



Red Hat Single Sign-On 7.6

入门指南

使用 Red Hat Single Sign-On 7.6

Red Hat Single Sign-On 7.6 入门指南

使用 Red Hat Single Sign-On 7.6

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

本指南帮助您在生产环境中使用 Red Hat Single Sign-On 前对它进行评估。其中包括在单机模式中安装红帽单点登录服务器的说明，创建用于管理用户和应用的帐户和域，以及保护 JBoss EAP 服务器应用的安全。

目录

使开源包含更多	3
第 1 章 安装 RED HAT SINGLE SIGN-ON 的示例实例	4
1.1. 安装 RED HAT SINGLE SIGN-ON 服务器	4
1.2. 为 RED HAT SINGLE SIGN-ON 启用 JAVA 17	5
1.3. 启动 RED HAT SINGLE SIGN-ON 服务器	5
1.4. 创建 ADMIN 帐户	6
1.5. 登录到 ADMIN 控制台	6
第 2 章 创建域和用户	9
2.1. REALMS 和用户	9
2.2. 创建域	9
2.3. 创建用户	10
2.4. 登录到帐户控制台	12
第 3 章 保护示例应用程序	14
3.1. 调整 RED HAT SINGLE SIGN-ON 使用的端口	14
3.2. 安装 JBOSS EAP 客户端适配器	15
3.3. 注册 JBOSS EAP 应用程序	16
3.4. 修改 JBOSS EAP 实例	17
3.5. 安装示例代码来保护应用程序	18

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 安装 RED HAT SINGLE SIGN-ON 的示例实例

这部分论述了如何在单机模式中安装并启动 Red Hat Single Sign-On 服务器，设置初始 admin 用户，并登录到 Red Hat Single Sign-On Admin Console。

其它资源

此安装旨在练习使用红帽单点登录。有关在生产环境中安装和所有产品功能的完整详情，请参阅 [Red Hat Single Sign-On](#) 文档中的其他指南。

1.1. 安装 RED HAT SINGLE SIGN-ON 服务器

对于这个 Red Hat Single Sign-On 实例示例，这个过程涉及独立模式的安装。服务器下载 ZIP 文件包含运行 Red Hat Single Sign-On 服务器的脚本和二进制文件。您可以在 Linux 或 Windows 上安装服务器。

流程

1. 访问[红帽客户门户](#)。
2. 下载 Red Hat Single Sign-On Server: **rh-sso-7.6.zip**
3. 将文件放在您选择的目录中。
4. 使用适当的 **unzip** 实用程序（如 unzip、tar 或 Expand-Archive）解包 ZIP 文件。

Linux/Unix

```
$ unzip rh-sso-7.6.zip  
or  
$ tar -xvzf rh-sso-7.6.tar.gz
```

Windows

```
> Expand-Archive -Path 'C:\Downloads\rh-sso-7.6.zip' -DestinationPath 'C:\Downloads'
```

5. 返回到 [红帽客户门户](#)。
6. 点 **Patches** 选项卡。
7. 下载 Red Hat Single Sign-On 7.6.9 服务器补丁。
将下载的 ZIP 文件放在您选择的目录中。
8. 进入 Red Hat Single Sign-On 服务器的根目录。
9. 启动 JBoss EAP 命令行界面。

Linux/Unix

```
$ ./bin/jboss-cli.sh
```

Windows


```
> .\bin\jboss-cli.bat
```

10. 应用补丁。

```
$ patch apply <path-to-zip>/rh-sso-7.6.9-patch.zip
```

1.2. 为 RED HAT SINGLE SIGN-ON 启用 JAVA 17

如果 Java SE 17 想要用于运行 Red Hat Single Sign-On，则需要额外的步骤。应该运行捆绑的 **enable-elytron-se17.cli** 脚本文件来准备服务器。如果使用较早版本的 Java，则不需要这一步。

