[Oracle Homeage](http://www.oracle.com/)test

[Documentation Home](http://www.oracle.com/technetwork/indexes/documentation/index.html)  > [系统管理指南：安全性服务](https://docs.oracle.com/cd/E19253-01/819-7061/index.html)  > [第 6 部分 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vak/index.html)  > 第 24 章 管理 Kerberos 主体和策略（任务）

系统管理指南：安全性服务

* [*Previous*: 第 23 章 Kerberos 错误消息和疑难解答](https://docs.oracle.com/cd/E19253-01/819-7061/trouble-1/index.html)
* [*Next*: 第 25 章 使用 Kerberos 应用程序（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/user-7/index.html)

**第 24 章 管理 Kerberos 主体和策略（任务）**

本章介绍有关管理主体及与其关联的策略的过程。本章还将说明如何管理主机的密钥表文件。

需要管理主体和策略的用户应该阅读本章。阅读本章之前，应熟悉主体和策略，包括所有规划注意事项。请分别参阅[第 20 章，Kerberos 服务介绍](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vam/index.html)和[第 21 章，规划 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vas/index.html)。

以下是本章中信息的列表。

* [管理 Kerberos 主体和策略的方法](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd9/index.html)
* [SEAM Administration Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vda/index.html)
* [管理 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdh/index.html)
* [管理 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdt/index.html)
* [SEAM Tool 参考](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html)
* [管理密钥表文件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve7/index.html)

**管理 Kerberos 主体和策略的方法**

主 KDC 上的 Kerberos 数据库包含您所在领域的所有 Kerberos 主体、主体口令、策略和其他管理信息。 创建和删除主体以及修改其属性时，可以使用 kadmin 或 gkadmin 命令。

kadmin 命令提供一个交互式的命令行界面，用于维护 Kerberos 主体、策略和密钥表文件。kadmin 命令具有以下两个版本：

* kadmin－使用 Kerberos 验证从网络中的任何位置安全操作
* kadmin.local－必须直接在主 KDC 上运行

除 kadmin 使用 Kerberos 来验证用户外，这两个版本的功能完全相同。如果要设置足够的数据库以便使用远程版本，则必须使用本地版本。

另外，Solaris 发行版还提供了 SEAM Administration Tool (gkadmin)，这是一个交互式的图形用户界面 (graphical user interface, GUI)，其功能基本上与 kadmin 命令相同。有关更多信息，请参见[SEAM Administration Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vda/index.html)。

**SEAM Administration Tool**

SEAM Administration Tool (SEAM Tool) 是一个交互式的图形用户界面 (graphical user interface, GUI)，用于维护 Kerberos 主体和策略。此工具提供的功能与 kadmin 命令基本相同。但是，此工具不支持密钥表文件管理。必须使用 kadmin 命令来管理密钥表文件，如[管理密钥表文件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve7/index.html)中所述。

与 kadmin 命令类似，SEAM Tool 使用 Kerberos 验证和加密 RPC 从网络中的任何位置安全操作。SEAM Tool 可以执行以下操作：

* 创建基于缺省值或现有主体的新主体。
* 创建基于现有策略的新策略。
* 为主体添加注释。
* 设置缺省值以创建新主体。
* 在不退出工具的情况下以其他主体身份登录。
* 打印或保存主体列表和策略列表。
* 查看和搜索主体列表和策略列表。

SEAM Tool 还会提供关联说明和一般联机帮助。

以下任务列表提供了指向可借助 SEAM Tool 完成的各种任务的链接：

* [管理 Kerberos 主体（任务列表）](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdj/index.html)
* [管理 Kerberos 策略（任务列表）](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdv/index.html)

此外，还可转至[SEAM Tool 面板说明](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-223)，了解可在 SEAM Tool 中指定或查看的所有主体属性和策略属性的说明。

**SEAM Tool 的等效命令行**

本节列出了一些 kadmin 命令，其提供的功能与 SEAM Tool 相同。无需运行 X 窗口系统，便可使用这些命令。尽管本章中的大多数过程使用 SEAM Tool，但其中许多过程还提供了使用等效命令行的对应示例。

表 24–1 SEAM Tool 的等效命令行

| **SEAM Tool 过程** | **等效的 kadmin 命令** |
| --- | --- |
| 查看主体列表。 | list\_principals 或 get\_principals |
| 查看主体属性。 | get\_principal |
| 创建新主体。 | add\_principal |
| 复制主体。 | 无等效命令行 |
| 修改主体。 | modify\_principal 或 change\_password |
| 删除主体。 | delete\_principal |
| 设置缺省值以创建新主体。 | 无等效命令行 |
| 查看策略列表。 | list\_policies 或 get\_policies |
| 查看策略属性。 | get\_policy |
| 创建新策略。 | add\_policy |
| 复制策略。 | 无等效命令行 |
| 修改策略。 | modify\_policy |
| 删除策略。 | delete\_policy |

**SEAM Tool 修改的唯一文件**

SEAM Tool 修改的唯一文件是 $HOME/.gkadmin 文件。该文件包含用于创建新主体的缺省值。通过从 "Edit" 菜单中选择 "Properties"，可以更新该文件。

**SEAM Tool 的打印和联机帮助功能**

SEAM Tool 提供了打印功能和联机帮助功能。通过 "Print" 菜单，可将以下各项发送至打印机或文件：

* 指定主 KDC 上的可用主体列表
* 指定主 KDC 上的可用策略列表
* 当前选择的主体或装入的主体
* 当前选择的策略或装入的策略

通过 "Help" 菜单，可以访问关联说明和一般帮助。从 "Help" 菜单中选择 "Context-Sensitive Help" 时，将显示 "Context-Sensitive Help" 窗口并且工具会切换为帮助模式。在帮助模式下，如果单击该窗口中的任何字段、标签或按钮，将在 "Help" 窗口中显示有关该项的帮助。要切换回工具的一般模式，请在 "Help" 窗口中单击 "Dismiss"。

此外，还可选择 "Help Contents"，这将打开一个 HTML 浏览器，其中会提供指向本章中介绍的一般概述和任务信息的链接。

**在 SEAM Tool 中处理大型列表**

随着站点开始积累大量主体和策略，使用 SEAM Tool 装入并显示主体和策略列表所需的时间将会越来越长。因此，使用该工具时的工作效率会下降。解决此问题有多种办法。

首先，通过使 SEAM Tool 不装入列表，可以完全省去装入列表的时间。可以设置此选项，方法是从 "Edit" 菜单中选择 "Properties"，然后取消选中 "Show Lists" 字段。当然，如果该工具不装入列表，则不能显示这些列表，因此将无法再使用列表面板来选择主体或策略。而必须在提供的新 "Name" 字段中键入主体或策略名称，然后选择要对其执行的操作。键入名称与从列表中选择项的结果相同。

处理大型列表的另一种方法是对其进行高速缓存。实际上，已将 SEAM Tool 的缺省行为设置为将列表高速缓存一段时间。最初 SEAM Tool 还是必须将这些列表装入高速缓存。但在此后，该工具就可以使用高速缓存，而不必再次获取列表。这样便无需不断从服务器装入列表（正是此操作占用了大量时间）。

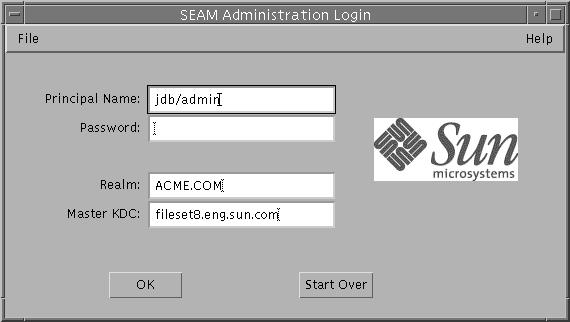
通过从 "Edit" 菜单中选择 "Properties"，可以设置列表高速缓存。有两种高速缓存设置。可以选择将列表永久高速缓存；也可以指定必须将列表从服务器重新装入高速缓存的时间限制。

