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

[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 25 章 使用 Kerberos 应用程序（任务）

系统管理指南：安全性服务

* [*Previous*: 第 24 章 管理 Kerberos 主体和策略（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/aadmin-1/index.html)
* [*Next*: 第 26 章 Kerberos 服务（参考）](https://docs.oracle.com/cd/E19253-01/819-7061/refer-1/index.html)

**第 25 章 使用 Kerberos 应用程序（任务）**

本章适用于其系统中配置了 Kerberos 服务的人员。本章介绍如何使用提供的基于 Kerberos 的命令和服务。阅读本章中的这些命令之前，您应该对非基于 Kerberos 的版本中的这些命令比较熟悉。

由于本章适用于一般读者，因此其中包含有关票证的信息：获取、查看和销毁票证。本章还包含有关选择或更改 Kerberos 口令的信息。

以下是本章中信息的列表：

* [Kerberos 票证管理](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veg/index.html)
* [Kerberos 口令管理](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veh/index.html)
* [Kerberos 用户命令](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html)

有关 Solaris Kerberos 产品的概述，请参见[第 20 章，Kerberos 服务介绍](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vam/index.html)。

**Kerberos 票证管理**

本节介绍如何获取、查看和销毁票证。有关票证的介绍，请参见[Kerberos 服务的工作方式](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vap/index.html)。

**是否需要担心票证？**

安装任何 SEAM 发行版或 Solaris 10 发行版后，Kerberos 便内置在 login 命令中，并且您将在登录时自动获取票证。通常，由于会将基于 Kerberos 的命令 rsh、rcp、rdist、telnet 和 rlogin 设置为将票证副本转发到其他计算机，因此您不必显式请求票证来访问这些计算机。配置中可能不包括此自动转发，但这是缺省行为。有关转发票证的更多信息，请参见[基于 Kerberos 的命令概述](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#userkerbopts1)和[转发 Kerberos 票证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#user-68)。

有关票证生命周期的信息，请参见[票证生命周期](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veo/index.html#refer-502)。

**创建 Kerberos 票证**

通常，如果 PAM 配置正确，则会在登录时自动创建票证，并且无需执行任何特殊操作即可获取票证。但是，如果票证到期，则可能需要创建票证。另外，可能还需要使用缺省主体以外的其他主体，例如，如果使用 rlogin **-l** 以其他人的身份登录到计算机。

要创建票证，请使用 kinit 命令。

|  |
| --- |
| % **/usr/bin/kinit** |

kinit 命令将提示您输入口令。有关 kinit 命令的完整语法，请参见 [kinit(1)](https://docs.oracle.com/docs/cd/E19253-01/816-5165/6mbb0m9iq/index.html) 手册页。

**示例－创建 Kerberos 票证**

本示例说明用户 jennifer 如何在自己的系统上创建票证。

|  |
| --- |
| % **kinit**  Password for jennifer@ENG.EXAMPLE.COM: *<Type password>* |

在以下示例中，用户 david 使用 **-l** 选项创建了一个有效期为三个小时的票证。

|  |
| --- |
| % **kinit -l 3h david@EXAMPLE.ORG**  Password for david@EXAMPLE.ORG: *<Type password>* |

本示例说明用户 david 如何使用 **-f** 选项为其自身创建可转发票证。例如，该用户可以使用此可转发票证登录到第二个系统，然后 telnet 到第三个系统。

|  |
| --- |
| % **kinit -f david@EXAMPLE.ORG**  Password for david@EXAMPLE.ORG: *<Type password>* |

有关转发票证如何工作的更多信息，请参见[转发 Kerberos 票证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#user-68)和[票证类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veo/index.html#refer-123456)。

**查看 Kerberos 票证**

并非所有票证都相同。例如，一个票证可能是*可转发*票证，另一个票证则可能是*以后生效的*票证，而第三个票证既可能是可转发票证，又可能是以后生效的票证。使用带有 **-f** 选项的 klist 命令，可以查看所拥有的票证以及这些票证的属性：

|  |
| --- |
| % **/usr/bin/klist -f** |

以下符号表示与每个票证关联的属性，如 klist 输出所示：

A

已预验证

D

可以后生效

d

以后生效

F

可转发

f

已转发

I

初始

i

无效

P

可代理

p

代理

R

可更新

[票证类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veo/index.html#refer-123456)介绍了票证可以具有的各种属性。