先决条件

- 您会在 Red Hat Single Sign-On 服务器安装过程中看到任何错误。

流程

1. 进入 Red Hat Single Sign-On 服务器的根目录。
2. 运行 **jboss-cli** 命令，传递 **enable-elytron-se17.cli** 脚本。

Linux/Unix

```
$ ./bin/jboss-cli.sh --file=docs/examples/enable-elytron-se17.cli
```

Windows

```
> .\bin\jboss-cli.bat --file=docs\examples\enable-elytron-se17.cli
```

1.3. 启动 RED HAT SINGLE SIGN-ON 服务器

您会在安装它的系统中启动服务器。

先决条件

- 您会在 Red Hat Single Sign-On 服务器安装过程中看到任何错误。

流程

1. 转到服务器分发的 **bin** 目录。
2. 运行 **独立** 引导脚本。

Linux/Unix

```
$ cd bin  
$ ./standalone.sh
```

Windows

```
> ...\bin\standalone.bat
```

1.4. 创建 ADMIN 帐户

在使用 Red Hat Single Sign-On 前，您需要创建一个 admin 帐户，用于登录 Red Hat Single Sign-On 管理控制台。

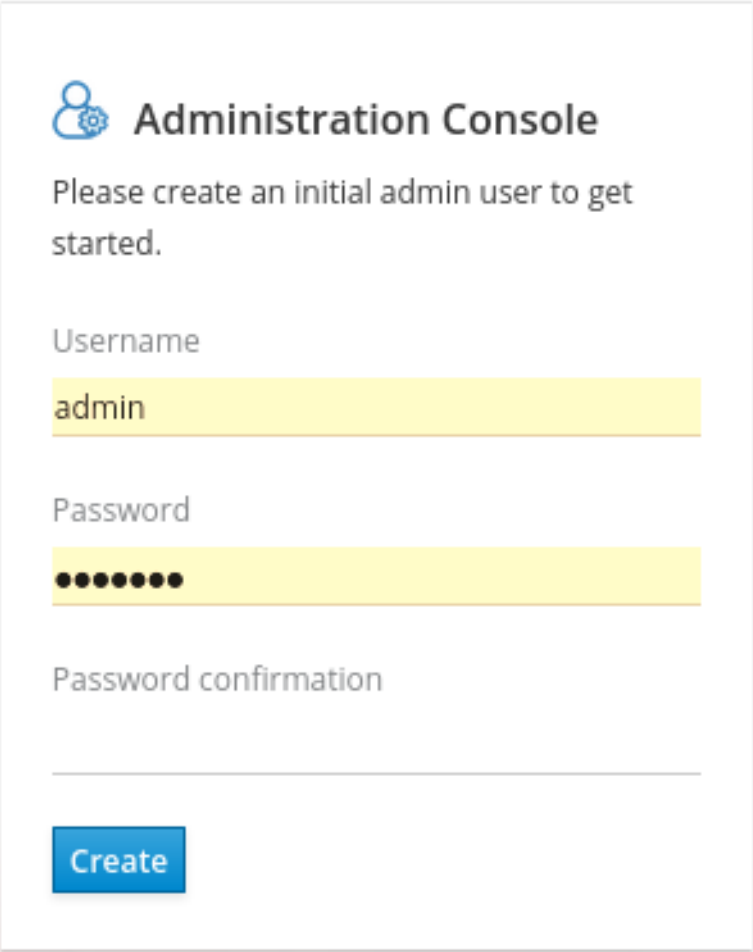
先决条件


- 当您启动 Red Hat Single Sign-On 服务器时，您看到了任何错误。

流程

1. 在您的网页浏览器中访问 <http://localhost:8080/auth>。
欢迎页面将打开，确认服务器正在运行。

欢迎页面



 **Administration Console**

Please create an initial admin user to get started.

