Red Hat JBoss Core Services 2.4.57

Apache HTTP 服务器安装指南

用于 Red Hat JBoss Middleware 产品。

Last Updated: 2024-03-20

Red Hat JBoss Core Services 2.4.57 Apache HTTP 服务器安装指南

用于 Red Hat JBoss Middleware 产品。

法律通告

摘要

在支持的操作系统上安装、升级并配置 Red Hat JBoss Core Services Apache HTTP Server。

目录

提供有关 RED HAT JBOSS CORE SERVICES 文档的反馈

要报告错误或改进文档，请登录到 Red Hat JIRA 帐户并提交问题。如果您没有 Red Hat Jira 帐户，则会提示您创建一个帐户。

流程

1. 单击以下链接 **以创建 ticket**。
2. 在 **Summary** 中输入问题的简短描述。
3. 在 **Description** 中提供问题或功能增强的详细描述。包括一个指向文档中问题的 URL。
4. 点 **Submit** 创建问题，并将问题路由到适当的文档团队。

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 JBCS APACHE HTTP 服务器安装简介

红帽 JBoss 核心服务(JBCS)提供了一组补充软件，包括 Apache HTTP 服务器，可用于各种红帽 JBoss 中间件产品。红帽将此补充软件打包在 JBCS 下，以便更快地发布更新以及更一致的更新体验。

有关 JBCS 支持的组件的完整列表，请参阅 Core Services Apache HTTP Server 组件详情 网页。

注意

在尝试访问 Core Services Apache HTTP Server 组件详情 网页前，请确保您有有效的红帽订阅，并登录到红帽客户门户网站。

1.1. JBCS APACHE HTTP SERVER

红帽 JBoss 核心服务(JBCS)提供多个红帽 JBoss 中间件产品使用的 Apache HTTP 服务器分布。Apache HTTP 服务器处理 Web 客户端通过 Hypertext 传输协议(HTTP)发送的请求。

JBoss 中间件产品的 Apache HTTP 服务器发行版本

在较旧的 JBoss 产品版本中，每个 JBoss 中间件产品都提供单独的 Apache HTTP 服务器分发。从以下产品版本开始，每个 JBoss 中间件产品都使用 Apache HTTP 服务器的 JBCS 发行版：

- Red Hat JBoss Enterprise Application Platform (JBoss EAP) 7.0 或更高版本
- Red Hat JBoss Web Server 3.1 或更高版本

Apache HTTP 服务器的 JBCS 和 RHEL 发行版之间的区别

JBCS 和 Red Hat Enterprise Linux (RHEL)提供 Apache HTTP 服务器的独立分发。

重要

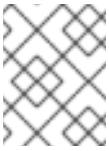
在 RHEL 9 中，JBCS 不提供 Apache HTTP 服务器的 RPM 发行版。JBCS 仅为 RHEL 9 系统提供 Apache HTTP 服务器的存档文件分发。

与早期 RHEL 版本上的 JBCS 版本不同，适用于 RHEL 9 系统的 Apache HTTP 服务器的 JBCS 发行版取决于 Apache HTTP 服务器 **httpd** 软件包的 RHEL 发行版。JBCS 在 RHEL 9 上提供了一个存档文件分发，以支持可以同时运行多个 Apache HTTP 服务器实例。

考虑 JBCS 和 RHEL 提供的 Apache HTTP 服务器发行版本之间的以下区别：

在 RHEL 版本 7 和 8 中

- 您可以从归档文件或 RPM 软件包安装 JBCS Apache HTTP 服务器。您只能从 RPM 软件包安装 RHEL Apache HTTP 服务器。
- 只有 JBCS Apache HTTP 服务器提供负载均衡 HTTP 连接器 **mod_jk** 和 **mod_proxy_cluster**。RHEL Apache HTTP 服务器不提供这些模块。

  注意

  在 JBCS 2.4.37 及更早的版本中，**mod_proxy_cluster** 连接器被命名为 **mod_cluster**。

- 在 RHEL 7 上，只有 JBCS Apache HTTP 服务器提供 **mod_proxy_uwsgi** 模块。从 RHEL 8 开始，Apache HTTP 服务器的 JBCS 和 RHEL 发行版都提供 **mod_proxy_uwsgi** 模块。

对于 RHEL 9

- 与 RHEL 7 和 RHEL 8 上的 JBCS 发行版本不同，RHEL 9 上的 JBCS 发行版本基于 Apache HTTP Server **httpd** 软件包的 RHEL 发行版。因此，RHEL 9 上的 JBCS 与早期 RHEL 版本上的 Apache HTTP 服务器的 JBCS 发行版相比，有一些行为差异。如需更多信息，请参阅 不同 RHEL 版本的 JBCS 发行版之间的区别。
- JBCS 仅提供 Apache HTTP 服务器的存档文件分发。如果要从 RPM 软件包安装 Apache HTTP 服务器，则唯一选项是使用 Application Streams 安装 **httpd** 软件包的 RHEL 发行版。
- JBCS 提供的 Apache HTTP 服务器版本与 RHEL 通过 Application Streams 功能提供的 Apache HTTP 服务器版本不同。
- Apache HTTP 服务器的 JBCS 和 RHEL 发行版提供 **mod_jk** 连接器和 **mod_proxy_cluster** 连接器的相同副本。

在所有 RHEL 版本中

- JBCS Apache HTTP 服务器使用顶级 **jbcs-httpd24-2.4/httpd** 安装目录。RHEL Apache HTTP 服务器使用标准 RHEL 目录来安装 **httpd** 软件包，如 **/etc/httpd**、**usr/share/httpd**、**var/log/httpd** 等等。
- 当您从归档文件或使用 **groupinstall** 选项安装 Apache HTTP 服务器的 JBCS 发行版时，您还要自动安装 **mod_jk** 和 **mod_proxy_cluster** 连接器。
- JBCS Apache HTTP 服务器不提供或支持 **mod_php** 模块。只有 RHEL Apache HTTP 服务器支持 **mod_php** 模块。

不同 RHEL 版本的 JBCS 发行版本之间的行为区别

与 RHEL 7 或 RHEL 8 上的 JBCS 2.4.57 不同，RHEL 9 系统的 JBCS 2.4.57 发行版基于 Apache HTTP Server **httpd** 软件包的 RHEL 发行版。这与红帽发布 RHEL 9 的 **httpd** 软件包的方式有所改变，有助于为 Apache HTTP 服务器用户提供更一致且简化的用户体验。

因此，RHEL 9 上的 JBCS 2.4.57 与早期 RHEL 版本上的 JBCS 2.4.57 与 JBCS 2.4.57 相比有一定的行为。

请考虑以下指南：

- 在 RHEL 9 上，**mod_security** 模块不支持 **SecCollectionGCFrequency** 指令来指定垃圾回收频率。JBCS 在 RHEL 7 和 RHEL 8 上提供的 **mod_security** 模块支持 **SecCollectionGCFrequency** 指令。
- 在 RHEL 9 上，**mod_deflate** 模块不支持 **DeflateAlterEtag** 指令，用于指定在压缩响应时如何更改 ETag 标头。JBCS 在 RHEL 7 和 RHEL 8 上提供的 **mod_deflate** 模块支持 **DeflateAlterEtag** 指令。
- 在 RHEL 9 中，**httpd.conf.sample** 文件不包括以下内容：
  - 用于指定服务器记录守护进程的进程 ID 的文件的默认 **PidFile** 指令
  - **mod_mime** 部分中的 **AddLanguage** 指令列表，用于将特定文件名扩展映射到特定内容语言
  - 用于基于 Web 的分布式编写和版本控制(WebDav)的 **web_dav** 模块的配置部分.

