[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 22 章 配置 Kerberos 服务（任务）

系统管理指南：安全性服务

* [*Previous*: 第 21 章 规划 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/seamplan-1/index.html)
* [*Next*: 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)

**第 22 章 配置 Kerberos 服务（任务）**

本章介绍 KDC 服务器、网络应用程序服务器、NFS 服务器和 Kerberos 客户机的配置过程。其中许多过程都要求超级用户访问权限，因此这些过程应由系统管理员或高级用户来执行。本章还将介绍跨领域配置过程以及与 KDC 服务器相关的其他主题。

本章包含以下主题：

* [配置 Kerberos 服务（任务列表）](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbd/index.html)
* [配置 KDC 服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbf/index.html)
* [配置跨领域验证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbj/index.html)
* [配置 Kerberos 网络应用程序服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbn/index.html)
* [配置 Kerberos NFS 服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbq/index.html)
* [配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc1/index.html)
* [同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)
* [交换主 KDC 和从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcc/index.html)
* [管理 Kerberos 数据库](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcg/index.html)
* [增强 Kerberos 服务器的安全性](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcv/index.html)

**配置 Kerberos 服务（任务列表）**

部分配置过程依赖于其他配置过程，且必须按特定顺序执行。这些过程通常会建立使用 Kerberos 服务所需的服务。其他过程不依赖于任何顺序，且可以在适当的情况下执行。以下任务列表给出了 Kerberos 安装的建议顺序。

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 1. 规划 Kerberos 安装。 | 在开始软件配置过程之前先解决配置问题。从长远来看，提前规划可以节省时间和其他资源。 | [第 21 章，规划 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vas/index.html) |
| 2. （可选）安装 NTP。 | 配置网络时间协议 (Network Time Protocol, NTP) 软件或其他时钟同步协议。要使 Kerberos 服务正常工作，必须同步领域中所有系统的时钟。 | [同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html) |
| 3. 配置主 KDC 服务器。 | 配置并构建领域的主 KDC 服务器和数据库。 | [如何配置主 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbh/index.html) |
| 4. 配置从 KDC 服务器。 | 配置并构建领域的从 KDC 服务器。 | [如何配置从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbi/index.html) |
| 5. （可选）增强 KDC 服务器的安全性。 | 阻止对 KDC 服务器的安全性破坏。 | [如何限制对 KDC 服务器的访问](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd2/index.html) |
| 6. （可选）配置可交换的 KDC 服务器。 | 使交换主 KDC 和从 KDC 的任务更容易执行。 | [如何配置可交换的从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vce/index.html) |

**配置其他 Kerberos 服务（任务列表）**

完成所需步骤之后，可以在适当的情况下执行以下过程。

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 配置跨领域验证。 | 启用领域之间的通信。 | [配置跨领域验证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbj/index.html) |
| 配置 Kerberos 应用程序服务器。 | 使服务器支持使用 Kerberos 验证的服务，例如 ftp、telnet 和 rsh。 | [配置 Kerberos 网络应用程序服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbn/index.html) |
| 配置 Kerberos 客户机。 | 使客户机使用 Kerberos 服务。 | [配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc1/index.html) |
| 配置 Kerberos NFS 服务器。 | 使服务器共享要求 Kerberos 验证的文件系统。 | [配置 Kerberos NFS 服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbq/index.html) |
| 增强应用程序服务器的安全性。 | 通过只允许访问经过验证的事务来增强应用程序服务器的安全性。 | [如何仅启用基于 Kerberos 的应用程序](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd1/index.html) |

**配置 KDC 服务器**

安装 Kerberos 软件后，必须配置 KDC 服务器。配置一个主 KDC 和至少一个从 KDC 以提供颁发凭证的服务。这些凭证是 Kerberos 服务的基础，因此在尝试其他任务之前必须安装 KDC。

主 KDC 和从 KDC 之间的最大差别是，只有主 KDC 可以处理数据库管理请求。例如，更改口令或添加新的主体必须在主 KDC 上完成。然后可以将这些更改传播到从 KDC。从 KDC 和主 KDC 都可生成凭证。此功能可在主 KDC 无法响应时提供冗余性。

**Procedure如何配置主 KDC**

在此过程中，将配置增量传播。此外，还将使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* DNS 域名 = example.com
* 主 KDC = kdc1.example.com
* admin 主体 = kws/admin
* 联机帮助 URL = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956

**注 –**

调整该 URL 以指向“SEAM Administration Tool”部分，如[SEAM Administration Tool 中的联机帮助 URL](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vba/index.html)中所述。

**开始之前**

此过程要求 DNS 必须正在运行。有关此主 KDC 是否可交换的特定命名说明，请参见[交换主 KDC 和从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcc/index.html)。

1. 成为主 KDC 的超级用户。
2. 编辑 Kerberos 配置文件 (krb5.conf)。

需要更改领域名称和服务器名称。有关此文件的完整说明，请参见 [krb5.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufn/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/krb5.conf**  [libdefaults]  default\_realm = **EXAMPLE.COM**  [realms]  **EXAMPLE.COM** = {  kdc = **kdc1.example.com**  admin\_server = **kdc1.example.com**    }  [domain\_realm]  **.example.com = EXAMPLE.COM**  #  # if the domain name and realm name are equivalent,  # this entry is not needed  #  [logging]  default = FILE:/var/krb5/kdc.log  kdc = FILE:/var/krb5/kdc.log  [appdefaults]  gkadmin = {  help\_url = **http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956**  } |

在此示例中，更改了 default\_realm、kdc 和 admin\_server 行以及所有 domain\_realm 项。此外，还编辑了定义 help\_url 的行。

**注 –**

如果要限制加密类型，可以设置 default\_tkt\_enctypes 或 default\_tgs\_enctypes 行。有关限制加密类型涉及的问题的说明，请参阅[使用 Kerberos 加密类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ver/index.html)。

1. 编辑 KDC 配置文件 (kdc.conf )。

需要更改领域名称。有关此文件的完整说明，请参见 [kdc.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufl/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kdc.conf**  [kdcdefaults]  kdc\_ports = 88,750  [realms]  **EXAMPLE.COM**= {  profile = /etc/krb5/krb5.conf  database\_name = /var/krb5/principal  admin\_keytab = /etc/krb5/kadm5.keytab  acl\_file = /etc/krb5/kadm5.acl  kadmind\_port = 749  max\_life = 8h 0m 0s  max\_renewable\_life = 7d 0h 0m 0s  **sunw\_dbprop\_enable = true**  **sunw\_dbprop\_master\_ulogsize = 1000** } |

在此示例中，更改了 realms 部分中的领域名称定义。此外，在 realms 部分中，添加了用于启用增量传播和选择主 KDC 将保留在日志中的更新数的行。

**注 –**

如果需要限制加密类型，可以设置 permitted\_enctypes、supported\_enctypes 或 master\_key\_type 行。有关限制加密类型涉及的问题的说明，请参阅[使用 Kerberos 加密类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ver/index.html)。

1. 使用 kdb5\_util 命令创建 KDC 数据库。

kdb5\_util 命令创建 KDC 数据库。此外，与 **-s** 选项一起使用时，此命令会在启动 kadmind 和 krb5kdc 守护进程之前，创建一个用于向自己验证 KDC 的存储文件。

|  |
| --- |
| kdc1 # **/usr/sbin/kdb5\_util create -r EXAMPLE.COM -s**  Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM'  master key name 'K/M@EXAMPLE.COM'  You will be prompted for the database Master Password.  It is important that you NOT FORGET this password.  Enter KDC database master key: *<Type the key>*  Re-enter KDC database master key to verify: *<Type it again>* |

如果领域名称与服务器的名称空间中的域名相同，则无需后跟领域名称的 **-r** 选项。

1. 编辑 Kerberos 访问控制列表文件 (kadm5.acl)。

填充后，/etc/krb5/kadm5.acl 文件应包含允许管理 KDC 的所有主体名称。

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

通过该项，EXAMPLE.COM 领域中的 kws/admin 主体可以修改 KDC 中的主体或策略。缺省安装包括用于匹配所有 admin 主体的星号 (\*)。此缺省安装可能会存在安全风险，因此更安全的方法是包括所有 admin 主体的列表。有关更多信息，请参见 [kadm5.acl(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufk/index.html) 手册页。

1. 启动 kadmin.local 命令并添加主体。

接下来的子步骤创建 Kerberos 服务使用的主体。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin.local**  kadmin.local: |

* 1. 向数据库中添加管理主体。

可以根据需要添加任意数量的 admin 主体。要完成 KDC 配置过程，必须至少添加一个 admin 主体。对于此示例，将添加一个 kws/admin 主体。可以将 "kws" 替换为相应的主体名称。

|  |
| --- |
| kadmin.local: **addprinc kws/admin**  Enter password for principal kws/admin@EXAMPLE.COM:*<Type the password>*  Re-enter password for principal kws/admin@EXAMPLE.COM: *<Type it again>*  Principal "kws/admin@EXAMPLE.COM" created.  kadmin.local: |

* 1. 创建 kiprop 主体。

kiprop 主体用于授权来自主 KDC 的更新。

|  |
| --- |
| kadmin.local: **addprinc -randkey kiprop/kdc1.example.com**  Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.  kadmin.local: |

* 1. 为 kadmind 服务创建密钥表文件。

此命令序列创建包含 kadmin 和 changepw 的主体项的特殊密钥表文件。kadmind 服务需要使用这些主体。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin.local: **ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com**  Entry for principal kadmin/kdc1.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/kdc1.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/kdc1.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin.local: **ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com**  EEntry for principal changepw/kdc1.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 changepw/kdc1.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 changepw/kdc1.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin.local: **ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw**  Entry for principal kadmin/changepw 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 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 with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin.local: |

* 1. 将主 KDC 服务器的 kiprop 主体添加到 kadmind 密钥表文件中。

通过将 kiprop 主体添加到 kadm5.keytab 文件中，kadmind 命令可以在启动增量传播时对其自身进行验证。

|  |
| --- |
| kadmin.local: **ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com**  Entry for principal kiprop/kdc1.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 kiprop/kdc1.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 kiprop/kdc1.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin.local: |

* 1. 退出 kadmin.local。

已经添加了接下来的步骤所需的所有主体。

|  |
| --- |
| kadmin.local: **quit** |

1. 启动 Kerberos 守护进程。

|  |
| --- |
| kdc1 # **svcadm enable -r network/security/krb5kdc**  kdc1 # **svcadm enable -r network/security/kadmin** |

1. 启动 kadmin 并添加更多主体。

此时，可以使用 SEAM Administration Tool 添加主体。为此，必须使用此过程前面创建的一个 admin 主体名称登录。但是，为简单起见，给出了以下命令行示例。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 创建主 KDC host 主体。

基于 Kerberos 的应用程序（例如 klist 和 kprop）将使用主机主体。Solaris 10 客户机在挂载经过验证的 NFS 文件系统时将使用此主体。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **addprinc -randkey host/kdc1.example.com**  Principal "host/kdc1.example.com@EXAMPLE.COM" created.  kadmin: |

* 1. （可选的）创建 kclient 主体。

安装 Kerberos 客户机过程中 kclient 实用程序将使用此主体。如果不打算使用此实用程序，则无需添加该主体。kclient 实用程序的用户需要使用此口令。

|  |
| --- |
| kadmin: **addprinc clntconfig/admin**  Enter password for principal clntconfig/admin@EXAMPLE.COM:*<Type the password>*  Re-enter password for principal clntconfig/admin@EXAMPLE.COM: *<Type it again>*  Principal "clntconfig/admin@EXAMPLE.COM" created.  kadmin: |

* 1. 将主 KDC 的 host 主体添加到主 KDC 的密钥表文件中。

通过将主机主体添加到密钥表文件中，可以自动使用此主体。

|  |
| --- |
| kadmin: **ktadd host/kdc1.example.com**  Entry for principal host/kdc1.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/kdc1.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/kdc1.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

