Red Hat build of Keycloak 24.0

发行注记

Last Updated: 2024-06-28

法律通告

摘要

本指南包含红帽构建的 Keycloak 发行注记。

目录

第 1 章 红帽构建的 KEYCLOAK 24.0

1.1. 概述

红帽非常自信，引入一个名为 Red Hat build of Keycloak 的新身份和访问管理。红帽 Keycloak 构建基于 Keycloak 项目，您可以通过根据常见标准（如 OpenID Connect、OAuth 2.0 和 SAML 2.0）提供 Web SSO 功能来保护 Web 应用程序。红帽构建的 Keycloak 服务器充当 OpenID Connect 或基于 SAML 的用户身份供应商(IdP)，允许您的企业用户目录或第三方 IdP 使用基于标准的安全令牌来保护应用程序。

在保留 Red Hat Single Sign-on 的电源和功能时，Red Hat build of Keycloak 速度更快、更灵活且高效。红帽构建的 Keycloak 是一个使用 Quarkus 构建的应用程序，它为开发人员提供了灵活性和模块化性。Quarkus 提供了一个框架，针对容器优先方法进行了优化，并为开发云原生应用程序提供许多功能。

1.2. 24.0.5 更新

此发行版本包含多个 固定的问题，包括 CVE-2024-4540 的修复。在这个版本中，存在一个使用 PAR（推送的授权请求）影响某些 OIDC 机密客户端的安全问题。如果您将 OIDC 机密客户端与 PAR 一起使用，且您基于在 HTTP 请求正文中的参数发送 **client_id** 和 **client_secret** （在 OIDC 规格中指定的 method **client_secret_post** ）使用客户端验证，则强烈建议您在升级到此版本后轮转客户端的客户端 secret。

1.3. 24.0.4 的更新

此发行版本包括 修复的问题。

1.4. 22.0 更新

如果您要从 Red Hat Single Sign-On 7.6 迁移，红帽构建的 Keycloak 版本 22 中添加了其他新功能。详情请查看 版本 22 发行注记。

1.5. 新功能及功能增强

以下发行注记适用于红帽构建的 Keycloak 24.0.3，这是产品的第一个 24.0 发行版本。

1.5.1. 用户配置文件和进度分析

用户配置集预览功能被提升为完全支持，用户配置集会被默认启用。

以下是此功能的一些亮点：

- 精细控制用户和管理员可以管理的属性，以便您可以防止设置意外属性和值。
- 能够指定管理哪些用户属性，并应在表单上显示给常规用户或管理员。
- 动态表单 - 之前，用户创建或更新其配置集的表单包含四个基本属性，如用户名、电子邮件、名字和姓氏。创建自定义主题需要添加任何属性（或删除一些默认属性）。现在，可能不需要自定义主题，因为用户会根据特定部署的要求准确看到请求的属性。
- 验证 - 禁止为用户属性指定验证器，包括可用于指定最大或最小长度、特定正则表达式或将特定属性限制为 URL 或数字的内置验证器。

- annotations - 用于指定应将特定属性呈现为文本区域、带有指定选项的 HTML 选择或日历或多个其他选项。您还可以将 JavaScript 代码绑定到特定字段，以更改属性的呈现方式并自定义其行为。
- progressive 分析 - 可以指定某些字段是必需的或仅在 **scope** 参数的特定值上提供。这可以有效地允许进度分析。您不再需要在注册过程中询问用户进行二个属性；您可以要求用户根据用户所使用的各个客户端应用程序的要求逐步填写属性。
- 从之前的版本迁移 - 用户配置集现在总是被启用，但它作为不使用此功能的用户运行。您可以从用户配置文件功能中受益，但您不需要使用它们。有关迁移说明，请参阅 升级指南。

用户配置集的第一个发行版本只是一个支持功能的起点和基线，用于提供有关身份管理的更多功能。

有关用户配置文件功能的详情，请查看 服务器管理指南。

1.5.1.1. 破坏对用户配置文件 SPI 的更改

在这个发行版本中，对 User Profile SPI 的更改可能会影响这个 SPI 的现有实现。如需了解更多详细信息，请参阅 升级指南。

1.5.1.2. 对 Freemarker 模板的更改，以根据用户配置集和域呈现页面

在这个发行版本中，以下模板已更新，以便可以根据用户配置集配置设置为 realm 来动态呈现属性：

- **login-update-profile.ftl**
- **register.ftl**
- **update-email.ftl**

如需了解更多详细信息，请参阅 升级指南。

1.5.1.3. 首次通过代理登录时为更新配置集页面新的 Freemarker 模板

在本发行版本中，当用户首次使用 **idp-review-user-profile.ftl** 模板进行身份验证时，服务器会呈现更新配置集页面。

如需了解更多详细信息，请参阅 升级指南。

1.5.2. 多站点主动-被动部署

将红帽构建的 Keycloak 部署到多个独立站点对于某些环境而言至关重要，以提供高可用性和从故障恢复速度。此发行版本支持红帽构建的 Keycloak 的主动 - 被动部署。