Username
admin

Password
●●●●●●

Password confirmation

[Create](#)

2. 输入用户名和密码来创建初始 admin 用户。

1.5. 登录到 ADMIN 控制台

创建初始 admin 帐户后，您可以登录 admin 控制台。在这个控制台中，您可以添加用户并注册应用程序，使其受 Red Hat Single Sign-On 的安全。

先决条件

- 您有一个 admin 帐户，用于 admin 控制台。

流程

1. 点击 **Welcome** 页面上的 **Administration Console** 链接，或直接进入 <http://localhost:8080/auth/admin/>（控制台 URL）。



注意

管理控制台通常被称为 Red Hat Single Sign-On 文档中的短期的管理控制台。

2. 输入您在 **Welcome** 页面上创建的用户名和密码，以打开 **admin 控制台**。

管理控制台登录屏幕

Username or email

admin

Password

●●●●●●

Remember me

Log In

此时会出现管理控制台的初始屏幕。

管理控制台

Master

General Login Keys Email Themes Cache Tokens Client Registration Security Defenses

* Name

Display name

HTML Display name

Frontend URL

Enabled ON

User-Managed Access OFF

Endpoints

Save Cancel

后续步骤

现在，您可以登录到 admin 控制台，可以开始创建域，以供管理员创建用户并为其提供对应用程序的访问权限。如需了解更多详细信息，[请参阅创建域和用户](#)。

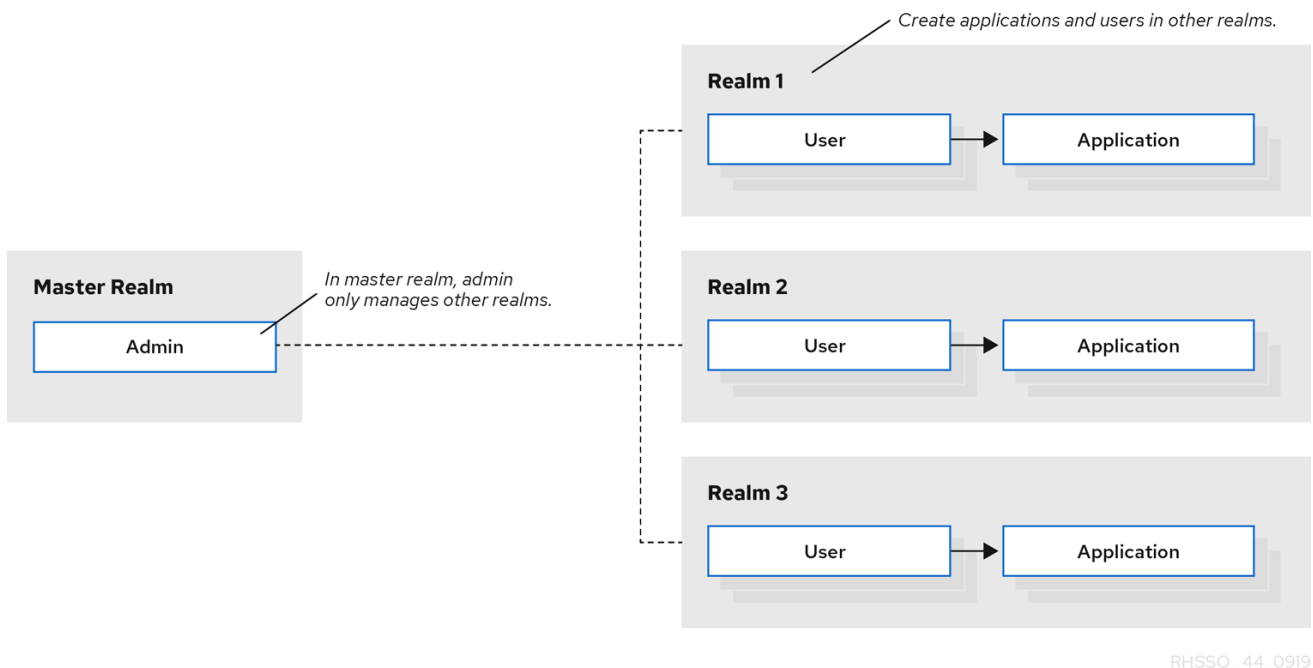
第 2 章 创建域和用户

Red Hat Single Sign-On 管理控制台的第一个使用是创建域并在该域中创建用户。您可以使用该用户登录到新域，并访问所有用户有权访问的内置帐户控制台。