对列表进行高速缓存时，仍然可以使用列表面板来选择主体和策略，因此该方法不会像第一种方法那样影响 SEAM Tool 的使用方式。另外，尽管使用高速缓存使您无法查看其他用户所做的更改，但您仍可以根据自己所做的更改查看最新列表信息，因为您所做的更改会对服务器和高速缓存中的列表进行更新。而且，如果要更新高速缓存以查看其他更改并获取最新列表副本，可在需要从服务器刷新高速缓存时使用 "Refresh" 菜单。

**Procedure如何启动 SEAM Tool**

1. 使用 gkadmin 命令启动 SEAM Tool。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 此时会显示 "SEAM Administration Login" 窗口。
2. 
3. 如果不想使用现有的缺省值，请指定新的缺省值。

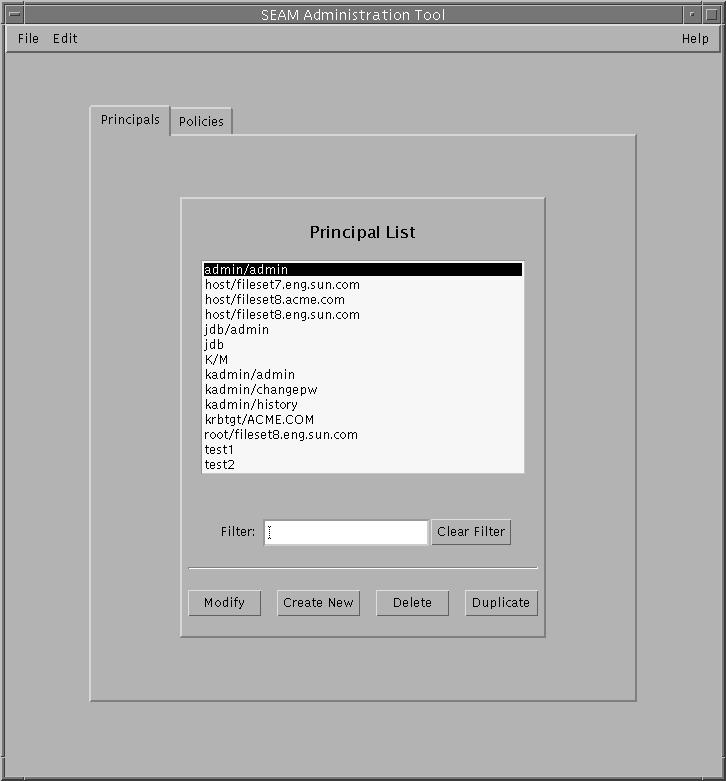
该窗口会自动使用缺省值填充。缺省主体名称 (*username*/admin) 是通过从 USER 环境变量获取当前身份并在其后附加 /admin 确定的。缺省的 "Realm" 和 "Master KDC" 字段选自 /etc/krb5/krb5.conf 文件。如果要恢复这些缺省值，请单击 "Start Over"。

**注 –**

每个主体名称可以执行的管理操作在 Kerberos ACL 文件 /etc/krb5/kadm5.acl 中指定。有关受限权限的信息，请参见[以受限 Kerberos 管理权限使用 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-206)。

1. 键入指定主体名称的口令。
2. 单击 "OK"。

此时会显示以下窗口：



**管理 Kerberos 主体**

本节提供使用 SEAM Tool 管理主体的逐步说明，还提供等效命令行示例（如果有）。

**管理 Kerberos 主体（任务列表）**

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 查看主体列表。 | 通过单击 "Principals" 选项卡来查看主体列表。 | [如何查看 Kerberos 主体列表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdl/index.html) |
| 查看主体属性。 | 通过在 "Principal List" 中选择 "Principal"，然后单击 "Modify" 按钮来查看主体的属性。 | [如何查看 Kerberos 主体属性](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdm/index.html) |
| 创建新主体。 | 通过单击 "Principal List" 面板中的 "Create New" 按钮来创建新主体。 | [如何创建新的 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdn/index.html) |
| 复制主体。 | 通过在 "Principal List" 中选择要复制的主体，然后单击 "Duplicate" 按钮来复制主体。 | [如何复制 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdo/index.html) |
| 修改主体。 | 通过在 "Principal List" 中选择要修改的主体，然后单击 "Modify" 按钮来修改主体。  请注意，不能修改主体的名称。要重命名主体，必须首先复制该主体，为其指定一个新名称并保存，然后删除旧主体。 | [如何修改 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdp/index.html) |
| 删除主体。 | 通过在 "Principal List" 中选择要删除的主体，然后单击 "Delete" 按钮来删除主体。 | [如何删除 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdq/index.html) |
| 设置缺省值以创建新主体。 | 通过从 "Edit" 菜单中选择 "Properties" 来设置缺省值以创建新主体。 | [如何设置缺省值以创建新的 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdr/index.html) |
| 修改 Kerberos 管理权限（kadm5.acl 文件）。 | **仅限命令行。**Kerberos 管理权限确定主体可对 Kerberos 数据库执行的操作，如添加和修改。  要修改每个主体的 Kerberos 管理权限，需要编辑 /etc/krb5/kadm5.acl 文件。 | [如何修改 Kerberos 管理权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vds/index.html) |

**自动创建新的 Kerberos 主体**

尽管 SEAM Tool 使用方便，但它不提供自动创建新主体的方法。如果需要在短时间内添加 10 个甚至 100 个新主体，则自动创建尤其有用。而在 Bourne shell 脚本中使用 kadmin.local 命令正好可满足这一需要。

以下 shell 脚本行示例说明了如何自动创建新主体：

|  |
| --- |
| awk '{ print "ank +needchange -pw", $2, $1 }' < /tmp/princnames |  time /usr/sbin/kadmin.local> /dev/null |

为了方便阅读，已将此示例拆分为两行。该脚本将读入一个称为 princnames 的文件（其中包含主体名称及其口令）然后将其添加到 Kerberos 数据库。您必须创建 princnames 文件，并在每一行上包含一个主体名称及其口令，中间用一个或多个空格分隔。+needchange 选项用于配置主体，以便在用户第一次使用该主体登录时提示其输入新口令。此做法有助于确保 princnames 文件中的口令不会引入安全风险。

可以生成更详细的脚本。例如，脚本可使用名称服务中的信息来获取主体名称的用户名列表。所执行的操作和执行操作的方式取决于站点的需要以及脚本编制技术。

**Procedure如何查看 Kerberos 主体列表**

此过程后附等效命令行示例。

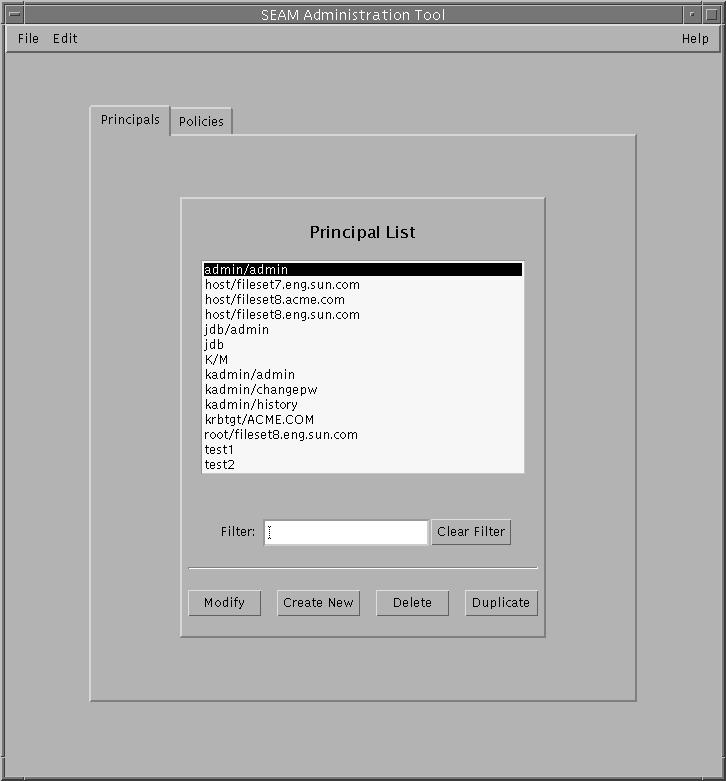
1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Principals" 选项卡。

