Red Hat Certificate System 10

发行注记

突出显示与 Red Hat Certificate System 10 相关的功能和更新

Last Updated: 2023-10-26

Red Hat Certificate System 10 发行注记

突出显示与 Red Hat Certificate System 10 相关的功能和更新

法律通告

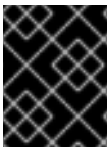
摘要

本发行注记包含与 Red Hat Certificate System 10 相关的信息，如系统要求、安装备注、显著变化和当前问题。在部署 Red Hat Certificate System 10 之前，您应该仔细阅读这些发行注记。

目录

第 1 章 RED HAT CERTIFICATE SYSTEM 10

本节包含有关 Red Hat Certificate System 10 的常规信息，如支持的平台和系统要求、安装说明和弃用。



重要

Red Hat Certificate System 10 软件包及其依赖项通过 **redhat-pki** 模块在 Red Hat Enterprise Linux 8 上提供。

1.1. 先决条件

安装 Red Hat Certificate System 10 需要 Red Hat Enterprise Linux 8。有关如何安装 Red Hat Enterprise Linux 8 的详情，请参考 执行标准的 RHEL 安装。

1.2. 硬件要求

这部分论述了 Red Hat Certificate System 10 的最小和推荐的硬件。请注意，根据您的环境，可能需要更多资源。

1.2.1. 最低要求

- CPU：2 个线程
- RAM：2 GB
- 磁盘空间：20 GB

最低要求基于 Red Hat Enterprise Linux 8 最低要求。详情请查看 Red Hat Enterprise Linux 技术功能和限制。

1.2.2. 推荐的要求

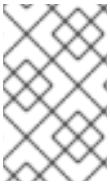
- CPU：4 个或更多线程，AES-NI 支持
- RAM：4 GB 或更高
- 磁盘空间： 80 GB 或更高

1.3. 支持的平台

这部分论述了 Red Hat Certificate System 10 支持的不同服务器平台、硬件、令牌和软件。

1.3.1. 服务器支持

Red Hat Enterprise Linux 8 及更高版本支持运行证书颁发机构(CA)、密钥恢复授权机构(KRA)、在线证书状态协议(OCSP)、令牌密钥服务(TKS)和令牌处理系统(TPS)子系统。支持的 Red Hat Directory Server 版本为 11 及更新的版本。



注意

Red Hat Certificate System 10 支持在认证的虚拟机监控程序上的 Red Hat Enterprise Linux 8 虚拟客户机中运行。详情请查看 哪个 hypervisor 经过认证可运行 RHEL？ 解决方案文章。

1.3.2. 客户端支持

企业级安全客户端(ESC)支持：

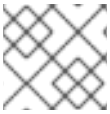
- Red Hat Enterprise Linux 8.
- Red Hat Enterprise Linux 6 和 7 的最新版本。
  虽然这些平台不支持 Red Hat Certificate System 10，但这些客户端可与 Red Hat Certificate System 10 中的 Token Management System (TMS)系统一起使用。

1.3.3. 支持的 Web 浏览器

Red Hat Certificate System 10 支持以下浏览器：

表 1.1. 平台支持的 Web 浏览器

平台	代理服务	最终用户页面
Red Hat Enterprise Linux	Firefox 60 及更新的版本[a]	Firefox 60 及更新的版本
[a] 此 Firefox 版本不再支持用于从浏览器中生成和归档密钥的加密 Web 对象。因此，在这个区域中预期具有有限的功能。		



注意

基于 HTML 的实例配置的唯一完全支持的浏览器是 Mozilla Firefox。

1.3.4. 支持的智能卡

企业安全客户端(ESC)支持全局平台 2.01- 兼容智能卡和 JavaCard 2.1 或更高版本。

证书系统子系统已使用以下令牌进行测试：

- Gemalto TOP IM FIPS CY2 64K 令牌(SCP01)
- Giesecke & Devrient (G&D) SmartCafe the 7.0 (SCP03)
- SafeNet39）Technologies SC-650 (SCP01)

证书系统唯一支持的卡管理器小程序是 **CoolKey** 小程序，这是 Red Hat Certificate System 中的 pki-tps 软件包的一部分。

1.3.5. 支持的硬件安全模块

下表列出了红帽认证系统支持的硬件安全模块(HSM)。

HSM	firmware	设备软件	客户端软件
nCipher nShield Connect XC (High)	nShield_HSM_Firmware-12.72.1	12.71.0	SecWorld_Lin64-12.71.0

HSM	firmware	设备软件	客户端软件
Thales TCT Luna Network HSM Luna-T7	lunafw_update-7.11.1-4	7.11.0-25	610-500244-001_LunaClient-7.11.1-5

1.4. 安装 RHCS 子系统的快速入门

The following procedure describes the prerequisites and the basic installation process for {RHCS} 10.