  JBCS 上提供的 **httpd.conf.sample** 文件包括在 RHEL 7 和 RHEL 8 上，包括上述所有内容。

1.2. JBCS APACHE HTTP 服务器支持的操作系统和安装方法

红帽 JBoss 核心服务(JBCS)为不同版本的 Red Hat Enterprise Linux (RHEL)和 Windows Server 操作系统提供 Apache HTTP 服务器分发。

考虑在支持的操作系统中安装 JBCS Apache HTTP 服务器的以下准则：

- 在所有支持的 RHEL 和 Windows Server 版本中，您可以使用每个平台可用的归档安装文件来安装 JBCS Apache HTTP 服务器。
- 在 RHEL 版本 7 和 8 中，您可以使用 Red Hat Package Manager (RPM)软件包安装 JBCS Apache HTTP 服务器。
- 在 RHEL 9 中，如果要从 RPM 软件包安装 Apache HTTP 服务器，则必须使用 Application Streams 安装 Apache HTTP 服务器的 RHEL 发行版。*您不能使用* RPM 软件包在 RHEL 9 上安装 JBCS Apache HTTP 服务器。

其他资源

- Core Services HTTP Server 支持的配置 网页

1.3. 将现有 JBCS 安装升级到 2.4.57 发行版本

如果您之前安装了 Red Hat JBoss Core Services (JBCS) 2.4.51 或更早版本，您可以将现有的 JBCS 安装升级到最新的 2.4.57 版本。升级 JBCS 的步骤因您从存档文件还是 RPM 软件包安装产品而有所不同。

1.3.1. 从存档文件安装时升级现有的 JBCS 安装

如果您之前从存档文件安装了 JBCS Apache HTTP Server 2.4.51 或更早版本，您可以升级到最新的 2.4.57 版本。

升级过程包括以下步骤：

1. 安装 Apache HTTP Server 2.4.57
2. 设置 Apache HTTP 服务器 2.4.57
3. 删除早期版本的 Apache HTTP 服务器

先决条件

- 如果您使用 Red Hat Enterprise Linux (RHEL)，则具有 root 用户访问权限。
- 如果您使用 Windows Server，则具有管理访问权限。
- 您有从存档文件安装的 JBCS Apache HTTP Server 2.4.51 或更早版本的现有安装。

流程

1. 关闭 Apache HTTP Server 2.4.51 的任何正在运行的实例。
2. 备份 Apache HTTP Server 2.4.51 安装和配置文件。
3. 为当前系统使用存档文件安装方法安装 Apache HTTP Server 2.4.57。如需更多信息，请参阅本节末尾的附加资源。

4. 将您的配置从 Apache HTTP 服务器版本 2.4.51 迁移到 2.4.57 版本。

注意

自 Apache HTTP Server 2.4.51 发行版本起，JBCS 配置文件可能已更改。更新 2.4.57 版本配置文件，而不是用不同版本（如 Apache HTTP Server 2.4.51）的配置文件覆盖它们。

5. 删除 Apache HTTP Server 2.4.51 根目录。

其他资源

- 从归档文件在 RHEL 上安装 JBCS Apache HTTP 服务器
- 在 Windows Server 上安装 JBCS Apache HTTP 服务器

1.3.2. 从 RPM 软件包安装时升级现有的 JBCS 安装

如果您之前从 RPM 软件包安装了 JBCS Apache HTTP Server 2.4.51 或更早版本，您可以使用 **yum groupupdate** 命令升级到最新的 2.4.57 版本。

先决条件

- 您有从 RHEL 7 或 RHEL 8 上的 RPM 软件包安装的 JBCS Apache HTTP Server 2.4.51 或更早版本的现有安装。

流程

- 以 root 用户身份输入以下命令：

```
# yum groupupdate jbcs-httpd24
```

其他资源

- 从 RPM 软件包在 RHEL 7 或 RHEL 8 上安装 JBCS Apache HTTP 服务器

1.4. RHEL 7 和 RHEL 8 之间的主要区别

本节概述 Red Hat Enterprise Linux (RHEL) 8 中引入的一些关键更改。

删除的安全功能

RHEL 7 中弃用了完全由数字组成的用户和组群名称，其支持在 RHEL 8 中已完全删除。

内存管理

在 RHEL 7 中，现有内存总线具有 48/46 位的虚拟/物理内存寻址的容量，而 Linux 内核则实施 4 级页表，以将这些虚拟地址管理到物理地址。使用扩展地址范围时，RHEL 8 中的内存管理支持实现 5 级页表，以允许处理扩展的地址范围。在 RHEL 8 中，默认禁用对 5 级页表的支持，即使系统支持此功能。

XFS 支持

RHEL 7 只能在只读模式下使用共享 copy-on-write 数据扩展挂载 XFS 文件系统。在 RHEL 8 中，XFS 文件系统支持共享的 copy-on-write 数据扩展功能。这个功能可让两个或者多个文件共享一组通用的数据块。

NFS 配置

在 RHEL 7 中，NFS 配置位于 **/etc/sysconfig/nfs** 文件中。在 RHEL 8 中，NFS 配置位于 **/etc/nfs.conf** 文件中。

其他资源

- 使用 RHEL 8 时的注意事项

1.5. RHEL 8 和 RHEL 9 之间的主要区别

本节概述 Red Hat Enterprise Linux (RHEL) 9 中引入的一些关键更改。

应用程序流增强

RHEL 8 引入了一个名为 *Application Streams* 的功能。RHEL 使用 Application Streams 提供和更新用户空间组件的多个版本，如应用程序、运行时语言和数据库频率高于核心操作系统软件包。每个 Application Stream 代表一个组件的特定版本，Application Stream 中的每个组件都有定义的生命周期。Application Streams 为用户提供了更大的灵活性，使用满足特定用例和工作负载的组件的组件版本，而不影响平台或部署的底层稳定性。

在 RHEL 8 中，红帽将内容打包在 Application Streams 中，作为 RPM 软件包、模块（软件包组）和 Software Collections 的组合。RHEL 9 通过提供初始 Application Stream 版本来进一步增强 Application Streams 功能，您可以使用标准 **dnf install** 命令作为 RPM 软件包安装

Apache 连接器和负载均衡器的可用性

RHEL 9 提供 Apache Tomcat Connector (**mod_jk**)和 JBoss HTTP Connector (**mod_proxy_cluster**) 的分发，用于对后端应用服务器的 Web 客户端请求进行负载平衡。**mod_jk** 和 **mod_proxy_cluster** 的 RHEL 发行版与这些模块的 JBCS 发行版相同。