首先，请使用 高可用性指南，其中包含一个全面的蓝图，将高度可用的红帽 Keycloak 构建部署到云环境。

1.5.3. 帐户控制台版本 3

帐户控制台版本 3 具有用户配置文件功能的内置支持，它允许管理员在帐户控制台中的用户配置哪些属性，并在登录后直接在其个人帐户页面中访问用户。

如果您使用或扩展此主题的自定义功能，您可能需要执行其他迁移。如需了解更多详细信息，请参阅 升级指南。

帐户控制台版本 2 已被弃用，并将在以后的版本中删除。

1.5.4. 欢迎页面重新设计

欢迎页面会出现在红帽构建的 Keycloak 首次使用时被重新设计。它提供更好的设置体验，并符合 PatternFly 的最新版本。简化的页面布局仅包含注册第一个管理用户的表单。完成注册后，用户将直接发送到管理控制台。

如果您使用自定义主题，您可能需要更新它以支持新的欢迎页面。详情请参阅 升级指南。

1.5.5. 增强的反向代理设置

现在，可以使用新的 **--proxy -headers** 选项单独启用 **Forwarded 或 X** -Forwardedjpeg 标头的解析。详情请查看使用反向代理。原始 **--proxy** 选项现已弃用，并将在以后的发行版本中删除。有关迁移说明，请参阅 升级指南。

1.5.6. OAuth/OIDC 相关改进

1.5.6.1. 轻量级访问令牌支持

此发行版本包含对轻量级访问令牌的支持。因此，您可以为指定客户端具有较小的访问令牌。这些令牌只有几个声明，因此它们更小的原因。请注意，轻量级访问令牌仍然是由 realm 密钥签名的 JWT，仍然包含一些非常基本的声明。

此发行版本引入了一个 **Add to lightweight access token**标记，它包括在一些 OIDC 协议映射程序中。使用此标志指定特定的声明是否应添加到轻量级访问令牌中。默认为 **OFF**，这意味着不会添加大多数声明。

另外，也存在客户端策略 executor。使用它指定特定的客户端请求是否应该使用轻量级访问令牌或常规访问令牌。executor 的替代方法是在客户端高级设置上使用 **Always 使用轻量级访问令牌** 标志，这会导致客户端始终使用轻量级访问令牌。如果您需要更大的灵活性，则 executor 可以作为替代方案。例如，您可以选择默认使用轻量级访问令牌，但仅对指定的 **scope** 参数使用常规令牌。

在以前的版本中，内省端点会自动返回大多数声明，这些声明在访问令牌中可用。现在，大多数协议映射程序都包含一个新的 **Add to token 内省** 交换机。这种添加可以更灵活，因为内省端点可以返回与访问令牌不同的声明。这个变化是"轻量级访问令牌"支持的第一步，因为访问令牌可以省略大量声明，这仍然会被内省端点返回。从之前的版本迁移时，内省端点应返回从访问令牌返回的相同声明，因此升级后，行为应该与默认相同。

如需了解更多详细信息，请参阅使用轻量级访问令牌。

1.5.6.2. OAuth 2.1 支持

此发行版本包含可选的 OAuth 2.1 支持。本发行版本中引入了新的客户端策略配置集，管理员可以使用它来确保客户端和特定的客户端请求符合 OAuth 2.1 规范。此发行版本包含机密客户端的专用客户端配置文件，以及用于公共客户端的专用配置集。

如需了解更多详细信息，请参阅 OAuth 2.1 支持。

1.5.6.3. 刷新令牌流中支持的 scope 参数

从这个版本开始，支持 OAuth2/OIDC 端点用于令牌刷新的 **scope** 参数。使用此参数请求比最初授予的范围较小的访问令牌，这意味着您无法增加访问令牌范围。此范围限制不会影响刷新令牌的范围。这个功能可以正常工作，如 OAuth2 规格中所述。