1. （可选的）使用 NTP 或其他时钟同步机制同步主 KDC 时钟。

安装和使用网络时间协议 (Network Time Protocol, NTP) 并非必需。但是，要成功验证，每个时钟都必须处于 krb5.conf 文件的 libdefaults 部分中定义的缺省时间内。有关 NTP 的信息，请参见[同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)。

1. 配置从 KDC。

要提供冗余性，请确保至少安装一个从 KDC。有关特定说明，请参见[如何配置从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbi/index.html)。

**Procedure如何配置从 KDC**

在此过程中，将配置一个名为 kdc2 的新从 KDC。此外，还将配置增量传播。此过程使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* DNS 域名 = example.com
* 主 KDC = kdc1.example.com
* 从 KDC = kdc2.example.com
* admin 主体 = kws/admin
* 联机帮助 URL = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956

**注 –**

调整该 URL 以指向“SEAM Administration Tool”部分，如[SEAM Administration Tool 中的联机帮助 URL](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vba/index.html)中所述。

**开始之前**

必须配置主 KDC。有关此从 KDC 是否可交换的特定说明，请参见[交换主 KDC 和从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcc/index.html)。

1. 在主 KDC 上，成为超级用户。
2. 在主 KDC 上，启动 kadmin。

必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 在主 KDC 上，将从主机主体添加到数据库中（如果尚未执行此操作）。

要使从 KDC 正常工作，该从 KDC 必须具有主机主体。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **addprinc -randkey host/kdc2.example.com**  Principal "host/kdc2@EXAMPLE.COM" created.  kadmin: |

* 1. 在主 KDC 上，创建 kiprop 主体。

kiprop 主体用于授权来自主 KDC 的增量传播。

|  |
| --- |
| kadmin: **addprinc -randkey kiprop/kdc2.example.com**  Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.  kadmin: |

* 1. 退出 kadmin。

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

1. 在主 KDC 上，编辑 Kerberos 配置文件 (krb5.conf)。

需要添加每个从 KDC 的项。有关此文件的完整说明，请参见 [krb5.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufn/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/krb5.conf**  .  .  [realms]  EXAMPLE.COM = {  kdc = kdc1.example.com  **kdc = kdc2.example.com**  admin\_server = kdc1.example.com  } |

1. 在主 KDC 上，将 kiprop 项添加到 kadm5.acl 中。

通过此项，主 KDC 可以接收对 kdc2 服务器的增量传播请求。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kadm5.acl**  \*/admin@EXAMPLE.COM \*  **kiprop/kdc2.example.com@EXAMPLE.COM p** |

1. 在主 KDC 上，重新启动 kadmind 以使用 kadm5.acl 文件中的新项。

|  |
| --- |
| kdc1 # **svcadm restart network/security/kadmin** |

1. 在所有从 KDC 上，复制主 KDC 服务器的 KDC 管理文件。

由于主 KDC 服务器已更新每台 KDC 服务器所需的信息，因此需要在所有从 KDC 上执行此步骤。可以使用 ftp 或类似的传送机制从主 KDC 获取以下文件的副本：

* 1. /etc/krb5/krb5.conf
  2. /etc/krb5/kdc.conf

1. 在所有从 KDC 上，将主 KDC 和每个从 KDC 的项添加到数据库传播配置文件 kpropd.acl 中。

需要更新所有从 KDC 服务器上的此信息。

|  |
| --- |
| kdc2 # **cat /etc/krb5/kpropd.acl**  host/kdc1.example.com@EXAMPLE.COM  host/kdc2.example.com@EXAMPLE.COM |

1. 在所有从 KDC 上，请确保未填充 Kerberos 访问控制列表文件 kadm5.acl。

未修改的 kadm5.acl 文件如下所示：

|  |
| --- |
| kdc2 # **cat /etc/krb5/kadm5.acl**  \*/admin@\_\_\_default\_realm\_\_\_ \* |

如果此文件中包含 kiprop 项，请删除它们。

1. 在新的从 KDC 上，更改 kdc.conf 中的项。

将 sunw\_dbprop\_master\_ulogsize 项替换为定义 sunw\_dbprop\_slave\_poll 的项。该项将轮询时间设置为 2 分钟。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kdc.conf**  [kdcdefaults]  kdc\_ports = 88,750  [realms]  EXAMPLE.COM= {  profile = /etc/krb5/krb5.conf  database\_name = /var/krb5/principal  admin\_keytab = /etc/krb5/kadm5.keytab  acl\_file = /etc/krb5/kadm5.acl  kadmind\_port = 749  max\_life = 8h 0m 0s  max\_renewable\_life = 7d 0h 0m 0s  sunw\_dbprop\_enable = true  **sunw\_dbprop\_slave\_poll = 2m**  } |

1. 在新的从 KDC 上，启动 kadmin 命令。

必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| kdc2 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 使用 kadmin 将从 KDC 的主机主体添加到从 KDC 的密钥表文件中。

此项可使 kprop 和其他基于 Kerberos 的应用程序正常工作。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **ktadd host/kdc2.example.com**  Entry for principal host/kdc2.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/kdc2.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/kdc2.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/kdc2.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 将 kiprop 主体添加到从 KDC 的密钥表文件中。

通过将 kiprop 主体添加到 krb5.keytab 文件中，kpropd 命令可以在启动增量传播时对其自身进行验证。

|  |
| --- |
| kadmin: **ktadd kiprop/kdc2.example.com**  Entry for principal kiprop/kdc2.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 kiprop/kdc2.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 kiprop/kdc2.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

1. 在新的从 KDC 上，启动 Kerberos 传播守护进程。

|  |
| --- |
| kdc2 # **/usr/lib/krb5/kpropd** |

1. 在新的从 KDC 上，使用 kdb5\_util 创建一个存储文件。

|  |
| --- |
| kdc2 # **/usr/sbin/kdb5\_util stash**  kdb5\_util: Cannot find/read stored master key while reading master key  kdb5\_util: Warning: proceeding without master key  Enter KDC database master key: *<Type the key>* |

1. 中止 Kerberos 传播守护进程。

|  |
| --- |
| kdc2 # **pkill kpropd** |

1. （可选的）在新的从 KDC 上，使用 NTP 或其他时钟同步机制同步主 KDC 时钟。

安装和使用网络时间协议 (Network Time Protocol, NTP) 并非必需。但是，要成功验证，每个时钟必须处于 krb5.conf 文件的 libdefaults 部分中定义的缺省时间内。有关 NTP 的信息，请参见[同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)。

1. 在新的从 KDC 上，启动 KDC 守护进程 (krb5kdc)。

启用 krb5kdc 服务时，如果系统配置为从 KDC，则还将启动 kpropd。

|  |
| --- |
| kdc2 # **svcadm enable network/security/krb5kdc** |

**配置跨领域验证**

有几种方法可以将各个领域链接在一起，从而可以在一个领域中验证另一个领域中的用户。通常，跨领域验证通过在两个领域之间建立共享私钥来实现。领域之间的关系可以是分层关系或直接关系（请参见[领域分层结构](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vav/index.html#planning-29)）。

**Procedure如何建立分层跨领域验证**

此过程中的示例使用 ENG.EAST.EXAMPLE.COM 和 EAST.EXAMPLE.COM 两个领域。将按两个方向建立跨领域验证。必须在两个领域的主 KDC 上完成此过程。

**开始之前**

必须配置每个领域的主 KDC。要完全测试验证过程，必须安装多个客户机或从 KDC。

1. 成为第一个主 KDC 的超级用户。
2. 为两个领域创建票证授予票证服务主体。

必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: **addprinc krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM**  Enter password for principal krgtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM: *<Type password>*  kadmin: **addprinc krbtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM**  Enter password for principal krgtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: *<Type password>*  kadmin: **quit** |

**注 –**

在两个 KDC 中为每个服务主体指定的口令必须相同。因此，服务主体 krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM 的口令在两个领域中一定相同。

1. 将相应项添加到 Kerberos 配置文件 (krb5.conf) 中以定义每个领域的域名。

|  |
| --- |
| # **cat /etc/krb5/krb5.conf**  [libdefaults]  .  .  [domain\_realm]  **.eng.east.example.com = ENG.EAST.EXAMPLE.COM**  **.east.example.com = EAST.EXAMPLE.COM** |

1. 在此示例中，定义了 ENG.EAST.EXAMPLE.COM 和 EAST.EXAMPLE.COM 领域的域名。由于会从上向下搜索文件，因此先包含子域非常重要。
2. 将 Kerberos 配置文件复制到此领域中的所有客户机。

要使跨领域验证正常工作，所有系统（包括从 KDC 和其他服务器）必须安装 Kerberos 配置文件 (/etc/krb5/krb5.conf) 的新版本。

1. 在第二个领域中重复以上所有步骤。

**Procedure如何建立直接跨领域验证**

此过程中的示例使用 ENG.EAST.EXAMPLE.COM 和 SALES.WEST.EXAMPLE.COM 两个领域。将按两个方向建立跨领域验证。必须在两个领域的主 KDC 上完成此过程。

**开始之前**

必须配置每个领域的主 KDC。要完全测试验证过程，必须安装多个客户机或从 KDC。

1. 成为一台主 KDC 服务器的超级用户。
2. 为两个领域创建票证授予票证服务主体。

必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: **addprinc krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM**  Enter password for principal  krgtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM: *<Type the password>*  kadmin: **addprinc krbtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM**  Enter password for principal  krgtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: *<Type the password>*  kadmin: **quit** |

**注 –**

在两个 KDC 中为每个服务主体指定的口令必须相同。因此，服务主体 krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM 的口令在两个领域中一定相同。

1. 在 Kerberos 配置文件中添加相应的项以定义指向远程领域的直接路径。

此示例显示了 ENG.EAST.EXAMPLE.COM 领域中的客户机。可能需要交换领域名称以获取 SALES.WEST.EXAMPLE.COM 领域中相应的定义。

|  |
| --- |
| # **cat /etc/krb5/krb5.conf**  [libdefaults]  .  .  **[capaths]**  **ENG.EAST.EXAMPLE.COM = {**  **SALES.WEST.EXAMPLE.COM = .**  **}**  **SALES.WEST.EXAMPLE.COM = {**  **ENG.EAST.EXAMPLE.COM = .**  **}** |

1. 将 Kerberos 配置文件复制到当前领域中的所有客户机。

要使跨领域验证正常工作，所有系统（包括从 KDC 和其他服务器）必须安装 Kerberos 配置文件 (/etc/krb5/krb5.conf) 的新版本。

1. 对第二个领域重复以上所有步骤。

**配置 Kerberos 网络应用程序服务器**

网络应用程序服务器是使用以下一个或多个网络应用程序提供访问的主机：ftp、rcp、rlogin、rsh 和 telnet。要在服务器上启用这些命令的 Kerberos 版本，只需执行几个步骤。

**Procedure如何配置 Kerberos 网络应用程序服务器**

此过程使用以下配置参数：

* 应用程序服务器 = boston
* admin 主体 = kws/admin
* DNS 域名 = example.com
* 领域名称 = EXAMPLE.COM

**开始之前**

此过程要求已配置主 KDC。要完全测试该过程，必须安装多个客户机。

1. 安装 Kerberos 客户机软件。
2. （可选的）安装 NTP 客户机或其他时钟同步机制。

有关 NTP 的信息，请参见[同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)。

1. 为新服务器添加主体并更新该服务器的密钥表。

以下命令报告是否存在主机主体：

|  |
| --- |
| boston # **klist -k |grep host**  4 host/boston.example.com@EXAMPLE.COM  4 host/boston.example.com@EXAMPLE.COM  4 host/boston.example.com@EXAMPLE.COM  4 host/boston.example.com@EXAMPLE.COM |

