[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 20 章 Kerberos 服务介绍

系统管理指南：安全性服务

* [*Previous*: 第 5 部分 验证服务和安全通信](https://docs.oracle.com/cd/E19253-01/819-7061/authtm-1/index.html)
* [*Next*: 第 21 章 规划 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/seamplan-1/index.html)

**第 20 章 Kerberos 服务介绍**

本章介绍 Kerberos 服务。以下是本章中概述信息的列表：

* [什么是 Kerberos 服务？](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vao/index.html)
* [Kerberos 服务的工作方式](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vap/index.html)
* [Kerberos 安全服务](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vaq/index.html)
* [各种 Kerberos 发行版的组件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2var/index.html)

**什么是 Kerberos 服务？**

**Kerberos 服务**是一种通过网络提供安全事务处理的客户机/服务器体系结构。该服务可提供功能强大的用户验证以及完整性和保密性服务。通过**验证**，可保证网络事务的发送者和接收者的身份真实。该服务还可以检验来回传递的数据的有效性（**完整性**），并在传输过程中对数据进行加密（**保密性**）。 使用 Kerberos 服务，可以安全登录到其他计算机、执行命令、交换数据以及传输文件。此外，该服务还提供**授权**服务，管理员可通过此服务限制对服务和计算机的访问。而且，作为 Kerberos 用户，您还可以控制其他用户对您帐户的访问。

Kerberos 服务是**单点登录**系统，这意味着您对于每个会话只需向服务进行一次自我验证，即可自动保护该会话过程中所有后续事务的安全。服务对您进行验证后，即无需在每次使用基于 Kerberos 的命令（如ftp 或 rsh）或访问 NFS 文件系统上数据时都进行自我验证。因此，无需在每次使用这些服务时都在网络上发送口令（口令在网络上可能会被拦截）。

Solaris Kerberos 服务基于麻省理工学院 (Massachusetts Institute of Technology, MIT) 开发的 Kerberos V5 网络验证协议。因此，使用过 Kerberos V5 产品的用户会感觉对 Solaris 版本非常熟悉。因为 Kerberos V5 协议是网络安全性的**实际**行业标准，所以 Solaris 版本可提高与其他系统的互操作性。换句话说，因为可在使用 Kerberos V5 协议的系统中使用 Solaris Kerberos 服务，所以该服务甚至允许在异构网络上进行安全事务处理。此外，该服务还会在各个域之间以及单个域内提供验证和安全服务。

通过 Kerberos 服务可灵活运行 Solaris 应用程序。可以将该服务配置为允许同时向网络服务（如 NFS 服务、telnet 和 ftp）发出基于 Kerberos 的请求和非基于 Kerberos 的请求。因此，即使当前 Solaris 应用程序运行的系统上未启用 Kerberos 服务，这些程序仍能工作。当然，也可以将 Kerberos 服务配置为仅允许基于 Kerberos 的网络请求。

Kerberos 服务提供了一种安全机制，通过该安全机制，在使用采用通用安全服务应用程序编程接口 (Generic Security Service Application Programming Interface, GSS-API) 的应用程序时，可使用 Kerberos 提供验证、完整性和保密性服务。但是，如果开发了其他安全机制，则应用程序无需继续承诺使用 Kerberos 服务。因为该服务设计为以模块形式集成到 GSS-API 中，所以使用 GSS-API 的应用程序可以利用最好地满足其需求的任何安全机制。

**Kerberos 服务的工作方式**

以下概述了 Kerberos 验证系统。有关更详细的说明，请参见[Kerberos 验证系统的工作方式](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vep/index.html)。

从用户的角度来看，启动 Kerberos 会话后，Kerberos 服务通常不可见。一些命令（如 rsh 或 ftp）也是如此。初始化 Kerberos 会话通常仅包括登录和提供 Kerberos 口令。

Kerberos 系统的工作围绕**票证**的概念展开。票证是一组标识用户或服务（如 NFS 服务）的电子信息。正如您的驾驶证可标识您的身份并表明您的驾驶级别一样，票证也可标识您的身份以及您的网络访问权限。执行基于 Kerberos 的事务时（例如，远程登录到另一台计算机），您将透明地向**密钥分发中心** (KDC) 发送票证请求。KDC 将访问数据库以验证您的身份，然后返回授予您访问其他计算机的权限的票证。“透明”意味着您无需显式请求票证。请求是在执行 rlogin 命令过程中进行的。因为只有通过验证的客户机可以获取特定服务的票证，所以其他客户机不能以虚假身份使用 rlogin。