先决条件

- 最新的 Red Hat Enterprise Linux 8 版本安装有活跃网络同步。有关最新的 iso 镜像，请参阅 下载 Red Hat Enterprise Linux。

流程

1. 使用 Red Hat Subscription Manager (RHSM)将系统注册到客户门户网站帐户中，然后列出此帐户中注册的系统的订阅：

```
$ subscription-manager register
$ subscription-manager list --available --all
```

2. 使用上一步中获得的对应池 ID 为 Red Hat Enterprise Linux 服务器和 Red Hat Certificate System 附加所需的订阅：

```
$ subscription-manager attach --pool=POOL_ID_RHEL_SERVER
$ subscription-manager attach --pool=POOL_ID_CERT_SYSTEM
```

3. 确保 Red Hat Enterprise Linux 具有最新的更新：

```
$ dnf update
```

4. 安装 Directory Server 模块：

```
& dnf module enable 389-ds:1.4 && dnf install 389-ds-base
```

5. 确保指定了实际域名，即 **/etc/resolv.conf** 在 **/etc/hosts** 中设置主机名。

6. 运行目录服务器交互式安装程序并根据需要进行自定义。

```
$ dscreate interactive
```

如需更多信息或其它安装方法，请参阅 Red Hat Directory Server 安装指南 。

7. 安装证书系统软件包和依赖项：

```
$ dnf module enable redhat-pki:10 && dnf install redhat-pki
```

8. 运行 **pkispawn** 脚本来创建和配置子系统实例。在配置任何其他类型的子系统之前，您必须至少安装并完全配置一个 CA 子系统。详情请查看 **pkispawn** 手册页。如果没有选项，pkispawn 以互动模式运行，提示用户获取安装所需的基本信息。

```
$ pkispawn
```

9. 使用正确配置的本地或远程 Mozilla Firefox Web 浏览器访问各种 Red Hat Certificate System 子系统的代理界面。

规划、安装和部署指南 中详细介绍了安装和配置 Red Hat Certificate System 子系统。

其他资源

- 下载 Red Hat Enterprise Linux 。
- 执行标准 RHEL 安装.
- Red Hat Directory Server 安装指南 。
- 规划、安装和部署指南

1.5. 过时的功能

这部分论述了 Red Hat Certificate System 10 中已弃用的功能。

证书系统中的 SCP01 支持已弃用

对安全频道协议 01 (SCP01)的支持已在证书系统 10 中弃用，并可能被删除。红帽建议使用支持 SCP03 的智能卡。

pkiconsole 工具已弃用

在证书系统 10 中，**pkiconsole** 工具将被弃用。

第 2 章 RED HAT ENTERPRISE LINUX 8.6 上的 RED HAT CERTIFICATE SYSTEM 10.4

这部分论述了 RHEL 8.6 上 Red Hat Certificate System 10.4 的显著变化，如突出显示的更新和新功能、重要的程序错误修复以及用户应该了解的当前已知问题。

注意

不支持将 Red Hat Certificate System 降级到以前的次版本。

2.1. CS 10.4 中的更新和新功能

本节记录了 Red Hat Certificate System 10.4 中的新功能和重要更新：

更新 pki-core 软件包中的新功能：

证书系统软件包 rebase 到版本 10.13.0

pki-core、**redhat-pki**、**redhat-pki-theme** 和 **pki-console** 软件包已升级到上游版本 10.13.0，它提供了很多程序错误修复和增强。

2.2. 技术预览

RHCS 中的 ACME 支持作为技术预览提供

通过自动化证书管理环境(ACME)响应器为红帽认证系统(RHCS)提供服务器证书颁发。ACME 响应器支持 ACME v2 协议(RFC 8555)。

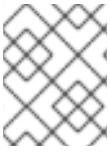
在以前的版本中，用户必须使用证书颁发机构(CA)的专有证书签名请求(CSR)提交例程。例程有时需要证书颁发机构(CA)代理来手动检查请求并颁发证书。

RHCS ACME 响应器现在为自动化服务器证书颁发。以及不需要涉及 CA 代理的生命周期管理提供了一个标准的机制。此功能允许 RHCS CA 与现有的证书颁发基础架构集成，来针对公共 CA 进行部署，针对内部 CA 进行开发。

