移动所跳动的最大垂直距离（像素）。 默认值为 250。

更多信息：

segrace 实用程序－在 UNIX 上显示用户登录设置 (p. 157)

selockcom 实用程序－控制 selock 实用程序

在 UNIX 上有效

selockcom 实用程序可控制当前处于活动状态的 selock 进程。 这包括重新启动和停止 selock，以及在锁定模式、保护程序模式和显示器模式之间切换。

注意：加载 selock 时，它会禁用终端的内置屏幕保护程序，以防止 selock 和内置的屏幕保护程序之间发生竞争或重叠的情况。-- 如果使用 selockcom exit 开关参数停止 selock，则终端上不会激活任何屏幕保护程序。 可以使用标准 X 命令 xset s on 重新启动 selock 或终端的内置屏幕保护程序。- 有关 xset 命令的详细信息，请参阅您的 UNIX 文档。

此命令格式如下：

```
selockcom {-activate|-deactivate|-exit|-restart|-lock} \
    [-display hostname:display#.screen#]
```

-activate

将 selock 从显示器模式切换到保护程序模式，无需等待预定义的超时时间度过。键盘处于锁定状态，CA Access Control 徽标显示在屏幕上。

-deactivate

将 selock 切换回显示器模式。 此开关参数可模拟用户在 selock 进程中输入。 如果 selock 当前处于锁定模式，则会显示密码对话框；输入您的密码可返回显示器模式。 如果 selock 处于保护程序模式，您会返回到显示器模式。

-exit

终止 selock 进程。 您还可以通过向 selock 发送 sigterm 信号来终止它。 还可以使用 sigkill 信号 (kill -9)，这是最后的手段。 如果使用最后一种方法，selock 不会正常退出，因此，通常您不应使用该方法。如果您正在运行虚拟根窗口管理器，则使用 kill -9 会强制您重新启动窗口管理器，以还原虚拟窗口。-

-restart

终止 selock 进程，之后立即使用上一次调用时所使用的同一命令行选项重新启动它。 如果自您上次调用 selock 之后数据库发生了更改，这便是让 selock 重新读取资源数据库的一个好办法。-

lock-

将 selock 切换到锁定模式（不考虑当前锁定超时值）。-

-display *hostname*:*display#*.*screen#*

指示 selockcom 控制在指定显示器上运行的 selock 进程。 通过此选项，您可以从远程终端控制 selock。

可以在系统的 X 会话列表中找到显示器和屏幕编号。- 要执行此操作，您必须从当前正在运行指定显示器的用户处得到授权。 默认的假设是您要锁定自己的显示器。

selogmix 实用程序－分割和合并审核日志文件

在 UNIX 上有效

selogmix 实用程序可分割和合并 CA Access Control 审核日志文件。

此命令格式如下：

```
selogmix {-s|-m} [-fn fileName] [-l fileName1 fileName2] \
    [-c weight1:weight2] [-t days] [-d] [-i]
```

-c *weight1*:*weight2*

指定分割文件的文件大小关联，其中 *weight1* 指明第一个文件的相对权重，而 *weight2* 指明第二个文件的相对权重。 如果忽略此选项，selogmix 将使用一对一的关联。

-d

指定在调试模式下运行 selogmix。在此模式下，selogmix 会显示所有设置。

-fn *fileName*

指定要分割的审核日志文件的名称或合并所生成文件的名称。 如果忽略此选项，selogmix 会使用由 seos.ini 文件 [logmgr] 部分中的 audit_log 标记指定的文件名。

-h

显示该实用程序的帮助。

-i

指定在交互模式下运行 selogmix。在此模式下，selogmix 覆盖现有文件前会提示您确认；否则，将不提示确认直接覆盖。

-l *fileName1 fileName2*

指定在合并或分割操作中使用的文件。

您必须为此选项同时指定这两个文件名。 要进行合并，请指定要合并的两个文件名；要进行分割，请指定两个目标文件。 如果忽略此选项，selogmix 会使用由 seos.ini 文件中的 audit_log 标记指定的文件名，并向文件名添加后缀 1 和 2。

-m

合并两个审核日志文件。

-s

分割指定的审核日志文件。

-t *days*

指定天数。 此选项只能用于分割文件。 指定分成单个文件记录结束后的天数。 如果忽略此选项，selogmix 会分隔上一个记录日。

示例

- 要将标准日志文件分割为两个同等大小的文件，请使用以下命令：

  ```
  selogmix -s
  ```

  原审核文件名为 *ACInstallDir*/log/seos.audit

  新的分割文件名为 *ACInstallDir*/log/seos.audit1 和 *ACInstallDir*/log/seos.audit2。

- 要将最后两天的记录与日志文件分开，请使用以下命令：

  ```
  selogmix -s -t 2
  ```

- 要将日志文件拆分为两个具有所定义的大小关联的文件，请使用以下命令：

  ```
  selogmix -s -c 1:2
  ```

- 要将两个指定文件合并为一个命名文件，请使用以下命令：

  ```
  selogmix -m -l seos.audit1 seos.audit2 -fn seos.audit.merge
  ```

更多信息：

seaudit 实用程序－显示审核日志记录 (p. 98)

semsgtool 实用程序—维护消息文件

通过 semsgtool 实用程序可以：

- 显示 CA Access Control 消息文件中的一条消息
- 列出消息的整个部分
- 将整个文件转储到多个 ASCII 文件，每个部分对应一个 ASCII 文件
- 构建新的消息文件
- 将消息更改为新消息
- 列出消息，包括子字符串
- 验证消息文件

每次执行 semsgtool 时，只能指定一个命令。

消息文件的默认位置为 *ACInstallDir*/data/seos.msg

注意：CA Access Control 消息文件由部分和消息编号组成。 每个部分保存不同 CA Access Control 模块或子模块的消息。-

此命令格式如下：

```
semsgtool {-build|-b} asciiSourceFile OutputMessageFile

semsgtool {-change|-c} [messageFile] {0xerror-code|section# msg#} new-message

semsgtool {-dump|-d} messageFile

semsgtool {-list|-l} [messageFile] sectionNumber

semsgtool {-number|-n} [messageFile] subString

semsgtool {-show|-s} [messageFile] [0xerror-code|section# msg#]

semsgtool {-validate|-v} [messageFile]
```

-build|-b

从 ASCII 源文件创建新的 CA Access Control 消息文件。

-number|-n

列出包含定义字符串的消息文件中的消息。

-change|-c

创建新消息文件，名为 *messageFile*.new，其中指定的消息具有定义的已修改字符串。

-dump|-d

将消息文件转储到多个文件中，每个文件针对消息文件中的每一部分。 此操作会创建 ASCII 源文件，以后可使用 ASCII 源文件创建新的 CA Access Control 消息文件。

-h

显示该实用程序的帮助。

-list|-l

列出消息文件给定部分中的所有消息。

-show|-s

显示与特定消息代码相关联的消息。

-validate|-v

（仅限于 Windows）。 通过检查重复消息和超出分配界限的消息来验证消息文件。

0x*error-code*

为要显示或更改的消息定义错误代码的十六进制数字。

asciiSourceFile

定义 semsgtool 用于构建新消息文件的 ASCII 格式源文件。

messageFile

定义消息文件的名称。 如果忽略此选项，则 semsgtool 将使用配置设置中指定的消息文件。

OutputMessageFile

定义要构建的新消息的名称。

section# msg#

为要显示或更改的消息定义错误代码的部分号和消息号。

sectionNumber

定义要列出所有消息的部分的部分号。

示例

- 要列出与错误代码 0x205 相关联的消息，请输入以下命令：

```
semsgtool -s seos.msg 0x205
```

- 要列出部分 512 中的消息，请输入以下命令：

```
semsgtool -l seos.msg 512
```

- 要创建经修改的 CA Access Control 消息文件，请按以下步骤操作：
  1. 通过经修改的消息创建新消息文件：

     ```
     semsgtool -c 0x2501 "This is the new message"
     ```

     新消息文件 seos.msg.new 是通过经修改的消息创建的。
  2. 将新文件复制到 CA Access Control 消息文件：

     ```
     copy seos.msg.new seos.msg
     ```

     复制带有旧 seos.msg 文件顶部经过修改的消息的新消息文件。
- 要显示与错误代码 0x0205 相关联的消息，请输入以下命令：

  ```
  semsgtool -s 0x205
  ```

senable 实用程序—启用已禁用的用户帐户

在 UNIX 上有效

senable 实用程序可在禁用用户的任何位置（包括 PMDB）启用出于任何原因而被禁用的该用户的登录。 例如：某用户可能被 serevu 后台进程禁用，或者某用户由于达到挂起日期或到期日期而被禁用。

启用用户帐户后，senable 会调用 sepass 实用程序，该实用程序会提示输入新用户密码。 要还原最近使用的密码，请使用 -n 选项。

senable 工具通过从本地 /etc/passwd 文件中删除未定义的用户帐号来启用该帐号。

要远程执行 senable，必须在授予本地工作站对远程工作站 WRITE 访问权限的规则中明确指出本地工作站的需求；否则，将无法在该处执行 CA Access Control 管理。

注意：有关远程管理限制的详细信息，请参阅*《适用于 UNIX 的端点管理指南》*。

此命令格式如下：

```
senable [-host hostname] userNames [-n]
```

-host *hostname*

选择要将帐户从禁用改为启用的主机。

必须在以下两类主机上具有 ADMIN 或 PWMANAGER 属性才能使用 -host 选项：

- 要将帐户从禁用改为启用的主机。
- 要在其中输入 senable 命令的主机。

-h

显示该实用程序的帮助。

-n

以非交互方式运行命令。- 如果使用此选项，senable 不会调用 sepass，将还原最近使用的密码。

userNames

为要从禁用改为启用的帐户定义以空格分隔的用户名列表。

更多信息：

serevu 实用程序－处理失败的登录尝试 (p. 206)

senone 实用程序－以未授权的用户身份执行命令

在 UNIX 上有效

senone 实用程序可将得到高级授权的用户发出的命令作为未授权的用户进程执行。

注意：只有要测试不可信程序的经过高度授权的用户可以使用该工具。

调用 senone 实用程序时，它会从授权后台进程中删除进程凭据。 之后，senone 将使用未向 CA Access Control 定义的用户的凭据执行 shell。从现在起，执行从此 shell 中调用的任何程序时，都将使用非 CA Access Control 用户的凭据。- 因为 senone 不会更改调用者的用户 ID，所以用户的 UNIX 权限保持不变。

重要说明！ 建议以 root 身份登录的用户不要运行未受托的程序。 即使通过 senone 运行未受托的程序，也可能会发生意外的问题。

如果在不指定命令的情况下调用 senone，它会按照 /etc/passwd 中的定义执行用户的 shell。

此命令格式如下：

senone [*command*]

-h

显示该实用程序的帮助。

命令

指定您希望 senone 以未授权用户的身份执行的命令。

更多信息：

sesu 实用程序－替代用户 (p. 209)
sewhoami 实用程序 — 在 UNIX 上显示您的 CA Access Control 用户名和安全凭据 (p. 217)

SEOS_load 实用程序－加载 CA Access Control 拦截模块

在 UNIX 上有效

SEOS_load 实用程序可控制动态 CA Access Control 内核模块 (SEOS_syscall)。 运行任何 CA Access Control 实用程序之前，都必须加载拦截模块。

注意：您可以使用 UNIX exits 在加载和卸载内核之前和之后自动运行程序。

在支持数据流的平台上，此实用程序可根据 seos.ini 文件 [SEOS_syscall] 部分中的 SEOS_use_streams 标记，将 CA Access Control 模块加载到数据流。 如果将该标记设置为 yes，则会将该模块推入数据流中。

此命令格式如下：

```
SEOS_load [-i|-k|-s|-u]
```

-i

（仅限于 HP-UX 和 Sun Solaris 平台）显示有关 CA Access Control 内核扩展的信息。

-k

（仅限于 HP-UX 和 Sun Solaris 平台）将 CA Access Control 模块加载到内核中，而不将其推入数据流。

-s

（仅限适用于 HP-UX 和 Sun Solaris 平台。）将 CA Access Control 内核模块插入数据流中。 此选项将忽略 seos.ini 文件 SEOS_syscall 部分中的 SEOS_use_streams 标记。

-u

将 CA Access Control 内核扩展从内核中卸载，然后从数据流中删除该模块。

注意：如果在 CA Access Control 之上加载的应用程序具有被 CA Access Control 钩住的开放系统调用 (syscall)，您就无法卸载 CA Access Control。 使用 *secons -sc* 或 *secons -scl* 查找这些进程。 然后可以关闭这些进程并卸载 CA Access Control 内核模块，或使用 UNIX exits 在卸载内核之前自动关闭这些进程，并在内核卸载后重新启动。

sepass 实用程序－设置或替换密码

在 UNIX 上有效

sepass 实用程序可在本地主机、策略模型、NIS 或 NIS+ 服务器（如果适用）中设置新密码或替换现有密码。

sepass 实用程序可更改用户密码。 此外，特权用户可以使用 sepass 更改其他用户的密码。 当您更改自己的密码时，sepass 会提示您输入旧密码。

注意：如果 seosd 未运行，则 sepass 会运行默认的密码程序。 seos.ini 文件 passwd 部分中的 DefaultPasswdCmd 标记指定了默认的密码程序。 密码以加密格式存储并通过网络传输。

此命令格式如下：

```
sepass [-d] [-l] [-p] [-s policy_model@hostname] \
    [-g number] [-x] [userName]
```

-d

显示它所拥有的有关密码更新的所有信息，如哪些工作站上已成功更新，以及如果未激活 setoptions class+(PASSWORD)，也就未检查密码质量。 此开关参数在调试时十分有用。

-g *number*

定义 *userName* 的宽限登录次数。

-h

显示该实用程序的帮助。

-l

仅替换本地工作站上的密码；即，在本地密码文件（通常为 /etc/passwd）、安全文件和本地数据库中替换。

在 NIS/NIS+ 环境中，通常不在客户端的 /etc/passwd 文件中定义用户；因此，不会更新客户端工作站上的密码。

在 NIS/NIS+ 服务器工作站中，会在本地更新密码并由 NIS/NIS+ 将密码传播。

此开关参数与 -p 和 -s 开关参数是互斥的。

-p

仅在远程工作站上和在该开关参数中的指定主机的 PMDB 上更改密码。 此开关参数与 -l 和 -s 开关参数是互斥的。

-s *policy_model@hostname*

在本地工作站上和在该开关参数中的指定主机的 PMDB 上替换密码。此开关参数与 -l 和 -p 开关参数是互斥的。

-x

像用户 *username* 更改密码一样替换密码。此开关参数会更新上一次更改数据库的时间和日期。 宽限登录将终止。

注意：要像由 root 用户更改那样更改 root 密码，需要设置相应的 RootPwAsOwn。 有关 seos.ini 标记的详细信息，请参阅*《参考指南》*。

username

（可选）指定要更改其密码 sepass 的用户名。 如果忽略此选项，将设置您自己的密码。

示例

以下示例说明了如何在各种情况下使用 sepass。

- 要在本地主机上更改自己的密码，请输入以下命令：

  ```
  sepass -l
  ```

  注意：如果未在站点上定义 PMDB，则可以忽略 -l 开关参数。 如果正在站点中使用 PMDB，则一旦忽略 -l 开关参数，将在 PMDB 的所有订户数据库上更改您的密码。 在 NIS/NIS+ 客户端中，此开关参数*不会*更改密码；在 NIS/NIS+ 服务器中，会先更改密码，然后传播密码。

- 要仅在本地主机上更改除您自己以外的任何用户的密码，请输入以下命令：

  sepass -l *username*

  username 必须存在于 /etc/passwd 文件、相应的 UNIX 安全文件以及数据库中。

  在 NIS/NIS+ 客户端中，sepass 不会更改密码。 在 NIS/NIS+ 服务器中，会先更改密码，然后传播密码。

- 要在未使用 NIS 的站点的多个工作站上更改用户密码，请按照以下步骤操作：

  1. 创建 PMDB。

     注意：有关创建 PMDB 的详细信息，请参阅*《适用于 UNIX 的端点管理指南》*。

  2. 对于必须将其详细信息分发到订户计算机的所有用户，将他们添加到 PMDB 的 UNIX 和 CA Access Control 环境中。

  3. 订阅所有工作站以接收 PMDB 的更新密码。

  4. 在每个订户上，将 seos.ini 文件 [seos] 部分中的标记设置为 PMDB 的名称。 例如：

     ```
     passwd_pmd = PMD1@morocco
     parent_pmd = PMD1@casablanca
     ```

  5. 输入以下命令：

     sepass *username*

     sepass 执行完成后，将在所有订户数据库上更改该用户密码。

sepmd 实用程序

sepmd 实用程序是策略模型管理实用程序。

通过它可以执行下列任务：

- 管理订户和更新文件
- 管理双重控制
- 管理策略模型日志文件
- 管理 PMDB
- 备份 PMDB
- 还原 PMDB

注意：您必须在策略模型所在的主机上运行 sepmd 实用程序。

更多信息：

sepmd 实用程序－管理订户和更新文件 (p. 183)
sepmd 实用程序－管理双重控制 (p. 187)
sepmd 实用程序－备份 PMDB (p. 188)
sepmd 实用程序－管理策略模型日志文件 (p. 190)
sepmd 实用程序－管理 PMDB (p. 191)
sepmd 实用程序－还原 PMDB (p. 193)

sepmd 实用程序－管理订户和更新文件

sepmd 实用程序可创建、删除和分配订户。

此命令格式如下：

```
sepmd {-C|-de|-l|-L|-p|-R} pmd

sepmd {-n|-r|-u} pmd subscriber

sepmd -s pmd subscriber offset

sepmd -sm pmd mf_subscriber mf_type mf_sysid mf_admin offset

sepmd -t pmd {auto|offset}
```

-C

显示更新文件中的所有命令及其偏移量。 偏移量表明更新在文件中的位置，订阅另一数据库或 PMDB 时，您可能需要指定该文件。

-de

（仅限于 UNIX）对加密的 updates.dat 文件中的信息进行解密。 如果将 UseEncryption PMDB 配置设置设为 yes，则会为此文件进行数据加密。

-l

列出策略模型的订户。

-L

列出策略模型及其状态，包括错误数量、可用性、偏移量、同步模式以及要传播的下一个命令。 更新文件包含必须（或已经）通过策略模型传播的所有更新。 偏移量指明必须发送给订阅者的下一个更新的位置。 也会显示初始的偏移量和最新的偏移量。

-n

创建新订户，然后以追溯方式根据策略模型对其进行更新。 有关适用于更新订阅者的一般规则的信息，请参阅 -s 选项的说明。

注意：此选项会将整个 PMDB 的内容（包括 LOGINAPPL [仅适用于 UNIX] 和 SPECIALPGM 对象）发送给新订户。 如果订户的对象与父订户的对象有所不同，您可能需要筛选这些对象。

-n 选项不会替换目标订户数据库定义上的策略模型数据库定义，而是将其添加到现有策略模型。 如果目标数据库包含其他资源或属性，则新的策略模型不会在订阅完成之后删除它们。

利用 *-n* 添加的订阅者标记为 sync，表示它现在处于同步模式并接收所有 PMDB 规则。 当订阅者接收到所有规则时，会从同步模式中释放它，它就成为一个正常的订阅者。 -n 选项可能会花费一些时间进行处理。 如果有多个更新或互相矛盾的更新，则使用最后一个更新。

重要说明！ 当你使用 *sepmd -n* 为 CA Access Control 端点或 PMDB 订阅另一 PMDB 时，新的父 PMDB 不应包含已存在于新订户中的任何策略（POLICY 对象名）。 在为订户订阅新的父 PMDB 之前，先从该订户取消部署每个现有策略，然后从该订户删除 POLICY 对象和链接的 RULESET 对象。

在 UNIX 上，如果 seos.ini 文件中的 send_unix_env 标记设置为 yes，则 -n 选项还会发送策略模型密码和组文件的内容。 建议使用 dbmgr -export -l 查看数据库，以确定被转发的命令。

-p

列出驻留的策略模型用户及其状态。

--r

由 sepmdd 维护的不可用订户列表中删除该订户，从而可以立即更新该订户。 正常情况下，如果订阅者关闭，无法从策略模型接收更新，则 sepmdd 就尝试仅在特定时间段后将更新发送给该订阅者。 但是，如果指定了此选项，则 sepmdd 会跳过等待时间段，立即尝试将更新发送给订户。

-R

用实际偏移量更新所有订购者。

-s

将为其他数据库或 PMDB 订阅策略模型。 为主机订阅策略模型时，主机必须已启动，且 CA Access Control 必须在该主机上运行。 此外，PMDB 必须是订阅主机的父 PMDB。 可通过 parent_pmd 订户的配置设置建立这种关系，该设置必须包含该主机所订阅的 PMDB 的名称。

当为一个策略模型订阅另一个策略模型时，

- 被订阅的策略模型的 pmd.ini 文件中的内标识 parent_pmd，必须包含它所订阅的策略模型（它的父策略模型）的名称。
- CA Access Control 必须在订阅策略模型驻留的主机上运行。

PMDB 只能有一个父级。 如果您决定建立具有多个父项的策略模型，请为 parent_pmd 标记指定包含父策略模型列表的文件的名称。 但是建议不要建立多个父，这非常冒险，因为数据库将会充斥着来自多个源的大量不可靠指令。

-sm

为策略模型分配大型机订户。

-t

通过从更新文件中删除条目来截短更新文件。

注意：在 UNIX 上，如果 force_auto_truncate PMDB 配置设置被设置为 no，则 sepmd -t 不会截断更新文件。 如果将该标记设置为 yes，即使该策略模型没有任何订户，该命令也将截短更新文件。

- 如果使用 *offset*（手工剪切），可以通过运行带 -L 选项的 sepmd 找到偏移量。

  注意：必须使用 -L 参数所提供的确切偏移量来截断文件，而不是使用通过对起始偏移量进行减法运算而得出的偏移量。

- 如果要使用 auto，sepmd 会计算第一个未传播条目的偏移量并删除该条目前面的所有条目。 使用 auto 可省去运行带 -L 参数的此实用程序的步骤。

如果订户未在指定偏移量前接收到所有更新，则 sepmd 会显示一条错误消息，不会截短文件。 如果无论如何都要截短文件，请执行以下操作：

- 取消订阅未更新的主机
- 截短文件
- 重新为主机订阅策略模型

如果这样做，订户将无法从策略模型接收一个或多个更新。 订户的偏移量会更改为更新文件的最后一个偏移量。

-u

从策略模型订阅列表中删除订户。

auto

指示 sepmd 计算第一个未传播条目的偏移量，并删除该条目**前面的所有条目。**

offset

与 -s 或 -sm 选项配合使用，在更新文件内指定最新添加的订户开始接收更新的点。

与 -t 选项配合使用，指定从更新文件的开头到特定订户位置的距离。

使用 -C 选项可查看有效的更新偏移量。 如果指定偏移量位于更新的中间，则会将偏移量向前移至下一个更新的开头。 如果指定偏移量无效（小于第一个偏移量或者大于最后一个偏移量），则会显示一条错误消息。

pmd

指定策略模型的名称。

订户

指定订户工作站或订户 PMDB 的主机。

sepmd 实用程序—管理双重控制

在 UNIX 上有效

sepmd 实用程序可管理双重控制事务。 sepmd 实用程序在创建每个事务时为其指定唯一的 ID 号。

注意：有关双重控制的详细信息，请参阅*《适用于 UNIX 的端点管理指南》*。

使用双重控制时，PMDB 的名称必须是 *maker*，且 PMDB 和 CA Access Control 的 is_maker_checker 配置设置的值必须为 yes。

此命令格式如下：

```
sepmd -m {l|la|lo}

sepmd -m {d|r} transactionId

sepmd -m p transactionId code
```

-m d

删除事务。 事务是必须得到批准后才能在 PMDB 上实施的一个或多个命令。 只有创建事务的用户可以删除该事务。

-m l

列出调用命令的用户的未处理事务（等待检查者）。 列出每个事务时还会列出它的 ID 号、它的制定者（创建事务的用户，在本例中，即为调用命令的用户）的名称及其说明（如果有）。

-m la

列出所有制定者的全部未处理事务。 列出每个事务时还会列出它的 ID 号、它的制定者的名称及其说明（如果有）。

-m lo

列出*除*调用该命令的用户的事务以外，所有制定者的未处理事务（等待检查者）。

-m p

处理事务。 当检查者（*除*创建事务的制定者以外的任何管理员用户）输入 ID 号时，指定事务中的所有命令都会显示在列表中。

此选项在以下情况下不适用：

- 如果事务中的一个或多个命令与调用该命令的用户相关。
- 如果事务由其他检查者锁定。
- 如果事务由调用该命令的用户创建，即制定者无法作为自己事务的检查者。
- 如果指定的事务 ID 不存在。
- 如果调用该命令的用户不具有成为检查者的权限。

-m r

检索或锁定事务。

- 如果您是创建事务的用户（制定者），此参数可检索特定的未经处理的事务。 检索完该事务以后，可以将它定向到相应的文件并使用所选择的 ASCII 编辑器（vi、emacs 等）更新该事务。
- 如果您*不是*制定者（检查者）用户，此参数可在处理前锁定该事务。 您无法更改锁定的事务。

transacationID

指定 sepmdd 在创建事务时为事务分配的唯一标识号。

code

指定用于在处理事务时指明检查者 应执行哪些操作的数字代码：

0

拒绝事务，在这种情况下，会删除事务中的所有命令，且不会在 PMDB 中实施任何更改

1

授权事务，在这种情况下，会立即在 PMDB 中实施命令

2

解除事务的锁定，以便之后进行处理或由其他检查者处理。

sepmd 实用程序—备份 PMDB

通过 sepmd 实用程序可以备份策略模型数据库。

此命令格式如下：

```
sepmd {-bl|-ul} pmd

sepmd -bd pmd destination

sepmd -bh pmd destination backup_host
```

-bd

将 *pmd* 备份到*目标*目录。

-bh

将 *pmd* 备份到层级结构中策略模型的*目标*目录中。 也就是说，备份将修改 PMDB 订户，以便将备份移至 *backup_host* 主机后，订阅仍可正常使用。

-bl

锁定 *pmd* 以便其不能将命令传播给订户。

如果策略模型具有订户，而您要确在保备份过程中不接受更新，请使用此命令。

-ul

为锁定的 *pmd* 解除锁定。

backup_host

定义要将备份主机移至其中的主机名称。

目标

定义要将 PMDB 文件备份至其中的目录名称。

pmd

定义策略模型数据库，该数据库位于由 _pmd_directory_ 配置设置指定的位置。

示例：备份 PMDB

以下命令可将名为 myPMDB 的 PMDB 备份至 /tmp/my_pmdb 目录：

```
sepmd -bd pmdb /tmp/my_pmdb
```

您现在可以根据需要管理 PMDB：

```
selang -d /tmp/my_pmdb
```

示例：备份具有订户的 PMDB

以下命令将展示如何备份具有订户的 PMDB，然后将 PMDB 移至另一主机：

1. 锁定 PMDB：

   ```
   sepmd -bl mainPMDB
   ```

   CA Access Control 将锁定 PMDB，这样就无法发送或接收更新。

2. 备份 PMDB：

   ```
   sepmd -bh mainPMDB /tmp/my_pmdb host63
   ```

   CA Access Control 会将 PMDB 备份至 /tmp/my_pmdb

   在 UNIX 上，CA Access Control 将使用您指定的备份主机名更新 subscribers.dat。

   在 Windows 上，CA Access Control 将创建 *pmd*.reg 文件，该文件是 *pmd* 注册表设置的转储文件，为了与您指定的新主机相匹配，其中的 Parent_Pmd 配置设置值已进行了更改。

3. 解除锁定 PMDB：

   ```
   sepmd -ul mainPMDB
   ```

   CA Access Control 将为 PMDB 解除锁定。

4. 将 PMDB 备份传输至其新主机。

   注意：新主机必须使用与当前计算机相同的操作系统和 CA Access Control 版本。

5. （仅限于 Windows）。 将 mainPMDB.reg 文件导入新主机上的注册表。

   现在您可以继续照常使用 PMDB 了。

sepmd 实用程序—管理策略模型日志文件

sepmd 实用程序可管理策略模型日志文件。 策略模型日志文件提供了策略模型数据库活动的详细审核跟踪。 例如：

```
Wed Nov  4 10:08:02 2003 pmdb1:Processing list request for missouri.yourco.com
Wed Nov  4 10:08:02 2003 pmdb1:Processing list request for oregon.yourco.com
Wed Nov  4 10:09:14 2003 pmdb1:Empty request
Wed Nov  4 10:09:15 2003 pmdb1:Processing shutdown request
Wed Nov  4 10:09:15 2003 pmdb1:Delete filters
Wed Nov  4 10:10:04 2003 pmdb1:Opened error logs
Wed Nov  4 10:10:04 2003 pmdb1:Try to load filters
Wed Nov  4 10:10:04 2003 pmdb1:Filters file : nis_filter.dat
```

首次运行 sepmdd 时，会自动创建策略模型日志文件。

在 UNIX 上，您可以使用 pmd_log_level PMDB 配置设置控制 PMDB 记录哪些内容：

- **0**－不记录任何条目。
- **1**－仅列出错误消息。
- **2**－列出错误消息和通知消息（默认值）。

注意：如果超过了文件大小限制，日志文件中会出现一条警告消息通知您。 如果日志文件大小超出限制，可使用配置设置来增加大小。

此命令格式如下：

```
sepmd {-sl|-kl|-dl|-cl} pmd
```

-cl

清除策略模型日志文件的内容。

-dl

显示策略模型日志文件。

-kl

使策略模型日志文件不可用。

-sl

使策略模型日志文件可用。

pmd

指定策略模型的名称。

sepmd 实用程序－管理 PMDB

sepmd 实用程序可停止和启动策略模型，在 UNIX 上，它还可重新加载影响策略模型的配置设置。

注意：与 UNIX 不同，在 Windows 上 sepmd 并不停止或启动策略模型服务。 而可以激活和取消激活策略模型。

您必须在策略模型中拥有 ADMIN 权限，才能使用 sepmd 启动或查询策略模型。

此命令格式如下：

```
sepmd {-c|-e|-k|-S} pmd
```

```
sepmd -tm seconds
```

-c

清除策略模型错误日志。

-e

显示策略模型错误日志。

-k

在 UNIX 上，可安全地关闭策略模型后台进程。在 Windows 上，它可取消激活策略模型服务。

注意：请勿在 UNIX 上使用 kill 命令关闭策略模型后台进程。

-ri

在 UNIX 上，sepmdd 运行时该命令将重新加载策略模型和 CA Access Control 配置文件（分别为 pmd.ini 和 seos.ini）。 您只能以一分钟或更长的时间间隔来使用此选项。 此选项将检查以下标记中的配置更改：parent_pmd、_retry_timeout_、_min_retries_ 和 _shutoff_time_。

在 Windows 上，它会将策略模型信息从注册表重新加载至主机。 如果您更改了数据且希望确保将更改发送到主机 PMDB，请使用此命令。

-S

在 UNIX 上，可启动策略模型后台进程。在 Windows 上，它可激活策略模型服务。

如果没有任何其他命令要执行，可使用此选项启动后台进程。

-tm *seconds*

（仅限于 Windows）为已执行的请求设置初始超时间隔（秒）。

pmd

指定策略模型的名称。

sepmd 实用程序—还原 PMDB

sepmd 可在本地主机上还原 PMDB。 您用来还原 PMDB 的备份文件必须来自与还原主机运行相同的平台、操作系统和 CA Access Control 版本的主机。 CA Access Control 必须正在还原主机上运行。

注意：如果您在不同的终端上备份和还原 PMDB，PMDB 将不会在还原的 PMDB 数据库中自动更新终端资源。 您必须将新的终端资源添加到还原的 PMDB 中。 要添加新的终端资源，请停止还原的 PMDB，运行 *selang -p pmdb* 命令，然后再启动还原的 PMDB。

此命令格式如下：

```
sepmd -restore pmd [-source path] [-admins user[,user...]]\
[-xadmins user[,user...]] [-parent_pmd name[,name...]]
```

-restore

在本地主机上还原 PMDB。

-admins *user*[,*user*...]

(UNIX) 将内部用户定义为还原的 PMDB 的管理员。

-parent_pmd *name*[,*name*...]

（可选）定义还原的 PMDB 的父 PMDB 的名称。 按照 *pmdb@host* 格式指定父 PMDB 名称。

pmd

定义要还原的 PMDB 的名称。

-source(*path*)

（可选）定义备份文件所在的目录。 如果未指定源目录，将从默认位置中的文件还原 PMDB。默认位置在 *_pmd_backup_directory_* 标记中定义。

默认值：(UNIX) *ACInstallDir*/data/policies_backup/pmdName

默认值：(Windows) *ACInstallDir*\data\policies_backup\pmdName

-xadmins *user*[,*user*...]

(UNIX) 将企业用户定义为还原的 PMDB 的管理员。

sepmdadm 实用程序－创建 PMDB 定义

在 UNIX 上有效

sepmdadm 实用程序可创建运行 PMDB 所需的定义。 sepmdadm 实用程序是一个脚本，包括定义 PMBD、定义该 PMDB 与它上方和下方的 PMDB 的关系，以及定义其订户工作站所需的 CA Access Control 和 UNIX 命令。 默认情况下，会将 root 用户定义为 PMDB 的管理员和审核员。 虽然也可以通过远程 shell 运行 sepmdadm 实用程序，但您必须在本地运行它。 使用 sepmdadm 创建新的 PMDB 后，接下来可能需要将订户指向该 PMDB 以及将 UID 和 GID 同步。

可以在交互模式或非交互模式下运行此实用程序：-

- 在非交互模式下，在命令行中输入参数。- 该实用程序根据它收到的值构建 PMDB 及其层级结构。
- 在交互模式下，无需在命令行中输入参数。 sepmdadm 实用程序会询问用户是否希望使用交互模式。 如果用户回答“y”，则该实用程序会继续要求用户提供选项值。

使用 sepmdadm 创建新的 PMDB 时，需识别作为策略模型订户的工作站。 但是，还必须使用工作站订阅的 PMDB 的名称更新每个订户的 seos.ini 文件中的 parent_pmd 标记。 如果不执行此操作，则订户将不接受来自 PMDB 的更新。

通过为多个工作站订阅同一 PMDB，以及通过为一个 PMDB 工作站订阅另一个 PMDB 工作站，可以创建 PMDB 的层次结构。

此命令格式如下：

`sepmdadm` *`options`*

--admin *name*

定义 PMDB 的 CA Access Control 管理员。

--auditor *name*

定义 PMDB 的 CA Access Control 审核员。

-c | --clean *pmdbName*

删除指定的策略模型。 此选项可关闭策略模型后台进程、移除数据库中的文件保护，以及删除策略模型目录及其所有内容。

不能将此选项与 --noconfirm 选项一起使用。

--desktop *hostname*

指定管理员可用于管理位于本地主机上的 PMDB 的工作站。 如果不指定任何工作站，则管理员只能通过本地主机管理 PMDB。

--group_fname *fileName*

定义组文件在 NIS 下的位置。

-h | --help

显示帮助屏幕。

-i | --interactive

以交互模式运行 sepmdadm。

-l

指定在本地模式下运行 sepmdadm，这意味着您可以在 CA Access Control 未运行时创建 PMDB。

注意：除非您指定此选项，否则必须让 CA Access Control 运行才能使用 sepmdadm。

--nis | --NIS

在策略模型上执行 NIS 安装。 如果 NIS 服务器上安装了 PMDB，则必须使用此选项。

--noconfirm

指定不要求用户确认回答。 此选项可用于在非交互模式下从 shell 脚本调用 sepmdadm。-

--parentpmd *pmdbName*

指定该 PMDB 订阅的父 PMDB 的名称。 如果将此参数与 -subsconfig 参数一起使用，sepmdadm 会更新 seos.ini 文件中的 parent_pmd 标记。 如果使用此参数但不使用 --subsconfig 参数，sepmdadm 会更新 pmd.ini 文件中的 parent_pmd 标记。

注意：如果您要定义多个父策略模型，则必须使用引号。 例如：要创建一个“策略模型”并定义其父项，请使用以下命令：

```
sepmdadm --pmdname subs2 --admin abc123 --admin root --auditors abc123
--desktop pcp36949 \
--parentpmd "aa@pcp36949,bb@pcp36949"
```

--passwd_fname *fileName*

定义 passwd 文件在 NIS 下的位置。

--passwdpmd *pmdbName*

指定 sepass 将密码更新发送至的 PMDB。 此选项可更新 seos.ini 文件 [seos] 部分中的 passwd_pmd 标记。

注意：仅当同时使用 --subsconfig 开关参数时，才能使用此参数。

创建多级别策略模型时，在最顶层将此参数设置为 PMDB，以便可以将密码更改传播到 PMDB 系统中的所有级别。-

--pmdname *pmdbName*

指定要创建的 PMDB 的名称。

--pwmanager *name*

指定 PMDB 的 CA Access Control 密码管理员。

--seosdir *directory*

指定 CA Access Control 的安装目录。仅当 CA Access Control 未安装在默认目录中时，才使用此选项。

--subsconfig

指定本地工作站为订户。 使用此参数时，必须指定参数 --parentpmd *pmdbName* 和 --passwdpmd *pmdbName* ， 以更新 seos.ini 文件中的相关标记。

注意：配置订户时，这些参数应跟在 -subsconfig 选项之后。

--subscriber *name*

指定此 PMDB 的订户。 它们可以是 PMDB 或工作站。

--xadmin *name*

定义 PMDB 的企业用户管理员。

--xauditor *name*

定义 PMDB 的企业用户审核员。

--xpwmanager *name*

指定 PMDB 的企业用户密码管理员。

示例：使用命令行创建 PMDB

假设您有一个名为 bigcentral 的工作站，您要在其中维护一个其他工作站要订阅的 PMDB。 要在 bigcentral 中创建 PMDB，请在此处运行 sepmdadm。 此实用程序位于目录 *ACInstallDir*/bin 中。

要在 bigcentral 中创建名为 pmdb1 的 PMDB，并将 workstat1 和 workstat2 作为订户，将企业用户 adm1 和 adm2 作为管理员，请通过 bigcentral 运行以下命令：

```
sepmdadm --pmdname pmdb1 --subscriber workstat1 --subscriber workstat2 \
    --xadmin adm1 --xadmin adm2
```

示例：将订户工作站指向 PMDB

要将某个工作站建立为 PMDB 的订户，只在 PMDB 的工作站中指定订户的名称是不够的，还必须在订户工作站中执行一个程序。

要使用命令行为本地工作站订阅 PMDB，必须使用参数 --parentpmd 和 --passwdpmd 以及参数 --subsconfig。

例如：要为本地工作站订阅位于 HOST2 的名为 pmdb2 的 PMDB，以及位于 HOST1 的名为 master1 的密码 PMDB，请输入以下命令：

```
sepmdadm --subsconfig --parentpmd pmdb2@HOST2 --passwdpmd master1@HOST1
```

sepropadm 实用程序—管理数据库属性

sepropadm 实用程序在数据库中添加、更新和删除属性。 在*未*运行 CA Access Control 时，从数据库所在的目录中调用此实用程序。 sepropadm 实用程序一次只能添加一个属性。

重要说明！ 此实用程序仅供 CA Access Control 技术支持人员使用。 请*勿*将 sepropadm 用于*未*经 CA Access Control 技术支持人员认证的说明文件。

此命令格式如下：

```
sepropadm file
```

file

指定由 CA Access Control 支持人员提供的说明文件。该说明文件使用以下格式：

- 必须有一行以井号 (#) 开头；该行必须位于说明行之前。
- 以分号 (;) 开头的行是注释，不会被处理。
- 用于添加新的双链接 OID 的说明行必须符合以下格式：

  ```
  CLASS=%s  PROPERTY=%s  TYPE=%d  SIZE=%d  FLAGES=%x
  ```

- 用于添加新属性的说明行必须符合以下格式：

  ```
  CLASS=%s  PROPERTY=%s  TYPE=%d  SIZE=%d  FLAGS=%x  LINK2CLASS=%s
  ```

- 用于删除属性的说明行必须符合以下格式：

  ```
  CLASS=%s  PROPERTY=%s
  ```

- 用于更改属性的说明行必须符合以下格式：

  ```
  CLASS=%s  PROPERTY=%s  TYPE=%d  SIZE=%d  FLAGES=%x REPLACE=YES
  ```

示例：sepropadm 的说明文件

```
The following is a sample description file.
 ; CA Access Control 数据库的示例修补程序文件
 ; 版权所有 2004 Computer Associates International, Inc.
 ; ----------------------------------------
 ; 除非您知道如何使用该文件，否则不要使用它！
 # seclassadm database add property patch utility
 ; Format is :
 CLASS=PROGRAM PROPERTY=MD5 TYPE=31 SIZE=16 FLAGS=0
```

sepurgdb 实用程序—清除对未定义记录的数据库引用

在 UNIX 上有效

sepurgdb 实用程序可在整个数据库中搜索对未定义记录的引用，然后从数据库中删除这些引用，从而减小数据库。

重要说明！ 出于安全目的，请先备份数据库，然后在*未*运行 CA Access Control 后台进程时调用该实用程序。

删除某个记录后，列表（如 ACL 或组成员资格列表）中对它的引用通常保持原状，可减少处理时间。 这不会导致任何问题，因为 CA Access Control 为每个新记录分配了以前未使用过的唯一 ID。 您只需使用此实用程序释放一些磁盘空间。

要运行 sepurgdb，您必须为 root 用户，并从包含数据库文件的目录中调用实用程序。 数据库管理系统使用预先分配的磁盘空间。- 清除之后，数据库文件的大小通常不会有显著变化。 当以后数据库的大小增加时，由于预先进行了分配，文件大小可能不会发生明显变化。-

此命令格式如下：

```
sepurgdb FilePath [Username]
```

FilePath

为实用程序的日志文件指定基本名称。 sepurgdb 实用程序将创建两个日志文件：

***FilePath*.err**

包含所出现的错误的日志。

***FilePath*.log**

包含所采取的操作的日志。

注意：您可以为 *FilePath* 指定一个负号 (-)，以合并两个日志并将其定向到标准输出。

用户名

（可选）指定 sepurgdb 用于替换 USER 记录组连接中已删除的所有者（不再存在的用户）的用户名。

注意：您定义的用户必须存在于数据库中，否则实用程序将忽略此选项。

sereport 实用程序报告配置

sereport 实用程序可提供数据库和策略模型信息的 HTML 报告，可通过 Web 浏览器访问。 sereport 在授权引擎所使用的当前数据库上运行。

您可以为该实用程序设置 sereport 选项：

- 在 UNIX 上，sereport 使用您通过 -f 选项指定的配置文件。

  默认情况下为 *ACInstallDir*/etc/sereport.cfg

- 在 Windows 上，sereport 使用您可以进行配置的注册表。 sereport 的注册表设置在以下密钥下定义：

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Report
  ```

对于您可以生成的报告，其说明和对应的配置文件设置或注册表键显示在下表中。

报表编号	标题和说明	部分\子键	标记\条目
1	管理权限 显示用户的指定管理权限。	admin_report	■ 主机名 ■ Objects_Pattern ■ User_Mode
2	登录限制 显示用户的登录限制。	disablelogins_report	■ 主机名 ■ Objects_Pattern ■ 属性 ■ User_Mode
3	休眠帐号 按日期（天）显示不活动的帐号。 如果某个帐号没有任何登录信息，则会使用创建时间计算休眠天数。	dormant_report	■ 主机名 ■ Objects_Pattern ■ Dormant_account ■ User_Mode
4	上次登录 显示用户的上次登录日期。	login_report	■ 主机名 ■ Objects_Pattern ■ User_Mode
5	密码更改 显示必须在指定天数内更改其密码的用户的列表。	passwd_report	■ Days_to_change ■ 主机名 ■ Objects_Pattern ■ User_Mode
6	警告模式 显示处于警告模式的资源及对象。	warning_report	■ Class_Name ■ 主机名 ■ Objects_Pattern
7	不可信的程序 显示处于不可信模式的程序。	untrust_report	■ 主机名 ■ Objects_Pattern
8	用户的特权访问权限 显示用户对指定资源的访问权限。	accessor_report	■ 访问者 ■ Class_Name ■ 主机名 ■ Objects_Pattern

报表编号	标题和说明	部分\子键	标记\条目
9	比较数据库中的用户/组 显示在一些（而不是所有）数据库中定义的用户和组。	grp_usr_compare	■ 主机名 ■ Objects_Pattern
10	比较受保护的资源 显示是否在指定数据库中定义了资源。	res_compare	■ Class_Name ■ 主机名 ■ Objects_Pattern
11	比较访问权限 显示策略模型和订阅者数据库之间在资源限制方面的差异。	acc_compare	■ Class_Name ■ 主机名 ■ Objects_Pattern
12	比较用户信息 显示策略模型和订阅者数据库之间在用户定义方面的差异。	usr_compare	■ 主机名 ■ Objects_Pattern ■ 属性
13	比较 PMDB 和订阅者 显示 PMDB 上存在但订阅者数据库上不存在的规则（由 Class_Name 和 Object_pattern 内标识定义）。 注意：如果 PMDB 上的所有规则在订阅者数据库上都存在，则会将数据库报告为完全相同 (IDENTICAL)。	pmdb_compare	■ Class_Name ■ 主机名 ■ Objects_Pattern

访问者

指定访问者选择的模式（掩码）。 使用 * 可选择所有访问者。

Class_Name

指定类列表。

Days_to_change

指定要求用户更改密码前剩余的天数。

Dormant_account

指定将帐户视为睡眠的时间段。

主机名

指定从中检索数据的主机列表。

Objects_pattern

指定对象选择的模式（掩码）。 使用 * 可选择所有对象。

属性

指定与对象相关联的属性。

Report_place

（仅限于 UNIX）指定打印报告位置的完整路径。

注意：在 Windows 上，需使用该命令的 -f 选项定义输出的位置。

User_Mode

指定以逗号分隔的用户模式列表。

您也可以在颜色部分\键中查找以下其他配置设置：

title

指定报告标题的颜色。

class_title

指定报告的 class_title 的颜色。

background

（仅限于 UNIX）指定标题报告背景的颜色。 背景和徽标必须以完整路径书写。

logo

创建徽标。 背景和徽标必须以完整路径书写。

sereport 实用程序—在 UNIX 上创建 HTML 报告

在 UNIX 上有效

sereport 实用程序可创建数据库和策略模型信息的 HTML 报告，可通过 Web 浏览器进行访问。 sereport 在授权引擎所使用的当前数据库上运行。

要使用 sereport，需要在所有被查询数据库中拥有 READ 权限。

注意：默认的配置文件为 *ACInstallDir*/etc/sereport.cfg

此命令格式如下：

```
sereport [-f|-file pathname] -r|-report number [-host hostnames]
```

-f | -file *pathname*

（可选）指定配置文件的完整路径。 如果您未指定文件，sereport 将使用默认文件 *ACInstallDir*/etc/sereport.cfg

-host *hostnames*

（可选）指定要报告的一个或多个主机的名称。 如果您未指定主机，sereport 会从 config 文件中获取主机。

-r | report *number*

指定要创建的报告编号。

sereport 实用程序—在 Windows 上创建 HTML 报告

在 Windows 上有效

sereport 实用程序可创建数据库和策略模型信息的 HTML 报告，可通过 Web 浏览器进行访问。 sereport 在授权引擎所使用的当前数据库上运行。

要使用 sereport，需要在所有被查询数据库中拥有 READ 权限。

此命令格式如下：

```
sereport -f|-file pathname -r|-report number [-host hostnames]
```

-f | -file *pathname*

指定输出文件（报告）的完整路径名。

注意：指定文件的内容以 HTML 格式构建，因此您应为自动文件关联指定 *.html* 扩展名。

-host *hostnames*

（可选）指定要报告的一个或多个主机的名称。

如果未指定主机，sereport 将使用 *localhost*。

-r | report *number*

指定要创建的报告编号。

seretrust 实用程序－生成重新信任程序和安全文件的命令

seretrust 实用程序可生成重新托管在数据库中定义的程序和安全文件所需的 selang 命令。 seretrust 实用程序报告定义为可信任、但已经更改的 SECFILE 和 PROGRAM 资源的状态。 seretrust 也检查程序是否已经更改但尚未被 Watchdog 捕获。（这意味着在 CA Access Control 数据库中，这些程序仍标记为受托。）这些程序已添加到 seretrust 输出，带有注释表明程序内容或时间戳已经改变，程序需要重新托管。

注意：在 UNIX 上，具有 setuid 和 setgid 位的程序与它们的完整说明（包括其 inode 值）一起存储在数据库中。 如果从备份中还原系统，则程序会占用不同的 inode。 CA Access Control 检测到 inode 之间的不匹配，会将所有受托程序标记为取消受托。 seretrust 实用程序可查找在数据库中定义的受托程序并更新它们的 inode 值，这样，当您调用 CA Access Control 时，受托程序可保持受托状态。

如果不指定任何必选项，则只处理不可信任的程序和不可信任的安全文件。

此命令格式如下：

```
seretrust [-a] [-l|-m|-p|-s] path
```

-a

处理所有受托和未受托的对象。

-h

显示该实用程序的帮助。

-l

从当前目录的数据库中提取有关程序和文件的信息。

如果忽略此选项，seretrust 将处理 CA Access Control 所使用的数据库。

-m

计算所有内核模块的签名。 如果内核模块记录的签名属性无效，则 seretrust 将使用正确的签名进行更新，这可以确保该内核模块受托。签名仅用于 Linux 内核模块。

-p

只处理 PROGRAM 类中的记录。

-s

只处理 SECFILE 类中的记录。

path

指定用于搜索需重新托管的程序和安全文件的基路径。

该实用程序将处理指定的目录和所有子目录。

示例：重新托管取消受托的程序和安全文件

此示例展示了如何使用 seretrust 实用程序重新托管程序和安全文件。

注意：此示例展示了 UNIX 上的示例命令输出，但该实用程序在 Windows 上的工作原理与此相同。

要重新托管程序和安全文件，请按照以下步骤操作：

1. 以 CA Access Control 数据库管理员的身份，输入以下 seretrust 命令：

   ```
   seretrust > retrust_script
   ```

   因为未指定任何选项，所以该实用程序既要处理受托程序又要处理安全文件；由于未指定任何基路径，所以还会使用 root 路径。

   seretrust 将在屏幕上显示以下信息：

   ```
   Retrusting PROGRAMs & SPECFILEs, Base path = /
   Total of 0 entries retrusted. (Class=SECFILE)
   Total of 16 entities retrusted. (class=PROGRAM)
   ```

   以下是脚本文件 seretrust 可以创建的内容：

   ```
   chres PROGRAM ("/usr/bin/chgrpmem") trust
   chres PROGRAM ("/usr/bin/chie") trust
   chres PROGRAM ("/usr/bin/crontab") trust
   chres PROGRAM ("/usr/bin/cu") trust
   chres PROGRAM ("/usr/bin/ecs") trust
   chres PROGRAM ("/usr/bin/newgrp") trust
   chres PROGRAM ("/usr/bin/rmquedev") trust
   chres PROGRAM ("/usr/bin/rsh") trust
   chres PROGRAM ("/usr/bin/sysck") trust
   chres PROGRAM ("/usr/bin/uuname") trust
   chres PROGRAM ("/usr/lib/methods/showled") trust
   chres PROGRAM ("/usr/lib/mh/post") trust
   chres PROGRAM ("/usr/lib/mh/slocal") trust
   chres PROGRAM ("/usr/lpp/X11/bin/xlock") trust
   chres PROGRAM ("/usr/lpp/X11/bin/xterm") trust
   chres PROGRAM ("/usr/sbin/chvirprt") trust
   ```

2. 运行为重新托管程序和文件而创建的 selang 脚本文件 seretrust：

   ```
   selang -f retrust_script
   ```

serevu 实用程序－处理失败的登录尝试

在 UNIX 上有效

serevu 实用程序可处理在指定时间内失败登录尝试达到指定次数的用户。 根据您指定的内容，它可以禁用、报告或忽略该用户。 默认情况下，它会在本地工作站的 UNIX 环境中禁用该用户。 如果本地不存在此类用户，serevu 会检查 NIS 信息以查找该用户。

如果在 passwd_pmd 配置设置中设置了值，CA Access Control 会更新相应的 PMDB，之后 PMDB 会将更新传播给其订户。 如果未在 passwd_pmd 标记中设置值，CA Access Control 会使用 parent_pmd 配置设置中的值，之后该设置会将更新传播给其订户。

注意：如果希望 serevu 将命令发送至 PMD（可以在 serevu.cfg 中进行配置），但未在具有 ADMIN 属性或终端访问权限的 PMD 上定义根，则应在 PMD 及其所有订户上定义以下内容：

```
eu _serevu logical
authorize admin USER uid(_serevu) access(a)
# 下面的行仅可在主 PMD 上执行
authorize terminal localTerminalName uid(_serevu) access(a)
```

注意：为使 serevu 实用程序正常运行，root 用户必须具有文件 /etc/passwd 的写入权限。 如需在 serevu 配置文件 (serevu.cfg) 中定义远程计算机，还必须为该远程计算机授予登录权限。 例如：

```
eu _serevu admin logical
authorize terminal localTerminalName uid(_serevu) access(a)
er specialpgm $ACDIR/bin/serevu seosuid(_serevu ) unixuid(root)
```

此命令格式如下：

```
serevu {daemon|nodeamon} [-f nn] \
    [-d {nn[s|m|h|d|w]|FOREVER}] \
    [{-s|-t} nn[s|m|h|d|w]]
```

后台进程

将实用程序作为后台进程运行。 这是默认值。

nodaemon

将实用程序作为常规进程运行。

-d

指定禁用用户登录的时间长度。 默认情况下，此值以秒为单位。

注意：用户帐户的禁用时间长度不能小于每次 serevu 扫描之间的间隔时间。 用户帐户的禁用时间长度应为每次 serevu 扫描之间的间隔时间的倍数。

-f

指定失败登录的次数。 serevu 实用程序将禁用在指定时间内失败登录达到该次数的用户帐户。

注意：建议通过 *def_fail_count* 配置设置的值定义的失败登录次数始终与系统中设置的允许失败登录尝试的值相同。（例如：在 Solaris 上，此项的系统值在 /etc/default/login 中由 RETRIES 标记设置。）有关详细信息，请参阅操作系统文档。

-h

显示该实用程序的帮助。

-s

指定时间段，从*现在*开始向后推移，serevu 将在此时间段内扫描失败的登录。

默认值：300 秒（配置设置）。

-t

指定连续的 serevu 检查之间间隔的时间。

默认值：120 秒（配置设置）。

FOREVER

与 -d 选项配合使用，将时间指定为无限制。 如果使用此参数，用户登录将永远被禁用。

***nn*[s|m|h|d|w]**

与 -d、-s 和 -t 选项配合使用，指定选项的时间。

s

nn 以秒为单位（默认）。

m

nn 以分钟为单位。

h

nn 以小时为单位。

d

nn 以天为单位。

-w

nn 以周为单位。

sessfgate 实用程序—将 Unicenter 安全请求传递给 CA Access Control

sessfgate 实用程序可将消息队列中的 Unicenter 安全 API 传递并重新格式化到 CA Access Control。 UNIX 上的 Unicenter 安全 API 全部引导至消息队列。 sessfgate 实用程序可处理通过消息队列发送的 API 请求，并将这些重新格式化和重新传递的请求发送至 CA Access Control。 然后，该实用程序会将 CA Access Control 的返回代码转换为 Unicenter TNG 等同代码。

要激活网关，您必须运行 Unicenter 集成安装程序。 Unicenter 集成安装将在 *ACInstallDir*/tng/bin 目录（其中 *ACInstallDir* 是您安装 CA Access Control 的目录，默认情况下为 /opt/CA/AccessControl/）中安装 sessfgate 程序。 关闭 Unicenter 安全并启动 CA Access Control 之后，sessfgate 将接受 API 请求而不是 SSF。

此命令格式如下：

```
sessfgate [-i|-s|-l] -t
```

-I

指定启动网关。

-s

指定停止网关。

-l

指定状态。

-t

切换跟踪文件 (log file = /opt/CA/AccessControl//log/sessftrace.log)。

注意：如果在运行 Unicenter TNG 之前运行 seload，必须使用以下命令手动启动 sessfagte：

```
ACInstallDir/tng/bin/sessfagte -I
```

其中 *ACInstallDir* 是安装 CA Access Control 的目录。

sesu 实用程序－替代用户

通过 sesu 实用程序可以暂时以另一用户的身份进行操作。 该实用程序是 UNIX 的 su 命令的 CA Access Control 版本。 但是，sesu 实用程序提供的用户替代命令不需要您提供被替代用户的密码。 身份验证过程根据 SURROGATE 类中定义的 CA Access Control 访问规则进行，还可根据执行命令的用户密码进行（可选）。

sesu 实用程序使用 seos.ini 文件 sesu 部分中的标记。 它还会使用以下特殊文件：

- /etc/passwd
- /etc/group
- /etc/shells

为了避免不经意使用该程序，在文件系统中对 sesu 进行了标记，没有任何用户可以运行它。 安全管理员必须将该程序标记为可执行并将 setuid 设为 root，您才能使用该程序。

重要说明！ 在您使用 sesu 实用程序前向 CA Access Control 数据库定义所有用户并设置 sesu 先决条件。 这样可以避免未定义到 CA Access Control 的用户打开整个系统。

使用注意事项：

- 如果找不到 CA Access Control 授权服务器，该实用程序会执行系统的标准 su 命令。
- 如果 sesu.old_sesu 配置标记设为 no，则该实用程序将执行系统的标准 su 命令。
- 如果 /etc/shells 存在，且未指定当前的 shell，那么 sesu 将不允许替代 root。

该实用程序格式如下：

```
sesu [-] [username] [-l] [-n] [-s shell] [-c command]
```

-

将环境设为目标用户的环境。

注意：在 Linux 上，这与使用 *-l* 选项相同。

-c *command*

执行指定命令后退出。

将包含空格的命令用引号引起。

-h

显示该实用程序的帮助。

-l

（仅限于 Linux）。 指定打开的 shell 为登录 shell。

-n

指定不为用户提示输入密码

重要说明！ 在使用时，实用程序作为根帐户运行并执行 LOGIN 事件。

注意：如果找不到安全授权服务器，实用程序则使用 /bin/su。

-s *shell*

（仅限于 Linux）。 指定要打开的 shell，而不打开来自用户密码条目的 shell。

该 shell 必须在 /etc/shells 文件中列出。

用户名

将与会话相关联的 ID 更改为指定目标用户的 *username* ID。

如果不指定 *username*，sesu 将默认使用 root。

示例

- 以下命令可将 UID 更改为 root。 环境保持为执行命令的用户的环境。

  ```
  sesu
  ```

- 以下命令可将 UID 更改为 root。 该实用程序会将环境更改为 root 环境。

  ```
  sesu -
  ```

- 以下命令替代用户 John。

  ```
  sesu John
  ```

- 以下命令将代理用户 Carol 并从 /home/carol 目录执行指定的命令 ls -la。

  ```
  sesu - Carol -c "ls -la /home/carol"
  ```

- 以下命令可代理用户 Angelo，使用 bash shell 并将该 bash shell 作为登录 shell 打开。

  ```
  sesu Angelo -l -s /bin/bash
  ```

  注意：此命令仅在 Linux 上有效。

sesudo 实用程序

sesudo 实用程序使用一个用户的权限为另一个用户执行命令。 这使得普通用户可以执行需要具有管理员权限的操作。

用于以这种方式管理用户命令执行授权的规则在 SUDO 类中定义为访问规则。 SUDO 类中的记录包含命令脚本，可以指定获准使用和禁止使用 sesudo 运行脚本的用户。

sesudo 实用程序—在 UNIX 上以另一用户的身份执行命令

在 UNIX 上有效

sesudo 实用程序使用一个用户的权限为另一个用户执行命令。 sesudo 实用程序借用另一个用户（*目标*用户）的权限来执行一个或多个命令。这样，普通用户便可执行诸如需要超级用户权限的操作（如 mount 命令）。

用于以这种方式管理用户命令执行授权的规则在 SUDO 类中定义为访问规则。 SUDO 类中的记录包含命令脚本，可以指定获准使用和禁止使用 sesudo 运行脚本的用户。

每次运行 sesudo 时，都会返回下列值之一。

-2

找不到目标用户，或者命令中断

-1

密码错误

0

执行成功

10

参数的用法有问题

11

未装入 系统调用

20

目标用户错误

22

已装入系统调用但后台进程未运行

30

授权错误

此命令格式如下：

```
sesudo {-h|-list|record [params]}
```

-h

显示帮助屏幕。

-列表

列出您可以执行的 sesudo 命令。 这些是在 CA Access Control 数据库中定义，且您有权执行的 SUDO 记录。

记录

指定 SUDO 类记录（安全管理员为您希望通过 sesudo 实用程序执行的命令分配的）的名称。

params

（可选）指定要发送给正执行的命令的参数。

sesudo 实用程序—在 Windows 上以另一用户的身份执行命令

在 Windows 上有效

sesudo 实用程序使用一个用户的权限为另一个用户执行命令。 sesudo 实用程序借用另一个用户（*目标*用户）的权限来执行一个或多个命令。这样，普通用户便可执行诸如需要超级用户权限的操作（如 mount 命令）。

用于以这种方式管理用户命令执行授权的规则在 SUDO 类中定义为访问规则。 SUDO 类中的记录包含命令脚本，可以指定获准使用和禁止使用 sesudo 运行脚本的用户。

注意：执行 sesudo 调用的程序的用户无法从 Windows 的 CA Access Control 更改。

此命令格式如下：

```
sesudo {-h|-list|-do record [params]}
```

-h

显示联机帮助屏幕。

-list

列出您可以执行的 sesudo 命令。 这些是在 CA Access Control 数据库中定义，且您有权执行的 SUDO 记录。

-do *record* [*params*]

指定 sesudo 以另一用户的身份执行命令。

记录

指定 SUDO 类记录（安全管理员为您希望通过 sesudo 实用程序执行的命令分配的）的名称。

params

（可选）指定要发送给正执行的命令的参数。

seuidpgm 实用程序－提取受托的程序

在 UNIX 上有效

seuidpgm 实用程序提取 Set-User-ID 位或 Set-Group-ID 位为开启状态的所有程序。 seuidpgm 将遍历文件系统并创建 selang 命令以将这些程序添加到 PROGRAM 类。

seuidpgm 使用 selang 命令语言创建命令，并将其写入标准输出。 您可以对 selang 实用程序使用管线，也可以将输出重定向至文件。 建议您将输出重定向至文件，因为这样您便可以编辑输出以删除不需要的程序或添加其他程序。 通过此过程可在您的系统中搜索不需要的 setuid 程序。

注意：建议您在运行 seuidpgm 实用程序之前运行 UxImport 实用程序来定义用户和组。 然而，如果未运行 UxImport，可以使用带有 -g 和 -u 选项的 seuidpgm 来定义用户和组。

seuidpgm 通过在命令行中指定的路径，向下遍历到开始路径的所有子目录。 允许有多个开始路径。

可以指定任意数量的选项。 指定多个选项时，请用空格分隔选项。

如果某个程序是 setuid 程序并且具有写入权限，则 seuidpgm 不仅会像对待所有其他 setuid 程序一样对待该程序，还会向标准错误发送警告。

注意：有关如何控制 PROGRAM 类记录的详细信息，请参阅 *《适用于 UNIX 的端点管理指南》*。

此命令格式如下：

```
seuidpgm option startDir ... [-x excludeDir]
```

-d

自动为 PROGRAM 类中的 setuid 和 setgid 程序创建条目，并将 defaccess 设置为 execute，而不是分析 UNIX 中的文件权限以确定允许的文件访问。 在某些情况下，一个 setuid 或 setgid 程序会执行另一个 setuid 或 setgid 程序。 如果未包括此选项，尝试执行 setuid 或 setgid 程序的程序*不*能执行该程序。

建议您使用此选项。

-f

为 FILE 类和 PROGRAM 类创建规则。

--g

为 setgid 程序创建 GROUP 记录。

注意：*只有*您*未*运行 UxImport 时，才能使用此选项。

-l

为包含*硬*链接或*符号*链接的程序创建单个许可。

如果只想从一些目录（而不从根目录）扫描文件系统，并且希望包括 -l 选项，请在命令行中使用多个开始路径；否则，-l 选项可能会无效。

-n

完全不遍历 NFS。

建议您使用此选项。

--o

将文件名写入标准输出，但不创建 selang 命令。

-p

从 NFS 目录启用 setuid 程序，但仅当挂接表允许所挂接文件系统中的 setuid 时启用。

-q

以静默模式运行实用程序；错误消息不发送到标准错误。-

-s

为类 SECFILE 中的 setuid/setgid 程序创建条目，而不是为 PROGRAM 类创建条目。

-u

为 setuid 程序创建 USER 记录。

注意：*只有*您*未*运行 UxImport 时，才能使用此选项。

-x *excludeDir*

从树中排除目录。 不在指定目录中搜索 setuid 和 setgid 程序。 此选项必须为在命令行中指定的最后一个选项。 *Path* 为要排除的目录的完整路径。 要排除多个目录，请为每个目录重复使用 -x 选项。

startDir

指定以空格分隔的顶部目录列表，以搜索受托程序。

示例

- 下面的命令会输出 selang 命令，以添加开启了 set-user-id 或 set-group-id 并且 defaccess 为 execute 的所有程序，从而以静默模式检查重复的名称或相同的 inode，并且不通过 NFS 传递。 该程序将从 /usr 目录及其子目录、/var 目录及其子目录，以及 /etc 目录及其子目录进行扫描。 输出将定向到主目录中的 seprogs.seos 文件。

  ```
  seuidpgm -dlqn /usr /var /etc > ~/seprogs.seos
  ```

  输出的外观应类似如下：

  ```
  ## ************************************************
  ## seuidpgm List Sun Feb 9 14:24:16 1997
  # Start Path= /usr
  # ************************************************
  nr PROGRAM /usr/lpp/bos/inst_root/lpp/inu_LOCK defaccess(EXEC)
  nr PROGRAM /usr/lpp/X11/bin/xlock defaccess(EXEC)
  nr PROGRAM /usr/bin/setsenv defaccess(EXEC)
  nr PROGRAM /usr/bin/shell defaccess(EXEC)
  nr PROGRAM /usr/bin/su defaccess(EXEC)
  nr PROGRAM /usr/bin/sysck defaccess(EXEC)
  nr PROGRAM /usr/bin/tcbck defaccess(EXEC)
  nr PROGRAM /usr/bin/usrck defaccess(EXEC)
  nr PROGRAM /usr/bin/vmstat defaccess(EXEC)
  ```

- 以下命令扫描根目录以及它的除 /home 目录以外的所有子目录：

  ```
  seuidpgm -qln / -x /home
  ```

更多信息：

UxImport 实用程序－从 UNIX 操作系统中提取信息 (p. 237)
selang 实用程序－运行 CA Access Control 命令行 (p. 164)
seoswd 后台进程 (p. 263)
seosd 后台进程 (p. 258)

seversion 实用程序－显示 CA Access Control 程序模块版本信息

在 UNIX 上有效

seversion 实用程序可显示有关 CA Access Control 模块版本的信息。 您可以显示以下数据：

- 全局版本号和次要版本号。
- 编译模块的日期和时间。
- 在其上编译模块的工作站。

此命令格式如下：

```
seversion [-a|-l|-g|-h|-m|-s|-5] module
```

-a

以表的格式显示请求的信息。

--g

仅显示全局版本号，省略标题。

-h

显示该实用程序的帮助。

-l

显示包括的库信息。

-m

仅显示副版本号，省略标题。

-s

显示 SHA1 签名，省略标题。

-5

显示 MD5 签名，省略标题。

只有不处于仅 FIPS 模式中时，才可使用此选项。

模块

指定要显示版本号的模块的文件名。

示例

要显示 sesudo 工具的版本信息，请输入以下命令：

```
seversion /opt/CA/AccessControl//bin/seosd
```

不处于 FIPS 模式中时，屏幕上会显示一条包含以下类似内容的消息：

```
CA Access Control seversion vX.X.X.xxx—显示模块的版本
版权所有 (c) YYYY CA。 保留所有权利。
Running under:  Linux
File name: /opt/CA/AccessControl//bin/seosd
Version   : major.minor.sp.build
Created   : MMM DD YYYY hh:mm:ss
OS info   : i86PC
SHA1      : 10068CC6A70195B84AF896682CCBA1A4B7B43CD1
MD5:      : 1F9BD56CA523A33FFBC47551ECE093E5
```

sewhoami 实用程序 — 在 UNIX 上显示您的 CA Access Control 用户名和安全凭据

在 UNIX 上有效

sewhoami 实用程序可显示已为 CA Access Control 授权后台进程所知的用户名。 sewhoami 与 UNIX 系统提供的 whoami 实用程序相似，但它可生成不同的信息，通常会更加有用：

- 如果用户先执行 su 命令，然后执行 UNIX whoami 工具，则它会在执行 su 命令后根据所获得的用户 ID 显示用户名。
- 如果用户先执行 su 命令，然后执行 CA Access Control sewhoami 实用程序，则它会显示该用户的原始登录 ID；此外还会显示授权信息。

此命令格式如下：

```
sewhoami [-a|-d]
```

-a

显示用户凭据；即，用户 ACEE 的内容。

注意：有关 ACEE 详细信息，请参阅*《适用于 UNIX 的端点管理指南》*。

-d

显示与用户关联的 ACEE 句柄，以及该句柄在数据库中的名称。

示例：在 UNIX 上显示您的 CA Access Control 用户名和安全凭据

此示例将显示已为 CA Access Control 授权后台进程所知的您自己的用户名和安全凭据：

```
sewhoami -a
```

如果您是根用户，sewhoami 输出类似于以下示例：

```
根
ACEE 内容
 用户名                : root
  ACEE 的句柄          : 52
  组连接表:
    组名称              连接模式
          ==========    ==============================
    adm                 常规
    bin                 常规
    daemon              常规
    disk                常规
    root                常规
    seosaudt            常规
    sys                 常规
    wheel               常规
类别                : <无>
配置文件组          : <无>
安全标签            : <无>
用户的审核模式      : Failure LoginSuccess LoginFailure
用户的安全级别  : 0
源终端          : <未知>
ACEE 的进程计数  : 19
用户的模式          : Admin Auditor
ACEE 的创建时间  : 2009 年 3 月 17 日星期二 14:53:07
```

如果您是名为 test 的用户且不是根用户，sewhoami 输出类似于以下示例：

```
test
ACEE 内容
  用户名              ：  test
  ACEE 的句柄          ：  65
  组连接表：
    组名称              连接模式
          ==========    ==============================
    seosaudt            常规
    users               常规
类别              ：  <无>
配置文件组          ：  secadmin
安全标签          ：  <无>
用户的审核模式      ：  Failure LoginSuccess LoginFailure
用户的安全级别    ：  0
源终端          ：  localhost.localdomain
ACEE 的进程计数  ：  2
用户的模式            ：  Admin Auditor
ACEE 的创建时间    ：  2009 年 3 月 18 日星期三 15:34:53
```

更多信息：

secons -whoami 函数 －显示您的用户名和安全凭据 (p. 153)

uninstall_AC 实用程序－从当前计算机中删除 CA Access Control

在 UNIX 上有效

uninstall_AC 实用程序可从您执行命令的工作站中删除整个或部分 CA Access Control。 使用默认值 (-all) 将从工作站中删除整个产品。

注意：应在卸载之前卸载 CA Access Control 内核扩展。

此命令使用以下语法：

```
uninstall_AC [-all | -admin] [-f] [-force] [-h] [-ignore_dep] [-d path] [-fn file]
```

-admin

仅从工作站中删除如 Security Administrator 和 seauditx 等管理工具。

注意：CA Access Control 不再包括 *admin* 程序包。 此选项用于删除较旧版本的 CA Access Control。

-所有

从工作站中删除整个产品。

-d *path*

定义 CA Access Control 的安装目录。

注意：如果在默认目录 (/opt/CA/AccessControl/) 下安装 CA Access Control，则无需指定此选项。

-f

以静默模式删除 CA Access Control。

-fn *file*

在卸载完成后执行指定的文件。

-force

强制卸载继续进行，即使内核扩展卸载进程失败也是如此。

-h

显示该实用程序的帮助。

-ignore_dep

指定卸载过程不检查与其他产品的依存关系。

示例：从计算机中完全删除 CA Access Control

要将 CA Access Control 从此计算机中完全删除，如果它安装在默认目录下，请输入以下命令：

```
uninstall_AC
```

uxauthd.sh 脚本－管理 UNIX 身份验证代理 代理

使用 uxauthd.sh 脚本可管理 UNIX 身份验证代理 代理。 建议您使用 uxauthd.sh 脚本来管理 UNIX 身份验证代理 代理，因为该帮助可以确保环境配置正确。

默认情况下，uxauthd.sh 脚本位于 /opt/CA/uxauthd/lbin 目录中。

此命令格式如下：

```
uxauthd.sh {start | stop | restart | status | debug level}
```

启动

启动 UNIX 身份验证代理 代理。

停止

停止 UNIX 身份验证代理 代理。

重新启动

重新启动 UNIX 身份验证代理 代理

状态

显示 UNIX 身份验证代理 代理的状态。 状态包括：

- uxauthd 正在运行
- uxauthd 未在运行

debug *level*

指定在调试级别启动 UNIX 身份验证代理 代理。

范围：1-3

注意：使用 uxauthd.sh 启动或停止 UNIX 身份验证代理 代理时，会影响报告代理的状态。

uxconsole 实用程序—管理 UNIX 身份验证代理 端点

uxconsole 实用程序可用来管理 UNIX 身份验证代理 端点。 使用 uxconsole 实用程序可以显示有关 UNIX 身份验证代理 安装的信息，在 Active Directory 中注册 UNIX 身份验证代理 端点，并管理及迁移用户和组。

该实用程序可处理多个任务，并具有以下函数：

任务	函数
在 Active Directory 中注册 UNIX 计算机	uxconsole -register (p. 226)
在 Active Directory 中取消注册 UNIX 计算机	uxconsole -deregister (p. 226)
设置详细级别	uxconsole -debug (p. 234)
激活 Active Directory 用户的登录	uxconsole -activate
取消激活 Active Directory 用户的登录	uxconsole -deactivate
将用户和组迁移到 Active Directory	uxconsole -migrate (p. 223)

任务	函数
管理用户和组	uxconsole -manage (p. 222)
显示端点状态	uxconsole -status (p. 228)
执行 Kerberos 操作	uxconsole -krb (p. 231)
在 Active Directory 中执行 LDAP 查询	uxconsole -ldap (p. 232)
显示 UNAB NSS 缓存数据	uxconsole -dbdump (p. 233)
验证 Active Directory 用户帐户	uxconsole -verify (p. 235)

uxconsole -manage—管理用户和组

在 UNIX 上有效

使用此命令可以列出、显示或编辑本地或企业用户和组的信息。

此命令具有以下格式：

```
uxconsole -manage {-find | -show [-detail]} {-user <filter> | -group <filter>}
```

-find

指定显示本地和企业用户或组的列表。

-show

指定显示特定用户或组的详细信息，或用户和组的子集。

-detail

指定显示详细的用户设置。

-user *filter*

定义返回用户子集的通配符。

-group *filter*

定义返回组的子集的通配符。

示例：显示用户状态

下面的示例显示了本地 UNIX 用户 (local1) 的输出，该用户映射到具有不同名称 (ent1) 的 Active Directory 用户。 Active Directory 用户启用了 UNIX 属性，因此可以登录到 UNIX 身份验证代理 端点：

```
uxconsole> ./uxconsole -manage -show -detail -user ent1
CA Access Control UNAB uxconsole v12.52.0.160—控制台实用程序
版权所有 (c) 2009 CA。 保留所有权利。

USER 'ent1' 信息
-----------------------------------------------------
类型                  : 本地用户
登录名           : local1
映射到            : ent1@example.com
企业帐户   : 已启用
本地帐户        : 已启用
登录                  : 允许
登录原因         : 用户在本地存在
Uid                   : 300
Gid                   : 101
Shell                 : /bin/bash
主目录       : /home/local1

类型                  : 企业用户
登录名           : ent1
主要名称       : ent1@example.com
企业帐户   : 已启用
登录                  : 允许
登录原因         : 根据内部默认值
Uid                   : 10133
Gid                   : 13870
Shell                 : /bin/sh
主目录       : /home/ent1
```

uxconsole -migrate—将 UNIX 用户和组迁移到 Active Directory

在 UNIX 上有效

使用 migrate 命令将用户和组从 UNIX 主机迁移到 Active Directory 中。迁移过程尝试将本地用户和组迁移到 Active Directory 中，并禁用本地帐户。

此命令格式如下：

```
uxconsole -migrate [-scope {l|n|a}] {-mode {p|f}|-input file} [-emulate] [-d
domain] [-a name [-w pass]] [-users] [-groups] [-cgc container] [-new] [-v level]
[-h]

uxconsole -migrate [-show {-user filter|-group filter}]
```

-migrate

定义 UNIX 用户迁移选项。

-scope {l | n | a}

指定迁移范围：

- l—仅迁移本地用户和组。
- n—从 NIS\NIS+ 服务器迁移 NIS 用户和组。
- a—迁移本地及 NIS/NIS+ 用户和组。

默认值：l

-mode {p | f}

指定迁移模式。

选项：partial、full

默认值：f

-input *file*

定义帐户映射文件的完整路径。

注意：使用映射文件可解决在迁移过程中发现的用户帐户冲突。 使用以下字段和参数创建 CSV 格式的映射文件：
类型 <USER|GROUP>, UNIX 名称 <用户名>, 请求的操作 <KEEPLOCAL|MIGRATE|MAP>, AD 名称 <AD 映射名称>

示例：USER, uxuser, MAP, aduser。

-emulate

指定在模拟模式下运行迁移进程。

注意：在模拟模式下运行 uxconsole -migrate 命令时，不会将用户迁移至 Active Directory。 在模拟模式下，uxconsole 将创建一个日志文件，报告用户和组 ID 可能存在的冲突。 使用模拟模式可以解决 UNIX 和 Active Directory 用户和组 ID 之间的冲突。

-d *domain*

定义用户和组迁移到的域的名称。

注意：运行 -migrate -d 命令时，如果不提供管理员凭据，则不允许 UNIX 身份验证代理 将用户和组迁移到 Active Directory。

-a *name*

指定在 Active Directory 中用来注册、创建和更新用户属性的 Active Directory 管理员。

注意：如果运行 -migrate 命令时不提供管理员凭据，则不允许 UNIX 身份验证代理 附加 UNIX 属性，也不允许将帐户或组添加到 Active Directory 中。 如果不提供 Active Directory 管理员凭据，则无法解决在迁移过程中发现的冲突。

-w *passwd*

指定 Active Directory 管理员的帐户密码。

-users

（可选）指定仅将特定用户迁移到 Active Directory。

注意：如果不指定此选项，则将所有用户都将迁移到 Active Directory。

-groups

（可选）指定仅将特定组迁移到 Active Directory。

注意：如果不指定此选项，则将所有组都将迁移到 Active Directory。

-cgc *container*

指定创建新组时所在的 Active Directory 容器的名称。

-new

指定仅迁移先前未迁移的新用户和组。

-v *level*

指定详细级别。

范围：1-5

-h

显示帮助。

-show

显示用户和组迁移信息。

注意：如果指定此选项，将不迁移用户和组。

-user *filter*

仅显示与筛选条件匹配的用户。

-group *filter*

仅显示与筛选条件匹配的组。

uxconsole -register—在 Active Directory 中注册 UNIX 计算机

在 UNIX 上有效

使用此命令可以在 Active Directory 中注册 UNIX 主机。 注册 UNIX 主机是 UNIX 身份验证代理 配置过程的一部分，注册后，Active Directory 用户将可以登录 UNIX 主机。

注意：在注册 UNIX 主机后，必须激活 UNIX 身份验证代理，以允许 Active Directory 用户登录主机。

在下列情况中，实用程序无法注册 UNIX 主机：

- 如果不含域后缀的 UNIX 计算机主机名超过 15 个字符，则注册将失败。 这是因为，Active Directory 会对计算机对象名称中的字符数应用基于 NetBIOS 的限制。

  例如：您无法在 Active Directory 中注册名为 engineering-dept-sol2 的 UNIX 计算机，因为该主机名超过 15 个字符。 您可以注册名为 eng-dept-sol2.example.com 的 UNIX 计算机，因为不含域名 (eng-dept-sol2) 的主机名不超过 15 个字符。 要显示 UNIX 计算机的主机名，请运行 hostname 命令。

- 在 uxauth.ini 文件 ad 部分的 ignore_dc_list 配置设置中，如果指定了 Active Directory 站点中 UNIX 主机用来与 Active Directory 通讯的所有 DC，则注册将失败。

  默认情况下，当您在 Active Directory 中注册 UNIX 主机时，uxconsole 实用程序会自动发现最接近端点实际位置的 Active Directory 站点，并且仅与该站点中的 DC 进行通讯。 还可以使用 -t 选项来指定此 Active Directory 站点。

可以在同一计算机上多次运行此命令。 例如：如果 keytab 文件被删除，您可以运行此命令来修复 UNIX 身份验证代理 主机在 Active Directory 中的注册。

注意：可以运行不带参数的 uxconsole - register 命令，以使用默认设置。 程序会提示您输入所需的附加信息。

此命令格式如下：

```
uxconsole -register [-a name] [-w pass] [-d domain] [-v level] [-n] [-o container] [-s server] [port #] [-h] [-t site] [-sso]

uxconsole -deregister [-a name] [-w pass] [-v level] [-o container] [-s server] [port #]
```

-register

指定 Active Directory 注册 UNIX 身份验证代理。

-deregister

指定 Active Directory 取消注册 UNIX 身份验证代理。

-a *name*

定义有权在 Active Directory 中注册计算机的用户的用户名。

默认值：administrator

-w *pass*

定义有权在 Active Directory 中注册计算机的用户的密码。

-d *domain*

定义 Active Directory 所属域的名称。

-h

显示程序帮助。

-n

指定在注册过程完成后运行 uxauthd 代理。

如果不指定此选项，在注册过程完成后将不会运行 uxauthd。

-o *container*

定义 UNIX 计算机所注册的 Active Directory 容器的名称。

注意：必须存在 Active Directory 容器才能注册 UNIX 计算机。

-port #

定义 Active Directory 侦听端口号。

-s *server*

定义 Active Directory 服务器名称。

-sso

指定 uxconsole 管理用于单点登录 (SSO) 的 Kerberos 文件。

-t *site*

定义 Active Directory 站点，UNIX 身份验证代理 使用该站点中所包含的 DC 与 Active Directory 通讯，并将站点的名称写入 uxauth.ini 文件 ad 部分中的 ad_site 配置设置。

建议您不要指定此选项。 如果不指定此选项，实用程序会自动选择使用最合适的 Active Directory 站点。

注意：ignore_dc_list 和 lookup_dc_list 配置设置中的值将影响 UNIX 身份验证代理 实施 Active Directory 站点支持的方式。

-v *level*

定义在安装过程中使用的详细级别。

示例：在 Active Directory 中注册 UNIX 主机

此示例展示了如何在 Active Directory 中注册 UNIX 计算机。 键入用户名 (-a administrator) 和密码 (-w admin)，设置详细级别 (-v 3)，指定在安装结束时不运行 UNIX 身份验证代理 代理 (-n)，并且定义 Active Directory 中容器的名称 (-o OU=COMPUTERS)。 必须存在容器才能在 Active Directory 中注册 UNIX 计算机：

```
./uxconsole -register -a administrator -w admin -v 3 -n -o OU=COMPUTERS
```

uxconsole -status—显示 UNIX 身份验证代理 状态

在 UNIX 上有效

使用此命令可以显示端点上 UNIX 身份验证代理 的状态。 使用 -detail 参数显示有关 UNIX 身份验证代理 状态的所有可用信息。

此命令格式如下：

```
uxconsole -status [-detail]
```

-status

指定显示 UNIX 身份验证代理 状态。

-detail

指定详细地显示 UNIX 身份验证代理 状态。

示例：详细地显示 UNIX 身份验证代理 状态

下面的示例显示了运行 uxconsole - status -detail 命令时的输出。

```
#./uxconsole -status -detail
CA Access Control uxconsole v12.52.0.160－控制台实用程序
版权所有 (c) 2009 CA。 保留所有权利。

注册域     - example.com
DC                    - computer1, computer2
用户搜索库        - DC=unixauth,DC=example,DC=com
用户搜索筛选
                包括    - CN=Users; OU=Test
               排除    - OU=WrongOU
组搜索库       - CN=Users,DC=example,DC=com
组搜索筛选
               排除    - OU=Computers
受托域          - DC=unab,DC=example,DC=com
DC                    - winserver
用户搜索库        - DC=unabdom,dc=example,dc=com
用户搜索筛选
             包括     - CN=users
组搜索库       - DC=unab,DC=example,DC=com
UNAB 模式              - 完全集成
UNAB 状态             - 已激活
代理状态            - 正在运行，pid = 6178
时间同步              - 已启用（NTP 服务器: 192.168.1.100）
企业策略       - login@computer.com（更新: 2009 年 10 月 19 日星期一 14:36:47）
企业策略       - loginHG@GHNODE#01（更新: 2009 年 10 月 19 日星期一 14:36:47）
本地策略            - 已启用
默认登录访问    - 拒绝
AD Unix 用户          - 16（更新: 2009 年 10 月 19 日星期天 15:53:04）
AD Unix 组          - 8（更新: 2009 年 10 月 19 日星期天 15:53:04）
AD Windows 组       - 19（更新: 2009 年 10 月 19 日星期天 15:53:04）
迁移               - 未迁移
CA Access Control      - 已安装
                       在 AC ladb 中包括 AD 用户和组: 是
                       在 AC 审核中显示 AD 名称: 否
                       在 AC 中支持 AD 非 Unix 组: 是
                       在 AC 实用程序进行 PAM 身份验证: 是
```

在此示例中，输出中显示以下信息：

- Active Directory 域名－example.com
- 与端点通讯的 DC－computer1、computer2
- 用户和组搜索基本筛选
- 受信任域－unab.example.com
- UNAB 模式－完全集成
- UNAB 状态－已激活

- UNAB 代理 (uxauthd) 状态－正在运行， pid = 6178
- 时间同步是否已激活－已启用
- NTP 服务器 IP 地址－192.168.1.100
- 部署的企业登录策略的名称－login@computer.com，loginHG@GHNODE#01
- 企业登录策略的最后更新时间－更新时间：2009 年 10 月 19 日星期一 14:36:47
- 本地登录策略是否已激活－已启用
- 默认登录策略是否已启用－拒绝
- Active Directory 中 UNIX 用户的数目－16 以及最后更新时间
- Active Directory 中 UNIX 组的数目－8 以及最后更新时间
- Active Directory 中 Windows 组的数目－19
- UNIX 用户和组以及 Windows 组的最后更新时间－更新时间：2009 年 10 月 19 日（星期日）15:53:04
- 用户的迁移状态－未迁移
- CA Access Control 是否安装在该端点上－已安装
- 是否在 CA Access Control ladb 中包含有关 Active Directory 用户和组的信息－是
- 是否在 CA Access Control 审核记录中显示 Active Directory 用户和组名称－是
- CA Access Control 是否支持非 UNIX 的 Active Directory 组－是
- 在 CA Access Control 实用程序中是否支持 PAM 身份验证－是

uxconsole -krb—执行 Kerberos 操作

在 UNIX 上有效

使用此命令可以从 UNIX 身份验证代理 端点执行 Kerberos 操作，例如创建票证。 不必在端点上安装 Kerberos 即可执行 Kerberos 操作。

此命令格式如下：

```
uxconsole -krb [-init | -list | -vno | -destroy
```

-init

指定获得并缓存票证

-list

显示凭据缓存或 keytab 的内容

-vno

显示 Kerberos 主体的关键版本号

-destroy

指定销毁凭据缓存

示例：使用 UNIX 身份验证代理 keytab 获得票证授予票证 (TGT)

下面的示例展示了如何使用 UNIX 身份验证代理 keytab 获得 TGT：

```
./uxconsole -krb -init -k
```

示例：列出凭据缓存的内容

下面的示例展示了如何列出凭据缓存的内容：

```
./uxconsole -krb -list
```

示例：列出含加密数据的 keytab 内容

下面的示例展示了如何显示 keytab 的内容，包括可用的加密信息：

```
./uxconsole -krb -list -ke
```

uxconsole -ldap—在 Active Directory 中执行 LDAP 查询

在 UNIX 上有效

使用此命令可以从未安装 LDAP 的 UNIX 身份验证代理 端点在 Active Directory 上执行 LDAP 查询。 应使用此命令，而不是 ldapsearch 实用程序。 可以使用此命令解决 UNIX 身份验证代理 安装问题，例如可以在 Active Directory 中查询要使用的容器。

重要说明！ 在使用此命令之前，请验证您是否具有票证授予票证 (TGT)。 可以使用 uxconsole -krb 命令获得 TGT。

注意：LDAP 筛选必须符合 RFC 2254 标准。

此命令的格式如下：

```
uxconsole -ldap -search [-d DC] [-p port] [-b base] [-s scope] [filter
[attributes]]
```

-search

指定搜索选项

-d *DC*

指定要查询的域控制器

-p *port*

指定要使用的 LDAP 端口

-b *base*

指定搜索库

-s scope

指定搜索范围

默认值：sub

filter *[attributes]*

指定要使用的筛选和属性

注意：如果不指定筛选，则使用“(objectClass=*)”。 如果不指定任何属性，将使用代表全选的选项 ('*')。

示例：显示 DSE

下面的示例展示了如何显示 DSE：

```
./uxconsole -ldap -search '(&(objectClass=user) (objectCategory=user) )'
```

uxconsole -dbdump－显示 UNAB NSS 缓存数据

在 UNIX 上有效

使用此命令可显示来自 UNIX 身份验证代理 NSS 数据库的用户和组信息。 可以使用此命令来查看有关 Active Directory 中所定义的用户和组的信息。

此命令格式如下：

```
uxconsole -dbdump [table [item]]
```

table [*item*]

指定显示表格和项的内容。

注意：如果不指定表格名，此命令将显示所有可用的表格。

示例：显示存储在缓存中的所有 Active Directory 用户

下面的示例展示了如何显示存储在端点缓存中的所有 Active Directory 用户：

```
./uxconsole -dbdump pw
```

示例：显示存储在缓存中的所有 Active Directory 组

下面的示例展示了如何显示存储在端点缓存中的所有 Active Directory 组：

```
./uxconsole -dbdump -gr
```

uxconsole -debug—为模块设置详细级别

在 UNIX 上有效

使用该命令为每个模块设置详细级别。 UNIX 身份验证代理 也将 PAM 和 NSS 调试信息发送到文件。

此命令格式如下：

```
uxconsole -debug -m mod [-v level]
```

-m *mod*

指定设置详细级别的模块

选项： nss、pam、所有

-v *level*

定义详细级别。

限制： 0-5

UNIX 身份验证代理 将调试信息写入下列文件：

```
UNABInstallDir/log/debug/pam_debug
UNABInstallDir/log/debug/pam_debug.back
UNABInstallDir/log/debug/nss_debug
UNABInstallDir/log/debug/nss_debug.back
```

注意： 如果您将详细级别设置为超过 0，而代理未运行，那么您会收到消息，表示 UNIX 身份验证代理 PAM 模块已被激活。 UNIX 身份验证代理 仅将调试信息发送到 syslog。

uxconsole -verify—验证 Active Directory 用户帐户 UNIX 属性

在 UNIX 上有效

使用该命令验证 Active Directory 用户帐户已准备就绪由 UNIX 身份验证代理 使用。 该命令找到用户帐户，并验证 UNIX 身份验证代理 用户缓存数据库中存在的值与 UNIX 属性（登录 shell、主目录、UID 和 GID）值一致。

注意：该命令不验证用户密码。

此命令格式如下：

```
uxconsole -verify -user <user_name>[<user_name1>][<user_name2>...]
```

-user

指定在 Active Directory 中验证用户帐户 UNIX 属性

<user_name>

指定 Active Directory 用户帐户。

示例：验证 Active Directory 用户帐户 UNIX 属性

以下示例显示出如何验证 Active Directory 用户帐户 UNIX 属性：

```
./uxconsole -verify -user Joe
```

在该示例中，您使用 -verify 命令验证用户帐户 Joe UNIX 属性。 UNIX 身份验证代理 执行以下操作：

- 检查 /etc/shells 文件，验证登录 shell 是否指定为支持
- 验证用户名长度是否与操作系统实施的限制一致
- 验证是否指定主目录
- 验证是否指定 UID
- 验证是否指定 GID

uxconsole 如何发现 Active Directory 站点

在 Active Directory 中注册 UNIX 身份验证代理 端点时，默认情况下 uxconsole 实用程序会发现最近的 Active Directory 站点，并仅与此站点中的域控制器 (DC) 通讯。

下面的过程描述了 uxconsole 如何发现最近的 Active Directory 站点：

1. UNIX 身份验证代理 端点采用下列格式在 DNS 中查询 SRV（服务）记录：

   _ldap._tcp.dc._msdcs.*domainName*

   DNS 将返回域中 DC 的记录。

2. 端点通过绑定并验证到前面查询所返回的 DC 来访问 Active Directory。

   注意：端点可以绑定到任何一个返回的 DC。

3. 端点使用 LDAP 查询在 Active Directory 中搜索端点所在站点。 查询将使用以下筛选：

   - Base Dn—无值
   - Scope—基础
   - Attribute—Netlogon
   - DnsDomain—完全限定域名
   - ntver—6.00

   例如：Filter on (&(DnsDomain=example.company.com)(ntver=6.00))

   DC 将返回端点所在站点的名称。

   注意：DC 将使用端点 IP 地址来确定端点所在站点。

4. 端点采用下列格式在 DNS 中查询 SRV 记录：

   _ldap._tcp.*LocalSiteName*._sites.dc._msdcs.*domainName*。

   DNS 将返回端点所在站点中 DC 的记录。 端点仅与此站点中的 DC 通讯。

UxImport 实用程序－从 UNIX 操作系统中提取信息

在 UNIX 上有效

uximport 实用程序可从 UNIX 操作系统中提取有关所定义的用户、组、终端、主机和 TCP 服务的信息。 如果已安装，则它会从 NIS 中提取信息，并且会相应地对系统进行配置。 它还提供 DNS 支持。 应将 uximport 作为安装程序的一部分使用。

uximport 可自动处理所提取的信息，以生成可用于将用户和组添加到 CA Access Control 数据库的 selang 命令。 生成的命令将打印到标准输出中。 对文件使用重定向，或对 selang 实用程序使用管线。

此命令格式如下：

`UxImport switches [options]`

-a

生成导入用户、组和主机以及将用户加入其默认组所需的 selang 命令。

-c

生成将用户显式加入其默认组所需的 selang 命令。

注意：如果还使用 -g 开关参数导入组，CA Access Control 会生成相应命令，用于将用户加入其显式链接到的组。

--g

生成将组从 UNIX 和 NIS 导入 CA Access Control 数据库所需的 selang 命令。

-h

生成将主机从 UNIX、NIS 和 DNS 导入 CA Access Control 数据库所需的 selang 命令。 uximport 从文件 /etc/hosts 和 NIS 中提取主机信息，并构建 HOST 资源。 对于文件 /etc/hosts 中的或从 NIS 提取的每个主机条目，会构建相应的 newres 命令，并且会为该主机分配接收任何 TCP 服务的权限。

此外，-d 选项也支持 DNS。 在某些计算机中，如果指定的 DNS 后台进程正在运行，将忽略来自文件 /etc/hosts 和 NIS 的信息。 在 Solaris 中，搜集的信息取决于文件 /etc/nsswitch.conf 中的系统配置。

-t

生成将终端规则从 UNIX 和 NIS 导入 CA Access Control 数据库所需的 selang 命令。

uximport 从文件 /etc/hosts 和 NIS 中提取主机信息，并构建 TERMINAL 资源。 对于文件 */etc/hosts* 中的或从 NIS 提取的每个条目，会生成相应的 newres TERMINAL 命令，并授予从终端登录的权限。

此外，-d 选项也支持 DNS。 在某些计算机中，如果指定的 DNS 后台进程正在运行，将忽略来自文件 /etc/hosts 和 NIS 的信息。 在 Solaris 中，搜集的信息取决于文件 /etc/nsswitch.conf 中的系统配置。

-T

生成将 TCP 服务从 UNIX 和 NIS 导入 CA Access Control 数据库所需的 selang 命令。 根据 UNIX 中的 GECOS 设置名称。 如果名称超过 40 个字符，会被截短为 40 个字符。

-u

生成将用户从 UNIX 和 NIS 导入 CA Access Control 数据库所需的 selang 命令。根据 UNIX 中的 GECOS 设置实际用户名。如果名称超过 40 个字符，会被截短为 40 个字符。

options

-d

指定使用 DNS 生成要导入的主机和终端的列表。必须与 -h 或 -t 开关参数结合使用。

-f

跳过对同一名称多次出现的搜索。由于不使用标准的 uximport 进程，此选项可快速处理许多用户和组的导入，并可节省内存。-f 选项不适用于主机；应将它们与下列一个或多个开关参数结合使用：-u、-g 或 -a。 此外，如果包含与 -f 选项组合使用的 -c 开关参数，也应使用这些开关参数之一。

加入规则和替代规则与创建记录一起显示。

-G

为组创建 SURROGATE 类规则。 uximport 可将记录添加到它定义的每个组的 SURROGATE 类，从而使 SURROGATE 请求成为受保护的资源。此外，它还会添加规则，以便 root 用户可以代理每个组。

-gr *n*

为有用户指定宽限登录的次数，强制用户在 *n* 次登录之后更改他们的密码。 这可确保 USER 记录中的 PASSWD_L_C 属性得到更新

-o *owner*

为每个记录设置所有权规则。 建议您使用此项防止 root 用户自动成为全部记录的所有者。 *Owner* 是用户或组的名称，将为这些用户或组分配由 uximport 定义的所有记录的所有权。

注意：必须将此选项指定为后跟 *owner* 的独立参数。

-pr *groupname*

为用户分配配置文件组。如果指定此选项，则 CA Access Control 将在构建用户配置文件时使用该组；否则，它会使用主 UNIX 组。

-r

指定失败后继续扫描。

-s

为用户和组创建 SURROGATE 类规则。 uximport 函数可为它定义的每个组添加 SURROGATE 记录，从而使针对组的 SURROGATE 请求成为受保护资源。

-U

为用户创建 SURROGATE 类规则。 uximport 可为它定义的每个用户将记录添加到 SURROGATE 类，从而使 SURROGATE 请求成为受保护的资源。 此外，它还会添加规则，以便 root 用户可以代理每个用户。

--v

显示程序的状态（冗余模式）。 如果您的站点拥有许多用户、组或主机，建议您使用此选项，这样您便可以验证程序的进度。

示例

以下命令可从 UNIX 和 NIS 数据库中提取用户、组和主机的全部信息。 然后创建将这些记录添加到数据库的 selang 命令。 之后 uximport 会创建 SURROGATE 类记录并提供进度指示。 输出将定向到您主目录中的文件 uxinfo.seos。

```
UxImport -a -s -v > ~/uxinfo.seos
```

更多信息：

seerrlog 实用程序－显示错误日志记录 (p. 156)
selang 实用程序－运行 CA Access Control 命令行 (p. 164)
seuidpgm 实用程序－提取受托的程序 (p. 213)

uxpreinstall 实用程序—检查系统遵从性

在 UNIX 上有效

uxpreinstall 实用程序可验证 UNIX 端点是否符合 UNIX 身份验证代理 系统要求。 uxpreinstall 执行以下检查：

- 查询操作系统的安装版本、补丁、库以及模块
- 通过查询 DNS 服务器来解析域名
- 搜索 LDAP 和 Kerberos 服务
- 使用 LDAP 服务在 Active Directory 中查询信息
- 扫描可用端口
- 验证本地主机与 Active Directory 域之间是否存在时钟偏差
- 验证网络应用程序、网络服务器和 ssh 及 sshd 特征是否支持 Kerberized 单点登录 (SSO)

如果 uxpreinstall 实用程序发现严重错误，以至于无法执行后续检查，则该实用程序会立即停止。

uxpreinstall 运行后，会显示检查结果。 uxpreinstall 输出中的任何错误或冲突都可能导致 UNIX 身份验证代理 操作问题，例如用户身份验证失败。 强烈建议您在激活并使用 UNIX 身份验证代理 之前，先解决 uxpreinstall 所发现的任何错误或冲突。

重要说明！ uxpreinstall 实用程序会通知您真实或潜在的问题，但不会更正这些问题。 您不能使用该实用程序配置操作系统或 UNIX 身份验证代理。

在安装 UNIX 身份验证代理 前后均可运行 uxpreinstall。 如果在安装 UNIX 身份验证代理 之前运行 uxpreinstall，实用程序会创建临时 Kerberos 文件，并检查 Kerberos 文件的配置，而不是 uxauth.ini 配置。 如果在安装 UNIX 身份验证代理 之后运行 uxpreinstall，实用程序则不会创建临时 Kerberos 文件。 相反，它会检查 uxauth.ini 文件 [ad] 部分中 lookup_dc_list 标记的值。

注意：要在安装 UNIX 身份验证代理 之前运行 uxpreinstall，请从安装了 UNIX 身份验证代理 的另一个端点复制实用程序。

uxpreinstall 输出的下列部分检查端点配置是否允许 UNIX 身份验证代理用户使用 Kerberized SSO 登录。 如果不想为 UNIX 身份验证代理 用户启用 SSO 登录，可以忽略以下部分中的所有信息：

- 正在检查 KERBEROS RPM
- 检查本地 KERBEROS
- == 报告影响 SSO 操作的 sshd 特性 ==
- == 报告影响 SSO 操作的 ssh 特性 ==
- 检查网络应用程序
- 检查网络服务器

注意：有关使用 uxpreinstall 检查系统遵从性的详细信息，请参阅*《实施指南》*。

此命令格式如下：

```
uxpreinstall [-a user] [-w passwd] [-n ntp_server] [{-d domain | -s server}] [-p port] [-f logfile] [-v level] [-l] [-h]
```

-a *user*

定义用来登录到 Active Directory 的用户帐户。

默认值：Administrator

-w *passwd*

定义用户帐户的密码。

-n *ntp_server*

定义网络时间服务器 (NTP) 的名称。

-d *domain*

定义安装 Active Directory 的域名。

-s *server*

输入 Active Directory 服务器的名称。

-p *port*

定义 Active Directory 侦听的端口号。

-f *logfile*

定义要使用的日志文件的名称。

-v *level*

定义 uxpreinstall 输出的详细级别。

选项：

0—显示 uxpreinstall 所执行的检查以及所发现的任何错误或冲突的汇总。

1—显示与 0 选项相同的信息以及有关各项检查的附加信息。

2—显示与 1 选项相同的信息以及 uxpreinstall 对各项检查所用的命令。

3—显示与 2 选项相同的信息以及各命令的输出。

4—显示与 3 选项相同的信息以及一些检查的额外信息（例如：数据包详细信息）。

默认值：0

-l

指定对 syslog 文件执行检查。 仅适用于根用户。

-h

指定显示实用程序帮助和退出。

示例：运行 uxpreinstall 实用程序

此示例使用管理员用户凭据针对 Active Directory 域 mydomain.com 运行 uxpreinstall 实用程序，详细级别为 1：

```
/opt/CA/uxauth/bin/uxpreinstall -a administrator -w admin -d mydomain.com -v 1
```

示例：uxpreinstall 实用程序报告

下面是一段 uxpreinstall 实用程序报告，显示了如何确定系统是否满足系统要求：

```
检测到的操作系统：Linux 2.6.5-7.244-默认值
*********************************************
 检查时钟同步
*********************************************
正在将 DSE 中的 currentTime 属性值与本地时间进行比较 ...
当前的时钟偏差为 34 秒。
最大的时钟偏差的默认值为 300 秒。
警告！ 重大的时钟偏差可以导致用户身份验证失败
---------------------------------------------
 警告
---------------------------------------------
```

```
*****************************************
 检查通过 AD 的 KERBEROS 身份验证
*****************************************
principal_name = <Administrator@mydomain.com>

<Administrator@mydomain.com> 的 Kerberos 身份验证成功

-----------------------------------------
 成功
-----------------------------------------

*****************************************
 正在检查 AD 架构版本
*****************************************
正在尝试位于 server.mydomain.com:389 的服务
正在通过 'server1.mydomaiin.com' 绑定到 Active Directory ...