2.1. REALMS 和用户

当您登录到 admin 控制台时，您位于一个 realm 中，这是您管理对象的空间。存在两种类型的域：

- **Master realm** - 首次启动 Red Hat Single Sign-On 时为您创建此域。它包含您在第一次登录时创建的 admin 帐户。您只使用此域来创建其他域。
- **其他域** - 这些域由 master 域中的管理员创建。在这些域中，管理员创建用户和应用程序。应用程序由用户所有。



2.2. 创建域

作为 master 域中的 admin，您将创建管理员创建用户和应用的域。

先决条件

- 安装了 Red Hat Single Sign-On。
- 您有 admin 控制台的初始 admin 帐户。

流程

1. 进入 <http://localhost:8080/auth/admin/>，再使用 admin 帐户登录 Red Hat Single Sign-On 管理控制台。
2. 在 **Master** 菜单中，单击 **Add Realm**。当您登录到 master 域时，此菜单将列出所有其他域。
3. 在 **Name** 字段中输入 **demo**。

新域



注意

realm 名称是区分大小写的，因此请注意您使用的大小写。

- 点 **Create**。
此时会打开主管理控制台页面，域设为 **demo**。

演示域

- 在管理 **master** 域和您刚才创建的域之间的切换，方法是单击 **Select realm** 下拉列表中的条目。

2.3. 创建用户

在 **demo** 域中，您可以为该新用户创建一个新用户和一个临时密码。

流程

- 从菜单中，单击 **Users** 以打开用户列表页面。
- 在空用户列表的右侧，单击 **Add User** 以打开 Add user 页面。
- 在 **Username** 字段中输入名称。

这是唯一的必填字段。

添加用户页面

Users > Add user

Add user

ID

Created At

Username *

Email

First Name

Last Name

User Enabled

Email Verified

Required User Actions

4. 将 电子邮件验证 切换为 **On**，然后单击保存。
新用户的管理页面将打开。
5. 点 **Credentials** 选项卡为新用户设置临时密码。
6. 键入新密码并确认。
7. 点 **Set Password** 将用户密码设置为您指定的新密码。

管理凭证页面

Users > johndoe

Johndoe

Details Attributes **Credentials** Role Mappings Groups Consents Sessions

Manage Credentials

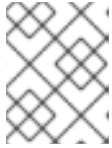
Position	Type	User Label	Data
----------	------	------------	------

Set Password

Password

Password Confirmation

Temporary



注意

此密码是临时的，用户在第一次登录时需要更改密码。如果要创建永久的密码，请将 **Temporary** 开关设置为 **Off**，然后单击 **Set Password**。


2.4. 登录到帐户控制台

realm 中的每个用户都可以访问帐户控制台。您可以使用此控制台更新您的配置集信息并更改凭证。现在，您可以使用您创建的域中的该用户测试登录。

流程

1. 打开用户菜单并选择 **Sign Out**，从管理控制台注销。
2. 进入 <http://localhost:8080/auth/realms/demo/account> 并以您刚刚创建的用户身份登录您的 **demo** 域。
3. 当要求您提供新密码时，请输入一个可以记住的密码。

更新密码

 You need to change your password to activate your account.