**示例－查看 Kerberos 票证**

本示例说明用户 jennifer 拥有一个*初始*票证，该票证是*可转发* (F) 和*以后生效的* (d) 票证，但尚未经过验证 (i)。

|  |
| --- |
| % **/usr/bin/klist -f**  Ticket cache: /tmp/krb5cc\_74287  Default principal: jennifer@ENG.EXAMPLE.COM    Valid starting Expires Service principal  09 Mar 04 15:09:51 09 Mar 04 21:09:51 nfs/EXAMPLE.SUN.COM@EXAMPLE.SUN.COM  renew until 10 Mar 04 15:12:51, Flags: Fdi |

以下示例说明用户 david 拥有两个从另一台主机*转发* (f) 到其主机的票证。这些票证也是*可转发* (F) 票证。

|  |
| --- |
| % **klist -f**  Ticket cache: /tmp/krb5cc\_74287  Default principal: david@EXAMPLE.SUN.COM    Valid starting Expires Service principal  07 Mar 04 06:09:51 09 Mar 04 23:33:51 host/EXAMPLE.COM@EXAMPLE.COM  renew until 10 Mar 04 17:09:51, Flags: fF    Valid starting Expires Service principal  08 Mar 04 08:09:51 09 Mar 04 12:54:51 nfs/EXAMPLE.COM@EXAMPLE.COM  renew until 10 Mar 04 15:22:51, Flags: fF |

以下示例说明如何使用 **-e** 选项显示会话密钥和票证的加密类型。如果名称服务可以执行转换操作，则可使用 **-a** 选项将主机地址映射至主机名。

|  |
| --- |
| % **klist -fea**  Ticket cache: /tmp/krb5cc\_74287  Default principal: david@EXAMPLE.SUN.COM    Valid starting Expires Service principal  07 Mar 04 06:09:51 09 Mar 04 23:33:51 krbtgt/EXAMPLE.COM@EXAMPLE.COM  renew until 10 Mar 04 17:09:51, Flags: FRIA  Etype(skey, tkt): DES cbc mode with RSA-MD5, DES cbc mode with CRC-32  Addresses: client.example.com |

**销毁 Kerberos 票证**

如果要销毁在当前会话期间获取的所有 Kerberos 票证，请使用 kdestroy 命令。该命令可销毁凭证高速缓存，从而销毁所有凭证和票证。虽然通常不必销毁凭证高速缓存，但运行 kdestroy 可减少您未登录期间凭证高速缓存遭受破坏的机会。

要销毁票证，请使用 kdestroy 命令。

|  |
| --- |
| % **/usr/bin/kdestroy** |

kdestroy 命令将销毁**所有**票证。不能使用此命令来有选择性地销毁特定票证。

如果要离开系统而又担心入侵者会使用您的权限，则应使用 kdestroy 或用于锁定屏幕的屏幕保护程序。

**Kerberos 口令管理**

配置 Kerberos 服务后，您即会拥有两个口令：常规 Solaris 口令和 Kerberos 口令。可以将这两个口令设置为相同，也可以不同。

**口令选择建议**

口令几乎可以包括能够键入的任何字符，但 Ctrl 键和回车键除外。好口令是易于记忆而其他人不容易猜到的口令。以下是一些不合适的口令示例：

* 可在字典中找到的单词
* 任何常见名称或通俗名称
* 名人的姓名或字符
* 您的姓名或用户名的任何形式（例如：反向拼写您的姓名、姓名重复两次等）
* 配偶姓名、子女姓名或宠物名称
* 您的生日或亲戚的生日
* 您的社会安全号、驾照号、护照号或其他类似的身份标识号
* 本手册或任何其他手册中出现的任何口令样例

一个好的口令的长度至少为八个字符。此外，口令还应包含混合字符，如大小写字母、数字和标点符号。以下是一些好的口令示例（如果未出现在本手册中）：

* 首字母缩略词，如 "I2LMHinSF"（全称为 "I too left my heart in San Francisco"）
* 发音容易的无意义单词，如 "WumpaBun" 或 "WangDangdoodle!"
* 故意拼错的短语，如 "6o'cluck" 或 "RrriotGrrrlsRrrule!"

