Red Hat Single Sign-On 7.6

发行注记

使用 Red Hat Single Sign-On 7.6

Last Updated: 2024-06-05

Red Hat Single Sign-On 7.6 发行注记

使用 Red Hat Single Sign-On 7.6

法律通告

摘要

本指南包括红帽单点登录发行注记

目录

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。有关更多详情，请参阅我们的首席技术官 Chris Wright 提供的消息。

第 1 章 RED HAT SINGLE SIGN-ON 7.6.0.GA

1.1. 概述

红帽很自豪地宣布，红帽单点登录(RH-SSO)版本 7.6 版本。RH-SSO 基于 Keycloak 项目，您可以通过提供基于常见标准（如 OpenID Connect、OAuth 2.0 和 SAML 2.0）的 Web SSO 功能来保护 Web 应用。RH-SSO 服务器充当基于 OpenID Connect 或基于 SAML 的身份供应商(IdP)，允许您的企业用户目录或第三方 IdP 通过基于标准的安全令牌保护应用程序。

注意

Red Hat Single Sign-On for IBM Z 和 IBM Power Systems 只在 OpenShift 环境中被支持。不支持 IBM Z 和 IBM Power Systems 上的裸机安装。

以下注释适用于 RH-SSO 7.6 发行版本。

1.2. 新的或改进的功能

1.2.1. 步骤验证

Red Hat Single Sign-On 现在支持步骤验证。如需了解更多详细信息，请参阅 服务器管理指南。

1.2.2. 客户端 secret 轮转

Red Hat Single Sign-On 现在支持通过客户策略进行客户端 Secret 轮转。这个功能现在作为技术预览提供，并允许为机密客户端提供域策略，以便同时使用最多两个 secret。

如需了解更多详细信息，请参阅 服务器管理指南。

1.2.3. 恢复代码

现在，恢复代码作为进行双因素身份验证的另一种方式可用。

1.2.4. OpenID Connect Logout 提高

对一些修复和增强已被改进，以确保 Red Hat Single Sign-On 现在完全符合所有 OpenID Connect logout 规格：

- OpenID Connect RP-Initiated Logout 1.0
- OpenID Connect Front-Channel Logout 1.0
- OpenID Connect Back-Channel Logout 1.0
- OpenID Connect Session Management 1.0

如需了解更多详细信息，请参阅 服务器管理指南。

1.2.5. WebAuthn 的改进

WebAuthn 不再是一个技术预览功能。现在完全受支持。

另外，Red Hat Single Sign-On 现在支持 WebAuthn id-less 身份验证。此功能允许 WebAuthn 安全密钥在身份验证期间识别用户，只要安全密钥支持 Resident Keys。如需了解更多详细信息，请参阅 服务器管理指南。

1.2.6. 会话限制

Red Hat Single Sign-On 现在支持对用户可以拥有的会话数量的限制。限制可以置于 realm 级别或客户端级别。

如需了解更多详细信息，请参阅 服务器管理指南。

1.2.7. SAML ECP Profile 默认禁用

为了缓解滥用 SAML ECP 配置集的风险，Red Hat Single Sign-On 现在会为未明确允许的所有 SAML 客户端阻止这个流。该配置集可以在客户端配置中使用 *Allow ECP Flow* 标志来启用，请参阅 服务器管理指南。

1.3. LDAP 和 KERBEROS 集成的改进

从 RH-SSO 7.6.9，红帽单点登录支持域中多个 LDAP 提供程序，它支持与同一 Kerberos 域的 Kerberos 集成。当 LDAP 供应商找不到通过 Kerberos/SPNEGO 进行身份验证的用户时，红帽单点登录将绑定到下一个 LDAP 供应商。当单个 LDAP 供应商支持多个 Kerberos 域时，Red Hat Single Sign-On 也具有更好的支持，这些 Kerberos 域相互信任。

1.3.1. 其他改进

- 帐户控制台与最新的 PatternFly 发行版本一致。
- 支持加密的 User Info 端点响应。
- 支持使用加密密钥的 A256GCM 的算法 RSA-OAEP。
- 支持使用 GitHub Enterprise 服务器登录。