New Password

Confirm password

为此用户打开帐户控制台。

帐户控制台

Account >

- Password
- Authenticator
- Sessions
- Applications

Edit Account

* Required fields

Username

Email *

First name *

Last name *

4. 使用任何值填写必填字段，以使用此页面进行测试。

后续步骤

现在，您已准备好进行最终过程，这是保护在 JBoss EAP 上运行的示例应用程序。请参阅 [保护示例应用程序](#)。

第 3 章 保护示例应用程序

现在，您有一个 admin 帐户、一个域和用户，您可以使用 Red Hat Single Sign-On 来保护 JBoss EAP servlet 应用示例。安装 JBoss EAP 客户端适配器，在管理控制台中注册应用程序，修改 JBoss EAP 实例以使用 Red Hat Single Sign-On，并使用带有一些示例代码的红帽单点登录来保护应用。

先决条件

- 您需要调整红帽单点登录使用的端口，以避免与 JBoss EAP 产生端口冲突。

3.1. 调整 RED HAT SINGLE SIGN-ON 使用的端口

本指南中的说明适用于在红帽单点登录服务器相同的计算机上运行 JBoss EAP。在这种情形中，即使 JBoss EAP 捆绑了红帽单点登录，但您不能将 JBoss EAP 用作应用容器。您必须为您 servlet 应用运行单独的 JBoss EAP 实例。

为避免端口冲突，您需要不同的端口来运行 Red Hat Single Sign-On 和 JBoss EAP。

先决条件

- 您有一个 admin 帐户，用于 admin 控制台。
- 您创建了演示域。
- 您在 demo 域中创建了用户。

流程

1. 从红帽客户门户下载 JBoss [EAP 7.3](#)。
2. 解压下载的 JBoss EAP。

```
$ unzip <filename>.zip
```

3. 更改到 Red Hat Single Sign-On root 目录。
4. 为 **jboss.socket.binding.port-offset** 系统属性提供值，启动 Red Hat Single Sign-On 服务器。这个值添加到 Red Hat Single Sign-On 服务器打开的每个端口的基本值中。在本例中，100 是值。

Linux/Unix

```
$ cd bin  
$ ./standalone.sh -Djboss.socket.binding.port-offset=100
```

Windows

```
> ...bin\standalone.bat -Djboss.socket.binding.port-offset=100
```

Windows Powershell

```
> ...bin\standalone.bat -D"jboss.socket.binding.port-offset=100"
```

5. 确认 Red Hat Single Sign-On 服务器正在运行。前往 <http://localhost:8180/auth/admin/>。如果打开了管理控制台，您已准备好安装客户端适配器，使 JBoss EAP 能够与红帽 Sign-On 配合使用。

3.2. 安装 JBOSS EAP 客户端适配器

当 JBoss EAP 和红帽单点登录安装在同一机器上时，JBoss EAP 需要进行一些修改。要进行这个修改，请安装 Red Hat Single Sign-On 客户端适配器。

先决条件

- 已安装 JBoss EAP。
- 如果您自定义了此文件，则具有 `./standalone/configuration/standalone.xml` 文件的备份。

流程

1. 从红帽客户门户下载 EAP 7 的 [客户端适配器](#)。
2. 更改到 JBoss EAP 的根目录。
3. 在此目录中解压下载的客户端适配器。例如：

```
$ unzip <filename>.zip
```

4. 更改到 bin 目录。

```
$ cd bin
```

5. 为您的平台运行适当的脚本。



注意

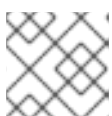
如果您收到 **未找到的文件**，请确保在上一步中使用了 **unzip**。这种提取方法会在正确的位置安装文件。

Linux/Unix

```
$ ./jboss-cli.sh --file=adapter-elytron-install-offline.cli
```

Windows

```
> jboss-cli.bat --file=adapter-elytron-install-offline.cli
```



注意

此脚本对 `.../standalone/configuration/standalone.xml` 文件进行必要的编辑。

6. 启动应用服务器。

Linux/Unix

-

```
$ ./standalone.sh
```

Windows

```
> ...\standalone.bat
```

3.3. 注册 JBOSS EAP 应用程序

现在，您可以在 Red Hat Single Sign-On 管理控制台中定义并注册客户端。

先决条件

- 已安装客户端适配器以用于 JBoss EAP。

流程

1. 使用 admin 帐户登录到 admin 控制台：<http://localhost:8180/auth/admin/>
2. 在左侧下拉列表中，选择 **Demo** realm。
3. 点左侧菜单中的 **Clients** 打开 Clients 页面。