票证具有一些与其关联的属性。例如，票证可以是**可转发的**，这意味着它可以在其他计算机上使用，而不必进行新的验证。票证也可以是**以后生效的**，这意味着它要到指定时间后才会生效。票证的使用方式（例如，如何指定允许哪些用户获取哪些类型的票证）由**策略**设置。策略在安装或管理 Kerberos 服务时确定。

**注 –**

您可能会经常看到术语**凭证**和**票证**。在更为广泛的 Kerberos 范围内，两者通常可互换使用。但是，从技术上讲，凭证指的是票证和会话的**会话密钥**。[使用 Kerberos 获取服务访问权限](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2veq/index.html)中对此区别进行了更详细的说明。

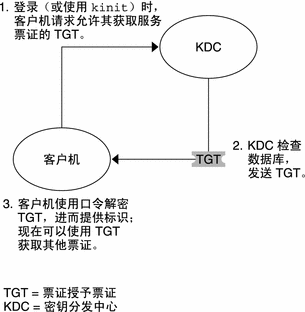
以下各节将进一步说明 Kerberos 验证过程。

**初始验证：票证授予票证**

Kerberos 验证分为两个阶段：允许进行后续验证的初始验证以及所有后续验证自身。

下图显示了如何进行初始验证。

**图 20–1 Kerberos 会话的初始验证**



1. 客户机（用户或 NFS 等服务）通过从密钥分发中心 (Key Distribution Center, KDC) 请求**票证授予票证** (Ticket-Granting Ticket, TGT) 开始 Kerberos 会话。此请求通常在登录时自动完成。

要获取特定服务的其他票证，需要票证授予票证。票证授予票证类似于护照。与护照一样，票证授予票证可标识您的身份并允许您获取多个“签证”，此处的“签证”（票证）不是用于外国，而是用于远程计算机或网络服务。与护照和签证一样，票证授予票证和其他各种票证具有有限的生命周期。区别在于基于 Kerberos 的命令会通知您拥有护照并为您取得签证。您不必亲自执行该事务。

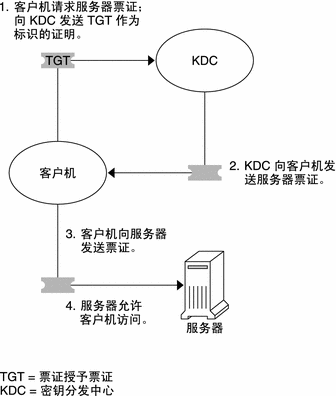
与票证授予票证类似的另一种情况是可以在四个不同的滑雪场使用的三天滑雪入场卷。只要入场券未到期，您就可以在决定要去的任意一个滑雪场出示入场卷，并获取该滑雪场提供的缆车票。获取缆车票后，即可在该滑雪场随意滑雪。如果第二天去另一个滑雪场，您需要再次出示入场卷，并获取新滑雪场的另一张缆车票。区别在于基于 Kerberos 的命令会通知您拥有周末滑雪入场卷，并会为您取得缆车票。因此，您不必亲自执行该事务。

1. KDC 可创建票证授予票证，并采用加密形式将其发送回客户机。客户机使用其口令来解密票证授予票证。
2. 拥有有效的票证授予票证后，只要该票证授予票证未到期，客户机便可以请求所有类型的网络操作（如 rlogin 或 telnet）的票证。此票证的有效期通常为几个小时。每次客户机执行唯一的网络操作时，都将从 KDC 请求该操作的票证。

**后续 Kerberos 验证**

客户机收到初始验证后，每个后续验证都按下图所示的模式进行。

**图 20–2 使用 Kerberos 验证获取对服务的访问权**



1. 客户机通过向 KDC 发送其票证授予票证作为其身份证明，从 KDC 请求特定服务（例如，远程登录到另一台计算机）的票证。
2. KDC 将该特定服务的票证发送到客户机。

例如，假定用户 joe 要访问已通过要求的 krb5 验证共享的 NFS 文件系统。 由于该用户已经通过了验证（即，该用户已经拥有票证授予票证），因此当其尝试访问文件时，NFS 客户机系统将自动透明地从 KDC 获取 NFS 服务的票证。

