CA Access Control

selang 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：

-

目录

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 selang 命令、数据库类和属性以及 Windows 值的信息。 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

本指南面向执行 selang 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而编写。

第 2 章： selang 命令语言

此部分包含以下主题：

CA Access Control 命令行解释程序

CA Access Control 的管理是通过名为 selang 的命令 shell（CA Access Control 命令语言）执行的。 通过 selang 命令语言，您可以在 CA Access Control 数据库中进行定义。 selang 命令语言是命令定义语言。

selang 实用程序位于 CA Access Control 安装 bin 目录下。 输入 selang shell 时，将显示特定的 selang 提示。 提示符的确切形式取决于您的工作环境。 它与如下所示类似：

```
AC>
```

默认情况下，selang 命令 shell 在本地数据库中运行。 要在另一工作站的 CA Access Control 数据库中运行，请在输入 selang 命令之前指定 hosts 命令。

更多信息：

selang 环境 (p. 32)
hosts 命令 — 连接至远程 CA Access Control 终端 (p. 113)

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。

更多信息：

hosts 命令 — 连接至远程 CA Access Control 终端 (p. 113)

selang 命令 Shell 的功能

进入 selang 命令 shell 后，将显示下面的提示符：

```
AC>
```

出现该提示符后，可以输入 selang 命令。 输入命令时请用分号 (;) 分隔命令。 如果需要在多行中输入一条命令，请在每一行的末尾键入反斜线 (\)，以便在下一行中继续键入该命令。 可以编辑命令行。 使用向左箭头和向右箭头在行内移动。 可以通过直接键入的方式插入字符，使用标准的 Backspace 键和 Delete 键删除字符，或通过按 Ctrl+D（在 UNIX 中）删除字符。

selang 支持 UNIX shell tcsh 和其他智能 shell 中提供的许多命令行输入功能。 包括以下功能：

- 特殊字符
- 快捷键
- 命令历史记录
- 特殊功能

注意：在 UNIX 中，您可以使用 *UNIX exit* 程序，通过该程序可指定 shell 脚本或可执行程序在添加或更新用户或组之前或之后自动运行。 有关 UNIX exit 的详细信息，请参阅 *《端点管理指南：用于 UNIX》*。

特殊字符

selang 支持下列特殊字符：

字符	说明	含义
# 或 *	井号或星号	在行首，表示该行是注释行；该行不执行。 当输入某个文件中的 selang 命令时，注释行很有用。
!	感叹号	在行首，表示该行剩余的部分是 shell 命令。 selang 将命令发送到操作系统 shelll 程序以供执行；CA Access Control 不执行该行。
\	反斜线	作为行中的最后一个字符，指示命令在下一行继续。
;	分号	终止命令并在同一行引入新命令。
| 竖线	竖线	将前面命令的输出发送到后面命令的输入（指定的*竖线*）。

快捷键

selang 支持下列快捷键：

键	适用系统	含义
向上-键、*向下-键*或^	全部	用于从命令历史记录中导航和检索命令。
Tab	UNIX	用于完词处理。
Ctrl+D	UNIX	在光标位于行尾时，显示与命令行中的完词处理字符串匹配的单词列表。 在光标位于行中任何其他位置时，删除光标右侧的字符。
Esc、Esc Ctrl+2	UNIX	显示命令行中命令的帮助文本。 命令行中的所有文本均会保留下来，这样，您便可以继续在离开的位置键入命令。
F1	Windows	逐个字符地插入上一命令。
F2	Windows	显示带有以下说明的窗口：“Enter char to copy up to :（输入要复制的字符，直到：）”。输入上一命令中的某个字符后，selang 将输入该命令，直到第一次出现该字符的位置。 如果该字符在命令中多次出现，那么，可以再次按 F2 键以插入命令，直到下一次出现该字符的位置。 使用退格键取消。
F3	Windows	输入上一命令（与向上箭头相同）。

键	适用系统	含义
F4	Windows	编辑上一说明。 显示带有以下说明的窗口：“Enter char to delete up to:（输入要删除的字符，直到：）”。 使用退格键取消。
F5	Windows	输入上一命令（与向上箭头相同）。
F6	Windows	在命令行中输入 Ctrl Z (^Z)。 这样，可以按 Enter 键并在下一行中继续输入命令。
F7	Windows	显示一个窗口，其中列出命令历史记录。 您可以使用向上箭头和向下箭头选择任何以前的命令。 使用 Esc 键可取消。
F8	Windows	输入上一命令，与向上箭头相同，但将光标置于命令行的开头而不是末尾。
F9	Windows	显示带有以下说明的窗口：“Enter command number:（输入命令编号：）”。输入的编号会插入 F7 列表中具有相应编号的命令。 使用 Esc 键可取消。

命令历史记录

selang 可将已执行的命令存储在*历史记录列表*中。 使用向上键和向下键可在命令行中显示历史记录列表中的命令。 要只查看以特定字符或字符串开头的命令，请在使用向上箭头和向下箭头之前键入命令的开头部分。 按下 *Enter* 键后，将执行当前显示在命令行中的文本。

要查看先前发出的命令，请输入历史记录命令。

selang 命令 shell 支持使用存储在历史记录列表中的命令的下列快捷方式：

快捷方式	运行
^^ [*string*]	上一个命令。 如果指定 *string*，则 selang 会将其附加到原始命令后面。
^*n* [*string*]	历史记录列表中的第 *n* 个命令，其中 *n* 是正整数。 如果指定 *string*，则 selang 会将其附加到原始命令后面。
^-*n* [*string*]	列表中倒数第 *n* 个命令。其中 *n* 是正整数。 如果指定 *string*，则 selang 会将其附加到原始命令后面。

快捷方式	运行
^*mask* [*string*]	最近发出的以 *mask* 开头的命令，其中 *mask* 是文本字符串。 如果指定 *string*，则 selang 会将其附加到原始命令后面。

注意：在 Windows 中，可以使用 F7 键查看历史记录列表。

特殊功能

可以使用一些其他技术在 selang 命令 shell 中保存键击。

注意：在 UNIX 中记录和类名区分大小写，但在 Windows 中不区分。

- 命令识别

  只要您键入的字符足以将您要执行的命令与所有其他可用命令区分开，selang 即可识别。 例如，可以键入 **ho** 运行 *hosts* 命令，因为它是唯一一个以这两个字母开头的命令。 只要键入 **ho**，selang 即可识别要执行的命令。 反之，有多个命令以字符串 **new** 开头。 您必须添加足够多的字符以区分 newusr、newgrp、newfile 和 newres。

- 缩写

  每个命令还与一个由一到四个字母组成的缩写相关联。 例如，由于有多个命令以字符串 new 开头，因此您还可使用命令 **newusr** 的缩写 **nu**。 这些缩写记录为每个命令的命令语法的一部分。 可以以大写字母或小写字母输入命令。

- 完词处理（仅适用于 UNIX）

  在单词的中间按 *Tab* 键可以完成该单词。 完词处理是上下文相关的。 如果与指定字符串匹配的单词不只一个，则 selang 将使用与该字符串匹配的最短单词或单词片段。 例如，如果键入字母 *n*，selang 将提供 ew，以组成单词 new。 如果没有所需的单词，请键入另一个或两个字符，然后再次按 *Tab* 键以完成该单词。 按 Ctrl+D 可以查看所有可能的选项。 如果您不确定要使用哪个命令，这十分有用。 使用上一段中的示例，如果您向单词 new 添加 u 并按 *Tab* 键，selang 会提供 sr，从而为您提供命令 newusr。

  不属于 *selang* 命令一部分的单词存储在内存中，供同一会话中的完词处理功能稍后使用。例如，如果键入 newusr Mercedes，然后键入 showusr Me，再按 *Tab*，则缩写 Me 将扩展为 Mercedes，如下所示：

  ```
  showusr Mercedes
  ```

  这假定您没有输入任何其他以“Me”开头的用户名。

通配符匹配

selang 支持下列通配符字符：

***（星号）**

零个或更多字符的任何序列。

?（问号）

任何单个字符（文件的路径分隔符除外）。

要使单个字符成为可匹配任何其他单个字符的“无关”字符，请使用一个问号 (?)，如下例所示：

指定。。。	执行。。。
mmc?	mmc3、mmcx、mmc5
mmc?.t	mmc1.t、mmc2.t
mmc04.?	mmc04.a、mmc04.1

要匹配任何包含零个或多个字符的字符串，请使用星号 (*)，如下例所示：

指定。。。	执行。。。
i.c	main.c、list.c
st*.h	stdio.h、stdlib.h、string.h
*	指定类的所有记录

selang 命令语法

每个 selang 命令均可对 CA Access Control 数据库执行特定的操作。selang 命令的语法为：

```
commandname parameters
```

命令名可告知 CA Access Control 要执行的命令。 通常，命令后跟一个或多个参数，这些参数为 CA Access Control 提供执行该命令所需的其他信息。

selang 参数的语法为：

parameterName[(arguments)]

参数名可标识 CA Access Control 的参数。 许多参数都需要 argument，argument 可为 CA Access Control 提供处理参数所需的信息。 有些参数接受多个 argument。 当指定多个 argument 时，要用逗号或空格来分隔这些 argument。 参数的 argument 本身可能就是参数。

要在字符串定义 argument 时删除记录属性，只须用空括号 **()** 输入该属性即可。 在某些情况下，可以使用星号 **(*)** 作为 argument，以包含该 argument 的所有可能值。 使用星号时，星号并*不*覆盖之前或之后为同一 argument 提供特定值的命令。 此外，如果 argument 是一个文件名，则可以使用通配符作为文件名模式的一部分。 通配符为 *（表示零个或多个字符）和 ?（表示一个字符）。

在 UNIX 环境中，用户提供的信息是区分大小写的，并且可以同时包含小写字母和大写字母。 例如，您可以将用户 ID 为 user53 的用户的全名指定为 Mike Jones。 *Windows* 无法识别区分大小写的信息，但仍旧保存该信息。 如果您从 UNIX 工作站管理远程 Windows 主机，UNIX 将查找用户提供的存储信息。 例如，如果在 Windows 环境中将某用户标识为 Mike Jones，则在管理本地 CA Access Control 数据库时，可以将该用户名输入为 mike jones。 但是，如果要从远程 UNIX 计算机管理该数据库，则必须将其用户名输入为 Mike Jones。

selang 命令授权

要使用可更改 AC 或本地操作系统（本地 OS）环境中的记录的 selang 命令，您必须拥有足够权限。 对于大多数命令，必须符合下列条件之一：

- 您是资源的所有者。
- 您具有 ADMIN 属性。
- 资源记录在某一组的范围内，您在该组中具有 GROUP-ADMIN 属性。
- 在 ADMIN 类的记录的 ACL 中，您拥有 CREATE 或 MODIFY 访问权限。
- (Windows) 如果安装只允许管理本地 Windows 环境，那么您应该是 Windows 数据库中 CA Access Control 管理员组的成员。
- (UNIX) 如果安装只允许管理本地 UNIX 环境，那么您应该是本地 UNIX 主机的安全文件中 CA Access Control 管理员组的成员。

注意：每个命令的说明中都记录了这些一般规则的例外情况。

Access Control 列表支持

要授予或拒绝授予访问权限，可以使用以下七类 Access Control 列表：

ACL

标准 Access Control 列表，包含授权访问资源的用户名和组名以及授予每个用户或组的访问级别。

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。

INET-ACL

Internet Access Control 列表。

CACL

条件 Access Control 列表。

CALACL

日历 Access Control，即依赖于 Unicenter TNG 日历的资源 ACL。

AZNACL

授权 ACL，即允许基于资源说明访问资源的 ACL。

在检查用户访问资源的权限时，CA Access Control 将使用所有相关的列表。

注意：可以用单个 authorize 命令维护任何单个列表。 要更改多个列表，您需要再次发出 authorize。 不能用一个授权规则为多个用户和组定义多个访问权限。 必须分隔这些规则。

下表列出了可以与每个类配合使用的 Access Control 列表。 未显示该表中的类没有 Access Control 列表，所以不能通过 authorize 命令对其进行控制。

类	ACL/ NACL	CALACL	PACL	INET-ACL	CACL	AZNACL
ADMIN	x	x	x			
APPL	x	x				x
AUTHHOST	x	x				x
CONNECT	x	x	x			

类	ACL/ NACL	CALACL	PACL	INET-ACL	CACL	AZNACL
CONTAINER	x	x	x			
DOMAIN	x	x	x			
FILE	x	x	x			
GAPPL	x	x				x
GAUTHHOST	x	x				x
GFILE	x	x	x			
GHOST				x		
GSUDO	x	x				
GTERMINAL	x	x				
HOLIDAY	x	x				
HOST				x		
HOSTNET				x		
HOSTNP				x		
LOGINAPPL	x	x				
MFTERMINAL	x	x	x			
PROCESS	x	x	x			
PROGRAM	x	x				
REGKEY	x	x	x			
REGVAL	x	x	x			
SUDO	x	x	x			
SURROGATE	x	x	x			
TCP	x	x	x		x	
TERMINAL	x	x	x			
UACC	x	x				
USER_DIR	x					x

访问权限（按类）

有效访问值取决于资源所属的类。 下表按类列出了 AC 环境中的有效访问值。

类	有效访问值	允许访问者...
所有类	所有	对该类执行*所有*有效操作。
	无	对该类*不执行任何*有效操作。
ADMIN	create	在此类中创建记录。
	delete	在此类中删除记录。
	join-	将组添加到 USER 记录并完成用户到组的链接。 **注意：** 访问者还必须拥有*修改*权限。
	修改	修改现有记录。 **注意：** 要将用户链接到组（将用户名添加到 GROUP 记录），访问者还必须具有*加入*权限。
	密码	更改其他用户的密码。 **注意：** 该访问类型只影响 USER 类。
	read	列出该类中的记录
AUTHHOST	read	从已通过身份验证的主机登录。
CONNECT	read	连接到远程主机。
CONTAINER	*inherited*	**注意：** 该类的有效访问值是包含的对象类的有效值。
DOMAIN	chmod	创建和删除两个域之间的信任关系。 **注意：** 两个域都必须具有这种访问类型。
	execute	从域添加或删除成员。
	read	列出域成员。
FILE、GFILE	chdir	使用等同于 read 和 execute 的权限访问目录。
	chmod	更改文件系统模式。 **注意：** 仅适用于 UNIX 主机。
	chown	更改记录所有者。
	control	执行*所有*有效操作（*删除*和*重命名*除外）。
	create	在此类中创建记录。
	delete	在此类中删除记录。

类	有效访问值	允许访问者...
	execute	执行程序。 **注意：**访问者还必须拥有*读取*权限。
	read	使用文件或目录而不能对其进行更改。 **注意：**在 UNIX 上，如果您需要*读取*权限以控制用户是否可以执行获取有关文件的信息的操作（例如 ls -l），请将 STAT_intercept 配置设置为 1。 有关详细信息，请参阅 *Reference Guide*。
	rename	重命名该类中的记录。
	sec	更改该类中记录的 ACL。
	update	执行*读取*、*写入*和*执行*的组合操作。
	utime	更改文件的修改时间。 **注意：**仅适用于 UNIX 主机。
	write	更改文件或目录。
HNODE	read	列出类中的记录。
	write	编辑记录的详细信息。
HOLIDAY	read	在指定假日登录。
KMODULE	load	加载内核模块。
	unload	卸载内核模块。
MFTERMINAL	read	从大型机终端登录。
	write	从大型机终端管理。
POLICY	delete	删除策略。
	execute	部署策略。
	read	查看策略详细信息。
	write	编辑记录的详细信息。
	undeploy	执行*删除*和*执行*的组合操作。
PROCESS	read	终止进程。
PROGRAM、SUDO、GSUDO	execute	执行程序。
REGKEY	delete	删除 Windows 注册表键。
	read	列出 Windows 注册表键的内容。
	write	更改 Windows 注册表键。

类	有效访问值	允许访问者...
REGVAL	delete	删除 Windows 注册表值。
	read	读取 Windows 注册表值。
	write	更改 Windows 注册表值。
RULESET	read	查看记录的详细信息。
	write	编辑记录的详细信息。
SURROGATE	execute	代理用户。
TCP	read	从远程主机或主机组访问 TCP 服务。
TERMINAL、GTERMINAL	read	登录到终端。
	write	管理终端。
UACC	*inherited*	**注意：**该类的有效访问值是它所定义的类的有效值。
WINSERVICE	read	查看 Windows 服务的属性。
	启动	启动 Windows 服务。
	修改	更改 Windows 服务的属性。
	resume	恢复暂停的 Windows 服务。
	停止	停止 Windows 服务。
	暂停	暂停 Windows 服务

注意：值 none 和 all 适用于所有类。 与 none 不同，值 all 代表特定类的整组访问值。 有关访问权限的详细信息，请参阅适用于您的操作系统的 *《端点管理指南》*。

Windows 访问权限（按类）

有效访问值取决于资源所属的类。 下表按类列出了 Windows (nt) 环境中的有效访问值。

类	有效访问值	允许访问者...
所有类	所有	对该类执行*所有*有效操作。
	无	对该类*不执行任何*有效操作。
COM、DISK	更改	执行*删除*、*读取*和*写入*的组合操作。

类	有效访问值	允许访问者...
	changepermissions	修改资源的 ACL。
	delete	删除资源。
	read	访问资源上的数据而不能对其进行更改。
	takeownership、chown、owner	更改指定资源的所有者。
	write	将数据写入指定的资源。
FILE		**注意：**只可能定义对 NTFS 文件的访问权限；FAT 文件不能拥有访问权限。
	更改	执行*删除*、*读取*和*写入*的组合操作。
	changepermissions、sec	修改资源的 ACL。
	chmod	执行所有操作（*删除*除外）。
	chown	更改指定资源的所有者。
	delete	删除资源。
	execute	执行程序。 **注意：**要使用该访问，访问者还必须拥有*读取*权限。
	read	访问资源而不能对其进行更改。
	rename	重命名资源。 **注意：**要重命名文件，必须具有对资源的*删除*权限和对目标的*重命名*权限。 审核日志可反映事件的顺序。
	write	修改资源。
	update	执行*读取*、*写入*和执行的组合操作。
PRINTER	管理	管理打印机。 例如，为指定的打印机设置数据、暂停打印、恢复打印、清除所有打印作业、更新 ACL 或更改打印机属性。
	print	使用打印机打印。
REGKEY	append、create、subkey	创建或修改注册表键的子键
	takeownership、chown、owner	更改资源所有者
	changepermissions、sec、dac、writedac	修改资源的 ACL。

类	有效访问值	允许访问者...
	delete	删除资源。
	enum	枚举子键。
	link	创建指向注册表键的链接。
	notify	更改注册表键或注册表键子键的通知。
	query	查询注册表键的值
	read	访问资源而不能对其进行更改。
	readcontrol、manage	读取注册表键的安全描述符中的信息，不包括系统（审核）ACL 中的信息。
	set	创建或设置注册表键的值。
	write	更改注册表键及其子键。
SHARE	更改	更改资源的属性或从资源中删除共享。
	read	访问资源而不能对其进行更改。

注意：值 none 和 all 适用于*所有类*。 与 *none* 不同，值 *all* 代表特定类的整组访问值。 有关访问权限的详细信息，请参阅*《端点管理指南：用于 Windows》*。

selang 环境

除了在本地 CA Access Control 数据库中工作以外，selang 还可用于修改本地（Windows 或 UNIX）数据库，本地策略模型数据库 (PMDB)，安装了 CA Access Control 的远程主机（Windows 或 UNIX）上的数据库，或 CA Access Control 配置设置上的数据库。 要切换环境，请使用 *env*（环境）命令，该命令适用于所有环境。

在不同的环境中，有些命令是相同的，但它们使用的参数和 argument 可能会有所不同。 因此，开始在新环境中工作之前，首先应该对语法进行仔细检查。

注意：如果您正在使用 env 输入某个命令的 *native* 属性，则将同时在*本地*环境和当前环境中输入该命令。

支持下列环境：

环境	命令	提示	说明
策略模型	`env pmd`	`AC(pmd)>`	所有 selang 命令均可在本地 PMDB 上运行。
本地 Windows	`env nt`	`AC(nt)>`	所有 selang 命令均可修改 Windows 数据库。
AC	`env ac`	`AC>`	所有 selang 命令均可在 CA Access Control 数据库上运行。 **注意：**这是默认设置。
本地 UNIX	`env unix`	`AC(unix)>`	所有 selang 命令均可在本地 UNIX 主机的安全文件上运行。
本地	`env native`	`AC(native)>`	所有 selang 命令均可在主机的本地环境中运行。
远程配置	`env config`	`AC(config)>`	所有 selang 命令均可在主机的 CA Access Control 配置设置上运行。

更多信息：

environment 命令 - 设置安全环境 (p. 107)
AC 环境中的类 (p. 210)
UNIX 环境中的类 (p. 445)
Windows 环境中的类 (p. 416)

UNIX 上的 selang 配置

在 UNIX 上，您可以管理 selang 的工作方式。 大多数选项都与 selang 管理 UNIX 安全系统的方式有关（适用于 selang UNIX 环境）。

selang 实用程序将以下两个文件用于配置选项：

seos.ini

包含 CA Access Control 配置选项。 这是 CA Access Control 的主配置文件。

lang.ini

包含 selang 使用的配置信息。

selang 在以下 *一个或两个*位置使用 lang.ini 文件：

- seos.ini 文件所在的目录。
- 用户的主目录。

如果只在其中一个 lang.ini 文件中指定标记，则 selang 将使用该文件中的值。 如果在两个 lang.ini 文件中指定的标记不同，则用户的主目录中的值将覆盖另一个值。

服务器的 seos.ini 文件中的标记 DefaultShell 和 DefaultHome 的值将 *覆盖* lang.ini 文件中标记 DefaultShell 和 HomeDirPrefix 中设置的值。

注意：示例 lang.in 文件位于目录 *ACInstallDir*/samples/lang.init 中。

更改用户文件

更新 UNIX 用户的默认文件位于 /etc/passwd，不过您可以更改该默认路径。 如果您在 NIS 下工作，通常需要在 NIS 服务器上执行此操作。

要更改用户文件，请修改 seos.ini 文件中的 *passwd* 部分中的 *YpServerPasswd*，以指向您的用户文件完整路径名。

更改更新组的文件

更新 UNIX 组的默认文件位于 /etc/group，不过您可以更改该默认路径。 如果您在 NIS 下工作，通常需要在 NIS 服务器上执行此操作。

要更改更新组的文件，请修改 **seos.ini** 文件中的 **passwd** 部分中的 **YpServerGroup**，以指向您的用户文件完整路径名。

UNIX 用户和组文件的自动备份

首次在会话中更新 UNIX 用户之前，以及首次在会话中更新 UNIX 组之前，CA Access Control 将创建文件 /etc/passwd or /etc/group 的备份副本。 备份文件分别称为 /etc/passwd.SeOS.bak 和 /etc/group.SeOS.bak。 如果在更新 UNIX 系统时出现错误，则原始信息将可恢复。 仅在首次在 selang 命令 shell 会话中更改 UNIX 系统之前进行备份。

获得 selang 帮助

在交互式 selang 命令环境中，可以随时获得帮助。

要进入 selang 在线帮助，请输入以下内容之一：

? 或帮助

屏幕上将显示您所在环境的 selang 在线帮助文本，其中显示了目录。

帮助主题

主题

定义了 selang 命令或与 selang 命令 shell 相关的其他主题。

将显示说明主题的帮助文本。

帮助环境

env

定义了 selang 环境。

屏幕上将显示指定环境的 selang 在线帮助文本，其中显示了目录。

注意：在 UNIX 上，要显示在命令行中键入的命令的帮助文本，而不删除命令行中的文本，请键入 Ctrl+2（或按 Esc、Esc）。

更多信息：

help 命令 — 获取 selang 帮助 (p. 112)
selang 环境 (p. 32)
selang 命令参考 (p. 37)

第 3 章： selang 命令

此部分包含以下主题：

selang 命令参考

下表按字母顺序列出了所有 selang 命令。

注意：在所有环境中以同样的方式运行的命令仅在 AC 环境中进行记录。 不过，某些命令在多个环境中有效，但它们在每个环境中的运行方式不同。 这些命令在下表的*"说明"*列中用星号 (*) 做了标记，并在其有效的每个环境中分别进行记录。

命令	缩写	环境	说明
alias		AC 和 Unix **注意：**仅适用于 UNIX 主机。	列出或定义 selang 命令和属性的别名。
authorize-	auth	AC 和 NT	*设置特定访问者访问特定资源时所拥有的权限。
authorize-	auth-	AC 和 NT	*删除以前授予特定访问者的访问特定资源的权限。
backuppmd		pmd	将 PMDB 数据库中的数据备份到指定目录。
check		AC	检查用户是否具有对特定资源的访问权限。
checklogin		AC	确定用户的登录权限、是否需要进行密码检查以及是否需要进行终端访问检查。
checkpwd		AC	检查用户的新密码，但不对其进行更改，以确保其符合密码规则。
chfile	cf	AC 和本地	*更改 CA Access Control 或本地操作系统数据库中文件记录的定义。

命令	缩写	环境	说明
chgrp	cg	AC 和本地	*更改 CA Access Control 或本地操作系统数据库中的现有内部组设置。
chres	cr	AC 和 NT	*更改 CA Access Control 或本地操作系统数据库中的现有资源记录。
chusr	cu	AC 和本地	*更改 CA Access Control 或本地操作系统数据库中的现有内部用户。
chxgrp	cxg	AC	更改 CA Access Control 数据库中的现有企业组设置。
chxusr	cxu	AC	更改 CA Access Control 数据库中的现有企业用户设置。
createpmd		pmd	在远程主机上创建 PMDB。
deletepmd		pmd	从远程主机上删除 PMDB 的 selang 保护文件、PMDB 目录的内容和 PMDB 目录。
部署		AC	执行特定 POLICY 的 RULESET 对象中存储的部署 selang 命令。
deploy-		AC	执行特定 POLICY 的 RULESET 对象中存储的策略取消部署 selang 命令。
editfile	ef	AC 和本地	*向 CA Access Control 或本地操作系统数据库中添加文件记录的定义，或对其进行更改。
editgrp	eg	AC 和本地	*向 CA Access Control 或本地操作系统数据库中添加新组，或更改其中的现有组设置。
editres	er	AC 和 NT	向 CA Access Control 或本地操作系统数据库中添加新资源记录，或更改其中的现有资源记录。
editres config		配置	列出您指定的源中的配置设置。
editusr	eu	AC 和本地	向 CA Access Control 或本地操作系统数据库中添加新用户，或更改其中的现有用户。
editxgrp	exg	AC	向 CA Access Control 数据库中添加新企业组，或更改其中的现有企业组属性。
editxusr	exu	AC	向 CA Access Control 数据库中添加新企业用户，或更改其中的现有企业用户属性。
end_transaction		AC	为双控制 PMDB 过程完成 start_transaction 命令。
环境	env	*所有*	设置 selang 所作用于的安全环境。

命令	缩写	环境	说明
find	f	AC 和本地	列出环境中的类或类中的记录。
findpmd		pmd	列出计算机上的所有 PMDB。
find config		配置	列出该主机上您可以管理的配置设置的源（ini 文件或注册表项）。
find file		native	列出系统文件。
find xgroup		nt	列出当前或受托域中的企业组的名称。
find xuser		nt	列出当前或受托域中的企业用户的名称。
get dbexport		AC	检索从 CA Access Control 或 PMD 数据库导出的规则。
get devcalc		AC	检索策略偏差计算结果。
help		*所有*	显示 selang 帮助。
history		*所有*	显示以前在会话中执行的命令。
主机		*所有*	显示或设置 selang 命令发送到的主机。
join-	j	AC 和本地	*将用户加入组。
join-	j-	AC 和本地	*将用户从组中删除。
joinx	jx	AC	将企业用户加入组。
joinx-	jx-	AC	从组中删除企业用户。
列表		AC 和本地	*find* 命令的别名。
listpmd		pmd	列出有关 PMDB 及其订阅者、更新文件和错误日志的信息。
newfile	nf	AC	向 CA Access Control 数据库中添加文件记录的定义。
newgrp	ng	AC 和本地	*向 CA Access Control 或本地操作系统数据库中添加新组。
newres	nr	AC 和 NT	*向 CA Access Control 或本地操作系统数据库中添加新的资源记录。
newusr	nu	AC 和本地	*向 CA Access Control 或本地操作系统数据库中添加新的内部用户。
newxgrp	nxg	AC	向 CA Access Control 数据库添加新企业组。
newxusr	nxu	AC	向 CA Access Control 数据库添加新企业用户。

命令	缩写	环境	说明
pmd		pmd	清除策略模型错误日志、更新订阅者列表、发布订阅者、启动和停止策略模型服务、截短更新文件以及重新加载初始化文件。
rename		AC	重命名数据库中的对象。
restorepmd		pmd	在本地主机上还原 PMDB。
rmfile	rf	AC	从 CA Access Control 数据库中删除文件资源记录。
rmgrp	rg	AC 和本地	*从 CA Access Control 或本地操作系统数据库中删除组。
rmres	rr	AC 和 NT	*从 CA Access Control 或本地 Windows 数据库中删除资源记录。
rmusr	ru	AC 和本地	*从 CA Access Control 或本地操作系统数据库中删除用户。
rmxgrp	rxg	AC	从 CA Access Control 数据库中删除企业组。
rmxusr	rxu	AC	从 CA Access Control 中删除企业用户。
ruler		AC 和本地	设置执行 show 命令时显示的属性。
search		AC 和本地	*find* 命令的别名。
setoptions	so	AC 和 NT	*设置或显示控制数据库行为的全局选项。
showfile	sf	AC 和本地	*列出 CA Access Control 或本地操作系统数据库中文件记录的属性。
showgrp	sg	AC 和本地	*列出 CA Access Control 或本地操作系统数据库中组记录的属性。
showres	sr	AC 和 NT	*列出 CA Access Control 或本地 Windows 数据库中记录的属性。
showres config		配置	列出您指定的源中的配置设置。
showusr	su	AC 和本地	*列出 CA Access Control 数据库或本地操作系统数据库中用户记录的属性。
showxusr	sxu	AC	列出 CA Access Control 中企业用户记录的属性。
source		*所有*	执行特定文件中的命令。
start dbexport		AC	导出 CA Access Control 或 PMD 数据库。
start devcalc		AC	触发策略偏差计算。

命令	缩写	环境	说明
start_transaction		AC	使用一个或多个命令开始记录包含双控制 PMDB 过程的未处理事务的文件。
subs		pmd	将订阅者添加到父 PMDB 或将数据库订阅到父 PMDB。
subspmd		pmd	更改您所连接到的主机中的数据库的父级。
unalias		AC 和 Unix	删除 selang 命令和属性的别名。
undeploy		AC	deploy- 命令的别名。
unsubs		pmd	从 PMDB 的订阅者列表中删除订阅者。
xaudit		nt	设置审核条件并开始记录访问事件。
xaudit-		nt	删除审核条件并停止记录访问事件。

注意：本地环境符合 Windows (nt) 或 UNIX 环境的规则，这取决于您所连接的主机的操作系统。

AC 环境下的 selang 命令

本节包含在 CA Access Control 数据库运行的所有 selang 命令的完整参考（AC 环境下的命令），这些命令按字母顺序排列。

alias 命令 - 定义 selang 别名

在 UNIX 主机上有效

使用 alias 命令列出或定义 selang 命令和属性的别名。 任何用户都可以使用 alias 命令。

注意：您可以通过在启动文件中定义别名以及使用 *selang -r* 命令来构建要在所有 selang 会话中使用的一组别名。

此命令有以下格式：

```
alias [aliasName [aliasValue]]
```

aliasName

（可选）定义要用作别名的名称。

如果未指定该选项，则 alias 命令将列出所有定义的别名。

aliasValue

（可选）定义 selang 命令 shell 应与 *aliasName* 相关联的意义。

如果未指定该选项，则 alias 命令将显示指定别名的值。

您最多还可以在 *aliasValue* 中包括十个变量（$0 至 $9）。 如果 *aliasValue* 包含变量，则调用别名时，必须使用括号中正确的值替换每个变量。

示例：使用变量简化新管理员的创建

要创建一个别名，以使向数据库添加新管理员更加方便，请输入以下命令：

```
alias newadm newusr ($0) admin
```

要使用该别名，只需在方括号中添加新管理员的名称。 例如：

```
newadm(Terri)
```

这样将把名为 Terri 的用户添加到数据库。 Terri 将被赋予管理数据库所需的 ADMIN 属性。 这与输入以下命令等效：

```
newusr Terri admin
```

示例：简化属性名称

要创建别名以便使用缩短的别名 *acc* 替换属性名称 *access*，请输入以下命令：

```
alias acc access
```

您现在可以输入以下内容以使用该别名：

```
authorize file x uid(y) acc(z)
```

示例：在上下文中使用别名

别名不只是扩展的变量；它们仅在应指定命令名和属性名的上下文中进行解释。 例如，定义别名：

```
alias newterm newres terminal
```

然后发出以下命令：

```
newterm newterm owner(nobody)
```

将替换第一个 newterm 字符串而不是第二个，因为上下文需要字符串的第二个实例成为终端名。 这与输入以下命令等效：

```
newres terminal newterm owner(nobody)
```

更多信息：

unalias 命令 — 删除 selang 别名 (p. 150)
selang 实用程序—运行 CA Access Control 命令行 (p. 18)

authorize 命令 - 设置对资源的访问权限

在 AC 环境中有效

使用 authorize 命令更改访问者对资源的访问权限。

该命令可修改与资源相关联的 Access Control 列表。 它一次仅更改 Access Control 列表中的一个条目。

访问者尝试访问资源时，CA Access Control 将检查相应的 Access Control 列表以确定访问权限。 这些 Access Control 列表可包括资源记录中的那些，还可以包括资源组记录中的 Access Control 列表。 如果拒绝授予访问者对包括资源的任何 NACL 的访问权限，则拒绝授予该权限，即使该权限是由其他 ACL 授予的。

资源的所有者拥有对该资源的所有访问权限。 如果要更改用户（所有者）的访问权限，请更改资源的所有者，例如，用户 nobody。

注意：此命令同样存在于 Windows 环境中，但操作方式有所不同。

要使用 authorize 命令，您需要有足够的权限，这意味必须符合下列要求一个或多个要求：

- 您具有 ADMIN 属性。
- 您具有资源所属的资源组的 GROUP-ADMIN 属性。
- 您是资源的所有者。
- 您具有在与资源相对应的 ADMIN 类记录中的修改权限。

对于不同的类集，authorize 命令具有不同的形式。 这些类集包括：

- TCP
- HOST、GHOST、HOSTNET 和 HOSTNP
- 其他所有类

对于 TCP 类，此命令具有以下格式：

```
{authorize|auth} TCP tcpServiceName \
    [{access|deniedaccess}(accessType)] \
    {[ghost(ghostName [,ghostName]...)] | \
    [host(hostName [,hostName]...)] | \
    [hostnet(hostNetName [,hostNetName]...)] | \
    [hostnp(hostNamePattern [,hostNamePattern]...)]} \
    [{gid|uid|xgid|xuid}(accessor [,accessor]...])] ...
```

对于 HOST、GHOST、HOSTNET 和 HOSTNP 类，此命令具有以下格式：

```
{authorize|auth} {HOST|GHOST|HOSTNET|HOSTNP} stationName
    [{access|deniedaccess}(accessType)] \
    service({serviceName|serviceNumber|serviceNumberRange}) \
    { gid | uid | xgid | xuid}(accessor [,accessor...]) ...
```

对于所有其他类，该命令具有以下格式：

```
{authorize|auth} className resourceName \
    [{access|deniedaccess}(accessType)] \
    [calendar(calendarName)] \
    [{unix|nt}]\
    [via (pgm ( program [,program]...))] \
    { gid | uid | xgid | xuid}(accessor [,accessor...]) ...
```

access (*accessType*)

定义资源 ACL Access Control 列表中的访问权限条目。 该 ACL 可指定向访问者授予的访问权限。

accessType

定义资源 ACL 中的访问类型，例如读取或写入。

注意：如果您同时忽略 authorize 命令的 access(*accessType*) 和 deniedaccess(*accessType*) 选项，则 CA Access Control 将为资源（例如，如果资源为文件，则在 UACC 文件记录中）类分配由 UACC 类中记录的隐性访问权限属性指定的访问权限。

calendar(*calendarName*)

指定用于确定访问权限的日历。

className

定义 *resourceName* 所属的类。

deniedaccess(*accessType*)

更改资源 NACL 中的访问权限。 NACL 可指定拒绝授予访问者的访问类型。

accessType

指定要拒绝授予的访问类型，例如读取或写入。

gid (*accessor* [,*accessor*...])

定义一个或多个您要为其设置访问权限的内部组。

ghost(*ghostName [,ghostName]*...)

定义一个或多个您要为其设置对 TCP/IP 服务的访问权限的主机组。

host(*hostName [,hostName]*...)

定义一个或多个您要为其设置对 TCP/IP 服务的访问权限的主机。

hostnet(*hostNetName [,hostNetName]*...)

定义一个或多个您要为其设置对 TCP/IP 服务的访问权限的 HOSTNET 记录。

hostnp(*hostNamePattern [,hostNamePattern]*...)

定义一个或多个您要为其设置对 TCP/IP 服务的访问权限的 HOSTNP 记录。

nt

指定是否向 Windows 中的系统 ACL 添加值。

仅对 FILE 类有效。

resourceName

定义正在修改其 Access Control 列表的资源记录。

service(*serviceName*|*serviceNumber*|*serviceNumberRange*)

定义允许本地主机向远程主机提供的服务。

serviceNumber |serviceNumberRange

定义服务编号或范围。

指定范围，两个整数之间用 -（连字符）分隔，例如 1-99。

限制：整数的范围在 0 到 65535 之间。

stationName

在指明的类中指定记录名称，如下所述：

- **HOST -** 单个工作站的名称。
- **GHOST** - 通过 ghost 命令在数据库中定义的主机组的名称。
- **HOSTNET** - 通过 IP 地址的一组掩码和匹配值定义的主机组的名称。
- **HOSTNP** - 通过名称模式定义的主机组的名称。

对于无法解析的主机，请以 IPv4 格式指定 IP 地址范围。

tcpServiceName

指定要为其设置访问权限的 CA Access Control TCP 服务记录。

uid (*accessor* [,*accessor*...])

定义一个或多个您要为其设置访问权限的内部用户。

可以使用 * 代表所有内部用户。

unix

指定是否向 UNIX 中的系统 ACL 添加值。

仅在支持 ACL 的 UNIX 环境中有效，且仅适用于 FILE 类中的记录。

via(pgm(*programName [,programName]*...))

为条件程序访问定义一个或多个程序。 via 参数可指定资源的 PACL 中的一个条目。 *programName* 可指定可以访问该资源的程序。 *programName* 可以包含通配符。 如果程序与 PACL 中的多个条目匹配，则具有最长非通配符匹配项的条目优先。

如果 *pgmName* 指定的程序或 shell 脚本未在 PROGRAM 类中定义，则 CA Access Control 将自动创建 PROGRAM 记录以对其进行保护。

xgid (*accessor* [,*accessor*...])

定义一个或多个您要为其设置访问权限的企业组。

xuid (*accessor* [,*accessor*...])

定义一个或多个您要为其设置访问权限的企业用户。

示例：授权 Angela 读取文件

以下 selang 命令可授权企业用户 Angela 读取受 FILE 资源 /projects/secrets 保护的文件：

```
auth FILE /projects/secrets xuid(Angela) access(read)
```

示例：仅授权 Angela 读取文件

以下 selang 命令仅授权企业用户 Angela 自己读取受 FILE 资源 /projects/secrets 保护的文件：

```
auth FILE /projects/secrets xuid(Angela) access(read)
auth FILE /projects/secrets defaccess (none)
chres FILE /projects/secrets owner(nobody)
```

注意：在 UNIX 上，如果您需要 *读取*权限以控制用户是否可以执行获取有关文件的信息的操作（例如 ls -l），请将 STAT_intercept 配置设置为 1。有关详细信息，请参阅 *Reference Guide*。

示例：授权组中的所有用户登录终端

以下 selang 命令可授权企业组 RESEARCH 的所有成员登录受 TERMINAL 资源 *tty10* 保护的终端：

```
auth TERMINAL tty10 xgid(RESEARCH) access(read)
```

示例：授权 Joe 备份文件

以下 selang 命令授权企业用户 Joe 备份受 GFILE 资源 secret_files 保护的文件：

```
auth GFILE secret_files xuid(Joe) \
via(pgm(/bin/backup)) access(read)
```

对于 Windows 端点，以下命令等效：

```
auth GFILE secret_files xuid(Joe) \
via(pgm(C:\WINDOWS\system32\ntbackup.exe)) access(read)
```

这些命令仅在 Joe 的访问权限不是由资源的 ACL 或 NACL 确定的时有效。

更多信息：

authorize- 命令 - 从资源删除访问权限 (p. 47)
authorize 命令 — 设置访问者对 Windows 资源的访问权限 (p. 169)
chfile 命令 - 修改文件记录 (p. 54)
ch[x]grp 命令 - 更改组属性 (p. 60)
chres 命令 - 修改资源记录 (p. 72)
ch[x]usr 命令 - 更改用户属性 (p. 87)
authorize- 命令 — 删除访问者对 Windows 资源的访问权限 (p. 171)

authorize- 命令 - 从资源删除访问权限

在 AC 环境中有效

使用 authorize- 命令从资源的 Access Control 列表 (ACL) 中删除访问者。

注意：此命令同样存在于本地 Windows 环境中，但操作方式有所不同。

您需要具有与使用 authorize 命令相同的访问权限，才能使用 authorize- 命令。

对于不同的类集，authorize- 命令具有不同的格式。 这些类集包括：

- TCP
- HOST、GHOST、HOSTNET 和 HOSTNP
- 其他所有类

对于 TCP 类，此命令具有以下格式：

```
{authorize-|auth-} TCP tcpServiceName \
    {gid |uid |xgid |xuid } (accessorName [,accessorName]...)\
    [host(hostName [,hostName]...)] \
    [ghost(ghostName [,ghostname]...)] \
    [hostnet(hostNetName [,hostNetName]...)] \
    [hostnp(hostNamePattern [,hostNamePattern]...)]
```

对于 HOST、GHOST、HOSTNET 和 HOSTNP 类，此命令具有以下格式：

```
{authorize-|auth-} className stationName \
    service({serviceName | serviceNumber |serviceNumberRange})
```

对于所有其他类，该命令具有以下格式：

```
{authorize-|auth-} className resourceName \
    [{access-|deniedaccess-}]\
    [calendar(calendarName)] \
    {gid |uid |xgid |xuid } (accessorName [,accessorName]...)
```

access-

指定命令应从资源 ACL（授予访问权限）中而非 NACL 中删除访问者。

如果既未指定 access- 也未指定 deniedaccess-，则命令将从两个 ACL 中删除访问者。

calendar(*calendarName*)

删除指定用于确定访问权限的日历。

className

指定 *resourceName* 所属的类的名称。

deniedaccess-

指定命令应从资源 NACL（拒绝授予访问权限）中而非 ACL 中删除访问者。

gid (*accessor* [,*accessor*]...)

定义一个或多个要从中删除条目的内部组。 用逗号或空格分隔每个 *访问者*。

ghost(*ghostName*)

指定 GHOST 类中对象的名称。

host(*hostName*)

指定 HOST 类中对象的名称。

hostnet(*hostNetName*)

指定 HOSTNET 类中对象的名称。

hostnp(*hostNamePattern*)

指定 HOSTNP 类中定义的模式。

nt

指定是否从 Windows 中的系统 ACL 中删除值。

仅对 FILE 类有效。

resourceName

指定要修改其 Access Control 列表的资源记录的名称。 仅指定一个资源记录。

service(*serviceName*|*serviceNumber*|*serviceNumberRange*)

定义要从 ACL 中删除的服务。

stationName

在指明的类中指定记录名称，如下所述：

- **HOST -** 单个工作站的名称。
- **GHOST** - 通过 ghost 命令在数据库中定义的主机组的名称。
- **HOSTNET** - 通过 IP 地址的一组掩码和匹配值定义的主机组的名称。
- **HOSTNP** - 通过名称模式定义的主机组的名称。

对于无法解析的主机，请指定 IP 地址范围。

serviceNumber |serviceNumberRange

定义服务编号或范围。

指定范围，两个整数之间用 -（连字符）分隔，例如 1-99。

限制：整数的范围在 0 到 65535 之间

uid (*accessor* [,*accessor*]...)

定义一个或多个要删除其条目的内部用户。 用逗号或空格分隔每个*访问者*。

可以使用 uid(*) 指定所有内部用户。

unix

指定是否从 UNIX 中的系统 ACL 中删除添加项。

仅在支持 ACL 的 UNIX 环境中有效，且仅适用于 FILE 类中的记录。

xgid (*accessor* [,*accessor*]...)

定义一个或多个要删除其条目的企业用户。 使用逗号或空格分隔每个 *accessorName*。

xuid (*accessor* [,*accessor*]...)

定义一个或多个要删除其条目的企业组。 用逗号或空格分隔每个*访问者*。

示例：删除某个组访问文件的权限

以下命令可从资源 /products/new 所包含文件的 ACL 和 NACL 删除组 research：

```
auth- FILE /products/new xgid(research)
```

research 组现在具有对文件的默认访问权限。

更多信息：

authorize 命令 - 设置对资源的访问权限 (p. 43)
authorize 命令 — 设置访问者对 Windows 资源的访问权限 (p. 169)
authorize- 命令 — 删除访问者对 Windows 资源的访问权限 (p. 171)
chfile 命令 - 修改文件记录 (p. 54)
ch[x]grp 命令 - 更改组属性 (p. 60)
chres 命令 - 修改资源记录 (p. 72)
ch[x]usr 命令 - 更改用户属性 (p. 87)

check 命令 - 确定用户访问权限

在 AC 环境中有效

使用 check 命令可确定用户是否拥有对特定资源的访问权限。 该命令可根据资源的 ACL 和默认访问属性检查访问权限。 但是，它不支持 PACL；即，它不指明用户是否可以使用特定程序访问资源。

注意：seos 关闭时，该命令不可用。 有关 PACL 的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

要使用此命令，您必须按照以下任一条件的定义，对资源具有足够的权限：

- 运行此命令的进程具有 SERVER 属性。
- 您具有 ADMIN 属性。

此命令有以下格式：

```
check className resourceName uid(userName) access(authority)
```

access(*authority*)

定义要为由 uid 参数标识的访问者检查的访问权限。

有效值取决于被检查的值。

className

定义 *resourceName* 所属的类名。

resourceName

定义资源记录的名称。

uid(*userName*)

定义要验证其对 *resourceName* 的访问权限的 CA Access Control 用户的名称。

示例：确定用户是否具有对资源的访问权限

要确定用户 Alain 是否具有对 *file* 类的资源 *testfile* 的写入权限，请输入以下命令：

```
check FILE /testfile uid(Alain) access(w)
```

该命令的以下示例输出表明用户 Alain 具有对被拒绝文件的写入权限，因为 Alain 是资源的所有者：

```
Access to FILE /testfile GRANTED
Stage: Resource OWNER check
```

checklogin 命令 - 确定登录信息

在 AC 环境中有效

使用 checklogin 命令可确定用户的登录权限、是否需要进行密码检查以及是否需要进行终端访问检查。

注意：seos 关闭时，该命令不可用。

要使用此命令，您必须按照以下任一条件的定义，对资源具有足够的权限：

- 运行此命令的进程具有 SERVER 属性。
- 您具有 ADMIN 属性。

此命令有以下格式：

```
checklogin userName [password(password)] [terminal(terminalName)]
```

password(*password*)

（可选）定义在已启用密码检查时，CA Access Control 要根据操作系统密码和数据库检查的密码。

userName

定义要验证登录权限的用户的名称。

terminal(*terminalName*)

（可选）定义终端，CA Access Control 将对其进行检查以确定用户是否具有从该终端登录的权限。

示例：确定用户是否具有登录权限

要确定用户 Frank 是否拥有从终端 *mutra* 登录到 *localhost* 的权限，请输入以下命令：

```
checklogin Frank terminal(mutra)
```

以下命令输出表明用户 Frank 可以从终端 mutra 登录到主机 winsome (localhost)：

```
Login by USER frank to host winsome is GRANTED
Stage: Resource class global universal access
```

要验证用户 Frank 的密码，请输入以下命令：

```
checklogin frank password(111) terminal(localhost)
```

要根据 CA Access Control 数据库中的密码验证用户 Frank 的密码，请输入下列命令：

```
so class+(PASSWORD) (localhost)
checklogin frank password(moonshine) terminal(tack)
```

上述 *so* 命令可启用密码检查。

checkpwd 命令 - 检查密码的遵从性

在 AC 环境中有效

使用 checkpwd 命令检查用户密码是否遵从密码规则。 这种检查并不更改密码。

要使用该命令，您必须是具有 ADMIN 属性的超级用户。

将根据 CA Access Control 密码规则接受或拒绝新密码。

- 如果接受新密码，将显示下面的成功消息：

  ```
  Changing userName's password is permitted.
  ```

- 如果拒绝新密码，将显示下面的失败消息：

  ```
  Changing userName's password is denied.
  denied_reason
  ```

  其中 *denied_reason* 是未通过的实际密码规则。

  例如：

  ```
  Changing JDoe's password is denied.
  Too few lowercase letters in password.
  ```

denied_reason 中只显示密码失败的第一个规则。 例如，如果密码过短，*且*该密码的大写字母过少，则仅会显示*密码太短*。

注意：seos 关闭时，该命令不可用。 有关密码规则的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

此命令有以下格式：

```
checkpwd userName password(newPassword)
```

userName

指定要检查其新密码的 CA Access Control 用户的名称。

password(*newPassword*)

指定要检查的密码。

chfile 命令 - 修改文件记录

在 AC 环境中有效

使用 chfile、editfile 和 newfile 命令可以处理 FILE 类中的记录。 这些命令结构相同，仅在以下方面有所不同：

- chfile 命令可*修改* FILE 类中的一个或多个记录。
- editfile 命令可*创建或修改* FILE 类中的一个或多个记录。
- newfile 命令可*创建* FILE 类中的一个或多个记录。

注意：该命令还存在于本地环境中，但运行方式不同。

要添加或更改属于 FILE 类的某个文件的记录，您必须对该文件拥有足够的权限。 CA Access Control 将进行下列检查，直到满足下列条件之一为止：

1. 您具有 ADMIN 属性。
2. 资源记录在某一组的范围内，您在该组中具有 GROUP-ADMIN 属性。
3. 更改记录时，您是记录的所有者。
4. 您在 ADMIN 类中的 FILE 记录的 ACL 中具有 CREATE （对于 newfile 或 editfile）或 MODIFY（对于 chfile）访问权限。
5. 如果将 seos.ini 文件中的标记 use_unix_file_owner 设置为“yes”，则您将是文件的所有者（向存在于本地操作系统中的 CA Access Control 定义文件时）。

```
{{chfile|cf}|{editfile|ef}|{newfile|nf}} filename... \
    [audit{none|all|success|failure}] \
    [category[-](categoryName)] \
    [comment(string)|comment-] \
    [defaccess(accessAuthority)] \
    [label(labelName)|label-] \
    [level(number)|level-] \
    [notify(mailAddress)|notify-] \
    [gowner(groupName)] \
    [owner({userName|groupName})] \
    [restrictions( \
        [days({anyday|weekdays|{[mon] [tue] [wed] \
                [thu] [fri] [sat] [sun]}})] \
        [time({anytime|startTime:endTime}) \
    |restrictions-] \
    [warning|warning-]
```

audit{none|all|success|failure}

指定记录哪些访问事件。 访问类型包括：

- **all** - CA Access Control 既记录授权的访问，也记录检测到的未经授权的访问尝试。
- **failure** - CA Access Control 记录检测到的未经授权的访问尝试。这是默认值。
- **none** - CA Access Control 不向日志文件写入任何记录。
- **success** - CA Access Control 记录对资源的授权访问。

注意：要使用 audit 参数，您必须具有 AUDITOR 属性。

category(*categoryName*)

定义要分配给文件的安全类别记录的列表（用空格或逗号分隔）（在 CATEGORY 类中定义）。

如果在 CATEGORY 类不活动时指定 category 参数，CA Access Control 将更新数据库中的文件定义；但是，在再次激活 CATEGORY 类之前，更新的类别分配不会生效。

注意：有关安全类别检查的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

category-(*categoryName*)

从资源记录删除一个或多个安全类别。 删除多个安全类别时，请用空格或逗号分隔安全类别名称。

将从资源记录中删除指定的安全类别，无论 CATEGORY 类是否是活动的。

注意：此参数仅在修改记录时有效。

comment(*string*)

将最多包含 255 个字符的字母数字字符串添加到文件记录中。 如果字符串中包含任何空格，请用单引号将整个字符串引起。 字符串将替换先前定义的任何现有注释。

comment-

从文件记录中删除注释字符串。

注意：此参数仅在修改记录时有效。

defaccess(*accessAuthority*)

指定文件的默认访问权限。 默认访问权限是授予请求文件访问权限的任何访问者的权限，但它并不在文件的 Access Control 列表中。 默认访问权限也适用于未在数据库中定义的用户。

文件名

定义文件记录的名称。 必须至少指定一个文件名。

如果使用通用文件名将记录添加到 FILE 类中或在其中更改记录，请使用在 selang 中允许的通配符表达式。 定义或更改多个记录时，请使用括号括起文件名列表，并用空格或逗号分隔文件名。