此时会显示主体列表。



1. 显示特定主体或主体子列表。

在 "Filter" 字段中键入过滤字符串，然后按 "Return"。如果过滤操作成功，则会显示与过滤器匹配的主体列表。

过滤字符串必须由一个或多个字符组成。由于过滤机制区分大小写，因此需要对过滤器使用正确的大小写字母。例如，如果键入过滤字符串 ge，则过滤机制仅显示包含 ge 字符串的主体（如 george 或 edge）。

如果要显示主体的完整列表，请单击 "Clear Filter"。

**示例 24–1 查看 Kerberos 主体列表（命令行）**

在以下示例中，kadmin 的 list\_principals 命令用于列出与 test\* 匹配的所有主体。通配符可与 list\_principals 命令一起使用。

|  |
| --- |
| kadmin: **list\_principals test\***  test1@EXAMPLE.COM  test2@EXAMPLE.COM  kadmin: **quit** |

**Procedure如何查看 Kerberos 主体属性**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Principals" 选项卡。
2. 在列表中选择要查看的主体，然后单击 "Modify"。

此时会显示包含该主体某些属性的 "Principal Basics" 面板。

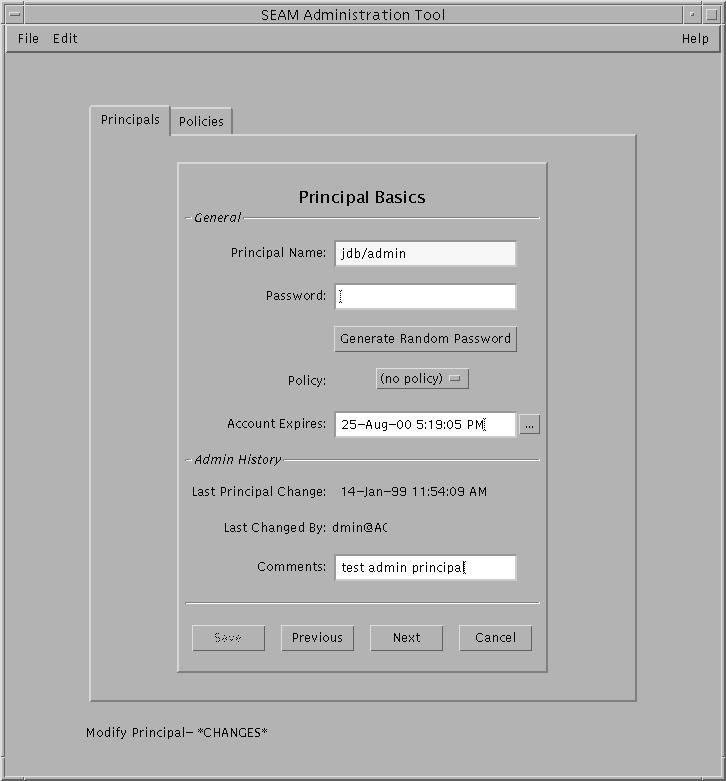
1. 继续单击 "Next" 以查看该主体的所有属性。

有三个窗口包含属性信息。请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关每个窗口中各种属性的信息。或者，转至[SEAM Tool 面板说明](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-223)，了解所有主体属性说明。

1. 查看完毕后，单击 "Cancel"。

**示例 24–2 查看 Kerberos 主体属性**

以下示例显示了查看 jdb/admin 主体时的第一个窗口。



**示例 24–3 查看 Kerberos 主体属性（命令行）**

在以下示例中，kadmin 的 get\_principal 命令用于查看 jdb/admin 主体的属性。

|  |
| --- |
| kadmin: **getprinc jdb/admin**  Principal: jdb/admin@EXAMPLE.COM  Expiration date: Fri Aug 25 17:19:05 PDT 2004  Last password change: [never]  Password expiration date: Wed Apr 14 11:53:10 PDT 2003  Maximum ticket life: 1 day 16:00:00  Maximum renewable life: 1 day 16:00:00  Last modified: Thu Jan 14 11:54:09 PST 2003 (admin/admin@EXAMPLE.COM)  Last successful authentication: [never]  Last failed authentication: [never]  Failed password attempts: 0  Number of keys: 1  Key: vno 1, DES cbc mode with CRC-32, no salt  Attributes: REQUIRES\_HW\_AUTH  Policy: [none]  kadmin: **quit** |

**Procedure如何创建新的 Kerberos 主体**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

**注 –**

如果要创建一个可能需要新策略的新主体，则应在创建新主体之前创建新策略。请转至[如何创建新的 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve2/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Principals" 选项卡。
2. 单击 "New"。

此时会显示包含某些主体属性的 "Principal Basics" 面板。

1. 指定主体名称和口令。

必须提供主体名称和口令。

1. 指定该主体属性的值，然后继续单击 "Next" 以指定其他属性。

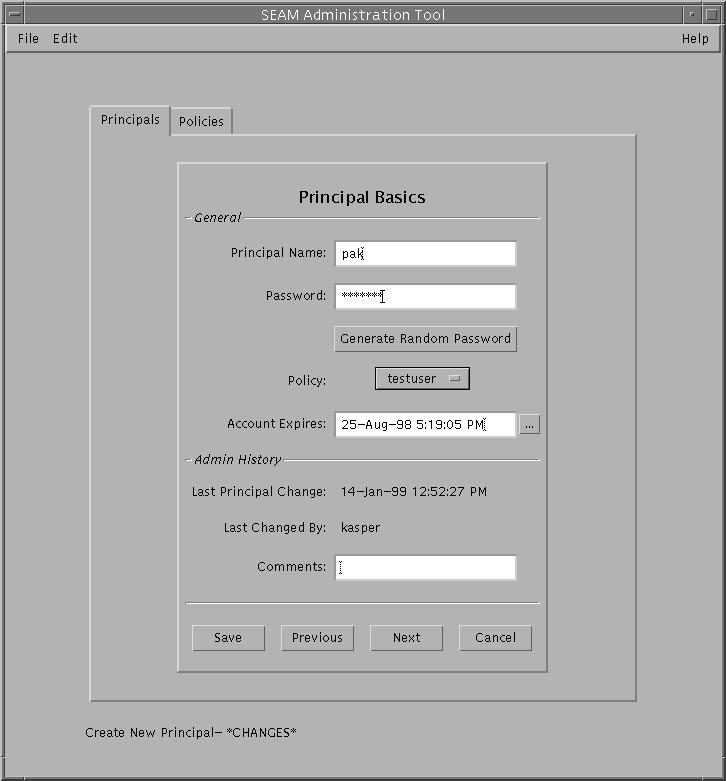
有三个窗口包含属性信息。请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关每个窗口中各种属性的信息。或者，转至[SEAM Tool 面板说明](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-223)，了解所有主体属性说明。

1. 单击 "Save" 以保存主体，或在最后一个面板上单击 "Done"。
2. 如有必要，在 /etc/krb5/kadm5.acl 文件中为新主体设置 Kerberos 管理权限。

有关更多详细信息，请参见[如何修改 Kerberos 管理权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vds/index.html)。

**示例 24–4 创建新的 Kerberos 主体**

以下示例显示了创建称为 pak 的新主体时的 "Principal Basics" 面板。该策略设置为 testuser。



**示例 24–5 创建新的 Kerberos 主体（命令行）**

在以下示例中，kadmin 的 add\_principal 命令用于创建称为 pak 的新主体。该主体的策略设置为 testuser。

|  |
| --- |
| kadmin: **add\_principal -policy testuser pak**  Enter password for principal "pak@EXAMPLE.COM": *<Type the password>*  Re-enter password for principal "pak@EXAMPLE.COM": *<Type the password again>*  Principal "pak@EXAMPLE.COM" created.  kadmin: **quit** |

**Procedure如何复制 Kerberos 主体**

此过程说明如何使用某个现有主体的全部或部分属性来创建新主体。此过程没有等效命令行。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Principals" 选项卡。
2. 在列表中选择要复制的主体，然后单击 "Duplicate"。

此时会显示 "Principal Basics" 面板。除空的 "Principal Name" 和 "Password" 字段之外，选定主体的其他属性都将被复制。

1. 指定主体名称和口令。

必须提供主体名称和口令。要完全复制选定主体，请单击 "Save" 并跳至[步骤 7](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdo/index.html#aadmin-dup-princ-1)。

