[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 21 章 规划 Kerberos 服务

系统管理指南：安全性服务

* [*Previous*: 第 20 章 Kerberos 服务介绍](https://docs.oracle.com/cd/E19253-01/819-7061/intro-1/index.html)
* [*Next*: 第 22 章 配置 Kerberos 服务（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/setup-8/index.html)

**第 21 章 规划 Kerberos 服务**

参与安装和维护 Kerberos 服务的管理员应学习本章。本章介绍管理员在安装或配置服务之前必须确定的一些安装和配置选项。

以下是系统管理员或其他技术支持人员应学习的主题的列表：

* [为什么要规划 Kerberos 部署？](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vau/index.html)
* [Kerberos 领域](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vav/index.html)
* [将主机名映射到领域](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb0/index.html)
* [客户机名称和服务主体名称](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb1/index.html)
* [KDC 端口和管理服务端口](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb2/index.html)
* [从 KDC 数](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb3/index.html)
* [要使用的数据库传播系统](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb6/index.html)
* [领域内的时钟同步](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb7/index.html)
* [客户机安装选项](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb8/index.html)
* [Kerberos 加密类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vb9/index.html)
* [SEAM Administration Tool 中的联机帮助 URL](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vba/index.html)

**为什么要规划 Kerberos 部署？**

在安装 Kerberos 服务之前，必须解决几个配置问题。虽然在初始安装后可以更改配置，但每向系统中添加一台新客户机便会增加执行此操作的难度。而且某些更改可能需要进行完全重新安装，所以在规划 Kerberos 配置时最好应考虑长期目标。

部署 Kerberos 基础结构涉及以下任务：安装 KDC、为主机创建密钥以及迁移用户。 重新配置 Kerberos 部署与执行初始部署一样困难，因此要认真规划部署以避免必须进行重新配置。

**Kerberos 领域**

**领域**是一个类似于域的逻辑网络，用于定义一组系统，这些系统位于同一主 KDC 下。与建立 DNS 域名一样，在配置 Kerberos 服务之前，应解决以下问题以便进行跨领域验证：领域名称、领域数和每个领域的大小以及各领域之间的关系。

**领域名称**

领域名称可以由任何 ASCII 字符串组成。通常，领域名称与 DNS 域名相同，只不过领域名称采用大写。使用常见的名称时，这种约定有助于将 Kerberos 服务问题与 DNS 名称空间问题区分开来。如果不使用 DNS 或选择使用其他字符串，则可以使用任何字符串。但是，配置过程需要更多工作。采用符合标准 Internet 名称结构的领域名称是明智之举。

**领域数**

安装需要的领域数取决于下列因素：

* 要支持的客户机数。一个领域中具有太多客户机会增加管理难度，最终会要求对领域进行分割。确定可以支持的客户机数的主要因素如下：
  + 每台客户机产生的 Kerberos 通信量
  + 物理网络的带宽
  + 主机的速度

由于每种安装都有不同的限制，所以不存在确定最大客户机数的原则。

* 客户机间相隔的距离。如果客户机位于不同的地理区域中，则可以设置几个较小的领域。
* 可作为 KDC 安装的主机数。每个领域中应至少有两台 KDC 服务器：一台主服务器和一台从服务器。

建议将 Kerberos 领域与管理域结合使用。请注意，Kerberos V 领域可以跨与该领域相对应的 DNS 域的多个子域。

**领域分层结构**

为进行跨领域验证而配置多个领域时，需要决定如何将这些领域绑定在一起。可以在这些领域之间建立分层关系，以便提供到相关域的自动路径。当然，必须正确配置分层链中的所有领域。自动路径可以减轻管理负担。但是，如果域有许多层，您可能不想使用缺省路径，因为它需要太多事务。

您也可以选择直接建立连接。当两个分层领域之间存在的层太多或不存在分层关系时，直接连接最有用。必须在使用连接的所有主机上的 /etc/krb5/krb5.conf 文件中定义连接。因此，还需要执行一些其他工作。有关介绍，请参见[Kerberos 领域](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vap/index.html#intro-56)。有关多个领域的配置过程，请参见[配置跨领域验证](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbj/index.html)。

**将主机名映射到领域**

主机名到领域名称的映射在 krb5.conf 文件的 domain\_realm 部分中定义。可以根据需要对整个域和个别的主机定义这些映射。

DNS 还可用于查找有关 KDC 的信息。如果使用 DNS，则会使信息更改变得更加容易，因为每次执行更改时，无需编辑所有客户机上的 krb5.conf 文件。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。