AD 架构版本 31（Windows Server 2003 R2 或 Windows Server 7 (AD LDS)）

支持全部和部分 UNAB 集成模式。
-----------------------------------------
 成功
-----------------------------------------
。 。 。
```

此示例中的输出显示了以下信息：

- 本地主机上运行的操作系统－Linux 2.6.5-7.244-default
- 时钟偏差－34 秒
- Kerberos 服务－<Administrator@mydomain.com> 的 Kerberos 身份验证成功
- Active Directory 架构版本－AD 架构版本 31
- 安装了 Active Directory 的操作系统版本－Windows Server 2003 R2 或 Windows Server 7
- Active Directory 架构支持完全和部分 UNIX 身份验证代理 集成模式

服务和后台进程详情信息

本部分包含所有 CA Access Control 后台进程和服务的完整参考，按字母顺序排列。

CA Access Control 代理管理器

在 Windows 上有效

CA Access Control 代理管理器服务向 CA Access Control 插件提供管理服务。 CA Access Control 代理管理器服务提供插件以及以下服务：

- 排定服务－管理插件排定。
- Watchdog 服务－确认插件在失败之后是否正在运行并启动插件。
- 发送消息服务－在企业管理服务器不可用的情况下，提供插件以及消息队列服务并存储消息。

代理管理器注册表键包含用于精细调整代理管理器的注册表项。 可以在下列位置找到注册表键：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager
```

CA Access Control 消息队列服务

在 Windows 上有效

CA Access Control 消息队列服务用于管理消息队列（TIBCO 服务器），这些消息队列可处理企业管理服务器与其他 CA Access Control 组件之间的所有入站和出站消息。 对于每个与企业管理服务器通讯的客户端组件，消息队列都有一个专用队列，这些队列如下：

- 报告队列－接收端点数据库的排定快照。

  报告服务使用这些快照来生成 CA Access Control 报告。

- 审核队列－接收在端点上发生的审核事件。

  您可以配置 CA Enterprise Log Manager 来收集和报告有关审核事件的情况。

- 服务器到端点队列－从 DMS 接收端点收集的数据。

  例如：在部署 UNAB 配置策略时，DMS 将配置策略发送到该队列。然后 UNAB 代理收集来自队列的策略，并在 UNAB 端点上部署此策略。

- 端点到服务器队列－从端点接收 DMS 收集的信息。

  例如：UNAB 端点将检测信号通知发送到此队列。 然后 DMS 从此队列收集检测信号通知，并在其数据库中更新端点状态。

CA Access Control Web 服务

在 Windows 上有效

Web 服务管理基于 Web 的应用程序，您将使用这些应用程序管理 CA Access Control 的企业安装。 基于 Web 的应用程序安装在应用程序服务器上。 应用程序服务器默认情况下安装在企业管理服务器上。

应用程序服务器包含以下基于 Web 的应用程序：

- CA Access Control 企业管理－允许您管理整个企业的策略并配置 UNIX 身份验证代理 端点。 CA Access Control 企业管理 还包含特权用户密码管理 (PUPM)，该组件用于管理整个企业的特权帐户，并充当特权帐户的密码存储库。
- CA Access Control 端点管理－允许您通过中央管理服务器管理和配置各 CA Access Control 端点。
- CA Access Control 密码管理器－允许您管理 CA Access Control 用户密码。 您可以修改 CA Access Control 用户的密码，或者强制用户在下一次登录时更改自己的密码。

WebService 注册表键中包含用于精细调整 Web 服务的注册表项。 可以在下列位置找到注册表键：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService
```

注意：如果在 UNIX 计算机上安装企业管理服务器，eacws 后台进程将管理基于 Web 的应用程序。

CA Identity Manager－连接器服务器 (Java) 服务

在 Windows 上有效

CA Identity Manager－连接器服务器 (Java) 服务用于管理与支持 Java 的受管设备（如 Windows 操作系统和 SQL Server）之间的通讯。 此服务还管理 特权用户密码管理 端点上的特权帐户。

eacws 后台进程

在 UNIX 上有效

eacws 后台进程用于管理基于 Web 的应用程序，您可以使用这些应用程序管理 CA Access Control 的企业安装。 基于 Web 的应用程序安装在应用程序服务器上。 应用程序服务器默认情况下安装在企业管理服务器上。

应用程序服务器包含以下基于 Web 的应用程序：

- CA Access Control 企业管理－允许您管理整个企业的策略并配置 UNIX 身份验证代理 端点。 CA Access Control 企业管理 还包含特权用户密码管理 (PUPM)，该组件用于管理整个企业的特权帐户，并充当特权帐户的密码存储库。
- CA Access Control 端点管理－允许您通过中央管理服务器管理和配置各 CA Access Control 端点。
- CA Access Control 密码管理器－允许您管理 CA Access Control 用户密码。 您可以修改 CA Access Control 用户的密码，或者强制用户在下一次登录时更改自己的密码。

注意：如果在 Windows 计算机上安装企业管理服务器，CA Access Control Web 服务将管理基于 Web 的应用程序。

KBLAudMgr 后台进程－会话日志记录

在 UNIX 上有效

KBLAudMgr 后台进程用于管理键盘记录器会话记录代理。 可使用键盘记录器在 UNIX 和 Linux 端点中跟踪特权用户会话。 键盘记录器会将记录交互式会话，这样，在这些会话终止后您可以进行重放，并将其发送到 CA Enterprise Log Manager 以进行分析和报告。

seos.ini 文件的 [kblaudit] 部分包含用于精细调整键盘记录器代理的标记。

PolicyFetcher 后台进程

在 UNIX 上有效

PolicyFetcher 后台进程会定期检查已部署策略中的偏差，在 DH 上查找部署任务，将策略更新应用于本地 CA Access Control 数据库 (seosdb)，并按固定时间间隔将检测信号发送到 DH。

可使用 start DEVCALC selang 命令来启动偏差计算器。 如果在端点上安装了高级策略管理，PolicyFetcher 会为您运行偏差计算器。

ReportAgent 后台进程

在 UNIX 上有效

ReportAgent 后台进程将管理 ReportAgent，该组件会将报告快照和审核事件发送到分发服务器，以便包含在 CA Access Control、UNIX 身份验证代理 和 CA Enterprise Log Manager 报告中。 在 UNIX 计算机上可从 *ACSharedDir*/bin 目录运行 ReportAgent 实用程序，其中 *ACSharedDir* 是默认目录 /opt/CA/AccessControlShared。 也可以使用 report_agent.sh 脚本来配置、启动和停止 ReportAgent。

accommon.ini 文件的 [ReportAgent] 部分包含用于控制报告代理后台进程行为的标记。

ReportAgent 服务 (Windows)

在 Windows 上有效

ReportAgent 服务将管理 ReportAgent，该组件会将报告快照和审核事件发送到分发服务器，以便包含在 CA Access Control、UNIX 身份验证代理和 CA Enterprise Log Manager 报告中。 如果在端点上安装了 CA Access Control 并选择安装 ReportAgent，在启动时会自动运行 ReportAgent 服务。

ReportAgent 注册表键中包含用于精细调整 ReportAgent 的注册表项。可以在下列位置找到注册表键：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent
```

sepmdd 后台进程 (UNIX)

策略模型后台进程。

sepmdd 后台进程是 PMDB 后台进程。 sepmdd 后台进程执行以下函数：

- 管理 CA Access Control 和策略模型的 UNIX 数据库。
- 管理订户的数据库。
- 它将更改从 PMDB 传播到订阅者数据库。

可以在 *ACInstallDir*/lbin 目录中找到 sepmdd 后台进程。 如果已创建，则它会启动 PMDB。

语法

```
sepmdd policyModel
```

参数

policymodel

策略模型的名称。

其他文件

不使用其他特殊文件。

注意：

使用 selang 并选择某个策略模型作为目标（使用主机 pmd@hostname）时，对 sepmdd 的查询会应用到 PMDB，但不会应用到各个订阅者数据库。

- 确保 PMDB 不会成为其自身的订户。 如果 PMDB 订阅它自己，则策略模型可能会阻塞或者网络可能会过载，从而在进程中填充磁盘。
- 当在 selang 的 UNIX 环境中更新策略模型时，即不能在 newusr 命令中指定多个用户，也不能在 newgrp 命令中指定多个组。
- 当从 selang 更新 UNIX 文件属性时，策略模型会生成一条消息，指出已将该命令传递至它的订阅者。
- 当在策略模型上工作时，无法查询 UNIX 文件属性的状态。
- 如果将 _shutoff_timeout_ 的值设置为零，则 sepmdd 后台进程仍保持启动状态并无限期地运行，直到您手动将其关闭。 可使用命令 sepmd -k 来关闭策略模型后台进程。

更多信息：

sepmd 实用程序 (p. 183)
sepmdadm 实用程序－创建 PMDB 定义 (p. 194)
seagent 后台进程 (p. 256)

sepmdd 的工作原理

CA Access Control 代理 seagent 会启动 sepmdd；无需显式运行 sepmdd。sepmdd 后台进程使用逻辑用户 id“_seagent”在 CA Access Control 中运行，使用用户 id *root* 在 UNIX 中运行。 您无法指定用于运行 sepmdd 的其他逻辑用户。

PMDB 存储在公用目录中。 在策略模型所在的站上，使用 seos.ini 文件 [pmd] 部分中的 _pmd_directory_ 标记，可指定公用目录的名称。 每个策略模型位于该公用目录的子目录中。 策略模型的名称是它所在的子目录的名称。

sepmdd 启动时，它会检查是否有任何订户数据库需要更新，并在必要时进行更新。 在此启动过程之后，sepmdd 会等待用户请求，这些请求由策略模型管理程序 sepmd 以及 selang 实用程序使用 seagent 发送。

sepmdd 接收到请求时，它会将请求应用到 PMDB 并将结果发回给用户。 如果需要传播该请求，sepmdd 会将更新传播给它的订阅者数据库。

sepmdd 后台进程将在 _QD_timeout_ 标记中指定的时间段内尝试更新订户数据库。 如果超出最长等待时间，但该后台进程无法成功更新某个订户，则它会忽略该订户，并尝试更新列表中的其余订户。 完成订户列表的首次扫描后，sepmdd 会接着执行第二次扫描，在这次扫描期间，它会尝试更新在第一次扫描期间未成功更新的订户。 第二次扫描期间，它将尝试更新订阅者，直到连接系统调用超时（大约 90 秒）。

注意： _QD_timeout_ 标记可以同时存在于 seos.ini 文件和 pmd.ini 文件中。 如果是这样，sepmdd 会使用 pmd.ini 文件中的值。

如果某个订阅者在第二次扫描期间不可用，sepmdd 会尝试每隔 30 分钟向它发送一次更新。 要修改此时间间隔，请设置 _retry_timeout_ 标记。 由于必须按照接收更新的顺序发送更新，因此 sepmdd 不会将后续更新发送给该订阅者数据库，直到它变为可用。

如果将订户数据库的 seos.ini 文件 [pmd] 部分中的 pull_option 标记设置为 yes，则会尽快更新该订户数据库。 seagent 会通知父策略模型：主机已为计算机上的每个策略模型启动，其订户 PMDB 已启动，sepmdd 会立即发送更新。

只要 sepmdd 无法更新订户数据库，它就会在策略模型错误日志中写入一条警告消息。 有关策略模型错误日志的详细信息，请参阅 *《适用于 UNIX 的端点管理指南》*。

在向策略模型中添加或删除订户时，CA Access Control 会尝试完全限定订户。

要从不可用订阅者列表中删除某个订阅者，请输入以下命令：

```
sepmd -r policyModel subscriber
```

如果订阅者数据库拒绝某个更新（如果订阅者数据库不同于 PMDB，可能会发生这种情况），sepmdd 会在策略模型错误日志中写入一条错误消息并继续。

要查看错误日志，请在 PMDB 所在的主机上输入以下命令：

```
sepmd -e policyModel
```

您可以让 sepmdd 在一段时间不活动后自动关闭。 但在默认情况下，sepmdd 不会自行关闭。 如果希望 sepmdd 自行关闭，可将 _shutoff_time_ 标记设置为大于 0 的值。 该值表明在 sepmdd 自行关闭前所允许的不活动时间（分钟）。 要手动关闭 sepmdd，请输入：

```
sepmd -k policyModel
```

重要说明！ *请勿*使用 UNIX 命令 *kill -9* 手动关闭 sepmdd；这样会损坏 PMDB。

UID/GID 同步

因为您可能会接收到按 UID 而非按用户名引用用户的消息，所以，知道每个用户的 UID 十分重要。 但是，如果您使用的是 PMDB，则无需关注如何为新用户分配 UID，用户在每台订户计算机上接收到的 UID 可能会有所不同。 因此，最好确保每个用户在任何位置都具有相同的 UID，对于 GID 也是如此。 请参阅*《适用于 UNIX 的端点管理指南》*中的 UID/GID 同步。

筛选机制

您可能希望 PMDB 有选择地更新它下面的订户工作站。 要定义将哪些记录发送到订户工作站，请将 pmd.ini 文件中的筛选标记指向一个筛选文件。 这样，会将对订阅者工作站的更新限制为通过筛选文件的记录。

筛选文件由每行具有六个字段的行组成。 这些字段包含以下信息：

- 允许或禁止的访问形式。 可能的值有 AUTHORIZE_DELETE、AUTHORIZE_MODIFY、CREATE、DELETE、DEPLOY、EDIT、FILESCAN、GET、SEOS_ACCS_READ、JOIN_DELETE、JOIN_MODIFY、MODIFY、READ、START 或 UNDEPLOY。
- 受影响的环境。 可能的值有 AC、CONFIG、UNIX、NT 或 NATIVE
- 记录的类。 可能的值包括 CA Access Control 中的所有类，其中包括用户定义的类。-
- 规则覆盖的类中的对象。 例如：User1、AuditGroup 或 TTY1
- 记录授予或取消的属性。 例如：用户记录的筛选行中的 OWNER 和 FULL_NAME 表示具有这些用户属性的任何命令都会被筛选。 必须准确输入每个属性。
- 此类记录是否应转发到订户工作站。
  可能的值有 PASS 或 NOPASS

您可以在任何窗口项中使用星号表示“所有可能的值”。如果有多个行涉及相同的记录，则使用第一个适用行。

在筛选文件的每一行中，空格分隔字段。 在具有多个值的字段中，使用分号分隔值。 任何以“#”开始的行均被视为注释行。 不允许有空行。 下面是某筛选文件中的某个行的示例：

CREATE	AC	USER	*	FULL-NAME;OBJ_TYPE	NOPASS
访问形式	*环境*	*类*	*记录名（* = 全部）*	*属性*	*处理*

例如：假设具有该行的文件名为 TTY1_FILTER，且策略模型 TTY1 的 pmd.ini 文件包含行 filter=/opt/CA/AccessControl//TTY1_FILTER。 策略模型 TTY1 不会发送通过 FULL_NAME 和 OBJ_TYPE（管理员、审核员等）创建新 CA Access Control 用户的记录。 星号表示“任何名称”。

以下是与每个访问值相关的 selang 命令：

访问	selang 命令
AUTHORIZE_DELETE	authorize--
AUTHORIZE_MODIFY	authorize-
CREATE	newres、newusr、newgrp、newfile
DELETE	rmres、rmusr、rmgrp、rmfile、join- (UNIX)
DEPLOY	deploy
EDIT	editres、editusr、editgrp、editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join-
MODIFY	chres、chusr、chgrp、chfile、join (UNIX)
READ	list
START	start devcalc
UNDEPLOY	deploy- (undeploy)

CA Access Control 不验证规则；因此，如果在某个规则中输入的值无效，该规则永远不会与更新事务匹配。

CA Access Control 策略模型服务 (sepmdd)

在 Windows 上有效

CA Access Control 策略模型服务 (sepmdd) 即 PMDB 服务。 它可执行以下函数：

- 管理 CA Access Control 和策略模型的 Windows 数据库
- 管理订户数据库
- 将更改从 PMDB 传播到订户数据库

SeOSAgent 启动 sepmdd 服务。 不需要显式运行 sepmdd。 每个策略模型的两个可能状态是“已启动”和“已停止”。

PMDB 存储在公用目录中。 注册表子键 HKLM\Software\ComputerAssociates\AccessControl\Pmd 中的注册表值 _pmd_directory_ 指定公用目录的名称。 每个策略模型位于该公用目录的子目录中。 策略模型的名称是它所在的子目录的名称。

当 sepmdd 启动时，它检查是否有任意订阅者数据库需要更新，如果需要，就更新它们。 在该启动进程后，sepmdd 服务等待用户的请求。 用户请求是通过策略模型管理实用程序 sepmd，以及通过使用 CA Access Control 代理的 selang 发送的。

当接收到某个请求时，sepmdd 将其应用到 PMDB，然后将结果发送回用户。 如果需要传播该请求，sepmdd 会将更新传播给它的订阅者数据库。

sepmdd 服务试图花费 30 秒时间来更新订阅者数据库。 如果时间已过而服务并没有成功更新订阅者，则它会忽略特定的订阅者，并尝试更新列表中的剩余订阅者。 完成订户列表的首次扫描后，sepmdd 会接着执行第二次扫描，在这次扫描期间，它会尝试更新在第一次扫描期间未成功更新的订户。 第二次扫描期间，它将尝试更新订阅者，直到连接系统调用超时（大约 90 秒）。

如果某个订阅者在第二次扫描期间不可用，sepmdd 会尝试每隔 30 分钟向它发送一次更新。

由于必须按照接收更新的顺序发送更新，因此 sepmdd 不会将后续更新发送给该订阅者数据库，直到它变为可用。

每次 sepmdd 更新订阅者数据库失败时，会在策略模型错误日志中写入警告消息。

筛选机制

您可能希望 PMDB 选择性地更新在其下面的订阅者工作站。 要规定哪些记录发送到订阅者工作站，请将注册表项字符串值设置到一个筛选文件中。 这样，会将对订阅者工作站的更新限制为通过筛选文件的记录。

下面是一个示例：

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd*PolicyModelName*\Filter

筛选文件由每行具有六个字段的行组成。 字段包含如下信息：

允许或禁用的形式

有效值包括：AUTHORIZE_DELETE、AUTHORIZE_MODIFY、CREATE、DELETE、DEPLOY、EDIT、FILESCAN、GET、SEOS_ACCS_READ、JOIN_DELETE、JOIN_MODIFY、MODIFY、READ、START 或 UNDEPLOY。

受影响的环境

有效值包括：AC、CONFIG、UNIX、NT 或 NATIVE。

记录的类

有效值包括 CA Access Control 中的所有类，其中包括用户定义的类。-

规则涵盖的类中的对象

例如：User1、AuditGroup 或 COM2。

记录授予或取消的属性

例如：将 GROUPS 和 FULLNAME 包括在用户记录的筛选行中意味着具有这些用户属性的任何命令都会被筛选。 必须按照显示准确输入每个属性。

这样的记录是否应该转发到订阅者工作站

有效值包括：PASS、NOPASS。

注意：可以在任意字段中使用星号表示“所有可能值”。 如果不止一行包括相同的记录，则使用适用的第一行。

在筛选文件的每一行中，空格分隔字段。 在具有多个值的字段中，使用分号分隔值。 任何以“#”开始的行均被视为注释行。 不允许有空行。 下面是某筛选文件中的某个行的示例：

CREATE	AC	USER	*	FULLNAME;OBJ_TYPE	NOPASS
访问的 access	环境	类	记录名（* = 全部）	属性	处理

例如：如果带有该行的文件名为 Printer1_Filter.flt，并且注册表键 HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd\PM-\Filter 包含行“C:\Program Files\CA\AccessControl\\data\Printer1_Filter.flt”，则策略模型 PM-1 不会发送以 FULLNAME 和 OBJ_TYPE（管理员、审核员等）创建新 CA Access Control 用户的记录。 星号表示“任何名称”。

与每个访问权限值相关的 selang 命令为：

访问	selang 命令
AUTHORIZE_DELETE	authorize--
AUTHORIZE_MODIFY	authorize-
CREATE	newres、newusr、newgrp、newfile
DELETE	rmres、rmusr、rmgrp、rmfile、join- (UNIX)
DEPLOY	deploy
EDIT	editres、editusr、editgrp、editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join-
MODIFY	chres、chusr、chgrp、chfile、join (UNIX)
READ	list
START	start devcalc
UNDEPLOY	deploy- (undeploy)

注意：CA Access Control 不验证规则；因此，如果在某个规则中输入的值无效，该规则永远不会与更新事务匹配。

注册表子键

每个 PMDB 在以下路径下都有其自己的注册表子键：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Pmd
```

此子键包含定义和确定 PMDB 活动的值。 如果子键尚不存在，则 sepmdd 实用程序会进行创建，并具有所需的最少项数。

Notes

- 使用 selang 并选择某个策略模型作为目标（使用主机 pmd@hostname）时，对 sepmdd 的查询会应用到 PMDB，但不会应用到各个订阅者数据库。
- 确保 PMDB 不会成为订阅者本身。 如果 PMDB 订阅它自己，则策略模型可能会阻塞或者网络可能会过载，从而在进程中填充磁盘。

- 如果在 UNIX 环境中工作时使用 selang 更新策略模型，则无法使用 newusr 命令指定多个用户。
- 如果在 UNIX 环境中工作时使用 selang 更新策略模型，则无法使用 newgrp 命令指定多个组。
- 当从 selang 更新 UNIX 文件属性时，策略模型会生成一条消息，指出已将该命令传递至它的订阅者。
- 当在策略模型上工作时，无法查询 Windows 文件属性的状态。
- sepmdd 服务会无限期地保持活动状态，直到利用 -k 选项停止该服务为止。

更多信息：

seagent 后台进程 (p. 256)
sepmd 实用程序 (p. 183)
sepmdadm 实用程序－创建 PMDB 定义 (p. 194)

seagent 后台进程

在 UNIX 上有效

seagent 后台进程可接受远程工作站的请求，并将它们应用到本地 CA Access Control 和 UNIX 数据库或应用到 PMDB。 它还将检查 Watchdog 后台进程 seoswd 是否正在运行，如果未运行，则重新启动该程序。

注意：加载 CA Access Control (seload) 时，也会启动 seagent；该后台进程不独立工作且无法使用 seagent 命令启动。

Seagent 将等待 seoslang 和 seoslang2 TCP 服务（它们的默认值分别为 8890 和 8891）上的连接。 连接请求到达时，seagent 会再生子进程以处理有关连接的通讯，并继续等待新连接。

seagent 的子进程获取客户端的请求，并将其应用到本地数据库。

代理还负责执行以下任务：

- 更新 UNIX 用户文件 /etc/passwd、系统的 shadow 密码文件以及 UNIX 组文件 /etc/group
- 在发送更新时提醒策略模型后台进程
- 在订阅者工作站（已经关闭）可用于更新时提醒本地主机和计算机上任何策略模型这两者的父策略模型

CA Access Control 只使用端口 8890 和 8891。 建议您不要更改这些端口。

seagent 代理使用 RPC 机制，因此，portmapper 必须在本地计算机上运行。 有关 portmapper 的其他信息，请查阅系统文档。

此命令格式如下：

```
seagent
```

更多信息：

seoswd 后台进程 (p. 263)
sepmdd 后台进程 (UNIX) (p. 248)

seauxd 后台进程

在 UNIX 上有效

seauxd 后台进程是 CA Access Control 的辅助后台进程，用于管理 Unicenter 日历更新。

要激活 seauxd，请将 TNG_calendars 配置设置的值设置为 yes。

seauxd 后台进程由 seosd 后台进程根据初始化设置启动。 seauxd 后台进程可执行以下函数：

- seosd 的分析请求
- Unicenter TNG 日历检索－要激活此函数，请将 seos.ini 文件 [seauxd] 部分中的标记 TNG_calendars 设置为 yes。 激活此函数后，seosd 会将 Unicenter TNG 日历的列表发送给 seauxd。 seauxd 后台进程将调用 Unicenter TNG、更新每个日历的状态并将更新过的日历列表返回给 seosd。

seos.ini 的 [seauxd] 部分包含许多内标识，使用这些内标识可以微调 seauxd 后台进程。

seosd 后台进程

在 UNIX 上有效

CA Access Control 授权后台进程。 可执行文件 seosd 是 CA Access Control 的主后台进程。 后台进程是已与其控制 TTY 和父进程断开连接的进程。 CA Access Control 后台进程将做出授权或拒绝对资源进行访问所需的运行时决策。

只有超级用户可以调用 seosd，只有拥有 ADMIN 或 OPERATOR 属性的用户可以关闭 seosd。

CA Access Control 后台进程将打开、读取并更新数据库。 当 CA Access Control 后台进程运行时，任何其他进程都无法访问该数据库。 CA Access Control 后台进程还将阻止对关键文件（如 CA Access Control 审核文件和跟踪文件，也可以包括 CA Access Control 二进制文件）进行任何写入、删除或重命名访问。

seosd 可执行文件仅在满足下面一个或所有两个条件时才成为后台进程：

- 不向屏幕发送跟踪消息；即，将 seos.ini 文件中的 trace_to 标记设置为 *file*、*file,stop* 或 *none*。
- 在调用实用程序时，在命令行中未指定任何参数（除 -d 外）。

如果这些条件均不满足，则 seosd 会保留一个常规进程，该进程与调用它时所使用的终端相连接。

在启动过程中，seosd 还将调用以下进程：

- seagent，CA Access Control 代理后台进程。
- seoswd，CA Access Control watchdog 后台进程。

仅当这些后台进程也在运行时，CA Access Control 后台进程才可以完全初始化。 初始化以后，这三个后台进程会保持一类信息交换协议，以确保它们全部处于活动状态并能够响应。 如果发现这些后台进程中有一个未活动，则另外两个后台进程之一会自动重新启动它。

此命令格式如下：

```
seosd [-d|argument]
```

注意：如果不使用参数输入 seosd，则它会作为后台进程运行 seosd。

argument

忽略。 但是，如果指定一个参数，seosd 仍为常规进程。

-d

将 seosd 作为后台进程运行，并强制跟踪 trace_file。

selogrcd 后台进程－收集审核记录

在 UNIX 上有效

CA Access Control 日志传递系统的后台收集程序。

注意：selogrcd 在仅 IPv6 环境中无法正常运行。

CA Access Control 日志传递后台进程 selogrd 和 selogrcd 可为系统管理员提供对审核日志记录的方便、有选择性的访问。

selogrcd 实用程序是收集后台进程。 此后台进程可收集由各种辅助系统发送的选定审核日志记录并将它们存储在审核收集文件中。 默认文件为 *ACInstallDir*log/seos.collect.audit。

两个标记可增强审核收集文件管理。 两个标记都在 seos.ini 文件的 [selogrd] 部分中

- 使用 Caudit_size 标记可指定审核收集文件的最大大小。 文件达到该大小时，CA Access Control 会创建一个备份文件并打开一个新文件。
- 使用 CbackUp_Date 内标识可为审核收集文件指定自动备份时间间隔和时间戳。

您可以通过向 selogrcd 发送 USR1 信号，强制它启动新的审核文件。 获得 selogrcd 进程 ID 后，便可以使用以下类似的 kill 命令向它发送 USR1 信号：

```
kill -USR1 processID
```

selogrcd 收到 USR1 信号时，会将现有的审核文件重命名为 *ACInstallDir*/log/seos.collect.bak，并创建一个新的审核文件。 您还可以使用 cron 作业定期执行该任务。 目录 *ACInstallDir*/samples/selogrcd 中提供了执行该任务的示例脚本。

注意：通过在使用随 CA Access Control 提供的 API 的站点编写程序，可以扩展 selogrcd 后台进程的功能。 有关详细信息，请参阅*《SDK 指南》*。

此命令格式如下：

```
selogrcd [-d] [-l lock-file-name]
```

-d

指定调试模式。 在此模式下，selogrcd 不会成为后台进程。 它会将调试信息发送到终端。

-h

显示该实用程序的帮助。

-l *lock-file-name*

指定要使用的锁定文件的名称 (*lock-file-name*)。默认情况下，selogrcd 将使用文件 *ACInstallDir*/lock/selogrcd。

注意：如果将 selogrd 设置为在其他日志文件（如 PMDB 日志文件）上运行，则锁定文件的扩展名基于用作 selogrd 命令 (p. 260)参数的 PMDB 名称或数据文件名称。

selogrd 后台进程—发出审核记录

在 UNIX 上有效

用于 CA Access Control 日志传递系统的发射器后台进程。

注意：selogrd 在仅 IPv6 环境中无法正常运行。

CA Access Control 日志传递后台进程 selogrd 和 selogrcd 可为系统管理员提供对审核日志记录的方便、有选择性的访问。

selogrd 实用程序是发射器后台进程。 该后台进程可将所选的本地审核日志记录分发到各个目标主机；将审核日志记录重新格式化为电子邮件、ASCII 文件或用户窗口；并可根据审核的事件发出通知消息。

注意：必须先启动并运行 CA Access Control 后台进程，日志传递后台进程才可以收集有关 CA Access Control 事件的任何有意义的信息。 如果 CA Access Control 后台进程并未运行，则 selogrd 只传递旧审核记录。

日志传递后台进程使用配置文件确定向何处发送每个审核日志记录、日志记录的编写格式以及要传递哪些记录。 默认情况下，selogrd 将使用 *ACInstallDir*/log/selogrd.cfg 审核日志传递配置文件。 selogrd 和 selogrcd 使用的配置文件和其他全局环境变量的名称在 CA Access Control 初始化文件 seos.ini 中指定。

selogrd 后台进程将定期重新启动并读取配置文件。 此外，可以强制 selogrd 后台进程在指定时间重新启动。 要执行此操作，必须发送以下 HUP 信号：

```
kill -HUP processID
```

processID

定义 selogrd 进程 ID。（使用 UNIX ps 命令查找它；请参阅 UNIX 文档以获取详细信息。）

selogrd 实用程序可为在 CA Access Control 中工作的程序员提供 API 访问。 LogRoute API 允许程序员将自己的选项并入 CA Access Control 审核日志系统，以支持并非由当前日志传递工具提供的内部报警。-- 通过 Logroute API，程序员还可以使用日志传递后台进程为自己的程序提供函数。 有关所有 CA Access Control API 的详细信息，请参阅*《SDK 开发人员指南》*。

此命令格式如下：

```
selogrd [-audit fileName] [-config fileName] [-d] \
    [-data fileName] [-pmdb policy-model-name]
```

-audit *fileName*

定义要用作输入审核文件的审核文件，而不使用在 seos.ini 中列出的文件。

-config *fileName*

定义要用作配置文件的配置文件，而不使用在 seos.ini 中列出的文件。

-d

指定打印调试消息。

-data *fileName*

定义要用于存储传递进度信息的数据文件，而不使用在 seos.ini 中列出的文件。

-h

显示该实用程序的帮助。

-pmdb *policy-model-name*

指示 selogrd 将审核数据从 PMDB 中传递到何处。 该命令可通知 selogrd 将审核数据从您在命令中指定的 PMDB 发送到您在 PMDB 的 pmd.ini 文件中的 audit_log 标记中指定的审核文件。

默认情况下，selogrd 将使用包含策略模型名称的数据文件和锁定文件。 如果您在命令行指定数据文件、锁定文件或两者，则这些文件会覆盖默认值。 锁定文件和数据文件的名称应该与 selogrd 传递工作站审核数据的这些文件的名称有所区别。selogrd 只支持 12 个字符的策略模型名称。

从 PMDB 发送的审核数据会显示在所收集的审核文件中，就好像它来自名为 policy-model-name@station-name 的工作站一样

更多信息：

审核日志传递配置文件 selogrd.cfg (p. 391)

seostngd 后台进程

在 UNIX 上有效

Unicenter TNG 的 CA Access Control 同步后台进程。

Unicenter 安全和 CA Access Control 共同负责在进行整体迁移前企业 IT 环境的管理。 为了降低使用不同产品工具执行管理任务的复杂性，我们提供了同步后台进程。

该后台进程称为 seostngd。 CA Access Control 通过 CA Common Communication Interface (CAICCI) 将策略模型数据库 (PMDB) 更新发送到 seostngd。 该后台进程在 CAICCI 上拦截更新，然后将消息转换成等效的 cautil 命令，以使用此全局数据更新 Unicenter 安全数据库。

当前的 Unicenter TNG 处理仍可更新其他 Unicenter TNG 客户端安装。 您必须在 Unicenter 安全数据库所在的计算机（通常指 Unicenter 主计算机）上运行 seostngd。CA Access Control 也应当在同一台计算机上运行。

此命令格式如下：

```
seostngd

seostngd {-stop|-shut}
```

seoswd 后台进程

在 UNIX 上有效

CA Access Control watchdog 后台进程。

Watchdog (seoswd) 可监控在数据库中被定义为受托程序的程序的文件信息和数字签名。 监控在后台执行，系统负载最小。 CA Access Control 代理后台进程 seagent 将自动启动 seoswd。

seoswd 后台进程执行下列函数：

- 监视您在数据库的 PROGRAM 类中定义的程序。 如果 watchdog 检测到程序经过修改，它会通知可将该程序标记为未受托的 CA Access Control 后台进程 seosd。 seosd 后台进程不允许未受托的程序运行。 seosd 后台进程还会在数据库中标记程序的状态更改为未受托，然后创建审核记录。
- 其监控被定义为安全文件的文件。 在数据库的 SECFILE 类中定义这些文件。
- 其监控 seosd 以确保它保持运行状态。 如果 watchdog 检测到 seosd 出现问题，会自动重新启动它。
- seoswd 后台进程检测到 seosd 已停止响应时，将使用系统日志 syslogd 通知安全管理员。 所有系统日志消息均作为 AUTH 工具进行提交。 有关系统日志工具的详细信息，请参阅 syslogd 和 syslog.conf 部分下的系统说明页面。
- 向 CA Access Control 报告若干事件，并为发现要更改的程序和安全文件创建审核记录。
- 通过它，可为可信任的程序和安全文件指定时间间隔和固定扫描日程。
- Watchdog 将忽略除 SIGHUP 以外的任何信号；除非先关闭 seosd，否则无法终止 seoswd 后台进程。 但是，如果执行命令 kill -SIGHUP *pid*，则 watchdog 会扫描数据库中所有受信任的程序和安全文件。

设置 Watchdog 扫描机制的方式有两种:

1. 确定开始时间，然后以给定时间间隔重复执行扫描。

   例如：检查受托的程序时，Watchdog 将在 *PgmTestStartTime* 启动第一次扫描，并检查所有受托的程序。 在上一次扫描开始后 *PgmTestInterval* 秒，将会进行再次扫描。

2. 在给定时间扫描。

注意：在这两种情况下，在每次扫描的过程中，Watchdog 都将在预定义的休息时间段（*PgmRest* 秒）内定期睡眠。 Watchdog 进行休息是为了防止系统过载。

您可以选择使用一种机制或同时使用两种机制。 例如：在 12:00 开始，每隔 4 小时扫描一次，并在 13:00 和 17:30 扫描。

除上述针对受托程序和安全文件的常规扫描机制外，还可以通过发送 HUP 信号按需执行一次性扫描（请参阅标记 SignalMinInterval）。

如果调用 seoswd 时不使用参数，则它会作为后台进程运行。 如果使用 -d 参数调用 seoswd，则它会作为后台进程运行，但会在执行调用的终端上显示所有调试信息。

更多信息：

seuidpgm 实用程序－提取受托的程序 (p. 213)

第 3 章： 配置文件

此部分包含以下主题：

accommon.ini 文件

accommon.ini 配置文件包含用于控制报告代理初始化进程的标记，以及用于控制常规通讯设置（例如：CA Access Control 企业管理 的 UNIX 身份验证代理 注册设置）的标记。 accommon.ini 文件分为以下几部分：

部分	说明
通讯	包含用于控制常规通讯设置的标记
global	包含 CA Access Control 全局设置
ReportAgent	包含用于控制报告代理设置的标记
AccountManager	包含控制客户经理设置的标记

通讯

在 [communication] 部分中，各标记用于控制通讯和加密选项。

Distribution_Server

定义分发服务器 URL。 可以在逗号分隔列表中定义多个分发服务器。

示例： tcp://ds.comp.com:7222, tcp://ds_dr.comp.com:7222

默认值： none

endpoint_to_server_queue

定义端点用来将信息发送到 CA Access Control 企业管理 的消息队列的名称。

默认值：ac_endpoint_to_server

server_to_endpoint_broadcast_queue

定义 CA Access Control 企业管理 用来对所有端点广播消息的消息队列的名称。

默认值：ac_server_to_endpoint_broadcast

server_to_endpoint_queue

定义 CA Access Control 企业管理 用来将消息发送到端点的消息队列的名称。

默认值：ac_server_to_endpoint

ServerVersion

定义分发服务器版本以实现前向兼容。

示例：12.01.0648

默认值：none

ssl_custom

指定是否使用主机名验证程序函数。

限制：0，不使用主机名验证程序函数；1，使用主机名验证程序函数

默认值：0

ssl_hostname

定义 SSL 主机名。

默认值：none

ssl_identity

定义报告代理的身份。

限制：到包含证书数据的文件的完整路径名。

默认值：none

ssl_issuer

定义对 SSL 连接的发布程序证书。

限制：到包含证书数据的文件的完整路径名。

默认值：none

ssl_key

定义报告代理私钥。

限制：到包含私钥的文件的完整路径名。

默认值：none

ssl_noverifyhost

指定是否启用主机证书验证功能。

限制：0，禁用主机证书验证；1，启用主机证书验证

默认值：0

ssl_noverifyhostname

指定是否启用主机名验证功能。

限制：0，禁用主机名验证；1，启用主机名验证

默认值：0

ssl_trace

指定是否启用 SSL 跟踪。

限制：0，禁用 SSL 跟踪；1，启用 SSL 跟踪

默认值：0

ssl_trusted

定义对 SSL 连接的受托证书。

限制：到包含证书数据的文件的完整路径名。

默认值：none

global

在 [global] 部分中，各标记用于控制 CA Access Control 端点的行为。

accommon_path

指定 accommon 目录的完整路径名。

默认值：/opt/CA/AccessControlShared/

AC_Version

定义端点上安装的 CA Access Control 的版本。

默认值：none

java_home

(Linux s390) 定义 Java 库的路径。

示例：对于 Linux390 计算机上安装的 IBM J2SE 版本 5.0 JRE，路径为 /opt/ibm/java2-s390-50/jre

默认值：none

ReportAgent

在 [ReportAgent] 部分中，标记控制报告代理后台进程 (ReportAgent) 的行为。

audit_enabled

指定是否要将端点审核数据发送到分发服务器。

值：0—否；**1**—是

默认值：0

audit_filter

定义包含筛选规则的文件的完整路径名，这些规则用于报告代理传递到外部来源（例如：CA Enterprise Log Manager）的审核记录。 此文件将确定报告代理传递哪些记录。

默认值：*ACSharedDir*/etc/auditrouteflt.cfg

audit_queue

定义报告代理向其发送端点审核数据的队列的名称。

默认：queue/audit

audit_read_chunk

定义报告代理尝试在每次读取审核文件时收集的最大审核记录数量。

限制：正整数。

默认值：300

audit_send_chunk

定义报告代理在每次连接中向分发服务器发送的最大审核记录数。当报告代理收集的审核记录数达到此值时，它会将这些记录发送到分发服务器。

限制：正整数

默认值：1800

audit_sleep

定义报告代理在生成审核报告间隔的睡眠持续时间。

限制：正整数代表数秒。

默认值：10

audit_timeout

定义报告代理必须将端点审核数据发送到分发服务器的周期。 如果自上次发送起经过的时间达到此数值，即使报告代理收集的记录数量少于 audit_send_chunk 值，仍会将审核数据发送到分发服务器。

限制：正整数代表数秒。

默认值：300

Debug

指定报告代理是否记录调试信息。

如果指定 yes (1)，报告代理会将以下内容记录到日志中：

- 将 CA Access Control 报告记录到 *ACSharedDir*/log/ac2xml.log
- 将 UNIX 身份验证代理 报告 (uxauthd) 记录到 *ACSharedDir*/log/unab2xml.log
- 将发送到 CA Enterprise Log Manager 的 CA Access Control 审核报告记录到 *ACSharedDir*/log/ac2elm.log
- 将发送到 CA Enterprise Log Manager 的 UNIX 身份验证代理 审核报告记录到 *ACSharedDir*/log/unab2elm.log
- 将发送到 CA Enterprise Log Manager 的键盘记录器报告记录到 *ACSharedDir*/log/kbl2elm.log

限制：0，报告代理不记录调试信息；1，报告代理记录调试信息

默认值：0

elm_event_interval

定义报告代理向 CA Enterprise Log Manager 发送用户会话审核事件的时间间隔（秒）。

限制：0；无时间间隔，在消息大小超出 elm_max_msg_size 标记中指定的值时发送审核事件；任意正整数。

默认值：60

elm_max_msg_size

定义报告代理向 CA Enterprise Log Manager 发送的键盘记录器消息的最大大小（字节）。

值：任意正整数

默认值：300000

interval

定义 CA Access Control 生成报告并将报告发送到分发服务器的时间间隔（分钟）。

*排定*设置用于定义时间间隔开始的时间以及它运行的天数。 如果报告代理启动时间晚于排定时间，它将在下个计算的时间间隔（从排定起）发送一个报告，然后在排定天数后的定义时间间隔发送一个报告。

示例：如果 schedule = 8:30@Mon,Tue,Wed，interval = 5，则报告代理将在星期二上午 8:47 加载，报告代理将在上午 8:50 生成并发送报告。这是使用 5 分钟时间间隔从排定开始时间计算出的最早周期。

值：**0**—无时间间隔（仅使用排定发生时间）； *正整数*—用作时间间隔的分钟数

默认值：0

reportagent_enabled

指定是否在本地计算机上启用报告 (1)。

默认值：0

schedule

定义生成报告并将其发送到分发服务器的时间。

您可以使用以下格式指定设置：time@day[,day2][...]

例如：“19:22@Sun,Mon”可在每个星期日和星期一晚上 7:22 生成报告。

默认值：00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

send_queue

定义分发服务器上报告队列的名称，报告代理向该队列发送本地数据库和任何 PMDB 的快照。

默认值：queue/snapshots

更多信息：

auditrouteflt.cfg 文件—筛选审核记录传递 (p. 383)

AccountManager

在 [AccountManager] 部分中，标记控制客户经理插件的行为。

OperationMode

定义 AccountManager 插件是否插入被启用或禁用。

选项：1，启用插件，0，禁用插件

默认值：1

PluginPath

定义 AccuntManager 插件的完整路径名。

默认值：/opt/CA/AccessControlShared/lib/AccountManager.so

ScheduleType

定义 AccountManager 插件排定类型。

选项：

- 0－运行一次
- 1－按需运行
- 2－每 N 秒运行
- 3－依照排定字符串运行：
  00:00@Sun.Mon,tue,Wed,Thu,Fri,Sat

默认值：2

时间间隔

指定 AccountManager 插件时间间隔（秒）

默认值：300

注意：如果您将 ScheduleType 控件值设置为 2，则适用。

排定

指定 AccountManager 插件排定字符串。

默认值：00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

注意：如果您将 ScheduleType 控件值设置为 3，则适用。

QueryFilter

指定添加到消息队列接收队列筛选的自定义值

选项：

- "ENDPOINT_CUSTOM1="
- "ENDPOINT_CUSTOM2="
- "ENDPOINT_CUSTOM3="
- "ENDPOINT_CUSTOM4="
- "ENDPOINT_CUSTOM5="
- "ENDPOINT_OWNER="
- ENDPOINT_DEPARTMENT="

默认值：无值

注意：您可以使用多个自定义属性，使用 AND 操作数。

示例：“ENDPOINT_DEPARTMENT='Finance' AND 'ENDPOINT_CUSTOM1=Accounting'”

重要说明！ 在指定自定义属性时，请验证：

- 您使用撇号来指定属性值
- 指定多个属性时，您使用 AND、OR 操作数
- 使用 OR 操作数时，您使用括号

kblaudit.cfg—筛选键盘记录器审核记录

在 UNIX 上有效

kblaudit.cfg 文件通过定义发送到审核文件的记录来筛选主机上的审核记录。 每行均代表筛选出审核信息的一条规则。 您配置的筛选规则适用于 kbl.audit 文件。

默认情况下，kblaudit.cfg 文件位于以下目录：

```
/opt/CA/AccessControl/etc
```

kblaudit.cfg 文件包含两个部分，即 [EXCLUDE] 和 [INCLUDE]，帮助您筛选键盘记录器审核记录。 每个部分包含表示筛选规则的条目。

示例：kblaudit.cfg 筛选部分

kblaudit.cfg 文件的以下片段是您编辑 kblaudit.cfg [EXCLUDE] 和 [INCLUDE] 部分的方式的示例：

```
[EXCLUDE]
TRACE;*;*;test_user; test_user; test_user;*;*seos.ini*
[INCLUDE]
TRACE;*;*; test_user; test_user; test_user;*;*AccessControl*
```

在该示例中，您从 kbl.audit 文件排除审核记录（用户 test_user 执行的 seos.ini），并包括用户 test_user 在 Access Control 中执行的记录。

使用 kblaudit.cfg 文件筛选出以下审核事件类型的记录（每种类型使用的语法不同）：

- 登录事件 (p. 273)
- 有关用户的跟踪消息 (p. 274)

注意：在每种语法类型的任意列中，* 均表示“任意值”。

Kblaudit.cfg－登录事件筛选语法

在 UNIX 上有效

属于登录事件的审核记录具有以下筛选格式：

LOGIN;*UserName*;*UserId*;*TerminalName*;*LoginProgram*

登录

指定该规则筛选用户跟踪记录。

用户名

定义访问者的名称。

UserId

定义访问者的本地用户 ID。

TerminalName

定义事件发生的远程主机名。

LoginProgram

定义尝试登录或注销的程序名称。

限制：cmdlog

kblaudit.cfg－关于用户事件筛选语法的跟踪消息

在 UNIX 上有效

属于有关用户事件的跟踪消息的审核记录具有以下筛选格式：

TRACE;*TracedClassName;TracedObjectName;RealUserName;ACUserName;AuthorizationResult;TraceMessageMask;KBLSessionID*

TRACE

指定该规则筛选用户跟踪记录。

TracedClassName

定义用户尝试访问的对象类的名称。

选项： KBL 原始、KBL 输出、KBL 输入、KBL execargs

TracedObjectName

定义用户尝试访问的对象的名称。

RealUserName

定义生成跟踪记录的登录用户的名称。

ACUserName

定义生成跟踪记录的有效用户的名称。

AuthorizationResult

定义授权结果。

值： P（已允许）、D（已拒绝）、*

TraceMessageMask

定义生成的跟踪消息。

KBLSessionID

显示键盘记录器会话 ID

seos.ini 初始化文件

在 UNIX 上有效

seos.ini 文件包含 CA Access Control 使用的各种设置和初始化标记。 每个标记在文件中占用一行，格式如下：

token = *value*

在各部分中，包含 CA Access Control 特定实用程序、后台进程或其他工具标记的行分组到一起。 每部分都以一个标题行开始，在方括号内提供该部分名称。 每个标记都属于一个部分。 例如：以下行就是管理 serevu 实用程序的部分的开头：

```
[serevu]
```

安装的 seos.ini 文件由 CA Access Control 保护，且在 CA Access Control 正在运行时无法更新。 默认情况下在 CA Access Control 中定义的文件具有读取权限，因为许多实用程序在处理期间访问该文件。 如果它们无法读取 seos.ini 文件，则将失败。

CA Access Control 正在运行时，输入以下 selang 命令以便允许授权用户更新文件：

```
newres FILE /opt/CA/AccessControl//seos.ini owner(authUser)
```

其中 *authUser* 是授权用户的名称。 该命令建立 *authUser* 是文件的所有者，作为文件的所有者，*authUser* 总是可以更新它。

您可以使用 CA Access Control 端点管理 或 seini 实用程序以读取、添加、修改和删除初始化文件中的标记。

注意：seini 实用程序只能在 seosd *未*运行或数据库中的规则明确允许时才能更新 seos.ini 文件。

使用 *secons -rl* 命令，可以重新加载具有更新标记的 seos.ini 文件，而无需重新启动 seosd 后台进程。

下表列出了 seos.ini 文件中的所有部分。

部分	说明
AccountManager	多个 JCS 端点模块
AgentManager	CA Access Control 插件管理
crypto	加密模块库设置。

部分	说明
daemons	seload 实用程序自动运行的 CA Access Control 后台进程列表。
Dependency	产品列表，这些产品使用 CA Access Control 作为嵌入的组件，由用户定义。
devcalc	策略偏差计算器 (devcalc) 设置。
kblaudit	键盘记录会话跟踪设置。
lang	CA Access Control 管理接口 (selang) 设置。
ldap	用于 LDAP 示例退出 的 LDAP 服务器设置。
logmgr	记录工具设置。
message	消息文件设置。
mfsd	大型机同步后台进程 (mfsd) 设置。
OS_user	企业用户存储使用设置。
package	已安装的 CA Access Control 包的列表。
pam_seos	可插拔验证模块 (PAM) 编程接口设置。
passwd	密码替换以及与用户相关的服务设置。-
pmd	公用策略模型数据库设置。
policyfetcher	策略提取器后台进程 (policyfetcher) 设置。
PUPMAgent	特权用户密码管理 后台进程 (pupmagent) 设置。
seagent	seagent 后台进程设置。
seauxd	用于 Unicenter 日历更新的辅助后台进程 (seauxd) 设置。
segrace	用户登录信息实用程序 (segrace) 设置。
seini	配置文件管理实用程序 (seini) 属性。
selock	桌面非活动状态保护实用程序 (selock) 设置。
selogrd	日志传递后台进程（selogrd 和 selogrcd）设置。
seos	全局配置设置。
SEOS_syscall	SEOS_syscall 内核模块设置。
seosd	授权后台进程 (seosd) 设置。
seosdb	数据库检查和重建设置。
seoswd	Watchdog 后台进程 (seoswd) 设置。

部分	说明
serevu	失败登录尝试次数解决方案实用程序 (serevu) 实用程序设置。
sesu	CA Access Control 开关参数用户实用程序 (sesu) 设置。
sesudo	CA Access Control 代替用户执行实用程序 (sesudo) 实用程序设置。
standalone	独立计算机管理设置。
tcp_communication	公用 TCP 连接设置。
tng	CA Access Control 与 Unicenter 设置集成。

AgentManager

在 [AgentManager] 部分中，标记控制与 CA Access Control 插件管理关联的各个方面。

exclude_endpoint_types

指定客户经理不管理的端点类型的以逗号分隔的列表。

Interval

定义插件排定，以秒为单位。

默认值： 1

注意： 只有在 ScheduleType 设置为 2 时适用。

max_threads_count

指定池中工作线程的最大数目。

默认值： 10

OperationMode

定义插件操作模式。

选项： 0－插件已禁用，1－插件已启用

默认值： 1

Plugins

指定 CA Access Control 代理管理器使用的插件。

默认值： AccountManager、Heartbeat、Policyfetcher

PluginPath

定义插件的完整路径名。

默认值： /opt/CA/AccessControlShared/lib/Heartbeat.so

RefreshTimeout

定义插件刷新超时。

默认值： 10

Schedule

定义插件的排定字符串。

默认值： 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

注意： 只有在 ScheduleType 设置为 2 时适用。

ScheduleType

定义插件排定类型。

选项： 0－执行一次，1－按需执行，2－间隔执行，3－按排定执行

默认值： 1

TraceEnabled

定义 CA Access Control 代理管理器跟踪模式。

选项： 0、1

默认值： 1

注意： 跟踪消息在以下位置：<WorkSpace>/AgentManager.log 文件中记录。

WorkSpace

指定 CA Access Control 代理管理器工作区的完整路径名。

默认值： /opt/CA/AccessControlShared/data/AgentManager

AccountManager

在 [AccountManager] 部分中，标记控制与多个 JCS 管理关联的各个方面。

时间间隔

定义插件排定，以秒为单位。

默认值：1

注意：只有在 ScheduleType 设置为 2 时适用。

OperationMode

定义插件操作模式。

选项：0－插件已禁用，1－插件已启用

默认值：1

PluginPath

定义插件的完整路径名。

默认值：/opt/CA/AccessControlShared/lib/AccountManager.so

QueryFilter

指定添加到消息队列的其他值，以接收队列筛选。

选项：ENDPOINT_CUSTOM 1...5=, ENDPOINT_OWNER=, ENDPOINT_DEPARTMENT=

请注意下列事项：

- 将属性值放置在撇号中
- 使用 AND 和 OR 操作数指定多个单个属性
- 需要时使用括号

排定

定义插件的排定字符串。

默认值：00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

注意：只有在 ScheduleType 设置为 2 时适用。

ScheduleType

定义插件排定类型。

选项：0－执行一次，1－按需执行，2－间隔执行，3－按排定执行

默认值：1

crypto

在 [crypto] 部分中，与加密模块关联的标记控制方面。

ca_certificate

定义证书颁发机构 (CA) 证书数据库的完整路径名。

默认值：*ACInstallDir*/data/crypto/def_root.pem

communication_mode

指定是否启用安全套接字层 (SSL) 协议。

如果将此项设置为 ssl_only，则仅启用 SSL V2、SSL V3 和 TLS 连接。这意味着此计算机无法与不支持 SSL 的计算机通讯，因此无法与运行 CA Access Control r12.0 之前版本的计算机通讯，这些版本不支持 SSL。

注意：运行 CA Access Control r12.0 及更高版本的计算机支持 SSL。

如果将 fips_only 标记设置为 1，则在 FIPS 模式（即 TLS）下实际的通讯模式设置为 ssl_only，且忽略 communication_mode 标记。

有效值包括：

- all_modes
- ssl_only
- non_ssl

默认值：non_ssl

CAPKIHOME

定义 CAPKI 的安装目录。

默认值：/opt/CA/SharedComponents/CAPKI

encryption_methods

指定 CA Access Control 代理用来解密消息的加密库。代理会依次尝试使用列表中的每个库，直到解密成功。

限制：libaes256、libaes192、libaes128、libdes、libtripledes、libscramble

默认值：libaes256、libaes192、libaes128、libdes、libtripledes

fips_only

此标记用于控制 CA Access Control 是否以仅 FIPS 模式工作。 在此模式下，禁用所有非 FIPS 函数。

有效值:

1 CA Access Control 以仅 FIPS 模式工作

0 CA Access Control 以非 FIPS 模式工作

默认值：0

LIBRARY_PATH

定义 ETPKI 加密库的目录。

private_key

定义主题私钥的完整路径名。

默认值：*ACInstallDir*/data/crypto/sub.key

ssl_port

定义 CA Access Control 客户端和服务之间的 SSL 通讯端口。

默认值：5249

subject_certificate

定义主题证书的完整路径名。

默认值：*ACInstallDir*/data/crypto/sub.pem

后台进程

在 [daemons] 部分中，每个标记都用于指定 seload 实用程序是否（如果是，如何）从 CA Access Control 安装目录中执行特定的程序。 每个标记名称或者对应一个 CA Access Control 后台进程名称，或者是程序昵称，可以为其分配多个值。

program-name

指定两种可能性之一：

- 与以下设置匹配的后台进程或其他程序的名称：
  - 值为 *yes*，则 seload 将使用默认参数运行该程序
  - 值为 *no*，则 seload 不会运行该程序
  - 一组参数，则 seload 将使用这些参数运行该程序

  例如：输入以下命令将使用默认参数从 CA Access Control 安装目录中运行 serevu：

  ```
  serevu=yes
  ```

  输入以下命令阻止运行 serevu；这与不使用 serevu 内标识是相同的。

  ```
  serevu=no
  ```

  输入以下命令将使用指定的参数从 CA Access Control 安装目录中运行 serevu：

  ```
  serevu=-f 3 -d 6m -t 1m -s 5m
  ```

- 虚拟字符串（需与后台进程或其他程序的绝对路径名相匹配，后跟可选参数），则 seload 将相应地运行该程序。

  例如：输入以下命令将使用指定的参数运行位于 /opt/CA/AccessControl//bin 目录中的 serevu 实用程序：

  ```
  run_it=/opt/CA/AccessControl//bin/serevu -f 3 -d 6m -t 1m
  ```

  要包括多个程序的规范，请对每个程序都使用一次该内标识。

默认值：no

注意：您无需指定 seosd 后台进程。 Seload 可始终确保 seosd 后台进程处于运行状态。

Dependency

在 [Dependency] 部分中，用户定义的每个标记都指定了将 CA Access Control 用作嵌入式组件的产品。

product-name

指定将 CA Access Control 用作嵌入式组件的产品。 有效值包括：

0－不是嵌入式产品

1－嵌入式 CA Access Control 产品。

默认值：未指定任何默认产品。

devcalc

在 [devcalc] 部分中，标记控制与策略偏差计算关联的方面。

dms_command_retry_interval

定义每个 DMS 通知命令重试之间的时间间隔（秒）。

默认值：60

init_ac_db

过时。

max_dms_command_retry

定义在放弃操作之前，策略偏差计算器重试向 DMS 发送更新通知的最多次数。

默认值：3

max_lines_request

定义 *get devcalc* selang 命令任意一次返回的最大行数（从策略偏差数据文件中）。 然后，您还需要使用以下命令检索其他行：

```
get devcalc params("offset=X")
```

x

定义上一个 *get devcalc* 输出返回的行偏移量。

默认值：50

kblaudit

[kblaudit] 部分中的标记用于控制键盘记录器会话跟踪程序的行为。

audit_back

指定键盘记录器备份审核日志文件的名称。

默认值：*ACInstallDir*/log/kbl.audit.bak

audit_group

指定可读取审核日志的组。 如果将该标记设置为 **none**，则只有 root 用户可以读取审核日志。 CA Access Control 不会验证该标记值，因此如果您输入了无效的组名，CA Access Control 就不会将任何组权限分配到审核日志文件。

要更改现有审核日志文件的组所有权，请完成以下步骤：

使用 selang 命令 chgrp 设置文件的组所有权。

通过输入以下命令，更改 UNIX 权限：

```
chmod 640 ACInstallDir/log/seos.audit
```

默认值：none

audit_log

指定键盘记录器审核日志文件的名称。

默认值：*ACInstallDir*/log/kbl.audit

audit_max_files

指定备份模式中最多保留的审核日志文件数。 达到此数目时，CA Access Control 在创建最新的备份文件时会删除最早的文件。

限制：正整数。

默认值：0

注意：设置为 0 时，CA Access Control 会累积备份文件而不会删除较早的文件。

audit_size

指定审核日志文件的最大大小 (KB)。

最大值：50 KB。

默认值：24000

注意：在审核文件大小超过 2 GB 时，CA Access Control 会停止将审核记录写入审核文件。

BackUp_Date

指定 CA Access Control 备份审核日志文件的条件，以及 CA Access Control 是否在备份文件名中添加时间戳。

CA Access Control *始终*在审核日志文件达到 audit_size 配置设置中指定的大小时备份该文件。

值：none、yes、daily、weekly 和 monthly。

- yes－CA Access Control 在审核日志文件达到 audit_size 中指定的大小时对其进行备份，并在备份文件名中添加时间戳。
- none－CA Access Control 在审核日志文件达到 audit_size 中指定的大小时对其进行备份，但不在备份文件名中添加时间戳。
- daily、weekly、monthly－只要达到指定的时间间隔*且*审核日志文件达到 audit_size 中指定的大小，CA Access Control 就会备份审核日志文件，并在备份文件名中添加时间戳。 但是，如果在指定时间间隔内没有审核事件写入审核日志文件，则 CA Access Control 不会在经过该时间间隔后备份文件。

  注意：CA Access Control 从第一个审核日志文件的创建时间起计算指定的时间间隔，并在相应日期的午夜备份文件。

示例：该配置设置的值为 weekly，并且 CA Access Control 在 4 月 1 日星期五上午 9:00 创建了审核日志文件。 在这一周发生了许多审核事件，审核日志文件在 4 月 4 日星期一超过了 audit_size 配置设置。 CA Access Control 在 4 月 4 日备份审核日志文件，并在备份文件名中添加时间戳。 在第一次创建审核日志文件之后的一周，即 4 月 8 日星期五的午夜，CA Access Control 再次备份审核日志文件，并在备份文件名中添加时间戳。

默认值：NONE

cmd_log

指定与键盘记录器 cmdlog 二进制文件的链接。

默认值：/etc/AC

error_back

指定键盘记录器错误日志备份文件的名称。

默认值：*ACInstallDir*/log/kbl.error.bak

error_group

指定可读取错误日志文件的组。 如果将此标记设置为 **none**，则只有 root 用户可以读取错误日志文件。 CA Access Control 不会验证该标记值，因此如果您输入了无效的组名，CA Access Control 就不会将任何权限分配到错误日志文件。

要更改现有错误日志文件的组所有权，请完成以下步骤：

使用 selang 命令 chgrp 设置文件的组所有权。

通过输入以下命令，更改 UNIX 权限：

```
chmod 640 ACInstallDir/log/seos.audit
```

默认值：none

error_log

指定键盘记录器错误日志文件的名称。

默认值：*ACInstallDir*/log/kbl.error

error_size

定义错误日志文件的最大大小 (KB)。

限制：最小值为 50 KB。

默认值：500

kbl_enabled

指定是否启用键盘记录器。

值：yes、no

默认值：no

kbl_flush_timeout

指定用户会话非活动状态的时间间隔（秒），在此间隔后可打印的记录数据将存储在 kbl 审核文件中。 将此标记设置为 0 可将其禁用。

默认值：30

Kbl_seos_trace

指定 seosd 是否在会话上激活跟踪，并将用户活动数据发送到键盘记录器。

值：yes、no

默认值：yes

OS_etc_shells

指定操作系统 shell 文件的名称。

默认值：/etc/shells

socket_name

指定键盘记录器审核管理器的套接字名称。

默认值：*ACInstallDir*/kblserver

lang

在 [lang] 部分中，标记指定 selang 命令语言程序所使用的属性：selang、Security Administrator 和 seadm。

check_password

确定 selang 是否请求用户指定他们各自的密码。 有效值包括：

no－selang 不要求输入任何密码

yes－系统提示用户输入他们的密码。

默认值：no

exit_timeout

指定 CA Access Control 允许 exit 程序执行的最大时间（秒）。 此时间过去后，CA Access Control 将会关闭 exit 程序。

默认值：30

exits_dir

指定 *ACInstallDir*/lbin/install_exits.sh shell 脚本将 exit 安装到的目标目录。

默认值：*ACInstallDir*/exits

exits_source_dir

指定 *ACInstallDir*/install_exits.sh shell 脚本要安装 exit 的源目录。

默认值：*ACInstallDir*/samples/exits-src

help_path

指定 lang 帮助文件所在的目录。

默认值：*ACInstallDir*/data/langhelp

language

定义安装 CA Access Control 所使用的语言（供内部使用）。

默认值：english

max_groups_buffsize

指定安全管理员与数据库进行通讯时所使用的缓存大小 (KB)。 该内标识在需要应用 UNIX 更新时使用。

默认值：128

no_check_password_users

指定不要求输入其密码的用户。

仅当内标识 **check_password** 设置为 yes 时，该内标识才有意义：

有效值包括以逗号分隔的用户列表。

默认值：none

passwd_copy

指定在更改用户信息后将临时文件复制回原文件时，如何更新计算机密码文件 (/etc/passwd) 或 PMDB 密码文件 (*/PMDB_Directory*/policies/pmdb/ passwd)。有效值包括：

fast_copy－复制文件中的信息。

rename－将目录更改为指向新文件。

默认值：fast_copy

post_group_exit

指定在 UNIX 环境中执行组命令之后调用的 exit 程序的路径。

默认值：*ACInstallDir*/exits/lang_exit.sh

post_user_exit

指定在 UNIX 环境中执行用户命令之后调用的 exit 程序的路径。

默认值： *ACInstallDir*/exits/lang_exit.sh

pre_group_exit

指定在 UNIX 环境中执行组命令之前调用的 exit 程序的路径。

默认值：*ACInstallDir*/exits/lang_exit.sh

pre_user_exit

指定在 UNIX 环境中执行用户命令之前调用的 exit 程序的路径。

默认值：*ACInstallDir*/exits/lang_exit.sh

query_size

指定数据库查询中要列出的最大记录数。

默认值：100

RecvTimeOut

指定 selang 在超时前等待接收信息的最长时间（秒）。

如果将该值设置为 0，则不会有超时。

默认值：60

SendTimeOut

指定 selang 在超时前等待发送信息的最长时间（秒）。

如果将该值设置为 0，则不会有超时。

默认值：60

SetBlockRun

指定是否检查程序受信任与否，以及是否阻止执行不受信任的程序。无论程序是 setuid 还是常规程序，都会阻止执行它。

有效值包括以下各项：

yes－采用 viapgm 授权规则定义的所有程序都将 blockrun 属性设置为 yes。

no－采用 viapgm 授权规则定义的所有程序都将 blockrun 属性设置为 no。

suid－所有的 setuid 程序都将 blockrun 属性设置为 yes，而所有其他程序都将 blockrun 属性设置为 no。

默认值：yes

swap_deletion_order

定义在 selang 中执行“ru *userName* unix”命令（用户删除）的顺序。此命令通常先在 AC 环境中执行，然后在 UNIX 环境中执行。 某些情况下（例如：组管理员删除用户时），需要颠倒此顺序。

有效值包括：

no－先从 AC 环境中删除用户，然后从 UNIX 环境中删除用户。

yes－先从 UNIX 环境中删除用户，然后从 AC 环境中删除用户。

默认值：no

timeout

指定客户端等待 seosd 后台进程响应的最长时间（秒）。如果 seosd 在此时间段内未响应，则系统将发送一条错误消息，说明 seosd 未响应。之后，该客户端会停止尝试连接至 seosd。

默认值：90

use_old_commands

指定是否禁用旧的 ACF2™ 兼容性命令（ag、lg、rg、lu、au 等）。

限制：0－不支持旧命令，1－支持旧命令

默认值：1（支持旧命令）

use_unix_file_owner

指定文件的 UNIX 所有者是否可以将该文件定义至 CA Access Control。如果该值为 yes，则 UNIX 中的文件所有者可以使用 newres 或 newfile 命令将该文件定义至 CA Access Control。

如果已将该文件定义至 CA Access Control，则用户无法在数据库中更改其参数，除非系统允许用户根据常规的 CA Access Control 授权规则执行该操作。

有效值包括 yes 和 no。

默认值：no

ldap

在 [ldap] 部分中，标记指定用于查找 LDAP 服务器和输入数据的属性。这些参数仅由位于 *ACInstallDir*/samples/ldap/exits/S50CREATE_Ldap_u.sh 的 ldap 示例 exit 使用。

base_entry

指定 LDAP 目录树中用作基本入口点的位置。

例如：您可以使用 *o*=organization_name, c=country_name。

默认值：标记未设置

主机

指定 LDAP 服务器的主机名。

默认值：标记未设置 (localhost)

path

指定 LDAP 客户端基本目录。

默认值：标记未设置 (/usr/local/ldap)

port

指定 LDAP 服务器端口（可选）

默认值：标记未设置 (389)

logmgr

在 [logmgr] 部分中，标记控制记录工具的行为。

audit_back

指定审核日志备份文件的名称。 只有 CA Access Control 可写入该文件。 用户仅可对该文件具有读取权限。

默认值：*ACInstallDir*/log/seos.audit.bak

audit_group

指定可读取审核日志的组。 如果将该标记设置为 **none**，则只有 root 用户可以读取审核日志。 CA Access Control 不会验证该标记值，因此如果您输入了无效的组名，CA Access Control 就不会将任何组权限分配到审核日志文件。

要更改现有审核日志文件的组所有权，请完成以下步骤：

使用 selang 命令 chgrp 设置文件的组所有权。

通过输入以下命令，更改 UNIX 权限：

```
chmod 640 ACInstallDir/log/seos.audit
```

默认值：none

audit_log

指定审核日志文件的名称。 如果此文件达到 *audit_size* 中指定的大小，则 CA Access Control 会关闭此文件，使用 *audit_back* 中的名称重命名该文件并创建新的审核日志。只有 CA Access Control 可写入该文件。 用户仅可对该文件具有读取权限。

默认值：*ACInstallDir*/log/seos.audit

audit_max_files

定义当 CA Access Control 执行数据触发的备份时所累积的审核日志备份文件的最大数量。 当 BackUp_Date 配置设置被设为除 *none* 外的任何值时，CA Access Control 将继续累积数据触发的备份文件。 通过此配置设置，可以减少 CA Access Control 用于审核日志备份的磁盘空间。当审核日志备份文件的数量达到设置的限制时，CA Access Control 会在创建最新的备份文件时删除最早的备份文件。

值：

- **0**—保留所有审核日志备份文件。
- *n*—大于零的正整数。

注意：您无法手动删除冗余审核日志备份文件，因为 CA Access Control 将自动保护这些文件。 此外，如果启用审核报告功能，则直到报告代理完成报告处理时，CA Access Control 才会删除备份文件。

默认值：0

audit_size

指定审核日志文件的最大大小 (KB)。

最大值：50 KB。

默认值：10240

注意：在审核文件大小超过 2 GB 时，CA Access Control 会停止将审核记录写入审核文件。

BackUp_Date

指定 CA Access Control 备份审核日志文件的条件，以及 CA Access Control 是否在备份文件名中添加时间戳。

CA Access Control *始终*在审核日志文件达到 audit_size 配置设置中指定的大小时备份该文件。

值：none、yes、daily、weekly 和 monthly。

- yes－CA Access Control 在审核日志文件达到 audit_size 中指定的大小时对其进行备份，并在备份文件名中添加时间戳。
- none－CA Access Control 在审核日志文件达到 audit_size 中指定的大小时对其进行备份，但不在备份文件名中添加时间戳。
- daily、weekly、monthly－只要达到指定的时间间隔*且*审核日志文件达到 audit_size 中指定的大小，CA Access Control 就会备份审核日志文件，并在备份文件名中添加时间戳。 但是，如果在指定时间间隔内没有审核事件写入审核日志文件，则 CA Access Control 不会在经过该时间间隔后备份文件。

  注意：CA Access Control 从第一个审核日志文件的创建时间起计算指定的时间间隔，并在相应日期的午夜备份文件。

示例：该配置设置的值为 weekly，并且 CA Access Control 在 4 月 1 日星期五上午 9:00 创建了审核日志文件。 在这一周发生了许多审核事件，审核日志文件在 4 月 4 日星期一超过了 audit_size 配置设置。 CA Access Control 在 4 月 4 日备份审核日志文件，并在备份文件名中添加时间戳。 在第一次创建审核日志文件之后的一周，即 4 月 8 日星期五的午夜，CA Access Control 再次备份审核日志文件，并在备份文件名中添加时间戳。

默认值：NONE

error_back

指定错误日志备份文件的名称。

默认值：*ACInstallDir*/log/seos.error.bak

error_group

指定可读取错误日志文件的组。 如果将此标记设置为 **none**，则只有 root 用户可以读取错误日志文件。 CA Access Control 不会验证该标记值，因此如果您输入了无效的组名，CA Access Control 就不会将任何权限分配到错误日志文件。

要更改现有错误日志文件的组所有权，请完成以下步骤：

使用 selang 命令 chgrp 设置文件的组所有权。

通过输入以下命令，更改 UNIX 权限：

```
chmod 640 ACInstallDir/log/seos.audit
```

默认值： none

error_log

指定错误日志文件的名称。 当该文件达到 *error_size* 中指定的大小时，CA Access Control 将关闭该文件，使用 *error_back* 中的名称重命名该文件并创建新的错误日志。 只有 CA Access Control 可写入该文件。

默认值： *ACInstallDir*/log/seos.error

error_size

定义错误日志文件的最大大小 (KB)。

限制： 最小值为 50 KB。

默认值： 50

irecorder_audit

指定除本地安全后台进程审核事件之外，IR API 库是否也传递现有 PMD 的审核事件。

“all”- 除本地安全后台进程审核事件之外，也传递策略模型的审核事件。

“localhost”- 仅传递本地安全后台进程的审核事件。

默认值： all

logconnected

防止将 TCP-CONNECTED 记录写入审核日志。

将 logconnected 设置为“否”便可以使用该功能。

默认值： no

更多信息：

seaudit 实用程序－显示审核日志记录 (p. 98)
seerrlog 实用程序－显示错误日志记录 (p. 156)

message

在 [message] 部分中，标记控制消息实用程序 semsgtool 的行为。

filename

指定提供对键入的 selang 命令做出响应时所显示的大多数消息的文件的位置和名称。

默认值：*ACInstallDir*/data/seos.msg

MessagesDirectory

指定 CA Access Control 消息文件的位置。

默认值：*ACInstallDir*/data/msg

mfsd

在 [mfsd] 部分中，标记定义大型机同步后台进程选项。

mfsd_trace_file

指定写入 CA Access Control 大型机同步后台进程 mfsd 跟踪消息的文件的位置。

如果将该内标识设置为 no，则不会创建跟踪文件。

默认值：*ACInstallDir*/log/mfsd.trace

OS_User

在 [OS_User] 部分中，标记定义 CA Access Control 为企业用户和企业组所使用的设置。

create_user_in_db

指定当未针对 CA Access Control 定义的用户登录时，CA Access Control 是否为该用户创建 XUSER 记录。

注意：只有在使用企业用户（osuser_enabled 设置为 1）时，此设置才适用。

限制：yes、no

默认值：yes

nonunix_unabgroup_enabled

指定在 UNIX 身份验证代理 数据库中 CA Access Control 是否支持非 UNIX 用户组。

限制：yes、no

默认值：no

osuser_enabled

指定是否启用企业用户和组。

限制：yes、no

默认值：yes

UserCache_groups_max

定义运行时间用户缓存表中的最大组数。

默认值：1000

UserCache_max

定义运行时间用户缓存表中的最大条目数。

默认值：20000

UserCache_timeout

定义从运行时间用户缓存表中删除记录之前的时间间隔（分钟）。

默认值：60

verify_osuser

指定在 CA Access Control 中创建企业用户记录 (XUSER) 之前，CA Access Control 是否验证用户是否存在于企业存储中。

限制：no（只有在企业用户存储中定义了该用户时，CA Access Control 才允许您创建企业用户记录）；yes（CA Access Control 始终允许您创建企业用户记录）。

默认值：no

package

在 [package] 部分中，标记指定您选择安装的程序包。

Client、Server、Admin、Mfsd、Tng,、Stop、Api

指示您是否已选择安装指定的软件包。

默认值：no

pam_seos

在 [pam_seos] 部分中，标记帮助您更充分地利用编程接口 PAM（可插入验证模块）。

api_update_lastaccterm

指定 API 库是否更新用户上次访问时间和日期（通过 SEOS_VerifyCreate）。

有效值为：

0—不更新上一次访问的时间和日期。

1—更新上一次访问的时间和日期。

默认值：不设置标记 (0)

bypass_services

定义 PAM 将绕过哪些服务。

默认值：ftp,vsftpd

call_segrace

指定是否在登录时自动调用 segrace 实用程序。

有效值包括 yes 和 no。

默认值：no

call_sepass

指定是否在 pam_seos 密码管理服务中使用 sepass 实用程序。

值：No、Yes

默认值：不设置标记 (No)

debug_mode_for_user

指定是否通知用户拒绝登录的原因。

有效值包括 yes 和 no。

默认值：no

failed_login_file

指定失败登录审核文件 pam_seos 的位置。

默认值：*ACInstallDir*/pam_seos_failed_logins.log

pam_login_events_enabled

指定 pam_seos 是否将登录事件发送到 seosd。

值：0—不发送登录事件；**1**—发送登录事件

默认值：1

pam_get_groups

指定 pam_seos 是否尝试从操作系统检索用户组。

值：0－不尝试检索组；1－试图检索组

默认值：1

pam_groups_timeout

定义 CA Access Control PAM 用于为 API 检索用户组的超时间隔（单位为秒）。

默认值：10

PamPassUserInfo

指定 pam_seos 是否将用户信息发送到 seosd。 在使用企业用户时，这是必需的，CA Access Control 没有企业用户的信息。 如果不使用企业用户 (osuser_enabled = no)，应将此设置的值设置为 0。

值：0－不发送用户信息；**1**－发送用户信息。

默认值：0

pam_surrogate_events_enabled

指定 pam_seos 是否将代理事件发送到 seosd。

值：0－不发送代理事件；**1**－发送代理事件。

默认值：1

process_failed_logins

指定 pam_seos 是否调用 pam_authenticate 来验证失败登录的用户密码和过程。

如果您*不*想要调用两次 pam_authenticate，将该设置指定为 0。

值：0－不从 CA Access Control PAM 模块调用 pam_authenticate；**1**－从 CA Access Control PAM 模块调用 pam_authenticate。

默认值：1

serevu_use_pam_seos

指定 serevu 是否应使用 pam_seos 登录失败日志文件，而不是系统文件。

此功能可提高 serevu 的准确性。

默认值：*yes*，在 HP-UX Itanium (IA64) 和 Linux 上，*no*，在所有其他操作系统上

passwd

在 [passwd] 部分中，各标记用于定义密码替换以及其他与用户相关的服务。-

AllowedGidRange

指定用户可添加、更新和删除的 GID 的范围。此范围以外的值代表 CA Access Control 无法更新的保留 GID。

注意：如果仅指定了一个整数，则 1 和该指定整数之间的所有整数均为保留的 GID。 如果您指定的数字超过上限，则应用默认的上限 (30000)。 如果您指定一个负数，则应用默认的下限 (1)。

限制：1 至 2147483647

默认值：100,30000

AllowedUidRange

指定用户可添加、更新和删除的 UID 的范围。此范围以外的值代表 CA Access Control 无法更新的保留 UID。

注意：如果仅指定了一个整数，则 1 和该指定整数之间的所有整数均为保留的 UID。 如果您指定的数字超过上限，则应用默认的上限 (30000)。 如果您指定一个负数，则应用默认的下限 (1)。

限制：1 至 2147483647

默认值：100,30000

AllowRootProp

指定是否将使用 sepass -p 或 sepass -s 进行的 root 密码更改发送到策略模型。 之后，PMD 会将密码传播到其订户。

有效值包括 yes 和 no。

默认值：no

change_pam

指定本地主机是否使用 PAM 在 LDAP 数据库中进行密码验证和更改。

默认值：no

Check_Adm_Rules

指定是否对 ADMIN 和 PWMANAGER 用户强制密码规则。

默认值：no

Check_All_User_Rules

指定 selang 是否应该检查所有用户的密码规则。

有效值包括 yes 和 no。

如果将该内标识设置为 yes，则 selang 将检查所有用户的密码规则。

如果将该内标识设置为 no，则 selang 将仅对更改密码的用户检查密码规则。

默认值：no

注意：仅使用 API 时，支持该标记。

CreateHashedPasswdDatabase

（仅限于 DEC UNIX）。 指定是否在创建、更新或删除用户记录的每个 CA Access Control 命令之后，或者在使用 sepass 实用程序更改了每个用户密码之后自动运行 exit 脚本。

注意：有关更多使用说明，请参阅 *ACInstallDir*/samples/exits-src/USER_POST 目录下的自述文件。

默认值：no

DefaultHome

指定系统的默认主目录。用户的主目录为指定系统主目录的子目录。例如：如果系统主目录为 /home，则新用户的主目录为 /home/*username*。 如果指定了此标记的值，则该值将会覆盖客户端 lang.ini 文件中的值。 如果指定 *nohomedir*，则不会自动设置主目录。

默认值：/home

DefaultPasswdCmd

指定默认密码程序。 如果指定密码程序，则在启动 sepass 后但未运行 seosd 的情况下将使用此密码程序。

默认值：/bin/passwd

DefaultPgroup

指定在未输入值的情况下 CA Access Control 分配给新 UNIX 用户的主组。

默认值：other

DefaultShell

指定在未输入值的情况下 CA Access Control 分配给新 UNIX 用户的默认 shell。 如果指定了此标记的值，则该值将会覆盖客户端 lang.ini 文件中的值。

默认值：/bin/sh（在 HP-UX 上为 /sbin/sh）

Dictionary

定义包含*不能*用作密码的单词的文件的完整路径名。

注意：要使用此文件，必须将词典格式密码规则 (use_dbdict) 设置为 *file*，并将 UseDict 设置为 *yes*。 如果词典格式设置为 *db*，则无法使用的密码取自 CA Access Control 数据库，并将忽略此设置。 这是 UNIX 上的默认值。

重要说明！ 该标记过时。 请使用数据库中的词典。

默认值：/usr/dict/words

GeneratePasswd

指定 sepass 是否自行生成新密码。

有效值包括 yes 和 no。

如果将此内标识设置为 no，则系统会要求用户输入新密码。

默认值：no

HomeDirUpd

指定用户主组发生更改时，CA Access Control 是否更新用户的主目录组所有权。

有效值包括 **yes** 和 **no**

默认值：yes

nis_env

指定本地主机是 NIS 客户端还是 NIS+ 客户端。

有效值包括 no、nis 或 nisplus。

默认值：no

NisPlus_server

指定此工作站是否为 NIS+ 服务器。

有效值包括 yes 和 no。

如果标记的值为 yes，则 CA Access Control 会将密码替换视为 NIS+ 密码替换。

默认值：no

only_local

确定 sepass 的默认设置是否包括 -l 标志。

有效值包括 yes 和 no。

如果将此内标识设置为 yes，则 sepass 仅在本地替换密码，即在本地密码文件 (usually /etc/passwd)、安全文件及本地数据库中。

默认值： no

only_pmdb

指定 sepass 的默认设置是否包括 -p 标志。 如果该标记的值为 yes，则它将指示 sepass 仅在指定主机的 PMDB 上更改密码。

如果未定义此类数据库，则 sepass 不会执行任何操作。

默认值： no

passwd_distribution_encryption_mode

指定当将密码作为策略模型服务的一部分分发时，加密用户密码所使用的方法。

有效值包括：

1－兼容模式，用于在不使用长密码的 CA Access Control 系统（这包括运行 CA Access Control 12.0 之前版本的所有计算机）之间分发密码。

2－MD5 模式，用于在使用长密码且运行 Linux 的 CA Access Control 系统之间分发密码。

3－双向密码，用于在使用长密码的任何 CA Access Control 系统之间安全地分发密码（作为加密消息中的明文）。

默认值： 1

passwd_format

指示是否将密码更改传播至 NT 主机。

将此内标识设置为 NT，表示您所管理的主机中有一台是 NT 主机。

默认值： 无

passwd_local_encryption_method

指定在本地存储这些密码时加密用户密码所使用的方法。

有效值包括：

crypt－仅使用密码前八个字符（作为 DES 密钥）的标准单向 UNIX 加密。 指定 crypt 禁用长密码。

md5－可加密不定长度的密码的 MD5 散列函数。指定 md5 启用长密码。

默认值：crypt

PromptOldPassword

指定当通过 /opt/CA/AccessControl// bin/segrace 调用 sepass 时，是否提示本地用户输入其旧密码。 （必须使用完整路径）。

如果将此内标识设置为 yes，则表示提示用户提供他们的旧密码。

默认值：yes

quiet_mode

指定 sepass 是否显示版权通知以及关于将密码传播至策略模型的消息。

默认值：no

RootPwAsOwn

指定特权用户是否可以使用 sepass 像 root 用户一样更改 root 密码（使用 *-x* 选项）。

有效值包括：

yes－特权用户可以使用 sepass 像 root 用户一样更改 root 密码。 它们无法以自己的身份更改 root 密码（管理更改）。

no－特权用户仅可以自己的身份使用 sepass 更改 root 密码（管理更改）。

例如：如果将此标记设置为 *yes*，则特权用户可以使用以下命令更改 root 密码：