如需了解更多详细信息，请参阅 服务器管理指南。

1.5.6.4. 用于安全重定向 URI 的客户端策略 executor

引入了一个新的客户端策略 executor **secure-redirect-uris-enforcer**。使用它来限制客户端可以使用哪些重定向 URI。例如，您可以指定客户端重定向 URI 无法具有通配符，应该只来自特定域，必须兼容 OAuth 2.1，以此类推。

如需了解更多详细信息，请参阅 客户端策略。

1.5.6.5. 用于强制执行 DPoP 的客户端策略执行器

引入了一个新的客户端策略 executor **dpop-bind-enforcer**。如果启用了 **dpop** preview，您可以使用它来为特定客户端强制执行 DPoP。

如需了解更多详细信息，请参阅 客户端策略。

1.5.6.6. 支持 EdDSA

您可以创建 EdDSA 域密钥，并将它们用作各种客户端的签名算法。例如，您可以使用这些密钥为令牌签名，或使用已签名 JWT 进行客户端身份验证。此功能包括红帽构建的 Keycloak 本身为客户端断言（用于对第三方身份提供程序的 **private_key_jwt** 身份验证）签名的身份代理。

如需了解更多详细信息，请参阅配置 Realm 密钥

1.5.6.7. JavaKeystore 供应商支持的 EC 密钥

提供域密钥的供应商 **JavaKeystoreProvider** 现在除了之前支持的 RSA 密钥外还支持 EC 密钥。

如需了解更多详细信息，请参阅配置 Realm 密钥

1.5.6.8. 在对身份提供程序使用 private_key_jwt 身份验证时，将 X509 thumbprint 添加到 JWT

现在，当使用由私钥签名的 **JWT 进行客户端身份验证时，OIDC 身份提供程序现在向 JWT 选项添加 X.509** 标头。这个选项可用于与 Azure AD 等某些身份提供程序的互操作性，这需要 JWT 上存在 thumbprint。

如需了解更多详细信息，请参阅 集成身份提供程序。

1.5.6.9. OAuth Grant Type SPI

红帽构建的 Keycloak 代码库包括了一个内部更新，用于引入 OAuth Grant Type SPI。在这个版本中，在引入红帽构建的 Keycloak OAuth 2 令牌端点支持的自定义授权类型时，这个更新提供了额外的灵活性。

如需了解更多详细信息，请参阅 授权服务。

1.5.6.10. FAPI 2 草案支持

红帽构建的 Keycloak 具有新的客户端配置集 **fapi-2-security-profile** 和 **fapi-2-message-signing**，这样可确保红帽构建的 Keycloak 强制实施与客户端通信时的最新 FAPI 2 草案规范的合规性。

如需了解更多详细信息，请参阅 客户端策略。

1.5.6.11. DPoP preview 支持

红帽构建的 Keycloak 具有预览以支持应用程序层(DPoP)上的 OAuth 2.0 Demonating proof-of-Possession。

1.5.6.12. OAuth 2.0 设备授权流的功能标志

OAuth 2.0 设备授权流现在包含一个功能标记，因此您可以轻松禁用此功能。此功能仍然默认启用。

如需了解更多详细信息，请参阅 设备授权授权。

1.5.7. 身份验证

1.5.7.1. 支持 Passkeys

红帽构建的 Keycloak 支持 Passkeys。

Passkey 注册和验证是由 WebAuthn 的功能实现的。因此，红帽构建的 Keycloak 用户可以通过现有的 WebAuthn 注册和验证进行 Passkey 注册和验证。

同步的 Passkeys 和 device-bound Passkeys 都可用于 Same-Device 和 Cross-Device 身份验证。但是，Passkeys 操作成功取决于用户的环境。确保在 环境中 哪些操作可以成功。

1.5.7.2. Webauthn 改进

Webauthn 策略包含一个新字段： **Extra Origins**。它提供更好的与非 Web 平台的互操作性（例如，原生移动应用程序）。

1.5.7.3. 您已登录

此发行版本解决了用户在多个浏览器标签页中打开的登录页面时的问题，并在一个浏览器标签页中进行身份验证。当用户试图在另一个浏览器标签页中进行身份验证时，会出现一条消息： **您已登录**。现在，在第一个标签页中进行身份验证后，这个情况已被改进。但是，需要更多改进。例如，当身份验证会话过期并在一个浏览器标签页中重启时，其他浏览器标签页不会自动遵循。