如果此命令未返回主体，则可以使用以下步骤创建新主体。

有关如何使用 SEAM Administration Tool 添加主体的说明将在[如何创建新的 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdn/index.html)中介绍。以下步骤中的示例说明如何使用命令行添加所需的主体。必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| boston # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 创建服务器的 host 主体。

|  |
| --- |
| kadmin: **addprinc -randkey host/boston.example.com**  Principal "host/boston.example.com" created.  kadmin: |

* 1. 将服务器的 host 主体添加到服务器的密钥表中。

如果未运行 kadmin 命令，请使用以下类似命令重新启动该命令： /usr/sbin/kadmin -p *kws*/admin

|  |
| --- |
| kadmin: **ktadd host/boston.example.com**  Entry for principal host/boston.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/boston.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/boston.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/boston.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

**配置 Kerberos NFS 服务器**

NFS 服务可以使用 UNIX 用户 ID (user ID, UID) 标识用户，但不能直接使用 GSS 凭证。要将凭证转换为 UID，可能需要创建将用户凭证映射到 UNIX UID 的凭证表。有关缺省凭证映射的更多信息，请参见[将 GSS 凭证映射到 UNIX 凭证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb4/index.html)。本节中的过程重点介绍配置 Kerberos NFS 服务器、管理凭证表以及对已挂载 NFS 的文件系统启动 Kerberos 安全模式所需的任务。以下任务列表说明了本节中所包含的任务。

表 22–1 配置 Kerberos NFS 服务器（任务列表）

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 配置 Kerberos NFS 服务器。 | 使服务器共享要求 Kerberos 验证的文件系统。 | [如何配置 Kerberos NFS 服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbs/index.html) |
| 创建凭证表。 | 在缺省映射不满足要求的情况下，生成可用于提供从 GSS 凭证到 UNIX 用户 ID 的映射的凭证表。 | [如何创建凭证表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbt/index.html) |
| 更改将用户凭证映射到 UNIX UID 的凭证表。 | 更新凭证表中的信息。 | [如何向凭证表中添加单个项](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbu/index.html) |
| 在两个类似领域之间创建凭证映射。 | 在多个领域共享同一个口令文件的情况下，提供有关如何将 UID 从一个领域映射到另一个领域的说明。 | [如何提供各领域之间的凭证映射](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbv/index.html) |
| 使用 Kerberos 验证共享文件系统。 | 使用安全模式共享文件系统，以便要求 Kerberos 验证。 | [如何使用多种 Kerberos 安全模式设置安全的 NFS 环境](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc0/index.html) |

**Procedure如何配置 Kerberos NFS 服务器**

在此过程中，将使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* DNS 域名 = example.com
* NFS 服务器 = denver.example.com
* admin 主体 = kws/admin

1. 完成配置 Kerberos NFS 服务器的先决条件。

必须配置主 KDC。要完全测试此过程，需要多个客户机。

1. （可选的）安装 NTP 客户机或其他时钟同步机制。

安装和使用网络时间协议 (Network Time Protocol, NTP) 并非必需。但是，要成功验证，每个时钟必须处于 krb5.conf 文件的 libdefaults 部分中定义的缺省时间内。有关 NTP 的信息，请参见[同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)。

1. 启动 kadmin。

可以使用 SEAM Administration Tool 添加主体，如[如何创建新的 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdn/index.html)中所述。为此，必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。不过，以下示例说明如何使用命令行添加所需的主体。

|  |
| --- |
| denver # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 创建服务器的 NFS 服务主体。

请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

对系统上可能用于访问 NFS 数据的每个唯一接口重复此步骤。如果主机有多个接口具有唯一名称，则每个唯一名称必须具有自己的 NFS 服务主体。

|  |
| --- |
| kadmin: **addprinc -randkey nfs/denver.example.com**  Principal "nfs/denver.example.com" created.  kadmin: |

* 1. 将服务器的 NFS 服务主体添加到服务器的密钥表文件中。

对[步骤 a](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbs/index.html#seamtask-step-388) 中创建的每个唯一服务主体重复此步骤。

|  |
| --- |
| kadmin: **ktadd nfs/denver.example.com**  Entry for principal nfs/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 nfs/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 nfs denver.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

1. （可选的）如果需要，可创建特殊 GSS 凭证映射。

通常，Kerberos 服务在 GSS 凭证和 UNIX UID 之间生成相应的映射。缺省映射在[将 GSS 凭证映射到 UNIX 凭证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb4/index.html)中介绍。如果缺省映射不满足要求，请参见[如何创建凭证表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbt/index.html)以获取更多信息。

1. 使用 Kerberos 安全模式共享 NFS 文件系统。

有关更多信息，请参见[如何使用多种 Kerberos 安全模式设置安全的 NFS 环境](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc0/index.html)。

**Procedure如何创建凭证表**

NFS 服务器使用 gsscred 凭证表将 Kerberos 凭证映射到 UID。对于从使用 Kerberos 验证的 NFS 服务器挂载文件系统的 NFS 客户机，如果缺省映射不满足要求，则必须创建此表。

1. 编辑 /etc/gss/gsscred.conf 并更改安全机制。

将机制更改为 files。

1. 使用 gsscred 命令创建凭证表。

|  |
| --- |
| # **gsscred -m kerberos\_v5 -a** |

1. gsscred 命令从 /etc/nsswitch.conf 文件的 passwd 项列出的所有源中收集信息。如果希望凭证表中不包括本地口令项，则可能需要临时删除 files 项。有关更多信息，请参见 [gsscred(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq2g/index.html) 手册页。

**Procedure如何向凭证表中添加单个项**

**开始之前**

此过程要求已在 NFS 服务器上创建 gsscred 表。有关说明，请参见[如何创建凭证表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbt/index.html)。

1. 成为 NFS 服务器上的超级用户。
2. 使用 gsscred 命令向凭证表中添加项。

|  |
| --- |
| # **gsscred -m *mech* [ -n *name* [ -u *uid* ]] -a** |

1. *mech*
2. 定义要使用的安全机制。
3. *name*
4. 定义用户的主体名称，如 KDC 中所定义。
5. *uid*
6. 定义用户的 UID，如口令数据库中所定义。
7. **-a**
8. 向主体名称映射中添加 UID。

**示例 22–1 向凭证表中添加多组成部分主体**

在以下示例中，将添加名为 sandy/admin 的主体的项，该主体映射到 UID 3736。

|  |
| --- |
| # **gsscred -m kerberos\_v5 -n sandy/admin -u 3736 -a** |

**示例 22–2 向凭证表中添加其他域中的主体**

在以下示例中，将添加名为 sandy/admin@EXAMPLE.COM 的主体的项，该主体映射到 UID 3736。

|  |
| --- |
| # **gsscred -m kerberos\_v5 -n sandy/admin@EXAMPLE.COM -u 3736 -a** |

**Procedure如何提供各领域之间的凭证映射**

此过程在使用相同口令文件的领域之间提供相应的凭证映射。在此示例中，领域 CORP.EXAMPLE.COM 和 SALES.EXAMPLE.COM 使用相同的口令文件。bob@CORP.EXAMPLE.COM 和 bob@SALES.EXAMPLE.COM 的凭证映射到相同的 UID。

1. 成为超级用户。
2. 在客户机系统上，向 krb5.conf 文件中添加项。

|  |
| --- |
| # **cat /etc/krb5/krb5.conf**  [libdefaults]  **default\_realm = CORP.EXAMPLE.COM**  .  **[realms]**  **CORP.EXAMPLE.COM = {**  .  **auth\_to\_local\_realm = SALES.EXAMPLE.COM**  .  } |

**故障排除**

有关对凭证映射问题进行疑难解答的过程的帮助，请参见[观察从 GSS 凭证到 UNIX 凭证的映射](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd6/index.html#fabaf)。

**Procedure如何使用多种 Kerberos 安全模式设置安全的 NFS 环境**

通过此过程，NFS 服务器可以使用不同的安全模式或特性提供安全的 NFS 访问。客户机与 NFS 服务器协商安全特性时，将使用该客户机有权访问的服务器所提供的第一种特性。此特性用于 NFS 服务器共享的文件系统的所有后续客户机请求。

1. 成为 NFS 服务器上的超级用户。
2. 验证在密钥表文件中是否存在 NFS 服务主体。

klist 命令报告是否存在密钥表文件并显示主体。如果结果显示不存在密钥表文件或者不存在 NFS 服务主体，则需要验证是否已完成[如何配置 Kerberos NFS 服务器](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbs/index.html)中的所有步骤。

|  |
| --- |
| # **klist -k**  Keytab name: FILE:/etc/krb5/krb5.keytab  KVNO Principal  ---- ---------------------------------------------------------  3 nfs/denver.example.com@EXAMPLE.COM  3 nfs/denver.example.com@EXAMPLE.COM  3 nfs/denver.example.com@EXAMPLE.COM  3 nfs/denver.example.com@EXAMPLE.COM |

1. 在 /etc/nfssec.conf 文件中启用 Kerberos 安全模式。

编辑 /etc/nfssec.conf 文件并删除位于 Kerberos 安全模式前面的 "#"。

|  |
| --- |
| # **cat /etc/nfssec.conf**  .  .  #  # Uncomment the following lines to use Kerberos V5 with NFS  #  krb5 390003 kerberos\_v5 default - # RPCSEC\_GSS  krb5i 390004 kerberos\_v5 default integrity # RPCSEC\_GSS  krb5p 390005 kerberos\_v5 default privacy # RPCSEC\_GSS |

1. 编辑 /etc/dfs/dfstab 文件，并将带有所需安全模式的 **sec=** 选项添加到相应的项中。

|  |
| --- |
| **share -F nfs -o sec=*mode* *file\_system*** |

1. *mode*
2. 指定共享文件系统时要使用的安全模式。使用多种安全模式时，会将列表中的第一种模式用作缺省模式。
3. *file\_system*
4. 定义要共享的文件系统的路径。
5. 尝试从指定的文件系统访问文件的所有客户机都要求 Kerberos 验证。要访问文件，应验证 NFS 客户机上的用户主体。
6. 请确保服务器上正在运行 NFS 服务。

如果此命令是您所启动的第一个 share 命令或 share 命令集，则 NFS 守护进程可能未运行。以下命令将重新启动该守护进程：

|  |
| --- |
| # **svcadm restart network/nfs/server** |

1. （可选的）如果使用的是自动挂载程序，请编辑 auto\_master 数据库以选择非缺省安全模式。

如果不使用自动挂载程序访问文件系统或者安全模式的缺省选择可接受，则无需执行此过程。

|  |
| --- |
| *file\_system* auto\_home -nosuid,sec=*mode* |

1. （可选的）使用非缺省模式手动发布用于访问文件系统的 mount 命令。

或者，可以使用 mount 命令指定安全模式，但此替代方法不会利用自动挂载程序。

|  |
| --- |
| # **mount -F nfs -o sec=*mode* *file\_system*** |

**示例 22–3 使用一种 Kerberos 安全模式共享文件系统**

在此示例中，dfstab 文件行表明：在通过 NFS 服务访问任何文件之前，必须先成功完成 Kerberos 验证。

|  |
| --- |
| # **grep krb /etc/dfs/dfstab**  share -F nfs -o sec=krb5 /export/home |

**示例 22–4 使用多种 Kerberos 安全模式共享文件系统**

在此示例中，选择了所有三种 Kerberos 安全模式。如果发出挂载请求时未指定任何安全模式，则将在所有 NFS V3 客户机中使用列出的第一种模式（在此例中为 krb5）。有关更多信息，请参见 [nfssec(5)](https://docs.oracle.com/docs/cd/E19253-01/816-5175/6mbba7f21/index.html) 手册页。

|  |
| --- |
| # **grep krb /etc/dfs/dfstab**  share -F nfs -o sec=krb5:krb5i:krb5p /export/home |

**配置 Kerberos 客户机**

Kerberos 客户机是网络上需要使用 Kerberos 服务的任何主机（不是 KDC 服务器）。本节介绍有关安装 Kerberos 客户机的过程以及使用 root 验证以挂载 NFS 文件系统的特定信息。