请注意，这个技术预览只包含 ACME 服务器支持。ACME 客户端没有作为这个版本的一部分提供 。另外，这个 ACME 预览不会保留数据或处理用户注册。

请注意，将来的 Red Hat Enterprise Linux 更新可能会破坏 ACME 安装。

如需更多信息，请参阅 ACME 的 IETF 定义 。



注意

请注意，这个功能作为技术预览提供，提供对即将推出的产品功能的早期访问，且还没有在订阅协议中被完全支持。

2.3. CS 10.4 中的程序错误修复

这部分论述了 Red Hat Certificate System 10.4 中修复的、对用户有严重影响的错误。

TPS 现在为 tps-cert-find正确强制实施 Token Profile Separation

在这个版本中，**tps-cert-find** 命令可以正确地限制令牌 ID、用户 ID、状态、日期、根据用户配置文件的条目，与 **tps-token-find** 命令类似。

现在，在 TPS Web UI 上可以正确地显示令牌

在以前的版本中，当通过 **tpsclient** 工具格式化和注册令牌或通过 Web UI 添加令牌时，TPS Web UI 不会看到任何令牌，但调试日志显示成功记录的条目。在这个版本中，Web UI 会正确列出所有令牌。

pki-core 软件包中的程序错误修复：

在写入文件时，pki-server ca-cert-request-show 不再失败

在以前的版本中，**pki-server ca-cert-request-show &lt ;*request_id&gt*; -i *<instance* > -- *output-file <output_file* >** 命令会失败，并显示以下错误： **ERROR: a bytes-like object，而不是 'str'**。在这个版本中，在写入文件前，将证书请求编码为字节。现在，命令应该可以成功导出证书。

2.4. CS 10.4 中已知的问题

这部分论述了用户在 Red Hat Certificate System 10.4 中应该了解的已知问题，以及（如果适用）临时解决方案。

TPS 需要添加匿名绑定 ACI 访问

在以前的版本中，默认允许匿名绑定 ACI，但现在在 LDAP 中被禁用。因此，这可以防止注册或格式化 TPS 智能卡。

要临时解决这个问题，直到修复前，您需要在目录服务器中添加匿名绑定 ACI：

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core 软件包中的已知问题：

因为 auditSigningCert缺少属性，使用 HSM 克隆 KRA 会失败

当使用 HSM 克隆 KRA 时，**auditSigningCert** 信任属性 **u,u,Pu** 应该隐式在 master 和克隆间的 alias DB 中同步。但是，它现在无法在克隆的别名 DB 中复制。因此，使用 HSM 克隆 KRA 会失败，并显示 **auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101)**证书类型没有为应用程序批准。

要临时解决这个问题，您必须在克隆 KRA 的别名 DB 中明确为 **auditSigningCert** 添加 **u,u,Pu** trust 属性，并重新启动实例。例如：

- 在临时解决方案前：

```
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-
topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is invalid: Certificate type not approved for application.
```

- 在临时解决方案后：

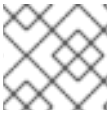
```
# certutil -M -d /var/lib/pki/clone-KRA/alias/ -n 'token:auditSigningCert cert-topology-02-KRA KRA' -t u,u,Pu
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is valid
```

使用带有 --agent-uid pkidbuser 选项的 cert-fix 工具会破坏证书系统

使用带有 **--agent-uid pkidbuser** 选项的 **cert-fix** 工具会破坏证书系统的 LDAP 配置。因此，证书系统可能会变得不稳定，需要手动步骤才能恢复该系统。

第 3 章 RED HAT ENTERPRISE LINUX 8.5 上的 RED HAT CERTIFICATE SYSTEM 10.3

这部分论述了 RHEL 8.5 上 Red Hat Certificate System 10.3 的显著变化，如突出显示的更新和新功能、重要的程序错误修复以及用户应该了解的当前已知问题。



注意

不支持将 Red Hat Certificate System 降级到以前的次版本。

3.1. CS 10.3 中的更新和新功能

本节记录了 Red Hat Certificate System 10.3 中的新功能和重要更新：

更新 pki-core 软件包中的新功能：

证书系统软件包 rebase 到版本 10.12.4

pki-core、**redhat-pki**、**redhat-pki-theme** 和 **pki-console** 软件包已升级到上游版本 10.12.4，它提供了很多程序错误修复和增强。

3.2. 技术预览

RHCS 中的 ACME 支持作为技术预览提供

通过自动化证书管理环境(ACME)响应器为红帽认证系统(RHCS)提供服务器证书颁发。ACME 响应器支持 ACME v2 协议(RFC 8555)。

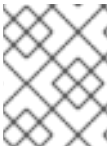
在以前的版本中，用户必须使用证书颁发机构(CA)的专有证书签名请求(CSR)提交例程。例程有时需要证书颁发机构(CA)代理来手动检查请求并颁发证书。

RHCS ACME 响应器现在为自动化服务器证书颁发。以及不需要涉及 CA 代理的生命周期管理提供了一个标准的机制。此功能允许 RHCS CA 与现有的证书颁发基础架构集成，来针对公共 CA 进行部署，针对内部 CA 进行开发。