例如，假定用户 joe 在服务器 boston 上使用 rlogin。由于该用户已经通过了验证（即，该用户已经拥有票证授予票证），所以在运行 rlogin 命令时，该用户将自动透明地获取票证。该用户使用此票证可随时远程登录到 boston，直到票证到期为止。如果 joe 要远程登录到计算机 denver，则需要按照步骤 1 获取另一个票证。

1. 客户机将票证发送到服务器。

使用 NFS 服务时，NFS 客户机会自动透明地将 NFS 服务的票证发送到 NFS 服务器。

1. 服务器允许此客户机进行访问。

从这些步骤来看，服务器似乎并未与 KDC 通信。但服务器实际上与 KDC 进行了通信，并向 KDC 注册了其自身，正如第一台客户机所执行的操作。为简单起见，该部分已省略。

**Kerberos 远程应用程序**

用户（如 joe）可以使用的基于 Kerberos 的（即 "Kerberized"）命令包括：

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

这些应用程序与同名的 Solaris 应用程序相同。但是，它们已扩展为使用 Kerberos 主体来验证事务，因此会提供基于 Kerberos 的安全性。有关主体的信息，请参见[Kerberos 主体](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vap/index.html#intro-26)。

[Kerberos 用户命令](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vei/index.html)中将进一步介绍这些命令。

**Kerberos 主体**

Kerberos 服务中的客户机由其**主体**标识。主体是 KDC 可以为其指定票证的唯一标识。主体可以是用户（如 joe）或服务（如 nfs 或 telnet）。

根据约定，主体名称分为三个部分：**主名称**、**实例**和**领域**。例如，典型的 Kerberos 主体可以是 joe/admin@ENG.EXAMPLE.COM。在本示例中：

* joe 是主名称。主名称可以是此处所示的用户名或 nfs 等服务。主名称还可以是单词 host，这表示此主体是设置用于提供各种网络服务（如 ftp、rcp、rlogin 等）的服务主体。
* admin 是实例。对于用户主体，实例是可选的；但对于服务主体，实例则是必需的。例如，如果用户 joe 有时充当系统管理员，则他可以使用 joe/admin 将其自身与平时的用户身份区分开来。同样，如果 joe 在两台不同的主机上拥有帐户，则他可以使用两个具有不同实例的主体名称，例如 joe/denver.example.com 和 joe/boston.example.com。请注意，Kerberos 服务会将 joe 和 joe/admin 视为两个完全不同的主体。

对于服务主体，实例是全限定主机名。例如，bigmachine.eng.example.com 就是这种实例。此示例的主名称/实例可以为 ftp/bigmachine.eng.example.com 或 host/bigmachine.eng.example.com。

* ENG.EXAMPLE.COM 是 Kerberos 领域。领域将在 [Kerberos 领域](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vap/index.html#intro-56)中介绍。

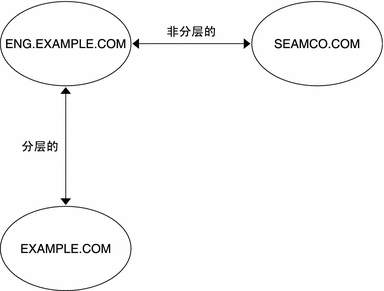
以下都是有效的主体名称：

* joe
* joe/admin
* joe/admin@ENG.EXAMPLE.COM
* ftp/host.eng.example.com@ENG.EXAMPLE.COM
* host/eng.example.com@ENG.EXAMPLE.COM

**Kerberos 领域**

**领域**是定义属于同一**主 KDC** 的一组系统的逻辑网络，类似于域。[图 20–3](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vap/index.html#intro-fig-43) 显示了各领域相互之间的关系。有些领域是分层的，其中，一个领域是另一个领域的超集。另外一些领域是不分层（或“直接”）的，必须定义两个领域之间的映射。Kerberos 服务的一种功能是它允许进行跨领域验证。每个领域只需在其 KDC 中有对应于另一个领域的主体项即可。此 Kerberos 功能称为**跨领域验证**。

**图 20–3 Kerberos 领域**



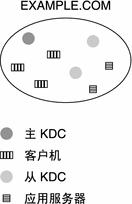
**Kerberos 领域和服务器**

每个领域都必须包括一台用于维护主体数据库的主副本的服务器。此服务器称为**主 KDC 服务器**。此外，每个领域还应至少包含一台**从 KDC 服务器**，该服务器包含主体数据库的多个副本。主 KDC 服务器和从 KDC 服务器都可创建用于建立验证的票证。