**配置 Kerberos 客户机（任务列表）**

以下任务列表包括有关设置 Kerberos 客户机的所有过程。每行都包括任务说明（说明执行该项任务的原因）以及指向该任务的链接。

| **任务** | **说明** | **参考** |
| --- | --- | --- |
| 建立 Kerberos 客户机安装配置文件。 | 生成可用于自动安装 Kerberos 客户机的客户机安装配置文件。 | [如何创建 Kerberos 客户机安装配置文件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc4/index.html) |
| 配置 Kerberos 客户机。 | 手动安装 Kerberos 客户机。如果每台客户机安装要求唯一的安装参数，请使用此过程。 | [如何手动配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc7/index.html) |
|  | 自动安装 Kerberos 客户机。如果每台客户机的安装参数都相同，请使用此过程。 | [如何自动配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc5/index.html) |
|  | 交互式安装 Kerberos 客户机。如果仅需要更改一些安装参数，请使用此过程。 | [如何交互配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc6/index.html) |
| 允许客户机以 root 用户身份访问 NFS 文件系统。 | 在客户机上创建 root 主体，以便客户机可以挂载使用 root 访问权限共享的 NFS 文件系统。此外，允许为客户机设置对 NFS 文件系统的非交互 root 访问权限，以便可以运行 cron 作业。 | [如何以 root 用户身份访问受 Kerberos 保护的 NFS 文件系统](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc8/index.html) |

**Procedure如何创建 Kerberos 客户机安装配置文件**

此过程创建可在安装 Kerberos 客户机时使用的 kclient 配置文件。使用 kclient 配置文件，可降低出现键入错误的可能性。此外，与交互式过程相比，使用该配置文件可以减少用户干预。

1. 成为超级用户。
2. 创建 kclient 安装配置文件。

kclient 配置文件样例与以下内容类似：

|  |
| --- |
| client# **cat /net/kdc1.example.com/export/install/profile**  REALM EXAMPLE.COM  KDC kdc1.example.com  ADMIN clntconfig  FILEPATH /net/kdc1.example.com/export/install/krb5.conf  NFS 1  DNSLOOKUP none |

**Procedure如何自动配置 Kerberos 客户机**

**开始之前**

此过程使用安装配置文件。请参见[如何创建 Kerberos 客户机安装配置文件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc4/index.html)。

1. 成为超级用户。
2. 运行 kclient 安装脚本。

要完成此过程，需要提供 clntconfig 主体的口令。

|  |
| --- |
| client# **/usr/sbin/kclient -p /net/kdc1.example.com/export/install/krb5.conf**  Starting client setup  ---------------------------------------------------  kdc1.example.com  Setting up /etc/krb5/krb5.conf.  Obtaining TGT for clntconfig/admin ...  Password for clntconfig/admin@EXAMPLE.COM: *<Type the password>*  nfs/client.example.com entry ADDED to KDC database.  nfs/client.example.com entry ADDED to keytab.  host/client.example.com entry ADDED to KDC database.  host/client.example.com entry ADDED to keytab.  Copied /net/kdc1.example.com/export/clientinstall/krb5.conf.  ---------------------------------------------------  Setup COMPLETE.  client# |

**示例 22–5 使用命令行覆盖项自动配置 Kerberos 客户机**

以下示例将覆盖在安装配置文件中设置的 DNSARG 和 KDC 参数。

|  |
| --- |
| # **/usr/sbin/kclient -p /net/kdc1.example.com/export/install/krb5.conf**\  **-d dns\_fallback -k kdc2.example.com**  Starting client setup  ---------------------------------------------------  kdc1.example.com  Setting up /etc/krb5/krb5.conf.  Obtaining TGT for clntconfig/admin ...  Password for clntconfig/admin@EXAMPLE.COM: *<Type the password>*  nfs/client.example.com entry ADDED to KDC database.  nfs/client.example.com entry ADDED to keytab.  host/client.example.com entry ADDED to KDC database.  host/client.example.com entry ADDED to keytab.  Copied /net/kdc1.example.com/export/install/krb5.conf.  ---------------------------------------------------  Setup COMPLETE.  client# |

**Procedure如何交互配置 Kerberos 客户机**

此过程使用 kclient 安装实用程序而不是使用安装配置文件。

1. 成为超级用户。
2. 运行 kclient 安装脚本。

需要提供以下信息：

* + Kerberos 领域名称
  + 主 KDC 主机名
  + 管理主体名称
  + 管理主体的口令

**示例 22–6 运行 kclient 安装实用程序**

以下输出给出了运行 kclient 命令的结果。

|  |
| --- |
| client# **/usr/sbin/kclient**  Starting client setup  ---------------------------------------------------  Do you want to use DNS for kerberos lookups ? [y/n]: **n**  No action performed.  Enter the Kerberos realm: **EXAMPLE.COM**  Specify the KDC hostname for the above realm: kdc1.example.com  Setting up /etc/krb5/krb5.conf.  Enter the krb5 administrative principal to be used: **clntconfig/admin**  Obtaining TGT for clntconfig/admin ...  Password for clntconfig/admin@EXAMPLE.COM: *<Type the password>*  Do you plan on doing Kerberized nfs ? [y/n]: **n**  host/client.example.com entry ADDED to KDC database.  host/client.example.com entry ADDED to keytab.  Do you want to copy over the master krb5.conf file ? [y/n]: **y**  Enter the pathname of the file to be copied: \  **/net/kdc1.example.com/export/install/krb5.conf**  Copied /net/kdc1.example.com/export/install/krb5.conf.  ---------------------------------------------------  Setup COMPLETE !  # |

**Procedure如何手动配置 Kerberos 客户机**

在此过程中，将使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* DNS 域名 = example.com
* 主 KDC = kdc1.example.com
* 从 KDC = kdc2.example.com
* 客户机 = client.example.com
* admin 主体 = kws/admin
* 用户主体 = mre
* 联机帮助 URL = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956

**注 –**

调整该 URL 以指向“SEAM Administration Tool”部分，如[SEAM Administration Tool 中的联机帮助 URL](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vba/index.html)中所述。

1. 成为超级用户。
2. 编辑 Kerberos 配置文件 ( krb5.conf)。

要从 Kerberos 缺省版本更改该文件，需要更改领域名称和服务器名称。您还需要标识 gkadmin 帮助文件的路径。

|  |
| --- |
| kdc1 # **cat /etc/krb5/krb5.conf**  [libdefaults]  default\_realm = **EXAMPLE.COM**  [realms]  **EXAMPLE.COM** = {  **kdc = kdc1.example.com**  **kdc = kdc2.example.com**  admin\_server = **kdc1.example.com**  }  [domain\_realm]  **.example.com = EXAMPLE.COM**  #  # if the domain name and realm name are equivalent,  # this entry is not needed  #  [logging]  default = FILE:/var/krb5/kdc.log  kdc = FILE:/var/krb5/kdc.log  [appdefaults]  gkadmin = {  help\_url = **http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956** |

**注 –**

如果要限制加密类型，可以设置 default\_tkt\_enctypes 或 default\_tgs\_enctypes 行。有关限制加密类型涉及的问题的说明，请参阅[使用 Kerberos 加密类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ver/index.html)。

1. （可选的）更改用于定位 KDC 的过程。

缺省情况下，使用主机和域名到 kerberos 领域的映射定位 KDC。可以通过将 dns\_lookup\_kdc、dns\_lookup\_realm 或 dns\_fallback 添加到 krb5.conf 文件的 libdefaults 部分来更改此行为。有关更多信息，请参见 [krb5.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufn/index.html) 手册页。

1. （可选的）使用 NTP 或其他时钟同步机制将客户机时钟与主 KDC 时钟同步。

安装和使用网络时间协议 (Network Time Protocol, NTP) 并非必需。但是，要成功验证，每个时钟必须处于 krb5.conf 文件的 libdefaults 部分中定义的缺省时间内。有关 NTP 的信息，请参见[同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)。

1. 启动 kadmin。

可以使用 SEAM Administration Tool 添加主体，如[如何创建新的 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdn/index.html)中所述。为此，必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。不过，以下示例说明如何使用命令行添加所需的主体。

|  |
| --- |
| denver # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. （可选的）如果不存在用户主体，请创建用户主体。

仅当尚未对与此主机关联的用户指定主体时，才需要创建用户主体。

|  |
| --- |
| kadmin: **addprinc mre**  Enter password for principal mre@EXAMPLE.COM: *<Type the password>*  Re-enter password for principal mre@EXAMPLE.COM: *<Type it again>*  kadmin: |

* 1. （可选的）创建 root 主体。

如果客户机不要求对使用 NFS 服务挂载的远程文件系统拥有 root 访问权限，则可以跳过此步骤。为了避免创建领域范围的 root 主体，root 主体应是由两个部分组成的主体（第二个组成部分为 Kerberos 客户机系统的主机名）。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **addprinc -randkey root/client.example.com**  Principal "root/client.example.com" created.  kadmin: |

* 1. 创建 host 主体。

host 主体用于验证应用程序。

|  |
| --- |
| kadmin: **addprinc -randkey host/denver.example.com**  Principal "host/denver.example.com@EXAMPLE.COM" created.  kadmin: |

* 1. （可选的）将服务器的 NFS 服务主体添加到服务器的密钥表文件中。

仅当客户机需要使用 Kerberos 验证访问 NFS 文件系统时，才需要执行此步骤。

|  |
| --- |
| kadmin: **ktadd nfs/denver.example.com**  Entry for principal nfs/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 nfs/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 nfs/denver.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. （可选的）将 root 主体添加到服务器的密钥表文件中。

如果添加了 root 主体，则必须执行此步骤，以便客户机对使用 NFS 服务挂载的文件系统拥有 root 访问权限。如果需要非交互 root 访问权限（例如，以 root 身份运行 cron 作业），也必须执行此步骤。

|  |
| --- |
| kadmin: **ktadd root/client.example.com**  Entry for principal root/client.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 root/client.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 root/client.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 将 host 主体添加到服务器的密钥表文件中。

|  |
| --- |
| kadmin: **ktadd host/denver.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: |

* 1. 退出 kadmin。

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

1. （可选的）要在 NFS 上使用 Kerberos，请在 /etc/nfssec.conf 文件中启用 Kerberos 安全模式。

编辑 /etc/nfssec.conf 文件并删除位于 Kerberos 安全模式前面的 "#"。

|  |
| --- |
| # **cat /etc/nfssec.conf**  .  .  #  # Uncomment the following lines to use Kerberos V5 with NFS  #  krb5 390003 kerberos\_v5 default - # RPCSEC\_GSS  krb5i 390004 kerberos\_v5 default integrity # RPCSEC\_GSS  krb5p 390005 kerberos\_v5 default privacy # RPCSEC\_GSS |

1. 如果希望客户机自动更新 TGT 或者向用户发出有关 Kerberos 票证失效的警告，请在 /etc/krb5/warn.conf 文件中创建相应的项。

有关更多信息，请参见 [warn.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ukr/index.html) 手册页。

**示例 22–7 使用非 Kerberos KDC 设置 Kerberos 客户机**

可以设置 Kerberos 客户机，使其与非 Kerberos KDC 协同工作。在此情况下，必须在 realms 部分的 /etc/krb5/krb5.conf 文件中包括一行。该行更改客户机与 Kerberos 口令更改服务器通信时要使用的协议。该行的格式如下：

|  |
| --- |
| [realms]  EXAMPLE.COM = {  kdc = kdc1.example.com  kdc = kdc2.example.com  admin\_server = kdc1.example.com  **kpasswd\_protocol = SET\_CHANGE**  } |