1. 指定该主体属性的其他值，然后继续单击 "Next" 以指定其他属性。

有三个窗口包含属性信息。请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关每个窗口中各种属性的信息。或者，转至[SEAM Tool 面板说明](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-223)，了解所有主体属性说明。

1. 单击 "Save" 以保存主体，或在最后一个面板上单击 "Done"。
2. 如有必要，在 /etc/krb5/kadm5.acl 文件中为主体设置 Kerberos 管理权限。

有关更多详细信息，请参见[如何修改 Kerberos 管理权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vds/index.html)。

**Procedure如何修改 Kerberos 主体**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Principals" 选项卡。
2. 在列表中选择要修改的主体，然后单击 "Modify"。

此时会显示包含该主体某些属性的 "Principal Basics" 面板。

1. 修改该主体的属性，然后继续单击 "Next" 以修改其他属性。

有三个窗口包含属性信息。请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关每个窗口中各种属性的信息。或者，转至[SEAM Tool 面板说明](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-223)，了解所有主体属性说明。

**注 –**

不能修改主体的名称。要重命名主体，必须首先复制该主体，为其指定一个新名称并保存，然后删除旧主体。

1. 单击 "Save" 按钮以保存主体，或在最后一个面板上单击 "Done"。
2. 在 /etc/krb5/kadm5.acl 文件中，修改该主体的 Kerberos 管理权限。

有关更多详细信息，请参见[如何修改 Kerberos 管理权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vds/index.html)。

**示例 24–6 修改 Kerberos 主体口令（命令行）**

在以下示例中，kadmin 的 change\_password 命令用于修改 jdb 主体的口令。change\_password 命令不允许将口令更改为主体口令历史记录中的口令。

|  |
| --- |
| kadmin: **change\_password jdb**  Enter password for principal "jdb": *<Type the new password>*  Re-enter password for principal "jdb": *<Type the password again>*  Password for "jdb@EXAMPLE.COM" changed.  kadmin: **quit** |

要修改主体的其他属性，必须使用 kadmin 的 modify\_principal 命令。

**Procedure如何删除 Kerberos 主体**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Principals" 选项卡。
2. 在列表中选择要删除的主体，然后单击 "delete"。

确认删除后，将删除该主体。

1. 从 Kerberos 访问控制列表 (access control list, ACL) 文件 /etc/krb5/kadm5.acl 中删除该主体。

有关更多详细信息，请参见[如何修改 Kerberos 管理权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vds/index.html)。

**示例 24–7 删除 Kerberos 主体（命令行）**

在以下示例中，kadmin 的 delete\_principal 命令用于删除 jdb 主体。

|  |
| --- |
| kadmin: **delete\_principal pak**  Are you sure you want to delete the principal "pak@EXAMPLE.COM"? (yes/no): **yes**  Principal "pak@EXAMPLE.COM" deleted.  Make sure that you have removed this principal from all ACLs before reusing.  kadmin: **quit** |

**Procedure如何设置缺省值以创建新的 Kerberos 主体**

此过程没有等效命令行。

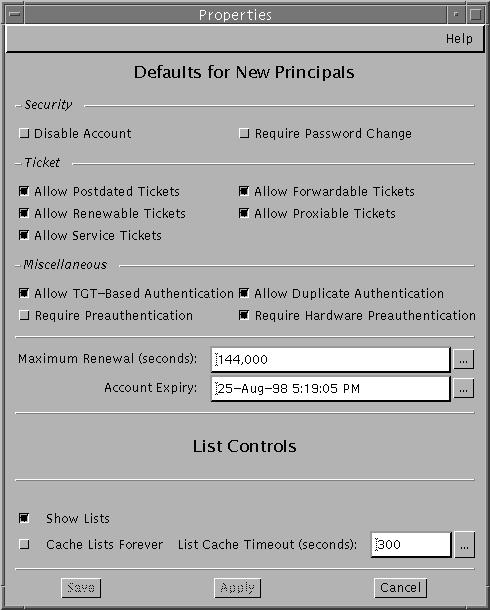
1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 从 "Edit" 菜单中选择 "Properties"。

此时会显示 "Properties" 窗口。



1. 选择要在创建新主体时使用的缺省值。

请从 "Help" 菜单中选择 "Context-Sensitive Help"，以获取有关每个窗口中各种属性的信息。

1. 单击 "Save"。

**Procedure如何修改 Kerberos 管理权限**

尽管您的站点可能有许多用户主体，但您通常只希望一小部分用户能够管理 Kerberos 数据库。管理 Kerberos 数据库的权限由 Kerberos 访问控制列表 (access control list, ACL) 文件 kadm5.acl 确定。通过 kadm5.acl 文件，可以允许或禁用各个主体的权限。或者，可在主体名称中使用 "\*" 通配符来指定主体组的权限。

1. 成为主 KDC 的超级用户。
2. 编辑 /etc/krb5/kadm5.acl 文件。

kadm5.acl 文件中的项必须使用以下格式：

|  |
| --- |
| *principal* *privileges* [*principal-target*] |

|  |  |  |
| --- | --- | --- |
| *principal* | 指定要为其授予权限的主体。 主体名称的任何部分都可以包含 "\*" 通配符，这在为一组主体提供相同权限时很有用。例如，如果要指定包含 admin 实例的所有主体，则可使用 \*/admin@*realm*。  请注意，admin 实例常用于将单独的权限（如对 Kerberos 数据库的管理访问权限）授予单独的 Kerberos 主体。 例如，用户 jdb 可能具有用于管理的主体 jdb/admin。这样，用户 jdb 便仅在实际需要使用这些权限时，才会获取 jdb/admin 票证。 | |
| *privileges* | 指定主体能够执行和不能执行的操作。 此字段由一个或多个下列字符或其对应大写形式的字符组成。 如果字符为大写形式（或未指定），则不允许执行该操作。 如果字符为小写形式，则允许执行该操作。 | |
|  | a | [不]允许添加主体或策略。 |
|  | d | [不]允许删除主体或策略。 |
|  | m | [不]允许修改主体或策略。 |
|  | c | [不]允许更改主体的口令。 |
|  | i | [不]允许查询 Kerberos 数据库。 |
|  | l | [不]允许列出 Kerberos 数据库中的主体或策略。 |
|  | x 或 \* | 允许所有权限 (admcil)。 |
| *principal-target* | 在此字段中指定主体时，*privileges* 仅在 *principal* 对 *principal-target* 进行操作时，才应用于 *principal*。主体名称的任何部分都可以包含 "\*" 通配符，这在对主体分组时很有用。 | |

**示例 24–8 修改 Kerberos 管理权限**

kadm5.acl 文件中的以下项授予 EXAMPLE.COM 领域中包含 admin 实例的任何主体对 Kerberos 数据库的所有权限：

|  |
| --- |
| \*/admin@EXAMPLE.COM \* |

kadm5.acl 文件中的以下项授予 jdb@EXAMPLE.COM 主体添加、列出和查询包含 root 实例的任何主体的权限。

|  |
| --- |
| jdb@EXAMPLE.COM ali \*/root@EXAMPLE.COM |

**管理 Kerberos 策略**

本节提供使用 SEAM Tool 管理策略的逐步说明，还提供等效命令行示例（如果有）。

**管理 Kerberos 策略（任务列表）**

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 查看策略列表。 | 通过单击 "Policies" 选项卡来查看策略列表。 | [如何查看 Kerberos 策略列表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve0/index.html) |
| 查看策略属性。 | 通过在 "Policy List" 中选择策略，然后单击 "Modify" 按钮来查看策略的属性。 | [如何查看 Kerberos 策略属性](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve1/index.html) |
| 创建新策略。 | 通过单击 "Policy List" 面板中的 "Create New" 按钮来创建新策略。 | [如何创建新的 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve2/index.html) |
| 复制策略。 | 通过在 "Policy List" 中选择要复制的策略，然后单击 "Duplicate" 按钮来复制策略。 | [如何复制 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve3/index.html) |
| 修改策略。 | 通过在 "Policy List" 中选择要修改的策略，然后单击 "Modify" 按钮来修改策略。  请注意，不能修改策略的名称。要重命名策略，必须首先复制该策略，为其指定一个新名称并保存，然后删除旧策略。 | [如何修改 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve4/index.html) |
| 删除策略。 | 通过在 "Policy List" 中选择要删除的策略，然后单击 "Delete" 按钮来删除策略。 | [如何删除 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve5/index.html) |