注意 – 注意 –

请勿使用这些示例。手册中出现的口令是入侵者将首先尝试的口令。

**更改口令**

如果 PAM 配置正确，则可以采用以下两种方法来更改 Kerberos 口令：

* 使用常见的 UNIX passwd 命令。配置 Kerberos 服务后，Solaris passwd 命令还会自动提示您输入新的 Kerberos 口令。

使用 passwd 而非 kpasswd 的优点在于可以同时设置 UNIX 口令和 Kerberos 口令。但是，在一般情况下，**无需**使用 passwd 同时更改这两个口令。通常，只能更改 UNIX 口令并保持 Kerberos 口令不变，反之亦然。

**注 –**

passwd 的行为取决于 PAM 模块的配置方式。在某些配置中，可能会要求您同时更改这两个口令。对于一些站点，必须更改 UNIX 口令，而对于其他站点，则要求更改 Kerberos 口令。

* 使用 kpasswd 命令。kpasswd 与 passwd 非常类似。这两个命令的一个区别是 kpasswd 仅更改 Kerberos 口令。如果要更改 UNIX 口令，则必须使用 passwd。

另一个区别是 kpasswd 可以更改非有效 UNIX 用户的 Kerberos 主体的口令。例如，david/admin 是 Kerberos 主体，但不是实际的 UNIX 用户，因此必须使用 kpasswd 而非 passwd。

更改口令后，所做更改在系统中传播需要一些时间（尤其是通过大型网络传播）。此延迟可能需要几分钟到一个小时或更长时间，具体取决于系统的设置方式。如果需要在更改口令后立刻获取新的 Kerberos 票证，请首先尝试新口令。如果新口令无效，请使用旧口令重试。

通过 Kerberos V5 协议，系统管理员可以设置允许每个用户使用的口令的条件。此类条件由为每个用户设置的**策略**（或缺省策略）定义。有关策略的更多信息，请参见[管理 Kerberos 策略](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdt/index.html)。

例如，假定用户 jennifer 的策略（称为 jenpol）要求口令长度至少为八个字母，并且至少由两种类型的字符混合组成。这样，kpasswd 便会拒绝尝试使用 "sloth" 作为口令。

|  |
| --- |
| % **kpasswd**  kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.  Old password: *<Jennifer types her existing password>*  kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by  the policy jenpol  which requires a minimum of 8 characters from at least 2 classes  (the five classes are lowercase, uppercase, numbers, punctuation,  and all other characters).  New password: *<Jennifer types 'sloth'>*  New password (again): *<Jennifer re-types 'sloth'>*  kpasswd: New password is too short.  Please choose a password which is at least 4 characters long. |

在以下示例中，jennifer 使用 "slothrop49" 作为口令。由于 "slothrop49" 的长度超过八个字母，并且包含两种不同类型的字符（数字和小写字母），因此此口令符合条件。

|  |
| --- |
| % **kpasswd**  kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.  Old password: *<Jennifer types her existing password>*  kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by  the policy jenpol  which requires a minimum of 8 characters from at least 2 classes  (the five classes are lowercase, uppercase, numbers, punctuation,  and all other characters).  New password: *<Jennifer types 'slothrop49'>*  New password (again): *<Jennifer re-types 'slothrop49'>*  Kerberos password changed. |

**示例－更改口令**

在以下示例中，用户 david 使用 passwd 同时更改其 UNIX 口令和 Kerberos 口令。

|  |
| --- |
| % **passwd**  passwd: Changing password for david  Enter login (NIS+) password: *<Type the current UNIX password>*  New password: *<Type the new UNIX password>*  Re-enter password: *<Confirm the new UNIX password>*  Old KRB5 password: *<Type the current Kerberos password>*  New KRB5 password: *<Type the new Kerberos password>*  Re-enter new KRB5 password: *<Confirm the new Kerberos password>* |