注意：如果指定了多个文件名，CA Access Control 将根据指定的参数分别处理每个文件记录。 如果处理文件时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个文件。

gowner(*groupName*)

将 CA Access Control 组指定为文件记录的所有者。如果文件记录的组所有者的安全级别、安全标签和安全类别权限使其足以能够访问文件，则该组所有者对该文件拥有不受限制的访问权限。 文件的组所有者始终可以更新和删除文件记录。

label(*labelName*)

将在 SECLABEL 类中定义的安全标签分配给文件。 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。 如果资源记录当前包含一个安全标签，在此处指定的安全标签将替换当前的安全标签。

注意：有关安全标签的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

label-

删除在文件记录中定义的安全标签。

注意：此参数仅在修改记录时有效。

level(*number*)

为资源记录指定安全级别。 请输入介于 1 和 255 之间的正整数。 如果以前为资源记录指定了安全级别，则新值将替换当前值。

注意：有关安全级别的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

level-

阻止 CA Access Control 对资源执行安全级别检查。

注意：此参数仅在修改记录时有效。

notify(*mailAddress*)

只要该资源记录代表的资源被成功访问，便指示 CA Access Control 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）。

只有在日志路由系统活动时，才进行通知。 通知消息将发送到屏幕上或用户的邮箱，具体取决于日志路由系统的设置。

每次发送通知消息时，都会在审核日志中写入审核记录。

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。

范围：30 个字符。

注意：有关筛选和查看审核记录的信息，请参阅适用于您的操作系统的*《端点管理指南》*。

notify-

指定在 CA Access Control 授予对记录所代表的文件的访问权限时不通知任何人。

注意：此参数仅在修改记录时有效。

owner(*Name*)

将 CA Access Control 用户或组指定为文件记录的所有者。如果文件记录所有者的安全级别、安全标签和安全类别权限使其足以能够访问文件，则该所有者对该文件拥有不受限制的访问权限。 文件的所有者始终可以更新和删除文件记录。

restrictions(days(*dayData*) time(*timeData*))

指定用户可以在一周的哪几天以及一天的哪几个小时访问文件。

如果省略 days 参数而指定 time 参数，则时间限制将应用于记录中已经指出的任何“工作日”限制。 如果省略 time 而指定 days，则日期限制将应用于记录中已经指出的任何时间限制。 如果同时指定了 days 和 time，则用户只能在指定日期的指定时间段内访问系统。

days(*dayData*)

指定用户可以访问文件的日期。 days 参数可使用下列子参数：

- **anyday** - 授予在任何一天访问文件的权限。
- **weekdays** - 授予只能在工作日（星期一至星期五）访问资源的权限。
- **mon tue wed thu fri sat sun** - 授予只能在指定日期访问资源的权限。 您可以按任何顺序指定日期。 如果指定多个日期，请使用空格或逗号分隔各日期。

time(*timeData*)

指定用户可以访问文件的时间段。 time 参数可使用下列子参数：

- **anytime** - 授予在一天中的任何时间访问资源的权限。
- *startTime*:*endTime* - 授予只能在指定时间段内访问资源的权限。 *startTime* 和 *endTime* 的格式均为 *hhmm*，其中 *hh* 是采用 24 小时表示法的小时（00 至 23），而 *mm* 是分钟（00 至 59）。 请注意，2400 是无效的时间值。 *StartTime* 必须小于 *endTime*，并且这两个时间必须在同一天。 如果终端与处理器位于不同的时区，请通过将终端的开始时间和结束时间转换为等同的处理器本地时间来调整时间值。 例如，如果处理器位于纽约而终端位于洛杉矶，那么，要允许从上午 8:00 到下午 5:00 在洛杉矶访问终端，请指定时间 (1100:2000)。

限制-

删除限制文件访问能力的所有限制。

注意：此参数仅在修改记录时有效。

warning

将文件置于“警告”模式。

warning-

使文件退出“警告”模式。

示例：将对文件的访问权限限制为除超级用户之外的所有用户

要将对 /etc/passwd 文件的访问权限限制为除超级用户之外的所有用户的读取权限，请输入以下命令：

```
chfile /etc/passwd defaccess(read) owner(root)
```

必须符合以下条件：

- 您具有 ADMIN 属性。
- 数据库中定义了记录 /etc/passwd。
- 记录 /etc/passwd 的 ACL 中无任何条目。

示例：将对文件的访问权限限制为按时间

要阻止对 /home/bob/secrets 文件的访问权限，且只允许所有者在工作日的 08:00 到 18:00 访问文件，请输入以下命令：

```
newfile /home/bob/secrets defac(none) restrictions(d(weekdays) t(0800:1800))
```

必须符合以下条件：

- 您具有 ADMIN 属性。
- Bob 是 CA Access Control 用户，而且是 FILE 类中 /home/ bob/secrets 记录的所有者。

示例：阻止对您主目录的访问

要阻止其他所有用户访问您主目录 (/home/bob) 中的任何文件，请在 UNIX 上输入以下命令：

```
newfile /home/bob/* defaccess(none)
```

您可以使用以下命令在 Windows 上执行相同的操作：

```
newfile %userprofile%\* defaccess(none)
```

必须符合以下条件：

- 您已被定义到 CA Access Control。
- 您是该文件的本地所有者。

更多信息：

authorize 命令 - 设置对资源的访问权限 (p. 43)
rmfile 命令 — 删除文件记录 (p. 122)
showfile 命令 — 显示文件属性 (p. 136)
chfile 命令 — 修改 UNIX 文件设置 (p. 156)
chfile 命令 — 修改 Windows 文件设置 (p. 172)
访问权限（按类） (p. 28)

ch[x]grp 命令 - 更改组属性

在 AC 环境中有效

使用命令 chgrp、chxgrp、editgrp、editxgrp、newgrp 和 newxgrp 可以更改组属性，还可以在 CA Access Control 数据库中创建组（如有必要）。

这些命令均具有同义词，具体如下：

- chgrp—cg
- chxgrp—cxg
- editgrp—eg
- editxgrp—exg
- newgrp—ng
- newxgrp—nxg

这些命令的结构相同，只是范围在以下方面有所不同：

- chgrp、editgrp 和 newgr 命令可以处理 GROUP 类中的记录。 这些命令用于创建或修改与企业用户存储无关的 CA Access Control 组。 这些命令之间的差异如下：
  - chgrp 命令可*修改* GROUP 类中的一个或多个记录。
  - editgrp 命令可*创建或修改* GROUP 类中的一个或多个记录。
  - newgrp 命令可*创建* GROUP 类中的一个或多个记录。

  注意：这些命令同样存在于本地环境中，但操作方式有所不同。
- chxgrp、editxgrp 和 newxgrp 命令可以处理 XGROUP 类中的记录。 这些命令用于创建或修改在企业用户存储中定义的 CA Access Control 组。 它们之间的差异如下：
  - chxgrp 命令可*修改* XGROUP 类中的一个或多个记录。
  - editxgrp 命令可*创建或修改* XGROUP 类中的一个或多个记录。
  - newxgrp 命令可*创建* XGROUP 类中的一个或多个记录。

所需授权

要创建新的 CA Access Control 组，至少必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 在 ADMIN 类中的 GROUP 或 XGROUP 记录的 Access Control 列表中为您分配了创建权限。

要添加或修改组，至少必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是组的所有者。
- 在 ADMIN 类中的 GROUP 或 XGROUP 记录的 Access Control 列表中为您分配了修改（对于 ch[x]grp）或创建（对于 edit[x]grp）权限。

```
{{chgrp|cg}|{chxgrp|cxg}|{editgrp|eg}|{editxgrp|exg}|{newgrp|ng}|{newxgrp|nxg
}} groupName ...
    [{admin | admin-}] \
    [audit(none|all|success|failure|loginsuccess|loginfail|trace|interactive)
    |audit-] \
    [{auditor | auditor-}] \
    [comment(string)|comment-] \
    [expire[(mm/dd/yy[yy[@hh:mm])]|expire-] \
    [gowner(groupName)] \
    [homedir(fullPath|nohomedir)] \
    [inactive(numInactiveDays)|inactive-] \
    [maxlogins(maximumNumberOfLogins)|maxlogins-] \
    [mem(groupName)|mem+(groupName)|mem-(groupName)]\
    [name('fullName')] \
    [nt[(comment(comment))]
    [{operator | operator-}] \
    [owner(userName|groupName)] \
    [parent(groupName)|parent-] \
    [password( \
        [history(numberStoredPasswords)|history-] \
        [interval(maximumPasswordChangeInterval)|interval-] \
        [min_life(minimumPasswordChangeInterval)|min_life-] \
        [rules( \
                [alpha(minimumAlphaCharacters)] \
                [alphanum(minimumAlphanumericCharacters)] \
                [bidirectional|bidirectional-] \
                [grace(numberOfGraceLogins)] \
                [min_len(minimumPasswordLength)] \
                [max_len(maximumPasswordLength)] \
                [lowercase(minimumLowercaseCharacters)] \
                [max_rep(maxRepetitiveCharacters)] \
                [namechk|namechk-] \
                [numeric(minimumNumericCharacters)] \
                [oldpwchk|oldpwchk-] \
                [special(minimumSpecialCharacters)] \
                [uppercase(minimumUppercaseCharacters)] \
                [use_dbdict|use_dbdict-] \
        )|rules-] \
        )] \
```

```
[pmdb(PolicyModelName)|pmdb-] \
[{pwmanager | pwmanager-}] \
[restrictions( \
    [days({anyday|weekdays|{[mon] [tue] [wed] \
            [thu] [fri] [sat] [sun]}})] \
    [time(anytime|startTime:endTime) \
|restrictions-] \
[resume[(mm/dd/yy[yy][@hh:mm])]|resume-] \
[{server | server-}] \
[shellprog(fullPath)] \
[supgroup(superiorGroup)|supgroup-] \
[suspend[(mm/dd/yy[yy][@hh:mm])]|suspend-] \
[unix[( \
    [appl(quotedString)] \
    [groupid(groupidNumber)] \
    [userlist(userName...)] \
)]] \
```

要删除由字符串定义属性的任何记录属性，请键入属性，后面紧跟 -（减号）或 ()（空圆括号）。

注意：只有在组用作配置文件组时，某几个参数才相关。 配置文件组不能为企业组。

admin

为组分配 ADMIN 属性。所在组具有 ADMIN 属性的用户可以发出带有除 audit 参数以外所有参数的所有 selang 命令。 您必须具有 ADMIN 属性才能使用 admin 参数。

admin-

从组中删除 ADMIN 属性。 （CA Access Control 可确保至少一个用户具有 ADMIN 属性。）

不能将此参数与 new[x]grp 命令一起使用。

audit(*mode*)

打开该命令的跟踪审核。 审核模式为：none、all、success、failure、loginsuccess、loginfail、trace、interactive。

审核-

关闭该命令的跟踪审核。

auditor

为组分配 AUDITOR 属性。 所在组具有 AUDITOR 属性的用户可以审核系统资源的使用，并且能够控制是否记录在 CA Access Control 授权检查过程中检测到的对任何受 CA Access Control -保护资源的访问以及对数据库的访问。 有关授予具有 AUDITOR 属性的用户的权限的详细信息，请参阅适用于您的操作系统的 *《端点管理指南》*。

auditor-

从组记录中删除 AUDITOR 属性。

不能将此参数与 new[x]grp 命令一起使用。

comment(*string*)

向组记录添加最多为 255 个字母数字字符（单字节）的注释字符串。如果字符串中包含空格，请用单引号将整个字符串引起。 该字符串将替换以前添加的任何现有字符串。

注意：在德语中，只记录 128 个字符。

comment-

从组记录中删除注释字符串（如果有）。该参数仅与 chgrp 或 editgrp 命令一起使用。

expire(*date*)

设置组成员帐号的过期日期。 如果未指定日期，当用户当前未登录时，用户帐号会立即过期。 如果用户已登录，则帐号在用户注销时过期。 该参数仅适用于配置文件组。

用下面的格式指定到期日期和可选时间：
mm/dd/yy [yy][@HH:MM]。 年份可以是 2 位数或 4 位数。

注意：不能通过用恢复日期指定 resume 参数来启用过期的用户记录。 请使用 expire- 参数来启用过期的用户记录。

expire-

对于 newgrp 命令，它定义不具有到期日期的用户帐户。对于 chgrp 和 editgrp 命令，它从用户帐号删除过期日期。 该参数仅适用于配置文件组。

gowner(*groupName*)

将 CA Access Control 用户或组指定为组记录的所有者。指定多个组名时，请用括号括起名称，并用空格或逗号分隔组名。 如果将组添加到数据库并忽略该参数，您便是组记录的所有者。

grace(*numberOfGraceLogins*)

设置在挂起用户之前允许的最大登录次数。宽限登录次数必须介于 0 和 255 之间。 达到宽限登录次数后，将拒绝用户访问系统，并且用户必须与系统管理员联系以选择新密码。 如果将宽限设置为零，用户便不能登录。 该参数仅适用于配置文件组。

grace-

删除组的宽限登录设置。该参数仅与 chgrp 或 editgrp 命令一起使用。该参数仅适用于配置文件组。

groupName

指定要为其创建或要更改属性的组名。 对于命令 new[x]grp，每个组名必须是唯一的，并且当前在数据库中不存在。 不过，组和用户可以共享同一名称。

history

指定已存储密码的数目。 可以使用 history- 删除历史记录文件。

homedir(*fullPath*|nohomedir)

指定用户主目录的完整路径。 如果指定的路径以斜线结尾，则 *groupName* 将连接到指定的路径。如果指定 nohomedir，则不会自动设置主目录。

inactive(*numInactiveDays*)

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。 当达到该天数时，用户便无法登录。 该参数仅适用于配置文件组。

为 *numInactiveDays* 输入正整数或零。 如果将 inactive 设置为零，效果与使用 inactive- 参数相同。

注意：在用户记录中，不标记非活动用户。 要识别非活动用户，必须将“上次访问时间”值与“空闲日”值进行比较。

非活动-

将用户的状态从不活动更改为活动。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

interval(*maximumPasswordChangeInterval*)

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。 输入正整数或零。 时间间隔为零可禁用组的密码时间间隔检查，这样，密码便不会过期。将不使用 setoptions 命令设置的默认值。 仅为安全要求低的用户将时间间隔设置为零。

达到指定的天数时，CA Access Control 将通知用户当前的密码已到期。用户可立即更新密码，或继续使用旧密码，直到达到宽限登录次数。达到宽限登录次数后，将拒绝用户访问系统，用户必须与系统管理员联系以选择新密码。 该参数仅适用于配置文件组。

interval-

取消组的密码时间间隔设置。 如果取消，将使用用户记录中的任何值。 否则，将使用 setoptions 命令设置的默认值。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

maxlogins(*maximumNumberOfLogins*)

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。 如果未指定该参数，将使用用户记录中的任意值。 否则，将使用全局最大登录设置。 该参数仅适用于配置文件组。

注意：如果将 maxlogins 设置为 1，则无法运行 selang。 必须关闭 CA Access Control，将 maxlogins 设置更改为大于 1 的值，然后再次启动 CA Access Control。

maxlogins-

删除组的最大登录设置。 如果未指定该参数，将使用用户记录中的任意值。 否则，将使用全局最大登录设置。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

mem(*GroupName*) | mem+(*GroupName*)

将成员组（或子组）添加到 CA Access Control 中的组。 必须已在 CA Access Control 中定义了成员组 *(GroupName)*。 如果要添加多个成员组，请用逗号分隔组名。 如果组名包含空格，请用引号将它引起。

注意：要将用户添加到内部组，请使用 join[x] 命令。

此选项仅适用于内部组。

mem-(*GroupName*)

从该组删除成员组。 必须已在 CA Access Control 中定义了成员组 *(GroupName)*。 如果要删除多个成员组，请用逗号分隔组名。 如果组名包含空格，请用引号将它引起。

注意：要将用户从内部组删除，请使用 join[x]- 命令。

此选项仅适用于内部组。

min_life(*minimumPasswordChangeInterval*)

在允许用户再次更改密码之前必须经过的最少天数。 该参数仅适用于配置文件组。

min_life-

删除组的 min_life 设置。如果未指定该参数，且在用户记录中设置了 min_life 参数，则将使用该用户记录中的值。 否则，将使用全局 min_life 设置。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

name(*fullname*)

指定组的全名。输入最多为 47 个字符的字母数字字符串。如果字符串中包含任何空格，请用单引号将整个字符串引起。

nt(*nt-group-attributes*)

（仅适用于 Windows）向本地 Windows 系统中添加组定义，或更改其中的组定义。

comment('*comment*')

将注释字符串添加到本地记录中。如果以前向记录添加了注释字符串，则此处指定的新字符串将替换现有字符串。

comment 是字母数字字符串，最多为 255 个字符。如果字符串中包含任何空格，请用单引号将整个字符串引起。

operator

为组分配 OPERATOR 属性。 所在组具有 OPERATOR 属性的用户可以列出数据库中的所有资源记录，并对 CA Access Control 定义的所有文件拥有读取权限。

所在组具有该属性的成员还可以使用 secons 命令的所有选项。 有关 secons 实用程序的详细信息，请参阅 *《参考指南》*。

operator-

从组记录中删除 OPERATOR 属性。

不能将此参数与 new[x]grp 命令一起使用。

owner(*Name*)

将 CA Access Control 用户或组指定为组记录的所有者。如果将组添加到数据库并且省略该参数，则您便是所有者。 有关详细信息，请参阅适用于您的操作系统的 *《端点管理指南》*。

parent(*groupName*)

将现有 CA Access Control 组指定为组记录的父组。有关父子关系的详细信息，请参阅适用于您的操作系统的 *《端点管理指南》*。

父项-

删除组与其父组之间的链接。 该参数仅与 chgrp 或 editgrp 命令一起使用。

password

将密码分配到该组。

password-

取消该组的密码需要。

pmdb(*PolicyModelName*)

指定当组中的用户通过实用工具 sepass 更改密码时将新密码传播给指定的策略模型。 输入 PMDB 的完全限定名称。

密码将发送到在 seos.ini 的 [seos] 部分的 parent_pmd 或 passwd_pmd 标记中定义的策略模型。 该参数仅适用于配置文件组。

pmdb-

从组记录中删除 PMDB 属性。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

pwmanager

为组分配 PWMANAGER 属性。 所在组具有该属性的成员可以更改数据库中的用户的密码。 有关详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

pwmanager-

从组记录中删除 PWMANAGER 属性。

不能将此参数与 new[x]grp 命令一起使用。

restrictions(days(*dayData*) time(*timeData*))

指定组成员可以在一周的哪几天以及一天的哪几个小时登录系统。

如果在用户登录时，登录时间到期，CA Access Control 不会强制用户退出系统。 另外，登录限制不适用于批处理作业；用户可在任何时候运行后台进程。 该参数仅适用于配置文件组。

如果省略 days 参数而指定 time 参数，则时间限制将应用于记录中已经指出的任何“工作日”限制。 如果省略 time 而指定 days，则日期限制将应用于记录中已经指出的任何时间限制。 如果同时指定 days 和 time，则只允许组成员在指定日期的指定时间段访问系统。

days(*dayData*)

指定用户可以登录系统的日期。 days 参数可使用下列子参数：

- **anyday** - 允许用户在任何一天登录。
- **weekdays** - 仅允许用户在工作日（星期一至星期五）登录。
- **mon tue wed thu fri sat sun** - 只允许用户在指定日期登录。 您可以按任何顺序指定日期。 如果指定多个日期，请使用空格或逗号分隔各日期。

time(***timeData***)

指定用户可以登录系统的时间段。 time 参数可使用下列子参数：

- **anytime -** 允许用户在一天中的任何时间登录。
- *startTime*:*endTime* - 只允许用户在指定时间段登录。 *startTime* 和 *endTime* 的格式均为 *hhmm*，其中 *hh* 是采用 24 小时表示法的小时（00 至 23），而 *mm* 是分钟（00 至 59）。 请注意，2400 是无效的时间值。 如果 *endTime* 是小于 *startTime* 的数字，则认为该时间段已延长至午夜以后。 否则，便认为该时间段在同一日。

  注意：CA Access Control 使用处理器所在位置的时区。 如果用户在处于与处理器不同时区的终端上登录，您必须将此因素考虑在内。

限制-

从组记录中删除任何限制用户登录系统的能力的限制。 如果未指定该参数，并在用户记录中设置了 restrictions 参数，将使用用户记录中的值。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

resume(*date*)

启用通过指定挂起参数禁用的用户记录 用以下格式输入日期和（可选）时间：*mm /dd/yy[@HH:MM]*。

如果同时指定 suspend 参数和 resume 参数，恢复日期必须在挂起日期之后。如果忽略 *date*，则在执行 chgrp 命令时将立即启用用户。有关详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。 该参数仅适用于配置文件组。

resume-

从组记录中清除恢复日期和时间（如果已使用）。 因此，用户的状态将从活动（启用）更改为挂起。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

规则

为密码指定规则：

alpha(*minimumAlphaCharacters*)

最少字母字符数。

alphanum(*minimumAlphanumericCharacters*)

最少字符数。

bidirectional|bidirectional-

指定是否使用双向密码加密。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，会激活单向密码历史记录加密，并且无法解密旧密码。

注意：必须将历史记录设置为比 1 大的值，才能使用该功能。

注意：在 UNIX 上，还必须将配置设置 passwd_format 设置为 NT，才能使用该功能。

重要说明！ 如果您将 seos.ini 文件标记“passwd_format”（[passwd] 部分）设置为“NT”，则当您用 selang 创建用户时必须使用“native”选项（而不是“unix”）。 例如：

```
nu uSr_1026 native password(uSr_1026)
```

另外，请确保您在本地环境（而不是 unix 环境）中工作，如下：

```
env native
chusr usr_1 password(mypassword)
```

min_len(*minimumPasswordLength*)

最小密码长度。

max_len(*maximumPasswordLength*)

最大密码长度。

lowercase(*minimumLowercaseCharacters*)

最少小写字母字符数。

max_rep(*maximumRepetitiveCharacters*)

最多重复字符数。

namechk|namechk-

根据名称检查密码。

numeric(*minimumNumericCharacters*)

最少数字字符数。

oldpwchk|oldpwchk-

根据旧密码检查密码。

注意：仅在 Unix 和 Linux 操作系统上有效。

special(*minimumSpecialCharacters*)

最少特殊字符数

uppercase(*minimumUppercaseCharacters*)

最少大写字母字符数。

use_dbdict|use_dbdict-

设置密码词典。 use_dbdict 将标记设置为 **db**，并将密码与 CA Access Control 数据库中的单词进行比较。 **use_dbdict-** 将内标识设置为 file 并根据在 UNIX 的 seos.ini 文件或 Windows 的 Windows 注册表中指定的文件检查密码。

server

将 SERVER 属性设置为“on”。 如果当前用户的所在组具有 SERVER 属性，则允许代表当前用户运行的进程询问其他用户的授权。 有关详细信息，请参阅适用于您的操作系统的 *《端点管理指南》*。

server-

将 SERVER 属性设置为“off”。

不能将此参数与 new[x]grp 命令一起使用。

shellprog(fullPath)

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。 *FullPath* 是字符型字符串。

supgroup(*Group*'sSuperiorGroup)

指定超级组（或父组）。

suspend(*date*)

禁用用户记录，但将其保留在数据库中进行定义。 用以下格式输入日期和（可选）时间：*mm /dd/yy[@HH:MM]*。

用户不能使用挂起的用户帐号登录系统。 如果指定 *date*，将在指定的日期挂起用户记录。如果省略 *date*，则在执行 chgrp 命令时立即挂起用户记录。 该参数仅适用于配置文件组。

suspend-

从用户记录中清除挂起日期，并将用户的状态从禁用更改为活动（启用）。 该参数仅与 chgrp 或 editgrp 命令一起使用。 该参数仅适用于配置文件组。

unix(*groupidNumber*)

（仅适用于 UNIX）在 UNIX 上设置组属性或创建组（如果尚不存在）。

groupidNumber 是一个十进制数字。 不能将组 ID 指定为零。 如果忽略该数字，CA Access Control 将查找最大的当前组 ID，并将该组的 ID 设置为该数字。CA Access Control 在一次添加或修改多个组时以相同方式创建组 ID 编号。 seos.ini 文件中的内标识 AllowedGidRange 可定义某些不可用的数字。

userlist*(userName)*

为组分配成员。 *UserName* 是一个或多个 UNIX 用户的用户名。 指定多个用户时，请用逗号或空格分隔用户名。 对于 chgrp 和 editgrp 命令，在此处指定的成员列表将替换当前为组定义的任何成员列表。

示例

- 用户 Bob 希望将企业组 Sales 的父组和所有组从 ACCOUNTS 更改为 PAYROLL。

  ```
  chxgrp Sales parent(PAYROLL) owner(PAYROLL)
  ```

- 用户 Admin1 希望将组 projectB 的父组从 divisionA 更改为 divisionB，并将组 RESEARCH 指定为新所有者。

  Admin1 具有 ADMIN 属性。

  ```
  chxgrp projectB parent(divisionB) owner(RESEARCH)
  ```

- 管理用户 Sally 希望删除主目录和组配置文件 NewEmployee 的 shell 程序说明。

  Sally 是 NewEmployee 的所有者。

  ```
  editgrp NewEmployee homedir() shellprog()
  ```

- 用户 Admin1 希望将组 ProjectA 添加为组 RESEARCH 的子组。 用户 Admin1 将成为 ProjectA 组的所有者。

  Admin1 具有 ADMIN 属性。

  默认值为 owner(Admin1)。

  ```
  newgrp ProjectA parent(RESEARCH)
  ```

更多信息：

join[x] 命令 — 将用户添加至内部组 (p. 115)
join[x]- 命令 — 从组中删除用户 (p. 118)
rm[x]grp 命令 — 删除组记录 (p. 123)
show[x]grp 命令 — 显示组属性 (p. 138)
chgrp 命令 — 修改 UNIX 组 (p. 157)
chgrp 命令 — 修改 Windows 组 (p. 173)

chres 命令 - 修改资源记录

在 AC 环境中有效

使用 chres、editres 和 newres 命令，可以处理属于 CA Access Control 类的资源记录。 这些命令结构相同，仅在以下方面有所不同：

- chres 命令可*修改*一个或多个资源。
- editres 命令可*创建或修改*一个或多个资源。
- newres 命令可*创建*一个或多个资源。

注意：此命令同样存在于本地 Windows 环境中，但操作方式有所不同。

要使用 newres 命令添加资源，至少必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 您在 ADMIN 类中的资源类记录的 ACL 中具有创建权限。
- 如果 seos.ini 文件中的标记 use_unix_file_owner 设置为 yes，则 UNIX 中文件的所有者可以将其定义为 CA Access Control 的新资源。

要使用 chres 或 editres 命令添加或更改资源，必须对该资源具有足够的权限。 CA Access Control 将按照以下顺序检查是否满足下列任意一个条件：

1. 您具有 ADMIN 属性。
2. 资源记录在某一组的范围内，您在该组中具有 GROUP-ADMIN 属性。
3. 您是记录的所有者。
4. 在 ADMIN 类中的资源类记录的 Access Control 列表中为您分配了修改（对于 chres）或创建（对于 editres）权限。

注意：资源名的最大长度为 255 个单字节字符。

下表列出了适用于可以使用 chres、editres 和 newres 命令管理的每个类的命令参数。

类	属性											
	审核	**日历**	**category**	**comment**	**defaccess**	**label**	**level**	**notify**	**owner**	**restrictions[-]**	**warning**	**其他**
ACVAR				x					x			VARIABLE_TYPE、VARIABLE_VALUE
ADMIN	x	x	x	x	x	x	x	x	x	x	x	
CALENDAR				x					x			
CATEGORY				x					x			
CONNECT	x	x	x	x	x	x	x	x	x	x	x	
CONTAINER	x	x		x					x		x	MEM
DOMAIN	x	x	x	x	x	x	x	x	x	x	x	MEM
FILE	x	x	x	x	x	x	x	x	x	x	x	
GFILE	x	x		x				x	x		x	MEM
GHOST	x	x		x					x	x	x	MEM
GSUDO		x		x	x				x			MEM

类	属性											
	审核	日历	category	comment	deaccess	label	level	notify	owner	restrictions[-]	warning	其他
GTERMINAL	x	x		x	x				x	x		MEM
HNODE	x	x	x	x	x	x	x	x	x	x	x	SUBSCRIBER、POLICY
HOLIDAY	x		x	x	x	x	x	x	x	x	x	DATES
HOST	x	x		x					x	x	x	
HOSTNET	x	x		x					x		x	MASK、MATCH
HOSTNP	x	x		x					x	x	x	
LOGINAPPL	x	x		x	x			x	x	x	x	LOGINFLAGS、LOGINMETHOD、LOGINPATH、LOGINSEQUENCE
MFTERMINAL	x	x	x	x		x	x	x	x		x	DAYTIME
POLICY	x	x	x	x	x	x	x	x	x	x	x	SIGNATURE、RULESET
PROCESS	x	x	x	x	x	x	x	x	x	x	x	
PROGRAM	x	x	x	x	x	x	x	x	x	x	x	TRUST
PWPOLICY				x					x			
REGKEY	x	x		x	x			x	x		x	DAYTIME
REGVAL	x	x		x	x			x	x		x	DAYTIME

类	属性											
	审核	日历	category	comment	defaccess	label	level	notify	owner	restrictions[-]	warning	其他
RULESET	x	x	x	x	x	x	x	x	x	x	x	SIGNATURE、CMD、UNDOCMD
SECFILE				x					x			TRUST、FLAGS
SECLABEL			x	x			x		x			
SEOS		x	x	x		x	x					HOST
SPECIALPGM				x					x			
SUDO	x	x	x	x	x	x	x	x	x	x	x	TARGUID、PASSWORD
SURROGATE	x	x	x	x	x	x	x	x	x	x	x	
TCP	x		x	x	x	x	x	x	x	x	x	
TERMINAL	x	x	x	x	x	x	x	x	x	x	x	
UACC	x		x	x	x				x			
USER-ATTR									x		x	
USER-DIR	x			x					x			

```
{{chres|cr}|{editres|er}|{newres|nr}} className resourceName \
    [ac_id(id)] \
    [audit({none|all|success|failure})] \
    [calendar[-](calendarName)] \
    [category[-](categoryName)] \
    [cmd+(selang_command_string)|cmd-] \
    [comment(string)|comment-] \
    [container[-](containerName)] \
    [dates(time-period)] \
    [dh_dr{-|+}(dh_dr)] \
    [disable|disable-] \
    [defaccess(accessAuthority)] \
    [filepath(filePaths)] \
    [flags[-|+](flagName)] \
    [gacc(access-value)] \
    [gowner(groupName)] \
    [host(host-name)|host-] \
    [label(labelName)|label-] \
    [level(number)|level-] \
    [mask(inetAddress)|match(inetAddress)] \
    [mem(resourceName)|mem-(resourceName)] \
    [node_alias{-|+}(alias)] \
    [node_ip{-|+}(ip)] \
    [notify(mailAddress)|notify-] \
    [of_class(className)]  \
    [owner({userName | groupName})] \
    [{password | password-}] \
    [policy(name(policy-name) {{deviation+|dev+}|{deviation-|dev-}})] \
    [policy(name(policy-name) status(policy-status)
    {updator|updated_by}(user-name))] \
    [{restrictions([days({anyday|weekdays|{[mon] [tue] [wed] \
        [thu] [fri] [sat] [sun]}})] \
        [time({anytime|startTime:endTime}) \
    |restrictions-}] \
    [targuid(userName)] \
    [trust | trust-] \
    [value{+|-}(value)] \
    [warning | warning-]
```

ac_id(*id*)

为端点（HNODE 对象）定义唯一 ID，该 ID 将保存在本地 CA Access Control 数据库和 DMS 上。 CA Access Control 使用该 ID 标识 HNODE，从而使对端点 IP 地址或名称的更改不会影响高级策略管理功能；CA Access Control 仍可以跟踪端点。

审核

表明记录哪些访问事件。 指定以下属性之一：

- **all** - CA Access Control 既记录授权的访问尝试，也记录未经授权的访问尝试。
- **failure** - CA Access Control 记录未经授权的访问尝试。 这是默认值。
- **none** - CA Access Control 不向日志文件写入任何记录。
- **success** - CA Access Control 记录授权的访问尝试。

calendar(*calendarName*)

定义代表 Unicenter TNG 中时间限制的 Unicenter NSM 日历记录。 CA Access Control 维护这些对象的列表只是为了进行管理，但不对它们进行保护。 指定多个日历时，请用空格或逗号分隔日历名称。

calendar-(*calendarName*)

从资源记录中删除一个或多个 Unicenter TNG 日历记录。 该参数仅与 chres 或 editres 命令一起使用。

category(*categoryName* [,*categoryName...*])

为资源记录分配一个或多个安全类别。

如果在 CATEGORY 类不活动时指定 category 参数，CA Access Control 将更新数据库中的资源定义；但是，在再次激活 CATEGORY 类之前，更新的类别分配不会生效。

category-(*categoryName* [,*categoryName...*])

从资源记录删除一个或多个安全类别。

将从资源记录中删除指定的安全类别，无论 CATEGORY 类是否是活动的。 该参数仅与 chres 或 editres 命令一起使用。

className

指定资源所属的类的名称。 要列出为 CA Access Control 定义的资源类，请使用 find 命令。

cmd+(*selang_command_string*)

指定定义策略的 selang 命令列表。 这些是用于部署策略的命令。 例如：

```
editres RULESET IIS5#02 cmd+("nr FILE /inetpub/* defaccess(none)
owner(nobody)")
```

cmd-

从 RULESET 对象删除策略部署命令列表。

comment(*string*)

将最多为 255 个字符的字母数字字符串添加到资源记录中。 如果字符串中包含任何空格，请用单引号将整个字符串引起。 字符串将替换先前定义的任何现有字符串。

注意：对于 SUDO 类，该字符串具有特殊的含义。 有关定义 SUDO 记录的详细信息，请参阅*《端点管理指南：用于 UNIX》*。

comment-

从资源记录中删除注释。 该参数仅与 chres 或 editres 命令一起使用。

container(*containerName*)

代表 CONTAINER 对象，即一种一般的分组类。

containerName 是在 CONTAINER 类中定义的一个或多个 CONTAINER 记录的名称。指定多个 CONTAINER 时，请使用空格或逗号分隔名称。

container-(*containerName*)

从资源记录中删除一个或多个 CONTAINER 记录。 该参数仅与 chres 或 editres 命令一起使用。

dates(*time-period*)

定义用户不能登录的一个或多个时间段，如假日。 如果指定多个时间段，请用空格分隔时间段。 使用以下格式：

```
mm/dd[/yy[yy]][@hh:mm][-mm/dd]/[/yy[yy]][@hh:mm]
```

如果未指定年份（或指定 1990 年之前的年份），则表示时间段或假日是一年一次的。 可以指定二位数或四位数的年份，例如：98 或 1998。

如果未指定开始时间，则使用一天的开始时间（午夜）；如果未指定结束时间，则使用一天的结束时间（午夜）。 小时和分钟的格式为 *hh:mm*，其中 *hh* 是采用 24 小时表示法的小时（00 至 23），而 *mm* 是分钟（00 至 59）。

如果未指定时间间隔（例如，12/25@14:00-12/25@17:00），而仅指定了日和月 (12/25)，则假日将持续一整天。

如果执行命令时所在的时区与假日发生地的时区不同，请将时间段转换为您的本地时间。 例如，如果您在纽约，而洛杉矶有半天的假日，则您必须输入 09/14/98@18:00-09/14/98@20:00。这可以防止用户在洛杉矶的下午 3:00 至下午 5:00 进行登录。

defaccess([*accessAuthority*])

定义资源的默认访问权限。 默认访问权限是授予请求访问资源但不在资源的访问控制列表中的任何访问者的权限。 默认访问权限也适用于未在数据库中定义的用户。 有效访问权限值因类而异。

如果忽略 *accessAuthority*，CA Access Control 将分配隐性访问权限，该访问权限是在 UACC 类中代表资源类的记录的 UACC 属性中指定的。

dh_dr{+|-}(*dh_dr*)

定义该端点用于灾难恢复的分布式主机。

filepath(*filePaths*)

定义一个或多个绝对文件路径，其中每个都构成一个有效内核模块。多个文件路径用冒号 (:) 分隔。

flags(*flagName*)

定义如何受托资源以及如何检查它的受托状态。可用标志有：Ctime、Mtime、Mode、Size、Device、Inode、Crc 和 Own/All/None。

gacc(*access-value*)

让程序采用比其他方式快得多的速度访问受保护的、频繁打开的文件。

gowner(*groupName*)

将 CA Access Control 组指定为资源记录的所有者。如果记录资源的组所有者的安全级别、安全标签和安全类别权限使其足以能够访问资源，则该组所有者对该资源拥有不受限制的访问权限。 资源的组所有者始终可以更新和删除资源记录。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

label(*labelName*)

为资源记录分配安全级别。

label-

从资源记录中删除安全标签。 该参数仅与 chres 或 editres 命令一起使用。

level(*number*)

为资源记录指定安全级别。 请输入介于 1 和 255 之间的正整数。

level-

从资源中删除任何安全级别。 该参数仅与 chres 或 editres 命令一起使用。

mask (*IPv4-address*) match (*IPv4-address*)

mask 和 *match* 参数仅适用于 HOSTNET 记录。 创建 HOSTNET 记录时需要它们，并且它们在修改记录时可选。

将 mask 和 match 一起使用可以定义由 HOSTNET 记录定义的主机组。 如果带有 mask 地址的主机 IP 地址的 AND 生成了 match 地址，则主机是 HOSTNET 记录组的成员。

例如，指定 mask(255.255.255.0) 和 match(192.16.133.0) 意味着主机是组的成员，如果该组的 IP 地址范围在 192.16.133.0 到 192.16.133.255 之间。

mask 和 match 参数需要 IPv4 地址。

mem(*resourceName*)

将成员资源添加到资源组。 如果要添加多个成员资源，请用逗号分隔每个名称。

可以将 mem 参数仅与以下类的资源记录一起使用：

- CONTAINER。 该类定义其他资源类的一组对象。
- GFILE。 该类包含定义文件组的资源记录。
- GHOST。 该类包含定义主机组的资源记录。
- GSUDO。 该类包含定义命令组的资源记录。
- GTERMINAL。 该类包含定义终端组的资源记录。
- GPOLICY。 该类包含定义逻辑策略的资源记录。
- GHNODE。 该类包含定义主机组的资源记录。
- GDEPLOYMENT。 该类包含定义策略部署的资源记录。

使用 mem 参数将相应类型的记录添加到资源组，例如，将 FILE 记录添加到类 GFILE 资源组。

注意：如果将 mem 参数用于 CONTAINER 资源，还必须包括 of_class 参数。

必须已在 CA Access Control 中定义成员资源和资源组。 要创建资源组，请创建所需的类资源。 例如，以下命令可创建 GFILE 资源组：

```
newres GFILE myfiles
```

mem-(*resourceName*)

从资源组中删除成员资源。 如果要删除多个成员资源，请使用空格或逗号分隔资源名称。 该参数仅与 chres 或 editres 命令一起使用。

node_alias{-|+}(*alias*)

定义端点别名。

通过为端点别名定义别名，CA Access Control 可以将高级策略管理命令发送到基于别名的实际端点。

node_ip[-|+](*ip*)

定义主机的 IP 地址。 高级策略管理可使用 IP 地址以及端点名称找到所需端点。

notify(*mailAddress*)

只要该资源记录代表的资源被访问，便指示 CA Access Control 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）。

只有在日志路由系统活动时，才进行通知。 通知消息将发送到屏幕上或用户的邮箱，具体取决于日志路由系统的设置。

每次发送通知消息时，都会在审核日志中写入审核记录。 有关筛选和查看审核记录的信息，请参阅*《端点管理指南：用于 UNIX》*。

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。

范围：30 个字符。

notify-

指定在成功访问资源记录代表的资源时不通知任何人。 该参数仅与 chres 或 editres 命令一起使用。

of_class(*className*)

指定要使用 mem 参数添加到 CONTAINER 类的记录的资源类型。

owner(*Name*)

将 CA Access Control 用户或组指定为资源记录的所有者。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。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

密码

对于 SUDO 类，指定 sesudo 命令需要原始用户密码。

密码-

取消 password 参数，以使 sesudo 命令不再需要原始用户密码。 该参数仅与 chres 或 editres 命令一起使用。 如果以前未使用 password 参数，则没有必要使用该参数。

policy(name(*name#xx*) status(*status*) updated_by(*name*)) |
policy(name(*name#xx*) deviation{+|-})

在传播树中添加节点的订户，并指定其状态。 另外，还可以更新现有策略版本以指定是否存在策略偏差。 更新策略状态时必须更新 updated_by 属性。 它是代表更改策略状态的用户的名称的字符串。

策略状态可以是以下之一：已传输、已部署、已取消部署、已失败、SigFailed、已排队、UndeployFailed 或 TransferFailed。

policy-[(name(*name#xx*))]

从节点删除已命名的策略版本。 如果未指定策略，则将删除部署到该节点的所有策略。

resourceName

定义要修改或添加的资源记录的名称。 当更改或添加多个资源时，请将资源名称的列表括在括号中，并用空格或逗号分隔这些资源名称。 必须至少指定一个资源名称。

CA Access Control 将根据指定的参数分别处理每个资源记录。如果处理资源时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个资源。

注意：如果您在资源名称中使用变量，请使用以下语法来引用变量：<!*variable*>，例如 <!AC_ROOT_PATH>\bin。您只能在策略中使用 selang 规则中的变量。

restrictions([days] [time])

指定用户可以在一周的哪几天以及一天的哪几个小时访问文件。

如果省略 days 参数而指定 time 参数，则时间限制将应用于记录中已经指出的任何“工作日”限制。 如果省略 time 而指定 days，则日期限制将应用于记录中已经指出的任何时间限制。 如果同时指定了 days 和 time，则用户只能在指定日期的指定时间段内访问系统。

- [Days] 指定用户可以访问文件的日期。 days 参数可使用下列子参数：
  - **anyday** - 允许用户在任何日期访问文件。
  - **weekdays** - 仅允许用户在工作日（星期一至星期五）访问资源。
  - **Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**、**Sun** - 仅允许用户在指定的日期访问资源。 您可以按任何顺序指定日期。 如果指定了多个日期，请用空格或逗号分隔这些日期。
- [Time] 指定用户可以访问资源的时间段。 time 参数可使用下列子参数：
  - **anytime** - 允许用户在一天中的任何时间访问资源。
  - **startTime:endTime** - 仅允许用户在指定的时间段内访问资源。 startTime 和 endTime 的格式均为 *hhmm*，其中 *hh* 是采用 24 小时表示法的小时（00 至 23），而 *mm* 是分钟（00 至 59）。 请注意，2400 是无效的时间值。 startTime 必须小于 endTime，并且这两个时间必须在同一天。 如果终端与处理器位于不同的时区，请通过将终端的开始时间和结束时间转换为等同的处理器本地时间来调整时间值。 例如，如果处理器位于纽约而终端位于洛杉矶，那么，要允许从上午 8:00 到下午 5:00 在洛杉矶访问终端，请指定时间 (1100:2000)。

restrictions-([days] [time])

删除限制用户访问文件的能力的任何限制。

ruleset+(*name*)

指定与策略相关联的规则集。

ruleset-(*name*)

从策略中删除规则集。 如果未指定规则集，则将从策略中删除所有规则集。

signature(*hash_value*)

指定散列值。 对于策略，这基于与策略相关联的 RULESET 对象的签名。 对于规则集，这基于策略部署命令列表和策略取消部署（删除）命令列表。

subscriber(name(*sub_name*) status(*status*))

在传播树中添加节点的订户，并指定其状态。 状态可以是以下之一：**未知**、**可用**、**不可用**或**同步**。

subscriber-(name(*sub_name*)) | sub-

从节点中删除订户数据库。 如果未指定订户，则所有订户都将被删除。

targuid(*userName*)

对于 SUDO 类，指定用户的名称，将借用该用户的权限来执行命令。 默认值为 root。

trust

指定资源为受托资源。 trust 参数仅适用于 PROGRAM 和 SECFILE 类的资源。 只要程序保持受托，用户就可执行该程序。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。 该参数仅与 chres 或 editres 命令一起使用。

trust-

指定资源为取消受托资源。trust- 参数仅适用于 PROGRAM 和 SECFILE 类的资源。用户不能执行取消受托程序。有关详细信息，请参阅《端点管理指南：用于 UNIX》。 该参数仅与 chres 或 editres 命令一起使用。

undocmd+(*selang_command_string*)

指定定义策略取消部署的 selang 命令列表。 这些是用于删除已部署策略（取消部署）的命令。 例如：

```
editres RULESET IIS5#02 undocmd+("rr FILE /inetpub/*")
```

undocmd-

从 RULESET 对象删除策略删除命令列表。

value+(*value*)

将指定值添加到指定的变量（ACVAR 对象）中。

value-(*value*)

从指定的变量（ACVAR 对象）中删除指定值。

warning

指定即使访问者的权限不足以访问资源，CA Access Control 也允许该访问者访问资源。 但是，CA Access Control 将在审核日志中写入警告消息。

注意：在警告模式中，CA Access Control 不为资源组创建警告消息。

warning-

指定如果访问者的权限不足以访问资源，<eAC 将拒绝该用户访问资源，并且不写入警告消息。 该参数仅与 chres 或 editres 命令一起使用。

示例

- 用户 *admin1* 希望更改终端 tty30 的所有者和默认访问，并限制在工作日工作时间（上午 8:00 至下午 6:00）使用终端。
  - 用户 admin1 具有 ADMIN 属性。

```
chres TERMINAL tty30 owner(admin1) defaccess(read)  restrictions \
(days(weekdays)time(0800:1800))
```

- 管理员用户 Sally 希望删除存储于文件 account.txt 的 FILE 类记录中的 group 和 owner 属性。
  - 用户 Sally 是 Jared 的用户记录的所有者。

```
chres FILE /account.txt group() owner()
```

要删除任何记录属性（如果属性是由字符串定义的），请键入带“-”符号或空圆括号“()”的该属性。

- 用户 Bob 希望删除终端 tty190 的备注字段，而且每当授予对终端的访问权限时都得到通知。
  - 用户 Bob 是 CA Access Control 用户，而且是终端 tty190 的所有者。

```
chres TERMINAL tty190 comment- notify(Bob@athena)
```

- 用户 Admin1 希望将 OPERATOR 类别添加到资源 USER.root（它在 SURROGATE 类中）的安全类别列表中。
  - 用户 Admin1 具有 ADMIN 属性。
  - OPERATOR 类别已在数据库中定义。

```
chres SURROGATE USER.root category(OPERATOR)
```

- 用户 admin1 希望将 /bin/su 定义为具有 EXECUTE 的全局访问的受信任程序。
  - 用户 admin1 具有 ADMIN 属性。
  - 将应用以下默认项：
    - restrictions(days(anyday) time(anytime))
    - owner(admin1)
    - audit(failure)

```
newres PROGRAM /bin/su defaccess(x) trust
```

- 用户 admin1 希望将用组 ID 替代“system”组定义为受保护的资源，所有用户（包括 admin1）都不能访问它。
  - 用户 admin1 具有 ADMIN 属性。 向 CA Access Control 定义了用户 nobody。
  - 将应用以下默认项：
    - restrictions(days(anyday) time(anytime))
    - audit(failure)

```
newres SURROGATE GROUP.system defaccess(n) owner(nobody)
```

- 用户 SecAdmin 希望定义 ProjATerms，一个包含终端 T1、T8 和 T11 的终端组。 终端组只能由组 PROJECTA 在工作日的常规营业时间（上午 8：00 到下午 6:00）使用。
  - 用户 SecAdmin 具有 ADMIN 属性。
  - 向 CA Access Control 定义了终端 T1、T8 和 T11。
  - 向 CA Access Control 定义了组 PROJECTA。
  - audit(failure)

```
newres GTERMINAL ProjATerms mem(T1,T8,T11) owner(PROJECTA) \
restrictions(days(weekdays) time(0800:1800)) defaccess(n)
```

更多信息：

rmres 命令 — 删除资源 (p. 124)
showres 命令 — 显示资源属性 (p. 139)
authorize 命令 - 设置对资源的访问权限 (p. 43)
chres 命令 — 修改 Windows 资源 (p. 175)
find 命令 - 列出数据库记录 (p. 108)
CONTAINER 类 (p. 233)
访问权限（按类） (p. 28)

ch[x]usr 命令 - 更改用户属性

在 AC 环境中有效

使用命令 chusr、chxusr、editusr、editxusr、newusr 和 newxusr 可更改用户属性，并可在 CA Access Control 数据库中定义用户记录（如有必要）。

这些命令均具有同义词，具体如下：

- chusr—cu
- chxusr—cxu
- editusr—eu
- editxusr—exu
- newusr—nu
- newxusr—nxu

这意味着，例如，命令 cu 与命令 chusr 相同。

所有这些命令的结构相同，只是范围有所不同。 按如下所述使用这些命令：

- 将 chusr、editusr 和 newusr 命令用于内部用户。 这些命令之间的差异如下：
  - chusr 命令可*修改*一个或多个 USER 记录。
  - editusr 命令可*创建或修改*一个或多个 USER 记录。
  - newusr 命令可*创建*一个或多个 USER 记录。

  注意：这些命令同样存在于本地环境中，但操作方式有所不同。
- 将 chxusr、editxusr 和 newxusr 命令用于企业用户。 这些命令之间的差异如下：
  - chxusr 命令可*修改*一个或多个 XUSER 记录。
  - editxusr 命令可*创建或修改*一个或多个 XUSER 记录。
  - newxusr 命令可*创建*一个或多个 XUSER 记录。

USER 和 XUSER 类记录的所有属性都相同，除了在企业用户存储中定义的属性，XUSER 记录不会重新定义它们。

执行这些命令时，您所做的更改将立即修改用户记录，即使用户当前已登录系统。

所需授权

要创建 CA Access Control 用户，至少必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 在 ADMIN 类中的 USER 或 XUSER 记录的 Access Control 列表中为您分配了创建权限。

要添加或修改用户，至少必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 如果用户记录在一个组的范围内，并且您在该组中具有 GROUP-ADMIN 属性，则您拥有与该记录的所有者相同的权限。
- 如果用户记录在一个组的范围内，并且您在该组中具有 GROUP-AUDITOR 属性，则您可以指定 audit 参数。
- 您是组的所有者。
- 在 ADMIN 类中的 USER 或 XUSER 记录的 Access Control 列表中为您分配了 MODIFY（对于 ch[x]usr）或 CREATE（对于 edit[x]usr）权限。

```
{{chusr|cu}|chxusr|cxu}|{editusr|eu}|{editxusr|eu}|{newusr|nu}| {newxusr|nxu}}
\
    {userName|(userName [,userName...])} \
    [{admin | admin-}] \
    [audit({none | all |
    {[success][failure][loginsuccess]|[loginfail]|[trace]|[interactive]}})] \
    [{auditor | auditor-}] \
    [{category(categoryName) | category-(categoryName)}] \
    [{comment(string) | comment-}] \
    [country(string)] \
    [email(emailAddress)] \
    [enable] \
    epwasown(password) \
    [{expire[(date)] | expire-}] \
    [fullname (fullName)]
    [{gowner(groupName)] \
    [{grace(nLogins) | grace-}] \
    [{ign_hol | ign_hol-}] \
    [{inactive(nDays) | inactive-}] \
    [{interval(nDays) | interval-}] \
    [{label(labelName) | label-}] \
    [{level(number) | level-}] \
    [location(string)] \
    [{logical|logical-}] \
    [{maxlogins(nLogins) | maxlogins-}] \
    [{min_life(nDays) | min_life-}] \
    [{notify(mailAddress) | notify-}] \
    [{operator | operator-}] \
    [organization(string)] \
    [org_unit(string) \
    [owner({userName | groupName})] \
    [password(string)] \
    [phone(string)] \
    [{pmdb(pmdbName) | pmdb-}] \
    [{profile(groupName) | profile-}] \
    [pwasown(string)] \
    [{pwmanager | pwmanager-}] \
    [regular] \
    [{restrictions( \
        [days({anyday|weekdays|[mon] [tue] [wed] [thu] [fri] [sat] [sun]})] \
        [time({anytime|startTime:endTime})]
        ) |restrictions-}] \
    [{resume[(date)] | resume-}] \
    [{server | server-}] \
    [{suspend[(date)] | suspend-}] \
```

```
[nt|nt( ] \
    [admin|admin-] \
    [comment('comment')|comment- ] \
    [country('country-name')] \
    [expire|expire(mm/dd/yy[@hh:mm])|expire-] \
    [flags({account-flags)|-account-flags})] \
    [homedir(any-string)] \
    [homedrive(home-drive)] \
    [location(any-string)] \
    [logonserver(server-name)] \
    [name(full_name)] \
    [organization(name)] \
    [org_unit(name)] \
    [password(user's temporary password)] \
    [pgroup(primary-group)] \
    [phone(any-string)] \
    [privileges(privilege-list)] \
    [restrictions(days(day-data) time(hhmm:hhmm|anytime) )] \
    [script(logon-script-path)] \
    [workstations(workstations-list)] )] \
[unix({ [gecos(string)] \
    [homedir(path)] \
    [pgroup(groupName)] \
    [shellprog(fileName)] \
    [userid(number)]}]
```

admin

为用户分配 ADMIN 属性。 具有 ADMIN 属性的用户可以发出带有除 audit 以外的所有参数的所有 selang 命令。您必须具有 ADMIN 属性才能使用 admin 参数。

admin-

删除用户的 ADMIN 属性。 （CA Access Control 验证至少一个用户具有 ADMIN 属性。）

不能将此参数与 new[x]usr 命令一起使用。

审核

指定将受 CA Access Control 保护的资源上的哪些用户活动记录到审核日志中。 要指定多个事件类型，请用空格或逗号分隔事件类型名称。 audit 属性如下所示：