**Procedure如何查看 Kerberos 策略列表**

此过程后附等效命令行示例。

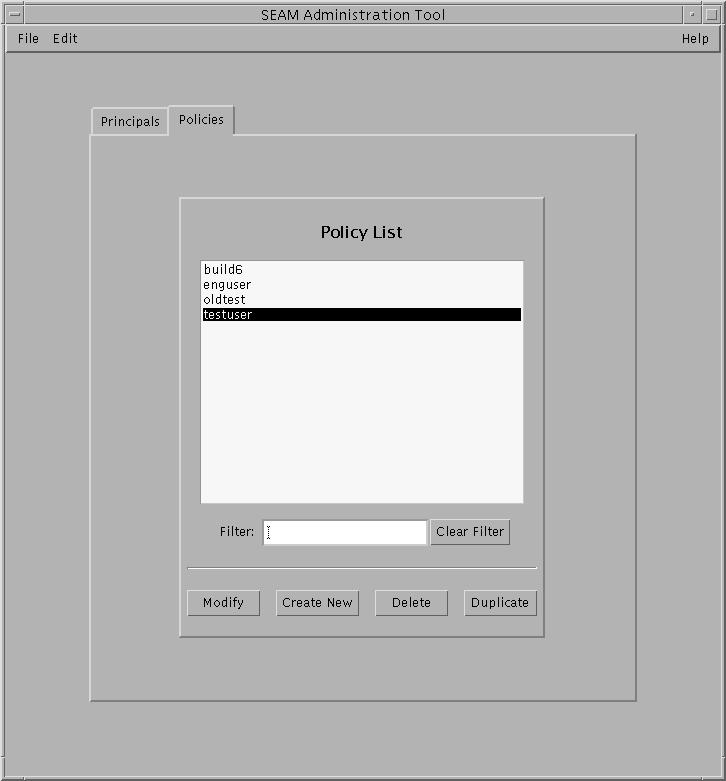
1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Policies" 选项卡。

此时会显示策略列表。



1. 显示特定策略或策略子列表。

在 "Filter" 字段中键入过滤字符串，然后按 "Return"。如果过滤操作成功，则会显示与过滤器匹配的策略列表。

过滤字符串必须由一个或多个字符组成。由于过滤机制区分大小写，因此需要对过滤器使用正确的大小写字母。例如，如果键入过滤字符串 ge，则过滤机制仅显示包含 ge 字符串的策略（如 george 或 edge）。

如果要显示策略的完整列表，请单击 "Clear Filter"。

**示例 24–9 查看 Kerberos 策略列表（命令行）**

在以下示例中，kadmin 的 list\_policies 命令用于列出与 \*user\* 匹配的所有策略。通配符可与 list\_policies 命令一起使用。

|  |
| --- |
| kadmin: **list\_policies \*user\***  testuser  enguser  kadmin: **quit** |

**Procedure如何查看 Kerberos 策略属性**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

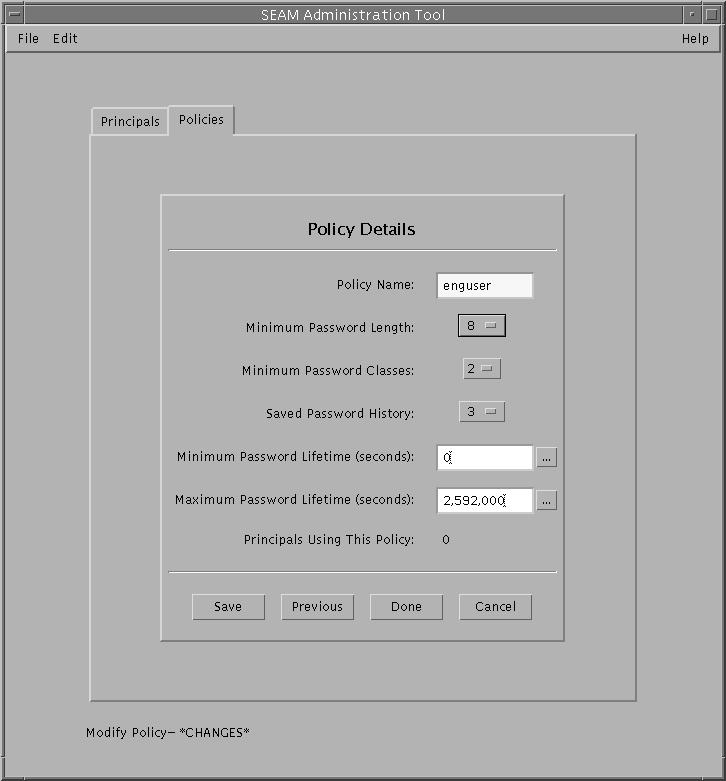
1. 单击 "Policies" 选项卡。
2. 在列表中选择要查看的策略，然后单击 "Modify"。

此时会显示 "Policy Details" 面板。

1. 查看完毕后，单击 "Cancel"。

**示例 24–10 查看 Kerberos 策略属性**

以下示例显示了查看 test 策略时的 "Policy Details" 面板。



**示例 24–11 查看 Kerberos 策略属性（命令行）**

在以下示例中，kadmin 的 get\_policy 命令用于查看 enguser 策略的属性。

|  |
| --- |
| kadmin: **get\_policy enguser**  Policy: enguser  Maximum password life: 2592000  Minimum password life: 0  Minimum password length: 8  Minimum number of password character classes: 2  Number of old keys kept: 3  Reference count: 0  kadmin: **quit** |

引用计数是使用此策略的主体数。

**Procedure如何创建新的 Kerberos 策略**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Policies" 选项卡。
2. 单击 "New"。

此时会显示 "Policy Details" 面板。

1. 在 "Policy Name" 字段中指定策略的名称。

必须提供策略名称。

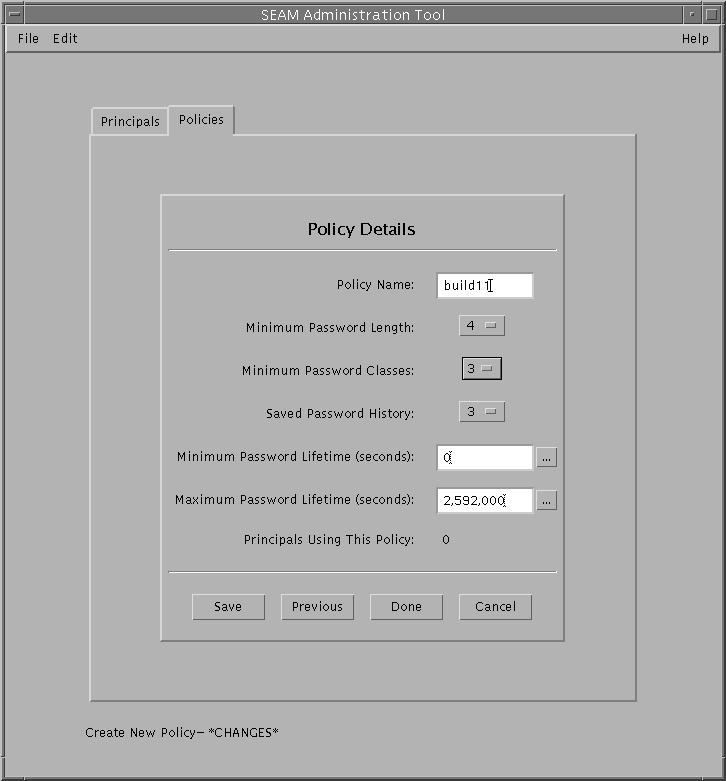
1. 指定策略属性的值。

请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关此窗口中各种属性的信息。或者，转至[表 24–5](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-tbl-226)，了解所有策略属性说明。

1. 单击 "Save" 按钮以保存策略，或单击 "Done"。

**示例 24–12 创建新的 Kerberos 策略**

在以下示例中，创建了一个称为 build11 的新策略。"Minimum Password Classes" 设置为 3。



**示例 24–13 创建新的 Kerberos 策略（命令行）**

在以下示例中，kadmin 的 add\_policy 命令用于创建 build11 策略。此策略要求口令中至少有 3 类字符。

|  |
| --- |
| $ **kadmin**  kadmin: **add\_policy -minclasses 3 build11**  kadmin: **quit** |