1.5.7.4. 用于指定最大身份验证时间的密码策略

红帽构建的 Keycloak 支持一个新的密码策略，允许您指定用户可在不重新身份验证的情况下更改密码的最长期限。当此密码策略设置为 0 时，用户需要重新进行身份验证以更改帐户控制台中的密码或其他方法。您还可以指定低于默认值 5 分钟的值。

1.5.8. 服务器分发

1.5.8.1. 载入 Shedding 支持

红帽构建的 Keycloak 现在带有 **http-max-queued-requests** 选项，以允许在高负载下正确拒绝传入的请求。详情请查看 服务器指南。

1.5.8.2. RESTEasy Reactive

红帽构建的 Keycloak 已切换到 RESTEasy Reactive。使用 **quarkus-resteasy-reactive** 的应用程序应该仍受益于更好的启动时间、运行时性能和内存占用，即使不使用被动风格/语义。直接依赖于 JAX-RS API 的 SPI 应该与这个更改兼容。依赖于 RESTEasy Classic （包括 **ResteasyClientBuilder** ）的 SPI 将不兼容，并将需要更新。此更新还需要执行诸如 Jersey 等 JAX-RS API 的其他实施。

1.5.9. Keycloak CR

1.5.9.1. Keycloak CR 优化字段

Keycloak CR 现在包含 **startOptimized** 字段，该字段可用于覆盖有关是否为 start 命令使用 **--optimized** 标记的默认假设。因此，您可以在使用自定义 Keycloak 镜像时，使用 CR 来配置构建时间选项。

1.5.9.2. Keycloak CR 资源选项

Keycloak CR 现在允许指定管理 Keycloak 容器计算资源的资源选项。**它提供对使用 Keycloak CR 的 Keycloak 部署独立请求和限制资源的功能，以及使用 Realm Import CR 的域导入作业。**

如果没有指定值，则默认 请求内存 设置为 1700MiB，限值 内存设置为 2GiB。

您可以根据您的要求指定自定义值，如下所示：

```
apiVersion: k8s.keycloak.org/v2alpha1
kind: Keycloak
metadata:
  name: example-kc
spec:
  ...
  resources:
    requests:
      cpu: 1200m
      memory: 896Mi
    limits:
      cpu: 6
      memory: 3Gi
```

如需了解更多详细信息，请参阅 Operator 指南。

1.5.9.3. keycloak CR cache-config-file 选项

Keycloak CR 现在允许使用 cache spec configMapFile 字段指定 cache-config-file 选项，例如：

```
apiVersion: k8s.keycloak.org/v2alpha1
kind: Keycloak
metadata:
  name: example-kc
spec:
  ...
  cache:
    configMapFile:
      name: my-configmap
      key: config.xml
```

1.5.10. 版本的功能

功能现在支持版本控制。为了保持向后兼容性，所有现有功能（包括 帐户2 和帐户3）标记为版本 1。新引入的功能将使用版本控制，这意味着用户可以在所需功能的不同实现之间进行选择。

详情请查看 服务器指南。

1.5.10.1. Keycloak CR Truststores

您还可以使用 Keycloak CR 利用新的服务器端处理信任存储，例如：

```
spec:
 truststores:
   mystore:
     secret:
       name: mystore-secret
   myotherstore:
     secret:
       name: myotherstore-secret
```

目前只支持 Secret。

1.5.10.2. 信任 Kubernetes CA

Kubernetes CA 的证书会自动添加到由 Operator 管理的 Keycloak Pod 的红帽构建中。

1.5.11. 组可扩展性

对于具有多个组和子组的用例，改进了搜索组的性能。有一些改进，允许分页查找子组。

1.5.12. Keycloak JS

1.5.12.1. 在 package.json中使用 exports 字段

红帽构建的 Keycloak JS 适配器现在使用 package.json 中的 exports 字段。这个变化改进了对 Webpack 5 和 Vite 等现代捆绑包的支持，但有一些不可避免的破坏更改。如需了解更多详细信息，请参阅升级指南。

1.5.12.2. 默认启用 PKCE

红帽构建的 Keycloak JS 适配器现在默认将 pkceMethod 选项设置为 S256。这个变化为使用适配器的所有应用程序启用概念验证代码交换(PKCE)。如果您在不支持 PKCE 的系统上使用适配器，您可以将 pkceMethod 选项设置为 false 来禁用它。