安装 Apache HTTP 服务器的 RHEL 发行版不会自动安装 **mod_jk** 和 **mod_proxy_cluster** 模块。有关从 RHEL 9 上的 RPM 软件包安装 **mod_jk** 和 **mod_proxy_cluster** 的更多信息，请参阅 Apache HTTP 服务器连接器和负载平衡指南。

其他资源

- 使用 RHEL 9 时的注意事项

1.6. 其他资源（或后续步骤）

- 从归档文件在 RHEL 上安装 JBCS Apache HTTP 服务器
- 从 RPM 软件包在 RHEL 7 或 RHEL 8 上安装 JBCS Apache HTTP 服务器
- 在 Windows Server 上安装 JBCS Apache HTTP 服务器
- 使用 Application Streams 在 RHEL 9 上安装 Apache HTTP 服务器

第 2 章 从归档文件在 RHEL 上安装 JBCS APACHE HTTP 服务器

在 Red Hat Enterprise Linux (RHEL)版本 7、8 和 9 中，Red Hat JBoss Core Services (JBCS)提供了 Apache HTTP 服务器的一个发行版本，您可以从存档文件中安装。您可以从红帽客户门户网站上的 Software Downloads 页面下载并提取存档文件。您必须为原始 2.4.57 发行版本安装基本存档文件。您还可以安装最新的服务包版本（若有）。

从存档文件安装 Apache HTTP 服务器时，您可以以不同的方式管理产品。例如，您可以在系统启动时使用系统守护进程，或者从命令行管理 Apache HTTP 服务器。

注意

从 2.4.57 Service Pack 2 以后，JBCS 也支持从 RHEL 9 上的存档文件安装 Apache HTTP Server 2.4.57。对于 RHEL 9 上的 JBCS Apache HTTP Server 2.4.57 安装，基本存档文件是 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 Patch 02 for RHEL 9 x86_64**。

2.1. 在 RHEL 上下载并提取 APACHE HTTP 服务器存档文件

您可以从红帽客户门户网站上的 软件下载页面 下载 Apache HTTP Server 归档文件。根据您使用的 Red Hat Enterprise Linux (RHEL)版本，下载存档文件的步骤略有不同。

注意

如果您有对预期的安装目录的写入权限，您可以使用非 root 权限安装存档文件。

先决条件

- 您已安装了 **elinks**、**krb5-workstation** 和 **mailcap** 软件包。
  如果要安装这些软件包，请以 root 用户身份输入以下命令：

```
# yum install elinks krb5-workstation mailcap
```

流程

1. 打开浏览器并登录到红帽客户门户网站中的 Software Downloads 页面。
2. **在产品** 下拉菜单中，选择 **Apache HTTP Server**。
3. 在 **Version** 下拉菜单中选择正确的 JBCS 版本。
4. 根据您使用的 RHEL 版本，执行以下步骤之一：
   - 如果您在 **Releases** 选项卡中使用 RHEL 7，点 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 for RHEL 7 x86_64** 文件旁边的 **Download**。
   - 如果您使用 RHEL 8，在 **Releases** 选项卡中点 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 for RHEL 8 x86_64** 文件旁的 **Download**。
   - 如果您使用 RHEL 9，点 **安全公告** 标签页。然后单击 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 Patch 02 for RHEL 9 x86_64** 文件旁边的 **Download**。

注意

Red Hat JBoss Core Services Apache HTTP Server 2.4.57 Patch 02 for RHEL 9 x86_64 文件是 RHEL 9 上安装 JBCS Apache HTTP Server 2.4.57 的基本存档文件。

5. 将下载的存档文件提取到您的安装目录中。

注意

在 RHEL 系统上，在 **/opt/** 目录中安装 Apache HTTP 服务器。

归档文件的提取会自动为 Apache HTTP 服务器创建顶级 **jbcs-httpd24-2.4/httpd** 目录。本文档将 **jbcs-httpd24-2.4/httpd** 目录称为 ***HTTPD_HOME***。

6. 要安装最新的服务包版本（若有），请执行以下步骤：

   a. 在 Software Downloads 页面中，点 **Security Advisories** 选项卡。

   b. 在 **安全公告** 选项卡中，点与您的系统平台和架构匹配的最新的 JBCS Apache HTTP Server 2.4.57 补丁归档文件旁的 **Download**。
   例如，如果您要在 RHEL 8 上安装 Apache HTTP Server 2.4.57 的 Service Pack *X* 版本，请单击 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 Patch *X* for RHEL 8 x86_64** 文件旁边的 **Download**。

注意

Service pack 发行版本是累计的。通过下载最新的服务包版本，您还会自动安装任何以前的服务包版本。

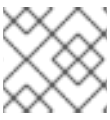
2.2. 用于从命令行管理归档安装的 APACHE HTTP 服务器配置

当您从 RHEL 上的存档文件安装 JBCS Apache HTTP 服务器时，您可以从命令行直接启动和停止 Apache HTTP 服务器。使用命令行运行 Apache HTTP 服务器前，您必须执行以下一系列配置任务：

- 创建 Apache 用户
- 禁用或启用 SSL 支持
- 运行 Apache HTTP 服务器安装后脚本

2.2.1. 创建 Apache 用户

首次从命令行运行 Apache HTTP 服务器之前，您必须创建 **apache** 用户帐户和组。您还必须将 Apache 目录的所有权分配给 **apache** 用户，以便用户可以运行 Apache HTTP 服务器。



注意

您必须以 root 用户身份执行此流程中的所有步骤。

先决条件

- 您已从 存档文件 安装了 Apache HTTP 服务器。

流程

1. 在命令行中，前往 ***HTTPD_HOME*** 目录。
2. 运行以下命令来创建 **apache** 用户组：

```
# groupadd -g 48 -r apache
```

3. 要在 **apache** 用户组中创建 **apache** 用户，请输入以下命令：

```
# /usr/sbin/useradd -c "Apache" -u 48 -g apache -s /sbin/nologin -r apache
```

4. 要为 **apache** 用户分配 Apache 目录的所有权，请输入以下命令：

```
# chown -R apache:apache *
```

验证

- 要验证 **apache** 用户是否为目录的所有者，请输入以下命令：

```
# ls -l
```

2.2.2. 禁用或启用 SSL 支持

在运行 Apache HTTP 服务器之前，您可以选择通过重命名 SSL 配置文件来禁用或启用 SSL 支持。Apache HTTP 服务器默认支持 SSL。

流程

1. 进入 ***HTTPD_HOME*****/conf.d/** 目录。
2. 要启用或禁用 SSL，请执行以下步骤之一：
   - 如果要禁用 SSL，将 ssl.conf 重命名为 **ssl.conf.disabled**。
   - 如果要重新启用 SSL，请将 **ssl.conf.disabled** 重命名为 **ssl.conf**。