**客户机名称和服务主体名称**

使用 Kerberos 服务时，强烈建议已在所有主机上配置并运行 DNS 服务。如果使用 DNS，则必须在所有主机或未在任何主机上启用它。如果 DNS 可用，则主体应包含每台主机的全限定域名 (Fully Qualified Domain Name, FQDN)。例如，如果主机名是 boston，DNS 域名是 example.com，领域名称是 EXAMPLE.COM，则该主机的主体名称应为 host/boston.example.com@EXAMPLE.COM。本书中的示例要求对每台主机配置 DNS 并且使用 FQDN。

包含主机的 FQDN 的主体名称应与 /etc/resolv.conf 文件中说明 DNS 域名的字符串匹配。指定主体的 FQDN 时，Kerberos 服务要求 DNS 域名必须为小写字母。DNS 域名可以包含大小写字母，但在创建主机主体时只可以使用小写字母。例如，DNS 域名为 example.com、Example.COM 还是任何其他变体并不重要。主机的主体名称仍为 host/boston.example.com@EXAMPLE.COM。

Kerberos 服务可以在没有运行 DNS 服务的情况下运行。但是，一些主要功能（例如，与其他领域通信的功能）将不能工作。如果未配置 DNS，则可以将简单的主机名用作实例名称。在此情况下，主体将为 host/boston@EXAMPLE.COM。如果稍后启用 DNS，则必须删除并替换 KDC 数据库中的所有主机主体。

此外，还配置了服务管理工具，以便未运行 DNS 服务时，不会启动许多守护进程或命令。已将 kdb5\_util、kadmind 和 kpropd 守护进程以及 kprop 命令配置为依赖于 DNS 服务。要充分利用使用 Kerberos 服务和 SMF 时可用的功能，必须在所有主机上配置 DNS。

**KDC 端口和管理服务端口**

缺省情况下，端口 88 和端口 750 用于 KDC，而端口 749 用于 KDC 管理守护进程。可以使用不同的端口号。但是，如果更改端口号，则必须在每台客户机上更改 /etc/services 文件和 /etc/krb5/krb5.conf 文件。此外，还必须更新每个 KDC 上的 /etc/krb5/kdc.conf 文件。

**从 KDC 数**

与主 KDC 一样，从 KDC 也会为客户机生成凭证。如果主 KDC 不可用，则从 KDC 将提供备份。每个领域应至少有一个从 KDC。可能会需要其他从 KDC，这取决于以下因素：

* 领域中的物理段的个数。通常，应将网络设置为至少每个段都可以独立于领域的其他部分而单独工作。为此，必须能够从每个段访问 KDC。此实例中的 KDC 可以是主 KDC 或从 KDC。
* 领域中的客户机数。通过添加更多从 KDC 服务器，可以减少当前服务器的负荷。

可能会添加太多从 KDC。请记住，必须将 KDC 数据库传播到每台服务器，因此安装的 KDC 服务器越多，更新领域中的数据所用的时间就越长。此外，因为每个从 KDC 都会保存一份 KDC 数据库的副本，所以较多的从 KDC 会增加破坏安全性的风险。

另外，可以很容易地将一个或多个从 KDC 配置为与主 KDC 交换。采用这种方式配置至少一个从 KDC 的优点是：如果主 KDC 由于任何原因出现故障，则可以使用很容易交换为主 KDC 的预配置系统。有关如何配置可交换的从 KDC 的说明，请参见[交换主 KDC 和从 KDC](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcc/index.html)。

**将 GSS 凭证映射到 UNIX 凭证**

对于需要 GSS 凭证名称到 UNIX 用户 ID (user ID, UID) 的映射的 GSS 应用程序（例如 NFS），Kerberos 服务提供了该缺省映射。使用 Kerberos 服务时，GSS 凭证名称相当于 Kerberos 主体名称。缺省映射算法是采用具有一个组成部分的 Kerberos 主体名称，并使用该组成部分（即主体的主名称）来查找 UID。可以使用 /etc/krb5/krb5.conf 中的 auth\_to\_local\_realm 参数在缺省领域或允许的任何领域中进行查找。例如，可以使用口令表将用户主体名称 bob@EXAMPLE.COM 映射到名为 bob 的 UNIX 用户的 UID。但不会映射用户主体名称 bob/admin@EXAMPLE.COM，因为该主体名称包括 admin 的实例部分。如果用户凭证的缺省映射满足要求，则无需填充 GSS 凭证表。在先前的发行版中，需要填充 GSS 凭证表才能使 NFS 服务工作。如果缺省映射不满足要求（例如，如果要映射包含实例部分的主体名称），应使用其他方法。有关更多信息，请参见：

* [如何创建凭证表](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbt/index.html)
* [如何向凭证表中添加单个项](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vbu/index.html)
* [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)
* [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)