请注意，passwd 需要 UNIX 口令和 Kerberos 口令。此行为由缺省配置确定。在这种情况下，用户 david 必须使用 kpasswd 将其 Kerberos 口令设置为其他内容，如下所示。

本示例说明用户 david 如何使用 kpasswd 仅更改其 Kerberos 口令。

|  |
| --- |
| % **kpasswd**  kpasswd: Changing password for david@ENG.EXAMPLE.COM.  Old password: *<Type the current Kerberos password>*  New password: *<Type the new Kerberos password>*  New password (again): *<Confirm the new Kerberos password>*  Kerberos password changed. |

在本示例中，用户 david 更改了 Kerberos 主体 david/admin（非有效的 UNIX 用户）的口令。该用户必须使用 kpasswd。

|  |
| --- |
| % **kpasswd david/admin**  kpasswd: Changing password for david/admin.  Old password: *<Type the current Kerberos password>*  New password: *<Type the new Kerberos password>*  New password (again): *<Type the new Kerberos password>*  Kerberos password changed. |

**授予对帐户的访问权限**

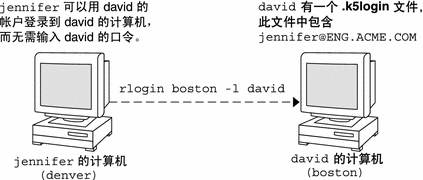
如果需要授予某个用户访问权限以登录到您的帐户（以您的身份），则可以通过 Kerberos 执行此操作而不必显示您的口令，方法是将 .k5login 文件放置在起始目录中。.k5login 文件是一个列表，其中包含一个或多个与要为其授予访问权限的各用户对应的 Kerberos 主体。每个主体都必须单独占一行。

假定用户 david 在其起始目录中按如下所示保存了一个 .k5login 文件：

|  |
| --- |
| jennifer@ENG.EXAMPLE.COM  joe@EXAMPLE.ORG |

如果用户 jennifer 和 joe 在其各自的领域中已经拥有 Kerberos 票证，则此文件允许这两个用户采用 david 的身份。例如，jennifer 可以使用 david 的身份远程登录到 david 的计算机 (boston)，而不必提供 david 的口令。

**图 25–1 使用 .k5login 文件授予对帐户的访问权限**



如果 david 的起始目录使用 Kerberos V5 协议从另一台（第三台）计算机挂载了 NFS，则 jennifer 必须具有可转发票证才能访问 david 的起始目录。有关使用可转发票证的示例，请参见[创建 Kerberos 票证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veg/index.html#user-9)。

如果您要通过网络登录到其他计算机，则需要在这些计算机上的 .k5login 文件中包括您自己的 Kerberos 主体。

使用 .k5login 文件比公布口令安全得多，原因如下：

* 您可以随时通过从 .k5login 文件中删除主体来收回访问权限。
* 虽然在您的起始目录的 .k5login 文件中指定的用户主体对您在该计算机（或一组计算机，例如如果通过 NFS 共享 .k5login 文件）上的帐户拥有完全访问权限，但是，所有基于 Kerberos 的服务都将根据该用户的身份而不是您的身份来授权访问。因此，jennifer 可以登录到 joe 的计算机并在其中执行任务。但是，如果该用户使用基于 Kerberos 的程序（如 ftp 或 rlogin），则将以其自身身份执行此操作。
* Kerberos 会记录获取票证的用户，以便系统管理员在必要时查找在特定时间可以使用您的用户身份的人员。

使用 .k5login 文件的一种常见方法是将其放置在 root 的起始目录中，从而为列出的 Kerberos 主体提供对该计算机的 root 访问权限。此配置允许系统管理员成为本地 root，或以 root 身份远程登录，而不必公布 root 口令，并且不需要任何人通过网络键入 root 口令。