```
sepass -x root
```

同一用户无法使用以下命令更改 root 密码：

```
sepass root
```

如果将此标记设置为 *no*，则将出现相反的情况。

默认值：no

SaveGroupAttrs

指定在更新 UNIX 环境中的组后是否保留以前的组文件所有者、组及模式。

有效值包括 yes 和 no。

如果将此标记设置为 **no**，则新值将分别被设置为 0、0、644。

默认值： no

SavePasswdAttrs

指定在更新 UNIX 环境中的用户后是否保留以前的密码文件所有者、组及模式。

有效值包括 yes 和 no。

如果将此标记设置为 **no**，则新值将分别被设置为 0、0、644。

默认值： no

Shadow_Admin_Change

（仅限于 AIX 平台）。 指定当管理员通过 selang 或使用 sepass 更改密码时，是否将 ADMCHG 标志添加到 /etc/security/passwd 文件的用户条目中。

默认值： no

UIDAlgorithm

指定添加新用户时使用哪一个可用的 UID 算法。 将它设置为其他任何值都将选择较旧的进程。*新*算法可提供超过 64 KB 的 UID 编号，通常速度更快。

默认值： new

UseDict

指定在验证密码时是否使用词典文件（通过 Dictionary 设置进行设置）。

注意： 要使用词典文件，还必须将词典格式密码规则 (use_dbdict) 设置为 *file*。 如果词典格式设置为 *db*，则无法使用的密码取自 CA Access Control 数据库，并将忽略此设置。

默认值： no

YpGrpCmd

指定用于生成 NIS 组映射的命令。

默认值： make group

YpMakeDir

指定创建 NIS 映射时使用的生成文件目录名。

默认值：/var/yp

YpPassCmd

指定用于生成 NIS 密码映射的命令。

默认值：make passwd

YpServerGroup

指定从中创建 NIS 组映射的组文件。

默认值：/etc/group

YpServerPasswd

指定从中创建 NIS 密码映射的密码文件。

默认值：/etc/passwd

YpServerSecure

指定包含密码且用于构建 NIS 密码映射的安全文件的名称。

默认值：因平台而异：

- IBM AIX：/etc/security/passwd
- HP-UX：/.secure/etc/passwd
- Sun Solaris：/etc/shadow

YpTimeOut

指定新的客户端（selang、Security Administrator 等）可运行 ypbind 测试的时间（秒），该测试可确定本地主机是否连接至 NIS 服务器。 到期时，该客户端将退出并显示错误消息。

默认值为零 (0)，表示不执行 ypbind 测试。

默认值：0

更多信息：

sepass 实用程序－设置或替换密码 (p. 180)

pmd

[pmd] 部分中的标记可确定 PMDB 属性。

注意：除了 seos.ini 以外，每种策略模型都具有一个配置文件 pmd.ini。

_min_retries_

指定 sepmdd 至少应尝试向不可用订户重新发送下一个排队更新的次数。 sepmdd 将遍历订户列表以寻找未完成的更新，并在每次无法将更新重新发送到不可用订户时，使计数器递增。 在达到此标记中指定的最少尝试次数后，会将订户标记不可用状态。

默认值：4

_pmd_backup_directory_

定义 CA Access Control 用来存储策略模型备份的目录。 CA Access Control 将每个 PMD 备份存储在名为 *pmd_name* 的子目录中。

默认值：*ACInstallDir*/data/policies_backup

_pmd_directory_

指定 PMDB 所在的目录。 该目录名最多可包含 70 个字母数字字符。指定该目录的完整路径。 每个策略模型都位于目录 *pmdDirectory*/*pmdName* 中。

默认值：*ACInstallDir*/policies

_PMD_DIRECTORY_

与 _pmd_directory_ 相同

_PMD_EXEC

定义策略模型后台进程的名称。

_QD_timeout_

指定 sepmdd 后台进程在第一次扫描其订户列表期间，尝试更新订户数据库时等待的最长时间（秒）。 如果超出此时间而该后台进程仍无法成功更新某个订户，则会忽略该特定订户，并尝试更新列表中的其余订户。

完成订户列表的首次扫描后，sepmdd 会接着执行第二次扫描，在这次扫描期间，它会尝试更新在第一次扫描期间未成功更新的订户。第二次扫描期间，它将尝试更新订阅者，直到连接系统调用超时（大约 90 秒）。

默认值：3

_retry_timeout_

在 _min_retries_ 中指定尝试的最少次数后，指定尝试向不可用订户重新发送更新之前等待的时间（分钟）。 在超过此标记所定义的分钟数后，它将订户标记为可用状态。

直到发生以下情况，订户才会标记为不可用状态：

- 手动发布该用户。
- sepmdd 被手动关闭并重新启动。 在以下情况下会重新启动 sepmdd：
  - 如果有语言工具尝试连接该程序。
  - 如果父 PMDB 要发送更新。
  - pull 选项由订户触发。 在订户上启动 CA Access Control 时，可以进行触发。
- pull 选项由不可用订户触发。

注意：过于频繁地关闭 sepmdd 不可取，因为重新启动后台进程需要花费时间，这会导致整个传播过程变慢。 将该程序始终处于运行状态也不可取，因为这样可能引发一些稳定性问题，但这仅仅是推测。

默认值：30

_shutoff_time_

指定 sepmdd 退出之前的活动时间（分钟）。如果标记值为零，sepmdd 永不退出。

默认值：0

ClientOperationTimeout

定义客户端等待策略模型响应的超时期（秒）。

默认值：60

is_maker_checker

指定是否使用双重控件。

有效值包括 yes 和 no。

如果该标记的值为 **yes**，则您无法直接更新数据库，只能通过 PMDB 来实现，两个管理员（制定者和检查者）必须协作进行更新。

默认值：不设置标记 (no)

pass_auth

指定远程密码更改期间 sepass 是否验证调用程序的密码。 sepass 实用程序总是将用户输入的旧密码与存储在本地 prodname 数据库中的密码进行比较。 如果将此标记设置为 yes，则 sepass 还会将运行 sepass 的用户输入的旧密码与其存储在远程 prodname 数据库（通常为 pmdb）中的自身密码进行比较。 这表示 sepass 用户 必须输入其自身密码，即使在更改其他用户的密码时也是如此。

值：yes、no

默认值：yes

pull_option

指定是否在订阅者数据库可用后立即进行更新。

有效值包括 yes 和 no。

如果该标记的值为 **yes**，则在订户工作站可用后，seagent 会立即向本地主机和该计算机上的任何策略模型的父策略模型发送消息。 随后 sepmdd 会立即更新订户，而不会等待下一个半小时后的重试。-

默认值：yes

send_unix_env

指定 sepmd -n 选项是否发送策略模型密码文件和组文件的内容。

有效值包括 yes 和 no。

yes—*sepmd -n* 选项发送策略模型密码文件和组文件的内容。

no —**sepmd -n** 选项不发送策略模型密码文件和组文件的内容。

默认值：yes

ShutdownWaitingTimeout

定义策略模型等待其组件完全关闭的超时期（秒）。 如果策略模型组件未完全关闭，策略模型会强制将其关闭。

默认值：60

synch_uid

指定创建新的 UNIX 用户时，CA Access Control 是否强制订户使用与父策略模型主机相同的 uid。

updates_in_chunk

定义策略模型在每次循环中最多向每个订户发送的命令数。

默认值：10

更多信息：

sepmd 实用程序 (p. 183)

policyfetcher

在 [policyfetcher] 部分中，标记可控制策略提取器后台进程 (policyfetcher) 的行为。

check_deployment_tasks

定义 policyfetcher 在分发主机上检查新部署任务（DEPLOYMENT 资源）的频率（秒）。

默认值：600（每 10 分钟）

限制：最小值为 60。

deploy_timeout

定义 policyfetcher 在端点上等待部署任务或取消部署任务完成的秒数。

默认值：900

devcalc_command

定义 policyfetcher 用来运行偏差计算的 selang 命令。

默认值：start DEVCALC params(-nonotify)

示例：start DEVCALC params(-nonotify -precise)

dh_command_retry_interval

定义每个 DH 通知命令重试之间的时间间隔（秒）。

默认值：30

endpoint_heartbeat

定义 policyfetcher 将心跳发送到分发主机 (DH) 的频率。 该频率是 check_deployment_task 设置的一个要素，可确定 policyfetcher 在发送心跳之前检查部署任务的次数。例如：如果将 check_deployment_task 设置为默认的 600 秒（10 分钟）且将此标记设置为 6，那么 policyfetcher 将每 3600 秒（1 小时）发送一次心跳。

在发送心跳后，policyfetcher 还将运行偏差计算器（start devcalc 命令），然后等待 60 秒，使系统完成偏差计算。 在 60 秒之后，policyfetcher 会继续检查本地端点信息是否与 DH 信息相同。

默认值：10

max_dh_command_retry

定义 policyfetcher 在放弃前最多重复尝试从 DH 获取更新通知的次数。

默认值：3

max_dh_retry_cycles

定义 policyfetcher 在切换到灾难恢复 DH 前最多重复尝试从生产 DH 获取更新通知的循环数。

默认值：3

policy_verification

指定 policyfetcher 后台进程在执行任务之前是否在备份 CA Access Control 数据库上验证新的部署任务。

有效值:

1－运行策略验证

0－禁用策略验证

默认值：0

policyfetcher_enabled

指定是否运行 policyfetcher 后台进程。

有效值:

1－运行 policyfetcher

0－禁用 policyfetcher

默认值：0

PUPMAgent

在 [PUPMAgent] 部分中，各标记决定着特权用户密码管理代理的功能。

EnableLogonIntegration

指定启用终端集成。

限制：0，禁用终端集成；1，启用终端集成。

默认值：1

InterfaceName

定义通讯接口名称，即 特权用户密码管理 代理用来处理请求的 UNIX 套接字名称。 套接字文件位于 /opt/CA/AccessControl/data/PUPMAgent 目录中。

默认值：PUPMAgentInterface

OperationMode

指定 特权用户密码管理 代理工作模式。

限制：0，特权用户密码管理 代理处于禁用状态，不运行；1，特权用户密码管理 代理处于启用状态，运行但不将数据记录到跟踪文件中；2，特权用户密码管理 代理处于启用状态，运行并将数据记录到跟踪文件中。

默认值：0

seagent

在 [seagent] 部分中，各标记控制着 seagent 后台进程的行为。

debug_backup

指定 CA Access Control 是否使用 seagent 调试消息备份文件。

限制：yes、no

默认值：yes

debug_backup_file

定义 seagent 调试消息备份文件的名称。

默认值：*ACInstallDir*/log/seagent_debug.back

debug_file

定义 CA Access Control 将 seagent 调试消息写入到的文件的名称。

默认值：*ACInstallDir*/log/seagent_debug

debug_level

指定 CA Access Control 写入调试文件的调试消息的最低级别。

限制：

- disabled－不将任何消息写入调试文件
- critical－将 CRITICAL 消息写入调试文件
- very_high－将 CRITICAL 和 VERY_HIGH 消息写入调试文件
- high－将 CRITICAL、VERY_HIGH 和 HIGH 消息写入调试文件
- normal－将 CRITICAL、VERY_HIGH、HIGH 和 NORMAL 消息写入调试文件
- low－将 CRITICAL、VERY_HIGH、HIGH、NORMAL 和 LOW 消息写入调试文件

默认值：critical

watchdog_check_interval

定义 seagent 检查 seoswd 存在性的时间间隔（秒）。

注意：只有在 seagent 有大量传入连接时，此标记才适用。 如果 seagent 空闲，它将每隔 3 秒检查一次 seoswd 是否存在，此标记将被忽略。

默认值：30

seauxd

在 [seauxd] 部分中，标记确定 Unicenter TNG 日历的使用和刷新间隔，并有助于管理名称解析。

client_request_timeout

指定保留解析请求的时间间隔（秒）。

默认值：120

file_time_check

指定检查 /etc/passwd 中的更改的时间间隔（秒）。

指定 0 即禁用检查。

默认值：10

init_delay

指定等待 seauxd 启动的时间 (秒)。

默认值：10

log_file_name

指定辅助日志文件的名称。 其位于 SEOSPATH/log。

默认值：seauxd.log

log_file_size

指定辅助日志文件的最大大小 (KB)。 如果文件大小超出该值，文件将被截短为 0。

默认值：100

log_level

指定要使用的日志记录级别。

有效值包括以下各项：

0-Minimum info
1-ERR
2-WARN + ERR
3-NOTIC + WARN + ERR
4-DEBUG + INFO + WARN + ERR

默认值：0

req_poll_timeout

指定等待输入请求的时间间隔（毫秒）。

默认值：200

respawn_seauxd_delay

定义 seauxd 退出后，seosd 再生该后台进程的最小时间（秒）。

默认值：60

TNG_cal_lib

指定包含 Unicenter TNG 日历的共享库的名称。

默认值：libcalendar

TNG_calendars

指定是否使用 Unicenter TNG 日历限制设置时间间隔时的资源。

默认值：no

TNG_lib_path

指定 CA Access Control 查找包含 Unicenter TNG 日历的共享库的路径。

默认值：/opt/CA/CAlib

TNG_refresh_interval

指定 CA Access Control 从 Unicenter TNG 中检索活动日历信息的刷新间隔（分钟）。

默认值：10

trace_cnt

指明是否在跟踪文件中写入计数器。

有效值包括 yes 和 no。

默认值：no

segrace

在 [segrace] 部分中，该标记可确定 segrace 实用程序的属性。

sepass_command

指定当用户没有剩余的宽限登录时执行的 CA Access Control 密码替换命令的位置。

默认值：*ACInstallDir*/bin/sepass

更多信息：

segrace 实用程序－显示用户登录信息 (p. 157)

seini

在 [seini] 部分中，标记可确定 seini 智能搜索功能的属性。

get_error_warning

指定是否显示智能搜索功能的错误和警高消息。

默认值：yes

perform_action

指定 seini 是否对智能搜索功能找到的内标识或部分执行操作。

有效值包括 yes 和 no。

如果将此标记设置为 **yes**，则其他智能搜索找到的部分和标记将用于所请求的 seini 操作。

默认值：no

use_intelligent_search

指定是否在调用 seini 工具时执行智能搜索。

默认值：no

更多信息：

seini 实用程序－管理配置文件 (p. 162)

selock

在 [selock] 部分中，标记可控制 selock 实用程序的行为。

unlocking_user

指定所有者以外，可为锁定屏幕取消锁定的用户的名称。

默认值：root

更多信息：

selock 实用程序－锁定 X 终端屏幕 (p. 169)

selogrd

在 [selogrd] 部分中，标记可控制日志传递后台进程 selogrd 和 selogrcd 的行为。

Caudit_size

指定在 *selogrcd* 创建备份文件并打开新文件前，审核收集文件的最大大小 (KB)。

最小值为 50 KB。

默认值：1024

CBackUp_Date

设置 selogrcd 执行备份所依据的标准。

有效值包括：none、yes、daily、weekly 和 monthly。

如果指定 **yes**，则 CA Access Control 将根据大小限制标记 Caudit_size 执行备份并为文件添加时间戳。

如果指定 **none**，则 CA Access Control 将根据 Caudit_size 标记执行备份，但不为文件添加时间戳。

如果指定 **daily**、**weekly** 或 **monthly**，selogrcd 将在第一次创建文件时添加时间戳。如果当前日期晚于该时间戳，CA Access Control 会自动创建一个备份文件并为其添加时间戳。

但是，如果该文件的大小先超过 Caudit_size 标记的值，则 CA Access Control 将创建一个备份文件，但不会发出时间戳。

默认值：NONE

ChangeLogFactor

指定在测试日志文件是否已更改为备份文件前，对标记 *Interval* 中的值所应用的系数。 例如：如果将 *interval* 标记设置为 5，并将 *ChangeLogFactor* 标记设置为 5（默认值），则在检查日志文件是否更改为备份文件之前 CA Access Control 将等待 25 秒。

默认值：5

CipherName

指定包含 selogrd 所使用的加密功能的文件的名称（如果将 UseEncryption 内标识设置为 eTrust）。

必须将此文件放置在 *ACInstallDir*/lib/ 目录中。

CipherName 是共享对象文件的符号链接。

默认值：adcipher

CollectFile

指定审核收集器后台进程 selogrcd，将收集的审核记录存储到的文件的名称。

默认值： *ACInstallDir*/log/seos.collect.audit

CollectFileBackup

指定 selogrcd 在接收到 USR1 信号的情况下，备份和重命名所收集的审核记录的文件时所使用的名称。

默认值：*ACInstallDir*/log/seos.collect.bak

ConsolePort

指定用于 selogrd - secmon 通讯的名称或端口号。 只有打算在同一台主机上运行 selogrcd 和 secmon 时，才需设置此标记。

如果指定了此标记，seolgrd - secmon 通讯将使用指定的端口完成；否则它们将使用在 *ServicePort* 标记中指定的端口，或使用 RPC portmapper 动态分配端口（如果该标记也为空）。 服务名称必须为 UDP 端口，因为日志传递后台进程使用 UDP 进行通讯。

如果此标记值为数字，则后台进程将绑定到指定的端口号。

如果该内标识的值为服务名（字符串），则将使用 /etc/services 或 NIS 服务映射来解析端口号。

默认值：标记未设置（从 *ServicePort* 标记中获取的值）

DataFile

指定将目标路由信息发送至指定的目标之前将其写入到的文件的名称。

默认值：*ACInstallDir*/log/logroute.dat

时间间隔

指定 selogrd 后台进程对日志文件进行各次轮询之间的时间间隔（秒）。

默认值：5

KeyFile

指定保存审核加密密钥的文件的名称。

在 selogrd 执行 CA Access Control 审核加密时使用此密钥。 密钥文件位于 *ACInstallDir*/lib 目录中。

该密钥可由 sechkey 工具更改。

默认值：adcipher.bin

Mailer

指定 selogrd 用来发送电子邮件的程序名称。

注意：只有将 UseSmtpMail 标记设置为 yes 时，此选项才相关。

默认值：/bin/mail

MaxErrorSending

指定 selogrd 是否将向 syslog 发送有关向 selogrcd 发送审核记录所遇到的困难的错误消息，但仅在困难数超过此内标识值以后才发送。

默认值为 1，这表示每次 selogrd 在向 selogrcd 进行发送遇到困难时，它就会向 syslog 发送一条消息。

默认值：1

MaxSeqNoSleep

指定 selogrd 在不休眠的情况下扫描的日志记录的最大数目。

默认值：50

RefuseUnencrypted

指定 selogrcd 是否会接受不加密的审核。 如果 UseEncryption 设置为 **no**，它将与 UseEncryption 标记结合使用，并且是冗余的。因此它仅在 selogrcd 使用加密的情况下适用。

有效值包括：

yes－拒绝不加密的审核

no－既接受加密的审核，也接受不加密的审核

默认值：no

RouteFile

指定日志传递配置文件的名称。除非通过 selogrd 实用程序的 -config 选项进行覆盖，否则将会使用该文件。

默认值：*ACInstallDir*/log/selogrd.cfg

SavePeriod

指定保存有关所发送的记录数的信息之间的时间间隔（分钟）。

默认值：2

sendmail_header_format

确定 selogrd 发送的邮件的头中的用户名格式。

注意：只有在 selogrd 不能发送邮件时，才更改此标记值。（即，如果您在 syslog 中看到 selogrd 的错误 4634。）

有效值包括以下各项：

1－用户名格式为 *SmtpMailFrom*

例如：eTrust_Admin

2－用户名格式为 *SmtpMailFrom*@*hostnam*e（其中，*hostname* 是运行 selogrd 的主机）。

例如：eTrust_Admin@machine

默认值：1

ServicePort

指定日志路由工具必须使用的名称或端口号。

如果指定，selogrd 和 selogrcd 将使用指定的端口；否则，selogrd 和 selogrcd 将使用 RPC portmapper 动态分配端口。

如果此标记具有值，selogrd 和 selogrcd 将使用指定的端口；否则，selogrd 和 selogrcd 将使用 RPC portmapper 动态分配 UDP 端口。服务名称必须为 UDP 端口，因为日志传递后台进程使用 UDP 进行通讯。

如果此标记值为数字，则后台进程将绑定到指定的端口号。

如果该内标识的值为服务名（字符串），则将使用 /etc/services 或 NIS 服务映射来解析端口号。

仅可指定 UDP 端口/服务。

默认值：标记未设置（selogrd 和 selogrcd 使用 RPC portmapper 动态分配端口）

SmtpMailFrom

指定 UseSmtpMail 的发送者身份。

默认值：AccessControl_Admin

SmtpMailServer

指定远程邮件服务器主机的地址。当 UseSmtpMail 设置为 yes 时使用此标记。 如果未指定此标记，则将假定本地计算机为邮件服务器。

默认值：（空－本地服务器）-

SmtpTimeLimit

指定 selogrd 在超时前等待邮件服务器做出答复的时间限制（秒）。

默认值：100

tec_conf_file

指定后台进程 selogrd 用于创建 TEC 事件的配置文件的名称。

默认值：/etc/tecad_seos.conf

UseEncryption

确定加密类型。

有效值包括以下各项：

native－selogrd 使用 CA Access Control 标准加密。

eTrust－selogrd 通过 adcipher 使用审核日志加密。

no－selogrd 不使用加密。

默认值：no

UseSmtpMail

确定是使用直接邮件功能，还是以前的邮件程序。

默认值：yes

更多信息：

seaudit 实用程序－显示审核日志记录 (p. 98)
selogrcd 后台进程－收集审核记录 (p. 259)
selogrd 后台进程－发出审核记录 (p. 260)

seos

在 [seos] 部分中，以下标记确定 CA Access Control 所使用的全局设置。

admin_data

指定存储 CA Access Control Security Administrator ruler 和其他配置文件的目录。

默认值：*ACInstallDir*/data

auth_login

确定登录授权方法。 有效值包括：

native－登录时，将对照 UNIX 密码或影子文件来检查用户密码。

eTrust－当用户在本地环境中不存在时，对照 CA Access Control 数据库检查用户密码。

PAM－当用户在本地环境中不存在时，通过 PAM 模块检查登录。 这仅在支持 PAM 的计算机上受支持。 PAM 用于验证用户，例如：LDAP 定义的用户。

默认值：native

auth_module_names

定义允许在本地身份验证以外进行身份验证的语言客户端模块。 此标记在执行身份验证前由客户端在 Ica API 调用内设置。 更改此标记会影响其他客户端在非本地模式下的身份验证。

无默认值。

fast_create_db

指定 PMDB 是否使用快速数据库复制设备。

有效值包括：

no－使用旧设备。

yes－使用快速数据库复制设备。

默认值：yes

full_year

指定使用四位数字或后两位数字显示年份的格式。

例如：如果将该内标识设置为 yes，则将显示 2000，而不是 00。

有效值包括以下各项：

yes－四位数字

no－两位数字

此内标识影响 secons -tv、dbmgr d 和 seaudit 工具生成的输出。

默认值：yes（四位数字）-

ldap_base

定义搜索库的辨别名称，此名称用于通过启用了 LDAP 的 CA Access Control 实用程序（例如：sebuildla）在 LDAP 目录信息树 (DIT) 中查询用户数据。

例如：您可以使用以下格式，并使用您自己的内容来替换输入内容：

o=*organization_name*,c=*country_name*

默认值：标记未设置

重要说明！ 要设置 sebuildla 和所需的 LDAP 配置设置，您必须熟悉 LDAP 并能够执行 ldapsearch 命令。 建议您阅读 ldap(1)、ldapsearch(1) 的说明页面以及 LDAP 客户端文档中关于设置的信息。

ldap_hostname

定义以空格分隔的主机名列表，该列表中 LDAP 服务器正在针对启用了 LDAP 的 CA Access Control 实用程序而运行。

默认值：标记未设置 (localhost)

ldap_certdb_path

定义 Netscape 样式证书数据库所在的目录。

对于 sebuildla，在使用 Netscape LDAP SDK API for LDAP over SSL（Solaris）的平台上这是必需的。 要使 sebuildla 工作，证书数据库必须包含 LDAP 服务器的有效证书。

注意：sebuildla 将结合使用 LDAP over SSL 和服务器身份验证，即不进行客户端身份验证。 请参阅 PKI 工具包文档，以了解设置安全服务的详细信息。

默认值：/.netscape

ldap_keydb

定义密钥数据库文件的名称。

注意：此设置仅用于 AIX，因为 AIX 密钥数据库可以具有任意名称（不同于具有如 certX.db 和 keyY.db 名称的 Netscape 安全数据库，Netscape 安全数据库的名称取决于实施版本，因此要查找它们只需要使用 ldap_certdb_path）。

默认值：标记未设置

ldap_method

指定 CA Access Control 针对启用了 LDAP 的实用程序访问 LDAP 服务所使用的绑定方法。

默认情况下，sebuildla 使用带有所有安全机制的*简单*身份验证。 在简单身份验证中，ldap_userdn 和相应凭据被传送到 LDAP 服务器。 sebuildla 将用户凭据以加密形式存储在位于 *ACInstallDir*/etc 下的 ldapcred.dat 中。这两个参数接近 LDAP 服务器所需的帐户和密码组合。

注意：对于 SASL 或 TLSv.1/SSL，请参阅 LDAP 服务器文档。 要使特定 ldap_method 设置生效，必须支持相应的机制且对正在执行 sebuildla 的计算机中部署的本地 LDAP 客户端进行配置（即使用 TLS/SSL 操作，有效证书应安装在服务器和客户端）。

有效值包括：

0－标准 LDAP

1－SASL (RFC 2222)

2－LDAPS（LDAP over SSL－仅服务器身份验证。）

注意：您使用的方法将决定您设置 ldap_userdn 标记及其相应凭据（通过 seldapcred 实用程序）需使用的方法。

默认值：0

ldap_port

定义启用了 LDAP 的 CA Access Control 实用程序的 LDAP 服务器端口。 您只需在 LDAP 服务器未使用标准 LDAP 端口 (389) 时更改此标记。

默认值：标记未设置 (389)

ldap_query_size

定义 sebuildla 在每个批处理查询中检索的 LDAP 条目的最大数量。

如果您不想更改 LDAP 服务器端的大小限制参数，请使用此标记。 通常，sebuildla 尝试一次检索所有数据，如果存在许多用户条目时，这样可能会超出服务器的大小限制并导致 LDAP 操作失败。如果设置了 ldap_query_size，sebuildla 不需要检索所有条目，该操作不会失败。如果用户条目总数超过 ldap_query_size 或服务器端的大小限制，则检索的条目数将与这两种设置中的较低数相一致。

重要说明！ 启用批处理查询会影响 sebuildla 的性能。 只有在 DIT（目录信息树）中带有许多用户数据（数千个条目）的 LDAP 环境才考虑使用此设置。

注意：有关服务器端 LDAP 控制的信息，例如：OpenLDAP 服务器 (slapd)、大小限制参数，请参阅 LDAP 服务器文档。

默认值：不设置标记（空）

ldap_timeout

定义启用了 LDAP 的 CA Access Control 实用程序在绑定到 LDAP 服务并获得 LDAP 搜索结果时需等待的最长时间（秒），超过该时间即中断连接。 从 LDAP 服务检索信息所需的时间取决于 LDAP 服务的速度以及存储在 DIT 中的用户数据量。 使用此标记可说明上述各方面。

注意：您可能还需要调整服务器端 LDAP 控制以避免截短搜索结果。 例如：对于 OpenLDAP 服务器 (slapd)，您需要调整大小限制参数。 有关详细信息，请参阅 LDAP 服务器文档。

默认值：标记未设置（15 秒）

ldap_uid_attr

定义在 LDAP DIT 中包含用户名的属性的名称。RFC 2307（一种将 LDAP 用作网络信息服务的方法）规定了此标记的默认值 *uid* 作为此属性。更改此标记可防止支持 LDAP 的 CA Access Control 实用程序使用具有非标准架构的 LDAP DIT。

默认值：标记未设置 (uid)

ldap_uidNumber_attr

定义在 LDAP DIT 中包含 UID 号的属性的名称。 RFC 2307 规定了此标记的默认值 *uidNumber* 作为此属性。更改此标记可防止支持 LDAP 的 CA Access Control 实用程序使用具有非标准架构的 LDAP DIT。

默认值：标记未设置 (uidNumber)

ldap_user_class

定义在 LDAP DIT 中包含用户数据的对象类的名称。 RFC 2307 规定了此标记的默认值 *posixAccount* 作为此对象类。更改此标记可防止支持 LDAP 的 CA Access Control 实用程序使用具有非标准架构的 LDAP DIT。

默认值：标记未设置 (posixAccount)

ldap_userdn

定义 LDAP 用户的辨别名称 (DN)，启用了 LDAP 的 CA Access Control 实用程序使用此名称从 LDAP DIT 中检索用户数据。 根据 RFC 2307，在 DIT 中，CA Access Control 应查找 *ou=People* 级别的 *uid* 和 *uidNumber* 属性中的用户数据。 由于安全原因，建议您仅授予此用户 (ldap_userdn) 访问此数据的权限。

如果允许匿名访问 DIT，您可以保持此标记为空。 否则，您必须设置此标记，并针对启用了 LDAP 的 CA Access Control 实用程序对 LDAP 服务进行身份验证而运行 seldapcred 实用程序（您只需执行此操作一次，因为 seldapcred 会将您的加密凭据存储在某个文件中以便重复使用）。

例如：按如下所示设置此标记：

```
ldap_userdn = uid=user1,ou=People,dc=myCompany,dc=com
```

默认值：标记未设置

ldap_verbose

指定是否启用涉及 sebuildla 获取用户数据的 LDAP 操作的详细帐户信息。

请在设置 sebuildla 中的 LDAP 数据检索或疑难解答时使用此设置。

有效值为 **0**（禁用）；非零整数（启用）。

默认值：0

locale

确定 CA Access Control 后台进程和实用程序所使用的语言。CA Access Control 可以在多种语言环境中运行。

支持的语言包括：C、日语、简体中文、繁体中文-

有关语言的完整列表，请参阅 /etc/ca/localeX/calocmap.txt；在 Linux 中，请参阅 /opt/CA/SharedComponents/cawin/locale/

默认值：C

pam_enabled

仅在 SOLARIS、HP-UX 和 LINUX 上有效。

指定本地主机是否允许使用 PAM 在 LDAP 数据库中进行身份验证和密码更改。

为此，它将检查是否能动态加载 PAM 库（该库必须在系统上存在）。

有效值包括：“no”、“yes”。

默认值：yes

parent_pmd

定义用逗号分隔的策略模型数据库 (PMDB) 列表，此计算机可以从这些数据库接受更新。本地 CA Access Control 数据库拒绝来自未在此列表中指定的任何 PMDB 的更新。

也可以指定一个包含行分隔 PMDB 列表的文件路径。

将此标记设置为“_NO_MASTER_”，以使本地 CA Access Control 数据库接受来自任何 PMDB 的更新。

如果您没有设置此标记，本地 CA Access Control 数据库将不接受来自任何 PMDB 的更新。

按 pmd_name@hostname 格式指定每个 PMDB

例如：

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
parent_pmd = /opt/CA/AccessControl//parent_pmdbs_file
```

默认值：标记未设置（数据库不接受来自任何 PMDB 的更新）。

passwd_pmd

指定 sepass 将密码更新发送至的 PMDB。

如果不设置此内标识，它将继承 parent_pmd 内标识的值。

格式为 *pmd_name@hostname*。

parent_pmd 和 passwd_pmd 标记可以拥有相同的值。 如果 parent_pmd 和 passwd_pmd 标记中的值不相同，则 passwd_pmd 数据库将其更新发送到 parent_pmd 数据库以便进行分发。 因此，此 parent_pmd 数据库必须是 passwd_pmd 数据库的子项（订户）。

无默认值。

ReverseIpLookup

控制 seagent 识别连接客户端的方式。

有效值包括以下各项：

yes－seagent 查找开放客户端套接字的 IP 地址。

no－seagent 使用从客户端接收的主机名；seagent 不解析任何主机名。（通过禁用 TERMINAL 类可以达到同样的效果。）

默认值：yes

secondary_pmd

指定用作未在主要目标 (passwd_pmd) 中定义的用户的辅助密码替换目标的 PMDB。

格式为 *pmd_name@hostname*。

无默认值。

SEOSPATH

指定 CA Access Control 的安装目录。

如果尚未在 NFS 挂接文件系统中安装 CA Access Control，可以将其安装在任何目录中。-

默认值：*ACInstallDir*

SyncUnixFilePerms

指定 CA Access Control 是否应将其 ACL 权限与本地 UNIX 系统的 ACL 权限及其他权限进行同步（如果存在这些权限）。

有效值包括以下各项：

no－不将 UNIX 文件权限与 CA Access Control ACL 进行同步。

warn－不同步 ACL 权限，但是如果 CA Access Control 中的权限与 UNIX 发生冲突，则发出警告。

traditional－根据 CA Access Control ACL 更改组和所有者的 rwx 权限，并在所有其他情况下发出警告。

acl－根据 CA Access Control ACL 更改本地文件系统 ACL（在支持 ACL 的平台上）。

force－函数与 traditional 或 acl 相同（在支持 ACL 的平台上），但是也强制将 defaccess 映射到“其他”权限。

注意：在 HP-UX 和 Sun Solaris 2.5（及更高版本）上，为文件系统 ACL 提供支持。 在其他平台和操作系统版本上，只支持传统的文件权限模式。

默认值：no

TNG_Environment

指定是否使用特殊的 Unicenter TNG 类和资源创建数据库。

有效值包括以下各项：

0－在不使用特殊 Unicenter TNG 类的情况下创建数据库。

1－使用所有特殊的 Unicenter TNG 类创建数据库。

默认值：0

TNGDir

指定 Unicenter TNG 的安装目录。

有效值为基本 Unicenter TNG 目录（即 .uniprodloc）。

无默认值

TRUEPATH

指定 CA Access Control 所在的物理目录。 CA Access Control 目录可以是指向另一物理位置的符号链接。此标记指向安装 CA Access Control 的实际物理位置。

默认值：*ACInstallDir*

use_rpc_protocol

确定是否需要 RPC portmapper。 如果要使用旧的 (1.43) CA Access Control 协议，则必须显示 RPC portmapper。 支持 NIS+ 密码更改需要这一旧协议。

此内标识替换 old_protocol 内标识。

有效值包括以下各项：

yes－使用 RPC portmapper 来指定端口。

no－使用由 ServicePort 标记指定的端口。

默认值：no

更多信息：

sebuildla 实用程序－创建后备数据库 (p. 105)
seldapcred 实用程序－加密和存储凭据 (p. 167)
sepass 实用程序－设置或替换密码 (p. 180)

SEOS_syscall

在 [SEOS_syscall] 部分中，以下标记由 SEOS_syscall 内核模块使用。

bypass_NFS

确定是否回避 SEOS 事件中的 NFS 文件。

有效值包括以下各项：

0－不跳过 NFS 文件。
1－跳过 NFS 文件。

默认值：0

bypass_realpath

指定是否跳过实际文件路径解析而进行授权。

如果启用此设置 (1)，CA Access Control 将不解析文件路径而进行授权。 这样可以加快文件事件的处理。但是，对于使用链接进行的文件访问不会强制执行通用规则。

示例：如果启用此设置并且用户从链接访问 /realpath/files/* 目录中的文件，则对于此目录将不考虑拒绝访问规则。 对于链接 (/alternatepath/*) 也需要具有通用规则。

默认值：0

cache_enabled

确定是否使用缓存进行完整路径解析，以确定文件的访问权限。

有效值包括以下各项：

0－不缓存。
1－使用缓存。

默认值：0

cache_rate

确定当为完整路径解析启用缓存时，将会使用的缓存速率。

值越大，表示缓存越好。

默认值：10000

call_tripAccept_from_seload

确定是否在 CA Access Control 启动后从 seload 命令调用 tripAccept，如果调用 tripAccept，则定义以逗号分隔的 TCP/IP 端口列表，tripAccept 将连接到这些端口并唤醒端口侦听器。

有效值为任意 TCP/IP 端口号，以及：

0－不从 seload 调用 tripAccept。

限制：0－64000

默认值：0

cdserver_conn_res

确定是否将 T_CONN_RES 数据流消息视为 UnixWare 上 fiwput 例程中的高优先级消息。

有效值包括：

1－将 T_CONN_RES 数据流消息作为 fiwput 例程中的高优先级消息进行处理。

0－将 T_CONN_RES 数据流消息作为 fiwput 例程中的低优先级消息进行处理。

默认值：0（在 UnixWare 上应为 1）

debug_protect

确定是否允许在 CA Access Control 运行期间调试任何程序。

有效值包括以下各项：

0－允许调试。
1－不允许调试。

默认值：1

DESCENDENT_dependent

确定 SEOS 后台进程的子级是否可以注册 SEOS 服务。

有效值包括以下各项：

0－任何程序都可以注册 SEOS 服务。
1－只有后代可以注册 SEOS 服务。

默认值：0

exec_read_enabled

指定 CA Access Control 内核是否识别脚本执行。

有效值包括以下各项：

0－CA Access Control 内核不识别脚本执行。

1－CA Access Control 内核识别脚本执行。

默认值：0

注意：如果 特权用户密码管理 代理安装在端点上，默认值为 1。 启用此标记后，特权用户密码管理 代理无需将 shell 脚本定义为 PROGRAM 资源，即可识别使用 特权用户密码管理 代理文件 (acpwd) 的已命名 shell 脚本。

file_bypass

指明 CA Access Control 是否检查数据库中未定义文件的文件访问权限。 默认情况下，CA Access Control 不检查数据库中未定义的文件。

有效值包括以下各项：

-1－不检查任何文件。
0－检查所有文件。

默认值：-1

GAC_root

确定当用户为 root 时，是否对文件使用 GAC 缓存。 默认情况下，不会在用户为 root 用户时使用 GAC。

有效值包括以下各项：

0－不为 root 用户使用缓存。
1－为 root 用户使用缓存。

默认值：0

HPUX11_SeOS_Syscall_number

确定与 HP-UX 上的 SEOS_syscall 通讯的默认 syscall 编号。

有效值包括 sysent 中所有未使用的 syscall 条目编号。

默认值：254

kill_signal_mask

定义要保护哪些信号。

有效值包括对希望 SEOS 事件用于的所有信号进行 OR（包括）运算的掩码。

默认值：SIGKILL、SIGSTOP 或 SIGTERM 事件。实际值根据平台不同而有所差异：

- HP-UX：0x804100
- Sun Solaris：0x404100
- IBM AIX 和 Digital DEC UNIX：0x14100
- Linux：0x44100

link_protect

确定是否会保护符号链接。

有效值包括以下各项：

0－不保护链接。
1－保护链接。

默认值：0

max_generic_file_rules

定义数据库中允许的最大一般文件规则数。

注意：如果使用非常大的值，则可能会导致不同平台上出现异常行为。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

有效值包括大于 (>) 511 的所有数字。

注意：只有 AIX、HP、Linux 和 Solaris 支持此标记。

默认值：512

max_regular_file_rules

定义数据库中允许的最大文件规则数。

注意：如果使用非常大的值，则可能会导致不同平台上出现异常行为。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

有效值包括大于 (>) 4095 的所有数字。

注意：只有 AIX、HP、Linux 和 Solaris 支持此标记。

默认值：4096

mount_protect

确定是否允许挂接和取消挂接由 CA Access Control 使用的目录。

有效值包括以下各项：

0－允许挂接。
1－不允许挂接。

默认值：1

proc_bypass

确定当文件属于进程文件系统 (/proc) 时是否检查文件访问权限。 有效值包括以下各项：

0－忽略标记

1－跳过文件访问检查

默认值：1

SEOS_network_intercept_type

指定要使用的网络截获类型（仅 HP-UX）。

注意：必须还要设置 SEOS_use_streams = yes

有效值包括：

0—TCP hook

1—数据流

默认值：1

重要说明！ 请勿自行修改此标记。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

SEOS_streams_attach

指定 CA Access Control 是否附带运行 STREAMS。

如果更改此设置，则需要重新启动已侦听网络的后台进程，以使 CA Access Control 保护这些后台进程。

注意：此设置仅适用于 Solaris 9 或更早期的版本。

默认值：yes

SEOS_unload_enabled

确定是否可以卸载 SEOS_syscall 内核模块。

有效值包括以下各项：

0—不允许卸载。
1—允许卸载。

默认值：1

SEOS_use_ioctl

指定 CA Access Control 内核模块的通讯方式（ioctl 或系统调用）。

当操作系统正在使用所有可用的系统调用号时，可以使用 *ioctl* 通讯方式。

值：0—系统调用 **1**—ioctl

默认值：0

重要说明！ 请勿自行修改此标记。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

SEOS_use_streams

指定是否使用数据流子系统进行网络拦截（SEOS_load 是否自动将模块推入数据流）。

此设置仅可用于 HP-UX 和 Sun Solaris 版本 8 和 9。

默认值： no

silent_admin

定义维护用户的用户 ID。 在停止安全保护且 silent_deny 为 *yes* 时，则允许此用户的活动。 使用用户的数字 UNIX UID 定义维护用户。

默认值： 0（root 的用户 ID）

silent_deny

确定在关闭安全保护时是否拒绝所有事件。

有效值包括以下各项：

yes－启用静默拒绝（维护模式）。

no－禁用静默拒绝。

默认值： no

STAT_intercept

指定 stat 系统调用发生时是否检查文件访问权限。

如果指定 1（检查文件访问权限），对于没有 *读取*权限的用户，CA Access Control 将不允许其执行获取有关文件信息的操作，并在审核日志中记录 *读取*。如果将此标记设置为 0，则任何用户均可获取文件信息。

值： 0（不检查文件访问权限），1（检查文件访问权限）。

默认值： 0

STOP_enabled

确定是否使用 STOP 功能从而防御堆栈溢出攻击。

有效值包括以下各项：

0－关。
1－开。

默认值： 0

synchronize_fork

确定如何管理派生同步。

在 *HP-UX 平台*上

1－父项报告再生
2－子项报告再生

在*其他平台*上

1－父项只进行报告而不进行同步
2－父项既进行报告又进行同步（在 Linux 上不受支持）

限制：任何小于 1 的值都被解析为 1。任何大于 1 的值都被解析为 2。

注意：不要修改此设置，因为这样可能会导致不同平台上出现异常行为。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

默认值：1

syscall_monitor_enabled

指定 CA Access Control 是否监控正在执行 CA Access Control 代码的进程。如果您已启用此功能(默认设置)，则可以使用 *secons -s* 或 *secons -scl* 查看这些进程。

有效值包括：

0－不活动

1－活动

默认值：1

threshold_time

定义截获的系统调用在被认为存在风险之前可被阻止的时间（秒）。如果一个进程被阻止的时间长于此时间，CA Access Control 将报告 SEOS_syscall 模块卸载可能失败。

注意：此值将影响 CA Access Control 提供的卸载准备情况报告。 有关详细信息，请参阅*《企业管理指南》*。

默认值：60

trace_enabled

确定是否使用 SEOS_syscall 循环跟踪缓冲区。

有效值包括以下各项：

0－不使用跟踪。
1－使用跟踪。

默认值：0

use_tripAccept

确定在卸载 SEOS_syscall 时是否使用 tripAccept 实用程序唤醒受阻的接受系统调用。 这将避免在卸载模块后运行 SEOS_syscall 代码。

有效值包括 yes 和 no。

默认值：yes

seosd

在 [seosd] 部分中，标记确定授权后台进程和缓存实用程序的行为，从而提高它们的性能。

bypass_filenames

指定包含要从 seos 事件中免除的文件名列表的文件。

例如：bypass_filenames = /opt/CA/AccessControl//bin/bypass_filenames

默认值：标记未设置

bypass_nfs_port

指定是否为 CONNECT 跳过由 nfs 使用的端口（端口 2049）。 跳过该端口的目的是让 NFS 能够正确运行。

如果将此标记的值更改为 *no*，则不跳过该端口。 确保过后提供所需的 CA Access Control 规则以替换此跳过。下面是此类规则的一个示例（*不能*按原样使用）：

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
nr TCP 2049 owner(nobody) defaccess(none)
authorize TCP 2049 hostnet(all) access(w) uid(root)
nr TCP nfsd owner(nobody) defaccess(none)
authorize TCP nfsd hostnet(all) access(w) uid(root)
```

注意：如果将此标记的值设置为 *no*，但未提供正确的 CA Access Control 规则，NFS 将停止运行。

默认值：yes

bypass_outgoing_TCPIP

定义以逗号分隔的端口列表，seos_syscall 不会将这些端口的传出连接事件传递给 seosd。

默认值：标记未设置

bypass_suid_for_login

指定应对其忽略 dummy SUID 系统调用的登录程序的路径。

此标记将在某些登录程序（例如：samba）中使用，这些程序将生成大量的虚拟 SUID 系统调用。 这些系统调用可能会影响对登录用户的正确识别。

默认值：无

bypass_suid_program

允许多个 su 命令。在某些平台上，系统的 su 二进制文件以非标准方式运行：当请求对非 root 用户执行 su 命令时，它会先对 root 用户执行 su，然后再对请求的用户执行 su。

如果 CA Access Control 为该 root 用户设置了代理保护，它可能也会阻止对非 root 用户成功执行 su。

要想在此类平台上对 root 用户使用 surrogate 保护，并且仍旧可以不中断地对非 root 用户执行 su，请将 bypass_suid_program 内标识设置为包含系统的 su 二进制文件的真实路径。

默认值：无

bypass_system_files

确定 CA Access Control 授权引擎是否应跳过对 /etc/passwd 和 /etc/group 系统文件的读取访问。

有效值包括：

yes－跳过对系统文件的读取访问权限。

no－不跳过对系统文件的读取访问权限。

默认值：yes

bypass_TCPIP

允许您添加 seos_syscall 无法通过其将事件传递给 seosd 的一个或多个端口（以逗号分隔）。

语法为 *bypass_TCPIP=port1[,*port2,portx]

默认值：标记未设置

bypass_xdm_ports

是否为 CONNECT 跳过由 XDM 使用的端口（端口 6000-6010）。 跳过该端口的目的是让 xdm 能够正确运行。

如果将此标记的值更改为 *no*，则不跳过这些端口。 确保过后提供所需的 CA Access Control 规则以替换此跳过。下面是此类规则的一个示例（*不能*按原样使用）：

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
nr TCP X-Win owner(nobody) defaccess(none)
authorize TCP X_Win hostnet(all) access(r)
authorize TCP X_Win hostnet(all) access(w) uid(root)
authorize TCP X_Win hostnet(all) access(w) gid(mygroup)
nr TCP 6000 owner(nobody) defaccess(none)
authorize TCP 6000 hostnet(all) access(r)
authorize TCP 6000 hostnet(all) access(w) uid(root)
authorize TCP 6000 hostnet(all) access(w) gid(mygroup)
```

注意：如果将此标记的值设置为 *no*，但未提供正确的 CA Access Control 规则，xdm 将停止运行。 如果此标记的值为 *yes*，且通过端口 6000-6010 进行传出连接，则相应审核记录中的类名为 TERMINAL。

默认值：yes

cron_program

改进 seosd 中的 cron 登录的检查。

将 cron_program 内标识设置为包含系统的 cron 二进制文件的真实路径。

默认值：无

dbdir

指定 CA Access Control 数据库的位置。

默认值：*ACInstallDir*/seosdb

device_file

指定是否扫描 /dev 中的所有设备。

如果将此标记的值设置为 Yes，并且在标准列表中找不到 tty，则 CA Access Control 将扫描位于 /dev 中的所有设备。

（qplib 从标准设备中解析 tty 名称。）

注意：您可以将设备添加到 tty 名称列表中。

默认值：no

dns_server

指定 DNS 服务器名，它用来将主机解析从默认服务器更改为另一台服务器。

此内标识通常在启用 DNS 缓存选项时使用。

默认值：无

domain_names

指定为进行授权，seosd 向所接收的短主机名附加的域名列表（目的是创建完全限定名称），因此可以在有关的 HOST、CONNECT 或 TERMINAL 类中对这些名称进行授权。

为标识全名，seosd 会尝试在短名称中附加 domain_names 列表中的域名，从而进行授权。

seosd 首先会仅使用短名称在其数据库中寻找有关的规则。如果找不到与短名称匹配的记录，则它会逐个附加在 domain_names 标记中指定的每个域名，直到找到匹配的记录为止。

例如：假设您为 domain_names 指定以下列表：

domain_names= market.com, journey.com, total.com

以下是当订户 *acme*（未在数据库中定义为规则）的请求进入时 seosd 处理匹配进程的方式：

acme（在数据库中找不到）
acme.market.com（找不到）
acme.journey.com（找不到）
acme.total.com（已找到）

seosd 将使用匹配的第一个记录（在本例中为 acme.total.com）执行授权。

默认值：如 /etc/resolv.conf 中所定义

EnablePolicyCache

确定是否应该使用运行时表来存储授权所需要的数据库值。 运行时表是在 seosd 启动时加载到内存中的。这样就避免了连接数据库，因此可以缩短授权时间。

有效值包括 yes 和 no。

默认值：no

enf_register

确定 seosd 是否向 Unicenter NSM Event Notification Facility (ENF) 注册。

有效值包括以下各项：

yes—seosd 向 ENF 注册。

no—seosd 不向 ENF 注册。

默认值：no

FileCache_auths

如果启用缓存，则应指定授权池中的记录数。 可缓存的最大授权记录数为 800。

默认值：80

FileCache_CleanInt

指定清除文件缓存的频率（分钟）。

默认值：60

FileCache_files

如果启用缓存，则应指定文件池中的记录数。 可缓存的最大文件记录数为 200。

默认值：20

FileCache_InitPrio

指定缓存表中的新记录的初始优先级值。

默认值：10

FileCache_PriorInt

如果启用缓存，则应指定在缓存表中重新计算优先级的频率。 每次保存一个新记录就会计入一

默认值：1

FileCache_users

如果启用缓存，则应指定用户池中的记录数。 可缓存的最大用户记录数为 500。

默认值：50

get_login_terminal

确定 seosd 是否尝试通过另一种方式查找登录程序的对等地址。它对于诸如 ssh 等的连接非常有用。

有效值包括 yes 和 no。

默认值：yes

grace_admin

确定管理员更改用户密码时设置的宽限登录的次数。

默认值：标记未设置 (1)

GroupidResolution

确定 CA Access Control 将 GID 号解析为组名的方式。

有效值包括以下各项：

system—CA Access Control 使用系统调用来转换 GID 号。 该值可用于单机、DNS 客户端和 DNS 服务器站。-（另请参阅此表中的 resolve_timeout 标记。）

cache—GID 号和组名都将缓存在 seosd 中。 这是最快、最简单的转换方法，但是运行时无法对缓存进行更新。

ladb—CA Access Control 使用后备数据库来转换 GID 号。 每次更新相关事务表时，都必须运行 sebuildla 实用程序来重新创建 lookaside 数据库。

对于 NIS 和 NIS+ 服务器，您可以使用 cache 或 ladb。

对于 Sun Solaris 2.5 及更高版本和 HP-UX 11.x，您同样可以使用 cache 或 ladb。

对于所有的工作站，将首选值 ladb。

默认值：标记未设置 (system)

HostResolution

确定 CA Access Control 将 IP 地址解析为主机名的方式。

有效值包括以下各项：

system－CA Access Control 使用系统调用来转换 IP 地址。该值可用于单机、NIS/NIS+ 客户端和 DNS 客户端站。-（另请参阅此表中的 resolve_timeout 标记。）

cache－主机名及其 IP 地址全部缓存在 seosd 中。 这是最快、最简单的转换方法，但是运行时无法对缓存进行更新。

ladb－CA Access Control 使用后备数据库来转换 IP 地址。每次更新相关事务表时，都必须运行 sebuildla 实用程序来重新创建 lookaside 数据库。

对于 NIS、NIS+ 及 DNS 服务器，您可以使用 cache 或 ladb；值 ladb 是首选设置。

默认值：标记未设置 (system)

IsolatedDaemon

确定 seosd 是否在文件描述符 stdin、stdout 和 stderr 成为后台进程时关闭它们。

有效值包括以下各项：

yes－seosd 会在文件描述符变成后台进程时关闭它们。

no－seosd 不会在文件描述符变成后台进程时关闭它们。

默认值：no

kill_ignore

指定 seosd 是否忽略（拒绝）定向到三个主要 CA Access Control 后台进程之一的“kill -9”命令。 有效值包括以下各项：

yes－忽略 kill 命令。 这是默认值。

no－kill 命令将终止 seosd。

默认值：yes

login_parent_check

指定父进程应该继续（一旦子进程已登录）登录序列，还是放弃该序列并继承子进程的登录。

有效值包括 0 和 1。

如果该值为 0，则父进程将继续登录序列。

如果该值为 1，则父进程将放弃登录序列并继承子进程的登录。

默认值：标记未设置 (0)

lookaside_allowdupuid

确定 sebuildla 是否注册重复的 UID

有效值:

yes—注册重复的 UID

no—在出现重复的 UID 时，只注册一个 UID

注意：重复的 UID 可能会在 UNIX 操作系统上造成不一致

默认值：no

lookaside_path

指定后备数据库所在的目录。 请在运行 sebuildla 实用程序之前创建此目录。

注意：后备数据库文件是使用 sebuildla 实用程序创建和更新的。

默认值：*ACInstallDir*/ladb

max_loggedin_users

定义最多登录用户人数。

注意：该值决定着其中一个内部内存表的大小。 表越大，其占用的内存越多。

限制：4096-20480

默认值：8192

MultiLoginPgm

定义执行多次登录的程序的名称和完整路径。 此标记用于为这些特殊的登录应用程序检测正确的登录顺序。

MultiLoginPgm 是带有完整路径的登录应用程序的名称。

默认值：none

network_cache_timeout

指定在使用网络缓存的情况下，网络每隔多长时间缓存一次表清除（分钟）。 使用此标记可以为存储的已接受传入 TCP 请求设置时间限制。

注意：有关使用网络缓存的详细信息，请参阅*《适用于 UNIX 的端点管理指南》*。

默认值：10

nfs_devices

指定包含 NFS 主设备号的文件的名称和路径。指定完整的文件路径。

如果 CA Access Control 无法使用设备和 inode 号获取程序，也无法使用程序的名称获取程序，则将使用此文件。 此文件包含每个平台的主设备号的 NFS 默认值。在不同的系统中，此值可能会有所差异。为找到您所用系统的编号，请使用包含 UNIX getmajor() 函数的小程序。然后编辑 nfsdevs.init 文件（或使用此标记命名的文件）以包含要查找的编号。

注意：每次挂接和取消挂接 NFS 系统时，您都应该更新 nfsdevs.init 文件。 您还可以仅使用该设备的前四位数字。 这些编号将保留不变（即使您取消挂接并重新挂接该系统，也是一样）。

默认值：*ACInstallDir*/etc/nfsdevs.init

protect_bin

指定 seosd 是否保护 CA Access Control 二进制文件。 指定以下值之一：

yes－seosd 将保护 CA Access Control 二进制文件，除非定义允许此类访问的规则。

注意：当 FILE 记录的 _default 访问权限为 none 时，请不要指定 yes，因为那样的话，除非所有的 /opt/CA/AccessControl//bin 文件都包含 FILE 记录，否则文件的不可访问性可能会导致 CA Access Control 不能用。

no－seosd 不保护 CA Access Control 二进制文件。

默认值：no

resolve_rebind

指定 seosd 在出现超时故障后是否重新与 NIS 服务器建立连接。-

强烈建议您不要更改默认值。

默认值：yes

resolve_timeout

指定 seosd 尝试将 IP 解析为地址、将用户 ID 解析为用户名、将组 ID 解析为组名，或将服务端口号解析为服务名的最大秒数。

该值在以下两种情况下生效：

当 seosd 使用系统解析时。（请参阅 HostResolution、ServiceResolution、UseridResolution 及 GroupidResolution 标记。）

将 under_NIS_server 内标识设置为 no 时。

如果指定时间过后没有任何解析，seosd 会假定指定的 IP、ID 或端口没有解析。

如果将该值设置为 0，则没有超时。

默认值：5

rt_priority

确定 seosd 是否具有实时优先级。

有效值包括 yes 和 no

如果将此内标识设置为 yes，seosd 将具有实时优先级。

默认值：yes

ServiceResolution

确定 CA Access Control 将 TCP 端口号转换为服务名的方式。

有效值包括以下各项：

system—CA Access Control 使用系统调用来转换 TCP 端口号。此值可用于单机、NIS/NIS+ 客户端、DNS 客户端以及 DNS 服务器站。-（另请参阅此表中的 resolve_timeout 标记。）

cache—服务名及其 TCP 端口号都将缓存在 seosd 中。这是最快、最简单的转换方法，但是运行时无法对缓存进行更新。

ladb—CA Access Control 使用后备数据库来转换 TCP 端口号。每次更新相关事务表时，都必须运行 sebuildla 实用程序来重新创建 lookaside 数据库。

对于 NIS 和 NIS+ 服务器，请使用 cache 或 ladb。

默认值：system

sim_login_timeout

定义 CA Access Control 从 Accessor Element Entry 表 (ACEE) 中删除未使用的模拟登录用户条目之前的超时时间（分钟）。

当 CA Access Control 需要访问可在 ACEE 中找到的信息时，它会执行模拟登录以创建 ACEE 条目。

默认值：60

special_check

指定是否在内核模块加载时启用文件路径检查。如果启用，CA Access Control 将检查要加载的内核模块是否与 KMODULE 记录的文件路径属性相匹配（对于非 Linux 系统），或者是否与 KMODULE 记录的签名相匹配（对于 Linux 系统）。

默认值：no

terminal_default_ignore

确定在授权管理访问权限时，是否考虑 _default TERMINAL 和特定 TERMINAL 记录的 defaccess 值。

有效值包括 yes 和 no。

yes－管理权限将忽略 _default 和任何特定 TERMINAL 记录的 defaccess 值。 在这种情况下，对于相关的特定 TERMINAL 记录，管理权限需要显示授权规则。

no－管理权限将考虑所有相关的 TERMINAL 记录的 defaccess 值，而无论它是 _default 记录还是特定记录。

默认值：yes

terminal_search_order

指定 seosd 是否尝试先按名称再按 IP 地址来检查所定义的 TERMINAL。

有效值包括：

name－先按名称再按 IP 地址来检查 TERMINAL。

ip－先按 IP 地址再按名称来检查 TERMINAL。

注意：TERMINAL 类支持由通配符定义的一般规则（IP 地址或主机名模式匹配）。 *始终*先检查特定（全名）规则，然后再检查一般规则。例如：如果将此设置为 *ip*，seosd 将按照以下顺序查找 TERMINAL 资源：完整 IP 地址匹配、完整主机名匹配、IP 地址模式匹配、主机名模式匹配。

默认值：name

trace_file

指定将跟踪消息发送到的文件名称（如果请求跟踪消息）。

默认值：*ACInstallDir*/log/seosd.trace

trace_file_type

确定跟踪文件是采用二进制格式还是文本格式写入的。

有效值包括以下各项：

二进制－跟踪文件应该采用二进制格式写入。 此选项将减少此文件占据的空间。

文本－跟踪文件应以文本格式写入。

后台进程 seosd 将检查此标记的值，并将其与跟踪文件的内容进行比较。如果该标记的值与跟踪文件的格式不匹配，则 seosd 会将跟踪文件保存在其名称下并添加扩展名 .backup。

默认值：text

trace_filter

指定包含用于筛选跟踪消息的筛选数据的文件的名称和路径。

默认值：*ACInstallDir*/data/*language*/etc/trcfilter.init

trace_space_saver

指定要在文件系统中保留的可用空间量（MB）。 当可用空间量小于此数量时，CA Access Control 将禁用跟踪。

注意：即使以后会有更多的可用空间，**也不会自动启用跟踪。**

默认值：512

trace_to

指定跟踪消息的目标。

有效值包括以下各项：

file－CA Access Control 会将跟踪消息发送至 trace_file 标记指定的文件中。 要禁用跟踪，请使用 *secons -t-* 命令。 有关详细信息，请参阅此表中的 trace_file 标记。

file,stop－CA Access Control 将在初始化后台进程期间生成跟踪消息。初始化后台进程之后，将停止生成跟踪消息。

none－CA Access Control 不发出跟踪消息。 这是安装并实施 CA Access Control 后的正常设置。

注意：如果将此标记设置为 **file** 或 **file,stop**，则可以使用带有 -t 选项的 secons 命令来切换 CA Access Control 跟踪。

默认值：file,stop

UpdSurrogLogin

指定 CA Access Control 是否在代理登录时更新用户的最后访问时间。

有效值包括：

1－CA Access Control 将在代理登录时更新用户的最后访问时间。

0－CA Access Control 将在代理登录时*不*更新用户的最后访问时间。

Undef_ForPacl

确定当 PACL 中的访问者名称包含星号 (*) 时，seosd 是否检查未定义的用户。

有效值包括以下各项：

1－seosd 不包括 PACL 中带星号的未定义用户。

0－seosd 包括 PACL 中带星号的未定义用户。

默认值：0

under_NIS_server

确定 seosd 是否使用内部名称解析替代系统名称解析。

有效值包括以下各项：

yes－seosd 将在启动过程中把所有用户、组、主机和端口信息存储在内存或后备数据库中（请参阅 use_lookaside 标记）。

对于 NIS、NIS+ 和 DNS 服务器计算机，以及以下操作系统，此内标识是必需的：Sun Solaris 2.5 及更高版本、HP-UX 11.x、IBM AIX 4.3.x 及 IRIX 6.5。

重要说明！ 如果使用的是 NIS 服务器或上述操作系统之一，关闭此标记可能会导致计算机挂起。

no－seosd 将使用系统名称解析，并且 resolve_timeout 标记将生效。

注意：安装期间自动为此内标识指定值。

该内标识仅具备向后兼容的作用。 如果您具有新安装的 CA Access Control，或者安装的是版本 2 或更高版本，请使用 HostResolution、ServiceResolution、UseridResolution 和 GroupidResolution 标记。

默认值：在安装期间指定

use_lookaside

确定 seosd 将用户、组、主机和端口信息存储在 lookaside 数据库中，还是存储在内存中。

注意：此标记与 under_NIS_server 标记一起使用，并且，除非将 under_NIS_server 标记设置为 yes，否则它没有任何实际意义。

有效值包括以下各项：

yes－seosd 将使用后备数据库存储用户、组、主机和服务详细信息。后备数据库是通过 sebuildla 实用程序构建的，而且可以使用它随时进行刷新。

lookaside 数据库的位置是由 lookaside_path 内标识设置的。

no－seosd 会在启动期间缓存所有用户、组、主机和服务信息，以便可以在内存中完成所有转换。建议您每天都重新启动 seosd 以刷新该缓存。

该内标识仅具备向后兼容的作用。 如果您具有新安装的 CA Access Control，或者安装的是版本 2 或更高版本，请使用 HostResolution、ServiceResolution、UseridResolution 和 GroupidResolution 标记。

默认值：no

use_mapped_user_name

（适用于安装了 CA Access Control 和 UNIX 身份验证代理 的环境）指定 seosd 是否在审核记录中使用用户企业名称。

值：yes、no

默认值：no

use_nfs_devices

确定是否使用 NFS 设备。 有效值包括 yes 或 no。

默认值：Yes

use_standard_functions

确定 NIS 环境中的 sebuildla 检索用户的方式：通过调用标准系统函数 getpwent，或通过分析 ypcat passwd 和 cat/etc/passwd 命令的输出。

有效值包括：

yes－使用标准系统函数 getpwent

no－分析 ypcat passwd 和 cat/etc/passwd 命令的输出。

默认值：yes

use_trusted_script

指定 seosd 是否使用受信任的脚本机制。

使用受托脚本机制时，从 shell 脚本调用的程序将在内部 CA Access Control 表中保留 shell 脚本的名称。

这意味着如果在 PACL 中使用了某个脚本，则这些程序将继承该权限。这还意味着您无法通过 CA Access Control 保护这些程序。

受托脚本的第一行 以 #! 开头。

在**不**使用受托脚本机制时，这些程序将在内部 CA Access Control 表中各自的名称下注册。

默认值：yes

use_unab_db

（适用于安装了 CA Access Control 和 UNIX 身份验证代理 的环境）指定 seosd 是否使用 UNIX 身份验证代理 数据库来解析用户和组名称（如果当前方法无法实现）。此标记与以下标记一致：use_lookaside、UseridResolution、GroupidResolution。

值：yes、no

默认值：no

UseFileCache

指定是否使用文件记录缓存工具来提高性能。

默认值：yes

UseNetworkCache

确定 CA Access Control 是否缓存接受的传入 TCP 请求。

注意：有关使用网络缓存的详细信息，请参阅 *《适用于 UNIX 的端点管理指南》*。

有效值包括 yes 和 no。

默认值：no

UseridResolution

指定 CA Access Control 将 UID 号转换为用户名的方式。

有效值包括以下各项：

system—CA Access Control 使用系统调用来转换 UID 号。 此值可用于单机、NIS/NIS+ 客户端、DNS 客户端以及 DNS 服务器站。-

cache—用户名及其 UID 号都将缓存在 seosd 中。 这是最快、最简单的转换方法，但是运行时无法对缓存进行更新。

ladb—CA Access Control 使用后备数据库来转换 UID 号。 每次更新相关事务表时，都必须运行 sebuildla 实用程序来重新创建 lookaside 数据库。

对于 NIS 和 NIS+ 服务器、Sun Solaris 2.5 及更高版本或 HP-UX 11.x 操作系统，您必须使用 cache 或 ladb。

默认值： system

watchdog_refresh

确定 seosd 是否将刷新 Watchdog 以在特权程序和安全文件中扫描每个文件句柄。

有效值包括以下各项：

yes—seosd 将刷新 Watchdog。

no—seosd 将不刷新 Watchdog。

默认值： no

seosdb

在 [seosdb] 部分中，以下标记管理数据库检查和重建。

CheckAlways

确定是否应在 CA Access Control 初始化时检查数据库是否损坏。

有效值包括 yes 和 no。

默认值： yes

CheckProgram

指定要使用的替代命令的完整路径和参数，而不是用于检查数据库的内部代码。 如果数据库有效，则该命令应返回 0，如果数据库存在应更正的问题，则返回非零数字。

默认值： 标记未设置（与使用 *dbmgr -u -fast* 一样，不运行任何程序）

CreateNewClasses

指定您是否可以在数据库中添加使用 seclassadm 工具新建的类。

有效值包括 yes 和 no。

默认值：yes

CreateNewProps

指定是否要在 CA Access Control sepropadm 实用程序创建新数据库属性时将有关新属性的数据保存在文件中。

有效值包括 yes 和 no。

如果值为 yes，则 sepropadm 会将有关新属性的数据保存在文件中，并且在 dbmgr -c 实用程序以后生成新的 CA Access Control 数据库时，dbmgr 将会使用此文件在该数据库中添加这些属性。

默认值：yes

RebuildAlways

指明是否应该始终在初始化 CA Access Control 时重建 CA Access Control 数据库。

有效值包括 yes 和 no。

默认值：no

RebuildProgram

指定要使用的替代命令的完整路径和参数，而不是用于纠正数据库的内部代码。

默认值：不设置标记（不运行任何程序，相当于使用 *dbmgr -u -build all*）

seoswd

在 [seoswd] 部分中，以下标记确定 Watchdog 的行为。

BlockingInterval

指定 watchdog 等待主要后台进程响应的时间间隔（秒）。 如果超过此时间，watchdog 会向主要后台进程发送信号。

默认值：60

IgnoreScanInterval

指定是否按特定时间间隔扫描程序和文件。

如果该内标识的值为 no，则 Watchdog 将执行间隔扫描；如果为 yes，则它不会按时间间隔进行扫描。

注意：如果您不使用 PgmTestTime 或 SecFileTestTime 标记指定扫描时间，并且此标记设置为 yes，则 Watchdog 不会对受托程序或受保护的文件分别进行扫描。

默认值：no

PgmRest

指定从最后一个事件完成到准备再次检查程序之间的时间段（秒）。该程序进行休息是为了防止系统过载。

默认值：10

PgmTestInterval

指定对受信任程序进行重新扫描之间的时间间隔（秒）。

注意：如果该值等于或大于一天（86400 秒），则 IgnoreScanInterval 的默认值为 *yes*。

默认值：18000（5 小时）

PgmTestStartTime

指定对受信任程序进行第一次扫描的开始时间 *(*采用 hh:mm 格式)。

如果您不设置此内标识，则 Watchdog 将在启动之后立即执行第一次扫描。

无默认值。

PgmTestTime

指定受托程序的固定扫描时间（采用 *hh:mm* 格式）。 可以指定多个扫描时间，以空格来分隔。

注意：如果您不指定扫描时间并且将 IgnoreScanInterval 标记设置为 yes，则 Watchdog 将不会扫描受托程序。

无默认值。

policyfetcher_refresh_interval

指定验证 policyfetcher 后台进程是否在运行的时间间隔（秒）。

默认值：600

RefreshParams

指定 seos.ini 内标识的 Watchdog 进行相继读取之间的时间间隔（秒）。

默认值：86400（1 天）

SecFileRest

指定从最后一个事件完成到准备再次检查安全文件之间的时间段（秒）。 Watchdog 进行休息是为了防止系统过载。

注意：如果您不指定扫描时间并且将 IgnoreScanInterval 标记设置为 yes，则 seoswd 将不会扫描受保护文件。

默认值：10

SecFileTestInterval

指定对安全文件进行重新扫描之间的时间间隔（秒）。

默认值：36000（10 小时）

SecFileTestStartTime

指定对安全文件进行第一次扫描的开始时间（采用 *hh*:mm 格式）。

如果未指定任何值，则 Watchdog 将会在 CA Access Control 后台进程启动后很短的时间内执行第一次扫描。

无默认值。

SecFileTestTime

指定受保护文件的固定扫描时间（采用 *hh:mm* 格式）。 可以指定多个扫描时间，以空格来分隔。

无默认值。

SeosAYT

指定 Watchdog 检查后台进程 seosd 之间的时间间隔（秒）。

重要说明！ 请勿自行修改此标记，因为不正确的值可能会导致 CA Access Control 操作中发生重大问题。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

默认值：60

SignalMinInterval

指定在 HUP 信号按需触发一次性扫描后为防止系统过载而执行扫描的时间间隔（秒）。-

注意：对于受信任程序和安全文件均可以执行按需扫描。

默认值：60

UnTrustMissing

确定 Watchdog 是否应尝试取消对某个程序或文件的信任，即使它找不到该程序或文件（例如：如果删除了该文件或者没有挂接相关的 NFS 分区)。

有效值包括以下各项：

yes—尝试对缺少的文件取消受托。

no—不尝试对缺少的文件取消受托。

默认值：yes

unab_check_enabled

指定是否保护身份验证后台进程。

值：yes、no

默认值：no

unab_refresh_interval

指定验证身份验证后台进程是否在运行的时间间隔（秒）。

默认值：600

VerifyCtime

指定 CA Access Control Watchdog 是否检查上次对受托程序和受保护文件的文件状态进行更改的时间。

有效值包括 yes 或 no。

默认值：no

serevu

在 [serevu] 部分中，标记确定 serevu 实用程序的属性。

config_file

指定 serevu 配置文件的位置。

默认值：*ACInstallDir*/etc/serevu.cfg

def_diff_time

指定时间间隔，在此期间 serevu 扫描失败登录的相关系统。

该值可指定为秒（即 300）或分钟（即 5m）。

例如：如果将此内标识设置为 300，则 serevu 会搜索在之前的 300 秒内发生的失败登录。

建议您此值为 def_sleep_time 标记中值的偶数倍。

默认值：5m（5 分钟）

def_disable_time

指定由于过多的失败登录尝试次数而禁用用户帐户的时间。

该值可指定为秒（即 300）或分钟（即 5m）。

默认值：6m（6 分钟）

def_fail_count

指定授予每个用户在标记 def_diff_time 中每段时间内失败登录的次数。

在指定时间段内至少有此失败登录次数的用户，会被禁用。

注意：建议您始终使失败登录次数与系统上设置的允许失败登录尝试的值相同。 例如：在 Sun Solaris 中，使用 /etc/default/login 文件中的 RETRIES 标记设置该系统值。

对于 Solaris，默认值为 5，对于 HP-UX 和 AIX，默认值为 3。 有关详细信息，请参阅操作系统文档。

默认值：5

def_sleep_time

指定连续 serevu 检查之间的时间。

该值可指定为秒（即 120）或分钟（即 2m）。

默认值：2m（2 分钟）

save_disable_path

指定禁用用户帐户列表的位置，以便在关闭时，serevu 可以处理禁用用户。

默认值：*ACInstallDir*/log/serevu_disable.users

更多信息：

serevu 实用程序－处理失败的登录尝试 (p. 206)

sesu

在 [sesu] 部分中，以下标记控制以您自己以外的其他用户身份而又不必输入其他用户密码的登录。

AlwaysTargetShell

确定使用目标 shell（SysV 样式）还是调用程序 shell（BSD 样式）。如果该标记的值为 yes，则 CA Access Control 将使用目标用户 shell。

有效值包括 yes 和 no。

默认值：no

FilterEnv

指定当目标用户为 root 时，sesu 不传递给 shell 的环境变量的列表。用空格或制表符将变量名分隔开。

无默认值。

old_sesu

确定使用旧的 sesu 工具，还是使用新的 sesu 工具。

有效值包括以下各项：

yes－如果在以前的版本中，则使用旧的 sesu 实用程序。

no－新 sesu 实用程序调用本地 su 程序(如 SystemSu 标记中定义的那样），以确保 su 和 sesu 之间的一致性。 如果 SystemSu 内标识无效，则 sesu 会恢复为旧机制。

注意：如果将此标记设置为 no，则会忽略标记 Path、AlwaysTargetShell、sys_env_file 和 FilterEnv。

默认值：yes

路径

指定 sesu 用来设置 PATH 环境变量的值。如果未设置该标记，则 sesu 不会设置 PATH 变量。

无默认值。

request_target_password

指定 *old_sesu* 标记设置为 no 且目标用户对非 root 用户执行 sesu 时，是否请求目标用户的密码。

默认值：yes

sys_env_file

指定包含 sesu 会话的环境变量值的 ASCII 文件。 只有在启动带有“-”参数的 sesu (sesu -) 时，此标记才有意义。 该文件的每一行的格式均为 *variable* = *value*。

默认值： None（IBM AIX 除外，IBM AIX 的默认值为 */etc/environment*）

SystemSu

指定 /bin/su 程序的位置。 如果您在默认位置以外的其他位置中使用程序，请更新此标记。 如果 sesu 找不到授权后台进程，则它将执行在此标记中指定的程序。

注意： 在 AIX 中，请将系统 su 二进制文件替换成指向 sesu 包装程序（而不是 sesu 二进制文件）的符号链接。

默认值： /bin/su

UseInvokerPassword

确定 sesu 是否要求调用程序指定其自己的密码。 如果该标记值设置为 no，则 sesu 不要求指定任何密码。

默认值： no

更多信息：

sesu 实用程序－替代用户 (p. 209)

sesudo

在 [sesudo] 部分中，以下标记确定 sesudo 实用程序的属性。

echo_command

确定 sesudo 是否应在执行命令之前显示命令。 要回显命令，请将该标记的值设置为 yes。

默认值： No

echo_success

确定 sesudo 是否应在成功运行 sesudo 命令时，向终端打印成功消息。

有效值包括 yes 和 no。

默认值： yes

更多信息：

sesudo 实用程序 (p. 211)

standalone

在 [standalone] 部分中，以下标记指定使用独立计算机进行管理的选项。

full_login_check

指定是否将使用 standalone 管理站点视为登录。

有效值包括 0 和 1。

如果将该内标识设置为 1，则将其视为计算机登录。

默认值：0

tcp_communication

在 [tcp_communication] 部分中，此标记用于定义公用 TCP 连接设置。

listening_backlog

定义每个侦听块可以建立的新并发 TCP 连接请求的数目。

默认值：128

tng

在 [tng] 部分中，以下标记控制 CA Access Control 在 Unicenter TNG 环境中的集成。

defsesid

为没有定义特定会话组 ID 的用户，指定默认的会话组 ID。

会话组由 CA SSO 使用。

默认值：CAUNICENTER

ssf_numsubp

指定 sessfgate 后台进程启动以处理传入的 SSF 请求所需的子进程数。

默认值：1

sso_applname

适用于使用 CA SSO 的 CA-Ticket 功能的站点，指定由八个字符组成的字符串，该字符串*必须*与在 seos 主目录下的文件夹 data/keymgmt 中找到的 keymgmt 文件相对应。 这些文件的名称位于 SSO_APPLNAME_key 下。

例如：如果采用了 UNICENTR 的默认值，则文件的名称将为 UNICENTR_key。

默认值：UNICENTR

pmd.ini 文件

在 UNIX 上有效

pmd.ini 文件包含 CA Access Control 在构建和维护特定 PMDB 时使用的各种设置和初始化设置。 该文件包含多个部分，每一部分包含多种设置：

部分	说明
endpoint_management	策略模型端点管理设置。
lang	CA Access Control 管理界面 (selang) 设置，用于与策略模型配合使用。
logmgr	PMDB 日志记录工具设置。
passwd	用户和密码数据设置。
pmd	策略模型后台进程 (sepmdd) 设置。
seos	通用 PMDB 设置。

endpoint_management

[endpoint_management] 部分包含用于为策略模型定义端点管理设置的参数。

debug_mode

指定 CA Access Control 是否将调试消息写入 DMS 目录 (1) 中的 endpoint_management.log 文件。

限制：0、1

默认值：0（禁用调试）

注意：此日志文件位于 *ACInstallDir*/log/endpoint_management.log

operation_mode

指定是否启用通过 CA Access Control 消息队列进行中央 (DMS) 端点管理。

限制：0、1

默认值：1（启用）

lang

[lang] 部分包含 CA Access Control 语言程序 (selang) 在构建和维护 PMDB 时使用的参数。

pre_user_exit

指定 CA Access Control 发出语言命令以更新 UNIX 用户数据库之前要执行的 exit 程序的路径。

post_user_exit

指定 CA Access Control 发出语言命令以更新 UNIX 用户数据库之后要执行的 exit 程序的路径。

pre_group_exit

指定 CA Access Control 发出语言命令以更新 UNIX 组数据库之前要执行的 exit 程序的路径。

post_group_exit

指定 CA Access Control 发出语言命令以更新 UNIX 组数据库之后要执行的 exit 程序的路径。

logmgr

[logmgr] 部分包含 PMDB 日志记录工具所使用的参数。

audit_back

指定 PMDB 审核备份文件的名称。

默认值：pmd_audit.bak

audit_log

指定 PMDB 审核日志文件的名称。

默认值：pmd_audit

audit_group

指定可以读取 PMDB 审核文件的组。如果未指定任何组，则只有 root 用户可以读取审核文件。 CA Access Control 不会验证该标记值，因此如果您输入了无效的组名，CA Access Control 就不会将任何组权限分配到审核日志文件。

要更改现有审核日志文件的组所有权，请执行以下步骤：

1. 使用 selang 命令 chgrp 设置文件的组所有权。
2. 通过输入以下命令，更改 UNIX 权限：

```
chmod 640 /opt/CA/AccessControl//log/seos.audit
```

默认值： none

audit_size

指定 PMDB 审核日志文件的大小（KB）。 不要指定小于 50 KB 的值。

默认值： 50 KB

error_back

指定 PMDB 错误备份文件的名称。

默认值： pmd_error.bak

error_log

指定 PMDB 错误日志文件的名称。

默认值： pmd_error

error_group

指定可以读取 PMDB 错误文件的组。如果未指定任何组，则只有 root 用户可以读取错误文件。 CA Access Control 不会验证该标记值，因此如果您输入了无效的组名，CA Access Control 就不会将任何权限分配到错误日志文件。

要更改现有错误日志文件的组所有权，请执行以下步骤：

1. 使用 selang 命令 chgrp 设置文件的组所有权。
2. 通过输入以下命令，更改 UNIX 权限：

```
chmod 640 /opt/CA/AccessControl//log/seos.error
```

默认值： none

error_size

定义 PMDB 错误日志文件（由 error_log 定义）的最大大小（KB）。

限制： 最小值为 50 KB。

默认值： 50

max_log_size

指定 PMDB 一般日志文件的大小 (KB)。

默认值： 50 KB

pmd_log_level

确定在 PMDB 日志文件中记录的消息。

有效值包括以下各项：

0－不记录任何条目。

1－只列出错误消息。

2－列出错误消息和通知消息。

默认值： 2

use_syslog

确定策略模型后台进程是否应写入 syslog 消息。

默认值： yes

passwd

[passwd] 部分包含 UID 和 GID 的参数。

AllowedGidRange

指定保留的数字。

小于第一个数字且大于第二个数字的整数为 CA Access Control 无法更新的保留 GID。

注意： 如果仅指定了一个整数，则 1 和该指定整数之间的所有整数均为保留的 GID。 如果您指定的数字超过上限，则应用默认的上限 (30000)。 如果您指定一个负数，则应用默认的下限 (1)。

限制： 1 至 2147483647

默认值： 100,30000

AllowedUidRange

指定保留的数字。

小于第一个数字且大于第二个数字的整数为 CA Access Control 无法更新的保留 UID。

注意： 如果仅指定了一个整数，则 1 和该指定整数之间的所有整数均为保留的 UID。

默认值： 100,30000

pmd

[pmd] 部分包含 sepmdd 后台进程在构建和维护 PMDB 时所使用的属性。

_min_retries_

指定 sepmdd 至少应尝试向不可用订户重新发送下一个排队更新的次数。 sepmdd 将遍历订户列表以寻找未完成的更新，并在每次无法将更新重新发送到不可用订户时，使计数器递增。 在达到此标记中指定的最少尝试次数后，会将订户标记不可用状态。

默认值：4

_QD_timeout_

指定 sepmdd 后台进程在第一次扫描其订户列表期间，尝试更新订户数据库时等待的最长时间（秒）。 如果超出此时间而该后台进程仍无法成功更新某个订户，则会忽略该特定订户，并尝试更新列表中的其余订户。

完成订户列表的首次扫描后，sepmdd 会接着执行第二次扫描，在这次扫描期间，它会尝试更新在第一次扫描期间未成功更新的订户。第二次扫描期间，它将尝试更新订阅者，直到连接系统调用超时（大约 90 秒）。

默认值：3

_retry_timeout_

在 _min_retries_ 中指定尝试的最少次数后，指定尝试向不可用订户重新发送更新之前等待的时间（分钟）。 在超过此标记所定义的分钟数后，它将订户标记为可用状态。

直到发生以下情况，订户才会标记为不可用状态：

- 手动发布该用户。
- sepmdd 被手动关闭并重新启动。 在以下情况下会重新启动 sepmdd：
  - 如果有语言工具尝试连接该程序。
  - 如果父 PMDB 要发送更新。
  - pull 选项由订户触发。 在订户上启动 CA Access Control 时，可以进行触发。
- pull 选项由不可用订户触发。

注意：过于频繁地关闭 sepmdd 不可取，因为重新启动后台进程需要花费时间，这会导致整个传播过程变慢。 将该程序始终处于运行状态也不可取，因为这样可能引发一些稳定性问题，但这仅仅是推测。

默认值：30

_shutoff_time_

指定 sepmdd 退出之前的活动时间（分钟）。如果标记值为零，sepmdd 永不退出。

默认值：0

always_propagate

如果此标记设为 no，则策略模型无法执行的命令不会传播给订户。

默认值：none

exclude_file

指定一个排除文件。

排除文件包含应被排除以禁止其接收策略模型更新的主机名（每行一个）。

默认值：none

exclude_localhost

告知 pmdb 排除本地主机，不让它作为订户接收更新。

可能的值：yes、no。

默认值：no

exclude_method

启用/禁用在排除订户时增加更新文件中的偏移量。

值:

“pmdwait”- 不增加偏移量

或者 -“bypass”

默认值：pmdwait

filter

指定筛选文件的名称。

force_auto_truncate

指定 CA Access Control 是否截短更新文件，即使策略模型没有订户。

您可以手动截短更新文件 (sepmd -t)，CA Access Control 也会根据定义触发自动截短事件的单独配置设置 (trigger_auto_truncate) 自动截短文件。

注意：如果策略模型的所有订户都“不同步”，则策略模型实际上没有订户。

默认值：Yes

group_file_name

指定新的 UNIX 组的组文件的名称。sepmdd 会将新的 UNIX 组的组条目保存到此文件中。

默认值：group

is_maker_checker

指定是否使用双重控件。 此标记的有效值是 yes 和 no。

如果选择 yes，则您无法直接更新 PMDB，而只能通过事务进行更新；并且在 PMDB 上实现命令以前，由一个管理员输入的每一事务都必须由其他管理员来执行。

默认值：no

password_file_name

指定新的 UNIX 用户的密码文件的名称。sepmdd 会将新的 UNIX 用户的密码条目存储到此文件中。

默认值：passwd

send_unix_env

指明 sepmd 是否发送策略模型密码文件和组文件的内容。

如果将此内标识设置为 *yes*，则 sepmd -n 选项将发送策略模型密码文件和组文件的内容。

如果将此内标识设置为 *no*，则 sepmd -n 选项不会发送策略模型密码文件和组文件的内容。

默认值：yes

synch_uid

确定 sepmdd 是否尝试在策略模型与其订户之间同步 UID。此标记的有效值是 yes 和 no。

如果此标记为 **no**，则 sepmdd 不会尝试同步 UID。系统会向用户指定每个订户主机上的第一个可用 UID。

如果此标记为 **yes**，则 sepmdd 会尝试同步 UID。例如：如果使用 UID 1000 在 PMDB 上新建一个 UNIX 用户，则 sepmdd 会将该 UID 传输给所有订户。 如果 UID 1000 已被其中一个订户使用，则该订户更新将失败。

仅当发送给 PMDB 的原始命令没有为用户指定 UID 时，sepmdd 才会尝试同步 UID。 如果原始命令指定了 UID，则指定的 UID 会被发送给所有订户。

默认值：yes

TNG_Environment

指定数据库是不是利用特殊的 TNG 类和资源创建的。

有效值包括：

“0”在不使用特殊 TNG 类的情况下创建数据库

“1”使用所有特殊的 TNG 类创建数据库

默认值：0

transaction_lib

指定 maker-checker 策略的路径。

默认值：/opt/CA/eTrustAccessControl/policies/maker

trigger_auto_truncate

定义触发更新文件自动截短功能的策略模型更新文件大小（兆字节）。

如果使用的值小于下限值，CA Access Control 会使用默认值。 如果使用大于上限的值，CA Access Control 将使用上限值。

限制：1-2000 MB

默认值：1024 MB

update_while_processing

在处理传入事件时定义策略模型将命令传播给订户的频率。

频率是 updates_in_chunk 设置的一个因素，并确定在按顺序将命令集发送给下一订户之前 PMD 处理的命令数量。 例如：如果将此设置为 3 且 updates_in_chunk 设置为 10，在一次将命令集 (10) 按顺序发送给下一订户之前，PMD 将会处理 30 个命令。 值为 0 表示 PMD 在处理传入事件时不传播命令。