领域还可以包含两种其他类型的 Kerberos 服务器。Kerberos 网络的**应用程序服务器**是用于提供对基于 Kerberos 的应用程序（如 ftp、telnet 和 rsh）的访问的服务器。领域还可以包括 **NFS 服务器**，该服务器使用 Kerberos 验证来提供 NFS 服务。如果安装了 SEAM 1.0 或 1.0.1，则领域可能会包括 Kerberos 网络应用程序服务器。

下图显示了一个假设的领域可能包含的内容。

**图 20–4 典型的 Kerberos 领域**



**Kerberos 安全服务**

除了提供安全的用户验证外，Kerberos 服务还会提供两种安全服务：

* **完整性－**正如验证服务可确保网络中客户机的身份真实可靠一样，完整性服务可确保客户机发送的数据有效并且在传输过程中未被篡改。完整性服务通过数据的加密校验和计算来实现。完整性还包括用户验证。
* **保密性－**保密性服务可进一步增强安全性。保密性服务不仅包括对所传输数据的完整性进行验证，还会在传输之前加密数据，防止数据遭到窃听。保密性服务也对用户进行验证。

当前，在属于 Kerberos 服务的各种基于 Kerberos 的应用程序中，仅有 ftp 命令允许用户在运行时（“即时”）更改安全服务。开发者可以设计基于 RPC 的应用程序，以便使用 RPCSEC\_GSS 编程接口来选择安全服务。

**各种 Kerberos 发行版的组件**

许多发行版中已包括 Kerberos 服务组件。Kerberos 服务以及对用于支持 Kerberos 服务的基本操作系统进行的更改最初都使用产品名 "Sun Enterprise Authentication Mechanism"（缩写为 SEAM）来发行。由于 Solaris 软件中包括的 SEAM 产品部件越来越多，因此 SEAM 发行版的内容会相应减少。Solaris 10 发行版中包括了 SEAM 产品的所有部件，因此不再需要 SEAM 产品。由于历史原因，文档中仍存在 SEAM 产品名。

下表说明了每个发行版中包括的组件。各个产品发行版按时间顺序列出。以下各节中对所有组件进行了说明。

表 20–1 Kerberos 发行版内容

| **发行版名称** | **内容** |
| --- | --- |
| Solaris Easy Access Server 3.0 中的 SEAM 1.0 | Solaris 2.6 和 7 发行版中 Kerberos 服务的完整发行版 |
| Solaris 8 发行版中的 Kerberos 服务 | 仅 Kerberos 客户机软件 |
| Solaris 8 Admin Pack 中的 SEAM 1.0.1 | Solaris 8 发行版中的 Kerberos KDC 和远程应用程序 |
| Solaris 9 发行版中的 Kerberos 服务 | 仅 Kerberos KDC 和客户机软件 |
| SEAM 1.0.2 | Solaris 9 发行版中的 Kerberos 远程应用程序 |
| Solaris 10 发行版中的 Kerberos 服务 | 带有增强功能的 Kerberos 服务的完整发行版 |

**Kerberos 组件**

与 MIT 发布的 Kerberos V5 产品类似，Solaris Kerberos 服务也包括以下内容：

* 密钥分发中心 (Key Distribution Center, KDC)（主）：
  + Kerberos 数据库管理守护进程－kadmind。
  + Kerberos 票证处理守护进程－krb5kdc。
* 从 KDC。
* 数据库管理程序－kadmin 和 kadmin.local。
* 数据库传播软件－kprop。
* 用于获取、查看和销毁票证的用户程序－kinit、klist 和 kdestroy。
* 用于更改 Kerberos 口令的用户程序－kpasswd。
* 远程应用程序－ftp、rcp、rdist、rlogin、rsh、ssh 和 telnet。
* 远程应用程序守护进程－ftpd、rlogind、rshd、sshd 和 telnetd。
* 管理实用程序－ktutil 和 kdb5\_util。
* 通用安全服务应用程序编程接口 (Generic Security Service Application Programming Interface, GSS-API)－允许应用程序使用多种安全机制，并且不需要在每次添加新机制时重新编译应用程序。因为 GSS-API 与计算机无关，所以适用于 Internet 上的各种应用程序。使用 GSS-API，应用程序可包括完整性和保密性的安全服务以及验证。
* RPCSEC\_GSS 应用程序编程接口 (Application Programming Interface, API)－允许 NFS 服务使用 Kerberos 验证。RPCSEC\_GSS 是一种安全特性，可提供与要使用的机制无关的安全服务。RPCSEC\_GSS 位于 GSS-API 层的顶部。使用 RPCSEC\_GSS 的应用程序可以使用所有基于可插拔 GSS\_API 的安全机制。
* 多个库。