- **all —** CA Access Control 记录所有用户活动。 监视的活动有：failure、loginfail、loginsuccess、success、interactive 和 trace。
- **failure —** CA Access Control 记录失败的访问尝试。
- **loginfail —** CA Access Control 记录失败的登录尝试。
- **loginsuccess —** CA Access Control 记录成功的登录。
- **none —** CA Access Control 不记录任何用户活动。
- **success —** CA Access Control 记录成功的访问。
- **interactive—**CA Access Control 记录交互式会话。
- **trace -** CA Access Control 记录由于用户操作而显示在跟踪文件中的每条消息。

auditor

为用户分配 AUDITOR 属性。 具有 AUDITOR 属性的用户可以审核系统资源的使用，并且能够控制是否记录在 CA Access Control 授权检查过程中检测到的对任何受 CA Access Control 保护资源的访问以及对数据库的访问。 有关授予具有 AUDITOR 属性的用户权限的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

auditor-

从用户记录中删除 AUDITOR 属性。

不能将此参数与 new[x]usr 命令一起使用。

auth_type

指定身份验证方法。

只能由 SSO 使用。

不能将该参数用于企业用户。

category(*categoryName*[, *categoryName...*])

为用户分配一个或多个安全类别。

category-(*categoryName*[, *categoryName...*])

从用户记录中删除一个或多个安全类别。

不能将此参数与 new[x]usr 命令一起使用。

comment(*commentString*)

为用户记录分配注释。

commentString

Specifies the comment. *commentString* 是字母数字字符串，最多为 255 个字符。 如果 *commentString* 包含空格，请用单引号将它引起。

comment-

从用户记录中删除注释。

不能将此参数与 new[x]usr 命令一起使用。

country(*countryName*)

指定用户所在的国家/地区。 授权过程中不使用该国家/地区。

countryName

定义国家/地区。 该参数是最多为 19 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

email(*emailAddress*)

定义用户的电子邮件地址。

emailAddress

定义用户的电子邮件地址。

限制：最多为 128 个字符

enable

启用因任何原因而禁用的用户登录。

不能将此参数与 new[x]usr 命令一起使用。

epwasown(*password*)

更改用户密码，就如同用户更改其自己的密码一样。 该密码更改不是管理更改，因此不会自动使该密码到期。

注意：该命令仅供内部使用。 该命令在纯文本中设置密码，指定为 /etc/shadow 或 passwd 文件的参数。

expire(*dateTime*)

设置用户帐户的到期日期。 如果未指定日期或用户已登录，则当用户注销时帐户将立即到期。

如果用户记录具有该属性的值，该值将覆盖 GROUP 记录中的值。

注意：使用 expire- 参数可以启用到期的用户记录；不需要使用 resume 参数执行该操作。

dateTime

定义日期，也可定义时间。 它具有以下格式：
mm/*dd*/[*yy*]*yy*[@*HH:MM*]

可以使用两位数或四位数指定年份。

expire-

对于 new[x]usr 命令，可定义没有到期日期的用户帐户。

对于 ch[x]usr 和 edit[x]usr 命令，可从用户帐户中删除到期日期。

flags(*accountFlags*|*-accountFlags*)

指定用户帐号的特定属性。 有关有效标志值的列表，请参阅附录 “Windows 值”。

要从用户记录中删除标志，请在 *accountFlags* 前面添加减号 (-)。

fullname(*fullName*)

指定用户的全名。

fullName

定义全名。这是一个字母数字字符串，最多为 255 个字符。如果 *fullName* 包含空格，请用单引号将整个字符串引起。

gecos(*string*)

为用户指定注释字符串。 用单引号将字符串引起。

gowner(*groupName*)

将 CA Access Control 组指定为用户记录的所有者。如果组所有者的安全级别和安全类别权限足够，则用户记录的组所有者对其拥有不受限制的访问权限。用户记录的组所有者始终可以更新和删除用户记录。

grace(*nLogins*)

定义用户可以执行的宽限登录次数。

达到宽限登录次数后，用户无法访问系统，用户必须与系统管理员联系以选择新密码。 如果将 grace 设置为零，则用户无法登录。

如果用户记录具有该参数的值，该值将覆盖 GROUP 记录中的值。

如果未指定该参数，并且用户所具有的配置文件组包含该参数的值，则使用 GROUP 记录中的值。 如果 USER 和 GROUP 记录都不包含值，则使用 CA Access Control 全局宽限登录设置。

nLogins

定义宽限登录的次数。 输入 0 到 255 之间的整数。

注意：在宽限值达到 0 之前，该用户应更改密码。 如果已达宽限登录值，则请联系系统管理员选择新的密码。

grace-

删除用户的宽限登录设置。改为使用 CA Access Control 全局宽限登录设置。

不能将此参数与 newusr 命令一起使用。

homedir(*path*)

指定用户主目录的完整路径。 如果*路径*的结尾是斜线，CA Access Control 会将 *userName* 与路径连接。

homedrive(*drive*)

指定用户主目录的驱动器。

ign_hol

为用户分配 IGN_HOL 属性。 具有 IGN_HOL 属性的用户可在假日记录中定义的任何时间段内登录。

ign_hol-

删除用户的 IGN_HOL 属性。

inactive(*nDays*)

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。

注意：用户记录中不标记不活动用户。 要识别非活动用户，必须将“上次访问时间”值与“空闲日”值进行比较。

nDays

定义天数。 *nDays* 为零或正整数。 如果 *nDays* 为零，则效果与使用 inactive- 参数相同。

非活动-

将用户的状态从不活动更改为活动。

不能将此参数与 newusr 命令一起使用。

interval(*nDays*)

定义在设置或更改密码之后而系统提示用户输入新密码之前必须经过的天数。 输入零或正整数。 如果 *nDays* 为零，CA Access Control 将禁用密码间隔检查且密码不会到期。这意味着将不使用 setoptions 命令设置的默认值。 仅为安全要求较低的用户将 *nDays* 设置为零。

达到 *nDays* 后，CA Access Control 将通知用户密码已到期。 用户可继续使用该密码，直到达到宽限登录次数。 达到宽限登录次数后，将拒绝用户访问系统，用户必须与系统管理员联系以获得新密码。

interval-

取消用户的密码时间间隔设置。 如果该用户所具有的配置文件组具有该参数的值，则使用该值。 否则，将使用 setoptions 命令设置的默认值。

不能将此参数与 new[x]usr 命令一起使用。

label(*labelName*)

为用户分配安全标签。

label-

从用户记录中删除安全标签。

不能将此参数与 new[x]usr 命令一起使用。

level(*levelNumber*)

为用户记录分配安全级别。

levelNumber 为 0 到 255 之间的整数。

level-

从用户记录中删除安全级别。

不能将此参数与 newusr 命令一起使用。

localapps

由 CA SSO 使用。

location(*locationString*)

指定用户的位置。 授权过程中不使用该位置。

locationString

定义位置。 *locationString* 是字母数字字符串，最多为 47 个字符。如果 *locationString* 包含空格，请用单引号将它引起。

logical

为用户分配 LOGICAL 属性。 具有 LOGICAL 属性的用户无法登录，且仅可用于内部 CA Access Control 使用。

例如，您可用作资源所有者的用户 nobody 甚至可以防止资源所有者访问资源，该用户在默认情况下是逻辑用户。 这意味着，没有用户可以使用该帐户登录。

logical-

删除用户的 LOGICAL 属性。

logonserver(*server-name*)

指定验证用户的登录信息的服务器。 当用户登录到域工作站时，CA Access Control 会将登录信息传输到服务器，该服务器将为该用户授予工作所需的工作站权限。

maxlogins(*nLogins*)

为用户设置并发登录的最大次数。 0（零）值表示用户可同时从任意数量的终端登录。 如果未指定该参数，将使用全局最大登录设置。

注意：如果将 maxlogins 设置为 1，则无法运行 selang。 必须关闭 CA Access Control，将 maxlogins 设置更改为大于 1（例如通过使用 setpropadm 实用程序），然后再次启动 CA Access Control。

maxlogins-

删除用户的最大登录设置。 改为使用全局设置。

不能将此参数与 new[x]usr 命令一起使用。

min_life(*nDays*)

在允许用户再次更改密码之前必须经过的最少天数。 请输入正整数。

min_life-

删除用户的 min_life 设置。如果该用户所具有的配置文件组具有该参数的值，则使用该值。 否则，将使用 setoptions 命令设置的默认值。

不能将此参数与 new[x]usr 命令一起使用。

nochngpass

指定不允许该用户更改其他用户的密码。

notify(*notifyAddress*)

每次用户登录时，向 *notifyAddress* 发送电子邮件。 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。

CA Access Control 发送通知消息时，都会在审核日志中写入一条审核记录。

notifyAddress

定义用户名或电子邮件地址。

范围：30 个字符。

notify-

指定在用户登录时不通知任何人。

不能将此参数与 new[x]usr 命令一起使用。

nt

对于 chusr 和 editusr 命令，该参数可更改本地 Windows 系统中的用户定义。

对于 newusr 命令，该参数会将用户添加到本地 Windows 系统中。

如果指定了多个参数，请使用空格将这些参数分隔开。

有关如何在 CA Access Control 中的本地 Windows 系统上操作的详细信息，请参阅环境命令。

nt 选项下的 nt 选项和子选项对企业用户无效。

operator

为用户分配 OPERATOR 属性。 具有 OPERATOR 属性的用户可以列出数据库中的所有资源记录，并对 CA Access Control 定义的所有文件拥有读取权限。

具有该属性的用户还可以使用 secons 命令的所有选项。 有关 secons 实用程序的详细信息，请参阅 *《参考指南》*。

operator-

将 OPERATOR 属性从用户记录中删除。

不能将此参数与 newusr 命令一起使用。

organization(*organizationString*)

指定用户组织。 授权过程中不使用该组织。

organizationString

定义组织。 *organizationString* 是字母数字字符串，最多为 255 个字符。 如果 *organizationString* 包含空格，请用单引号将其引起。

org_unit(*org_unitString*)

指定用户的组织部门。 授权过程中不使用该组织部门。

org_unitString

定义组织部门。*org_unitString* 是字母数字字符串，最多为 255 个字符。 如果 *organizationString* 包含空格，请用单引号将其引起。

owner(*Name*)

将 CA Access Control 用户或组指定为用户记录的所有者。有关详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

password(*string*)

为用户分配密码。 指定除空格或逗号之外的任何字符。 如果启用了密码检查，那么该密码只对于一次登录有效。 用户下次登录系统时，必须设置新密码。

要更改自己的密码，您需要使用 *setoptions cng_ownpwd* 或使用 sepass 设置 selang 选项。

pgroup(*groupName*)

设置用户的主组 ID。 *groupName* 是 UNIX 组的名称。

phone(*phoneString*)

定义用户的电话号码。 授权过程中不使用该电话号码。

phoneString

定义电话号码。 *phoneString* 是字母数字字符串，最多为 19 个字符。 如果 *phoneString* 包含空格，请用单引号将它引起。

pmdb(*pmdbName*)

指定在用户使用 sepass 实用程序更改密码时，将新密码传播给指定 PMDB。 输入 PMDB 的完全限定名称。 密码将发送到在 seos.ini 的 [seos] 部分的 parent_pmd 或 passwd_pmd 标记中定义的策略模型。

不能对企业用户使用此选项。

pmdb-

从用户记录中删除 PMDB 属性。

不能将此参数与 new[x]usr 命令一起使用。

privileges(*privilege-list*)

向 Windows 用户记录添加特定权限，或者，如果 privList 前面带有减号 (-)，则可删除指定权限。

不能将此参数与 newusr 命令一起使用。

profile(*groupName*)

将用户指定给配置文件组。 可从配置文件组获得下列值：

- 审核
- auth_type
- expire
- grace
- 非活动
- interval
- maxlogins
- min_life
- password rules
- pmdb
- pwd_autogen
- pwd_policy
- pwd_sync
- restrictions (days，time)
- resume
- suspend
- unix (homedir, shellprog)

配置文件-

从配置文件组中删除用户。

不能将此参数与 new[x]usr 命令一起使用。

pwmanager

为用户分配 PWMANAGER 属性。 具有该属性的用户可以更改数据库中用户的密码。 有关详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

pwmanager-

从用户记录中删除 PWMANAGER 属性。

不能将此参数与 new[x]usr 命令一起使用。

pwasown(*string*)

像用户更改密码一样替换密码。 指定该参数可更新上一次在数据库中进行更改的时间和日期。 宽限登录将终止。

regular

重置记录的 OBJ_TYPE 属性，以删除用户的权限属性。

restrictions([*Days*] [*Time*])

指定用户可以在一周的哪几天以及一天的什么时间登录。 这些限制存储在 [X]USER 记录的 DAYTIME 属性中。

如果省略 *Days* 而指定 *Time*，则时间限制将应用于记录中已经定义的任何“工作日”限制。

如果忽略 *Time* 而指定 *Days*，则 *Days* 限制将应用于已在记录中定义的任何时间限制。

如果同时指定了 *Days* 和 *Time*，则用户只能在指定日期的指定时间段内访问系统。

天数

指定用户可以登录的日期。 指定 *Days* 时可以使用以下关键字：

- **anyday —** 允许用户在任何一天访问文件。
- **weekdays** - 只允许用户在工作日（星期一至星期五）访问资源。
- **Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**、**Sun —** 只允许用户在指定日期访问资源。 您可以按任何顺序指定日期。 如果指定了多个日期，请用空格或逗号分隔这些日期。

时间

指定用户可以登录的时间段。 time 参数可使用下列子参数：

- **anytime —** 允许用户在某天的任何时间访问资源。
- *startTime*:*endTime —* 只允许用户在指定时间段内访问资源。

  startTime 和 *endTime* 的格式均为 *hhmm*，其中 *hh* 是小时（00 至 23），而 *mm* 是分钟（00 至 59）。 请注意，2400 是无效的时间值；请改为使用 0000。

  StartTime 必须小于 *endTime*。

  注意：CA Access Control 使用处理器所在位置的时区。 如果用户在处于与处理器不同时区的终端上登录，您必须将此因素考虑在内。

restrictions-([days] [time])

删除限制用户登录能力的任何限制。

resume([*dateTime*])

启用通过指定挂起参数禁用的用户记录。如果同时指定 suspend 参数和 resume 参数，恢复日期必须在挂起日期之后。如果忽略 *dateTime*，则执行 chusr 命令时，将立即恢复用户记录。 有关详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

以 *[m]m/[d]d/yy[@HH:MM]* 格式输入 *dateTime*。

resume-

从用户记录中清除恢复日期和时间（如果已使用）。 因此，用户的状态将从活动（启用）更改为挂起。

不能将此参数与 new[x]usr 命令一起使用。

script(*logon-script-path*)

指定用户登录时自动运行的文件的位置。 该参数是可选的。 通常，该登录脚本可配置工作环境。 还可以使用 profile 参数设置用户的工作环境。

server

将 SERVER 属性设置为“on”。 该属性允许代表当前用户运行的进程要求其他用户的授权。 有关详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

server-

将 SERVER 属性设置为“off”。

不能将此参数与 new[x]usr 命令一起使用。

shellprog(*fileName*)

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。 *fileName* 是字符字符串。

不能对企业用户使用此选项。

suspend([*dateTime*])

禁用用户记录，但将其保留在数据库进行定义。 用户不能使用禁用的用户帐户登录系统。

如果指定 *dateTime*，将在指定日期禁用用户记录。 如果忽略 *dateTime*，则执行 ch[x]usr 命令时，将立即禁用用户记录。

以 *mm/dd/yy[@HH:MM]* 格式输入 *dateTime*。

suspend-

从用户记录中清除挂起日期，并将用户的状态从禁用更改为启用（活动）。

不能将此参数与 new[x]usr 命令一起使用。

unix

对于 chusr 和 editusr 命令，该参数可更改本地 UNIX 系统中的用户定义。

对于 newusr 命令，该参数会将用户添加到本地 UNIX 系统中。

如果指定了多个参数，请使用空格将这些参数分隔开。

有关如何在 CA Access Control 中的本地 UNIX 系统上操作的详细信息，请参阅本章中的环境命令。

unix 选项下的 unix 选项和子选项对企业用户无效。

userid(*number*)

设置用户的唯一数字 ID (UID)，用于唯一的自由访问控制。 *数字*是小数数字。 默认情况下，不接受小于 100 的数字。 有关不包括的数字的详细信息，请参阅附录*《参考指南》*中的“AllowedGidRange 标记”。

***userName*|(*userName* [,*userName...*])**

定义用户的名称。 每个用户名必须唯一。

使用 newusr 命令时，*userName* 向 CA Access Control 标识新用户。 如果要使用 newusr 命令且用户已定义到本地环境，则 CA Access Control 会将该用户名用作与该用户对应的 USER 记录。但是，通常应利用 CA Access Control 使用企业用户的能力，而不使用 newusr 为已存在于本地环境中的用户名创建 USER 记录。 改为使用 chgxusr 命令更改该用户的 CA Access Control 属性。

有时，可能会需要不是本地登录名的 CA Access Control 用户名。（这种情况下，登录命令无法让该用户工作，但是另一个命令 [如 sesu] 则可以。）

注意：在 UNIX 中，如果用户名中包含反斜线，则在指定 *userName* 时，请使用两个反斜线。

示例

- 用户 Bob 希望将 FINANCIAL 类别添加到 Jim 的记录中，将 Jim 的安全级别更改为 155，并将 Jim 对系统的访问限制在工作日的上午 8:00 到下午 8:00。
  - 用户 Bob 具有 ADMIN 属性。
  - 向 CA Access Control 定义了用户 Jim。
  - 向 CA Access Control 定义了 FINANCIAL 类别。

```
chuxsr Jim category(FINANCIAL) level(155) restrictions \
(days(weekdays)time(0800:2000))
```

- 用户“admin”希望挂起用户 Joel，该用户将休假三个星期，从 1995 年 8 月 5 日开始。
  - 用户 admin 具有 ADMIN 属性。
  - 向 CA Access Control 定义了用户 Joel。
  - 今天的日期为 1994 年 8 月 3 日。

  ```
  chxusr Joel suspend(8/5/95) resume(8/26/95)
  ```

- 用户 Security2 希望删除用户 Bill 的 AUDITOR 属性，并且希望审核 Bill 的所有活动。
  - 用户 Security2 具有 ADMIN 和 AUDITOR 属性。
  - 向 CA Access Control 定义了用户 Bill。

  ```
  chxusr Bill auditor audit(all)
  ```

- 用户 Rob 希望更改存储在用户 Mary 的记录中的备注。
  - 用户 Rob 是 Mary 的用户记录的所有者。

  ```
  chxusr Mary comment ('Administrator of the SALES group')
  ```

- 管理用户 Sally 希望删除存储在用户 Jared 的记录中的国家或地区名称和位置属性。
  - 用户 Sally 是 Jared 的用户记录的所有者。

  ```
  chxusr Jared country() location()
  ```

- 用户 Bob 希望向 CA Access Control 定义用户 Peter 和 Joe。
  - 用户 Bob 具有 ADMIN 属性。
  - 没有向 CA Access Control 定义用户 Peter 和 Joe。
  - 将应用以下默认项：
    - owner(Bob)
    - audit(failure,loginfailure)

  ```
  newusr (Peter Joe)
  ```

- 用户 Bob 希望向 CA Access Control 定义用户 Jane，并将“payroll”指定为所有者组。
  - 用户 Bob 具有 ADMIN 属性。
  - 没有向 CA Access Control 定义用户 Jane。
  - 用户 Jane 的全名是 JG Harris。
  - audit(failure,loginfailure)

  ```
  newusr Jane owner(payroll) name('J.G. Harris')
  ```

- 用户 Bob 希望向 CA Access Control 定义用户 *JohnD*，并将其安全类别设为 NewEmployee，将其安全级别设为 3。 JohnD 只能在工作日的上午 8:00 到下午 6:00 使用系统。
  - 用户 Bob 具有 ADMIN 属性。
  - 向 CA Access Control 定义了 NewEmployee 类别。
  - 新用户的全名为 John Doe。
  - 将应用以下默认项：
    - owner(Bob)
    - audit(failure)

```
newusr JohnD name('John Doe') category(NewEmployee) level(3) \
restrictions(days(weekdays) time(0800:1800))
```

deploy 命令 - 启动策略部署

在 AC 环境中有效

使用 deploy 命令启动策略部署。 该命令将执行通过 RULESET 对象存储的 selang 命令，RULESET 对象与您所部署的 POLICY 对象相关联。 这些是策略部署命令。

重要说明！ 我们强烈建议您使用 policydeploy 实用程序部署已存储的策略。 deploy 命令仅执行部分策略部署，且为端点部署策略时不更新 DMS。

要运行 deploy 命令，需要具有：

- 对您要部署策略的数据库下的层级结构中每个数据库中的 POLICY、HNODE 和 RULESET 类的子管理权限。
- 对您要部署策略的数据库下的层级结构中每个数据库的相应子管理权限。

  这些是在所有这些计算机上执行构成策略的 selang 命令必需的权限。

  例如，如果您要创建新的文件资源，则需要拥有对 FILE 类的子管理权限。

  ```
  nr FILE /inetpub/* defaccess(none)
  ```

注意：有关策略部署的详细信息，请参阅 *《企业管理指南》*。

此命令有以下格式：

```
deploy POLICY name#xx
```

name#xx

要部署的策略的 POLICY 对象的名称（策略名和版本号）。

deploy- 命令 - 启动策略删除

在 AC 环境中有效

使用 te deploy-（或 undeploy）命令可启动策略取消部署。 该命令将执行通过 RULESET 对象存储的 selang 命令，RULESET 对象与您所部署的 POLICY 对象相关联。 这些是策略取消部署命令。

重要说明！ 我们强烈建议您使用 policydeploy 实用程序取消部署策略。 deploy- 命令仅执行部分策略取消部署，且从端点取消部署策略时不更新 DMS。

要运行该命令，需要具有：

- 对您要取消部署策略的数据库下的层级结构中每个数据库中的 POLICY、HNODE 和 RULESET 类的子管理权限。
- 对您要取消部署的数据库下的层级结构中每个数据库的相应子管理权限。

  这些是在所有这些计算机上执行构成策略取消部署脚本的 selang 命令必需的权限。

注意：有关部署策略的详细信息，请参阅*《企业管理指南》*。

此命令有以下格式：

```
{deploy-|undeploy} POLICY name#xx
```

name#xx

要取消部署的策略的 POLICY 对象的名称（策略名和版本号）。

editfile 命令 - 创建和修改文件记录

在 AC 环境中有效

此命令与 chfile 命令一起说明。

更多信息：

chfile 命令 - 修改文件记录 (p. 54)

edit[x]grp 命令 - 创建和修改组记录

在 AC 环境中有效

该命令记录与 ch[x]grp 命令一起记录。

更多信息：

ch[x]grp 命令 - 更改组属性 (p. 60)

editres 命令 - 修改资源记录

在 AC 环境中有效

此命令与 chres 命令一起说明。

更多信息：

chres 命令 - 修改资源记录 (p. 72)

edit[x]usr 命令 - 修改用户记录

在 AC 环境中有效

该命令记录与 chxusr 命令一起记录。

更多信息：

ch[x]usr 命令 - 更改用户属性 (p. 87)

end_transaction 命令 - 完成双控制事务的记录

在 AC 环境中的 UNIX 主机上有效

end_transaction 命令可完成双控制 PMDB 过程的 start_transaction 命令。

environment 命令 - 设置安全环境

在所有环境中有效

environment 命令可设置安全环境。 CA Access Control 支持 CA Access Control 和 UNIX 安全环境。 调用 selang 命令 shell 时，默认情况下将选定 AC 环境。

此命令有以下格式：

```
environment {ac|config|etrust|native|nt|pmd|seos|unix}
```

ac

指定 CA Access Control 安全环境。 selang 命令可影响本地 CA Access Control 数据库。有些命令支持同时对您所连接到的主机的本机 OS 安全设置进行更新。 在 CA Access Control 环境中，selang 提示如下：

```
AC>
```

配置

指定远程配置环境，在该环境中可更改端点配置设置。

etrust

指定 CA Access Control 安全环境。

注意：这与指定 *AC* 相同，对其进行维护是为了与早期版本兼容。

native

指定您连接到的主机（无论本地还是远程）的本地操作系统安全环境（Windows 或 UNIX）。 selang 命令可影响本机 OS 数据库。 在本地环境中，selang 提示为：

```
AC(native)>
```

nt

指定 Windows 安全环境。 selang 命令会影响 Windows 数据库。 有些命令支持对 CA Access Control 安全设置的同时更新。 在 Windows 环境中，selang 提示为：

```
AC(nt)>
```

pmd

指定远程管理环境中的 selang 命令。将 selang 命令 shell 设置为 pmd 环境后，该命令将在选定主机的 PMDB 中运行。 在 pmd 环境中，selang 提示如下：

```
AC(pmd)>
```

seos

指定 CA Access Control 安全环境。

注意：这与指定 *AC* 相同，对其进行维护是为了与早期版本兼容。

unix

指定 UNIX 安全环境。 selang 命令可在 UNIX 安全系统上运行。 在 UNIX 环境中，selang 提示如下：

```
AC(unix)>
```

find 命令 - 列出数据库记录

在 AC 和本地环境中有效

find 命令显示指定类中的记录的名称。 如果未指定任何参数，则将显示所有类的名称。

注意：find 命令与 *list* 和 *search* 命令相同。

要使用该命令，必须具有足够的权限，如以下条件所定义的权限：

- 如果您具有 ADMIN、AUDITOR 或 OPERATOR 属性，则您可以将 find 命令与所有参数一起使用。
- 如果您对 ADMIN 类中的某个记录拥有读取权限，则您可以为该记录所代表的类指定 class 参数。

此命令有以下格式：

```
{find|f|list|search} [{className|class(className)} [objName]]
```

className

指定 *find* 要从中搜索记录的类。 如果未提供 *className*，*find* 将列出所有类。

objName

指定 CA Access Control 要搜索的记录。 *objName* 可包括通配符。

示例：显示 TERMINAL 类中的所有记录

要显示 TERMINAL 类中的所有成员，请输入以下命令：

```
find terminal
```

get dbexport 命令 — 检索导出的数据库规则

在 AC 环境中有效

get dbexport 命令检索从您连接到的主机上的 CA Access Control 数据库或 PMD 数据库中导出的规则。 对于是否存在导出的数据库，您必须在发出 get dbexport 命令之前发出 start dbexport 命令。

此命令有以下格式：

```
get dbexport [pmdname(name)] [params(OFFSET=number)]
```

pmdname(*name*)

（可选）定义您导出的 PMD 数据库的名称。

params(OFFSET=*number*)

（可选）定义偏移量以便从数据库输出中检索更多行。 对于每次请求，get dbexport 命令只能从导出的数据库返回 200 行。 如果输出中有更多信息，该命令将返回指定返回的最后一行的偏移数据。

示例：从导出的数据库检索规则

下列示例显示如何使用 get dbexport 命令从您连接到的主机上的导出 CA Access Control 数据库中检索信息。 第一个命令检索前 200 行，然后第二个命令检索输出中随后的 200 行：

```
AC > get dbexport
(localhost)
Data for DBEXPORT 'seosdb'
-------------------------------------------
setoptions class+(CLASS)
setoptions class+(CLASS)
setoptions class+(CLASS)
...
chres CLASS ("resource") defaccess(none)
OFFSET: 201

AC> get dbexport params("offset=201")
(localhost)
Data for DBEXPORT 'seosdb'

-------------------------------------------
chres CLASS ("resource") defaccess(none)
chres CLASS ("resource") defaccess(none)
chres CLASS ("resource") defaccess(none)
...
chres CLASS ("resource") defaccess(none)
OFFSET: 401
```

更多信息：

start dbexport 命令 — 启动数据库导出 (p. 144)

get devcalc 命令 — 检索策略偏差数据

在 AC 环境中有效

get devcalc 命令从策略偏差数据文件（deviation.dat，其中包含策略偏差计算结果）中检索信息，并可将结果发送到一个或多个规定的 DMS 数据库。 要使该数据文件存在，之前必须已经发布 start devcalc 命令。

创建策略或主机报告时，还可以指定包括偏差计算结果。 报告实用程序随后将发布该命令。

重要说明！ 偏差计算不会检查是否应用了本地规则。 它还忽略从数据库中删除对象（用户或对象属性、用户或资源授权，或者实际用户或资源）的规则。 例如，计算无法验证是否应用了以下规则：
rr SUDO admCommand

注意：有关策略偏差数据文件和高级策略报告的详细信息，请参阅*《企业管理指南》*。

要运行 get devcalc 命令，您必须具有对计算机的终端访问权限以及对 DEVCALC 子层管理类的读取权限。

此命令有以下格式：

```
get devcalc [params("offset=number")]
```

偏移量=*数字*

（可选）定义偏移量以便从策略偏差数据文件检索更多行。 get devcalc 命令只能根据请求从策略偏差数据文件返回最大行数（由 max_lines_request 配置设置来设置）。 如果文件中有更多信息，该命令将返回指定返回的最后一行的偏移量数据。

示例：获取策略偏差数据

以下示例显示了当 max_lines_request 设置设置为 10 时，如何使用 get devcalc 命令从策略偏差数据文件检索信息。 第一个命令检索前十行，然后第二个命令检索输出的随后十行：

```
AC> get devcalc
(localhost)
Data for DEVCALC 'deviation'
-------------------------------------------
DATA    : DATE, Mon Mar 20 11:22:15 2006
POLICYSTART, myPolicy#01
DIFF, (FILE), (file1), (*), (*)
DIFF, (FILE), (file2), (*), (*)
DIFF, (FILE), (file3), (*), (*)
DIFF, (FILE), (file4), (*), (*)
DIFF, (FILE), (file5), (*), (*)
DIFF, (FILE), (file6), (*), (*)
DIFF, (FILE), (file7), (*), (*)
OFFSET  : 11

AC> get devcalc params("offset=11")
(localhost)
Data for DEVCALC 'deviation'
-------------------------------------------
DATA    : DIFF, (FILE), (file8), (*), (*)
DIFF, (FILE), (file9), (*), (*)
DIFF, (FILE), (file10), (*), (*)
DIFF, (FILE), (file11), (*), (*)
DIFF, (FILE), (file12), (*), (*)
DIFF, (FILE), (file13), (*), (*)
DIFF, (FILE), (file14), (*), (*)
DIFF, (FILE), (file15), (*), (*)
DIFF, (FILE), (file16), (*), (*)
DIFF, (FILE), (file17), (*), (*)
OFFSET  : 21
```

更多信息：

start devcalc 命令 — 启动策略偏差计算 (p. 146)
setoptions 命令 — 设置 t CA Access Control 选项 (p. 128)

help 命令 — 获取 selang 帮助

在所有环境中有效

help 命令显示 selang 语法的方式有如下几种：

- 不与参数一起使用，该命令将显示 selang 命令的列表，并带有每个 selang 命令的简短解释。
- 将它与 selang 命令名称一起使用时，它显示给定命令的语法。
- 与 access 参数一起使用，该命令将显示一个列表，该列表包含 authorize 命令的 access 参数及 new*、ch* 和 edit* 命令的 defaccess 参数的值。
- 与 lineedit 参数一起使用，该命令将显示操作 selang 命令行所用的特殊字符的列表。

注意：要显示在命令行中键入的命令的帮助文本，并且不删除命令行中的文本，请键入 Ctrl+2。

```
{help|h} [commandName|access|lineedit|className|properties|privilege]
```

access

请求 access 和 defaccess 参数可以指定的访问类型的类列表（按类）。

className

请求关于该指定类的简短说明。

command-name

请求指定命令的语法。

lineedit

请求操作 selang 命令行所用的特殊字符的列表。

属性

（AC 环境）请求有关如何更新用户定义的属性的信息。

privilege

（Windows 环境）请求可能的 Windows 权限（针对 ch[x]grp、ch[x]usr、edit[x]grp 和 edit[x]usr 命令）列表。

更多信息：

selang 命令参考 (p. 37)
selang 环境 (p. 32)
获得 selang 帮助 (p. 35)

history 命令 — 显示之前已发布的命令

在所有环境中有效

history 命令可列出在当前 selang 命令 shell 会话中输入的所有命令。 这些命令按照时间顺序排列。 每个命令前面都有该命令的编号。 例如，输入的第三个命令前面会有数字 3。

即使在执行 ch[x]usr、new[x]usr 或 edit[x]usr 命令的过程中输入了密码也是如此。 history 命令显示一系列星号 (***)，而不是明文密码。

此命令有以下格式：

```
history
```

更多信息：

命令历史记录 (p. 22)

hosts 命令 — 连接至远程 CA Access Control 终端

在所有环境中有效

hosts 命令指定 selang 命令将发送到的主机或策略模型。 通过该命令，您可以用其他名称连接到远程 CA Access Control 计算机，以便可以在本地 CA Access Control 服务运行时远程管理该计算机。 默认情况下，所有 selang 命令都定向到本地主机上的数据库。

在执行定向到这些主机的命令之前，必须首先执行 hosts 命令。

要从本地主机管理（更新）远程主机数据库，您必须满足下列条件之一：

- 已被显式授予从本地数据库更新远程主机数据库的权限
- 是可以从本地数据库更新远程主机数据库的组的成员
- 是本地主机的所有者，如远程主机中所定义的那样

要列出当前可用的所有主机和 PMDB，请不带任何参数指定 hosts 命令。

注意：CA Access Control 通过正规主机名而非别名来保护主机。 为了避免别名造成混淆，在为别名定义 HOST 规则时 CA Access Control 会发出警告。 与之相似，如果使用非完全限定名定义 HOST，CA Access Control 也会发出警告，这是因为 CA Access Control 使用主机的完全限定名（例如 mymachine.yourcompany.com）。

此命令有以下格式：

```
hosts [{systemIds|policyModel@[hostname]}]
```

systemIds

指定执行 selang 命令的主机的系统 ID。 指定多个主机时，请用括号括起系统 ID 的列表，并用空格或逗号分隔系统 ID。

***policyModel*@[*hostname*]**

指定执行 selang 命令的策略模型的地址。 指定多个策略模型时，请用括号将策略模型地址列表括起，并用空格或逗号分隔策略模型地址。

如果未指定*主机名*，CA Access Control 将尝试连接至本地主机上的 PMDB。

注意：与显式指定主机相比，使用策略模型的优势在于：策略模型所在的系统不断尝试更新针对该策略模型定义的所有系统，即使它们当前不可用也是如此。 有关策略模型的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

示例：让用户或组更新远程主机

要授权用户从本地数据库更新远程主机数据库，请在远程主机上输入以下命令：

```
authorize TERMINAL local_host uid user_name access(write)
```

要授权组从本地数据库更新远程主机数据库，请在远程主机上输入以下命令：

```
authorize TERMINAL local_host gid(group_name) access(write)
```

示例：将 selang 命令应用于远程策略模型

要将所有后续命令应用于工作站 h1 上的策略模型，请键入以下命令：

```
hosts Policy@h1
```

如果成功连接到 *Policy@h1*，将显示下面的消息。

```
成功连接 h1
```

从现在起输入的所有命令都将定向到 Policy@h1，而不是定向到本地主机。 selang 提示符更改为以下形式：

```
Remote_AC>
```

示例：将 selang 命令应用于远程主机

要将所有将来的命令应用于工作站 athena，请键入以下命令：

```
hosts athena
```

如果成功连接到 athena，屏幕上将显示下面的消息。

```
(athena)
Successfully connected
信息：目标版本为 2.50
```

您输入的任何命令均将应用于 athena，而不是发送到本地主机。 如果添加新用户，则仅将用户添加到 athena，如下例所示：

```
Remote_AC>newusr steve
(athena) 成功添加用户 steve。
```

join[x] 命令 – 将用户添加至内部组

在 AC 环境中有效

join[x] 命令可将用户添加至一个或多个内部组，或更改与组相关的用户属性。 指定的用户和组必须已定义到 CA Access Control。

使用 join 将内部用户添加至组。

使用 joinx 将企业用户添加至组。

注意：此命令同样存在于本地环境中，但操作方式有所不同。

来自 join 命令的属性集将*完全替换*指定组内指定用户的以前所有属性集。 如果以前已定义这种属性，将不会保留这些属性，除非新的 join 命令重新指定它们。

注意：有关组属性的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。

如果至少满足下列条件之一，则可以使用 join 命令：

- 您具有 ADMIN 属性。

  注意：如果要修改 CA Access Control 组记录*和*企业组，您需要同时具有 MODIFY 和 JOIN 访问权限。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是组的所有者。
- 在 ADMIN 类中 GROUP 记录的访问控制列表中，为您分配了 CONNECT 权限。

此命令有以下格式：

```
{join[x]|j[x]} {userName|(userName [,userName...])} \
    group(groupName [,groupName...]) \
    [admin|admin-] \
    [auditor|auditor-] \
    [gowner(group-name)] \
    [operator|operator-] \
    [owner(userName|groupName)] \
    [pwmanager | pwmanager-] \
    [regular] \
    [nt | unix]
```

admin

为 *userName* 指定的用户分配 GROUP-ADMIN 属性。

admin-

删除用户的 GROUP-ADMIN 属性。

auditor

为 *userName* 指定的用户分配 GROUP-AUDIT 属性。

auditor-

删除用户的 GROUP-AUDIT 属性。

gowner(*groupName*)

指定将用户添加到组 *groupName*。

group(*groupName* [,*groupName...*])

指定要将用户作为成员添加至的组。

nt

将 *userName* 连接到 Windows 数据库中的组。

operator

为 *userName* 指定的用户分配 GROUP-OPERATOR 属性。

operator-

删除用户的 GROUP-OPERATOR 属性。

owner(*Name*)

将 CA Access Control 用户或组指定为加入记录的所有者。如果您要创建连接，但未指定所有者，则您即为该连接的所有者。

pwmanager

为 *userName* 指定的用户分配 GROUP-PWMANAGER 属性。

regular

为用户重置管理标志。

unix

将 *userName* 连接到 UNIX 安全系统中的组。

userName

指定连接（或使用一组新属性重新连接）至由 group 参数指定的组的用户。

如果命令为 join，则 *userName* 为用户记录的名称。如果命令为 joinx，则 *userName* 为企业用户的名称。

示例

- 用户 Rorri 希望将用户 Bob 加入到内部组 staff 中。
  - Rorri 拥有 ADMIN 属性。
  - 将应用以下默认项：
    - admin
    - auditor
    - owner(Rorri)
    - pwmanager

```
join Bob group(staff)
```

- 用户 Rorri 希望更改组 staff 中 Sue 的定义。 她当前是 GROUP-AUDITOR；Rorri 希望添加 GROUP-PWMANAGER 属性。
  - Rorri 拥有 ADMIN 属性。
  - 将应用以下默认项：
    - admin
    - owner(Rorri)

  ```
  join Sue group(staff) auditor pwmanager
  ```

  selang 执行该命令时，将删除上一条记录。 有关 Sue 的以前属性的记录将不会保留。 因此，Rorri 必须指定 Sue 现在应该具有的两个属性。

更多信息：

join[x]- 命令 — 从组中删除用户 (p. 118)
show[x]grp 命令 — 显示组属性 (p. 138)
show[x]usr 命令 — 显示用户属性 (p. 142)

join[x]- 命令 — 从组中删除用户

在 AC 环境中有效

join[x]- 命令可从内部组中删除用户。

join- 可从内部组中删除内部用户。

joinx- 从内部组中删除企业用户。

注意：join[-] 命令还可存在于本地环境中，但操作方式有所不同。

要使用 join[x]- 命令，必须满足下列条件之一：

- 您具有 ADMIN 属性。

  注意：如果要修改 CA Access Control 组记录*和*本地组，您需要同时具有 MODIFY 和 JOIN 访问权限。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是组的所有者。
- 在 ADMIN 类中 GROUP 记录的访问控制列表中，为您分配了 CONNECT 权限。

此命令有以下格式：

```
{join[x]-|j[x]-} {userName|(userName [,userName...])} \
    group(groupName [,groupName...])
```

group(*groupName* [,*groupName*...])

指定要从中删除用户的组。

userName

指定要从组中删除的用户。

如果命令为 join，则 *userName* 为用户记录的名称。

如果命令为 joinx，则 *userName* 为企业用户的名称。

示例

用户 Bill 希望从组 PAYROLL 删除用户 sales25 和 sales43。

用户 Bill 具有 ADMIN 属性。

```
joinx- (sales25 sales43) group(PAYROLL)
```

更多信息：

join[x] 命令 — 将用户添加至内部组 (p. 115)
show[x]grp 命令 — 显示组属性 (p. 138)
show[x]usr 命令 — 显示用户属性 (p. 142)

list 命令 — 列出数据库记录

在 AC 和本地环境中有效

这与 find 命令相同。

更多信息：

find 命令 - 列出数据库记录 (p. 108)

newfile 命令 — 创建文件记录

在 AC 环境中有效

此命令与 chfile 命令一起说明。

更多信息：

chfile 命令 - 修改文件记录 (p. 54)

new[x]grp 命令 — 创建组记录

在 AC 环境中有效

此命令与 chgrp 命令一起说明。

更多信息：

ch[x]grp 命令 - 更改组属性 (p. 60)

newres 命令 — 创建资源记录

在 AC 环境中有效

此命令与 chres 命令一起说明。

更多信息：

chres 命令 - 修改资源记录 (p. 72)

new[x]usr 命令 — 创建用户记录

在 AC 环境中有效

此命令与 ch[x]usr 命令一起说明。

更多信息：

ch[x]usr 命令 - 更改用户属性 (p. 87)

rename 命令 — 重命名数据库记录

在 AC 环境中有效

重命名数据库中的记录名。 该记录现在仅被其新名称识别。

注意：您不能重命名 SEOS、UACC 和 ADMIN 类中的记录。

要使用 rename 命令，您必须对记录具有足够的权限。 CA Access Control 将进行下列检查，直到满足下列条件之一：

- 您具有 ADMIN 属性。
- 资源记录在某一组的范围内，您在该组中具有 GROUP-ADMIN 属性。
- 您是记录的所有者。
- 在 ADMIN 类中的资源类记录的 Access Control 列表中，为您分配了 CREATE（针对 editres）访问权限。

此命令有以下格式：

```
rename className oldresourceName newresourceName
```

className

定义您要重命名的记录所属的类。

oldresourceName

定义 CA Access Control 中记录的当前名。

newresourceName

定义您要分配给记录的新名。

示例

用户 *ADMIN 1* 希望将类 *Host* 中的记录 spree3 重命名为 spree4。

- 安全管理员具有 ADMIN 属性。

```
rename host spree3 spree4
```

rmfile 命令 — 删除文件记录

在 AC 环境中有效

rmfile 命令可从数据库中删除属于 FILE 类的记录。

如果满足下列条件之一，则您可以删除文件记录：

- 您具有 ADMIN 属性。
- 该记录在您拥有 GROUP-ADMIN 属性的组范围内。
- 您是该文件的所有者。
- 在 ADMIN 类中 FILE 记录的访问控制列表中，为您分配了 DELETE 访问权限。

此命令有以下格式：

```
{rmfile|rf} {fileName | (filename [,filename...])}
```

文件名

定义要删除的文件。

CA Access Control 将单独处理每个文件记录。如果处理文件时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个文件。

示例：删除文件保护

安全管理员（具有 ADMIN 权限）想删除某个文件的 CA Access Control 保护。 在 UNIX 上，这可能如下所示：

```
rmfile /etc/passwd
```

在 Windows 上，同样的命令可能如下所示：

```
rmfile C:\temp\passwords.txt
```

更多信息：

chfile 命令 - 修改文件记录 (p. 54)
showfile 命令 — 显示文件属性 (p. 136)

rm[x]grp 命令 – 删除组记录

在 AC 环境中有效

rmgrp 和 rmxgrp 命令从 CA Access Control 和本地环境（可选）中删除一个或多个组。

注意：数据库中可能存在 rmgrp 命令无法删除的组的组 ID。 例如，该组可能是其他组的所有者、其他记录的所有者或者在某个资源的 Access Control 列表中。 根据需要使用 chgrp、chusr、chres 和 authorize 命令手动更改所有权和删除与要删除的组记录相关的访问权限。 也可以使用 sepurgedb 实用程序自动清除数据库中的不一致。

注意：rmgrp 命令还可存在于本地环境中，但操作方式有所不同。

要使用 rmgrp 命令，至少需要满足下列条件之一：

- 您具有 ADMIN 属性。
- 要删除的组在您拥有 GROUP-ADMIN 属性的组范围内。
- 您是这个要删除组的所有者。
- 在 AUDIT 类的 GROUP 记录中为您分配了 DELETE 权限。

此命令有以下格式：

```
{rmgrp|rg | rmxgrp|rxg} { groupName | (groupName [,groupName...]) } [unix|nt]
```

groupName

指定要删除的 CA Access Control 组。

nt

（可选）除了从 CA Access Control 数据库中删除组之外，还从本地 Windows 数据库中删除该组。

unix

（可选）除了从 CA Access Control 数据库中删除组之外，还从本地 UNIX 数据库中删除该组。

示例

用户 Joe 希望从数据库中删除组 DEPT1 和 DEPT2。

- 用户 Joe 对 SALES 组拥有 GROUP-ADMIN 权限。
- 组 DEPT1 和 DEPT2 都由 SALES 组所有。

```
rmxgrp (DEPT1, DEPT2)
```

更多信息：

ch[x]grp 命令 - 更改组属性 (p. 60)
join[x] 命令 — 将用户添加至内部组 (p. 115)
join[x]- 命令 — 从组中删除用户 (p. 118)
show[x]grp 命令 — 显示组属性 (p. 138)
rmgrp 命令 — 删除 UNIX 组 (p. 164)
rmgrp 命令 — 删除 Windows 组 (p. 188)

rmres 命令 — 删除资源

在 AC 环境中有效

rmres 命令可将资源从数据库中删除。 可使用 rmres 命令删除属于下列类的记录：ACVAR、ADMIN、APPL、CATEGORY、CONNECT、FILE、GAPPL、GHOST、GSUDO、GTERMINAL、HNODE、HOST、HOSTNET、HOSTNP、LOGINAPPL、MFTERMINAL、POLICY、PWPOLICY、SECFILE、SECLABEL、SPECIALPGM、SUDO、SURROGATE、TERMINAL、PROGRAM、PROCESS、RULESET、TCP、UACC 和任何用户定义的类。

注意：该命令还存在于本地 Windows 环境中，但操作有所不同。

要从数据库中删除记录，您必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 资源记录在某一组的范围内，您在该组中具有 GROUP-ADMIN 属性。
- 您是资源记录的所有者。
- 在 ADMIN 类中该资源类记录的 Access Control 列表中，为您分配了 DELETE 权限。

此命令有以下格式：

```
{rmres|rr} className resourceName
```

className

指定资源所属的类的名称。 要列出为 CA Access Control 定义的资源类，请使用 find 命令。 有关详细信息，请参阅本章的“find 命令”。

resourceName

指定要删除的资源记录的名称。 删除多个资源时，请用括号将资源名列表括起，并用空格或逗号分隔资源名。

CA Access Control 将单独处理每个资源记录。如果处理资源时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个资源。

示例

用户 Admin1 希望将记录 TERMS 从数据库中的 TERMINAL 类中删除。

- 用户 Admin1 具有 ADMIN 属性。

```
rmres TERMINAL TERMS
```

更多信息：

chres 命令 - 修改资源记录 (p. 72)
showres 命令 — 显示资源属性 (p. 139)
rmres 命令 — 删除 Windows 资源 (p. 189)
find 命令 - 列出数据库记录 (p. 108)

rm[x]usr 命令 — 删除用户记录

在 AC 环境中有效

rmusr 和 rmxusr 命令可从 CA Access Control 数据库删除用户，还可删除 CA Access Control 组记录中存在的用户记录的引用。

rmxusr 可从 CA Access Control 数据库中删除企业用户。 rmusr 可从数据库中删除内部用户。 rmusr 命令还可从本地环境中删除用户（可选）。

注意：数据库中可能存在 rm[x]usr 无法删除的用户。 例如，该用户可能是组的所有者、其他记录的所有者或者在资源的 Access Control 列表中。 可根据需要使用 ch[x]grp、ch[x]usr、ch[x]res 和 authorize 命令手动更改所有权和删除与要删除的用户记录相关的访问权限。 也可以使用 sepurgedb 实用程序自动清除数据库中的不一致。

注意：rmgrp 命令还可存在于本地环境中，但操作方式有所不同。

要执行 rm[x]usr 命令，您需要至少满足下列要求之一：

- 您具有 ADMIN 属性。
- 要删除的用户记录在您拥有 GROUP-ADMIN 属性的组范围内。
- 在 ADMIN 类中的 USER 记录的访问控制列表中为您分配了 DELETE 权限。
- 您是该用户记录的所有者。

ru 是 rmusr 的同义词。

rxu 是 rmxusr 的同义词。

此命令有以下格式：

```
{rmusr|ru | rmxusr | rxu} { userName | (userName [,userName...]) } \
    [unix|nt] [appl(homedir=yes)]
```

appl(homedir=yes)

（仅适用于 UNIX）。 删除用户的主目录

该参数可检查用户的主目录在 /home、/tmp 或 /users 中是否存在。如果主目录位于其他目录中，请编辑 S99DELETE_postrmusrdir.sh 脚本以包含该主目录。

注意：在指定该选项之前，必须指定 unix 选项。

nt

不但将用户从 Windows 环境中删除，还从 CA Access Control 中删除。

仅对 rmusr 有效。

userName

定义用户记录。

unix

不但将用户从 UNIX 环境中删除，还从 CA Access Control 中删除。

仅对 rmusr 有效。

示例

以下命令可从 CA Access Control 中删除企业用户 Terry 和 Jane：

```
rxu (Terry, Jane)
```

更多信息：

ch[x]usr 命令 - 更改用户属性 (p. 87)
show[x]usr 命令 — 显示用户属性 (p. 142)
rmusr 命令 — 删除 UNIX 用户 (p. 165)
rmusr 命令 — 删除 Windows 用户 (p. 189)

ruler 命令 — 选择要显示的属性

在 AC 和本地环境中有效

ruler 命令可定义类的 ruler，从而使您可以定义 CA Access Control 可显示类的属性集。

ruler 命令仅适用于当前会话的主机。 每个主机的属性显示在不同的列表中。 如果更改主机，ruler 命令无法更改新主机中的属性显示。

下列用户可以执行该命令：

- 具有 ADMIN、AUDITOR 或 OPERATOR 属性的用户。
- 在您要为其设置标尺的类的 ADMIN 类中拥有读取权限的用户。 例如，如果您在代表类 TERMINAL 的记录的类 ADMIN 中拥有读取权限，则您可以为类 TERMINAL 设置标尺。

此命令有以下格式：

```
ruler className [props( all| propertyName [,propertyName...])]
```

className

要更改其显示的类的名称。

[props(all | *propertyName* [,*propertyName*...])]