默认值：1

updates_in_chunk

确定策略模型向每个循环中的每个订阅者发送的最大命令数。

默认值：20

UseEncryption

指定是否加密保存到 updates.dat 文件中的更新信息。

默认值：no

UseShadow

确定在引用 PMDB 本机环境时是否使用卷影文件。

默认值：no

YpServerSecure

指定用于构建 NIS 密码映射的密码 shadow 文件（NIS 服务器上的安全文件）的名称。 仅在将 UseShadow 设置为 yes 时，此标记才有意义。

默认值：/etc/shadow

seos

下表介绍了包含 CA Access Control 所使用的全局设置的 [seos] 部分的标记。

parent_pmd

定义用逗号分隔的策略模型数据库 (PMDB) 列表，此 PMDB 可以从这些数据库接受更新。 此 PMDB 拒绝来自未在此列表中指定的任何 PMDB 的更新。

也可以指定一个包含行分隔 PMDB 列表的文件路径。

将此标记设置为“NO_MASTER_”，以使此 PMDB 接受来自任何 PMDB 的更新。

如果您没有设置此标记，此 PMDB 将不接受来自任何 PMDB 的更新。

按 pmd_name@hostname 格式指定每个 PMDB

例如：

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
parent_pmd = /opt/CA/AccessControl//parent_pmdbs_file
```

默认值：标记未设置（PMDB 不接受来自任何 PMDB 的更新）。

lang.ini 文件

在 UNIX 上有效

本部分说明 lang.ini 文件中由 selang 实用程序使用的标记。

lang.ini 文件包含以下部分：

general

包含适用于多种类型资源（即新资源和新用户）的默认参数。

history

包含 selang 历史信息机制的默认参数。

newres

包含为新资源记录的属性分配的默认值。 除非您明确设置其他值，否则将指定默认值。

newusr

包含为新用户记录的属性分配的默认值。 除非您显式设置其他值，否则将分配默认值。

属性

包含用来指定用户定义属性值的标记，例如用户定义属性的文件位置。-- 标记没有默认值；您必须显式设置它们。

unix

包含从 selang 命令 shell 内向 UNIX 定义新用户时分配的默认值。 除非您明确设置其他值，否则将指定默认值。

general

[general] 部分包含适用于多种类型资源的默认参数。

defaultOwner

分配给新记录的所有者的名称。

如果您不指定值，则会将新记录的创建者分配为所有者。

history

[history] 部分包含 selang 历史记录机制的默认参数。

HistFile

存储历史记录列表中命令的文件的名称。 在每个会话开始时加载命令列表。

无默认值；即，在会话结束时不保存历史信息列表。

HistSize

历史信息机制存储的命令数（介于 10 和 100 之间的正整数）。

默认值：30

newres

[newres] 部分包含由 newres 命令分配的默认值。 newres 命令用于在数据库中创建新的资源记录。 本部分中的每个标记都表示一个 newres 参数。 对于 lang.ini 文件中所未表示的参数，将在 CA Access Control 中分配硬编码的默认值。- 如果不指定内标识的值，则应用表中指定的默认值。

DefaultAudit

新资源的默认审核模式。 有效值包括：none、all、success、failure。

默认值：failure

DefaultDay

适用于资源的默认日期限制。有效值包括：anyday、weekdays、mon、tue、wed、thu、fri、sat、sun。

默认值：anyday

DefaultNotify

向其发送有关资源记录的报警消息的默认电子邮件地址。

无默认值；即，不发送通知消息。

DefaultTime

适用于资源的默认时间限制。 有效值包括：anytime、startTime:endTime。

默认值：anytime

DefaultWarning

默认情况下是否启用警告模式。 有效值包括：yes、no。

默认值：no

newusr

[newusr] 部分包含由 newusr 命令（用于在数据库中创建新的用户记录）分配的默认值。 本部分中的每个标记都表示一个 newusr 参数。 对于 lang.ini 文件中所未表示的参数，将在 CA Access Control 中分配硬编码的默认值。- 如果不指定内标识的值，则应用表中指定的默认值。

DefaultAudit

新用户的默认审核模式。 有效值包括：none、all、success、failure、loginsuccess loginfailure。

默认值：failure loginfailure loginsuccess

DefaultDay

在用户登录到系统时适用的默认日期限制。 有效值包括：anyday、weekdays、mon、tue、wed、thu、fri、sat、sun。

默认值：anyday

DefaultExpire

用户记录的默认到期日期。有效值包括：expire[*dd*/*mm*/*yy*]、expire-。

默认值：expire-

DefaultLocation

用户的默认工作位置。

无默认值

DefaultNotify

在用户登录时向其发送报警消息的默认电子邮件地址。

无默认值；即，不发送通知消息。

DefaultOrg

用户为其工作的组织。

无默认值

DefaultOrgUnit

用户在其中工作的组织机构。

无默认值

DefaultTime

在用户登录到系统时适用的默认时间限制。 有效值包括：anytime、startTime:endTime。

默认值：anytime

属性

[properties] 部分包含适用于用户定义属性的参数。-

UserDefinedTokensFile

包含用户定义属性上下文信息的定义文件的路径。-

默认值：none

UserDefinedAttributesFile

包含用户定义属性特征信息的定义文件的路径。-

默认值：none

用户定义的属性

本部分是对 sepropadm 实用程序的补充说明。 它定义 selang 上下文，据此可识别用 sepropadm 创建的数据库属性。 采用与 sepropadm 所用格式类似的格式的两个定义文件可实现这一点。 这些文件的位置在本部分的两个标记中指定。

注意：执行 selang 加载定义文件之前，必须在数据库中定义属性（使用 sepropadm 实用程序）。 在初始化阶段，运行 selang 时将自动加载定义文件。

在两个相应的定义文件和数据库中都定义了这些属性时，您可以像使用任何其他 CA Access Control 定义的属性一样，在 selang 命令中使用它们。

重要说明！ 不要将 sepropadm 实用程序与**未**经提供商支持人员认证的说明文件一起使用。

更多信息：

sepropadm 实用程序—管理数据库属性 (p. 197)

定义文件

为使 selang 能够识别新的用户定义属性，selang 将在其初始化过程中加载两个 *.def 文件：标记文件和属性文件。-

内标识文件

用户定义的内标识文件

由供应商支持人员提供的定义文件。 定义文件具有以下格式：

以分号 (;) 开头的行是注释，不予处理。

行必须以哈希符号 (#) 开始。 该行必须在说明行之前。

说明行必须遵照下列格式:

```
TOKEN=%s DOMAIN=%d CLASS=%d COMMAND=%d
```

下面是内标识定义文件示例：

```
; 用户定义属性的内标识定义文件示例
; 版权所有 2004 Computer Associates International, Inc.
; ----------------------------------------
; 除非您知道如何使用该文件，否则不要使用它!
# token definition file
; Format is :
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=NOEMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=NOAGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=217
TOKEN=NOTERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
```

属性文件

用户定义的属性文件

由供应商支持人员提供的定义文件。 定义文件具有以下格式：

以分号 (;) 开头的行是注释，不予处理。

行必须以哈希符号 (#) 开始。 该行必须在说明行之前。

说明行必须遵照下列格式:

```
PROPERTY=%s TYPE=%d FLAGS=%x
```

下面是属性定义文件示例：

```
; 用户定义属性的属性定义文件示例
; 版权所有 2004 Computer Associates International, Inc.
; ----------------------------------------
; 除非您知道如何使用该文件，否则不要使用它！
# attributes definition file
; Format is :
PROPERTY=EMAIL TYPE=306 FLAGS=8000
PROPERTY=EMAIL TYPE=5 FLAGS=8000
PROPERTY=AGE TYPE=306 FLAGS=8000
PROPERTY=AGE TYPE=5 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=306 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=5 FLAGS=8000
```

重要说明！ 不要将 selang 与**未**经提供商支持人员认证的说明文件一起使用。

unix

[unix] 部分包含用户添加到 UNIX 时由 newusr 命令分配的默认值。 本部分中的每个标记都表示 *unix* 参数的一个参数。 对于 lang.ini 文件中所未表示的 UNIX 参数，将在 CA Access Control 中分配硬编码的默认值。-

DefaultPGroup

分配给新用户的默认组。如果在服务器的 seos.ini 文件中指定了默认 shell，则它将覆盖此处指定的值。

默认值：other

DefaultShell

新用户的默认 shell。 如果在服务器的 seos.ini 文件中指定了默认 shell，则它将覆盖此处指定的值。

默认值：/bin/sh

DefaultHome

系统的默认主目录。 如果在服务器的 seos.ini 文件中指定了默认 shell，则它将覆盖此处指定的值。 用户的主目录为指定系统主目录的子目录。 例如：如果系统主目录为 /home，则新用户的主目录为 /home/userName。 如果在服务器的 seos.ini 文件中指定了主目录前缀，则它将覆盖此处指定的值。

对于熟悉早期版本的那些用户而言，内标识 DefaultHome 替换了 HomeDirPrefix。

默认值：/home

trcfilter.init

在 UNIX 上有效

CA Access Control 后台进程还将使用 trcfilter.ini 初始化文件。

该可选文件包含一些指定筛选掩码的条目，用以滤出 CA Access Control 跟踪消息。 文件的每一行都包含一个常规表达式。 当向跟踪文件发送消息时，seosd 会检查该消息是否与 trcfilter.init 文件中的某个条目匹配。 仅当跟踪消息与在 trcfilter.init 文件中指定的任何表达式都不匹配时，seosd 才会将它写入该文件。

例如：以下 trcfilter.init 文件会导致放弃所有以“INFO”或“WATCHDOG”开头的消息。 这些消息不会被写入跟踪文件。

```
WATCHDOG*
INFO*
```

注意：该文件不筛选用户跟踪所生成的审核记录。 要筛选这些审核记录，请编辑 audit.cfg 文件。

audit.cfg 文件—筛选审核记录

audit.cfg 可通过定义未发送至审核文件的记录来筛选主机上的审核记录。 每行均代表筛选出审核信息的一条规则。

默认情况下，audit.cfg 文件位于以下目录：

- (UNIX) /opt/CA/AccessControl/etc
- (Windows) C:\\ProgramFiles\CA\AccessControl\data

您可以通过编辑 seos.ini 文件 (UNIX) 中的 [logmgr] AuditFiltersFile 标记或 logmgr 注册表键 (Windows) 中的 AuditFiltersFile 条目，更改 audit.cfg 文件的位置。

使用 audit.cfg 文件筛选出以下审核事件类型的记录（每种类型使用的语法不同）：

- 资源访问
- 网络连接 (p. 379)
- 登录和注销事件 (p. 380)
- 安全数据库管理 (p. 381)
- 有关用户的跟踪消息

注意：在每种语法类型的任意列中，* 均表示“任意值”。

audit.cfg 文件－资源访问事件筛选语法

属于资源访问事件的审核记录具有以下筛选格式：

```
ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult
```

ClassName

定义被访问对象所属的类的名称。

注意：以大写字母输入类的名称。

对象名

定义被访问的对象的名称。

用户名

定义访问者的名称。

ProgramPath

定义用于访问对象的程序的名称。

访问

定义所请求的对象访问。

注意：以下为该参数的值，您可以在 audit.cfg 文件中使用该参数筛选出审核记录。 在某些情况下，audit.cfg 文件中该参数的值与 CA Access Control 在该事件的审核记录中写入的值会有所不同。 任何此类差异都会在每个值的说明后面注明。 按该参数在以下列表中出现的情况键入它。

值：

*****

代表任意访问类型的通配符。

Chdir

更改目录－访问者请求将对象移至其他目录。

Chmod

更改模式－访问者请求更改对象的模式。

Chgrp

(UNIX) 更改组－访问者请求更改对象所属的组。

Chown

更改所有者－访问者请求更改对象的所有者。

连接

将用户加入组－访问者请求将新用户添加到组中。

注意：connect 值与 join 值相同。

控制

(UNIX) Control－访问者要求对对象的 Chown、Chmod、Utime、Sec、Chdir 和 Update 权限。

Cre

创建－访问者请求创建一个对象。

Crrdwr

Create、Read 和 Write－访问者要求对对象的创建、读取和写入权限。

注意：CA Access Control 会在对应的审核记录中将该值写入为 CrRdWrite。

Crread

Create 和 Read－访问者要求对对象的创建和读取权限。

注意：CA Access Control 会在对应的审核记录中将该值写入为 CrRead。

Crwrite

Create 和 Write－访问者要求对对象的创建和写入权限。

注意：CA Access Control 会在对应的审核记录中将该值写入为 CrWrite。

Del

删除－访问者请求删除一个对象。

注意：CA Access Control 会在对应的审核记录中将该值写入为 Erase。

Filereplace

创建和擦除－访问者请求对象的创建和擦除访问权限。

注意：CA Access Control 会在对应的审核记录中将该值写入为 Replace。

Filescan

Filescan－访问者要求对对象的 List 权限。

注意：CA Access Control 会在对应的审核记录中将该值写入为 Scan。

Join

将用户加入组－访问者请求将新用户添加到组中。

注意：join 值与 connect 值相同。

Kill

终止－访问者请求终止进程。

修改

Modify－访问者要求对对象的修改权限。

OwnGrp

Change owner 和 Change group－访问者要求对对象的更改所有者和更改组权限。

PW

Password－访问者请求更改密码。

注意：CA Access Control 会在对应的审核记录中将该值写入为 Password。

R

读取－访问者请求对对象的访问权限。

注意：(UNIX) 如果将 STAT_intercept 设置为 1，该参数将包括 *stat* 拦截。

重命名

更改文件名－访问者请求更改对象的文件名。

Sec

更改 ACL－访问者请求编辑对象的 ACL。

注意：CA Access Control 会在对应的审核记录中将该值写入为 ACL。

更新

Read、Write 和 Execute－访问者要求对对象的读取、写入和执行权限。

注意：当访问者请求对对象的读取和写入权限时，Update 值也可筛选事件。

Utime

(UNIX) 更改时间－访问者请求更改对象的修改时间。

注意：CA Access Control 会在对应的审核记录中将该值写入为 Utimes。

W

写入－访问者请求对对象的写入权限。

x

执行－访问者请求执行一个对象。

注意：某些值并非对每个类均有效。 例如：kill 对 FILE 类无效，因为不可对 FILE 类中的对象执行终止操作。 如果在写入规则时输入了对某个类别无效的值，CA Access Control 将在读取文件时忽略该规则。

AuthorizationResult

定义授权结果。

值：P（已允许）、D（已拒绝）、*

示例：审核筛选策略

- 此示例为您展示了审核筛选策略的格式：

```
env config
er config audit.cfg line+("FIEL;*;*;*;R;P")
```

- 此策略将以下行写入 audit.cfg 文件。 该行将筛选用来记录任何访问者在经允许情况下对任何文件资源进行的读取尝试的审核记录。

```
FILE;*;*;*;R;P
```

audit.cfg 文件－网络连接事件筛选语法

属于网络连接事件的审核记录具有以下筛选格式：

{HOST|TCP};*ObjectName*;*HostName*;*ProgramPath*;*Access*;*AuthorizationResult*

HOST

指定该规则筛选由 HOST 类对象（即传入 TCP 连接）生成的记录。

TCP

指定该规则筛选由 HOST 类对象（即连接服务事件）生成的记录。

对象名

定义被访问的对象的名称。 *ObjectName* 可以是服务名称或端口号。

HostName

定义主机的名称。 *HostName* 必须是 HOST 类中的对象。

ProgramPath

定义登录程序类型。

(Windows) 对于传出连接，此参数定义了尝试建立连接的进程的程序路径。

注意：此参数对传入连接事件没有任何意义。 为此参数使用 * 可筛选由传入连接事件生成的审核记录。

访问

定义所尝试的连接的类型。

值:

- (HOST) *
- (TCP) R（传入连接）、W（传出连接）、*

AuthorizationResult

定义授权结果。

值：P（已允许）、D（已拒绝）、*

示例：筛选网络连接事件

- 此示例将筛选来自主机 ca.com，且由成功传入之 telnet 连接生成的所有审核记录：

  ```
  HOST;telnet;ca.com;*;*;P
  ```

- 此示例将筛选来自主机 ca.com，且由被拒绝的传入和传出登录 TCP 连接生成的所有审核记录：

  ```
  TCP;login;ca.com;*;*;D
  ```

- 此示例可筛选由传出的 telnet 连接生成的主机 ca.com 中的所有审核记录：

  ```
  TCP;telnet;ca.com;*;W;*
  ```

audit.cfg 文件－登录和注销事件筛选语法

属于登录或注销事件的审核记录具有以下筛选格式：

LOGIN;*UserName*;*UserId*;*TerminalName*;*LoginProgram*;*AuthorizationResultOrLoginType*

LOGIN

指定该规则筛选由登录和注销事件生成的审核记录。

用户名

定义访问者的名称。

UserId

(UNIX) 定义访问者的本地用户 ID。

TerminalName

定义发生事件的终端。

LoginProgram

定义尝试登录或注销的程序名称。

AuthorizationResultorLoginType

定义授权结果。

值:

*****

代表任意授权结果类型的通配符。

D

已拒绝登录尝试。

P

已允许登录尝试。

O

(UNIX) 访问者注销。

I

(UNIX) serevu 后台进程已吊销访问者的帐户。

E

(UNIX) serevu 后台进程已启用访问者的帐户。

A

(UNIX) serevu 后台进程或可插入身份验证模块对用户使用不正确的密码登录的尝试进行了审核。

注意：Windows 不会记录注销事件。

示例：筛选登录或注销事件

- 此示例可筛选在 root 登录已获得许可的帐户时生成的所有审核记录：

  ```
  LOGIN;root;*;*;*;P
  ```

- 此示例可筛选在由系统的 CRON 程序引起的 root 登录成功时生成的所有审核记录：

  ```
  LOGIN;root;*;*;SBIN_CRON;P
  ```

- 此示例可筛选在 _CRONJOB_ 进程注销 root 用户时生成的所有审核记录：

  ```
  LOGIN;root;*;_CRONJOB_;*;O
  ```

audit.cfg 文件－安全数据库管理事件筛选语法

属于安全数据库管理事件的审核记录具有以下筛选格式：

```
ADMIN;ClassName;ObjectName;UserName;EffectiveUserName;TerminalName;Command;CommandResult
```

ADMIN

指定该规则筛选由管理员执行的事件生成的审核记录。

ClassName

定义管理员执行命令的类。

对象名

定义管理员的命令更新的对象。

用户名

定义执行命令的用户的名称。

EffectiveUserName

(UNIX) 定义适用该规则的有效用户的名称。

(Windows) 定义适用该规则的本地用户的名称。

TerminalName

定义发生事件的终端。

命令

定义管理员执行的 selang 命令。

CommandResult

定义授权或命令结果。

值：S（命令已成功）、F（命令已失败）、D（命令已拒绝）、*

示例：筛选安全数据库管理事件

此示例可筛选由 admin01 使用的 FILE 管理命令成功时生成的所有审核记录：

```
ADMIN;FILE'*;admin01;*;*;*;S
```

audit.cfg 文件－用户事件跟踪消息筛选语法

属于有关用户事件的跟踪消息的审核记录具有以下筛选格式：

```
TRACE;TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;AuthorizationResult;TraceMessage
```

注意：跟踪筛选的最大限制是 1000 个记录。

TRACE

指定该规则筛选用户跟踪记录。

TracedClassName

定义用户尝试访问的对象类的名称。

注意：以大写字母输入类的名称。

TracedObjectName

定义用户尝试访问的对象的名称。

RealUserName

(UNIX) 定义生成跟踪记录的真实用户的名称。

(Windows) 定义生成跟踪记录的本地用户的名称。

EffectiveUserName

(UNIX) 定义生成跟踪记录的有效用户的名称。

(Windows) 定义生成跟踪记录的本地用户的名称。 此参数与 RealUserName 参数相同。 为此参数使用 *。

ACUserName

定义 CA Access Control 选择用于授权事件的用户名。

AuthorizationResult

定义授权结果。

值： P（已允许）、D（已拒绝）、*

TraceMessage

定义生成的跟踪消息。

示例：筛选有关用户消息事件的跟踪

此示例可筛选在有效用户是 root 且 root 访问 FILE 类中的对象时生成的用户跟踪记录：

```
TRACE;FILE;*;*;root;*;*;*
```

auditrouteflt.cfg 文件—筛选审核记录传递

auditrouteflt.cfg 文件可以通过定义 CA Access Control 不应发送到分发服务器的记录来筛选审核记录传递。 每行均代表筛选出审核信息的一条规则。 文件路径名由 ReportAgent 部分中的 audit_filter 配置设置定义。

注意： 筛选的审核事件将写入本地审核文件，但 CA Access Control 不会将其发送到分发服务器上的消息队列。 要从本地审核文件筛选出审核消息，请修改由 logmgr 部分中 AuditFiltersFile 配置设置定义的文件（默认为 audit.cfg）中的筛选规则。

您可以使用 auditrouteflt.cfg 文件筛选出以下审核事件类型的记录（各种类型使用的语法不同）：

- 资源访问
- 网络连接
- 登录和注销事件
- 安全数据库管理
- 有关用户的跟踪消息

注意：在每种语法类型的任意列中，* 均表示“任意值”。

资源访问事件筛选语法

属于资源访问事件的审核记录具有以下筛选格式：

ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult

ClassName

定义被访问对象所属的类的名称。

注意：您必须以大写字母输入类的名称。

对象名

定义被访问的对象的名称。

用户名

定义访问者的名称。

ProgramPath

定义用于访问对象的程序的名称。

访问

定义所请求的对象访问。

值:

*****

代表任意访问类型的通配符。

Chdir

更改目录－访问者请求将对象移至其他目录。

Chmod

更改模式－访问者请求更改对象的模式。

Chgrp

(UNIX) 更改组－访问者请求更改对象所属的组。

Chown

更改所有者－访问者请求更改对象的所有者。

Cre

创建－访问者请求创建一个新对象。

Del

删除－访问者请求删除一个对象。

Join

将用户加入组－访问者请求将新用户添加到组中。

Kill

终止－访问者请求终止进程。

R

读取－访问者请求对对象的访问权限。

注意：(UNIX) 如果 STAT_intercept 设置为 1，则此参数包括 *stat* 拦截。

重命名

更改文件名－访问者请求更改对象的文件名。

Sec

更改 ACL－访问者请求编辑对象的 ACL。

Utime

(UNIX) 更改时间－访问者请求更改对象的修改时间。

W

写入－访问者请求对对象的写入权限。

x

执行－访问者请求执行一个对象。

注意：某些值并非对每个类均有效。 例如：kill 对 FILE 类无效，因为不可对 FILE 类中的对象执行终止操作。 如果在写入规则时输入了对某个类别无效的值，CA Access Control 将在读取文件时忽略该规则。

AuthorizationResult

定义授权结果。

值：P（已允许）、D（已拒绝）、*

网络连接事件筛选语法

属于网络连接事件的审核记录具有以下筛选格式：

{HOST|TCP};*ObjectName*;*HostName*;*ProgramPath*;*Access*;*AuthorizationResult*

HOST

指定该规则筛选由 HOST 类对象（即传入 TCP 连接）生成的记录。

TCP

指定该规则筛选由 HOST 类对象（即连接服务事件）生成的记录。

对象名

定义被访问的对象的名称。 *ObjectName* 可以是服务名称或端口号。

HostName

定义主机的名称。 *HostName* 必须是 HOST 类中的对象。

ProgramPath

定义登录程序类型。

(Windows) 对于传出连接，此参数定义了尝试建立连接的进程的程序路径。

注意：此参数对传入连接事件没有任何意义。 为此参数使用 * 可筛选由传入连接事件生成的审核记录。

访问

定义所尝试的连接的类型。

值:

- (HOST) *
- (TCP) R（传入连接）、W（传出连接）、*

AuthorizationResult

定义授权结果。

值：P（已允许）、D（已拒绝）、*

登录和注销事件筛选语法

属于登录或注销事件的审核记录具有以下筛选格式：

LOGIN;*UserName*;*UserId*;*TerminalName*;*LoginProgram*;*AuthorizationResultOrLoginType*

LOGIN

指定该规则筛选由登录和注销事件生成的审核记录。

用户名

定义访问者的名称。

UserId

定义访问者的本地用户 ID。

TerminalName

定义发生事件的终端。

LoginProgram

定义尝试登录或注销的程序名称。

AuthorizationResultorLoginType

定义授权结果。

值:

*****

代表任意授权结果类型的通配符。

D

已拒绝登录尝试。

P

已允许登录尝试。

O

(UNIX) 访问者注销。

I

(UNIX) serevu 后台进程已吊销访问者的帐户。

E

(UNIX) serevu 后台进程已启用访问者的帐户。

A

(UNIX) serevu 后台进程或可插入身份验证模块对用户使用不正确的密码登录的尝试进行了审核。

注意：Windows 不会记录注销事件。

安全数据库管理事件筛选语法

属于安全数据库管理事件的审核记录具有以下筛选格式：

ADMIN;*ClassName*;*ObjectName*;*UserName*;*EffectiveUserName*;*TerminalName*;*Command*;*CommandResult*

ADMIN

指定该规则筛选由管理员执行的事件生成的审核记录。

ClassName

定义管理员执行命令的类。

对象名

定义管理员的命令更新的对象。

用户名

定义执行命令的用户的名称。

EffectiveUserName

(UNIX) 定义适用该规则的有效用户的名称。

(Windows) 定义适用该规则的本地用户的名称。

TerminalName

定义发生事件的终端。

命令

定义管理员执行的 selang 命令。

CommandResult

定义授权或命令结果。

值：S（命令已成功）、F（命令已失败）、D（命令已拒绝）、*

有关用户事件的跟踪消息的筛选语法

属于有关用户事件的跟踪消息的审核记录具有以下筛选格式：

TRACE;*TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;AuthorizationResult;TraceMessage*

TRACE

指定该规则筛选用户跟踪记录。

TracedClassName

定义用户尝试访问的对象类的名称。

注意：您必须以大写字母输入类的名称。

TracedObjectName

定义用户尝试访问的对象的名称。

RealUserName

(UNIX) 定义生成跟踪记录的真实用户的名称。

(Windows) 定义生成跟踪记录的本地用户的名称。

EffectiveUserName

(UNIX) 定义生成跟踪记录的有效用户的名称。

(Windows) 定义生成跟踪记录的本地用户的名称。 此参数与 RealUserName 参数相同。 为此参数使用 *。

ACUserName

定义 CA Access Control 选择用于授权事件的用户名。

AuthorizationResult

定义授权结果。

值：P（已允许）、D（已拒绝）、*

TraceMessage

定义生成的跟踪消息。

示例：筛选网络连接事件

- 此示例将筛选来自主机 ca.com，且由成功传入之 telnet 连接生成的所有审核记录：

  ```
  HOST;telnet;ca.com;*;*;P
  ```

- 此示例将筛选来自主机 ca.com，且由被拒绝的传入和传出登录 TCP 连接生成的所有审核记录：

  ```
  TCP;login;ca.com;*;*;D
  ```

- 此示例可筛选由传出的 telnet 连接生成的主机 ca.com 中的所有审核记录：

  ```
  TCP;telnet;ca.com;*;W;*
  ```

示例：筛选登录或注销事件

- 此示例可筛选在 root 登录已获得许可的帐户时生成的所有审核记录：

  ```
  LOGIN;root;*;*;*;P
  ```

- 此示例可筛选在由系统的 CRON 程序引起的 root 登录成功时生成的所有审核记录：

  ```
  LOGIN;root;*;*;SBIN_CRON;P
  ```

- 此示例可筛选在 _CRONJOB_ 进程注销 root 用户时生成的所有审核记录：

  ```
  LOGIN;root;*;_CRONJOB_;*;O
  ```

示例：筛选安全数据库管理事件

此示例可筛选由 admin01 使用的 FILE 管理命令成功时生成的所有审核记录：

```
ADMIN;FILE'*;admin01;*;*;*;S
```

示例：筛选有关用户消息事件的跟踪

此示例可筛选在有效用户是 root 且 root 访问 FILE 类中的对象时生成的用户跟踪记录：

```
TRACE;FILE;*;*;root;*;*;*
```

示例：审核筛选策略

此示例为您展示了审核筛选策略的格式：

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

此策略会将以下行写入 auditrouteflt.cfg 文件：

```
FILE;*;*;R;P
```

此行可筛选用于记录在任何访问者试图对任何文件资源进行读取时，得到允许的访问尝试的审核记录。

审核日志传递配置文件 selogrd.cfg

在 UNIX 上有效

以下是配置文件的格式，后跟详细说明。

```
section-name-1
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
。
section-name-2
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
。
...
```

指定审核记录

配置文件是要传递（及不传递）到各种目标的审核记录的列表。 要指定审核记录，请说明一个或多个特定字段的内容。 您可以使用标准的 UNIX 模式匹配（通配符 * 和 ?）。

例如：要指定涉及用户名以字母 dbms 开头的用户的记录，请输入以下内容：

```
User(dbms*)
```

该示例匹配使用诸如 dbms1、dbms_mgr 等名称的用户。

要指定相同用户，但只指定涉及其登录尝试的记录，请输入：

```
User(dbms*) Class(LOGIN)
```

注意：当一行指定涉及多个字段的记录时，它只指定与*所有*这些字段匹配的记录。

在指定记录的同一行的开头，指定是希望包括还是排除记录。 例如：要在传递中包括这些记录，请输入以下内容：

```
include User(dbms*) Class(LOGIN).
```

这种类型的行的总体格式如下：

```
[{include|exclude} match-field(match-pattern) ... .]
```

此处，“...”表示第一对匹配字段（匹配模式）后面可以跟有其他匹配对。--

可以为匹配字段（匹配模式）使用以下任何值：--

Access(*access-type*)

用于所需的访问类型；*access-type* 可以是以下任何一项：

ACL、Chdir、Chgrp、Chmod、Chown、连接、控制、创建、清除、执行、终止、修改、Owngrp、密码、读取、重命名、替换、更新、Utimes 和写入。

Class(LOGIN)

表示登录记录。

Class(LOGOUT)

表示注销记录。

Class(PWCHANGE)

表示密码管理。

Class(HOST)

表示 TCP/IP 记录。

Class(UPDATE *CA Access Control-class*)

表示数据库管理。 CA Access Control-class 是任何访问者或资源类（例如：USER、GROUP、FILE、HOSTNP...）或者要匹配的类名的模式。 因此，对于所有数据库管理，都可以指定 UPDATE *。

Class(*CA Access Control-class*)

表示对受保护资源的访问。 例如：Class(FILE) 是指报告文件访问尝试的记录。

注意，您可以使用星号将 Class(*CA Access Control-class*) 和 Class(UPDATE *CA Access Control-class*) 组合成 *Class(*CA Access Control-class*)*。 例如：指定 Class(*FILE) 与同时指定 Class(FILE) 和 Class(UPDATE FILE) 相似。 它既指访问文件的尝试，又指更新 FILE 类中记录的尝试。

Code(*return-code*)

用于指示所发生情况的 CA Access Control 返回代码；return-code 可以接受以下值。 （另请参阅本节中的示例 1。）

A－因为重复输入无效的密码，所以登录尝试失败。

D－CA Access Control 拒绝对资源的访问、不允许登录或不允许对数据库进行更新，原因是访问者权限不足。

E－Serevu 启用了一个禁用的用户帐户。

F－尝试更新数据库失败。

I－Serevu 禁用了一个用户帐户。

M－执行的命令已启动或已关闭后台进程。

O－用户注销。

P－CA Access Control 允许访问资源或允许登录。

S－数据库已成功更新。

T－因为正在跟踪该用户的所有操作，所以已写入审核记录。

U－受托程序（setuid 或 setgid）已更改；因此它不再受托。

W－对资源的访问违反了该资源的访问规则。 但是，因为在资源中设置了警告模式，所以 CA Access Control 允许访问。

Host(*host-name*)

表示 TCP/IP 连接中涉及的主机。

Object(*resource-name*)

表示用户尝试访问的资源。

Reason(*reason-number*)

表示触发审核记录的原因。

Service(*service-name*)

表示从远程主机请求的服务的名称，如 telnet 或 ftp。

Source Host(*hostname*)

表示为合并审核提供记录的主机的名称。

Stage(*stage-number*)

表示允许或拒绝访问的阶段。（请参阅*《参考指南》*中阶段代码的列表。）

Terminal(*terminal-name*)

表示尝试进行访问或管理的终端。

Uid(*uid-number*)

表示尝试进行访问或管理的用户的 uid。

User(*username*)

表示尝试进行访问或管理的用户；username 是名称或模式。

注意：虽然一些变量更有可能被指定为模式，但是可以将一种模式用于任何变量（甚至是诸如阶段编号的变量）。

使用更多行改进

要改进您的规范，可以同时按不同的条件进行筛选。 只需在一个 include/exclude 行后面添加另一个这样的行。 例如：

```
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*).
```

该示例指定了其名称以 dbms 开头的用户以及其名称不以 console_ 开头的终端用户进行的所有登录尝试。

指定目标

在 include 和 exclude 行的顺序的*上面*使用一行，来指定要包括的审核记录的目标。 例如：

```
mail weekwatch
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*).
```

该示例指定了电子邮件地址 weekwatch，它用于接收有关其名称以 dbms 开头的用户以及其名称不以 console_ 开头的终端用户进行的所有登录尝试的报告。

这种类型的行以日志路由配置文件的格式显示，如下所示：

routing-method destination

您可以使用以下任一方法：

mail *address*

通过电子邮件发送审核记录；*address* 是目标地址。 如果它不采用 user@host 形式，则会根据本地用户列表和 NIS 邮件别名映射对它进行检查。

注意：如果 address 是用户名并且审核了对该用户的帐户的代理请求，则审核记录会无休止地累积。

screen *username*

如果用户在 selogrd 转发审核记录时在当前主机上登录，则在指定用户的屏幕上显示审核记录。 如果该用户没有登录，则取消显示，而不是延迟显示。

cons *hostname*

将审核记录发送到指定主机上 secmon 实用程序的安全管理员 GUI。 如果该主机不可用，则终止显示，而不是延迟显示。

file *textfilename*

在指定 ASCII 文件中写入审核记录；*textfilename* 必须是绝对路径名，且 selogrd 必须具有访问该文件的权限。

host *hostname*

将审核记录发送到指定主机上的审核日志收集程序。如果该主机不可用，则 selogrd 会在以后重试。

notify mail *或* notify default

通过电子邮件将审核记录发送到审核记录自身指定的地址。

notify screen

在审核记录自身指定的用户的屏幕上显示审核记录。如果该用户未登录，将取消显示，而不是延迟显示。

syslog *priority*

审核记录发送到具有指定日志优先级的 syslog：

- **LOG_EMERG**－系统不能使用。
- **LOG_ALERT**－必须立即采取措施。
- **LOG_CRIT**－危急情况。
- **LOG_ERR**－错误情况。
- **LOG_WARNING**－警告情况。
- **LOG_NOTICE**－正常但重要的情况。
- **LOG_INFO**－参考信息。
- **LOG_DEBUG**－调试级消息。

uni hostname

将审核记录发送到指定主机上的 Unicenter TNG 事件管理器。 您还必须设置 selogrd 以加载 uni.so 共享库（位于 *ACInstallDir*/lib 目录中）。请注意，如果安装发现指定主机上安装了 Unicenter TNG 并且您选择执行该任务，则安装会这样做。

正确的行序列

按正确的顺序排列 include 和 exclude 行并正确分隔各行很重要。

- 您必须在要视为单个复杂筛选的每个行序列（或单行）前面添加一个标题行，并在它的末尾添加一个由单个点组成的终止行；例如：

  从非控制台进行 dbms 登录-

  ```
  mail weekwatch
  ```

  include User(dbms*) Class(*LOGIN*).

  ```
  exclude Terminal(console_*).
  ```

  。

  整个序列（包括标题行和终止行）称为文件的“*部分*”。

- 如果 include 行和 exclude 行都与相同部分中的相同审核记录匹配，则最后一项匹配会覆盖所有其他匹配。
- 如果没有行与特定审核记录匹配，则该部分的第一行是该记录的决定行。 （如果第一行是 include 行，则匹配失败不包括该记录。 如果第一行是 exclude 行，则匹配失败包括传递记录。）
- 如果该部分不包括 include 行和 exclude 行，则它包括路由的所有审核记录。

部分如何共存

虽然某个部分的行共同协作来就是否要发送记录生成一个决策，但是配置文件的不同部分以完全独立的方式工作。 一个部分是否发送审核记录对另一部分是否发送同一审核记录没有影响。

您可以将所选择的相同审核记录发送到多个目标，并且同一目标可以接收对审核记录的多种选择。

在配置文件中，所有部分中所有包括行和排除行的总数不能超过 64 行。

包括注释

要向配置文件中添加注释行，请以分号开始该行。

示例 1

以下是示例配置文件，后面有它的解释。

```
; Product : CA Access Control
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-------------------------------------------------------
 Rule#1
 mail jones@admhost
 include       Class(*LOGIN*) Code(D).
 。
 Rule#2
 mail smith
 include       Class(*SURROGATE*) Object(USER.root*).
 。
 Rule#3
 host venus
 exclude       Class(UPDATE SU*).
 。
 Rule#4
 host venus
 include       Class(*PROGRAM*) Object(/usr/bin/ps).
 。
```

前五行是注释行。

接下来四行组成第一部分（名为 Rule#1）。 无论何时登录请求被拒绝（代码 D 报告拒绝），它们就会告知 selogrd 通过邮件将日志记录发送到地址 jones@admhost：

```
Rule#1
mail jones@admhost
include       Class(*LOGIN*) Code(D).
。
```

下一部分名为 Rule#2。 无论何时有人尝试使用 su 命令输入 root 帐户（SURROGATE 类中的对象是 su 命令的目标），它就会告知 selogrd 通过邮件将日志记录发送到地址 smith：

```
Rule#2
mail smith
include       Class(*SURROGATE*) Object(USER.root*).
。
```

下一部分名为 Rule#3。 无论何时有人尝试管理数据库，它就会告知 selogrd 将日志记录发送到主机 venus 上的收集程序，除非类名以字母 SU 开头（匹配类是 SURROGATE 和 SUDO）：

```
Rule#3
host venus
exclude       Class(UPDATE SU*).
```

最后的部分名为 Rule#4。 无论何时有人尝试使用 ps 命令，它就会告知 selogrd 将日志记录发送到主机 venus 上的收集程序：

```
(Code 1 8pt) Rule#4
host venus
include       Class(*PROGRAM*) Object(/usr/bin/ps).
。
```

示例 2

以下配置文件将*所有*审核记录发送到名为 loghost 的工作站上的收集器：

```
; Product : CA Access Control
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-----------------------------------------------------
 Rule#1
 host loghost
 。
```

返回代码

您可以将配置文件中的每一类记录与一个或多个 CA Access Control 返回代码相关联。（有关返回代码的完整列表，请参阅本部分“指定审核记录”中有关 *code(return-code)* 的描述。）下表介绍记录类型及其关联的返回代码。

记录类型	类或事件	相关联的返回代码
登录	LOGIN LOGINDISABLE LOGINENABLE	D、P、W I E
注销	LOGOUT	O
TCP/IP	HOST	D、P
资源类	*类名*	D、P、W
Watchdog	PROGRAM SECFILE	U U
密码管理	PWCHANGE	D
关闭	SHUTDOWN	D、S
启动	START	S
CA Access Control 数据库管理	UPDATE	D、F、S

uxauth.ini 文件

在 UNIX 上有效

uxauth.ini 配置文件包含用于控制 UNIX 身份验证代理 功能的各种标记。UNIX 身份验证代理 配置文件分为多个部分，分别对应于控制 UNIX 身份验证代理 功能的不同标记集：

部分	说明
ad	包含 Active Directory 标记以及您在安装期间输入的参数
agent	包含用于控制各种 UNIX 身份验证代理 参数的标记
global	包含用于控制 UNIX 身份验证代理 常规设置的标记
libdefaults	包含用于控制 Kerberos 配置设置的标记
logmgr	包含 UNIX 身份验证代理 日志记录实用程序所使用的标记

部分	说明
map	包含用于指定 Active Directory 属性名称的标记
message	包含 UNIX 身份验证代理 用来定义消息文件的标记
migrate	包含 UNIX 身份验证代理 在迁移过程中使用的标记
pam	包含用于控制 UNIX 身份验证代理 PAM 模块的标记
passwd	包含 UNIX 身份验证代理 用来在迁移过程中控制密码更改的标记
register	包含用于控制 UNIX 身份验证代理 注册功能的标记

ad

[ad] 部分包含 Active Directory 标记以及您在安装期间输入的参数。

ad_domain

定义 Active Directory 域的名称。

注意：不要手动编辑此配置设置的值。 可使用 uxconsole -register 实用程序来设置此配置设置的值。

ad_gc_port

指定 Active Directory 全局目录服务所使用的端口。

默认值：3268

ad_site

定义 Active Directory 站点的名称，该站点包含 UNIX 主机用来与 Active Directory 进行通讯的 DC。

lookup_dc_list 中的任何值都将覆盖此配置设置的值。 UNIX 主机不与 ignore_dc_list 配置设置中列出的任何 DC 进行通讯。

注意：不要手动编辑此配置设置的值。 可使用 uxconsole -register 实用程序来设置此配置设置的值。

默认值：none

base_dn

定义 Active Directory 服务器的 base_dn。 CA Access Control 自动设置该配置设置的值。

computer_container

定义 UNIX 主机在 Active Directory 中的位置。

默认值：cn=Computers

domain_query_order

指定 UNIX 身份验证代理 为用户和组查询 Active Directory 域的顺序。

选项：none，不指定顺序；Active Directory 域的以逗号分隔列表

默认值：none

group_container

指定在 Active Directory 中搜索 UNIX 用户的基本条目。

限制：容器名称 (cn=groups)，ROOT 表示进行完整的 Active Directory 查询。

默认值：ROOT

group_custom_filter

指定自定义搜索筛选以在 Active Directory 的组搜索期间应用。

示例：gidNumber=*

默认值：none

ignore_dc_list

指定为 LDAP 连接忽略的 Active Directory 域控制器。

选项：none，逗号分隔的完全限定主机名列表

默认值：none

ignore_domain_list

指定 UNIX 身份验证代理 在查询用户和组时忽略的 Active Directory 域。

选项：none－查询当前和所有受信任域；all－不查询受信任域；要忽略的域的逗号分隔列表。

默认值：none

ignore_group_container

指定要忽略的 Active Directory 组容器。 容器由其可分辨名称（逗号分隔）来定义。

限制：none，可分辨名称的逗号分隔列表

默认值：none

ignore_user_container

指定要忽略的 Active Directory 用户容器。 容器由其可分辨名称（逗号分隔）来定义。

限制：none，可分辨名称的逗号分隔列表

默认值：none

ldap_port

定义 Active Directory LDAP 服务所使用的端口。

默认值：389

lookup_dc_list

指定用于 LDAP 连接的 Active Directory 域控制器。如果您指定域控制器的列表，则 UNIX 身份验证代理 仅使用指定的域控制器。如果您不指定要使用的 DC，UNIX 身份验证代理 会发现最接近端点实际位置的 Active Directory 站点，并与所发现站点中的 DC 进行通讯。

选项：none，逗号分隔的完全限定主机名列表。

默认值：none

lookup_domain_list

指定 Active Directory 域，这些域与注册的 UNIX 身份验证代理 域建立双向信任。

选项：none，UNIX 身份验证代理 自动发现信任域，信任域的以逗号分隔列表

默认值：none

user_container

指定在 Active Directory 中搜索 UNIX 用户的基本条目。

限制：容器名称，ROOT 表示完整的 Active Directory 查询。

默认值：ROOT

user_custom_filter

指定自定义搜索筛选以在 Active Directory 的组搜索期间应用。

默认值：none

agent

[agent] 部分包含用于控制各种 UNIX 身份验证代理 参数的标记。

ac_registration_interval

定义在 CA Access Control 端点中注册 UNIX 身份验证代理 的时间间隔（秒）。 值为 0 表示不注册。

默认值：60

注意：只有当 UNIX 主机上安装了 CA Access Control 时，UNIX 身份验证代理 才会尝试在端点中注册。

ad_group_deny_gid_list

定义无法登录的 Active Directory 组的 GID（逗号分隔）。

示例：ad_group_deny_gid_list = 11,14

注意：此参数仅在完全集成模式下有效。

默认值：不设置标记（无默认值）

ad_group_minimal_gid

定义可以登录的 Active Directory 组的最小 GID。

注意：此参数仅在完全集成模式下有效。

默认值：不设置标记（无默认值）

ad_user_deny_uid_list

定义无法登录的 Active Directory 用户的 UID（逗号分隔）。

示例：ad_user_deny_uid_list = 12,37

注意：此参数仅在完全集成模式下有效。

默认值：不设置标记（无默认值）

ad_user_minimal_uid

定义可以登录的 Active Directory 用户的最小 UID。

注意：此参数仅在完全集成模式下有效。

默认值：不设置标记（无默认值）

debug_backup

指定是否备份调试消息文件。

限制：yes、no

默认值：yes

debug_backup_file

定义备份调试消息文件的名称。 如果您不使用文件的完整路径名，UNIX 身份验证代理 会在目录 *InstallDir*/log/debug/ 中创建该文件

默认值：agent_debug.back

debug_file

定义 UNIX 身份验证代理 将调试消息写入到的文件名。如果您不使用文件的完整路径名，UNIX 身份验证代理 会在目录 *InstallDir*/log/debug/ 中创建该文件

默认值：agent_debug

debug_size

定义调试消息文件的最大大小 (MB)。

默认值：512

注意：文件超过最大大小时，代理重命名文件以备份并创建新的消息文件。

debug_level

指定调试文件中调试消息的级别。

限制：disabled、high、medium、low

- disabled：不将调试消息写入文件
- high：将级别为 HIGH 的调试消息写入文件
- medium：将级别为 HIGH 和 MEDIUM 的调试消息写入文件
- low：将级别为 HIGH、MEDIUM 和 LOW 的调试消息写入文件

默认值：disabled

debug_zones

指定是否将子模块（区域）的调试消息记入日志。 要写入多个区域的调试消息，请指定区域值的总数。

限制：-1、1、2、4、8、16 或正值的总和。

- zone -1：写入所有区域的调试消息
- zone 1：写入 General 区域的调试消息
- zone 2：写入整个通讯区域的调试消息
- zone 4：写入 Scheduler 区域的调试消息
- zone 8：写入 PAM 通讯区域的调试消息
- zone 16：写入 NSS 通讯区域的调试消息

示例：要将 "General" 和 "Scheduler" 区域的调试消息记入日志，请将 debug_zones 的值设置为 5。

默认值：-1

default_login_access

如果没有用来定义用户和组访问权限的规则，请指定默认访问模式。

限制：0 表示没有访问权限，1 表示授予访问权限

默认值：0

注意：此参数仅在完全集成模式下有效。

groups_allow_file

定义本地 groups.allow 文件的位置。

默认值：/opt/CA/uxauth/etc/groups.allow

注意：此参数仅在完全集成模式下有效。

groups_deny_file

定义本地 groups.deny 文件的位置。

默认值：/opt/CA/uxauth/etc/groups.deny

注意：此参数仅在完全集成模式下有效。

heartbeat_send_interval

定义向 CA Access Control 分发主机发送检测信号的时间间隔（秒）。

默认值：3600

ldap_connection_lifetime

定义将未使用的 LDAP 连接保持打开状态的最长时段（秒）。 如果设为 0，UNIX 身份验证代理 会在 LDAP 操作之后立即销毁连接。

默认值：60

LIC98Dir

定义 CA 许可库的位置。

默认值：/opt/CA/SharedComponents/ca_lic

login_name_type

指定映射用户可以使用 UNIX 用户名还是企业用户名来登录。

限制：1－UNIX 登录名、2－企业登录名

默认值：1

message_read_interval

指定读取 CA Access Control 策略队列的时间间隔（秒）。

默认值：60

message_read_timeout

定义读取 CA Access Control 策略队列的超时期（毫秒）。

默认值：1

nss_cache_update_grp_login

指定 NSS 是否在每次用户登录之后更新组缓存。

限制：yes、no

默认值：yes

注意：此参数仅在完全集成模式下有效。

nss_cache_update_grp_mode

指定组缓存的更新方法。

限制：0－不更新、1－增量式更新、2－完全更新

默认值：1

注意：此参数仅在完全集成模式下有效。

nss_cache_update_interval

定义更新用户和组缓存的时间间隔（分钟）。

默认值：60

注意：此参数仅在完全集成模式下有效。

nss_cache_update_startup

指定在代理启动期间更新 NSS 用户和组缓存的方法。

限制：0 表示不更新、1 表示增量式更新、2 表示完全更新

默认值：1

注意：此参数仅在完全集成模式下有效。

nss_cache_update_usr_login

指定 NSS 是否在每次用户登录之后更新用户缓存。

限制：yes、no

默认值：yes

注意：此参数仅在完全集成模式下有效。

nss_cache_update_usr_mode

指定用户缓存的更新方法。

限制：0 表示不更新、1 表示增量式更新、2 表示完全更新

默认值：1

注意：此参数仅在完全集成模式下有效。

ntp_server

定义 NTP 服务器的名称或 IP 地址。

默认值：none

offline_logon

指定当 Active Directory 不可用时用户是否可以继续访问 UNIX 主机。

限制：no（禁用脱机连接）；yes（启用脱机连接）

默认值：yes

offline_logon_max_fail

定义最大的失败脱机登录尝试次数。

默认值：5

offline_logon_period

定义在上一次联机身份验证成功后允许进行脱机身份验证的最长时间段（天）。

默认值：30

report_user_mapped_name

指定当用户处于映射模式时审核文件和报告中的显示用户名。

限制：no（显示报告及 UNIX 用户名）；yes（显示报告及用户映射名）。

默认值：no

tgt_renew_interval

定义续订票证授予票证 (TGT) 的时间间隔（秒）。

默认值：7200

tgt_renewable_lifetime

定义票证授予票证 (TGT) 的最长续订期限（天）。

默认值：30d

time_sync_interval

定义时钟同步间隔（秒）。

默认值：300

unix_shells

定义用于将 Active Directory 用户 shell 转化为受支持的 UNIX shell 的规则。 如果未找到匹配项，则使用定义为 other 的 shell。

默认值 (HP-UX)：
sh=/sbin/sh,csh/sbin/csh,bash=/sbin/bash,ksh=/sbin/ksh,tcsh=/sbin/tcsh,other=/sbin/sh

默认值（所有其他操作系统）：
sh=/bin/sh,csh/bin/csh,bash=/bin/bash,ksh=/bin/ksh,tcsh=/bin/tcsh,other=/bin/sh

注意：此参数仅在完全集成模式下有效。

use_local_policy

指定是否使用本地登录策略（.allow 和 .deny 文件）。

限制： no（仅使用企业登录策略）；yes（使用企业登录策略，然后使用本地登录策略）

默认值： no

use_nested_group_acl

指定是否将嵌套组用于用户 ACL。

限制： no（不使用嵌套组）；yes（使用嵌套组）

默认值： yes

use_time_sync

指定时钟同步选项。

限制： no（手动同步）；yes（自动同步）

默认值： no

use_wingrp

指定 UNAB 是否将 Active Directory 组存储在数据库中以供 CA Access Control 使用。

要在不集成 CA Access Control 时以部分集成模式工作，请在配置 UNAB 时禁用组数据库创建。

限制： no、yes

默认值： yes

users_allow_file

定义本地 users.allow 文件的位置。

默认值： /opt/CA/uxauth/etc/users.allow

注意： 此参数仅在完全集成模式下有效。

users_deny_file

定义本地 users.deny 文件的位置。

默认值： /opt/CA/uxauth/etc/users.deny

注意： 此参数仅在完全集成模式下有效。

user_ticket_cleanup_interval

指定删除过期用户票证的清理时间间隔（秒）。

限制： 任何正整数

默认值： 3600

wingrp_update_interval

定义更新 UNIX 身份验证代理 Active Directory 组数据库的时间间隔（分钟）。

默认值：60

注意：此参数仅在完全集成模式下有效。

wingrp_update_login

指定是否在每次用户登录时更新 Windows 组数据库。

限制：yes、no

默认值：yes

注意：此参数仅在完全集成模式下有效。

windgrp_update_mode

指定更新 UNIX 身份验证代理 Active Directory 组数据库的方法。

限制：0 表示不更新、1 表示增量式更新、2 表示完全更新

默认值：1

注意：此参数仅在完全集成模式下有效。

wingrp_update_startup

指定在 UNIX 身份验证代理 启动期间更新 Active Directory 组数据库的方法。

限制：0 表示不更新、1 表示增量式更新、2 表示完全更新

默认值：1

注意：此参数仅在完全集成模式下有效。

working_threads

定义代理中的工作线程数目。

默认值：64

global

[global] 部分包含用于控制 UNIX 身份验证代理 常规设置的参数。

activation

指定主机激活级别。

限制：0、1、2

- 0－未注册
- 1－已注册（仅允许本地用户存储中定义的用户登录）
- 2－已激活（允许在本地用户存储中定义的用户或者在 .allow 文件或 UNIX 身份验证代理 登录策略中定义的用户登录）

默认值：0

CASHCOMP

指定 CA 共享组件安装目录的路径。

默认值：/opt/CA/SharedComponents

integration_mode

指定 UNIX 身份验证代理 安装方法。

限制：1－部分集成、2－完全集成

注意：如果想保留 UNIX 用户存储，请指定部分集成 (1)。

默认值：2

locale

定义 UNAB 代理和实用程序的语言。

示例：C（英语）、japanese、chinese-s、chinese-t

默认值：C

kerberos_configuration

指定在实施 UNIX 身份验证代理 辅助的 Kerberos SSO 时如何使用 Kerberos 配置。

限制：

- internal—指定配置文件和用户凭据缓存存储在 /opt/CA/uxauth 和 opt/CA/uxauth/etc 目录之下
- external—指定配置文件和用户凭据缓存存储在本地位置中

注意：在 UNIX 身份验证代理 注册期间系统自动对该标记进行配置。

注意：Linux、HPUX 和 Solaris 在 /tmp 目录中存储用户凭据。 AIX 将用户凭据存储在 /var/krb5/security/creds 目录中

默认值：internal

product_path

定义 UNIX 身份验证代理 安装目录的名称。

默认值：/opt/CA/uxauth

libdefaults

[libdefaults] 部分包含控制 Kerberos 配置设置的标记。

default_realm

为 UNIX 身份验证代理 端点定义默认 Kerberos 领域。 值 *unregistered* 指定 UNIX 身份验证代理 不使用 Kerberos。

默认值：unregistered

dns_lookup_kdc

指定 UNIX 身份验证代理 使用 DNS SRV（服务定位器）记录来查找 KDC（密钥分发中心）服务位置。

限制：true、false

默认值：true

dns_lookup_realm

指定 UNIX 身份验证代理 使用 DNS TXT 记录来查找域到领域的映射。

限制：true、false

默认值：false

ticket_lifetime

定义票单使用寿命（秒）。

默认值：2400

logmgr

[logmgr] 部分包含 UNIX 身份验证代理 日志记录实用程序所使用的一些标记。

audit_back

定义审核日志备份文件的完整路径名。

默认值：/opt/CA/uxauth/log/uxauth.audit.bak

audit_group

指定获准读取审核日志文件的组的名称。

限制：none、*group_name*

- None—没有组访问权限，只有 root 可以读取审核日志文件
- *group_name* —定义可以读取审核日志文件的组的名称

注意：如果在 UNIX 身份验证代理 创建审核日志文件之后更改该标记的值，则必须使用 selang 命令设置文件组所有权以及读取日志的组权限。 在设置该标记的值之后所创建的任何文件都将拥有您指定的权限。

默认值：none

audit_log

定义审核日志文件的完整路径名。

默认值：/opt/CA/uxauth/log/uxauth.audit

audit_max_files

定义为每种指定备份模式所保存的审核日志文件最大数目。 达到备份审核日志文件的最大数目时，UNIX 身份验证代理 会在创建最新文件时删除最早的备份文件。值 0 指定 UNIX 身份验证代理 持续累积备份文件。

默认值：0

audit_size

定义审核日志文件的最大大小 (KB)。

注意：可以为此标记指定的最小值为 50 KB。

默认值：1024

audit_to_syslog

指定是否将审核事件记录到 syslog 文件中。

限制：yes、no

默认值：no

BackUp_Date

指定备份审核日志文件的时间间隔。

限制：none、yes、daily、weekly、monthly

- none－在文件达到 audit_size 标记内指定的大小时执行备份，但不为文件加时间戳。
- yes－当审核文件达到 audit_size 标记内所指定的大小时，执行审核日志文件备份
- daily－每天执行审核日志文件备份
- weekly－每周执行审核日志文件备份

monthly－每月执行审核日志文件备份

注意：如果您为此标记指定 daily、weekly 或 monthly，UNIX 身份验证代理 会在当前日期超过指定的间隔时，创建时间戳，备份审核日志文件，并将时间戳附加到备份文件的名称中。 但是，如果在当前日期超过指定间隔之前审核日志文件的大小达到了 audit_size 标记中所指定的大小，则 UNIX 身份验证代理 会备份审核日志文件，但不会将时间戳附加到备份文件的名称中。 如果为此标记指定 yes，则始终将时间戳附加到备份文件的名称中。

默认值：none

error_back

定义错误日志文件备份副本的完整路径名。

默认值：/opt/CA/uxauth/log/uxauth.error.bak

error_group

指定获准读取错误日志文件的组的名称。

限制：none、*group_name*

- None－没有组访问权限，只有 root 可以读取错误日志文件
- *group_name* －定义可以读取错误日志文件的组的名称

注意：如果在 UNIX 身份验证代理 创建错误日志文件之后更改该标记的值，则必须使用 selang 命令设置文件组所有权以及读取日志的组权限。 在设置该标记的值之后所创建的任何文件都将拥有您指定的权限。

默认值：none

error_log

定义错误日志文件的完整路径名。

默认值：/opt/CA/uxauth/log/uxauth.error

error_size

指定错误日志文件的最大大小 (KB)。

注意：可以为此标记指定的最小值为 50 KB。

默认值：50

map

在完全集成模式下有效

[map] 部分包含 UNIX 身份验证代理 用来指定 Active Directory 属性名称的标记。

group_gid_attr_name

指定 Active Directory 属性名称，这些属性名称表示 UNIX 组 ID。

默认值：gidNimber

group_member_attr_name

指定列出组的成员的 Active Directory 属性名称。

限制：member、memberUid

注意：仅在 user_name_attr_name = msSFU30Name 时使用值 memberUid。

默认值：member

user_gecos_attr_name

指定 Active Directory 属性名称，这些属性名称指示 UNIX 用户 gecos。

默认值：gecos

user_gid_attr_name

指定 Active Directory 属性名称，这些属性名称表示 UNIX 组 ID。

默认值：gidNumber

user_homedir_attr_name

指定 Active Directory 属性名称，这些属性名称指示 UNIX 用户主目录。

默认值：unixHomeDirectory

user_loginshell_attr_name

指定 Active Directory 属性名称，这些属性名称指示 UNIX 用户登录 shell。

默认值：loginShell

user_name_attr_name

指定 UNIX 用户名的 Active Directory 属性名称。

默认值：sAMAccountName

user_uid_attr_name

指定 Active Directory 属性名称，这些属性名称指示 UNIX 用户 ID。

默认值：uidNumber

message

[message] 部分包含 UNIX 身份验证代理 用来定义消息文件的标记。

filename

定义消息文件的完整路径名。

默认值：/opt/CA/uxauth/data/uxauth.msg

migrate

[migrate] 部分包含 UNIX 身份验证代理 在迁移过程中使用的标记。

conflicts_file

定义迁移冲突文件的完整路径名。

默认值：/opt/CA/uxauth/log/migrate.conflicts

create_ad_groups

指定当 Active Directory 中没有相同的组时，是否在迁移期间创建新的 Active Directory 组。

限制：yes、no

默认值：yes

disable_mapped_user

指定是否禁用部分迁移的（映射）用户的 UNIX 密码。

限制：yes、no

默认值：yes

ignore_gecos_conflict

定义是否忽略 UNIX 身份验证代理 在迁移过程中发现的 gecos 用户属性相关的冲突。

限制：yes、no

默认值：yes

is_gid_migration_a_prerequisite

指定迁移用户的主要组是否是迁移用户的先决条件。

限制：yes、no

默认值：no

journal

定义迁移日志文件的完整路径名。

默认值：/opt/CA/uxauth/log/migrate.journal

minimal_gid

定义在迁移过程中将迁移到 Active Directory 的最小组 ID。 不迁移具有更小 GID 的组。

默认值：101

minimal_uid

定义在迁移过程中将迁移到 Active Directory 的最小用户 ID。 不迁移具有更小 GID 的用户。

默认值：101

remove_migrated_user

指定是否在迁移之后删除本地用户帐户。

限制：yes、no

默认值：yes

try_to_map_on_conflict

指定如果完整迁移过程失败，是否映射冲突帐户。

限制：yes、no

默认值：yes

passwd

[passwd] 部分包含 UNIX 身份验证代理 用来在迁移过程中控制密码更改的标记。

YpGrpCmd

定义用来生成 NIS 组映射的命令。

默认值：make group

YpMakeDir

定义在创建 NIS 映射时使用的 makefile 目录。

默认值：/var/yp

YpPassCmd

定义用于生成 NIS 密码映射的命令。

默认值：make passwd

YpServerGroup

定义 NIS 服务器上的组文件的完整路径名。

默认值：/etc/group

YpServerPasswd

定义 NIS 服务器上的密码文件的完整路径名。

默认值：/etc/passwd

YpServerSecure

定义操作系统的密码文件的完整路径名。

默认值 (AIX)：/etc/security/passwd

默认值 (HP-UX)：/.secure/etc/passwd

默认值 (Solaris)：/etc/shadow

默认值（所有其他操作系统）：/etc/shadow

pam

[pam] 部分包含 UNIX 身份验证代理 用来与 PAM 模块交互的标记。

debug_mode_for_user

定义 PAM 模块是否在登录期间可以将消息打印到用户屏幕。

选项：yes、no

默认值：yes

pam_exit_on_deny

定义 PAM 模块行为，在登录由于企业或本地策略设置或 Active Directory 状态而遭到拒绝时。

选项：yes；PAM 模块关闭顺序，并阻止其他 PAM 模块验证用户；no；PAM 模块不关闭并启用其他 PAM 模块验证用户，并允许服务器中日志重试 PAM 顺序调用

默认值：yes

pam_receive_timout

指定 PAM 模块等待 UNIX 身份验证代理 代理 (uxauthd) 响应的时间（秒）。

限制：任何正整数。

默认值：10

register

[register] 部分包含控制 UNIX 身份验证代理 注册功能的标记。

start_uxauthd

指定是否在安装过程结束时运行 uxactivate 实用程序。

限制：yes、no

默认值：yes

verbose

定义在安装过程中使用的详细级别。

默认值：0

UNIX 身份验证代理 冲突文件

在您尝试将用户和组迁移到 Active Directory 之后，会创建 UNIX 身份验证代理 冲突文件。 该文件详细描述由 UNIX 身份验证代理 在迁移过程中发现的冲突。 查看该文件以解决在文件中报告的冲突。

此文件包含以下字段：

解决方案实体类型、解决方案实体名称、解决方案操作、解决方案 AD 映射名称、冲突、UID、主目录、GID、成员属于、成员、GECOS

解决方案实体类型

显示要迁移的解决方案实体的类型。

限制：user、group

解决方案实体名称

显示实体的名称。

解决方案操作

显示实体迁移状态。

限制：Keeplocal、Migrate、Map

解决方案 AD 映射名称

显示本地帐户所映射的 Active Directory 帐户名称。

冲突

显示在迁移期间发现的冲突。

UID

显示用户 ID。

主目录

显示用户主目录。

GID

显示组 ID。

成员属于

显示用户所属的组。

成员

显示属于组的成员的用户列表。

GECOS

显示 GECOS 信息。

SSH 设备 XML 文件

SSH 设备 XML 文件允许您配置 特权用户密码管理 如何连接 SSH 设备端点、发现用户帐户，并更改端点上的特权帐户密码。

不同的 SSH 设备 XML 文件配置与不同类型的 SSH 设备端点的交互。 例如：aix_connector_conf.xml 文件配置与 AIX 端点的连接，device_connector_conf.xml 文件配置与 SSH 设备（如路由器）的连接。

注意：有关 SSH 设备 XML 文件类型的详细信息，请参阅 *《企业管理指南》*。

SSH 设备 XML 文件位于以下目录：

ACServerInstallDir/Connector Server/conf/override/sshdyn

如果需要，可以根据自己企业的要求自定义 SSH 设备 XML 文件。

结构

SSH 设备 XML 文件包含以下元素：

- <class name="SSHConnectionManager">—包含管理 SSH 连接的参数
- <class name="CommandProcessor">—包含指定连接设置的参数
- <class name="CommandSet">—包含一些阵列元素，这些元素指定 特权用户密码管理 在端点上执行的命令

<class name="CommandSet"> 元素包含组成命令集的阵列元素：

- <array name="oGetUsers">—包含 特权用户密码管理 所执行以获取用户的命令
- <array name="oChangePassword">—包含 特权用户密码管理 所执行的用于更改用户密码的命令
- <array name="oSubstituteUser">—包含 特权用户密码管理 为使用 su 切换到其他用户而执行的命令

  注意：<array name="oSubstituteUser"> 元素仅对 aix_connector_conf.xml、checkpoint_connector_conf.xml 和 ssh_connector_conf.xml 文件有效。

每个阵列元素包含多个 <item> 元素。 <item> 元素定义 特权用户密码管理 在端点上执行的专用命令的参数。 例如：<array name="oGetUsers"> 元素中的 <item> 元素可能指定：

- 特权用户密码管理 为获得本地用户而执行的命令
- 特权用户密码管理 等待响应的时间长度
- 特权用户密码管理 在继续之前等待接收的文本字符串
- 表示命令失败的响应中的文本字符串

注意：有关 SSH 设备 XML 文件中的 <item> 元素如何与 SSH 设备端点交互的示例，请参阅 *《企业管理指南》*。

使用嵌套参数来为每个元素定义配置设置，如下所示：

- <class name="SSHConnectionManager"> 和 <class name="CommandProcessor"> 元素包含定义连接设置的参数
- <item> 元素中包含的一些参数可定义特定命令的参数

每个嵌套的参数具有以下格式：

```
<param name="name" value="value" />
```

SSH 设备 XML 文件的以下片段说明元素是如何嵌套的：

```
<package name="com.ca.jcs.sshdyn">
        <class name="SSHConnectionManager">
                <param name="name" value="value" />
        </class>
</package>
<package name="com.ca.sessame.conn.unix">
        <class name="CommandProcessor">
                <param name="name" value="value" />
        </class>
        <class name="CommandSet">
                <instance name="ssh">
                        <array name="oGetUsers">
                                <item>
                                        <param name="name" value="value" />
                                </item>
                        </array>
                        <array name="oChangePassword">
                                <item>
                                        <param name="name" value="value" />
                                </item>
                        </array>
                        <array name="oSubstituteUser">
                                <item>
                                        <param name="name" value="value" />
                                </item>
                        </array>
                </instance>
        </class>
</package>
```

元素

SSHConnectionManager

指定 特权用户密码管理 用来管理 SSH 连接的设置。

该类元素包含以下参数：

I_CONNECTIONS

定义端点的并发连接数。

默认值： 10

CommandProcessor

指定 特权用户密码管理 用来连接到 SSH 设备端点的设置。

该类元素包含以下参数：

bToLog

指定 特权用户密码管理 是否将消息写入 sLogFileName。

限制：true、false

默认值：true

sLogFileName

定义日志文件的相对路径名。

默认值：..\logs\uxlog.txt

limitResultCharsToLog

定义 CA Access Control 为每个连接写入日志文件中的最多字符数。

默认值：1500

bSkipOperationAdminTestConnection

指定

限制：true、false

默认值：true

maxTimeLimit

定义 特权用户密码管理 等待值的最长时间（毫秒）。

默认值：1500

waitIntervalDefault

定义 特权用户密码管理 等待的时间（毫秒）

默认值：500

login_str

指定用户名的 Telnet 请求命令。

示例;：login

password_str

指定密码的 Telnet 请求命令。

示例：password

AYT_answer

指定设备针对 Telnet 命令“Are You There”的回答

默认值：Solaris-Yes、Linux-yes、AIX-here

注意：由于不同配置，每个 SSH 设备可以针对 AYT 命令有唯一的回答。 您可以相应修改 SSH XML 文件。

要发现格式，请将 telnet 会话打开到设备并运行以下命令：

```
^+]
send ayt
```

iPort

定义 SSH 端口号。

注意：默认情况下，此参数将被注释掉。

默认值：22

CommandSet

指定 特权用户密码管理 在端点上执行的命令。

该类元素包含将 特权用户密码管理 在端点上执行的命令分组的阵列元素。

oGetUsers

指定 特权用户密码管理为获取用户而执行的命令。

该阵列元素包含一些项目元素，这些元素定义 特权用户密码管理 为获取用户而执行的特定命令的参数。

oChangePassword

指定 特权用户密码管理 为更改用户密码而执行的命令。

该阵列元素包含一些项目元素，这些元素定义 特权用户密码管理 为更改用户密码而执行的特定命令的参数。

oSubstituteUser

指定 特权用户密码管理 为使用 su 切换到其他用户而执行的命令。

该阵列元素包含一些项目元素，这些元素定义 特权用户密码管理 为使用 su 切换到其他用户而执行的特定命令。

注意：该元素仅对 aix_connector_conf.xml、checkpoint_connector_conf.xml 和 ssh_connector_conf.xml 文件有效。

item

指定 特权用户密码管理 在端点上执行的特定命令的参数。

每个项目元素可以包含以下参数：

sCommand

定义 特权用户密码管理 发送到端点的命令。

iWait

定义 特权用户密码管理 在执行下一步前等待的时间间隔（毫秒）。

默认值：500

sWaitForText

定义 特权用户密码管理 等待接收的文本字符串，以响应在 sCommand 中定义的命令。

sFailureResult

定义 特权用户密码管理 从端点接收的指示命令失败的文本字符串。

sToFilterOut

定义 特权用户密码管理 从端点输出删除的文本字符串。

bHideSentLog

指定是否将命令写入日志文件。

限制：true－特权用户密码管理 不将命令写入日志文件，false－特权用户密码管理 将命令写入日志文件

默认值：true

sTrueResultRegex

（可选）指定将命令结果与指定的字符串进行比较。如果结果与字符串不匹配，则显示错误消息。

注意：默认情况下，此参数将被注释掉。

iXMLVersion

指出 XML 文件版本。 XML 版本不能比 SSL 连接程序中定义的 XML 版本新。

默认值：0

ToReport

指定是否将 XML 处理数据记录到 $XML_NAME..lodaing_report.xml 中。 该日志文件位于以下目录：

ACServerInstallDir/Connector Server/conf/override/sshdyn

限制：true、false

默认值：true

FileIsLoaded

表示已成功加载 XML 文件。

默认值：OK

特权用户密码管理 自动登录应用程序 Visual BASIC 脚本

特权用户密码管理 自动登录应用程序使用 Visual Basic 脚本来启用自动用户登录。 您可以自定义 Visual Basic 脚本，以便创建新登录应用程序或修改现有登录应用程序。

从企业管理服务器下载到客户端计算机时，特权用户密码管理 自动登录应用程序脚本会包含 ActiveX 以值替换的变量。 企业管理服务器处理脚本，并以值替换关键字。 然后，ActiveX 执行客户端计算机上的脚本。

特权用户密码管理 自动登录应用程序脚本位于以下目录：

JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

元素

特权用户密码管理 登录应用程序脚本包含以下键：

#host#

指定用户自动登录到的端点名称

#username#

指定签出特权帐户

#password#

指定要签出的特权帐户密码

#userdomain#

(Active Directory) 指定特权帐户域名

#isActiveServletUrl#

指定 ACLauncher ActiveX 用于检查帐户密码签入事件的 URL。

#CheckinUrl#

在用户注销端点的情况下，指定 ACLauncher ActiveX 用于签入帐户密码的 URL。

#SessionidUrl#

如果会话记录在 ObserverIT Enterprise，指定 ACLauncher ActiveX 用于发送已记录会话 ID 的 URL。

特权用户密码管理 自动登录应用程序脚本的以下片段显示变量如何出现：

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#", "#password#")
' Set window close event
pupmObj.SetWindowCloseEvent(hwnd)
' Set server checkin event
pupmObj.SetServerCheckinEvent("#isActiveServletUrl#")
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
    call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
    call pupmObj.CloseWindow(hwnd, 120)
End If
```

结构

特权用户密码管理 自动登录应用程序脚本结构如下所示：

- COM 对象的初始化

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
```

- 自动登录应用程序的执行

```
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#",
"#password#")
```

- Post execution tasks—password check in, interactive login or timeout

```
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
    pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
    call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the
window
    call pupmObj.CloseWindow(hwnd, 120)
End If
```

要记录登录应用程序会话，请将记录说明添加到脚本中，如下所示：

- 在初始化部分， 添加以下内容：

```
Set observeIT = CreateObject("ObserverIT.AgentAPI.Proxy")
```

- 在应用程序执行部分，添加以下内容：

```
'Get application processid
processID = pupmObj.GetWindowProcessID(hwnd)
'Start recording
sessionid = observeIT.StartByProcessID(processID, true)
'Send the sessions if to the ENTM server
pupmObj.AssignSessionID "#SessionidUrl#" ,sessionId
```

- 在后执行部分，添加以下内容：

```
'Stop recording

observeIT.StopBySessionId sessionId, true
```

方法

ACLauncher ActiveX 使用以下方法：

```
LauncheRDP (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT
*phWindow);
```

启动带有输入凭据的远程桌面会话并返回远程桌面窗口句柄

示例： Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LauncheRDP("hostname.com", "hostname\administrator", "password")

```
LaunchePUTTY  (BSTR bsHostName,  BSTR bsUserName, BSTR bsPassword,  VARIANT
*phWindow);
```

启动带有输入凭据的 PuTTY 会话并返回 PuTTY 窗口句柄

示例： Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test。 LaunchePUTTY ("hostname.ca.com", "root", "password")

```
LaunchеProcessAsUser (BSTR bsApplication, BSTR bsCommandline, BSTR bsUsername,
BSTR bsPassword, VARIANT *phWindow);
```

启动带有输入凭据的过程并返回过程窗口句柄

示例： Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LaunchеProcessAsUser("cmd.exe", "/k echo This console is run under %USERNAME% account...", "administrator" , "password")

```
GetWindowProcessID(VARIANT *phWindow, LONG *pProcessID);
```

返回指定窗口句柄的过程 ID

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") id = test.GetWindowProcessID(hwnd) test.Echo "Process ID = " & id

```
GetWindowTitle(VARIANT *phWindow, BSTR *pbsTitle);
```

返回指定窗口句柄的标题 ID

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") title = test.GetWindowTitle(hwnd)

```
CloseWindow(VARIANT *phWindow, LONG Seconds);
```

显示对话框，消息指定窗口将在 X 秒内关闭，并关闭指定窗口句柄的窗口

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.Sleep(5000) test.CloseWindow(hwnd, 60)

```
SetTimeoutEvent(LONG seconds);
```

为“WaitForEvents”方法指定超时。 一旦到达超时值，WaitForEvents 方法则从其阻止调用返回一个返回值，表示到达超时

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

```
SetWindowCloseEvent(VARIANT *phWindow);
```

指定“WaitForEvents”方法的窗口闭事件。 关闭窗口之后，“WaitForEvents”方法从其阻止调用返回并显示返回值，这些返回值表示窗口已关闭

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetWindowCloseEvent(hwnd)

```
SetServerCheckinEvent(BSTR bsURL);
```

将 特权用户密码管理 签入事件设置为块执行条件。 每 5 秒 ActiveX 查询 特权用户密码管理

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb") (replace with variable)

```
WaitForEvents(VARIANT *pRetVal);
```

阻止脚本执行，直到注册条件之一正确。

选项： 1－用户已关闭窗口，2－已用超时时间，3－在服务器端密码签入

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb")

test.SetWindowCloseEvent(hwnd) test.SetTimeoutEvent(360) rc = test.WaitForEvents() If rc = 3 Then call test.CloseWindow(hwnd, 10) End If

```
SwitchToThisWindow(VARIANT *phWindow);
```

定位 Z 顺序顶端的窗口

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SwitchToThisWindow(hwnd)

```
SendCheckinEvent(BSTR bsURL);
```

用户关闭窗口时，发送签入事件

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password")

```
Sleep(LONG milliseconds);
```

暂停脚本执行

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Sleep(2000)

```
Echo(VARIANT* pArgs);
```

打印消息到屏幕

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Echo("Password Checkin")

第 4 章： 注册表项

此部分包含以下主题：

CA Access Control 注册表

CA Access Control 在以下注册表键下创建其注册表项，该注册表键在 CA Access Control 端点管理 远程配置中称为 ACROOT：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl
```

主注册表键包含以下注册表项：

CurrentVersion

定义产品的当前版本和内部版本。

加密程序包

定义用于实施对称加密的 DLL 的完整路径名。

默认值：*ACInstallDir*\bin\aes256enc.dll

<Build_Number>

CA Access Control 在下列注册表键中定义产品的当前版本和内部版本：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Build_Number
```

该注册表键仅供内部使用。

AccessControl

CA Access Control 在以下注册表键下保留其使用的常规设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl

AccessControl 注册表键包含以下注册表项：

AccessControl 服务

定义 CA Access Control 服务名的列表和可执行文件。

默认值：“SeOSAgent;SeOS Agent”、“SeSudo;SeOS TD”、“seoswd;SeOS Watchdog”

注意：端点是企业管理服务器的组成部分，其中还包含该注册表项的以下默认值："Sepmdd;SeOS Policy Model(DMS__)"、"Sepmdd;SeOS Policy Model(DH__)"、"Sepmdd;SeOS Policy Model(DH__WRITER)"

admin_default_check

指定即使远程终端资源的 *defaccess* 属性被设置为 *all*，或允许访问 _default 终端资源时，是否拒绝 CA Access Control 登录访问 CA Access Control 服务器。

保留该项是为了后向兼容。

默认值： 0（不拒绝访问）

AdminInst

仅限内部使用。

默认值：0

auth_login

指定如何出于管理目的验证用户身份。

有效值包括：

native—对于本地操作系统用户，对照操作系统检查用户密码。

eTrust—对于本地操作系统中不存在的用户，对照 CA Access Control 数据库检查用户密码。

默认值：native

auth_module_names

可以在本机验证范围外部进行身份验证的语言客户端模块的列表。客户端模块的名称由身份验证之前 lca API 调用内部的客户端设置。更改该注册表值可能影响非本机模式中的其他客户端身份验证。

默认值：none

CPF_TARGETS

CPF 服务与之通讯的目标大型机 CPF 系统（远程 CPF 目标节点）的列表。

默认值：ACF2 TOP RACF

eACPipePrefix

新的管道服务器和管道客户端将使用的管道名称部分的值。 如果系统中存在 CA Access Control 的旧版本客户端，则必须设置该值，这些客户端才能工作。 否则，将该值更改为更安全的管道名称。

默认值：SEOS

eACPipeTranslator

过时。

full_year

指定在使用 secons -tv、seaudit 和 dbmgr 实用程序时，使用两位数字（值 = no）还是四位数字（值 = yes）的格式显示年份。

默认值：yes

GenerateMemDump

指定在处理 CA Access Control 服务的代码异常时，CA Access Control 是否创建内存转储 (1)。 CA Access Control 在 *ACInstallDir*\bin*serviceProcessName*.*PID*.dmp（例如：SeOSAgent.5704.dmp）中创建内存转储

注意：内存转储仅用于用户模式，不用于内核模式。

默认值：1

parent_pmd

该工作站使用 *pmdb@host* 格式订阅的 *PMDB*。 这是唯一可以更新本地数据库的策略模型。

如果您未指定值，则工作站不接受来自任何 PMDB 的更新。 如果您将该项设置为 _NO_MASTER_，则任何 PMDB 都可更新该工作站。

无默认值。

示例：pmd1@host1;pmd2@host1;pmd3@host2

passwd_pmd

策略模型密码替换的目标，格式为 *pmdb@host*。

parent_pmd 和 passwd_pmd 注册表值可以相同。如果 parent_pmd 和 passwd_pmd 注册表值不相同，则 passwd_pmd 数据库将其更新发送到 parent_pmd 数据库以进行分发。 parent_pmd 数据库必须是 passwd_pmd 数据库的订阅者。

如果您不设置该值，它将继承 parent_pmd 注册表项的值。

无默认值。

ReverseIpLookup

控制解析客户端 IP 地址的方式，以确定是否允许用户从该终端登录。

有效值包括：

yes－查找开放客户端套接字的 IP 地址，并相应允许登录。

no－seagent 使用从客户端接收的主机名，且不解析任何主机名。（通过禁用 TERMINAL 类可以达到同样的效果。）

默认值： yes

secondary_pmd

用作密码替换的辅助目标的策略模型数据库。

无默认值。

SeOSPath

安装 CA Access Control 的目录。

SplashEnable

在交互 (GINA) 登录过程中启用或禁用保护消息的开关。 该消息告知用户 CA Access Control 将保护计算机。值为 1 说明已启用该消息，值为 0 说明已禁用该消息。

默认值： 1

TNG_Environment

启用或禁用 Unicenter 集成的切换。

值： 1－启用 Unicenter 集成并使用 Unicenter TNG 类创建数据库，0－禁用 Unicenter 集成，并在没有 Unicenter TNG 类的情况下创建数据库

默认值： 0

TrustedServices

受信任程序的列表。

无默认值。

UseFsiDrv

启用或禁用驱动程序装入的切换。

值：1－启用驱动程序加载，0－禁用驱动程序加载

默认值：1

代理

CA Access Control 在以下注册表键下保留其使用的代理设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Agent

Agent 注册表键的注册表项（和任何子键）仅限内部使用。

ShutdownWaitingTimeout

定义 CA Access Control 代理等待其组件正常关闭的超时时间段（毫秒）。 如果 CA Access Control 组件不正常关闭，代理会强制关闭。

注意：该注册表项仅供内部使用。

默认值：60000

应用程序

CA Access Control 在以下注册表键下保留其使用的应用程序设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications

Applications 注册表键包含以下注册表项：

OperationMode

指定受控应用程序模式是否处于活动状态 (1)。

该值已设置为 1。

默认值：1

<Application_Name>

CA Access Control 在以下注册表键下保留其使用的特定应用程序设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Applications*Application_Name*

每个 Applications*Application_Name* 注册表键包含以下注册表项：

ApplicationName

定义受控进程的名称。

您必须使用以下格式指定完整路径名：*device*:*path**name*.exe。

默认值：可执行文件的完整路径名

参数

定义 CA Access Control 在启动应用程序时使用的参数。

默认值：""（无参数）

桌面

定义工作站和会话名称。

默认值：无默认值

OperationMode

指定应用程序是否处于活动状态 (1)。

默认值：1

RestartApplication

指定如果应用程序已关闭或终止，是否重新启动该应用程序 (1)。

默认值：1

StartAplication

指定唤醒 Watchdog 时，CA Access Control 是否启动应用程序 (1)。

默认值：1

WorkingDirectory

定义启动应用程序的工作目录。

默认值：*ACInstallDir*\bin

客户端

CA Access Control 在以下注册表键下保留其使用的客户端应用程序设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Client

Client 注册表键包含以下注册表项：

ConnectTo

定义默认情况下 CA Access Control 客户端管理应用程序（例如：selang）连接到的主机的名称。

默认值：localhost

Standalone

CA Access Control 在以下注册表键下保留其使用的独立客户端设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Client\Standalone

Client\Standalone 注册表键包含以下注册表项：

full_login_check

在从独立应用程序请求连接期间，使 CA Access Control 服务器检查其他用户属性（grace 和 max_login）并执行登录的切换。

如果一个远程密码将要过期，使用该值可帮助更改远程密码。

如果将该值设置为 1，将启用检查。

默认值：0

通用

CA Access Control 在下列注册表键下保留通用组件所使用的设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common

Common 键不包含任何注册表项。 它包含通用组件的注册表子键。

AgentManager

CA Access Control 在以下位置维护代理管理器相关设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager
```

代理管理器注册表键包含以下注册表项：

RefreshTimeout

定义代理管理器刷新时间间隔，以秒为单位。

类型：REG_DWORD

默认值：600

StandAloneService

指定该服务是否为独立服务。

类型：REG_DWORD

默认值：0

TraceEnabled

定义 CA Access Control 代理管理器跟踪模式。

选项：0、1

默认值：1

WorkSpace

指定 CA Access Control 代理管理器工作区的完整路径名。

默认值：
\ProgramFiles\CA\AccessControlShared\APMS\AccessControl\Data\AgentManager

Plugins

CA Access Control 在以下键维护由插件使用的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\AgentManager\Plugins
```

插件键不包含任何注册表项。 它包含插件的注册表子键。

AccountManager

CA Access Control 在以下位置维护帐户管理器相关设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\AgentManager\Plugins\AccountManager
```

帐户管理器注册表键包含以下注册表项：

时间间隔

定义插件排定，以秒为单位。

默认值：1

注意：只有在 ScheduleType 设置为 2 时适用。

OperationMode

定义插件操作模式。

选项：0－插件已禁用，1－插件已启用

默认值：1

PluginPath

定义插件的完整路径名。

类型：REG_SZ

默认值：
\ProgramFiles\CA\AccessControlServer\APMS\AccessControl\bin\AccountManager.dll

QueryFilter

指定添加到消息队列的其他值，以接收队列筛选。

选项：ENDPOINT_CUSTOM 1...5=, ENDPOINT_OWNER=, ENDPOINT_DEPARTMENT=

请注意下列事项：

- 将属性值放置在撇号中
- 使用 AND 和 OR 操作数指定多个单个属性
- 需要时使用括号

排定

定义插件的排定字符串。

默认值：00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

注意：只有在 ScheduleType 设置为 2 时适用。

ScheduleType

定义插件排定类型。

选项：0－执行一次，1－按需执行，2－间隔执行，3－按排定执行

默认值：1

通讯

CA Access Control 在以下键中保留其使用的消息队列服务器通讯设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication

通讯注册表键包含以下注册表项：

证书

定义 SSL 连接的证书文件。

限制：到包含证书数据的文件的完整路径名。

Distribution_Server

定义分发服务器 URL。 可以在逗号分隔列表中定义多个分发服务器。

示例：tcp://ds.comp.com:7222, tcp://ds_dr.comp.com:7222

默认值：none

endpoint_to_server_queue

定义端点用来将信息发送到 CA Access Control 企业管理 的消息队列的名称。

默认值：ac_endpoint_to_server

server_to_endpoint_broadcast_queue

定义 CA Access Control 企业管理 用来对所有端点广播消息的消息队列的名称。

默认值：ac_server_to_endpoint_broadcast

server_to_endpoint_queue

定义 CA Access Control 企业管理 用来将消息发送到端点的消息队列的名称。

默认值：ac_server_to_endpoint

ssl_custom

指定是否使用主机名验证程序函数。

限制：0，不使用主机名验证程序函数；1，使用主机名验证程序函数

默认值：0

ssl_hostname

定义 SSL 主机名。

默认值：none

ssl_identity

定义报告代理的身份。

限制：到包含证书数据的文件的完整路径名。

默认值：none

ssl_issuer

定义对 SSL 连接的发布程序证书。

限制：到包含证书数据的文件的完整路径名。

默认值：none

ssl_key

定义报告代理私钥。

限制：到包含私钥的文件的完整路径名。

默认值：none

ssl_noverifyhost

指定是否启用主机证书验证功能。

限制：0，禁用主机证书验证；1，启用主机证书验证

默认值：0

ssl_noverifyhostname

指定是否启用主机名验证功能。

限制：0，禁用主机名验证；1，启用主机名验证

默认值：0

ssl_trace

指定是否启用 SSL 跟踪。

限制：0，禁用 SSL 跟踪；1，启用 SSL 跟踪

默认值：0

ssl_trusted

定义对 SSL 连接的受托证书。

限制：到包含证书数据的文件的完整路径名。

默认值：none

crypto

CA Access Control 在以下注册表键下保留其使用的加密模块设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\crypto
```

crypto 注册表键包含以下注册表项：

ca_certificate

定义证书颁发机构 (CA) 证书数据库的完整路径名。

默认值：*ACInstallDir*\data\crypto\def_root.pem

communication_mode

指定是否启用安全套接字层 (SSL) 协议。

如果将此项设置为 ssl_only，则仅启用 SSL V2、SSL V3 和 TLS 连接。这意味着此计算机无法与不支持 SSL 的计算机通讯，因此无法与运行 CA Access Control r12.0 之前版本的计算机通讯，这些版本不支持 SSL。

注意：运行 CA Access Control r12.0 及更高版本的计算机支持 SSL。

如果将 fips_only 标记设置为 1，则在 FIPS 模式（即 TLS）下实际的通讯模式设置为 ssl_only，且忽略 communication_mode 标记。

有效值包括：

- all_modes
- ssl_only
- non_ssl

默认值：non_ssl

encryption_methods

指定 CA Access Control 代理用来解密消息的加密库。代理会依次尝试使用列表中的每个库，直到解密成功。

限制：aes256enc、aes192enc、aes128enc、desenc、tripledesenc、defenc

默认值：aes256enc、aes192enc、aes128enc、desenc、tripledesenc

fips_only

此标记用于控制 CA Access Control 是否以仅 FIPS 模式工作。 在此模式下，禁用所有非 FIPS 函数。

有效值:

1 CA Access Control 以仅 FIPS 模式工作

0 CA Access Control 以非 FIPS 模式工作

默认值：0

private_key

定义主题私钥的完整路径名。

默认值：*ACInstallDir*\data\crypto\sub.key

ssl_port

定义 CA Access Control 客户端和服务之间的 SSL 通讯端口。

默认值：5249

subject_certificate

定义主题证书的完整路径名。

默认值：*ACInstallDir*\data\crypto\sub.pem

数据

CA Access Control 在下列注册表键下保留其使用的内部设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Data

数据键条目仅供内部使用。 无法打开该键。

Dependency

CA Access Control 在以下注册表键下保留其使用的依存设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Dependency

如果将 CA Access Control 组件模块安装为另一产品的嵌入组件，则该注册表键的所有子键都是依赖于 CA Access Control 的产品的名称。 升级或卸载 CA Access Control 时，CA Access Control 会检查该注册表，并确定该进程是否可继续或必须中止。

devcalc

CA Access Control 在以下注册表键下保留其使用的偏差计算设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\devcalc

devcalc 注册表键包含以下注册表项：

dms_cmd_retry_interval

定义每个 DMS 通知命令重试之间的时间间隔（秒）。

默认值：60

max_dms_cmd_retry

定义在放弃操作之前，策略偏差计算器重试向 DMS 发送更新通知的最多次数。

默认值：3

max_lines_request

定义 *get devcalc* selang 命令任意一次返回的最大行数（从策略偏差数据文件中）。 然后，您还需要使用以下命令检索其他行：

```
get devcalc params("offset=X")
```

x

定义上一个 *get devcalc* 输出返回的行偏移量。

默认值：50

Exits

CA Access Control 在以下注册表键下保留其使用的 agent exit 设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits
```