2.2.3. 在安装后脚本运行 Apache HTTP 服务器

首次从命令行运行 Apache HTTP 服务器之前，您必须运行 Apache HTTP 服务器安装后脚本。

流程

1. 在命令行中，前往 ***HTTPD_HOME*** 目录。
2. 输入以下命令：

```
./.postinstall
```

2.3. 从存档文件安装时从命令行启动 APACHE HTTP 服务器

当您从 RHEL 上的存档文件安装 JBCS Apache HTTP 服务器时，您可以从命令行直接启动 Apache HTTP 服务器。

先决条件

- 您已创建了 **apache** 用户。
- 您已 禁用或重新启用 SSL 支持。
- 您已在 安装后运行 Apache HTTP 服务器。

流程

1. 在命令行中，前往 ***HTTPD_HOME*/sbin/** 目录。
2. 以 root 用户身份输入以下命令：

```
./apachectl start
```

2.4. 从存档文件安装时从命令行停止 APACHE HTTP 服务器

当您从 RHEL 上的存档文件安装 JBCS Apache HTTP 服务器时，您可以直接从命令行停止 Apache HTTP 服务器的运行实例。

先决条件

- 您已 启动 Apache HTTP 服务器。

流程

1. 在命令行中，前往 ***HTTPD_HOME*/sbin/** 目录。
2. 以 root 用户身份输入以下命令：

```
./apachectl stop
```

2.5. 从命令行没有 ROOT 特权运行 APACHE HTTP 服务器

当您从 RHEL 上的存档文件安装 JBCS Apache HTTP 服务器时，您可以以没有 root 特权的用户的身份从命令行启动 Apache HTTP 服务器。在这种情况下，您可以使用非 root 用户帐户，如 **apache** 用户。

流程

1. 停止 Apache HTTP 服务器 的所有实例：

```
pkill httpd
```

2. 在 ***HTTPD_HOME*/conf/httpd.conf** 文件中，将 **http** 侦听端口设置为高于 1024 ：

```
Listen 2080
ServerName <hostname>:2080
```

3. 在 ***HTTPD_HOME*/conf.d/ssl.conf** 文件中，将 **https** 侦听端口设置为高于 1024:

```
Listen 2443
```

4. 更改 **logs** 目录的所有权：

```
chown -R apache:apache HTTPD_HOME/logs/
```

5. 更改 **run** 目录的所有权：

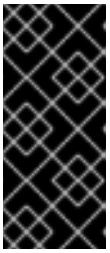
```
chown -R apache:apache HTTPD_HOME/var/run/
```

6. 验证 **httpd** 是否在 **apache** 用户下运行，而不是 **root** 用户和 **apache** 用户：

```
$ ps -eo euser,egroup,comm | grep httpd
```

这个命令会产生以下类型的输出：

```
apache   apache   httpd
apache   apache   httpd
apache   apache   httpd
...
```



重要

限制 **apache** 用户的文件权限并启用 SELinux。这有助于防止以下情况：

- 由网站用户进行未授权访问或修改文件和目录
- 对 Apache HTTP 服务器配置文件不需要的更改

2.6. 从存档文件安装时使用 SYSTEMD 管理 APACHE HTTP 服务器

当您从 RHEL 上的存档文件安装 JBCS Apache HTTP 服务器时，您可以使用系统守护进程来执行管理任务。将 Apache HTTP 服务器与系统守护进程搭配使用，可以在系统引导时启动 Apache HTTP 服务器服务。系统守护进程还提供 start、stop 和 status 检查功能。

在 RHEL 版本 7、8 和 9 中，默认的系统守护进程是 **systemd**。

先决条件

- 您已从 存档文件 安装了 Apache HTTP 服务器。

流程

1. 要确定哪个系统守护进程正在运行，请输入以下命令：

```
$ ps -p 1 -o comm=
```

如果 **systemd** 正在运行，则会显示以下输出：

```
systemd
```

2. 要为 **systemd** 设置 Apache HTTP 服务器，以 root 用户身份运行 **.postinstall.systemd** 脚本：

```
# cd HTTPD_HOME
# sh httpd/.postinstall.systemd
```

3. 要使用 **systemd** 控制 Apache HTTP 服务器，请以 root 用户身份输入以下命令：

- 启用 Apache HTTP 服务器服务在系统启动时启动：

```
# systemctl enable jbcs-httpd24-httpd.service
```

- 启动 Apache HTTP 服务器：

```
# systemctl start jbcs-httpd24-httpd.service
```

- 停止 Apache HTTP 服务器：

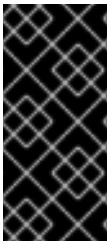
```
# systemctl stop jbcs-httpd24-httpd.service
```

- 验证 Apache HTTP 服务器的状态：

```
# systemctl status jbcs-httpd24-httpd.service
```

注意

任何用户都可以运行 **systemctl status** 命令。



重要

要恢复 **.postinstall.systemd** 脚本影响的任何更改，您可以输入以下命令：

```
# cd HTTPD_HOME
# sh httpd/.postinstall.services.cleanup
```

有关使用 **systemd** 的更多信息，**请参阅附加资源** 链接。

其他资源

- RHEL 7 ：系统管理员指南：管理系统服务
- RHEL 8 ：配置基本系统设置：使用 systemctl 管理系统服务
- RHEL 9 ：配置基本系统设置：使用 systemctl 管理系统服务

2.7. APACHE HTTP 服务器的 SELINUX 策略

您可以使用 Security-Enhanced Linux (SELinux)策略来定义 Apache HTTP 服务器的访问控制。这些策略是一组决定对产品的访问权限的规则。

2.7.1. SELinux 策略信息

SELinux 安全模型由内核强制执行，并确保应用程序对文件系统位置和端口等资源的有限访问权限。SELinux 策略可确保任何被入侵或配置不当的进程都受到限制或阻止了运行。

Apache HTTP 服务器安装中的 **jbcs-httpd24-httpd-selinux** 软件包提供了一个 **mod_proxy_cluster** 策略。下表包含有关提供的 SELinux 策略的信息。

表 2.1. RPM 和默认 SELinux 策略

Name	端口信息	策略信息
mod_proxy_cluster	为 **httpd_port_t** 添加了两个端口（用于 **TCP** 的**6666** 和 **23364**） 以允许 **httpd** 进程使用它们。	安装后脚本配置 **/var/cache/mod_proxy_cluster** 的上下文映射，以使 **httpd** 进程在此位置写入。

其他资源

- RHEL 7： SELinux 用户和管理员指南
- RHEL 8： 使用 SELinux
- RHEL 9: 使用 SELinux

2.7.2. 为 Apache HTTP 服务器归档安装安装 SELinux 策略

在这个发行版本中，归档软件包提供 SELinux 策略。根 Apache HTTP 服务器文件夹包含一个 **.postinstall.selinux** 文件。如果需要，您可以运行 **.postinstall.selinux** 脚本。

重要

默认情况下，Apache HTTP 服务器提供的 SELinux 策略不处于活动状态，而 Apache HTTP 服务器进程在 **unconfined_t** 域中运行。这个域不会限制进程。如果您选择不要启用 SELinux 策略，请限制 **apache** 用户的文件访问，以便 **apache** 用户只能访问 Apache HTTP 服务器运行时所需的文件和目录。

流程

1. 安装 **selinux-policy-devel** 软件包：

```
yum install -y selinux-policy-devel
```

2. 运行 **.postinstall.selinux** 脚本：

```
cd <httpd_home>
sh .postinstall.selinux
```