**Procedure如何复制 Kerberos 策略**

此过程说明如何使用某个现有策略的全部或部分属性来创建新策略。此过程没有等效命令行。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Policies" 选项卡。
2. 在列表中选择要复制的策略，然后单击 "Duplicate"。

此时会显示 "Policy Details" 面板。除空的 "Policy Name" 字段以外，选定策略的其他所有属性都将被复制。

1. 在 "Policy Name" 字段中指定复制策略的名称。

必须提供策略名称。要完全复制选定策略，请跳至[步骤 6](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve3/index.html#aadmin-pol-done-1)。

1. 指定策略属性的其他值。

请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关此窗口中各种属性的信息。或者，转至[表 24–5](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-tbl-226)，了解所有策略属性说明。

1. 单击 "Save" 按钮以保存策略，或单击 "Done"。

**Procedure如何修改 Kerberos 策略**

此过程后附等效命令行示例。

1. 如有必要，启动 SEAM Tool。

有关详细信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Policies" 选项卡。
2. 在列表中选择要修改的策略，然后单击 "Modify"。

此时会显示 "Policy Details" 面板。

1. 修改该策略的属性。

请从 "Help" 菜单中选择 "Context-Sensitive Help"，获取有关此窗口中各种属性的信息。或者，转至[表 24–5](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-tbl-226)，了解所有策略属性说明。

**注 –**

不能修改策略的名称。要重命名策略，必须首先复制该策略，为其指定一个新名称并保存，然后删除旧策略。

1. 单击 "Save" 按钮以保存策略，或单击 "Done"。

**示例 24–14 修改 Kerberos 策略（命令行）**

在以下示例中，kadmin 的 modify\_policy 命令用于将 build11 策略的最小口令长度修改为 5 个字符。

|  |
| --- |
| $ **kadmin**  kadmin: **modify\_policy -minlength 5 build11**  kadmin: **quit** |

**Procedure如何删除 Kerberos 策略**

此过程后附等效命令行示例。

**注 –**

删除某策略之前，必须从当前正在使用该策略的所有主体取消该策略。为此，需要修改这些主体的策略属性。如果有任何主体在使用该策略，则无法将其删除。

1. 如有必要，启动 SEAM Tool。

有关更多信息，请参见[如何启动 SEAM Tool](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdg/index.html)。

|  |
| --- |
| $ **/usr/sbin/gkadmin** |

1. 单击 "Policies" 选项卡。
2. 在列表中选择要删除的策略，然后单击 "Delete"。

确认删除后，将删除该策略。

**示例 24–15 删除 Kerberos 策略（命令行）**

在以下示例中，kadmin 的 delete\_policy 命令用于删除 build11 策略。

|  |
| --- |
| kadmin: **delete\_policy build11**  Are you sure you want to delete the policy "build11"? (yes/no): **yes**  kadmin: **quit** |

删除某策略之前，必须从当前正在使用该策略的所有主体取消该策略。为此，需要对受影响的主体使用 kadmin 的 modify\_principal **- policy** 命令。如果主体正在使用该策略，则 delete\_policy 命令将会失败。

**SEAM Tool 参考**

本节为 SEAM Tool 中的每个面板提供说明。另外，还提供有关以受限权限使用 SEAM Tool 的信息。

**SEAM Tool 面板说明**

本节提供可在 SEAM Tool 中指定或查看的每个主体和策略属性的说明。这些属性按显示它们的面板进行组织。

表 24–2 SEAM Tool 的 "Principal Basics" 面板中的属性

| **属性** | **说明** |
| --- | --- |
| Principal Name | 主体的名称（全限定主体名称的 *primary*/*instance* 部分）。主体是 KDC 可以为其指定票证的唯一标识。  修改主体时不能编辑其名称。 |
| Password | 主体的口令。可使用 "Generate Random Password" 按钮为主体创建随机口令。 |
| Policy | 主体的可用策略菜单。 |
| Account Expires | 主体帐户的失效日期和时间。帐户失效后，主体就无法再获取票证授予票证 (Ticket-Granting Ticket, TGT)，并且可能无法登录。 |
| Last Principal Change | 上次修改主体信息的日期。（只读） |
| Last Changed By | 上次更改此主体帐户的主体的名称。（只读） |
| 注释 | 与主体有关的注释（如“临时帐户”）。 |

表 24–3 SEAM Tool 的 "Principal Details" 面板中的属性

| **属性** | **说明** |
| --- | --- |
| Last Success | 主体上次登录成功的日期和时间。（只读） |
| Last Failure | 主体上次登录失败的日期和时间。（只读） |
| Failure Count | 主体登录失败的次数。（只读） |
| Last Password Change | 上次更改主体口令的日期和时间。（只读） |
| Password Expires | 主体当前口令失效的日期和时间。 |
| Key Version | 主体的密钥版本号。通常，只有在口令已泄漏的情况下才会更改此属性。 |
| Maximum Lifetime (seconds) | 可将票证授予主体的最长时间（不续用）。 |
| Maximum Renewal (seconds) | 主体可续用现有票证的最长时间。 |

表 24–4 SEAM Tool 的 "Principal Flags" 面板中的属性

| **属性（单选按钮）** | **说明** |
| --- | --- |
| Disable Account | 选中此项后，将禁止主体登录。此属性提供了一种临时冻结主体帐户的简便方法。 |
| Require Password Change | 选中此项后，将使主体的当前口令失效，这将会强制用户使用 kpasswd 命令来创建新口令。如果安全性被破坏，并且需要确保替换旧口令，则此属性很有用。 |
| Allow Postdated Tickets | 选中此项后，将允许主体获取以后生效的票证。  例如，如果 cron 作业必须在几小时后运行，但您又因为票证的生命周期不够长而无法提前获取票证，则可能需要对其使用以后生效的票证。 |
| Allow Forwardable Tickets | 选中此项后，将允许主体获取可转发的票证。  可转发的票证即可转发至远程主机以提供单点登录会话的票证。例如，如果使用可转发的票证并且通过 ftp 或 rsh 进行自我验证，则可使用其他服务（如 NFS 服务），而不会提示您输入其他口令。 |
| Allow Renewable Tickets | 选中此项后，将允许主体获取可续用的票证。  主体可以自动延长可续用票证的失效日期或时间，而不必在票证首次失效后获取新的票证。目前，NFS 服务是可以续用票证的票证服务。 |
| Allow Proxiable Tickets | 选中此项后，将允许主体获取可代理的票证。  可代理票证即可被服务以客户机名义执行客户机操作时使用的票证。借助可代理票证，服务可采用客户机的身份来获取其他服务的票证。但是，该服务不能获取票证授予票证 (Ticket-Granting Ticket, TGT)。 |
| Allow Service Tickets | 选中此项后，将允许为主体颁发服务票证。  不允许为 kadmin/*hostname* 和 changepw/*hostname* 主体颁发服务票证。此做法可确保只有这些主体才能更新 KDC 数据库。 |
| Allow TGT-Based Authentication | 选中此项后，将允许服务主体为其他主体提供服务。具体而言，此属性允许 KDC 为服务主体颁发服务票证。  此属性仅对服务主体有效。如果取消选中此项，将无法为服务主体颁发服务票证。 |
| Allow Duplicate Authentication | 选中此项后，将允许用户主体获取其他用户主体的服务票证。  此属性仅对用户主体有效。如果取消选中此项，用户主体将仍可获取服务主体的服务票证，但不能获取其他用户主体的服务票证。 |
| Required Preauthentication | 选中此项后，KDC 在验证（通过软件）主体确为请求 TGT 的主体之前，不会将请求的票证授予票证 (Ticket-Granting Ticket, TGT) 发送给该主体。此预验证通常通过附加口令（如 DES 卡）完成。  如果取消选中此项，则 KDC 不必在向主体发送请求的 TGT 之前预先验证主体。 |
| Required Hardware Authentication | 选中此项后，KDC 在验证（通过硬件）主体确为请求 TGT 的主体之前，不会将请求的票证授予票证 (Ticket-Granting Ticket, TGT) 发送给该主体。例如，可对 Java 环形阅读器进行硬件预验证。  如果取消选中此项，则 KDC 不必在向主体发送请求的 TGT 之前预先验证主体。 |