此外，Solaris Kerberos 服务还包括：

* SEAM 管理工具 (gkadmin)－允许您管理 KDC。借助此基于 JavaTM 技术的 GUI，管理员可以执行通常通过 kadmin 命令执行的任务。
* 可插拔验证模块 (Pluggable Authentication Module, PAM)－允许应用程序使用各种验证机制。使用 PAM 可使登录和注销操作对用户而言透明化。
* 内核模块－为 NFS 提供 GSS-API 和 RPCSEC\_GSS API 的内核实现。

**Solaris 10 发行版中的 Kerberos 增强功能**

Solaris 10 发行版中包括以下 Kerberos 增强功能。其中的一些增强功能已在先前的 Software Express 发行版中引入，并在 Solaris 10 Beta 版中进行了更新。

* 远程应用程序（如 ftp、rcp、rdist、rlogin、rsh、ssh 和 telnet）支持 Kerberos 协议。有关更多信息，请参见每个命令或守护进程的手册页和 [krb5\_auth\_rules(5)](https://docs.oracle.com/docs/cd/E19253-01/816-5175/6mbba7f0t/index.html) 手册页。
* Kerberos 主体数据库现在可以通过增量更新进行传送，而不必每次传送整个数据库。增量传播有以下优点：
  + 增强了跨服务器数据库的一致性
  + 所需资源（网络、CPU 等）更少
  + 更新的传播更加及时
  + 是一种自动传播方法
* 可提供有助于自动配置 Kerberos 客户机的新脚本。此脚本可以帮助管理员迅速而轻松地安装 Kerberos 客户机。有关使用新脚本的过程，请参见[配置 Kerberos 客户机](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vc1/index.html)。此外，有关更多信息，请参见 [kclient(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq5c/index.html) 手册页。
* 在 Kerberos 服务中添加了几种新的加密类型。这几种加密类型提高了安全性，并增强了与支持这几种类型的其他 Kerberos 实现的兼容性。有关更多信息，请参见[使用 Kerberos 加密类型](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2ver/index.html)。新的加密类型包括：
  + AES，该加密类型可用于高速、高安全性的 Kerberos 会话加密。通过加密框架启用 AES。
  + ARCFOUR-HMAC，该加密类型可提供与其他 Kerberos 实现的更好兼容性。
  + 带有 SHA1 的三重 DES (3DES)，该加密类型提高了安全性，还增强了与支持此种加密类型的其他 Kerberos 实现的互操作性。
* KDC 软件、用户命令和用户应用程序现在支持使用 TCP 网络协议。这种增强功能可提供更强健的操作，以及与其他 Kerberos 实现（包括 Microsoft 的 Active Directory）之间更好的互操作性。现在，KDC 可在传统的 UDP 端口和 TCP 端口进行侦听，因此可响应使用 UDP 或 TCP 协议的请求。用户命令和应用程序在将请求发送到 KDC 时，首先尝试使用 UDP，如果该操作失败，则尝试使用 TCP。
* KDC 软件（包括 kinit、klist 和 kprop 命令）中增加了对 IPv6 的支持。缺省情况下，提供对 IPv6 地址的支持。无需更改任何配置参数即可启用 IPv6 支持。kadmin 和 kadmind 命令不支持 IPv6。
* kadmin 命令的多个子命令中添加了新的 **-e** 选项。使用此新选项可以在创建主体过程中选择加密类型。有关更多信息，请参见 [kadmin(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq58/index.html) 手册页。
* 对 pam\_krb5 模块进行扩充是为了使用 PAM 框架来管理 Kerberos 凭证高速缓存。有关更多信息，请参见 [pam\_krb5(5)](https://docs.oracle.com/docs/cd/E19253-01/816-5175/6mbba7f2b/index.html) 手册页。
* 支持自动搜索以下各项：Kerberos KDC、管理服务器、kpasswd 服务器以及使用 DNS 查找的主机（或域名）到领域的映射。此增强功能减少了安装 Kerberos 客户机所需的某些步骤。客户机可通过使用 DNS 而不是通过读取配置文件来找到 KDC 服务器。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。
* 引入了称为 pam\_krb5\_migrate 的新 PAM 模块。该新模块可以帮助那些尚未有 Kerberos 帐户的用户自动向本地 Kerberos 领域迁移。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。