客户端

Client ID	Enabled	Base URL	Actions		
account	True	http://localhost:8080/auth/realms/demo/account/	Edit	Export	Delete
account-console	True	http://localhost:8080/auth/realms/demo/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	http://localhost:8080/auth/admin/demo/console/	Edit	Export	Delete

4. 在右侧，点 **Create**。
5. 在 Add Client 对话框中，通过完成字段来创建名为 **vanilla** 的客户端，如下所示：

添加客户端

Clients > Add Client

Add Client

Import

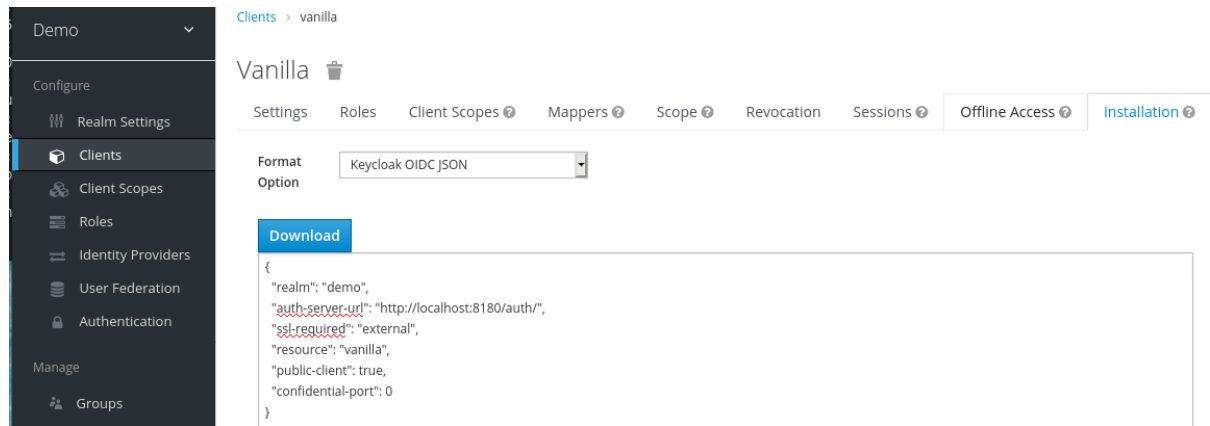
Client ID *

Client Protocol

Root URL

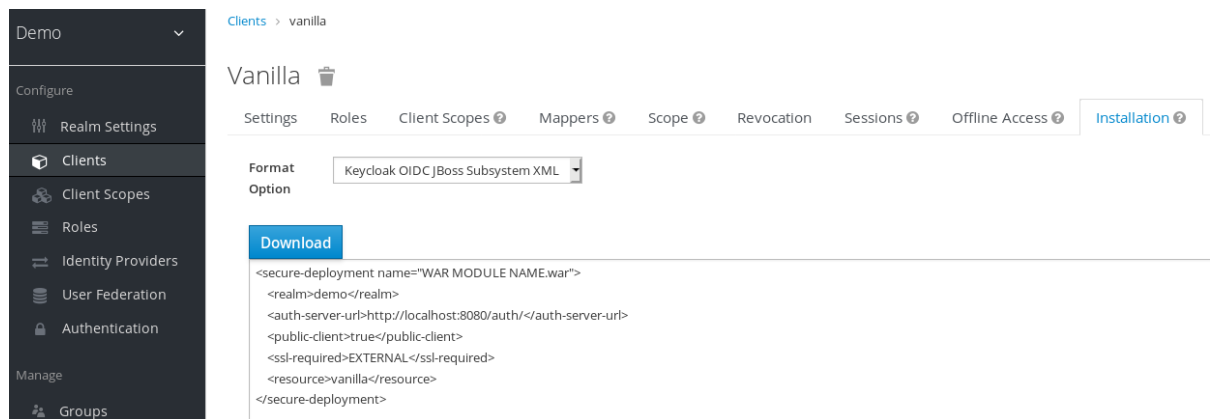
- 点 **Save**。
- 在显示的 **Vanilla** 客户端页面中，单击 **Installation** 选项卡。
- 选择 **Keycloak OIDC JSON** 生成您稍后所需的文件。