指定被显示的属性。

如果省略 props 参数，则 CA Access Control 会显示当前 ruler 内的属性的名称。

所有

指定被显示类的所有属性。

propName

指定被显示的 CA Access Control 属性。 您最多可指定 40 个属性，用空格或逗号隔开。

示例

- 用户 admin 希望 CA Access Control 只显示每个用户的两个属性：所有者和收到更改通知的用户。

  ```
  ruler USER props(NOTIFY, OWNER)
  ```

- 用户 admin 希望显示类 USER 的当前标尺中的属性。

  ```
  ruler USER
  ```

- 用户 admin 希望 CA Access Control 返回显示类 USER 中的所有属性的默认 ruler。

  ```
  ruler USER props(all)
  ```

更多信息：

showfile 命令 — 显示文件属性 (p. 136)
show[x]grp 命令 — 显示组属性 (p. 138)
showres 命令 — 显示资源属性 (p. 139)
show[x]usr 命令 — 显示用户属性 (p. 142)

setoptions 命令 — 设置 t CA Access Control 选项

在 AC 环境中有效

setoptions 命令在运行的系统中设置系统范围的 CA Access Control 选项。 例如，您可以使用 setoptions 为每个类或所有类启用或禁用安全检查，设置密码策略，以及列出 CA Access Control 选项的当前设置。

注意：此命令同样存在于 Windows 环境中，但操作方式有所不同。

需要具有 ADMIN 属性才能使用 setoptions 命令，但存在例外情况 - 只需具有 AUDITOR 或 OPERATOR 属性即可使用命令 setoptions 列表。

此命令格式如下：

```
{setoptions|so} \
    [accgrr|accgrr-] \
    [accpacl|accpacl-] \
    [class+ (className)] \
    [class- (className)] \
    [class (className)] \
    [flags{+|-} (I|W)] \
    [cng_adminpwd|cng_adminpwd-] \
    [cng_ownpwd|cng_ownpwd-] \
    [cwarnlist] \
    [dms{+|-}(dms@hostname)] \
    [inactive(nDays)|inactive-] \
    [is_dms{+|-}] \
    [list] \
    [maxlogins(nLogins)|maxlogins-] \
    [password( \
        [{history(nStoredPasswords) | history-}] \
        [(interval(nDays) | interval-)] \
        [(min_life(nDays) | min_life-)] \
        [{rules( \
                [alpha(nCharacters)] \
                [alphanum(nCharacters)] \
                [(bidirectional) | (bidirectional-)] \
                [grace(nLogins)] \
                [lowercase(nCharacters)] \
                [min_len(nCharacters)] \
                [max_len(nCharacters)] \
                [max_rep(nCharacters)] \
                [{namechk|namechk-}] \
                [numeric(nCharacters)] \
                [{oldpwchk|oldpwchk-}] \
                [prohibited(prohibitedCharacters)] \
                [special(nCharacters)] \
                [sub_str_len(nCharacters)] \
                [uppercase(nCharacters)] \
                [use_dbdict|use_dbdict-] \
        )|rules-}] \
    )] \
```

accgrr

启用累积组权限 (ACCGRR) 选项。

默认值为 enabled。

accgrr-

禁用累积组权限 (ACCGRR) 选项。

accpacl

在所有资源中启用使用 PACL。

accpacl-

禁用使用 PACL。

class (*className*)

为 CA Access Control 类设置或清除设置。

class+(*className*)

启用一个或多个 CA Access Control 类。必须启用 CA Access Control 类才能保护该类的资源。 在激活类之前，必须定义必要的记录以允许访问属于该类的资源。有关随 CA Access Control 提供的资源类的详细信息，请参阅 *《端点管理指南：用于 UNIX》*。

请使用下列值之一：

- CA Access Control 类的名称
- SECLEVEL。 这可启用安全级别检查。
- PASSWORD。 这可激活密码规则。 在 Windows 上，还可启用任意长度的密码。

class-(*className*)

禁用一个或多个 CA Access Control 类。 CA Access Control 不保护属于禁用类的资源。 请使用下列值之一：

- CA Access Control 类的名称
- SECLEVEL。 这可禁用安全级别检查。
- PASSWORD。 这可禁用密码规则。 在 Windows 上，还可禁用长密码。

您无法禁用类 GROUP、SECFILE、SEOS、UACC 和 USER。

cng_adminpwd

使具有 PWMANAGER 属性的用户能够更改 ADMIN 用户的密码。

cng_adminpwd-

禁止具有 PWMANAGER 属性的用户更改 ADMIN 用户的密码。这是默认设置。

cng_ownpwd

使用户能够通过 selang 更改自己的密码。

cng_ownpwd-

禁止用户通过 selang 更改自己的密码。 这是默认设置。

cwarnlist

显示关于哪些类处于警告模式的数据表。

dms{+|-}(*dms@hostname*)

向/从该数据库的 DMS 数据库列表添加/删除 DMS 数据库。

flags{+|-} (I|W)

设置或清除与类有关的功能。 有效值包括：

I

指定类中的对象区分大小写。

W

指定类的警告模式。

注意：标志区分大小写；请使用大写字符。

history(*NStoredPasswords*)

指定历史记录列表中存储的以前使用的密码的数目。 更改密码后，之前的密码将添加至列表，最旧的密码将从该列表中删除（如果需要）。 CA Access Control 可防止用户将其密码更改为列表中已有的密码。

输入从 1 到 24 的整数。 如果指定为零，将不保存密码。

在 Windows 上，history 选项可启用长于 8 个字符的密码。 存储密码时使用的加密形式由 setoptions bidirectional 或 bidirectional- 选项确定。

在 UNIX 上，history 选项*不*影响是否启用长密码。 使用 passwd_local_encryption_method 配置设置以确定是否启用长密码。

history-

禁用密码历史记录检查。

在 Windows 上，该选项可禁用长密码。

inactive(*nDays*)

指定经过多少个不活动天后挂起用户的登录。 空闲日是指用户不登录的日子。 请输入正整数。 如果将 inactive 设置为零，效果与使用 inactive- 参数相同。

非活动-

禁用非活动登录检查。

interval(*nDays*)

interval(nDays)设置在设置或更改密码后且在系统提示用户输入新密码之前必须经过的天数。 输入正整数或零。 如果时间间隔为零，则禁用对用户的密码时间间隔检查。 如果不希望密码过期，请将时间间隔设置为零。

如果实用程序 segrace 是用户登录脚本的一部分，则 CA Access Control 会在达到指定天数时，通知这些用户当前的密码已到期。 用户可立即更新密码，或继续使用旧密码，直到达到宽限登录次数。达到宽限登录次数后，将拒绝用户访问系统，并且用户必须与系统管理员联系以选择新密码。

interval-

取消密码时间间隔设置。

is_dms+

将当前数据库指定为 DMS。

is_dms-

取消将当前数据库指定为 DMS。

list

在屏幕上显示当前的 CA Access Control 设置。

maxlogins(*nLogins*)

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。 通过在用户的用户记录中指定值，可以覆盖该值。

注意：如果将 maxlogins 设置为 1，则无法运行 selang。 必须关闭 CA Access Control，将 maxlogins 设置更改为大于 1 的值，然后重新启动 CA Access Control。

注意：仅在 Unix 和 Linux 操作系统上有效。

maxlogins-

禁用全局最大登录检查。 用户可以登录的终端数目为无限个，除非在该用户的用户记录中对该用户的登录进行了限制。

min_life(*NDays*)

设置密码更改间隔的最小天数。 请输入正整数。

password

设置密码选项。

规则

设置一个或多个供 CA Access Control 用于检查新密码质量的密码规则。 这些规则有：

alpha(*nCharacters*)

设置新密码必须包含的最少字母字符数。 输入一个整数。

alphanum(*nCharacters*)

设置新密码必须包含的最少字母数字字符数。 输入一个整数。

bidirectional

指定将密码作为 PMDB 的一部分发送至其他系统时，以明文（在加密消息中）分发这些密码。

在 UNIX 上，此选项与设置以下 passwd 区设置值等效：

```
Passwd_distribution_encryption_mode=bidirectional
```

注意：建议您设置配置设置，而不要使用 setoptions 命令。

在 Windows 上，密码以在注册表值中指定的加密方式存储在历史记录列表中：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Encryption Package
```

bidirectional-

指定将密码以其哈希加密形式发送。

在 Windows 上，所用哈希函数为 SHA-1。

在 UNIX 上，此选项与设置以下 passwd 区设置值等效：

```
Passwd_distribution_encryption_mode=compatibility
```

注意：建议您设置配置设置，而不要使用 setoptions 命令。

如果指定了该选项，则将无法在不同种类的操作系统之间分发长密码。

grace(*nLogins*)

设置在挂起用户之前允许的最大宽限登录次数。宽限登录次数必须介于 0 和 255 之间（包含 0 和 255）。

lowercase(*nCharacters*)

设置新密码必须包含的最少小写字符数。 输入一个整数。

min_len(*nCharacters*)

设置最小密码长度。 输入新密码必须包含的最少字符总数。

max_len(*nCharacters*)

设置最大密码长度。 输入新密码最多必须包含的字符总数。

max_rep(*nCharacters*)

设置新密码必须包含的最大重复字符数。 输入一个整数。

namechk

检查密码是否包含用户的名称或被用户的名称包含。 默认情况下，CA Access Control 将执行此检查。

namechk-

关闭 namechk 检查。

numeric(*nCharacters*)

设置新密码必须包含的最少数字字符数。 输入一个整数。

oldpwchk

检查新密码是否包含要替换的密码或被要替换的密码包含。默认情况下，CA Access Control 将执行此检查。

注意：仅在 Unix 和 Linux 操作系统上有效。

oldpwchk-

关闭 oldpwchk。

prohibited(*prohibitedCharacters*)

指定用户不能在密码中使用的字符。 输入禁止字符。

注意：我们建议您验证控制字符“\”和“t”都在 prohibitedCharacters 列表中被指定，阻止使用 Tab 键。

special(*nCharacters*)

设置新密码必须包含的最少特殊字符数。 输入一个整数。

sub_str_len(*nCharacters*)

设置新密码可以与以前密码共享的最大字符数。 输入一个整数。

uppercase(*nCharacters*)

设置新密码必须包含的最少大写字符数。 输入一个整数。

use_dbdict | use_dbdict-

设置密码词典。 use_dbdict 将标记设置为 **db**，并将密码与 CA Access Control 数据库中的单词进行比较。 **use_dbdict-** 将内标识设置为 file 并根据在 UNIX 的 seos.ini 文件或 Windows 的 Windows 注册表中指定的文件检查密码。

规则-

禁用密码质量检查。rules 参数指定的规则均不会用于密码质量检查。

示例：设置 CA Access Control 选项

- 用户 John 希望激活 OpsAct 类，这是一个安装定义的类，用于保护操作员的操作。

  用户 John 拥有 ADMIN 属性。

  ```
  setoptions class+(OpsAct)
  ```

- 用户 Mike 希望设置密码策略，以强制用户提供长度至少为 6 个字符的密码。 Mike 还希望激活密码策略实施。

  用户 Mike 具有 ADMIN 属性。

  ```
  setoptions class+(PASSWORD)
  setoptions password(rules(min_len(6)))
  ```

- 用户 SecAdmin 希望启用安全级别检查。

  用户 SecAdmin 具有 ADMIN 属性。

  ```
  setoptions class+(SECLEVEL)
  ```

- 用户 Janani 希望为该数据库设置一个将通知发送到的 DMS。

  用户 Janani 拥有 ADMIN 属性。

  ```
  setoptions dms+(apache@myHost)
  ```

示例：将类置于警告模式

通过对类设置 Warning 属性将类置于警告模式。 您可以使用 setoptions selang 命令执行该操作，如下如示：

```
setoptions class(classname) flags+ (W)
```

classname

定义您要置于警告模式的类的名称。

注意：W 标志区分大小写，该标志必须为大写。

要清除类的警告模式，您还可以使用 setoptions 命令，如下所示：

```
setoptions class(classname) flags- (W)
```

更多信息：

setoptions 命令 — 设置 CA Access Control Windows 选项 (p. 190)

search 命令 — 列出数据库记录

在 AC 和本地环境中有效

这与 find 命令相同。

更多信息：

find 命令 - 列出数据库记录 (p. 108)

showfile 命令 — 显示文件属性

在 AC 环境中有效

showfile 命令列出文件记录的属性。 属性按字母顺序列出。 CA Access Control 可单独处理每个记录，并且只显示您对其拥有足够权限的资源的信息。

注意：此命令同样存在于本地环境中，但操作方式有所不同。

要执行 showfile 命令，至少需要满足下列条件之一：

- 您至少拥有下列属性之一：ADMIN、AUDITOR 和 OPERATOR。
- 您是该文件的所有者。
- 在 ADMIN 类中代表 FILE 类记录的对象的访问控制列表中为您指定了读取权限。
- 在拥有该文件的组中，或在某个拥有该文件的组的父组中，您拥有 GROUP-ADMIN 或 GROUP-AUDITOR 属性。

此命令有以下格式：

```
{showfile|sf} {fileName |(fileName [,fileName...])} \
    [addprops(propName [,propName ...])] \
    [next] \
    [props(all | propName [,propName ...])] \
    [useprops(propName [,propName ...])] \
    [nt|unix]
```

addprops(*propName* [,*propName* ...])

定义要添加至类 ruler 的属性，仅用于本次查询。

文件名

指定要列出其属性的文件记录的名称。

CA Access Control 将单独处理每个文件记录。如果处理文件时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个文件。

fileName 可包含通配符字符，这样可匹配多个文件名。

在 UNIX 上，要显示名称中包含特殊字符或空格的文件的属性，请在文件名前额外键入一个斜线 (/)。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。默认的 query_size 设置为 100。

nt

显示 Windows 文件属性及 CA Access Control 属性。

props(all|*propName* [,*propName* ...])

为此查询和将来的查询定义此类新的 ruler。

unix

显示 UNIX 文件属性及 CA Access Control 属性。

useprops(*propName* [,*propName* ...])

仅为此查询定义 ruler。 类 ruler 不受影响。

示例

用户 root 希望列出文件记录 /etc/passwd 的属性。

- 用户 root 拥有 ADMIN 属性。

```
showfile /etc/passwd
```

更多信息：

checklogin 命令 - 确定登录信息 (p. 51)
chfile 命令 - 修改文件记录 (p. 54)
rmfile 命令 — 删除文件记录 (p. 122)
showfile 命令 — 显示本地文件属性 (p. 165)

show[x]grp 命令 — 显示组属性

在 AC 环境中有效

show[x]grp 命令可显示组记录所有 CA Access Control 属性的设置。（可选）也可以显示本地环境属性。

注意：showgrp 命令还可存在于本地环境中，但操作方式有所不同。

如果至少满足下列条件之一，则可以执行 show[x]grp 命令：

- 您至少拥有下列属性之一：ADMIN、AUDITOR 和 OPERATOR。
- 在要列出的每个组中，您拥有 GROUP-ADMIN 或 GROUP-AUDITOR 属性，或者要列出的每个组都在您拥有 GROUP-ADMIN 属性的组范围内。
- 您是组的所有者。
- 在 ADMIN 类中 GROUP 记录的访问控制列表中，为您分配了读取权限。

此命令有以下格式：

```
{showgrp|sg} {groupName |groupName [,groupName...] )} \
    [addprops(propName[,propName ...])] \
    [next] \
    [props(all | propName[,propName ...])] \
    [useprops(propName[,propName ...])] \
    [nt|unix]
```

addprops(*propName* [,*propName* ...])

仅为此查询定义要添加到 ruler 的属性。

groupName

指定要列出属性的组的名称。

groupName 可包含通配符字符。

在 UNIX 上，要显示名称中包含特殊字符或空格的组的属性，请在组名前额外键入一个斜线 (/)。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 默认的 query_size 为 100。

nt

显示数据库中的属性以及来自本地 Windows 系统的组详细信息。

props(all|*propName* [,*propName* ...])

为此查询和将来的查询定义该类的 ruler。

useprops(*propName* [,*propName* ...])

仅为此查询定义 ruler。 类 ruler 不受影响。

unix

显示数据库中的属性以及来自本地 UNIX 系统的组详细信息。

示例

- 超级用户希望显示 security 组的属性。
  - 超级用户在 security 组中具有 GROUP-ADMIN 属性。

```
showgrp security
```

- 用户 admin 希望显示所有企业组的属性。
  - 用户 admin 具有 ADMIN 和 AUDITOR 属性。

```
showxgrp *
```

将列出针对 CA Access Control 定义的所有企业组的属性。

更多信息：

ch[x]grp 命令 - 更改组属性 (p. 60)
rm[x]grp 命令 — 删除组记录 (p. 123)
showgrp 命令 —显示本地组属性 (p. 167)

showres 命令 — 显示资源属性

在 AC 环境中有效

showres 命令可显示属于数据库中的类的资源的属性。 属性按字母顺序列出。 可使用 showres 命令列出下列类：ACVAR、ADMIN、CATEGORY、CONNECT、FILE、GHOST、GSUDO、GTERMINAL、HOST、HOSTNET、HOSTNP、SECFILE、SECLABEL、SUDO、SURROGATE、TERMINAL、PROGRAM、PROCESS、TCP、UACC 和任何用户定义的类。 CA Access Control 可单独处理每个资源，并且只显示您对其拥有足够权限的资源的信息。

注意：此命令同样存在于本地 Windows 环境中，但操作方式有所不同。

showres 还可以显示已经取消受托的任何程序的相关信息。 这些信息包括：

- 取消对程序的信任的原因。
- 最后一个访问该程序的用户的 UID（不一定是导致该程序不受信任的用户）。
- 该用户访问该程序的日期和时间。

如果至少满足下列条件之一，则可以执行 showres 命令：

- 您至少拥有下列属性之一：ADMIN、AUDITOR 和 OPERATOR。
- 您是资源的所有者。
- 在 ADMIN 类中代表资源类记录的对象的访问控制列表中为您指定了读取权限。

此命令有以下格式：

```
{showres|sr} className resourceName \
    [addprops(propName [,propName...])] \
    [next] \
    [props(all | propName [,propName...])] \
    [useprops(propName [,propName...])]
```

addprops(*propName* [,*propName...*])

仅为此查询定义要添加到当前 ruler 的属性。

className

指定资源所属的类的名称。 要列出为 CA Access Control 定义的资源类，请使用 find 命令。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName* [,*propName ...*])

为此查询和将来的查询定义此类新的 ruler。

resourceName

指定要列出其属性的资源记录的名称。 列出多个资源的属性时，请用括号括起资源名列表，并用空格或逗号分隔资源名。

CA Access Control 将单独处理每个资源记录。如果处理资源时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个资源。

resourceName 可包含通配符字符。

在 UNIX 上，要显示名称中包含特殊字符或空格的单个资源的属性，请在资源名前额外键入一个斜线 (/)。

useprops(*propName* [,*propName* ...])

仅为此查询定义 ruler。 类 ruler 不受影响。

示例：列出记录属性

在该示例中，用户 Admin1 希望列出名称与 TERMINAL 类中的掩码 ath* 匹配的记录的属性。

用户 Admin1 具有 ADMIN 和 AUDITOR 属性。

```
showres TERMINAL ath*
```

示例：列出主机属性

在该示例中，用户 Admin1 列出 HNODE 类中的本地主机的属性。

```
AC> showres HNODE '__local__'
(localhost)
Data for HNODE '__local__'
------------------------------------------------------------
Owner             : LOCALHOST\Administrator (USER)
Create time       : 13-Oct-2010 11:12
Update time       : 13-Oct-2010 11:13
Updated by        : LOCALHOST\Administrator (USER)
Attributes        :
    REGISTERED_NAME=localhost.domain.com
    MAC_ADDRESS=00-50-56-B5-6B-XD
```

在该示例中，命令返回以下属性：

- REGISTERED_NAME=localhost.domain.com
- MAC_ADDRESS=00-50-56-B5-6B-XD

更多信息：

chres 命令 - 修改资源记录 (p. 72)
rmres 命令 — 删除资源 (p. 124)
showres 命令 — 显示本地资源属性 (p. 194)
find 命令 - 列出数据库记录 (p. 108)

show[x]usr 命令 — 显示用户属性

在 AC 环境中有效

show[x]usr 命令可显示针对 CA Access Control 定义的一个或多个用户的所有属性的值。

使用 showusr 显示内部用户的属性。 使用 showusr 显示企业用户的属性。

注意：showusr 命令还可存在于本地环境中，但操作方式有所不同。

您始终可以列出您自己的用户记录的属性。 要列出其他用户记录的属性，必须满足下列条件之一：

- 您是该用户记录的所有者。
- 您至少拥有下列属性之一：ADMIN、AUDITOR 和 OPERATOR。
- 该用户记录在您至少拥有下列组属性之一的组范围内：ADMIN、AUDITOR、OPERATOR。
- 在 ADMIN 类中 USER 记录的访问控制列表中，为您分配了读取权限。

此命令有以下格式：

```
{showusr|su |showxusr |sxu } [ {userName |(userName [,userName...]) } ] \
    [addprops(propName [,propName...])] \
    [next] \
    [props( all | propName [,propName...])] \
    [useprops(propName[,propName...])] \
    [nt|unix]
```

addprops(*propName* [,*propName...*])

仅为此查询定义要添加到当前 ruler 的属性。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

nt

显示除数据库中的属性以及用户 Windows 的属性。

props(all|*propName* [,*propName* ...])

为此查询和将来的查询定义此类新的 ruler。

unix

显示除数据库中的属性以及用户的 UNIX 的属性。

userName

定义用户名。 它可包括通配符字符。

在 UNIX 上，要显示名称中包含特殊字符或空格的单个用户记录的属性，请在组名前额外键入一个斜线 (/)。

如果不指定*用户名*，该命令将显示您自己的用户记录的属性。

useprops(*propName* [,*propName* ...])

仅为此查询定义 ruler。 类 ruler 不受影响。

示例

- 用户 root 希望列出企业用户 Robin 的属性。 root 具有 ADMIN 和 AUDITOR 属性。

  ```
  showxusr Robin
  ```

- 用户 root 希望列出企业用户 Robin 和 Leslie 的用户属性。 root 具有 ADMIN 和 AUDITOR 属性。

  ```
  showxusr (Robin,Leslie)
  ```

更多信息：

rm[x]usr 命令 — 删除用户记录 (p. 125)
ch[x]usr 命令 - 更改用户属性 (p. 87)
showusr 命令 — 显示本地用户属性 (p. 168)

source 命令 – 执行来自文件的命令

在所有环境中有效

使用 source 命令，可以执行一个或多个已放入文件中的 selang 命令。 CA Access Control 可读取指定文件，执行这些命令并返回 selang 提示符。 在数据库中定义的任何用户都可以使用该命令。

该命令与 UNIX 的 csh 和 tcsh 中的 source 命令相似。

此命令有以下格式：

```
source fileName
```

文件名

指定包含 selang 命令的文件的名称。

示例

用户 admin 希望执行名为 initf1 的文件中的命令。 该用户输入以下命令。

```
source initf1
```

start dbexport 命令 – 启动数据库导出

在 AC 环境中有效

start dbexport 命令导出您连接到的主机的 CA Access Control 数据库，并将输出复制到缓冲区。 如果连接到 PMDB，您也可以使用该命令导出 PMD 数据库。

注意：使用 get dbexport 命令查看输出。

此命令有以下格式：

```
start dbexport [pmdname(name)] [filter("CLASS, CLASS...")] [param("depend=yes")]
[param("edit=yes")]
```

filter("*CLASS, CLASS...*")

（可选）定义要从数据库导出的类。 如果您不指定类，将会导出数据库中的所有规则。

param("depend=yes")

（可选）指定导出依存类以及您在 filter 参数中指定的类。 当指定该参数时，CA Access Control 会导出指定的类和以下依存类：

- 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。

param("edit=yes")

（可选）指定 CA Access Control 将创建新资源或访问者的每个规则都更改为修改资源或访问者的规则。

示例：如果您指定该参数，CA Access Control 会将所有 newres 规则更改为 editres 规则。

pmdname(*name*)

（可选）定义要导出的 PMD 数据库的名称。

示例：启动数据库导出

下列示例启动对修改 FILE 和 GFILE 类资源的规则的导出。 规则从 seosdb（您连接到的主机上的 CA Access Control 数据库）中导出。

```
start dbexport filter("FILE, GFILE")
```

示例：启动具有依存类的数据库导出

下列示例启动对修改 FILE 类资源和依存于 FILE 类资源的任何类的规则的导出，并将创建新资源或访问者的每个规则都更改为修改资源或访问者的规则：

```
start dbexport filter("FILE") param("depend=yes edit=yes")
```

更多信息：

get dbexport 命令 — 检索导出的数据库规则 (p. 109)

start devcalc 命令 — 启动策略偏差计算

在 AC 环境中有效

start devcalc 命令可启动策略偏差计算并发送偏差状态。 偏差数据存储在本地策略偏差数据文件 (deviation.dat) 中，并将策略偏差状态通过一个或多个设置的 DH 发送至 DMS。 要检索实际的偏差数据，需要运行 get devcalc 命令。

注意：您不需要手工运行偏差计算器。 如果您使用高级策略管理，policyfetcher 会为您定期执行该操作。 如果您启用了企业报告，报告代理也会定期执行该操作。 有关策略偏差计算的详细信息，请参阅*《企业管理指南》*。

要运行 start devcalc 命令，必须具有对计算机的终端访问权限以及对 DEVCALC 子层管理类的执行权限。

此命令有以下格式：

```
start devcalc [params("-pn name#xx -strict -nonotify -precise")]
```

-nonotify

（可选）指定 devcalc *不*通过 DH 将偏差状态发送到 DMS。

注意：偏差计算命令 policyfetcher 运行在 devcalc_command 配置设置中有所定义，默认情况下，使用该选项避免两次发送偏差状态。

-pn *name#xx*

（可选）定义逗号隔开的 POLICY 对象（策略版本）列表，偏差计算器应为这些对象计算差异。 如果未指定策略，则偏差计算器将计算在本地主机上部署的所有策略的差异。

-strict

（可选）在与本地 HNODE 对象相关的策略和与第一个可用 DMS 上的 HNODE 对象相关的策略之间进行比较。

正常情况下，偏差计算器只检查本地主机上的偏差。 如果指定了该选项，则偏差计算器还将本地策略与列表中第一个可用 DMS 上的策略进行比较。 它比较以下方面：

1. 与代表本地主机的 HNODE 对象相关联的策略列表。
2. 每个与 HNODE 对象关联的 POLICY 对象的策略状态。
3. 每个与 HNODE 对象关联的 POLICY 对象的策略签名。

当您需要验证偏差计算结果时，请使用该选项。

注意：如果有大量端点同时运行偏差计算，则 DMS 将负载过重。 我们建议您将端点配置为使用 DMS 列表，或将您的层级结构划分为较小的层级结构，然后在这些较小的层级结构中使用该选项。

-precise

（可选）指定偏差报告还显示端点数据库中存在、但在策略中找不到的已添加对象、属性和值。 默认情况下，该报告仅显示缺失的项和不匹配的项。 当想查看端点数据库上的内容并将其与部署的策略进行比较时，可使用该选项。

示例：启动特定策略的策略偏差计算

下面的示例显示了您可以如何使用 start devcalc 命令，为名为 myPolicy 的第二个策略版本计算策略偏差，并将偏差状态发送至在本地 CA Access Control 数据库中指定的 DMS 列表：

```
AC> start devcalc params("-pn myPolicy#02")
```

start_transaction 命令 — 启动记录双重控制事务

在 AC 环境中的 UNIX 主机上有效

start_transaction 和 end_transaction 命令以及一个或多个命令可创建包含 Dual Control PMDB 进程未处理事务的文件。 在事务中输入命令的管理员（具有 ADMIN 属性的任意用户）称为制定者。 这些命令在 PMDB 中执行之前，必须获得检查者（*不*是制定者的任意管理者）的授权。

检查者必须首先锁定事务，然后才能处理这些事务。 在事务被检查者锁定之前，制定者可以对其进行检索，更改这些命令或者删除该事务。（有关详情，请参阅*《参考指南》*中的 sepmd 实用程序）当制定者输入 end_transaction 命令时，该事务会收到一个唯一的 ID 号。 如果 Maker 想稍后编辑或检索该事务，则必须在 start_transaction 命令中将该标识号添加在该事务名的后面。 当制定者检索该事务时，将显示制定者的名称、该事务的 ID 号及简要说明（如果制定者已在 *transactionName* 参数中输入了说明）。

制定者无法更改其他制定者的事务。 一个事务中使用的对象直到处理这些命令之后才能被其他事务中的其他制定者使用。

每个未处理的事务在被检查者处理之前，都会保存在一个单独的文件中。 检查者可以授权或拒绝事务。 如果事务得到授权，则会执行这些命令，并相应地更改 PMDB。 如果检查者拒绝该事务，则会删除这些命令，且不更改 PMDB。

在操作者的操作结尾输入 end_transaction 命令时，将显示该事务的数字 ID。 这些命令可能会由于下列原因而失败：

- 如果某个命令引用的对象已在另一个尚未处理的事务中使用
- 如果某个命令与制定者有关 - 您无法更改自己
- 如果某个命令包含无效语法
- 如果某个命令引用的对象不存在（这种情况下将显示一条警告消息）
- 如果您拥有 ADMIN 属性，则可以执行 start_transaction 和 end_transaction 命令。
- 因为在调用 start_transaction 和 end_transaction 命令之前必须执行 hosts 命令，所以您必须得到授权才能使用 hosts 命令。

注意：有关双重控制的详细信息，请参阅*《端点管理指南：用于 UNIX》*。

使用注意事项：

- 调用 start_transaction 和 end_transaction 命令之前必须执行 hosts 命令，并且 PMDB 的名称必须为“制定者”。
- 要使 start_transaction 和 end_transaction 命令生效，必须将 pmd.ini 文件和 seos.ini 文件的 [pmd] 部分中的 is_maker_checker 标记值设置为 yes。

此命令有以下格式：

```
start_transaction transactionName [transactionId]
。
。
。
end_transaction
```

transactionName

指定事务的名称或说明。可输入最多 256 个字母数字字符的字符串。

transactionId

指定创建事务时指定给该事务的唯一号。 创建事务时，该数字 ID 将自动显示。 更新同一个事务时，必须是定该 ID 号。

示例

- Maker Sally 希望将用户 Anne 添加到 PMDB 中，并将其访问该系统的权限限制在工作日的上午 8:00 到晚上 8:00 之间。然后，Sally 希望将 tty30 终端的默认访问权限更改为只读。 Sally 希望称此事务为“general”。

  – 该 Maker 拥有 ADMIN 属性。

  ```
  hosts maker@
  start_transaction general
  newusr anne
  (days(weekdays)time(0800:2000))
  chres TERMINAL tty30
  defaccess(read)
  end_transaction
  ```

  当 Sally 输入 end_transaction 命令时，会为该事务分配一个 ID 号，如 7。

- Maker Sally 希望将 FINANCIAL 类添加至用户 Anne。 Sally 在当天早些时候添加了用户 Anne 记录，但该命令尚未在 PMDB 上处理或执行。

  – 该 Maker 拥有 ADMIN 属性。

  ```
  hosts maker@
  start_transaction general 7
  chusr anne category(FINANCIAL)
  end_transaction
  ```

unalias 命令 — 删除 selang 别名

在 UNIX 主机上有效

unalias 命令可删除由 alias 命令定义的别名。

注意：您可使用 alias 命令列出所有已定义的别名及其值。

此命令有以下格式：

unalias *aliasName*

aliasName

指定希望从数据库中删除的别名的名称。

更多信息：

alias 命令 - 定义 selang 别名 (p. 41)

undeploy 命令 — 启动策略删除

在 AC 环境中有效

该命令是 deploy- 命令的同义词。

更多信息：

deploy- 命令 - 启动策略删除 (p. 105)

远程配置环境中的 selang 命令

本节包含在 CA Access Control 配置资源上执行的所有 selang 命令的完整参考，这些命令按字母顺序排列。

editres config — 修改配置设置

在配置环境中有效

使用 editres config 命令修改 CA Access Control 配置设置。

对于不同的文件集，editres config 命令具有不同的格式。 这些类集包括：

- 审核配置文件（audit.cfg 和 auditrouteflt.cfg）和 PMDB 筛选文件
- 其他所有文件

用于审核配置文件和 PMDB 筛选文件时，此命令语法如下：

```
editres config name [line+|-(value)] [clear]
```

用于其他所有文件时，此命令语法如下：

```
editres config name section(path) token[-](name) value[+|-](value)
data_type(type)
```

名称

指定希望修改的配置资源。 要修改 PMDB 筛选文件，采用格式 *pmdname@filter* 来指定文件名，例如 master_pmdb@filter.flt

注意：要获得您所管理的主机的配置资源列表，请使用 *find config* 命令。

clear

删除审核配置文件或 PMDB 筛选文件中的所有值。

注意：该选项不会删除文件中的注释。

data_type(*type*)

指定配置条目的数据类型。

值：str、numeric、multi_str

默认值：str

注意：对于 UNIX，data_type 只能为 *str*。 其他数据类型不适用于 UNIX，因为它将配置设置存储在文件中（文本字符串）。

line+(*value*)

定义您想添加到审核配置文件或 PMDB 筛选文件中的值。

注意：*value* 可以是值或注释。

line-(*value*)

定义您想从审核配置文件或 PMDB 筛选文件中删除的值。

注意：*value* 可以是值或注释。

section(*path*)

定义您要修改的配置资源的部分。

注意：对于 Windows 注册表设置，如果未指定该选项，则该命令将修改注册表键*名称*定义。

token(*name*)

定义您要修改的配置条目的名称。

token-(*name*)

定义您要删除的配置条目的名称。

value(*value*)

定义您要分配给配置条目的值。 如果配置条目的值已经存在，CA Access Control 会将该值替换成 *value*。

如果未指定*值*，该命令将重置配置条目值。

value+(*value*)

（仅适用于 Windows REG_MULTI_SZ 注册表项）定义想要附加到配置条目的值。

（所有其他配置值）定义想要分配给配置条目的值。 如果配置条目的值已经存在，CA Access Control 会将该值替换成 *value*。

注意：要确保 selang 正确地转换分配的值，请将值放入引号 (" ") 中。

value-(*value*)

（仅适用于 Windows REG_MULTI_SZ 注册表项）定义想要从配置条目中删除的值。

（所有其他配置值）指定从配置条目中删除任何值。

示例：在 Windows 上修改 ACROOT 配置设置

下面的示例说明如何为 Windows 配置设置修改 CA Access Control。

- 此示例将 CA Access Control 配置为使用“仅审核模式”：

  ```
  er CONFIG ACROOT section(SeOSD) token(GeneralInterceptionMode) value(1)
  ```

- 此示例将在 CA Access Control 维护以用于主机名解析的域名列表中添加一个域名。 domain_names 注册表项是 REG_MULTI_SZ 注册表项：

  ```
  er CONFIG ACROOT section(SeOSD) token(domain_names) value+(company.com)
  ```

- 此示例将从 CA Access Control 维护以用于主机名解析的域名列表中删除一个域名。 domain_names 注册表项是 REG_MULTI_SZ 注册表项：

  ```
  er CONFIG ACROOT section(SeOSD) token(domain_names) value-(company.com)
  ```

- 此示例将删除一个配置设置：

  ```
  er CONFIG ACROOT section(AccessControl) token-(Emulate)
  ```

- 此示例将在所管理的主机上配置策略模型的父策略模型配置：

  ```
  er config myPMDB@PMDROOT token(Parent_Pmd) value(topPMDB@host1.comp.ca)
  ```

示例：在 UNIX 上修改 seos.ini 配置设置

下面的示例说明如何为 UNIX 配置设置修改 CA Access Control。

- 此示例将 CA Access Control 配置为启用 PAM 验证：

  ```
  er CONFIG seos.ini section(seos) token(pam_enabled) value(yes)
  ```

- 该示例配置 CA Access Control 维护以用于主机名解析的域名：

  ```
  er CONFIG seos.ini section(seosd) token(domain_names) value+(company.com)
  ```

- 该示例删除 CA Access Control 维护以用于主机名解析的域名：

  ```
  er CONFIG seos.ini section(seosd) token(domain_names) value-(company.com)
  ```

- 此示例将删除一个配置设置：

  ```
  er CONFIG seos.ini section(serevu) token-(admin_user)
  ```

示例：修改审核配置文件

以下示例将行添加到审核配置文件中：

```
er CONFIG audit.cfg line+("FILE;*;Administrator;*;R;P")
```

示例：修改 PMD 筛选文件

以下示例将行添加到 PMD 筛选文件中：

```
er config pmdb@filter line+("*;*;USER;*;OLD_PASSWD;PASS")
```

find config — 列出配置资源

在配置环境中有效

find config 命令可列出用于您所管理的主机的 CA Access Control 配置资源。 这些资源可以为注册表键或配置文件。

可用的资源随主机类型而不同：

UNIX	Windows
seos.ini	ACROOT
pmd.ini@*pmd_name*	pmd_name@PMDROOT
	SEOSDRV

此命令有以下格式：

```
find config
```

注意：该命令不返回 audit.cfg 或 auditrouteflt.cfg 配置文件的列表。

示例：列出 Windows 主机的配置资源

以下示例显示了在具有名为 pmdb 的策略模型的 Windows 主机上执行 find config 命令时的输出：

```
AC(config)> find config
(localhost)
pmdb@PMDROOT
ACROOT
SEOSDRV
```

showres config — 显示配置信息

在配置环境中有效

使用 showres config 命令显示 CA Access Control 配置信息。

对于不同的文件集，showres config 命令具有不同的格式。 这些类集包括：

- 审核配置文件（audit.cfg 和 auditrouteflt.cfg）和 PMDB 筛选文件
- 其他所有文件

用于审核配置文件和 PMDB 筛选文件时，此命令语法如下：

```
showres config name
```

用于其他所有文件时，此命令语法如下：

```
showres config name [section(path)] [token(name)] [recursive] [section_only]
```

名称

指定希望查看其信息的配置资源。 要查看有关 PMDB 筛选文件的信息，请采用格式 *pmdname@filter* 来指定文件名，例如 master_pmdb@filter.flt

注意：要获得您所管理的主机的配置资源列表，请使用 *find config* 命令。

section(*path*)

（可选）定义您要查看其信息的配置资源的部分。

如果您未指定该选项，则该命令将列出 *名称*配置资源中的所有配置条目和部分。

token(*name*)

（可选）定义您要查看其信息的配置资源的名称。

如果您未指定该选项，则该命令将列出您已定义的部分（*路径*）中的所有配置文件条目和部分。

recursive

指定显示有关所有子部分中的所有配置条目和部分的信息。

section_only

指定仅显示有关部分的信息（不会列出任何配置条目）。

本地 UNIX 环境中的 selang 命令

本节包含在 UNIX 系统文件执行的所有 selang 命令（本地 UNIX 环境中的命令）的完整参考，这些命令按字母顺序排列。

chfile 命令 — 修改 UNIX 文件设置

在本地 UNIX 环境中有效

chfile 和 editfile 命令可以更改一个或多个 UNIX 文件的设置。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{{chfile|cf}|{editfile|ef}} fileName \
    [owner(userName)] \
    [group(groupName)] \
    [mode( \
        [fowner(string)] \
        [fgroup(string)] \
        [fother(string)] \
    )]
```

文件名

指定要更改其设置的文件的名称。至少输入一个 UNIX 文件名。更改多个文件时，请用括号将文件名列表括起，并用空格或逗号分隔文件名。

group(*groupName*)

更改文件所属的组。 指定有效的组名。

事务模式

更新文件的访问模式。

fowner(*string*)

为文件所有者指定访问模式。 在 *string* 中使用字母 r、w 和 x，可分别指定读取、写入和执行权限。 使用字母 s 生成文件 setuid。

在 *string* 前面加上加号 (+) 可向现有权限添加权限。 在 *string* 前面加上减号 (-) 可删除权限。 如果未指定前缀，则之前的权限将重置到 *string*。

fgroup(*string*)

指定文件组的访问模式。 在 *string* 中使用字母 r、w 和 x，可分别指定读取、写入和执行权限。 使用字母 s 生成文件 setgid。

在 *string* 前面加上加号 (+) 可向现有权限添加权限。 在 *string* 前面加上减号 (-) 可删除权限。 如果未指定前缀，则之前的权限将重置到 *string*。

fother(*string*)

指定应用到其他访问者的访问模式。 在 *string* 中使用字母 r、w 和 x，可分别指定读取、写入和执行权限。 在 *string* 前面加上加号 (+) 可向现有权限添加权限。 在 *string* 前面加上减号 (-) 可删除权限。 如果未指定任何前缀，则先前的权限将重置到 *string*。

owner(*userName*)

更改文件的所有者。 指定有效的 UNIX 用户的用户名。

更多信息：

find file 命令 — 列出本地文件 (p. 161)
showfile 命令 — 显示本地文件属性 (p. 165)
chres 命令 - 修改资源记录 (p. 72)

chgrp 命令 — 修改 UNIX 组

在本地 UNIX 环境中有效

使用 chgrp、editgrp 和 newgrp 命令处理 UNIX 组。 这些命令结构相同，仅在以下方面有所不同：

- chgrp 命令*修改*一个或多个 UNIX 组。
- editgrp 命令*创建或修改*一个或多个 UNIX 组。
- chgrp 命令*创建*一个或多个 UNIX 组。

注意：在配置设置 (seos.ini) 中指定的文件内对组进行读取、添加、更新和删除；默认情况下，此文件为 /etc/group。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{{chgrp|cg}|{editgrp|eg}|{newgrp|ng}} groupName \
    [groupid(integer)] \
    [userlist(userNames)]
```

groupid(*integer*)

设置组的组 ID。 输入表示组的唯一数字 ID 的正整数。 CA Access Control 不允许组 ID 为零。

groupName

指定要修改的组的名称。 指定现有 UNIX 组的名称。 更改多个组时，将组名列表括在圆括号中并以空格或逗号分隔组名。

userlist(*userNames*)

指定新的成员列表。必须已针对 UNIX 定义每个用户名。列表中存在多个用户时，请使用空格或逗号分隔用户名。 此处指定的用户列表将替代定义到该组的所有先前的用户列表。

更多信息：

rmusr 命令 — 删除 UNIX 用户 (p. 165)
showusr 命令 — 显示本地用户属性 (p. 168)
ch[x]grp 命令 - 更改组属性 (p. 60)

chusr 命令 — 修改 UNIX 用户

在本地 UNIX 环境中有效

使用 chgusr、editusr 和 newusr 命令处理 UNIX 用户。 这些命令结构相同，仅在以下方面有所不同：

- chgrp 命令*修改*一个或多个 UNIX 用户。
- editgrp 命令*创建或修改*一个或多个 UNIX 用户。
- newusr 命令*创建*一个或多个 UNIX 用户。

注意：在配置设置 (seos.ini) 中指定的文件内对用户进行读取、添加、更新和删除；默认情况下，此文件为 /etc/passwd。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

注意：此命令同样存在于 CA Access Control 环境中，但操作方式有所不同。

此命令有以下格式：

```
{{chusr|cu}|{editusr|eu}|{newusr|nu}} userName \
    [enable] \
    [gecos(string)] \
    [homedir({path|nohomedir})] \
    [password(string)] \
    [pgroup(groupName)] \
    [shellprog(path)] \
    [userid(number)]
```

enable

启用因任何原因而被禁用的用户帐户登录。这是一个 chusr 和 editusr 参数。

gecos(*string*)

指定一个包含有关用户的一般注释的字符串，例如用户全名。 用单引号将字符串引起。

homedir(*path*|nohomedir)

指定用户主目录的完整路径。CA Access Control 尝试创建目录。更新 UNIX 文件，无论 CA Access Control 是否成功创建了主目录。

如果指定了 nohomedir，则 UNIX 将不会为用户创建 homedir。

password(*string*)

为用户分配密码。 指定除空格之外的任何字符。 该密码只能用于一次登录。 用户下次登录系统时，必须设置新密码。

pgroup(*groupName*)

指定用户的主组名。

shellprog(*path*)

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。

userid(*number*)

指定用户的唯一数字 ID，用于任意 Access Control。输入一个大于 100 的十进制数字；不接受小于 100 的值。

userName

指定现有 UNIX 用户的名称。 更改多个用户时，请用括号将用户名列表括起，并用空格或逗号分隔用户名。

更多信息：

rmusr 命令 — 删除 UNIX 用户 (p. 165)
showusr 命令 — 显示本地用户属性 (p. 168)
ch[x]usr 命令 - 更改用户属性 (p. 87)

editfile 命令 — 修改 UNIX 文件设置

在本地 UNIX 环境中有效

此命令与 chfile 命令一起说明。

更多信息：

chfile 命令 — 修改 UNIX 文件设置 (p. 156)

editgrp 命令 — 创建和修改 UNIX 组

在本地 UNIX 环境中有效

此命令与 chgrp 命令一起说明。

更多信息：

chgrp 命令 — 修改 UNIX 组 (p. 157)

editusr 命令 — 创建和修改 UNIX 用户

在本地 UNIX 环境中有效

此命令与 chusr 命令一起说明。

更多信息：

chusr 命令 — 修改 UNIX 用户 (p. 158)

find file 命令 – 列出本地文件

在本地环境中有效

使用 find file 命令列出与掩码（一个字符串）匹配的所有系统文件。 这些文件按照时间顺序排列在一列中。

此命令有以下格式：

```
find file [directory][/mask]
```

目录

列出目录 *directory* 中的所有文件。

mask

列出目录 *directory* 中与 *mask* 变量匹配的所有文件。 *mask* 可能会包括通配符字符。

示例：在 Windows 上特定路径中查找可执行程序文件

以下命令可列出 CA Access Control bin 目录下的所有可执行文件：

```
查找文件 C:\Program\Files\CA\AccessControl\bin\*.exe
```

示例：在 UNIX 上查找与某种模式匹配的文件

以下命令可列出 CA Access Control bin 目录下以字母 *se* 开头的所有文件：

```
find file /opt/CA/AccessControl//bin/se*
```

join 命令 — 将用户添加至本地组

在本地环境中有效

join 命令可将用户添加到组中。 必须已针对本地操作系统定义的指定用户和组。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

要使用 join 命令，以下条件至少有一条成立：

- 您在您的 CA Access Control 用户记录中具有 ADMIN 属性。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是数据库中该条组记录的所有者。
- 您在 ADMIN 类的 GROUP 记录的访问控制列表中具有 JOIN 或 MODIFY 的访问权限。

注意：如果 ADMIN 要拥有修改 CA Access Control GROUP 记录和本地组的权限，则要求必须同时拥有 MODIFY 和 JOIN 属性。

此命令有以下格式：

```
{join|j} userName group(groupName)
```

group(*groupName*)

指定将用户添加到的本地组。

userName

指定连接到由 group 参数指定的组的本地用户的用户名。 当指定多个用户时，请将用户名括在括号中，并用空格或逗号分隔这些用户名。

示例

用户 Eli 想将用户 Bob 加入组“staff”。

- Eli 具有 ADMIN 属性，且当前环境为*本地*。

```
join Bob group(staff)
```

更多信息：

join- 命令 — 从本地组中删除用户 (p. 163)
showgrp 命令 —显示本地组属性 (p. 167)
showusr 命令 — 显示本地用户属性 (p. 168)
join[x] 命令 — 将用户添加至内部组 (p. 115)

join- 命令 — 从本地组中删除用户

在本地环境中有效

join- 命令可从组中删除用户。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

要使用 join- 命令，必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是数据库中该条组记录的所有者。
- 您在 ADMIN 类的 GROUP 记录的访问控制列表中具有 JOIN 或 MODIFY 的访问权限。

如果您只具有用户配置文件的所有权，那么您不具有足够权限即可从组中删除用户。 如果 ADMIN 要拥有修改 CA Access Control 记录和本地组的权限，则要求必须同时拥有 MODIFY 和 JOIN 属性。

此命令有以下格式：

```
{join-|j-} userName group(groupName)
```

group(*groupName*)

指定要从中删除用户的本地组。

userName

指定要从组中删除的用户的用户名。 从组中删除多个用户时，请用括号将用户名列表括起，并用空格或逗号分隔用户名。

示例

用户 Bill 想要从 PAYROLL 组中删除用户 sales25 和 sales43。

- 用户 Bill 具有 ADMIN 属性，且当前环境为*本地*。

```
join- (sales25 sales43) group(PAYROLL)
```

更多信息：

join 命令 — 将用户添加至本地组 (p. 162)
showgrp 命令 —显示本地组属性 (p. 167)
showusr 命令 — 显示本地用户属性 (p. 168)
join[x]- 命令 — 从组中删除用户 (p. 118)

newgrp 命令 — 创建 UNIX 组

在本地 UNIX 环境中有效

此命令与 chgrp 命令一起说明。

更多信息：

chgrp 命令 — 修改 UNIX 组 (p. 157)

newusr 命令 — 创建 UNIX 用户

在本地 UNIX 环境中有效

此命令与 chusr 命令一起说明。

更多信息：

chusr 命令 — 修改 UNIX 用户 (p. 158)

rmgrp 命令 — 删除 UNIX 组

在本地 UNIX 环境中有效

rmgrp 命令可从 UNIX 系统中删除一个或多个组。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

注意：在配置设置 (seos.ini) 中指定的文件内对组进行读取、添加、更新和删除；默认情况下，此文件为 /etc/group。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

此命令有以下格式：

`{rmgrp|rg}` *groupName*

groupName

指定要删除的组的名称。该组名必须是当前的 UNIX 组名。可指定一个或多个组名。 删除多个组时，请用括号将组名列表括起，并用空格或逗号分隔组名。

更多信息：

chgrp 命令 — 修改 UNIX 组 (p. 157)
showgrp 命令 —显示本地组属性 (p. 167)
rm[x]grp 命令 — 删除组记录 (p. 123)

rmusr 命令 — 删除 UNIX 用户

在本地 UNIX 环境中有效

rmusr 命令可从 UNIX 系统中删除一个或多个用户。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

注意：在配置设置 (seos.ini) 中指定的文件内对用户进行读取、添加、更新和删除；默认情况下，此文件为 /etc/passwd。 有关详细信息，请参阅 *《端点管理指南：用于 UNIX》*。

此命令有以下格式：

```
{rmusr|ru} userName
```

userName

指定现有 UNIX 用户的用户名。 删除多个用户时，请用括号将用户名列表括起，并用空格或逗号分隔用户名。

更多信息：

chusr 命令 — 修改 UNIX 用户 (p. 158)
showusr 命令 — 显示本地用户属性 (p. 168)
rm[x]usr 命令 — 删除用户记录 (p. 125)

showfile 命令 — 显示本地文件属性

在本地环境中有效

showfile 命令可列出一个或多个系统文件的本地详细信息。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{showfile|sf} fileName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

文件名

指定要列出其详细信息的文件的名称。可输入一个或多个 UNIX 文件名。 当指定多个文件时，请用括号将文件名列表括起，并用空格或逗号分隔各个文件名。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

示例：显示 UNIX 文件的详细信息

要列出 UNIX 文件 /tmp/foo 的详细信息。

```
showfile /tmp/foo
```

示例：显示 Windows 文件的所有者

您想知道 Windows 文件 C:\tmp\foo.exe 的所有者是谁。

```
showfile C:\tmp\foo.exe props(Owner)
```

更多信息：

chfile 命令 — 修改 UNIX 文件设置 (p. 156)
chfile 命令 — 修改 Windows 文件设置 (p. 172)
showfile 命令 — 显示文件属性 (p. 136)

showgrp 命令 —显示本地组属性

在本地环境中有效

showgrp 命令可显示本地操作系统中的一个或多个组的详细信息。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

注意：在 UNIX 上，在配置设置 (seos.ini) 中指定的文件内对组进行读取、添加、更新和删除；默认情况下，此文件为 /etc/group。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

此命令有以下格式：

```
{showgrp|sg} groupName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

groupName

指定要显示其详细信息的组的名称。该组名必须是现有的本地组名。可指定一个或多个组名。列出多个组时，请用括号将组名列表括起，并用空格或逗号分隔组名。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

示例

当您处于 *Unix* 环境中时，要列出 UNIX 组 *security* 的详细信息，请输入以下命令：

```
showgrp security
```

更多信息：

chgrp 命令 — 修改 UNIX 组 (p. 157)
chgrp 命令 — 修改 Windows 组 (p. 173)
show[x]grp 命令 — 显示组属性 (p. 138)

showusr 命令 — 显示本地用户属性

在本地 UNIX 环境中有效

showusr 命令可显示本地操作系统中的一个或多个用户的属性。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

注意：在 UNIX 上，在配置设置 (seos.ini) 中指定的文件内对用户进行读取、添加、更新和删除；默认情况下，此文件为 /etc/passwd。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

此命令有以下格式：

```
{showusr|su} userName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

userName

指定要显示其本地属性的用户的名称。 指定现有的本地用户名。 列出多个用户的属性时，请用括号括起用户名列表，并用空格或逗号分隔用户名。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

示例

当您处于 *Unix* 环境中时，要列出 UNIX 用户 *leslie* 的详细信息，请输入以下命令：

```
showusr leslie
```

更多信息：

chusr 命令 — 修改 UNIX 用户 (p. 158)
chusr 命令 — 修改 Windows 用户 (p. 178)
show[x]usr 命令 — 显示用户属性 (p. 142)

本地 Windows 环境中的 selang 命令

本节包含在本地 Windows 环境中执行的所有 selang 命令的完整参考，这些命令按字母顺序排列。

authorize 命令 — 设置访问者对 Windows 资源的访问权限

在本地 Windows 环境中有效

authorize 命令可维护有权访问特定资源的用户和组的列表。 使用 authorize，可以将列表更改为：

- 允许特定的 CA Access Control 用户或组访问资源。
- 禁止特定的 CA Access Control 用户或组访问资源。
- 更改特定用户或组对资源的访问权限的级别。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

下列 Windows 环境中的类支持 ACL，并且可通过 authorize 命令对这些类进行控制。

- COM
- DISK
- FILE
- PRINTER
- REGKEY
- SHARE

未显示在以上列表中的类没有访问控制列表，所以不能通过 authorize 命令对其进行控制。

此命令有以下格式：

```
{authorize|auth} className resourceName \
    [access(accessValue)|deniedaccess(accessvalue)] \
    [gid(groupName, ...)] \
    [uid(userName, ...)]
```

access(*accessValue*)

对于您在 uid 或 gid 参数中标识的访问者，指定希望其对资源所具有的访问权限。

className

指定 *resourceName* 所属的类的名称。

deniedaccess(*accessvalue*)

对于您在 uid 或 gid 参数中标识的访问者，指定希望其对资源所具有的否定访问权限。

拒绝的 accessvalue 可以是：all、create、delete、join、modify、none、password 或 read。

注意：只能将 *accessValue* 用于 authorize 命令，而不能将其用于 authorize- 命令。

gid(*groupName*)

指定要设置其资源访问权限的 Windows 组。值 groupName 表示一个或多个 Windows 组的名称。 指定多个组时，请用空格或逗号分隔组名。

resourceName

要修改或添加的资源记录的名称。 当更改或添加多个资源时，请将资源名称的列表括在括号中，并用空格或逗号分隔这些资源名称。必须至少指定一个资源名称。

CA Access Control 将根据指定的参数分别处理每个资源记录。如果处理资源时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个资源。

uid(*userName*)

指定要设置其资源访问权限的 Windows 用户。*userName* 是一个或多个 Windows 用户的用户名。 当指定多个用户时，请使用空格或逗号来分隔用户名。 要指定在 Windows 中定义的所有用户，请将 *userName* 指定为星号 (*)。

更多信息：

authorize- 命令 — 删除访问者对 Windows 资源的访问权限 (p. 171)
chfile 命令 — 修改 Windows 文件设置 (p. 172)
chgrp 命令 — 修改 Windows 组 (p. 173)
chres 命令 — 修改 Windows 资源 (p. 175)
chusr 命令 — 修改 Windows 用户 (p. 178)
authorize 命令 - 设置对资源的访问权限 (p. 43)
Windows 访问权限（按类） (p. 30)

authorize- 命令 — 删除访问者对 Windows 资源的访问权限

在本地 Windows 环境中有效

authorize- 命令可通过从标准访问控制列表中删除访问者来删除对资源的访问权限。 这样将保留默认的访问权限，从而确定访问者是否能够访问特定的资源。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{authorize-|auth-} className resourceName \
    [gid(groupName, ...)] \
    [uid(userName, ...)]
```

className

指定 *resourceName* 所属的类的名称。

gid(*groupName*)