Exits 注册表键不包含任何注册表项。 它包含每个 agent exit 的注册表子键。

AuthenticatePassword

CA Access Control 在以下注册表键下保留其使用的密码身份验证 agent exit 设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\AuthenticatePassword
```

Exits\AuthenticatePassword 注册表键包含以下注册表项：

Enable

启用或禁用密码规则实施代理退出的切换。 值为 0 则禁用退出。 任何其他值启用退出。

默认值：0

EnforcePasswordControl

使用 CA Access Control 客户端的密码规则实施的条件：

0－不实施密码规则

1－在常规用户更改其自己的密码时激活密码规则实施

2－管理员或密码管理员更改其他用户的密码或他们自己的密码时激活密码规则实施

3－值为 1 和 2 时的两种条件的累积

默认值： 1

引擎

CA Access Control 在以下注册表键下保留其使用的 CA Access Control engine (seos) agent exit 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Engine

默认情况下，Exits\Engine 注册表键不包含任何注册表项。

Remote Grace Info

CA Access Control 在以下注册表键下保留其使用的远程宽限信息 agent exit 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Remote Grace Info

Exits\Remote Grace Info 注册表键包含以下注册表项：

DefaultWarningDays

定义为 segrace\SegraceW 实用程序的用户显示密码到期警告的默认天数。 它表示如果正在应用这两个实用程序之一，并且用户的密码将在该注册表值指定的天数内到期，则向用户显示警告消息。

默认值： 7

远程关闭

CA Access Control 在以下注册表键下保留其使用的远程关闭 agent exit 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Exits\Remote Shutdown

Exits\Remote Shutdown 注册表键包含以下注册表项：

路径

远程关闭 DLL 的完整路径名称。

默认值：*ACInstallDir*\bin\remshut.dll

前缀

远程关闭 DLL 使用的定义前缀。

默认值：SD

FsiDrv

CA Access Control 在以下注册表键下保留其使用的驱动程序设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\FsiDrv

FsiDrv 注册表键包含以下注册表项：

AuditRefreshPeriod

定义来自同一个源的两个连续审核事件之间的最短时间（秒）。 CA Access Control 不记录在此时间内发生的来自同一个源的连续事件的审核消息。

默认值：0（记录所有审核事件）

BatchOplockStatus

指定是否禁用整个文件的批处理 OpLocks (opportunistic locking)。 禁用（值为零）时，驱动程序会收集文件访问的 100% 的审核信息，但性能会降低。 非零值可保持批处理 OpLocks 正常操作（启用）并提高性能，但是所提供的审核信息可能会不完整（可能不包括访问相关文件的尝试）。

注意：必须重新加载驱动程序才能使用新设置。 停止 CA Access Control (secons -s) 后，卸载驱动程序 (net stop seosdrv)。

默认值：1（启用）

CacheLimit

定义 seosdrv 内核内存缓存限制大小（兆字节）。

类型：REG_DWORD

限制：8 - 64

默认值：16

目录

驱动程序的位置。

默认位置： *system_drive**Windows_path*\system32\drivers

DynamicSysThreadDetection

指定 CA Access Control 跟踪所有内核模式线程，该线程由创建系统线程的其他产品所创建，例如：Trend Micro™ PC-cillin Antivirus。

注意：启用该注册表值可以在性能方面引发问题。 建议在您启用该注册表值前先联系 CA Technologies。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

类型：REG_DWORD

默认值：0（禁用）

FileCacheDisabled

启用或禁用常规文件缓存的切换。

值：0－启用常规文件缓存，1－禁用常规文件缓存

默认值：0

LoopHoleProtectionDisabled

指定是否禁用漏洞保护，漏洞保护可保护 CA Access Control 免受应用程序（例如可关闭其句柄的 Process Monitor (procmon.exe)）的影响。

值：0－启用漏洞保护；**1**－禁用漏洞保护。

默认值：0

注意：该键适用于 32 位 Windows 环境。

MaxAuditRecordLimit

定义审核队列限制。 队列长度超过该限制时，CA Access Control 会故意地降低生成审核事件的线程，以便可以读取队列并写入到日志文件中，比将新项目添加到队列要快一些。

注意：当新项目添加到队列的速度快于 CA Access Control 可读取和处理的速度时，系统的内存可能会耗尽。

默认值：200

MaxTimeoutLimit

定义触发驱动程序跳过之前 CA Access Control 检测到的连续超时数。到达该数时，驱动程序将会停止将授权请求发送到授权引擎，直到引擎表明处理事件就绪时才会继续。

值为 0 时禁用该跳过。

默认值： 5

QueueTimeout

等待 seosd 响应的最长时间（秒）。

默认值： 10

QueueTimeoutAnswer

驱动程序在超时后的响应。

默认值： 0（拒绝）

RegistryCacheDisabled

启用或禁用常规注册表缓存的切换。

值： 0－启用常规注册表缓存，1－禁用常规注册表缓存

默认值： 0

SilentModeAdmins

用线分隔的可在维护模式 (SilentModeEnabled =1) 下管理计算机的用户名列表。

无默认值

SilentModeEnabled

确定维护模式是否处于活动状态 (1)。

默认值： 0（禁用）

SystemBypassRestricted

指定 CA Access Control 是否跳过系统进程的访问权限检查。默认情况下，CA Access Control 不会将系统进程视为受信任，因此不会跳过系统进程的访问权限检查。

值：0－跳过访问权限检查；**1**－不跳过访问权限检查。

默认值： 1

Instrumentation

CA Access Control 在以下注册表键下保留其使用的 cainstrm.dll 行为设置（适用于所有已加载的插件）：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation
```

Instrumentation 注册表键包含以下注册表项：

活动

指定 cainstrm.dll 是否处于活动状态 (1)。

如果指定 0，则 cainstrm.dll 可加载但不处理任何插件。

类型： REG_DWORD

默认值： 1

ApplyOnProcess

定义要应用 instrumentation 的进程的列表。

可以定义服务名称或完整路径名。 名称*不*区分大小写。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型： REG_MULTI_SZ

默认情况下，未设置此标记（instrumentation 可应用于任何进程）。

ExcludeProcess

定义*不*应用 instrumentation 的进程的列表。

注意： 此项仅在未设置 ApplyOnProcess 时有效。

类型： REG_MULTI_SZ

默认情况下，未设置此标记。

OperationMode

指定 cainstrm.dll 是否将插件 (1) 加载到内存中。

类型： REG_DWORD

默认值： 1

RunTimeInstrumentationDisabled

指定运行时的 CA Access Control 检测策略。

类型： REG_DWORD

限制： 0（启用运行时检测)；1（已禁用运行时检测）。

默认值： 0

RunTimeInstrumentationIncludeList

定义要应用运行时检测的进程的列表。

类型：REG_MULTI_SZ

默认值：空

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型： REG_DWORD

默认值： 0

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

UnloadIfNoPlugins

指定如果没有为当前进程指定插件，cainstrm.dll 是否会自动卸载 (1)。

如果指定 0，则 cainstrm.dll 可加载但不处理插件。

类型： REG_DWORD

默认值： 1

.NET

CA Access Control 在以下注册表键下保留其使用的 .NET 设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET
```

Instrumentation\.NET 注册表键不包含任何注册表项。 它包含 .NET 探查器的注册表子键。

Profiler

CA Access Control 在以下注册表键下保留其使用的探查器设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET\Profiler
```

Instrumentation\.NEt\Profiler 注册表键包含以下注册表项：

ApplyOnProcess

定义要应用 instrumentation 的进程的列表。

可以定义服务名称或完整路径名。 名称不区分大小写。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型： REG_MULTI_SZ

默认值： w3wp.exe MultiCLRs.exe

CLSID

定义探查器的 CLSID。

类型：REG_SZ

默认值：{753C5090-0ADD-41B9-B074-8B9A7B833D7E}

OperationMode

指定是否将探查器加载到内存。

类型：REG_DWORD

限制：0、1

默认值：1

ReadConfigPeriodSec

指定汇集注册表更改的间隔。

类型：REG_DWORD

默认值：0x600

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileEnable

启用对文件的跟踪

类型：REG_DWORD

默认值：0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型：REG_DWORD

Assemblies

CA Access Control 在以下注册表键下保留其使用的 .NET 探查器程序集设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET\Profiler\Assemblies
```

.NET\Profiler\Assemblies 注册表键不包含任何注册表项。 它包含 .NET 探查器程序集的注册表子键。

CAPUPM.NETDBPlg

CA Access Control 在以下注册表键下保留其使用的 CAPUPM.NETBDPlg 设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET\Profiler\Assemblies\CAPUPM.NETDBPlg
```

Instrumentation\.NEt\Profiler\Assemblies\CAPUPM.NETDBPlg 注册表键包含以下注册表项：

BuildNumber

定义 .NET 程序集内部版本。

类型：REG_DWORD

默认值：0

MajorVersion

定义 .NET 程序集主要版本号。

类型：REG_DWORD

默认值：1

MinorVersion

定义 .NET 程序集次要版本号。

类型：REG_DWORD

默认值：0

PublicKeyToken

定义 .NET 程序集公钥令牌。

类型：REG_BINARY

默认值：5e 84 2e 72 e9 8c 10 e0

RevisionNumber

定义 .NET 程序集修订号。

类型：REG_DWORD
默认值：0

Plugins

CA Access Control 在以下注册表键下保留其使用的 .NET 探查器插件：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET\Profiler\Plugins
```

Instrumentation\.NET\Profiler\Plugins 注册表键不包含任何注册表项。 它包含 .NET 探查器插件的注册表子键。

DB

CA Access Control 在以下注册表键下保留其使用的数据库设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET\Profiler\Plugins\DB
```

Instrumentation\.NET\Profiler\Plugins\DB 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。
类型：REG_DWORD

默认值：1

ApplyOnProcess

定义要应用 instrumentation 的进程的列表。

可以定义服务名称或完整路径名。 名称不区分大小写。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

默认值：w3wp.exe MultiCLRs.exe

AutoBlockNativeAssemblies

定义是否阻止 CAPUPMProfilerDBPlg.dll 加载以及是否加载字节代码备份。

类型：REG_DWORD

默认值：1

OperationMode

指定是否将 CAPUPMProfilerDBPlg.dll 插件加载到内存。

类型：REG_DWORD

限制：0、1

默认值：1

PluginPath

指定 CAPUPMProfilerDBPlg.dll 插件的完整路径名。

类型：REG_SZ

默认值：C:\Program Files\CA\AccessControl\bin\CAPUPMProfilerDBPlg.dll

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型： RED_DWORD

限制： 0，假；1，真。

默认值： 0

TraceFileEnable

启用对文件的跟踪

类型： REG_DWORD

默认值： 0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型： REG_DWORD

限制： 0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值： 0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型： REG_DWORD

默认值： 0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型： REG_DWORD

默认值： 0

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型： REG_SZ

默认值： 空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型： REG_DWORD

默认值： 0

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

PluginManagement

CA Access Control 在以下键下维护其使用的动态插件的加载和卸载设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\
Instrumentation\PluginManagement
```

Instrumentation\PluginManagement 注册表键包含以下注册表项：

活动

指定插件动态加载是否为活动状态 (1)。

类型： REG_DWORD。

默认值： 1

Altitude

定义链中动态管理存根的顺序。

类型： REG-DWORD

默认值： 0x0fffffff（保留值）

ApplyOnDLL

只读值。

默认值： Kernel32.dll

ApplyOnProcess

定义要应用动态加载的进程列表。

可以定义服务名称或完整路径名。 名称不区分大小写。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型： REG_MULTI_SZ

默认情况下，未设置该标记（动态加载适用于任何插件）。

ExcludeProcess

定义动态加载*不*应用的进程列表。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下，未设置此标记。

LoadLibraryA

仅限内部使用。

默认值：0

LoadLibraryExA

仅限内部使用。

默认值：0

LoadLibraryExW

仅限内部使用。

默认值：1

LoadLibraryW

仅限内部使用

默认值：0

OperationMode

仅限内部使用。

默认值：1

ProcessCommanArguments

指定检测仪表模块是否在进程创建事件时通知 CA Access Control 安全服务。

类型：REG_DWORD

值：

0－检测仪表模块不在进程创建时通知 CA Access Control 安全服务。

1－检测仪表模块在进程创建时通知 CA Access Control 安全服务。

注意：注册表项值由 CA Access Control 安全服务自动更改，这取决于配置设置和数据库定义。 不要手动改变注册表项值。

PluginName

只读值。

默认值：*ACInstallDir*\bin\cainstrm.dll

PlugIns

CA Access Control 在以下注册表键下保留其使用的插件设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns
```

Instrumentation\PlugIns 注册表键不包含任何注册表项。 它包含每个已加载插件的注册表子键。

CMDPlg

CA Access Control 在以下注册表键下保留其使用的 CMD 插件设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\CMDPlg
```

Instrumentation\PlugIns\CMDPlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制：1-1000（此限制范围以外的值留作内部使用）

类型：REG_DWORD

默认值：5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型：REG_SZ

默认值：Kernel32.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

注意：如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认值：CMD.exe

CommunicationWaitTimeout

定义插件在发送或接收事务时等待的最长时间（秒）。

类型：REG_DWORD

默认值：15

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下为空。

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：1

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\CMDPlg.dll

ServiceTimeOut

定义等待具有 seosd 的事务的最大时间间隔（毫秒）。

注意：如果超时到期，则将授权请求。

类型：REG_DWORD

默认值：0x00000bb8（换转成十进制数为 3000）

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileEnable

启用对文件的跟踪

类型：REG_DWORD

默认值：0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型：REG_DWORD

默认值：60

OCIPlg

CA Access Control 在以下注册表键下保留其使用的 OCI 插件设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\OCIPlg

Instrumentation\PlugIns\OCIPlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制：1-1000（此限制范围以外的值留作内部使用）

类型：REG_DWORD

默认值：5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型：REG_SZ

默认值：oci.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

注意：如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认值：sqlplus.exe w3wp.exe

CommunicationWaitTimeout

定义插件在发送或接收事务时等待的最长时间（秒）。

类型：REG_DWORD

默认值：15

EnvironmentVariables

指定转发到 特权用户密码管理 代理的环境变量

类型：REG_MULTI_SZ

默认值：TNS_ADMIN ORACLE_HOME

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下为空。

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：0

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\OCIPlg.dll

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileEnable

启用对文件的跟踪

类型：REG_DWORD

默认值：0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型：REG_DWORD

默认值：60

UpgradeWaitTimeOutMaxTries

指定更新插件的重试次数。

类型：REG_DWORD

默认值：3

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

UpgradeWaitTimeOutMilliseconds

指定宣布升级失败的超时时间（毫秒）。

类型：REG_DWORD

默认值：0x1ffff (131071)

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

ODBCPlg

CA Access Control 在以下注册表键下保留其使用的 特权用户密码管理 代理 ODBC 插件设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\ODBCPlg
```

Instrumentation\PlugIns\ODBCPlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制：1-1000（此限制范围以外的值留作内部使用）

类型：REG_DWORD

默认值：5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型：REG_MULTI_SZ

默认值：ODBC32.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

注意：如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认值：w3wp.exe

CommunicationWaitTimeout

定义插件在发送或接收事务时等待的最长时间（秒）。

类型：REG_DWORD

默认值：15

EnvironmentVariables

指定转发到 特权用户密码管理 代理的环境变量

类型：REG_MULTI_SZ

默认值：TNS_ADMIN ORACLE_HOME

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下为空。

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：0

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\ODBCPlg.dll

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型： RED_DWORD

限制： 0，假；1，真。

默认值： 0

TraceFileEnable

启用对文件的跟踪

类型： REG_DWORD

默认值： 0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型： REG_DWORD

限制： 0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值： 0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型： REG_DWORD

默认值： 0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0ffffffff，不筛选任何信息（显示所有信息）。

类型： REG_DWORD

默认值： 0

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型： REG_SZ

默认值： 空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型： REG_DWORD

默认值： 0

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型： REG_DWORD

默认值： 60

UpgradeWaitTimeOutMaxTries

指定更新插件的重试次数。

类型： REG_DWORD

默认值： 3

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

UpgradeWaitTimeOutMilliseconds

指定宣布升级失败的超时时间（毫秒）。

类型： REG_DWORD

默认值： 0x1ffff (131071)

注意： 建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

OLEDBPlg

CA Access Control 在以下注册表键下保留其使用的 特权用户密码管理 代理 OLEDB 插件设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns\OLEDBlg

Instrumentation\PlugIns\OLEDBPlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制：1-1000（此限制范围以外的值留作内部使用）

类型：REG_DWORD

默认值：5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型：REG_MULTI_SZ

默认值：kernel32.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

注意：如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认值：w3wp.exe sqlcmd.exe

CommunicationWaitTimeout

定义插件在发送或接收事务时等待的最长时间（秒）。

类型：REG_DWORD

默认值：15

EnvironmentVariables

指定转发到 特权用户密码管理 代理的环境变量

类型：REG_MULTI_SZ

默认值：TNS_ADMIN ORACLE_HOME

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下为空。

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：0

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\OLEDBPlg.dll

SerializationWaitTimeout

定义 loadlibrary 与 DllGetClassObject 类的内部同步。

类型：REG_DWORD

默认：0xa（转换成十进制数为 10）

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileEnable

启用对文件的跟踪

类型：REG_DWORD

默认值：0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型：REG_DWORD

默认值：60

UpgradeWaitTimeOutMaxTries

指定更新插件的重试次数。

类型：REG_DWORD

默认值：3

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

UpgradeWaitTimeOutMilliseconds

指定宣布升级失败的超时时间（毫秒）。

类型：REG_DWORD

默认值：0x1ffff (131071)

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

Providers

CA Access Control 在以下注册表键下保留 OLEDB 插件支持的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers
```

Instrumentation\PlugIns\OLEDBPlg\Providers 注册表键不包含任何注册表项。 此注册表键包含 OLEDB 插件支持的每个提供程序的注册表子键。

注意：OLEDB 插件支持的一些提供程序在 CA Access Control 中不受支持。

一般

CA Access Control 在以下注册表键下保留 OLEDB 插件支持的常规提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Generic
```

Instrumentation\PlugIns\OLEDBPlg\Providers\Generic 注册表键不包含任何注册表项。 此注册表键包含 OLEDB 插件支持的常规提供程序的注册表子键。

CLSID

CA Access Control 在以下注册表键下保留 OLEDB 插件支持的常规提供程序的 CLSID（类标识符）设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Generic\CLSID
```

默认情况下，Instrumentation\PlugIns\OLEDBPlg\Providers\Generic\CLSID 注册表键不包含任何注册表项。 在该子键中创建的项必须具有以下格式：

CLSID

定义提供商的类标识符。

类型：REG_SZ

限制：1，启用对提供商的支持；0，禁用对提供商的支持。

名称

CA Access Control 在以下注册表键下保留 OLEDB 插件支持的常规提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Generic\Name
```

Instrumentation\PlugIns\OLEDBPlg\Providers\Generic\Name 注册表键包含以下注册表项：

Microsoft OLE DB Provider for ODBC Drivers

指定 OLEDB 插件支持 Microsoft OLE DB Provider for ODBC Drivers。

类型：REG_DWORD

限制：1（启用支持）；0（禁用支持）。

默认值：1

Jet

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Microsoft Jet 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Jet
```

Instrumentation\PlugIns\OLEDBPlg\Providers\Jet 注册表键不包含任何注册表项。 此注册表键包含 OLEDB 插件所支持基于 Microsoft Jet 的提供程序的注册表子键。

注意：CA Access Control 目前不支持基于 Microsoft Jet 的提供商。

CLSID

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Microsoft Jet 的提供程序的 CLSID（类标识符）设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Jet\CLSID
```

注意：CA Access Control 目前不支持基于 Microsoft Jet 的提供商。

默认情况下，Instrumentation\PlugIns\OLEDBPlg\Providers\Jet\CLSID 注册表键不包含任何注册表项。 在该子键中创建的项必须具有以下格式：

CLSID

定义提供商的类标识符。

类型：REG_SZ

限制：1，启用对提供商的支持；0，禁用对提供商的支持。

名称

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Microsoft Jet 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Jet\Name
```

注意：CA Access Control 目前不支持基于 Microsoft Jet 的提供商。

Instrumentation\PlugIns\OLEDBPlg\Providers\Jet\Name 注册表键包含以下注册表项：

Microsoft Jet 4.0 OLE DB Provider

指定 OLEDB 插件支持 Microsoft Jet 4.0 OLE DB Provider。

类型： REG_DWORD

限制： 1（启用支持）；0（禁用支持）。

默认值： 1

Microsoft Office 12.0 Access Database Engine OLE DB Provider

指定 OLEDB 插件支持 Microsoft Office 12.0 Access Database Engine OLE DB Provider。

类型： REG_DWORD

限制： 1（启用支持）；0（禁用支持）。

默认值： 1

MSSQL

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Microsoft SQL Server 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\MSSQL
```

Instrumentation\PlugIns\OLEDBPlg\Providers\MSSQL 注册表键不包含任何注册表项。 此注册表键包含 OLEDB 插件所支持基于 Microsoft SQL Server 的提供程序的注册表子键。

CLSID

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Microsoft SQL Server 的提供程序的 CLSID（类标识符）设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\MSSQL\CLSID
```

默认情况下，Instrumentation\PlugIns\OLEDBPlg\Providers\MSSQL\CLSID 注册表键不包含任何注册表项。 在该子键中创建的项必须具有以下格式：

CLSID

定义提供商的类标识符。

类型： REG_SZ

限制： 1，启用对提供商的支持；0，禁用对提供商的支持。

名称

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Microsoft SQL Server 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\MSSQL\Name
```

Instrumentation\PlugIns\OLEDBPlg\Providers\MSSQL\Name 注册表键包含以下注册表项：

Microsoft OLE DB Provider for SQL Server

指定 OLEDB 插件支持 Microsoft OLE DB Provider for SQL Server。

类型： REG_DWORD

限制： 1（启用支持）；0（禁用支持）。

默认值： 1

SQL Native Client

指定 OLEDB 插件支持 SQL Native Client 提供程序。

类型： REG_DWORD

限制： 1（启用支持）；0（禁用支持）。

默认值： 1

SQL Server Native Client 10.0

指定 OLEDB 插件支持 SQL Server Native Client 10.0 提供程序。

类型： REG_DWORD

限制： 1（启用支持）；0（禁用支持）。

默认值： 1

MySQL

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 MySQL 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\MySQL
```

Instrumentation\PlugIns\OLEDBPlg\Providers\MySQL 注册表键不包含任何注册表项。 此注册表键包含 OLEDB 插件所支持基于 MySQL 的提供程序的注册表子键。

注意： CA Access Control 目前不支持基于 MySQL 的提供商。

CLSID

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 MySQL 的提供程序的 CLSID（类标识符）设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\MySQL\CLSID
```

注意：CA Access Control 目前不支持基于 MySQL 的提供商。

默认情况下，Instrumentation\PlugIns\OLEDBPlg\Providers\MySQL\CLSID 注册表键不包含任何注册表项。 在该子键中创建的项必须具有以下格式：

CLSID

定义提供商的类标识符。

类型：REG_SZ

限制：1，启用对提供商的支持；0，禁用对提供商的支持。

名称

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 MySQL 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\MySQL\Name
```

注意：CA Access Control 目前不支持基于 MySQL 的提供商。

Instrumentation\PlugIns\OLEDBPlg\Providers\MySQL\Name 注册表键包含以下注册表项：

MySQL 提供程序

指定 OLEDB 插件支持 MySQL Provider。

类型：REG_DWORD

限制：1（启用支持）；0（禁用支持）。

默认值：1

MySQL.OLEDB Provider

指定 OLEDB 插件支持 MySQL.OLEDB Provider。

类型：REG_DWORD

限制：1（启用支持）；0（禁用支持）。

默认值：1

Oracle

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Oracle 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Oracle
```

Instrumentation\PlugIns\OLEDBPlg\Providers\Oracle 注册表键不包含任何注册表项。 此注册表键包含 OLEDB 插件所支持基于 Oracle 的提供程序的注册表子键。

CLSID

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Oracle 的提供程序的 CLSID（类标识符）设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Oracle\CLSID
```

默认情况下，Instrumentation\PlugIns\OLEDBPlg\Providers\Oracle\CLSID 注册表键不包含任何注册表项。 在该子键中创建的项必须具有以下格式：

CLSID

定义提供商的类标识符。

类型：REG_SZ

限制：1，启用对提供商的支持；0，禁用对提供商的支持。

名称

CA Access Control 在以下注册表键下保留 OLEDB 插件所支持基于 Oracle 的提供程序的设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\
OLEDBPlg\Providers\Oracle\Name
```

Instrumentation\PlugIns\OLEDBPlg\Providers\Oracle\Name 注册表键包含以下注册表项：

Microsoft OLE DB Provider for Oracle

指定 OLEDB 插件支持 Microsoft OLE DB Provider for Oracle。

类型：REG_DWORD

限制：1（启用支持）；0（禁用支持）。

默认值：1

Oracle Provider for OLE DB

指定 OLEDB 插件支持 Oracle Provider for OLE DB。

类型： REG_DWORD

限制： 1（启用支持）；0（禁用支持）。

默认值： 1

RunAsPlg

CA Access Control 在以下注册表键下保留其使用的 RunAs 插件设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\RunAsPlg
```

Instrumentation\PlugIns\RunAsPlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制： 1-1000（此限制范围以外的值留作内部使用）

类型： REG_DWORD

默认值： 5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型： REG_MULTI_SZ

默认值： advapi32.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型： REG_MULTI_SZ

注意： 如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认值： runas.exe explorer.exe consent.exe

注意： consent.exe 值仅适用于 Windows Server 2008 计算机。

CommunicationWaitTimeout

定义插件在发送或接收事务时等待的最长时间（秒）。

类型： REG_DWORD

默认值： 15

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下为空。

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：1

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\RunAsPlg.dll

ServiceTimeOut

定义等待具有 seosd 的事务的最大时间间隔（毫秒）。

注意：如果超时到期，则将授权请求。

类型：REG_DWORD

默认值：0x00000bb8（换转成十进制数为 3000）

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileEnable

启用对文件的跟踪

类型：REG_DWORD

默认值：0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型：REG_DWORD

默认值：60

StopPlg

CA Access Control 在以下注册表键下保留其使用的堆栈溢出保护 (STOP) 插件设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\StopPlg
```

Instrumentation\PlugIns\StopPlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制：1-1000（此限制范围以外的值留作内部使用）

类型：REG_DWORD

默认值：5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型：REG_MULTI_SZ

默认值：Kernel32.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

注意：如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认情况下，未设置此标记（插件可应用于任何进程）。

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认值 (Windows 2008)：slsvc.exe

默认值（所有其他 Windows 版本）：空白（未设置标记）

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：0

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\StopPlg.dll

STOPClientTraceEnabled

指定 STOP 客户端模块是否已启用跟踪记录。

类型：REG_DWORD

默认值：0（禁用）

STOPClientTraceModulePath

定义 STOP 客户端模块跟踪记录模块的完整路径名。

类型：REG_SZ

默认值：*ACInstallDir*\bin\STOPClientTrace.dll

STOPSEHHandlingModeDisabled

指定是否启用对基于 SEH 的 exploit 的 STOP 扩展检查。

类型：REG_DWORD

默认值：1（禁用）

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

WinServicePlg

CA Access Control 在以下注册表键下保留其使用的 Windows 服务保护插件设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
PlugIns\WinServicePlg
```

Instrumentation\PlugIns\WinServicePlg 注册表键包含以下注册表项：

Altitude

定义插件的加载顺序。

限制：1-1000（此限制范围以外的值留作内部使用）

类型：REG_DWORD

默认值：5

ApplyOnDLL

定义应用当前插件的 DLL 名称（模块）。

类型：REG_MULTI_SZ

默认值：Rpcrt4.dll

ApplyOnProcess

定义要应用当前插件的进程。

您可以提供服务名、文件名或完整的路径名。 例如：“services.exe”、“\system32\services.exe”、“c:\windows\system32\services.exe”。

类型：REG_MULTI_SZ

注意：如果此注册表项只有一个值，则 REG_SZ 也是有效的类型。

默认值：Services.exe

ExcludeProcess

定义不应用插件的进程。

注意：此项仅在未设置 ApplyOnProcess 时有效。

类型：REG_MULTI_SZ

默认情况下为空。

OperationMode

指定是否将插件 (1) 加载到内存中。

类型：REG_DWORD

默认值：1

PluginName

定义插件动态链接库 (DLL) 的名称。

类型：REG_SZ

默认值：*ACInstallDir*\bin\WinServicePlg.dll

ServiceTimeOut

定义等待具有 seosd 的事务的最大时间间隔（毫秒）。

注意：如果超时到期，则将授权请求。

类型：REG_DWORD

默认值：0x00000bb8（换转成十进制数为 3000）

TraceDbgEnable

指定是否跟踪 cainstrm 模块的状态标志，即启用对 DbgView 或内核调试器的跟踪。

类型：RED_DWORD

限制：0，假；1，真。

默认值：0

TraceFileEnable

启用对文件的跟踪

类型：REG_DWORD

默认值：0（禁用）

TraceFileIsCyclic

指定跟踪文件的类型。

类型：REG_DWORD

限制：0，跟踪文件不是循环使用的；1，跟踪文件是循环使用的。

默认值：0

TraceFileSizeLimit

定义跟踪文件的最大大小（字节）。 值为 0 表示跟踪文件没有最大大小限制。

类型：REG_DWORD

默认值：0

TraceFilteringMask

为每个插件定义筛选掩码。 对于此注册表值，受支持的值因要定义注册表值的软件组件的状态而异。 有两个预先定义的值：0，筛选所有信息（不显示任何信息）；0x0fffffff，不筛选任何信息（显示所有信息）。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceFolderPath

定义跟踪文件的完整路径名。

类型：REG_SZ

默认值：空

TraceOutputMask

为跟踪输出通道（调试流、文件或 ETW）定义筛选掩码。 可以指定将跟踪结果输出到文件、DbgView 调试通道或 WinDbg 调试通道。 值为 0 时禁用所有输出。

类型：REG_DWORD

默认值：0

注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

TraceReadParamsSec

定义更新跟踪参数的时间间隔：WinServicePlg.dll 每隔 TraceReadParamsSec 读取更新跟踪参数一次。

类型：REG_DWORD

默认值：0x0000003c（60 进制）

lang

CA Access Control 在以下注册表键下保留其使用的管理语言 (selang) 设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\lang
```

lang 注册表键包含以下注册表项：

HandleHomeDir

确定是否已更新本机用户帐号的 HOME_DIR 属性和是否已创建主目录的值。

如果该值被设置为 0，则只有用户的 HOME_DIR 属性被更新。如果该值被设置为 1，则用户的属性被更新且在文件系统中实际创建主目录。

默认值：1

help_path

lang 帮助文件所在的目录。

默认值：*ACInstallDir*\data\help

ModifiableClassFlags

指定 CA Access Control 管理员可以使用以下 selang 命令更改的标志：setoptions class *className* flags{+ | -} (*flag*)

值：W－为指定的类设置警告模式；I－为指定类中的资源更改区分大小写功能；WI－设置警告模式，并为指定类中的资源更改区分大小写功能

默认值：W

query_size

数据库查询中列出的最大记录数。

默认值：100

SetBlockRun

指定是否检查程序受信任与否，以及是否阻止执行不受信任的程序。

有效值包括：

yes－采用 viapgm 授权规则定义的所有程序都将 blockrun 属性设置为 yes。

no－采用 viapgm 授权规则定义的所有程序都将 blockrun 属性设置为 no。

默认值：Yes

SpaceReplace

仅限内部使用。 该项应始终为空。

默认值：""

use_old_commands

指定是否禁用旧的 ACF2™ 兼容性命令（ag、lg、rg、lu、au 等）。

限制：0－不支持旧命令，1－支持旧命令

默认值：1（支持旧命令）

logmgr 键－注册表设置

CA Access Control 在以下注册表键下保留其使用的记录设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\logmgr

logmgr 注册表键包含以下注册表项：

audit_back

CA Access Control 审核备份文件的名称。 只有 CA Access Control 可写入该文件。

默认值：*ACInstallDir*\log\seos.audit.bak

audit_group

可读取审核日志的组。

默认值：ComputerAssociates

audit_log

CA Access Control 审核日志文件的名称。 如果此文件达到 audit_size 中指定的大小，则 CA Access Control 会关闭此文件，使用 audit_back 中的名称重命名该文件并创建新的审核日志。只有 CA Access Control 可写入该文件。

默认值：*ACInstallDir*\log\seos.audit

audit_max_files

定义当 CA Access Control 执行数据触发的备份时所累积的审核日志备份文件的最大数量。 当 BackUp_Date 配置设置被设为除 *none* 外的任何值时，CA Access Control 将继续累积数据触发的备份文件。 通过此配置设置，可以减少 CA Access Control 用于审核日志备份的磁盘空间。当审核日志备份文件的数量达到设置的限制时，CA Access Control 会在创建最新的备份文件时删除最早的备份文件。

值：

- **0**－保留所有审核日志备份文件。
- *n*－大于零的正整数。

注意：您无法手动删除冗余审核日志备份文件，因为 CA Access Control 将自动保护这些文件。 此外，如果启用审核报告功能，则直到报告代理完成报告处理时，CA Access Control 才会删除备份文件。

默认值：50

audit_size

CA Access Control 审核日志文件的最大大小（KB）。不要指定小于 50 KB 的值。

默认值：10240

注意：在审核文件大小超过 2 GB 时，CA Access Control 会停止将审核记录写入审核文件。

AuditFiltersFile

CA Access Control 审核筛选文件的名称。

默认值：*ACInstallDir*\data\audit.cfg

BackUp_Date

指定 CA Access Control 备份审核日志文件的条件，以及 CA Access Control 是否在备份文件名中添加时间戳。

CA Access Control *始终*在审核日志文件达到 audit_size 配置设置中指定的大小时备份该文件。

值：none、yes、daily、weekly 和 monthly。

- yes－CA Access Control 在审核日志文件达到 audit_size 中指定的大小时对其进行备份，并在备份文件名中添加时间戳。
- none－CA Access Control 在审核日志文件达到 audit_size 中指定的大小时对其进行备份，但不在备份文件名中添加时间戳。

- daily、weekly、monthly－只要达到指定的时间间隔*且*审核日志文件达到 audit_size 中指定的大小，CA Access Control 就会备份审核日志文件，并在备份文件名中添加时间戳。 但是，如果在指定时间间隔内没有审核事件写入审核日志文件，则 CA Access Control 不会在经过该时间间隔后备份文件。

  注意：CA Access Control 从第一个审核日志文件的创建时间起计算指定的时间间隔，并在相应日期的午夜备份文件。

示例：该配置设置的值为 weekly，并且 CA Access Control 在 4 月 1 日星期五上午 9:00 创建了审核日志文件。 在这一周发生了许多审核事件，审核日志文件在 4 月 4 日星期一超过了 audit_size 配置设置。 CA Access Control 在 4 月 4 日备份审核日志文件，并在备份文件名中添加时间戳。 在第一次创建审核日志文件之后的一周，即 4 月 8 日星期五的午夜，CA Access Control 再次备份审核日志文件，并在备份文件名中添加时间戳。

限制：这些值必须全部为大写字母或全部以小写字母。

默认值：yes

error_back

CA Access Control 错误备份文件的名称。

默认值：*ACInstallDir*\log\seos.error.bak

error_group

可读取错误日志文件的组。

如果该值被设置为 none，则只有管理员可读取该文件。

默认值：none

error_log

CA Access Control 错误日志文件的名称。 当该文件达到 error_size 中指定的大小时，CA Access Control 将关闭该文件，使用 error_back 中的名称重命名该文件并创建新的错误日志。只有 CA Access Control 可写入该文件。

默认值：*ACInstallDir*\log\seos.error

error_size

CA Access Control 错误日志文件的最大大小（KB）。

默认值：50

irecorder_audit

指定除本地安全服务审核事件外，IR API 库是否传递现有 PMD 的审核事件。

all－除本地安全服务审核事件外，还传递策略模型的审核事件。

localhost－仅传递本地安全服务的审核事件。

默认值：all

SendAuditToNativeChannel

（仅限 Windows 2008）指定 seosd 是否将审核事件发送到 CA Access Control 的 Windows 2008 事件日志通道 (1)。

默认值：0（不发送）

SendAuditToNativeLog

指定 seosd 是否将审核事件发送到 Windows 事件日志 (1)。

默认值：0（不发送）

message

CA Access Control 在以下注册表键下保留其使用的消息传送设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\message
```

message 注册表键包含以下注册表项：

filename

可提供 CA Access Control 命令响应中显示的大多数消息的文件的名称。

默认值：*ACInstallDir*\Data\SeOS.msg

MessagesDirectory

指定 CA Access Control 消息文件的位置。

默认值：*ACInstallDir*\Data\Messages

OS_user

CA Access Control 在以下注册表键下保留其使用的企业用户设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\OS_user

OS_user 注册表键包含以下注册表项：

create_user_in_db

指定当未针对 CA Access Control 定义的用户登录时，CA Access Control 是否为该用户创建 XUSER 记录。

注意：只有在使用企业用户（osuser_enabled 设置为 1）时，此设置才适用。

有效值包括：

0—CA Access Control 不自动创建 XUSER 记录。

1—CA Access Control 自动创建 XUSER 记录

默认值：1

osuser_enabled

指定是否启用企业用户和组。

有效值包括：

0—禁用企业用户和组。

1—启用企业用户和组。

默认值：1

passwd

CA Access Control 在以下注册表键下保留其使用的密码设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\passwd

passwd 注册表键包含以下注册表项：

DefaultPgroup

仅限内部使用。

默认值： other

Dictionary

定义包含*不能*用作密码的单词的文件的完整路径名。

注意： 要使用此文件，必须将词典格式密码规则 (use_dbdict) 设置为 *file*，并将 UseDict 设置为 *yes*。 如果词典格式设置为 *db*，则无法使用的密码取自 CA Access Control 数据库，并将忽略此设置。

默认值： *ACInstallDir*\data\words

EnforceViaEtrust

指定是否仅通过 CA Access Control 强制更新或创建用户的密码。

默认值： 0（不一定使用 CA Access Control）

PasswordTimeOut

定义 CA Access Control 密码筛选器等待授权响应的最长时间（毫秒）。

默认值： 4000

PasswordTimeOutAnswer

指定如果授权进程在给定超时内未响应，则将应答发送回 LSA。

如果将其设置为 0，则拒绝密码更改。 如果将其设置为 1，则批准密码更改。

默认值： 0

UseDict

指定在验证密码时是否使用词典文件（通过 Dictionary 设置进行设置）。

注意： 要使用词典文件，还必须将词典格式密码规则 (use_dbdict) 设置为 *file*。 如果词典格式设置为 *db*，则无法使用的密码取自 CA Access Control 数据库，并将忽略此设置。

默认值： no

Pmd

CA Access Control 在以下注册表键下保留其使用的常规策略模型设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd

Pmd 注册表键包含以下注册表项：

__pmd_backup_directory__

定义 CA Access Control 用来存储策略模型备份的目录。 CA Access Control 将每个 PMD 备份存储在名为 *pmd_name* 的子目录中。

默认值：*ACInstallDir*\Data\policies_backup

_Pmd_directory_

定义 PMDB 数据库文件所在的目录。

默认值：*ACInstallDir*\Data

ClientOperationTimeout

定义本计算机上的策略模型客户端等待策略模型的响应时间（秒）。如果策略模型没有在该时间范围内响应，那么策略模型客户端假设该策略模型没有响应。

默认值：60

MaximumPolicyModels

定义可以创建的策略模型的最大数量。

默认值：16

SendAuditToNativeLog

指定 CA Access Control 是否将策略模型审核事件发送到 Windows 事件日志。

值：0－不将审核事件发送到 Windows 事件日志，1－将审核事件发送到 Windows 事件日志。

默认值：0

ShutdownWaitingTimeout

定义本计算机上的策略模型等待其组件正常关闭的时间（毫秒）。如果策略模型组件在该时间范围内未正常关闭，则策略模型将强制其关闭。

默认值：60000（1 分钟）

TCPReceiveTimeout

定义本计算机上的策略模型等待其订户响应的时间（秒）。 如果策略模型订户在该时间范围内未响应，则策略模型将关闭它与该订户的连接。

默认值：60

<PMDB_Name>

CA Access Control 在以下注册表键下保留其使用的特定策略模型设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*PMDB_Name*

每个 Pmd*PMDB_Name* 注册表键包含以下注册表项：

_Min_Retries

定义策略模型尝试连接订户的失败次数，达到该次数后将认为该订户不可用。

默认值：4

_Retry_Timeout

定义策略模型在达到 _Min_Retries 中指定的最少尝试次数之后、尝试将更新重新发送到不可用订户之前等待的时间（分钟）。

默认值：30

_Shutoff_Time_

过时。

Active_Policy

定义策略模型的名称。

Always_Propagate

指定出错时，策略模型是否传播命令。 默认情况下，策略模型始终发送要传播的命令。 如果将其设置为 *no*，则出错时，策略模型将不发送命令。

默认值：Yes

Auto_Truncate

指定在未指定 auto 和 offset 的情况下执行 sepmd -t 时 sepmd 是否截短更新文件。

值：Yes－如果不指定 sepmd -t 参数，sepmd 将自动截短更新文件，No－如果不指定 sepmd -t 参数，sepmd 不截短更新文件

默认值：Yes

筛选

定义更新文件的筛选文件完整路径名。

无默认值。

force_auto_truncate

指定 CA Access Control 是否截短更新文件，即使策略模型没有订户。

您可以手动截短更新文件 (sepmd -t)，CA Access Control 也会根据定义触发自动截短事件的单独配置设置 (trigger_auto_truncate) 自动截短文件。

注意：如果策略模型的所有订户都“不同步”，则策略模型实际上没有订户。

默认值：Yes

Parent_Pmd

定义作为此策略模型更新源的父 PMDB 的名称。

无默认值。

trigger_auto_truncate

定义触发更新文件自动截短功能的策略模型更新文件大小（兆字节）。

如果将此项设置为 0，CA Access Control 将使用硬编码的默认值 (100 MB)。 如果使用大于上限的值，CA Access Control 将使用上限值。

类型：REG_DWORD

限制：1-2000 MB

默认值（DMS__ 和 DH__WRITER）：1024 MB

默认值（所有其他 PMDB）：100 MB

UseEncryption

指定是否对保存到 updates.dat 文件的更新信息进行加密。

值：0－不加密 updates.dat 文件，1－加密 updates.dat 文件

默认值：0

logmgr

CA Access Control 在以下注册表键下保留其使用的特定策略模型日志设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*PMDB_Name*\logmgr

每个 Pmd*PMDB_Name*\logmgr 注册表键包含以下注册表项：

audit_back

定义策略模型审核备份文件的名称。只有 CA Access Control 可写入该文件。

默认值： pmd_audit.bak

audit_group

定义可读取审核日志的组。

默认值： Computer Associates

audit_log

定义策略模型审核日志文件的名称。如果该文件达到 audit_size 中指定的大小，则 CA Access Control 将关闭该文件、使用在 audit_back 中设置的名称重命名该文件并创建新的审核日志。 只有 CA Access Control 可写入该文件。

默认值： pmd.audit

audit_size

定义策略模型审核日志文件的最大大小（KB）。 不要指定小于 50 KB 的值。

默认值： 1024

error_back

定义策略模型错误备份文件的名称。

默认值： pmd_error.back

error_group

定义可读取错误日志文件的组。

如果该值被设置为 *none*，则只有管理员可读取该文件。

默认值： none

error_log

指定策略模型错误日志文件的名称。当该文件达到 error_size 中指定的大小时，CA Access Control 将关闭该文件，使用 error_back 中的名称重命名该文件并创建新的错误日志。只有 CA Access Control 可写入该文件。

默认值： pmd.error

error_size

定义 CA Access Control 错误日志文件的最大大小（KB）。

默认值： 1024

<DMS_Name>

CA Access Control 在以下注册表键下保留其使用的特定 DMS 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*DMS_Name*

Pmd*DMS_Name* 注册表键包含以下注册表项：

_Min_Retries

定义策略模型尝试连接订户的失败次数，达到该次数后将认为该订户不可用。

默认值： 4

_Retry_Timeout

定义策略模型在达到 _Min_Retries 中指定的最少尝试次数之后、尝试将更新重新发送到不可用订户之前等待的时间（分钟）。

默认值： 30

_Shutoff_Time_

过时。

Active_Policy

定义策略模型的名称。

Always_Propagate

指定出错时，策略模型是否传播命令。 默认情况下，策略模型始终发送要传播的命令。 如果将其设置为 *no*，则出错时，策略模型将不发送命令。

默认值： Yes

Auto_Truncate

指定在未指定 auto 和 offset 的情况下执行 sepmd -t 时 sepmd 是否截短更新文件。

值：Yes－如果不指定 sepmd -t 参数，sepmd 将自动截短更新文件，No－如果不指定 sepmd -t 参数，sepmd 不截短更新文件

默认值：Yes

筛选

定义更新文件的筛选文件完整路径名。

无默认值。

force_auto_truncate

指定 CA Access Control 是否截短更新文件，即使策略模型没有订户。

您可以手动截短更新文件 (sepmd -t)，CA Access Control 也会根据定义触发自动截短事件的单独配置设置 (trigger_auto_truncate) 自动截短文件。

注意：如果策略模型的所有订户都“不同步”，则策略模型实际上没有订户。

默认值：Yes

Parent_Pmd

定义作为此策略模型更新源的父 PMDB 的名称。

无默认值。

trigger_auto_truncate

定义触发更新文件自动截短功能的策略模型更新文件大小（兆字节）。

如果将此项设置为 0，CA Access Control 将使用硬编码的默认值 (100 MB)。 如果使用大于上限的值，CA Access Control 将使用上限值。

类型：REG_DWORD

限制：1-2000 MB

默认值（DMS__ 和 DH__WRITER）：1024 MB

默认值（所有其他 PMDB）：100 MB

UseEncryption

指定是否对保存到 updates.dat 文件的更新信息进行加密。

值：0－不加密 updates.dat 文件，1－加密 updates.dat 文件

默认值：0

endpoint_management

CA Access Control 在以下注册表键下保留其使用的特定 DMS 端点管理设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*DMS_NAME*\endpoint_management

在创建 DMS 时，dmsmgr 会在该注册表键中定义注册表值。 如果主机上不存在 DMS，则不定义该注册表键。

Pmd*DMS_Name*\endpoint_management 注册表键包含以下注册表项：

commands_to_exec_before_sleep

指定 DMS 在进入休眠前在一个循环中执行的端点命令数。

默认值：10

debug_mode

指定 CA Access Control 是否将调试消息写入 DMS 目录 (1) 中的 endpoint_management.log 文件。

限制：0、1

默认值：0（禁用调试）

注意：日志文件位于 *DMSInstallDirectory*\endpoint_management.log

operation_mode

指定是否启用通过 CA Access Control 消息队列进行中央 (DMS) 端点管理。

限制：0、1

默认值：1（启用）

sleep_between_exec_commands

指定 DMS 休眠的时间长度（毫秒）。 当 DMS 唤醒时，它会执行 commands_to_exec_before_sleep 注册表值所指定个数的端点命令。

默认值：100

policyfetcher

CA Access Control 在以下注册表键下保留其使用的 policyfetcher 服务设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\policyfetcher
```

policyfetcher 注册表键包含以下注册表项：

check_deployment_tasks

定义 policyfetcher 在分发主机上检查新部署任务（DEPLOYMENT 资源）的频率（秒）。

默认值：600（每 10 分钟）

deploy_timeout

定义 policyfetcher 在端点上等待部署任务或取消部署任务完成的秒数。

默认值：900

devcalc_command

定义 policyfetcher 用来运行偏差计算的 selang 命令。

默认值：start DEVCALC params(-nonotify)

示例：start DEVCALC params(-nonotify -precise)

dh_command_retry_interval

定义每个 DH 通知命令重试之间的时间间隔（秒）。

默认值：30

endpoint_heartbeat

定义 policyfetcher 将心跳发送到分发主机 (DH) 的频率。 该频率是 check_deployment_task 设置的一个要素，可确定 policyfetcher 在发送心跳之前检查部署任务的次数。例如：如果将 check_deployment_task 设置为默认的 600 秒（10 分钟）且将此标记设置为 6，那么 policyfetcher 将每 3600 秒（1 小时）发送一次心跳。

在发送心跳后，policyfetcher 还将运行偏差计算器（start devcalc 命令），然后等待 60 秒，使系统完成偏差计算。 在 60 秒之后，policyfetcher 会继续检查本地端点信息是否与 DH 信息相同。

默认值：10

max_dh_command_retry

定义 policyfetcher 在放弃前最多重复尝试从 DH 获取更新通知的次数。

默认值：3

max_dh_retry_cycles

定义 policyfetcher 在切换到灾难恢复 DH 前最多重复尝试从生产 DH 获取更新通知的循环数。

默认值：3

policy_verification

指定 policyfetcher 是否在执行任务之前先验证备份 CA Access Control 数据库上的新部署任务。

有效值:

1—运行策略验证

0—禁用策略验证

默认值：0

policyfetcher_enabled

指定是否运行 policyfetcher 服务。

有效值:

1—运行 policyfetcher

0—禁用 policyfetcher

默认值：0

PUPMAgent

CA Access Control 在以下注册表键下保留其使用的 特权用户密码管理 代理设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\PUPMAgent
```

特权用户密码管理 代理注册表键包含以下注册表项：

EnableLogonIntegration

指定启用终端集成。

限制：0，禁用终端集成；1，启用终端集成。

默认值：1

EnableRunAsInterface

指定是否提示 特权用户密码管理 代理输入目标用户密码。

限制：0（未安装 特权用户密码管理 代理）、1（已安装 特权用户密码管理 代理）。

默认值：1

InterfaceName

定义 特权用户密码管理 代理用来处理请求的接口名称。

默认值： PUPMAgentInterface

OperationMode

指定 特权用户密码管理 代理工作模式。

限制： 0，特权用户密码管理 代理处于禁用状态，不运行；1，特权用户密码管理 代理处于启用状态，运行但不将数据记录到跟踪文件中；2，特权用户密码管理 代理处于启用状态，运行并将数据记录到跟踪文件中。

默认值： 0

ProcessArgumentsReplacement

指定 特权用户密码管理 代理是否支持进程参数替换。

限制： 0、1

默认值： 0

注意： 如果选择支持进程参数替换，即，将该注册表项的值设置为 1，您还必须启用 CMD 插件。 要启用 CMD 插件，请将以下注册表项设置为 1：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\plugins\CMDPlg\OperationMode

Report

CA Access Control 在以下注册表键下保留其使用的 sereport 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Reports

Reports 注册表键不包含任何注册表项。 它包含 sereport 生成的每个报告的注册表子键。

注意： 有关 sereport 生成的每个报告的注册表项的信息，请参阅 sereport 实用程序 (p. 199)。

colors

CA Access Control 在以下注册表键下保留其使用的 sereport 样式设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Reports\colors

Reports\colors 注册表键包含以下注册表项：

background

仅限内部使用。

该键应保留不变。

class_title

定义报告的 class_title 的颜色。

默认值：绿色

logo

定义徽标文件的完整路径名。

默认值：*ACInstallDir*\data\logo.jpg

title

定义报告标题的颜色。

默认值：深蓝

ReportAgent 键—注册表设置

CA Access Control 在以下注册表键下保留其使用的报告代理设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\ReportAgent

ReportAgent 注册表键包含以下注册表项：

audit_enabled

指定是否要将端点审核数据发送到分发服务器。

值：0—否；**1**—是

默认值：0

audit_filter

定义包含筛选规则的文件的完整路径名，这些规则用于报告代理传递到外部来源（例如：CA Enterprise Log Manager）的审核记录。 此文件将确定报告代理传递哪些记录。

默认值：*ACInstallDir*\Data\AuditRouteFlt.cfg

audit_queue

定义报告代理向其发送端点审核数据的队列的名称。

默认：queue/audit

audit_read_chunk

定义报告代理尝试在每次读取审核文件时收集的最大审核记录数量。

限制：正整数。

默认值：300

audit_send_chunk

定义报告代理在每次连接中向分发服务器发送的最大审核记录数。当报告代理收集的审核记录数达到此值时，它会将这些记录发送到分发服务器。

限制：正整数

默认值：1800

audit_sleep

定义报告代理在生成审核报告间隔的睡眠持续时间。

限制：正整数代表数秒。

默认值：10

audit_timeout

定义报告代理必须将端点审核数据发送到分发服务器的周期。 如果自上次发送起经过的时间达到此数值，即使报告代理收集的记录数量少于 audit_send_chunk 值，仍会将审核数据发送到分发服务器。

限制：正整数代表数秒。

默认值：300

interval

定义 CA Access Control 生成报告并将报告发送到分发服务器的时间间隔（分钟）。

*排定*设置用于定义时间间隔开始的时间以及它运行的天数。 如果报告代理启动时间晚于排定时间，它将在下个计算的时间间隔（从排定起）发送一个报告，然后在排定天数后的定义时间间隔发送一个报告。

示例：如果 schedule = 8:30@Mon,Tue,Wed，interval = 5，则报告代理将在星期二上午 8:47 加载，报告代理将在上午 8:50 生成并发送报告。这是使用 5 分钟时间间隔从排定开始时间计算出的最早周期。

值：**0**—无时间间隔（仅使用排定发生时间）；*正整数*—用作时间间隔的分钟数

默认值：0

reportagent_enabled

指定是否在本地计算机上启用报告 (1)。

默认值：0

schedule

定义生成报告并将其发送到分发服务器的时间。

您可以使用以下格式指定设置：time@day[,day2][...]

例如：“19:22@Sun,Mon”可在每个星期日和星期一晚上 7:22 生成报告。

默认值：00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

send_queue

定义分发服务器上报告队列的名称，报告代理向该队列发送本地数据库和任何 PMDB 的快照。

默认值：queue/snapshots

更多信息：

auditrouteflt.cfg 文件—筛选审核记录传递 (p. 383)

SeOSD 键—注册表设置

CA Access Control 在以下键下维护其使用的常规设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSD
```

SeOSD 注册表键包含以下注册表项：

AuditCollectorInterfaceName

定义管道名，此管道名充当审核收集器组件（在 seosd 之内）和审核收集器（内核）的不同的客户端之间的审核接口。

默认值：AuditCollector

AuditServerCacheSize

定义审核缓存的大小，以条目数计。

默认值：1024

CreateNewClasses

指定是否可以将使用 seclassadm 实用程序创建的新类添加到 CA Access Control 数据库中。

默认值：yes

CreateNewProps

确定是否可以将使用 sepropadm 实用程序创建的新属性添加到 CA Access Control 数据库中。

默认值：yes

dbdir

CA Access Control 数据库所在的目录。

默认值：*ACInstallDir*\data\seosdb

DefLookupThreads

定义 CA Access Control 可用于将 SID 解析为帐户名称的线程数目。

默认值：5

DefLookupTimeout

定义在 CA Access Control 停止尝试将 SID 解析为帐户名称之前的超时时间（以毫秒为单位）。

默认值：2000

domain_names

用于匹配的名称后缀列表。

CA Access Control 将这些后缀附加在短的主机名中，以便创建长的、完全限定的主机名。 可以在相关的 HOST、CONNECT 或 TERMINAL 类中授权这些名称。为了识别全名，出于授权目的，CA Access Control 会试图将 domain_names 列表中的域名附加到短名中。对于类 HOSTNP，CA Access Control 将所有域名（在该注册表中列出）与模式匹配，以便解析为真正 IP 地址。

无默认值。

EnablePolicyCache

该值可控制授权引擎是使用缓存的记录还是直接使用数据库中的记录。

有效值：

no－授权引擎将使用数据库记录。

yes－授权引擎将使用缓存记录。

默认值：no

EnvVarResolvingMode

解析嵌入式环境变量的方式（对于 FILE、SECFILE、PROGRAM、PROCESS、SPECIALPGM、TERMINAL 或 USER 类中的对象）。 例如：

newfile %SystemRoot%\temp.txt。

如果选择 0，CA Access Control 试图解析所有环境变量，给用户发出错误消息，且不创建对象。

如果选择 1，CA Access Control 试图解析所有环境变量，给用户发出警告消息，且创建对象。

如果选择 2，CA Access Control 试图解析所有环境变量，创建对象，但不发出任何消息。

如果选择 3，CA Access Control 不尝试解析环境变量。

注意： PMDB 假定没有环境变量，因此从未尝试解析。

默认值： 2

GeneralInterceptionMode

指定是否使用完整强制模式 (0) 或仅审核模式 (1)。

默认值： 0

GraceCountForMessage

定义剩余的宽限登录（显示“更改密码”对话框）的次数。

默认值： 0

HostResolutionMode

指定 CA Access Control 用于解析主机名的方式。

值：

0－HOST 解析同步（当前行为）。

1－HOST 解析异步（带有“事件日志”报告）

该设置的结果为：

- 控制立即返回到 selang。
- 如果不能解析 HOST 记录，将不会显示 selang 消息（与 0 相同）。
- 通知消息被写入“事件日志”。

2－HOST 解析异步（不带有“事件日志”报告）。

同“1”，只是不会将通知消息写入任何地方。

默认值： 0

HostResolutionRenewal

刷新内部缓存的时间。 网络截获授权事件使用注册表值。

默认值：30000

HostResolutionTimeout

网络截获事件时，授权引擎等待反向 IP 查找请求的时间。

默认值：2000

LogonTimeOut

定义 CA Access Control 在放弃之前等待使用子身份验证 DLL (eACSubAuth.dll) 进行的事务的时间(毫秒)。此时间通过时，CA Access Control 使用 LogonTimeOutAnswer 中的值集回复。

默认值：4000

LogonTimeOutAnswer

LogonTimeOut 设置过去时（没有 CA Access Control 的回答），定义对操作系统的登录答案。

默认值：1 (true)

MaximumDiscreteFILELimit

可在 CA Access Control 数据库中创建的个别 FILE 记录数。

最小值是默认值；如果用户将该值设置为小于默认值，那么 CA Access Control 则表现为如同设置最小值一样。

默认值：4096

MaximumGenericFILELimit

可在 CA Access Control 数据库中创建的通用 FILE 记录（基于名称模式的记录）数。

最小值是默认值；如果用户将该值设置为小于默认值，那么 CA Access Control 则表现为如同设置最小值一样。

默认值：512

ProcessCreationNotificationMode

指定是否拦截进程创建并使用内核或检测仪表模式通知 seosd。

类型：REG_DWORD

值：

0－使用内核模块执行进程创建

1－使用检测仪表模块执行进程创建

默认值：0

注意：如果将密钥设置为 1，CA Access Control 则仅通过 Windows API 拦截进程创建。

RebuildSuspiciousDatabase

只有当数据库没在前一会话中正常关闭时，才考虑该值。

如果该值设置为 0，将通过启发式程序检查数据库的正确性（在启动过程中）。 如果检查发现数据库中存在问题，则重新建立数据库。

如果该值设置为 1，将忽略启发式程序检查函数。根据数据库完整性检查重新建立数据库。

默认值：1

RefreshIPInterval

连续自动 IP 刷新请求之间的时间（分钟）。

如果该值设置为 0，将不会自动执行 IP 刷新。 如果使用 1 到 30 之间的值，则 CA Access Control 将 30 分钟用作值，这是您可以设置的最短时间数。

注意：刷新请求消耗时间。 有关详细信息，请参阅 secons 实用程序 -refIP 选项。

默认值：0

ResponseFile

eACOexist.exe 实用程序所使用的 response.ini 所在的位置。

默认值：*ACInstallDir*\data\response.ini

sim_login_timeout

定义在 CA Access Control 从 Accessor Element Entry 表 (ACEE) 中删除未用过的模拟登录用户条目之前的超时时间（以分钟为单位）。

需要访问可在 ACEE 中找到的信息时，CA Access Control 执行模拟登录来创建 ACEE 条目。

默认值：60

SurrogateInterceptionMode

指定 SURROGATE 类拦截模式。

类型：REG_DWORD

限制：0－用户模式拦截，CA Access Control 仅拦截源自 RunAs 实用程序的模拟请求；1－内核模式拦截，CA Access Control 拦截所有模拟请求。

默认值：0

SusrauthReadParamsSec

定义更新跟踪参数的频率。

默认值：30

SusrauthTraceDbgEnable

指定是否跟踪到 DbgView 或是否启用内核调试程序 (1)。

默认值：0

SusrauthTraceFileEnable

指定是否跟踪到启用的跟踪文件 (SusrauthTraceFileName) (1)。

默认值：0

SusrauthTraceFileName

定义跟踪文件的完整路径名。

无默认值

TerminalSearchOrder

指定授权引擎如何确定在授权过程中应检查哪个 TERMINAL 记录。

值：

name－授权引擎首先按名称查找 TERMINAL 记录，如果未找到，则查找 IP 地址匹配。

nameonly－授权引擎按名称查找 TERMINAL 记录，如果未找到，则停止搜索。 使用 IP 地址格式忽略 TERMINAL 记录。

IP－授权引擎首先按 IP 地址查找 TERMINAL 记录，如果未找到，则查找名称匹配。

注意：TERMINAL 类支持由通配符定义的通用规则（IP 地址或主机名模式匹配）。 始终先检查特定（全名）规则，然后再检查一般规则。例如：如果将此设置为 IP，seosd 将按照以下顺序查找 TERMINAL 资源：完整 IP 地址匹配、完整主机名匹配、IP 地址模式匹配、主机名模式匹配。

默认值：nameonly

TermSrvTimeout

指定进行终端服务连接时授权引擎等待第二次连续登录的超时值（毫秒）。

默认值：2000

注意：在用户使用本地帐户登录时，CA Access Control 会接收两个登录尝试通知：第一个来自本地终端，第二个来自终端服务器。 如果将用户分配了宽限登录计数，那么将记录两个登录尝试，并减少宽限登录计数。 因此，如果登录尝试在指定的超时时期内发生，CA Access Control 则不会使用第二个登录来更新宽限登录计数。

trace_file

将跟踪消息发送到的文件名称（如果已请求跟踪消息）。

默认值：*ACInstallDir*\log\seosd.trace

trace_file_type

跟踪文件的类型。

如果您更改该值的值且已存在跟踪文件，那么将使用文件扩展名 .backup 保存当前跟踪文件，然后使用您指定的格式启动新的跟踪文件。

默认值：text

trace_filter

包含用于筛选跟踪消息的筛选数据的文件名。 指定文件的完整路径。

默认值：*ACInstallDir*\log\trcfilter.ini

trace_space_saver

要在文件系统中保留的可用空间量 (KB)。 可用空间量少于该数目时，CA Access Control 禁用跟踪。

注意：即使更大的空间在稍后时间可用，也不会自动启用跟踪。

默认值：5120

trace_to

跟踪消息的目标。 设置为 none、file 或 file,stop。

如果选择 none，CA Access Control 则不会生成跟踪消息。

如果选择 file，一旦 CA Access Control 成为活动状态，CA Access Control 则会生成跟踪消息，并将他们发送到注册表 trace_file 中所列的文件。

如果选择 file,stop，CA Access Control 会在服务初始化期间生成跟踪消息。 服务初始化完成后，不会生成其他跟踪消息。

默认值：file,stop

SeOSWD

CA Access Control 在以下注册表键下保留其使用的 Watchdog 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\SeOSWD

SeOSWD 注册表键包含以下注册表项：

PgmRest

指定从最后一个事件完成到准备再次检查程序之间的时间段（秒）。该程序进行休息是为了防止系统过载。

默认值：10

PgmTestInterval

重新扫描程序之间间隔的时间段（秒）。

默认值：18000

SecFileRest

指定从最后一个事件完成到准备再次检查安全文件之间的时间段（秒）。 该程序进行休息是为了防止系统过载。

默认值：10

SecFileTestInterval

重新扫描受保护文件之间间隔的时间段（秒）。

默认值：36000

STOP

CA Access Control 在以下注册表键下保留其使用的堆栈溢出保护 (STOP) 设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\STOP

STOP 注册表键包含以下注册表项：

STOPIniFileName

定义 STOP 初始化文件的完整路径和名称。 此文件包含启用了 STOP 的函数列表。

默认值：*ACInstallDir*\Data\stop.ini

STOPLearningModeEnabled

指定 STOP 是否在特定的学习模式中运行。在该模式中，事件会被记录，但始终被允许。 即，拒绝的时间被相应记录，但被允许继续。

默认值：0（禁用）

STOPLogFileName

定义堆栈溢出保护 (STOP) 的动态事件数据库的完整路径和名称。

默认值：*ACInstallDir*\Log\STOPRTEvents.dat

STOPServerTraceEnabled

指定 STOP 服务器模块是否已启用跟踪记录。

默认值：0（禁用）

STOPSignatureBrokerName

定义用于从中检索 STOP 签名数据库的计算机（如果已定义）的主机名。

无默认值。

STOPSignatureFileName

定义 STOP 签名文件（受托事件数据库）的完整路径和名称。

默认值：*ACInstallDir*\Data\stopsignature.dat

STOPUpdateInterval

定义两次连续尝试更新 STOP 签名数据库之间的时间间隔（分钟）。

默认值：60

STOPZeroSnapshotBypassEnabled

指定 STOP 是否应使用大小为零的代码快照允许事件。

默认值：0（不允许）

Tracer

CA Access Control 在以下注册表键下保留其使用的跟踪模块设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Tracer
```

Tracer 注册表键包含以下注册表项：

TraceCfgFile

定义包含用于跟踪 CA Access Control 模块的初始化配置设置的文件的完整路径。

默认值：*ACInstallDir*\Data\tracer.ini

TraceEnabled

指定是否启用跟踪机制。

默认值：0（禁用）

UCTNG

CA Access Control 在以下注册表键下保留其使用的 Unicenter 集成设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\UCTNG

UCTNG 注册表键包含以下注册表项：

EvtManagerServer

定义 Unicenter TNG 主机的名称。

Integration

指定是否启用与 Unicenter TNG 的集成并发送审核数据。

默认值：0（不启用集成）

uxauth 键－注册表设置

UNIX 身份验证代理 在以下注册表键下保留其使用的 Active Directory 架构设置：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth

当您在 Active Directory 服务器上安装 CA Access Control UNIX 属性插件时，UNIX 身份验证代理 会安装该注册表键。 该注册表键不会作为 CA Access Control 的一部分安装。

注意：默认属性适用于 Active Directory 2003 R2 架构。

uxauth 注册表键包含以下注册表项：

group_gid_attr_name

指定 UNIX 身份验证代理 将所迁移 UNIX 组的 GID 映射到的 Active Directory 属性。

默认值：gidNumber

Trace_Enabled

指定是否对 CA Access Control UNIX 属性插件启用跟踪。

值：0－禁用跟踪，1－启用跟踪

默认值：0

user_gecos_attr_name

指定 UNIX 身份验证代理 将所迁移 UNIX 用户的 gecos 属性映射到的 Active Directory 属性。

默认值：gecos

user_gid_attr_name

指定 UNIX 身份验证代理 将所迁移 UNIX 用户的 GID 映射到的 Active Directory 属性。

默认值：gidNumber

user_homedir_attr_name

指定 UNIX 身份验证代理 将所迁移 UNIX 用户的主目录属性映射到的 Active Directory 属性。

默认值：unixHomeDirectory

user_loginshell_attr_name

指定 UNIX 身份验证代理 将所迁移 UNIX 用户的登录 shell 属性映射到的 Active Directory 属性。

默认值：loginShell

user_uid_attr_name

指定 UNIX 身份验证代理 将所迁移 UNIX 用户的 UID 映射到的 Active Directory 属性。

默认值：uidNumber

WebService

CA Access Control 在以下注册表键下保留其使用的 Web 服务设置：

`HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\WebService`

注意：WebService 注册表键和相关项可作为 CA Access Control 端点管理安装的一部分添加。

WebService 注册表键包含以下注册表项：

auditFileCheckInterval

定义 CA Access Control Web 服务检查审核文件大小是否已达到定义的限制的频率（秒）。

默认值：60

auditFileMaxSize

定义 CA Access Control Web 服务审核日志文件的最大大小（KB）。

当文件达到此大小时，Web 服务会将该文件重命名为 *“Backup_of_logFileName”*，然后创建一个新审核日志文件。

默认值：20000

backLog

定义 CA Access Control Web 服务所维护的请求队列的最大大小。

默认值：101

LogFileName

定义 CA Access Control Web 服务审核日志文件的名称。

如果保留该值为空字符串 ("")，则运行带有 -debug 选项的 Web 服务时，Web 服务会将日志消息发送至终端。

默认值：*ACServerInstallDir*\WebService\log\WebService.log

machineName

定义安装了 CA Access Control Web 服务的计算机的名称。

默认值：127.0.0.1

maxRequestsQueue

定义套接字的全局请求队列的大小。

默认值：1001

maxThreads

定义 CA Access Control Web 服务使用的线程数。

默认值：7

portNumber

定义 CA Access Control Web 服务用于通讯的端口。

默认值：5248

sessionTimeOut

定义 CA Access Control Web 服务终止会话之前的无操作时间（秒）。

默认值：601

StandAloneService

指定 CA Access Control Web 服务是否作为独立的服务操作。

如果 CA Access Control Web 服务作为独立的服务操作，则在您使用 secons 来停止 CA Access Control 服务或使用 seosd 来启动服务时，该服务不会也随之被停止或启动。 可使用 Windows 本地工具来启动和停止 CA Access Control Web 服务。

如果 CA Access Control Web 服务不作为独立的服务运行，则在您使用 secons 来停止 CA Access Control 服务或使用 seosd 来启动 ®CA Access Control 服务时，该服务也会停止和启动。 不能使用 Windows 本地工具来启动和停止 CA Access Control Web 服务。 但是，要使用 seosd -start 来启动 CA Access Control Web 服务，您必须在 AccessControl\AccessControlServices 注册表项中定义 CA Access Control Web 服务。

值：1－作为独立服务运行；0－不作为独立的服务运行

默认值：1

TraceEnabled

指定是否对 CA Access Control Web 服务组件启用跟踪。

值：0－禁用跟踪，1－启用跟踪

默认值：0

其他注册表项

您还可以添加或修改以下键和值，以更改 CA Access Control 的执行方式：

注册表项	类型	说明
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableFileInterception	REG_DWORD	指定文件截获挂钩是否被禁用（引导时相关函数不进行初始化）。 **值：**1（禁用） **注意：**如果此注册表项不存在（默认值），或者将其设置为 1 以外的任意值，那么文件截获会在引导时进行初始化。

注册表项	类型	说明
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableNetworkInterception	REG_DWORD	指定网络截获挂钩是否被禁用（引导时相关函数不进行初始化）。 **值：**1（禁用） **注意：**如果该注册表项不存在（默认值），或设置为 1 以外的任意值，那么网络截获会在引导时进行初始化。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableProcessInterception	REG_DWORD	指定进程截获挂钩是否被禁用（引导时相关函数不进行初始化）。 **值：**1（禁用） **注意：**如果此注册表项不存在（默认值），或者将其设置为 1 以外的任意值，那么进程截获会在引导时进行初始化。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\drveng\Parameters\DisableRegistryInterception	REG_DWORD	指定注册表截获挂钩是否被禁用（引导时相关函数不进行初始化）。 **值：**1（禁用） **注意：**如果此注册表项不存在（默认值），或者将其设置为 1 以外的任意值，那么注册表截获会在引导时进行初始化。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SeosDrv\Parameters\KernelBuffersSize	REG_DWORD	默认情况下，当 CA Access Control 内核驱动程序 (seosdrv.sys) 启动时，该驱动程序根据以下公式分配内存以供内部使用： number_of_buffers = amount_of_RAM 例如：为 256 MB RAM 分配 256 个缓冲区。 每个缓冲区的长度为 4096 字节。 如果希望控制 seos.drv 分配的缓冲区数量，请创建该注册表键，并将其值设置为要分配的缓冲区数量。 **注意：**缓冲区的最小数量为 32。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\SeosDrv\EventMessageFile	REG_EXPAND_SZ	定义 seosdrv.sys 驱动程序的路径名。 **默认** **值：**%SystemRoot%\System32\drivers\seosdrv.sys
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\SeosDrv\TypesSupported	REG_DWORD	定义所支持的事件类型的位掩码的标准 Windows 项。 **默认值：**7

注册表项	类型	说明
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cainstrm\parameters\DllScanList	REG_SZ	定义以逗号分隔的 DLL 列表（按名称），这些 DLL 将触发 cainstrm.sys 插入 **默认值：**无默认值
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\cainstrm\parameters\DllScanListRefreshPeriod	REG_DWORD	定义扫描 cainstrm 注册表项的间隔（秒）。 **默认值：**600
HKEY_LOCAL_MACHINE\System\CCS\Services\Cainstrm\parameters\ExcludeProcess	REG_MULTI_SZ	按名称指定驱动程序要从本地 instrumentation 排除的进程。 **默认值：**none

附录 A： 审核日志记录

此部分包含以下主题：

审核记录

审核日志中的每个记录都包含排列在列中的数据。 两列（日期和时间戳）是所有记录类型共有的。 其余列以及这些列中包含的数据取决于触发创建审核记录的事件类型。

注意：显示的审核日志记录的列的顺序、编号和内容取决于您选择的查看审核日志的方法。 某些字段不会在 CA Access Control 端点管理、seaudit 输出或详细的 seaudit 输出中显示。 同样，如果您使用 seaudit 实用程序，您所指定的选项也可能会决定列的编号、顺序和内容。

如何识别审核记录的事件类型

要了解审核记录的内容，您必须先识别该审核记录的事件类型。 这是因为记录所包含的数据取决于触发审核记录创建的事件类型。

注意：显示的审核日志记录的列的顺序、编号和内容取决于您选择的查看审核日志的方法。 某些字段不会在 CA Access Control 端点管理、seaudit 输出或详细的 seaudit 输出中显示。 同样，如果您使用 seaudit 实用程序，您所指定的选项也可能会决定列的编号、顺序和内容。

识别审核记录的事件类型：

- 如果您是在 CA Access Control 端点管理 中查看审核记录，审核记录所属的事件类型会在“审核记录结果”窗格的第一列中显示。

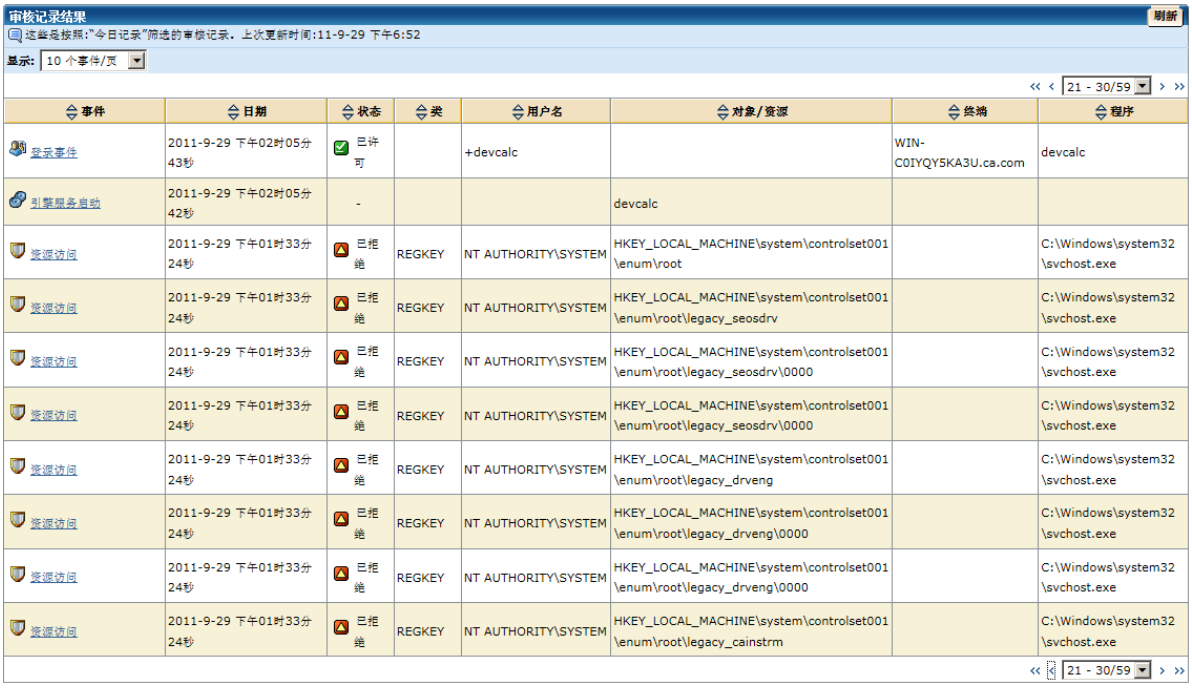
  要显示关于审核记录的详细信息，请单击第一列中的链接审核事件类型。

- 如果您是在 seaudit 输出中查看审核记录，需要显示详细输出（-detail 选项）以查看事件类型。

识别事件类型之后，您便可继续解读剩余的消息详细信息。

示例：CA Access Control 端点管理 中的审核记录

下图向您展示了 CA Access Control 端点管理 显示审核事件的方式：



审核记录结果 刷新

这些是按照:"今日记录"筛选的审核记录. 上次更新时间:11-9-29 下午6:52

显示: 10 个事件/页 << < 21 - 30/59 > >>

事件	日期	状态	类	用户名	对象/资源	终端	程序
登录事件	2011-9-29 下午02时05分43秒	已许可		+devcalc		WIN-C0IYQY5KA3U.ca.com	devcalc
引擎服务启动	2011-9-29 下午02时05分42秒	-			devcalc		
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_seosdrv		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_seosdrv\0000		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_seosdrv\0000		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_drveng		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_drveng\0000		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_drveng\0000		C:\Windows\system32\svchost.exe
资源访问	2011-9-29 下午01时33分24秒	已拒绝	REGKEY	NT AUTHORITY\SYSTEM	HKEY_LOCAL_MACHINE\system\controlset001\enum\root\legacy_cainstrm		C:\Windows\system32\svchost.exe

<< < 21 - 30/59 > >>

示例：默认 seaudit 输出中的审核记录

以下 seaudit 输出片段向您展示了默认情况下 seaudit 实用程序显示审核事件的方式：

```
19 Dec 2008 16:46:47 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:46:52 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:46:53 P LOGIN       TM123VM-AC\Administrator   55  2 TM123VM-AC
C:\WINDOWS\system32\lsass.exe
19 Dec 2008 16:46:57 P WINSERVICE  TM123VM-AC\Administrator Read   1059  2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
```

```
19 Dec 2008 16:47:02 P WINSERVICE  TM123VM-AC\Administrator Read   1059 2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:07 P WINSERVICE  TM123VM-AC\Administrator Read   1059 2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:12 P WINSERVICE  TM123VM-AC\Administrator Read   1059 2 VMTools
C:\WINDOWS\system32\services.exe TM123VM-AC
19 Dec 2008 16:47:16 S UPDATE      GROUP     TM123VM-AC\Administrator  336  0
test       TM123VM-AC egtest audit-
19 Dec 2008 18:28:18 P LOGIN       TM123VM-AC\Administrator   55 10 TM123VM-AC
selang
19 Dec 2008 18:28:18 S UPDATE      TERMINAL   TM123VM-AC\Administrator  305  0
TM123VM-AC-SC1.ca.com TM123VM-AC er terminal TM123VM-AC-SC1.ca.com
```

以上第一个消息的详细 seaudit 输出如下所示：

```
19 Dec 2008 16:46:47 P WINSERVICE  TM123VM-AC\Administrator Read   1059 2 VMTools
C:\WINDOWS\system32\services.exe TW852VM-AC
事件类型：资源访问
状态：已允许
类：WINSERVICE
资源：VMTools
访问：读取
用户名：TM123VM-AC\Administrator
用户登录会话 ID：00000000:05647d29
终端：TM123VM-AC
程序：C:\WINDOWS\system32\services.exe
日期：19 Dec 2008
时间：16:46
详细信息：默认记录通用访问权限检查
审核标志：AC 数据库用户
```

审核事件类型

CA Access Control 在审核日志中存储的信息是由其审核的事件类型决定的。

CA Access Crontrol 将记录以下事件类型的审核记录：

登录事件

登录事件对登录 CA Access Control 或 CA Access Control 保护的主机的尝试进行了说明。

此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 会话 ID 详细信息 原因 终端 程序审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值：可以为以下值之一：

- D（已拒绝）- 由于授权不足而拒绝事件。
- P（已允许）- 允许事件。
- W（警告）- 允许事件，原因是虽然访问请求违反了访问规则，但是设置了警告模式。

事件类型

指明此记录所属的事件类型。

注意：CA Access Control 端点管理 只是简单地将此字段作为 *事件*进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

用户登录会话 ID

指明访问者的会话 ID。

注意：默认情况下，在非详细 seaudit 输出中不显示此字段。 要在非详细 seaudit 输出中显示此字段，请在 seaudit 命令中指定 -sessionid 选项。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

终端

指明访问者用于连接到主机的终端的名称。

程序

指明触发事件的程序的名称。 即访问者用于尝试登录的程序。 对于 CA Access Control 管理登录，此为已登录的 CA Access Control 模块（selang、Web 服务等）。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：登录事件消息

以下审核记录取自详细的 seaudit 输出。

```
28 Oct 2008 12:15:01 P LOGIN  root  49047159:0000034b  59  2  _CRONJOB_  SBIN_CRON
事件类型：登录事件
状态：已允许
用户名：root
终端：_CRONJOB_
程序：SBIN_CRON
日期：2008 年 10 月 28 日
时间：12:15
详细信息：资源 UACC 检查
用户登录会话 ID：49047159:0000034b
审核标志：AC 数据库用户
```

该审核记录表明 2008 年 10 月 28 日 12:15:01 用户 root 从终端 _CRONJOB_ 登录到受保护的主机并运行了 SBIN_CRON 程序。 CA Access Control 允许该操作，原因是资源的默认访问权限允许此操作（授权阶段代码 59－资源 UACC 检查）。 CA Access Control 已记录此事件，原因是访问者的审核模式指定应记录此事件（原因代码 2－用户审核模式要求记录）。

更多信息：

适用于登录和注销事件的授权阶段代码 (p. 561)
指定记录创建原因的原因代码 (p. 593)

注销事件

在 UNIX 上有效

注销事件说明了尝试从 CA Access Control 或受 CA Access Control 保护的主机进行注销。

注意：注销事件仅在 UNIX 上受支持。 CA Access Control 实际上不截获注销。 相反，它假设在会话的最后一个进程终止时发生注销事件。

此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 会话 ID 详细信息 原因 终端 审核标志

日期

指明事件发生的日期。

格式：DD MMM YYYY

注意：CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式：HH:MM:SS

注意：CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明发生用户注销事件。

值：O（注销）

事件类型

指明此记录所属的事件类型。

注意：CA Access Control 端点管理 只是简单地将此字段作为*事件*进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

用户登录会话 ID

指明访问者的会话 ID。

注意：默认情况下，在非详细 seaudit 输出中不显示此字段。 要在非详细 seaudit 输出中显示此字段，请在 seaudit 命令中指定 -sessionid 选项。

详细信息

表明检测注销的方式。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

终端

指明访问者用于连接到主机的终端的名称。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：注销事件消息

以下审核记录取自详细的 seaudit 输出。

```
29 Jan 2009 17:23:33 0 LOGOUT       root                  49  2 computer.com
事件类型：注销
状态：注销
用户名：root
终端：computer.com
日期：2009 年 1 月 29 日
时间：17:23
详细信息：最后一个进程终止后检测到注销。
审核标志：AC 数据库用户
```

此审核日志表明，2009 年 1 月 29 日，CA Access Control 检测到在远程终端 computer.com 上工作的用户 root 的最后一个会话进程已关闭，因此假设该用户已注销系统（授权阶段代码 49－最后一个进程终止后检测注销）。

更多信息：

适用于登录和注销事件的授权阶段代码 (p. 561)
指定记录创建原因的原因代码 (p. 593)

已启用登录帐户事件

在 UNIX 上有效

已启用登录帐户事件说明了 serevu 启用用户登录事件的地点。

此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 详细信息 原因 终端 程序 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明 serevu 已启用用户登录。

值： E（已启用登录）

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为*事件*进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

终端

指明访问者用于连接到主机的终端的名称。

程序

指明触发事件的程序的名称。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：已启用登录帐户事件消息

以下审核记录取自详细的 seaudit 输出。

```
13 Jan 2009 17:05:00 E LOGINENABLE  test1           0  5 computer.com      serevu
事件类型：已启用登录帐户
状态：已启用登录
用户名：test1
详细信息：阶段代码 0
终端：computer.com
日期：2009 年 1 月 13 日
时间：17:05
程序：serevu
审核标志：已禁用 AC 数据库用户登录帐户  -
```

此审核记录表明，2009 年 1 月 13 日，serevu 后台进程使用户 test1 可以从终端 computer.com 登录。 CA Access Control 记录了此事件，原因是 serevu 后台进程请求了审核（原因代码 5－CA Access Control serevu 实用程序请求了审核）。

更多信息：

适用于登录和注销事件的授权阶段代码 (p. 561)
指定记录创建原因的原因代码 (p. 593)

已禁用登录帐户事件

在 UNIX 上有效

已禁用登录帐户事件说明了 serevu 禁用用户登录事件的地点。

此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 详细信息 原因 终端 程序 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明 serevu 已禁用用户登录。

值： I（已禁用登录）

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为 *事件*进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

用户登录会话 ID

指明访问者的会话 ID。

注意：默认情况下，在非详细 seaudit 输出中不显示此字段。 要在非详细 seaudit 输出中显示此字段，请在 seaudit 命令中指定 -sessionid 选项。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

终端

指明访问者用于连接到主机的终端的名称。

程序

指明触发事件的程序的名称。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：已禁用登录帐户事件消息

以下审核记录取自详细的 seaudit 输出。

```
13 Jan 2009 16:53:26 I LOGINDISABLE test1                    0  5
computer.com      serevu
事件类型：禁用登录帐户
状态：已禁用登录
用户名：test1
```

终端：computer.com
日期：2009 年 1 月 13 日
时间：16:53
程序：serevu
详细信息：阶段代码 0
用户登录会话 ID：496b629c:00000003
审核标志：AC 数据库用户

此审核记录表明，2009 年 1 月 13 日，serevu 后台进程阻止用户 test1 从终端 computer.com 进行登录。 CA Access Control 记录了此事件，原因是 serevu 后台进程请求了审核（原因代码 5—CA Access Control serevu 实用程序请求了审核）。

更多信息：

适用于登录和注销事件的授权阶段代码 (p. 561)
指定记录创建原因的原因代码 (p. 593)

密码尝试事件

在 UNIX 上有效

密码尝试事件说明了访问者尝试使用错误的密码进行登录。

此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 详细信息 原因 终端 程序 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明错误的密码尝试。

值： A（密码尝试）

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为 *事件* 进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意： 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意： 详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

终端

指明访问者用于连接到主机的终端的名称。

程序

指明触发事件的程序的名称。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意： 如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：密码尝试事件消息

以下审核记录取自详细的 seaudit 输出。

```
13 Jan 2009 16:21:12 A LOGIN        admin                 17  8
localhost.localdomain login
事件类型：密码尝试
状态：密码尝试
用户名：admin
终端：localhost.localdomain
```

日期：2009 年 1 月 13 日
时间：16:21
程序：login
详细信息：本地环境拒绝的尝试
审核标志：AC 数据库用户

此审核记录表明，2009 年 1 月 13 日，用户 admin 尝试更改其帐户密码。 由于登录失败，该尝试被本地环境拒绝（授权阶段代码 17－本地环境拒绝的尝试）。 pam _seos 模块记录了此事件（原因代码 8－CA Access Control pam 支持 UNIX 失败登录）。

更多信息：

适用于登录和注销事件的授权阶段代码 (p. 561)
指定记录创建原因的原因代码 (p. 593)

资源访问事件

资源访问事件说明了尝试访问资源，例如：FILE、TERMINAL、PROGRAM 及更多资源。 此事件中的审核记录数据可以显示在其他记录中，例如：访问者尝试访问 TERMINAL 资源时，可以显示在 LOGIN 事件。 虽然此示例中的事件记录属于 LOGIN 类型，但是记录中显示的审核记录数据是其中一个资源访问事件消息。

此事件中的审核记录格式如下：

日期 时间 状态 类 用户名 会话 ID 访问 详细信息 原因 资源 程序 终端 有效用户名 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值：可以为以下值之一：

- D（已拒绝）- 由于授权不足而拒绝事件。
- P（已允许）- 允许事件。
- W（警告）- 允许事件，原因是虽然访问请求违反了访问规则，但是设置了警告模式。

类

指明被访问的资源所属的类。

用户名

指明执行触发此事件的操作的访问者名称。

用户登录会话 ID

指明访问者的会话 ID。

注意：默认情况下，在非详细 seaudit 输出中不显示此字段。 要在非详细 seaudit 输出中显示此字段，请在 seaudit 命令中指定 -sessionid 选项。

访问

指明触发此事件的尝试访问的类型。

示例：读取

注意：访问值取决于截获资源所属的类。 有关每个类的访问授权的详细信息，请参阅 *《selang 参考指南》*。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

资源

指明正在被访问或更新的实际资源的名称。

程序

指明触发事件的程序的名称。即，访问者用于尝试访问资源的程序。

终端

指明访问者用于连接到主机的终端的名称。（仅 UNIX。）

有效的用户名

（仅 UNIX）识别触发该事件的本机操作系统有效用户的名称。如果用户替换（替代）为不同的用户或运行 setuid 程序，则不同于用户名。

注意：在 KBL 审核输出中不显示此字段。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。否则，此字段保留为空。

示例：资源访问事件消息

以下审核记录取自详细的 seaudit 输出。

```
18 Nov 2008 15:23:56 D FILE         admabc  4922ae61:00000132 Read       69  3
/tmp/one             /usr/local/bin/tcsh  localhost      admabc
事件类型：资源访问
状态：已拒绝
类：FILE
资源：/tmp/one
访问：读取
用户名：admabc
终端：localhost
程序：/usr/local/bin/tcsh
日期：2008 年 11 月 18 日
时间：15:23
详细信息：没有允许访问的步骤
用户登录会话 ID：4922ae61:00000132
审核标志：AC 数据库用户
有效用户名：admabc
```

此审核记录表明，2008 年 11 月 18 日 15:23:56，用户 admabc 使用本地计算机中的 UNIX tcsh shell 程序尝试读取受保护的 /tmp/one 文件资源。CA Access Control 拒绝用户执行该操作，原因是数据库中没有授权此类访问的规则（授权阶段代码 69－没有允许访问的步骤）。 CA Access Control 已记录此事件，原因是资源的审核模式指定应记录此事件（原因代码 3－资源审核模式要求记录）。

更多信息：

适用于资源访问事件的授权阶段代码 (p. 564)
指定记录创建原因的原因代码 (p. 593)

取消托管消息事件

取消托管事件说明了 CA Access Control Watchdog 为事件生成的警告消息。

此事件中的审核记录格式如下：

日期 事件 状态 类 模块 详细信息 消息 ID/errno 文件

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明发生取消托管事件。

值： U（取消托管）

类

指明触发 Watchdog 消息的资源所属的 CA Access Control 类。

值： PROGRAM 或 SECFILE

模块名

显示 CA Access Control Watchdog 的名称。

值：seoswd

详细信息

表明发生取消托管事件的原因。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为取消托管原因代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与取消托管原因代码关联的消息。 要获得密码质量代码的完整列表，请运行 seaudit -t。

消息 ID

（仅限 UNIX）表明 CA Access Control 取消托管 PROGRAM 或 SECFILE 的原因。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为状态代码，不显示在详细的输出或 CA Access Control 端点管理 中。 要了解状态代码的含义，请运行 seaudit -Stat *取消托管代码*。 仅在授权阶段代码为 1 时显示此字段。在所有其他情况下，均改为显示“错误号”字段。

错误号

表明 errno 变量的返回值（错误条件的错误代码）。

值：可以为以下值之一：

0—无错误。仅在授权阶段代码为 1 时返回此值。在此示例中，不显示“错误号”字段，而改为显示“消息 ID”字段。

错误号—表示错误的非零整数。

注意：要了解 UNIX 上错误的含义，请参阅本地计算机上的 /usr/include/errno.h 或 /usr/include/sys/errno.h 文件。 在 Windows 上，请在本地计算机上输入以下命令：net helpmsg *错误号*

文件

指明触发 Watchdog 消息的受保护资源的完整路径名。

示例：取消托管消息事件消息

以下审核记录取自详细的 seaudit 输出。

```
18 Nov 2008 14:01:18 U PROGRAM      seoswd                1 11776 /tmp/testsuid
事件类型：取消托管消息
类：PROGRAM
模块名称：seoswd
消息 ID：11776
日期：2008 年 11 月 18 日
```

```
时间：14:01
文件：/tmp/testsuid
详细信息：文件系统上的 Stat 信息已更改
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 11 月 15 日，Watchdog 将程序 /tmp/testsuid 标记为取消托管 (U)。 该程序已取消托管，原因是文件状态信息已被修改（取消托管原因代码 1－文件系统上的 File 信息已更改）。

示例：使用 seaudit -Stat 查看程序取消托管的原因 (UNIX)

以下 seaudit -Stat 输出显示了可以如何获得有关审核记录提及的 Watchdog 消息 ID 的更多详细信息。

```
# seaudit -Stat 11776
CA Access Control seaudit v12.01.00.45－审核日志列出程序
版权所有 (c) 2008 CA。 保留所有权利。

文件的 MODE 被更改
文件 INODE 被更改
文件 SIZE 被更改
文件 MTIME 被更改
```

通过消息 ID 运行 seaduit -Stat 命令，将显示对文件所做的更改的列表。在此示例中，文件的 MODE、INODE、SIZE 和 MTIME 被更改。 因此，CA Access Control 将此文件标记为取消托管的文件。

更多信息：

适用于取消托管消息事件的授权阶段代码 (p. 574)
指定记录创建原因的原因代码 (p. 593)

传入网络连接事件

传入网络连接事件表明受保护主机的传入流量。 将以两种形式审核传入网络事件（根据本地数据库类的激活情况）。 两种审核事件类型包含完全相同的信息，但位于不同的视图中。 例如：一个审核事件包含 HOST 作为类名，而其他事件显示 TCP 作为类名。