1.4. 现有技术预览功能

以下功能继续处于技术预览状态：

- 令牌交换
- 精细的授权权限

1.5. 删除或弃用的功能

这些功能在状态有变化：

- 在 Red Hat Single Sign-On 7.2 中作为技术预览功能引入的跨站点复制不再作为任何 Red Hat SSO 7.x 发行版本中支持的功能提供，包括最新的 RH-SSO 7.6 发行版本。红帽不推荐任何客户在其环境中实施或使用此功能，因为它不被支持。另外，对这个功能的支持例外不再被视为或接受。
  将讨论跨站点复制的新解决方案，并在未来的 Red Hat build of Keycloak (RHBK)中考虑，这是引入的产品，而不是 Red Hat SSO 8。稍后会提供更详细的信息。

- Keycloak CR 中的 **podDisruptionBudget** 字段已弃用，并在 Operator 部署到 OpenShift 4.12 及更高版本中时忽略。作为临时解决方案，请参阅升级指南。
- 弃用的 **upload-script** 功能已被删除。
- 对 Red Hat Enterprise Linux 6(RHEL 6)上的 Red Hat Single Sign-On(RH-SSO)的支持已被弃用，在 RHEL 6 上不支持 RH-SSO 的 7.6 版本。RHEL 6 在 2020 年 11 月 30 日进入 ELS 阶段，RH-SSO 依赖的 Red Hat JBoss Enterprise Application Platform (EAP) 在 EAP 7.4 版本中不再支持 RHEL 6。客户应在 RHEL 7 或 8 版本中部署其 RH-SSO 7.6 升级。
- Spring Boot Adapter 已被弃用，它不包括在 8.0 及更高版本和更高版本的 RH-SSO 版本中。此适配器将在 RH-SSO 7.x 生命周期中维护。用户应迁移到 Spring Security，以便将其 Spring Boot 应用程序与 RH-SSO 集成。
- 从 RPM 安装已弃用。Red Hat Single Sign-On 将继续在 7.x 产品的生命周期内提供 RPM，但不会为下一个主要版本提供 RPM。该产品将继续支持从 ZIP 文件安装并在 OpenShift 中安装。
- Red Hat Single Sign-On for OpenShift on Eclipse OpenJ9 已弃用。但是，OpenShift 上的 Red Hat Single Sign-On 现在支持所有平台（x86、IBM Z 和 IBM Power Systems），如 OpenShift 指南 中所述。有关此变化的详情，请参阅 PPC 和 s390x OpenShift Images 中的 Java 更改 。
- 授权服务 Drools 策略已被删除。

1.6. 修复的问题

有关 RH-SSO 7.5 和 7.6.0 之间修复的问题的详情，请参阅 RHSSO 7.6.0 修复的问题。

在 7.6.0 发布后，我们为 Red Hat Single Sign-On Operator 引入了一个补丁发行版本，以修复阻止使用 Operator 从 7.5.2 升级到 7.6.0 的严重问题。如需了解更多详细信息和注意事项，请参阅升级指南。

1.7. 使用基于 CLIENT_SECRET_POST 的身份验证，修复 PAR 客户端中的安全问题

此发行版本包含 CVE-2024-4540 的修复，这是影响使用 PAR (Pushed 授权请求)的一些 OIDC 机密客户端的重要安全问题。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。

1.8. 已知问题

此发行版本包括以下已知问题：

- KEYCLOAK-18115 - Attempt 以编辑拒绝在 RHSSO 7.4.6 中的属性

1.9. 支持的配置

客户门户网站上 提供了 RH-SSO Server 7.6 的支持功能和配置。

1.10. 组件版本

客户门户网站上 提供了 RH-SSO 7.6 支持的组件版本列表。

1.11. RED HAT OPENSHIFT 的 RED HAT SINGLE SIGN-ON METERING 标签

您可以在 Red Hat Single Sign-On pod 中添加 metering 标签，并使用 OpenShift Metering Operator 检查红帽订阅详情。

注意

不要将 metering 标签添加到 Operator 部署和管理的任何 pod 中。

Red Hat Single Sign-On 可以使用以下 metering 标签：

- **com.redhat.component-name: Red Hat Single Sign-On**
- **com.redhat.component-type: application**
- **com.redhat.component-version: 7.6**
- **com.redhat.product-name: "Red_Hat_Runtimes"**
- **com.redhat.product-version: 2020/Q2**

其他资源

- 在 OpenShift Container Platform 中配置和使用 Metering