指定要设置其资源访问权限的 Windows 组。值 groupName 表示一个或多个 Windows 组的名称。 指定多个组时，请用空格或逗号分隔组名。

resourceName

指定要修改或添加的资源记录的名称。 当更改或添加多个资源时，请将资源名称的列表括在括号中，并用空格或逗号分隔这些资源名称。 必须至少指定一个资源名称。

CA Access Control 将根据指定的参数分别处理每个资源记录。如果处理资源时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个资源。

uid(*userName*)

指定要设置其资源访问权限的 Windows 用户。*userName* 是一个或多个 Windows 用户的用户名。 当指定多个用户时，请使用空格或逗号来分隔用户名。 要指定在 Windows 中定义的所有用户，请将 *userName* 指定为星号 (*)。

更多信息：

authorize 命令 — 设置访问者对 Windows 资源的访问权限 (p. 169)
chfile 命令 — 修改 Windows 文件设置 (p. 172)
chgrp 命令 — 修改 Windows 组 (p. 173)
chres 命令 — 修改 Windows 资源 (p. 175)
chusr 命令 — 修改 Windows 用户 (p. 178)
authorize- 命令 - 从资源删除访问权限 (p. 47)

chfile 命令 — 修改 Windows 文件设置

在本地 Windows 环境中有效

chfile 和 editfile 命令是相同的。 它们可修改一个或多个 Windows 文件。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

对于 NTFS 文件系统，该命令具有以下格式：

```
{{chfile|cf}|{editfile|ef}} fileName \
    [attrib(attributeValue)] \
    [attrib(-attributeValue)] \
    [defaccess(accessValue)] \
    [owner(userName|groupName)]
```

对于 FAT 文件系统，该命令具有以下格式：

```
{{chfile|cf}|{editfile|ef}} fileName \
    [attrib([-]attributeValue)]
```

attrib([-]*attributeValue*)

指定用于确定文件特征的一组属性。当参数 *value* 前面有减号 (-) 时，该参数将删除该属性。

defaccess(*accessValue*)

指定本地安全内置组 Everyone 的访问权限。 所有系统用户都是 Everyone 组的成员。除了所有经过身份验证的用户以外，为 Everyone 组提供访问权限还将包括所有潜在的匿名用户。

注意：对于在 CA Access Control 环境中定义的对象，Defaccess 具有不同的含义；对于不在资源的 CA Access Control 列表中但请求访问该资源的任何访问者，将授予默认访问权限。 对于未在 CA Access Control 中定义的用户，也将授予默认访问权限。

defaccess 参数仅适用于 NTFS 文件系统。

owner(*userName*|*groupName*)

将某个用户或组指定为文件记录的所有者。 文件记录的所有者拥有对该文件的无限制访问权限。 文件的所有者始终可以更新或删除该文件记录。

更多信息：

showfile 命令 — 显示本地文件属性 (p. 165)
chfile 命令 - 修改文件记录 (p. 54)
Windows 文件属性 (p. 449)

chgrp 命令 — 修改 Windows 组

在本地 Windows 环境中有效

使用 chgrp、editgrp 和 newgrp 命令处理 Windows 组。 这些命令结构相同，仅在以下方面有所不同：

- chgrp 命令*修改*一个或多个 Windows 组。
- editgrp 命令*创建或修改*一个或多个 Windows 组。
- chgrp 命令*创建*一个或多个 Windows 组。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

当定义多个组或更改多个组的属性时，请将组名列表括在括号中，并用空格或逗号分隔这些组名。

注意：要向组中添加成员或从组中删除成员，请使用 join 或 join- 命令。

此命令有以下格式：

```
{{chgrp|cg}|{editgrp|eg}|{newgrp|ng}} groupName \
    [global] \
    [comment(string)|comment-] \
    [privileges(privList)] \
    [privileges(-privList)] \
    [rename_group]
```

comment(*string*)

向组记录中添加最多为 255 个字符的字母数字注释字符串。 如果以前向组记录中添加了备注字符串，则此处指定的新字符串将替换当前的字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

安装系统时，标准 Windows 组会添加一个说明性备注。 如果同时在 Windows 和 AC 环境中创建一个新组，CA Access Control 将插入注释“CA Access Control 组”。

global

指出全局组。 每个组名必须唯一，并且当前不能存在于 Windows 数据库中。 Windows 不允许组和用户使用同一名称。

注意：创建全局组并使用 CA Access Control 4.1 版的服务时，请使用 *~groupName*。 为了向后兼容，4.1 版及更高版本均支持这种格式。

groupName

对于命令 newgrp，指定添加到数据库中的组记录的名称。 每个组名必须唯一，并且当前不能存在于 Windows 数据库中。 与 CA Access Control 数据库不同，Windows 不允许组和用户使用同一名称。

对于命令 chgrp，指定您要更改其属性的组的名称。

当定义多个组或更改多个组的属性时，请将组名列表括在括号中，并用空格或逗号分隔这些组名。

privileges(*privList*|*-privList*)

向 Windows 组记录中添加特定权限，或者，当 privList 前面带有减号 (-) 时，删除该指定的权限。 有效值为本机 Windows 中的任何可用权限。

只能使用 chgrp 或 editgrp 命令来指定该参数，并且只有在更改当前组记录时才能指定。 新建组记录时，不能使用它来分配权限。

rename_group

重命名 Windows 数据库中的组帐户。 旧组名的所有属性均适用于重命名的组帐号。 每个组名必须唯一，并且必须存在于 Windows 数据库中。与 CA Access Control 数据库不同，Windows 不允许组和用户使用同一名称。

注意：在带有 Active Directory 的 Windows 2000 上安装 CA Access Control 时， CA Access Control 会重命名以前的 Windows 2000 组名。

chres 命令 — 修改 Windows 资源

在本地 Windows 环境中有效

在 Windows 环境中使用 chres、editres 和 newres 命令处理属于 CA Access Control 类的资源的资源记录。 这些命令结构相同，仅在以下方面有所不同：

- chres 命令可*修改*一个或多个资源。
- editres 命令可*创建或修改*一个或多个资源。
- newres 命令可*创建*一个或多个资源。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令具有以下格式：

```
{{chres|cr}|{editres|er}|{newres|nr}} className resourceName \
    [comment(string)|comment-] \
    [defaccess(accessValue)] \
    [dword(integer)|string(string)|binary(hexastring)|multistring(string)] \
    [location(string)|location()] \
    [maxusers(integer)] \
    [owner(userName|groupName)] \
    [share_name(string)|sharename-]
```

或

```
{{chres|cr}|{editres|er}|{newres|nr}} \
    DOMAIN resourceName \
    [computer(workstationName)|computer-(workstationName)] \
    [domainpwd(connectPassword)] \
    [trusted(domainName)|trusted-(domainName)]
```

binary(*hexastring*)

如果注册表键的值是十六进制，则指定该值。

className

指定 *resourceName* 所属的类的名称。

对于 newres 命令，有效值为：REGKEY、REGVAL、OU 和 SHARE。 对于 chres 和 editres 命令，有效值为：COM、DISK、DOMAIN、FILE、PRINTER、REGKEY、REGVAL、SERVICE、DEVICE、SESSION、OU 和 SHARE。

comment(*string*)

向资源记录中添加注释字符串。 如果以前向资源记录添加了备注字符串，则此处指定的新字符串将替换当前的字符串。 该参数只对 SHARE 和 PRINTER 资源有效。

computer(*workstationName*)|computer-(*workstationName*)

指定要向域添加的工作站的名称，或者，如果该参数前面带有减号，则指定要从域中删除的工作站的名称。 该参数只能用于 DOMAIN 资源。 您只能用 chres 或 editres 命令来指定该参数。

defaccess(*accessValue*)

指定本地安全内置组 Everyone 的访问权限。 所有系统用户都是 Everyone 组的成员。除了所有经过身份验证的用户以外，为 Everyone 组提供访问权限还将包括所有潜在的匿名用户。

注意：对于在 CA Access Control 环境中定义的对象，Defaccess 具有不同的含义；对于不在资源的 CA Access Control 列表中但请求访问该资源的任何访问者，将授予默认访问权限。 对于未在 CA Access Control 中定义的用户，也将授予默认访问权限。

defaccess 参数仅适用于 NTFS 文件系统。

domainpwd(*connectPassword*)

指定管理员在更改信任关系时必须输入的密码。

该参数只能用于 DOMAIN 资源。 您只能用 chres 或 editres 命令来指定该参数。

dword(*integer*)

如果注册表键的值为整数，则指定该值。

gen_prop(*propertyName*)

指定 OU 类的属性。

该参数只对 OU 类有效。

gen_value(*valueName*)

指定 OU 类的属性值。

该参数只对 OU 类有效。

location(*string*)

指明打印机的位置。 使用包含空格的 ( ) 可删除该属性。

该参数只对 PRINTER 资源有效。

maxusers(*integer*)

指定可以同时连接到共享目录的最大用户数 (*integer*)。

该参数只对 SHARE 资源有效。

multistring(*string*)

如果注册表键的值是多字符串，则指定该值。

owner(*userName*|*groupName*)

将某个用户或组指定为资源记录的所有者。 资源记录的所有者对该资源拥有无限制的访问权限。 资源的所有者始终可以更新和删除资源记录。 有关详细信息，请参阅*《端点管理指南：用于 Windows》*。

对于 FAT 文件系统上的 FILE 或 SHARE 记录，不能指定 owner 参数。此外，该参数对于 DEVICE、DOMAIN、OU、PROCESS、REGVAL、SERVICE 和 SESSION 资源也无效。

resourceName

要修改或添加的资源记录的名称。 当更改或添加多个资源时，请将资源名称的列表括在括号中，并用空格或逗号分隔这些资源名称。必须至少指定一个资源名称。

CA Access Control 将根据指定的参数分别处理每个资源记录。如果处理资源时发生错误，CA Access Control 将发出一条消息，并继续处理列表中的下一个资源。

share_name(*shareName*)|share_name-

标识打印机的共享点。

该参数只对 PRINTER 资源有效。

string(*string*)

如果注册表键的值为字符串，则指定该值。

trusted(*domainName*) | trusted-(*domainName*)

指定要向可信任的域添加的域的名称，或者，如果该参数前面带有减号，则指定要取消信任的域的名称。 该参数只能用于 DOMAIN 资源。 您只能用 chres 或 editres 命令来指定该参数。

更多信息：

rmres 命令 — 删除 Windows 资源 (p. 189)
showres 命令 — 显示本地资源属性 (p. 194)
chres 命令 - 修改资源记录 (p. 72)

chusr 命令 — 修改 Windows 用户

在本地 Windows 环境中有效

使用 chgusr、editusr 和 newusr 命令处理 Windows 用户。 这些命令结构相同，仅在以下方面有所不同：

- chgrp 命令*修改*一个或多个 Windows 用户。
- editusr 命令*创建或修改*一个或多个 Windows 用户。
- newusr 命令*创建*一个或多个 Windows 用户。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{{chusr|cu}|{editusr|eu}|{newusr|nu}} userName \
    [comment(string)|comment-] \
    [country(string)] \
    [expire|expire(mm/dd/yy[@hh:mm])|expire-] \
    [flags{(accountFlags)|-(accountFlags)}] \
    [full_name(fullName)] \
    [homedir(homeDir)] \
    [homedrive(homeDrive)] \
    [location(string)] \
    [logonserver(serverName)] \
    [organization(name)] \
    [org_unit(name)] \
    [password(password)] \
    [pgroup(primaryGroup)] \
    [phone(string)] \
    [privileges(privList)] \
    [profile(path)] \
    [restrictions( \
        days({[mon] [tue] [wed] [thu] [fri] [sat] [sun]}|anyday|weekdays) \
        time(startTime:endTime|anytime))]\
    [restrictions-] \
    [resume[(date)]|resume-} \
    [script(logonScriptPath)] \
    [suspend[(date)] | suspend-] \
    [terminals(terminalList)|terminals-(terminalList)] \
    [workstations(workstationList)|workstations-(workstationList)|workstation
    s-]
```

comment(*string*)|comment-

为用户记录指定注释字符串。

该参数是最多为 255 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

country(*string*)

指定用户所在的国家/地区。 在授权过程中不使用该字符串。

该参数是最多为 19 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

expire|expire(*mm/dd/yy[@hh:mm*) | expire-

设置用户帐号的过期日期。 如果未指定日期，那么，当用户当前并未登录时，用户帐号会立即过期。 如果用户已经登录，则帐户在用户注销时到期。

expire- 参数与 newusr 命令一起使用可定义没有过期日期的用户帐户。 对于 chusr 和 editusr 命令，该参数可从指定的用户帐号中删除过期日期。

date 参数的格式为：*mm/dd/*yy [@hh:mm]。

flags(*accountFlags*|- *accountFlags*)

指定用户帐号的特定属性。 有关有效标志值的列表，请参阅附录 “Windows 值”。

要从用户记录中删除标志，请在 *accountFlags* 前面添加减号 (-)。

full_name(*fullName*)

指定与用户记录相关联的用户的全名。

该参数是最多为 256 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

gecos(*string*)

为用户指定注释字符串，例如该用户的全名。 用单引号将字符串引起。

homedir(*homeDir*)

指定用户的主目录。 用户自动登录到自己的主驱动器和主目录。

homedrive(*homeDrive*)

指定用户主目录的驱动器。 用户自动登录到自己的主驱动器和主目录。

location(*string*)

指定用户的位置。 在授权过程中不使用该字符串。

该参数是最多为 19 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

logonserver(*serverName*)

指定验证用户的登录信息的服务器。 当用户登录到域工作站时，CA Access Control 会将登录信息传输到服务器，该服务器将为该用户授予工作所需的工作站权限。

organization(*name*)

指定用户工作的组织。 授权过程中不使用该信息。

该参数是最多为 256 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

org_unit(*name*)

指定用户在其中工作的组织机构。 授权过程中不使用该信息。

该参数是最多为 256 个字符的字母数字字符串。 如果字符串中包含任何空格，请用单引号将整个字符串引起。

password(*password*)

为用户分配密码。 如果启用了密码检查，那么该密码只对于一次登录有效。 用户下次登录系统时，必须设置新密码。

该参数是最多为 14 个字符的字符串，并且不能包含空格或逗号。 如果启用了密码检查，那么该密码只对于一次登录有效。 用户下次登录系统时，必须设置新密码，除非您设置了“密码永不到期”的标志。

要更改自己的密码，您需要使用 *setoptions cng_ownpwd* 或使用 sepass 设置 selang 选项。

如果您正在为 Windows NT 系统上的用户设置密码，则可能出现下列消息：

密码太短，不符合要求。

该错误表明密码不符合策略要求。 这可能是由以下任何一种原因造成的：

- 该密码短于或长于要求长度。
- 该密码最近已被使用，并存在于“Windows NT 更改历史记录”字段中。
- 该密码没有足够多的唯一字符。
- 该密码不符合其他密码策略要求（例如通过 CA Access Control 密码策略设置的要求）。

为了避免该错误，请确保设置符合所有相关要求的密码。

pgroup(*primaryGroup*)

设置用户的主组 ID。 主组是用于定义用户的组之一，必须是全局组。

该参数是最多为 14 个字符的字符串，并且不能包含空格或逗号。

phone(*string*)

指定用户的电话号码。 授权过程中不使用该信息。

privileges(*privList*)

向 Windows 用户记录添加特定权限，或者，如果 *privList* 前面带有减号 (-)，则可删除指定的权限。 您只能用 chusr 或 editusr 命令来指定该参数，并且只能在更改当前用户记录时指定。 创建新的用户记录时，不能使用它来分配权限。

profile(*path*)

为桌面环境（程序组、网络连接）指定包含用户配置文件的文件的完整路径位置。 每当用户登录到任何工作站时，都在屏幕上显示相同的环境。

restrictions([*days*] [*time*])|restrictions-([*days*] [*time*])

指定用户可以在一周的哪几天以及一天的哪些时间访问文件。

如果省略 days 参数而指定 time 参数，则时间限制将应用于记录中已经指出的任何“工作日”限制。 如果省略 time 而指定 days，则日期限制将应用于记录中已经指出的任何时间限制。 如果同时指定了 days 和 time，则用户只能在指定日期的指定时间段内访问系统。

- [Days] 指定用户可以访问文件的日期。 days 参数可使用下列子参数：
  - **anyday** - 允许用户在任何日期访问文件。
- **weekdays** - 仅允许用户在工作日（星期一至星期五）访问资源。
  - **Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**、**Sun** - 仅允许用户在指定的日期访问资源。 您可以按任何顺序指定日期。 如果指定了多个日期，请用空格或逗号分隔这些日期。
- [Time] 指定用户可以访问资源的时间段。 time 参数可使用下列子参数：
  - **anytime** - 允许用户在一天中的任何时间访问资源。
  - **startTime:endTime** - 仅允许用户在指定的时间段内访问资源。 startTime 和 endTime 的格式均为 *hhmm*，其中 *hh* 是采用 24 小时表示法的小时（00 至 23），而 *mm* 是分钟（00 至 59）。 请注意，2400 是无效的时间值。 startTime 必须小于 endTime，并且这两个时间必须在同一天。 如果终端与处理器位于不同的时区，请通过将终端的开始时间和结束时间转换为等同的处理器本地时间来调整时间值。 例如，如果处理器位于纽约而终端位于洛杉矶，那么，要允许从上午 8:00 到下午 5:00 在洛杉矶访问终端，请指定时间 (1100:2000)。

resume(*date*)|resume-

Windows 恢复用户帐户的日期和（可选）时间。如果同时指定 suspend 参数和 resume 参数，请确保恢复日期在挂起日期之后或用户将无限期地处于挂起状态。

按照下面的格式输入日期和（可选）时间：

```
mm/dd/yy[@HH:MM]
```

使用 resume- 参数可将用户帐号的状态从“活动”（启用）更改为“挂起”。 该参数只能与 chusr 或 editusr 命令一起使用。

script(*loginScriptPath*)

指定用户登录时自动运行的文件的位置。 该登录脚本对工作环境进行配置。 由于 profile 参数也可对用户的工作环境进行设置，因此该参数是可选的。

suspend(*date*)|suspend-

禁用用户帐号。 用户不能使用挂起的用户帐号登录系统。 如果指定 date，Windows 将在指定日期挂起用户帐号。如果忽略 date，Windows 将在执行 chusr 命令后立即挂起用户帐户。

用以下格式输入日期和（可选）时间：*mm /dd/yy[@HH:MM]*。

使用 suspend- 参数可将用户帐户的状态从“禁用”更改为“活动”（启用）。 该参数只能与 chusr 或 editusr 命令一起使用。

terminals(*terminalList*)|terminals-(*terminalList*)

最多指定八个可供用户用于登录的终端。 用引号将该列表引起，并用逗号分隔名称。 例如：

```
“terminal1,terminal2”
```

workstations(*workstationList*)|workstations-(*workstationList*)|workstations-

最多指定八个可供用户用于登录的工作站。 用引号将该列表引起，并用逗号分隔名称。 例如：

```
“workstation1,workstation2”
```

editfile 命令 — 修改 Windows 文件设置

在本地 Windows 环境中有效

此命令与 chfile 命令一起说明。

更多信息：

chfile 命令 — 修改 Windows 文件设置 (p. 172)

editgrp 命令 — 创建和修改 Windows 组

在本地 Windows 环境中有效

此命令与 chgrp 命令一起说明。

更多信息：

chgrp 命令 — 修改 Windows 组 (p. 173)

editusr 命令 — 创建和修改 Windows 用户

在本地 Windows 环境中有效

此命令与 chusr 命令一起说明。

更多信息：

chusr 命令 — 修改 Windows 用户 (p. 178)

editres 命令 — 创建和修改 Windows 资源

在本地 Windows 环境中有效

此命令与 chres 命令一起说明。

更多信息：

chres 命令 — 修改 Windows 资源 (p. 175)

find file 命令 — 列出本地文件

在本地环境中有效

使用 find file 命令列出与掩码（一个字符串）匹配的所有系统文件。 这些文件按照时间顺序排列在一列中。

此命令有以下格式：

```
find file [directory][/mask]
```

目录

列出目录 *directory* 中的所有文件。

mask

列出目录 *directory* 中与 *mask* 变量匹配的所有文件。 *mask* 可能会包括通配符字符。

示例：在 Windows 上特定路径中查找可执行程序文件

以下命令可列出 CA Access Control bin 目录下的所有可执行文件：

```
查找文件 C:\Program\Files\CA\AccessControl\bin\*.exe
```

示例：在 UNIX 上查找与某种模式匹配的文件

以下命令可列出 CA Access Control bin 目录下以字母 *se* 开头的所有文件：

```
find file /opt/CA/AccessControl//bin/se*
```

find {xuser|xgroup} 命令 – 列出企业用户或组

在本地 Windows 环境中有效

find {xuser|xgroup} 命令可列出当前或*受托*域中的企业用户或组的名称。

注意：该命令仅在带 Directory Services 的 Windows 2000 操作系统上受支持。

此命令有以下格式：

```
find {xuser|xgroup} mask [domain(domainName)] [next]
```

xgroup

指定该命令返回的企业组。

xuser

指定该命令返回的企业用户。

domain(*domainName*)

定义受托域以限制搜索返回目标。

如果未指定该选项，则该命令将返回当前域中的用户。

mask

为企业用户定义掩码。

下一个

指定 selang 输出是否应继续列出由先前的 find xuser 或 find xgroup 命令启动的企业用户或组。

如果列表中的项目超过 100 个，则使用该选项。

示例：显示企业用户

以下命令列出了当前域中以 abc 开头的前 100 个企业用户：

```
find xuser abc*
```

join 命令 — 将用户添加至本地组

在本地环境中有效

join 命令可将用户添加到组中。 必须已针对本地操作系统定义的指定用户和组。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

要使用 join 命令，以下条件至少有一条成立：

- 您在您的 CA Access Control 用户记录中具有 ADMIN 属性。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是数据库中该条组记录的所有者。
- 您在 ADMIN 类的 GROUP 记录的访问控制列表中具有 JOIN 或 MODIFY 的访问权限。

注意：如果 ADMIN 要拥有修改 CA Access Control GROUP 记录和本地组的权限，则要求必须同时拥有 MODIFY 和 JOIN 属性。

此命令有以下格式：

```
{join|j} userName group(groupName)
```

group(*groupName*)

指定将用户添加到的本地组。

userName

指定连接到由 group 参数指定的组的本地用户的用户名。 当指定多个用户时，请将用户名括在括号中，并用空格或逗号分隔这些用户名。

示例

用户 Eli 想将用户 Bob 加入组“staff”。

- Eli 具有 ADMIN 属性，且当前环境为*本地*。

```
join Bob group(staff)
```

更多信息：

join- 命令 — 从本地组中删除用户 (p. 163)
showgrp 命令 —显示本地组属性 (p. 167)
showusr 命令 — 显示本地用户属性 (p. 168)
join[x] 命令 — 将用户添加至内部组 (p. 115)

join- 命令 — 从本地组中删除用户

在本地环境中有效

join- 命令可从组中删除用户。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

要使用 join- 命令，必须满足下列条件之一：

- 您具有 ADMIN 属性。
- 该组记录在您具有 GROUP-ADMIN 属性的组范围内。
- 您是数据库中该条组记录的所有者。
- 您在 ADMIN 类的 GROUP 记录的访问控制列表中具有 JOIN 或 MODIFY 的访问权限。

如果您只具有用户配置文件的所有权，那么您不具有足够权限即可从组中删除用户。 如果 ADMIN 要拥有修改 CA Access Control 记录和本地组的权限，则要求必须同时拥有 MODIFY 和 JOIN 属性。

此命令有以下格式：

```
{join-|j-} userName group(groupName)
```

group(*groupName*)

指定要从中删除用户的本地组。

userName

指定要从组中删除的用户的用户名。 从组中删除多个用户时，请用括号将用户名列表括起，并用空格或逗号分隔用户名。

示例

用户 Bill 想要从 PAYROLL 组中删除用户 sales25 和 sales43。

- 用户 Bill 具有 ADMIN 属性，且当前环境为*本地*。

```
join- (sales25 sales43) group(PAYROLL)
```

更多信息：

join 命令 — 将用户添加至本地组 (p. 162)
showgrp 命令 —显示本地组属性 (p. 167)
showusr 命令 — 显示本地用户属性 (p. 168)
join[x]- 命令 — 从组中删除用户 (p. 118)

newgrp 命令 — 创建 Windows 组

在本地 Windows 环境中有效

此命令与 chgrp 命令一起说明。

更多信息：

chgrp 命令 — 修改 Windows 组 (p. 173)

newres 命令 — 创建 Windows 资源

在本地 Windows 环境中有效

此命令与 chres 命令一起说明。

更多信息：

chres 命令 — 修改 Windows 资源 (p. 175)

newusr 命令 — 创建 Window 用户

在本地 Windows 环境中有效

此命令与 chusr 命令一起说明。

更多信息：

chusr 命令 — 修改 Windows 用户 (p. 178)

rmgrp 命令 — 删除 Windows 组

在本地 Windows 环境中有效

rmgrp 命令可从 Windows 数据库中删除一个或多个组。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{rmgrp|rg} groupName
```

groupName

指定要删除的组的名称。 该组名必须是当前的 Windows 组名。 可指定一个或多个组名。 删除多个组时，请用括号将组名列表括起，并用空格或逗号分隔组名。

rmres 命令 — 删除 Windows 资源

rmres 命令可从 Windows 系统数据库中删除一个或多个资源。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{rmres|rr} className resourceName
```

className

指定资源所属的类的名称。

resourceName

指定 *className* 类的现有 Windows 资源名称。 删除多个资源时，请用括号将用户名列表括起，并用空格或逗号分隔用户名。

更多信息：

chres 命令 — 修改 Windows 资源 (p. 175)
showres 命令 — 显示本地资源属性 (p. 194)
rm[x]usr 命令 — 删除用户记录 (p. 125)

rmusr 命令 — 删除 Windows 用户

在本地 Windows 环境中有效

rmusr 命令可从 Windows 系统数据库中删除一个或多个用户。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{rmusr|ru} userName
```

userName

指定现有 Windows 用户的用户名。 删除多个用户时，请用括号将用户名列表括起，并用空格或逗号分隔用户名。

更多信息：

chusr 命令 — 修改 Windows 用户 (p. 178)
showusr 命令 — 显示本地用户属性 (p. 168)
rm[x]usr 命令 — 删除用户记录 (p. 125)

setoptions 命令 — 设置 CA Access Control Windows 选项

setoptions 命令自动设置与 Windows 操作系统相关的系统范围的 CA Access Control 选项。

注意：此命令同样存在于 AC 环境中，但操作方式有所不同。

需要具有 ADMIN 属性才能使用 setoptions 命令，但存在例外情况 - 只需具有 AUDITOR 或 OPERATOR 属性即可使用命令 setoptions 列表。

此命令有以下格式：

```
setoptions|so \
    [audit_policy( \
        [success(system|logon|access|rights \
                |process|security|manage)] \
        [failure(system|logon|access|rights \
                |process|security|manage)] \
    )]
    [password(
        [history(number-stored-passwords)]
        [interval(nDays)]
        [min_life(NDays)]
        )]
```

audit_policy{+|-}

指定是启用 (+) 还是禁用 (-) 审核。

audit_policy(success(system|logon|access|rights|process|security|manage))

指定记录哪些检测到的已授权访问事件。 访问类型包括：

- **system** - 尝试关闭或重新启动计算机。
- **logon** - 尝试登录系统或从系统注销。
- **access** - 尝试访问可获得对象（例如文件）。
- **rights** - 尝试使用 Windows Server 权限。
- **process** - 程序激活、某些形式的句柄重复、间接访问对象和进程退出等事件。
- **security** - 尝试更改策略对象规则。
- **manage** - 尝试创建、删除或更改用户帐户或组帐户。 同时，密码也会更改。

audit_policy(failure(system|logon|access|rights|process|security|manage))

指定记录哪些检测到的未授权访问事件。 访问类型包括：

- **system** - 尝试关闭或重新启动计算机。
- **logon** - 尝试登录系统或从系统注销。
- **access** - 尝试访问可获得对象（例如文件）。
- **rights** - 尝试使用 Windows Server 权限。
- **process** - 程序激活、某些形式的句柄重复、间接访问对象和进程退出等事件。
- **security** - 尝试更改策略对象规则。
- **manage** - 尝试创建、删除或更改用户帐户或组帐户。 同时，密码也会更改。

history(*number-stored-passwords*)

指定数据库中存储的以前使用的密码的数目。 提供新密码时，用户不能指定历史记录列表中存储的任何密码。*NStoredPasswords* 是介于 1 和 24 之间的整数。 如果指定为零，将不保存密码。

interval(*nDays*)

interval(nDays)设置在设置或更改密码后且在系统提示用户输入新密码之前必须经过的天数。

nDays 的值必须是正整数或零。如果时间间隔为零，则禁用对用户的密码时间间隔检查。 如果不希望密码过期，请将时间间隔设置为零。

min_life(*NDays*)

设置密码更改间隔的最小天数。 *NDays* 必须是正整数。

更多信息：

showfile 命令 — 显示文件属性 (p. 136)

showfile 命令 — 显示本地文件属性

在本地环境中有效

showfile 命令可列出一个或多个系统文件的本地详细信息。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

此命令有以下格式：

```
{showfile|sf} fileName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

文件名

指定要列出其详细信息的文件的名称。可输入一个或多个 UNIX 文件名。 当指定多个文件时，请用括号将文件名列表括起，并用空格或逗号分隔各个文件名。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

示例：显示 UNIX 文件的详细信息

要列出 UNIX 文件 /tmp/foo 的详细信息。

```
showfile /tmp/foo
```

示例：显示 Windows 文件的所有者

您想知道 Windows 文件 C:\tmp\foo.exe 的所有者是谁。

```
showfile C:\tmp\foo.exe props(Owner)
```

更多信息：

chfile 命令 — 修改 UNIX 文件设置 (p. 156)
chfile 命令 — 修改 Windows 文件设置 (p. 172)
showfile 命令 — 显示文件属性 (p. 136)

showgrp 命令 —显示本地组属性

在本地环境中有效

showgrp 命令可显示本地操作系统中的一个或多个组的详细信息。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

注意：在 UNIX 上，在配置设置 (seos.ini) 中指定的文件内对组进行读取、添加、更新和删除；默认情况下，此文件为 /etc/group。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

此命令有以下格式：

```
{showgrp|sg} groupName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

groupName

指定要显示其详细信息的组的名称。该组名必须是现有的本地组名。可指定一个或多个组名。列出多个组时，请用括号将组名列表括起，并用空格或逗号分隔组名。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

示例

当您处于 *Unix* 环境中时，要列出 UNIX 组 *security* 的详细信息，请输入以下命令：

```
showgrp security
```

更多信息：

chgrp 命令 — 修改 UNIX 组 (p. 157)
chgrp 命令 — 修改 Windows 组 (p. 173)
show[x]grp 命令 — 显示组属性 (p. 138)

showres 命令 — 显示本地资源属性

显示 Windows 资源的属性。

此命令有以下格式：

```
showres|sr className resourceName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

className

指定资源所属的类的名称。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

resourceName

指定 *className* 类的现有 Windows 资源名称。

showusr 命令 – 显示本地用户属性

在本地 UNIX 环境中有效

showusr 命令可显示本地操作系统中的一个或多个用户的属性。

注意：此命令同样存在于 AC 环境中，但操作有所不同。

注意：在 UNIX 上，在配置设置 (seos.ini) 中指定的文件内对用户进行读取、添加、更新和删除；默认情况下，此文件为 /etc/passwd。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

此命令有以下格式：

```
{showusr|su} userName [next] \
    [{props|addprops}(propNames)]
```

addprops(*propName*)

设置要显示的属性（标尺）。属性的列表将添加到当前标尺中。ruler 设置为仅用于本次查询，并将恢复到以前设置的 ruler。

userName

指定要显示其本地属性的用户的名称。 指定现有的本地用户名。 列出多个用户的属性时，请用括号括起用户名列表，并用空格或逗号分隔用户名。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

props(all|*propName*)

设置要显示的属性（标尺）。

该标尺仍对未来的查询有效。

示例

当您处于 *Unix* 环境中时，要列出 UNIX 用户 *leslie* 的详细信息，请输入以下命令：

```
showusr leslie
```

更多信息：

chusr 命令 — 修改 UNIX 用户 (p. 158)
chusr 命令 — 修改 Windows 用户 (p. 178)
show[x]usr 命令 — 显示用户属性 (p. 142)

xaudit 命令 — 修改系统 Access Control 列表

xaudit 命令可在系统访问控制列表 (SACL) 中添加项。 当指定用户或组尝试获取对资源的访问权限时，该列表中的每个项都会导致记录一条审核消息。 xaudit- 命令可从 SACL 中删除项，并且对资源类型 FILE、PRINTER、REGKEY、DISK、COM 或 SHARE 有效。

此命令有以下格式：

```
xaudit className resourceName \
    [failure(auditMode)]\
    [gid(groupName)] \
    [success(auditMode)] \
    [uid(userName)]
```

className

指定资源所属的资源类型的名称。

failure(*auditMode*)

记录尝试对资源进行的未经授权的访问。

auditmode 的有效值取决于它所属的资源类型：

注意：只有 NTFS 文件可以具有审核模式

- **DISK** 和 **COM**：changePermissions、delete、modify、query、read、synchronize、takeOwnership。
- **FILE**：changePermissions、delete、execute、read、takeOwnership 和 write。
- **PRINTER**：changePermissions、delete、print 和 takeOwnership。
- **REGKEY**：delete、enumerate、link、notify、queryValue、readControl、setValue、subkey 和 write。

对于所有资源类型：*none* 和 all。

gid(*groupName*)

指定正在审核其对资源的访问权限的组。 指定多个组时，请用空格或逗号分隔组名。

resourceName

指定正在修改其系统 Access Control 列表 (SACL) 的资源记录的名称。

success(*auditMode*)

记录对资源的授权访问。

auditmode 的有效值取决于它所属的资源类型：

注意：只有 NTFS 文件可以具有审核模式

- **DISK** 和 **COM**：changepermissions、delete、modify、query、read、synchronize、takeownership。
- **FILE**：changePermissions、delete、execute、read、takeOwnership 和 write。
- **PRINTER**：changePermissions、delete、print 和 takeOwnership。
- **REGKEY**：delete、enumerate、link、notify、queryValue、readControl、setValue、subkey 和 write。

对于所有资源类型：*none* 和 all。

uid(*userName*)

指定要审核其资源访问权限的用户。 如果指定多个用户，请用空格或逗号分隔用户名。 要指定在 Windows NT 数据库中定义的所有用户，请将 *userName* 指定为星号 (*)。

更多信息：

xaudit- 命令 — 删除系统 Access Control 列表 (p. 197)

xaudit- 命令 — 删除系统 Access Control 列表

xaudit- 命令可从 SACL 中删除项，并且对资源类型 FILE、PRINTER、REGKEY、DISK、COM 或 SHARE 有效。

此命令有以下格式：

```
xaudit- className, resourceName \
     [gid(groupName)] \
     [uid(userName)]
```

className

指定资源所属的资源类型的名称。

gid(*groupName*)

指定正在审核其对资源的访问权限的组。 指定多个组时，请用空格或逗号分隔组名。

resourceName

指定正在删除其系统 Access Control 列表 (SACL) 的资源记录的名称。

uid(*userName*)

指定要审核其资源访问权限的用户。 如果指定多个用户，请用空格或逗号分隔用户名。 要指定在 Windows NT 数据库中定义的所有用户，请将 *userName* 指定为星号 (*)。

更多信息：

xaudit 命令 — 修改系统 Access Control 列表 (p. 196)

策略模型环境中的 selang 命令

本节包含在策略模型环境中执行的所有 selang 命令的完整参考，这些命令按字母顺序排列。

backuppmd 命令 — 备份 PMDB

在 pmd 环境中有效

backuppmd 命令将 PMDB 数据库中的数据备份到指定的目录。 PMDB 数据库中的所有数据都进行备份，包括策略、部署信息和配置文件。

对于 DMS，该命令有以下格式：

```
backup pmdName destination(path)
```

对于 PMDB，该命令有以下格式：

```
backup pmdName [destination(path)|hir_host(name)]
```

destination(*path*)

定义您想存储备份文件的目录。

注意：如果您不指定路径，文件将会备份到在 *_pmd_backup_directory_* 标记中指定的默认位置。

默认值：(UNIX) *ACInstallDir*/data/policies_backup/pmdName

默认值：(Windows) *ACInstallDir*\data\policies_backup\pmdName

pmdName

定义要备份的 PMDB 或 DMS 的名称。

hir_host(*name*)

将一个层级结构中的所有 PMDB 备份到您指定的主机 *name* 并修改 PMDB 订户，从而当备份移到 *name* 主机时订阅仍可进行。

注意：仅当主 PMDB 和子 PMDB 部署在同一主机上时，才支持该命令。

createpmd 命令 — 在主机上创建 PMDB

在 pmd 环境中有效

createpmd 命令可在远程主机上定义 PMDB。 可将一个或多个用户指定为 PMDB 的管理员、审核者和密码管理员。 还可以定义 PMDB 的父 PMDB 和订阅者 PMDB。 可通过远程主机运行 createpmd 命令。

此命令有以下格式：

```
createpmd pmdname \
    [admins(user [user ...])] \
    [auditors(user [user ...])] \
    [pwman(user [user ...])] \
    [parentpmd(pmdname@host)] \
    [desktop(host-names...)] \
    [subscriber(host-names|pmdnames...)] \
    [pwdfile(file-name))] \
    [grpfile(file-name))] \
    [nis] \
    [xadmins(user [user ...])] \
    [xauditors(user [user ...])] \
```

admins(*user [user ...]*)

将一个或多个内部用户指定为 PMDB 管理员。用空格隔开多个用户。

auditors(*user [user ...]*)

指定可查看 PMDB 的审核文件的一个或多个内部用户。 用空格隔开多个用户。

pwmans(*user [user ...]*)

将一个或多个用户指定为 PMDB 密码管理员。用空格隔开多个用户。

parentpmd(*pmdname@host*)

指定您要创建的 PMDB 的父 PMDB 的名称。

注意：如果要使用 selang 远程命令定义多个父“策略模型”，您必须使用引号。 例如，要创建一个“策略模型”并定义其父项，请使用以下命令：

```
createpmd subs2 admins(abc123 root) auditors(abc123 root) desktop(pcp36949)
\
parentpmd("aa@pcp36949,bb@pcp36949")
```

desktop(*host [host ...]*)

指定一个或多个管理员可以用来管理 PMDB 的主机。 用空格隔开多个主机。 默认为新 PMDB 的主机。

subscribers(*host | pmd [host | pmd ...]*)

将主机或 PMDB 指定为新 PMDB 的订阅者。 用空格隔开多个主机或 PMDB。

pwdfile(*filename*)

指定 PMDB 密码文件。

grpfile(*filename*)

指定 PMDB 组文件。

nis

在新 PMDB 的主机上执行 NIS 安装，并创建筛选文件以筛选出所有 UNIX 更新。

xadmins(*user [user ...]*)

将一个或多个企业用户指定为 PMDB 管理员。用空格隔开多个用户。

xauditors(*user [user ...]*)

指定可查看 PMDB 的审核文件的一个或多个企业用户。 用空格隔开多个用户。

pwmans(*user [user ...]*)

将一个或多个企业用户指定为 PMDB 密码管理员。 用空格隔开多个用户。

deletepmd 命令 — 从主机删除 PMDB

在 pmd 环境中有效

deletepmd 命令可以从主机上删除以下项目：

- PMDB 的 selang 保护文件：
  - 数据库文件
  - 注册表项
- PMDB 目录的内容
- PMDB 目录

重要说明！ 要防止出现严重的操作问题，请避免通过手动删除 PMDB 文件来删除 PMDB。 请始终对 PMDB 使用 deletepmd 命令。

此命令有以下格式：

```
deletepmd pmdname
```

findpmd 命令 — 列出主机上的 PMDB

在 pmd 环境中有效

findpmd 命令可列出您连接到的主机中的 PMDB 及其后台程序是否已加载。

此命令有以下格式：

```
findpmd
```

listpmd 命令 – 列出有关 PMDB 的信息

在 pmd 环境中有效

listpmd 命令可列出有关 PMDB 及其订阅者、更新文件和错误日志的信息。 如果未使用任何选项，则该命令会列出策略模型 *pmdName* 的所有订阅者。

此命令有以下格式：

```
listpmd pmdName \
    [{info|subscriber(subNames)|cmd(offset) \
    |errors|all_errors|log}] \
    [next]
```

cmd*(offset)*

显示更新文件中的所有命令及其偏移量。

偏移量指明更新在文件中的位置。 如果指定了偏移量，列表将从偏移量开始显示。 如果未指定偏移量，列表将从更新文件的开头开始显示。

注意：更新文件包含的更新必须或者已经通过 PMDB 传播。 偏移量指明必须发送给订阅者的下一个更新的位置。 将显示更新文件的初始偏移量和最新偏移量。

errors|all_errors

显示策略模型错误日志。*errors* 参数显示除了非连接失败错误以外所有类型的错误。 *all_errors* 显示所有错误。

通知

显示有关策略模型 *pmdName* 的常规信息，包括策略模型是否有父项。

下一个

显示所请求的数据部分。 当查询数据大于设置的查询大小时，该选项非常有用。

最大查询大小由 query_size 配置设置确定。 查询大小默认值为 100。

pmdname

定义您要列出其信息的 PMDB 的名称。

subscriber(*subNames*)

列出策略模型的订阅者及其状态，包括错误数、可用性、偏移量以及要传播的下一个命令。通过 *subNames* 参数，您可以选择订阅者的子集。

日志

显示策略模型常规日志文件。

示例：显示选定订阅者的 PMDB 订阅者信息

要显示订阅以字母 *compInt* 开头的 myPMDB 策略模型的订阅者列表，请输入以下命令：

```
listpmd myPMDB subscriber(compInt*)
```

pmd 命令 – 控制 PMDB

在 pmd 环境中有效

pmd 命令可清除策略模型错误日志、更新订阅者列表、启动和停止策略模型服务，以及截短更新文件。

此命令有以下格式：

```
pmd pmdName \
    {[release(subname)|start|stop|truncate(offset)|lock|unlock \
    |reloadini|startlog|killog|clrerror|backup|operation]}
```

backup

将策略模型移动到备份状态。

clrerror|clrerr

清除策略模型错误日志。

killog

禁用策略模型常规日志文件。 如果您指定了此选项，则任何消息都无法写入日志中。

重要说明！ 不要使用 kill 命令关闭 PMDB 服务。

lock

将策略模型移到锁定状态，并让策略模型停止向其订户发送更新。

操作

将策略模型从备份状态移动到可操作状态。

pmdname

定义要对其执行所选选项的 PMDB 的名称。

release(*subName*)

从不可用订阅者列表中删除由 *subName* 指定的订阅者。 这表示该订阅者可以立即接收更新。 *subName* 指定将可以接收更新的订阅者。

reloadini

（仅适用于 UNIX）重新读取策略模型 pmd.ini 文件和 seos.ini 文件，通过这您可以更改配置设置而无需重新加载策略模型后台程序。

startlog

允许写入策略模型一般日志文件。 如果已经禁用日志文件，请使用此选项。

启动

启动 CA Access Control 策略模型服务。 当没有其他要执行的命令时，使用此选项。

停止

停止 CA Access Control 策略模型后台程序/服务。

truncate|trunc[(*offset*)]

从更新文件中删除项。 如果未指定 offset，将从最大可能偏移量处截短文件。 最大可能偏移量是成功更新订阅者的上一命令的位置。 如果指定了 *offset*，将删除指定偏移量前的所有条目。

注意：必须使用 *listpmd* 命令提供的真实偏移量来截短文件，而不是与开始偏移量相减而得出的偏移量。

解锁

将策略模型从锁定状态移到解锁状态，并允许策略模型将更新发送给其订户。

restorepmd 命令 — 还原 PMDB

在 pmd 环境中有效

restorepmd 命令还原本地主机上的 PMDB。 您用来还原 PMDB 的备份文件所源自的主机必须运行与还原主机相同的平台、操作系统和 CA Access Control 版本。 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，然后启动还原的 PMDB。

此命令有以下格式：

`restorepmd` *`pmdName`* `[source(`*`path`*`)] [admin(`*`user`*`)] [xadmin(`*`user`*`)] [parentpmd(`*`name`*`)]`

admin(*user*)

（UNIX）将内部用户定义为还原的 PMDB 的管理员。

pmdName

定义要还原的 PMDB 的名称。

parentpmd(*name*)

（可选）定义还原的 PMDB 父项的名称。 采用格式 *pmd@host* 指定名称。

source(*path*)

（可选）定义备份文件所在的目录。如果您不指定源目录，PMDB 会从默认位置的文件进行还原。默认位置在 *_pmd_backup_directory_* 标记中有所定义。

默认值：(UNIX) *ACInstallDir*/data/policies_backup/pmdName

默认值：(Windows) *ACInstallDir*\data\policies_backup\pmdName

xadmin(*user*)

（UNIX）将企业用户定义为还原的 PMDB 的管理员。

subs 命令 — 添加订阅者或订阅数据库

在 pmd 环境中有效

subs 命令将订阅者添加到父 PMDB 或将数据库订阅到父 PMDB。

为主机订阅 PMDB 时：

- 该主机必须已启动。
- CA Access Control 必须正在该主机上运行
- PMDB 必须是进行订阅的主机的父 PMDB。

为一个 PMDB 订阅另一个 PMDB 时：

- 被订阅 PMDB 的 parent_pmd 配置设置必须包含正在订阅的 PMDB（父 PMDB）的名称。
- CA Access Control 必须正在被订阅 PMDB 所在的主机上运行。

此命令有以下格式：

```
subs pmdname \
    [subs(subsname)] \
    [host_type(mfHost) sysid(sysID) mf_admin(mfAdmin) port(port)] \
    {offset(offset) }
```

或

```
subs pmdname [newsubs(subsname)]
```

或

```
subs pmdname [parentpmd(pmdname2@host)]
```

host_type(*mfhost*)

订阅者的大型主机类型。

mf_admin(*mfAdmin*)

订阅者的大型机管理员。

newsubs(*subsname*)

为策略模型 *pmdName* 订阅 *subName* 并将整个 PMDB 的内容、密码和组文件发送给新订阅者。

parentpmd(*pmdName2@host*)

将 PMDB *pmdName2@host* 作为 *pmdName* 的父策略模型。

pmdname

定义要对其执行所选选项的 PMDB 的名称。

port(*port*)

订阅者的端口号。

subs(*subsname*)

将订阅者分配到 PMDB。

sysid(*sysId*)

订阅者的系统 ID。

subspmd 命令 — 更改父 PMDB

在 pmd 环境中有效

subspmd 命令可更改您所连接到的主机中 CA Access Control 数据库的父项。

此命令有以下格式：

```
subspmd parentpmd(pmdname@host)
```

parentpmd(*pmdname@host*)

使 *pmdname@host* 成为当前主机的父策略模型。

unsubs 命令 — 删除订阅者

在 pmd 环境中有效

unsubs 命令可从策略模型的订阅者列表中删除订阅者。

此命令有以下格式：