此事件中的审核记录格式如下：

Date Time Status Event Service Details Reason Host Program

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值： 可以为以下值之一：

- D（已拒绝）- 由于授权不足而拒绝事件。
- P（已允许）- 允许事件。
- W（警告）- 允许事件，原因是虽然访问请求违反了访问规则，但是设置了警告模式。

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为*事件*进行参阅。

服务

标识连接使用的服务名。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

主机名

标识网络流量所源自的主机的名称。

程序

（仅限 UNIX）标识访问者尝试运行的程序的名称。

示例：传入网络连接事件消息

以下审核记录取自详细的 seaudit 输出。

```
17 Nov 2008 12:22:04 D HOST        telnet              173  3 computer.org.com
/usr/sbin/inetd
事件类型：传入网络连接
状态：已拒绝
主机名：computer.org.com
服务：telnet
程序：/usr/sbin/inetd/
日期：2008 年 11 月 17 日
时间：12:22
详细信息：HOST 条目日期和时间限制
审核标志：AC 数据库用户
```

该审核记录表明在 2008 年 11 月 17 日，一名访问者尝试使用 telnet 服务运行 inetd 程序来访问主机 computer.org.com，但是由于受保护主机上强制执行的日期和时间限制（授权阶段代码 173－HOST 条目日期和时间限制），该访问被拒绝。 CA Access Control 已记录此事件，原因是资源的审核模式指定应记录此事件（原因代码 3－资源审核模式要求记录）。

更多信息：

适用于传入网络连接事件的授权阶段代码 (p. 575)
指定记录创建原因的原因代码 (p. 593)

传出网络连接事件

传出网络连接事件表明了至受保护主机的传出流量。 传出网络事件以两种形式进行审核（取决于本地数据库中的类激活）。 两种审核事件类型包含完全相同的信息，但位于不同的视图中。 例如：一个审核事件包含 HOST 作为类名，而其他事件显示 TCP 作为类名。

此事件中的审核记录格式如下：

日期 时间 状态 类 服务 用户名 详细信息 原因 主机 程序 终端 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值： 可以为以下值之一：

- D（已拒绝）- 由于授权不足而拒绝事件。
- P（已允许）- 允许事件。
- W（警告）- 允许事件，原因是虽然访问请求违反了访问规则，但是设置了警告模式。

类

指明类的名称。

服务

标识连接使用的服务名。

用户名

指明执行触发此事件的操作的访问者名称。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

主机名

指明目标主机的名称。

程序

指明触发事件的程序的名称。

终端

指明访问者用于连接到主机的终端的名称。

用户登录会话 ID

指明访问者的会话 ID。

注意：默认情况下，在非详细 seaudit 输出中不显示此字段。 要在非详细 seaudit 输出中显示此字段，请在 seaudit 命令中指定 -sessionid 选项。 只能将“用户登录会话 ID”字段添加到由于 TCP 或 CONNECT 类定义而生成的事件。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：传出网络连接事件消息

以下审核记录取自详细的 seaudit 输出。

```
21 Jan 2009 15:37:43 D TCP      telnet    root    408  2 computer.org /usr/bin/telnet
computer.com
事件类型：传出网络连接
状态：已拒绝
主机名：computer.org
服务：telnet
程序：/usr/bin/telnet
用户名：Administrator
终端：computer.com
用户名：root
日期：2009 年 1 月 21 日
时间：15:37:43
详细信息：TCP 服务的默认访问
用户登录会话 ID：4977248c:0000012a5248
审核标志：AC 数据库用户
```

此审核记录表明，2009 年 1 月 21 日，管理员通过 telnet 服务打开了一个从终端 computer.org 至名为 computer.com 的计算机的传出连接。 由于 TCP 记录的 defaccess 属性，CA Access Control 拒绝用户执行此操作。（授权阶段代码 408－TCP 服务的默认值）。CA Access Control 记录了此事件，原因是访问者的 AUDIT_MODE 属性与记录的结果相匹配。（原因代码 2－用户审核模式需要记录）。

更多信息：

适用于传出网络连接事件的授权阶段代码 (p. 580)
指定记录创建原因的原因代码 (p. 593)

安全数据库管理事件

安全数据库管理事件对由具有合适权限（CA Access Control 截获）的 CA Access Control 管理员或子管理员执行的操作进行了说明。

事件中的审核记录格式如下：

日期 时间 状态 事件 类 管理员 详细信息 原因 对象 终端 命令 审核标志

日期

指明事件发生的日期。

格式：DD MMM YYYY

注意：CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式：HH:MM:SS

注意：CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值：可以为以下值之一：

- D（已拒绝）- 由于授权不足而拒绝事件。
- S（成功）- 允许事件。
- F（已失败）- 使事件失败。

事件类型

指明此记录所属的事件类型。

注意：CA Access Control 端点管理 只是简单地将此字段作为*事件*进行参阅。

类

标识受管理资源所归属的类。

管理员

标识执行 selang 命令的管理用户的名称。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意：详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

对象

标识受管理资源的名称。

终端

指明访问者用于连接到主机的终端的名称。

注意：如果命令源自父策略模型，该字段会显示完全限定的 PMD 名称。

命令

显示用户执行的 selang 命令。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

命令类型

指明此事件说明的数据库管理命令的类型。

可以为以下值之一：

- **添加用户**－用于 newusr 命令
- **添加组**－用于 newgrp 命令
- **添加资源**－用于 newres 或 newfile 命令
- **修改用户**－用于 chusr 命令
- **修改组**－用于 chgrp 命令

- **修改组成员资格**－用于 join 命令
- **修改资源**－用于 chres 命令
- **修改资源访问**－用于 authorize 命令
- **删除用户**－用户 rmusr 命令
- **删除组**－用于 rmgrp 命令
- **删除资源**－用于 rmres 或 rmfile 命令
- **设置选项**－用于 setoptions 命令
- **添加/修改用户**－用于 editusr 命令
- **添加/修改组**－用于 editgrp 命令
- **添加/修改资源**－用于 editres 或 editfile 命令
- **管理命令**－用于其他命令

示例：安全数据库管理事件消息

以下审核记录取自详细的 seaudit 输出。

```
05 Nov 2008 15:45:12 S UPDATE      FILE      DOMAIN_NAME\computer 305  0 dfdok
computer.com cr file dfdok defacc(r)
事件类型：安全数据库管理
命令类型：修改资源
状态：成功
管理员：DOMAIN_NAME\computer
类：FILE
对象：dfdok
终端：computer.com
日期：2008 年 11 月 05 日
时间：15:45
详细信息：ADMIN 用户成功使用命令。
命令：cr file dfdok defacc(r)
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 11 月 5 日，CA Access Control 拒绝管理员试图通过在从终端 computer.com 登录的受保护主机上执行命令 cr file dfdok defacc(r) 来更新文件的访问（授权阶段代码 305－允许 ADMIN 用户使用的命令）。

更多信息：

适用于安全数据库管理事件的授权阶段代码 (p. 583)
指定记录创建原因的原因代码 (p. 593)

启动事件

CA Access Control 启动事件说明了 CA Access Control 服务 (Windows) 或后台进程 (UNIX) 的启动顺序。

事件中的审核记录格式如下：

日期 时间 M *事件服务*

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为*事件*进行参阅。

服务

seosd－主 CA Access Control 后台进程或服务。seosd 后台进程或服务控制 CA Access Control 的启动和关闭顺序。

示例：后台进程启动事件消息 (UNIX)

以下审核记录取自详细的 seaudit 输出。

```
02 Nov 2008 15:41:06 M START                                    seoswd
事件类型：后台进程启动
后台进程：seoswd
日期：2008 年 11 月 02 日
时间：15:41
审核标志：AC 数据库用户
```

此审核记录标明，2008 年 11 月 2 日启动了 seoswd Watchdog。

示例：引擎服务启动事件消息 (Windows)

以下审核记录取自详细的 seaudit 输出。

```
02 Nov 2008 15:34:48 M START                                    seosd
事件类型：引擎服务启动
引擎服务：seosd
日期：2008 年 11 月 02 日
时间：15:34
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 11 月 2 日启动了负责启动 CA Access Control 的 seosd 服务引擎。

关闭事件

CA Access Control 关闭事件说明了由管理员或具有关闭系统权限的子管理员用户执行的关闭进程。

此事件中的审核记录格式如下：

日期 时间 M *事件 用户名 会话 ID 详细信息 服务 审核标志*

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为 *事件*进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

用户登录会话 ID

指明访问者的会话 ID。

注意：默认情况下，在非详细 seaudit 输出中不显示此字段。 要在非详细 seaudit 输出中显示此字段，请在 seaudit 命令中指定 -sessionid 选项。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

后台进程 (UNIX)/引擎服务 (Windows)

指明已关闭的 CA Access Control 后台进程 (UNIX) 或服务 (Windows) 的名称。

值：seosd（CA Access Control 引擎）。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：UNIX 上的关闭事件消息

以下审核记录取自详细的 seaudit 输出。

```
24 Sep 2008 15:40:46 M SHUTDOWN      root     452 seosd
事件类型：后台进程关闭
用户名：root
后台进程：seosd
日期：2008 年 9 月 24 日
时间：15:40:46
详细信息：用户为 ADMIN 或 SPECIAL
用户登录会话 ID：48da26ce:00000142
审核标志：CA Access Control 数据库用户
```

此审核记录表明，2008 年 9 月 24 日，允许正尝试关闭 CA Access Control 的用户 root 执行此操作，原因是该用户具有 ADMIN 属性（授权阶段代码 452－用户为 ADMIN 或 SPECIAL）。

示例：Windows 上的关闭事件消息

以下审核记录取自详细的 seaudit 输出。

```
23 Dec 2008 12:56:20 D SHUTDOWN     tst002                    460 seosd
事件类型：引擎服务关闭
用户名：tst002
引擎服务：seosd
日期：2009 年 2 月 10 日
时间：12:56
详细信息：不允许用户关闭 CA Access Control

用户登录会话 ID：00000000:04c240d5
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 12 月 23 日，CA Access Control 关闭被拒绝，原因是不允许用户 tst002 关闭 CA Access Control（授权阶段代码 460－不允许用户关闭 CA Access Control）。

更多信息：

适用于关闭事件的授权阶段代码 (p. 588)

密码验证事件

密码验证事件类型消息表明用户无法更改其帐户的密码。

此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 详细信息 原因 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值： F（失败）- 无法更改帐户密码。

事件类型

指明此记录所属的事件类型。

注意： CA Access Control 端点管理 只是简单地将此字段作为 *事件* 进行参阅。

用户名

指明尝试应用密码的用户的名称。

详细信息

表明密码更改尝试失败的原因。

注意： 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为密码质量代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与密码质量代码相关的消息。 要获得密码质量代码的完整列表，请运行 seaudit -t。

原因

表明 CA Access Control 写入审核记录的原因。

注意： 详细的 seaudit 输出或 CA Access Control 端点管理 中不显示此字段。 无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为原因代码。 要获得原因代码的完整列表，请运行 seaudit -t。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意： 如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：密码验证事件消息

以下审核记录取自详细的 seaudit 输出。

```
02 Dec 2008 10:23:47 F PASSWORD     test1         1 10
事件类型：密码验证
状态：失败
用户名：test1
详细信息：密码太短
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 12 月 2 日，尝试更改帐户密码的用户被拒绝，原因是该密码未符合由密码策略定义的所需的最小字符数（授权阶段代码 1－密码太短）。 CA Access Control 根据显性请求记录了此事件消息（原因代码 10－接收到记录操作的显性请求）。

更多信息：

适用于密码验证事件的授权阶段代码 (p. 589)
指定记录创建原因的原因代码 (p. 593)

有关用户的跟踪消息

有关用户事件的跟踪消息描述了打开、运行或使用受保护资源的尝试。

在 Windows 上，此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 会话 ID 真实用户 ID 真实用户名 类 资源 详细信息 跟踪 审核标志

在 UNIX 上，此事件中的审核记录格式如下：

日期 时间 状态 事件 用户名 会话 ID 真实用户名 有效用户名 类 资源 详细信息 跟踪 审核标志

日期

指明事件发生的日期。

格式： DD MMM YYYY

注意： CA Access Control 端点管理 根据您计算机的设置对日期的显示进行格式化。

时间

指明事件发生的时间。

格式： HH:MM:SS

注意： CA Access Control 端点管理 根据您计算机的设置对时间的显示进行格式化。

状态

表明事件的返回代码。

值：可以为以下值之一：

- D（已拒绝）- 由于授权不足而拒绝事件。
- P（已允许）- 允许事件。
- W（警告）- 允许事件，原因是虽然访问请求违反了访问规则，但是设置了警告模式。

注意：在详细的 seaudit 输出中，此字段会显示跟踪信息。

事件类型

指明此记录所属的事件类型。

注意：CA Access Control 端点管理 只是简单地将此字段作为 *事件*进行参阅。

用户名

指明执行触发此事件的操作的访问者名称。

用户登录会话 ID

指明访问者的会话 ID。

真实用户 ID

指明调用进程的用户的用户 ID。

注意：(UNIX) 在非详细 seaudit 输出中不显示此字段。

真实用户名

指明执行跟踪操作的用户的名称。

有效用户 ID

（仅限 UNIX）表明本地操作系统有效用户的 ID。

注意：在非详细 seaudit 输出中不显示此字段。

有效的用户名

（仅 UNIX）识别触发该事件的本机操作系统有效用户的名称。 如果用户替换（替代）为不同的用户或运行 setuid 程序，则不同于用户名。

注意：在 KBL 审核输出中不显示此字段。

类

指明被访问的资源所属的类。

资源

指明正在被访问或更新的实际资源的名称。

详细信息

表明 CA Access Control 决定在哪个阶段为此事件执行何种操作。

注意：无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示一个数字。 此数字称为授权阶段代码。 在详细的输出或 CA Access Control 端点管理 中，审核记录将显示与授权阶段代码相关的消息。 要获得阶段代码的完整列表，请运行 seaudit -t。

跟踪信息

显示跟踪详细信息，包括类、资源以及在该资源上执行的操作或该操作的结果。

审核标志

表明访问者是内部用户（CA Access Control 数据库用户）还是企业用户。

注意：如果访问者是企业用户，则无详细信息的 seaudit 输出中显示的审核记录将在此字段中显示字符串“(OS user)”。 否则，此字段保留为空。

示例：UNIX 上有关用户事件消息的跟踪消息

以下审核记录取自详细的 seaudit 输出。

```
03 Nov 2008 10:38:47 P TRACE       root       490daddd:00000140 john       root
FILE         /home/jon/file.txt   55  FILE    > Result: 'P' [stage=55 gstag=55
ACEEH=8   rv=0(/home/john/file.txt
事件类型：有关用户的跟踪消息
日期：2008 年 11 月 03 日
时间：10:38
详细信息：资源 ACL 检查
跟踪信息：FILE    > Result: 'P' [stage=55 gstag=55 ACEEH=8
rv=0(/home/john/file.txt
类：FILE
资源：/home/admin/file.txt
用户名：root
真实用户 ID：108
真实用户名：john
有效用户 ID：108
有效用户名：root
用户登录会话 ID：490daddd:00000140
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 11 月 3 日，由于管理员尝试访问属于 FILE 类的资源而记录了跟踪消息。 根据被访问资源的 ACL 允许管理员进行访问（授权阶段代码 55－资源 ACL 检查）。

示例：Windows 上有关用户事件消息的跟踪消息

以下审核记录取自详细的 seaudit 输出。