Keycloak.json 文件



- 点 **Download** 将 **Keycloak.json** 保存到可在以后找到的位置。
- 选择 **Keycloak OIDC JBoss 子系统 XML** 来生成 XML 模板。

模板 XML



- 单击 **Download** 以保存供下一流程使用的副本，该副本涉及 JBoss EAP 配置。

3.4. 修改 JBOSS EAP 实例

在被红帽单点登录保护前，JBoss EAP servlet 应用需要额外的配置。

先决条件

- 您在 **demo** 域中创建了名为 **vanilla** 的客户端。
- 已为此客户端保存了一个模板 XML 文件。

流程

- 转到 JBoss EAP 根目录中的 **独立/配置目录**。
- 打开 **standalone.xml** 文件并搜索以下文本：

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1"/>
```

- 将 XML 条目从 self-closing 改为使用一对打开和关闭标签，如下所示：

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
</subsystem>
```

- 将 XML 模板的内容粘贴到 `<subsystem>` 元素中，如下例所示：

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="WAR MODULE NAME.war">
    <realm>demo</realm>
    <auth-server-url>http://localhost:8180/auth</auth-server-url>
    <public-client>true</public-client>
    <ssl-required>EXTERNAL</ssl-required>
    <resource>vanilla</resource>
  </secure-deployment>
</subsystem>
```

- 将 `WAR MODULE NAME.war` 更改为 `vanilla.war`：

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="vanilla.war">
    ...
</subsystem>
```

- 重启应用服务器。

3.5. 安装示例代码来保护应用程序

最后的步骤是通过从 <https://github.com/redhat-developer/redhat-ssso-quickstarts> 仓库安装一些示例代码来保证这个应用程序的安全。快速入门与最新的 Red Hat Single Sign-On 发行版本一起工作。

示例代码是 `app-profile-jee-vanilla` quickstart。它演示了如何更改具有基本身份验证保护的 Jakarta EE 应用，而不更改 WAR。Red Hat Single Sign-On 客户端适配器子系统更改了身份验证方法并注入配置。

先决条件

您已在机器上安装了以下内容，并可在 PATH 中可用。

- Java JDK 8
- Apache Maven 3.1.1 或更高版本
- Git

您有一个 `keycloak.json` 文件。

流程

1. 确保您的 JBoss EAP 应用服务器已经启动。
2. 使用以下命令下载代码并更改目录：

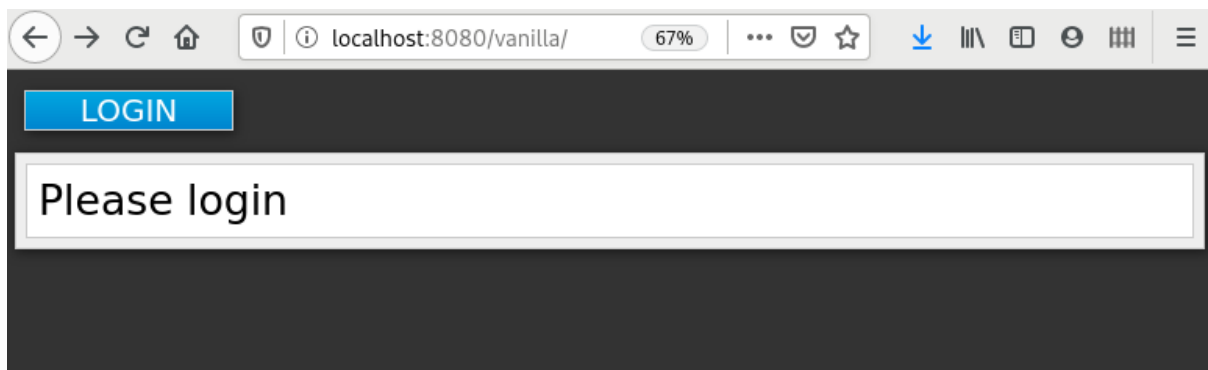
```
$ git clone https://github.com/redhat-developer/redhat-ssso-quickstarts
$ cd redhat-ssso-quickstarts/app-profile-jee-vanilla/config
```