**示例－使用 .k5login 文件授予对帐户的访问权限**

假定 jennifer 决定以 root 身份登录到计算机 boston.example.com。由于在 boston.example.com 的 root 起始目录的 .k5login 文件中存在该用户的主体名称项，因此不必再次键入其口令。

|  |
| --- |
| % **rlogin boston.example.com -l root -x**  This rlogin session is using DES encryption for all data transmissions.  Last login: Thu Jun 20 16:20:50 from daffodil  SunOS Release 5.7 (GENERIC) #2: Tue Nov 14 18:09:31 EST 1998  boston[root]% |

**Kerberos 用户命令**

Kerberos V5 产品是一个**单点登录**系统，这表示只需键入一次口令即可。Kerberos V5 程序将为您执行验证操作（并可以选择执行加密操作），因为 Kerberos 已内置在每个熟知的现有网络程序套件中。 Kerberos V5 应用程序是添加了 Kerberos 功能的现有 UNIX 网络程序的版本。

例如，使用基于 Kerberos 的程序连接到远程主机时，该程序、KDC 和远程主机将执行一组快速协商。完成这些协商后，该程序便已代表您向远程主机证明了您的身份，并且远程主机已授予您访问权限。

请注意，基于 Kerberos 的命令会首先尝试使用 Kerberos 进行验证。如果 Kerberos 验证失败，将会出现错误或尝试 UNIX 验证，具体取决于和命令一起使用的选项。有关更多详细信息，请参阅每个 Kerberos 命令手册页中的 Kerberos Security 部分。

**基于 Kerberos 的命令概述**

基于 Kerberos 的网络服务是一些连接到 Internet 中某个位置的其他计算机的程序。这些程序如下：

* ftp
* rcp
* rdist
* rlogin
* rsh
* ssh
* telnet

这些程序具有可透明地使用 Kerberos 票证与远程主机协商验证并选择协商加密的功能。在大多数情况下，您只会注意到不必再键入口令即可使用这些程序，因为 Kerberos 将为您提供身份证明。

Kerberos V5 网络程序包括可用于执行以下操作的选项：

* 将票证转发到其他主机（如果最初已获取可转发票证）。
* 加密在您的主机和远程主机之间传输的数据。

**注 –**

本节假定您已经熟悉这些程序的非 Kerberos 版本，并且将重点介绍 Kerberos V5 软件包添加的 Kerberos 功能。有关此处描述的命令的详细说明，请参阅其各自的手册页。

已将下列 Kerberos 选项添加至 ftp、rcp、rlogin、rsh 和 telnet：

**-a**

尝试使用现有票证自动登录。如果 **getlogin()** 返回的用户名与当前用户 ID 相同，则使用该用户名。有关详细信息，请参见 telnet(1) 手册页。

**-f**

将**不可重新转发的**票证转发到远程主机。此选项与 **-F** 选项互斥。在同一命令中不能同时使用这两个选项。

如果您有理由相信需要向第三台主机中其他基于 Kerberos 的服务验证您的身份，则应转发票证。例如，您可能要远程登录到另一台计算机，然后从该计算机远程登录到第三台计算机。

如果远程主机上的起始目录使用 Kerberos V5 机制挂载了 NFS，则必须使用可转发票证。否则，将无法访问起始目录。也就是说，假定您最初登录到系统 1，然后从系统 1 远程登录到您的主机（系统2），该主机从系统 3 挂载您的起始目录。在这种情况下，除非在 rlogin 中使用 **-f** 或 **-F** 选项，否则将无法访问起始目录，因为您的票证无法转发到系统 3。

缺省情况下，kinit 会获取可转发票证授予票证 (Ticket-Granting Ticket, TGT)。但是，您的配置在这方面可能会有所不同。

有关转发票证的更多信息，请参见[转发 Kerberos 票证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#user-68)。

**-F**

将 TGT 的**可重新转发**副本转发到远程系统。此选项与 **-f** 类似，但它允许访问更多（如第四台或第五台）计算机。因此，可将 **-F** 选项视为 **-f** 选项的超集。**-F** 选项与 **-f** 选项互斥。在同一命令中不能同时使用这两个选项。