请注意，这个技术预览只包含 ACME 服务器支持。ACME 客户端没有作为这个版本的一部分提供 。另外，这个 ACME 预览不会保留数据或处理用户注册。

请注意，将来的 Red Hat Enterprise Linux 更新可能会破坏 ACME 安装。

如需更多信息，请参阅 ACME 的 IETF 定义 。



注意

请注意，这个功能作为技术预览提供，提供对即将推出的产品功能的早期访问，且还没有在订阅协议中被完全支持。

3.3. CS 10.3 中的程序错误修复

这部分论述了 Red Hat Certificate System 10.3 中修复的、对用户有严重影响的错误。

pki-core 软件包中的程序错误修复：

使用某些 SCP03 和 SCP01 令牌完成安全频道不再会失败，因为 pcsc-lite、pcsc-lite-ccid、esc

从 Red Hat Certificate System 10.2 开始，**pcsc-lite**、**pcsc-lite-ccid** 和 **esc** 软件包的问题会导致无法完成具有特定 SCP03 和 SCP01 令牌的安全频道。这个问题已通过后续批处理更新解决。

在验证 SubCA 签名证书时，子 CA 双步安装不再失败

在以前的版本中，在启用了 FIPS 的 HSM 环境中安装 SubCA 会失败：且 RSA 或 ECC 选项之一，尝试验证 SubCA 签名证书会返回错误。在这个版本中，pki cli 命令从 **nss-import-cert** 改为 **client-import-cert**，-- **cert ' 改为 '--ca-cert**。因此，CA 签名证书会被正确导入到带有信任的 nssdb 中。另外，如果 pkispawn 失败 **pki-server subsystem-cert-validate** 调用，则此补丁允许提供故障的更多详情，同时允许 **pkispawn** 完成。这允许管理员手动添加 CA 签名证书，虽然上述修复现在应该阻止这个问题发生。

3.4. CS 10.3 中已知的问题

这部分论述了用户在 Red Hat Certificate System 10.3 中应该了解的已知问题，如果适用，临时解决方案。

TPS 需要添加匿名绑定 ACI 访问

在以前的版本中，默认允许匿名绑定 ACI，但现在在 LDAP 中被禁用。因此，这可以防止注册或格式化 TPS 智能卡。

要临时解决这个问题，直到修复前，您需要在目录服务器中添加匿名绑定 ACI：

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

在 TPS Web UI 中无法看到令牌

当通过 **tpsclient** 工具格式化和注册令牌或通过 Web UI 添加令牌时，TPS Web UI 不会看到任何令牌，但调试日志显示成功记录的条目。

要临时解决这个问题，直到修复前，您可以使用 **tps-token-find** 命令列出令牌，例如：

```
# pki -d /opt/pki/certdb/ -c SECret.123 -p 25443 -n 'PKI TPS Administrator for Example.Org'
tps-token-find
```

pki-core 软件包中的已知问题：

因为 auditSigningCert缺少属性，使用 HSM 克隆 KRA 会失败

当使用 HSM 克隆 KRA 时，**auditSigningCert** 信任属性 **u,u,Pu** 应该隐式在 master 和克隆间的 alias DB 中同步。但是，它现在无法在克隆的别名 DB 中复制。因此，使用 HSM 克隆 KRA 会失败，并显示 **auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101)证书类型没有为应用程序批准**。

要临时解决这个问题，您必须在克隆 KRA 的别名 DB 中明确为 **auditSigningCert** 添加 **u,u,Pu** trust 属性，并重新启动实例。例如：

- 在临时解决方案前：

```
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-
```

```
topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is invalid: Certificate type not approved for application.
```

- 在临时解决方案后：

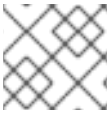
```
# certutil -M -d /var/lib/pki/clone-KRA/alias/ -n 'token:auditSigningCert cert-topology-02-KRA KRA' -t u,u,Pu
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is valid
```

使用带有 --agent-uid pkidbuser 选项的 cert-fix 工具会破坏证书系统

使用带有 **--agent-uid pkidbuser** 选项的 **cert-fix** 工具会破坏证书系统的 LDAP 配置。因此，证书系统可能会变得不稳定，需要手动步骤才能恢复该系统。

第 4 章 RED HAT ENTERPRISE LINUX 8.4 上的 RED HAT CERTIFICATE SYSTEM 10.2

这部分论述了 RHEL 8.4 上的 Red Hat Certificate System 10.2 的显著变化，如突出显示的更新和新功能、重要的程序错误修复以及用户应该了解的当前已知问题。