**示例 22–8 主机和域名到 Kerberos 领域的映射的 DNS TXT 记录**

|  |
| --- |
| @ IN SOA kdc1.example.com root.kdc1.example.com (  1989020501 ;serial  10800 ;refresh  3600 ;retry  3600000 ;expire  86400 ) ;minimum  IN NS kdc1.example.com.  kdc1 IN A 192.146.86.20  kdc2 IN A 192.146.86.21  \_kerberos.example.com. IN TXT "EXAMPLE.COM"  \_kerberos.kdc1.example.com. IN TXT "EXAMPLE.COM"  \_kerberos.kdc2.example.com. IN TXT "EXAMPLE.COM" |

**示例 22–9 Kerberos 服务器位置的 DNS SRV 记录**

此示例定义主 KDC、admin 服务器和 kpasswd 服务器的位置记录。

|  |
| --- |
| @ IN SOA kdc1.example.com root.kdc1.example.com (  1989020501 ;serial  10800 ;refresh  3600 ;retry  3600000 ;expire  86400 ) ;minimum  IN NS kdc1.example.com.  kdc1 IN A 192.146.86.20  kdc2 IN A 192.146.86.21  \_kerberos.\_udp.EXAMPLE.COM IN SRV 0 0 88 kdc1.example.com  \_kerberos-adm.\_udp.EXAMPLE.COM IN SRV 0 0 749 kdc1.example.com  \_kpasswd.\_udp.EXAMPLE.COM IN SRV 0 0 749 kdc1.example.com |

**Procedure如何以 root 用户身份访问受 Kerberos 保护的 NFS 文件系统**

通过此过程，客户机可以使用 root ID 权限访问要求 Kerberos 验证的 NFS 文件系统。特别是，可以访问使用以下选项共享的 NFS 文件系统：**-o** sec=krb5,root=client1.sun.com。

1. 成为超级用户。
2. 启动 kadmin。

可以使用 SEAM Administration Tool 添加主体，如[如何创建新的 Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vdn/index.html)中所述。为此，必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。不过，以下示例说明如何使用命令行添加所需的主体。

|  |
| --- |
| denver # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 为 NFS 客户机创建 root 主体。

此主体用于对要求 Kerberos 验证的已挂载 NFS 的文件系统提供 root 等效访问权限。为了避免创建领域范围的 root 主体，root 主体应是由两个部分组成的主体（第二个组成部分为 Kerberos 客户机系统的主机名）。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **addprinc -randkey root/client.example.com**  Principal "root/client.example.com" created.  kadmin: |

* 1. 将 root 主体添加到服务器的密钥表文件中。

如果添加了 root 主体，则必须执行此步骤，以便客户机对使用 NFS 服务挂载的文件系统拥有 root 访问权限。如果需要非交互 root 访问权限（例如，以 root 身份运行 cron 作业），也必须执行此步骤。

|  |
| --- |
| kadmin: **ktadd root/client.example.com**  Entry for principal root/client.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 root/client.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 root/client.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

**Procedure在 Kerberos 领域中配置用户自动迁移**

没有 Kerberos 主体的用户可以自动迁移到现有 Kerberos 领域。通过将 pam\_krb5\_migrate 模块堆叠在 /etc/pam.conf 的服务验证栈中，可以通过正在使用的服务的 PAM 框架实现迁移。

在此示例中，将配置 rlogin 和 other PAM 服务名称以使用自动迁移。将使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* 主 KDC = kdc1.example.com
* 承载迁移服务的计算机 = server1.example.com
* 迁移服务主体 = host/server1.example.com

**开始之前**

将 server1 设置为 EXAMPLE.COM 领域的 Kerberos 客户机。有关更多信息，请参见[配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc1/index.html)。

1. 检查是否存在 server1 的主机服务主体。

server1 的 keytab 文件中的主机服务主体用于向主 KDC 验证该服务器。

|  |
| --- |
| server1 # **klist -k**  Keytab name: FILE:/etc/krb5/krb5.keytab  KVNO Principal  ---- ------------------------------------------------  3 host/server1.example.com@EXAMPLE.COM  3 host/server1.example.com@EXAMPLE.COM  3 host/server1.example.com@EXAMPLE.COM  3 host/server1.example.com@EXAMPLE.COM |

1. 对 PAM 配置文件进行更改。

将 pam\_krb5\_migrate PAM 模块添加到 rlogin 和 other 服务名称的验证栈中。系统将自动为使用 rlogin、telnet 或 ssh 而不具有 Kerberos 主体的用户创建主体。

|  |
| --- |
| # **cat /etc/pam.conf**  .  .  #  # rlogin service (explicit because of pam\_rhost\_auth)  #  rlogin auth sufficient pam\_rhosts\_auth.so.1  rlogin auth requisite pam\_authtok\_get.so.1  rlogin auth required pam\_dhkeys.so.1  rlogin auth required pam\_unix\_cred.so.1  rlogin auth required pam\_unix\_auth.so.1  rlogin auth sufficient pam\_krb5.so.1  **rlogin auth optional pam\_krb5\_migrate.so.1**  #  .  .  #  # Default definitions for Authentication management  # Used when service name is not explicitly mentioned for authentication  #  other auth requisite pam\_authtok\_get.so.1  other auth required pam\_dhkeys.so.1  other auth required pam\_unix\_cred.so.1  other auth required pam\_unix\_auth.so.1  other auth sufficient pam\_krb5.so.1  **other auth optional pam\_krb5\_migrate.so.1** |

1. （可选的）如果需要，可强制立即更改口令。

可以将新建 Kerberos 帐户的口令失效时间设置为当前时间（现在），以便强制立即更改 Kerberos 口令。要将失效时间设置为当前时间，请将 **expire\_pw** 选项添加到使用 pam\_krb5\_migrate 模块的行中。有关更多信息，请参见 [pam\_krb5\_migrate(5)](https://docs.oracle.com/docs/cd/E19253-01/816-5175/6mbba7f2c/index.html) 手册页。

|  |
| --- |
| # **cat /etc/pam.conf**  .  .  **rlogin auth optional pam\_krb5\_migrate.so.1 expire\_pw**  #  .  .  **other auth optional pam\_krb5\_migrate.so.1 expire\_pw** |

1. 在主 KDC 上，更新访问控制文件。

以下项将为所有用户（root 用户除外）授予对 host/server1.example.com 服务主体的迁移和查询权限。务必注意，不应使用 U 权限迁移 kadm5.acl 文件中列出的用户。这些项必须位于允许所有用户或 ui 项之前。有关更多信息，请参见 [kadm5.acl(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufk/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kadm5.acl**  host/server1.example.com@EXAMPLE.COM U root  host/server1.example.com@EXAMPLE.COM ui \*  \*/admin@EXAMPLE.COM \* |

1. 在主 KDC 上，重新启动 Kerberos 管理守护进程。

通过此步骤，kadmind 守护进程可以使用新的 kadm5.acl 项。

|  |
| --- |
| kdc1 # **svcadm restart network/security/kadmin** |

1. 在主 KDC 上，向 pam.conf 文件中添加项。

通过以下项，kadmind 守护进程可以使用 k5migrate PAM 服务来验证需要迁移的帐户的 UNIX 用户口令。

|  |
| --- |
| # **grep k5migrate /etc/pam.conf**  k5migrate auth required pam\_unix\_auth.so.1  k5migrate account required pam\_unix\_account.so.1 |

**同步 KDC 和 Kerberos 客户机的时钟**

所有参与 Kerberos 验证系统的主机都必须在指定的最长时间（称为**时钟相位差**）内同步其内部时钟。针对这一要求，需要进行另一种 Kerberos 安全检查。如果任意两台参与主机之间的时间偏差超过了时钟相位差，则客户机请求会被拒绝。

时钟相位差还确定应用程序服务器必须跟踪所有 Kerberos 协议消息的时间长度，以便识别和拒绝重放的请求。因此，时钟相位差的值越大，应用程序服务器必须收集的信息就越多。

时钟相位差的最大缺省值为 300 秒（5 分钟）。可以在 krb5.conf 文件的 libdefaults 部分中更改此缺省值。

**注 –**

出于安全原因，不要将时钟相位差增大到超过 300 秒。

由于维护 KDC 和 Kerberos 客户机之间的同步时钟非常重要，因此应使用网络时间协议 (Network Time Protocol, NTP) 软件同步这些时钟。从 Solaris 2.6 发行版开始，Solaris 软件中提供了由美国特拉华大学开发的 NTP 公用软件。

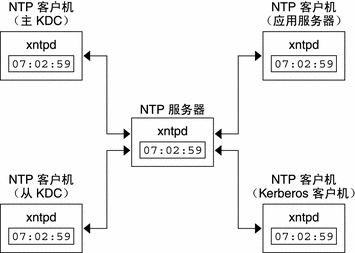
**注 –**

同步时钟的另一种方法是使用 rdate 命令和 cron 作业（一种比使用 NTP 参与性更小的过程）。但是，本节重点介绍如何使用 NTP。并且，如果使用网络来同步时钟，时钟同步协议本身必须是安全的。

通过 NTP，可以在网络环境中管理准确时间或网络时钟同步，或者同时管理这两者。 本质上，NTP 是一种服务器/客户机实现。可以选择一个系统（NTP 服务器）作为主时钟。然后，设置所有其他系统（NTP 客户机），使这些系统的时钟与主时钟同步。

为了同步时钟，NTP 使用 xntpd 守护进程，该守护进程设置并维护 UNIX 系统时间，使其与 Internet 标准时间服务器的时间保持一致。以下给出了此服务器/客户机 NTP 实现的示例。

**图 22–1 使用 NTP 同步时钟**



确保 KDC 和 Kerberos 客户机保持时钟同步涉及以下步骤的实现：

1. 在网络上设置 NTP 服务器。此服务器可以是除主 KDC 之外的任何系统。要了解 NTP 服务器任务，请参见[*《系统管理指南：网络服务》*中的*“管理网络时间协议（任务）”*](https://docs.oracle.com/docs/cd/E19253-01/819-7059/6n91h5tti/index.html)。
2. 在网络上配置 KDC 和 Kerberos 客户机时，将它们设置为 NTP 服务器的 NTP 客户机。要了解 NTP 客户机任务，请参见[*《系统管理指南：网络服务》*中的*“管理网络时间协议（任务）”*](https://docs.oracle.com/docs/cd/E19253-01/819-7059/6n91h5tti/index.html)。

**交换主 KDC 和从 KDC**

使用本节中的过程可以更容易地将主 KDC 与从 KDC 进行交换。仅当主 KDC 服务器由于某种原因出现故障时，或者需要重新安装主 KDC（例如，由于安装了新硬件）时，才应将主 KDC 与从 KDC 进行交换。

**Procedure如何配置可交换的从 KDC**

在希望其可以成为主 KDC 的从 KDC 服务器上执行此过程。此过程假定将使用增量传播。

1. 在安装 KDC 过程中使用主 KDC 和可交换从 KDC 的别名。

定义 KDC 的主机名时，请确保 DNS 中包括每个系统的别名。此外，在 /etc/krb5/krb5.conf 文件中定义主机时也应使用别名。

1. 逐步完成从 KDC 安装。

在进行任何交换之前，在该领域中此服务器的作用应与任何其他从 KDC 相同。有关说明，请参见[如何配置从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbi/index.html)。

1. 移动主 KDC 命令

要禁止从该从 KDC 运行主 KDC 命令，请将 kprop、kadmind 和 kadmin.local 命令移到一个保留位置。

|  |
| --- |
| kdc4 # **mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save**  kdc4 # **mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save**  kdc4 # **mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save** |

**Procedure如何交换主 KDC 和从 KDC**

在此过程中，要交换出的主 KDC 服务器名为 kdc1。将成为新的主 KDC 的从 KDC 名为 kdc4。此过程假定将使用增量传播。

**开始之前**

此过程要求已将该从 KDC 服务器设置为可交换的从 KDC。有关更多信息，请参见[如何配置可交换的从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vce/index.html)。

1. 在新的主 KDC 上，启动 kadmin。

|  |
| --- |
| kdc4 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 为 kadmind 服务创建新的主体。