表 24–5 SEAM Tool 的 "Policy Basics" 面板中的属性

| **属性** | **说明** |
| --- | --- |
| Policy Name | 策略的名称。策略是一组用于管理主体口令和票证的规则。  修改策略时不能编辑其名称。 |
| Minimum Password Length | 主体口令的最小长度。 |
| Minimum Password Classes | 主体口令中要求使用的最少不同字符类型数。  例如，最少类值为 2 表示口令必须至少使用两种不同的字符类型，如字母和数字 (hi2mom)。值为 3 表示口令必须至少使用三种不同的字符类型，如字母、数字和标点符号 (hi2mom!)。依此类推。  值为 1 则表示对口令字符类型数未设置任何限制。 |
| Saved Password History | 主体先前使用的口令数，以及无法重新使用的先前口令的列表。 |
| Minimum Password Lifetime (seconds) | 口令在可更改之前必须经历的最短时间。 |
| Maximum Password Lifetime (seconds) | 口令在必须更改之前可以经历的最长时间。 |
| Principals Using This Policy | 当前应用此策略的主体数。（只读） |

**以受限 Kerberos 管理权限使用 SEAM Tool**

如果 admin 主体拥有管理 Kerberos 数据库的所有权限，则可使用 SEAM Administration Tool 的所有功能。但是，您的权限可能受到限制，如仅允许查看主体列表或更改主体口令。借助受限 Kerberos 管理权限，仍然可以使用 SEAM Tool。但是，SEAM Tool 的各个部分会基于未拥有的 Kerberos 管理权限而变化。[表 24–6](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ve6/index.html#aadmin-tbl-209) 显示了 SEAM Tool 基于 Kerberos 管理权限变化的情况。

没有列表权限时，SEAM Tool 会发生最直观的变化。如果没有列表权限，列表面板便不会显示供您处理的主体和策略列表。相反，您必须使用列表面板中的 "Name" 字段来指定要处理的主体或策略。

如果您登录到 SEAM Tool，但却没有足够的权限来使用它执行任务，则会显示以下消息并且会返回到 "SEAM Administration Login" 窗口：

|  |
| --- |
| Insufficient privileges to use gkadmin: ADMCIL. Please try using another principal. |

要更改主体的权限以便它可管理 Kerberos 数据库，请转至[如何修改 Kerberos 管理权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vds/index.html)。

表 24–6 以受限 Kerberos 管理权限使用 SEAM Tool

| **禁用的权限** | **SEAM Tool 如何变化** |
| --- | --- |
| a（添加） | "Principal List" 和 "Policy List" 面板中的 "Create New" 和 "Duplicate" 按钮不可用。如果没有添加权限，则无法创建新主体或策略，也不能复制它们。 |
| d（删除） | "Principal List" 和 "Policy List" 面板中的 "Delete" 按钮不可用。如果没有删除权限，则无法删除主体或策略。 |
| m（修改） | "Principal List" 和 "Policy List" 面板中的 "Modify" 按钮不可用。如果没有修改权限，则无法修改主体或策略。  而且，如果 "Modify" 按钮不可用，则即使您拥有更改口令的权限，也不能修改主体的口令。 |
| c（更改口令） | "Principal Basics" 面板中的 "Password" 字段处于只读状态，无法更改。如果没有更改口令的权限，则无法修改主体的口令。  请注意，即使您拥有更改口令的权限，还必须同时拥有修改权限才能更改主体的口令。 |
| i（查询数据库） | "Principal List" 和 "Policy List" 面板中的 "Modify" 和 "Duplicate" 按钮不可用。如果没有查询权限，则无法修改或复制主体或策略。  而且，如果 "Modify" 按钮不可用，则即使您拥有更改口令的权限，也不能修改主体的口令。 |
| l（列出） | 列表面板中的主体和策略列表不可用。如果没有列表权限，则必须使用列表面板中的 "Name" 字段来指定要处理的主体或策略。 |

**管理密钥表文件**

提供服务的每台主机都必须包含称为 **keytab（密钥表）**的本地文件，keytab（密钥表）是“key table（密钥表）”的缩写。密钥表包含相应服务的主体，称为**服务密钥**。服务使用服务密钥向 KDC 进行自我验证，并且只有 Kerberos 和服务本身知道服务密钥。例如，如果您有基于 Kerberos 的 NFS 服务器，则该服务器必须具有包含其 nfs 服务主体的密钥表文件。

要将服务密钥添加至密钥表文件，应使用 kadmin 的 ktadd 命令，将相应的服务主体添加至主机的密钥表文件。由于要将服务主体添加至密钥表文件，因此该主体必须已存在于 Kerberos 数据库中，以便 kadmin 可验证其存在。在主 KDC 上，密钥表文件的缺省位置为：/etc/krb5/kadm5.keytab。在提供基于 Kerberos 的服务的应用程序服务器上，密钥表文件的缺省位置为：/etc/krb5/krb5.keytab。

密钥表类似于用户的口令。正如用户保护其口令很重要一样，应用程序服务器保护其密钥表文件同样也很重要。应始终将密钥表文件存储在本地磁盘上，并且只允许 root 用户读取这些文件。另外，绝不要通过不安全的网络发送密钥表文件。

还有一种特殊情况需要将 root 主体添加至主机的密钥表文件。如果希望 Kerberos 客户机用户挂载基于 Kerberos 的 NFS 文件系统（要求与超级用户等效的权限），则必须将客户机的 root 主体添加至客户机的密钥表文件。否则，每当用户要使用 root 权限挂载基于 Kerberos 的 NFS 文件系统时，即使正在使用自动挂载程序，也必须以 root 身份使用 kinit 命令来获取客户机 root 主体的凭证。

**注 –**

设置主 KDC 时，需要将 kadmind 和 changepw 主体添加至 kadm5.keytab 文件。

可用于管理密钥表文件的另一个命令是 ktutil 命令。使用此交互式命令，可在没有 Kerberos 管理权限的情况下管理本地主机的密钥表文件，因为 ktutil 不会像 kadmin 那样与 Kerberos 数据库交互，因此，将主体添加至密钥表文件后，可使用 ktutil 来查看密钥表文件中的密钥列表，或临时禁用对服务的验证。

**注 –**

使用 kadmin 中的 ktadd 命令更改密钥表文件中的主体时，将生成一个新的密钥并将其添加至密钥表文件。

**管理密钥表文件（任务列表）**

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 将服务主体添加至密钥表文件。 | 使用 kadmin 的 ktadd 命令将服务主体添加至密钥表文件。 | [如何将 Kerberos 服务主体添加至密钥表文件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vea/index.html) |
| 从密钥表文件中删除服务主体。 | 使用 kadmin 的 ktremove 命令从密钥表文件中删除服务主体。 | [如何从密钥表文件中删除服务主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veb/index.html) |
| 显示密钥表文件中的密钥列表（主体列表）。 | 使用 ktutil 命令来显示密钥表文件中的密钥列表。 | [如何显示密钥表文件中的密钥列表（主体）](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vec/index.html) |
| 临时禁用对主机上的服务的验证。 | 此过程可以快速地临时禁用对主机上的服务的验证，而不需要 kadmin 权限。  使用 ktutil 从服务器的密钥表文件中删除服务主体之前，应将原始密钥表文件复制到一个临时位置。如果要再次启用该服务，请将原始密钥表文件复制回其相应的位置。 | [如何临时禁用对主机上的服务的验证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ved/index.html) |

**Procedure如何将 Kerberos 服务主体添加至密钥表文件**

1. 确保 Kerberos 数据库中已存在该主体。

有关更多信息，请参见[如何查看 Kerberos 主体列表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdl/index.html)。

1. 成为需要将主体添加至其密钥表文件的主机的超级用户。
2. 启动 kadmin 命令。

|  |
| --- |
| # **/usr/sbin/kadmin** |

1. 使用 ktadd 命令将主体添加至密钥表文件。

|  |
| --- |
| kadmin: **ktadd** [**-e** *enctype*] [**-k** *keytab*] [**-q**] [*principal* | **-glob** *principal-exp*] |