注意

不支持将 Red Hat Certificate System 降级到以前的次版本。

4.1. CS 10.2 中的更新和新功能

本节记录了 Red Hat Certificate System 10.2 中的新功能和重要的更新：

更新 pki-core 软件包中的新功能：

证书系统软件包 rebase 到版本 10.10.5

pki-core、**redhat-pki**、**redhat-pki-theme** 和 **pki-console** 软件包已升级到上游版本 10.10.5，它提供了很多程序错误修复和增强。

4.2. 技术预览

RHCS 中的 ACME 支持作为技术预览提供

通过自动化证书管理环境(ACME)响应器为红帽认证系统(RHCS)提供服务器证书颁发。ACME 响应器支持 ACME v2 协议(RFC 8555)。

在以前的版本中，用户必须使用证书颁发机构(CA)的专有证书签名请求(CSR)提交例程。例程有时需要证书颁发机构(CA)代理来手动检查请求并颁发证书。

RHCS ACME 响应器现在为自动化服务器证书颁发。以及不需要涉及 CA 代理的生命周期管理提供了一个标准的机制。此功能允许 RHCS CA 与现有的证书颁发基础架构集成，来针对公共 CA 进行部署，针对内部 CA 进行开发。

请注意，这个技术预览只包含 ACME 服务器支持。ACME 客户端没有作为这个版本的一部分提供 。另外，这个 ACME 预览不会保留数据或处理用户注册。

请注意，将来的 Red Hat Enterprise Linux 更新可能会破坏 ACME 安装。

如需更多信息，请参阅 ACME 的 IETF 定义 。

注意

请注意，这个功能作为技术预览提供，提供对即将推出的产品功能的早期访问，且还没有在订阅协议中被完全支持。

4.3. CS 10.2 中的程序错误修复

这部分论述了 Red Hat Certificate System 10.2 中修复的、对用户有严重影响的错误。

pki-core 软件包中的程序错误修复：

连接到 PKI CA 的 PKI ACME Responder 发布的证书不再会出现 OCSP 验证失败

在以前的版本中，PKI CA 提供的默认 ACME 证书配置集包含一个 OCSP URL 示例，它不指向实际 OCSP 服务。因此，如果将 PKI ACME Responder 配置为使用 PKI CA 签发者，则响应者发布的证书可能会出现 OCSP 验证失败。在这个版本中，删除了 ACME 证书配置集中的硬编码 URL，并添加升级脚本来修复配置集配置文件，如果未自定义该文件。

pki-tools 文件现在位于单个文件夹中

pki-tools 软件包中的以下文件位于单独的 *java-tools* 和 *native-tools* 文件夹中：

- */usr/share/pki/java-tools/DRMTool.cfg*
- */usr/share/pki/java-tools/KRATool.cfg*
- */usr/share/pki/native-tools/setpin.conf*

为了实现一致性，它们现在合并到一个文件夹中：

- */usr/share/pki/tools/DRMTool.cfg*
- */usr/share/pki/tools/KRATool.cfg*
- */usr/share/pki/tools/setpin.conf*

4.4. CS 10.2 中已知的问题

这部分论述了用户在 Red Hat Certificate System 10.2 中应该了解的已知问题，如果适用，临时解决方案。

pcsc-lite、pcsc-lite-ccid 和 esc的已知问题

从 Red Hat Certificate System 10.2 的发行日期起，**pcsc-lite**、**pcsc-lite-ccid** 和 **esc** 软件包的版本存在一个已知问题，目前可用的 esc 软件包可能会导致无法完成具有特定 SCP03 和 SCP01 令牌的安全频道。RHEL 8.4 的批处理更新将提供这些软件包的修正版本。

使用 HSM 克隆 KRA 失败

使用 HSM 克隆 KRA 失败，错误 *auditSigningCert cert-topology-02-KRA KRA 无效： Invalid certificate: (-8101) certificate type not approved for application* in the clone debug log.

在验证 SubCA 签名证书时，子 CA 双步安装会失败

在启用了 FIPS 的 HSM 环境中使用两步安装 SubCA 会失败。使用 RSA 或 ECC 选项之一时，验证 SubCA 签名证书会返回错误。

TPS 需要添加匿名绑定 ACI 访问

在以前的版本中，默认允许匿名绑定 ACI，但现在在 LDAP 中被禁用。因此，这可以防止注册或格式化 TPS 智能卡。

要临时解决这个问题，直到修复前，您需要在目录服务器中添加匿名绑定 ACI：

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core 软件包中的已知问题：

使用带有 --agent-uid pkidbuser 选项的 cert-fix 工具会破坏证书系统

使用带有 **--agent-uid pkidbuser** 选项的 **cert-fix** 工具会破坏证书系统的 LDAP 配置。因此，证书系统可能会变得不稳定，需要手动步骤才能恢复该系统。