```
unsubs pmdName subs(subName)
```

pmdname

定义要对其执行所选选项的 PMDB 的名称。

subs(*subName*)

定义要从 *pmdname* 订阅者列表中删除的订阅者姓名。

第 4 章： 类和属性

本节包含了在 CA Access Control 数据库和本地操作系统中定义的每个类各个属性的说明。 本章按类的字母顺序排列方式提供有关以下内容的信息：您可以修改哪些属性、您使用哪些 selang 参数来更新这些属性以及哪些命令包含这些参数。

此部分包含以下主题：

类和属性信息

以下约定适用于指定的类和属性信息：

- 在属性列表前的说明材料中，要定义类记录的*关键字*。

  关键字是记录的标识符，当您创建新记录时要指定它。 一旦创建，它便成为不可修改的属性。

- 与参数一起使用的符号 [-] 表明，可以通过键入减号将参数从数据库中删除。

  例如，*comment*（带有相应文本）会在数据库记录中添加注释；*comment-* 从数据库中删除该注释。 当您创建记录时，不能使用带减号的参数。

- 数据库中的两种类是访问者类和资源类。

  您在访问者类（USER 和 GROUP）中处理记录时使用的 selang 命令集与在资源类中所用的不同：

  - 使用 chusr、editusr 和 newusr 可处理 USER 类记录。
  - 使用 chgrp、editgrp 和 newgrp 可处理 GROUP 类记录。
  - 使用 chres、editres 和 newres 可处理任何资源类中的记录。 如果资源是文件，则还可以使用 chfile 或 editfile 命令。
  - 使用 showgrp、showres、showfile 或 showusr 可列出记录的属性。
  - 使用 authorize 和 authorize- 可以为资源记录添加、更改或删除 ACL。

更多信息：

selang 命令参考 (p. 37)

AC 环境中的类

本节包含在 CA Access Control 数据库中存在的所有类和属性（AC 环境中的类）的完整参考，这些参考按字母顺序排列。

ACVAR 类

ACVAR 类中的每个记录都定义部署在端点上的一个变量。 您无法停用该类。

ACVAR 类的关键字是变量的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

POLICIES

（信息性）使用该变量的策略（POLICY 对象）列表。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

VARIABLE_TYPE

定义变量的类型。 有效值包括：

built-in

指定在安装期间由 CA Access Control 创建该变量。 静态变量基于端点的系统设置进行解析。

注意：您不得修改或删除内置变量。

osvar

指定该变量基于操作系统值进行解析。

regval

(Windows) 指定该变量基于注册表值进行解析。

注意：您只能定义指向 REG_SZ 或 REG_EXPAND_SZ 注册表类型的注册表值。

static

指定该变量解析为您定义的字符串值。

注意：您不得更改现有变量的变量类型。

VARIABLE_VALUE

定义变量的值。

注意：该属性不扩展变量值中的任何嵌套变量。

VARIABLE_EXPANDED_VALUE

（信息性）定义变量值，并扩展变量值中的任何嵌套变量。

ADMIN 类

ADMIN 类中的每个记录都包含允许非 ADMIN 用户管理特定类的定义。 必须创建 ADMIN 记录来表示被委派用户管理的每个 CA Access Control 类。 该记录包含一个访问者列表以及每个访问者的访问授权，并且还支持条件访问控制列表 (CACL)。

ADMIN 类记录的关键字是受保护的类的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

AAUDIT

（信息性）。 显示 CA Access Control 正在审核的活动的类型。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

AGENT 类

AGENT 类中的每个记录定义一个由 CA SSO 用作代理的对象。

AGENT 类记录的关键字是代理的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

AGENT_TYPE

代理的类型。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

AGENT_TYPE 类

AGENT_TYPE 类中的每个记录定义一个由 CA SSO 使用的代理类型。

AGENT_TYPE 类记录中的关键字是代理的类型。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

AGENT_FLAG

包含有关属性的信息。 标志中可以包含下列值：

- **aznchk - 指出**是否使用此属性进行授权。
- **predef**（预定义）、**freetext**（纯文本）或 **userdir**（用户目录）- 指定用户属性的源。
- **user** 或 **group** - 这些值指明属性（访问者）是用户还是组。

AGENT_LIST

AGENT 类中的对象列表，这些对象是使用 AGENT_TYPE 对象创建的，并且用作 agent_type 参数的值；例如，当在 AGENT 类中创建对象时，会隐式更新该属性。

CLASSES

与该代理相关的类或资源的多字符串列表。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

APPL 类

APPL 类中的每个记录定义一个由 CA SSO 使用的应用程序。

APPL 类记录中的关键字是应用程序的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

APPLTYPE

由 CA SSO 使用。

AZNACL

定义授权 ACL。 授权 ACL，即允许基于资源说明访问资源的 ACL。 说明发送到授权引擎，而不是发送到对象。 通常，使用 AZNACL 时，对象不在数据库中。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CAPTION

桌面上应用程序图标下的文本。 默认值为 APPL 记录的名称。

限制： 47 个字母数字字符。

CMDLINE

应用程序的可执行文件名。 由 CA SSO 使用。

范围： 255 个字符。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围： 255 个字符。

CONTAINED_ITEMS

所包含的应用程序的记录名称（如果记录是一个容器）。

在 chres、editres 和 newres 命令中使用 item[-](*applName*) 参数可以修改该属性。

CONTAINERS

容器应用程序的记录名称（如果记录包含在其他应用程序中）。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

DIALOG_FILE

包含应用程序登录顺序的目录中的 CA SSO 脚本的名称。 默认目录位置是 /usr/sso/scripts。 默认值为 no script。

在 chres、editres 和 newres 命令中使用 script[-](*fileName*) 参数可以修改该属性。

GROUPS

被授权使用应用程序的用户组列表。

HOST

应用程序所在的主机的名称。

在 chres、editres 和 newres 命令中使用 host[-](*hostName*) 参数可以修改该属性。

ICONFILE

包含表示桌面上应用程序图标的文件的文件名或完整路径。 CA Access Control 期望在最终用户的工作站上找到图标。 如果只输入文件名，则文件的搜索顺序如下：

1. 当前目录
2. 在 PATH 环境变量中列出的目录

默认值是工作站的默认图标。

ICONID

图标文件中图标的数字 ID（如果需要）。 如果没有指定 ICONID，则会使用默认图标。

IS_CONTAINER

应用程序是否为容器。 默认值为“no”。

在 chres、editres 和 newres 命令中使用 container[-] 参数可以修改该属性。

IS_DISABLED

应用程序是否被禁用。如果应用程序被禁用，用户就不能登录它。当您更改应用程序以及您不希望任何用户在您处理它时登录，该功能很有用。 禁用的应用程序显示在应用程序菜单列表中，但如果用户选择应用程序，登录就会终止，并随之显示相应的消息。 默认值为 not disabled。

IS_HIDDEN

应用程序图标是否显示在桌面上（甚至对于可以调用它的用户）。您也许想隐藏 master 应用程序，例如，只用于向其他应用程序提供密码的应用程序。 默认值为 not hidden。

在 chres、editres 和 newres 命令中使用 hidden[-] 参数可以修改该属性。

IS_SENSITIVE

当用户在达到预设时间后打开应用程序时，是否需要再次进行身份验证。 默认值为 not sensitive。

在 chres、editres 和 newres 命令中使用 sensitive[-] 参数可以修改该属性。

LOGIN_TYPE

提供用户密码的方式。 值为 *pwd*（纯密码）、*otp*（一次性密码）、*appticket*（大型机应用程序身份验证的专属票单）、*none*（不需要密码）或 *passticket*（由 IBM 创建、由大型机安全包使用的一次性密码替换格式）。 默认值为 pwd。

在 chres、editres 和 newres 命令中使用 *login_type(*value) 参数可以修改该属性。

MASTER_APPL

向其他应用程序提供密码的应用程序的记录名称。 默认值为 no master。

在 chres、editres 和 newres 命令中使用 master[-](*applName*) 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PGMDIR

应用程序的可执行文件所在的目录或目录列表。 由 CA SSO 使用。

PWD_AUTOGEN

指明应用程序密码是否是由 CA SSO 自动生成的。 默认值为 no。

PWD_SYNC

指明应用程序密码是否自动与其他应用程序的密码保持一致。 默认值为 no。

PWPOLICY

应用程序的密码策略的记录名称。 密码策略是一组规则，用于检查新密码的有效性和定义密码到期时间。 默认值为 no validity check。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SCRIPT_POSTCMD

指明在登录脚本后是执行一个还是多个命令。

SCRIPT_PRECMD

指明在登录脚本前是执行一个还是多个命令。

SCRIPT_VARS

由 CA SSO 使用，是一个变量列表，其中含有针对每个应用程序保存的应用程序脚本的变量值。

TKTKEY

仅供 CA SSO 使用。

TKTPROFILE

仅供 CA SSO 使用。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

AUTHHOST 类

AUTHHOST 类中的每个记录定义 CA SSO 中的一个身份验证主机。

AUTHHOST 类记录中的关键字是身份验证主机的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

AZNACL

定义授权 ACL。 授权 ACL，即允许基于资源说明访问资源的 ACL。 说明发送到授权引擎，而不是发送到对象。 通常，使用 AZNACL 时，对象不在数据库中。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

ETHINFO

主机的以太网信息。

GROUPS

资源记录所属的 GAUTHHOST 或 CONTAINER 记录的列表。

要修改 AUTHHOST 类记录中的该属性，必须在相应的 CONTAINER 或 GAUTHHOST 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

KEY

仅供 CA SSO 使用。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PATH

仅供 CA SSO 使用。

PROPERTIES

仅在 UNIX dbdump 中使用。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SEED

仅供 CA SSO 使用。

SERNUM

身份验证主机的序列号。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UNTRUST

定义资源是否未受托。 如果设置了 UNTRUST 属性，则访问者将无法使用该资源。 如果未设置 UNTRUST 属性，则资源数据库中列出的其他属性将用于确定访问者的访问权限。 如果以任何方式更改了受托资源，CA Access Control 会自动设置 UNTRUST 属性。

在 chres、editres 或 newres 命令中使用 trust[-] 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USER_DIR_PROP

（信息性）。 用户目录的名称。

USER_FORMAT

仅供 CA SSO 使用。

USERALIAS

包含定义到特定身份验证主机的所有用户的别名。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

CALENDAR 类

CALENDAR 类中的每个记录都为在 CA Access Control 中实施时间限制的用户、组和资源定义 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔检索 Unicenter TNG 活动日历，以查找实施的时间限制。使用 chgrp、chres、chusr、editgrp、editres、editusr、newgrp、newres 和 newusr 命令的日历 (*calendarName*) 属性将日历记录分配给资源。

下列类在其类记录中有 CALENDAR 属性。 向下列任一资源类中的每个对象 *仅*分配一个 CALENDAR 类对象。

- ADMIN
- APPL
- AUTHHOST
- CONNECT
- CONTAINER
- DOMAIN（仅 Windows）
- FILE
- GFILE
- GHOST
- GROUP
- GSUDO
- GTERMINAL
- HOST
- HOSTNET
- HOSTNP
- LOGINAPPL（仅 UNIX）
- MFTERMINAL
- PROCESS

- PROGRAM
- REGKEY（仅 Windows）
- SUDO
- SURROGATE
- TCP
- TERMINAL
- USER

CALENDAR 类的关键字是 Unicenter TNG 日历的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

CATEGORY 类

CATEGORY 类中的每个记录都定义数据库中的安全类别。

CATEGORY 类记录的关键字是安全类别的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

CONNECT 类

CONNECT 类中的每个记录均可定义一个远程主机，该主机使用 TCP over IPv4 从本地主机连接到该远程主机。

注意：CA Access Control 的 IP 通信访问规则仅适用于 IPv4。 CA Access Control 不控制通过 IPv6 进行的访问。

注意：如果 CONNECT 类用作访问的标准，则 TCP 类无法有效地控制访问。 使用 TCP 类或 CONECT 类保护连接，而不是同时使用这两类。

CONNECT 类记录中的关键字是远程主机的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

CONTAINER 类

CONTAINER 类中的每个记录都定义来自其他资源类的一组对象，从而简化了规则适用于几个不同对象类时的定义访问规则的工作。 CONTAINER 类记录的成员可以是下列任何类的对象：

- APPL
- AUTHHOST
- CONNECT
- CONTAINER
- DICTIONARY
- DOMAIN（仅 Windows）
- FILE
- GAPPL
- GAUTHHOST
- GFILE
- GHOST
- GSUDO

- GTERMINAL
- HNODE
- HOLIDAY
- HOST
- HOSTNET
- HOSTNP
- MFTERMINAL
- PARAM_DESC
- POLICY
- PROCESS
- PROGRAM
- REGKEY（仅 Windows）
- RULESET
- SUDO
- SURROGATE
- TCP
- TERMINAL
- WEBSERVICE

注意：CONTAINER 记录可以嵌套在其他 CONTAINER 记录中。

在将对象指定为 CONTAINER 记录的成员之前，必须先在其对应的类中为其创建记录。

如果容器中的对象在它的相应类记录中没有 ACL，则它继承它所属的 CONTAINER 记录的 ACL。

CONTAINER 类的关键字是 CONTAINER 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

来自组中任何成员类的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

DEPLOYMENT 类

DEPLOYMENT 类中的每个记录均可为一个端点定义一个部署或取消部署任务。 部署任务包括端点按要求部署或取消部署一个策略所需的信息。

DEPLOYMENT 类的关键字是部署任务的名称，通常是自动生成的。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

DMS_NAME

定义从中创建部署任务的 DMS 的名称。

GPOLICY

定义已为其创建部署任务的策略的名称。

GROUPS

定义此部署任务所属的部署程序包 (GDEPLOYMENT)。

HNODE

定义创建此部署任务所针对的主机。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OPERATION

指定端点应该作为此部署任务的结果执行的操作的类型。 可以为部署或取消部署。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

POLICY_VERSION

定义创建此部署任务所针对的策略版本。

RESULT_MESSAGE

定义部署或取消部署 selang 脚本的输出。 这些是策略部署或取消部署脚本运行时的消息 selang 输出。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

STATUS

定义部署任务的状态。 可以为以下项之一：

- **成功** - 策略部署未出错。
- **警告** - 执行部署脚本时出错。
- **失败** - 执行部署任务时出错。
- **无操作** - 部署程序包实际上为空，因此无需执行任何操作。

  注意：此状态还可能是已经通过其他部署路径分配到主机的策略导致的结果。
- **未执行** - 策略验证在策略中找到一个或多个错误。
- **不同步** - 策略包含一个变量，该变量值已经在端点上更改。
- **挂起部署** - 策略包含未定义的或未解析的变量。
- **挂起先决条件策略** - 仅在部署所有先决条件策略之后才执行部署任务。
- **挂起依存策略** - 仅在取消部署所有依存策略之后才执行部署任务（取消部署策略）。
- **修复** - 部署任务等待再次部署。

TARGETYPE

定义主机（目标）的类型以限制 policyfetcher 仅处理 CA Access Control 部署程序包。 可以是这些类型之一：UNAB、AC、无。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

DICTIONARY 类

DICTIONARY 类中的每个记录定义存储在 CA Access Control 数据库中的公用词典中的一个单词以便与密码比较。 当用户更改他们的密码时，系统会根据 DICTIONARY 类中的每个记录对这些密码进行检查。

除了向 DICTIONARY 类添加记录（单词）外，您还可以通过运行工具或程序从外部文件导入词典单词。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

DOMAIN 类

在 Windows 上有效

DOMAIN 类中的每个记录定义 Windows 网络中的一个域。

DOMAIN 记录中的关键字是域名。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

FILE 类

FILE 类中的每个记录定义允许对特定的文件或目录或者与*文件名模式*匹配的文件进行的访问。 要为某个文件定义规则，并不需要事先创建该文件。

设备文件和符号链接可以像任何其他文件那样进行保护。 但是，通过保护链接，您并不会自动保护链接所指向的文件。

注意：在 NTFS 文件系统中，FILE 类中的记录还定义对文件数据流的访问。 有关如何保护文件数据流的详细信息，请参阅*《端点管理指南：用于 Windows》*。

在将脚本定义为文件时，允许对该文件进行*读取*和*执行*访问。 当您定义二进制文件时，*执行*访问权限就足够了。

对于特殊的 _restricted 组之外的用户，FILE 类中的 _default 记录（如果不存在 _default 记录，则为 UACC 类中的 FILE 的记录）*只保护属于 CA Access Control 的文件*，例如 seos.ini、seosd.trace、seos.audit 和 seos.error 文件。 这些文件没有显式定义到 CA Access Control，但自动受到 CA Access Control 的保护。

FILE 类记录的关键字是受记录保护的文件或目录的名称。 必须指定完整路径。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

组

资源记录所属的 GFILE 或 CONTAINER 记录的列表。

DB 属性：GROUPS

要修改 FILE 类记录中的该属性，必须在相应的 CONTAINER 或 GFILE 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UNTRUST

定义资源是否未受托。 如果设置了 UNTRUST 属性，则访问者将无法使用该资源。 如果未设置 UNTRUST 属性，则资源数据库中列出的其他属性将用于确定访问者的访问权限。 如果以任何方式更改了受托资源，CA Access Control 会自动设置 UNTRUST 属性。

在 chres、editres 或 newres 命令中使用 trust[-] 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GAPPL 类

GAPPL 类中的每个记录定义由 CA SSO 使用的一组应用程序。 在将每个应用程序添加到 GAPPL 记录之前，必须先为其创建 APPL 类记录。 然后，必须显式地将 APPL 类的记录连接到 GAPPL 记录以便将它们组合在一起。

GAPPL 类记录的关键字是 GAPPL 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

AZNACL

定义授权 ACL。 授权 ACL，即允许基于资源说明访问资源的 ACL。 说明发送到授权引擎，而不是发送到对象。 通常，使用 AZNACL 时，对象不在数据库中。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改 GAPPL 类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

APPL 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

GAUTHHOST 类

GAUTHHOST 类中的每个记录定义由 CA SSO 使用的一组身份验证主机。 在将每个应用程序添加到 GAUTHHOST 记录之前，必须先为其创建 AUTHHOST 类记录。 然后，必须显式地将 AUTHHOST 类的记录连接到 GAUTHHOST 记录以便将它们组合在一起。

GAUTHHOST 类记录的关键字是 GAUTHHOST 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

AZNACL

定义授权 ACL。 授权 ACL，即允许基于资源说明访问资源的 ACL。 说明发送到授权引擎，而不是发送到对象。 通常，使用 AZNACL 时，对象不在数据库中。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改 GAUTHHOST 类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

AUTHHOST 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

GFILE 类

GFILE 类中的每个记录都定义允许对一组特定文件、特定目录或与名称模式匹配的文件的访问。 在将每个应用程序添加到 GFILE 记录之前，必须先为其创建 FILE 类记录。 然后，必须显式地将 FILE 类的记录连接到 GFILE 记录以便将它们组合在一起。 要为某个文件定义 FILE 类记录，并不需要事先创建该文件。

GFILE 类记录的关键字是 GFILE 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

FILE 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GDEPLOYMENT 类

GDEPLOYMENT 类中的每个记录定义一个部署程序包。 部署程序包在 DMS 上自动创建，并将由于相同事务（策略分配、升级等）对特定主机创建的所有部署任务分组到一起。 这意味着您执行的每个事务都会创建必需数量的部署任务（DEPLOYMENT 对象），并将这些任务按主机进行分组（GDEPLOYMENT 对象）。

GDEPLOYMENT 类的关键字是部署程序包的名称，通常会自动生成。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GHNODE

定义创建此部署程序包所针对的主机组。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

HNODE

定义创建此部署程序包所针对的主机。

MEMBERS

DEPLOYMENT 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

POLICY

定义创建此部署程序包所针对的策略。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

TRIGGER

指定创建此部署程序包的原因。 可以为以下项之一：

- 分配 - 由于将策略分配到主机或将主机分配到主机组。
- 自动分配 - DMS 的结果自动将主机分配给主机组。
- 取消分配 - 由于从主机取消分配策略或从主机组取消分配主机。
- 直接部署 - 由于直接部署操作。
- 直接取消部署 - 由于直接取消部署操作。
- 升级 - 由于升级操作。
- 还原 - 由于主机 (HNODE) 上的还原操作。
- Hnode 删除 - 由于删除主机 (HNODE)。
- Ghnode 删除 - 由于删除主机组 (GHNODE)。
- 重置 - 由于重置主机。
- 降级 - 由于主机上的策略降级。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GHNODE 类

GHNODE 类中的每个记录定义一个主机组，即一组主机（HNODE 对象）。在将每个主机添加到 GHOST 记录之前，必须为其创建一个 HNODE 类记录。

此类用于管理策略部署和分配。

GHNODE 类记录的关键字是主机组的逻辑名。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

CRITERIA

定义 DMS 用来自动将主机添加到该主机组中的条件。 您可以指定匹配或排除以下 HNODE 属性的条件：ATTRIBUTES、COMMENT、HNODE_INFO、HNODE_IP、HNODE_VERSION、NODE_TYPE

例如，Windows 端点的 HNODE 记录具有属性 HNODE_INFO=Windows。 如果 GHNODE 记录的 CRITERIA 属性具有值 HNODE_INFO=Windows，DMS 会自动将任何新的 Windows HNODE 添加到 GHNODE 中。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

HNODE 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

POLICIES

应在此对象上部署的策略列表。

POLICYASSIGN

定义分配给此对象的策略列表。

显示名称：分配的策略

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GHOST 类

GHOST 类中的每个记录都定义一组主机。 在将每个主机添加到 GHOST 记录之前，必须为其创建一个 HOST 类记录。 服务必须使用 /etc/services 文件（对于 UNIX）、\system32\drivers\etc\services 文件（对于 Windows）或其他文件名解析方法定义到系统。 当授权服务时，您可以根据它们在 TCP/IP 协议中的端口号而不是它们的名称来确定服务。 当添加服务时，您可以根据它们在 TCP/IP 协议中的端口号而不是它们的名称来确定服务。 然后，必须显式地将 HOST 类的记录连接到 GHOST 记录以便将它们组合在一起。

GHOST 记录定义访问规则，这些访问规则控制在使用 Internet 通讯时属于主机组的工作站（主机）拥有的对本地主机的访问权限。 对于每个客户端组（GHOST 记录），INETACL 属性都列出服务规则，用于控制本地主机可以为属于客户端组的主机提供的服务。

GHOST 类记录的关键字是 GHOST 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围： 255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

INETACL

定义允许本地主机向一组客户端主机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：

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。

CA Access Control 支持 /etc/rpc 文件（对于 UNIX）或 \etc\rpc 文件（对于 Windows）中指定的动态端口名称。

访问

定义访问者对资源的访问权限。

在 authorize[-] 命令中使用 access(*type-of-access*)、service 和 stationName 参数可以修改 INETACL 属性中的访问者及其访问类型。

INSERVRNGE

指定本地主机向一组客户端主机提供的服务的范围。

执行与 INETACL 属性相似的功能。

使用 service(*serviceRange*) 参数及 authorize[-] 命令可以修改 INSERVRANGE 属性中的访问者及其访问类型。

MEMBERS

HOST 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GPOLICY 类

GPOLICY 类中的每个记录定义一个逻辑策略。 它包含有关属于此策略的策略版本（POLICY 对象）以及该策略分配到的主机和主机组的信息。

GDEPLOYMENT 类的关键字是逻辑策略的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GHNODEASSIGN

定义将此策略分配到的主机组。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

HNODEASSIGN

定义将此策略分配到的主机。

LATEST_FINALIZED_VERSION

定义最终确定的最新策略版本（POLICY 对象）的名称。

LATEST_VERSION

定义与此策略相关联的最新策略版本（POLICY 对象）的名称。

MEMBERS

POLICY 类（策略版本）中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

POLICY TYPE

代表组策略类型的值。 有效值包括：

- None
- Login - 指定策略是 UNAB 登录策略。
- Configuration - 指定策略是 UNAB 配置策略。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GROUP 类

GROUP 类中的每个记录都定义数据库中的一个用户组。

每个 GROUP 类记录的关键字是组的名称。

注意：配置文件组的属性适用于与配置文件组相关的每个用户。 但是，如果在用户（USER 或 XUSER）记录中指定了同一属性，则该用户记录会覆盖配置文件组记录中的那些属性。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 chgrp 更改其中大多数属性。

注意：在多数情况下，除非明确指出使用 ch[x]grp 更改属性，否则请将属性名称用作命令参数。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 showgrp 查看所有属性。

APPLS

（信息性）显示授权访问者访问的应用程序列表。 由 CA SSO 使用。

AUDIT_MODE

定义 CA Access Control 在审核日志中记录的活动。可以指定下列活动的任何组合：

- 无登录
- 在跟踪文件中记录的所有活动
- 登录尝试失败
- 登录成功
- 对 CA Access Control 保护的资源进行的失败访问尝试
- 对 CA Access Control 保护的资源进行的成功访问
- 交互式登录

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的审核参数相对应。 您可以使用 GROUP 或 XGROUP 的 AUDIT_MODE 为组中所有成员设置审核模式。 然而，如果用户的审核模式定义为 USER 记录、XUSER 记录或配置文件组时，您不得使用 AUDIT_MODE 为组成员设置审核模式。

AUTHNMTHD

（信息性）显示用于组记录的身份验证方法，从方法 1 到方法 32，或无。 由 CA SSO 使用。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EXPIRE_DATE

定义访问者变为无效的日期。 用户记录中的 EXPIRE_DATE 属性值会覆盖组记录中的值。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 expire[-] 参数相对应。

FULLNAME

定义与访问者相关联的全名。CA Access Control 使用全名标识审核日志消息中的访问者，但不用于授权。

FULLNAME 是字母数字字符串。对于组，最大长度为 255 个字符。对于用户，最大长度为 47 个字符。

GAPPLS

定义向组授予了访问权限的应用程序组的列表。 由 CA SSO 使用。

GROUP_MEMBER

定义属于此组成员的组。

GROUP_TYPE

指定组权限属性。这些属性中的每个属性均与 ch[x]grp 命令中的同名参数相对应。 一个组可以具有以下一个或多个权限属性：

ADMIN

指定属于该组的用户是否可以执行管理功能，类似于 UNIX 环境中的 root 用户。

AUDITOR

指定属于该组的用户是否可以监控系统、列出数据库中的信息以及为现有记录设置审核模式。

OPERATOR

指定属于该组的用户是否可以列出数据库中的所有内容并使用 secons 实用程序。

PWMANAGER

指定属于该组的用户是否可以修改其他用户的密码设置，以及是否可以启用已经被 serevu 实用程序禁用的用户帐户。

SERVER

指定进程是否可以请求属于该组的用户进行授权，以及是否可以发出 SEOSROUTE_VerifyCreate API 调用。

HOMEDIR

定义分配给新组成员的主目录的路径。

在 chgrp、editgrp 或 newgrp 命令中使用 homedir 参数可以修改该属性。

限制：255 个字母数字字符。

INACTIVE

定义不活动天数，在该天数后系统会将用户的状态更改为不活动。如果帐户状态为不活动，则用户无法登录。

USER 记录中的 INACTIVE 属性值会覆盖 GROUP 记录中的值。 这二者都会覆盖 SEOS 类记录中的 INACT 属性。

注意：CA Access Control 不存储状态，而是动态地计算状态。 要标识不活动用户，必须将 INACTIVE 值与用户的 LAST_ACC_TIME 值进行比较。

INACTIVE 是配置文件功能的一部分。

MAXLOGINS

定义允许用户进行的并发登录的最大数目。 值为零表示用户可以进行任意数量的并发登录。

用户记录中的 MAXLOGINS 属性值会覆盖组记录中的值。 这二者都会覆盖 SEOS 类记录中的 MAXLOGINS 值。

MAXLOGINS 是配置文件功能的一部分。

MEMBER_OF

定义此组所属的组。

OWNER

定义拥有记录的用户或组。

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。

在 setoptions 命令中使用 password 参数以及 rules 或 rules- 选项可以修改该属性。

PASSWDRULES 是配置文件功能的一部分。

POLICYMODEL

指定当您使用 sepass 实用程序更改用户密码时接收新密码的 PMDB。如果为该属性输入了值，则密码就*不*发送到由 parent_pmd 或 passwd_pmd 配置设置定义的策略模型。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 pmdb[-] 参数相对应。

POLICYMODEL 是配置文件功能的一部分。

PROFUSR

显示与此配置文件组关联的用户列表。

PWD_AUTOGEN

指出组密码是否是自动生成。 默认设置为 no。由 CA SSO 使用。

PWD_SYNC

指出所有组应用程序的组密码是否都自动保持一致。默认设置为 no。由 CA SSO 使用。

PWPOLICY

定义组密码策略的记录名称。 密码策略是一组规则，用于检查新密码的有效性和定义密码到期时间。 默认值为 no validity check。 由 CA SSO 使用。

RESUME_DATE

定义挂起的 USER 帐户变为取消挂起的日期。

RESUME_DATE 与 SUSPEND_DATE 配合工作。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 resume[-] 参数相对应。

RESUME_DATE 是配置文件功能的一部分。

REVACL

显示访问者的 Access Control 列表。

SHELL

（仅适用于 UNIX）当新的 UNIX 用户是此组的成员时，会为该用户分配 shell 程序。

在 chxgrp 命令中使用 shellprog 参数可以修改该属性。

SUBGROUP

显示以该组为父组的组的列表。

SUPGROUP

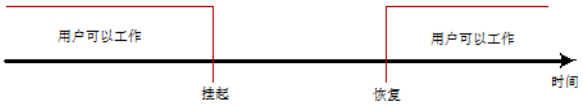
定义父组（“超越”组）的名称。

在 ch[x]grp 命令中使用 parent[-] 参数可以修改该属性。

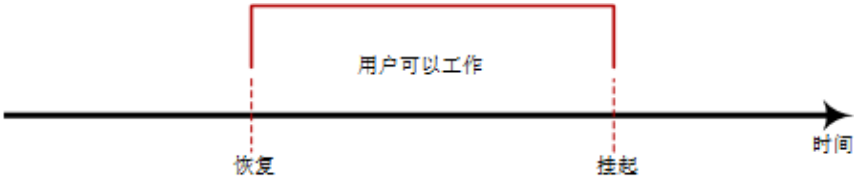
SUSPEND_DATE

定义用户帐户因挂起而变为无效的日期。

如果记录的挂起日期在其恢复日期之前，用户就可以在挂起日期前和恢复日期后工作。



如果用户的恢复日期早于挂起日期，则记录也会在该恢复日期*之前*无效。 用户仅可以在恢复日期和挂起日期之间进行工作。



用户记录中的 SUSPEND_DATE 属性值会覆盖组记录中的值。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 suspend[-] 参数相对应。

SUSPEND_WHO

显示激活挂起日期的管理员。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USERLIST

定义属于组的用户。

该属性中包含的用户列表可能与本机环境 USERS 属性中的用户列表不同。

使用 join[x][-] 命令可以修改该属性。

GSUDO 类

GSUDO 类中的每个记录定义任务指派（即 DO (sesudo)）允许用户执行或阻止用户执行的一组操作。 在将每个操作添加到 GSUDO 记录之前，必须为其创建一个 SUDO 类记录。

请使用 GSUDO 为一组 SUDO 资源定义访问规则，而不是为每个资源指定相同的访问规则。 必须显式地将 SUDO 类的记录连接到 GSUDO 记录以便将它们组合在一起。

GSUDO 类记录的关键字是组的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

SUDO 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GTERMINAL 类

GTERMINAL 类中的每个记录都定义一组终端。 在将每个终端添加到 GTERMINAL 之前，必须先为其创建 TERMINAL 类记录。 然后，必须显式地将 TERMINAL 类的记录连接到 GTERMINAL 记录以便将它们组合在一起。

终端组在定义访问规则时很有用。 可以使用单个命令为一组终端指定访问规则，而不必为每个终端指定相同的访问规则。 类似地，可以通过单个命令将一组终端的规则应用到一组用户。

GTERMINAL 类记录的关键字是终端组的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MEMBERS

TERMINAL 类中属于组的对象列表。

在 chres、editres 和 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

GWINSERVICE 类

GWINSERVICE 类中的每个记录定义一组 Windows 服务。 使用 GWINSERVICE 类中的记录为一组 Windows 服务定义访问规则。

GWINSERVICE 类记录的关键字是 GWINSERVICE 记录的名称。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

HNODE 类

HNODE 类包含有关组织的 CA Access Control 主机的信息。 该类中的每个记录代表企业中的一个节点。

该类用于管理从不同 PMDB 和端点上载并存储在 DMS 中的信息。

HNODE 类记录的关键字是端点的实际主机名（例如 myHost.ca.com）或者策略模型节点的 PMDB 名称（例如 myPMD@myHost.ca.com）。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

ATTRIBUTES

定义 DMS 用来评估主机是否自动被添加到主机组的自定义条件。

注意：DMS 还会检查以下 HNODE 属性，以便评估主机是否应自动被添加到主机组中：COMMENT、HNODE_INFO、HNODE_IP、HNODE_VERSION、NODE_TYPE

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

COMPLIANT

显示 HNODE 的自动计算的遵从性状态。 值为：

- yes - CA Access Control 已安装，并且已成功部署所有的有效策略。
- no - CA Access Control 已安装，但没有部署任何有效策略。
- Deviation - CA Access Control 已安装，但没有成功部署所有的有效策略。
- Unknown - CA Access Control 未安装，并且没有要部署的有效策略。

注意：UNAB 策略（登录和配置策略）没有分配给遵从性状态值。

COMPLIANT_UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EFFECTIVE_POLICIES

定义应在此对象上部署的策略版本列表。

显示名称：有效策略

GHNODES

定义此对象所属的主机组列表。

显示名称：节点组

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

HNODE_IP

主机的 IP 地址。

显示名称：IP

HNODE_KEEP_ALIVE

定义 HNODE 上次将心跳发送到分布式主机的时间。

显示名称：上次心跳

LOGIN

定义主机的默认访问权限类型。

显示名称：LOGIN

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NODE_INFO

（信息性）指定节点 OS 的详细信息。

NODE_TYPE

（信息性）定义主机上的 CA Access Control 安装类型。 有效值包括：

- ACU - 适用于 UNIX 的 CA Access Control
- ACW - 适用于 Windows 的 CA Access Control
- UNAB - UNIX 身份验证代理 (UNAB)

注意：HNODE 记录可以同时有 NODE_TYPE 属性的 ACU 和 UNAB 的值。

NODE_VERSION

（信息性）定义安装在主机上的 CA Access Control 版本。 版本号的前面带有 NODE_TYPE。

示例：ACU:12.50-00.647

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

PARENTS

（信息性）。 传播树中节点的父级 PMDB 列表（还由 parent_pmd 配置设置定义）。

POLICYASSIGN

定义分配给此对象的策略列表。

显示名称：分配的策略

POLICY_STATUS

在 POLICIES 属性中列出每个策略的状态。 该属性的值是带有以下字段的结构：

oidPolicy

POLICY 对象的对象 ID。 与 POLICIES 属性的值相同。

policy_status

表示以下其中一项的整数：

- 已部署 - 已在端点成功部署策略。
- 已部署，但存在失败 - 已使用一个或多个规则从部署脚本部署策略，但无法在端点上执行。
- 已取消部署 - 已成功从端点取消部署策略。

  注意：如果已取消部署某策略，则不显示主机的任何状态（即状态为空）。
- 已取消部署，但存在失败 - 已使用一个或多个规则从取消部署脚本取消部署策略，但无法在端点上执行。
- 部署失败 - 由于部署脚本出错导致策略部署失败。

  注意：此状态仅可在启用策略验证的情况下显示。 否则，即使策略包含错误，policyfetcher 仍然会部署策略（“已部署，但存在失败”状态）。
- 未知 - 策略状态未知。
- 部署挂起 - 正在等待部署先决条件策略，或者该策略包含未定义或未解析的变量。
- 取消部署挂起 - 等待取消部署从属策略。
- 不同步 - 策略包含一个变量，该变量值已经在端点上更改。
- 未执行 - 策略验证在策略中找到一个或多个错误。
- 已排队 - 过时（仅适用于向后兼容）。
- 已传输 - 过时（仅适用于向后兼容）。
- 传输失败 - 过时（仅适用于向后兼容）。
- 签名失败 - 过时（仅适用于向后兼容）。

deviation

表示此节点上是否存在策略偏差的值。 有效值包括：

- 是
- 否
- Unset

dev_time

上次偏差状态更新时间。

ptime

上次策略状态更新时间。

updator

部署或删除策略的用户的名称。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SUBSCRIBER_STATUS

每个父级的节点的状态。 该属性的值是带有以下字段的结构：

oidSubs

HNODE 对象的对象 ID。 与 SUBSCRIBERS 属性的值相同。

状态

表示以下其中一种状态的值：

- 可用的
- 不可用
- 同步（正在同步）
- 未知

stime

上次状态更新时间。

SUBSCRIBERS

传播树中节点的订户列表。 通过更新该属性，使用 HNODE 对象名称的值隐式更新 PARENTS 属性。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UNAB_ID

（信息性）显示 UNAB 主机 ID 以便进行报告。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

HOLIDAY 类

HOLIDAY 类中的每个记录定义一个或多个时间段，在这些时间段内，用户需要额外权限才能登录。

每个用户在记录中的所有时间段内拥有同样的访问权限。 也就是说，如果您在假日记录中有多个假日时间段，您就无法做到既允许用户在某些这样的时间段内登录又阻止用户在其他时间段内登录。 例如，如果要允许特定用户在元旦期间登录但不允许在圣诞节期间登录，则这两个假日必须定义在不同的记录中。

如果不指定年份，则认为假日是**每年一次。**

可以通过在 newusr、chusr 或 editusr 命令中指定 IGN_HOL 属性，来覆盖各个用户的 HOLIDAY 类限制。

HOLIDAY 类记录的关键字是 HOLIDAY 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

HOL_DATE

指定用户不能登录的时间段。

下列规则适用于 HOL_DATE 属性：

- 如果不指定年份，则表示时间段或假日是每年一次的。 可以指定二位数或四位数的年份，例如：99 或 1999。
- 如果不指定开始时间，则会使用一天的开始（午夜）；如果不指定结束时间，则使用一天的结束（午夜）。
- 如果不指定时间间隔，而只指定日期，那么假日会持续一整天。

在 chres、editres 和 newres 命令中使用 dates 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

HOST 类

HOST 类中的每个记录都定义主机在用 IPv4 连接时对本地计算机所拥有的访问权限。

注意：CA Access Control 的 IP 通信访问规则仅适用于 IPv4。 CA Access Control 不控制通过 IPv6 进行的访问。

CA Access Control 需要解析您添加到 HOST 类的主机名的地址。 也就是说，这些名称必须显示在操作系统主机文件中或定义到 NIS 或 DNS。

对于每个 HOST 记录，INETACL 属性定义本地主机可以向该主机提供的服务。

CA Access Control 允许对主机名使用别名，但表示别名的记录不用于授权检查。 您必须知道正规主机名，以便 CA Access Control 保护与该主机的连接。

HOST 类记录的关键字是主机的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 GHOST 或 CONTAINER 记录的列表。

要修改 HOST 类记录中的该属性，必须在相应的 CONTAINER 或 GHOST 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

INETACL

定义允许本地主机向一组客户端主机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：

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。

CA Access Control 支持 /etc/rpc 文件（对于 UNIX）或 \etc\rpc 文件（对于 Windows）中指定的动态端口名称。

访问

定义访问者对资源的访问权限。

在 authorize[-] 命令中使用 access(*type-of-access*)、service 和 stationName 参数可以修改 INETACL 属性中的访问者及其访问类型。

INSERVRNGE

指定本地主机向一组客户端主机提供的服务的范围。

执行与 INETACL 属性相似的功能。

使用 service(*serviceRange*) 参数及 authorize[-] 命令可以修改 INSERVRANGE 属性中的访问者及其访问类型。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

HOSTNET 类

HOSTNET 类中的每个记录定义特定网络中的一组主机。 HOSTNET 记录定义规则，这些规则用于管理组中的其他主机在使用 IPv4 通信时对本地主机所拥有的访问权限。

注意：CA Access Control 的 IP 通信访问规则仅适用于 IPv4。 CA Access Control 不控制通过 IPv6 进行的访问。

INMASKMATCH 确定哪些其他主机从属于 HOSTNET 记录。 INETACL 属性定义本地主机可以向这些主机提供的服务。

HOSTNET 类记录的关键字是 HOSTNET 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

INETACL

定义允许本地主机向一组客户端主机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：

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。

CA Access Control 支持 /etc/rpc 文件（对于 UNIX）或 \etc\rpc 文件（对于 Windows）中指定的动态端口名称。

访问

定义访问者对资源的访问权限。

在 authorize[-] 命令中使用 access(*type-of-access*)、service 和 stationName 参数可以修改 INETACL 属性中的访问者及其访问类型。

INSERVRNGE

指定本地主机向一组客户端主机提供的服务的范围。

执行与 INETACL 属性相似的功能。

使用 service(*serviceRange*) 参数及 authorize[-] 命令可以修改 INSERVRANGE 属性中的访问者及其访问类型。

INMASKMATCH

定义应用此 HOSTNET 记录的主机组。 该属性包含 mask 和 match 值，这些值会应用于发出请求的主机的 IP 地址，以确定发出请求的主机是否属于该组。

INMASKMATCH 属性仅支持 IPv4 格式的地址。

注意：该属性与 chres 命令的 mask 和 match 参数相对应。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

HOSTNP 类

HOSTNP 类中的每个记录都定义一组有相似主机名的主机。 HOSTNP 记录定义访问规则，这些访问规则用于管理与记录中的名称模式匹配的其他工作站（主机）在使用 IPv4 时对本地主机所拥有的访问权限。 对于每个掩码（HOSTNP 记录），INETACL 属性都列出服务规则，用于控制本地主机可以为主机组提供的服务。

HOSTNP 类记录中的关键字是用于筛选受该 HOSTNP 记录保护的主机的主机名的名称模式。

注意：CA Access Control 的 IP 通信访问规则仅适用于 IPv4。 CA Access Control 不控制通过 IPv6 进行的访问。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

INETACL

定义允许本地主机向一组客户端主机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：

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。

CA Access Control 支持 /etc/rpc 文件（对于 UNIX）或 \etc\rpc 文件（对于 Windows）中指定的动态端口名称。

访问

定义访问者对资源的访问权限。

在 authorize[-] 命令中使用 access(*type-of-access*)、service 和 stationName 参数可以修改 INETACL 属性中的访问者及其访问类型。

INSERVRNGE

指定本地主机向一组客户端主机提供的服务的范围。

执行与 INETACL 属性相似的功能。

使用 service(*serviceRange*) 参数及 authorize[-] 命令可以修改 INSERVRANGE 属性中的访问者及其访问类型。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

KMODULE 类

KMODULE 类中的每个记录定义一个操作系统的内核模块。

如果在 KMODULE 类中定义了某模块，则要求操作系统加载或卸载该模块的任何调用均会导致 CA Access Control 检查为该模块定义的授权。

KMODULE 记录的关键字是受保护的内核模块的名称。

每个 KMODULE 记录均包含以下属性：

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。KMODULE 记录的有效访问权限为加载和卸载。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

FILEPATH

定义文件的绝对路径列表，每个文件包含一个内核模块。用冒号 (:) 分隔每个文件路径。

如果同一模块有不同版本，请使用多个文件路径。

如果未提供文件路径，则 CA Access Control 在加载内核模块时不执行文件路径检查。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围： 30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SIGNATURE

显示在文件路径属性中定义的内核模块文件的唯一值。

CA Access Control 在启动及使用 selang 命令更改 KMODULE 记录时计算内核模块的签名。 您可以使用命令 seretrust -m 自行设置签名。

注意：CA Access Control 仅为 Linux 系统使用 SIGNATURE 属性。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

LOGINAPPL 类

在 UNIX 上有效

LOGINAPPL 类中的每个记录定义一个登录应用程序，标识可以使用该程序进行登录的用户，并控制使用该登录程序的方式。

LOGINAPPL 类记录的关键字是应用程序的名称，即表示登录应用程序的逻辑名称。 该逻辑名称在 LOGINPATH 属性中与可执行文件的完整路径名称相关联。

CA Access Control 还可以控制和保护通用登录应用程序；这意味着您可以用通用模式保护与某一规则匹配的登录应用程序组。 要用 selang 定义通用登录应用程序，请使用与设置常规登录限制一样的命令，但不使用 LOGINPATH 参数（该参数应包括一个通用路径，由使用下列一个或多个字符的常规表达式组成：[、]、*、?）。

CA Access Control 为标准登录程序预设 LOGINAPPL 类中记录的属性值。在进行任何更改之前，应该先列出并验证当前设置。

重要说明！ LOGINAPPL 不使用 _default 条目。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

LOGINFLAGS

控制登录应用程序的特殊功能，包括设备号的更改和宽限登录次数的减少。 有效值包括：

- **execlogin** - 指定登录触发器是进程执行的第一个 EXEC 操作。
- **loginprefix** - 指定 CA Access Control 将 LOGINAPPL 资源名称作为前缀添加到登录的用户名。 例如，如果您设置该属性，而名为 user1 的用户排定了 CRON 任务，那么当 CA Access Control 检测到 CRON 任务登录时，会将用户名设置为 USR_SBIN_CRON_user1。

  注意：CA Access Control 不会将 LOGINAPPL 资源名称作为前缀添加到 root 用户。
- **nograce** - 指出当用户通过该应用程序登录时不应减少宽限登录次数。
- **nograceroot** - 指出当 root 用户通过该应用程序登录时不应减少宽限登录次数。

- **nologin** - 确保只对用户计入登录次数。 对父程序不计入登录次数。

  某些平台上的程序（如 rlogin）会导致 rlogin 自身触发登录并关闭登录顺序，这样会导致对超级用户计入一个实际登录。 在执行登录以后，rlogin 会派生另一个程序以执行实际登录。

  如果您使用登录程序（例如 rlogin 或 telnet），并运行 seaudit -a，该问题就是显而易见的。 您将会看到同一次登录还对应其他登录记录，其 uid 是 root。

- **pamlogin** - 表示当用户通过该应用程序登录时，会使用 CA Access Control PAM 登录拦截。

在 chres、editres 或 newres 命令中使用 loginflags 参数可以修改该属性。

LOGINMETHOD

指出登录应用程序是否为用于保护 CA Access Control 的伪登录程序。有效值包括：

- **normal** - 指出此登录应用程序自身执行 setuid 和 setgid 调用。seosd 检查指定程序的规则。
- **pseudo** - 指出此登录应用程序调用另一个程序以执行 setuid 和 setgid 调用。 seosd 检查有关另一程序的规则。

在 chres、editres 或 newres 命令中使用 loginmethod 参数可以修改该属性。

重要说明！ 建议不要修改该预设属性。

LOGINPATH

登录应用程序的完整路径（或通用路径）。

在 chres、editres 或 newres 命令中使用 loginpath 参数可以修改该属性。

LOGINSEQUENCE

定义 seosd 处理 seteuid、setuid、setgid 和 setgroups 事件的顺序，以便将来自后台进程且启动登录进程的用户（通常是在 root 用户身份下的 inetd）设置为实际登录的用户。 最多可以定义八个系统事件。

登录截获顺序始终是以称为**触发器的 setgid 或 setgroups 事件开始，它以 setuid 事件结束，该事件用于将用户的身份更改为实际登录的用户。**

为成功完成登录，程序需要按照从 setgroups 或 setgid 开始并以 setuid 或 seteuid 结束的顺序执行所有指定进程。

为程序设置正确的登录顺序是一项很难的任务。 大多数登录程序在默认的 SGRP、SUID 设置中运行得很好，该设置意味着程序发出 setgroups 系统调用，然后发出 setuid 命令将用户的身份更改为目标用户。

不过，如果 SGRP、SUID 设置不起作用，您就必须使用下列标志指定正确的顺序：

- **SEID -** 第一个 seteuid 事件
- **SUID -** 第一个 setuid 事件
- **SGID -** 第一个 setgid 事件
- **SGRP -** 第一个 setgroup 事件
- **FEID -** 第二个 seteuid 事件
- **FUID -** 第二个 setuid 事件
- **FGID -** 第二个 setgid 事件
- **FGRP -** 第二个 setgroup 事件
- **N3EID -** 第三个 seteuid 事件
- **N3UID -** 第三个 setuid 事件
- **N3GID -** 第三个 setgid 事件
- **N3GRP -** 第三个 setgroup 事件

重要说明！ 您必须使用标志来指定正确的登录顺序。 但是，您可以在 LOGINSEQUENCE 参数内按任意顺序指定标志。 例如，SGRP、SEID、FEID、N3EID 等同于 N3EID、FEID、SGRP、SEID。

注意：如果您不知道登录程序执行的系统调用的顺序，则可以查看跟踪记录并查找将用户更改为目标 uid 的 setuid 事件，然后查看以前的以第一个 setgid 或 setgroups 事件开始的跟踪事件。

例如，如果有一个 setgroups 事件，之后只有第三个 setuid 调用设置目标用户，您就必须将 LOGINSEQUENCE 设置为 SGRP、SUID、FUID、N3UID。 您可以按任何顺序指定这些标志：

```
SETGRPS : P=565302 to 0,2,3,7,8,10,11,250,220,221,230

SUID  > P=565302 U=0   (R=0   E=0   S=0   ) to (R=0  E=0   S=0   ) () BYPASS
SUID  > P=565302 U=0   (R=0   E=0   S=0   ) to (R=0  E=0   S=-1  ) () BYPASS
LOGIN  : P=565302 User=target Terminal=mercury
```

- SETGRPS 进程表示的是触发器。
- 第一个 SUID 命令应该被忽略，因为您可以看见超级用户只是更改回超级用户，而不是触发器用户。 （这是顺序中的 SUID。）
- 第二个 SUID 命令也应该被忽略，因为您可以看见超级用户只是更改回超级用户，而不是触发器用户。 （这是顺序中的 FUID。）
- LOGIN 事件是实际引发登录的 SETUID 事件。 （因为它是第三个事件，所以它是顺序中的 N3UID 标志。)

在 chres、editres 或 newres 命令中使用 loginsequence 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

MFTERMINAL 类

MFTERMINAL 类中的每个记录定义一个用于管理 CA Access Control 的大型计算机。 该类具有与 TERMINAL 类相同的特性，但不会被 CA Access Control 截获。

MFTERMINAL 类的关键字是大型机的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

POLICY 类

POLICY 类中的每个记录都定义部署和取消部署策略版本所需的信息。 该类包括指向 RULESET 对象的链接，而这些对象包含用于部署和取消部署策略的 selang 命令列表。 部署策略后，将运行 deploy selang 命令，该命令执行定义策略并存储在已链接的 RULESET 对象中的所有命令。 取消部署策略后，将运行 deploy- selang 命令，该命令执行定义策略取消部署并存储在已链接的 RULESET 对象中的所有命令。

POLICY 类的关键字是后跟散列符号 (#) 和两位版本号的策略的名称。 例如，mypolicy#13。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EFFECTS_ON

定义此策略为有效（应部署）的主机（HNODE 对象）列表。

FINALIZE

指定此策略版本是否已最终确定（可以部署）。

GROUPS

定义资源记录所属的 CONTAINER 记录列表或此策略版本所属的 GPOLICY 对象列表。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

HNODES

（信息性）。 应已部署此策略的 CA Access Control 节点列表。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

POLICY_BASE_NAME

定义此策略版本所属的 GPOLICY 对象的名称。

POLICY_VERSION

定义此策略版本的版本号。

POLICY_TYPE

定义策略类型。 有效值包括：

- 无
- Login - 指定策略是 UNAB 登录策略。
- Configuration - 指定策略是 UNAB 配置策略。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

RULESETS

定义策略的 RULESET 对象的列表。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SIGNATURE

基于与策略相关联的 RULESET 对象签名的散列值。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

变量

（信息性）在策略中显示变量的所有版本。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

PROCESS 类

PROCESS 类中的每个记录定义一个程序（即可执行文件），该程序在自己的地址空间中运行并需要得到保护以免被终止。 主要工具和数据库服务器是 进程保护的最佳候选对象，因为这些进程是拒绝服务攻击的主要目标。

注意：在 PROCESS 类中定义程序时，我们建议您也在 FILE 类中定义该程序。 这可防止某些人未经授权修改（替换或损坏）可执行文件，从而保护可执行文件。

CA Access Control 可以防止三种终止信号：常规终止信号 (SIGTERM) 和应用程序无法屏蔽的两种信号（SIGKILL 和 SIGSTOP）：

环境	信号	数值
Windows	KILL	Win32 API
UNIX	终止进程	9
UNIX 和 Windows	STOP	视计算机而定
UNIX 和 Windows	TERM	15

其他信号（如 SIGHUP 或 SIGUSR1）传递给它们的目标进程，并且该进程决定是否忽略终止信号或是否以某种方式对它作出反应。

PROCESS 类记录的关键字是记录所保护的程序的名称。 请指定完整的路径。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不能修改标记为 *信息性*的属性。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

PROGRAM 类

PROGRAM 类中的每个记录都定义被认为是受信任计算基础的一部分的程序。 该类中的程序被认定是绝无安全漏洞的，因为它们由监视程序监控，可确保它们不会被修改。 如果受托程序被更改，CA Access Control 会自动将该程序标记为取消受托的程序，并阻止执行该程序。另外，您还可以使用 BLOCKRUN 属性来允许或阻止执行取消受托程序。

每个 PROGRAM 记录都包含几个可以定义可信任程序文件信息的属性。

使用注意事项：

- 在 UNIX 中，PROGRAM 类也可能包含未标记为 setuid 或 setgid 的程序。
- 可以在 CA Access Control 中将任何程序定义为受托程序。

  程序是不能在程序访问控制列表 (PACL) 中使用的，除非它已在 PROGRAM 类中定义。（但是，当程序添加到 PACL 中时也会自动添加到 PROGRAM 类中。）
- 不能在 PROGRAM 类中定义目录。

PROGRAM 类记录的关键字是记录所保护的程序的文件名。 必须将文件的完整路径指定为对象**名称。**

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不能修改标记为 *信息性* 的属性。

ACCSTIME

（信息性）。 上次访问记录的日期和时间。

ACCSWHO

（信息性）。 上次访问该记录的管理员。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

BLOCKRUN

指定是否对程序受托与否进行检查并阻止执行取消受托程序。 无论程序是 setuid 还是常规程序，都会阻止执行它。

在 chres、editres 和 newres 命令中使用 blockrun[-] 参数，可以修改该资源属性。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

MD5

（信息性）。 文件的 RSA-MD5 签名。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

注意：对于 PROGRAM 类中的资源，PACL 仅适用于 UNIX 中的 setuid/setgid 程序或 Windows 中具有*文件*资源的程序。 CA Access Control 首先检查文件资源记录，如果允许访问，则会检查程序资源记录。

PGMINFO

定义由 CA Access Control 自动生成的程序信息。

监视程序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。

可以选择下列任一标志，以便从该验证过程中*排除*关联信息：

crc

循环冗余检查和 MD5 签名。

ctime

（仅适用于 UNIX）上次更改文件状态的时间。

device

UNIX 中文件所在的逻辑磁盘。 Windows 中包含文件的磁盘的驱动器号。

group

拥有程序文件的组。

inode

UNIX 中程序文件的文件系统地址。 在 Windows 中，这没有任何意义

事务模式

程序文件的相关安全保护模式。

mtime

上次修改程序文件的时间。

owner

拥有程序文件的用户。

sha1

SHA1 签名。 称为安全散列算法的数字签名方法，可应用于程序或敏感文件。

大小

程序文件的大小。

在 chres、editres 或 newres 命令中使用 flags、flags+ 或 flags- 参数，可以修改该属性的标志。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UNTRUST

定义资源是否未受托。 如果设置了 UNTRUST 属性，则访问者将无法使用该资源。 如果未设置 UNTRUST 属性，则资源数据库中列出的其他属性将用于确定访问者的访问权限。 如果以任何方式更改了受托资源，CA Access Control 会自动设置 UNTRUST 属性。

在 chres、editres 或 newres 命令中使用 trust[-] 参数可以修改该属性。

UNTRUSTREASON

（信息性）。 程序已取消受托的原因。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

PWPOLICY 类

PWPOLICY 类中的每个记录定义一个密码策略。 这些策略是多个规则集，用于检查新密码的有效性并定义密码的有效时间。

PWPOLICY 类的关键字是密码策略的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

APPLS

（信息性）。 链接到密码策略的 CA SSO 应用程序的列表。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

OWNER

定义拥有记录的用户或组。

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。

在 setoptions 命令中使用 password 参数以及 rules 或 rules- 选项可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

REGKEY 类

在 Windows 上有效

REGKEY 类中的每个记录定义 Windows 注册表中的一个注册表键。

REGKEY 记录的关键字是 REGKEY 记录的完整注册表路径。

注意：可以将通配符用作路径规范的一部分。

默认情况下，CA Access Control 保护 CA Access Control 注册表项。 该注册表项的根路径是：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl
```

CA Access Control 还保护以下注册表键：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

REGKEY 类和 REGVAL 类具有相同的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

REGVAL 类

在 Windows 上有效

REGVAL 类中的每个记录定义 Windows 注册表中的一个值。

REGVAL 记录的关键字是该值的完整注册表路径。

注意：可以将通配符用作路径规范的一部分。

REGVAL 类允许使用以下访问类型：NONE、READ、WRITE、DELETE。

REGVAL 类和 REGKEY 类具有相同的属性。 这些参数如下所示。（不可修改的属性标记为*信息性*。）

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

RESOURCE_DESC 类

RESOURCE_DESC 类中的每个记录都定义 CA SSO 中允许用户定义的类对象访问的所有名称。 不能在 RESOURCE_DESC 类中创建新的对象，只能修改当前的对象。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

CLASS_RIGHT

32 种可选访问权限；全都可以修改。 前四种权限的默认设置如下：

- CLASS_RIGHT1 - 读取
- CLASS_RIGHT2 - 写入
- CLASS_RIGHT3 - 执行
- CLASS_RIGHT4 - 重命名

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

RESPONSE_LIST

包含该对象名称的 RESPONSE_TAB 类中的对象的名称。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

RESPONSE_TAB 类

RESPONSE_TAB 类中的每个记录为不同授权决策定义一个 CA SSO 响应表。

响应是拟人化的回答，在授权请求被准许或拒绝之后将它返回给应用程序。 它由特定应用程序所能理解的 KEY=VALUE 对组成。 响应提供根据用户的特定需要和授权许可将门户站点拟人化的能力。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