1.5.13. 更改密码哈希

在本发行版本中，我们调整了密码散列默认为与密码 存储 的 OWASP 建议 匹配。

作为此更改的一部分，默认密码散列提供程序已从 pbkdf2-sha256 改为 pbkdf2-sha512。另外，基于 pbkdf2 的默认哈希迭代数量也会改变。这个变化意味着更高的安全性与最新建议一致，但这会影响性能。通过将密码策略 hashAlgorithm 和 hashIterations 添加到您的域，可以坚持旧行为。如需了解更多详细信息，请参阅 升级指南。

1.5.14. truststore 的改进

红帽构建的 Keycloak 引入了改进的信任存储配置选项。红帽构建的 Keycloak 信任存储现在在服务器上使用，包括传出连接、mTLS 和数据库驱动程序。您不再需要为各个区域配置单独的信任存储。要配置信任存储，您可以将信任存储文件或证书放在默认的 conf/truststores 中，或使用新的 truststore-paths 配置选项。

详情请查看 服务器指南。

1.5.15. 更多更改

1.5.15.1. SAML 身份提供程序的自动证书管理

现在，可以将 SAML 身份提供程序配置为从 IDP 实体元数据描述符端点自动下载签名证书。要使用新功能，请在提供程序中配置 元数据描述符 URL 选项（发布 IDP 元数据信息的 URL），并将 使用元数据描述符 URL 设置为 ON。证书会自动在该 URL 中下载并缓存在 public-key-storage SPI 中。也可以使用供应商页面中的操作组合从管理控制台重新加载或导入证书。

有关新选项的详情，请参阅 服务器管理指南。

1.5.15.2. 对负载均衡器的非阻塞健康检查

添加了 /lb-check 的新健康检查端点。执行在事件循环中运行，这意味着当红帽构建的 Keycloak 需要处理等待请求队列中的很多请求时，这个检查也会响应过载情况。例如，在多站点部署中，这种行为很有用，以避免切换到负载过重的另一个站点。端点目前正在检查嵌入式和外部 Infinispan 缓存的可用性。以后可能会添加其他检查。

默认不提供此端点。要启用它，请使用 多站点 功能运行 Keyloak。如需了解更多详细信息，请参阅启用和禁用功能。

1.5.15.3. 在 Admin API 和帐户上下文中更改用户表示

在本发行版本中，我们通过将它们移到 base/abstract 类时，对 root 用户属性（如用户名、电子邮件、firstName、lastName 和 locale）进行封装。

此策略在客户端管理属性的方式中提供一致性，并确保它们符合设置为域的用户配置集配置。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.4. 不再支持通过 Admin User API 更新用户时对用户属性进行部分更新

通过 Admin User API 更新用户属性时，在更新用户属性时，您无法执行部分更新，包括 用户名、电子邮件、firstName 和 lastName 等 root 属性。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.5. 后续载入离线会话和远程会话

从这个版本开始，红帽构建的 Keycloak 集群的第一个成员将按顺序加载远程会话，而不是并行加载。如果启用了离线会话预加载，它们也会按顺序加载。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.6. 无法代表另一个已经经过身份验证的用户执行操作

在本发行版本中，如果用户已经验证并且操作绑定到另一个用户，则无法再执行电子邮件验证。例如，如果电子邮件链接绑定到其他帐户，用户无法完成验证电子邮件流。

1.5.15.7. 对电子邮件验证流的更改

在本发行版本中，如果用户试图按照链接来验证电子邮件，并且之前验证了电子邮件，则会显示正确的消息。

此外，还将触发一个新错误(EMAIL_ALREADY_VERIFIED)事件，以指示尝试验证电子邮件。如果链接已被泄漏，您可以使用此事件来跟踪可能的尝试，或警告用户（如果它们无法识别该操作）。

1.5.15.8. 它们的默认本地化文件到 UTF-8 编码

现在，sees 的消息属性文件在 UTF-8 编码中读取，自动回退到 ISO-8859-1 编码。

如需了解更多详细信息，请参阅升级指南。

1.5.15.9. 内存中离线会话生命周期覆盖的配置选项

为降低内存要求，我们引入了一个配置选项，用于缩短导入到 Infinispan 缓存的离线会话。目前，离线会话生命周期覆盖被默认禁用。

如需了解更多详细信息，请参阅 服务器管理指南。

1.5.15.10. Infinispan 指标使用标签进行缓存管理器和缓存名称

当为 Keycloak 的嵌入式缓存启用指标时，指标现在使用缓存管理器的标签和缓存名称。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.11. 用户属性值长度扩展