第 5 章 RED HAT ENTERPRISE LINUX 8.3 上的 RED HAT CERTIFICATE SYSTEM 10.1

这部分论述了 RHEL 8.3 上 Red Hat Certificate System 10.1 的显著变化，如突出显示的更新和新功能、重要的程序错误修复以及用户应该了解的当前已知问题。

注意

不支持将 Red Hat Certificate System 降级到以前的次版本。

5.1. CS 10.1 中的更新和新功能

本节记录了 Red Hat Certificate System 10.1 中的新功能和重要更新：

证书系统软件包 rebase 到版本 10.9.0

pki-core、**redhat-pki**、**redhat-pki-theme** 和 **pki-console** 软件包已升级到上游版本 10.9.0，它提供了很多程序错误修复和增强。

JSS 现在提供 FIPS 兼容 SSLContext

之前，Tomcat 使用来自 Java 加密架构(JCA)SSLContext 类的 SSLEngine 指令。默认的 SunJSSE 实现不符合联邦信息处理标准(FIPS)，因此 PKI 现在通过 JSS 提供符合 FIPS 的实现。

Server-Side keygen Enrollment

许多较新版本的浏览器删除了为密钥归档生成 PKI 密钥和 CRMF 支持的功能。为了解决这一问题，Red Hat Certificate System 10.1 引入了 Server-Side Keygen 注册机制：密钥会在 KRA 服务器上生成，然后安全地传输至 PKCS the 中的客户端。

注意

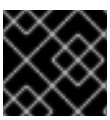
强烈建议您仅将服务器端密钥机制用于加密密钥。

功能高可用性：

- 证书请求密钥在 KRA 上生成（注意：必须安装 KRA 才能使用 CA）
- 配置集默认插件 *serverKeygenUserKeyDefaultImpl* 提供了启用或禁用密钥归档的选择（例如，**enableArchival**）
- 支持 RSA 和 EC 密钥
- 支持手动（代理）批准和自动批准（例如，基于密码的目录）

带有嵌入式签名证书时间戳的 CA 证书转换

Red Hat Certificate System 现在提供证书转换(CT) V1 支持(rfc 6962)的基本版本。它具有从任何可信日志发布带有嵌入式证书时间戳(SCT)的证书，每个部署站点选择包含其 root CA 证书。系统可以配置为支持多个 CT 日志。要使这个功能正常工作，至少需要一个可信的 CT 日志。



重要

部署站点负责建立与可信 CT 日志服务器的信任关系。

更新 pki-core 软件包中的新功能：

现在可以使用检查您的公钥基础架构的整体健康状况

pki-healthcheck 工具提供了几个检查，可帮助您查找和报告可能影响公钥基础架构(PKI)环境的健康状态的错误条件。

PKI 现在支持 RSA PSS (Probabilistic Signature Scheme)签名算法

在这个版本中，PKI 支持 RSA PSS（安全签名方案）签名算法。要启用此功能，请在 **pkispawn** 脚本文件中为给定子系统设置以下行： **pki_use_pss_rsa_signing_algorithm=True**

5.2. 技术预览

RHCS 中的 ACME 支持作为技术预览提供

通过自动化证书管理环境(ACME)响应器为红帽认证系统(RHCS)提供服务器证书颁发。ACME 响应器支持 ACME v2 协议(RFC 8555)。

在以前的版本中，用户必须使用证书颁发机构(CA)的专有证书签名请求(CSR)提交例程。例程有时需要证书颁发机构(CA)代理来手动检查请求并颁发证书。

RHCS ACME 响应器现在为自动化服务器证书颁发。以及不需要涉及 CA 代理的生命周期管理提供了一个标准的机制。此功能允许 RHCS CA 与现有的证书颁发基础架构集成，来针对公共 CA 进行部署，针对内部 CA 进行开发。

请注意，这个技术预览只包含 ACME 服务器支持。ACME 客户端没有作为这个版本的一部分提供 。另外，这个 ACME 预览不会保留数据或处理用户注册。

请注意，将来的 Red Hat Enterprise Linux 更新可能会破坏 ACME 安装。

如需更多信息，请参阅 ACME 的 IETF 定义 。

注意

请注意，这个功能作为技术预览提供，提供对即将推出的产品功能的早期访问，且还没有在订阅协议中被完全支持。

5.3. CS 10.1 中的程序错误修复

这部分论述了 Red Hat Certificate System 10.1 中修复的、对用户有严重影响的错误。

pki-core 软件包中的程序错误修复：

审核员 组现在可用于 TPS 安装

在以前的版本中，LDAP 缺少 TPS 特定审核员的组条目。新的安装现在具有默认的 TPS *审核员* 组。现有实例需要手动 LDAP 流程才能使用此组。

1. 要更正这个问题，请运行 **ldapmodify** 工具来连接到问题中的 LDAP 服务器，并添加缺少的对象：

```
$ ldapmodify -x -D "cn=Directory Manager" -w $PASSWORD << EOF
dn: cn=Auditors,ou=Groups,{rootSuffix}
changeType: add
objectClass: top
```

```
objectClass: groupOfUniqueNames
cn: Auditors
description: People who can read the signed audit logs for TPS
EOF
```