```
10 Nov 2008 10:14:53 P TRACE        MACHINE\Administrator 00000000:172ef9ef
MACHINE\john MACHINE\john WINSERVICE   _default     1059  WINSERVICE >
(C:\WINDOWS\system32\services.exe) Result: 'P' [stage=1059 gstag=1059 ACEEH=6
rv=0x0 (WebClient)]                              Why?  默认记录通用访问检查
事件类型：有关用户的跟踪消息
日期：2008 年 11 月 10 日
时间：10:14
详细信息：默认记录通用访问权限检查
跟踪信息：WINSERVICE > (C:\WINDOWS\system32\services.exe) Result: 'P' [stage=1059
gstag=1059 ACEEH=6    rv=0x0 (WebClient)]                        Why?  默认记录
通用访问检查
类：WINSERVICE
资源：_default
用户名：MACHINE\Administrator
真实用户名：MACHINE\john
用户登录会话 ID：00000000:172ef9ef
审核标志：AC 数据库用户
```

此审核记录表明，2008 年 11 月 10 日，由于管理员尝试访问属于 WINSERVICE 类的 resource _default 而触发跟踪消息。 由于记录通用访问权限检查而允许管理员进行访问（授权阶段代码 1059— 默认记录通用访问权限检查）。

更多信息：

有关用户的跟踪消息的授权阶段代码 (p. 592)
指定记录创建原因的原因代码 (p. 593)

适用于登录和注销事件的授权阶段代码

适用于登录和注销事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为登录和注销事件执行何种操作。

更多信息：

登录事件 (p. 528)
注销事件 (p. 531)
已启用登录帐户事件 (p. 533)
已禁用登录帐户事件 (p. 535)
密码尝试事件 (p. 537)

2—提取用户对象

表明登录尝试失败，原因是 CA Access Control 无法加载用户信息，例如用户模式、终端或登录程序。 如果数据库已损坏或 CA Access Control 未正确启动，CA Access Control 可能会将此信息写入审核日志。

3—对登录终端源进行终端检查

表明 CA Access Control 根据 TERMINAL 类规则允许或拒绝登录。

5—用户挂起检查

表明 CA Access Control 拒绝登录，原因是用户帐户已挂起。

6—用户过期检查

表明 CA Access Control 拒绝登录，原因是按照用户配置文件中的定义，用户帐户已过期。

7—用户日期-时间检查

表明 CA Access Control 拒绝登录，原因是用户尝试在 CA Access Control 数据库允许登录的日期和时间之外登录。

8—密码验证检查

在 UNIX 上有效

表明 CA Access Control 已检查用户的密码以确保它符合密码规则。 如果登录尝试失败，则 CA Access Control 可能会将此消息写入审核日志，原因是用户的密码不符合 CA Access Control 数据库密码规则。

9—用户宽限登录检查

表明 CA Access Control 拒绝登录，原因是用户帐户已经用完其宽限登录尝试。

10－密码已过期，并且没有更多的宽限登录

表明 CA Access Control 拒绝登录，原因是密码已过期。 在用户配置文件组的定义以及 CA Access Control 全局定义中，用户均未在密码间隔限制内更改其密码，并且未配置任何密码过期后的宽限次数。

11－构建用户 ACEE

表明 CA Access Control 已成功为用户生成 ACEE。

12－用户不活动天数检查

表明 CA Access Control 拒绝登录，原因是用户处于不活动状态的时间超出了允许的不活动间隔时间。 允许的不活动间隔时间在用户的配置文件或全局 CA Access Control 设置中定义。

13－用户登录次数过多

表明 CA Access Control 拒绝登录，原因是用户已超出从不同终端同时登录的最多允许次数。 允许同时登录的最多次数在用户配置文件或全局 CA Access Control 设置中的“Maxlogins”属性值中定义。

14－活动 HOLIDAY 检查

表明 CA Access Control 拒绝登录，原因是用户在受限假日期间尝试登录。 受限假日日期在 HOLIDAY 类中定义。

15－登录应用程序 (LOGINAPPL) 检查

在 UNIX 上有效

表明根据 LOGINAPPL 类规则，CA Access Control 拒绝登录。

16－用户组日期-时间检查

表明 CA Access Control 拒绝登录，原因是用户在用户或用户组成员允许访问的日期和时间之外尝试登录。

17－操作遭到本地环境拒绝

在 UNIX 上有效

表明由于本地环境设置，登录尝试失败。 通过 CA Access Control PAM 模块登录。

18－不带域限制的用户

在 Windows 上有效

表明 CA Access Control 拒绝登录，原因是用户未提供域名。

19－无理由拒绝－允许登录

表明 CA Access Control 已允许登录，原因是如果登录授权已分配至 TERMINAL 对象，登录尝试会通过所有检查阶段。

注意：显示此事件阶段消息可能表明登录授权已由未指定终端名的 CA Access Control 授权 API 触发。

20 -“逻辑”用户检查

表明 CA Access Control 拒绝登录，原因是 CA Access Control 不允许“逻辑”用户（带有*逻辑*属性设置的用户）登录。

49－最后一个进程终止后检测到注销

在 UNIX 上有效

表明 CA Access Control 检测到在最后一个进程终止后发生用户注销事件。

适用于资源访问事件的授权阶段代码

适用于资源访问事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为资源访问事件执行何种操作。

更多信息：

资源访问事件 (p. 539)

50－资源的安全 LABEL 检查

表明 CA Access Control 拒绝访问资源，原因是尝试访问资源的用户符合以下条件之一。

- 资源安全标签的安全级别高于用户安全标签
- 用户不具有安全标签

51－资源的安全 LEVEL 检查

表明 CA Access Control 拒绝访问资源，原因是尝试访问资源的用户符合以下条件之一。

- 资源的安全级别高于用户
- 用户不具有安全级别

52－资源的类别检查

表明 CA Access Control 拒绝访问资源，原因是未将分配给资源的安全类别分配给用户。

53－资源 DAYTIME 检查

表明 CA Access Control 拒绝访问资源，原因是用户尝试在对资源的允许访问日期和时间之外进行访问。

54－资源的 OWNER 检查

表明 CA Access Control 已允许访问资源，原因是访问用户拥有该资源。

55－资源 ACL 检查

表明 CA Access Control 已允许或拒绝访问资源，因为资源 ACL 中已列出用户。

56－在 ACL 检查资源组中

表明 CA Access Control 已允许或拒绝访问资源，因为资源组 ACL 列表中已列出用户。

57－资源 ACL 中的用户组

表明 CA Access Control 已允许或拒绝访问资源，因为用户组 ACL 至少列出了一项资源。

58－资源组 ACL 中的用户组

表明 CA Access Control 已允许或拒绝访问资源，因为资源组 ACL 至少列出了其中一个用户组。

59－资源 UACC 检查

表明根据资源的默认设置，CA Access Control 已允许访问资源。

61－用户是该资源的 OPERATOR

表明 CA Access Control 已允许访问资源，原因是用户具有 OPERATOR 属性。 OPERATOR 属性可让用户跳过对 FILE 资源进行读取访问和更改目录访问的授权过程。

注意：在 UNIX 上，CA Access Control 仅将此消息写入跟踪文件，而不会将该消息写入审核日志文件。

62－未受保护资源类的 UACC 检查

表明根据资源类中的 defaccess 值，CA Access Control 已允许或拒绝访问不包含 CA Access Control 数据库中记录的资源。

63－程序条件访问

表明 CA Access Control 已允许或拒绝访问资源，原因是资源 PACL 列出了程序和用户或其中一个用户组。

64－资源 ACL 中的用户 '*'

表明 CA Access Control 已允许或拒绝访问资源，因为资源 ACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

65－用户是该资源的 AUDITOR

表明 CA Access Control 允许访问审核文件，原因是用户具有 AUDITOR 属性。 AUDITOR 属性让用户可以跳过对读取访问和更改目录访问请求的授权过程。

注意：CA Access Control 仅将该消息写入跟踪文件，而不写入审核日志文件。

69－没有允许访问的步骤

表明 CA Access Control 拒绝访问资源，原因是它无法找到可让用户访问资源的规则。

70－资源组的 OWNER 检查

表明 CA Access Control 允许访问资源，因为尝试访问资源的用户是其中一个资源组的所有者。

75－资源组 ACL 中的用户 '*'

表明 CA Access Control 已允许或拒绝访问资源，因为资源组 ACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

76－资源已拒绝 ACL 检查

表明 CA Access Control 拒绝访问资源，因为资源 NACL 中已列出用户。

77－在已拒绝 ACL 检查的资源组中

表明 CA Access Control 拒绝访问资源，因为资源组 NACL 中已列出用户。

78－拒绝 ACL 的资源中的用户组

表明 CA Access Control 已允许或拒绝访问资源，因为资源 NACL 至少列出了其中一个用户组。

79－拒绝 ACL 的资源组中的用户组

表明 CA Access Control 已允许或拒绝访问资源，因为资源组 NACL 至少列出了其中一个用户组。

80－拒绝 ACL 的资源中的用户 '*'

表明 CA Access Control 拒绝访问资源，原因是资源 NACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

81－拒绝 ACL 的资源组中的用户 '*'

表明 CA Access Control 拒绝访问资源，因为资源组 NACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

82－资源组 DAYTIME 检查

表明 CA Access Control 拒绝访问资源，原因是用户尝试在资源组的允许访问日期和时间之外访问该资源。

86－用户的资源日历 ACL 检查

表明 CA Access Control 已允许或拒绝访问资源，原因是用户尝试在资源 CALACL 允许或拒绝访问的时间进行资源访问。

87－用户的资源组日历 ACL 检查

表明 CA Access Control 已允许或拒绝访问资源，原因是用户尝试在资源组 CALACL 允许或拒绝访问的时间进行资源访问。

88－用户组的资源日历 ACL 检查

表明 CA Access Control 已允许或拒绝访问资源，原因是用户尝试在允许或拒绝（用户所在的组已在资源 CALACL 中列出）的时候进行资源访问。

89－用户组的资源组日历 ACL 检查

表明 CA Access Control 已允许或拒绝访问资源，原因是用户组尝试在允许或拒绝（用户所在的组已在资源 CALACL 中列出）的时候进行资源访问。

90－资源日历 ACL 中的用户 *

表明 CA Access Control 已允许或拒绝访问资源，因为资源 CALACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

91－资源组日历 ACL 中的用户 *

表明 CA Access Control 已允许或拒绝访问资源，因为资源组 CALACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

92－尝试重命名受保护资源的路径

在 Windows 上有效

表明 CA Access Control 拒绝重命名受保护文件或注册表项的请求。

200－类检查不活动

表明 CA Access Control 已允许访问资源，原因是资源类不活动。

注意：当资源类不活动时，setoptions 列表命令显示类活动为“No”。

201－正在加载用户信息

表明 CA Access Control 无法授权请求，原因是检索用户信息失败。

202－警告模式下的资源

表明 CA Access Control 已允许访问资源，原因是资源处于警告模式。

203－资源的访问权限为 MAXIMUM_ALLOWED

在 Windows 上有效

允许时，表明 CA Access Control 将最大访问权限分配给注册表句柄。

拒绝时，表明 CA Access Control 阻止访问注册表句柄。

204－警告模式下的类

表明 CA Access Control 已允许访问资源，原因是资源类处于警告模式。

210－特殊内核模块加载检查

在 UNIX 上有效

表明根据 KMODULE 类定义，CA Access Control 已允许或拒绝内核模块的加载或卸载。

250－执行未受托的程序

表明 CA Access Control 拒绝执行未受托程序的尝试。

251－正在使用可拒绝参数

表明 CA Access Control 拒绝执行 sesudo 命令的尝试，原因是命令语法包含 SUDO 记录定义为禁止的参数。

252－由 _abspath 用户指定的相对路径

在 UNIX 上有效

表明 CA Access Control 拒绝执行由相对路径指定的程序的尝试，原因是尝试执行程序的用户是“_abspath”组的成员。

253－允许的 sesudo 作业

表明 CA Access Control 已允许执行 sesudo 命令的尝试。

254－sesudo 命令失败

在 UNIX 上有效

表明 sesudo 命令在操作系统中执行失败。

440－检测到无效日历

表明 CA Access Control 拒绝访问，因为获取日历信息时出现错误。例如：内存出现问题或日历表损坏。

441－日历不允许访问

表明 CA Access Control 拒绝访问，因为与所访问资源相关的日历对象的定义不允许此时访问。

1050－默认记录安全标签检查

表明 CA Access Control 拒绝对默认记录的访问，因为对于尝试访问资源的用户，满足以下条件之一：

- 资源安全标签的安全级别高于用户安全标签
- 用户不具有安全标签

1051－默认记录安全级别检查

表明 CA Access Control 拒绝对默认资源的访问，因为对于尝试访问资源的用户，满足以下条件之一：

- 资源的安全级别高于用户
- 用户不具有安全级别

1052－默认记录类别检查

表明 CA Access Control 拒绝对默认资源的访问，因为给该资源分配了一个安全类别，而该安全类别未分配给用户。

1053－默认记录日期和时间检查

表明 CA Access Control 拒绝对默认资源的访问，因为用户尝试访问的时间不在允许访问资源的日期和时间范围内。

1054－默认记录 OWNER 检查

表明 CA Access Control 允许对默认资源的访问，因为访问用户拥有该默认资源。

1055－用户的默认记录 ACL 检查

表明 CA Access Control 允许/拒绝对默认资源的访问，因为资源 ACL 列出/未列出该用户。

1056－用户的默认记录组 ACL 检查

表明 CA Access Control 允许/拒绝对默认资源的访问，因为资源组 ACL 列出/未列出该用户。

1057－用户组的默认记录 ACL 检查

表明 CA Access Control 允许对默认资源的读取或 chdir 访问。

注意：CA Access Control 仅将该消息写入跟踪文件，而不写入审核日志文件。

1058－用户组的默认记录组 ACL 检查

表明 CA Access Control 允许/拒绝对默认资源的访问，因为资源组 ACL 列出/未列出该用户组。

1059－默认记录通用访问权限检查

表明由于默认资源的默认设置，CA Access Control 允许对该资源的访问。

1061－默认记录 OPERATOR 属性检查

表明 CA Access Control 允许对默认资源的访问，因为用户具有 OPERATOR 属性。 OPERATOR 属性让用户可以跳过对读取访问和更改目录访问请求的授权过程。

注意：CA Access Control 仅将该消息写入跟踪文件，而不写入审核日志文件。

1062－默认记录类全局通用访问权限

表明 CA Access Control 根据资源类中的 defaccess 值，允许或拒绝对在 CA Access Control 数据库中没有记录的默认资源的访问。

1063－默认记录程序条件访问权限

表明 CA Access Control 允许/拒绝对默认资源的访问，因为资源 PACL 列出/未列出访问该资源的程序。

1064－默认记录 ACL 中的用户“*”

表明 CA Access Control 允许或拒绝对默认资源的访问，因为资源 ACL 包含星号 (*)。

注意：星号可指定所有已定义的用户。

1069－没有规则授予对于默认记录的访问权限

表明 CA Access Control 拒绝对默认资源的访问，因为未找到允许用户访问该资源的规则。

1202－警告模式下的默认记录

表明 CA Access Control 允许对默认资源的访问，因为该资源处于警告模式下。

1250－默认记录设置为了取消受托

表明 CA Access Control 拒绝对执行默认的取消受托程序的尝试。

适用于取消托管消息事件的授权阶段代码

适用于取消托管消息事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为取消托管消息事件执行何种操作。

更多信息：

取消托管消息事件 (p. 542)

0－Watchdog 文件检查时出现常规错误

表明在 CA Access Control 提取文件信息时发生错误。 如果文件未受托，CA Access Control 可能会将此消息写入审核日志。 要获得详细信息，应查看系统日志。

1－PROGRAM 或 SECFILE 的状态信息已更改

表明 PROGRAM 或 SECFILE 类的记录中的数据已更改。 如果 CA Access Control 检测到篡改程序或文件的尝试，可能会将此信息写入审核日志。 应查看程序或文件的审核事件、系统日志和跟踪记录。 如果程序或文件已由管理员更改，请考虑重新托管已更改程序或文件。

4－PROGRAM 或 SECFILE 的 CRC 检查已更改

表明循环冗余检查 (CRC) 已更改了 PROGRAM 或 SECFILE 类中的记录。 应查看程序或文件的系统日志、事件日志文件和跟踪记录。

5—无法获取 PROGRAM 或 SECFILE 的状态文件

表明 CA Access Control 检索指定文件的文件信息失败。 如果发生以下情况之一，CA Access Control 可能会将此消息写入审核日志：

- 已更改文件名或目录
- 文件名或目录不存在
- 文件的访问权限
- 系统内存不足

要确定错误的可能原因，请查看系统日志文件。

7—PROGRAM 或 SECFILE 的 MD5 签名已更改

表明 PROGRAM 或 SECFILE 类中记录的 MD5 签名已更改。 应查看程序或文件的系统日志文件、审核消息和跟踪日志。

8—PROGRAM 或 SECFILE 的 SHA1 签名已更改

表明 PROGRAM 或 SECFILE 类中记录的 SHA1 签名已更改。 应查看程序或文件的系统日志文件、审核消息和跟踪日志。

适用于传入网络连接事件的授权阶段代码

适用于传入网络连接事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为传入网络连接事件执行何种操作。

更多信息：

传入网络连接事件 (p. 545)

150—检查类表

表明无法在 CA Access Control 数据库中找到该类。 如果在 CA Access Control 数据库中出现问题，CA Access Control 可能会将此消息写入审核日志。 要更正此问题，请使用 dbmgr 实用程序来重建 CA Access Control 数据库。

重要说明！ 问题解决期间，请仅在支持人员的指导下使用 dbmgr 实用程序。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

更多信息：

dbmgr 实用程序 (p. 32)

153—inetacl 中的 HOST 条目星号

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是主机 INETACL 中包括一个星号 (*)。

注意：星号可指定包含零个或多个字符的任何序列，因此在 INETACL 中使用时可匹配所有服务。

156—HOST 条目 inetacl

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是主机 INETACL 已列出连接服务。

157—HOST 类 UACC

表明根据为主机 UACC 类定义的默认访问授权值，CA Access Control 已允许或拒绝受保护主机的连接。

159—HOST 条目服务范围 ACL

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是连接服务属于主机 INETACL 范围内。

163—没有授予服务访问权限的规则

表明 CA Access Control 拒绝主机的连接，原因是找不到允许访问的规则。 应查看针对该主机的 HOST 类访问规则。

164—HOST 组 inetacl

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是 GHOST 对象的 INETACL 已列出连接服务。

165—HOST 组服务范围 ACL

表明 CA Access Control 已允许或拒绝受保护主机的连接（即 GHOST 主机组对象的成员），原因是连接服务属于主机组的 INETACL 范围内。

166—inetacl 中的 HOST 组星号

表明 CA Access Control 已允许或拒绝属于 GHOST 主机组对象的受保护主机的连接，原因是主机组的 INETACL 中包括一个星号 (*)。

注意：星号可指定包含零个或多个字符的任何序列，因此在 INETACL 中使用时可匹配所有服务。

167—HOSTNET（网络或 IP 掩码/匹配）inetacl

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是 HOSTNET 记录 INETACL 已列出连接服务。

168—HOSTNET（网络或 IP 掩码/匹配）服务范围

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是连接服务属于 HOSTNET 记录 INETACL 范围内。

169—HOSTNET（网络或 IP 掩码/匹配）inetacl 星号

指明 CA Access Control 已允许或拒绝受保护主机的连接，原因是 HOSTNET 记录 INETACL 中包括一个星号 (*)。

注意：星号可指定包含零个或多个字符的任何序列，因此在 INETACL 中使用时可匹配所有服务。

170—HOSTNP（主机名称模式）inetacl

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是 HOSTNP 记录 INETACL 已列出连接服务。

171—HOSTNP（主机名称模式）服务范围

表明 CA Access Control 已允许或拒绝受保护主机的连接，原因是连接服务属于 HOSTNP 记录 INETACL 范围内。

172—HOSTNP（主机名称模式）inetacl 星号

指明 CA Access Control 已允许或拒绝受保护主机的连接，原因是 HOSTNP 记录 INETACL 中包括一个星号 (*)。

注意：星号可指定包含零个或多个字符的任何序列，因此在 INETACL 中使用时可匹配所有服务。

173—HOST 条目日期和时间限制

表明 CA Access Control 拒绝访问受保护主机，原因是访问尝试时间在 HOST 记录中的日期和时间限制范围之外。

174—HOST 组日期和时间限制

表明由于 GHOST 记录中的日期和时间限制，CA Access Control 拒绝访问受保护主机组。

175—HOSTNET（网络或 IP 掩码/匹配）日期和时间限制

表明由于 HOSTNET 记录中的日期和时间限制，CA Access Control 拒绝访问受保护主机。

176—HOSTNP（主机名称模式）日期和时间限制

表明由于 HOSTNP 记录中的日期和时间限制，CA Access Control 拒绝访问受保护主机。

177—HOST_default 日期和时间限制

表明由于 HOST _default 记录中的日期和时间限制，CA Access Control 拒绝访问受保护主机。

178—HOST_default inetacl

表明根据 HOST _default INETACL 中的值，CA Access Control 已允许或拒绝访问受保护主机。

179—HOST_default 服务范围

表明 CA Access Control 已允许或拒绝访问受保护主机，原因是连接服务属于 HOST _default 记录 INETACL 范围内。

180—HOST_default 服务星号

表明 CA Access Control 已允许或拒绝访问受保护主机，原因是 HOST _default 记录 INETACL 中包括一个星号 (*)。

注意：星号可指定包含零个或多个字符的任何序列，因此在 INETACL 中使用时可匹配所有服务。

404—TCP 服务 ACL 中的 HOST 条目

表明 CA Access Control 已允许或拒绝 HOST 的访问，原因是 TCP 记录 ACL 已列出 HOST。

405—TCP 服务 ACL 中的 GHOST 条目

表明 CA Access Control 已允许或拒绝 HOST 的访问，原因是 TCP 记录 ACL 已列出 GHOST（HOST 是其中的成员）。

406—TCP 服务 ACL 中的 HOSTNET 条目

表明 CA Access Control 已允许或拒绝 HOST 的访问，原因是 TCP 记录 ACL 已列出 HOSTNET 网络（HOST 是其中的一部分）。

407—TCP 服务 ACL 中的 HOSTNP 条目

表明 CA Access Control 已允许或拒绝 HOST 的访问，原因是 TCP 记录 ACL 已列出 HOSTNP 集（HOST 是其中的一部分）。

适用于传出网络连接事件的授权阶段代码

适用于传出网络连接事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为传出网络连接事件执行何种操作。

更多信息：

传出网络连接事件 (p. 547)

400—类 TCP 内的 _default 服务

表明根据连接服务的 TCP 记录中的 _default 对象权限，CA Access Control 已允许或拒绝访问受保护主机。

401—TCP 服务的类 UACC

表明根据 UACC 类中 TCP 对象的值，CA Access Control 已允许或拒绝访问受保护主机。

402—TCP 服务的日期和时间限制

表明由于 TCP 记录中的日期和时间限制，CA Access Control 拒绝访问 TCP 服务。

403—TCP 服务的 ACL 读取阶段

表明由于 TCP 记录中的 ACL 读取属性，CA Access Control 已允许或拒绝访问 TCP 服务。 如果数据库已损坏，CA Access Control 可能会将此消息写入审核日志。

408—TCP 服务的默认访问权限

表明由于 TCP 记录的 defaccess 属性，CA Access Control 已允许或拒绝访问 TCP 类服务。

注意：此事件消息还适用于传入 TCP 事件，以表明至 HOST 的传入连接。

409—TCP 服务的 CACL 读取阶段

表明由于 TCP 记录中的 CACL 读取属性，CA Access Control 拒绝访问 TCP 服务。 如果数据库已损坏，CA Access Control 可能会将此消息写入审核日志。

410—TCP 服务 CACL 中的 USER 的 HOST 条目

表明 CA Access Control 已允许或拒绝访问指定 USER 或 XUSER 的 HOSt 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

411—TCP 服务 CACL 中的 USER 的 GHOST 条目

表明 CA Access Control 已允许或拒绝访问指定 USER 或 XUSER 对象的 GHOST 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

412—TCP 服务 CACL 中的 USER 的 HOSTNET 条目

表明 CA Access Control 已允许或拒绝访问指定 USER 或 XUSER 对象的 HOSTNET 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

413—TCP 服务 CACL 中的 USER 的 HOSTNP 条目

表明 CA Access Control 已允许或拒绝访问指定 USER 或 XUSER 对象的 HOSTNP 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

414—TCP 服务 CACL 中 GROUP 的 HOST 条目

表明 CA Access Control 已允许或拒绝访问指定 GROUP 或 XGROUP 对象的 HOST 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

415—TCP 服务 CACL 中 GROUP 的 GHOST 条目

表明 CA Access Control 已允许或拒绝访问指定 GROUP 或 XGROUP 对象的 GHOST 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

416—TCP 服务 CACL 中 GROUP 的 HOSTNET 条目

表明 CA Access Control 已允许或拒绝访问指定 GROUP 或 XGROUP 对象的 HOSTNET 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

417—TCP 服务 CACL 中 GROUP 的 HOSTNP 条目

表明 CA Access Control 已允许或拒绝访问指定 GROUP 或 XGROUP 对象的 HOSTNP 对象。 CA Access Control 使用 TCP 服务的 CACL 中的访问规则来决定是允许还是拒绝访问。

418—TCP 服务 CACL 中 User '*' 的 HOST 条目

表明 CA Access Control 已允许或拒绝访问用户 HOST，原因是 HOST 记录 CACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

419—TCP 服务 CACL 中 User '*' 的 GHOST 条目

表明 CA Access Control 已允许或拒绝访问属于用户 GHOST 类的 HOST，原因是 GHOST 记录 CACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

420—TCP 服务中 User '*' 的 HOSTNET 条目

表明 CA Access Control 已允许或拒绝访问用户的 HOSTNET 对象，原因是 HOSTNET 记录 CACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

421—TCP 服务 CACL 中 User '*' 的 HOSTNP 条目

表明 CA Access Control 已允许或拒绝访问用户的 HOSTNP 对象，原因是 HOSTNET 记录 CACL 中包括一个星号 (*)。

注意：星号可指定所有已定义的用户。

适用于安全数据库管理事件的授权阶段代码

适用于安全数据库管理事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为安全数据库管理事件执行何种操作。

更多信息：

安全数据库管理事件 (p. 550)

300—未定义的 CA Access Control 用户

表明 CA Access Control 拒绝用户访问系统，原因是在 CA Access Control 数据库中无法找到访问用户。 应检查用户帐户配置文件。

301—尝试删除上一个 ADMIN 用户

表明 CA Access Control 拒绝用户执行以下操作之一的请求：

- 从 CA Access Control 数据库中删除上一个 ADMIN 用户
- 删除指定了 ADMIN 属性的唯一用户的 ADMIN 属性

302—尝试删除用户 root

在 UNIX 上有效

表明 CA Access Control 拒绝用户尝试删除系统 root 帐户。

303—用户正尝试更改其自有密码

表明 CA Access Control 拒绝用户尝试使用 selang 命令更改其自有密码。在 UNIX 上可以使用 sepass 实用程序更改密码。 在 Windows 上可以使用本地密码管理工具更改密码。

304—Nonauditor 用户正尝试设置审核模式

表明 CA Access Control 拒绝用户尝试更改记录的审核模式，原因是该用户不具有 AUDITOR 属性。 要使该用户可以更改记录的审核模式，请为该其指定 AUDITOR 属性。

305—允许 ADMIN 用户使用的命令

表明 CA Access Control 允许执行某项操作，原因是请求执行该操作的用户具有 ADMIN 属性。

306—允许 Showuser (myself)、Showxusr

表明 CA Access Control 允许用户或外部用户在 CA Access Control 数据库中显示其自有记录的属性。

注意：此消息不作为审核记录写入。

307—用户正尝试设置其不具有的类别

表明 CA Access Control 拒绝用户尝试将安全类别分配给用户，原因是尝试分配安全类别的用户本身不具有该安全类别。

308—用户正尝试设置其不具有的安全标签

表明 CA Access Control 拒绝用户尝试将安全标签分配给用户，原因是尝试分配安全标签的用户本身不具有该安全标签。

309—用户正尝试设置比自有的安全级别更高的安全级别

表明 CA Access Control 拒绝用户尝试将安全级别分配给用户，原因是该用户具有的安全级别低于其正尝试分配的安全级别。

310—NonADMIN 用户正尝试设置用户模式

表明 CA Access Control 拒绝用户尝试设置管理属性，原因是尝试设置该属性的用户不具有 ADMIN 属性。

311—允许对象所有者使用的命令

表明 CA Access Control 允许执行某项操作，原因是用户拥有记录。

312—本地文件所有者可以将其定义到 CA Access Control

在 UNIX 上有效

表明 CA Access Control 允许执行某项操作，原因是文件所有者将该文件定义到 CA Access Control。

注意：将 seos.ini 文件的 lang 部分中的 use_unix_file_owner 标记设置为 yes 时，文件所有者可以将文件定义到 CA Access Control。

313—允许 GROUP-ADMIN 用户使用的命令

表明 CA Access Control 允许具有 GROUP-ADMIN 属性的用户在组内修改记录。

314—GROUP-ADMIN 用户可以加入组

表明 CA Access Control 允许具有 GROUP-ADMIN 属性的用户将用户添加到组或从组中删除用户。

315—GROUP-AUDITOR/ADMIN 可以列出组

表明 CA Access Control 允许用户在组内列出记录的属性，原因是该用户具有该组的 GROUP-ADMIN 或 GROUP-AUDITOR 属性。

316—审核者可以列出任何对象

表明 CA Access Control 允许具有 AUDITOR 属性的用户显示数据库中的数据。

317—操作员可以列出任何对象

表明 CA Access Control 允许具有 OPERATOR 属性的用户显示数据库中的数据

318—GROUP-AUDITOR 可以列出组范围中的对象

表明 CA Access Control 允许具有 GROUP-AUDITOR 属性的用户显示数据库中有关该组的数据。

319—GROUP-OPERATOR 可以列出组范围中的对象

表明 CA Access Control 允许具有 GROUP-OPERATOR 属性的用户显示数据库中有关该组的数据。

320—允许 CLASS-ADMIN 用户使用的命令

表明 CA Access Control 允许执行某项操作，原因是该操作是由 ADMIN 类的 ACL 中列出的用户执行的。

321—允许具有访问权限的 PWMANAGER/ADMIN 使用的命令

表明 CA Access Control 允许用户更改密码，原因是该用户具有 PWMANAGER 或 ADMIN 属性。

322—没有允许此操作的规则

表明 CA Access Control 拒绝用户执行某项操作，原因是未找到允许该操作的规则。

324—用户正使用 sepass 更改其自有密码

表明 CA Access Control 允许用户使用 sepass 实用程序或密码策略模型更改其自有密码。

326—用户已为自己创建了“登录信息”

表明 CA Access Control 允许用户为自己创建登录信息。

327－允许 GROUP-PWMANAGER 使用的命令

表明 CA Access Control 允许使用该命令，原因是执行该命令的用户具有 GROUP-PWMANAGER 属性。

329－PWMANAGER 已启用一个用户

表明 CA Access Control 允许用户启用（重新激活）其他用户，原因是启用了其他用户的用户具有 PWMANAGER 属性。

330－允许 DOMAIN 更改的命令

在 Windows 上有效

表明 CA Access Control 允许用户更改 DOMAIN 类，例如：将新计算机添加到域中。

331－允许 PWMANAGER 使用的命令

表明 CA Access Control 允许执行该命令，原因是执行该命令的用户具有 PWMANAGER 属性。

332－允许 PWMANAGER 更改本地标志

在 Windows 上有效

表明 CA Access Control 允许用户修改分配给用户帐户的帐户标志，原因是该用户具有 PWMANAGER 属性。

333－允许 PWMANAGER 更改“下一次登录必须更改密码”属性

对 Windows 有效

表明 CA Access Control 允许用户修改用户帐户的“下一次登录必须更改密码”属性，原因是该用户具有 PWMANAGER 属性。

334－允许 GROUP-PWMANAGER 使用的命令

表明 CA Access Control 允许使用该命令，原因是执行该命令的用户具有 GROUP-PWMANAGER 属性。

335－允许 PWMANAGER 编辑“登录信息”

表明 CA Access Control 允许用户编辑用户帐户的“登录信息”属性，原因是该用户具有 PWMANAGER 属性。

336－允许 auditor 用户使用的命令

表明 CA Access Control 允许用户执行命令，原因是该用户具有 AUDITOR 属性。

337－无法使命令与数据库信息一致

表明 CA Access Control 未执行某个命令，原因是 CA Access Control 数据库中不存在嵌入到命令中的对象。 重新执行命令之前，应检查命令语法。

338－创建来自隐性请求的命令

表明 CA Access Control 创建了来自隐性请求的命令。

339－SEOS_syscall 模块卸载准备情况检查

在 UNIX 上有效

表明访问者正在执行“secons –scl”命令以检查截获的 syscall 中是否有进程正在运行。 CA Access Control 不允许卸载 SEOS_syscall 模块。

适用于关闭事件的授权阶段代码

适用于关闭事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为关闭事件执行何种操作。

更多信息：

关闭事件 (p. 554)

451—用户为 OPERATOR

表明 CA Access Control 允许关闭请求，原因是执行关闭顺序的用户具有 OPERATOR 属性。

452—用户为 ADMIN 或 SPECIAL

表明 CA Access Control 允许关闭请求，原因是正在执行关闭顺序的用户具有分配给他的 ADMIN 属性。

453—允许 _seagent 关闭 CA Access Control

在 UNIX 上有效

表明 CA Access Control 允许关闭请求，原因是允许 _seagent 关闭 CA Access Control。

460—不允许用户关闭 CA Access Control

表明 CA Access Control 拒绝用户关闭请求，原因是不允许请求用户关闭 CA Access Control。

600—正在试图终止 CA Access Control

表示 CA Access Control 已拒绝关闭请求，因为用户已尝试通过执行 kill 命令来终止 CA Access Control。

适用于密码验证事件的授权阶段代码

适用于密码验证事件的授权阶段代码说明了 CA Access Control 决定在哪个阶段为密码验证事件执行何种操作。

更多信息：

密码验证事件 (p. 556)

0—密码质量已验证

表明用户成功更改其密码，且新密码符合所有密码质量规则。

1—密码太短

表明密码更改失败，原因是新密码的长度不符合最小密码长度这一密码策略。

2—密码包含用户名

表明密码更改失败，原因是新密码包含用户的用户名。

3—密码中的小写字母太少

表明密码更改失败，原因是根据密码策略中定义的最小值，新密码未包含足够的小写字母。

4—密码中的大写字母太少

表明密码更改失败，原因是根据密码策略中定义的最小值，新密码未包含足够的大写字母。

5—密码中的数字字符太少

表明密码更改失败，原因是根据密码策略中定义的最小值，新密码未包含足够的数字字符。

6—密码中的其他字符太少

表明密码更改失败，原因是根据密码策略中定义的最小值，新密码未包含足够的其他字符。

7—密码中相同字符的重复太多

表明密码更改失败，原因是根据密码策略中定义的最大值，新密码包含太多重复字符。

8—与当前密码相同

表明密码更改失败，原因是新密码与当前密码相同。 应该选择以前未曾使用的密码。

9－密码以前使用过。 请选择不同的密码

表明密码更改失败，原因是新密码以前使用过。 应该选择以前未曾使用的密码。

10－密码中的字母字符太少

表明密码更改失败，原因是根据密码策略中定义的最小值，新密码未包含足够的字符。

11－密码中的字母数字字符太少

表明密码更改失败，原因是根据密码策略中定义的最小值，新密码未包含足够的字母数字字符。

12－密码最近已更改，此时无法再更改

表明密码更改失败，原因是密码最近已更改，此时无法再更改。 根据密码策略中定义的最小值，应仅在密码最短存留期过后更改密码。

13－密码包含以前的一个密码或者以前的密码包含该密码

表明密码更改失败，原因是新密码包含以前的一个密码或者以前的密码包含该密码。 应确保新密码不包含以前的一个密码，且以前的密码不包含该新密码。

16－密码太长

表明密码更改失败，原因是根据密码策略中定义的最大值，新密码太长。

20－密码不匹配

表明密码更改失败，原因是新密码与在“确认密码”字段中输入的密码不匹配。

21－无法包括预定义的禁止字符

表明密码更失败，原因是根据密码策略，新密码包含禁止字符。

22－密码以前使用过

表明 CA Access Control 拒绝访问，因为您输入的密码以前使用过。 请确保使用的新密码符合密码策略规则。

23－密码包含以前的一个密码或者以前的密码包含该密码

表明密码更改尝试失败，因为以前的密码包含所用密码，或该新密码包含以前的密码。 您选择的新密码应不包含以前使用的密码。

24－密码在字典文件中

表明密码更改失败，原因是新密码在 DICTIONARY 类或 DICTIONARY 文件中定义。 应该选择未在 DICTIONARY 类或 DICTIONARY 文件中定义的密码。

100－参数错误

表明密码更改失败，原因是将无效数据发送到授权引擎。

如果出现以下情况之一，CA Access Control 可能会将此消息写入审核日志：

- 内存问题
- CA Access Control 各种模块版本与 CA Access Control 的最新升级不匹配

确认没有混合 CA Access Control 环境，并且客户端和服务器使用相同版本的 CA Access Control。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

有关用户的跟踪消息的授权阶段代码

有关用户的跟踪事件的授权阶段代码用于说明 CA Access Control 确定在哪个阶段对用户活动事件采取何种操作。

更多信息：

有关用户的跟踪消息 (p. 558)

994—信息性消息

表明用户访问了跟踪审核记录。

注意：这只是信息性消息，可通过运行 seaudit –tr 命令查看。

995—对内部资源未经授权的访问

表明访问者尝试对内部受保护文件资源进行未经授权的访问。 例如：seos.audit 记录。

996—对内部资源的授权访问

表明 CA Access Control 允许通过内部跳过访问资源。 例如：读取 /etc/passwd。

997—用户可以执行 setuid\setgid 目录

仅限 UNIX

表明 CA Access Control 跳过了事件，因为访问者尝试执行标记有 setuid\setgid 标志位的目录。 该阶段是跟踪记录消息的一部分。

998—授权配置为“仅审核模式”

仅限 Windows

表明 CA Access Control 设置为在“仅审核模式”中工作。

999—资源未被保护（检查规则是否存在）

表明 CA Access Control 允许访问未受保护的资源。

指定记录创建原因的原因代码

指定记录创建原因的原因代码用于说明 CA Access Control 确定在哪个阶段对事件创建何种审核记录。

0—对记录操作无特定请求

表明 CA Access Control 在默认情况下记录该操作，因为不存在对于记录操作的特定请求。

2—用户审核模式需要记录

表明 CA Access Control 记录了该操作，因为访问者的审核属性或其配置文件与记录的结果匹配。 例如：AUDIT_MODE 属性设置为 FAILURE 一值的用户所执行的操作只有在用户无法访问受保护的资源时才被记录。

3—资源审核模式需要记录

表明 CA Access Control 记录了该操作，因为资源的 RAUDIT 属性与记录的结果匹配。

4—警告模式下的资源

表明 CA Access Control 记录了该操作，因为已为资源或资源的类设置了 WARNING 属性。

5—CA Access Control serevu 实用程序请求了审核

在 UNIX 上有效

表明 CA Access Control 记录了该操作，因为 serevu 实用程序请求了审核记录，例如：当用户尝试登录失败时。

7—出站连接记录

在 UNIX 上有效

表明 CA Access Control 记录了该操作，因为出站连接成功。

8—CA Access Control pam 支持 UNIX 失败登录

在 UNIX 上有效

表明 CA Access Control 记录了该操作，因为 CA Access Control PAM 模块请求了审核，例如：在失败的密码登录尝试这一事件中。

9—CALENDAR 类的日期时间限制检查

表明由于 CALENDAR 类的日期时间限制检查需要记录审核记录，因此 CA Access Control 记录了该消息。

10—记录操作的特定请求

表明由于对记录该操作的特定请求（例如：尝试终止 CA Access Control 后台进程），CA Access Control 记录了该操作。

11—CA Access Control secons 实用程序请求了审核

在 UNIX 上有效

表明 CA Access Control 记录了该操作，因为请求了 Syscall 调用监控选项 (secons-scl)。

审核日志中 FILE 记录大写

在 Windows 上有效

在不同版本的 CA Access Control 中，FILE 类记录的审核记录在审核日志中的显示有所不同。

- 在所有 r5 和 r8 版本中，文件路径为小写形式。
- 在 r12.0 和 r12.0 SP1 中，文件路径为大写形式，与操作系统在计算机上表示该路径的方式相同。
- 在 r12.5 及更高版本中，文件路径为大写形式，与在 CA Access Control FILE 规则中的显示方式相同。

示例：审核日志中 FILE 记录大写

下表显示了对于将为其创建名为 C:\TMP\TEST.txt 的 FILE 记录的 C:\tmp\TeSt.txt 文件，在每个 CA Access Control 版本中审核记录如何显示在审核日志中：

释放	审核文件中的显示
r5 和 r8	C:\tmp\test.txt
r12.0 和 r12.0 SP1	C:\tmp\TeSt.txt
r12.5 及更高版本	C:\TMP\TEST.txt

附录 B： 跟踪消息

此部分包含以下主题：

约定

所有消息均以一个日期和时间前缀开头，后跟一个表示事件类型的大写词和一个符号（如 *:*、*!* 或 *>*）。- 下表解释了符号的含义。

:

CA Access Control 接收事件通知或执行了操作。

>

CA Access Control 做出授权决定，导致出现 *D*（拒绝）、*P*（允许）或 *BYPASS*（事件不要求解释访问规则，例如：setuid 请求的 UID 就是当前 UID。）

!

CA Access Control 检测到一个错误，例如：来自未知进程的请求。

消息

上一节中说明的符号位于本节中说明的事件参数之前。

ACTION : CA Access Control 终止 P=ppp

CA Access Control 拒绝了 setuid 或登录请求，并作为预防措施终止了请求进程 (ppp)。

ALARM ! Uid uuu 侵入了系统!!!

未知的进程发出了诸如再生、执行或 setuid 之类的请求。 该进程对于 CA Access Control 是未知的，此外，分配给该进程的 UID 没有分配给系统中的任何其他进程。 也就是说，用户已经登录，但未通知 CA Access Control。 该情形可能由于以下原因而出现：软件错误，或者用户在 CA Access Control 扫描当前进程状态之后但在完成初始化之前立即登录。

APIAUTH ! P=ppp U=uuu ChangePasswd(user) 错误 0xerr

进程 *ppp*（与用户 *uuu* 关联）希望更改 *user* 的密码。 此请求的结果是以十六进制指定的代码出错。请使用 semsgtool 实用程序确定错误的性质。

APIAUTH ! P=ppp U=uuu CheckPasswd(user) 错误 0xerr

进程 *ppp*（与用户 *uuu* 关联）希望检查 *user* 的新密码是否有效。 此请求的结果是以十六进制指定的代码出错。请使用 semsgtool 实用程序确定错误的性质。

APIAUTH ! P=ppp U=uuu 错误，未知 API 服务 nnn

进程 *ppp* 使用应用程序界面并传递了 CA Access Control 编程界面不支持的服务代码，很可能是因为用户错误。 请检查错误原因，更正源代码，然后重新编译它。

APIAUTH ! P=ppp U=uuu GeneralResourceProc 错误 nnn >description

进程 *ppp*（以 UID *uuu* 运行）发出了访问一般资源的请求；但是，无法解析指定的资源。 要么是指定的类未定义，要么是指定的访问未知，很可能是因为用户错误。 请检查代码，更正它，然后重新编译。

APIAUTH ! P=ppp U=uuu 在 VerifyCreate 中仅用于 ROOT

进程 *ppp*（以 UID *uuu* 运行）发出了生成 ACEE 的 VerifyCreate 请求。 仅允许与 UID 0 (root) 关联的多用户进程执行该操作。

如果要将指定的进程作为多用户进程运行，请以 root 用户权限重新运行该进程。 否则，确定进程发出该请求的原因。

APIAUTH : VerifyDelete 中的 P=ppp U=uuu 仅用于 ROOT

进程 *ppp*（以 UID *uuu* 运行）发出了删除 ACEE 的 VerifyCreate 请求。 仅允许与 UID 0 (root) 关联的多用户进程执行此操作。

如果应该将指定的进程作为多用户进程运行，请以 root 用户权限重新运行它。 否则，确定发出该请求的原因。

APIAUTH ! P=ppp U=uuu LoginProc 错误 nnn >description

进程 *ppp*（以 UID *uuu* 运行）请求验证用户的登录。 CA Access Control 登录验证过程失败。 请与供应商的技术支持部门联系。

APIAUTH ! P=ppp U=uuu NULL ACEE 错误 VerifyCreate (ACEEH=hhh)

标记为“服务器”的用户进程发出了创建 ACEE 的请求（很可能是在服务器进程处理访问者的登录时）。 由于以下原因之一，结果为 NULL ACEE：

- 指定的用户未在 CA Access Control 数据库中定义。
- VerifyCreate 请求的发出者未正确提供所有信息。
- 不允许指定的用户登录。

APIAUTH ! P=ppp U=uuu NULL ACEE 错误 VerifyDelete (ACEEH=hhh)

进程 *ppp*（与用户 *uuu* 关联，而且很可能标记为“服务器”进程）请求删除 ACEE 句柄 *hhh*（很可能作为处理用户注销的一部分）。 但是，没有与该句柄关联的 ACEE，因此 CA Access Control 无法删除它。

APIAUTH : P=ppp U=uuu 用 ACEEH=1 > New ACEEH=hhh 请求

进程 *ppp*（以 UID *uuu* 运行）请求访问一般资源，并提供了 ACEE 句柄 -1。 CA Access Control 使用了与请求进程关联的 ACEE 句柄。 该消息是请求访问资源的单用户进程特有的。 不需要执行任何操作。

APIAUTH ! P=ppp U=uuu VerifyCreate(ACEEH=hhh) 错误 nnn

进程 *ppp*（以 UID *uuu* 运行）向 VerifyCreate 发出了请求（以生成 ACEE）。 VerifyCreate 过程失败。 请与供应商的技术支持部门联系。

APIAUTH > P=ppp U=uuu VerifyCreate DENY (Result=[P/D/C]) string

由于以下原因之一，VerifyCreate 请求被拒绝：

- 指定的用户因不符合时间或日期规则而无法登录
- 用户无法从指定的终端工作
- 指定的密码（如果已提供）不正确
- 在随后的消息中所述的原因之一。

APIAUTH > P=ppp U=uuu VerifyCreate OK (ACEEH=hhh)!

VerifyCreate 请求被接受。 在存储器中生成了访问者环境元素 (ACEE)。 CA Access Control 返回一个 ACEE 句柄 (ACEEH) 给调用程序。 如果在 CA Access Control 中未定义指定的用户，则函数返回的 ACEEH 为 -1。

APIAUTH ! P=ppp U=uuu VerifyDelete(ACEEH=hhh) [正常 I 错误 0xerr]

进程 *ppp*（与用户 *uuu* 关联，而且很可能标记为“服务器”进程）请求删除 ACEE 句柄 *hhh*（很可能作为处理用户注销的一部分）。 VerifyDelete 请求的结果是正常或错误；如果是后者，则错误代码显示为十六进制的 err。 请使用 semsgtool 实用程序确定错误的性质。

APIAUTH > P=ppp U=uuu VerifyRequest(ACEEH=hhh, C=ccc, R=rrr, A=nnn) DENY (Result='D') 原因 ? detaileddenialreason

使用访问权限 *xxx* 访问资源 *rrr*（其类别为 *ccc*）的请求被拒绝。 如果 ACEEH 是 1，则此拒绝是基于通用访问规则。-- 如果 ACEEH 不是 -1，则此拒绝是基于与指定句柄关联的用户。 第二行提供拒绝的详细原因。

APIAUTH > P=ppp U=uuu VerifyRequest(ACEEH=hhh, C=ccc R=rrr, A=xxx) PASS

使用访问权限 *xxx* 访问资源 *rrr*（其类别为 *ccc*）的请求被接受。 如果 ACEEH 是 1（用户未被定义为 CA Access Control），访问资源的权限基于通用访问规则。-- 如果 ACEEH 不是 -1，此权限基于与指定句柄关联的用户的相关访问规则。

连接 : P=ppp U=uuu ACEEH=hhh 从 ipip:port1 到套接字 socket 6000 主机=iiii

与 UID *uuu* 关联的进程 *ppp* 发出了在主机 *iiii*（X- 终端或工作站）上打开窗口的请求。

注意：端口号始终是 6000；所有其他 TCP/IP 连接请求都被 CA Access Control 忽略。

连接 > P=ppp U=uuu 从 ipip:port1 到套接字 6000 主机=iiii BYPASS

CA Access Control 跳过 CONNECT 请求，而不解释访问规则，因为在进程 *ppp* 中执行的程序是已注册的 XDM 程序。

CONNECT > 结果: [P/D/C] P=ppp ACEEH=hhh TERM=tttWhy ? detaileddecisiontext

CONNECT 结果是 *D*（拒绝）或 *P*（允许）。 第二行提供该决定的原因。

错误 ！无法派生。 错误号 nnn。

在初始化过程中，CA Access Control 再生数次以成为后台进程。 再生请求失败，且显示指定的错误号。

如果无法确定问题的原因，请与供应商的技术支持部门联系。

错误！ 执行 CA Access Control 代理失败 ddd

引擎无法启动代理后台进程。 检查 seagent 可执行文件是否处于正确的位置（通常为 *ACInstallDir*/bin/seagent）。 如果该文件位于正确的位置，请向供应商的技术人员报告该问题。 在消息文本中，*ddd* 是 CA Access Control 尝试执行 seagent 时从操作系统收到的错误号。

错误 !获取 LOGIN 程序的内存失败错误 !获取 NFS 设备的内存失败错误 !获取 PRIV 程序的内存失败错误 !无法为 XDM 程序获取内存

这些消息表示内存严重不足。 您的计算机不符合运行 CA Access Control 的最低内存要求，或者找到了软件错误。 请与供应商的技术支持部门联系。

错误！ 无法为 PROC 表获取内存

seosd 在启动时必须扫描所有运行的进程，才能解析有关每个运行进程的所有必需信息。 seosd 无法为该目的分配内存；因此它终止执行。 这是由于内存严重不足而导致的。

错误 !注册登录程序失败: programname

在启动过程中，CA Access Control 注册要视为登录程序的所有可执行文件。 登录程序的列表在每个操作系统环境的 CA Access Control 代码中定义。

在启动过程中，指定的 *programname* 不能位于文件系统中。 CA Access Control 会忽略该程序，并继续启动。

错误 !注册特权程序失败: programname

在启动过程中，CA Access Control 注册要视为特权程序的所有可执行文件。 在启动过程中，指定的 *programname* 不能位于文件系统中。 CA Access Control 会忽略该程序，并继续启动。

特权程序的列表在每个操作系统环境的 CA Access Control 代码中定义。

错误 !注册 XDM 程序失败: programname

在启动过程中，CA Access Control 注册要视为 XDM 程序的所有可执行文件。 XDM 程序的列表在每个操作系统环境的 CA Access Control 代码中定义。

在启动过程中，指定的 *programname* 不能位于文件系统中。 CA Access Control 会忽略该程序，并继续启动。

错误 : 无 FileDb 列表可用内存

在启动过程中，seosd 无法分配内存以保存受保护文件的列表。 这很可能是由于内存严重不足。 将终止 seosd 后台进程。

错误 ！没有用于 GroupDb 列表的内存错误 ！没有用于 HostDb 列表的内存错误 ！没有用于 ServDb 列表的内存错误 ！无 UserDb 列表可用内存

这些消息表示内存严重不足。 您的计算机不符合运行 CA Access Control 的最低内存要求，或者找到了软件错误。 请与供应商的技术支持部门联系。

错误 ！ PreMatureExec 采用 FORK Child=ppp Parent=PPP

该消息指示进程 ID (*ppp*) 发出了 EXEC 系统调用，但该调用对于 seosd 是未知的。 通常，这样的消息指示尚未将“执行”请求之前的 FORK 系统调用通知 seosd。 它可能指示 UNIX 内核的 CA Access Control 扩展 SEOS_syscall 必须维护的序列化锁中有问题。

如果消息文本中的 *ppp* 是 seagent 的 pid，则可以忽略该消息。 如果多次出现该消息，请向供应商的技术支持部门报告该问题。

错误 ！P=ppp 执行失败

CA Access Control 收到了“执行”事件，但可执行文件的 inode 编号为零。 调用开头不包含 #! shell- 程序声明行的脚本文件时，会出现该消息。 不需要执行任何操作。

错误 ！ CA Access Control 文件表设置失败

seosd 试图设置文件表（包含所有 CA Access Control 受保护文件的表）；但是，SEOS_syscall 拒绝了该请求。 最有可能的原因是内核中的内存不足，或者 seosd 和 SEOS_syscall 的版本不同。 CA Access Control 文件保护无法继续正常运行。

解决版本不匹配问题（如果能够解决）。 如果一切看起来正常，请向供应商的技术支持部门报告该问题。

错误 ！seosini_ShutDown rv=errorno

CA Access Control 在关闭过程中遇到错误。 请向供应商的技术支持部门报告该错误。

错误！ 字符串太常用 'path'

试图定义文件保护的一般规则，很可能是通过 newfile 或 newres FILE 命令。 但是，指定的路径不能是一般文件访问规则。 文件规则未定义。

错误 ！未知请求: 类型:ttt Pid=ppp，Buff=bbb

CA Access Control 从其系统调用收到了一个请求，但是请求类型 *ttt* 不可识别。 这可能是由于 CA Access Control 系统调用和 seosd 之间的软件版本不匹配，或者是因为软件错误。 该请求来自进程 *ppp*，*bbb* 是请求缓冲区的打印输出。 请向供应商的技术支持部门报告该问题。

执行 : P=ppp U=uuu G=ggg (D=ddd I=iii) 程序:ProgramName [已添加到: ipaddress]

CA Access Control 已从与 UID *uuu* 和 GID *ggg* 相关联的进程 *ppp* 接收到程序执行事件。 （*ggg* 值为 -1 时表示 CA Access Control 尚未注册该进程的 GID）。 在消息文本中，*ddd* 和 *iii* 分别为文件的设备编号和 inode。 *Program-Name* 是用于调用该程序的零参数。 指定的程序是常规程序（即，不是 setuid 或 setgid）；因此，CA Access Control 允许执行该程序，而不调用数据库访问规则决定机制。 如果该进程所附加的 *ip-address* 是可提取的，则 CA Access Control 会在消息文本中报告此信息。

执行 sg: P=ppp U=uuu G=ggg (D=ddd I=iii) 程序:ProgramName[已添加到: ipaddress]

CA Access Control 已从与 UID *uuu* 和 GID *ggg* 相关联的进程 *ppp* 接收到程序执行事件。 （*ggg* 值为 -1 时表示 CA Access Control 尚未注册该进程的 GID）。 在消息文本中，*ddd* 和 *iii* 分别为文件的设备编号和 inode。 *Program-Name* 是用于调用该程序的零参数。 指定的程序是 setgid 程序；CA Access Control 通过调用数据库访问规则决定机制确定是否允许执行它。 如果该进程所附加的 *ip-address* 是可提取的，则 CA Access Control 会在消息文本中报告此信息。

EXECsu : P=ppp U=uuu G=ggg (D=ddd I=iii) 程序:ProgramName[已添加到: ipaddress]

CA Access Control 已从与 UID *uuu* 和 GID *ggg* 相关联的进程 *ppp* 接收到程序执行事件。 （*ggg* 值为 -1 时表示 CA Access Control 尚未注册该进程的 GID）。 在消息文本中，*ddd* 和 *iii* 分别为文件的设备编号和 inode。 *Program-Name* 是用于调用该程序的零参数。 指定的程序是 setuid 程序；CA Access Control 通过调用数据库访问规则决定机制确定是否允许执行它。 如果该进程所附加的 *ip-address* 是可提取的，则 CA Access Control 会在消息文本中报告此信息。

EXECsusg: P=ppp U=uuu G=ggg (D=ddd I=iii) 程序:ProgramName[已添加到: ipaddress]

CA Access Control 已从与 UID *uuu* 和 GID *ggg* 相关联的进程 *ppp* 接收到程序执行事件。（*ggg* 值为 -1 时表示 CA Access Control 尚未注册该进程的 GID）。 在消息文本中，*ddd* 和 *iii* 分别为文件的设备编号和 inode。 *Program-Name* 是用于调用该程序的零参数。 指定的程序是 setuid 和 setgid 程序；CA Access Control 通过调用数据库访问规则决定机制确定是否允许执行它。 如果该进程所附加的 *ip-address* 是可提取的，则 CA Access Control 会在消息文本中报告此信息。

执行 > P=ppp U=uuu (R=rrr E=eee S=sss) 到 (E=EEE) BYPASS

虽然程序是 setuid、setgid 或这两者，而且其执行应该调用了访问规则决定机制，但是 CA Access Control 跳过该检查，因为文件 *EEE* 的所有者与当前有效的 UID (*eee*) 相同。 程序执行时无法更改进程权限的范围。 如果程序在数据库中定义为受托程序，而且被修改或以其他方式篡改，则不允许执行该程序。

EXEC > 结果: 'R' [stage=sss gstag=ggg ACEEH=hhh rv=rc]原因? DetailedDecisiontext

CA Access Control 检查执行程序的用户的权限以及结果 *R*，其中 *R* 是 D（拒绝）或 P（允许）。 阶段 *sss* 和授权阶段 *ggg* 表明结果由决策流的哪个阶段决定。- ACEE 句柄 *hhh* 用作程序的访问者。 如果结果是“C”（检查），则表示 CA Access Control 没有作出决定，很可能是因为软件错误，请与供应商的技术支持部门联系，并向他们提供返回值 *rc*。 *Detailed-Decision-text* 是阶段和授权阶段的文本说明。- 如果结果是 *P*，则成功执行了程序。 如果结果是 *D*，则将不执行程序，而且用户会收到拒绝授予权限的消息。

EXECARGS: 'execution arguments'

由于 EXEC 系统调用，CA Access Control 显示已执行的命令行及传递给它的所有参数。

退出 : 正在关闭...

CA Access Control 启动关闭进程，并禁用系统调用的拦截。

致命 ！位于 seosrt_InitDatabase (nnn) 层 = nnn 阶段 = nnn 返回代码 = 0xnnn

CA Access Control 无法初始化数据库 I/O 例程。 可能的原因如下：

- 目录中没有由 seos.ini 文件中的 dbdir 标记所标识的 CA Access Control 数据库。
- 调用 CA Access Control 的用户不是 root 用户。
- 数据库已损坏。

如果无法纠正问题，请与供应商的技术支持部门联系。

文件 ：P=ppp U=uuu (D=dev I=inode) acc ：pathname

与用户 id *uuu* 关联的进程 *ppp* 试图访问 CA Access Control 受保护文件。 在消息文本中，*dev* 和 *inode* 分别是所访问文件的设备和 inode；*acc* 是访问模式（例如读取、写入等）；*pathname* 是所访问文件的真实路径名。

FILE > 结果仅 'D' CA Access Control 文件 'filename'

文件访问请求的结果是 D（拒绝），因为只有 CA Access Control 可以访问该文件。 即使访问规则允许访问，CA Access Control 也会被硬编码为拒绝对此文件进行访问。-

FILE > 结果: 'R' [stage=sss gstag=gs ACEEH=hhh rv=rv (recordname)原因? detailedreasontext

文件访问请求的结果 R 是 D（拒绝）或 P（允许）。 阶段 *sss* 和授权阶段 *gs* 被映射到第二行的文本字符串原因（在“原因？”后面）。- 在消息文本中，*hhh* 是与请求的访问者关联的访问者句柄，*record-name* 是触发了拒绝或允许访问决策的访问规则记录的名称。

派生 ：P=ppp U=uuu G=ggg 子进程=cppp 程序:ProgramName

CA Access Control 截获了与 UID *uuu* 和 GID *ggg* 关联的进程 *ppp* 发出的再生请求。 子进程 id 是 *cppp*。 *Program-Name* 是在父进程中运行的程序（最初也在子进程中运行）。 CA Access Control 从不拒绝再生请求，而是始终接受它。 fork 系统调用的变体（如 vfork 和 kfork）也将报告为再生请求。

GETCRED : P=ppp，按传票获取证书

这是一条仅供参考性的消息，它表明 *ppp*（通常为策略模型后台进程 sepmdd 的进程 ID）请求了特定票证持有者（请求 sepmdd 的服务的客户端进程）的凭据。- 有关详细信息，请参阅本附录中对 GTICKET 的说明以及“实用程序详述”一章中对 sepmdd 的说明。

GPEERNAM: P=ppp, ADDR=addr, N=desc

CA Access Control 截获了 getpeername() 系统调用以验证哪个 IP 地址与当前进程相关联。 始终接受该系统调用。 在消息文本中，*ppp* 是发出 getpeername() 调用的进程 id，*addr* 是与套接字描述符 *desc* 相关联的 IP 地址。

GTICKET: P=ppp，获取身份验证传票

这是一条仅供参考性的消息，它表明 *ppp* 请求 seosd 为其发出身份验证票单。- 每当策略模型客户端 sepmd 与 sepmdd 进行通讯时，服务器都会通过传递的票证验证客户端的身份。 客户端使用套接字通讯将获取的票证发送到服务器。 然后，服务器将该票证传递到 seosd，以通过 GETCRED 请求获取票证持有者的凭据。 这样，sepmdd 确保了请求服务的客户端的身份。

INET : P=ppp，从 ipaddress:localport 到端口 portnumber

CA Access Control 截获了由请求 TCP/IP 服务 *port-number* 的远程 *ip-address* 所发出的传入 Internet 接受请求。

INET > 结果: 'R' ipaddr>locport, stg=stage gtsg=gstage 原因？ DetailedReasonText

Internet 请求的结果 *R* 是 P（允许）或 D（拒绝）。 在消息文本中，*ip_addr* 是请求的 IP 地址。 *Detailed-Reason-Text* 是文本说明，它指示决策流中最终做出拒绝或允许请求主机的 TCP/IP 服务的决策的阶段及授权阶段。

信息 : 由于文件系统空间 (space) 过小，自动禁止跟踪

当跟踪文件所驻留的文件系统中剩余的可用空间量低于 seos.ini 文件中 trace_space_saver 标记指定的阈值时，跟踪工具将自动禁用它自身。 在消息文本中，*space* 是文件系统中剩余的可用空间量。

信息 : 无法提取文件系统可用空间 (errno=err)

跟踪工具的“自动禁用”功能无法确定文件系统中的可用空间量。 在消息文本中，*err* 是从 UNIX statfs() 调用收到的错误编号（整数）。 请向供应商的技术支持部门报告该问题。

信息 : 数据库查询

seosd 后台进程收到了从 CA Access Control 数据库提取信息的请求。

信息 : 数据库请求

seosd 后台进程收到了修改或查询 CA Access Control 数据库中数据的请求。

信息 : 筛选掩码: 'mask' 已注册

seosd 后台进程注册从 trcfilter.init 文件读取的每个筛选掩码，以免将与掩码匹配的消息发送到跟踪文件。

信息 : GroupList 已注册 nnn 个条目

当 seosd 在 NIS 服务器下运行时，启动时它将缓存（/etc/group 和 NIS 映射中的）所有组条目，以便 seosd 可以实现 GID 到组名的转换，而不调用 ypserv 进程和 TCP/IP 请求。 该消息还指示将 seos.ini 中的 under_NIS_server 标记设置为 YES。 如果正在运行 CA Access Control 的工作站不是 NIS 服务器，请将 under_NIS_server 标记设置为 NO。在消息文本中，*nnn* 是已缓存的组条目数。

信息 : HostList 已注册 nnn 个条目

启动时 seosd 后台进程将缓存 /etc/hosts 中的所有条目。 在消息文本中，*nnn* 是已缓存的主机条目数。

信息 : 登录程序: programname 已注册

seosd 后台进程必须识别用户登录到系统所用的所有程序。 CA Access Control 将登录程序调用的 setuid 系统调用视为登录请求，而不是视为 setuid 请求。 在消息文本中，*programname* 是已注册的登录程序的完整路径。 seosd 后台进程在内部从 CA Access Control 启动代码获取登录程序的名称。

信息 : NFS 主要设备已注册，nnn 个条目

Watchdog 为受托程序执行的检查包括检查文件所驻留的设备的设备编号。 如果文件位于 NFS 挂接文件系统（尤其是自动挂接的文件系统），那么这种检查可能会导致错误，因为这种文件系统的设备编号在启动之后可能会改变。- 因此，CA Access Control 会注册 NFS 文件系统的主设备编号，这样它们可以忽略不稳定的次要设备编号。- CA Access Control 具有每个环境中 NFS 挂接文件系统的主设备编号列表。 如果您的安装使用 CA Access Control 无法识别的网络挂接文件系统，请与供应商的技术支持部门联系，以了解有关向列表中添加主设备编号的说明。 在消息文本中，*nnn* 是注册为 NFS 挂接文件系统的主设备编号的数目。

信息 : P=ppp 已结束

进程 *ppp* 已结束。 seosd 断开该进程号与其 ACEE（访问者环境元素）的关联。 如果进程 *ppp* 是与其 ACEE 关联的最后一个进程（即，没有其他父进程或子进程使用同一环境），则将从存储器中删除该 ACEE。 在进程终止后不会立即发出该消息；仅当 CA Access Control 执行某些“垃圾回收操作”以重用其内部表中的进程条目时，才会发出它。

信息 : P=ppp 执行失败

该消息指示进程 *ppp* 无法执行最后一个 EXEC 系统调用，因为 UNIX 拒绝该请求（在 CA Access Control 允许执行之后）。 因此，CA Access Control 还原与该进程相关联的以前可执行文件的值，因为此程序以该进程 ID 运行。 在大多数情况下，进程将终止。 这不一定是一个错误，您不必采取任何特殊操作。 但是，您应该使用 UNIX 工具查处执行失败的原因。 在大多数情况下，原因是 shell 脚本在第一行中没有“#!/bin/sh”标头。

信息 : P=ppp 未知 TTY 类型 typename

seosd 后台进程无法确定进程 *ppp* 使用的是真实 TTY 还是虚假 TTY。 请与供应商的技术支持部门联系。

信息 : 特权程序: programname 已注册

seosd 后台进程注册了几个特权程序。 允许此类程序对任何用户执行 setuid 操作，而不检查 SURROGATE 类。 当前，您只能使 /bin/sendmail 成为特权程序（由于其流要求）。 您必须使该列表尽可能小；建议 seoswd 监视所有特权程序以确保它们仍然是受托程序。 在消息文本中，*programname* 是已注册程序的完整路径。

信息 : 受限文件表已设置 nnn 个条目

在启动过程中，seosd 找到了 CA Access Control 受保护文件的 *nnn* 个条目，并成功将该列表传递到 UNIX 内核的 CA Access Control 扩展。 这是一条仅供参考性的消息。-

信息 : SEOS_syscall 取消注册 rc=nnn

在关闭过程中，seosd 在内核中取消注册它自己，以便它可以再次启动。 在消息文本中，*nnn* 是返回代码，它应该为零。 如果返回代码不为零，请向供应商的技术支持部门报告该问题。

信息 : ServList 已注册 nnn 个条目

启动时 seosd 后台进程将缓存 /etc/services 中的所有条目。 在消息文本中，*nnn* 是已缓存的主机条目数。

信息 : ServList 已注册 nnn 个 portmapper 条目

在启动时，seosd 注册由 portmapper 解析的 nnn 个 TCP/IP 服务。 这是一条仅供参考性的消息。-

信息 : 设置站点

seagent 后台进程（负责与其他 CA Access Control 工作站进行通讯的 CA Access Control 后台进程）从远程工作站向 seosd 发送了连接请求。

信息 : 设置 PV C=ccc O=ooo P=ppp

seoswd 后台进程在类 *ccc* 的对象 ooo 中设置属性 ppp 的值。

信息 : UserList 已注册 nnn 个条目

当 seosd 在 NIS 服务器下运行时，启动时它将缓存（/etc/passwd 和 NIS 映射中的）所有用户条目，以便 seosd 可以实现 UID 到用户名的转换，而不调用 ypserv 进程和 TCP/IP 请求。 该消息还指示将 seos.ini 中的 under_NIS_server 标记设置为 YES。 如果运行 CA Access Control 的计算机不是 NIS 服务器，请将 seos.ini 中的 under_NIS_server 标记设置为 NO。 在消息文本中，*nnn* 是已缓存的用户条目数。

信息 : XDM 程序: programname 已注册

XDM 程序是指在 X 终端显示用户 ID 和密码框的程序。- XDM 程序以 *superuser* 运行，此身份通常无法在 X 终端打开窗口。- 但是，XDM 程序必须在 X 终端上打开一个窗口，以便显示一个供用户指定用户 ID 和密码的方框。- 因此，如果发出 CONNECT 请求的程序是已注册的 XDM 程序，则 seosd 将跳过终端检查。

终止 : P=ppp U=uuu 终止 [进程 I 所有例外] (nn): (proclist)

与用户 *uuu* 相关联的进程 *ppp* 试图终止在 *proclist* 中列出的所有进程（或除列表中进程之外的所有进程）。 在消息文本中，*nn* 是目标进程数。

KILL > 结果 'R' [stage=sss gstag=gs rv=rr] ACEEH=hhh 原因? detailedreasontext

终止事件的结果 R 是 D（拒绝）或 P（允许）。 在消息文本中，*sss*、*gs* 和 *rr* 是阶段、授权阶段和 CA Access Control 决策例程的返回值，*hhh* 是与终止事件相关联的访问者句柄。 *detailed-reason-text* 显示在第二行，派生自阶段和授权阶段代码。

登录 : P=ppp 用户=uuu 终端=ttt

seosd 后台进程截获了在终端 *ttt* 上以进程号 *ppp* 工作的用户 *uuu* 发出的登录请求。 该消息应后跟登录结果消息。

LOGIN > 结果: 'R' [stage=stage gstag=gstage rv=nnn] ACEEH=hhh[原因 ?detaileddenialreason]

登录请求的结果 R 是 D（拒绝）或 P（允许）。 在消息文本中，*stage* 和 *gstage* 是指示 CA Access Control 流中做出允许或拒绝登录请求的决策的阶段的编号。 如果允许登录，则 *hhh* 是此时与发出进程相关联的 ACEEACEE 句柄。 如果拒绝登录，则 *hhh* 被设置为 -1，并且 *detailed-denial-reason* 会显示在第二行。 如果 *detailed-denial-reason* 与资源访问相关（例如：“没有授予资源访问权限的规则”），则所涉及的资源是用户从中发出了登录请求的终端。

LOGIN > 结果: 'D' 登录已针对 ALL 禁用

登录请求被拒绝，因为所有用户的登录当前被禁用。

LOGIN > 结果: 'D' 登录已针对 U=uuu 禁用

登录请求被拒绝，因为特定用户的登录当前被禁用。 可能可能是因为该用户已经登录。

消息 : string

控制台请求将标记消息置于跟踪文件中。

NEWPASS : 设置新密码

sepass 实用程序要求为用户 ID 设置新密码。

PW_ATTCK: P=ppp 在 sss 秒内从终端进行了 nnn 次尝试

seosd 后台进程检测到进程 *ppp*（它正在运行已注册的登录程序之一）进行了 *nnn* 次尝试以指定用户/密码组合，但没有成功。 CA Access Control 断定密码猜测攻击源自消息文本中指定的终端，并将审核记录写入 CA Access Control 审核文件。 PWATTACK 审核记录可以通过日志传递后台进程（selogrcd 和 selogrd）触发操作。

重新启动 : Watchdog (P=ppp) 重新启动 DBSERV

seoswd 后台进程已经重新启动 seosd。 在消息文本中，*ppp* 是 seosd 的进程 ID。

SCONSOLE: UID: uuu 的登录被禁用

CA Access Control 控制台实用程序 secons 发出了禁用用户 id *uuu* 的登录请求的请求。 从此时起，将拒绝指定用户 id 的登录请求。

SCONSOLE: U=uuu 的登录已被禁用

secons 实用程序发出了禁用用户 id *uuu* 的登录请求的请求。 但是，该用户 id 的登录已被禁用。

SCONSOLE: U=uuu 的登录未被禁用

secons 实用程序发出了重新启用用户 ID *uuu* 的登录的请求。- 但是，该用户 id 的登录已被启用。

SCONSOLE: 登录现在已禁用

secons 实用程序发出了禁用所有用户的登录请求。 从此时起，将拒绝所有用户的登录请求。

SCONSOLE: 登录被启用

secons 实用程序发出了重新启用所有用户的登录的请求。- 从此时起，将允许登录请求。

SCONSOLE: U=uuu 的登录被再次启用

secons 实用程序发出了重新启用指定用户的登录的请求。- 从此时起，将允许该特定用户的登录请求。

SCONSOLE: 禁用的登录表中无更多空间

secons 实用程序发出了禁用特定用户的登录请求。 但是，登录禁用表已满。 请与供应商的技术支持部门联系。

SCONSOLE: 操作中不允许 U=uuu

没有 OPERATIONS 属性的用户试图使用不允许非 OPERATIONS 用户使用的 secons 开关参数之一。-

SCONSOLE: 不允许使用 U=uuu 禁用 U=uuu2 的登录

用户 *uuu* 尝试通过 secons 禁用用户 *uuu2* 的登录。 但是，仅允许 root 用户和用户 *uuu2* 禁用 *uuu2* 的登录。

SCONSOLE: 不允许使用 U=uuu 再次启用 U=uuu2 的登录

用户 *uuu* 尝试通过 secons 重新启用用户 *uuu2* 的登录。- 但是，仅允许 root 用户和用户 *uuu2* 重新启用 *uuu2* 用户的登录-。

SETGRPS : P=ppp 到 grouplist

进程 *ppp* 为在 grouplist 中指定的组发出了 setgroups 系统调用。

SGID : P=ppp U=uuu G=ggg 到 GGG (GROUP.groupname) ACEEH=hhh D=devnum I=inode

使用 UID *uuu* 和 GID *ggg* 的权限运行的进程 *ppp* 为 GID *GGG* 发出了 setgid 系统调用。 CA Access Control 使用 SURROGATE 类和 GROUP.*groupname* 对象检查该进程的权限，并将 *hhh* 用作请求的访问者句柄。 在消息文本中，*devnum* 和 *inode* 分别是发出系统调用的程序的设备和 inode。 该消息应后跟“SGID 结果”消息。

SGID > P=ppp U=uuu (RG=rg EG=eg SG=sg) 到 (RG=trg EG=teg SG=tsg) () BYPASS

CA Access Control 接受了 setgid 请求，而不检查任何 SURROGATE 访问规则。 在消息文本中，*ppp* 是发出请求的进程 id；*uuu* 是与该进程相关联的用户 id；*rg*、*eg* 和 *sg* 分别是该进程的真实有效且已保存的 GID；*trg*、*teg* 和 *tsg* 分别是发出 setgid 请求所使用的有效真实且已保存的目标 GID。 跳过的原因通常是因为当前的真实或已保存 GID 与目标 GID 相同，因此 setgid 请求不会更改用户的安全范围。

SGID > 结果: 'R' [stage=stage gstag=gstage ACEEH=hhh]原因? detailedreasontext

CA Access Control 根据 SURROGATE 访问规则检查了 setgid 请求，结果 R 是 P（允许）或 D（拒绝）。 已代表访问者句柄 *hhh* 做出决定。 在消息文本中，*detailed-reason-text* 是拒绝或授权的原因。

SHUTDOWN! 请求被拒绝。 不允许 U=uuu SHUTDOWN 该服务器

用户 *id* uuu 尝试使用 secons 关闭 seosd；但是，该用户的配置文件不包含 OPERATIONS 属性。 因此请求被拒绝。

SHUTDOWN: 服务器正在根据 operator 的请求关闭

在授权操作员发出请求后，seosd 后台进程开始关闭。

SHUTDOWN: 正在终止 CA Access Control 后台进程 daemonname P=ppp RV=nnn

CA Access Control 在其关闭过程中终止了其后台进程 *ppp*；CA Access Control 还将关闭 seoswd 和 seagent。

STARTUP: CA Access Control 后台进程 PID=ppp

启动了 *seosd* 后台进程；其进程 ID 是 ppp。

数据流 c: P=ppp 关闭数据流 Id=iii

进程 *ppp* 关闭了数据流 ID 为 *iii* 的数据流。 CA Access Control 可跟踪所有数据流打开和数据流关闭操作，以便稍后在代表特定数据流 ID 处理 TCP/IP 请求时确定拥有该数据流的进程 ID。---

数据流 o: P=ppp 打开数据流 Id=iii

进程 *ppp* 打开了数据流 ID 为 *iii* 的数据流。 CA Access Control 可跟踪所有数据流打开和数据流关闭操作，以便稍后在代表特定数据流 ID 处理 TCP/IP 请求时确定拥有该数据流的进程 ID。---

SUID > P=ppp U=uuu (R=r E=e S=s) 到 (R=tr E=te S=ts) (reason) BYPASS

CA Access Control 接受了 setuid 请求，而不检查任何 SURROGATE 访问规则。 在消息文本中，*ppp* 是发出请求的进程 id；*uuu* 是与该进程相关联的用户 id；*r*、*e* 和 *s* 分别是进程 *ppp* 的真实有效且已保存的 GID；*tr*、*te* 和 *ts* 分别是发出 setgid 请求所使用的有效真实且已保存的目标 GID。 跳过的原因通常是因为当前的真实或已保存 UID 与目标 UID 相同，因此 setuid 请求不会更改用户的安全范围。 其他可能原因是发出 setuid 系统调用的程序是特权程序（在这种情况下 *reason* 是 For Priv），或者发出系统调用的程序是在实际登录前后数次切换 UID 的登录程序（在这种情况下 *reason* 被指定为 For Login）。

SUID : P=ppp U=uuu (R=r E=e S=s) 到 USER.username (R=tr E=te S=ts)D=devnum I=inode

使用用户 id *uuu* 的权限运行的进程 *ppp* 发出了 setuid 系统调用，以便将当前的真实有效且已保存的 UID 更改为 UID *uuu*。 CA Access Control 使用 SURROGATE 类和 USER.*usernam* 对象检查该进程的权限，并将 hhh 用作请求的访问者句柄。 在消息文本中，*devnum* 和 *inode* 分别是发出系统调用的程序的设备和 inode。 该消息应后跟“SUID 结果”消息。

SUID > 结果: 'R' [stage=stage gstag=gstage ACEEH=hhh rv=rv]原因? detailedreasontext

CA Access Control 根据 SURROGATE 访问规则检查了 setuid 请求，结果 R 是 P（允许）或 D（拒绝）。 已代表访问者句柄 *hhh* 做出决定。 在消息文本中，*detailed-reason-text* 是拒绝或授权的原因。

VERPASS : 验证密码

CA Access Control 收到了验证用户密码有效性的请求。

WAKE_UP : 服务器即启动

seosd 后台进程开始初始化。

警告: 取消关联 P=ppp ACEEH=hhh

CA Access Control 为任何再生请求在进程和访问者句柄 (ACEEH) 之间建立关联。 该消息指示无法执行此关联，原因可能是句柄 *hhh* 为 -1 或者 *hhh* 不是有效的访问者句柄。 对于后一种情况，请与供应商的技术支持部门联系。

警告：无法验证 P=ppp

该消息的前面是“未知 P=”消息，后者指示未知进程发出的再生请求。 CA Access Control 试图确定是哪个用户使 UNIX 与该用户相关联。 该验证任务无法完成。 可能原因是进程已经终止。 如果不是这样，请与供应商的技术支持部门联系。

警告: 取消关联 P=ppp ACEEH=hhh

CA Access Control 为已终止的任何进程取消进程和访问者句柄 (ACEEH) 之间的关联。 该消息指示无法执行取消关联，原因可能是句柄 *hhh* 为 -1 或者 *hhh* 不是以有效的访问者句柄形式存在。 对于后一种情况，请向供应商的技术支持部门报告该问题。

警告: 具有 P=ppp 的条目的 ExecArg 非空

当 CA Access Control 找到系统不知道的、且其执行程序未知的新进程时，将出现该警告。 在大多数情况下，您可以忽略该消息。 如果系统未产生预期的结果，请与供应商的技术支持部门联系。

警告: 无法获取 P=ppp 的 ACEEH

CA Access Control 被请求检查进程 *ppp* 的权限，但是没有该进程的有效访问者句柄。 在大多数情况下，原因是：与该进程相关联的用户不是 CA Access Control 定义的用户，或者该进程对 CA Access Control 系统是未知的。 在这两种情况下，CA Access Control 仅授予该进程通用访问权限。 如果系统未产生预期的结果，请与供应商的技术支持部门联系。

警告: P=0 的登录???

在除 AIX 之外的系统中的启动期间出现该消息时，可以忽略它。 如果在正常工作过程中（在 seosd 启动并正常工作后），或者在 AIX 下启动期间出现该消息，则表明存在软件错误，在这种情况下，您应该与供应商的技术支持部门联系。

警告: CA Access Control 终止 P=ppp 失败，原因=nnn

作为一种警告措施，CA Access Control 终止尝试获取可能产生漏洞的敏感权限的进程。 这种事件可能是在未经许可的情况下尝试替代 UID（setuid 系统调用）。- CA Access Control 试图终止违规进程，但无法终止它。 失败的原因在 kill 系统调用返回的原因代码中详述。

警告: 具有 P=ppp 的条目的终端非空

当 CA Access Control 发现系统不知道的、且其执行程序未知的新进程时，将出现该警告。 在大多数情况下，您可以忽略该消息。 如果系统未产生预期的结果，请与供应商的技术支持部门联系。

警告: 未知 P=ppp

该消息指示 CA Access Control 未知的进程发出了再生请求。 如果在启动过程中 seoswd 或 seagent 出现该消息，则可以忽略它。 在其他情况下，它会指示软件错误，因为 CA Access Control 无法验证该进程的实际权限。 对于后一种情况，请与供应商的技术支持部门联系。

WATCHDOG: 询问我是否在此 (AYT)

seoswd 后台进程尝试验证 seosd 是否处于活动状态并给出预期响应。 在消息文本中，AYT 是 seoswd 的“您是否在那里”质询。 您可以并且应该忽略该消息；使用 trcfilter.init 文件筛选出该消息。 该消息指示 seoswd 的正常行为。

WATCHDOG: 初始化 initializationtext

这是 seoswd 初始化消息，您可以忽略它。

WATCHDOG: 日志 logtext

seoswd 后台进程发出了日志请求。 日志请求详细记录在 *log-text* 中。

WATCHDOG: SecFile 操作结果

seoswd 后台进程请求该后台进程提取有关受保护文件的信息。 在消息文本中，*operation* 可以是 GETFIRST 或 GETNEXT；如果提取了这样的信息，则结果可以是 OK；如果在 CA Access Control 数据库中没有更多的受保护文件，则结果是 NOFOUND。 该消息表示扫描受保护文件的正常 seoswd 行为。

WATCHDOG: 计时器

seoswd 后台进程每隔几秒（在 seos.ini 文件中设置）就发出一个计时器请求。 您可以并且应该使用 trcfilter.init 文件筛选出该消息。

WATCHDOG: 信任程序: programname [OK I NOTOK]

seoswd 后台进程将指定程序标记为受托程序。 这表示指定程序通过了数字签名测试。 在消息文本中，OK 指示托管操作已成功完成，而 NOTOK 指示 seoswd 无法将程序标记为受托。 显示 NOTOK 的原因很可能是数据库已损坏，在这种情况下，您应该与供应商的技术支持部门联系。

WATCHDOG: 取消对程序: programname 的信任 [OK I NOTOK]

seoswd 后台进程将指定程序标记为取消受托。 这表示指定程序没有通过 seoswd 的数字签名检查。 在消息文本中，OK 指示托管操作已成功完成，而 NOTOK 指示 seoswd 无法将程序标记为取消受托。 显示 NOTOK 的原因很可能是数据库已损坏，在这种情况下，您应该与供应商的技术支持部门联系。

附录 C： 字符串匹配

此部分包含以下主题：

通配符表达式

本节说明可以用来生成通配符表达式的语法。

CA Access Control 使用通配符匹配和字符列表执行字符串匹配（文件名替换）。

通配符匹配

CA Access Control 支持下列通配符字符：

字符	匹配
*（星号）	零个或更多字符的任何序列。
?（问号）	任何单个字符。

字符列表

由方括号 ([ ]) 括起来的字符列表可以包含一个或多个字符。 CA Access Control 将这些字符用作肯定的或否定的匹配条件。

字符列表可以由一个或多个字符组成。 对于该类型的列表，CA Access Control 匹配列表中的任何单个字符。 如果方括号内的列表前面有脱字号 (^)，则 CA Access Control 将匹配*不*在列表中的任何单个字符。

范围是指定字符范围的字符列表类型。 CA Access Control 匹配列表中的所有字符（包括第一个字符和最后一个字符）。 如果列表前面有脱字号 (^)，则 CA Access Control 排除指定列表中的所有字符。 您可以同时指定范围的第一个字符和最后一个字符，或仅指定它的第一个字符或最后一个字符。

下表说明可以使用的字符列表。 请记住，在该语法中包含方括号。 表达式 *ch1*、*ch2* 和 *chN* 都代表单个字符。

列表	说明
[*ch1ch2...chN*]	CA Access Control 匹配由方括号括起来的列表中的任何单个字符。
[^*ch1ch2...chN*]	CA Access Control 匹配*不*在方括号括起来的列表中的任何单个字符。
[*ch1-ch2*]	CA Access Control 匹配范围中的任何单个字符（包括第一个字符和最后一个字符）。
[^*ch1-ch2*]	CA Access Control 匹配*不在*范围（包括第一个字符和最后一个字符）中的任何单个字符。
[-*ch2*]	CA Access Control 匹配 ASCII 值小于或等于指定字符 (*ch2*) 的任何单个字符。
[^-*ch2*]	CA Access Control 匹配 ASCII 值等于或大于指定字符 (*ch2*) 的任何单个字符。
[*ch1*-]	CA Access Control 匹配 ASCII 值等于或大于指定字符 (*ch1*) 的任何单个字符。
[^*ch1*-]	CA Access Control 匹配 ASCII 值等于或小于指定字符 (*ch1*) 的任何单个字符。

示例：通配符匹配

要使单个字符成为与任何其他单个字符匹配的“通配”字符，请使用问号 (?)：

指定	可以匹配
mmc?	mmc3、mmcx、mmc5
mmc?.t	mmc1.t、mmc2.t
mmc04.?	mmc04.a、mmc04.1

要匹配包含零个或更多字符的任何字符串，请使用星号 (*)：

指定	可以匹配
i.c	main.c、list.c 等等

指定	可以匹配
st*.h	stdio.h、stdlib.h、string.h 等等
*	指定类的所有记录

要匹配列表中的任何字符，请参照以下示例之一：

指定	可以匹配
[abcgk]	a、b、c、g 或 k
[^abcgk]	除 a、b、c、g 或 k 之外的任何字符，如 A、B、d、e、f 或 @。
[a-z]	a 和 z 之间的任何字符（包括 a 和 z）。
[^a-z]	ASCII 值比“a”小或比“z”大的任何字符。
[Z-]	ASCII 值比 Z 大的任何字符，如 a、b、\ 或 ~。
[^-A]	ASCII 值*不*小于 A 的任何字符，如 B、a、c 或 ~。

附录 D： 使用的端口

此部分包含以下主题：

UNIX 使用的端口

在 UNIX 上，CA Access Control 在默认情况下使用下列 TCP 端口：

数值	说明	侦听器	发件人	备注
8891	CA Access Control 客户端应用程序	CA Access Control 代理	dbmgr（seosd 运行时）、devcalc、dmsmgr、policydeploy、policyreport、sechkey（管理远程计算机时）、secons、segrace、segracex、seini（管理远程计算机时）、selang（seosd 运行时）、senable、sepass、sereport、seretrust、serevu、sesu、sesudo、sewhoami、sepmdd (PMD)	您可以通过修改 /etc/services 文件设置来更改默认端口号。 要完成此操作，请添加以下行，然后重新启动 CA Access Control 后台进程： `seoslang2 port-number/tcp`
5249	SSL 通讯	CA Access Control 代理	**注意：**有关哪些组件提供符合 FIPS 的通讯的信息，请参阅*《版本说明》*。	符合 FIPS 140-2

数值	说明	侦听器	发件人	备注
8892	从远程计算机启动 seosd	seosload	selaod	seload 在远程计算机上加载后台进程时，远程计算机上的 inetd（内部服务后台进程）执行 rseloadd 程序。 该程序可本地执行 seload 并退出；可在该端口接收参数。 您可以通过修改 /etc/services 文件设置来更改默认端口号。 要完成此操作，请添加以下行，然后重新启动 CA Access Control 后台进程： `seosload port-number/ tcp` **注意：**该端口上的通讯不加密，因为它不发送任何敏感信息。

Windows 使用的端口

在 Windows 上，CA Access Control 在默认情况下使用下列 TCP 端口：

数值	说明	侦听器	发件人	备注
8891	CA Access Control 客户端应用程序	CA Access Control 代理	selang.exe、sepmdd.exe (PMD)、eACSigUpdate.exe、SegraceW.exe（正常登录和密码设置）、secons.exe（远程关闭和 IP 地址刷新）、policydeploy.exe、devcalc.exe、policyfetcher.exe	您可以通过修改 %SystemRoot%\drivers\etc\services 文件设置更改默认端口号。 要完成此操作，请添加以下行，然后重新启动 CA Access Control 服务： `seoslang2 port-number/tcp`
5249	SSL 通讯	CA Access Control 代理	**注意：**有关哪些组件提供符合 FIPS 的通讯的信息，请参阅*《版本说明》*。	符合 FIPS 140-2

服务器组件使用的端口

默认情况下，CA Access Control 将以下 TCP 端口用于其服务器组件：

数值	说明	侦听器	发送者
7222	报告快照	分发服务器	报告代理
7243	使用 SSL 的报告快照	分发服务器	报告代理
5248	基于 Web 的本地接口通讯	CA Access Control Web 服务	CA Access Control 端点管理、CA Access Control 企业管理

除这些端口外，还需要打开位于以下位置的端口：

- 中央数据库计算机上用于与分发服务器或 CA Access Control 企业管理 通讯的的端口（如果这些端口位于一台单独的计算机上）。
- 用于从远程计算机（默认为 8080）访问 InfoView 应用程序的报告门户 (BusinessObjects) 计算机上的端口。
- 用于从远程计算机（默认为 18080）访问基于 Web 的界面的 CA Access Control 端点管理 和 CA Access Control 企业管理 计算机上的端口。
- 安装 Oracle 数据库，用于从远程计算机（默认为 8080，对于 SSL 为 7443）访问基于 Web 的界面的计算机上的端口。
- 用于通过 CA Access Control 代理端口（默认为 8891，对于 SSL 为 5249）连接以下组件的高级策略管理服务器组件上的端口：
  - DMS 至 DH
  - DH 至 DMS
  - policyfetcher 和 devcalc 至远程服务器上的 DH

UNIX 身份验证代理 使用的端口

在 UNIX 上，UNIX 身份验证代理 在默认情况下使用下列 TCP 端口：

号	说明	侦听器	发送者
88	Kerberos 流量	Active Directory	UNIX 身份验证代理
389	Kerberized LDAP	Active Directory	UNIX 身份验证代理

号	说明	侦听器	发送者
445	Microsoft 目录服务	Active Directory	UNIX 身份验证代理
464	Kerberos kpasswd	Active Directory	UNIX 身份验证代理
3268	全局目录	Active Directory	UNIX 身份验证代理
7222	报告快照	分发服务器	报告代理
7243	使用 SSL 报告快照	分发服务器	报告代理

在 UNIX 上，UNIX 身份验证代理 在默认情况下使用下列 UDP：

号	说明	侦听器	发送者
53	DNS	Active Directory	UNIX 身份验证代理
88	Kerberos 流量	Active Directory	UNIX 身份验证代理
123	NTP	Active Directory	UNIX 身份验证代理
389	Kerberized LDAP	Active Directory	UNIX 身份验证代理
464	Kerberos kpasswd	Active Directory	UNIX 身份验证代理

附录 E： 报告数据库模式

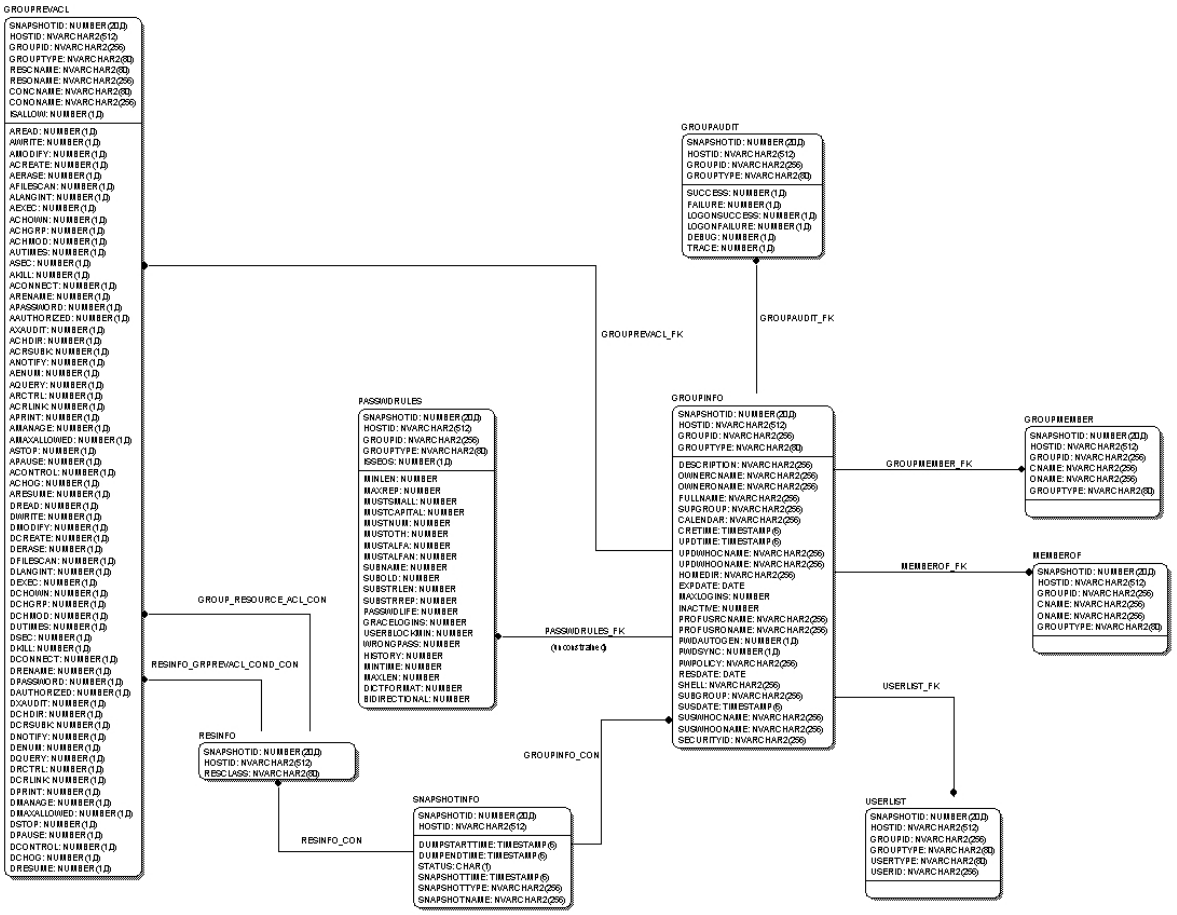
此部分包含以下主题：

模式图解

下面的主题对 CA Access Control 报告数据库模式进行了图解说明。

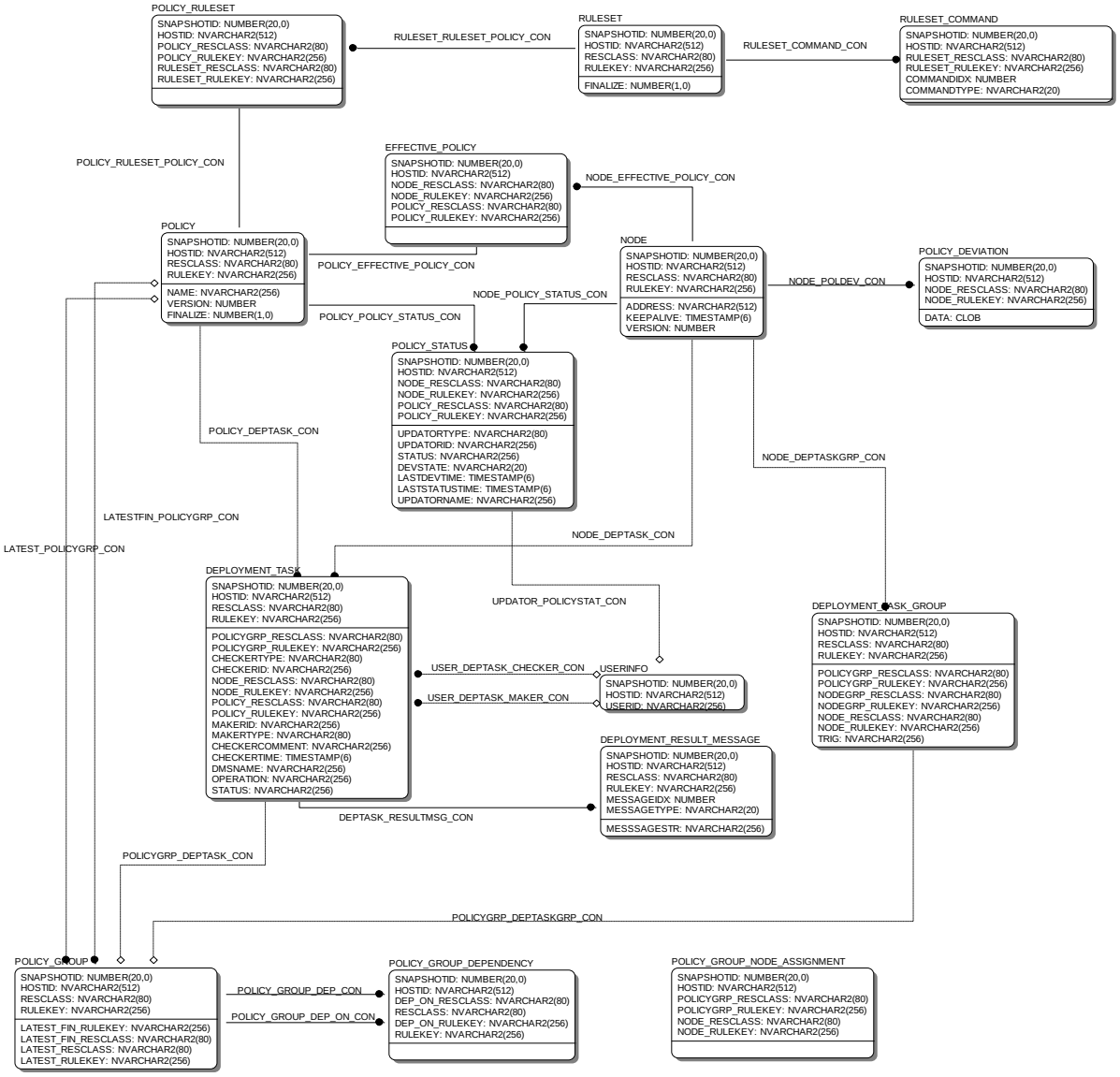
组

这是组相关表格的图解：



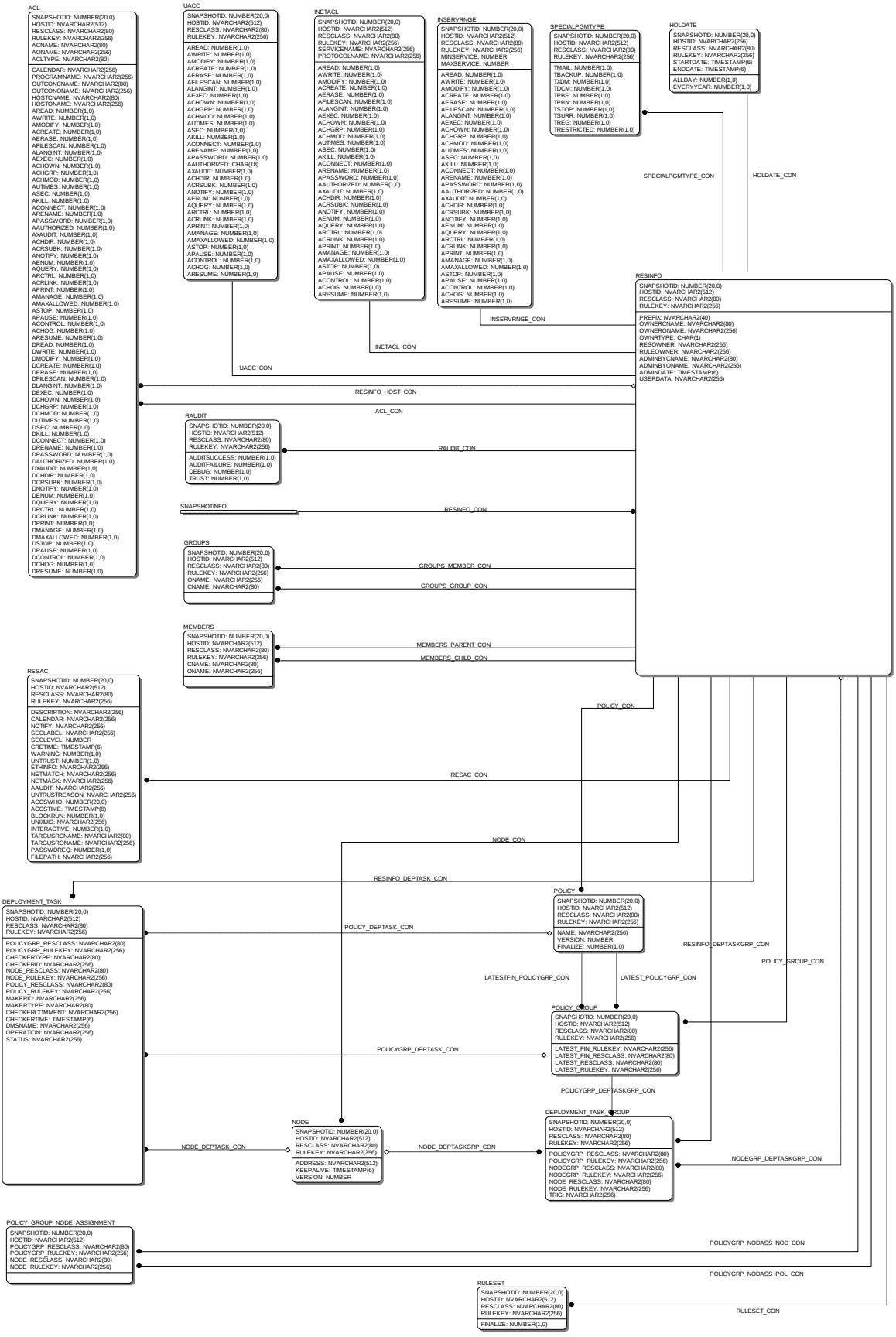
策略管理

这是策略管理相关表格的图解：



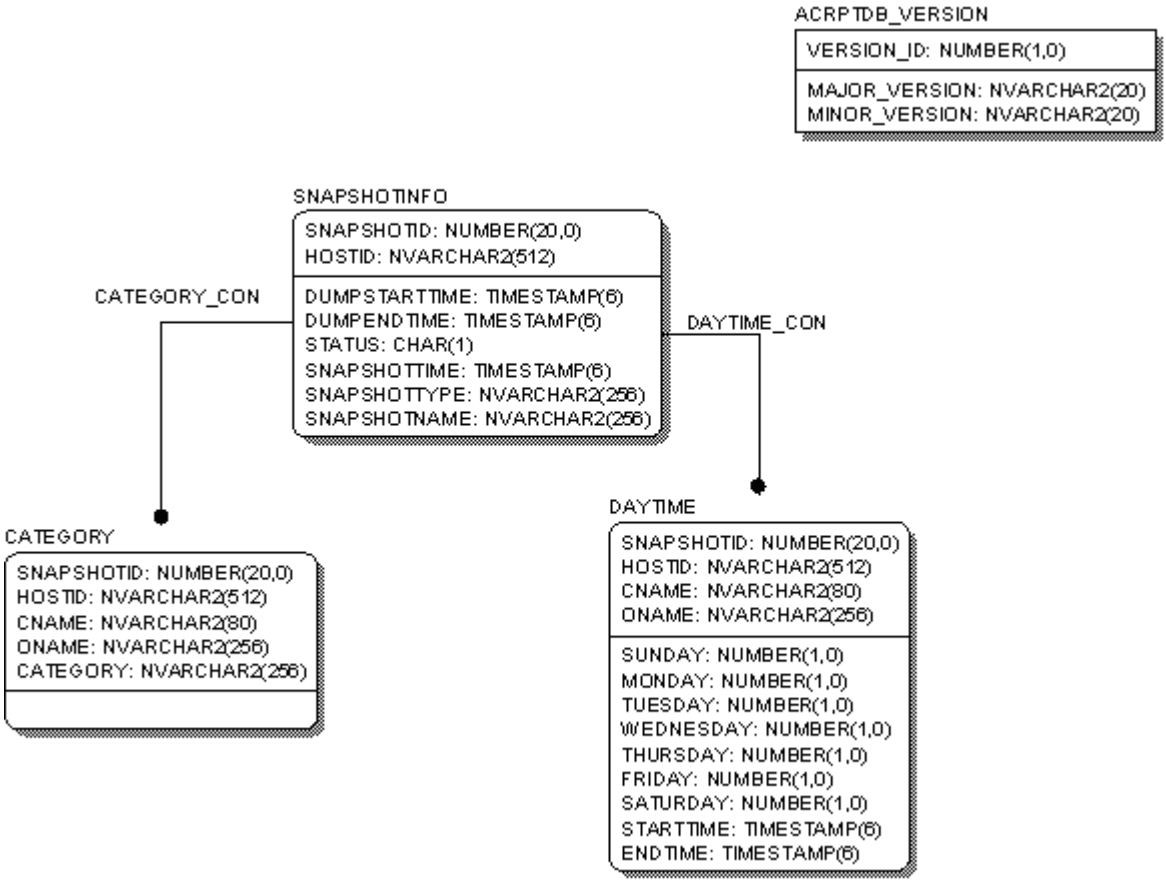
资源

这是资源相关表格的图解：


ACL
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
ACNAME: NVARCHAR2(80)
AONAME: NVARCHAR2(256)
ACLTYPE: NVARCHAR2(80)
CALENDAR: NVARCHAR2(256)
PROGRAMNAME: NVARCHAR2(256)
OUTCONCNAME: NVARCHAR2(80)
OUTCONONAME: NVARCHAR2(256)
HOSTCNAME: NVARCHAR2(80)
HOSTONAME: NVARCHAR2(256)
AREAD: NUMBER(1,0)
AWRITE: NUMBER(1,0)
AMODIFY: NUMBER(1,0)
ACREATE: NUMBER(1,0)
AERASE: NUMBER(1,0)
AFILESCAN: NUMBER(1,0)
ALANGINT: NUMBER(1,0)
AEXEC: NUMBER(1,0)
ACHOWN: NUMBER(1,0)
ACHGRP: NUMBER(1,0)
ACHMOD: NUMBER(1,0)
AUTIMES: NUMBER(1,0)
ASEC: NUMBER(1,0)
AKILL: NUMBER(1,0)
ACONNECT: NUMBER(1,0)
ARENAME: NUMBER(1,0)
APASSWORD: NUMBER(1,0)
AAUTHORIZED: NUMBER(1,0)
AXAUDIT: NUMBER(1,0)
ACHDIR: NUMBER(1,0)
ACRSUBK: NUMBER(1,0)
ANOTIFY: NUMBER(1,0)
AENUM: NUMBER(1,0)
AQUERY: NUMBER(1,0)
ARCTRL: NUMBER(1,0)
ACRLINK: NUMBER(1,0)
APRINT: NUMBER(1,0)
AMANAGE: NUMBER(1,0)
AMAXALLOWED: NUMBER(1,0)
ASTOP: NUMBER(1,0)
APAUSE: NUMBER(1,0)
ACONTROL: NUMBER(1,0)
ACHOG: NUMBER(1,0)
ARESUME: NUMBER(1,0)
DREAD: NUMBER(1,0)
DWRITE: NUMBER(1,0)
DMODIFY: NUMBER(1,0)
DCREATE: NUMBER(1,0)
DERASE: NUMBER(1,0)
DFILESCAN: NUMBER(1,0)
DLANGINT: NUMBER(1,0)
DEXEC: NUMBER(1,0)
DCHOWN: NUMBER(1,0)
DCHGRP: NUMBER(1,0)
DCHMOD: NUMBER(1,0)
DUTIMES: NUMBER(1,0)
DSEC: NUMBER(1,0)
DKILL: NUMBER(1,0)
DCONNECT: NUMBER(1,0)
DRENAME: NUMBER(1,0)
DPASSWORD: NUMBER(1,0)
DAUTHORIZED: NUMBER(1,0)
DXAUDIT: NUMBER(1,0)
DCHDIR: NUMBER(1,0)
DCRSUBK: NUMBER(1,0)
DNOTIFY: NUMBER(1,0)
DENUM: NUMBER(1,0)
DQUERY: NUMBER(1,0)
DRCTRL: NUMBER(1,0)
DCRLINK: NUMBER(1,0)
DPRINT: NUMBER(1,0)
DMANAGE: NUMBER(1,0)
DMAXALLOWED: NUMBER(1,0)
DSTOP: NUMBER(1,0)
DPAUSE: NUMBER(1,0)
DCONTROL: NUMBER(1,0)
DCHOG: NUMBER(1,0)
DRESUME: NUMBER(1,0)
UACC
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
AREAD: NUMBER(1,0)
AWRITE: NUMBER(1,0)
AMODIFY: NUMBER(1,0)
ACREATE: NUMBER(1,0)
AERASE: NUMBER(1,0)
AFILESCAN: NUMBER(1,0)
ALANGINT: NUMBER(1,0)
AEXEC: NUMBER(1,0)
ACHOWN: NUMBER(1,0)
ACHGRP: NUMBER(1,0)
ACHMOD: NUMBER(1,0)
AUTIMES: NUMBER(1,0)
ASEC: NUMBER(1,0)
AKILL: NUMBER(1,0)
ACONNECT: NUMBER(1,0)
ARENAME: NUMBER(1,0)
APASSWORD: NUMBER(1,0)
AAUTHORIZED: CHAR(18)
AXAUDIT: NUMBER(1,0)
ACHDIR: NUMBER(1,0)
ACRSUBK: NUMBER(1,0)
ANOTIFY: NUMBER(1,0)
AENUM: NUMBER(1,0)
AQUERY: NUMBER(1,0)
ARCTRL: NUMBER(1,0)
ACRLINK: NUMBER(1,0)
APRINT: NUMBER(1,0)
AMANAGE: NUMBER(1,0)
AMAXALLOWED: NUMBER(1,0)
ASTOP: NUMBER(1,0)
APAUSE: NUMBER(1,0)
ACONTROL: NUMBER(1,0)
ACHOG: NUMBER(1,0)
ARESUME: NUMBER(1,0)
INETACL
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
SERVICENAME: NVARCHAR2(256)
PROTOCOLNAME: NVARCHAR2(256)
AREAD: NUMBER(1,0)
AWRITE: NUMBER(1,0)
AMODIFY: NUMBER(1,0)
ACREATE: NUMBER(1,0)
AERASE: NUMBER(1,0)
AFILESCAN: NUMBER(1,0)
ALANGINT: NUMBER(1,0)
AEXEC: NUMBER(1,0)
ACHOWN: NUMBER(1,0)
ACHGRP: NUMBER(1,0)
ACHMOD: NUMBER(1,0)
AUTIMES: NUMBER(1,0)
ASEC: NUMBER(1,0)
AKILL: NUMBER(1,0)
ACONNECT: NUMBER(1,0)
ARENAME: NUMBER(1,0)
APASSWORD: NUMBER(1,0)
AAUTHORIZED: NUMBER(1,0)
AXAUDIT: NUMBER(1,0)
ACHDIR: NUMBER(1,0)
ACRSUBK: NUMBER(1,0)
ANOTIFY: NUMBER(1,0)
AENUM: NUMBER(1,0)
AQUERY: NUMBER(1,0)
ARCTRL: NUMBER(1,0)
ACRLINK: NUMBER(1,0)
APRINT: NUMBER(1,0)
AMANAGE: NUMBER(1,0)
AMAXALLOWED: NUMBER(1,0)
ASTOP: NUMBER(1,0)
APAUSE: NUMBER(1,0)
ACONTROL: NUMBER(1,0)
ACHOG: NUMBER(1,0)
ARESUME: NUMBER(1,0)
INSERVRNGE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
MINSERVICE: NUMBER
MAXSERVICE: NUMBER
AREAD: NUMBER(1,0)
AWRITE: NUMBER(1,0)
AMODIFY: NUMBER(1,0)
ACREATE: NUMBER(1,0)
AERASE: NUMBER(1,0)
AFILESCAN: NUMBER(1,0)
ALANGINT: NUMBER(1,0)
AEXEC: NUMBER(1,0)
ACHOWN: NUMBER(1,0)
ACHGRP: NUMBER(1,0)
ACHMOD: NUMBER(1,0)
AUTIMES: NUMBER(1,0)
ASEC: NUMBER(1,0)
AKILL: NUMBER(1,0)
ACONNECT: NUMBER(1,0)
ARENAME: NUMBER(1,0)
APASSWORD: NUMBER(1,0)
AAUTHORIZED: NUMBER(1,0)
AXAUDIT: NUMBER(1,0)
ACHDIR: NUMBER(1,0)
ACRSUBK: NUMBER(1,0)
ANOTIFY: NUMBER(1,0)
AENUM: NUMBER(1,0)
AQUERY: NUMBER(1,0)
ARCTRL: NUMBER(1,0)
ACRLINK: NUMBER(1,0)
APRINT: NUMBER(1,0)
AMANAGE: NUMBER(1,0)
AMAXALLOWED: NUMBER(1,0)
ASTOP: NUMBER(1,0)
APAUSE: NUMBER(1,0)
ACONTROL: NUMBER(1,0)
ACHOG: NUMBER(1,0)
ARESUME: NUMBER(1,0)
SPECIALPGMTYPE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
TMAIL: NUMBER(1,0)
TBACKUP: NUMBER(1,0)
TDDM: NUMBER(1,0)
TDCM: NUMBER(1,0)
TPBF: NUMBER(1,0)
TPBN: NUMBER(1,0)
TSTOP: NUMBER(1,0)
TSURR: NUMBER(1,0)
TREG: NUMBER(1,0)
TRESTRICTED: NUMBER(1,0)
HOLDATE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(256)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
STARTDATE: TIMESTAMP(6)
ENDDATE: TIMESTAMP(6)
ALLDAY: NUMBER(1,0)
EVERYYEAR: NUMBER(1,0)
SPECIALPGMTYPE_CON
HOLDATE_CON
RESINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
PREFIX: NVARCHAR2(40)
OWNERCNAME: NVARCHAR2(80)
OWNERONAME: NVARCHAR2(256)
OWNRTYPE: CHAR(1)
RESOWNER: NVARCHAR2(256)
RULEOWNER: NVARCHAR2(256)
ADMINBYCNAME: NVARCHAR2(80)
ADMINBYONAME: NVARCHAR2(256)
ADMINDATE: TIMESTAMP(6)
USERDATA: NVARCHAR2(256)
INSERVRNGE_CON
INETACL_CON
UACC_CON
RESINFO_HOST_CON
ACL_CON
RAUDIT
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
AUDITSUCCESS: NUMBER(1,0)
AUDITFAILURE: NUMBER(1,0)
DEBUG: NUMBER(1,0)
TRUST: NUMBER(1,0)
RAUDIT_CON
SNAPSHOTINFO
RESINFO_CON
GROUPS
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
ONAME: NVARCHAR2(256)
CNAME: NVARCHAR2(80)
GROUPS_MEMBER_CON
GROUPS_GROUP_CON
MEMBERS
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
CNAME: NVARCHAR2(80)
ONAME: NVARCHAR2(256)
MEMBERS_PARENT_CON
MEMBERS_CHILD_CON
RESAC
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
DESCRIPTION: NVARCHAR2(256)
CALENDAR: NVARCHAR2(256)
NOTIFY: NVARCHAR2(256)
SECLABEL: NVARCHAR2(256)
SECLEVEL: NUMBER
CRETIME: TIMESTAMP(6)
WARNING: NUMBER(1,0)
UNTRUST: NUMBER(1,0)
ETHINFO: NVARCHAR2(256)
NETMATCH: NVARCHAR2(256)
NETMASK: NVARCHAR2(256)
AAUDIT: NVARCHAR2(256)
UNTRUSTREASON: NVARCHAR2(256)
ACCSWHO: NUMBER(20,0)
ACCSTIME: TIMESTAMP(6)
BLOCKRUN: NUMBER(1,0)
UNIXUID: NVARCHAR2(256)
INTERACTIVE: NUMBER(1,0)
TARGUSRCNAME: NVARCHAR2(80)
TARGUSRONAME: NVARCHAR2(256)
PASSWDREQ: NUMBER(1,0)
FILEPATH: NVARCHAR2(256)
POLICY_CON
RESAC_CON
NODE_CON
RESINFO_DEPTASK_CON
DEPLOYMENT_TASK
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
POLICYGRP_RESCLASS: NVARCHAR2(80)
POLICYGRP_RULEKEY: NVARCHAR2(256)
CHECKERTYPE: NVARCHAR2(80)
CHECKERID: NVARCHAR2(256)
NODE_RESCLASS: NVARCHAR2(80)
NODE_RULEKEY: NVARCHAR2(256)
POLICY_RESCLASS: NVARCHAR2(80)
POLICY_RULEKEY: NVARCHAR2(256)
MAKERID: NVARCHAR2(256)
MAKERTYPE: NVARCHAR2(80)
CHECKERCOMMENT: NVARCHAR2(256)
CHECKERTIME: TIMESTAMP(6)
DMSNAME: NVARCHAR2(256)
OPERATION: NVARCHAR2(256)
STATUS: NVARCHAR2(256)
POLICY
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
NAME: NVARCHAR2(256)
VERSION: NUMBER
FINALIZE: NUMBER(1,0)
POLICY_DEPTASK_CON
RESINFO_DEPTASKGRP_CON
POLICY_GROUP_CON
LATESTFIN_POLICYGRP_CON
LATEST_POLICYGRP_CON
POLICY_GROUP
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
LATEST_FIN_RULEKEY: NVARCHAR2(256)
LATEST_FIN_RESCLASS: NVARCHAR2(80)
LATEST_RESCLASS: NVARCHAR2(80)
LATEST_RULEKEY: NVARCHAR2(256)
POLICYGRP_DEPTASK_CON
POLICYGRP_DEPTASKGRP_CON
NODE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
ADDRESS: NVARCHAR2(512)
KEEPALIVE: TIMESTAMP(6)
VERSION: NUMBER
NODE_DEPTASK_CON
NODE_DEPTASKGRP_CON
DEPLOYMENT_TASK_GROUP
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
POLICYGRP_RESCLASS: NVARCHAR2(80)
POLICYGRP_RULEKEY: NVARCHAR2(256)
NODEGRP_RESCLASS: NVARCHAR2(80)
NODEGRP_RULEKEY: NVARCHAR2(256)
NODE_RESCLASS: NVARCHAR2(80)
NODE_RULEKEY: NVARCHAR2(256)
TRIG: NVARCHAR2(256)
NODEGRP_DEPTASKGRP_CON
POLICY_GROUP_NODE_ASSIGNMENT
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
POLICYGRP_RESCLASS: NVARCHAR2(80)
POLICYGRP_RULEKEY: NVARCHAR2(256)
NODE_RESCLASS: NVARCHAR2(80)
NODE_RULEKEY: NVARCHAR2(256)
POLICYGRP_NODASS_NOD_CON
POLICYGRP_NODASS_POL_CON
RULESET
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
FINALIZE: NUMBER(1,0)
RULESET_CON

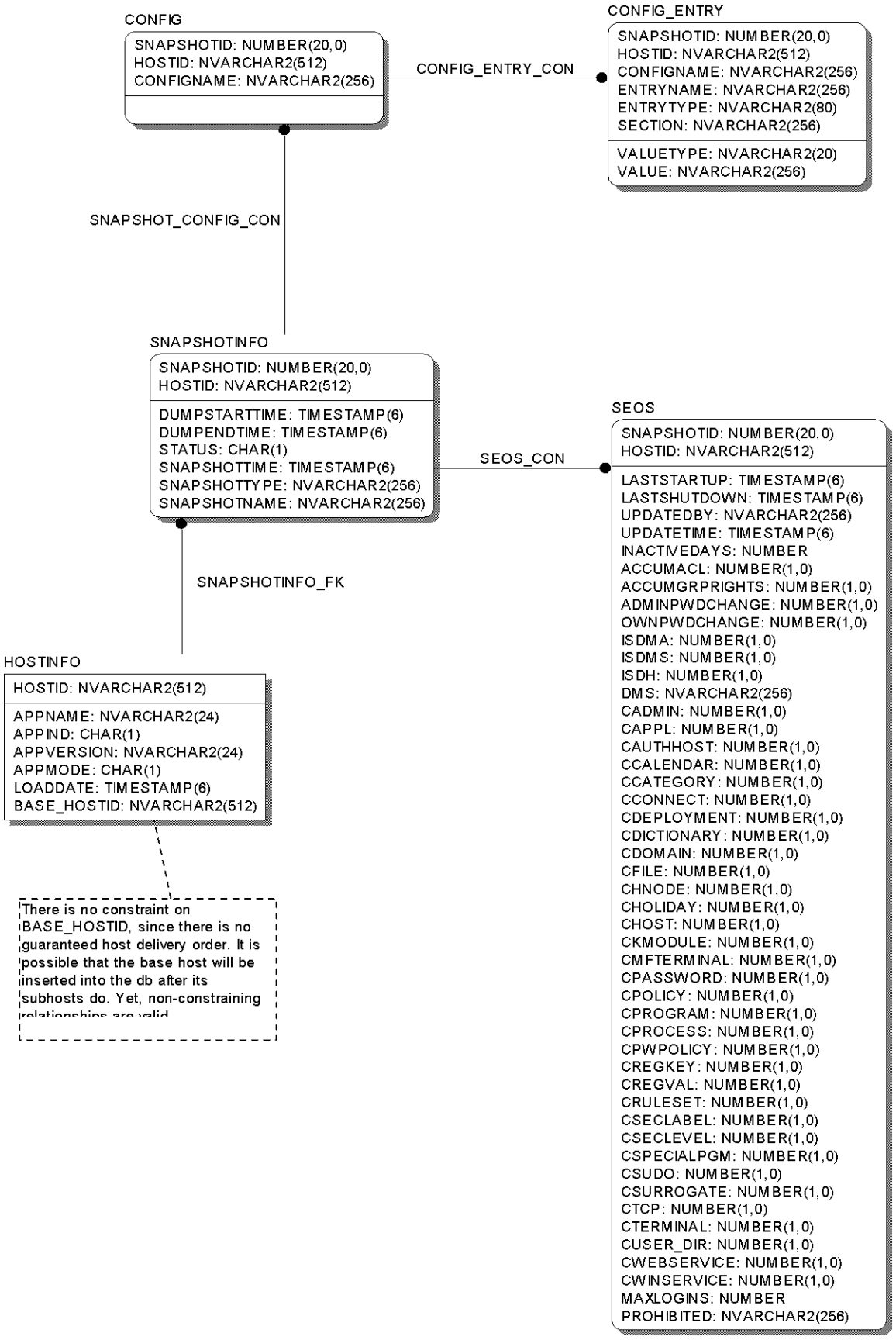
共享属性

这是用户、组和资源对象之间的共享属性的图解：



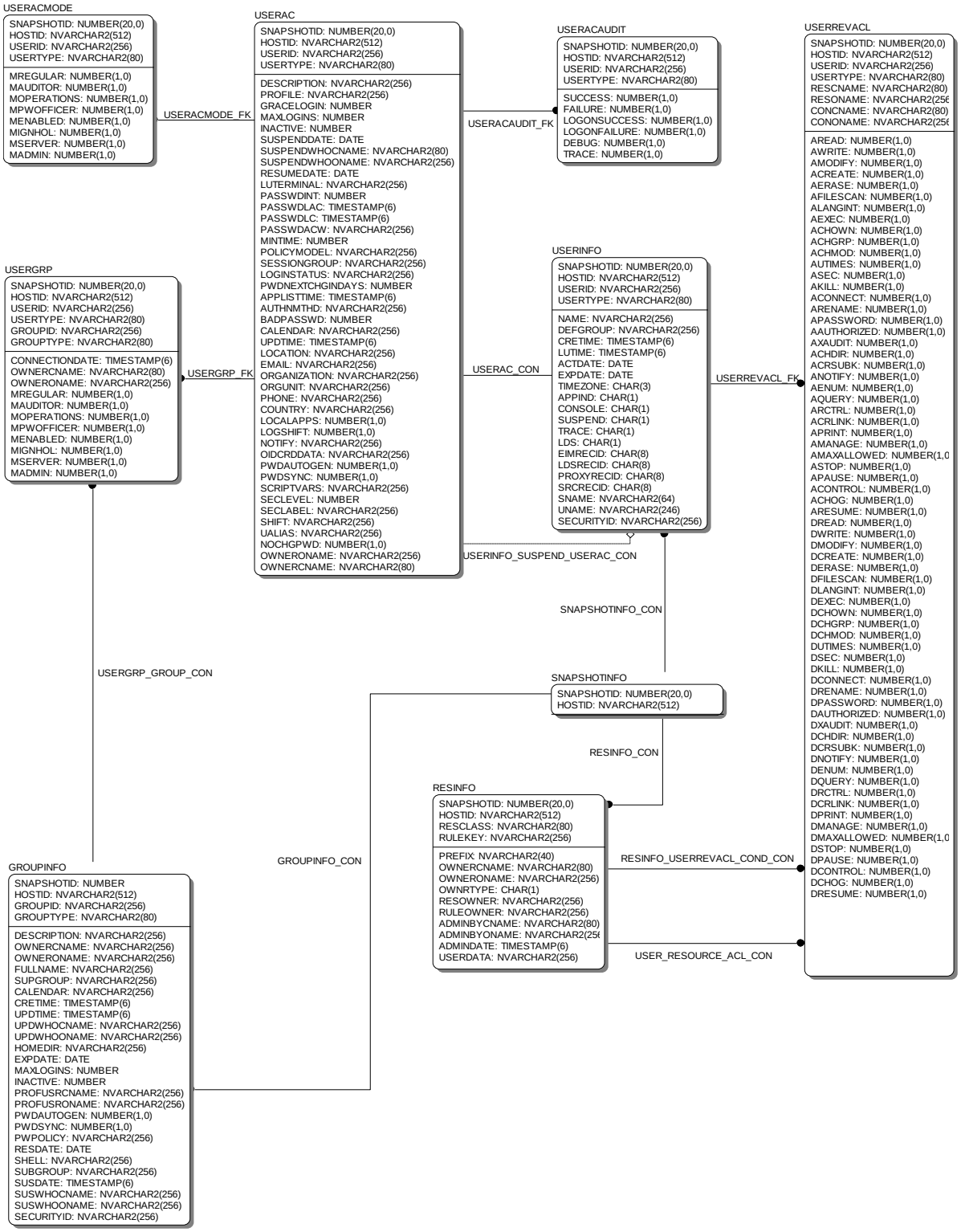
快照

这是快照相关和端点相关表格的图解：


CONFIG
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
CONFIGNAME: NVARCHAR2(256)
CONFIG_ENTRY_CON
CONFIG_ENTRY
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
CONFIGNAME: NVARCHAR2(256)
ENTRYNAME: NVARCHAR2(256)
ENTRYTYPE: NVARCHAR2(80)
SECTION: NVARCHAR2(256)
VALUETYPE: NVARCHAR2(20)
VALUE: NVARCHAR2(256)
SNAPSHOT_CONFIG_CON
SNAPSHOTINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
DUMPSTARTTIME: TIMESTAMP(6)
DUMPENDTIME: TIMESTAMP(6)
STATUS: CHAR(1)
SNAPSHOTTIME: TIMESTAMP(6)
SNAPSHOTTYPE: NVARCHAR2(256)
SNAPSHOTNAME: NVARCHAR2(256)
SEOS_CON
SEOS
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
LASTSTARTUP: TIMESTAMP(6)
LASTSHUTDOWN: TIMESTAMP(6)
UPDATEDBY: NVARCHAR2(256)
UPDATETIME: TIMESTAMP(6)
INACTIVEDAYS: NUMBER
ACCUMACL: NUMBER(1,0)
ACCUMGRPRIGHTS: NUMBER(1,0)
ADMINPWDCHANGE: NUMBER(1,0)
OWNPWDCHANGE: NUMBER(1,0)
ISDMA: NUMBER(1,0)
ISDMS: NUMBER(1,0)
ISDH: NUMBER(1,0)
DMS: NVARCHAR2(256)
CADMIN: NUMBER(1,0)
CAPPL: NUMBER(1,0)
CAUTHHOST: NUMBER(1,0)
CCALENDAR: NUMBER(1,0)
CCATEGORY: NUMBER(1,0)
CCONNECT: NUMBER(1,0)
CDEPLOYMENT: NUMBER(1,0)
CDICTIONARY: NUMBER(1,0)
CDOMAIN: NUMBER(1,0)
CFILE: NUMBER(1,0)
CHNODE: NUMBER(1,0)
CHOLIDAY: NUMBER(1,0)
CHOST: NUMBER(1,0)
CKMODULE: NUMBER(1,0)
CMFTERMINAL: NUMBER(1,0)
CPASSWORD: NUMBER(1,0)
CPOLICY: NUMBER(1,0)
CPROGRAM: NUMBER(1,0)
CPROCESS: NUMBER(1,0)
CPWPOLICY: NUMBER(1,0)
CREGKEY: NUMBER(1,0)
CREGVAL: NUMBER(1,0)
CRULESET: NUMBER(1,0)
CSECLABEL: NUMBER(1,0)
CSECLEVEL: NUMBER(1,0)
CSPECIALPGM: NUMBER(1,0)
CSUDO: NUMBER(1,0)
CSURROGATE: NUMBER(1,0)
CTCP: NUMBER(1,0)
CTERMINAL: NUMBER(1,0)
CUSER_DIR: NUMBER(1,0)
CWEBSERVICE: NUMBER(1,0)
CWINSERVICE: NUMBER(1,0)
MAXLOGINS: NUMBER
PROHIBITED: NVARCHAR2(256)
SNAPSHOTINFO_FK
HOSTINFO
HOSTID: NVARCHAR2(512)
APPNAME: NVARCHAR2(24)
APPIND: CHAR(1)
APPVERSION: NVARCHAR2(24)
APPMODE: CHAR(1)
LOADDATE: TIMESTAMP(6)
BASE_HOSTID: NVARCHAR2(512)
There is no constraint on BASE_HOSTID, since there is no guaranteed host delivery order. It is possible that the base host will be inserted into the db after its subhosts do. Yet, non-constraining relationships are valid.

用户

这是用户相关表格的图解：



表

下表对模式中的表格进行了描述，并提供了有关它们的简要说明：

名称	注释
ACL	大多数 CA Access Control 资源的 Access Control 列表。 它结合了以下 CA Access Control 属性：ACL、NACL、PACL、CACL、CALACL。 ACL－标准 Access Control 列表，包含得到授权可访问资源的用户名和组名，以及授予每个用户或组的访问权限级别。 NACL－否定式 Access Control 列表，包含无权访问资源的用户名或组名。 PACL－依赖于访问程序的程序 Access Control 列表。每个 PACL 都包含用户名和组名、访问级别以及用户要访问特定资源则必须执行的程序或 shell 脚本的名称。 CACL－条件 Access Control 列表 CALACL－日历访问控制，即依赖于 Unicenter® TNG 日历的资源 ACL。 Axxxx 和 Dxxxx 列代表所有支持资源类型的所有支持的 (A) 允许和 (D) 拒绝权限。 有些权限仅与特定类型的资源相关。 例如：开始、停止和暂停的权限仅与进程和服务相关，而与文件无关。
ACRPTDB_VERSION	数据库模式版本，用于控制数据库模式升级
CATEGORY	资源对象/用户对象/组对象的 B1 功能（安全类别）。
CONFIG	CA Access Control 配置存储，其中包含零个或多个配置条目（请参阅 CONFIG_ENTRY）。
CONFIG_ENTRY	配置存储内的单个配置条目。
DAYTIME	指定用户可以在一周中的哪几天以及一天中的哪几个小时内访问资源
DEPLOYMENT_RESULT_MESSAGE	部署任务的结果消息
DEPLOYMENT_TASK	说明单个策略部署任务：在单个节点上部署/取消部署单个策略的行为。

名称	注释
DEPLOYMENT_TASK_GROUP	准确说明以下部署相关任务之一： 1. 将节点分配至节点组 2. 将策略组分配至节点 3. 将策略组分配至节点组 可以看出，任务是二进制的，其中第一个操作符是节点或策略组，第二个操作符是节点或节点组。
DISTRIBUTION_HOST	灾难恢复模式的分发主机。 映射到 CA Access Control 类 SEOS 的 DH 和 DHDR 属性内的元素。
EFFECTIVE_POLICY	指出策略模式中哪些策略与哪些节点相关，包括隐性关系（通过节点组、策略组等）。
GROUPAUDIT	组对象的审核设置
GROUPINFO	组对象信息
GROUPMEMBER	属于该组的组。
GROUPREVACL	组反向 ACL，即组通过特定资源对哪些 ACL 赋予了特定条件。 有关所有 Axxx 和 Dxxxx（允许/拒绝）列的说明，请参阅 ACL 表。
GROUPS	资源对象和用户对象的组属性。 USER 记录所属的用户组（GROUP 记录）的列表。 另外，该属性中还包含任何组权限，如组管理权限 (GROUP-ADMIN)，分配给用户所属的每个组的用户。 该属性中包含的组列表可能与本机环境 GROUPS 属性中的组列表不同。
HOLDATE	假日对象的假日信息
HOSTINFO	主机信息代表网络中的 CA Access Control 端点

名称	注释
INETACL	INET-ACL－Internet Access Control 列表。 允许本地主机向客户端主机组提供的服务以及这些客户端主机的访问类型。 访问控制列表中的每个元素均包含下列信息： 1. 服务引用－对服务的引用（端口号或名称）。 要指定所有服务，请输入星号 (*) 作为服务引用。 2. 允许的访问－客户端主机对服务所具有的访问类型。 它们提供的有效访问类型和权限如下： - read（读取）－允许本地主机为主机组提供服务。 - none（无）－不允许本地主机为主机组提供服务。 有关所有 Axxx 和 Dxxxx（允许/拒绝）列的说明，请参阅 ACL 表。
INSERVRNGE	服务范围 ACL。 与 INETACL 属性相似。 但该属性不是显式地指定本地主机为一组客户端主机提供的服务，而是指定一系列服务。 有关所有 Axxx 和 Dxxxx（允许/拒绝）列的说明，请参阅 ACL 表。
LOCAL_PMD_SUBSCRIBER	代表策略模型订阅条目－通过 sepmd -L selang 命令，每个条目均映射到各个订阅条目。
LOGINAPPL	LOGINAPPL 类控制和检测登录应用程序。 通过它，用户可以定义登录应用程序，并使用此应用程序来设置控制登录的访问控制规则。 每个列的说明包含一个对它所代表的相应 CA Access Control 类、属性和值的引用。 有关完整信息，请参阅 *《selang 参考指南》*。
MEMBEROF	该组所属的组。
MEMBERS	资源对象的成员属性
NODE	定义要强制执行策略遵从的 CA Access Control 主机。 节点组由一个简单的资源实体表示（请参阅 RESINFO/RESAC）。 节点与节点组之间的关系由 GROUPS/MEMBERS 机制处理，处理机制与任何其他资源相同（请参阅 GROUPS/MEMBERS/RESINFO 表）
NODE_ADDRESS	零个或多个节点网络地址。 映射到 CA Access Control 类 HNODE 的 HNODE_IP 属性。
NODE_ALIAS	零个或多个节点别名。 映射到 CA Access Control 类 HNODE 的 ALIAS 属性。

名称	注释
NODE_DEVIATION	主机级别的偏差详细信息。
NODE_SUBSCRIPTION_STATUS	说明以策略分布为目的的多个 HNODE 之间的订阅关系和状态。
PASSWDRULES	指定密码规则。 此属性中包含许多用于确定 CA Access Control 如何处理密码保护的字段。 有关规则的完整列表，请参阅 USER 类的可修改属性 PROFILE。
POLICY	说明节点的遵从状态，以及需要强制执行遵从的操作。 每个策略实体代表另一策略的初始版本或后续版本。 初始策略始终分配给单个策略组（请参见 POLICY_GROU 表），该策略组还包含该策略的所有后续版本。
POLICY_DEVIATION	说明节点与其有效策略的偏差（策略不遵从性）
POLICY_GROUP	包含属于同一初始策略后续版本的所有策略
POLICY_GROUP_DEPENDENCY	说明哪些策略组依赖于其他策略组。 该表中不显示独立策略组。
POLICY_GROUP_NODE_ASSIGNMENT	说明在策略模型中将哪些策略分配给哪些节点（或节点组）。 将策略分配给节点后，NODE_RESCLASS 将为 HNODE。 如果将策略分配给节点组，则 NODE_RESCLASS 将为 GHNODE。 该表用于节点和节点组两种分配。 策略组与节点（或节点组）之间的关系由 GROUPS/MEMBERS 机制处理，处理机制与任何其他资源相同（请参阅 GROUPS/MEMBERS/RESINFO 表）
POLICY_RULESET	策略与其规则集之间的链接
POLICY_STATUS	说明与每个节点有关的策略的状态（请参阅 EFFECTIVE_POLICY）：无论是已部署还是取消部署等。
POLICYMODELINFO	策略模型信息。 包含有关由特定节点分发给其他节点的策略的状态。
RAUDIT	CA Access Control 在审核日志中记录的访问事件的类型。
RESAC	CA Access Control 资源信息
RESINFO	CA Access Control 资源信息
RULESET	要作为策略部署/取消部署的一部分执行的命令集。

名称	注释
RULESET_COMMAND	单个 selang 命令，许多个 selang 命令组成一个规则集。
SEOS	设置选项信息
SEOSSYSCALL	(r12.0 SP1) CA Access Control 主内核模块，主要用于截获将向 seosd 咨询来确定是否允许或拒绝的操作系统事件
SNAPSHOTINFO	快照信息表示所有从单个本地 AC 数据库（在单个主机中）在收集期间收集到的数据。
SPECIALPGMTYPE	SPECIALPGM 类的特殊程序类型。 由 AC 自动生成的程序信息。 Watchdog 会自动验证该属性中存储的信息。 如果它已被更改，则 CA Access Control 会将程序定义为未受托。 每个记录代表 CA Access Control 类 SPECIALPGM 的一个 SPECIALPGMTYPE 属性。
SYSCALL	(r12.0 SP1) CA Access Control 主内核模块，主要用于截获将向 seosd 咨询来确定是否允许或拒绝的操作系统事件
SYSCALLUSERSPECIALPGM	(r12.0 SP1) CA Access Control 主内核模块，主要用于截获将向 seosd 咨询来确定是否允许或拒绝的操作系统事件
UACC	默认访问权限是向请求对象访问权限的任何访问者授予的权限，但它并不在对象的 Access Control 列表中。 数据库中未定义的用户也会获得默认的访问权限。 有关所有 Axxx 和 Dxxxx（允许/拒绝）列的说明，请参阅 ACL 表。 每个记录代表多个 CA Access Control 资源类的 UACC 属性。 有关所有 Axxx 和 Dxxxx（允许/拒绝）列的说明，请参阅 ACL 表。
USERAC	CA Access Control 用户信息。 该表中的每个记录都代表类 USER/XUSER 的单个 CA Access Control 对象的特定于 AC 的属性。
USERACAUDIT	CA Access Control 用户审核设置 每个记录代表 CA Access Control 类 USER/XUSER 的 CA Access Control 属性 AUDIT_MODE 的一个条目。

名称	注释
USERACMODE	CA Access Control 用户模式 (OBJ_TYPE) 每个记录代表 CA Access Control 类 USER/XUSER 的 CA Access Control 属性 OBJ_TYPE 的一个条目。
USERGRP	用户与组的连接 每个记录代表 CA Access Control 类 USER/XUSER 的 CA Access Control 属性 GROUPS 的一个条目。
USERINFO	基本用户信息。 每个用户都必须在该表中具有一个记录。 该表是其他 USER 表（代表其他用户信息分段）的父表。
USERLIST	组对象的用户列表（成员） 每个记录代表 CA Access Control 类 GROUP/XGROUP 的 CA Access Control 属性 USERLIST 的一个 OID 条目。
USERREVACL	用户反向 ACL，即用户通过特定资源对哪些 ACL 赋予了特定条件。 有关所有 Axxx 和 Dxxxx（允许/拒绝）列的说明，请参阅 ACL 表。 每个记录代表 CA Access Control 类 USER/XUSER 的 CA Access Control 属性 REVACL 的一个条目。

ACL 表的列

下表说明了 ACL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该 ACL 记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该 ACL 记录的主机 ID
RESCLASS	是	NVARCHAR2(80)	不为 NULL	该 ACL 记录的资源类名（例如：FILE、PROCESS）
RULEKEY	是	NVARCHAR2(256)	不为 NULL	该 ACL 记录的资源对象名
ACNAME	是	NVARCHAR2(80)	不为 NULL	访问者类名
AONAME	是	NVARCHAR2(256)	不为 NULL	访问者对象名
ACLTYPE	是	NVARCHAR2(80)	不为 NULL	访问类型（例如：R = 读取、W = 写入）

名称	是否为 PK	数据类型	Null 选项	注释
ISALLOW	是	NUMBER(1,0)	不为 NULL	与该记录中的哪些列为相关列：Axxx（允许）或 Dxxx（拒绝）。 特别是，这是允许 ACL 条目还是拒绝 ACL 条目。
CONDHASH	是	NUMBER(20,0)	不为 NULL	根据 ACLTYPE，它代表该 ACL 条件的散列值。 对于 PACL，它代表 PROGRAMNAME 字段的散列值。 对于 CACL，散列算法用于 OUTCONCNAME、OUTCONONAME、HOSTCNAME、HOSTONAME。 对于 CALACL，它是 CALENDAR 的散列值 对于 ACL 和 NACL，它是 0。
CALENDAR	否	NVARCHAR2(256)	NULL	日历名称（用于 CALACL 记录）
PROGRAMNAME	否	NVARCHAR2(256)	NULL	程序名称（用于 PACL 记录）
OUTCONCNAME	否	NVARCHAR2(80)	NULL	当 ACLTYPE=CACL 时，该字段包含出站连接类名。 GROUP 或 XGROUP 表示相关记录包含在 GROUPINFO 表中。 USER 或 XUSER 表示它包含在 USERINFO 表中。 对于其他 ACLTYPE 值，该字段为 NULL。
OUTCONONAME	否	NVARCHAR2(256)	NULL	当 ACLTYPE=CACL 时，该字段包含传出连接对象名。 对于其他 ACNAME 值，该字段为 NULL。
HOSTCNAME	否	NVARCHAR2(80)	NULL	当 ACLTYPE=CACL 时，该字段包含主机类名（即“HOST”）并与 RESINFO 表中的相应记录相关。 对于其他 ACNAME 值，该字段为 NULL。

名称	是否为 PK	数据类型	Null 选项	注释
HOSTONAME	否	NVARCHAR2(256)	NULL	当 ACLTYPE=CACL 时，该字段包含主机对象名。 对于其他 ACNAME 值，该字段为 NULL。
AREAD	否	NUMBER(1,0)	NULL	允许读取
AWRITE	否	NUMBER(1,0)	NULL	允许写入
AMODIFY	否	NUMBER(1,0)	NULL	允许修改
ACREATE	否	NUMBER(1,0)	NULL	允许创建
AERASE	否	NUMBER(1,0)	NULL	允许清除
AFILESCAN	否	NUMBER(1,0)	NULL	允许扫描文件
ALANGINT	否	NUMBER(1,0)	NULL	
AEXEC	否	NUMBER(1,0)	NULL	允许执行
ACHOWN	否	NUMBER(1,0)	NULL	允许更改所有者
ACHGRP	否	NUMBER(1,0)	NULL	允许更改组
ACHMOD	否	NUMBER(1,0)	NULL	允许启动 Chmod 实用程序
AUTIMES	否	NUMBER(1,0)	NULL	允许更新文件/文件夹资源更新时间
ASEC	否	NUMBER(1,0)	NULL	
AKILL	否	NUMBER(1,0)	NULL	
ACONNECT	否	NUMBER(1,0)	NULL	允许连接
ARENAME	否	NUMBER(1,0)	NULL	允许重命名
APASSWORD	否	NUMBER(1,0)	NULL	
AAUTHORIZED	否	NUMBER(1,0)	NULL	
AXAUDIT	否	NUMBER(1,0)	NULL	
ACHDIR	否	NUMBER(1,0)	NULL	允许将文件夹资源设置为当前工作目录
ACRSUBK	否	NUMBER(1,0)	NULL	
ANOTIFY	否	NUMBER(1,0)	NULL	允许通知
AENUM	否	NUMBER(1,0)	NULL	允许枚举
AQUERY	否	NUMBER(1,0)	NULL	允许查询
ARCTRL	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
ACRLINK	否	NUMBER(1,0)	NULL	
APRINT	否	NUMBER(1,0)	NULL	允许打印
AMANAGE	否	NUMBER(1,0)	NULL	允许管理
AMAXALLOWED	否	NUMBER(1,0)	NULL	
ASTOP	否	NUMBER(1,0)	NULL	允许停止
APAUSE	否	NUMBER(1,0)	NULL	允许暂停
ACONTROL	否	NUMBER(1,0)	NULL	允许控制
ACHOG	否	NUMBER(1,0)	NULL	
ARESUME	否	NUMBER(1,0)	NULL	允许恢复
DREAD	否	NUMBER(1,0)	NULL	拒绝读取
DWRITE	否	NUMBER(1,0)	NULL	拒绝写入
DMODIFY	否	NUMBER(1,0)	NULL	拒绝修改
DCREATE	否	NUMBER(1,0)	NULL	拒绝创建
DERASE	否	NUMBER(1,0)	NULL	拒绝清除
DFILESCAN	否	NUMBER(1,0)	NULL	
DLANGINT	否	NUMBER(1,0)	NULL	
DEXEC	否	NUMBER(1,0)	NULL	拒绝执行
DCHOWN	否	NUMBER(1,0)	NULL	
DCHGRP	否	NUMBER(1,0)	NULL	
DCHMOD	否	NUMBER(1,0)	NULL	
DUTIMES	否	NUMBER(1,0)	NULL	
DSEC	否	NUMBER(1,0)	NULL	
DKILL	否	NUMBER(1,0)	NULL	拒绝终止
DCONNECT	否	NUMBER(1,0)	NULL	拒绝连接
DRENAME	否	NUMBER(1,0)	NULL	拒绝重命名
DPASSWORD	否	NUMBER(1,0)	NULL	
DAUTHORIZED	否	NUMBER(1,0)	NULL	
DXAUDIT	否	NUMBER(1,0)	NULL	
DCHDIR	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