3. 创建并安装 SELinux 模块：

```
cd <httpd_home>/selinux/
make -f /usr/share/selinux/devel/Makefile
semodule -i jbcs-httpd24-httpd.pp
```

4. 为 Apache HTTP 服务器应用 SELinux 上下文：

```
restorecon -r <httpd_home>
```

5. 为 Apache HTTP 服务器所需端口添加访问权限：

```
semanage port -a -t http_port_t -p tcp 6666
semanage port -a -t http_port_t -p udp 23364
```

6. 启动 Apache HTTP 服务器服务：

```
<httpd_home>/sbin/apachectl start
```

7. 检查预期 **httpd_t** 的正在运行的进程的上下文：

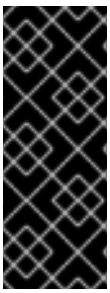
```
$ ps -eZ | grep httpd | head -n1

unconfined_u:unconfined_r:httpd_t:s0-s0:c0.c1023 2864 ? 00:00:00 httpd
```

8. 验证 httpd 目录的上下文。例如：

```
ls -lZ <httpd_home>/logs/
```

第 3 章 从 RPM 软件包在 RHEL 7 或 RHEL 8 上安装 JBCS APACHE HTTP 服务器

在 Red Hat Enterprise Linux (RHEL)版本 7 和 8 中，Red Hat JBoss Core Services (JBCS)提供了 Apache HTTP 服务器的发行版本，您可以从 RPM 软件包安装。JBCS Apache HTTP 服务器的 RPM 安装软件包可从红帽订阅管理中获得。从 RPM 软件包安装 Apache HTTP 服务器将 Apache HTTP 服务器安装为服务。



重要

JBCS 为 RHEL 版本 7 和 8 提供 Apache HTTP 服务器的 RPM 发行版。JBCS 没有为 RHEL 9 提供 Apache HTTP 服务器的 RPM 发行版。

如果要在 RHEL 9 中从 RPM 软件包安装 Apache HTTP 服务器，则必须使用 RHEL 的 Application Streams 功能。如需更多信息，请参阅使用 Application Streams 在 RHEL 9 上安装 Apache HTTP 服务器。

3.1. 将订阅附加到 RHEL

在为 Apache HTTP 服务器下载并安装 RPM 软件包前，您必须将订阅附加到 Red Hat Enterprise Linux (RHEL)。您可以通过 Red Hat Subscription Management 注册您的系统，并订阅相应的 Content Delivery Network (CDN)软件仓库来附加订阅。然后，您可以执行一些验证步骤，以确保订阅提供了所需的 CDN 软件仓库。

流程

1. 使用 Red Hat Subscription Management 注册您的系统：
   a. 登录到 Red Hat Subscription Management 网页。
   b. 点 **Systems** 选项卡。
   c. **点击** 您要向其添加订阅的系统名称。
   d. 从 **Details** 选项卡更改到 **Subscriptions** 选项卡，然后单击 **Attach Subscriptions**。
   e. 选中您要附加的订阅旁边的复选框，然后单击 **Attach Subscriptions**。
2. 要为您的操作系统版本订阅 Apache HTTP 服务器 CDN 软件仓库，请以 root 用户身份输入以下命令：

```
# subscription-manager repos --enable <repository>
```

注意

如果使用 RHEL 7，请将 < ***repository>*** 替换为 **jb-coreservices-1-for-rhel-7-server-rpms**。

如果您使用 RHEL 8，请将 < ***repository>*** 替换为 **jb-coreservices-1-for-rhel-8-x86_64-rpms**。

验证

1. 登录到 Red Hat Subscriptions 网页。

2. 在 **Subscription Name** 列中，点您要选择的订阅。
3. 在 **产品提供下**，您需要 **Red Hat JBoss Core Services**。

有关注册您安装的 RHEL 版本的更多信息，**请参阅附加资源** 链接。

其他资源

- RHEL 7 ：安装指南：订阅管理器.
- RHEL 8 ：配置基本系统设置： 注册系统并管理订阅。

3.2. 使用 YUM 从 RPM 软件包安装 APACHE HTTP 服务器

您可以使用 YUM 软件包管理器从 RHEL 7 或 RHEL 8 上的 RPM 软件包安装 JBCS Apache HTTP 服务器。

先决条件

- 您已将 订阅附加到 RHEL。

流程

- 要安装 Apache HTTP 服务器，请以 root 用户身份输入以下命令：

```
# yum groupinstall jbcs-httpd24
```

3.3. 从 RPM 安装时配置 APACHE HTTP 服务器安装

从 RPM 软件包安装 Apache HTTP 服务器时，您可以在运行 Apache HTTP 服务器前选择性地删除 SSL 支持。Apache HTTP 服务器默认支持 SSL。您可以通过删除 **mod_ssl** 软件包来选择删除 SSL 支持。

流程

- 在命令行中以 root 用户身份输入以下命令：

```
# yum remove jbcs-httpd24-mod_ssl
```

3.4. 从 RPM 安装时，从命令行启动 APACHE HTTP 服务器

当您从 RPM 软件包安装 JBCS Apache HTTP 服务器时，您可以使用命令行启动 Apache HTTP 服务器。

流程

- 在命令行中，以 root 用户身份启动 Apache HTTP Server 服务：

```
# systemctl start jbcs-httpd24-httpd.service
```

3.5. 从 RPM 安装时，从命令行停止 APACHE HTTP 服务器

当您从 RPM 软件包安装 JBCS Apache HTTP 服务器时，您可以使用命令行停止 Apache HTTP 服务器。

流程

- 在命令行中，以 root 用户身份停止 Apache HTTP Server 服务：

```
# systemctl stop jbcs-httpd24-httpd.service
```

3.6. 将 APACHE HTTP 服务器服务配置为在系统启动时启动

当您从 RPM 软件包安装 JBCS Apache HTTP 服务器时，您可以将 Apache HTTP Server 服务配置为在系统启动时启动。

流程

- 要使 Apache HTTP Server 服务在系统启动时启动，请以 root 用户身份输入以下命令：

```
# systemctl enable jbcs-httpd24-httpd.service
```

3.7. APACHE HTTP 服务器的 SELINUX 策略

您可以使用 Security-Enhanced Linux (SELinux)策略来定义 Apache HTTP 服务器的访问控制。这些策略是一组决定对产品的访问权限的规则。

3.7.1. SELinux 策略信息

SELinux 安全模型由内核强制执行，并确保应用程序对文件系统位置和端口等资源的有限访问权限。SELinux 策略可确保任何被入侵或配置不当的进程都受到限制或阻止了运行。

Apache HTTP 服务器安装中的 **jbcs-httpd24-httpd-selinux** 软件包提供了一个 **mod_proxy_cluster** 策略。下表包含有关提供的 SELinux 策略的信息。

表 3.1. RPM 和默认 SELinux 策略

Name	端口信息	策略信息
mod_proxy_cluster	为 **httpd_port_t** 添加了两个端口（用于 **TCP** 的**6666** 和 **23364**） 以允许 **httpd** 进程使用它们。	安装后脚本配置 **/var/cache/mod_proxy_cluster** 的上下文映射，以使 **httpd** 进程在此位置写入。