以下示例中的第一个 addprinc 命令显示为两行，但实际上该命令应在同一行中键入。

|  |
| --- |
| kadmin: **addprinc -randkey -allow\_tgs\_req +password\_changing\_service -clearpolicy \**  **changepw/kdc4.example.com**  Principal "changepw/kdc4.example.com@ENG.SUN.COM" created.  kadmin: **addprinc -randkey -allow\_tgs\_req -clearpolicy kadmin/kdc4.example.com**  Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.  kadmin: |

* 1. 创建密钥表文件。

|  |
| --- |
| kadmin: **ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc4.example.com**  Entry for principal kadmin/kdc4.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 kadmin/kdc4.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 kadmin/kdc4.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: **ktadd -k /etc/krb5/kadm5.keytab changepw/kdc4.example.com**  Entry for principal changepw/kdc4.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 changepw/kdc4.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 changepw/kdc4.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal changepw/kdc4.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

1. 在新的主 KDC 上，强制执行同步。

以下步骤将在从服务器上强制执行完全 KDC 更新。

|  |
| --- |
| kdc4 # **svcadm disable network/security/krb5kdc**  kdc4 # **rm /var/krb5/principal.ulog**  kdc4 # **svcadm enable network/security/krb5kdc** |

1. 在新的主 KDC 上，清除更新日志。

以下步骤将重新初始化新的主 KDC 服务器的更新日志。

|  |
| --- |
| kdc4 # **svcadm disable network/security/krb5kdc**  kdc4 # **rm /var/krb5/principal.ulog** |

1. 在旧的主 KDC 上，中止 kadmind 和 krb5kdc 进程。

中止 kadmind 进程后，可防止对 KDC 数据库进行任何更改。

|  |
| --- |
| kdc1 # **svcadm disable network/security/kadmin**  kdc1 # **svcadm disable network/security/krb5kdc** |

1. 在旧的主 KDC 上，指定请求传播的轮询时间。

将 /etc/krb5/kdc.conf 中的 sunw\_dbprop\_master\_ulogsize 项替换为定义 sunw\_dbprop\_slave\_poll 的项。该项将轮询时间设置为 2 分钟。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kdc.conf**  [kdcdefaults]  kdc\_ports = 88,750  [realms]  EXAMPLE.COM= {  profile = /etc/krb5/krb5.conf  database\_name = /var/krb5/principal  admin\_keytab = /etc/krb5/kadm5.keytab  acl\_file = /etc/krb5/kadm5.acl  kadmind\_port = 749  max\_life = 8h 0m 0s  max\_renewable\_life = 7d 0h 0m 0s  sunw\_dbprop\_enable = true  **sunw\_dbprop\_slave\_poll = 2m**  } |

1. 在旧的主 KDC 上，移动主 KDC 命令和 kadm5.acl 文件。

要禁止运行主 KDC 命令，请将 kprop、kadmind 和 kadmin.local 命令移到一个保留位置。

|  |
| --- |
| kdc1 # **mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save**  kdc1 # **mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save**  kdc1 # **mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save**  kdc1 # **mv /etc/krb5/kadm5.acl /etc/krb5/kadm5.acl.save** |

1. 在 DNS 服务器上，更改主 KDC 的别名。

要更改服务器，请编辑 example.com 区域文件并更改 masterkdc 的项。

|  |
| --- |
| masterkdc IN CNAME kdc4 |

1. 在 DNS 服务器上，重新启动 Internet 域名服务器。

运行以下命令以重新装入新的别名信息：

|  |
| --- |
| # **svcadm refresh network/dns/server** |

1. 在新的主 KDC 上，移动主 KDC 命令和从 kpropd.acl 文件。

|  |
| --- |
| kdc4 # **mv /usr/lib/krb5/kprop.save /usr/lib/krb5/kprop**  kdc4 # **mv /usr/lib/krb5/kadmind.save /usr/lib/krb5/kadmind**  kdc4 # **mv /usr/sbin/kadmin.local.save /usr/sbin/kadmin.local**  kdc4 # **mv /etc/krb5/kpropd.acl /etc/krb5/kpropd.acl.save** |

1. 在新的主 KDC 上，创建 Kerberos 访问控制列表文件 (kadm5.acl)。

填充后，/etc/krb5/kadm5.acl 文件应包含允许管理 KDC 的所有主体名称。该文件还应列出请求增量传播的所有从 KDC。有关更多信息，请参见 [kadm5.acl(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufk/index.html) 手册页。

|  |
| --- |
| kdc4 # **cat /etc/krb5/krb5.acl**  **kws/admin@EXAMPLE.COM \***  **kiprop/kdc1.example.com@EXAMPLE.COM p** |

1. 在新的主 KDC 上的 kdc.conf 文件中，指定更新日志大小。

将 sunw\_dbprop\_slave\_poll 项替换为定义 sunw\_dbprop\_master\_ulogsize 的项。该项将日志大小设置为 1000 项。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kdc.conf**  [kdcdefaults]  kdc\_ports = 88,750  [realms]  EXAMPLE.COM= {  profile = /etc/krb5/krb5.conf  database\_name = /var/krb5/principal  admin\_keytab = /etc/krb5/kadm5.keytab  acl\_file = /etc/krb5/kadm5.acl  kadmind\_port = 749  max\_life = 8h 0m 0s  max\_renewable\_life = 7d 0h 0m 0s  sunw\_dbprop\_enable = true  **sunw\_dbprop\_master\_ulogsize = 1000**  } |

1. 在新的主 KDC 上，将 kiprop 主体添加到 kadmind 密钥表文件中。

|  |
| --- |
| kdc4 # **kadmin.local**  kadmin.local: **ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc4.example.com**  Entry for principal kiprop/kdc4.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 kiprop/kdc4.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 kiprop/kdc4.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin.local: **quit** |

1. 在新的主 KDC 上，启动 kadmind 和 krb5kdc。

|  |
| --- |
| kdc4 # **svcadm enable network/security/krb5kdc**  kdc4 # **svcadm enable network/security/kadmin** |

1. 在旧的主 KDC 上，添加 kiprop 服务主体。

通过将 kiprop 主体添加到 krb5.keytab 文件中，kpropd 守护进程可以对其自身进行增量传播服务验证。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin -p kws/admin**  Authenticating as pricipal kws/admin@EXAMPLE.COM with password.  Enter password: *<Type kws/admin password>*  kadmin: **ktadd kiprop/kdc1.example.com**  Entry for principal kiprop/kdc1.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 kiprop/kdc1.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 kiprop/kdc1.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: **quit** |

1. 在旧的主 KDC 上，将 krb5.conf 中列出的每个 KDC 的项添加到传播配置文件 kpropd.acl 中。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kpropd.acl**  host/kdc1.example.com@EXAMPLE.COM  host/kdc2.example.com@EXAMPLE.COM  host/kdc3.example.com@EXAMPLE.COM  host/kdc4.example.com@EXAMPLE.COM |

1. 在旧的主 KDC 上，启动 kpropd 和 krb5kdc。

启动 krb5kdc 守护进程时，如果将系统配置为从 KDC，则 kpropd 也将启动。

|  |
| --- |
| kdc1 # **svcadm enable network/security/krb5kdc** |

**管理 Kerberos 数据库**

Kerberos 数据库是 Kerberos 的主干，必须正确维护。本节介绍有关如何管理 Kerberos 数据库的一些过程，例如备份和恢复数据库、设置增量或并行传播以及管理存储文件。[如何配置主 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbh/index.html) 中介绍了初始设置该数据库的步骤。

**备份和传播 Kerberos 数据库**

将 Kerberos 数据库从主 KDC 传播到从 KDC 是最重要的配置任务之一。如果传播频率不够高，则主 KDC 和从 KDC 将不能同步。因此，如果主 KDC 关闭，则从 KDC 将不能获取最新的数据库信息。此外，如果出于平衡负载目的将从 KDC 配置为主 KDC，则将该从 KDC 用作主 KDC 的客户机将不能获取最新的信息。所以，必须确保传播频率足够高，或者基于更改 Kerberos 数据库的频率配置服务器使其进行增量传播。增量传播优先于手动传播，因为手动传播数据库时需要更多的管理开销。此外，执行完全数据库传播时效率很低。

配置主 KDC 时，可以在 cron 作业中设置 kprop\_script 命令以自动将 Kerberos 数据库备份到 /var/krb5/slave\_datatrans 转储文件，并将该文件传播到从 KDC。不过，与其他文件一样，Kerberos 数据库可能会损坏。如果从 KDC 上的数据受损，您可能无法注意到，因为下一次数据库自动传播会安装一个新的副本。但是，如果主 KDC 上的数据受损，则下一次传播期间会将损坏的数据库传播到所有从 KDC。而且，损坏的备份会覆写主 KDC 上先前未损坏的备份文件。

由于在这种情况下不存在任何“安全”的备份副本，因此还应设置 cron 作业，以便定期将 slave\_datatrans 转储文件复制到另一位置，或者使用 kdb5\_util 的 dump 命令创建另一份单独的备份副本。这样，如果数据库受损，则可以使用 kdb5\_util 的 load 命令在主 KDC 上恢复最新备份。

另一条重要注意事项是：由于数据库转储文件包含主体密钥，因此需要阻止未经授权的用户访问该文件。缺省情况下，只有 root 身份才具有读写数据库转储文件的权限。要阻止未经授权的访问，请仅使用 kprop 命令传播数据库转储文件，该命令会对要传送的数据进行加密。此外，kprop 仅将数据传播到从 KDC，这可以最大程度地降低将数据库转储文件意外发送到未经授权的主机的几率。

注意 – 注意 –

如果传播 Kerberos 数据库之后对其进行了更新，并且在下一次传播之前该数据库受损，则从 KDC 将不包含这些更新。这些更新将丢失。因此，如果要在计划的定期传播之前向 Kerberos 数据库中添加重要的更新，应手动传播该数据库，以避免数据丢失。

**kpropd.acl 文件**

KDC 上的 kpropd.acl 文件提供主机主体名称的列表（一个名称占一行），用于指定 KDC 可以通过传播从其接收更新数据库的系统。如果使用主 KDC 传播所有从 KDC，则每个从 KDC 上的 kpropd.acl 文件仅需包含主 KDC 的主机主体名称。

但是，本书中的 Kerberos 安装和后续配置步骤将指导您如何将相同的 kpropd.acl 文件添加到主 KDC 和从 KDC 中。此文件包含所有 KDC 主机主体名称。通过此配置，在传播 KDC 临时不可用时，可以从任何 KDC 进行传播。而且，通过在所有 KDC 上保留相同副本，可以更容易地维护配置。

**kprop\_script 命令**

kprop\_script 命令使用 kprop 命令将 Kerberos 数据库传播到其他 KDC。如果在从 KDC 上运行 kprop\_script 命令，则会将该从 KDC 的 Kerberos 数据库副本传播到其他 KDC。kprop\_script 的参数接受主机名列表，该列表以空格分隔，表示要传播的 KDC。

运行 kprop\_script 时，将在 /var/krb5/slave\_datatrans 文件中创建 Kerberos 数据库的备份，并将该文件复制到指定的 KDC。在完成传播之前，Kerberos 数据库处于锁定状态。

**Procedure如何备份 Kerberos 数据库**

1. 成为主 KDC 的超级用户。
2. 使用 kdb5\_util 命令的 dump 命令备份 Kerberos 数据库。

|  |
| --- |
| # **/usr/sbin/kdb5\_util dump** [**-verbose**] [**-d** *dbname*] [*filename* [*principals*...]] |

1. **-verbose**
2. 列显要备份的每个主体和策略的名称。
3. *dbname*
4. 定义要备份的数据库的名称。请注意，可以指定文件的绝对路径。 如果未指定 **-d** 选项，则缺省数据库名称为 /var/krb5/principal。
5. *filename*
6. 定义用于备份数据库的文件。可以指定文件的绝对路径。如果未指定文件，则数据库将转储到标准输出。
7. *principals*
8. 定义要备份的一个或多个主体的列表（以空格分隔）。必须使用全限定主体名称。如果未指定任何主体，则将备份整个数据库。