* 现在，~/.k5login 文件可以用于 GSS 应用程序 ftp 和 ssh。有关更多信息，请参见 [gss\_auth\_rules(5)](https://docs.oracle.com/docs/cd/E19253-01/816-5175/6mbba7f05/index.html) 手册页。
* kproplog 实用程序已更新，可输出每个日志项的所有属性名。有关更多信息，请参见 [kproplog(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq5l/index.html) 手册页。
* 使用新的配置文件选项，可以基于每个领域对严格的 TGT 验证功能进行选择性配置。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。
* 通过扩充更改口令实用程序，Solaris Kerberos V5 管理服务器可接受未运行 Solaris 软件的客户机的口令更改请求。有关更多信息，请参见 [kadmind(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq59/index.html) 手册页。
* 重放高速缓存的缺省位置已从基于 RAM 的文件系统移动到 /var/krb5/rcache/ 中的持久性存储器。新位置在系统重新引导时可以避免重放。rcache 代码的性能得到增强。但是，由于使用了持久性存储器，因此整个重放高速缓存的性能有可能降低。
* 现在，可以将重放高速缓存配置为使用文件存储器或仅限于内存的存储器。 有关可为密钥表和凭证高速缓存类型或位置配置的环境变量的更多信息，请参阅 [krb5envvar(5)](https://docs.oracle.com/docs/cd/E19253-01/816-5175/6mbba7f0u/index.html) 手册页。
* 对 Kerberos GSS 机制来说，GSS 凭证表不再是必需的。有关更多信息，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)或 [gsscred(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq2g/index.html)、[gssd(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq2h/index.html) 和 [gsscred.conf(4)](https://docs.oracle.com/docs/cd/E19253-01/816-5174/6mbb98uep/index.html) 手册页。
* Kerberos 实用程序 kinit 和 ktutil 现在都基于 MIT Kerberos 版本 1.2.1。此更改为 kinit 命令添加了新的选项，并为 ktutil 命令添加了新的子命令。有关更多信息，请参见 [kinit(1)](https://docs.oracle.com/docs/cd/E19253-01/816-5165/6mbb0m9iq/index.html) 和 [ktutil(1)](https://docs.oracle.com/docs/cd/E19253-01/816-5165/6mbb0m9j1/index.html) 手册页。
* Solaris Kerberos 密钥分发中心 (KDC) 和 kadmind 现在都基于 MIT Kerberos 版本 1.2.1。现在，KDC 在缺省情况下是一个基于二叉树的数据库，这比当前基于散列的数据库更可靠。有关更多信息，请参见 [kdb5\_util(1M)](https://docs.oracle.com/docs/cd/E19253-01/816-5166/6mbb1kq5e/index.html) 手册页。
* kpropd、kadmind、krb5kdc 和 ktkt\_warnd 守护进程由服务管理工具管理。 可以使用 svcadm 命令对此服务执行管理操作，如启用、禁用或重新启动。 可使用 svcs 命令来查询此服务对应的所有守护进程的状态。有关服务管理工具的概述，请参阅[*《系统管理指南：基本管理》*中的第 14  章 *“管理服务（概述）”*](https://docs.oracle.com/docs/cd/E19253-01/819-6950/6n8u97h20/index.html)。

**Solaris 10 6/06 发行版的 Kerberos 新增功能**

在 Solaris 10 6/06 发行版中，ktkt\_warnd 守护进程可以自动更新凭证，而不是在凭证即将到期时才向用户发出警告。用户必须登录才能自动更新凭证。

**Solaris 9 发行版中的 Kerberos 组件**

Solaris 9 发行版包括[Kerberos 组件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2var/index.html#intro-58)中除远程应用程序外的所有组件。