其他资源

- RHEL 7： SELinux 用户和管理员指南
- RHEL 8： 使用 SELinux

3.7.2. 为 Apache HTTP 服务器 RPM 安装启用 SELinux 策略

当您从 RPM 软件包安装 JBCS Apache HTTP 服务器时，jbcs **-httpd2.4-httpd-selinux** 软件包为 Apache HTTP 服务器提供 SELinux 策略。**jbcs-httpd2.4-httpd-selinux** 软件包在 **jb-coreservices-1-for-rhel-7-server-rpms** 和 **jb-coreservices-1-for-rhel-8-x86_64-rpms** 内容交付网络(CDN)存储库中提供。

流程

- 为您要使用的 RHEL 版本安装 **jbcs-httpd2.4-httpd-selinux** 软件包。

第 4 章 在 WINDOWS SERVER 上安装 JBCS APACHE HTTP 服务器

您可以从红帽客户门户网站上的 软件下载 页面，在 Windows Server 上安装 JBCS Apache HTTP Server。

4.1. 在 WINDOWS SERVER 上下载并提取 APACHE HTTP SERVER 归档文件

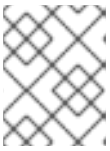
您可以从红帽客户门户网站上的 软件下载页面 下载 Apache HTTP Server 归档文件。您可以从 Software Downloads 页面上的 **Releases** 选项卡下载基础 JBCS Apache HTTP Server 2.4.57 版本的存档文件。您还可以从 Software Downloads 页面中的 **Security Advisories** 选项卡中下载最新的服务包版本（若有）。

注意

如果您有对预期的安装文件夹的写入权限，您可以使用非管理员用户权限安装存档文件。

流程

1. 打开浏览器并登录到红帽客户门户网站中的 Software Downloads 页面。
2. **在产品** 下拉菜单中，选择 **Apache HTTP Server**。
3. 在 **Version** 下拉菜单中选择正确的 JBCS 版本。
4. 在 Releases 选项卡中，点 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 for Windows Server x86_64** 文件旁边的 **Download**。
5. 将下载的存档文件提取到您的安装目录中。



注意

在 Windows Server 系统上，在 **C:\Program Files** 目录中安装 Apache HTTP 服务器。

归档文件的提取会自动为 Apache HTTP 服务器创建顶级 **jbcs-httpd24-2.4** 文件夹。本文档将 **jbcs-httpd24-2.4** 文件夹指代为 ***HTTPD_HOME***。

6. 要安装最新的服务包版本（若有），请执行以下步骤：
   a. 在 Software Downloads 页面中，点 **Security Advisories** 选项卡。
   b. 在 **安全公告** 选项卡中，点最新的 **Red Hat JBoss Core Services Apache HTTP Server 2.4.57 Patch *X* for Windows Server x86_64** 文件旁边的 **Download**。

注意

Service pack 发行版本是累计的。通过下载最新的服务包版本，您还会自动安装任何以前的服务包版本。

4.2. WINDOWS SERVER 上的 APACHE HTTP 服务器配置

当您在 Windows Server 上安装 JBCS Apache HTTP 服务器时，您可以使用命令提示符或使用计算机管理工具来管理 Apache HTTP 服务器。在 Windows Server 上运行 Apache HTTP 服务器前，您必须执行以下一系列配置任务：

- 运行 Apache HTTP 服务器安装后脚本
- 安装 Apache HTTP 服务器服务
- 为 Apache HTTP 服务器服务配置文件夹权限
- 禁用或启用 SSL 支持

4.2.1. 在 Windows Server 上运行 Apache HTTP 服务器安装后脚本

在 Windows 服务器上第一次运行 Apache HTTP 服务器前，您必须运行 Apache HTTP 服务器安装后脚本。

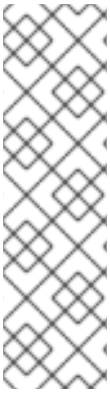
流程

1. **以管理用户身份打开** 命令提示。
2. 前往 ***HTTPD_HOME*\etc** 目录。
3. 输入以下命令：

```
call postinstall.httpd.bat
```

4.2.2. 安装 Apache HTTP 服务器服务

在 Windows 服务器上第一次运行 Apache HTTP 服务器前，您必须将 Apache HTTP Server 安装为 Windows 服务。



注意

默认情况下，Apache HTTP 服务器配置为使用端口 80。如果您安装了 Microsoft Internet Information Services (IIS)，您必须禁用或重新配置 Microsoft OC 以避免端口冲突：

- 停止 **World Wide Web** 服务，并将 **启动类型更改为 Manual**。
- 将 QPC 配置为使用不同的端口。

或者，您可以在安装 Apache HTTP 服务器服务前编辑 **httpd.conf**，并将 **Listen** 更改为与 Microsoft spend 端口不冲突的端口。

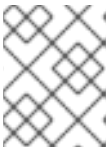
先决条件

- 您已在 安装后运行 Apache HTTP 服务器。

流程

1. **以管理用户身份打开** 命令提示。
2. 前往 ***HTTPD_HOME*\bin** 目录。
3. 要安装 Apache HTTP Server 服务，请输入以下命令：

```
httpd -k install
```



注意

可能会显示防火墙安全对话框，以请求 Apache HTTP 服务器的网络访问。点 **Allow** 从网络访问此服务。

4.2.3. 为 Apache HTTP 服务器服务配置文件夹权限

在 Windows 服务器上第一次运行 Apache HTTP 服务器之前，您必须确保用于运行该服务的帐户对 ***HTTPD_HOME*** 文件夹及其所有子文件夹完全控制。

先决条件

- 已安装 Apache HTTP Server 服务。

流程

1. 右键点击 ***HTTPD_HOME*** 文件夹，然后单击 **Properties**。
2. 选择 **Security** 选项卡。
3. 点 **Edit** 按钮。
4. 点击 **Add** 按钮。
5. 在文本框中，输入 **LOCAL SERVICE**。
6. 选择 **LOCAL SERVICE** 帐户的 **Full Control** 复选框。
7. 点**确定**。
8. 点 **Advanced** 按钮。
9. 在 **Advanced Security Settings** 对话框中，选择 **LOCAL SERVICE** 并点 **Edit**。
10. 选中 **替换此对象选项中所有存在的、具有可继承权限的所有现有可继承权限** 旁边的复选框。
11. 单击 **OK** through all open folder 属性窗口以应用设置。

4.2.4. 禁用或启用 SSL 支持

在运行 Apache HTTP 服务器之前，您可以选择通过重命名 SSL 配置文件来禁用或启用 SSL 支持。Apache HTTP 服务器默认支持 SSL。

先决条件

- 您已为 Apache HTTP 服务器服务配置了文件夹权限。

流程

1. 前往 ***HTTPD_HOME*\conf.d** 目录。
2. 要启用或禁用 SSL，请执行以下步骤之一：

- 如果要禁用 SSL，将 ssl.conf 重命名为 **ssl.conf.disabled**。
- 如果要重新启用 SSL，请将 **ssl.conf.disabled** 重命名为 **ssl.conf**。