**示例 22–10 备份 Kerberos 数据库**

在以下示例中，Kerberos 数据库将备份到名为 dumpfile 的文件中。由于指定了 **-verbose** 选项，因此备份时会列显每个主体。

|  |
| --- |
| # **kdb5\_util dump -verbose dumpfile**  kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM  krbtgt/eng.example.com@ENG.EXAMPLE.COM  kadmin/history@ENG.EXAMPLE.COM  pak/admin@ENG.EXAMPLE.COM  pak@ENG.EXAMPLE.COM  changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM |

在以下示例中，将备份 Kerberos 数据库中的 pak 和 pak/admin 主体。

|  |
| --- |
| # **kdb5\_util dump -verbose dumpfile pak/admin@ENG.EXAMPLE.COM pak@ENG.EXAMPLE.COM**  pak/admin@ENG.EXAMPLE.COM  pak@ENG.EXAMPLE.COM |

**Procedure如何恢复 Kerberos 数据库**

1. 成为主 KDC 的超级用户。
2. 使用 kdb\_util 命令的 load 命令恢复 Kerberos 数据库。

|  |
| --- |
| # **/usr/sbin/kdb5\_util load** [**-verbose**] [**-d** *dbname*] [**-update**] [*filename*] |

1. **-verbose**
2. 列显要恢复的每个主体和策略的名称。
3. *dbname*
4. 定义要恢复的数据库的名称。请注意，可以指定文件的绝对路径。如果未指定 **-d** 选项，则缺省数据库名称为 /var/krb5/principal。
5. **-update**
6. 更新现有数据库。否则，会创建新数据库或覆写现有数据库。
7. *filename*
8. 定义用于恢复数据库的文件。可以指定文件的绝对路径。

**示例 22–11 恢复 Kerberos 数据库**

在以下示例中，将从 dumpfile 文件将名为 database1 的数据库恢复到当前目录。由于未指定 **-update** 选项，恢复操作将创建一个新数据库。

|  |
| --- |
| # **kdb5\_util load -d database1 dumpfile** |

**Procedure如何重新装入 Kerberos 数据库**

如果未在运行 Solaris 10 发行版的服务器上创建 KDC 数据库，则通过重新装入该数据库，可以利用改进的数据库格式。

**开始之前**

请确保数据库使用的是旧格式。请参见特定说明。

1. 在主 KDC 上，停止 KDC 守护进程。

|  |
| --- |
| kdc1 # **svcadm disable network/security/krb5kdc**  kdc1 # **svcadm disable network/security/kadmin** |

1. 转储 KDC 数据库。

|  |
| --- |
| kdc1 # **kdb5\_util dump /tmp/prdb.txt** |

1. 保存当前数据库文件的副本。

|  |
| --- |
| kdc1 # **cd /var/krb5**  kdc1 # **mkdir old**  kdc1 # **mv princ\* old/** |

1. 装入数据库。

|  |
| --- |
| kdc1 # **kdb5\_util load /tmp/prdb.txt** |

1. 启动 KDC 守护进程。

|  |
| --- |
| kdc1 # **svcadm enable network/security/krb5kdc**  kdc1 # **svcadm enable network/security/kadmin** |

**Procedure如何重新配置主 KDC 以使用增量传播**

此过程中的步骤可用于重新配置现有的主 KDC，以使用增量传播。在此过程中，将使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* DNS 域名 = example.com
* 主 KDC = kdc1.example.com
* 从 KDC = kdc2.example.com
* admin 主体 = kws/admin

1. 向 kdc.conf 中添加项。

需要启用增量传播，并选择主 KDC 将在日志中存储的更新数。有关更多信息，请参见 [kdc.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufl/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kdc.conf**  [kdcdefaults]  kdc\_ports = 88,750  [realms]  **EXAMPLE.COM**= {  profile = /etc/krb5/krb5.conf  database\_name = /var/krb5/principal  admin\_keytab = /etc/krb5/kadm5.keytab  acl\_file = /etc/krb5/kadm5.acl  kadmind\_port = 749  max\_life = 8h 0m 0s  max\_renewable\_life = 7d 0h 0m 0s  **sunw\_dbprop\_enable = true**  **sunw\_dbprop\_master\_ulogsize = 1000**  } |

1. 创建 kiprop 主体。

kiprop 主体用于验证主 KDC 服务器和授权来自主 KDC 的更新。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: **addprinc -randkey kiprop/kdc1.example.com**  Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.  kadmin: **addprinc -randkey kiprop/kdc2.example.com**  Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.  kadmin: |

1. 将 kiprop 主体添加到 kadmind 密钥表文件中

通过将 kiprop 主体添加到 kadm5.keytab 文件中，kadmind 命令可以在启动时对其自身进行验证。

|  |
| --- |
| kadmin: **ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com**  Entry for principal kiprop/kdc1.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 kiprop/kdc1.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 kiprop/kdc1.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.  kadmin: **quit** |

1. （可选的）在主 KDC 上，将 kiprop 项添加到 kpropd.acl 中

通过此项，主 KDC 可以接收对 kdc2 服务器的增量传播请求。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kpropd.acl**  host/kdc1.example.com@EXAMPLE.COM  host/kdc2.example.com@EXAMPLE.COM  \*/admin@EXAMPLE.COM \*  **kiprop/kdc2.example.com@EXAMPLE.COM p** |

1. 注释掉 root crontab 文件中的 kprop 行。

此步骤禁止从 KDC 传播其 KDC 数据库副本。

|  |
| --- |
| kdc1 # **crontab -e**  #ident "@(#)root 1.20 01/11/06 SMI"  #  # The root crontab should be used to perform accounting data collection.  #  # The rtc command is run to adjust the real time clock if and when  # daylight savings time changes.  #  10 3 \* \* \* /usr/sbin/logadm  15 3 \* \* 0 /usr/lib/fs/nfs/nfsfind  1 2 \* \* \* [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1  30 3 \* \* \* [ -x /usr/lib/gss/gsscred\_clean ] && /usr/lib/gss/gsscred\_clean  **#**10 3 \* \* \* /usr/lib/krb5kprop\_script kdc2.example.sun.com #SUNWkr5ma |

1. 重新启动 kadmind。

|  |
| --- |
| kdc1 # **svcadm restart network/security/kadmin** |

1. 重新配置所有使用增量传播的从 KDC 服务器。

**Procedure如何重新配置从 KDC 以使用增量传播**

1. 向 krb5.conf 中添加项。

这些新项启用增量传播并将轮询时间设置为 2 分钟。

|  |
| --- |
| kdc2 # **cat /etc/krb5/kdc.conf**  [kdcdefaults]  kdc\_ports = 88,750  [realms]  EXAMPLE.COM= {  profile = /etc/krb5/krb5.conf  database\_name = /var/krb5/principal  admin\_keytab = /etc/krb5/kadm5.keytab  acl\_file = /etc/krb5/kadm5.acl  kadmind\_port = 749  max\_life = 8h 0m 0s  max\_renewable\_life = 7d 0h 0m 0s  **sunw\_dbprop\_enable = true**  **sunw\_dbprop\_slave\_poll = 2m**  } |

1. 将 kiprop 主体添加到 krb5.keytab 文件中。

|  |
| --- |
| kdc2 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: **ktadd kiprop/kdc2.example.com**  Entry for principal kiprop/kdc2.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 kiprop/kdc2.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 kiprop/kdc2.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: **quit** |

1. 禁用 kpropd。

|  |
| --- |
| kdc2 # **svcadm disable network/security/krb5\_prop** |

1. 重新启动 KDC 服务器。

|  |
| --- |
| kdc2 # **svcadm restart network/security/krb5kdc** |

**Procedure如何配置从 KDC 以使用完全传播**

此过程说明如何重新配置运行 Solaris 10 发行版的从 KDC 服务器，以使用完全传播。通常，只有运行 Solaris 9 发行版或更早发行版的主 KDC 服务器才需要使用此过程。在这种情况下，主 KDC 服务器不支持增量传播，因此需要配置从 KDC 以允许进行传播。

在此过程中，将配置名为 kdc3 的从 KDC。此过程使用以下配置参数：

* 领域名称 = EXAMPLE.COM
* DNS 域名 = example.com
* 主 KDC = kdc1.example.com
* 从 KDC = kdc2.example.com 和 kdc3.example.com
* admin 主体 = kws/admin
* 联机帮助 URL = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956

**注 –**

调整该 URL 以指向“SEAM Administration Tool”部分，如[SEAM Administration Tool 中的联机帮助 URL](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vba/index.html)中所述。

**开始之前**

必须配置主 KDC。有关此从 KDC 是否可交换的特定说明，请参见[交换主 KDC 和从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcc/index.html)。

1. 在主 KDC 上，成为超级用户。
2. 在主 KDC 上，启动 kadmin。

必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| kdc1 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 在主 KDC 上，将从主机主体添加到数据库中（如果尚未执行此操作）。

要使从 KDC 正常工作，该从 KDC 必须具有主机主体。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **addprinc -randkey host/kdc3.example.com**  Principal "host/kdc3@EXAMPLE.COM" created.  kadmin: |

* 1. 退出 kadmin。

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

1. 在主 KDC 上，编辑 Kerberos 配置文件 (krb5.conf)。

需要添加每个从 KDC 的项。有关此文件的完整说明，请参见 [krb5.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98ufn/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/krb5.conf**  .  .  [realms]  EXAMPLE.COM = {  kdc = kdc1.example.com  kdc = kdc2.example.com  **kdc = kdc3.example.com**  admin\_server = kdc1.example.com  } |

1. 在主 KDC 上，将主 KDC 和每个从 KDC 的项添加到 kpropd.acl 文件中。

有关此文件的完整说明，请参见 [kprop(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq5j/index.html) 手册页。

|  |
| --- |
| kdc1 # **cat /etc/krb5/kpropd.acl**  host/kdc1.example.com@EXAMPLE.COM  host/kdc2.example.com@EXAMPLE.COM  **host/kdc3.example.com@EXAMPLE.COM** |

1. 在所有从 KDC 上，复制主 KDC 服务器的 KDC 管理文件。

由于主 KDC 服务器已更新每台 KDC 服务器所需的信息，因此需要在所有从 KDC 上执行此步骤。可以使用 ftp 或类似的传送机制从主 KDC 获取以下文件的副本：

* 1. /etc/krb5/krb5.conf
  2. /etc/krb5/kdc.conf
  3. /etc/krb5/kpropd.acl

1. 在所有从 KDC 上，请确保未填充 Kerberos 访问控制列表文件 kadm5.acl。

未修改的 kadm5.acl 文件如下所示：

|  |
| --- |
| kdc2 # **cat /etc/krb5/kadm5.acl**  \*/admin@\_\_\_default\_realm\_\_\_ \* |

如果此文件中包含 kiprop 项，请删除它们。

1. 在新的从 KDC 上，启动 kadmin 命令。

必须使用在配置主 KDC 时创建的一个 admin 主体名称登录。

|  |
| --- |
| kdc2 # **/usr/sbin/kadmin -p kws/admin**  Enter password: *<Type kws/admin password>*  kadmin: |

* 1. 使用 kadmin 将从 KDC 的 host 主体添加到从 KDC 的密钥表文件中。

此项可使 kprop 和其他基于 Kerberos 的应用程序正常工作。请注意，主体实例为主机名时，无论 /etc/resolv.conf 文件中的域名是大写还是小写，都必须以小写字母指定 FQDN。

|  |
| --- |
| kadmin: **ktadd host/kdc3.example.com**  Entry for principal host/kdc3.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/kdc3.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/kdc3.example.com with kvno 3, encryption type ARCFOUR  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  Entry for principal host/kdc3.example.com with kvno 3, encryption type DES cbc mode  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  kadmin: |