3. 将 **keycloak.json** 文件复制到当前目录中。
4. 向上移到 **app-profile-jee-vanilla** 目录。
5. 使用以下命令安装代码。

```
$ mvn clean wildfly:deploy
```

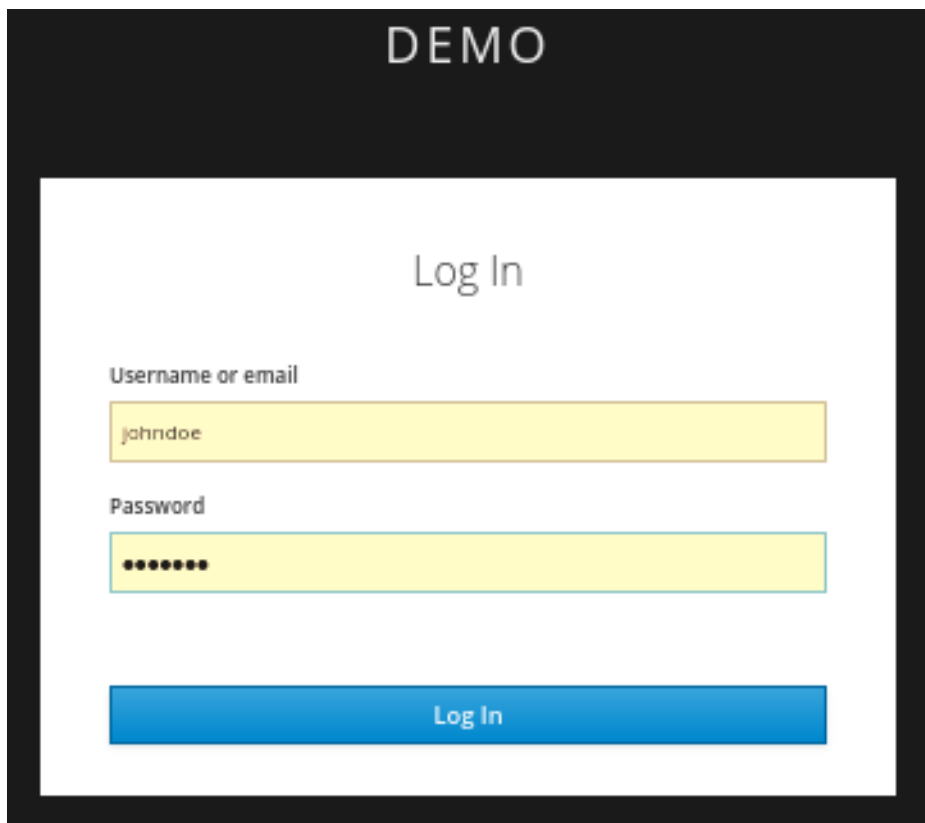
6. 确认应用安装是否成功。进入 <http://localhost:8080/vanilla>，其中显示登录页面。

登录页面确认成功



7. 使用您在 demo 域中创建的帐户登录。

demo 域的登录页面



这时将显示一条消息，表明您已成功完成了 Red Hat Single Sign-On 以保护示例 JBoss EAP 应用。祝贺您！

完成成功