CLASS_RIGHT

32 种可选响应属性是包含 KEY=VALUE 对（例如，button1=yes、picture2=no 等）的字符串的列表。 每个访问值都应该有一个对应属性。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OF_RESOURCE

RESOURCE_DESC 类中引用同一个用户定义类的对象的名称。

OWNER

定义拥有记录的用户或组。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

RULESET 类

RULESET 类中的每个记录都定义一组用于定义策略的规则。

RULESET 类记录的关键字是记录所链接的策略的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EXPANDED COMMANDS

（信息性）显示已部署策略中的命令的变量值。

EXPANDED UNDO COMMANDS

（信息性）显示已部署策略中的撤销命令的变量值。

FINALIZE

指定 selang 脚本是否已最终确定（因此可以部署策略版本）。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

RULESET_DOCMD_IDX

（信息性）。 命令索引，即 RULESET_DOCMDS 列表中命令数量的计数器。

RULESET_DOCMDS

同时还定义策略的 selang 命令的列表。 这些是部署策略需要执行的命令。

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。 UNIX（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。

RULESET_POLICIES

（信息性）。 使用该组规则的策略（POLICY 对象）列表。

RULESET_UNDOCMD_IDX

（信息性）。 命令索引，即 RULESET_UNDOCMDS 列表中命令数量的计数器。

RULESET_UNDOCMDS

同时还定义策略取消部署脚本的 selang 命令的列表。 这些是取消部署策略需要执行的命令。

SECLABEL

定义用户或资源的安全级别。

注意： SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意： 该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SIGNATURE

基于 RULESET_DOCMDS 和 RULESET_UNDOCMDS 属性的散列值。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

SECFILE 类

SECFILE 类中的每个记录都定义要监视的文件。 SECFILE 类记录为系统中的重要文件提供验证。 但它们不能显示在条件访问控制列表中。

将不常修改的敏感系统文件添加到该类中，以确认未经授权的用户没有改变它们。 下列是要包括在 SECFILE 类中的文件类型的一些示例：

在 UNIX 中	Windows
/.rhosts	\system32\drivers\etc\hosts
/etc/services	\system32\drivers\etc\services
/etc/protocols	\system32\drivers\etc\protocols
/etc/hosts	
/etc/hosts.equiv	

监视程序将扫描这些文件并确保有关这些文件的已知信息没有被修改。

注意：不能在 SECFILE 类中定义目录。

SECFILE 类记录的关键字是 SECFILE 记录所保护的文件的名称。 请指定完整的路径。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

AIXACL

AIX 系统 ACL。

AICEXTI

AIX 系统的扩展信息。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

HPUXACL

HP-UX 系统 ACL。

MD5

（信息性）。 文件的 RSA-MD5 签名。

OWNER

定义拥有记录的用户或组。

PGMINFO

定义由 CA Access Control 自动生成的程序信息。

监视程序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。

可以选择下列任一标志，以便从该验证过程中*排除*关联信息：

crc

循环冗余检查和 MD5 签名。

ctime

（仅适用于 UNIX）上次更改文件状态的时间。

device

UNIX 中文件所在的逻辑磁盘。 Windows 中包含文件的磁盘的驱动器号。

group

拥有程序文件的组。

inode

UNIX 中程序文件的文件系统地址。 在 Windows 中，这没有任何意义

事务模式

程序文件的相关安全保护模式。

mtime

上次修改程序文件的时间。

owner

拥有程序文件的用户。

sha1

SHA1 签名。 称为安全散列算法的数字签名方法，可应用于程序或敏感文件。

大小

程序文件的大小。

在 chres、editres 或 newres 命令中使用 flags、flags+ 或 flags- 参数，可以修改该属性的标志。

UNTRUST

定义资源是否未受托。 如果设置了 UNTRUST 属性，则访问者将无法使用该资源。 如果未设置 UNTRUST 属性，则资源数据库中列出的其他属性将用于确定访问者的访问权限。 如果以任何方式更改了受托资源，CA Access Control 会自动设置 UNTRUST 属性。

在 chres、editres 或 newres 命令中使用 trust[-] 参数可以修改该属性。

UNTRUSTREASON

（信息性）。 程序已取消受托的原因。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

SECLABEL 类

SECLABEL 类中的每个记录都将安全级别与安全类别相关联。 如果 SECLABEL 类处于活动状态，安全标签会覆盖 USER 记录中特定的安全级别和安全类别分配。 分配安全标签等同于显式地向用户分配安全标签的安全级别和安全类别。

当 USER 记录中包含安全标签时，则只有在符合下列条件时，用户才可以访问资源：

- 安全标签中指定的用户安全级别等于或高于资源安全级别。
- 资源记录中指定的所有类别都包含在用户安全标签的安全类别列表中。

注意：在 Windows 中，每个定义到 CA Access Control 的安全标签都必须在 SECLABEL 类中有记录。

SECLABEL 类记录的关键字是安全标签的名称。 将该名称分配给用户或资源时，它用于标识安全标签。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

OWNER

定义拥有记录的用户或组。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

SEOS 类

SEOS 类控制 CA Access Control 授权系统的行为。

该类中只包含一个记录，名为 SEOS，指定一般的安全和授权选项。 要查看或更改 SEOS 类属性的状态，请使用 setoptions 命令。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACCPACL

指出在授权期间 UACC (defaccess) 和 PACL 列表的扫描顺序。

当 ACCPACL 处于活动状态而且通过 ACL 为用户提供了显式访问时，该访问就是准许的访问。 如果没有通过 ACL 提供显式访问，而是通过 PACL 定义了显式访问，则 PACL 访问就是准许的访问。如果 ACL 或 PACL 都不包含显式访问，就会检查 defaccess 中是否有访问定义。

如果 ACCPACL 未被激活，则仍会首先检查 ACL 中是否有显式访问。如果 ACL 中不包含正被检查的资源的显式访问定义，就会接着检查 defaccess 定义。 如果在 defaccess 中没有定义显式访问，就会检查 PACL 访问定义。

当安装 CA Access Control 时，该属性的值设置为 yes。

在 setoptions 命令中使用 accpacl 或 accpacl- 参数可以修改该属性。

ADMIN

指出 ADMIN 类是否处于活动状态。 通常，ADMIN 类处于活动状态并控制执行安全管理任务的权限。 如果 ADMIN 类处于不活动状态，则所有用户都能够以 CA Access Control 管理员身份工作。

APPL

指出 APPL 类是否处于活动状态。

AUTHHOST

指出 AUTHHOST 类是否处于活动状态。

CALENDAR

指出 CALENDAR 类是否处于活动状态。

CATEGORY

指出 CATEGORY 类是否处于活动状态。

CNG_ADMIN_PWD

指出具有 PWMANAGER 属性的用户是否可以使用 selang 更改 ADMIN 用户密码。 默认值是 yes。

在 setoptions 命令中使用 class+ 或 class- 参数以及 *cng_adminpwd* 选项，可以激活或停用该属性。

CNG_OWN_PWD

指出用户是否可以使用 selang 更改自己的密码。

在 setoptions 命令中使用 class+ 或 class- 参数以及 *cng_ownpwd* 选项，可以激活或停用该属性。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CONNECT

指出 CONNECT 类是否处于活动状态。 当 CONNECT 类处于活动状态时，类中的记录会保护传出的连接。

如果 HOST 类处于活动状态，CONNECT 类就不用作活动类，即使被激活时也是如此。

如果 TCP 类处于活动状态，CONNECT 类就不用作活动类。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIMERES

（仅适用于 UNIX）指出 CA Access Control 是否检查对资源的日间限制。

DMS

此数据库应将通知发送到的 DMS 服务器的列表。

DOMAIN

（仅适用于 Windows）指出 DOMAIN 类是否处于活动状态。

ENDTIME

（信息性）。 上次按顺序关闭数据库文件的日期和时间。

FILE

指出 FILE 类是否处于活动状态。 当 FILE 类处于活动状态时，类中的记录会保护文件和目录。

ACCGRR

*累积组权限*选项 (ACCGRR) 影响 CA Access Control 检查资源的 ACL 的方式。 如果启用 ACCGRR，则 CA Access Control 会检查 ACL 以获得用户所属的所有组授予的权限。如果禁用 ACCGRR，则 CA Access Control 会检查 ACL 以查看是否有任何可应用的条目包含值 none。 如果有，则会拒绝访问。 否则 CA Access Control 将忽略所有组条目，Access Control 列表中的第一个可应用的条目除外。

使用命令 setoptions ACCGRR 命令来启用或禁用此属性。

HOLIDAY

指出 HOLIDAY 类是否处于活动状态。当 HOLIDAY 类处于活动状态时，在定义的假日时间段内，用户需要拥有额外的权限才能登录。

HOST

指出 HOST 类是否处于活动状态。 当 HOST 类处于活动状态时，CA Access Control 保护来自远程主机的传入 TCP/IP 服务请求。

如果 HOST 类处于活动状态，TCP 和 CONNECT 类就不用作活动类，即使被激活时也是如此。

默认情况下，HOST 类处于活动状态。

INACT

指出用户登录被挂起后的不活动天数。 非活动日是指用户不登录的日子。

USER 记录中的 INACTIVE 属性值会覆盖 GROUP 记录中的值。 这二者都会覆盖 SEOS 类记录中的 INACT 属性。

在 setoptions 命令中使用 inactive 或 inactive- 参数可以更新该属性。

ISDMS

如果 PMDB 用作 DMS 则为真。

LOGINAPPL

（仅适用于 UNIX）指出 LOGINAPPL 类是否处于活动状态。

MAXLOGINS

允许用户进行的并发登录（终端会话）的最大数目，超过此数目后用户被拒绝访问。 值为 0 表示没有最大数量限制，用户可以并发登录任何数量的终端会话。该值必须为零或大于 1（如果用户希望登录并运行 selang 或者管理数据库），因为 CA Access Control 认为每个任务（登录、selang、GUI 等）都是终端会话。

USER 记录中的 MAXLOGINS 属性值会覆盖 GROUP 记录中的值。 这二者都会覆盖 SEOS 类记录中的 MAXLOGINS 属性。 当访问者记录中没有显式值时，SEOS 记录中的值便用作默认值。

在 chres、editres 和 newres 命令中使用 maxlogins 参数可以修改 SEOS 类的该属性。

MFTERMINAL

指出 MFTERMINAL 类是否处于活动状态。

PASSWDRULES

指出密码规则。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。

在 setoptions 命令中使用 password 参数以及 rules 或 rules- 选项可以修改该属性。

PASSWORD

指出密码检查是否处于活动状态。

在 setoptions 命令中使用 class+ 或 class- 参数以及 PASSWORD 选项，可以激活或停用该属性。

PROCESS

指出 PROCESS 类是否处于活动状态。当 PROCESS 类处于活动状态时，类中的记录会保护定义的进程不受终止尝试的影响。

另外，相关的文件也必须在 FILE 类中定义。

PROGRAM

指出 PROGRAM 类是否处于活动状态。当 PROGRAM 类处于活动状态时，类中的记录会保护标记为受信任的已定义进程。

PWPOLICY

指出 PWPOLICY 类是否处于活动状态。

REGKEY

（仅适用于 Windows）指出 REGKEY 类是否处于活动状态。

REGVAL

（仅适用于 Windows）指出 REGVAL 类是否处于活动状态。

RESOURCE_DESC

指出 RESOURCE_DESC 类是否处于活动状态。

RESPONSE_TAB

指出 RESPONSE_TAB 类是否处于活动状态。

SECLABEL

指出 SECLABEL 类是否处于活动状态。

SECLEVEL

指出 SECLEVEL 类是否处于活动状态。

STARTTIME

（信息性）。 上次打开数据库文件的日期和时间。

SUDO

指出由 sesudo 使用的 SUDO 类是否处于活动状态。

SYSTEM_AAUDIT_MODE

为用户和企业用户指定默认审核模式（系统范围的审核模式）。

默认值：Failure LoginSuccess LoginFailure

SURROGATE

指出 SURROGATE 类是否处于活动状态。 当 SURROGATE 类处于活动状态时，CA Access Control 会保护代理请求。

TCP

指出 TCP 类是否处于活动状态。当 TCP 类处于活动状态时，CA Access Control 会保护传入和传出 TCP 服务，例如邮件、ftp 和 http。

如果 HOST 类处于活动状态，TCP 类就不用作活动类，即使被激活时也是如此。

如果 TCP 类处于活动状态，CONNECT 类就不用作活动类。

TERMINAL

指出 TERMINAL 类是否处于活动状态。 当 TERMINAL 类处于活动状态时，CA Access Control 会在登录期间执行终端访问检查并保护 X-window 会话。

USER_ATTR

指出 USER_ATTR 类是否处于活动状态。

USER_DIR

指出 USER_DIR 类是否处于活动状态。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

SPECIALPGM 类

SPECIALPGM 类为指定的程序提供特殊的安全权限。

SPECIALPGM 类中的每个记录都具有下面两种功能之一：

- 在 Windows 中注册 backup、DCM、PBF、PBN、STOP、SURROGATE、REGISTRY 和 KILL 程序，或者在 UNIX 中注册 xdm、backup、mail、DCM、PBF、PBN、stop 和 surrogate 程序。
- 将需要特殊的 CA Access Control 授权保护的应用程序与逻辑用户 ID 相关联。 这样，就可以有效地允许您根据正在做*什么*而不是*谁*在做来设置访问权限。

注意：在 SPECIALPGM 类中定义程序时，我们建议您也在 FILE 类中定义该程序。 FILE 资源通过防止某些人未经授权修改（替换或损坏）可执行文件来保护可执行文件，如果在 CA Access Control 未运行时修改了程序，则 PROGRAM 资源会确保该程序不运行。

注意：您无法在 SPECIALPGM 类中为传入网络截获事件定义记录。 这是因为传入网络截获事件在此上下文中没有进程名称。 要跳过为截获事件写入审核记录的过程，对于 TCP 类中的相应记录，请将 AUDIT 属性设置为 NONE。

使用 PGMTYPE 属性可以注册系统服务、后台进程或其他特殊程序。

使用 SEOSUID 和 NATIVEUID 属性可以将逻辑用户分配给程序。

SPECIALPGM 类记录的关键字是特殊程序的路径，或者特殊程序的范围或模式的路径。

注意：可以在 specialpgm 类表中写入的规则的最大数目是 512。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

NATIVEUID

指出调用程序或进程的用户。 使用 * 可以指定所有的 CA Access Control 用户。

在 chres、editres 或 newres 命令中使用 nativeuid 参数可以修改该属性。

注意：为了与 CA Access Control 的早期版本向后兼容，可以使用 UNIXUID 属性代替 NATIVEUID 属性。

OWNER

定义拥有记录的用户或组。

PGMTYPE

确定在授予访问权限时 CA Access Control 回避的访问检查的类型。

backup

回避 READ、CHDIR 和 UTIME 访问。

注意：有两种方法可以运行成功的备份。 如果 backup 程序由非超级用户执行，您就必须将该用户定义为 OPERATOR。 如果 backup 程序由超级用户执行，则只要在 SPECIALPGM 类中将 backup 程序注册为 pgmtype（备份）即可。

changeid

（仅适用于 UNIX）跳过 PAM 启用的 surrogate 身份更改工具，如 su。

例如：*er specialpgm /bin/su pgmtype(changeid)*

dcm

对于除 STOP 事件外的所有事件回避所有安全检查。

fullbypass

完全跳过所有的 CA Access Control 授权和数据库检查。 CA Access Control 会忽略具有该属性的进程，且不会在 CA Access Control 审核、跟踪或调试日志中显示任何进程事件的记录。

kill

（仅适用于 Windows）跳过进程的程序终止。

例如，如果此进程尝试打开带有访问掩码 KILL 的 CA Access Control 服务（进程）句柄，以下规则可跳过至 services.exe：

```
nr specialpgm c:\Windows\system32\services.exe pgmtype(kill)
```

在 Windows Server 2008 上，services.exe 进程（用于管理服务的启动和停止）可打开访问类型为 KILL 的 CA Access Control 服务（进程）句柄，管理进程的终止和启动。在安装到 Windows Server 2008 期间，CA Access Control 将运行搜索进程以查找 services.exe 并为其创建跳过规则。 若不应用此跳过，services.exe 尝试打开 CA Access Control 服务的句柄时您将收到 DENIED CA Access Control 审核事件。

mail

（仅适用于 UNIX）跳过对 setuid 和 setgid 事件的数据库检查。邮件回避允许您跟踪邮件访问尝试。

none

删除之前设置的所有 PGMTYPE。

pbf

对文件处理事件回避数据库检查。

pbn

对网络相关事件回避数据库检查。

propagate

（仅适用于 UNIX）将其本身的安全权限传播到由带有此 PGMTYPE 的程序调用的所有程序。 如果您不指定此参数，SPECIALPGM 权限仅可影响父程序。

注意：安全权限传播仅与 PBF、PBN、DCM、FULLBYPASS 以及 SURROGATE 权限一起使用。

registry

（仅适用于 Windows）跳过对控制 Windows 注册表的程序的数据库检查。

stop

对 STOP 功能回避数据库检查。

surrogate

对内核中的身份更改事件回避数据库检查。 如果使用替换回避，就无法跟踪。

xdm

（仅适用于 UNIX）跳过有限网络范围 (6000-6010) 的网络事件（如 TCP、HOST 和 CONNECT 类）。

在 chres、editres 或 newres 命令中使用 pgmtype 参数可以修改该属性。

SEOSUID

定义得到授权运行此特殊程序的代理逻辑用户。 该逻辑用户必须在带有 USER 记录的数据库中定义。

在 chres、editres 或 newres 命令中使用 seosuid 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

示例：保护 UNIX 文件

为保护驻留在 /DATABASE/data/* 中的文件，数据库管理员会使用名为 firmdb_filemgr 的文件服务器后台进程。 该文件服务器驻留在 /opt/dbfirm/bin/firmdb_filemgr 上。 该后台进程通常以 root 用户身份运行，从而使数据可以由任何 root 用户 shell 攻击进行访问。

在下面的示例中，逻辑用户被定义为这些文件的唯一访问者；禁止其他用户访问这些文件：

1. 使用以下命令在 CA Access Control 中定义“敏感”文件：

   ```
   newres file /DATABASE/data/* defaccess(NONE)owner(nobody)
   ```

2. 定义访问文件的逻辑用户：

   ```
   newusr firmDB_mgr
   ```

3. 只允许逻辑用户 firmDB_mgr 访问文件。

   ```
   authorize file /DATABASE/data/* uid(firmDB_mgr) access(ALL)
   ```

4. 最后，让 firmdb_filemgr 以逻辑用户 firmDB_mgr 的身份运行

   ```
   newres SPECIALPGM /opt/dbfirm/bin/firmdb_filemgr unixuid(root) \
   seosuid(firmDB_mgr)
   ```

因此，当后台程序访问文件时，CA Access Control 会认为逻辑用户是文件的访问者，而 root 用户不是文件的访问者。 尝试以超级用户身份访问文件的黑客是不会成功的。

示例：保护 Windows 文件

为保护位于 C:\DATABASE\data 中的文件，数据库管理员会使用名为 firmdb_filemgr.exe 的文件服务器服务。 该文件服务器位于 C:\Program Files\dbfirm\bin\firmdb_filemgr.exe 上。 该服务通常用系统帐户运行，从而使得任何系统黑客都可以访问该数据。

在下面的示例中，逻辑用户被定义为这些文件的唯一访问者；禁止其他用户访问这些文件：

1. 使用以下命令在 CA Access Control 中定义“敏感”文件：

   ```
   newres file C:\DATABASE\data\* defaccess(NONE)owner(nobody)
   ```

2. 定义访问文件的逻辑用户：

   ```
   newusr firmDB_mgr
   ```

3. 只允许逻辑用户 firmDB_mgr 访问文件：

   ```
   authorize file C:\DATABASE\data\* uid(firmDB_mgr) access(ALL)
   ```

4. 最后，让 firmdb_filemgr 以逻辑用户 firmDB_mgr 身份运行：

   ```
   newres SPECIALPGM ("C:\Program Files\dbfirm\bin\firmdb_filemgr.exe") \
   nativeuid(system) seosuid(firmDB_mgr)
   ```

因此，当服务访问文件时，CA Access Control 会认为逻辑用户是文件的访问者，而系统帐户不是文件的访问者。 尝试以系统帐号访问文件的黑客是不会成功的。

SUDO 类

SUDO 类中的每个记录标识一个用户可以从使用 sesudo 命令的另一个用户借用权限的一个命令。

SUDO 类记录的关键字是 SUDO 记录的名称。 当用户执行 SUDO 记录中的命令时，会使用该名称来代替命令名称。

注意：如果创建交互式 Windows 应用程序的 SUDO 记录，您必须设置 SUDO 记录的交互式标记。 如果不设置交互式标志，应用程序会在后台运行，而您无法与其进行交互。 有关详细信息，请参阅*《疑难解答指南》*。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

sesudo 执行的命令。

由字母数字组成的字符串，最多可包含 255 个字符，它包含命令以及准许和禁止的参数。

例如，以下配置文件定义正确地使用了 COMMENT 属性：

```
newres SUDO profile_name comment('command;;NAME')
```

注意：COMMENT 属性的这种用法与在其他类中不同。 有关定义 SUDO 记录的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。 该属性在 CA Access Control 的早期版本中还称为 DATA。

范围：255 个字符。

在 chres、editres 和 newres 命令中使用 comment[-] 参数可以修改该属性。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 GSUDO 或 CONTAINER 记录的列表。

要修改 SUDO 类记录中的该属性，必须在相应的 CONTAINER 或 GSUDO 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

INTERACTIVE

（仅适用于 Windows）。 如果您要通过 sesudo 运行的应用程序是互动式 Windows 应用程序（例如，notepad.exe 或 cmd.exe）而不是服务应用程序，则应标记该开关参数。 如果您尝试使用 sesudo 运行未标记为*互动式*的互动式应用程序，则该应用程序会在后台运行且无法与其交互。

注意：由于 Windows 限制，某些 Windows 应用程序无法在前台运行。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

PASSWORDREQ

（仅适用于 UNIX）指出 sesudo 命令是否在执行前请求最初用户的密码。

在 chres、editres 或 newres 命令中使用 password 参数可以修改该属性。

POLICYMODEL

指定当您使用 sepass 实用程序更改用户密码时接收新密码的 PMDB。如果为该属性输入了值，则密码就*不*发送到由 parent_pmd 或 passwd_pmd 配置设置定义的策略模型。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 pmdb[-] 参数相对应。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

TARGUSR

（仅 UNIX）指出标识被借用以执行命令的用户的目标 uid。默认值为 root。

在 chres、editres 或 newres 命令中使用 targuid 参数可以修改该属性。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

SURROGATE 类

SURROGATE 类中的每个记录都定义若干限制，以防止除某个用户外的其他用户将其身份更改为该用户的身份。 CA Access Control 将更改身份请求视为一个只能由授权用户访问的抽象对象。

SURROGATE 类中的记录表示每个具有替换保护的用户或组。 两个特殊的记录 USER._default 和 GROUP._default 表示没有单独 SURROGATE 记录的用户和组。 如果不需要区分用户的默认设置和组的默认设置，您可以将 _default 记录用于 SURROGATE 类。

注意：许多 Windows 实用程序和服务（例如“Run As”）标识为用户 *NT AUTHORITY\SYSTEM* 而不是将其作为原始用户运行。 要让使用这些实用程序或服务的用户模拟另一个用户，您必须在 CA Access Control 数据库中创建该 SYSTEM 用户并授权它模拟目标用户。

SURROGATE 类记录的关键字是 SURROGATE 记录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

TCP 类

TCP 类中的每个记录定义一个 TCP/IP 服务（例如邮件、ftp 和 http）。 当 TCP 类正被用于授权时，只有在 TCP 资源准许访问的情况下，主机才能从本地主机获取服务。 同样，只有在 TCP 资源授予访问权限的情况下，本地主机上的用户或组才能使用 TCP/IP 服务访问远程主机。

TCP 记录中的 ACL 可以为主机 (HOST)、主机组 (GHOST)、网络 (HOSTNET) 和主机集 (HOSTNP) 指定访问类型。

TCP 记录中的 CACL 可以为主机 (HOST)、主机组 (GHOST)、网络 (HOSTNET) 和主机集 (HOSTNP) 指定访问类型，还可以为用户和组指定访问类型。

可以基于 IPv4 地址而不仅仅基于主机名来设置规则。 也就是说，您可以更改域名。

注意：CA Access Control 的 IP 通信访问规则仅适用于 IPv4。 CA Access Control 不控制通过 IPv6 进行的访问。

注意：如果 CONNECT 类用作访问的标准，则 TCP 类无法有效地控制访问。 使用 TCP 类或 CONECT 类保护连接，而不是同时使用这两类。

TCP 记录的关键字是 TCP/IP 服务的名称。 TCP 类控制传出的服务和传入的服务。

以下定义介绍了 TCP 类记录中包含的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

ACL

定义本地主机提供服务的主机和允许的访问类型。

访问控制列表中的每个元素均包含下列信息：

主机引用

定义 HOST、GHOST、HOSTNET 或 HOSTNP 记录。

允许的访问权限

引用的主机对资源拥有的访问权限。 有效的访问权限包括：

- **无** - 不允许主机执行任何操作。
- **读取 -** 允许主机从本地主机获取 TCP 服务。

在 authorize 或 authorize- 命令中使用 access 参数可以修改该属性

CACL

允许访问资源的访问者（用户和组）及其可以访问的主机的列表。条件 Access Control 列表 (CACL) 中的每个元素均包含以下信息：

访问者

定义访问者。

主机引用

定义 HOST、GHOST、HOSTNET 或 HOSTNP 记录

访问

定义访问者对资源的访问权限。 有效的访问类型包括：

- **写入 -** 允许访问者使用该服务访问主机或主机组。
- **无 –** 不允许访问者使用该服务访问主机或主机组。

使用 authorize 或 authorize- 命令可以修改该属性。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

TERMINAL 类

TERMINAL 类中的每个记录都定义本地主机的终端、网络上的另一主机或者可以进行登录会话的 X 终端。 还可以定义与终端*名称或 IP 地址模式（使用通配符）匹配的终端。 用户登录过程中将检查终端权限，以使用户无法从未授权其使用的终端上成功登录。*

另外，TERMINAL 类还控制管理访问。 ADMIN 用户只能从其拥有适当访问权限的终端对 CA Access Control 进行管理。

当定义新的 TERMINAL 记录时，CA Access Control 尝试将您提供的名称转换为完全限定名。 如果成功，它会在数据库中存储完全限定的名称。 如果失败，它会存储您指定的名称。 当您发出引用该记录的后续命令（chres、showres、rmres、authorize 等）时，必须使用在数据库中显示的名称。

TERMINAL 记录的关键字是终端的名称。 该名称将终端标识到 CA Access Control。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 GTERMINAL 或 CONTAINER 记录的列表。

要修改 TERMINAL 类记录中的该属性，必须在相应的 CONTAINER 或 GTERMINAL 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

UACC 类

UACC 类中的每个记录都定义允许对资源类进行的默认访问。 另外，UACC 记录还确定允许对该类的不受 CA Access Control 保护的资源进行访问的访问级别。

UACC 适用于大多数类，但不是所有类。 下表说明每个类如何使用 UACC 类。

UACC 使用	类
标准	ADMIN、APPL、AUTHHOST、CALENDAR、CONNECT、CONTAINER、DOMAIN、GAPPL、GAUTHHOST、GHOST、GSUDO、GTERMINAL、HOLIDAY、HOST、HOSTNET、HOSTNP、MFTERMINAL、POLICY、PROCESS、PROGRAM、REGKEY、REGVAL、RULESET、SUDO、SURROGATE、TCP、TERMINAL、USER_DIR、用户定义的类
非标准	FILE、GFILE
无	AGENT、AGENT_TYPE、CATEGORY、GROUP、PWPOLICY、RESOURCE_DESC、RESPONSE_TAB、SECFILE、SECLABEL、SEOS、SPECIALPGM、USER、USER_ATTR

对于特殊的 _restricted 组之外的用户，UACC 类中的 FILE 记录只保护作为 CA Access Control 一部分的文件，例如 seos.ini、seosd.trace、seos.audit 和 seos.error 文件。 这些文件没有显式定义到 CA Access Control，但自动受到 CA Access Control 的保护。

UACC 类记录的关键字是为其定义 UACC 属性的类的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

ALLOWACCS

该类的所有允许的访问列表。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

OWNER

定义拥有记录的用户或组。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USER 类

USER 类中的每个记录定义 CA Access Control 数据库中的一个用户。

USER 记录的关键字是用户的名称 - 用户在登录系统时输入的名称。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 chusr 更改大多数 USER 属性。 使用 chusr 无法更改标记为*信息性*的属性。

注意：在多数情况下，除非明确指出使用 chusr 更改属性，否则请将属性名称用作命令参数。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 showusr 查看所有属性。

APPLIST

由 CA SSO 使用。

APPLIST_TIME

由 CA SSO 使用。

APPLS

（信息性）显示授权访问者访问的应用程序列表。 由 CA SSO 使用。

AUDIT_MODE

定义 CA Access Control 在审核日志中记录的活动。可以指定下列活动的任何组合：

- 无登录
- 在跟踪文件中记录的所有活动
- 登录尝试失败
- 登录成功
- 对 CA Access Control 保护的资源进行的失败访问尝试
- 对 CA Access Control 保护的资源进行的成功访问
- 交互式登录

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的审核参数相对应。

AUTHNMTHD

（信息性）显示用于组记录的身份验证方法，从方法 1 到方法 32，或无。 由 CA SSO 使用。

BADPASSWD

由 CA SSO 使用。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

COUNTRY

指定用户所在国家/地区描述符的字符串。 该字符串是 X.500 命名方案的一部分。 CA Access Control 不使用该信息进行授权。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EMAIL

定义用户的电子邮件地址，最多为 128 个字符。

EXPIRE_DATE

定义访问者变为无效的日期。 用户记录中的 EXPIRE_DATE 属性值会覆盖组记录中的值。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 expire[-] 参数相对应。

FULLNAME

定义与访问者相关联的全名。CA Access Control 使用全名标识审核日志消息中的访问者，但不用于授权。

FULLNAME 是字母数字字符串。对于组，最大长度为 255 个字符。对于用户，最大长度为 47 个字符。

GAPPLS

（信息性）指出用户有权访问的应用程序组的列表。由 CA SSO 使用。

GRACELOGIN

定义用户在密码到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。

宽限登录次数必须介于 0 和 255 之间。 如果该值为 0，用户就不能登录。

USER 记录中的 GRACELOGIN 属性值会覆盖 GROUP 记录中 NGRACE 的值。 这二者都会覆盖 SEOS 类记录中的 PASSWDRULES 属性。

注意：该属性与 ch[x]usr 命令的 grace 参数相对应。

GROUPS

（信息性）显示用户所属的用户组列表。 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。

注意：该属性不能通过 ch[x]usr 命令修改。而使用 join[-] 或 joinx[-] 命令可以修改该属性。

HOMEDIR

（仅适用于 UNIX）定义用户的主目录。 由 CA SSO 使用。

INACTIVE

定义不活动天数，在该天数后系统会将用户的状态更改为不活动。如果帐户状态为不活动，则用户无法登录。

USER 记录中的 INACTIVE 属性值会覆盖 GROUP 记录中的值。 这二者都会覆盖 SEOS 类记录中的 INACT 属性。

注意：CA Access Control 不存储状态，而是动态地计算状态。 要标识不活动用户，必须将 INACTIVE 值与用户的 LAST_ACC_TIME 值进行比较。

LAST_ACC_TERM

显示执行上次登录的终端。

LAST_ACC_TIME

显示上次登录的日期和时间。

LOCALAPPS

由 CA SSO 使用。

LOCATION

定义用户位置。 CA Access Control 不使用此信息进行授权。

LOGININFO

定义用户登录到特定应用程序和审核数据所需的信息。 对于用户得到授权可以访问的每个应用程序，LOGININFO 中都包含了一个单独的列表。 由 CA SSO 使用。

LOGSHIFT

指出是否允许在班次时间外登录。CA Access Control 会为该事件在审核日志中写入一条审核记录。

MAXLOGINS

定义允许用户进行的并发登录的最大数目。 值为零表示用户可以进行任意数量的并发登录。

用户记录中的 MAXLOGINS 属性值会覆盖组记录中的值。 这二者都会覆盖 SEOS 类记录中的 MAXLOGINS 值。

MIN_TIME

定义用户两次更改密码之间允许的最短时间。

USER 记录中的 MIN_TIME 属性值会覆盖 GROUP 记录中的值。这二者都会覆盖 SEOS 类记录中的 PASSWDRULES 属性。

注意：该属性与 ch[x]usr 命令的 min_life 参数相对应。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OBJ_TYPE

指定用户权限属性。这些属性中的每个属性均与 ch[x]usr 命令中的同名参数相对应。 用户可以具有以下一个或多个权限属性：

ADMIN

指定用户是否可以执行管理功能，与 UNIX 环境中的 root 用户类似。

AUDITOR

指定用户是否可以监控系统、列出数据库中的信息以及为现有记录设置审核模式。

IGN_HOL

指定用户是否可以在 HOLIDAY 记录定义的任何时间段内登录。

LOGICAL

指定该用户仅供 CA Access Control 内部使用，而不能用于真实用户登录。

例如，您可用作资源所有者的用户 nobody 甚至可以防止资源所有者访问资源，该用户在默认情况下是逻辑用户。这意味着，没有用户可以使用该帐户登录。

OPERATOR

指定用户是否可以列出数据库中的所有内容及是否可以使用 secons 实用程序。

PWMANAGER

指定用户是否可以修改其他用户的密码设置及是否可以启用已经被 serevu 实用程序禁用的用户帐户。

SERVER

指定进程是否可以请求用户进行授权及是否可以发出 SEOSROUTE_VerifyCreate API 调用。

OIDCRDDATA

由 CA SSO 使用。

OLD_PASSWD

包含用户的以前密码的加密列表。用户不能从该列表中选择新密码。OLD_PASSWD 中保存的密码最大数目由 setoptions 命令决定。

ORG_UNIT

用于存储有关用户工作所在组织机构的信息的字符串。 该字符串是 X.500 命名方案的一部分。CA Access Control 不使用该信息进行授权。

ORGANIZATION

定义用户工作的组织。 该字符串是 X.500 命名方案的一部分。 CA Access Control 不使用该信息进行授权。

OWNER

定义拥有记录的用户或组。

PASSWD_A_C_W

指出上次更改该记录的用户密码的 ADMIN 用户。

PASSWD_INT

定义用户两次更改密码之间允许的最长时间。

USER 记录中的 PASSWD_INT 属性值会覆盖 GROUP 记录中的值。这二者都会覆盖 SEOS 类记录中的 PASSWDRULES 属性。

注意：该属性与 ch[x]usr 命令的 interval 参数相对应。

PASSWD_L_A_C

显示管理员上次更新密码的日期和时间。

PASSWD_L_C

显示用户上次更新密码的日期和时间。

PGMINFO

定义由 CA Access Control 自动生成的程序信息。

监视程序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。

可以选择下列任一标志，以便从该验证过程中*排除*关联信息：

crc

循环冗余检查和 MD5 签名。

ctime

（仅适用于 UNIX）上次更改文件状态的时间。

device

UNIX 中文件所在的逻辑磁盘。 Windows 中包含文件的磁盘的驱动器号。

group

拥有程序文件的组。

inode

UNIX 中程序文件的文件系统地址。 在 Windows 中，这没有任何意义

事务模式

程序文件的相关安全保护模式。

mtime

上次修改程序文件的时间。

owner

拥有程序文件的用户。

sha1

SHA1 签名。 称为安全散列算法的数字签名方法，可应用于程序或敏感文件。

大小

程序文件的大小。

在 chres、editres 或 newres 命令中使用 flags、flags+ 或 flags- 参数，可以修改该属性的标志。

PHONE

定义用户的电话号码。 不使用该信息进行授权。

POLICYMODEL

指定当您使用 sepass 实用程序更改用户密码时接收新密码的 PMDB。 如果为该属性输入了值，则密码就*不*发送到由 parent_pmd 或 passwd_pmd 配置设置定义的策略模型。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 pmdb[-] 参数相对应。

PROFILE

定义用户配置文件的路径。 该字符串中可以包含本地绝对路径或 UNC 路径。

PUPM_FLAGS

指定终端集成属性。 当您将 CA Access Control 端点上的特权帐户与 PUPM 相集成时，可使用终端集成。特权帐户可以有以下一个或两个终端集成属性：

use_original_identity

指定当 CA Access Control 作出授权决策时，使用签出帐户的用户的名称，而不是特权帐户的名称。 该会话的审核记录列出了真实用户名称字段中的最初用户和有效用户名称字段中的特权帐户。

required_checkout

指定必须在 PUPM 中签出帐户，用户才能使用它登录到端点。

PWD_AUTOGEN

显示用户密码是否是自动生成。 由 CA SSO 使用。

默认值为 no。

PWD_SYNC

显示所有用户应用程序的用户密码是否都自动保持一致。 由 CA SSO 使用。

默认值为 no。

RESUME_DATE

定义挂起的 USER 帐户变为取消挂起的日期。

RESUME_DATE 与 SUSPEND_DATE 配合工作。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 resume[-] 参数相对应。

REVACL

显示访问者的 Access Control 列表。

REVOKE_COUNT

由 CA SSO 使用。

SCRIPT_VARS

由 CA SSO 使用，定义变量列表，该列表中列出了每个应用程序保存的应用程序脚本的变量值。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SESSION_GROUP

为用户定义 SSO 会话组。SESSION_GROUP 属性是最长为 16 个字符的字符串。

在 Windows 中，管理员可以在首选名称不在下拉列表中的情况下输入会话组的新名称。

由 CA SSO 使用。

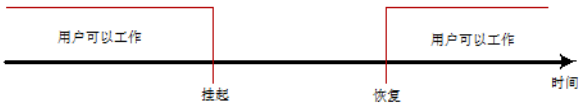
SHIFT

由 CA SSO 使用。

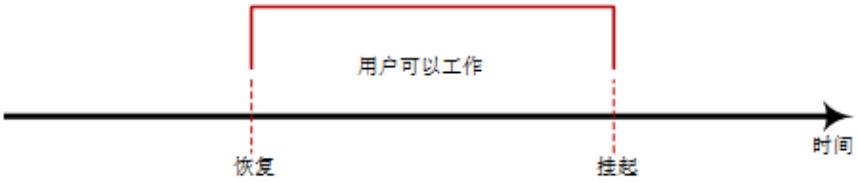
SUSPEND_DATE

定义用户帐户因挂起而变为无效的日期。

如果记录的挂起日期在其恢复日期之前，用户就可以在挂起日期前和恢复日期后工作。



如果用户的恢复日期早于挂起日期，则记录也会在该恢复日期*之前*无效。 用户仅可以在恢复日期和挂起日期之间进行工作。



用户记录中的 SUSPEND_DATE 属性值会覆盖组记录中的值。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 suspend[-] 参数相对应。

SUSPEND_WHO

显示激活挂起日期的管理员。

注意：该属性与 ch[x]usr 命令的 suspend[-] 参数相对应。

UALIAS

显示针对一个或多个身份验证主机定义的特定用户的别名。 由 CA SSO 使用。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USER_ATTR 类

USER_ATTR 类中的每个记录都定义 CA SSO 用户目录的有效用户属性。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ATTR_PREDEFS

特定属性的允许值列表。

ATTRNAME

（信息性）。 属性的名称。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DBFIELD

userdir 数据库中字段的名称。 由于不同的数据库可以包含不同的属性，因此应该对属性字段进行同步。

FIELDID

（信息性）。 DB 字段的 ID

OWNER

定义拥有记录的用户或组。

PARAMETER_TYPE

指出用户属性是字符串还是数字。

PRIORITY

用户属性的优先级：将授权规则设置为 PARAM_RULE 对象（例如 APPL、URL）时，根据用户属性所指的优先级定义规则。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USER_DIR_PROP

（信息性）。 用户目录的名称。

USERATTR_FLAGS

包含有关属性的信息。 标志中可以包含下列值：

- **aznchk - 指出**是否使用此属性进行授权。
- **predef**（预定义）、**freetex**（纯文本）或 **userdir**（用户目录）- 这三个值指定用户属性的源。
- **user** 或 **group -** 这些值指明属性（访问者）是用户还是组。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

USER_DIR 类

USER_DIR 类中的每个记录定义一个 CA SSO 用户目录。

USER_DIR 记录的关键字是目录的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ADMIN_NAME

目录管理员的登录名。

ADMIN_PWD

目录管理员的密码。 密码以明文格式存储。 它不在 selang 中显示，但可以用 seadmapi 功能获得。

AZNACL

定义授权 ACL。 授权 ACL，即允许基于资源说明访问资源的 ACL。 说明发送到授权引擎，而不是发送到对象。 通常，使用 AZNACL 时，对象不在数据库中。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CONTOBJ_CLS

容器对象继承的类的名称（在 LDAP 中新建登录信息容器时需要。）

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DIR_TYPE

目录的类型。 有效值是：ETRUST_AC、LDAP、ODBC、NT_Domain 或 none。

GRPOBJ_CLS

组对象继承的类的名称（在 LDAP 中新建组时需要。）

LICONTOBJ_CLS

登录信息容器对象继承的类的名称（在 LDAP 中新建登录信息容器时需要。）

LIOBJ_CLS

登录信息对象继承的类的名称（在 LDAP 中新建登录信息时需要。）

MAX_RET_ITEMS

已检索的最大项数。 默认值取决于目录类型。

OWNER

定义拥有记录的用户或组。

PATH

LDAP 树中开始所有查询的相对可分辨名称。

PORT_NUM

主机上用于访问目录的端口号。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

TIMEOUT_CON

在发出超时错误消息之前，系统等待连接到目录所经历的的时间（以秒为单位）。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USERATTR_LIST

USER_ATTR 类中对象的列表，USER_ATTR 类是将该 USER_DIR 对象作为 USER_DIR 参数的值创建的。

USERDIR_HOST

用于目录的主机名。 该属性必须在类记录中定义。

USROBJ_CLS

用户对象继承的类的名称（在 LDAP 中新建用户时需要）。

VERSION

目录的版本号。

WEBSERVICE 类

WEBSERVICE 类过时，CA Access Control 不使用该类。

WINSERVICE 类

WINSERVICE 类中的每个记录定义一个 Windows 服务。 使用 WINSERVICE 类中的记录可以为 Windows 服务定义访问规则。

WINSERVICE 类记录的关键字是 Windows 服务的名称。

注意：在多数情况下，除非明确指出使用 selang chres 命令更改属性，否则请将属性名称用作命令参数。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 showres WINSERVICE 查看所有属性。

ACL

定义可以访问资源的访问者（用户和组）及其访问类型的列表。

Access Control 列表 (ACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

访问

定义访问者对资源的访问权限。

在 authorize 或 authorize- 命令中使用 access 参数修改 ACL。

CALACL

根据 Unicenter NSM 日历状态定义可以访问资源的访问者（用户和组）及其访问类型的列表。

日历 Access Control 列表 (CALACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

日历

定义对 Unicenter TNG 中的日历的引用。

访问

定义访问者对资源的访问权限。

只有日历为 ON 时才允许访问， 其他所有情况下都拒绝访问。

可以在 authorize 命令中使用 calendar 参数根据在日历 ACL 中定义的访问权限来允许用户或组访问资源。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

GROUPS

资源记录所属的 CONTAINER 记录的列表。

要修改类记录中的该属性，必须在相应的 CONTAINER 记录中更改 MEMBERS 属性。

在 chres、editres 或 newres 命令中使用 mem+ 或 mem- 参数可以修改该属性。

NACL

资源的 *NACL* 属性是一个 Access Control 列表，可定义被拒绝访问资源的访问者及拒绝的访问类型（例如：写入）。另请参阅 ACL、CALACL、PACL。 NACL 中的每个条目均包含下列信息：

访问者

定义访问者。

访问

定义拒绝授权访问者的访问类型。

使用 authorize deniedaccess 命令或 authorize- deniedaccess- 命令修改该属性。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OWNER

定义拥有记录的用户或组。

PACL

定义由特定程序（或符合某种名称模式的程序）发出访问请求时被允许访问资源的访问者的列表及其访问类型。 程序 Access Control 列表 (PACL) 中的每个元素均包含下列信息：

访问者

定义访问者。

程序

定义对 PROGRAM 类中的记录的引用，方式为专门指定，或者按照通配符模式匹配。

访问

定义访问者对资源的访问权限。

注意：可以使用通配符指定 PACL 中的资源。

在 selang authorize 命令中使用 via(*pgm*) 参数可向 PACL 中添加程序、访问者及其访问类型；可以使用 authorize- 命令从 PACL 中删除访问者。

RAUDIT

定义在审核日志中 CA Access Control 记录的访问事件的类型。 RAUDIT 可从 *R*esource *AUDIT* 中派生出它的名称。 有效值包括：

所有

所有访问请求。

成功

已授权的访问请求。

failure

拒绝的访问请求（默认）。

无

无访问请求。

CA Access Control 可记录有关对资源的每个尝试访问事件，不记录是否将访问规则直接应用到资源，或应用到将资源作为成员的组或类。

使用 chres 和 chfile 命令的审核参数来修改审核模式。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

UACC

定义对资源的默认访问权限，它指明向未定义到 CA Access Control 或未出现在资源 ACL 中的访问者授予的访问权限。

在 chres、editres 或 newres 命令中使用 defaccess 参数可以修改该属性。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

WARNING

指明是否启用警告模式。 在资源上启用警告模式后，允许对该资源的所有访问请求；如果某个访问请求违反某条访问规则，将在审核日志中写入一条记录。

XGROUP 类

XGROUP 类中的每个记录都定义数据库中的一个用户组。

每个 XGROUP 类记录的关键字是组的名称。

注意：配置文件组的属性适用于与配置文件组相关的每个用户。 但是，如果在用户（USER 或 XUSER）记录中指定了同一属性，则该用户记录会覆盖配置文件组记录中的那些属性。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 chxgrp 更改其中大多数属性。

注意：在多数情况下，除非明确指出使用 chxgrp 更改属性，否则请将属性名称用作命令参数。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 showxgrp 查看所有属性。

APPLS

（信息性）显示授权访问者访问的应用程序列表。 由 CA SSO 使用。

AUDIT_MODE

定义 CA Access Control 在审核日志中记录的活动。可以指定下列活动的任何组合：

- 无登录
- 在跟踪文件中记录的所有活动
- 登录尝试失败
- 登录成功
- 对 CA Access Control 保护的资源进行的失败访问尝试
- 对 CA Access Control 保护的资源进行的成功访问
- 交互式登录

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的审核参数相对应。 您可以使用 GROUP 或 XGROUP 的 AUDIT_MODE 为组中所有成员设置审核模式。 然而，如果用户的审核模式定义为 USER 记录、XUSER 记录或配置文件组时，您不得使用 AUDIT_MODE 为组成员设置审核模式。

AUTHNMTHD

（信息性）显示用于组记录的身份验证方法，从方法 1 到方法 32，或无。 由 CA SSO 使用。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EXPIRE_DATE

定义访问者变为无效的日期。 用户记录中的 EXPIRE_DATE 属性值会覆盖组记录中的值。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 expire[-] 参数相对应。

FULLNAME

定义与访问者相关联的全名。CA Access Control 使用全名标识审核日志消息中的访问者，但不用于授权。

FULLNAME 是字母数字字符串。对于组，最大长度为 255 个字符。对于用户，最大长度为 47 个字符。

GAPPLS

定义向组授予了访问权限的应用程序组的列表。 由 CA SSO 使用。

GROUP_MEMBER

定义属于此组成员的组。

GROUP_TYPE

指定组权限属性。这些属性中的每个属性均与 ch[x]grp 命令中的同名参数相对应。 一个组可以具有以下一个或多个权限属性：

ADMIN

指定属于该组的用户是否可以执行管理功能，类似于 UNIX 环境中的 root 用户。

AUDITOR

指定属于该组的用户是否可以监控系统、列出数据库中的信息以及为现有记录设置审核模式。

OPERATOR

指定属于该组的用户是否可以列出数据库中的所有内容并使用 secons 实用程序。

PWMANAGER

指定属于该组的用户是否可以修改其他用户的密码设置，以及是否可以启用已经被 serevu 实用程序禁用的用户帐户。

SERVER

指定进程是否可以请求属于该组的用户进行授权，以及是否可以发出 SEOSROUTE_VerifyCreate API 调用。

MEMBER_OF

定义此组所属的组。

OWNER

定义拥有记录的用户或组。

PROFUSR

显示与此配置文件组关联的用户列表。

PWD_AUTOGEN

指出组密码是否是自动生成。 默认设置为 no。由 CA SSO 使用。

PWD_SYNC

指出所有组应用程序的组密码是否都自动保持一致。默认设置为 no。由 CA SSO 使用。

PWPOLICY

定义组密码策略的记录名称。 密码策略是一组规则，用于检查新密码的有效性和定义密码到期时间。 默认值为 no validity check。 由 CA SSO 使用。

REVACL

显示访问者的 Access Control 列表。

SHELL

（仅适用于 UNIX）当新的 UNIX 用户是此组的成员时，会为该用户分配 shell 程序。

在 chxgrp 命令中使用 shellprog 参数可以修改该属性。

SUBGROUP

显示以该组为父组的组的列表。

SUPGROUP

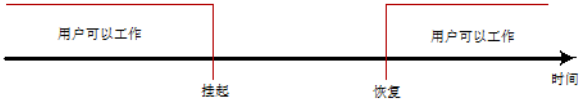
定义父组（“超越”组）的名称。

在 ch[x]grp 命令中使用 parent[-] 参数可以修改该属性。

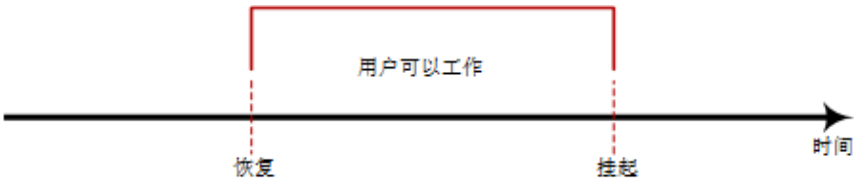
SUSPEND_DATE

定义用户帐户因挂起而变为无效的日期。

如果记录的挂起日期在其恢复日期之前，用户就可以在挂起日期前和恢复日期后工作。



如果用户的恢复日期早于挂起日期，则记录也会在该恢复日期*之前*无效。 用户仅可以在恢复日期和挂起日期之间进行工作。



用户记录中的 SUSPEND_DATE 属性值会覆盖组记录中的值。

注意： 该属性与 ch[x]usr 和 ch[x]grp 命令的 suspend[-] 参数相对应。

SUSPEND_WHO

显示激活挂起日期的管理员。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

USERLIST

显示属于组的用户。

该属性中包含的用户列表可能与本机环境 USERS 属性中的用户列表不同。

XUSER 类

XUSER 类中的每个记录定义数据库中的一个企业用户。

XUSER 记录的关键字是用户的名称 - 用户在登录系统时输入的名称。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 chxusr 更改其中大多数属性。

注意：在多数情况下，除非明确指出使用 chxusr 更改属性，否则请将属性名称用作命令参数。

可以从 CA Access Control 端点管理 或通过使用 selang 命令 showxusr 查看所有属性。

APPLIST

由 CA SSO 使用。

APPLIST_TIME

由 CA SSO 使用。

APPLS

（信息性）显示授权访问者访问的应用程序列表。 由 CA SSO 使用。

AUDIT_MODE

定义 CA Access Control 在审核日志中记录的活动。可以指定下列活动的任何组合：

- 无登录
- 在跟踪文件中记录的所有活动
- 登录尝试失败
- 登录成功
- 对 CA Access Control 保护的资源进行的失败访问尝试
- 对 CA Access Control 保护的资源进行的成功访问
- 交互式登录

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的审核参数相对应。

AUTHNMTHD

（信息性）显示用于组记录的身份验证方法，从方法 1 到方法 32，或无。 由 CA SSO 使用。

BADPASSWD

由 CA SSO 使用。

CALENDAR

表示 CA Access Control 中的用户、组和资源限制的 Unicenter TNG 日历对象。 CA Access Control 按指定的时间间隔引出 Unicenter TNG 活动日历。

CATEGORY

定义分配给用户或资源的一个或多个安全类别。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

COUNTRY

指定用户所在国家/地区描述符的字符串。 该字符串是 X.500 命名方案的一部分。 CA Access Control 不使用该信息进行授权。

CREATE_TIME

（信息性）显示创建记录的日期和时间。

DAYTIME

定义管理访问者何时可以访问资源的日期和时间限制。

在 chres、ch[x]usr 或 ch[x]grp 命令中使用 restrictions 参数可以修改该属性。

日期时间限制的解决方案为一分钟。

EMAIL

定义用户的电子邮件地址，最多为 128 个字符。

FULLNAME

定义与访问者相关联的全名。CA Access Control 使用全名标识审核日志消息中的访问者，但不用于授权。

FULLNAME 是字母数字字符串。对于组，最大长度为 255 个字符。对于用户，最大长度为 47 个字符。

GAPPLS

（信息性）指出用户有权访问的应用程序组的列表。由 CA SSO 使用。

GRACELOGIN

定义用户在密码到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。

宽限登录次数必须介于 0 和 255 之间。如果该值为 0，用户就不能登录。

USER 记录中的 GRACELOGIN 属性值会覆盖 GROUP 记录中 NGRACE 的值。 这二者都会覆盖 SEOS 类记录中的 PASSWDRULES 属性。