有关转发票证的更多信息，请参见[转发 Kerberos 票证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#user-68)。

**-k** *realm*

请求指定的 *realm* 中的远程主机的票证，而不是使用 krb5.conf 文件来确定领域本身。

**-K**

使用票证来向远程主机验证，但不自动登录。

**-m** *mechanism*

指定 /etc/gss/mech 文件中列出的要使用的 GSS-API 安全机制。缺省值为 kerberos\_v5。

**-x**

加密此会话。

**-X** *auth\_type*

禁用 *auth-type* 类型的验证。

下表显示具有特定选项的命令。"X" 表示命令包含该选项。

表 25–1 网络命令的 Kerberos 选项

|  | **ftp** | **rcp** | **rlogin** | **rsh** | **telnet** |
| --- | --- | --- | --- | --- | --- |
| **-a** |  |  |  |  | X |
| **-f** | X |  | X | X | X |
| **-F** |  |  | X | X | X |
| **-k** |  | X | X | X | X |
| **-K** |  |  |  |  | X |
| **-m** | X |  |  |  |  |
| **-x** | X | X | X | X | X |
| **-X** |  |  |  |  | X |

此外，ftp 还允许在其提示符下为会话设置保护级别：

clear

将保护级别设置为 "clear"（无保护）。此保护级别是缺省级别。

private

将保护级别设置为 "private"。通过加密保护数据传输的保密性和完整性。但是，并非所有 Kerberos 用户都可使用保密性服务。

safe

将保护级别设置为 "safe"。通过加密校验和保护数据传输的完整性。

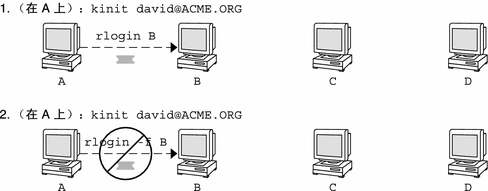
也可以通过键入 protect，并后跟以上所示的任何保护级别（clear、private 或 safe），在 ftp 提示符下设置保护级别。

**转发 Kerberos 票证**

如[基于 Kerberos 的命令概述](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#userkerbopts1)中所述，某些命令允许您使用 **-f** 或 **-F** 选项转发票证。通过转发票证，可以“链接”网络事务。例如，可以远程登录到一台计算机，然后从该计算机远程登录到另一台计算机。使用 **-f** 选项可转发票证，而使用 **-F** 选项则可重新转发已转发的票证。

在[图 25–2](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#user-fig-70) 中，用户 david 使用 kinit 获取了一个不可转发票证授予票证 (Ticket-Granting Ticket, TGT)。由于该用户未指定 **-f** 选项，因此该票证不可转发。在方案 1 中，该用户可以远程登录到计算机 B，但不能再登录到其他计算机。在方案 2 中，由于该用户尝试转发一个不可转发票证，因此 rlogin **-f** 命令失败。

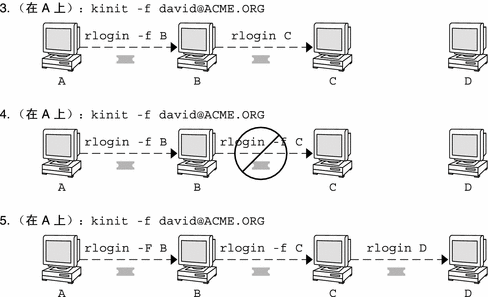
**图 25–2 使用不可转发票证**



实际上，已设置了 Kerberos 配置文件，以便 kinit 在缺省情况下可获取可转发票证。但是，您的配置可能有所不同。为了便于说明，假定 kinit **不会**获取可转发 TGT，除非使用 kinit **-f** 调用该命令。另请注意，kinit 不包含 **-F** 选项。TGT 可以是可转发，也可以是不可转发。