在这个版本中，Red Hat build of Keycloak 支持按用户属性值的存储和搜索，其比 255 个字符长，这之前是一个限制。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.12. brute 强制保护更改

Brute 保护有几个改进：

1. 当尝试因为 Brute 强制保护而尝试通过 OTP 或恢复代码进行身份验证时，活跃身份验证会

话无效。任何进一步尝试使用该会话进行身份验证都将失败。

2. 在以前的红帽构建的 Keycloak 版本中，管理员必须因为帐户有 Brute Force 攻击而临时或永久选择禁用用户。管理员现在可以在指定数量的临时锁定后永久禁用用户。

3. 属性 failedLoginNotBefore 已添加到 brute-force/users/{userId} 端点中

1.5.15.13. 授权策略

在以前的红帽构建的 Keycloak 版本中，当删除 User、Group 或 Client 策略的最后成员时，也会删除该策略。不幸的是，如果在聚合策略中使用了策略，这可能会导致特权升级。为避免特权升级，effect 策略将不再被删除，管理员需要更新这些策略。

1.5.15.14. 使用 event 替换临时锁定日志

现在，当用户被 brute 强制保护程序暂时锁定时，新的事件 USER_DISABLED_BY_TEMPORARY_LOCKOUT。ID KC-SERVICES0053 的日志已被删除，因为新事件以结构化的形式提供信息。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.15. Cookie 更新

Cookie 处理代码已被重构和改进，包括新的 Cookie 提供程序。这为由红帽构建的 Keycloak 处理的 Cookie 提供更好的一致性，并在需要时引入 Cookie 的配置选项。

1.5.15.16. SAML 用户属性映射程序用于 NameID 现在只建议有效的 NameID 格式

用户属性映射程序用于 NameID 允许将 Name ID Format 选项设置为以下值：

- urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
- urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName

- urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
- urn:oasis:names:tc:SAML:2.0:nameid-format:entity

但是，红帽构建的 Keycloak 不支持接收带有这些 NameIDPolicy 之一的 AuthnRequest 文档，因此不会使用这些映射器。支持的选项已更新为仅包含以下名称 ID 格式：

- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

1.5.15.17. 在容器中运行时的不同 JVM 内存设置

红帽构建的 Keycloak 使用与容器的总内存相对值，而不是为初始和最大堆大小指定硬编码值。JVM 选项 -Xms 和 -Xmx 被 -XX:InitialRAMPercentage 和 -XX:MaxRAMPercentage 替代。

警告

它可以显著影响内存消耗，因此可能需要执行特定的操作。

如需了解更多详细信息，请参阅 升级指南。

1.5.15.18. 弃用的离线会话预加载

红帽构建的 Keycloak 的默认行为是按需加载离线会话。在启动时预加载它们的旧行为现已弃用，因为在启动时预加载它们无法很好地扩展，并增加红帽构建的 Keycloak 内存用量。旧的行为将在以后的发

行版本中被删除。

如需了解更多详细信息，请参阅 升级指南。

1.6. 修复的问题

每个发行版本都包括修复的问题：

- 红帽构建的 Keycloak 24.0.5 修复的问题
- 红帽构建的 Keycloak 24.0.4 修复的问题
- 红帽构建的 Keycloak 24.0.3 修复的问题

1.7. 已知问题

Red Hat Single Sign-On 7.6 OIDC 适配器在 Red Hat build of Keycloak 24.0 中无法正常工作。

当使用红帽构建的 Keycloak 24.0 运行 Red Hat Single Sign-On 7.6 OIDC 适配器时，日志会显示 CODE_TO_TOKEN_ERROR 事件。要临时解决这个问题，请对每个红帽构建的 Keycloak 客户端进行这个更改，该客户端指向由 Red Hat Single Sign-On 7.6 适配器保护的应用程序。

1. 在 Admin Console 中，选择受影响的客户端。
2. 转至 高级 选项卡。
3. 找到 OpenID Connect Compatibility Modes 部分。
4. 将 Exclude Issuer From Authentication Response to ON 切换。

如需更多信息，请参阅 https://issues.redhat.com/browse/RHSSO-3030。

1.8. 支持的配置

有关红帽构建的 Keycloak 24.0 支持的配置，请参阅 支持的配置。

1.9. 组件详情

有关红帽构建的 Keycloak 24.0 支持的组件版本列表，请参阅 组件详情。