将 **{rootSuffix}** 替换为 TPS 配置文件的基本 DN (**pki_ds_base_dn**)。例如 **dc=tks,dc=pki,dc={DOMAIN...},dc={TLD}**。

因此，现有 TPS 安装可以使用 *审核员* 组以及新的 TPS 安装。

5.4. CS 10.1 中已知的问题

这部分论述了用户在 Red Hat Certificate System 10.1 中应该了解的已知问题，如果适用，临时解决方案。

TPS 需要添加匿名绑定 ACI 访问

在以前的版本中，默认允许匿名绑定 ACI，但现在在 LDAP 中被禁用。因此，这可以防止注册或格式化 TPS 智能卡。

要临时解决这个问题，直到修复前，您需要在目录服务器中添加匿名绑定 ACI：

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core 软件包中的已知问题：

由连接到 PKI CA 的 PKI ACME Responder 发布的证书可能无法通过 OCSP 验证

PKI CA 提供的默认 ACME 证书配置文件包含一个 OCSP URL 示例，它不指向实际 OCSP 服务。因此，如果将 PKI ACME Responder 配置为使用 PKI CA 签发者，则响应者发布的证书可能会失败 OCSP 验证

要临时解决这个问题，您需要在 */usr/share/pki/ca/profiles/ca/acmeServerCert.cfg* 配置文件中将 **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0** 属性设置为空白值：

1. 在 ACME Responder 配置文件中，将行 **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=http://ocsp.example.com** 改为 **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=**
2. 重启服务并重新生成证书

因此，PKI CA 将使用自动生成的 OCSP URL 生成 ACME 证书，指向实际 OCSP 服务。

使用带有 --agent-uid pkidbuser 选项的 cert-fix 工具会破坏证书系统

使用带有 **--agent-uid pkidbuser** 选项的 **cert-fix** 工具会破坏证书系统的 LDAP 配置。因此，证书系统可能会变得不稳定，需要手动步骤才能恢复该系统。

第 6 章 RED HAT ENTERPRISE LINUX 8.2 上的 RED HAT CERTIFICATE SYSTEM 10.0

这部分论述了 RHEL 8.2 上 Red Hat Certificate System 10.0 的显著变化，如突出显示的更新和新功能、重要的程序错误修复以及用户应该了解的当前已知问题。

6.1. CS 10.0 中的更新和新功能

本节记录了 Red Hat Certificate System 10.0 中的新功能和重要的更新：

证书系统软件包 rebase 到版本 10.8.3

pki-core、**redhat-pki**、**redhat-pki-theme** 和 **pki-console** 软件包已升级到上游版本 10.8.3，它比之前的版本提供了很多程序错误修复和增强。

更新 pki-core 软件包中的新功能：

检查您的公钥基础架构的整体健康状况现在作为技术预览提供

pki-healthcheck 工具提供了几个检查，可帮助您查找和报告可能影响公钥基础架构(PKI)环境的健康状态的错误条件。

注意

请注意，这个功能作为技术预览提供，提供对即将推出的产品功能的早期访问，且还没有在订阅协议中被完全支持。

pki subsystem-cert-find 和 pki subsystem-cert-show 命令现在显示证书的序列号

在这个版本中，证书系统中的 **pki subsystem-cert-find** 和 **pki subsystem-cert-show** 命令显示其输出中的证书的序列号。序列号是重要的信息，通常由多个其他命令要求。因此，现在更容易识别证书的序列号。

pki user 和 pki group 命令在证书系统中已被弃用

在这个版本中，新的 **pki <subsystem>-user** 和 **pki <subsystem>-group** 命令替换了证书系统中的 pki **用户和 pki group** 命令。替换的命令仍可以正常工作，但它们显示命令已弃用并引用新命令的消息。

证书系统现在支持系统证书离线续订

有了这个增强，管理员可以使用离线续订功能续订证书系统中配置的系统证书。当系统证书过期时，证书系统无法启动。因为这个改进，管理员不再需要临时解决方案来替换过期的系统证书。