4.3. 在 WINDOWS SERVER 上启动 APACHE HTTP 服务器

当您在 Windows Server 上安装 JBCS Apache HTTP 服务器时，您可以使用 Command Prompt 或 Computer Management 工具启动 Apache HTTP Server 服务。

先决条件

- 您已配置了 Apache HTTP 服务器。

流程

- 执行以下步骤：
  - 以管理员身份打开 Command Prompt，并输入以下命令：

```
net start Apache2.4
```

  - 点 **Start > Administrative Tools > Services**，右键单击 **httpd** 服务，然后点击 **Start**。

4.4. 在 WINDOWS SERVER 上停止 APACHE HTTP 服务器

当您在 Windows Server 上安装 JBCS Apache HTTP 服务器时，您可以使用 Command Prompt 或 Computer Management 工具停止 Apache HTTP Server 服务。

先决条件

- 您已 启动 Apache HTTP 服务器。

流程

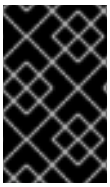
- 执行以下步骤：
  - 以管理员身份打开 Command Prompt，并输入以下命令：

```
net stop Apache2.4
```

  - 点 **Start > Administrative Tools > Services**，右键单击 **httpd** 服务，然后点击 **Stop**。

第 5 章 使用 APPLICATION STREAMS 在 RHEL 9 上安装 APACHE HTTP 服务器

Red Hat Enterprise Linux (RHEL) Application Streams 功能提供和更新 **AppStream** 存储库中的多个版本的用户空间组件，如应用程序、运行时语言和数据库。在 RHEL 9 中，如果要从 RPM 软件包安装 Apache HTTP 服务器，则必须使用 Application Streams 安装 Apache HTTP 服务器的 RHEL 发行版。



重要

Red Hat JBoss Core Services (JBCS)没有为 RHEL 9 提供 Apache HTTP 服务器的 RPM 发行版。RHEL **AppStream** 软件仓库提供的 Apache HTTP Server **httpd** 软件包是 RHEL 9 系统唯一支持的 Apache HTTP 服务器的 RPM 分发。

注意

安装 Apache HTTP 服务器的 RHEL 发行版不会自动安装 **mod_jk** 和 **mod_proxy_cluster** 软件包。有关从 RHEL 9 上的 RPM 软件包安装 **mod_jk** 和 **mod_proxy_cluster** 的更多信息，请参阅 Apache HTTP 服务器连接器和负载平衡指南。

5.1. 使用 APPLICATION STREAMS 安装 APACHE HTTP 服务器

您可以使用标准 **dnf install** 命令从 RPM 软件包安装 Apache HTTP 服务器的 RHEL 9 发行版。然后，您可以以 root 用户身份从命令行启动和停止 Apache HTTP 服务器。或者，您可以启用 Apache HTTP 服务器在系统启动时自动启动。

有关安装、启动和停止 Apache HTTP 服务器的 RHEL 发行版的更多信息，请参阅设置 Apache HTTP web 服务器。

其他资源

- 应用程序流
- 使用 DNF 工具管理软件

5.2. APACHE HTTP 服务器的 SELINUX 策略

您可以使用 Security-Enhanced Linux (SELinux)策略来定义 Apache HTTP 服务器的访问控制。这些策略是一组决定对产品的访问权限的规则。

Apache HTTP 服务器具有 SELinux 类型名称 **httpd_t**。默认情况下，Apache HTTP 服务器可以访问 **/var/www/html** 和其他 Web 服务器目录中具有 **httpd_sys_content_t** SELinux 类型上下文的其他 Web 服务器目录中的文件和目录。

如果要使用非标准配置，您还可以为 Apache HTTP 服务器自定义 SELinux 策略。

其他资源

- 使用 SELinux
- 在非标准配置中自定义 Apache HTTP 服务器的 SElinux 策略

第 6 章 为 JBCS APACHE HTTP 服务器启用 HTTP/2

Hypertext 传输协议(HTTP)是通过互联网在应用程序间传输数据的标准方法，如服务器和浏览器。
Apache HTTP 服务器支持使用 HTTP/2 作为使用传输层安全(TLS)的加密连接，该连接在启用时由 **h2** 关键字表示。

HTTP/2 通过提供以下改进来改进 HTTP/1.1：

- 标头压缩省略了指示的信息，以减少传输的标头大小。
- 单个连接中的多个请求和响应使用二进制 RAM 而不是文本中断响应消息。

注意

Apache HTTP 服务器不支持将 HTTP/2 用于使用传输控制协议(TCP)的未加密的连接，该连接在启用时由 **h2c** 关键字表示。

HTTP/2 不适用于使用多处理模块(MPM)预分叉(**modules/mod_mpm_prefork.so**)的 Web 服务器。

6.1. 先决条件

- 在 Red Hat Enterprise Linux 上具有 root 用户访问权限。
- 在 Windows 服务器上具有管理访问权限。
- 已安装 Red Hat JBoss Core Services Apache HTTP Server 2.4.23 或更高版本。
- 已安装 SSL 模块(**modules/mod_ssl.so**)。
  如果您需要安装 SSL 模块，请输入以下命令：

```
yum install mod_ssl
```

- 已安装 HTTP/2 模块(**modules/mod_http2.so**)。
  如果您需要安装 HTTP/2 模块，请输入以下命令：

```
yum install mod_http2
```

注意

Red Hat Enterprise Linux 6 不再被支持，之后从文档中删除了。

6.2. 为 APACHE HTTP 服务器启用 HTTP/2

您可以通过更新 ***HTTP_HOME*** 目录中的配置文件设置，为 Apache HTTP 服务器启用 HTTP/2。

流程

1. 将 **http2_module** 添加到配置中：
   a. 打开 ***HTTP_HOME*/conf.modules.d/00-base.conf** 文件。
   b. 输入以下行：

```
...
LoadModule http2_module modules/mod_http2.so
```

2. 在配置中添加 **h2** 协议：

   a. 打开 ***HTTP_HOME*/conf/httpd.conf** 文件。

   b. 如果要为虚拟主机启用 HTTP/2 支持，请将 **h2** 协议添加到虚拟主机配置中。
   或者，如果您要为所有服务器连接启用 HTTP/2 支持，请将 **h2** 协议添加到主服务器配置部分。

   例如：

```
<IfModule http2_module>
   Protocols h2 http/1.1
   ProtocolsHonorOrder on
</IfModule>
```

3. 更新安全套接字层(SSL)配置：

   a. 打开 ***HTTP_HOME*/conf.d/ssl.conf** 文件：

   b. 确保将 **SSLEngine** 指令设置为 enabled。SSL Engine 默认启用。

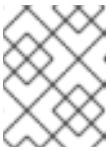
```
SSLEngine on
```

   c. 更新 **SSLProtocol** 指令，以禁用 **SSLv2** 和 **SSLv3** 协议。这会强制连接使用传输层安全(TLS)协议。

```
SSLProtocol all -SSLv2 -SSLv3
```

   d. 更新 **SSLCipherSuite** 指令，以指定哪些 SSL 密码可与 Apache HTTP 服务器一起使用。
   例如：

```
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK
```