**自动将用户迁移到 Kerberos 领域**

可以使用 PAM 框架自动迁移在缺省 Kerberos 领域中没有有效用户帐户的 UNIX 用户。具体而言，将在 PAM 服务的验证栈中使用 pam\_krb5\_migrate 模块。该模块将对服务进行设置，以便每当没有 Kerberos 主体的用户使用其口令成功登录系统时，便会自动为该用户创建 Kerberos 主体。新的主体将使用相同的口令。有关如何使用 pam\_krb5\_migrate 模块的说明，请参见[在 Kerberos 领域中配置用户自动迁移](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vca/index.html)。

**要使用的数据库传播系统**

存储在主 KDC 上的数据库必须定期传播到从 KDC。可以将数据库的传播配置为增量。增量过程只将更新的信息传播到从 KDC，而不是整个数据库。 有关数据库传播的更多信息，请参见[管理 Kerberos 数据库](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcg/index.html)。

如果不使用增量传播，则要解决的首要问题之一是确定更新从 KDC 的频率。需要获取所有客户机可用的最新信息时，必须权衡完成更新所需的时间。

在一个领域中有许多 KDC 的大型安装中，一个或多个从 KDC 可以传播数据，以便以并行方式完成该过程。此策略减少了更新所用的时间，但同时增加了管理领域的复杂性。有关此策略的完整说明，请参见[设置并行传播](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vcr/index.html)。

**领域内的时钟同步**

所有参与 Kerberos 验证系统的主机都必须在指定的最长时间内同步其内部时钟。称为**时钟相位差**的此功能提供了另一种 Kerberos 安全检查方法。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，则请求会被拒绝。

一种同步所有时钟的方法是使用网络时间协议 (Network Time Protocol, NTP) 软件。有关更多信息，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)。还存在其他同步时钟的方法，因此并非一定要使用 NTP。但是，由于存在时钟相位差，所以应使用某种形式的同步来防止访问失败。

**客户机安装选项**

Solaris 10 发行版中的一个新功能是 kclient 安装实用程序。该实用程序可以交互模式或非交互模式运行。在交互模式下，将提示用户输入特定于 Kerberos 的参数值，从而允许用户在安装客户机时更改现有安装。在非交互模式下，将使用先前设置了参数值的文件。此外，可以在非交互模式下使用命令行选项。交互模式和非交互模式所需的步骤都比手动过程所需的步骤少，因此该过程可以更快完成并且不容易出错。有关所有客户机安装过程的说明，请参见[配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc1/index.html)。

**Kerberos 加密类型**

**加密类型**是指定 Kerberos 服务中使用的加密算法、加密模式和散列算法的标识符。Kerberos 服务中的密钥具有关联的加密类型，用于标识服务使用该密钥执行加密操作时要使用的加密算法和模式。以下是 Solaris 10 发行版中支持的加密类型：

* des-cbc-md5
* des-cbc-crc
* des3-cbc-sha1
* arcfour-hmac-md5
* arcfour-hmac-md5-exp
* aes128-cts-hmac-sha1-96

**注 –**

此外，如果安装了非捆绑强加密软件包，则可以将 aes256-cts-hmac-sha1-96 加密类型用于 Kerberos 服务。

如果要更改加密类型，则应在创建新的主体数据库时进行更改。由于 KDC 服务器与 KDC 客户机之间存在交互，所以在现有数据库上更改加密类型很困难。除非您要重新创建数据库，否则不要设置这些参数。有关更多信息，请参阅[使用 Kerberos 加密类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ver/index.html)。

**注 –**

如果安装了未运行 Solaris 10 发行版的主 KDC，则在升级主 KDC 之前，必须将从 KDC 升级到 Solaris 10 发行版。Solaris 10 主 KDC 将使用新的加密类型，而较早版本的从 KDC 将无法处理这些加密类型。

**SEAM Administration Tool 中的联机帮助 URL**

SEAM Administration Tool 将使用联机帮助 URL，因此应正确定义该 URL，以使“帮助内容“菜单正常工作。可以在任何合适的服务器上安装本手册的 HTML 版本。或者，可以决定使用 [http://docs.sun.com](http://www.oracle.com/technetwork/indexes/documentation/index.html) 中的文档集。

该 URL 是在配置主机以使用 Kerberos 服务时在 krb5.conf 文件中指定的。该 URL 应指向本书的“管理主体和策略（任务）”章中标题为 "SEAM Administration Tool" 的一节。如果存在更适合的位置，可以选择另一个 HTML 页面。

* [*Previous*: 第 20 章 Kerberos 服务介绍](https://docs.oracle.com/cd/E19253-01/819-7061/intro-1/index.html)
* [*Next*: 第 22 章 配置 Kerberos 服务（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/setup-8/index.html)
* © 2010, Oracle Corporation and/or its affiliates