1. **-e** *enctype*
2. 覆盖 krb5.conf 文件中定义的加密类型列表。
3. **-k** *keytab*
4. 指定密钥表文件。缺省情况下，使用 /etc/krb5/krb5.keytab。
5. **-q**
6. 显示简要信息。
7. *principal*
8. 指定要添加至密钥表文件的主体。可以添加以下服务主体：host、root、nfs 和 ftp。
9. **-glob** *principal-exp*
10. 指定主体表达式。与 *principal-exp* 匹配的所有主体都将添加至密钥表文件。主体表达式的规则与 kadmin 的 list\_principals 命令的规则相同。
11. 退出 kadmin 命令。

|  |
| --- |
| kadmin: **quit** |

**示例 24–16 将服务主体添加至密钥表文件**

在以下示例中，kadmin/admin 和 kadmin/changepw 主体被添加至主 KDC 的密钥表文件。对于该示例，密钥表文件必须是在 kdc.conf 文件中指定的文件。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin.local**  kadmin.local: **ktadd -k /etc/krb5/kadm5.keytab kadmin/admin kadmin/changepw**  EnEntry for principal kadmin/admin@example.com with kvno 3, encryption type AES-128 CTS mode  with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/admin@example.com with kvno 3, encryption type Triple DES cbc  mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/admin@example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/admin@example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/changepw@example.com with kvno 3, encryption type AES-128 CTS  mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/changepw@example.com with kvno 3, encryption type Triple DES cbc  mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/changepw@example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/changepw@example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin.local: **quit** |

在以下示例中，denver 的 host 主体被添加至 denver 的密钥表文件，以便 KDC 验证 denver 的网络服务。

|  |
| --- |
| denver # **/usr/sbin/kadmin**  kadmin: **ktadd host/denver@example.com@EXAMPLE.COM**  Entry for principal host/denver@example.com with kvno 3, encryption type AES-128 CTS mode  with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/denver@example.com with kvno 3, encryption type Triple DES cbc mode  with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/denver@example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/denver@example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: **quit** |

**Procedure如何从密钥表文件中删除服务主体**

1. 成为包含必须从其密钥表文件中删除的服务主体的主机的超级用户。
2. 启动 kadmin 命令。

|  |
| --- |
| # **/usr/sbin/kadmin** |

1. （可选的）要显示密钥表文件中的当前主体（密钥）列表，请使用 ktutil 命令。

有关详细说明，请参见[如何显示密钥表文件中的密钥列表（主体）](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vec/index.html)。

1. 使用 ktremove 命令从密钥表文件中删除主体。

|  |
| --- |
| kadmin: **ktremove** [**-k** *keytab*] [**-q**] *principal* [*kvno* | **all** | **old** ] |

1. **-k** *keytab*
2. 指定密钥表文件。缺省情况下，使用 /etc/krb5/krb5.keytab。
3. **-q**
4. 显示简要信息。
5. *principal*
6. 指定要从密钥表文件中删除的主体。
7. *kvno*
8. 删除密钥版本号与 *kvno* 匹配的指定主体的所有项。
9. all
10. 删除指定主体的所有项。
11. old
12. 删除指定主体（具有最高密钥版本号的主体除外）的所有项。
13. 退出 kadmin 命令。

|  |
| --- |
| kadmin: **quit** |

**示例 24–17 从密钥表文件中删除服务主体**

在以下示例中，从 denver 的密钥表文件中删除了 denver 的 host 主体。

|  |
| --- |
| denver # **/usr/sbin/kadmin**  kadmin: **ktremove host/denver.example.com@EXAMPLE.COM**  kadmin: Entry for principal host/denver.example.com@EXAMPLE.COM with kvno 3  removed from keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: **quit** |

**Procedure如何显示密钥表文件中的密钥列表（主体）**

1. 成为包含密钥表文件的主机的超级用户。

**注 –**

尽管可以创建由其他用户拥有的密钥表文件，但使用密钥表文件的缺省位置需要 root 拥有权。

1. 启动 ktutil 命令。

|  |
| --- |
| # **/usr/bin/ktutil** |

1. 使用 read\_kt 命令将密钥表文件读入密钥列表缓冲区。

|  |
| --- |
| ktutil: **read\_kt** *keytab* |

1. 使用 list 命令显示密钥列表缓冲区。

|  |
| --- |
| ktutil: **list** |

1. 此时会显示当前的密钥列表缓冲区。
2. 退出 ktutil 命令。

|  |
| --- |
| ktutil: **quit** |

**示例 24–18 显示密钥表文件中的密钥列表（主体）**

以下示例显示了 denver 主机的 /etc/krb5/krb5.keytab 文件中的密钥列表。

|  |
| --- |
| denver # **/usr/bin/ktutil**  ktutil: **read\_kt /etc/krb5/krb5.keytab**  ktutil: **list**  slot KVNO Principal  ---- ---- ---------------------------------------  1 5 host/denver@EXAMPLE.COM  ktutil: **quit** |

**Procedure如何临时禁用对主机上的服务的验证**

有时可能需要在网络应用程序服务器上，临时禁用对服务（如 rlogin 或 ftp）的验证机制。例如，可能希望在执行维护过程时禁止用户登录到系统。使用 ktutil 命令，可以通过从服务器的密钥表文件中删除服务主体来完成此任务，而不需要 kadmin 权限。要再次启用验证，只需要将保存的原始密钥表文件复制回其原始位置。

**注 –**

缺省情况下，大多数服务都被设置为要求验证。如果某服务未设置为要求验证，则即使对该服务禁用验证，该服务仍然会运行。

1. 成为包含密钥表文件的主机的超级用户。

**注 –**

尽管可以创建由其他用户拥有的密钥表文件，但使用密钥表文件的缺省位置需要 root 拥有权。

1. 将当前密钥表文件保存到临时文件。
2. 启动 ktutil 命令。

|  |
| --- |
| # **/usr/bin/ktutil** |

1. 使用 read\_kt 命令将密钥表文件读入密钥列表缓冲区。

|  |
| --- |
| ktutil: **read\_kt** *keytab* |

1. 使用 list 命令显示密钥列表缓冲区。

|  |
| --- |
| ktutil: **list** |

1. 此时会显示当前的密钥列表缓冲区。请注意要禁用的服务的槽号。
2. 要临时禁用主机的服务，请使用 delete\_entry 命令从密钥列表缓冲区中删除特定的服务主体。

|  |
| --- |
| ktutil: **delete\_entry** *slot-number* |

1. 其中，*slot-number* 指定要删除的服务主体的槽号，可使用 list 命令来显示它。
2. 使用 write\_kt 命令，将密钥列表缓冲区写入新的密钥表文件。

|  |
| --- |
| ktutil: **write\_kt** *new-keytab* |

1. 退出 ktutil 命令。

|  |
| --- |
| ktutil: **quit** |

1. 移动新的密钥表文件。

|  |
| --- |
| # mv *new-keytab* *keytab* |

1. 如果要再次启用该服务，请将临时（原始）密钥表文件复制回其原始位置。

**示例 24–19 临时禁用主机上的服务**

在以下示例中，临时禁用了 denver 主机上的 host 服务。要重新启用 denver 上的主机服务，应将 krb5.keytab.temp 文件复制到 /etc/krb5/krb5.keytab 文件中。

|  |
| --- |
| denver # **cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.temp**  denver # **/usr/bin/ktutil**  ktutil:**read\_kt /etc/krb5/krb5.keytab**  ktutil:**list**  slot KVNO Principal  ---- ---- ---------------------------------------  1 8 root/denver@EXAMPLE.COM  2 5 host/denver@EXAMPLE.COM  ktutil:**delete\_entry 2**  ktutil:**list**  slot KVNO Principal  ---- ---- --------------------------------------  1 8 root/denver@EXAMPLE.COM  ktutil:**write\_kt /etc/krb5/new.krb5.keytab**  ktutil: **quit**  denver # **cp /etc/krb5/new.krb5.keytab /etc/krb5/krb5.keytab** |

* [*Previous*: 第 23 章 Kerberos 错误消息和疑难解答](https://docs.oracle.com/cd/E19253-01/819-7061/trouble-1/index.html)
* [*Next*: 第 25 章 使用 Kerberos 应用程序（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/user-7/index.html)
* © 2010, Oracle Corporation and/or its affiliates