DCRSUBK	否	NUMBER(1,0)	NULL	
DNOTIFY	否	NUMBER(1,0)	NULL	拒绝通知
DENUM	否	NUMBER(1,0)	NULL	拒绝枚举
DQUERY	否	NUMBER(1,0)	NULL	拒绝查询
DRCTRL	否	NUMBER(1,0)	NULL	
DCRLINK	否	NUMBER(1,0)	NULL	
DPRINT	否	NUMBER(1,0)	NULL	
DMANAGE	否	NUMBER(1,0)	NULL	拒绝管理
DMAXALLOWED	否	NUMBER(1,0)	NULL	
DSTOP	否	NUMBER(1,0)	NULL	拒绝停止
DPAUSE	否	NUMBER(1,0)	NULL	拒绝暂停
DCONTROL	否	NUMBER(1,0)	NULL	拒绝控制
DCHOG	否	NUMBER(1,0)	NULL	
DRESUME	否	NUMBER(1,0)	NULL	拒绝恢复

ACRPTDB_VERSION 表的列

下表说明了 ACRPTDB_VERSION 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
VERSION_ID	否	NUMBER(1,0)	不为 NULL	应始终为 1
MAJOR_VERSION	否	NVARCHAR2(20)	NULL	主版本
MINOR_VERSION	否	NVARCHAR2(20)	NULL	次版本

CATEGORY 表的列

下表说明了 CATEGORY 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
CNAME	是	NVARCHAR2(80)	不为 NULL	该记录的类名
ONAME	是	NVARCHAR2(256)	不为 NULL	该记录的对象名
CATEGORY	是	NVARCHAR2(256)	不为 NULL	该记录的类别名。 如果对资源分配了一个或更多个安全类别，则只有在用户的安全类别列表中包含所有分配给资源的安全类别时，用户才可以访问资源。

CONFIG 表的列

下表说明了 CONFIG 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
CONFIGNAME	是	NVARCHAR2(256)	不为 NULL	该记录的类别名。 如果对资源分配了一个或更多个安全类别，则只有在用户的安全类别列表中包含所有分配给资源的安全类别时，用户才可以访问资源。

CONFIG_ENTRY 表的列

下表说明了 CONFIG_ENTRY 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
CONFIGNAME	是	NVARCHAR2(256)	不为 NULL	配置存储的名称
ENTRYID	是	NVARCHAR2(256)	不为 NULL	配置条目名称
ENTRYTYPE	是	NVARCHAR2(80)	不为 NULL	配置条目类型。 “部分”值表示该条目的 VALUE 和 VALUETYPE 为 NULL
SECTION	否	NVARCHAR2(256)	不为 NULL	该条目的部分名称。 如果 ENRYTYPE=部分，则该字段等同于部分的名称。 否则，该字段等同于包含此条目的部分的名称。
ENTRYNAME	否	NVARCHAR2(256)	NULL	配置条目名。 该列映射到 AC 配置的标记元素 NAME 属性。
VALUETYPE	否	NVARCHAR2(20)	NULL	当 ENTRYTYPE 为非 NULL 时，此条目的值的类型。
值	否	NVARCHAR2(256)	NULL	当 ENTRYTYPE 为非 NULL 时，此条目的值。

DAYTIME 表的列

下表说明了 DAYTIME 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
CNAME	是	NVARCHAR2(80)	不为 NULL	该记录的类名
ONAME	是	NVARCHAR2(256)	不为 NULL	该记录的对象名
SUNDAY	否	NUMBER(1,0)	NULL	在星期日允许访问

名称	是否为 PK	数据类型	Null 选项	注释
MONDAY	否	NUMBER(1,0)	NULL	在星期一允许访问
TUESDAY	否	NUMBER(1,0)	NULL	在星期二允许访问
WEDNESDAY	否	NUMBER(1,0)	NULL	在星期三允许访问
THURSDAY	否	NUMBER(1,0)	NULL	在星期四允许访问
FRIDAY	否	NUMBER(1,0)	NULL	在星期五允许访问
SATURDAY	否	NUMBER(1,0)	NULL	在星期六允许访问
STARTTIME	否	TIMESTAMP(6)	NULL	在该开始时间后允许访问
ENDTIME	否	TIMESTAMP(6)	NULL	在该结束时间前允许访问

DEPLOYMENT_RESULT_MESSAGE 表的列

下表说明了 DEPLOYMENT_RESULT_MESSAGE 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA CA-ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
MESSAGEIDX	是	NUMBER	不为 NULL	消息已排序。 该列代表消息索引，以此方式说明其相对于其他消息的位置。 映射到 AC 类 DEPLOYMENT 的 AC 属性 RESULT_MESSAGE 的命令索引组件。
MESSSAGESTR	是	NVARCHAR2(256)	NULL	消息正文。 映射到 AC 类 DEPLOYMENT 的 AC 属性 RESULT_MESSAGE 的命令字符串组件。

DEPLOYMENT_TASK 表的列

下表说明了 DEPLOYMENT_TASK 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
POLICYGRP_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 DEPLOYMENT 类的 AC OID 属性 GPOLICY 的 CNAME。
POLICYGRP_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到 DEPLOYMENT 类的 AC OID 属性 GPOLICY 的 ONAME。
CHECKERTYPE	否	NVARCHAR2(80)	NULL	该用户的 AC 类：USER、XUSER。 映射到 DEPLOYMENT 类的 AC OID 属性 CHECKER 的 CNAME。
CHECKERID	否	NVARCHAR2(256)	NULL	系统中该对象的标识符。 映射到 DEPLOYMENT 类的 AC OID 属性 CHECKER 的 ONAME。
NODE_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 DEPLOYMENT 类的 AC OID 属性 HNODEY 的 CNAME。

名称	是否为 PK	数据类型	Null 选项	注释
NODE_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。映射到 DEPLOYMENT 类的 AC OID 属性 HNODE 的 ONAME。
POLICY_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 DEPLOYMENT 类的 AC OID 属性 POLICY 的 CNAME。
POLICY_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。映射到 DEPLOYMENT 类的 AC OID 属性 POLICY 的 ONAME。
MAKERID	否	NVARCHAR2(256)	NULL	系统中该对象的标识符。 映射到 DEPLOYMENT 类的 AC OID 属性 MAKER 的 ONAME。
MAKERTYPE	否	NVARCHAR2(80)	NULL	制定者的类。 值 USER 或 XUSER 表示制定者记录包含在 USERINFO 表中。 GROUP 或 XGROUP 表示它包含在 GROUPINFO 表中。 映射到 DEPLOYMENT 类的 AC OID 属性 MAKER 的 CNAME。
CHECKERCOMMENT	否	NVARCHAR2(256)	NULL	检查者添加的注释。 映射到 DEPLOYMENT 类的 AC 属性 CHECKER_COMMENT。
CHECKERTIME	否	TIMESTAMP(6)	NULL	检查时间戳。 映射到 DEPLOYMENT 类的 AC 属性 CHECKER_TIME。
DMSNAME	否	NVARCHAR2(256)	NULL	生成该任务的 DMS 的名称。 映射到 DEPLOYMENT 类的 AC 属性 DMS_NAME。

名称	是否为 PK	数据类型	Null 选项	注释
OPERATION	否	NVARCHAR2(256)	NULL	该任务应执行的操作：DEPLOY、UNDEPLOY。 映射到 DEPLOYMENT 类的 AC 属性 OPERATION。
STATUS	否	NVARCHAR2(256)	NULL	任务状态：SUCCESS、WARNING、FAIL、NOACTION。 映射到 DEPLOYMENT 类的 AC 属性 STATUS。

DEPLOYMENT_TASK_GROUP 表的列

下表说明了 DEPLOYMENT_TASK_GROUP 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
POLICYGRP_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 GDEPLOYMENT 类的 AC OID 属性 POLICY 的 CNAME。
POLICYGRP_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到 GDEPLOYMENT 类的 AC OID 属性 POLICY 的 ONAME。

名称	是否为 PK	数据类型	Null 选项	注释
NODEGRP_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 GDEPLOYMENT 类的 AC OID 属性 GHNODE 的 CNAME。
NODEGRP_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到 GDEPLOYMENT 类的 AC OID 属性 GHNODE 的 ONAME。
NODE_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 GDEPLOYMENT 类的 AC OID 属性 HNODE 的 CNAME。
NODE_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到 GDEPLOYMENT 类的 AC OID 属性 HNODE 的 ONAME。
TRIG	否	NVARCHAR2(256)	NULL	该任务组的触发器：ASSIGN、UNASSIGN、DIRECTDEPLOY、DIRECTUNDEPLOY。 映射到 GDEPLOYMENT 类的 AC 属性 TRIGGER。

DISTRIBUTION_HOST 表的列

下表说明了 DISTRIBUTION_HOST 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。

名称	是否为 PK	数据类型	Null 选项	注释
DH	是	NVARCHAR2(256)	不为 NULL	映射到 AC 类 SEOS 的 DH 或 DHDR 属性内的单个元素，取决于 DHTYPE 列的值。
DHTYPE	是	NVARCHAR2(20)	不为 NULL	如果 DHTYPE 为“DR”，则 DH 列映射到 AC 类 SEOS 的 DHDR 属性内的单个元素。 如果 DHTYPE 为“NORMAL”，则映射到该类的 DH 属性。

EFFECTIVE_POLICY 表的列

下表说明了 EFFECTIVE_POLICY 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
NODE_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
NODE_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
POLICY_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
POLICY_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。

GROUPAUDIT 表的列

下表说明了 GROUPAUDIT 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）。
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。
SUCCESS	否	NUMBER(1,0)	NULL	审核成功事件
FAILURE	否	NUMBER(1,0)	NULL	审核失败事件
LOGONSUCCESS	否	NUMBER(1,0)	NULL	审核成功登录
LOGONFAILURE	否	NUMBER(1,0)	NULL	审核失败登录
DEBUG	否	NUMBER(1,0)	NULL	从调试模式开始记录
TRACE	否	NUMBER(1,0)	NULL	跟踪组

GROUPINFO 表的列

下表说明了 GROUPINFO 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）。 映射到 AC 组 OID 的 ONAME。
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。
DESCRIPTION	否	NVARCHAR2(256)	NULL	组说明和注释。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 COMMENT。

名称	是否为 PK	数据类型	Null 选项	注释
OWNERCNAME	否	NVARCHAR2(256)	NULL	如果资源记录的所有者的安全级别、安全标签和安全类别权限使其足以能够访问资源，则该所有者对该资源拥有不受限制的访问权限。 资源的所有者始终可以更新和删除资源记录。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 OWNER 的 CNAME。
OWNERONAME	否	NVARCHAR2(256)	NULL	映射到 AC 类 GROUP/XGROUP 的 AC 属性 OWNER 的 ONAME。
FULLNAME	否	NVARCHAR2(256)	NULL	与组关联的全名。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 FULL_NAME。
SUPGROUP	否	NVARCHAR2(256)	NULL	父组（“超级”组）的名称。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 SUPGROUP。
CALENDAR	否	NVARCHAR2(256)	NULL	指定 Unicenter TNG 日历对象，表示在 Unicenter TNG 中的时间限制。 AC 仅出于管理目的来维护这些对象的列表，但不对它们进行保护。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 CALENDAR。
CRETIME	否	TIMESTAMP(6)	NULL	创建时间。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 CREATE_TIME。
UPDTIME	否	TIMESTAMP(6)	NULL	上次修改记录的日期和时间。
UPDWHOCNAME	否	NVARCHAR2(256)	NULL	上次修改记录的日期和时间。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 UPDATE_TIME。
UPDWHOONAME	否	NVARCHAR2(256)	NULL	映射到 AC 类 GROUP/XGROUP 的 AC 属性 UPDATE_WHO 的 ONAME。
HOMEDIR	否	NVARCHAR2(256)	NULL	分配给新组成员的主目录。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 HOMEDIR。

名称	是否为 PK	数据类型	Null 选项	注释
EXPDATE	否	DATE	NULL	设置组成员帐号的过期日期。映射到 AC 类 GROUP/XGROUP 的 AC 属性 EXPIRE_DATE。
MAXLOGINS	否	NUMBER	NULL	设置用户可同时登录的最多终端数。 0（零）值表示用户可同时从任意数量的终端登录。映射到 AC 类 GROUP/XGROUP 的 AC 属性 MAXLOGINS。
INACTIVE	否	NUMBER	NULL	指定在系统将用户更改为非活动状态之前必须经过的天数。映射到 AC 类 GROUP/XGROUP 的 AC 属性 INACTIVE。
PROFUSRCNAME	否	NVARCHAR2(256)	NULL	映射到 AC 类 GROUP/XGROUP 的 AC 属性 PROFUSR 的 CNAME。
PROFUSRONAME	否	NVARCHAR2(256)	NULL	映射到 AC 类 GROUP/XGROUP 的 AC 属性 PROFUSR 的 ONAME。
PWDAUTOGEN	否	NUMBER(1,0)	NULL	指明应用程序的密码是否由策略服务器自动生成。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 PWD_AUTOGEN。
PWDSYNC	否	NUMBER(1,0)	NULL	指明应用程序的密码是否可以与用户的其他应用程序密码相同。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 PWD_SYNC。
PWPOLICY	否	NVARCHAR2(256)	NULL	应用程序密码策略的记录名称。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 PWPOLICY。

名称	是否为 PK	数据类型	Null 选项	注释
RESDATE	否	DATE	NULL	启用通过指定挂起参数禁用的用户记录 映射到 AC 类 GROUP/XGROUP 的 AC 属性 RESUME_DATE。
SHELL	否	NVARCHAR2(256)	NULL	指定在用户调用 login 或 su 命令后执行的初始程序或 shell 的完整路径。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 SHELL。
SUBGROUP	否	NVARCHAR2(256)	NULL	以该组为父组的组的列表。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 SUBGROUP。
SUSDATE	否	TIMESTAMP(6)	NULL	禁用用户记录，但将其保留在数据库中进行定义。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 SUSPEND_DATE。
SUSWHOCNAME	否	NVARCHAR2(256)	NULL	激活挂起日期的管理员的类。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 SUSPEND_WHO 的 CNAME。
SUSWHOONAME	否	NVARCHAR2(256)	NULL	激活挂起日期的管理员的对象名称。 映射到 AC 类 GROUP/XGROUP 的 AC 属性 SUSPEND_WHO 的 ONAME。
SECURITYID	否	NVARCHAR2(256)	NULL	该组条目特定于提供商的安全 ID。 映射到 AC 类 XGROUP 的 AC 属性 SECURITY_ID。

GROUPMEMBER 表的列

下表说明了 GROUPMEMBER 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）
CNAME	是	NVARCHAR2(256)	不为 NULL	成员的类名
ONAME	是	NVARCHAR2(256)	不为 NULL	成员的对象名
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。

GROUPREVACL 表的列

下表说明了 GROUPREVACL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。
RESCNAME	是	NVARCHAR2(80)	不为 NULL	资源类名
RESONAME	是	NVARCHAR2(256)	不为 NULL	资源对象名
CONCNAME	是	NVARCHAR2(80)	不为 NULL	条件类名（即 PROGRAM、HOST、CALENDAR）。 非空字符串表示条件对象存在于 RESINFO 表中。 连字符字符串 ('-') 表示“无条件”。
CONONAME	是	NVARCHAR2(256)	不为 NULL	条件对象名
ISALLOW	是	NVARCHAR2(256)	不为 NULL	

名称	是否为 PK	数据类型	Null 选项	注释
AREAD	否	NUMBER(1,0)	NULL	
AWRITE	否	NUMBER(1,0)	NULL	
AMODIFY	否	NUMBER(1,0)	NULL	
ACREATE	否	NUMBER(1,0)	NULL	
AERASE	否	NUMBER(1,0)	NULL	
AFILESCAN	否	NUMBER(1,0)	NULL	
ALANGINT	否	NUMBER(1,0)	NULL	
AEXEC	否	NUMBER(1,0)	NULL	
ACHOWN	否	NUMBER(1,0)	NULL	
ACHGRP	否	NUMBER(1,0)	NULL	
ACHMOD	否	NUMBER(1,0)	NULL	
AUTIMES	否	NUMBER(1,0)	NULL	
ASEC	否	NUMBER(1,0)	NULL	
AKILL	否	NUMBER(1,0)	NULL	
ACONNECT	否	NUMBER(1,0)	NULL	
ARENAME	否	NUMBER(1,0)	NULL	
APASSWORD	否	NUMBER(1,0)	NULL	
AAUTHORIZED	否	NUMBER(1,0)	NULL	
AXAUDIT	否	NUMBER(1,0)	NULL	
ACHDIR	否	NUMBER(1,0)	NULL	
ACRSUBK	否	NUMBER(1,0)	NULL	
ANOTIFY	否	NUMBER(1,0)	NULL	
AENUM	否	NUMBER(1,0)	NULL	
AQUERY	否	NUMBER(1,0)	NULL	
ARCTRL	否	NUMBER(1,0)	NULL	
ACRLINK	否	NUMBER(1,0)	NULL	
APRINT	否	NUMBER(1,0)	NULL	
AMANAGE	否	NUMBER(1,0)	NULL	
AMAXALLOWED	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
ASTOP	否	NUMBER(1,0)	NULL	
APAUSE	否	NUMBER(1,0)	NULL	
ACONTROL	否	NUMBER(1,0)	NULL	
ACHOG	否	NUMBER(1,0)	NULL	
ARESUME	否	NUMBER(1,0)	NULL	
DREAD	否	NUMBER(1,0)	NULL	
DWRITE	否	NUMBER(1,0)	NULL	
DMODIFY	否	NUMBER(1,0)	NULL	
DCREATE	否	NUMBER(1,0)	NULL	
DERASE	否	NUMBER(1,0)	NULL	
DFILESCAN	否	NUMBER(1,0)	NULL	
DLANGINT	否	NUMBER(1,0)	NULL	
DEXEC	否	NUMBER(1,0)	NULL	
DCHOWN	否	NUMBER(1,0)	NULL	
DCHGRP	否	NUMBER(1,0)	NULL	
DCHMOD	否	NUMBER(1,0)	NULL	
DUTIMES	否	NUMBER(1,0)	NULL	
DSEC	否	NUMBER(1,0)	NULL	
DKILL	否	NUMBER(1,0)	NULL	
DCONNECT	否	NUMBER(1,0)	NULL	
DRENAME	否	NUMBER(1,0)	NULL	
DPASSWORD	否	NUMBER(1,0)	NULL	
DAUTHORIZED	否	NUMBER(1,0)	NULL	
DXAUDIT	否	NUMBER(1,0)	NULL	
DCHDIR	否	NUMBER(1,0)	NULL	
DCRSUBK	否	NUMBER(1,0)	NULL	
DNOTIFY	否	NUMBER(1,0)	NULL	
DENUM	否	NUMBER(1,0)	NULL	
DQUERY	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
DRCTRL	否	NUMBER(1,0)	NULL	
DCRLINK	否	NUMBER(1,0)	NULL	
DPRINT	否	NUMBER(1,0)	NULL	
DMANAGE	否	NUMBER(1,0)	NULL	
DMAXALLOWED	否	NUMBER(1,0)	NULL	
DSTOP	否	NUMBER(1,0)	NULL	
DPAUSE	否	NUMBER(1,0)	NULL	
DCONTROL	否	NUMBER(1,0)	NULL	
DCHOG	否	NUMBER(1,0)	NULL	
DRESUME	否	NUMBER(1,0)	NULL	

GROUPS 表的列

下表说明了 GROUPS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
RESCLASS	是	NVARCHAR2(80)	不为 NULL	资源类名
RULEKEY	是	NVARCHAR2(256)	不为 NULL	资源对象名
ONAME	是	NVARCHAR2(256)	不为 NULL	组中参与对象的对象名
CNAME	是	NVARCHAR2(80)	不为 NULL	组中参与对象的类名

HOLDATE 表的列

下表说明了 HOLDATE 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(256)	不为 NULL	该记录的主机 ID

名称	是否为 PK	数据类型	Null 选项	注释
RESCLASS	是	NVARCHAR2(80)	不为 NULL	资源类名（必须为 HOLIDAY）
RULEKEY	是	NVARCHAR2(256)	不为 NULL	资源对象名
STARTDATE	是	TIMESTAMP(6)	不为 NULL	假期的开始日期
ENDDATE	是	TIMESTAMP(6)	不为 NULL	假期的结束日期
ALLDAY	是	NUMBER(1,0)	NULL	该假期是全天事件
EVERYYEAR	是	NUMBER(1,0)	NULL	每年均享有该假期

HOSTINFO 表的列

下表说明了 HOSTINFO 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
APPNAME	否	NVARCHAR2(24)	NULL	包含安全数据的安全应用程序的名称
APPIND	否	CHAR(1)	NULL	应用程序指示器。 指明该记录从属于哪个应用程序
APPVERSION	否	NVARCHAR2(24)	NULL	安全应用程序的版本
APPMODE	否	CHAR(1)	NULL	对于该记录有效的处理模式
LOADDATE	否	TIMESTAMP(6)	NULL	从安全数据库卸载安全信息的日期
BASE_HOSTID	否	NVARCHAR2(512)	NULL	包含的主机 ID（如果有）。

INETACL 表的列

下表说明了 INETACL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符

名称	是否为 PK	数据类型	Null 选项	注释
RESCLASS	是	NVARCHAR2(80)	不为 NULL	资源类名
RULEKEY	是	NVARCHAR2(256)	不为 NULL	资源对象名
SERVICENAME	是	NVARCHAR2(256)	不为 NULL	服务名称
PROTOCOLNAME	是	NVARCHAR2(256)	不为 NULL	协议名称
AREAD	否	NUMBER(1,0)	NULL	
AWRITE	否	NUMBER(1,0)	NULL	
AMODIFY	否	NUMBER(1,0)	NULL	
ACREATE	否	NUMBER(1,0)	NULL	
AERASE	否	NUMBER(1,0)	NULL	
AFILESCAN	否	NUMBER(1,0)	NULL	
ALANGINT	否	NUMBER(1,0)	NULL	
AEXEC	否	NUMBER(1,0)	NULL	
ACHOWN	否	NUMBER(1,0)	NULL	
ACHGRP	否	NUMBER(1,0)	NULL	
ACHMOD	否	NUMBER(1,0)	NULL	
AUTIMES	否	NUMBER(1,0)	NULL	
ASEC	否	NUMBER(1,0)	NULL	
AKILL	否	NUMBER(1,0)	NULL	
ACONNECT	否	NUMBER(1,0)	NULL	
ARENAME	否	NUMBER(1,0)	NULL	
APASSWORD	否	NUMBER(1,0)	NULL	
AAUTHORIZED	否	NUMBER(1,0)	NULL	
AXAUDIT	否	NUMBER(1,0)	NULL	
ACHDIR	否	NUMBER(1,0)	NULL	
ACRSUBK	否	NUMBER(1,0)	NULL	
ANOTIFY	否	NUMBER(1,0)	NULL	
AENUM	否	NUMBER(1,0)	NULL	
AQUERY	否	NUMBER(1,0)	NULL	
ARCTRL	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
ACRLINK	否	NUMBER(1,0)	NULL	
APRINT	否	NUMBER(1,0)	NULL	
AMANAGE	否	NUMBER(1,0)	NULL	
AMAXALLOWED	否	NUMBER(1,0)	NULL	
ASTOP	否	NUMBER(1,0)	NULL	
APAUSE	否	NUMBER(1,0)	NULL	
ACONTROL	否	NUMBER(1,0)	NULL	
ACHOG	否	NUMBER(1,0)	NULL	
ARESUME	否	NUMBER(1,0)	NULL	

INSERVRNGE 表的列

下表说明了 INSERVRNGE 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 AC：资源对象名
MINSERVICE	是	NUMBER	不为 NULL	最小端口号
MAXSERVICE	是	NUMBER	不为 NULL	最大端口号
AREAD	否	NUMBER(1,0)	NULL	
AWRITE	否	NUMBER(1,0)	NULL	
AMODIFY	否	NUMBER(1,0)	NULL	
ACREATE	否	NUMBER(1,0)	NULL	
AERASE	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
AFILESCAN	否	NUMBER(1,0)	NULL	
ALANGINT	否	NUMBER(1,0)	NULL	
AEXEC	否	NUMBER(1,0)	NULL	
ACHOWN	否	NUMBER(1,0)	NULL	
ACHGRP	否	NUMBER(1,0)	NULL	
ACHMOD	否	NUMBER(1,0)	NULL	
AUTIMES	否	NUMBER(1,0)	NULL	
ASEC	否	NUMBER(1,0)	NULL	
AKILL	否	NUMBER(1,0)	NULL	
ACONNECT	否	NUMBER(1,0)	NULL	
ARENAME	否	NUMBER(1,0)	NULL	
APASSWORD	否	NUMBER(1,0)	NULL	
AAUTHORIZED	否	NUMBER(1,0)	NULL	
AXAUDIT	否	NUMBER(1,0)	NULL	
ACHDIR	否	NUMBER(1,0)	NULL	
ACRSUBK	否	NUMBER(1,0)	NULL	
ANOTIFY	否	NUMBER(1,0)	NULL	
AENUM	否	NUMBER(1,0)	NULL	
AQUERY	否	NUMBER(1,0)	NULL	
ARCTRL	否	NUMBER(1,0)	NULL	
ACRLINK	否	NUMBER(1,0)	NULL	
APRINT	否	NUMBER(1,0)	NULL	
AMANAGE	否	NUMBER(1,0)	NULL	
AMAXALLOWED	否	NUMBER(1,0)	NULL	
ASTOP	否	NUMBER(1,0)	NULL	
APAUSE	否	NUMBER(1,0)	NULL	
ACONTROL	否	NUMBER(1,0)	NULL	
ACHOG	否	NUMBER(1,0)	NULL	
ARESUME	否	NUMBER(1,0)	NULL	

LOCAL_PMD_SUBSCRIBER 表的列

下表说明了 LOCAL_PMD_SUBSCRIBER 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
SUBSCRIBER_HOSTID	是	NVARCHAR2(256)	不为 NULL	订户策略模型。 映射到 sepmd -L selang 命令输出的“订户”列。
ERRORCOUNT	否	NUMBER	NULL	订阅错误计数。 映射到 sepmd -L selang 命令输出的“错误”列。
STATUS	否	NVARCHAR2(256)	NULL	订阅状态说明。 映射到 sepmd -L selang 命令输出的“标志”列。
OFFSET	否	NUMBER	NULL	分发的策略文件内的当前订阅偏移量。 映射到 sepmd -L selang 命令输出的“偏移量”列。
NEXTCOMMAND	否	NVARCHAR2(256)	NULL	分发的策略文件内的当前订阅命令。 映射到 sepmd -L selang 命令输出的“下一命令”列。

LOGINAPPL 表的列

下表说明了 LOGINAPPL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。

名称	是否为 PK	数据类型	Null 选项	注释
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
LOGINHOW	否	NVARCHAR2(256)	NULL	登录方法（伪登录、正常登录……）。 映射到 AC 类 LOGINAPPL 的 LOGINHOW 属性。
LOGINPATH	否	NVARCHAR2(256)	NULL	登录应用程序的完整路径（或通用路径）。 映射到 AC 类 LOGINAPPL 的 LOGINPATH 属性。
FNFSPGM	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINFLAG 属性的登录标志 NFSPGM。
FINOGRACE	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINFLAG 属性的登录标志 NOGRACE。
FINOGRACEROOT	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINFLAG 属性的登录标志 NOGRACEROOT。
FNOLOGIN	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINFLAG 属性的登录标志 NOLOGIN。
SSEID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 SEID 登录顺序。
SSUID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 SUID 登录顺序。
SSGID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 SGID 登录顺序。

名称	是否为 PK	数据类型	Null 选项	注释
SSGRP	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 SGRP 登录顺序。
SFEID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 FEID 登录顺序。
SFUID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 FUID 登录顺序。
SFGID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 FGID 登录顺序。
SFGRP	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 FGRP 登录顺序。
SN3EID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 N3EID 登录顺序。
SN3UID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 N3UID 登录顺序。
SN3GID	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 N3GID 登录顺序。
SN3GRP	否	NUMBER(1,0)	NULL	映射到 AC 类 LOGINAPPL 的 LOGINSEQUENCE 属性的 N3GRP 登录顺序。

MEMBEROF 表的列

下表说明了 MEMBEROF 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID

名称	是否为 PK	数据类型	Null 选项	注释
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）
CNAME	是	NVARCHAR2(256)	不为 NULL	类名
ONAME	是	NVARCHAR2(256)	不为 NULL	对象名
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。

MEMBERS 表的列

下表说明了 MEMBERS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 AC：资源对象名
CNAME	是	NVARCHAR2(80)	不为 NULL	成员的类名
ONAME	是	NVARCHAR2(256)	不为 NULL	成员的对象名

NODE 表的列

下表说明了 NODE 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID

名称	是否为 PK	数据类型	Null 选项	注释
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
KEEPALIVE	是	TIMESTAMP(6)	NULL	上次活动时间。 映射到 AC 类 HNODE 的 AC 属性 HNODE_KEEP_ALIVE。
VERSION	是	NUMBER	NULL	节点版本。 映射到 AC 类 HNODE 的 AC 属性 HNODE_VERSION。
ACID	是	NVARCHAR2(256)	NULL	唯一的 AC 主机 ID。 映射到 AC 类 HNODE 的 ACID 属性。

NODE_ADDRESS 表的列

下表说明了 NODE_ADDRESS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
ADDRESS	是	NVARCHAR2(256)	不为 NULL	

NODE_ALIAS 表的列

下表说明了 NODE_ALIAS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
ALIAS	是	NVARCHAR2(256)	不为 NULL	节点别名。 映射到 AC 类 HNODE 的 ALIAS 属性内的单个字符串。

NODE_DEVIATION 表的列

下表说明了 NODE_DEVIATION 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。

名称	是否为 PK	数据类型	Null 选项	注释
DATA	是	CLOB	NULL	原始偏差数据。 在 DEVCALC 输出开始时映射到 DEVCALC 标头，即第一个 POLICYSTART 标签前的所有数据。

NODE_SUBSCRIPTION_STATUS 表的列

下表说明了 NODE_SUBSCRIPTION_STATUS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
PUBLISHERCNAME	是	NVARCHAR2(80)	不为 NULL	发布节点 CNAME
SUBSCRIBERCNAME	是	NVARCHAR2(80)	不为 NULL	订阅节点 CNAME。 映射到 AC 类 HNODE 的 SUBSCRIBER_STATUS 属性的 Subscriber OID 组件的类名称。
PUBLISHERONAME	是	NVARCHAR2(256)	不为 NULL	发布节点 ONAME
SUBSCRIBERONAME	是	NVARCHAR2(256)	不为 NULL	订阅节点 ONAME。 映射到订户 OID 的对象名称。
STATUS	否	NVARCHAR2(256)	NULL	订阅状态。 映射到 AC 类 HNODE 的 SUBSCRIBER_STATUS 属性的 Status 组件。
LASTSTATUSTIME	否	TIMESTAMP(6)	NULL	上次状态更新时间。 映射到 AC 类 HNODE 的 SUBSCRIBER_STATUS 属性的 Last Status Time 组件。

PASSWDRULES 表的列

下表说明了 PASSWDRULES 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。
ISSEOS	是	NUMBER(1,0)	不为 NULL	此密码规则记录是否与 SEOS 表中的记录相关？ 当（且仅当）此记录与 SEOS 记录相关联，而不与 GROUPINFO 记录相关联时，ISSEOS 为 1。ISSEOS 为 1 时，GROUPID 和 GROUPTYPE 为空
MINLEN	否	NUMBER	NULL	最小长度
MAXREP	否	NUMBER	NULL	最大单个字符重复数
MUSTSMALL	否	NUMBER	NULL	必须包含小写字符
MUSTCAPITAL	否	NUMBER	NULL	必须包含大写字母
MUSTNUM	否	NUMBER	NULL	必须包含数字
MUSTOTH	否	NUMBER	NULL	必须包含其他字符
MUSTALFA	否	NUMBER	NULL	必须包含至少 # 个字母字符
MUSTALFAN	否	NUMBER	NULL	必须包含至少 # 个字母数字字符
SUBNAME	否	NUMBER	NULL	不能是用户名的子字符串
SUBOLD	否	NUMBER	NULL	不能是旧密码的子字符串
SUBSTRLEN	否	NUMBER	NULL	密码中重复子字符串的最大长度
SUBSTRREP	否	NUMBER	NULL	子字符串的最大重复数
PASSWDLIFE	否	NUMBER	NULL	密码更改之间的默认天数

名称	是否为 PK	数据类型	Null 选项	注释
GRACELOGINS	否	NUMBER	NULL	密码到期之后的宽限登录次数
USERBLOCKMIN	否	NUMBER	NULL	阻止用户输入密码的分钟数
WRONGPASS	否	NUMBER	NULL	设置到期之前错误密码尝试次数
HISTORY	否	NUMBER	NULL	历史记录长度
MINTIME	否	NUMBER	NULL	更改之间的最少时间（天数）
MAXLEN	否	NUMBER	NULL	最大长度
DICTFORMAT	否	NUMBER	NULL	选择字典格式
BIDIRECTIONAL	否	NUMBER	NULL	启用或禁用双向密码加密。 如果启用双向密码加密，会为每个新密码加密，并可将其解密为明文。 这种加密可使新密码和旧密码（密码历史记录）之间进行更广泛的比较。 禁用双向加密时，将激活单向密码历史加密，且不能为旧密码加密。

POLICY 表的列

下表说明了 POLICY 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	yes	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。

名称	是否为 PK	数据类型	Null 选项	注释
NAME	是	NVARCHAR2(256)	NULL	策略的逻辑名。 映射到 AC 类 POLICY 的 AC 属性 POLICY_BASE_NAME。
VERSION	是	NUMBER	NULL	整数，表示策略版本。 策略版本是连续数字，从 1 开始。 映射到 AC 类 POLICY 的 AC 属性 POLICY_VERSION。
FINALIZE	否	NUMBER(1,0)	NULL	策略是否已最终确定（即，可部署？）。 映射到 AC 类 POLICY 的 AC 属性 FINALIZE。
EXTENDED_SIGNATURE	否	NVARCHAR2(256)	NULL	FIPS 140-2 遵从 SHA1 策略签名。 映射到 AC 类 POLICY 的 EXTENDED_SIGNATURE 属性。
SIGNATURE	否	NVARCHAR2(256)	NULL	策略签名。 映射到 AC 类 POLICY 的 SIGNATURE 属性。

POLICY_DEVIATION 表的列

下表说明了 POLICY_DEVIATION 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
NODE_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。
NODE_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源 掩码。 AC：资源对象名
DEVIATION_INDEX	是	NUMBER	不为 NULL	偏差行序号，每个策略从 0 开始。 映射到该偏差行的行号，相对于 DEVCALC 输出中的最新 POLICYSTART 标签。

名称	是否为 PK	数据类型	Null 选项	注释
DEVIATED_CLASS	否	NVARCHAR2(256)	NULL	偏差的类。 映射到 DEVCALC 输出中 DIFF 行的第二个标记。 NULL 值映射至 DEVCALC 输出中的值 (*)。
DEVIATED_OBJECT	否	NVARCHAR2(256)	NULL	偏差的对象。 映射到 DEVCALC 输出中 DIFF 行的第三个标记。 NULL 值映射至 DEVCALC 输出中的值 (*)。
DEVIATED_PROPERTY	否	NVARCHAR2(256)	NULL	偏差的属性。 映射到 DEVCALC 输出中 DIFF 行的第四个标记。 NULL 值映射至 DEVCALC 输出中的值 (*)。
DEVIATED_VALUE	否	NVARCHAR2(256)	NULL	偏差的值。 映射到 DEVCALC 输出中 DIFF 行的第五个标记。 NULL 值映射至 DEVCALC 输出中的值 (*)。
DEVIATION_DATA	否	CLOB	NULL	对于类型为已知（即与“UNKNOWN_%”不同）的偏差行，该值映射到 DEVCALC 输出 DIFF 行的第一个标记，例如“DIFF”。 对于其他偏差行，该字段按原样包含则整个 DEVCALC 行。
DEVIATION_TYPE	否	NVARCHAR2(256)	NULL	偏差类型，格式为 A_B，其中： A = EXPECTED 或 UNEXPECTED 或 UNKNOWN B = CLASS 或 OBJECT 或 PROPERTY 或 VALUE 或 GENERIC

POLICY_GROUP 表的列

下表说明了 POLICY_GROUP 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
LATEST_FIN_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到 GPOLICY 类的 OID AC 属性 LATEST_FINALIZED_VERSION 的 ONAME。
LATEST_FIN_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 GPOLICY 类的 OID AC 属性 LATEST_FINALIZED_VERSION 的 CNAME。
LATEST_RESCLASS	否	NVARCHAR2(80)	NULL	应用该权限的实体的资源类。 映射到 GPOLICY 类的 OID AC 属性 LATEST_VERSION 的 CNAME。

名称	是否为 PK	数据类型	Null 选项	注释
LATEST_RULEKEY	否	NVARCHAR2(256)	NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到 GPOLICY 类的 OID AC 属性 LATEST_VERSION 的 ONAME。

POLICY_GROUP_DEPENDENCY 表的列

下表说明了 POLICY_GROUP_DEPENDENCY 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
DEP_ON_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
DEP_ON_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源 掩码。 映射到资源的 AC OID 的 ONAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源 掩码。 映射到资源的 AC OID 的 ONAME。

POLICY_GROUP_NODE_ASSIGNMENT 表的列

下表说明了 POLICY_GROUP_NODE_ASSIGNMENT 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
POLICYGRP_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
POLICYGRP_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
NODE_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。 如果该字段等于“HNODE”，则此为节点分配。 如果该字段等于“GHNODE”，则此为节点组分配。
NODE_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 AC：资源对象名

POLICY_RULESET 表的列

下表说明了 POLICY_RULESET 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。

名称	是否为 PK	数据类型	Null 选项	注释
POLICY_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
POLICY_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
RULESET_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULESET_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。

POLICY_STATUS 表的列

下表说明了 POLICY_STATUS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
NODE_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
NODE_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。

名称	是否为 PK	数据类型	Null 选项	注释
POLICY_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
POLICY_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
UPDATORTYPE	是	NVARCHAR2(80)	NULL	该用户的类：USER、XUSER
UPDATORID	是	NVARCHAR2(256)	NULL	系统中该对象的标识符。
STATUS	否	NVARCHAR2(256)	NULL	策略状态：APPROVED、REJECTED、PROCESSING。
DEVSTATE	否	NVARCHAR2(20)	NULL	偏差状态：UNSET、YES、NO
LASTDEVTIME	否	TIMESTAMP(6)	NULL	上次偏差计算时间
LASTSTATUSTIME	否	TIMESTAMP(6)	NULL	已设置上次时间状态
UPDATORNAME	否	NVARCHAR2(256)	NULL	策略更新程序名。 映射到 AC 类 POLICY 的 POLICY_STATUS 属性的 UpdatorName 成员。
UPDATORID	否	NVARCHAR2(256)	NULL	更新程序对象名称。 映射到 AC 类 POLICY 的 POLICY_STATUS 属性的更新程序成员的 ONAME 组件。
UPDATORTYPE	否	NVARCHAR2(256)	NULL	更新程序对象名称。 映射到 AC 类 POLICY 的 POLICY_STATUS 属性的更新程序成员的 CNAME 组件。

POLICYMODELINFO 表的列

下表说明了 POLICYMODELINFO 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
INITIAL_POLICY_OFFSET	否	NUMBER	NULL	对于本地节点，此项将按照 sepmd -L selang 命令提供的结果映射到初始策略偏移量。
LAST_POLICY_OFFSET	否	NUMBER	NULL	对于本地节点，此项将按照 sepmd -L selang 命令提供的结果映射到最后策略偏移量。

RAUDIT 表的列

下表说明了 RAUDIT 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源 掩码。 AC：资源对象名
AUDITSUCCESS	是	NUMBER(1,0)	NULL	AC 记录对资源的授权访问
AUDITFAILURE	是	NUMBER(1,0)	NULL	AC 记录检测到的未经授权的访问尝试
DEBUG	否	NUMBER(1,0)	NULL	从调试模式开始记录

名称	是否为 PK	数据类型	Null 选项	注释
TRUST	否	NUMBER(1,0)	NULL	审核信任事件

RESAC 表的列

下表说明了 RESAC 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
DESCRIPTION	否	NVARCHAR2(256)	NULL	记录的说明/注释。 映射到相关 AC 资源类的 AC 属性 COMMENT。
CALENDAR	否	NVARCHAR2(256)	NULL	指定 Unicenter TNG 日历对象，表示在 Unicenter TNG 中的时间限制。 AC 仅出于管理目的来维护这些对象的列表，但不对它们进行保护。 映射到相关 AC 资源类的 AC 属性 CALENDAR。
NOTIFY	否	NVARCHAR2(256)	NULL	只要该资源记录代表的资源被访问，程序便指示 AC 发送通知消息。 请输入用户名、用户的电子邮件地址或邮件组的电子邮件地址（如果指定了别名）。 映射到相关 AC 资源类的 AC 属性 NOTIFY。

名称	是否为 PK	数据类型	Null 选项	注释
SECLABEL	否	NVARCHAR2(256)	NULL	安全标签代表特定安全级别与零个或多个安全类别之间的关联。 映射到相关 AC 资源类的 AC 属性 SECLABEL。
SECLEVEL	否	NUMBER	NULL	安全级别。 映射到相关 AC 资源类的 AC 属性 SECLEVEL。
CRETIME	否	TIMESTAMP(6)	NULL	创建时间。 映射到相关 AC 资源类的 AC 属性 CREATE_TIME。
WARNING	否	NUMBER(1,0)	NULL	指定即使访问者的权限不足以访问资源，AC 也将允许访问资源。 但是，AC 会在审核日志中写入警告消息。 映射到相关 AC 资源类的 AC 属性 WARNING。
UNTRUST	否	NUMBER(1,0)	NULL	指明程序是否受信任。 如果设置了该属性，就没有人可以运行该程序。 如果没有设置该属性，则使用数据库中为该程序列出的其他属性确定是否授权用户运行程序。 如果以任何方式更改了受信任的程序，AC 会自动正确设置该属性。 映射到相关 AC 资源类（例如：PROGRAM、SECFILE 和 HOST）的 AC 属性 UNTRUST。
ETHINFO	否	NVARCHAR2(256)	NULL	主机的以太网信息。 映射到 AC 资源类 HOST 的 AC 属性 ETHINFO。
NETMATCH	否	NVARCHAR2(256)	NULL	IP 地址匹配。 映射到 AC 资源类 HOSTNET 的 AC 属性 INMASKMATCH 的 NetworkMatch 组件。

名称	是否为 PK	数据类型	Null 选项	注释
NETMASK	否	NVARCHAR2(256)	NULL	IP 地址掩码。 映射到 AC 资源类 HOSTNET 的 AC 属性 INMASKMATCH 的 Mask 组件。
AAUDIT	否	NVARCHAR2(256)	NULL	显示 eTrust AC 正在审核的活动类型。 映射到 AC 资源类 ADMIN 的 AC 属性 AAUDIT。
UNTRUSTREASON	否	NVARCHAR2(256)	NULL	仅在 UNIX dbdump 中。 映射到 AC 资源类 PROGRAM、SECFILE 的 AC 属性 UNTRUSTREASON。
ACCSWHO	否	NUMBER(20,0)	NULL	访问对象名。 上次访问该记录的管理员。 映射到 AC 资源类 PROGRAM 的 AC 属性 ACCSWHO。 对于 Unix，包含 UID（数字值）。 对于 Windows，包含用户名。
ACCSTIME	否	TIMESTAMP(6)	NULL	访问对象时间（仅 UNIX）上次访问记录的日期和时间。 映射到 AC 资源类 PROGRAM 的 AC 属性 ACCSTIME。
BLOCKRUN	否	NUMBER(1,0)	NULL	阻止运行。 映射到 AC 资源类 PROGRAM 的 AC 属性 BLOCKRUN。
UNIXUID	否	NVARCHAR2(256)	NULL	UNIX UID。 映射到 AC 资源类 SPECIALPGM 的 AC 属性 UNIXUID。

名称	是否为 PK	数据类型	Null 选项	注释
INTERACTIVE	否	NUMBER(1,0)	NULL	交互。 要通过 sesudo 运行的应用程序为交互 Windows 应用程序（例如：notepad.exe、cmd.exe）而不是服务应用程序时，应对该选项做出标记。 如果尝试通过 sesudo 客户端命令运行交互应用程序，且未标记为“交互”时，程序将在后台运行且无法与其交互。 映射到 AC 资源类 SUDO 的 AC 属性 INTERACTIVE。
TARGUSRCNAME	否	NVARCHAR2(80)	NULL	指定用户名，SUDO 类将借用该用户的权限来执行命令。 默认为 administrator（针对 SUDO 类）。 映射到 AC 资源类 SUDO（仅限 UNIX）的 AC 属性 TARGUSR 的 CNAME。
TARGUSRONAME	否	NVARCHAR2(256)	NULL	映射到 AC 资源类 SUDO（仅限 UNIX）的 AC 属性 TARGUSR 的 ONAME。
PASSWDREQ	否	NUMBER(1,0)	NULL	需要密码。 指明 sesudo 命令是否在执行前请求目标用户密码。 映射到 AC 资源类 SUDO（仅限 UNIX）的 AC 属性 PASSWDREQ。
FILEPATH	否	NVARCHAR2(256)	NULL	映射到 AC 资源类 KMODULE 的 AC 属性 FILEPATH。

RESAC 表的列

下表说明了 RESINFO 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。映射到资源的 AC OID 的 ONAME。
PREFIX	否	NVARCHAR2(40)	NULL	（仅限 CA-ACF2）：规则集中的前缀字段。
OWNERCNAME	否	NVARCHAR2(80)	NULL	这是该资源的所有者类。 如果资源记录的所有者的安全级别、安全标签和安全类别权限使其足以能够访问资源，则该所有者对该资源拥有不受限制的访问权限。 资源的所有者始终可以更新和删除资源记录。 “GROUP”或“XGROUP”的值表示相关的记录在 GROUPINFO 表中。 “USER”或“XUSER”表示其在 USERINFO 表中。 映射到相关 AC 资源类的 OWNER 属性的 CNAME。
OWNERONAME	否	NVARCHAR2(256)	NULL	这是该资源所有者的对象名称。 映射到相关 AC 资源类的 OWNER 属性的 ONAME。
OWNRTYPE	否	CHAR(1)	NULL	指明该资源的所有者是用户 (U) 还是角色 (R)。 映射到相关 AC 资源类 OWNER 属性的 CNAME 的第一个字符。

名称	是否为 PK	数据类型	Null 选项	注释
RESOWNER	否	NVARCHAR2(256)	NULL	CA-ACF2：来自规则集的 $RESOWNER 值。 CA Top Secret：SMS RESOWNER。
RULEOWNER	否	NVARCHAR2(256)	NULL	仅限 CA ACF2。 来自规则集的 $OWNER 值。
ADMINBYCNAME	否	NVARCHAR2(80)	NULL	CA ACF2 和 AC：上次对该规则集进行更改的管理员类。 “GROUP”或“XGROUP”的值表示相关的记录在 GROUPINFO 表中。 “USER”或“XUSER”表示其在 USERINFO 表中。 映射到相关 AC 资源类的 UPDATE_WHO 属性的 CNAME。
ADMINBYONAME	否	NVARCHAR2(256)	NULL	上次对该规则集进行更改的管理员的对象名称。 映射到相关 AC 资源类的 UPDATE_WHO 属性的 ONAME。
ADMINDATE	否	TIMESTAMP(6)	NULL	CA ACF2 和 AC。 上次更改该规则集的日期。 映射到相关 AC 资源类的 AC 属性 UPDATE_TIME。
USERDATA	否	NVARCHAR2(256)	NULL	仅限 CA ACF2。 来自规则集的 $USERDATA 值。
ON_BEHALF_OF	否	NVARCHAR2(256)	NULL	有效用户 ID。 映射到各个 AC 类（例如：DEPLOYMENT、GDEPLOYMENT、HNODE、GHNODE、POLICY、GPOLICY、RULEKEY）的 AC 属性 ON_BEHALF_OF

RULESET 表的列

下表说明了 RULESET 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 映射到资源的 AC OID 的 ONAME。
FINALIZE	否	NUMBER(1,0)	NULL	此规则集是否已最终确定（即，可部署？）。 映射到 AC 类 RULESET 的 AC 属性 FINALIZE。
EXTENDED_SIGNATURE	否	NVARCHAR2(256)	NULL	FIPS 140-2 遵从 SHA1 规则集签名。 映射到 AC 类 RULESET 的 EXTENDED_SIGNATURE 属性。
SIGNATURE	否	NVARCHAR2(256)	NULL	规则集签名。 映射到 AC 类 RULESET 的 SIGNATURE 属性。

RULESET_COMMAND 表的列

下表说明了 RULESET_COMMAND 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RULESET_RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。 映射到资源的 AC OID 的 CNAME。

名称	是否为 PK	数据类型	Null 选项	注释
RULESET_RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。映射到资源的 AC OID 的 ONAME。
COMMANDIDX	是	NUMBER	不为 NULL	规则集命令已排序。 此列表示命令在命令顺序中的位置。 映射到 AC 类 RULESET 的 AC 属性 RULESET_DO/UNDOCMDS 的命令索引组件（有关详细信息，请参阅 COMMANDTYPE 列）
COMMANDTYPE	是	NVARCHAR2(20)	不为 NULL	命令类型：do、undo。 如果类型为“do”，则该记录映射到 AC 类 RULESET 的 AC 属性 RULESET_DOCMDS 中的命令。 如果类型为“undo”，记录则映射到 RULESET_UNDOCMDS 属性。
COMMANDSTR	是	NVARCHAR2(256)	NULL	命令字符串。 映射到 AC 类 RULESET 的 AC 属性 RULESET_DO/UNDOCMDS 的命令字符串组件（有关详细信息，请参阅 COMMANDTYPE 列）

SEOS 表的列

下表说明了 SEOS 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符

名称	是否为 PK	数据类型	Null 选项	注释
LASTSTARTUP	否	TIMESTAMP(6)	NULL	主机上次启动时间。 映射到 AC 类 SEOS 的 AC 属性 STARTTIME。
LASTSHUTDOWN	否	TIMESTAMP(6)	NULL	主机上次关闭时间。 映射到 AC 类 SEOS 的 AC 属性 ENDTIME。
UPDATEDBY	否	NVARCHAR2(256)	NULL	上次按对象名更新。 映射到 AC 类 SEOS 的 AC 属性 UPDATE_WHO 的 ONAME。
UPDATETIME	否	TIMESTAMP(6)	NULL	上次更新时间。 映射到 AC 类 SEOS 的 AC 属性 UPDATE_TIME。
INACTIVEDAYS	否	NUMBER	NULL	非活动天数。 映射到 AC 类 SEOS 的 AC 属性 INACT。
ACCUMACL	否	NUMBER(1,0)	NULL	累积 ACL 和 PACL。 映射到 AC 类 SEOS 的 AC 属性 ACCPACL。
ACCUMGRPRIGHTS	否	NUMBER(1,0)	NULL	累积组权限。 映射到 AC 类 SEOS 的 AC 属性 GRACCR。
ADMINPWDCHANGE	否	NUMBER(1,0)	NULL	管理员密码更改。 映射到 AC 类 SEOS 的 AC 属性 CNG_ADMIN_PWD。
OWNPWDCHANGE	否	NUMBER(1,0)	NULL	自己的密码更改。 映射到 AC 类 SEOS 的 AC 属性 CNG_OWN_PWD。
ISDMA	否	NUMBER(1,0)	NULL	是否是 DMS 主机。 映射到 AC 类 SEOS 的 AC 属性 ISDMA。
ISDMS	否	NUMBER(1,0)	NULL	是否是 DMS 主机。 映射到 AC 类 SEOS 的 AC 属性 ISDMS。
ISDH	否	NUMBER(1,0)	NULL	分发主机 (DH) 映射到 AC 类 SEOS 的 AC 属性 ISDH。

名称	是否为 PK	数据类型	Null 选项	注释
DMS	否	NVARCHAR2(256)	NULL	DMS 主机名。 映射到 AC 类 SEOS 的 AC 属性 DMS。
CADMIN	否	NUMBER(1,0)	NULL	类激活：ADMIN。 映射到 AC 类 SEOS 的 AC 属性 ADMIN。
CAPPL	否	NUMBER(1,0)	NULL	类激活：APPL。 映射到 AC 类 SEOS 的 AC 属性 APPL。
CAUTHHOST	否	NUMBER(1,0)	NULL	类激活：AUTHHOST。 映射到 AC 类 SEOS 的 AC 属性 AUTHHOST。
CCALENDAR	否	NUMBER(1,0)	NULL	类激活：CALENDAR。 映射到 AC 类 SEOS 的 AC 属性 CALENDAR。
CCATEGORY	否	NUMBER(1,0)	NULL	类激活：CATEGORY。 映射到 AC 类 SEOS 的 AC 属性 CATEGORY。
CCONNECT	否	NUMBER(1,0)	NULL	类激活：CONNECT。 映射到 AC 类 SEOS 的 AC 属性 CONNECT。
CDEPLOYMENT	否	NUMBER(1,0)	NULL	类激活：DEPLOYMENT。 映射到 AC 类 SEOS 的 AC 属性 DEPLOYMENT。
CDICTIONARY	否	NUMBER(1,0)	NULL	类激活：DICTIONARY。 映射到 AC 类 SEOS 的 AC 属性 DICTIONARY。
CDOMAIN	否	NUMBER(1,0)	NULL	类激活：DOMAIN。 映射到 AC 类 SEOS 的 AC 属性 DOMAIN。
CFILE	否	NUMBER(1,0)	NULL	类激活：FILE。 映射到 AC 类 SEOS 的 AC 属性 FILE。
CHNODE	否	NUMBER(1,0)	NULL	类激活：HNODE。 映射到 AC 类 SEOS 的 AC 属性 HNODE。

名称	是否为 PK	数据类型	Null 选项	注释
CHOLIDAY	否	NUMBER(1,0)	NULL	类激活：HOLIDAY。 映射到 AC 类 SEOS 的 AC 属性 HOLIDAY。
CHOST	否	NUMBER(1,0)	NULL	类激活：HOST。 映射到 AC 类 SEOS 的 AC 属性 HOST。
CKMODULE	否	NUMBER(1,0)	NULL	类激活：KMODULE。 映射到 AC 类 SEOS 的 AC 属性 KMODULE。
CMFTERMINAL	否	NUMBER(1,0)	NULL	类激活：MFTERMINAL。 映射到 AC 类 SEOS 的 AC 属性 MFTERMINAL。
CPASSWORD	否	NUMBER(1,0)	NULL	类激活：PASSWORD。 映射到 AC 类 SEOS 的 AC 属性 PASSWORD。
CPOLICY	否	NUMBER(1,0)	NULL	类激活：POLICY。 映射到 AC 类 SEOS 的 AC 属性 POLICY。
CPROGRAM	否	NUMBER(1,0)	NULL	类激活：PROGRAM。 映射到 AC 类 SEOS 的 AC 属性 PROGRAM。
CPROCESS	否	NUMBER(1,0)	NULL	类激活：PROCESS。 映射到 AC 类 SEOS 的 AC 属性 PROCESS。
CPWPOLICY	否	NUMBER(1,0)	NULL	类激活：PWPOLICY。 映射到 AC 类 SEOS 的 AC 属性 PWPOLICY。
CREGKEY	否	NUMBER(1,0)	NULL	类激活：REGKEY。 映射到 AC 类 SEOS 的 AC 属性 REGKEY。
CREGVAL	否	NUMBER(1,0)	NULL	类激活：REGVAL。 映射到 AC 类 SEOS 的 AC 属性 REGVAL。
CRULESET	否	NUMBER(1,0)	NULL	类激活：RULESET。 映射到 AC 类 SEOS 的 AC 属性 RULESET。

名称	是否为 PK	数据类型	Null 选项	注释
CSECLABEL	否	NUMBER(1,0)	NULL	类激活：SECLABEL。 映射到 AC 类 SEOS 的 AC 属性 SECLABEL。
CSECLEVEL	否	NUMBER(1,0)	NULL	类激活：SECLEVEL。 映射到 AC 类 SEOS 的 AC 属性 SECLEVEL。
CSPECIALPGM	否	NUMBER(1,0)	NULL	类激活：SPECIALPGM。 映射到 AC 类 SEOS 的 AC 属性 SPECIALPGM。
CSUDO	否	NUMBER(1,0)	NULL	类激活：SUDO。 映射到 AC 类 SEOS 的 AC 属性 SUDO。
CSURROGATE	否	NUMBER(1,0)	NULL	类激活：SURROGATE。 映射到 AC 类 SEOS 的 AC 属性 SURROGATE。
CTCP	否	NUMBER(1,0)	NULL	类激活：TCP。 映射到 AC 类 SEOS 的 AC 属性 TCP。
CTERMINAL	否	NUMBER(1,0)	NULL	类激活：TERMINAL。 映射到 AC 类 SEOS 的 AC 属性 TERMINAL。
CUSER_DIR	否	NUMBER(1,0)	NULL	类激活：USER_DIR。 映射到 AC 类 SEOS 的 AC 属性 USER_DIR。
CWEBSERVICE	否	NUMBER(1,0)	NULL	类激活：WEBSERVICE。 映射到 AC 类 SEOS 的 AC 属性 WEBSERVICE。
CWINSERVICE	否	NUMBER(1,0)	NULL	仅限 Windows：类激活：WINSERVICE。 映射到 AC 类 SEOS 的 AC 属性 WINSERVICE。
CDAYTIMERES	否	NUMBER(1,0)	NULL	仅限 UNIX：是否检查时间限制。 映射到 AC 类 SEOS 的 AC 属性 DAYTIMERES。

名称	是否为 PK	数据类型	Null 选项	注释
CLOGINAPPL	否	NUMBER(1,0)	NULL	仅限 UNIX。 映射到 AC 类 SEOS 的 AC 属性 LOGINAPPL。
MAXLOGINS	否	NUMBER	NULL	最大有效登录数。 映射到 AC 类 SEOS 的 AC 属性 MAXLOGINS。
PROHIBITED	否	NVARCHAR2(256)	NULL	映射到 AC 类 SEOS 的 AC 属性 PROHIBITED。
ACID	否	NVARCHAR2(256)	NULL	唯一的 AC 主机 ID。 映射到 AC 类 SEOS 的 ACID 属性。 此项用于识别具有同一 ACID 的 NODE 表中的节点。

SEOSSYSCALL 表的列

下表说明了 SEOSSYSCALL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
INTERCEPTEDSYSCALLS	否	NUMBER(20,0)	NULL	截获的 syscall 数
NONBLOCKINGSYSCALLS	否	NUMBER(1,0)	NULL	已截获的无“危险” syscall 数
ISOVERFLOW	否	NUMBER(20,0)	NULL	1（如果分配的缓冲区太小）
THRESHOLDTIME	否	NUMBER(20,0)	NULL	syscall 的“危险”时间（秒）
ALWAYSEXITSCRIPT	否	NUMBER(1,0)	NULL	1（如果存在 SEOS_unload_int.always）
OPTIONALEXITSCRIPT	否	NUMBER(1,0)	NULL	1（如果存在 SEOS_unload_int.opt）

名称	是否为 PK	数据类型	Null 选项	注释
USETRIPACCEPT	否	NUMBER(1,0)	NULL	1（如果 use_tripAccept 标记为“yes”）
TRIPACCEPT	否	NUMBER(1,0)	NULL	1（如果存在 bin/tripAccept）
NOVELLZMD	否	NUMBER(1,0)	NULL	1（如果存在 /etc/init.d/novell-zmd）
XM	否	NUMBER(1,0)	NULL	1（如果存在 /usr/sbin/xm）
NSCD	否	NUMBER(1,0)	NULL	1（如果存在 /etc/init.d/nscd）

SNAPSHOTINFO 表的列

下表说明了 SNAPSHOTINFO 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
DUMPSTARTTIME	否	TIMESTAMP(6)	NULL	快照开始时间
DUMPENDTIME	否	TIMESTAMP(6)	NULL	快照结束时间
STATUS	否	CHAR(1)	NULL	快照状态
SNAPSHOTTIME	否	TIMESTAMP(6)	NULL	
SNAPSHOTTYPE	否	NVARCHAR2(256)	NULL	
SNAPSHOTNAME	否	NVARCHAR2(256)	NULL	
OS	否	NVARCHAR2(100)	NULL	
ACVERSION	否	NVARCHAR2(50)	NULL	
ACVERSIONNUM1	否	NUMBER(20,0)	NULL	
ACVERSIONNUM2	否	NUMBER(20,0)	NULL	
ACVERSIONNUM3	否	NUMBER(20,0)	NULL	
ACVERSIONNUM4	否	NUMBER(20,0)	NULL	

SPECIALPGMTYPE 表的列

下表说明了 SPECIALPGMTYPE 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 AC：资源对象名
TMAIL	否	NUMBER(1,0)	NULL	
TBACKUP	否	NUMBER(1,0)	NULL	
TXDM	否	NUMBER(1,0)	NULL	
TDCM	否	NUMBER(1,0)	NULL	
TPBF	否	NUMBER(1,0)	NULL	
TPBN	否	NUMBER(1,0)	NULL	
TPROPAGATE	否	NUMBER(1,0)	NULL	(r12.0 SP1)
TSTOP	否	NUMBER(1,0)	NULL	
TSURR	否	NUMBER(1,0)	NULL	
TREG	否	NUMBER(1,0)	NULL	
TRESTRICTED	否	NUMBER(1,0)	NULL	

SYSCALL 表的列

下表说明了 SYSCALL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID

名称	是否为 PK	数据类型	Null 选项	注释
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
PID	是	NUMBER(20,0)	不为 NULL	键：进程 pid
PARENTPID	否	NUMBER(20,0)	NULL	父进程 ID
USERID	否	NUMBER(20,0)	NULL	真实用户 ID
GROUPID	否	NUMBER(20,0)	NULL	组 ID
INTERCEPTEDPGM	否	NVARCHAR2(256)	NULL	程序名
INTERCEPTEDTIME	否	NUMBER(20,0)	NULL	syscall 的存在时间
SYSCALLNUM	否	NUMBER(20,0)	NULL	系统调用数目
ISBLOCKING	否	NUMBER(1,0)	NULL	1（如果 syscall 很危险）

SYSCALLUSERSPECIALPGM 表的列

下表说明了 SYSCALLUSERSPECIALPGM 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
SAFEPGM	是	NVARCHAR2(256)	不为 NULL	

UACC 表的列

下表说明了 UACC 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符

名称	是否为 PK	数据类型	Null 选项	注释
RESCLASS	是	NVARCHAR2(80)	不为 NULL	应用该权限的实体的资源类。
RULEKEY	是	NVARCHAR2(256)	不为 NULL	CA ACF2：权限所在规则的规则集键。 CA Top Secret：该资源所拥有的资源掩码。 AC：资源对象名
AREAD	否	NUMBER(1,0)	NULL	
AWRITE	否	NUMBER(1,0)	NULL	
AMODIFY	否	NUMBER(1,0)	NULL	
ACREATE	否	NUMBER(1,0)	NULL	
AERASE	否	NUMBER(1,0)	NULL	
AFILESCAN	否	NUMBER(1,0)	NULL	
ALANGINT	否	NUMBER(1,0)	NULL	
AEXEC	否	NUMBER(1,0)	NULL	
ACHOWN	否	NUMBER(1,0)	NULL	
ACHGRP	否	NUMBER(1,0)	NULL	
ACHMOD	否	NUMBER(1,0)	NULL	
AUTIMES	否	NUMBER(1,0)	NULL	
ASEC	否	NUMBER(1,0)	NULL	
AKILL	否	NUMBER(1,0)	NULL	
ACONNECT	否	NUMBER(1,0)	NULL	
ARENAME	否	NUMBER(1,0)	NULL	
APASSWORD	否	NUMBER(1,0)	NULL	
AAUTHORIZED	否	CHAR(18)	NULL	
AXAUDIT	否	NUMBER(1,0)	NULL	
ACHDIR	否	NUMBER(1,0)	NULL	
ACRSUBK	否	NUMBER(1,0)	NULL	
ANOTIFY	否	NUMBER(1,0)	NULL	
AENUM	否	NUMBER(1,0)	NULL	
AQUERY	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
ARCTRL	否	NUMBER(1,0)	NULL	
ACRLINK	否	NUMBER(1,0)	NULL	
APRINT	否	NUMBER(1,0)	NULL	
AMANAGE	否	NUMBER(1,0)	NULL	
AMAXALLOWED	否	NUMBER(1,0)	NULL	
ASTOP	否	NUMBER(1,0)	NULL	
APAUSE	否	NUMBER(1,0)	NULL	
ACONTROL	否	NUMBER(1,0)	NULL	
ACHOG	否	NUMBER(1,0)	NULL	
ARESUME	否	NUMBER(1,0)	NULL	

USERAC 表的列

下表说明了 USERAC 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
USERID	是	NVARCHAR2(256)	不为 NULL	该记录的用户 ID（名称）。 映射至 USER/XUSER 对象的 AC OID。
USERTYPE	是	NVARCHAR2(80)	不为 NULL	该用户的 AC 类：USER、XUSER。
DESCRIPTION	否	NVARCHAR2(256)	NULL	该用户的说明/注释。 映射到 USER/XUSER 类的 AC 属性 COMMENT。

名称	是否为 PK	数据类型	Null 选项	注释
PROFILE	否	NVARCHAR2(256)	NULL	指定用户配置文件路径的字符串。 该字符串中可以包含本地绝对路径或 UNC 路径。 映射到 USER/XUSER 类的 AC 属性 PROFILE 的 ONAME。
GRACELOGIN	否	NUMBER	NULL	用户在密码过期后的宽限登录次数。 当超过宽限登录次数时，用户就会被拒绝访问系统并且必须向系统管理员申请新密码。 映射到 USER/XUSER 类的 AC 属性 GRACELOGIN。
MAXLOGINS	否	NUMBER	NULL	设置用户可同时登录的最多终端数。 0（零）值表示用户可同时从任意数量的终端登录。 映射到 USER/XUSER 类的 AC 属性 MAXLOGINS。
INACTIVE	否	NUMBER	NULL	指定在系统将用户更改为非活动状态之前必须经过的天数。 达到该天数时，用户无法登录。 映射到 USER/XUSER 类的 AC 属性 INACTIVE。
SUSPENDDATE	否	DATE	NULL	禁用用户记录，但将其保留在数据库进行定义。 用户不能使用挂起的用户帐号登录系统。 映射到 USER/XUSER 类的 AC 属性 SUSPEND_DATE。
SUSPENDWHOCNAME	否	NVARCHAR2(80)	NULL	激活挂起日期的管理员。 映射到 USER/XUSER 类的 AC 属性 SUSPEND_WHO 的 CNAME。

名称	是否为 PK	数据类型	Null 选项	注释
SUSPENDWHOONAME	否	NVARCHAR2(256)	NULL	系统中该对象的标识符。 映射到 USER/XUSER 类的 AC 属性 SUSPEND_WHO 的 ONAME。
RESUMEDATE	否	DATE	NULL	启用通过指定挂起参数禁用的用户记录。 映射到 USER/XUSER 类的 AC 属性 RESUME_DATE。
LUTERMINAL	否	NVARCHAR2(256)	NULL	终端的上次更新 映射到 USER/XUSER 类的 AC 属性 LAST_ACC_TERM。
PASSWDINT	否	NUMBER	NULL	设置在设置或更改密码之后且在系统提示用户输入新密码之前必须经过的天数。 映射到 USER/XUSER 类的 AC 属性 PASSWD_INT。
PASSWDLAC	否	TIMESTAMP(6)	NULL	管理员上次更新密码的日期和时间。 映射到 USER/XUSER 类的 AC 属性 PASSWD_L_A_C。
PASSWDLC	否	TIMESTAMP(6)	NULL	用户上次更新密码的日期和时间。 映射到 USER/XUSER 类的 AC 属性 PASSWD_L_C。
PASSWDACW	否	NVARCHAR2(256)	NULL	上次更改该记录的用户密码的 ADMIN 用户。 映射到 USER/XUSER 类的 AC 属性 PASSWD_A_C_W。
MINTIME	否	NUMBER	NULL	在允许用户再次更改密码之前必须经过的最少天数。 映射到 USER/XUSER 类的 AC 属性 MIN_TIME。

名称	是否为 PK	数据类型	Null 选项	注释
POLICYMODEL	否	NVARCHAR2(256)	NULL	指定在用户使用实用程序 sepass 更改密码时，eTrust AC 会将新密码传播给指定的策略模型 (pmdbName)。 该密码不会发送到由注册表子键 HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\eTrustAccessControl 中的 parent_pmd 或 passwd_pmd 值定义的策略模型。 映射到 USER/XUSER 类的 AC 属性 POLICYMODEL。
SESSIONGROUP	否	NVARCHAR2(256)	NULL	由 Single Sign-On 使用。该属性向用户分配 SSO 会话组。SESSION_GROUP 属性是最长为 16 个字符的字符串。 映射到 USER/XUSER 类的 AC 属性 SESSION_GROUP。
LOGINSTATUS	否	NVARCHAR2(256)	NULL	登录状态
PWDNEXTCHGINDAYS	否	NUMBER	NULL	下次更改密码的天数
APPLISTTIME	否	TIMESTAMP(6)	NULL	映射到 USER/XUSER 类的 AC 属性 APPLIST_TIME。
AUTHNMTHD	否	NVARCHAR2(256)	NULL	身份验证方法。 映射到 USER/XUSER 类的 AC 属性 AUTHNMTHD。
BADPASSWD	否	NUMBER	NULL	密码尝试错误的次数。映射到 USER/XUSER 类的 AC 属性 BADPASSWD。

名称	是否为 PK	数据类型	Null 选项	注释
CALENDAR	否	NVARCHAR2(256)	NULL	指定 Unicenter TNG 日历对象，表示在 Unicenter TNG 中的时间限制。 AC 仅出于管理目的来维护这些对象的列表，但不对它们进行保护。 映射到 USER/XUSER 类的 AC 属性 CALENDAR。
UPDTIME	否	TIMESTAMP(6)	NULL	上次修改记录的日期和时间。 映射到 USER/XUSER 类的 AC 属性 UPDTIME。
LOCATION	否	NVARCHAR2(256)	NULL	用户的位置。 映射到 USER/XUSER 类的 AC 属性 LOCATION。
EMAIL	否	NVARCHAR2(256)	NULL	用户的电子邮件地址。 映射到 USER/XUSER 类的 AC 属性 EMAIL。
ORGANIZATION	否	NVARCHAR2(256)	NULL	用户的组织名称。 映射到 USER/XUSER 类的 AC 属性 ORGANIZATION。
ORGUNIT	否	NVARCHAR2(256)	NULL	用户的组织部门。 映射到 USER/XUSER 类的 AC 属性 ORG_UNIT。
PHONE	否	NVARCHAR2(256)	NULL	用户的电话号码。 映射到 USER/XUSER 类的 AC 属性 PHONE。
COUNTRY	否	NVARCHAR2(256)	NULL	指定用户所在的国家/地区。 该字符串是 X.500 命名方案的一部分。 eTrust AC 不使用此项进行授权。 映射到 USER/XUSER 类的 AC 属性 COUNTRY。
LOCALAPPS	否	NUMBER(1,0)	NULL	映射到 USER/XUSER 类的 AC 属性 LOCALAPPS。

名称	是否为 PK	数据类型	Null 选项	注释
LOGSHIFT	否	NUMBER(1,0)	NULL	指明是否允许在班次时间外登录。 AC 会将该事件的审核记录写入审核日志。 映射到 USER/XUSER 类的 AC 属性 LOGSHIFT。
NOTIFY	否	NVARCHAR2(256)	NULL	用户每次登录时通知该用户。 请输入用户名、用户的电子邮件地址或邮件组的电子邮件地址（如果指定了别名）。 通知消息的接收者应该经常登录，以对每个消息中所描述的未经授权的访问尝试做出响应。 映射到 USER/XUSER 类的 AC 属性 NOTIFY。
OIDCRDDATA	否	NVARCHAR2(256)	NULL	由 CA Single Sign-On 和 CA Web Access Control 使用。 映射到 USER/XUSER 类的 AC 属性 OIDCRDDATA。
PWDAUTOGEN	否	NUMBER(1,0)	NULL	指明应用程序的密码是否由策略服务器自动生成。 映射到 USER/XUSER 类的 AC 属性 PWD_AUTOGEN。
PWDSYNC	否	NUMBER(1,0)	NULL	指明应用程序的密码是否可以与用户的其他应用程序密码相同。 映射到 USER/XUSER 类的 AC 属性 PWD_SYNC。
SCRIPTVARS	否	NVARCHAR2(256)	NULL	由 CA Single Sign-On 和 CA Web Access Control 使用，是一个变量列表，其中含有为每个应用程序保存的应用程序脚本的变量值。 映射到 USER/XUSER 类的 AC 属性 SCRIPT_VARS。

名称	是否为 PK	数据类型	Null 选项	注释
SECLEVEL	否	NUMBER	NULL	用户记录的安全级别。 映射到 USER/XUSER 类的 AC 属性 SECLEVEL。
SECLABEL	否	NVARCHAR2(256)	NULL	映射到 USER/XUSER 类的 AC 属性 SECLABEL 的 ONAME。
SHIFT	否	NVARCHAR2(256)	NULL	由 CA Single Sign-On 和 CA Web Access Control 使用。 映射到 USER/XUSER 类的 AC 属性 SHIFT 的 ONAME。
UALIAS	否	NVARCHAR2(256)	NULL	针对一个或多个验证主机定义的特定用户的所有别名。 由 CA Single Sign-On 和 CA Web Access Control 使用。 映射到 USER/XUSER 类的 AC 属性 UALIAS。
NOCHGPWD	否	NUMBER(1,0)	NULL	仅限 UNIX：没有更改密码。 映射到 AC 类 USER 的 AC 属性 NOCHNGPASS。
OWNERONAME	否	NVARCHAR2(256)	NULL	所有者对象名。 映射到 USER/XUSER 类的 AC 属性 OWNER 的 ONAME。
OWNERCNAME	否	NVARCHAR2(80)	NULL	所有者类名。 GROUP 或 XGROUP 表示所有者记录在 GROUPINFO 表中。 USER 或 XUSER 表示所有者记录在 USERINFO 表中。 映射到 USER/XUSER 类的 AC 属性 OWNER 的 CNAME。

USERACAUDIT 表的列

下表说明了 USERACAUDIT 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
USERID	是	NVARCHAR2(256)	不为 NULL	该记录的用户 ID（名称）
USERTYPE	是	NVARCHAR2(80)	不为 NULL	该用户的类：USER、XUSER
SUCCESS	否	NUMBER(1,0)	NULL	CA Access Control 将记录成功的访问。
FAILURE	否	NUMBER(1,0)	NULL	将记录失败的访问尝试。
LOGONSUCCESS	否	NUMBER(1,0)	NULL	CA Access Control 将记录成功的登录。
LOGONFAILURE	否	NUMBER(1,0)	NULL	CA Access Control 将记录失败的登录尝试。
DEBUG	否	NUMBER(1,0)	NULL	审核调试事件
TRACE	否	NUMBER(1,0)	NULL	审核跟踪事件

USERACMODE 表的列

下表说明了 USERACMODE 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符
USERID	是	NVARCHAR2(256)	不为 NULL	该记录的用户 ID（名称）
USERTYPE	是	NVARCHAR2(80)	不为 NULL	该用户的类：USER、XUSER
MREGULAR	否	NUMBER(1,0)	NULL	
MAUDITOR	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
MOPERATIONS	否	NUMBER(1,0)	NULL	
MPWOFFICER	否	NUMBER(1,0)	NULL	
MENABLED	否	NUMBER(1,0)	NULL	
MIGNHOL	否	NUMBER(1,0)	NULL	
MSERVER	否	NUMBER(1,0)	NULL	
MADMIN	否	NUMBER(1,0)	NULL	
MLOGICAL	否	NUMBER(1,0)	NULL	

USERGRP 表的列

下表说明了 USERGRP 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。记录所在系统的系统标识符。
USERID	是	NVARCHAR2(256)	不为 NULL	该记录的用户 ID（名称）。
USERTYPE	是	NVARCHAR2(80)	不为 NULL	该用户的类：USER、XUSER。
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）。 映射到 AC 组 OID 的 ONAME。
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。
CONNECTIONDATE	否	TIMESTAMP(6)	NULL	连接日期

名称	是否为 PK	数据类型	Null 选项	注释
OWNERCNAME	否	NVARCHAR2(80)	NULL	所有者类名。 GROUP 或 XGROUP 表示所有者记录在 GROUPINFO 表中。 USER 或 XUSER 表示所有者记录在 USERINFO 表中。
OWNERONAME	否	NVARCHAR2(256)	NULL	
MREGULAR	否	NUMBER(1,0)	NULL	
MAUDITOR	否	NUMBER(1,0)	NULL	
MOPERATIONS	否	NUMBER(1,0)	NULL	
MPWOFFICER	否	NUMBER(1,0)	NULL	
MENABLED	否	NUMBER(1,0)	NULL	
MIGNHOL	否	NUMBER(1,0)	NULL	
MSERVER	否	NUMBER(1,0)	NULL	
MADMIN	否	NUMBER(1,0)	NULL	

USERINFO 表的列

下表说明了 USERINFO 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
USERID	是	NVARCHAR2(256)	不为 NULL	系统中该对象的标识符。
USERTYPE	是	NVARCHAR2(80)	不为 NULL	该用户的类：USER、XUSER
NAME	否	NVARCHAR2(256)	NULL	安全数据库中定义的用户全名。 该列映射到 USER/XUSER 类的 AC 属性 FULL_NAME。

名称	是否为 PK	数据类型	Null 选项	注释
DEFGROUP	否	NVARCHAR2(256)	NULL	USS 的用户默认组。 这是 CA Top Secret 中的“DFLTGRP”字段和 CA ACF2 中的“GROUP”字段。
CRETIME	否	TIMESTAMP(6)	NULL	在安全数据库中创建用户的时间。 该列映射到 USER/XUSER 类的 AC 属性 CREATE_TIME。
LUTIME	否	TIMESTAMP(6)	NULL	用户上次进入系统的时间。 该列映射到 USER/XUSER 类的 AC 属性 LAST_ACC_TIME。
ACTDATE	否	DATE	NULL	仅限 CA ACF2。 激活用户帐户的日期。
EXPDATE	否	DATE	NULL	用户帐户到期的日期。 该列映射到 USER/XUSER 类的 AC 属性 EXPIRE_DATE。
TIMEZONE	否	CHAR(3)	NULL	与 CPU 时区有关的 ACID 物理时区。 时区值从 -12 到 +12。
APPIND	否	CHAR(1)	NULL	应用程序指示器。 指明该记录属于哪个应用程序。 等于 TSS/ACF2 DB 架构中的字符 ID。 应始终为“A”。
CONSOLE	否	CHAR(1)	NULL	CA ACF2：允许访问 TSO 控制台工具。 CA Top Secret：允许用户发出 TSS MODIFY 命令。
SUSPEND	否	CHAR(1)	NULL	阻止用户访问系统。
TRACE	否	CHAR(1)	NULL	激活诊断跟踪以记录所有用户活动（系统登录、资源访问、违规等）。
LDS	否	CHAR(1)	NULL	为 LDAP 同步启用的用户。
EIMRECID	否	CHAR(8)	NULL	记录标识符。
LDSRECID	否	CHAR(8)	NULL	记录标识符。

名称	是否为 PK	数据类型	Null 选项	注释
PROXYRECID	否	CHAR(8)	NULL	记录标识符。
SRCRECID	否	CHAR(8)	NULL	用于指定用户的 SOURCE 记录名。
SNAME	否	NVARCHAR2(64)	NULL	用于将用户身份从 Lotus Notes z/OS UNIX 映射到 CA Top Secret 或 CA ACF2 userid。
UNAME	否	NVARCHAR2(246)	NULL	用于将用户身份从 Novell Directory Services 映射到 CA Top Secret 或 CA ACF2 userid。
SECURITYID	否	NVARCHAR2(256)	NULL	该用户条目的特定于提供商的安全 ID。 该列映射到 XUSER 类的 AC 属性 SECURITY_ID。

USERLIST 表的列

下表说明了 USERLIST 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID。
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。
GROUPID	是	NVARCHAR2(256)	不为 NULL	该记录的组 ID（名称）。
GROUPTYPE	是	NVARCHAR2(80)	不为 NULL	该组的类：GROUP、XGROUP 等。映射到 AC 组 OID 的 CNAME。
USERTYPE	是	NVARCHAR2(80)	不为 NULL	用户的类名。
USERID	是	NVARCHAR2(256)	不为 NULL	用户的对象名。

USERREVACL 表的列

下表说明了 USERREVACL 表中列的属性：

名称	是否为 PK	数据类型	Null 选项	注释
SNAPSHOTID	是	NUMBER(20,0)	不为 NULL	该记录的快照 ID
HOSTID	是	NVARCHAR2(512)	不为 NULL	该记录的主机 ID。 记录所在系统的系统标识符。
USERID	是	NVARCHAR2(256)	不为 NULL	系统中该对象的标识符。 映射至 USER/XUSER 对象的 AC OID。
USERTYPE	是	NVARCHAR2(80)	不为 NULL	该用户的类：USER、XUSER。
RESCNAME	是	NVARCHAR2(80)	不为 NULL	资源类名
RESONAME	是	NVARCHAR2(256)	不为 NULL	资源对象名
CONCNAME	是	NVARCHAR2(80)	不为 NULL	条件类名（即 PROGRAM、HOST、CALENDAR）。 非空字符串表示条件对象存在于 RESINFO 表中。 空字符串表示无条件。
CONONAME	是	NVARCHAR2(256)	不为 NULL	条件对象名
AREAD	否	NUMBER(1,0)	NULL	
AWRITE	否	NUMBER(1,0)	NULL	
AMODIFY	否	NUMBER(1,0)	NULL	
ACREATE	否	NUMBER(1,0)	NULL	
AERASE	否	NUMBER(1,0)	NULL	
AFILESCAN	否	NUMBER(1,0)	NULL	
ALANGINT	否	NUMBER(1,0)	NULL	
AEXEC	否	NUMBER(1,0)	NULL	
ACHOWN	否	NUMBER(1,0)	NULL	
ACHGRP	否	NUMBER(1,0)	NULL	
ACHMOD	否	NUMBER(1,0)	NULL	
AUTIMES	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
ASEC	否	NUMBER(1,0)	NULL	
AKILL	否	NUMBER(1,0)	NULL	
ACONNECT	否	NUMBER(1,0)	NULL	
ARENAME	否	NUMBER(1,0)	NULL	
APASSWORD	否	NUMBER(1,0)	NULL	
AAUTHORIZED	否	NUMBER(1,0)	NULL	
AXAUDIT	否	NUMBER(1,0)	NULL	
ACHDIR	否	NUMBER(1,0)	NULL	
ACRSUBK	否	NUMBER(1,0)	NULL	
ANOTIFY	否	NUMBER(1,0)	NULL	
AENUM	否	NUMBER(1,0)	NULL	
AQUERY	否	NUMBER(1,0)	NULL	
ARCTRL	否	NUMBER(1,0)	NULL	
ACRLINK	否	NUMBER(1,0)	NULL	
APRINT	否	NUMBER(1,0)	NULL	
AMANAGE	否	NUMBER(1,0)	NULL	
AMAXALLOWED	否	NUMBER(1,0)	NULL	
ASTOP	否	NUMBER(1,0)	NULL	
APAUSE	否	NUMBER(1,0)	NULL	
ACONTROL	否	NUMBER(1,0)	NULL	
ACHOG	否	NUMBER(1,0)	NULL	
ARESUME	否	NUMBER(1,0)	NULL	
DREAD	否	NUMBER(1,0)	NULL	
DWRITE	否	NUMBER(1,0)	NULL	
DMODIFY	否	NUMBER(1,0)	NULL	
DCREATE	否	NUMBER(1,0)	NULL	
DERASE	否	NUMBER(1,0)	NULL	
DFILESCAN	否	NUMBER(1,0)	NULL	
DLANGINT	否	NUMBER(1,0)	NULL	

名称	是否为 PK	数据类型	Null 选项	注释
DEXEC	否	NUMBER(1,0)	NULL	
DCHOWN	否	NUMBER(1,0)	NULL	
DCHGRP	否	NUMBER(1,0)	NULL	
DCHMOD	否	NUMBER(1,0)	NULL	
DUTIMES	否	NUMBER(1,0)	NULL	
DSEC	否	NUMBER(1,0)	NULL	
DKILL	否	NUMBER(1,0)	NULL	
DCONNECT	否	NUMBER(1,0)	NULL	
DRENAME	否	NUMBER(1,0)	NULL	
DPASSWORD	否	NUMBER(1,0)	NULL	
DAUTHORIZED	否	NUMBER(1,0)	NULL	
DXAUDIT	否	NUMBER(1,0)	NULL	
DCHDIR	否	NUMBER(1,0)	NULL	
DCRSUBK	否	NUMBER(1,0)	NULL	
DNOTIFY	否	NUMBER(1,0)	NULL	
DENUM	否	NUMBER(1,0)	NULL	
DQUERY	否	NUMBER(1,0)	NULL	
DRCTRL	否	NUMBER(1,0)	NULL	
DCRLINK	否	NUMBER(1,0)	NULL	
DPRINT	否	NUMBER(1,0)	NULL	
DMANAGE	否	NUMBER(1,0)	NULL	
DMAXALLOWED	否	NUMBER(1,0)	NULL	
DSTOP	否	NUMBER(1,0)	NULL	
DPAUSE	否	NUMBER(1,0)	NULL	
DCONTROL	否	NUMBER(1,0)	NULL	
DCHOG	否	NUMBER(1,0)	NULL	
DRESUME	否	NUMBER(1,0)	NULL	

关系

FK 名称	注释
CONFIG_ENTRY_CON	包含条目
DEPTASK_RESULTMSG_CON	包含消息
USERGRP_GROUP_CON	用户组
USERLIST_FK	含有用户
PASSWDRULES_FK	包含密码规则
MEMBEROF_FK	含有组
GROUPMEMBER_FK	含有成员（组类型）
GROUPREVACL_FK	受 ACL 影响
GROUPAUDIT_FK	包含审核
SNAPSHOTINFO_FK	包含快照
NODE_ALIAS_FK	
NODE_SUBSCRIPTION_PUBLISHER	
NODE_EFFECTIVE_POLICY_CON	受策略影响
NODE_SUBSCRIPTION_SUBSCRIBER	
NODE_POLICY_STATUS_CON	含有策略状态
NODE_DEPTASKGRP_CON	任务组操作员
NODE_ADDRESS_FK	
NODE_NODE_DEVIATION_CON	含有偏差
NODE_DEPTASK_CON	由任务处理
POLICY_POLICY_STATUS_CON	含有节点状态
LATESTFIN_POLICYGRP_CON	最新确定的策略组
POLICY_EFFECTIVE_POLICY_CON	影响节点
POLICY_POLICY_DEVIATION_CON	
POLICY_RULEST_POLICY_CON	包含规则集
LATEST_POLICYGRP_CON	组中的最新策略
POLICY_DEPTASK_CON	由任务部署
POLICYGRP_DEPTASK_CON	由任务部署

FK 名称	注释
POLICYGRP_DEPTASKGRP_CON	任务组操作员
POLICY_GROUP_DEP_ON_CON	取决于策略组
POLICY_GROUP_DEP_CON	含有独立策略组
PMDSUBC_CON	
POLICYGRP_NODASS_POL_CON	含有节点分配
POLICY_GROUP_CON	超类
POLICY_CON	超类
RULESET_CON	超类
POLICYGRP_NODASS_NOD_CON	分配给策略组的资源 (NODE/GNODE)
NODE_CON	超类
HOLDATE_CON	超类
RESINFO_GRPREVACL_COND_CON	参与条件
RESINFO_HOST_CON	CACL 主机
USER_RESOURCE_ACL_CON	含有用户 ACL
UACC_CON	含有默认访问权限
SPECIALPGMTYPE_CON	超类
GROUP_RESOURCE_ACL_CON	含有组中的 ACL
GROUPS_GROUP_CON	容器成员
RESAC_CON	由 CA Access Control 属性扩展
RAUDIT_CON	超类
MEMBERS_PARENT_CON	包含成员
INSERVRNGE_CON	超类
INETACL_CON	超类
MEMBERS_CHILD_CON	成员的容器
RESINFO_DEPTASKGRP_CON	超类
RESINFO_DEPTASK_CON	超类
RESINFO_USERREVACL_COND_CON	参与条件（无约束）
RESINFO_HOST_CON	CACL 主机
GROUPS_MEMBER_CON	含有容器

FK 名称	注释
LOGINAPPL_CON	
INSERVRNGE_CON	超类
NODEGRP_DEPTASK_CON	组任务目标（节点组）
ACL_CON	受 ACL 保护
USER_RESOURCE_ACL_CON	含有用户 ACL
RULESET_RULESET_POLICY_CON	包括在策略中
RULESET_COMMAND_CON	包含命令
SEOS_DH_FK	
SNAPSHOTINFO_CON	包含用户
SNAPSHOT_CONFIG_CON	包含配置
SEOS_CON	包含选项
RESINFO_CON	包含资源
POLICYMODEL_CON	
CATEGORY_CON	包含类别
DAYTIME_CON	包含白天设置
GROUPINFO_CON	包含组
USERACMODE_FK	包含 CA Access Control 模式
USERACAUDIT_FK	包含 CA Access Control 审核
USERGRP_FK	属于组
USERREVACL_FK	受 ACL 影响
USERINFO_SUSPEND_USERAC_CON	由用户挂起
USER_DEPTASK_CHECKER_CON	该任务的检查者
USER_DEPTASK_MAKER_CON	任务制定者
USERAC_CON	由 CA Access Control 属性扩展

CONFIG_ENTRY_CON 关系的父表

CONFIG 是 CONFIG_ENTRY_CON 的父表。

CONFIG_ENTRY_CON 关系的子表

CONFIG_ENTRY 是 CONFIG_ENTRY_CON 的子表。

CONFIG_ENTRY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
CONFIGNAME	CONFIGNAME

DEPTASK_RESULTMSG_CON 关系的父表

DEPLOYMENT_TASK 是 DEPTASK_RESULTMSG_CON 的父表。

DEPTASK_RESULTMSG_CON 关系的子表

DEPLOYMENT_RESULT_MESSAGE 是 DEPTASK_RESULT_MSG_CON 的子表。

DEPTASK_RESULTMSG_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUPMEMBER_FK 关系的父表

GROUPINFO 是 GROUPMEMBER_FK 的父表。

GROUPMEMBER_FK 关系的子表

GROUPMEMBER 是 GROUPMEMBER_FK 的子表。

GROUPMEMBER_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

GROUPREVACL_FK 关系的父表

GROUPINFO 是 GROUPREVACL_FK 的父表。

GROUPREVACL_FK 关系的子表

GROUPREVACL 是 GROUPREVACL_FK 的子表。

GROUPREVACL_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

USERGRP_GROUP_CON 关系的父表

GROUPINFO 是 USERGRP_GROUP_CON 的父表。

USERGRP_GROUP_CON 关系的子表

USERGRP 是 USERGRP_GROUP_CON 的子表。

USERGRP_GROUP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

MEMBEROF_FK 关系的父表

GROUPINFO 是 MEMBEROF_FK 的父表。

MEMBEROF_FK 关系的子表

MEMBEROF 是 MEMBEROF_FK 的子表。

MEMBEROF_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

PASSWDRULES_FK 关系的父表

GROUPINFO 是 PASSWDRULES_FK 的父表。

PASSWDRULES_FK 关系的子表

PASSWDRULES 是 PASSWDRULES_FK 的子表。

PASSWDRULES_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

USERLIST_FK 关系的父表

GROUPINFO 是 USERLIST_FK 的父表。

USERLIST_FK 关系的子表

USERLIST 是 USERLIST_FK 的子表。

USERLIST_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

GROUPAUDIT_FK 关系的父表

GROUPINFO 是 GROUPAUDIT_FK 的父表。

GROUPAUDIT_FK 关系的子表

GROUPAUDIT 是 GROUPAUDIT_FK 的子表。

GROUPAUDIT_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

SNAPSHOTINFO_FK 关系的父表

HOSTINFO 是 SNAPSHOTINFO_FK 的父表。

SNAPSHOTINFO_FK 关系的子表

SNAPSHOTINFO 是 SNAPSHOTINFO_FK 的子表。

SNAPSHOTINFO_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
HOSTID	HOSTID

NODE_ALIAS_FK 关系的父表

NODE 是 NODE_ALIAS_FK 的父表。

NODE_ALIAS_FK 关系的子表

NODE_ALIAS 是 NODE_NODE_ALIAS_FK 的子表。

NODE_ALIAS_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID

父列名称	子列名称
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_SUBSCRIPTION_PUBLISHER 关系的父表

NODE 是 NODE_SUBSCRIPTION_PUBLISHER 的父表。

NODE_SUBSCRIPTION_PUBLISHER 关系的子表

NODE_SUBSCRIPTION_STATUS 是 NODE_SUBSCRIPTION_PUBLISHER 的子表。

NODE_SUBSCRIPTION_PUBLISHER 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	PUBLISHERCNAME
RULEKEY	PUBLISHERONAME

NODE_EFFECTIVE_POLICY_CON 关系的父表

NODE 是 NODE_EFFECTIVE_POLICY_CON 的父表。

NODE_EFFECTIVE_POLICY_CON 关系的子表

EFFECTIVE_POLICY 是 NODE_EFFECTIVE_POLICY_CON 的子表。

NODE_EFFECTIVE_POLICY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID

父列名称	子列名称
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_SUBSCRIPTION_SUBSCRIBER 关系的父表

NODE 是 NODE_SUBSCRIPTION_SUBSCRIBERER 的父表。

NODE_SUBSCRIPTION_SUBSCRIBER 关系的子表

NODE_SUBSCRIPTION_STATUS 是 NODE_SUBSCRIPTION_SUBSCRIBER 的子表。

NODE_SUBSCRIPTION_SUBSCRIBER 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	SUBSCRIBERCNAME
RULEKEY	SUBSCRIBERONAME

NODE_POLICY_STATUS_CON 关系的父表

NODE 是 NODE_POLICY_STATUS_CON 的父表。

NODE_POLICY_STATUS_CON 关系的子表

POLICY_STATUS 是 NODE_POLICY_STATUS_CON 的子表。

NODE_POLICY_STATUS_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID

父列名称	子列名称
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_DEPTASKGRP_CON 关系的父表

NODE 是 NODE_DEPTASKGRP_CON 的父表。

NODE_DEPTASKGRP_CON 关系的子表

DEPLOYMENT_TASK_GROUP 是 NODE_DEPTASKGRP_CON 的子表。

NODE_DEPTASKGRP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_ADDRESS_FK 关系的父表

NODE 是 NODE_ADDRESS_FK 的父表。

NODE_ADDRESS_FK 关系的子表

NODE_ADDRESS 是 NODE_ADDDRESS_FK 的子表。

NODE_ADDRESS_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

父列名称	子列名称
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_NODE_DEVIATION_CON 关系的父表

NODE 是 NODE_NODE_DEVIATION_CON 的父表。

NODE_NODE_DEVIATION_CON 关系的子表

NODE_DEVIATION 是 NODE_NODE_DEVIATION_CON 的子表。

NODE_NODE_DEVIATION_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_DEPTASK_CON 关系的父表

NODE 是 NODE_DEPTASK_CON 的父表。

NODE_DEPTASK_CON 关系的子表

DEPLOYMENT_TASK 是 NODE_DEPTASK_CON 的子表。

NODE_DEPTASK_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS

父列名称	子列名称
RULEKEY	NODE_RULEKEY

POLICY_POLICY_STATUS_CON 关系的父表

POLICY 是 POLICY_POLICY_STATUS_CON 的父表。

POLICY_POLICY_STATUS_CON 关系的子表

POLICY_STATUS 是 POLICY_POLICY_STATUS_CON 的子表。

POLICY_POLICY_STATUS_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

LATESTFIN_POLICYGRP_CON 关系的父表

POLICY 是 LATESTFIN_POLICYGRP_CON 的父表。

LATESTFIN_POLICYGRP_CON 关系的子表

POLICY_GROUP 是 LATESTFIN_POLICYGRP_CON 的子表。

LATESTFIN_POLICYGRP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	LATEST_FIN_RESCLASS
RULEKEY	LATEST_FIN_RULEKEY

POLICY_EFFECTIVE_POLICY_CON 关系的父表

POLICY 是 POLICY_EFFECTIVE_POLICY_CON 的父表。

POLICY_EFFECTIVE_POLICY_CON 关系的子表

POLICY_EFFECTIVE 是 POLICY_EFFECTIVE_POLICY_CON 的子表。

POLICY_EFFECTIVE_POLICY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICY_POLICY_DEVIATION_CON 关系的父表

POLICY 是 POLICY_POLICY_DEVIATION_CON 的父表。

POLICY_POLICY_DEVIATION_CON 关系的子表

POLICY_DEVIATION 是 POLICY_POLICY_DEVIATION_CON 的子表。

POLICY_POLICY_DEVIATION_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICY_RULESET_POLICY_CON 关系的父表

POLICY 是 POLICY_RULESET_POLICY_CON 的父表。

POLICY_RULESET_POLICY_CON 关系的子表

POLICY_RULESET 是 POLICY_RULESET_POLICY_CON 的子表。

POLICY_RULESET_POLICY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

LATEST_POLICYGRP_CON 关系的父表

POLICY 是 LATEST_POLICYGRP_CON 的父表。

LATEST_POLICYGRP_CON 关系的子表

POLICY_GROUP 是 LATEST_POLICYGRP_CON 的子表。

LATEST_POLICYGRP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	LATEST_RESCLASS
RULEKEY	LATEST_RULEKEY

POLICY_DEPTASK_CON 关系的父表

POLICY 是 POLICY_DEPTASK_CON 的父表。

POLICY_DEPTASK_CON 关系的子表

DEPLOYMENT_TASK 是 POLICY_DEPTASK_CON 的子表。

POLICY_DEPTASK_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICYGRP_DEPTASK_CON 关系的父表

POLICY_GROUP 是 POLICYGRP_DEPTASK_CON 的父表。

POLICYGRP_DEPTASK_CON 关系的子表

DEPLOYMENT_TASK 是 POLICYGRP_DEPTASK_CON 的子表。

POLICYGRP_DEPTASK_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

POLICYGRP_DEPTASKGRP_CON 关系的父表

POLICY_GROUP 是 POLICYGRP_DEPTASKGRP_CON 的父表。

POLICYGRP_DEPTASKGRP_CON 关系的子表

DEPLOYMENT_TASK_GROUP 是 POLICYGRP_DEPTASKGRP_CON 的子表。

POLICYGRP_DEPTASKGRP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

POLICY_GROUP_DEP_ON_CON 关系的父表

POLICY_GROUP 是 POLICY_GROUP_DEP_ON_CON 的父表。

POLICY_GROUP_DEP_ON_CON 关系的子表

POLICY_GROUP_DEPENDENCY 是 POLICY_GROUP_DEP_ON_CON 的子表。

POLICY_GROUP_DEP_ON_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	DEP_ON_RESCLASS
RULEKEY	DEP_ON_RULEKEY

POLICY_GROUP_DEP_CON 关系的父表

POLICY_GROUP 是 POLICY_GROUP_DEP_CON 的父表。

POLICY_GROUP_DEP_CON 关系的子表

POLICY_GROUP_DEPENDENCY 是 POLICY_GROUP_DEP_CON 的子表。

POLICY_GROUP_DEP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

PMD_SUBSC_CON 关系的父表

POLICYMODELINFO 是 PMD_SUBSC_CON 的父表。

PMD_SUBSC_CON 关系的子表

LOCAL_PMD_SUBSCRIBER 是 PMD_SUBSC_CON 的子表。

PMD_SUBSC_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

POLICYGRP_NODASS_POL_CON 关系的父表

RESINFO 是 POLICYGRP_NODASS_POL_CON 的父表。

POLICYGRP_NODASS_POL_CON 关系的子表

POLICY_GROUP_NODE_ASSIGNMENT 是 POLICYGRP_NODASS_POL_CON 的子表。

POLICYGRP_NODASS_POL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

POLICY_GROUP_CON 关系的父表

RESINFO 是 POLICY_GROUP_CON 的父表。

POLICY_GROUP_CON 关系的子表

POLICY_GROUP 是 POLICY_GROUP_CON 的子表。

POLICY_GROUP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

POLICY_CON 关系的父表

RESINFO 是 POLICY_CON 的父表。

POLICY_CON 关系的子表

POLICY 是 POLICY_CON 的子表。

POLICY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RULESET_CON 关系的父表

RESINFO 是 RULESET_CON 的父表。

RULESET_CON 关系的子表

RULESET 是 RULESET_CON 的子表。

RULESET_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

POLICYGRP_NODASS_NOD_CON 关系的父表

RESINFO 是 NODASS_POLICYGRP_NOD_CON 的父表。

POLICYGRP_NODASS_NOD_CON 关系的子表

POLICY_GROUP_NODE_ASSIGNMENT 是 POLICYGRP_NODASS_NOD_CON 的子表。

POLICYGRP_NODASS_NOD_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

NODE_CON 关系的父表

RESINFO 是 NODE_CON 的父表。

NODE_CON 关系的子表

NODE 是 NODE_CON 的子表。

NODE_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUP_RESOURCE_ACL_CON 关系的父表

RESINFO 是 GROUP_RESOURCE_ACL_CON 的父表。

GROUP_RESOURCE_ACL_CON 关系的子表

GROUPREVACL 是 GROUP_RESOURCE_ACL_CON 的子表。

GROUP_RESOURCE_ACL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	RESCNAME
RULEKEY	RESONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_USERREVACL_COND_CON 关系的父表

RESINFO 是 USERREVACL_RESINFO_COND_CON 的父表。

RESINFO_USERREVACL_COND_CON 关系的子表

USERREVACL 是 RESINFO_USERREVACL_COND_CON 的子表。

RESINFO_USERREVACL_COND_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	CONCNAME
RULEKEY	CONONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

UACC_CON 关系的父表

RESINFO 是 UACC_CON 的父表。

UACC_CON 关系的子表

UACC 是 UACC_CON 的子表。

UACC_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

SPECIALPGMTYPE_CON 关系的父表

RESINFO 是 SPECIALPGMTYPE_CON 的父表。

SPECIALPGMTYPE_CON 关系的子表

SPECIALPGMTYPE 是 SPECIALPGMTYPE_CON 的子表。

SPECIALPGMTYPE_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESAC_CON 关系的父表

RESINFO 是 RESAC_CON 的父表。

RESAC_CON 关系的子表

RESAC 是 RESAC_CON 的子表。

RESAC_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RAUDIT_CON 关系的父表

RESINFO 是 RAUDIT_CON 的父表。

RAUDIT_CON 关系的子表

RAUDIT 是 RAUDIT_CON 的子表。

RAUDIT_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

MEMBERS_PARENT_CON 关系的父表

RESINFO 是 MEMBERS_PARENT_CON 的父表。

MEMBERS_PARENT_CON 关系的子表

MEMBERS 是 MEMBERS_PARENT_CON 的子表。

MEMBERS_PARENT_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESINFO_DEPTASKGRP_CON 关系的父表

RESINFO 是 RESINFO_DEPTASKGRP_CON 的父表。

RESINFO_DEPTASKGRP_CON 关系的子表

DEPLOYMENT_TASK_GROUP 是 RESINFO_DEPTASKGRP_CON 的子表。

RESINFO_DEPTASKGRP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESINFO_DEPTASK_CON 关系的父表

RESINFO 是 RESINFO_DEPTASK_CON 的父表。

RESINFO_DEPTASK_CON 关系的子表

DEPLOYMENT_TASK 是 RESINFO_DEPTASK_CON 的子表。

LOGINAPPL_CON 关系的父表

RESINFO 是 LOGINAPPL_CON 的父表。

LOGINAPPL_CON 关系的子表

LOGINAPPL 是 LOGINAPPL_CON 的子表。

LOGINAPPL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

INSERVRNGE_CON 关系的父表

RESINFO 是 INSERVRNGE_CON 的父表。

INSERVRNGE_CON 关系的子表

INSERVRNGE 是 INSERVRNGE_CON 的子表。

INSERVRNGE_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODEGRP_DEPTASKGRP_CON 关系的父表

RESINFO 是 NODEGRP_DEPTASKGRP_CON 的父表。

NODEGRP_DEPTASKGRP_CON 关系的子表

DEPLOYMENT_TASK_GROUP 是 NODEGRP_DEPTASKGRP_CON 的子表。

NODEGRP_DEPTASKGRP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODEGRP_RESCLASS
RULEKEY	NODEGRP_RULEKEY

RESINFO_GRPREVACL_COND_CON 关系的父表

RESINFO 是 RESINFO_GRPREVACL_COND_CON 的父表。

RESINFO_GRPREVACL_COND_CON 关系的子表

GROUPREVACL 是 RESINFO_GRPREVACL_COND_CON 的子表。

RESINFO_GRPREVACL_COND_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	CONCNAME
RULEKEY	CONONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_HOST_CON 关系的父表

RESINFO 是 RESINFO_HOST_CON 的父表。

RESINFO_HOST_CON 关系的子表

ACL 是 RESINFO_HOST_CON 的子表。

RESINFO_HOST_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	HOSTCNAME
RULEKEY	HOSTONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

GROUPS_GROUP_CON 关系的父表

RESINFO 是 GROUPS_GROUP_CON 的父表。

GROUPS_GROUP_CON 关系的子表

GROUPS 是 GROUPS_GROUP_CON 的子表。

GROUPS_GROUP_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	CNAME
RULEKEY	ONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

INETACL_CON 关系的父表

RESINFO 是 INETACL_CON 的父表。

INETACL_CON 关系的子表

INETACL 是 INETACL_CON 的子表。

INETACL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

HOLDATE_CON 关系的父表

RESINFO 是 HOLDATE_CON 的父表。

HOLDATE_CON 关系的子表

HOLDATE 是 HOLDATE_CON 的子表。

HOLDATE_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUPS_MEMBER_CON 关系的父表

RESINFO 是 GROUPS_MEMBER_CON 的父表。

GROUPS_MEMBER_CON 关系的子表

GROUPS 是 GROUPS_MEMBER_CON 的子表。

GROUPS_MEMBER_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

ACL_CON 关系的父表

RESINFO 是 ACL_CON 的父表。

ACL_CON 关系的子表

ACL 是 ACL_CON 的子表。

ACL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

MEMBERS_CHILD_CON 关系的父表

RESINFO 是 MEMBER_CHILD_CON 的父表。

MEMBERS_CHILD_CON 关系的子表

MEMBER 是 MEMBERS_CHILD_CON 的子表。

MEMBERS_CHILD_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	CNAME
RULEKEY	ONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USER_RESOURCE_ACL_CON 关系的父表

USER 是 RESINFO_RESOURCE_ACL_CON 的父表。

USER_RESOURCE_ACL_CON 关系的子表

RESOURCE 是 USER_USERREVACL_ACL_CON 的子表。

USER_RESOURCE_ACL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
RESCLASS	RESCNAME
RULEKEY	RESONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RULESET_RULESET_POLICY_CON 关系的父表

RULESET 是 RULESET_RULESET_POLICY_CON 的父表。

RULESET_RULESET_POLICY_CON 关系的子表

RULESET_RULESET 是 POLICY_RULESET_POLICY_CON 的子表。

RULESET_RULESET_POLICY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RULESET_RESCLASS
RULEKEY	RULESET_RULEKEY

RULESET_COMMAND_CON 关系的父表

RULESET 是 RULESET_COMMAND_CON 的父表。

RULESET_COMMAND_CON 关系的子表

RULESET_COMMAND 是 RULESET_COMMAND_CON 的子表。

RULESET_COMMAND_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RULESET_RESCLASS
RULEKEY	RULESET_RULEKEY

SEOS_DH_FK 关系的父表

SEOS 是 SEOS_DH_FK 的父表。

SEOS_DH_FK 关系的子表

DISTRIBUTION_HOST 是 SEOS_DH_FK 的子表。

SEOS_DH_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

DAYTIME_CON 关系的父表

SNAPSHOTINFO 是 DAYTIME_CON 的父表。

DAYTIME_CON 关系的子表

DAYTIME 是 CATEGORY_CON 的子表。

DAYTIME_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SEOS_CON 关系的父表

SNAPSHOTINFO 是 SEOS_CON 的父表。

SEOS_CON 关系的子表

SEOS 是 SEOS_CON 的子表。

SEOS_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SEOSSYSCALL_CON 关系的父表

SNAPSHOTINFO 是 SEOSSYSCALL_CON 的父表。

SEOSSYSCALL_CON 关系的子表

SEOSSYSCALL 是 SEOSSYSCALL_CON 的子表。

SEOSSYSCALL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SNAPSHOT_CONFIG_CON 关系的父表

SNAPSHOTINFO 是 SNAPSHOT_CONFIG_CON 的父表。

SNAPSHOT_CONFIG_CON 关系的子表

CONFIG 是 SNAPSHOT_CONFIG_CON 的子表。

SNAPSHOT_CONFIG_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SYSCALL_CON 关系的父表

SEOSSYSCALL 是 SYSCALL_CONFIG_CON 的父表。

SYSCALL_CON 关系的子表

SYSCALL 是 SYSCALL_CON 的子表。

SYSCALL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SYSCALLUSERSPECIALPGM 关系的父表

SEOSSYSCALL 是 SYSCALLUSERSPECIALPGM 的父表。

SYSCALLUSERSPECIALPGM 关系的子表

SYSCALLUSERSPECIALPGM 是 SYSCALLUSERSPECIALPGM 的子表。

SYSCALLUSERSPECIALPGM 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

CATEGORY_CON 关系的父表

SNAPSHOTINFO 是 CATEGORY_CON 的父表。

CATEGORY_CON 关系的子表

CATEGORY 是 CATEGORY_CON 的子表。

CATEGORY_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

GROUPINFO_CON 关系的父表

SNAPSHOTINFO 是 GROUPINFO_CON 的父表。

GROUPINFO_CON 关系的子表

GROUPINFO 是 CATEGORY_CON 的子表。

GROUPINFO_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SNAPSHOTINFO_CON 关系的父表

SNAPSHOTINFO 是 SNAPSHOTINFO_CON 的父表。

SNAPSHOTINFO_CON 关系的子表

USERINFO 是 SNAPSHOTINFO_CON 的子表。

SNAPSHOTINFO_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_CON 关系的父表

SNAPSHOTINFO 是 RESINFO_CON 的父表。

RESINFO_CON 关系的子表

RESINFO 是 RESINFO_CON 的子表。

RESINFO_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

POLICYMODEL_CON 关系的父表

SNAPSHOTINFO 是 POLICYMODEL_CON 的父表。

POLICYMODEL_CON 关系的子表

POLICYMODELINFO 是 POLICYMODEL_CON 的子表。

POLICYMODEL_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USERACAUDIT_FK 关系的父表

USERAC 是 USERACAUDIT_FK 的父表。

USERACAUDIT_FK 关系的子表

USERACAUDIT 是 USERACAUDIT_FK 的子表。

USERACAUDIT_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERACMODE_FK 关系的父表

USERAC 是 USERACMODE_FK 的父表。

USERACMODE_FK 关系的子表

USERACMODE 是 USERACMODE_FK 的子表。

USERACMODE_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERGRP_FK 关系的父表

USERAC 是 USERGRP_FK 的父表。

USERGRP_FK 关系的子表

USERGRP 是 USERGRP_FK 的子表。

USERGRP_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERINFO_SUSPEND_USERAC_CON 关系的父表

USERINFO 是 USERINFO_SUSPEND_USERAC_CON 的父表。

USERINFO_SUSPEND_USERAC_CON 关系的子表

USERAC 是 USERINFO_SUSPEND_USERAC_CON 的子表。

USERINFO_SUSPEND_USERAC_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
USERTYPE	SUSPENDWHOCNAME
USERID	SUSPENDWHOONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USER_DEPTASK_CHECKER_CON 关系的父表

USER 是 USERINFO_DEPTASK_CHECKER_CON 的父表。

USER_DEPTASK_CHECKER_CON 关系的子表

DEPLOYMENT_TASK 是 USER_DEPTASK_CHECKER_CON 的子表。

USER_DEPTASK_CHECKER_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	CHECKERID
USERTYPE	CHECKERTYPE

USER_DEPTASK_MAKER_CON 关系的父表

USERINFO 是 USER_DEPTASK_CON 的父表。

USER_DEPTASK_MAKER_CON 关系的子表

DEPLOYMENT_TASK 是 USER_DEPTASK_CON 的子任务。

USER_DEPTASK_MAKER_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	MAKERID
USERTYPE	MAKERTYPE

USERREVACL_FK 关系的父表

USERINFO 是 USERREVACL_FK 的父表。

USERREVACL_FK 关系的子表

USERREVACL 是 USERREVACL_FK 的子表。

USERREVACL_FK 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERAC_CON 关系的父表

USERINFO 是 USERAC_CON 的父表。

USERAC_CON 关系的子表

USERAC 是 USERAC_CON 的子表。

USERAC_CON 关系的迁移列

下表说明了父表与子表中列之间的关系：

父列名称	子列名称
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE