[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 23 章 Kerberos 错误消息和疑难解答

系统管理指南：安全性服务

* [*Previous*: 第 22 章 配置 Kerberos 服务（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/setup-8/index.html)
* [*Next*: 第 24 章 管理 Kerberos 主体和策略（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/aadmin-1/index.html)

**第 23 章 Kerberos 错误消息和疑难解答**

本章将分析使用 Kerberos 服务时可能收到的错误消息，另外还针对各种问题提供一些疑难解答提示。以下是本章中错误消息和疑难解答信息的列表。

* [SEAM Administration Tool 错误消息](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd5/index.html#trouble-4)
* [常见的 Kerberos 错误消息 (A-M)](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd5/index.html#trouble-6)
* [常见的 Kerberos 错误消息 (N-Z)](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd5/index.html#trouble-27)
* [krb5.conf 文件的格式存在问题](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd6/index.html#trouble-16)
* [传播 Kerberos 数据库时出现问题](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd6/index.html#trouble-21)
* [挂载基于 Kerberos 的 NFS 文件系统时出现问题](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd6/index.html#trouble-22)
* [以 root 身份进行验证时出现问题](https://docs.oracle.com/cd/E19253-01/819-7061/6n91j2vd6/index.html#trouble-23)
* [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)

**Kerberos 错误消息**

本节介绍有关 Kerberos 错误消息的信息，包括每个错误出现的原因以及解决此错误的方法。

**SEAM Administration Tool 错误消息**

Unable to view the list of principals or policies; use the Name field.

**原因:**

登录时使用的 admin 主体在 Kerberos ACL 文件 (kadm5.acl) 中没有列出权限 (l)。因此，无法查看主体列表或策略列表。

**解决方法:**

必须在 "Name" 字段中键入主体名称和策略名称才能对其进行处理，或者需要使用具有相应权限的主体登录。

JNI: Java array creation failed

JNI: Java class lookup failed

JNI: Java field lookup failed

JNI: Java method lookup failed

JNI: Java object lookup failed

JNI: Java object field lookup failed

JNI: Java string access failed

JNI: Java string creation failed

**原因:**

SEAM Administration Tool (gkadmin) 使用的 Java 本机接口存在严重问题。

**解决方法:**

退出 gkadmin 然后重新启动。如果问题仍然存在，请报告错误。

**常见的 Kerberos 错误消息 (A-M)**

本节按字母顺序 (A-M) 列出了 Kerberos 命令、Kerberos 守护进程、PAM 框架、GSS 接口、NFS 服务和 Kerberos 库的常见错误消息。

All authentication systems disabled; connection refused

**原因:**

此版本的 rlogind 不支持任何验证机制。

**解决方法:**

请确保调用的 rlogind 带有 **-k** 选项。

Another authentication mechanism must be used to access this host

**原因:**

无法进行验证。

**解决方法:**

请确保客户机使用 Kerberos V5 机制进行验证。

Authentication negotiation has failed, which is required for encryption. Good bye.

**原因:**

无法与服务器协商验证。

**解决方法:**

请通过使用 toggle authdebug 命令调用 telnet 命令，启动验证调试并查看调试消息以获取更多线索。另外，请确保具有有效凭证。

Bad krb5 admin server hostname while initializing kadmin interface

**原因:**

在 krb5.conf 文件中为 admin\_server 配置了无效的主机名。

**解决方法:**

请确保在 krb5.conf 文件的 admin\_server 行中为主 KDC 指定了正确的主机名。

Bad lifetime value

**原因:**

提供的生命周期值无效或格式不正确。

**解决方法:**

请确保提供的值与 [kinit(1)](https://docs.oracle.com/docs/cd/E19253-01/816-5165/6mbb0m9iq/index.html) 手册页中的“时间格式”一节相符。

Bad start time value

**原因:**

提供的开始时间值无效或格式不正确。

**解决方法:**

请确保提供的值与 [kinit(1)](https://docs.oracle.com/docs/cd/E19253-01/816-5165/6mbb0m9iq/index.html) 手册页中的“时间格式”一节相符。

Cannot contact any KDC for requested realm

**原因:**

请求的领域中没有 KDC 响应。

**解决方法:**

请确保至少可访问一个 KDC（主 KDC 或从 KDC），或 krb5kdc 守护进程正在 KDC 上运行。有关已配置 KDC 的列表 (kdc = *kdc-name*)，请检查 /etc/krb5/krb5.conf 文件。

Cannot determine realm for host

**原因:**

Kerberos 无法确定主机的领域名称。

**解决方法:**

请确保存在缺省领域名称，或在 Kerberos 配置文件 (krb5.conf) 中设置了域名映射。

Cannot find KDC for requested realm

**原因:**

在请求的领域中找不到 KDC。

**解决方法:**

请确保 Kerberos 配置文件 (krb5.conf) 在 realm 部分中指定了 KDC。

cannot initialize realm *realm\_name*

**原因:**

KDC 可能没有存储文件。

**解决方法:**

请确保 KDC 具有存储文件。否则，请使用 kdb5\_util 命令创建一个存储文件，然后尝试重新启动 krb5kdc 命令。

Cannot resolve KDC for requested realm

**原因:**

Kerberos 无法确定该领域的任何 KDC。

**解决方法:**

请确保 Kerberos 配置文件 (krb5.conf) 在 realm 部分中指定了 KDC。

Cannot reuse password

**原因:**

指定的口令之前已被此主体使用。

**解决方法:**

请选择一个以前尚未选用的口令，至少不要是 KDC 数据库中为每个主体保存的那些口令。此策略由该主体的策略强制执行。

Can't get forwarded credentials

**原因:**

无法建立凭证转发。

**解决方法:**

请确保主体具有可转发的凭证。

Can't open/find Kerberos configuration file

**原因:**

Kerberos 配置文件 (krb5.conf) 不可用。

**解决方法:**

请确保 krb5.conf 文件在正确的位置中可用，并且具有正确的权限。此文件应可由 root 写入，并可由其他用户读取。

Client did not supply required checksum--connection rejected

**原因:**

未与客户机协商使用校验和进行验证。客户机使用的可能是不支持初始连接支持的早期 Kerberos V5 协议。

**解决方法:**

请确保客户机使用的是支持初始连接支持的 Kerberos V5 协议。

Client/server realm mismatch in initial ticket request

**原因:**

在初始票证请求中，客户机与服务器之间的领域不匹配。

**解决方法:**

请确保正在与您通信的服务器与客户机位于同一领域中，或确保领域配置正确。

Client or server has a null key

**原因:**

主体拥有空密钥。

**解决方法:**

请使用 kadmin 的 cpw 命令修改主体，使其拥有非空密钥。

Communication failure with server while initializing kadmin interface

**原因:**

为管理服务器指定的主机（也称为主 KDC）没有运行 kadmind 守护进程。

**解决方法:**

请确保为主 KDC 指定正确的主机名。如果指定了正确的主机名，请确保 kadmind 正在指定的主 KDC 上运行。

Credentials cache file permissions incorrect

**原因:**

您对凭证高速缓存 (/tmp/krb5cc\_ *uid*) 没有相应的读写权限。

**解决方法:**

请确保具有对凭证高速缓存的读写权限。

Credentials cache I/O operation failed *XXX*

**原因:**

Kerberos 在向系统的凭证高速缓存 (/tmp/krb5cc\_*uid*) 进行写入时出现问题。

**解决方法:**

请使用 df 命令确保尚未删除凭证高速缓存，并且设备中还有剩余空间。

Decrypt integrity check failed

**原因:**

您的票证可能无效。

**解决方法:**

请检验下列两种情况：

* 确保您的凭证有效。请使用 kdestroy 销毁票证，然后使用 kinit 创建新票证。
* 确保目标主机的密钥表文件的服务密钥版本正确。请使用 kadmin 查看 Kerberos 数据库中服务主体（例如 host/*FQDN-hostname*）的密钥版本号。另外，请在目标主机上使用 klist **-k**，以确保该主机具有相同的密钥版本号。

Encryption could not be enabled. Goodbye.

**原因:**

无法与服务器协商加密。

**解决方法:**

请通过使用 toggle encdebug 命令调用 telnet 命令，启动验证调试并查看调试消息以获取更多线索。

failed to obtain credentials cache

**原因:**

在 kadmin 初始化过程中，kadmin 尝试获取 admin 主体的凭证时失败。

**解决方法:**

请确保在执行 kadmin 时使用正确的主体和口令。

Field is too long for this implementation

**原因:**

基于 Kerberos 的应用程序所发送的消息太长。如果传输协议是 UDP，则可能会生成此错误。UDP 的缺省最大消息长度是 65535 字节。此外，对通过 Kerberos 服务发送的协议消息中的单个字段也有限制。

**解决方法:**

请检验是否已在 KDC 服务器的 /etc/krb5/kdc.conf 文件中将传输协议限制为 UDP。

GSS-API (or Kerberos) error

**原因:**

此消息是通用的 GSS-API 或 Kerberos 错误消息，可能由几种不同的问题所导致。

**解决方法:**

请检查 /var/krb5/kdc.log 文件，查找出现此错误时记录的更具体的错误消息。

Hostname cannot be canonicalized

**原因:**

Kerberos 无法设置全限定主机名。

**解决方法:**

请确保在 DNS 中定义了该主机名，并且主机名至地址的映射和地址至主机名的映射保持一致。

Illegal cross-realm ticket

**原因:**

发送的票证所跨的领域不正确。领域可能未设置正确的信任关系。

**解决方法:**

请确保使用的领域具有正确的信任关系。

Improper format of Kerberos configuration file

**原因:**

Kerberos 配置文件包含无效项。

**解决方法:**

请确保 krb5.conf 文件中的所有关系后面都跟有 "=" 符号和值。另外，请检验每个子段中的括号是否成对出现。

Inappropriate type of checksum in message

**原因:**

消息中包含无效的校验和类型。

**解决方法:**

请检查在 krb5.conf 和 kdc.conf 文件中指定的有效校验和类型。

Incorrect net address

**原因:**

网络地址不匹配。正在转发的票证中的网络地址与处理该票证的网络地址不同。转发票证时可能会出现此消息。

**解决方法:**

请确保网络地址正确。请使用 kdestroy 销毁票证，然后使用 kinit 创建新票证。

Invalid credential was supplied

Service key not available

**原因:**

凭证高速缓存中的服务票证可能不正确。

**解决方法:**

请在尝试使用此服务之前，销毁当前凭证高速缓存并重新运行 kinit。

Invalid flag for file lock mode

**原因:**

出现内部 Kerberos 错误。

**解决方法:**

请报告错误。

Invalid message type specified for encoding

**原因:**

Kerberos 无法识别基于 Kerberos 的应用程序发送的消息类型。

**解决方法:**

如果使用的基于 Kerberos 的应用程序是由您的站点或供应商开发的，请确保此应用程序正确使用 Kerberos。

Invalid number of character classes

**原因:**

指定的主体口令没有按照主体策略的强制要求包含足够的口令类。

**解决方法:**

请确保指定的口令包含策略要求的最少口令类数。

KADM err: Memory allocation failure

**原因:**

用于运行 kadmin 的内存不足。

**解决方法:**

请释放内存，然后再次尝试运行 kadmin。

KDC can't fulfill requested option

**原因:**

KDC 不允许请求的选项。一种可能是正在请求以后生效或可转发的选项，而 KDC 不允许这些选项。另一种可能是请求了 TGT 更新，但没有可更新的 TGT。

**解决方法:**

请确定是要请求 KDC 不允许的选项，还是请求不可用的票证类型。

KDC policy rejects request

**原因:**

KDC 策略不允许该请求。例如，向 KDC 发出的请求中没有 IP 地址。或者请求了转发，但 KDC 不允许转发。

**解决方法:**

请确保使用带有正确选项的 kinit。如有必要，请修改与主体关联的策略或更改主体的属性以允许该请求。通过使用 kadmin，可以修改策略或主体。

KDC reply did not match expectations

**原因:**

KDC 回复未包含期望的主体名称，或者响应中的其他值不正确。

**解决方法:**

请确保正在与您通信的 KDC 符合 RFC1510，正在发送的请求是 Kerberos V5 请求或该 KDC 可用。

kdestroy: Could not obtain principal name from cache

**原因:**

凭证高速缓存缺失或已损坏。

**解决方法:**

请检查提供的高速缓存位置是否正确。如有必要，请使用 kinit 删除 TGT 并获取新的 TGT。

kdestroy: No credentials cache file found while destroying cache

**原因:**

凭证高速缓存 (/tmp/krb5c\_ *uid*) 缺失或已损坏。

**解决方法:**

请检查提供的高速缓存位置是否正确。如有必要，请使用 kinit 删除 TGT 并获取新的 TGT。

kdestroy: TGT expire warning NOT deleted

**原因:**

凭证高速缓存缺失或已损坏。

**解决方法:**

请检查提供的高速缓存位置是否正确。如有必要，请使用 kinit 删除 TGT 并获取新的 TGT。

Kerberos authentication failed

**原因:**

Kerberos 口令不正确，或该口令可能与 UNIX 口令不同步。

**解决方法:**

如果口令不同步，则必须指定其他口令才能完成 Kerberos 验证。用户可能会忘记其原始口令。

Kerberos V5 refuses authentication

**原因:**

无法与服务器协商验证。

**解决方法:**

请通过使用 toggle authdebug 命令调用 telnet 命令，启动验证调试并查看调试消息以获取更多线索。另外，请确保具有有效凭证。

Key table entry not found

**原因:**

网络应用程序服务器的密钥表文件中不存在服务主体项。

**解决方法:**

请将相应的服务主体添加到服务器的密钥表文件中，以便该文件可提供基于 Kerberos 的服务。

Key version number for principal in key table is incorrect

**原因:**

密钥表文件中主体的密钥版本与 Kerberos 数据库中的版本不同。可能已更改了服务密钥，也可能正在使用旧服务票证。

**解决方法:**

如果服务密钥已被更改（例如通过使用 kadmin），则需要提取新密钥并将其存储在正在运行该服务的主机的密钥表文件中。

或者，您也可能正在使用具有较旧密钥的旧服务票证。在这种情况下，可能需要运行 kdestroy 命令，然后再次运行 kinit 命令。

kinit: gethostname failed

**原因:**

本地网络配置中的错误导致 kinit 失败。

**解决方法:**

请确保主机配置正确。

login: load\_modules: can not open module /usr/lib/security/pam\_krb5.so.1

**原因:**

Kerberos PAM 模块可能缺失，也可能该模块不是有效的可执行二进制文件。

**解决方法:**

请确保 Kerberos PAM 模块位于 /usr/lib/security 目录中，并且是有效的可执行二进制文件。另外，请确保 /etc/pam.conf 文件包含 pam\_krb5.so.1 的正确路径。

Looping detected inside krb5\_get\_in\_tkt

**原因:**

Kerberos 多次尝试获取初始票证，但均失败。

**解决方法:**

请确保至少有一个 KDC 正在响应验证请求。

Master key does not match database

**原因:**

未从包含主密钥的数据库创建装入的数据库转储。主密钥位于 /var/krb5/.k5.*REALM* 中。

**解决方法:**

请确保装入的数据库转储中的主密钥与 /var/krb5/.k5. *REALM* 中的主密钥匹配。

Matching credential not found

**原因:**

未找到与请求匹配的凭证。凭证高速缓存中没有请求需要的凭证。

**解决方法:**

请使用 kdestroy 销毁票证，然后使用 kinit 创建新票证。

Message out of order

**原因:**

使用顺序保密性发送的消息到达时顺序混乱。某些消息可能已在传输过程中丢失。

**解决方法:**

应重新初始化 Kerberos 会话。

Message stream modified

**原因:**

计算出的校验和与消息校验和不匹配。消息在传输过程中可能已被修改，这表明存在安全泄露。

**解决方法:**

请确保消息在网络中正确发送。由于此消息还可表明消息在发送过程中被篡改，因此请使用 kdestroy 销毁票证，然后重新初始化所使用的 Kerberos 服务。

**常见的 Kerberos 错误消息 (N-Z)**

本节按字母顺序 (N-Z) 列出了 Kerberos 命令、Kerberos 守护进程、PAM 框架、GSS 接口、NFS 服务和 Kerberos 库的常见错误消息。

No credentials cache file found

**原因:**

Kerberos 无法找到凭证高速缓存 (/tmp/krb5cc\_*uid*)。

**解决方法:**

请确保该凭证文件存在并且可以读取。否则，请再次尝试执行 kinit。

No credentials were supplied, or the credentials were unavailable or inaccessible

No credential cache found

**原因:**

用户的凭证高速缓存不正确或不存在。

**解决方法:**

用户应在尝试启动服务之前运行 kinit。

No credentials were supplied, or the credentials were unavailable or inaccessible

No principal in keytab matches desired name

**原因:**

尝试验证服务器时出现错误。

**解决方法:**

请确保主机或服务主体位于服务器的密钥表文件中。

Operation requires “*privilege*” privilege

**原因:**

正在使用的 admin 主体未在 kadm5.acl 文件中配置相应的权限。

**解决方法:**

请使用具有相应权限的主体。或者，请通过修改 kadm5.acl 文件来配置所使用的主体，使其具有相应的权限。通常，名称中包含 /admin 的主体具有相应的权限。

PAM-KRB5 (auth): krb5\_verify\_init\_creds failed: Key table entry not found

**原因:**

远程应用程序尝试在本地 /etc/krb5/krb5.keytab 文件中读取主机的服务主体，但不存在任何主体。

**解决方法:**

请将主机的服务主体添加到主机的密钥表文件中。

Password is in the password dictionary

**原因:**

指定的口令位于正在使用的口令字典中。您选择的口令不适合用作口令。

**解决方法:**

请选用包含混合口令类的口令。

Permission denied in replay cache code

**原因:**

无法打开系统的重放高速缓存。首次运行服务器时所使用的用户 ID 可能与当前的用户 ID 不同。

**解决方法:**

请确保重放高速缓存具有相应的权限。重放高速缓存存储在运行基于 Kerberos 的服务器应用程序的主机上。对于非 root 用户，重放高速缓存文件称为 /var/krb5/rcache/rc\_*service\_name*\_ *uid*。对于 root 用户，重放高速缓存文件称为 /var/krb5/rcache/root/rc\_ *service\_name*。

Protocol version mismatch

**原因:**

很可能向 KDC 发送了 Kerberos V4 请求。Kerberos 服务仅支持 Kerberos V5 协议。

**解决方法:**

请确保应用程序使用的是 Kerberos V5 协议。

Request is a replay

**原因:**

请求已发送到此服务器并进行了处理。票证可能已被盗用，并且其他用户正在尝试重新使用这些票证。

**解决方法:**

请等待几分钟，然后重新发出请求。

Requested principal and ticket don't match

**原因:**

您正在连接的服务主体与您所拥有的服务票证不匹配。

**解决方法:**

请确保 DNS 正常运行。如果使用的是其他供应商的软件，请确保该软件使用的主体名称正确。

Requested protocol version not supported

**原因:**

很可能向 KDC 发送了 Kerberos V4 请求。Kerberos 服务仅支持 Kerberos V5 协议。

**解决方法:**

请确保应用程序使用的是 Kerberos V5 协议。

Server refused to negotiate authentication, which is required for encryption. Good bye.

**原因:**

远程应用程序无法接受或已配置为不接受来自客户机的 Kerberos 验证。

**解决方法:**

请提供可以协商验证的远程应用程序，或配置该应用程序以使用相应标志来打开验证。

Server refused to negotiate encryption. Good bye.

**原因:**

无法与服务器协商加密。

**解决方法:**

请通过使用 toggle encdebug 命令调用 telnet 命令，启动验证调试并查看调试消息以获取更多线索。

Server rejected authentication (during sendauth exchange)

**原因:**

您正在尝试与其通信的服务器拒绝验证。此错误通常出现在 Kerberos 数据库传播过程中。一些常见的原因可能是 kpropd.acl 文件、DNS 或密钥表文件存在问题。

**解决方法:**

如果在运行 kprop 以外的应用程序时收到此错误，请检查服务器的密钥表文件是否正确。

The ticket isn't for us

Ticket/authenticator don't match

**原因:**

票证与验证者不匹配。请求中的主体名称可能与服务主体的名称不匹配，因为发送票证使用的是主体的 FQDN 名称，而服务期望非 FQDN 名称，反之亦然。

**解决方法:**

如果在运行 kprop 以外的应用程序时收到此错误，请检查服务器的密钥表文件是否正确。

Ticket expired

**原因:**

票证时间已到期。

**解决方法:**

请使用 kdestroy 销毁票证，然后使用 kinit 创建新票证。

Ticket is ineligible for postdating

**原因:**

主体不允许其票证以后生效。

**解决方法:**

请使用 kadmin 修改主体以允许以后生效。

Ticket not yet valid

**原因:**

以后生效的票证仍然无效。

**解决方法:**

请使用正确的日期创建新票证，或等待当前票证生效。

Truncated input file detected

**原因:**

操作中使用的数据库转储文件不是完整的转储文件。

**解决方法:**

请重新创建转储文件，或使用其他数据库转储文件。

Unable to securely authenticate user ... exit

**原因:**

无法与服务器协商验证。

**解决方法:**

请通过使用 toggle authdebug 命令调用 telnet 命令，启动验证调试并查看调试消息以获取更多线索。另外，请确保具有有效凭证。

Wrong principal in request

**原因:**

票证中包含无效的主体名称。此错误可能表明 DNS 或 FQDN 存在问题。

**解决方法:**

请确保服务主体与票证中的主体匹配。

**Kerberos 疑难解答**

本节介绍有关 Kerberos 软件的疑难解答信息。

**krb5.conf 文件的格式存在问题**

如果 krb5.conf 文件的格式不正确，telnet 命令将会失败。但是，dtlogin 和 login 命令仍将成功，即使按这些命令的要求指定 krb5.conf 文件也是如此。如果出现此问题，则会显示以下错误消息：

|  |
| --- |
| Error initializing krb5: Improper format of Kerberos configuration |

此外，格式不正确的 krb5.conf 文件还会阻止使用 GSSAPI 的应用程序使用 krb5 机制。

如果 krb5.conf 文件的格式存在问题，则安全性很容易受到破坏。您应首先解决该问题，然后再允许使用 Kerberos 功能。

**传播 Kerberos 数据库时出现问题**

如果传播 Kerberos 数据库失败，请在从 KDC 与主 KDC 之间尝试使用 /usr/bin/rlogin **-x**，反之亦然。

如果 KDC 已设置为限制访问，则会禁用 rlogin，因此无法使用它来解决此问题。要在 KDC 上启用 rlogin，必须启用 eklogin 服务。

|  |
| --- |
| # svcadm enable svc:/network/login:eklogin |

解决此问题后，需要禁用 eklogin 服务。

如果 rlogin 无法运行，则可能是因为 KDC 上的密钥表文件存在问题。如果 rlogin 可以运行，则问题不在于密钥表文件或名称服务，因为 rlogin 和传播软件使用相同的 host/*host-name* 主体。在这种情况下，请确保 kpropd.acl 文件正确。

**挂载基于 Kerberos 的 NFS 文件系统时出现问题**

* 如果挂载基于 Kerberos 的 NFS 文件系统失败，请确保 NFS 服务器上存在 /var/rcache/root 文件。如果该文件系统不属于 root，请将其删除并再次尝试挂载。
* 如果访问基于 Kerberos 的 NFS 文件系统时出现问题，请确保系统和 NFS 服务器上启用了 gssd 服务。
* 如果在尝试访问基于 Kerberos 的 NFS 文件系统时出现 invalid argument 或 bad directory 错误消息，则可能是因为在尝试挂载 NFS 文件系统时未使用全限定 DNS 名称。正在挂载的主机与服务器的密钥表文件中的服务主体的主机名部分不相同。

如果服务器有多个以太网接口，并且已将 DNS 设置为使用“每个接口一个名称”的方案，而不是“每台主机多条地址记录”的方案，则也可能会出现此问题。对于 Kerberos 服务，应为每台主机设置多条地址记录，如下所示 [Ken Hornstein，"Kerberos FAQ"，[<http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>]，访问时间：1998 年 12 月 11 日。] :

my.host.name. A 1.2.3.4

A 1.2.4.4

A 1.2.5.4

my-en0.host.name. A 1.2.3.4

my-en1.host.name. A 1.2.4.4

my-en2.host.name. A 1.2.5.4

4.3.2.1 PTR my.host.name.

4.4.2.1 PTR my.host.name.

4.5.2.1 PTR my.host.name.

在本示例中，此设置允许引用服务器的密钥表文件中的不同接口和一个服务主体（而非三个服务主体）一次。

**以 root 身份进行验证时出现问题**

如果在尝试成为系统超级用户时验证失败，并且已将 root 主体添加到主机的密钥表文件中，则需要检查两个可能的问题。首先，请确保密钥表文件中的 root 主体具有一个全限定主机名作为其实例。如果具有该名称，请检查 /etc/resolv.conf 文件，以确保系统已正确设置为 DNS 客户机。

**观察从 GSS 凭证到 UNIX 凭证的映射**

为了可以监视凭证映射，请首先在 /etc/gss/gsscred.conf 文件中取消对以下行的注释。

|  |
| --- |
| SYSLOG\_UID\_MAPPING=yes |

然后，指示 gssd 服务从 /etc/gss/gsscred.conf 文件中获取信息。

|  |
| --- |
| # pkill -HUP gssd |

现在，您应该可以在 gssd 请求凭证映射时对其进行监视。如果针对 auth 系统功能将 syslog.conf 文件设置为 debug 严重级别，则可通过 syslogd 记录这些映射。

* [*Previous*: 第 22 章 配置 Kerberos 服务（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/setup-8/index.html)
* [*Next*: 第 24 章 管理 Kerberos 主体和策略（任务）](https://docs.oracle.com/cd/E19253-01/819-7061/aadmin-1/index.html)
* © 2010, Oracle Corporation and/or its affiliates