在[图 25–3](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html#user-fig-69) 中，用户 david 使用 kinit **-f** 获取了可转发 TGT。在方案 3 中，由于该用户在 rlogin 中使用了可转发票证，因此可以访问计算机 C。在方案 4 中，由于票证不可重新转发，因此第二个 rlogin 失败。如方案 5 中所示，改用 **-F** 选项后，第二个 rlogin 将成功，并且票证可重新转发到计算机 D。

**图 25–3 使用可转发票证**



**示例－使用基于 Kerberos 的命令**

以下示例说明基于 Kerberos 的命令的选项的工作方式。

**示例－将 -a、-f 和 -x 选项用于 telnet**

在本示例中，用户 david 已经登录，并且要 telnet 到计算机 denver.example.com。该用户使用 **-f** 选项转发其现有票证，使用 **-x** 选项加密会话，并使用 **-a** 选项自动执行登录。由于该用户不打算使用第三台主机的服务，因此可使用 **-f** 而非 **-F**。

|  |
| --- |
| % **telnet -a -f -x denver.example.com**  Trying 128.0.0.5...  Connected to denver.example.com. Escape character is '^]'.  [ Kerberos V5 accepts you as "david@eng.example.com" ]  [ Kerberos V5 accepted forwarded credentials ]  SunOS 5.9: Tue May 21 00:31:42 EDT 2004 Welcome to SunOS  % |

请注意，david 的计算机使用 Kerberos 来向 denver.example.com 进行自我验证，并且以自己的身份自动登录。该用户具有一个加密会话（即该用户已有的票证副本），因此永远不必键入其口令。如果该用户使用了非 Kerberos 版本的 telnet，则可能会提示其输入口令，并将此口令在未加密的情况下通过网络发送。如果入侵者在此期间一直在观察网络通信流量，则可能会知道 david 的口令。

如果转发 Kerberos 票证，则 telnet（以及此处讨论的其他命令）将会在退出时销毁这些票证。

**示例－使用带有 -F 选项的 rlogin**

在此示例中，用户 jennifer 希望登录到自己的计算机 boston.example.com。该用户使用 **-F** 选项转发其现有票证，并使用 **-x** 选项加密会话。由于该用户在登录到 boston 后，可能希望执行需要重新转发票证的其他网络事务，因此会选择 **-F** 而非 **-f**。另外，由于该用户要转发其现有票证，因此不必键入其口令。

|  |
| --- |
| % **rlogin boston.example.com -F -x**  This rlogin session is using encryption for all transmissions.  Last login Mon May 19 15:19:49 from daffodil  SunOS Release 5.9 (GENERIC) #2 Tue Nov 14 18:09:3 EST 2003  % |

**示例－在 ftp 中设置保护级别**

假定 joe 要使用 ftp 从计算机 denver.example.com 的目录 ~joe/MAIL 中获取其邮件并加密该会话。交换过程如下所示：

|  |
| --- |
| % **ftp -f denver.example.com**  Connected to denver.example.com  220 denver.example.org FTP server (Version 6.0) ready.  334 Using authentication type GSSAPI; ADAT must follow  GSSAPI accepted as authentication type  GSSAPI authentication succeeded Name (daffodil.example.org:joe)  232 GSSAPI user joe@MELPOMENE.EXAMPLE.COM is authorized as joe  230 User joe logged in.  Remote system type is UNIX.  Using BINARY mode to transfer files.  ftp> **protect private**  200 Protection level set to Private  ftp> **cd ~joe/MAIL**  250 CWD command successful.  ftp> **get RMAIL**  227 Entering Passive Mode (128,0,0,5,16,49)  150 Opening BINARY mode data connection for RMAIL (158336 bytes).  226 Transfer complete. 158336 bytes received in 1.9 seconds (1.4e+02 Kbytes/s)  ftp> **quit**  % |

要加密该会话，joe 需要将保护级别设置为 private。

* [*Previous*: 第 24 章 管理 Kerberos 主体和策略（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/aadmin-1/index.html)
* [*Next*: 第 26 章 Kerberos 服务（参考）](https://docs.oracle.com/cd/E19253-01/819-7061/refer-1/index.html)
* © 2010, Oracle Corporation and/or its affiliates