注意：该属性与 ch[x]usr 命令的 grace 参数相对应。

GROUPS

（信息性）显示用户所属的用户组列表。 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。

注意：该属性不能通过 ch[x]usr 命令修改。 而使用 join[-] 或 joinx[-] 命令可以修改该属性。

INACTIVE

定义不活动天数，在该天数后系统会将用户的状态更改为不活动。如果帐户状态为不活动，则用户无法登录。

USER 记录中的 INACTIVE 属性值会覆盖 GROUP 记录中的值。 这二者都会覆盖 SEOS 类记录中的 INACT 属性。

注意： CA Access Control 不存储状态，而是动态地计算状态。 要标识不活动用户，必须将 INACTIVE 值与用户的 LAST_ACC_TIME 值进行比较。

LAST_ACC_TERM

显示执行上次登录的终端。

LAST_ACC_TIME

显示上次登录的日期和时间。

LOCALAPPS

由 CA SSO 使用。

LOCATION

定义用户位置。 CA Access Control 不使用此信息进行授权。

LOGININFO

定义用户登录到特定应用程序和审核数据所需的信息。 对于用户得到授权可以访问的每个应用程序，LOGININFO 中都包含了一个单独的列表。 由 CA SSO 使用。

LOGSHIFT

指出是否允许在班次时间外登录。CA Access Control 会为该事件在审核日志中写入一条审核记录。

MAXLOGINS

定义允许用户进行的并发登录的最大数目。 值为零表示用户可以进行任意数量的并发登录。

用户记录中的 MAXLOGINS 属性值会覆盖组记录中的值。这二者都会覆盖 SEOS 类记录中的 MAXLOGINS 值。

MIN_TIME

定义用户两次更改密码之间允许的最短时间。

USER 记录中的 MIN_TIME 属性值会覆盖 GROUP 记录中的值。这二者都会覆盖 SEOS 类记录中的 PASSWDRULES 属性。

注意： 该属性与 ch[x]usr 命令的 min_life 参数相对应。

NOTIFY

定义资源或用户生成审核事件时要通知到的用户。 CA Access Control 可将审核记录通过电子邮件发送给特定用户。

范围：30 个字符。

OBJ_TYPE

指定用户权限属性。这些属性中的每个属性均与 ch[x]usr 命令中的同名参数相对应。 用户可以具有以下一个或多个权限属性：

ADMIN

指定用户是否可以执行管理功能，与 UNIX 环境中的 root 用户类似。

AUDITOR

指定用户是否可以监控系统、列出数据库中的信息以及为现有记录设置审核模式。

IGN_HOL

指定用户是否可以在 HOLIDAY 记录定义的任何时间段内登录。

LOGICAL

指定该用户仅供 CA Access Control 内部使用，而不能用于真实用户登录。

例如，您可用作资源所有者的用户 nobody 甚至可以防止资源所有者访问资源，该用户在默认情况下是逻辑用户。 这意味着，没有用户可以使用该帐户登录。

OPERATOR

指定用户是否可以列出数据库中的所有内容及是否可以使用 secons 实用程序。

PWMANAGER

指定用户是否可以修改其他用户的密码设置及是否可以启用已经被 serevu 实用程序禁用的用户帐户。

SERVER

指定进程是否可以请求用户进行授权及是否可以发出 SEOSROUTE_VerifyCreate API 调用。

OIDCRDDATA

由 CA SSO 使用。

OLD_PASSWD

包含用户的以前密码的加密列表。用户不能从该列表中选择新密码。OLD_PASSWD 中保存的密码最大数目由 setoptions 命令决定。

ORG_UNIT

用于存储有关用户工作所在组织机构的信息的字符串。 该字符串是 X.500 命名方案的一部分。CA Access Control 不使用该信息进行授权。

ORGANIZATION

定义用户工作的组织。 该字符串是 X.500 命名方案的一部分。 CA Access Control 不使用该信息进行授权。

PASSWD_A_C_W

指出上次更改该记录的用户密码的 ADMIN 用户。

PASSWD_INT

定义用户两次更改密码之间允许的最长时间。

USER 记录中的 PASSWD_INT 属性值会覆盖 GROUP 记录中的值。这二者都会覆盖 SEOS 类记录中的 PASSWDRULES 属性。

注意：该属性与 ch[x]usr 命令的 interval 参数相对应。

PASSWD_L_A_C

显示管理员上次更新密码的日期和时间。

PASSWD_L_C

显示用户上次更新密码的日期和时间。

PHONE

定义用户的电话号码。 不使用该信息进行授权。

PUPM_FLAGS

指定终端集成属性。 当您将 CA Access Control 端点上的特权帐户与 PUPM 相集成时，可使用终端集成。特权帐户可以有以下一个或两个终端集成属性：

use_original_identity

指定当 CA Access Control 作出授权决策时，使用签出帐户的用户的名称，而不是特权帐户的名称。该会话的审核记录列出了真实用户名称字段中的最初用户和有效用户名称字段中的特权帐户。

required_checkout

指定必须在 PUPM 中签出帐户，用户才能使用它登录到端点。

PWD_AUTOGEN

显示用户密码是否是自动生成。 由 CA SSO 使用。

默认值为 no。

PWD_SYNC

显示所有用户应用程序的用户密码是否都自动保持一致。 由 CA SSO 使用。

默认值为 no。

RESUME_DATE

定义挂起的 USER 帐户变为取消挂起的日期。

RESUME_DATE 与 SUSPEND_DATE 配合工作。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 resume[-] 参数相对应。

REVACL

显示访问者的 Access Control 列表。

REVOKE_COUNT

由 CA SSO 使用。

SCRIPT_VARS

由 CA SSO 使用，定义变量列表，该列表中列出了每个应用程序保存的应用程序脚本的变量值。

SECLABEL

定义用户或资源的安全级别。

注意：SECLABEL 属性对应 chres 和 ch[x]usr 命令的 label[-] 参数。

SECLEVEL

定义访问者或资源的安全级别。

注意：该属性对应 ch[x]usr 和 chres 命令的 level[-] 参数。

SESSION_GROUP

为用户定义 SSO 会话组。SESSION_GROUP 属性是最长为 16 个字符的字符串。

在 Windows 中，管理员可以在首选名称不在下拉列表中的情况下输入会话组的新名称。

由 CA SSO 使用。

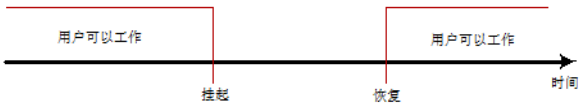
SHIFT

由 CA SSO 使用。

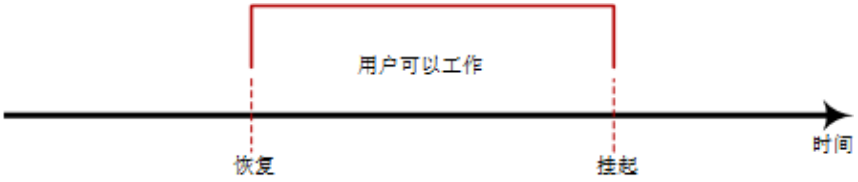
SUSPEND_DATE

定义用户帐户因挂起而变为无效的日期。

如果记录的挂起日期在其恢复日期之前，用户就可以在挂起日期前和恢复日期后工作。



如果用户的恢复日期早于挂起日期，则记录也会在该恢复日期*之前*无效。 用户仅可以在恢复日期和挂起日期之间进行工作。



用户记录中的 SUSPEND_DATE 属性值会覆盖组记录中的值。

注意：该属性与 ch[x]usr 和 ch[x]grp 命令的 suspend[-] 参数相对应。

SUSPEND_WHO

显示激活挂起日期的管理员。

UALIAS

显示针对一个或多个身份验证主机定义的特定用户的别名。 由 CA SSO 使用。

UPDATE_TIME

（信息性）显示上次修改记录的日期和时间。

UPDATE_WHO

（通知）显示执行更新的管理员。

Windows 环境中的类

本部分包含对 Windows 数据库中所有 Windows 类及属性（类在 nt 环境中）的完整参考（按字母顺序排列）。

注意：*nt 环境*一词是指使用 selang 命令 env nt 访问的数据库。 该数据库是 Windows 操作系统为用户、组和资源维护的数据库。

COM 类

COM 类中的每个记录定义一个设备，方法是指定串行端口 (COM) 或并行端口 (LPT)（在 Windows“控制面板”的“端口”下列出）。

注意：您不能使用 CA Access Control 在 COM 类中新建对象。

COM 类的关键字是所控制端口的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

DEV

（信息性）。 指出设备序列号的字符串。

DACL

定义标准 Access Control 列表，包含授权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。

希望修改该属性的用户必须是资源所有者，或者对资源拥有特殊的访问权限（以修改 ACL）。

访问控制列表中的每个元素均包含下列信息：

访问类型

指定对资源的权限：

- **允许** - 允许对资源进行特殊访问。
- **拒绝** - 拒绝对资源进行特殊访问。

访问者

允许或拒绝访问权限所针对的用户或组。

访问

访问者对资源拥有的访问权限。

注意：在空的 ACL 中，不显式授予访问权限，因此隐式拒绝访问权限。 对于没有 ACL 的资源，不为对象分配保护，所以准许任何访问请求。

可以使用 auth 或 auth- 命令来修改该属性。

GID

显示文件或设备的组信息。

OWNER

定义拥有记录的用户或组。

SACL

Windows 系统 Access Control 列表。 显示审核指令。

DEVICE 类

DEVICE 类中的每个记录定义一台 Windows 硬件设备（在 Windows“控制面板”的“设备”下列出）。

DEVICE 类记录的关键字是所控制的端口名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

STARTUPTYPE

定义启动设备的方式（时间）。 可用选项包括：

自动

在系统启动时自动启动设备。

引导

每次系统启动时，在启动所有其他设备之前启动设备。为系统运行必不可少的重要设备选择该选项。

禁用

禁止用户启动设备。 系统仍然能够启动禁用设备。

手动

允许用户或从属设备启动设备。

系统

每次系统启动时，在引导设备启动之后启动设备。为系统运行必不可少的重要设备选择该选项。

可以在 chres 或 editres 命令中使用 starttype 参数来修改该属性。

STATUS

更改当前的服务状态。 可用选项包括：started、stopped 和 paused。

可以在 chres 或 editres 命令中使用 status 参数来修改该属性。

IMAGEPATH

指定设备的完全限定路径。

PROFILE

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。

可以在 chusr、editusr 或 newusr 命令中使用 profile 参数来修改该属性。

示例：激活调制解调器

要显示调制解调器的状态，请输入以下 selang 命令：

```
showres DEVICE modem
```

要激活调制解调器，请输入以下命令：

```
chres device modem status(started)
```

DISK 类

DISK 类中的每条记录定义一个系统卷。 卷是一个通用术语，指您在运行 Windows 操作系统 (Server Edition) 的计算机上可创建和使用的任何实体，如主分区、扩展分区中的逻辑驱动器、卷集、带区集、镜像集或带奇偶校验的带区集。 为每个卷分配了一个驱动器号，并格式化卷以用于文件系统。

注意：您不能使用 CA Access Control 在 DISK 类中创建对象。

DISK 类的关键字是所分配的驱动器号（C:、D: 等等）。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ATIME

（信息性）。 上次访问记录的时间。

CTIME

（信息性）。 创建时间。

DACL

定义标准 Access Control 列表，包含授权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。

希望修改该属性的用户必须是资源所有者，或者对资源拥有特殊的访问权限（以修改 ACL）。

访问控制列表中的每个元素均包含下列信息：

访问类型

指定对资源的权限：

- **允许** - 允许对资源进行特殊访问。
- **拒绝** - 拒绝对资源进行特殊访问。

访问者

允许或拒绝访问权限所针对的用户或组。

访问

访问者对资源拥有的访问权限。

注意：在空的 ACL 中，不显式授予访问权限，因此隐式拒绝访问权限。 对于没有 ACL 的资源，不为对象分配保护，所以准许任何访问请求。

可以使用 auth 或 auth- 命令来修改该属性。

FILE_SYSTEM

（信息性）。 指定文件系统的名称（例如 FAT 或 NTFS）。

FREE_SPACE

（信息性）。 磁盘上的可用空间总数（以 KB 为单位）。

GID

显示文件或设备的组信息。

LABEL

（信息性）。 指定卷的名称。

LINK_NUMB

（信息性）。指定链接数。 对于非 NTFS 文件系统，该属性的值始终为 1。

MTIME

（信息性）。 上次修改记录的时间。

OWNER

定义拥有记录的用户或组。

SACL

Windows 系统 Access Control 列表。 显示审核指令。

TYPE

（信息性）。 指定磁盘是可移动磁盘、固定磁盘、CD-ROM、RAM 磁盘还是网络驱动器。

USED_SPACE

（信息性）。 磁盘上的已用空间总数（以 KB 为单位）。

DOMAIN 类

DOMAIN 类中的每条记录定义共享公用数据库和安全策略（域）的计算机集合。 域提供对由域管理员维护的集中用户帐号和组帐号的访问权限。 每个域具有独特名称。

注意：您不能使用 CA Access Control 在 DOMAIN 类中新建对象。

DOMAIN 记录中的关键字是域名。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

BDC

（信息性）。 接收域目录数据库副本并包含域的所有帐户和安全策略信息的计算机名称。自动定期将该副本与主域控制器 (PDC) 上的主副本同步。备份域控制器 (BDC) 还验证用户登录，并可以根据需要将其提升为具有 PDC 的功能。 一个域中可存在多个 BDC。

COMPUTERS

列出属于指定域的计算机。

可以在 chres 和 editres 命令中使用 computer 或 computer- 参数来修改该属性。

DOMAIN_NAME

定义域名。

DOMAIN_USERS

（信息性）。 列出属于指定域的用户和组帐户。

PDC

（信息性）。 在域中创建的第一台计算机的名称；该计算机包含域数据的主存储库。 它验证域登录并为域维护目录数据库。 主域控制器 (PDC) 跟踪对域中所有计算机的帐号所做的更改。它是唯一能够直接接收这些更改的计算机。 一个域中只能存在一个 PDC。

TRUSTED

列出受信任域和信任域。

信任关系是域之间用于验证传递的链接，在该传递过程中，信任域使受信任域的登录身份验证生效。 利用信任关系，在一个域中只拥有一个用户帐号的用户能够潜在访问整个网络。 您可以为受信任域中定义的用户帐号和全局组授予信任域中的权限和资源权限，即使这些帐号未存在于信任域的目录数据库中。

可以在 chres 和 editres 命令中使用 trusted 或 trusting- 参数来修改该属性。 您应当为该命令指定密码。

TRUSTING

托管域是托管目标域的域。

FILE 类

在 Windows 环境中有效

FILE 类中的每个记录定义位于计算机的物理驱动器或逻辑驱动器上的某个文件系统（例如 FAT、NTFS 或 CDFS）上的一个文件。

注意：您不能使用 CA Access Control 在磁盘上实际创建文件。

FILE 类记录的关键字是受记录保护的文件或目录的名称。 必须指定完整路径。

以下定义介绍了 FILE 记录中包含的属性。 您可以使用 selang 或基于 Web 的 GUI 更改记录的可修改属性。

ATIME

显示上次访问文件的时间。

ATTRIB

显示文件或目录的属性。 这些属性可以是以下一项或多项：

- ARCHIVE
- COMPRESSED
- DIRECTORY
- HIDDEN
- NORMAL
- OFFLINE
- READONLY
- SYSTEM
- TEMPORARY

CTIME

显示创建时间。

DACL

定义标准 Access Control 列表，包含授权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。

希望修改该属性的用户必须是资源所有者，或者对资源拥有特殊的访问权限（以修改 ACL）。

访问控制列表中的每个元素均包含下列信息：

访问类型

指定对资源的权限：

- **允许** - 允许对资源进行特殊访问。
- **拒绝** - 拒绝对资源进行特殊访问。

访问者

允许或拒绝访问权限所针对的用户或组。

访问

访问者对资源拥有的访问权限。

注意：在空的 ACL 中，不显式授予访问权限，因此隐式拒绝访问权限。 对于没有 ACL 的资源，不为对象分配保护，所以准许任何访问请求。

可以使用 auth 或 auth- 命令来修改该属性。

DEV

显示文件所在的卷的序列号。

FILE_SYSTEM

显示文件所在的文件系统的名称。

GID

显示文件或设备的组信息。

INDEX

显示与文件关联的唯一标识符。

ISDIR

指出该文件是否为目录。

LINKS_NUMB

显示指向文件的链接数。 对于 FAT 文件系统，该属性的值始终为 1。 对于 NTFS 文件系统，该属性值可以大于 1。

MTIME

显示上次修改文件的时间。

NAME

显示文件名。

OWNER

定义拥有记录的用户或组。

SACL

Windows 系统 Access Control 列表。 显示审核指令。

SIZE

显示文件的大小（以字节为单位）。

更多信息：

Windows 文件属性 (p. 449)
chfile 命令 — 修改 Windows 文件设置 (p. 172)

GROUP 类

GROUP 类包含为 Windows 操作系统定义的所有组记录。 GROUP 类中的每条记录代表一组用户。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*信息性*，并且不能修改。

COMMENT

希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

在 chgrp、editgrp 和 newgrp 命令中使用 comment[-] 参数可以修改该属性。

范围：255 个字符。

FULL_NAME

与用户关联的全名。CA Access Control 使用全名标识审核日志消息中的用户，但不使用该消息进行授权。

可以在 chusr、editusr 或 newusr 命令中使用 name 参数来修改该属性。

GID

（信息性）。 包含组的相对标识符的值。 相关标识符在创建组时由帐号数据库确定。 它在域中对帐号管理器唯一地标识组。

GLOBAL

指出全局组。 该属性仅适用于 Windows 组。 该属性替换早期 CA Access Control 版本中的 ISGLOBAL 属性。

可以在 newgrp 命令（仅该命令）中使用 global 参数来添加该属性。

USERLIST

属于组的用户和全局组（仅限本地组）的列表。 该属性包含的列表可能与 CA Access Control 数据库中的对应列表不同。

在 join[-] 命令中使用 username(*groupname)* 参数可以修改该属性。

PRIVILEGES

分配给组的 Windows 权限。

可以在 chgrp、editgrp 或 newgrp 命令中使用 privileges 参数来修改该属性。

更多信息：

chgrp 命令 — 修改 Windows 组 (p. 173)
Windows 特权 (p. 452)

OU 类

OU（组织机构）类包含用户、组或计算机等对象。 可以在主域控制器上创建 OU 类的对象，且这些对象可以将其他对象作为子对象（例如组），所以 OU 类的对象为容器对象。

注意：OU 类仅可用于安装了 Active Directory 的 Windows 2000 Advanced Server。

OU 类没有预定义属性（其他类有）。 不过，您可以更新下列 OU 属性：

- 国家/地区/区域
- 说明
- 桌面
- 城市
- 显示名称
- 文件夹（只读属性）
- 传真号码
- 受管对象（只读属性）
- 属于（只读属性）
- 名称（只读属性）
- 邮寄地址
- 邮政编码
- 邮 箱
- 省/自治区/直辖市
- 街道
- 电话
- 更改的对象（只读属性）
- 创建的对象（只读属性）
- 网页

PRINTER 类

PRINTER 类中的每个记录定义一个与可在介质（在“Printers”文件夹中列出）上复制可见图像的 Windows 计算机系统连接的设备。

注意：您不能使用 CA Access Control 新建 PRINTER 类的对象。

PRINTER 类记录的关键字是本地打印机的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

DACL

定义标准 Access Control 列表，包含授权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。

希望修改该属性的用户必须是资源所有者，或者对资源拥有特殊的访问权限（以修改 ACL）。

访问控制列表中的每个元素均包含下列信息：

访问类型

指定对资源的权限：

- **允许** - 允许对资源进行特殊访问。
- **拒绝** - 拒绝对资源进行特殊访问。

访问者

允许或拒绝访问权限所针对的用户或组。

访问

访问者对资源拥有的访问权限。

注意：在空的 ACL 中，不显式授予访问权限，因此隐式拒绝访问权限。 对于没有 ACL 的资源，不为对象分配保护，所以准许任何访问请求。

可以使用 auth 或 auth- 命令来修改该属性。

COMMENT

定义希望包含在记录中的其他信息。CA Access Control 不使用此信息进行授权。

范围：255 个字符。

LOCATION

指出打印机位置的字符串。 CA Access Control 不使用此信息进行授权。

可以在 chres 或 editres 命令中使用 location 参数来修改该属性。 可以使用带有空格的 () 来删除该属性。

OWNER

定义拥有记录的用户或组。

SHARE

标识打印机共享点的名称。 希望访问打印机的用户或组可使用其共享名称。

可以在 chres 或 editres 命令中使用 share_name 或 share_name- 参数来修改该属性。

NAME

打印机名称。

SACL

Windows 系统 Access Control 列表。 显示审核指令。

SERVER

（信息性）。 标识控制打印机的服务器的字符串。 如果没有这样的属性，则在本地控制打印机。

PROCESS 类

PROCESS 类中的每个记录定义由一个可执行程序、一组虚拟内存地址和一个线程（在 Windows 任务管理器中列出）组成的一个对象。

注意：您不能使用 CA Access Control 在 PROCESS 类中新建对象。

PROCESS 类记录的关键字是所运行程序的可执行模块的名称。

以下定义说明了此类记录所具有的属性。 此类中没有可修改的属性。 不可修改的属性标记为*“信息性”*。

IMAGE_PATH

（信息性）。 指定的可执行模块的完全限定路径。

PROCESS_ID

（信息性）。 进程的唯一标识符。 进程 ID 号被重用，所以它们仅在进程的寿命期间标识进程。

在使用 PROCESS 类时，请考虑以下限制：

- CA Access Control 在 Windows 中跟踪进程创建。 但是，仅当启动进程的用户被标为已跟踪时，seosd 才会获取新的进程参数并将参数写入一般跟踪。
- 当创建新的进程时，直到该进程完成初始化后，其参数才可用。 seosd 尝试异步跟踪进程参数；但是，如果进程非常短，该进程可能在 seosd 获取进程参数并将其写入跟踪之前就已终止。 在这种情况下，会在跟踪中显示以下消息：

  EXECARGS：不可用（87）
- 进程 ID 在 Windows 中被重复使用。 如果该进程非常短，理论上存在可能的情况是，seosd 将获取具有同一进程 ID 的其他进程的进程参数，并将这些参数写入跟踪。

REGKEY 类

REGKEY 类中的每个记录定义 Windows 注册表中的一个注册表键。

REGKEY 记录的关键字是 Windows 注册表键的完整注册表路径。

注意：可以将通配符用作路径规范的一部分。

以下定义介绍了 REGKEY 记录中包含的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

DACL

标准 Access Control 列表，包含授权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。

希望修改该属性的用户必须是资源所有者，或者对资源拥有特殊的访问权限（以修改 ACL）。

访问控制列表中的每个元素均包含下列信息：

访问类型

指定对资源的权限：

- **允许 -** 允许对资源进行特殊访问
- **拒绝 -** 拒绝对资源进行特殊访问

访问者

允许或拒绝其访问权限的用户或组的名称。

访问

访问者对资源拥有的访问权限。REGKEY 类的有效访问权限包括：

- **all** - 允许或拒绝访问者执行允许对类执行的所有操作
- **append/create/subkey** - 允许或拒绝访问者创建或修改注册表键的子键
- **changeperm/sec/dac/writedac/perm** - 允许或拒绝访问者修改资源的 ACL（即添加或删除访问者）。
- **chown/owner/takeownership** - 允许或拒绝访问者更改资源所有者
- **delete** - 允许或拒绝访问者删除资源
- **enum** - 允许或拒绝访问者枚举注册表键的子键
- **link** - 允许或拒绝访问者创建指向注册表键的链接
- **notify** - 允许或拒绝访问者请求注册表键或注册表键的子键的更改通知
- **query** - 允许或拒绝访问者查询注册表键的值
- **read** - 允许或拒绝访问者读取注册表键内容，但禁止保存更改
- **readcontrol/manage** - 允许或拒绝访问者读取注册表键的安全描述符中的信息，但不包括系统（审核）ACL 中的信息
- **set** - 允许或拒绝访问者创建或设置注册表键的值
- **write** - 允许或拒绝访问者更改注册表键及其子键

注意：注意空 ACL（即不包含条目的 ACL）与没有 ACL 的资源的不同很重要。 如果 ACL 为空，则不显式授予访问权限，所以访问被隐式拒绝。 对于没有 ACL 的资源，不为对象分配保护，所以准许任何访问请求。

可以使用 auth 或 auth- 命令来修改该属性。

OWNER

指定为资源所有者的用户或组。

可以在 newres、chres 和 editres 命令中使用 owner 参数来修改该属性。

SACL

Windows 系统 Access Control 列表指定审核指令。

SUBKEYS

（信息性）。 位于注册表键下的注册表键（子键）列表。

SUBVALUES

（信息性）。 当前注册表键中介绍的注册表值的列表。

REGVAL 类

REGVAL 类中的每条记录定义介绍注册表项的数据。 该数据存储为一个或多个用户、应用程序和硬件设备配置系统的必需信息。 注册表值包含操作中经常引用的信息。 示例包括：

- 每个用户的配置文件
- 计算机上安装的应用程序和每个应用程序可创建的文件类型
- 文件夹和应用程序图标的属性表设置
- 硬件配置
- 使用端口

REGVAL 记录的关键字是完整的注册表项名称及其值。

注意：错误地更改或删除注册表键及其值会导致出现严重影响系统的问题，可能需要重新安装 Windows 才能解决这些问题。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

TYPE

存储数据的格式。 当您在注册表值下存储数据时，您可以指定下列值之一以指明所存储的数据类型：

注意：在您创建或修改注册表值时指定类型。

DWORD

四个字节长的数字代表的数据。设备驱动程序和服务的多个参数都是这种类型，可以使用二进制、十六进制或十进制格式显示。

STRING

代表可读文本的字符序列。

MULTISTRING

多个字符串。 其值包括可读文本中的多个列表或多个值。 各条目之间使用空字符串分隔。

BINARY

原始二进制数据。大多数硬件组件信息使用二进制数据存储，并可以使用十六进制格式或便于读取的格式显示。

将上述类型之一作为参数与 newres、chres 或 editres 一起使用可修改该属性。

值

Windows 注册表值保留的值。

SEOS 类

SEOS 类控制本地安全系统的行为。

该类中只包含一个记录，名为 SEOS，指定常规本地安全选项。 要查看或更改 SEOS 类属性的状态，请使用 setoptions 命令。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

AuditCategory

指定审核哪些检测到的已授权和未授权的事件。

AccountLogon

指定是否审核登录或退出另一计算机（使用该计算机验证帐户）的用户的每个实例。

AccountManagement

指定是否审核计算机上帐户管理的每个事件。帐户管理事件的示例包括：

- 创建、更改或删除用户帐户或组。
- 重命名、禁用或启用用户帐户。
- 设置或更改密码。

DirectoryAccess

指定是否审核访问已定义自己的系统 Access Control 列表 (SACL) 的 Active Directory 对象的用户的事件。

登录

指定是否审核登录或退出某计算机的用户的每个实例。

ObjectAccess

指定是否审核访问对象的用户的事件。例如，已定义自己的系统 Access Control 列表 (SACL) 的文件、文件夹、注册表键、打印机等。

PolicyChange

指定是否审核对用户权限分配策略、审核策略或托管策略所做的更改的每个事件。

PrivilegeUse

指定是否审核行使用户权限的用户的每个实例。

DetailedTracking

指定是否审核诸如程序激活、进程退出、句柄重复及间接对象访问等事件的详细跟踪信息。

系统

指定是否审核用户何时重新启动或关闭计算机或何时发生影响系统安全或安全日志的事件。

历史记录

定义在旧密码可以重复使用之前必须与用户帐户关联的唯一新密码的数量。

限制：介于 1 和 24 之间的整数。 如果指定为零，将不保存密码。

时间间隔

定义系统要求用户更改密码之前密码可以使用的时间(以天为单位)。

最小时限

定义用户可以更改密码之前密码必须使用的时间（以天为单位）。

最小长度

定义用户帐户的密码可以包含的最少字符数。

Password fails

定义用户帐户锁定前失败的登录尝试次数。

Reset count after

定义在失败的登录尝试之后、将失败的登录尝试计数器重置为 0 次错误登录尝试之前必须经过的时间（以分钟为单位）。

SERVICE 类

SERVICE 类中的每个记录定义一个 Windows 服务(在 Windows“控制面板”的“服务”下列出）。

SERVICE 类记录的关键字是所控制服务的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

ACCOUNT

为服务更改登录帐户。 虽然大多数服务必须登录到系统帐号，但可将部分服务配置为登录到特殊用户帐号。 有关详细信息，请参阅相关的 Microsoft Windows 文档。 默认值是 LocalSystem。

可以在 chres 或 editres 命令中使用 account 参数来修改该属性。

BINARY_NAME

指向服务的可执行文件位置的完整路径。

IMAGEPATH

指定的可执行模块的完全限定路径。

INTERACTIVE

在桌面上提供一个用户界面，启动服务后登录的任何用户都可以使用该用户界面。仅在服务作为 LocalSystem 帐户运行时，该选项才可用。

可以在 chres 或 editres 命令中使用 interactive 参数来修改该属性。

PROFILE

指定用户的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。

可以在 chusr、editusr 或 newusr 命令中使用 profile 参数来修改该属性。

REG_KEY

该属性指向 Windows 注册表中服务定义的位置。

STARTUPTYPE

定义启动服务的方式（时间）。 可用选项包括：

- **自动** - 在系统启动时自动启动。
- **已禁用** - 禁止用户或从属服务启动服务。
- **手动** - 允许用户或从属服务启动服务。
- 在 chres 或 editres 命令中使用 startuptype 参数可以修改该属性。

STATUS

更改当前的服务状态。 可用选项包括：started、stopped 和 paused。

可以在 chres 或 editres 命令中使用 status 参数来修改该属性。

示例：将服务配置为手动启动

要将 SeOSAgent 服务更改为手工启动，请输入以下 selang 命令：

```
chres SERVICE "SeosAgent" starttype(manual)
```

示例：更改目录登录帐户

要将 Directory Replicator 的登录帐户更改为 ReplAdmin（密码为 abcde），请输入以下 selang 命令：

```
chres SERVICE directory replicator account(repladmin) domainpwd(abcde)
```

SESSION 类

SESSION 类中的每条记录定义本地主机上的一个用户会话。 该记录包括用户名、计算机名、已用的连接时间和正在使用的资源。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*"信息性"*。

CNAME

建立会话的主机名。

GUEST

指出是否在 Guest 帐户下创建会话。

IDLE

结束服务器与工作站之间的网络会话。

可以在 chres 或 editres 命令中使用 disconnect 参数来修改该属性。

OPENS

指出打开的会话数。

RESOURCES

提供有关服务器上共享文件信息的属性。 该信息包含打开的共享资源的路径，以及打开该资源的用户或计算机。

TIME

自创建会话后所经过的时间。

USER

包含用户的相对 ID (RID) 的值。在创建用户时，安全帐号管理器 (SAM) 确定 RID。 它在域内对 SAM 唯一地定义用户帐号。

示例：从本地会话断开用户的连接

要从本地主机上的会话断开 ZORRO 用户的连接，请输入以下 selang 命令：

```
chres SESSION zorro disconnect
```

注意：断开用户的连接可能会导致数据丢失。 最好在断开用户的连接前警告连接的用户。

SHARE 类

SHARE 类中的每个记录定义一个共享资源，这些资源可以是一台或多台设备或程序使用的任何设备、数据或程序。 对于 Windows，共享资源指网络用户可用的任何资源，如目录、文件、打印机和命名管道。 共享还指服务器上网络用户可用的资源。

SHARE 类记录的关键字是资源的共享名。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

CURR_USERS

（信息性）。 当前与资源的连接数。

DACL

定义标准 Access Control 列表，包含授权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。

希望修改该属性的用户必须是资源所有者，或者对资源拥有特殊的访问权限（以修改 ACL）。

访问控制列表中的每个元素均包含下列信息：

访问类型

指定对资源的权限：

- **允许** - 允许对资源进行特殊访问。
- **拒绝** - 拒绝对资源进行特殊访问。

访问者

允许或拒绝访问权限所针对的用户或组。

访问

访问者对资源拥有的访问权限。

注意：在空的 ACL 中，不显式授予访问权限，因此隐式拒绝访问权限。 对于没有 ACL 的资源，不为对象分配保护，所以准许任何访问请求。

可以使用 auth 或 auth- 命令来修改该属性。

MAX_USERS

共享资源可接受的最大并发连接数。

注意：不能提供零 (0) 作为该属性的值。 Windows 忽略零值。

可以在 newres、chres 或 editres 命令中使用 max_users 参数来修改该属性。

NAME

定义共享的名称。

PATH

指定共享资源本地路径的字符串。对于磁盘，该路径为共享路径。对于打印队列，该路径为共享打印队列的名称。

可以在 newres、chres 或 editres 命令中使用 path 参数来修改该属性。

PERMISSION

（信息性）。 表示使用共享级别安全运行的服务器的共享资源权限的值。 该属性可以是下表中的任意值：

ACCESS_READ

从资源读取数据的权限和默认情况下执行资源的权限。

ACCESS_WRITE

将数据写入资源的权限。

ACCESS_CREATE

创建资源（如文件）实例的权限；可在创建资源时将数据写入资源。

ACCESS_EXEC

执行资源的权限。

ACCESS_DELETE

删除资源的权限。

ACCESS_ATRIB

修改资源属性（如上次修改文件的日期和时间）的权限。

ACCESS_PERM

修改为用户或应用程序分配的资源权限（读取、写入、创建、执行和删除）的权限。

ACCESS_ALL

读取、写入、创建、执行和删除资源，以及修改资源的属性和权限的权限。

ACCESS_NONE

拒绝权限。

REMARK

希望包含在记录中的其他信息。 字母数字字符串最多可以包含 255 个字符。 CA Access Control 不使用此信息进行授权。

可以在 newres、chres 或 editres 命令中使用 comment 或 comment- 参数来修改该属性。

RESOURCES

（信息性）。 提供有关服务器上共享文件信息的属性。 该信息包含打开的共享资源的路径，以及打开该资源的用户或计算机。

TYPE

（信息性）。 共享的类型。 为共享资源使用下列类型之一：

文件文件夹

磁盘驱动器。 该类型还指服务器的远程管理 (ADMIN$) 和 C$、D$ 等管理共享。

打印队列

打印队列

通信设备

通信设备

进程间通信 (IPC)

为进程间通信 (IPC$) 保留的特殊共享

USERS

有关当前访问共享资源的用户的信息。 该信息包括发起连接的用户名 (USER)、服务器的共享资源的共享名或客户端的计算机名 (MACHINE)。 还包括建立连接以后持续的秒数 (TIME)，以及当前因建立该连接而打开的文件数 (INUSE)。

USER 类

USER 类包含为 Windows 操作系统定义的所有用户记录。 USER 记录的关键字是用户的名称，即用户在登录系统时输入的名称。

以下定义说明了此类记录所具有的属性。 大部分属性均可修改，还可使用 selang 或管理界面控制这些属性。 不可修改的属性标记为*“信息性”*。

BAD_PW_COUNT

（信息性）。用户使用不正确密码尝试登录帐户的次数。如果值为 -1，说明该值未知。

COMMENT

希望包含在记录中的其他信息。 CA Access Control 不使用此信息进行授权。

在 chusr、editusr 和 newusr 命令中使用 comment[-] 参数可以修改该属性。

范围： 255 个字符。

COUNTRY

指定用户所在国家/地区描述符的字符串。 该字符串是 X.500 命名方案的一部分。 CA Access Control 不使用该信息进行授权。

可以在 chusr、editusr 和 newusr 命令中使用 country 参数来修改该属性。

DAYTIME

管理用户访问资源的时间的天数和时间限制。

在 chusr、editusr 和 newusr 命令中使用 restrictions 参数可以修改该属性。

注意： 该属性中的信息与 AC 环境中 DAYTIME 属性的信息相同，区别在于输入的所有分钟值被截短。

DIAL_CALLBACK

为用户提供的回调权限的类型。 已定义下列选项：

NoCallBack

用户没有回叫特权。

SetByCaller

远程用户可在拨入时指定回叫电话号码。

回叫电话号码

管理员设置回叫号码。

可以在 chusr 或 editusr 命令中使用 gen_prop 或 gen_val 参数来修改该属性。

DIAL_PERMISSION

拨入 RAS 服务器的权限。如果指定 0 作为值，则用户不能拨入 RAS 服务器。

可以在 chusr 或 editusr 命令中使用 gen_prop 或 gen_val 参数来修改该属性。

EXPIRE_DATE

USER 记录因到期而无效的日期。USER 记录中的 EXPIRE_DATE 属性值会覆盖 GROUP 记录中的值。 要恢复已到期记录，请使用带有 expire- 参数的 chusr 命令。 到期用户是无法恢复的， 可以通过指定恢复日期来恢复挂起用户。

可以在 chusr、editusr 或 newusr 命令中使用 expire 或 expire- 参数来修改该属性。

FLAGS

为指定特定属性而为用户帐户分配的标志。 可以对每个帐号应用多个标志。

可以在 chusr、editusr 和 newusr 命令中使用 flags 参数来修改该属性。

FULL_NAME

与用户关联的全名。CA Access Control 使用全名标识审核日志消息中的用户，但不使用该消息进行授权。

可以在 chusr、editusr 或 newusr 命令中使用 name 参数来修改该属性。

GID

包含组的相对标识符的值。 相关标识符在创建组时由帐号数据库确定。 它在域中对帐号管理器唯一地标识组。

GROUPS

用户所属的组列表。 该属性中包含的组列表可能与 AC 环境 GROUPS 属性中的组列表不同。

在 join[-] 命令中使用 group 参数可以修改该属性。

HOME

主目录是用户可访问的文件夹，包含该用户的文件和程序。 可以将主目录分配给单个用户或在多个用户之间共享。

HOMEDIR

指定用户主目录的字符串。 用户会自动登录到其主目录。

可以在 chusr、editusr 或 newusr 命令中使用 homedir 参数来修改该属性。

HOME_DRIVE

指定用户主目录所在驱动器的字符串。 用户自动登录到其自己的主驱动器和主目录。

可以在 chusr、editusr 或 newusr 命令中使用 homedrive 参数来修改该属性。

ID

包含用户的相对 ID (RID) 的值。在创建用户时，安全帐号管理器 (SAM) 确定 RID。 它在域内对 SAM 唯一地定义用户帐号。

LAST_ACC_TIME

（信息性）。 上次登录的日期和时间。

LAST_LOGOFF

（信息性）。 上次注销的日期和时间。

LOCATION

用于存储用户位置的字符串。 CA Access Control 不使用此信息进行授权。

可以在 chusr、editusr 和 newusr 命令中使用 location 参数来修改该属性。

LOGON_SERVER

指定验证用户登录信息的服务器的字符串。 当用户登录到域工作站时，CA Access Control 将登录信息传输到服务器，为用户授予工作站权限以使其能够工作。

MAX_LOGINS

（信息性）。 用户已成功登录到该帐户的次数。 如果值为 -1，说明该值未知。

NAME

用户的名称。

ORGANIZATION

用于存储用户工作组织相关信息的字符串。该字符串是 X.500 命名方案的一部分。 CA Access Control 不使用该信息进行授权。

可以在 chusr、editusr 和 newusr 命令中使用 organization 参数来修改该属性。

ORG_UNIT

用于存储有关用户工作所在组织机构的信息的字符串。 该字符串是 X.500 命名方案的一部分。CA Access Control 不使用该信息进行授权。

可以在 chusr、editusr 和 newusr 命令中使用 org_unit 参数来修改该属性。

PASSWD_EXPIRED

用户帐户的到期日期。

PGROUP

用户的主组 ID。 主组是指在其中定义用户的组之一。 主组必须是全局组。 该字符串不能包含空格或逗号。

可以在 chusr、editusr 或 newusr 命令中使用 pgroup 参数来修改该属性。

PHONE

可以用来存储用户电话号码的字符串。 不使用该信息进行授权。

可以在 chusr、editusr 和 newusr 命令中使用 phone 参数来修改该属性。

PRIVILEGES

分配给用户的 Windows 权限。

可以在 chusr、editusr 或 newusr 命令中使用 privileges 参数来修改该属性。

PROFILE

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。

可以在 chusr、editusr 或 newusr 命令中使用 profile 参数来修改该属性。

PW_LAST_CHANGE

（信息性）。 更新密码的日期和时间。

RESUME_DATE

挂起的 USER 帐户变为有效的日期。

有关 RESUME_DATE 和 SUSPEND_DATE 如何一起工作的说明，请参阅 SUSPEND_DATE。

SCRIPT

指定用户登录脚本文件路径的字符串。 该脚本文件可以是下列文件：.CMD、.EXE 或 .BAT 文件。

TERMINALS

指定用户可从中登录的终端列表的字符串。

可以在 chusr、editusr 和 newusr 命令中使用 terminals 参数来修改该属性。

TS_CONFIG_PGM

表明客户端是否可指定初始程序的值。

TS_INITIAL_PGM 用户属性指明初始程序。 如果您指定用户的初始程序，则用户只能运行该程序；当用户退出该程序时，终端服务器将注销用户。

如果该值设置为 1，客户端可指定初始程序。 如果该值设置为 0，则客户端不能指定初始程序。

可以在 chusr 和 editusr 命令中使用 gen_prop 和 gen_val 参数来修改该属性。

TS_HOME_DIR

用户登录终端服务器所需的主目录路径。 该字符串可指定本地路径或 UNC 路径 (\\machine\share\path)。

可以在 chusr 和 editusr 命令中使用 gen_prop 和 gen_val 参数来修改该属性。

TS_HOME_DRIVE

在 TS_HOME_DIR 属性中指定的 UNC 路径所针对的驱动器规格（驱动器号，后跟一个冒号）。

可以在 chusr 和 editusr 命令中使用 gen_prop 和 gen_val 参数来修改该属性。

TS_INITIAL_PGM

用户登录时，终端服务运行的初始程序的路径。

如果您指定用户的初始路径，则用户只能运行该程序。 当用户退出该程序时，终端服务器注销该用户。

如果 TS_CONFIG_PGM 属性被设置为 1，则客户端可指定初始程序。

可以在 chusr 和 editusr 命令中使用 gen_prop 和 gen_val 参数来修改该属性。

TS_PROFILE_PATH

用户登录终端服务器所需的用户配置文件的路径。 必须手工创建该路径所标识的目录，且该目录在登录前必须已存在。

可以在 chusr 和 editusr 命令中使用 gen_prop 和 gen_val 参数来修改该属性。

TS_WORKING_DIR

用户登录时，终端服务运行的初始程序的工作目录路径。

可以在 chusr 和 editusr 命令中使用 gen_prop 和 gen_val 参数来修改该属性。

WORKSTATIONS

用户可从中登录的工作站列表。

可以在 chusr、editusr 和 newusr 命令中使用 workstations 参数来修改该属性。

更多信息：

chusr 命令 — 修改 Windows 用户 (p. 178)
Windows 帐号标志 (p. 450)
Windows 特权 (p. 452)

UNIX 环境中的类

本部分包含对 UNIX 系统文件中所有 UNIX 类（类在 unix 环境中）的完整参考（按字母顺序排列）。 这些本地类的属性由操作系统管理，并且因系统而异。

注意：*unix 环境*一词是指使用 selang 命令 env unix 访问的系统文件。 这些系统文件与 UNIX 操作系统为用户和组保留的系统文件及系统中的文件相同。

FILE 类

FILE 类中的每个记录定义位于文件系统上的计算机物理或逻辑驱动器上的一个文件。

注意：您不能使用 CA Access Control 在磁盘上实际创建文件。

FILE 类记录的关键字是受记录保护的文件或目录的名称。 必须指定完整路径。

此本地类的属性由操作系统管理，在系统之间有所不同。 chfile 命令会列出可以使用 selang 修改的本地属性。

GROUP 类

GROUP 类包含为 UNIX 操作系统定义的所有组记录。 GROUP 类中的每条记录代表一组用户。

此本地类的属性由操作系统管理，在系统之间有所不同。 chgrp 命令会列出可以使用 selang 修改的本地属性。

USER 类

USER 类包含为 UNIX 操作系统定义的所有用户记录。 USER 记录的关键字是用户的名称，即用户在登录系统时输入的名称。

此本地类的属性由操作系统管理，在系统之间有所不同。 chusr 命令会列出可以使用 selang 修改的本地属性。

用于自定义的类

本部分包含对用户定义的类和属性的参考。

用户定义的类

用户定义类中的每个记录都定义对满足您自己需要的自定义类的访问。对用户定义的类名称的唯一限制是：名称中不能都是大写字母。

用户定义类记录的关键字是记录的名称。

Unicenter TNG 用户定义的类

通过 CA Access Control 可以将 Unicenter TNG 资产类定义为资源。 可以创建、删除、激活和禁用 Unicenter TNG 用户定义的类。

可以在 UACC 类中找到 Unicenter TNG 用户定义的类。

注意：为常规 CA Access Control 类定义的任何属性都可以在用户定义的类中使用。

附录 A： Windows 值

此部分包含以下主题：

Windows 文件属性

可以使用 chfile、editfile 和 newfile 命令为文件分配属性。 属性决定文件的特征。

注意：虽然这些文件属性的全名是 FILE_ATTRIBUTE_*name*，CA Access Control 仅要求您输入 *name* 部分（例如，ARCHIVE 或 COMPRESSED）。

下面列出并介绍了可以在 Windows 中修改的文件属性。

FILE_ATTRIBUTE_ARCHIVE

可存档文件；标记为备份或删除的文件。

FILE_ATTRIBUTE_HIDDEN

隐藏文件。 常规目录列表中通常不包含隐藏文件。

FILE_ATTRIBUTE_NORMAL

不具有其他属性的文件。 该值仅在单独使用时有效。

FILE_ATTRIBUTE_READONLY

只读文件。 应用程序可读取文件，但不能写入或删除文件。

FILE_ATTRIBUTE_SYSTEM

一个或多个操作系统以独占方式使用的操作系统文件。

FILE_ATTRIBUTE_TEMPORARY

用于临时存储的文件。

下面列出并介绍了不能在 Windows 中修改的文件属性。

FILE_ATTRIBUTE_COMPRESSED

压缩文件或目录。 对于文件，意味着文件中的所有数据被压缩；对于目录，意味着在默认情况下压缩所有新创建的文件和子目录。

FILE_ATTRIBUTE_DIRECTORY

目录。

更多信息：

chfile 命令 — 修改 Windows 文件设置 (p. 172)

Windows 帐号标志

可以使用 chusr、editusr 和 newusr 命令，为用户帐号分配标志以指定该帐号的特定属性。 可以对每个帐号应用多个标志。

注意：CA Access Control 不要求您输入标志的全名。 可使用表中提供的快捷方式。

下列是 Windows 中的可用帐号标志。

快捷方式	标志	说明
blank	UF_PASSWRD_NOTREQD	指明用户帐号不需要密码。
cant_change	UF_PASSWORD_CANT_CHANGE	指明用户不能更改帐号密码。
disable	UF_ACCOUNTDISABLE	指明用户帐号被禁用。
dont_expire	UF_DONT_EXPIRE_PASSWORD	指明该帐号的密码永不过期。
homedir	UF_HOMEDIR_REQUIRED	指明需要主目录。 该值在 Windows 中被忽略。
interdomain	UF_INTERDOMAIN_TRUST_ACCOUNT	指明允许信任帐号。
lockout	UF_LOCKOUT	指明用户帐号当前被锁定；要解除已锁定帐号的锁定，请删除该标志。
normal	UF_NORMAL_ACCOUNT	指明代表正常用户的默认帐号类型。
notreq	UF_PASSWRD_NOTREQD	指明用户帐号不需要密码。
保护	UF_PASSWORD_CANT_CHANGE	指明用户不能更改帐号密码。

快捷方式	标志	说明
script	UF_SCRIPT	指明在用户启动应用程序时激活用于执行磁盘映射的登录脚本。 必须为 LAN Manager 2.0 或 Windows 设置该标志。
server	UF_SERVER_TRUST_ACCOUNT	指明该域中的 Windows NT 备份域控制器的帐号。
temp	UF_TEMP_DUPLICATE_ACCOUNT	指明拥有另一个域中的帐号的用户；为该帐号提供域的访问权限，但该帐号不是信任帐号。
trust	UF_INTERDOMAIN_TRUST_ACCOUNT	指明允许信任帐号。
workstation	UF_WORKSTATION_TRUST_ACCOUNT	指明作为该域成员的工作站或服务器的帐号。

更多信息：

chusr 命令 — 修改 Windows 用户 (p. 178)

Windows 权限

在 SHARE 资源类型中，您可以为访问者授予访问权限。

下面是 Windows 中的可用访问权限：

ACCESS_ALL

读取、写入、创建、执行和删除资源，以及修改资源的属性和权限的权限。

ACCESS_ATTRIB

修改资源属性的权限。

ACCESS_CREATE

创建资源的权限，包括在创建资源时将数据写入资源。

ACCESS_DELETE

删除资源的权限。

ACCESS_EXEC

执行资源的权限。

ACCESS_NONE

无访问权限。

ACCESS_PERM

修改为用户或应用程序分配的资源权限的权限。

ACCESS_READ

从资源读取数据的权限以及在默认情况下在资源中执行的权限。

ACCESS_WRITE

将数据写入资源的权限。

更多信息：

SHARE 类 (p. 437)

Windows 特权

可以将 Windows 特权分配给单个用户帐号和组。 管理员可以使用 chusr 或 editusr 命令将特权分配给用户，或者使用 chgrp 或 editgrp 命令将特权分配给组。 添加到组中的用户自动获得分配给组的所有特权。

您可以直接使用列表中显示的特权名称或用户权限名称，也可以在名称开头添加 Se 或在名称末尾添加 Privilege（BatchLogon、InteractiveLogon、NetworkLogon 和 ServiceLogon 除外，对于这些名称，添加 Right 而不是 Privilege）。

下面是 Windows 中的可用特权。

特权	默认分配	说明
AssignPrimaryToken	无	允许用户修改进程的安全访问内标识。
审核	无	生成安全审核。
Backup	Administrators Backup Operators	允许用户备份文件和目录。 该特权替换所有文件和目录权限。
BatchLogon	无	允许用户以批处理作业方式登录。
ChangeNotify	Everyone	通常，文件和子目录的权限向下传递；也就是说，不拥有特定目录权限的用户不拥有访问该目录下的子目录的权限。 该特权允许用户访问子目录，即使该用户不拥有父目录的权限。

特权	默认分配	说明
CreatePagefile	无	允许用户创建页面文件。 安全由用户对该项拥有的访问权限决定。 \CurrentControlSet\Control\SessionManagement
CreatePermanent	无	允许用户创建特殊永久对象，如 \\Device
CreateToken	无	创建内标识对象。 仅 Local Security Authority 可执行该操作。 Local Security Authority 确保拥有访问系统的权限。 不允许审核该权限的使用。 对于 C2 认证，建议不为任何用户分配该权限。
调试	管理员	调试程序或对象（如线程）。 您不能审核该特权。 对于 C2 认证，建议不为包括系统管理员在内的任何用户分配该特权。
IncreaseBasePriority	管理员 超级用户	允许用户提高进程的执行优先级。
IncreaseQuota	无	允许用户提高对象配额。
InteractiveLogon	Most groups	允许用户以交互方式登录。
LoadDriver	管理员	允许用户安装和删除设备驱动程序。
LockMemory	无	允许用户锁定计算机内存中的页，这样在 PAGEFILE.SYS 等备份存储上就不能自动备份这些页。
MachineAccount	无	允许用户将新计算机添加到域中。
NetworkLogon	Everyone	允许用户从网络中任意位置连接计算机。 这意味着用户不必位于特定位置或终端即可登录他们的计算机。
ProfileSingleProcess	管理员 超级用户	允许用户使用性能监视工具以便监视单个进程的性能。
RemoteShutdownPrivilege	管理员 超级用户	允许用户从远程关闭 Windows 系统。
Restore	管理员 Backup Operators	允许用户还原所备份的文件和目录。 该权限替换所有文件和目录权限。
安全	管理员	允许用户指定要审核的资源访问类型（如文件访问），并允许用户指定查看和清除安全日志。 **注意：** 该权限不允许用户在 Microsoft 用户管理器中的“策略”菜单上使用 Audit 命令设置系统审核策略。 管理员始终能够查看和清除安全日志。

特权	默认分配	说明
ServiceLogon	无	使进程能够作为服务注册到系统。
Shutdown	管理员 备份操作员 所有人 超级用户 用户	允许用户从系统控制台关闭系统。
SystemEnvironment	管理员	允许用户修改系统环境变量。 这使用户能够在其工作站上设置系统环境，并确保在同一工作站上工作的所有其他用户能够使用相同设置。
SystemProfile	管理员	允许用户在系统上执行配置（性能示例）。
SystemTime	管理员 Power Users	允许用户设置计算机的内部时钟的时间。
TakeOwnership	管理员	允许用户成为文件、目录、打印机或计算机上的其他对象的所有者。 该权限替换保护对象的所有权限。
Tcb	无	使进程能够作为操作系统的安全、受信任部分执行。 授予部分子系统该特权。

更多信息：

chusr 命令 — 修改 Windows 用户 (p. 178)
chgrp 命令 — 修改 Windows 组 (p. 173)