证书系统现在可以为外部 CA 签名使用 SKI 扩展创建 CSR

在这个版本中，证书系统支持为外部证书颁发机构(CA)签名创建带有 Subject Key Identifier (SKI)扩展的证书签名请求(CSR)。某些 CA 需要使用特定值或派生自 CA 公钥的扩展。现在，管理员可以使用传递给 **pkispawn** 工具的配置文件中的 ***pki_req_ski*** 参数来创建带有 SKI 扩展的 CSR。

6.2. 技术预览

RHCS 中的 ACME 支持作为技术预览提供

通过自动化证书管理环境(ACME)响应器为红帽认证系统(RHCS)提供服务器证书颁发。ACME 响应器支持 ACME v2 协议(RFC 8555)。

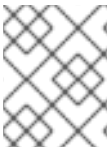
在以前的版本中，用户必须使用证书颁发机构(CA)的专有证书签名请求(CSR)提交例程。例程有时需要证书颁发机构(CA)代理来手动检查请求并颁发证书。

RHCS ACME 响应器现在为自动化服务器证书颁发。以及不需要涉及 CA 代理的生命周期管理提供了一个标准的机制。此功能允许 RHCS CA 与现有的证书颁发基础架构集成，来针对公共 CA 进行部署，针对内部 CA 进行开发。

请注意，这个技术预览只包含 ACME 服务器支持。ACME 客户端没有作为这个版本的一部分提供 。另外，这个 ACME 预览不会保留数据或处理用户注册。

请注意，将来的 Red Hat Enterprise Linux 更新可能会破坏 ACME 安装。

如需更多信息，请参阅 ACME 的 IETF 定义 。



注意

请注意，这个功能作为技术预览提供，提供对即将推出的产品功能的早期访问，且还没有在订阅协议中被完全支持。

6.3. CS 10.0 中的程序错误修复

这部分论述了 Red Hat Certificate System 10.0 中修复的、对用户有严重影响的错误。

pki-core 软件包中的程序错误修复：

pkidestroy 工具现在选择正确的实例

在以前的版本中，pki **destroy --force** 命令默认在一半删除的实例上执行 *pki-tomcat* 实例，无论使用 **-i *instance*** 选项指定的实例名称是什么。因此，这删除了 *pki-tomcat* 实例，而不是预期的实例，**--remove-logs** 选项不会删除预期的实例日志。**pkidestroy** 现在应用正确的实例名称，只删除预期的实例保留。

Nuxwdog 服务不再无法在 HSM 环境中启动 PKI 服务器

在以前的版本中，因为错误，keyutils 软件包没有作为 **pki-core** 软件包的依赖项安装。**另外，在使用硬件安全模块(HSM)的环境中，Nuxwdog watchdog 服务无法启动公钥基础架构(PKI)服务器。这个问题已被解决。因此，所需的 keyutils 软件包现在作为依赖项自动安装，Nuxwdog 会在带有 HSM 的环境中按预期启动 PKI 服务器。**

证书系统不再记录服务启动时 SetAllPropertiesRule 操作警告

在以前的版本中，当服务启动时，证书系统会在 */var/log/messages* 日志文件中记录 SetAllPropertiesRule 操作的警告。这个问题已被解决，上面提到的警告不再被记录。

证书系统现在支持轮转调试日志

在以前的版本中，证书系统使用自定义日志记录框架，它不支持日志轮转。因此，调试日志（如 /var/log/pki/instance_name/ca/debug ）无限期增长。在这个版本中，证书系统使用 java.logging.util 框架，它支持日志轮转。因此，您可以在 /var/lib/pki/instance_name/conf/logging.properties 文件中配置日志轮转。

证书系统 KRA 客户端 正确解析密钥 请求响应

证书系统切换到新的 JSON 库。因此，某些对象的序列化会有所不同，Python 密钥恢复颁发机构 (KRA)客户端无法解析 Key Request 响应。客户端已被修改，以支持使用旧和新的 JSON 库的响应。因此，Python KRA 客户端会正确解析 密钥请求 响应。

6.4. CS 10.0 中已知的问题

这部分论述了用户在 Red Hat Certificate System 10.0 中应该了解的已知问题，如果适用，临时解决方案。

TPS 需要添加匿名绑定 ACI 访问

在以前的版本中，默认允许匿名绑定 ACI，但现在在 LDAP 中被禁用。因此，这可以防止注册或格式化 TPS 智能卡。

要临时解决这个问题，直到修复前，您需要在目录服务器中添加匿名绑定 ACI：

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow
(read, search, compare) userdn="ldap:///anyone";)
EOF
```

pki-core 软件包中的已知问题：

使用带有 --agent-uid pkidbuser 选项的 cert-fix 工具会破坏证书系统

使用带有 --agent-uid pkidbuser 选项的 cert-fix 工具会破坏证书系统的 LDAP 配置。因此，证书系统可能会变得不稳定，需要手动步骤才能恢复该系统。