**SEAM 1.0.2 组件**

SEAM 1.0.2 发行版包括远程应用程序。这些应用程序是 Solaris 9 发行版唯一未包括的部分 SEAM 1.0。远程应用程序的组件如下：

* 客户机应用程序－ftp、rcp、rlogin、rsh 和 telnet
* 服务器守护进程－ftpd、rlogind、rshd 和 telnetd

**Solaris 8 发行版中的 Kerberos 组件**

Solaris 8 发行版仅包括 Kerberos 服务的客户端部分，因此有许多组件未包括在内。借助此产品，运行 Solaris 8 发行版的系统可成为 Kerberos 客户机，而不需要单独安装 SEAM 1.0.1。要使用这些功能，必须安装使用 Solaris Easy Access Server 3.0 或 Solaris 8 Admin Pack 的 KDC、MIT 分发或 Windows 2000。如果没有配置 KDC 来分发票证，则客户端组件将不起作用。此发行版中包括以下组件：

* 用于获取、查看和销毁票证的用户程序－kinit、klist 和 kdestroy。
* 用于更改 Kerberos 口令的用户程序－kpasswd。
* 密钥表管理实用程序－ktutil。
* 可插拔验证模块 (Pluggable Authentication Module, PAM) 的新增功能－允许应用程序使用各种验证机制。使用 PAM 可使登录和注销操作对用户而言透明化。
* GSS\_API 插件－提供 Kerberos 协议和加密支持。
* NFS 客户机和服务器支持。

**SEAM 1.0.1 组件**

SEAM 1.0.1 发行版包括 Solaris 8 发行版中未包括的所有 SEAM 1.0 发行版组件。这些组件包括：

* 密钥分发中心 (Key Distribution Center, KDC)（主）：
  + Kerberos 数据库管理守护进程－kadmind
  + Kerberos 票证处理守护进程－krb5kdc
* 从 KDC。
* 数据库管理程序－kadmin 和 kadmin.local。
* 数据库传播软件－kprop。
* 远程应用程序－ftp、rcp、rlogin、rsh 和 telnet。
* 远程应用程序守护进程－ftpd、rlogind、rshd 和 telnetd。
* 管理实用程序－kdb5\_util。
* SEAM 管理工具 (gkadmin)－允许您管理 KDC。借助此基于 Java 技术的 GUI，管理员可以执行通常通过 kadmin 命令执行的任务。
* 预配置过程－允许您设置用于安装和配置 SEAM 1.0.1 的参数，使用这些参数可以自动进行 SEAM 安装。此过程对于批量安装尤其有用。
* 多个库。

**SEAM 1.0 组件**

SEAM 1.0 发行版包括[Kerberos 组件](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2var/index.html#intro-58)中的所有项以及以下各项：

* 实用程序 (gsscred) 和守护进程 (gssd)－这些程序有助于将 UNIX 用户 ID (user ID, UID) 映射到主体名称。需要使用这些程序是因为 NFS 服务器使用 UNIX UID 来标识用户，而不是使用以不同格式存储的主体名称来标识用户。
* 通用安全服务应用程序编程接口 (Generic Security Service Application Programming Interface, GSS-API)－允许应用程序使用多种安全机制，并且不需要在每次添加新机制时重新编译应用程序。因为 GSS-API 与计算机无关，所以适用于 Internet 上的各种应用程序。使用 GSS-API，应用程序可包括完整性和保密性的安全服务以及验证。
* RPCSEC\_GSS 应用程序编程接口 (Application Programming Interface, API)－允许 NFS 服务使用 Kerberos 验证。RPCSEC\_GSS 是一种安全特性，可提供与要使用的机制无关的安全服务。RPCSEC\_GSS 位于 GSS-API 层的顶部。使用 RPCSEC\_GSS 的应用程序可以使用所有基于可插拔 GSS\_API 的安全机制。
* 预配置过程－允许您设置用于安装和配置 SEAM 1.0.1 的参数，使用这些参数可以自动进行 SEAM 安装。此过程对于批量安装尤其有用。
* [*Previous*: 第 5 部分 验证服务和安全通信](https://docs.oracle.com/cd/E19253-01/819-7061/authtm-1/index.html)
* [*Next*: 第 21 章 规划 Kerberos 服务](https://docs.oracle.com/cd/E19253-01/819-7061/seamplan-1/index.html)
* © 2010, Oracle Corporation and/or its affiliates