* 1. 退出 kadmin。

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

1. 在主 KDC 上，将从 KDC 名称添加到 cron 作业中，该作业通过运行 crontab **-e** 自动运行备份。

在 kprop\_script 行的结尾添加每个从 KDC 服务器的名称。

|  |
| --- |
| 10 3 \* \* \* /usr/lib/krb5/kprop\_script kdc2.example.com **kdc3.example.com** |

您可能还希望更改备份的时间。此项将在每天上午的 3:10 启动备份过程。

1. 在新的从 KDC 上，启动 Kerberos 传播守护进程。

|  |
| --- |
| kdc3 # **svcadm enable network/security/krb5\_prop** |

1. 在主 KDC 上，使用 kprop\_script 备份并传播数据库。

如果已存在数据库的备份副本，则无需完成其他备份。有关进一步的说明，请参见[如何手动将 Kerberos 数据库传播到从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcq/index.html)。

|  |
| --- |
| kdc1 # **/usr/lib/krb5/kprop\_script kdc3.example.com**  Database propagation to kdc3.example.com: SUCCEEDED |

1. 在新的从 KDC 上，使用 kdb5\_util 创建一个存储文件。

|  |
| --- |
| kdc3 # **/usr/sbin/kdb5\_util stash**  kdb5\_util: Cannot find/read stored master key while reading master key  kdb5\_util: Warning: proceeding without master key  Enter KDC database master key: *<Type the key>* |

1. （可选的）在新的从 KDC 上，使用 NTP 或其他时钟同步机制同步主 KDC 时钟。

安装和使用网络时间协议 (Network Time Protocol, NTP) 并非必需。但是，要成功验证，每个时钟必须处于 krb5.conf 文件的 libdefaults 部分中定义的缺省时间内。有关 NTP 的信息，请参见[同步 KDC 和 Kerberos 客户机的时钟](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcb/index.html)。

1. 在新的从 KDC 上，启动 KDC 守护进程 (krb5kdc)。

|  |
| --- |
| kdc3 # **svcadm enable network/security/krb5kdc** |

**Procedure如何验证 KDC 服务器是否已同步**

如果配置了增量传播，则此过程可确保已更新从 KDC 上的信息。

1. 在 KDC 主服务器上，运行 kproplog 命令。

|  |
| --- |
| kdc1 # **/usr/sbin/kproplog -h** |

1. 在从 KDC 服务器上，运行 kproplog 命令。

|  |
| --- |
| kdc2 # **/usr/sbin/kproplog -h** |

1. 检查最后一个序列号和最后一个时间标记的值是否匹配。

**示例 22–12 验证 KDC 服务器是否已同步**

以下是在主 KDC 服务器上运行 kproplog 命令的结果样例。

|  |
| --- |
| kdc1 # **/usr/sbin/kproplog -h**  Kerberos update log (/var/krb5/principal.ulog)  Update log dump:  Log version #: 1  Log state: Stable  Entry block size: 2048  Number of entries: 2500  First serial #: 137966  Last serial #: 140465  First time stamp: Fri Nov 28 00:59:27 2004  Last time stamp: Fri Nov 28 01:06:13 2004 |

以下是在从 KDC 服务器上运行 kproplog 命令的结果样例。

|  |
| --- |
| kdc2 # **/usr/sbin/kproplog -h**  Kerberos update log (/var/krb5/principal.ulog)  Update log dump:  Log version #: 1  Log state: Stable  Entry block size: 2048  Number of entries: 0  First serial #: None  Last serial #: 140465  First time stamp: None  Last time stamp: Fri Nov 28 01:06:13 2004 |

请注意，最后一个序列号和最后一个时间标记的值相同，这表示从 KDC 服务器与主 KDC 服务器同步。

请注意，在从 KDC 服务器的输出中，从 KDC 服务器的更新日志中不存在任何更新项。这是因为与主 KDC 服务器不同，从 KDC 服务器不保留更新。此外，由于第一个序列号或第一个时间标记不是相关信息，因此从 KDC 服务器也不包括这些信息。

**Procedure如何手动将 Kerberos 数据库传播到从 KDC**

此过程说明如何使用 kprop 命令传播 Kerberos 数据库。如果需要在定期的 cron 作业之外将从 KDC 与主 KDC 同步，可使用此过程。与 kprop\_script 不同，可以使用 kprop 仅传播当前数据库备份，而无需先创建 Kerberos 数据库的新备份。

**注 –**

如果使用的是增量传播，则不要使用此过程。

1. 成为主 KDC 的超级用户。
2. （可选的）使用 kdb5\_util 命令备份数据库。

|  |
| --- |
| # **/usr/sbin/kdb5\_util dump /var/krb5/slave\_datatrans** |

1. 使用 kprop 命令将数据库传播到从 KDC。

|  |
| --- |
| # **/usr/lib/krb5/kprop -f /var/krb5/slave\_datatrans *slave-KDC*** |

**示例 22–13 使用 kprop\_script 手动将 Kerberos 数据库传播到从 KDC**

如果要备份数据库，并在定期的 cron 作业之外将数据库传播到从 KDC，则还可以按如下所示使用 kprop\_script 命令：

|  |
| --- |
| # **/usr/lib/krb5/kprop\_script *slave-KDC*** |

**设置并行传播**

在大多数情况下，会以独占的方式使用主 KDC 将其 Kerberos 数据库传播到从 KDC。但是，如果站点上有很多从 KDC，则可以考虑共享装入传播进程，即所谓的**并行传播**。

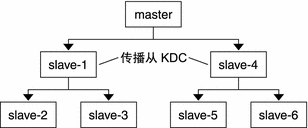
**注 –**

如果使用的是增量传播，则不要使用此过程。

通过并行传播，特定的从 KDC 可以与主 KDC 共享传播功能。通过共享此功能，可以更快地完成传播并减轻主 KDC 的工作。

例如，假设站点上有一个主 KDC 和六个从 KDC（如[图 22–2](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcr/index.html#setup-fig-316) 中所示），其中，slave-1 到 slave-3 组成一个逻辑组，slave-4 到 slave-6 组成另一个逻辑组。要设置并行传播，可以使主 KDC 将数据库传播到 slave-1 和 slave-4。而这些从 KDC 又可将数据库传播到其组中的从 KDC。

**图 22–2 并行传播配置示例**



**设置并行传播的配置步骤**

以下不是详细的逐步过程，而是用于启用并行传播的配置步骤的高级列表。这些步骤包括：

1. 在主 KDC 上，更改其 cron 作业的 kprop\_script 项，以仅包括将执行后续传播的从 KDC（**传播从 KDC**）的参数。
2. 在每个传播从 KDC 上，将 kprop\_script 项添加到其 cron 作业中，其中必须包括要传播的从 KDC 的参数。要成功地以并行方式进行传播，应设置 cron 作业，使其在将新 Kerberos 数据库传播到从 KDC 本身之后再运行。

**注 –**

对传播从 KDC 进行传播所需的时间取决于多种因素，例如网络带宽和 Kerberos 数据库的大小。

1. 在每个从 KDC 上，设置相应的传播权限。通过将从 KDC 传播的 KDC 的主机主体名称添加到其 kpropd.acl 文件中，可完成此步骤。

**示例 22–14 设置并行传播**

以[图 22–2](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcr/index.html#setup-fig-316) 为例，主 KDC 的 kprop\_script 项与以下示例类似：

|  |
| --- |
| 0 3 \* \* \* /usr/lib/krb5/kprop\_script slave-1.example.com slave-4.example.com |

slave-1 的 kprop\_script 项与以下示例类似：

|  |
| --- |
| 0 4 \* \* \* /usr/lib/krb5/kprop\_script slave-2.example.com slave-3.example.com |

请注意，从 KDC 上的传播在主 KDC 将数据库传播到它一小时后开始。

传播从 KDC 上的 kpropd.acl 文件将包含以下项：

|  |
| --- |
| host/master.example.com@EXAMPLE.COM |

要由 slave-1 传播的从 KDC 上的 kpropd.acl 文件将包含以下项：

|  |
| --- |
| host/slave-1.example.com@EXAMPLE.COM |

**管理存储文件**

**存储文件**包含 Kerberos 数据库的主密钥，该密钥在创建 Kerberos 数据库时自动创建。如果存储文件损坏，则可以使用 kdb5\_util 实用程序的 stash 命令替换损坏的文件。仅在使用 kdb5\_util 的 destroy 命令删除 Kerberos 数据库之后，才应删除存储文件。由于存储文件不会随数据库一起自动删除，所以必须删除存储文件以完成清除。

**Procedure如何删除存储文件**

1. 成为包含存储文件的 KDC 的超级用户。
2. 删除存储文件。

|  |
| --- |
| # **rm *stash-file*** |

1. 其中，*stash-file* 是存储文件的路径。缺省情况下，存储文件位于 /var/krb5/.k5. *realm* 中。
2. **注 –**
3. 如果需要重新创建存储文件，则可以使用 kdb5\_util 命令的 **-f** 选项。

**增强 Kerberos 服务器的安全性**

执行以下步骤以增强 Kerberos 应用程序服务器和 KDC 服务器的安全性。

**Procedure如何仅启用基于 Kerberos 的应用程序**

此过程限制对正在运行 telnet、ftp、rcp、rsh 和 rlogin 的服务器的网络访问，以便仅执行经过 Kerberos 验证的事务。

1. 更改 telnet 服务的 exec 属性。

将 **-a user** 选项添加到 telnet 的 exec 属性，以将访问权限限制为可以提供有效验证信息的那些用户。

|  |
| --- |
| # inetadm -m svc:/network/telnet:default exec="/usr/sbin/in.telnetd -a user" |

1. （可选的）如果尚未配置，则更改 telnet 服务的 exec 属性。

将 **-a** 选项添加到 ftp 的 exec 属性，以仅允许经过 Kerberos 验证的连接。

|  |
| --- |
| # inetadm -m svc:/network/ftp:default exec="/usr/sbin/in.ftpd -a" |

1. 禁用其他服务。

应禁用 in.rshd 和 in.rlogind 守护进程。

|  |
| --- |
| # **svcadm disable network/shell**  # **svcadm disable network/login:rlogin** |

**Procedure如何限制对 KDC 服务器的访问**

主 KDC 服务器和从 KDC 服务器都包含存储在本地的 KDC 数据库副本。限制对这些服务器的访问（以便保证数据库安全）对于 Kerberos 安装的整体安全非常重要。

1. 根据需要，禁用远程服务。

要提供安全的 KDC 服务器，应禁用所有不必要的网络服务。根据配置不同，可能已禁用其中某些服务。使用 svcs 命令检查服务状态。在大多数情况下，只需运行 time 和 krdb5\_kprop 服务。此外，使用回送 TLI（ticlts、ticotsord 和 ticots）的任何服务可以保持启用状态。

|  |
| --- |
| # **svcadm disable network/comsat**  # **svcadm disable network/dtspc/tcp**  # **svcadm disable network/finger**  # **svcadm disable network/login:rlogin**  # **svcadm disable network/rexec**  # **svcadm disable network/shell**  # **svcadm disable network/talk**  # **svcadm disable network/tname**  # **svcadm disable network/uucp**  # **svcadm disable network/rpc\_100068\_2-5/rpc\_udp** |

1. 限制对支持 KDC 的硬件的访问。

要限制物理访问，请确保 KDC 服务器及其监视器位于安全的设备中。用户应不能以任何方式访问此服务器。

1. 在本地磁盘或从 KDC 上存储 KDC 数据库备份。

仅在可以安全存储磁带时创建 KDC 的磁带备份。该做法同样适用于创建密钥表文件的副本。最好在未与其他系统共享的本地文件系统上存储这些文件。存储文件系统可以位于主 KDC 服务器或任何从 KDC 上。

* [*Previous*: 第 21 章 规划 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/seamplan-1/index.html)
* [*Next*: 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)
* © 2010, Oracle Corporation and/or its affiliates