注意

有关 SSL 模块和支持的指令的更多信息，请参阅 Apache HTTP 服务器文档版本 2.4 - 模块：Apache Module mod_ssl。

4. 要重启 Red Hat JBoss Core Services Apache HTTP 服务器并应用更改的配置，以 root 用户身份执行以下步骤：

- 如果要使用 **systemd** 在 Red Hat Enterprise Linux 上启动 Apache HTTP 服务器，请输入以下命令：

```
# systemctl restart jbcs-httpd24-httpd.service
```

- 如果要使用 **apachectl** 在 Red Hat Enterprise Linux 上启动 Red Hat JBoss Core Services，请输入以下命令：

```
# HTTP_HOME/sbin/apachectl restart
```

- 如果要在 Windows Server 上启动 Apache HTTP 服务器，请输入以下命令：

```
# net restart Apache2.4
```

其他资源

- 有关 HTTP/2 模块和支持的指令的更多信息，请参阅 Apache HTTP 服务器文档版本 2.4 - 模块：Apache 模块 mod_http2。
- 有关 SSL 模块和支持的指令的更多信息，请参阅 Apache HTTP 服务器文档版本 2.4 - 模块：Apache Module mod_ssl。

6.3. 查看 APACHE HTTP 服务器日志，以验证是否启用了 HTTP/2

您可以查看 Apache HTTP 服务器访问日志或请求日志，以验证是否启用了 HTTP/2。

先决条件

- 您已 启用了 HTTP/2。

流程

1. 从浏览器或使用 **curl** 命令行工具访问服务器。
2. 要检查 SSL/TLS 请求日志，请输入以下命令：

```
$ grep 'HTTP/2' HTTP_HOME/logs/ssl_request_log
```

3. 要检查 SSL/TLS 访问日志，请输入以下命令：

```
$ grep 'HTTP/2' HTTP_HOME/logs/ssl_access_log
```

验证

1. 如果启用了 HTTP/2，**grep 'HTTP/2' *HTTP_HOME*/logs/ssl_request_log** 命令会生成以下类型的输出：

```
[26/Apr/2018:06:44:45 +0000] 172.17.0.1 TLSv1.2 AES128-SHA "HEAD /html-single/index.html HTTP/2" -
```

2. 如果启用了 HTTP/2，**grep 'HTTP/2' *HTTP_HOME*/logs/ssl_access_log** 命令会生成以下类型的输出：

```
172.17.0.1 - - [26/Apr/2018:06:44:45 +0000] "HEAD /html-single/index.html HTTP/2" 200 -
```

6.4. 使用 CURL 命令验证是否启用了 HTTP/2

您可以使用 **curl** 命令行工具来验证是否启用了 HTTP/2。

注意

由 Red Hat Enterprise Linux 7 或更早版本提供的 **curl** 软件包不支持 HTTP/2。

先决条件

- 您已 启用了 HTTP/2。
- 您使用的是支持 **HTTP2** 的 **curl** 版本。
  要检查您是否使用支持 HTTP/2 的 **curl** 版本，请输入以下命令：

```
$ curl -V
```

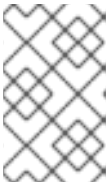
这个命令会产生以下类型的输出：

```
curl 7.55.1 (x86_64-redhat-linux-gnu) ...
Release-Date: 2017-08-14
Protocols: dict file ftp ftps gopher http https ...
Features: AsynchDNS IDN IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB
SSL libz TLS-SRP HTTP2 UnixSockets HTTPS-proxy Metalink PSL
```

步骤

1. 要检查 HTTP/2 协议是否活跃，请输入以下命令：

```
$ curl -I https://<JBCS_httpd_server>:<port>/<test.html>
```



注意

在前面的示例中，将 <***JBCS_httpd_server***> 替换为服务器的 URI，如 **example.com**，并将 <***test.html***> 替换为您要用来测试配置的任何 HTML 文件。不提供 HTML 测试页面示例。端口号取决于您的配置。

验证

- 如果 HTTP/2 协议处于活跃状态，则 **curl** 命令会生成以下输出：

```
HTTP/2 200
```

否则，如果 HTTP/2 协议不活跃，则 **curl** 命令会生成以下输出：

```
HTTP/1.1 200
```

6.5. 其他资源（或后续步骤）

- 有关使用 HTTP/2 的更多信息，请参阅 Apache HTTP 服务器文档版本 2.4 - How-To / Tutorials: HTTP/2 指南。
- 有关 SSL 配置的详情，请参考 Apache HTTP 服务器文档版本 2.4 - SSL/TLS Strong Encryption: How-To。
- 有关 HTTP/2 推荐的互联网标准的更多信息，请参阅 IETF: RFC 7540 - Hypertext Transfer Protocol Version 2 (HTTP/2)。

第 7 章 使用 OCSP 保护连接

在线证书状态协议(OCSP)是一种技术，它允许 Web 浏览器和 Web 服务器通过安全连接进行通信。加密的数据从一个端发送，并在处理前由另一端解密。Web 浏览器和 Web 服务器都加密和解密数据。

7.1. 在线证书状态协议

当 Web 浏览器和 Web 服务器通过安全连接进行通信时，服务器会以证书的形式提供一组凭据。然后，浏览器会验证证书，并发送请求以获取证书状态信息。服务器以当前、过期或未知的证书状态进行响应。

证书包含以下类型的信息：

- 通信的语法
- 控制时间、结束时间和地址信息来访问在线证书状态协议(OCSP)响应器等。

Web 服务器使用 OCSP 响应程序来检查证书状态。您可以将 Web 服务器配置为使用证书中列出的 OCSP 响应程序或其他 OCSP 响应程序。OCSP 为过期的证书允许宽限期，允许在续订证书前访问服务器。

OCSP 解决了较旧的证书撤销列表(CRL)方法的限制。

其他资源

- Red Hat Certificate System *规划、安装和部署指南*。

7.2. 为 SSL 连接配置 APACHE HTTP 服务器

您可以通过安装 **mod_ssl** 软件包并在 **ssl.conf** 文件中指定配置设置，将 Apache HTTP 服务器配置为支持 SSL 连接。

先决条件

- 您已生成了一个 SSL 证书和私钥。
- 您知道 SSL 证书和私钥文件的位置。
- 您已获得与 SSL 证书关联的通用名称(CN)。

流程

1. 要安装 **mod_ssl**，请输入以下命令：

```
# yum install jbcs-httpd24-mod_ssl
```

2. 指定 SSL 配置设置：
   a. 打开 ***JBCS_HOME*/httpd/conf.d/ssl.conf** 文件。
   b. 输入 **ServerName**、**SSLCertificateFile** 和 **SSLCertificateKeyFile** 的详细信息。
   例如：

```
<VirtualHost _default_:443>
ServerName www.example.com:443
SSLCertificateFile /opt/rh/jbcs-httpd24/root/etc/pki/tls/certs/localhost.crt
```

```
SSLCertificateKeyFile /opt/rh/jbcs-httpd24/root/etc/pki/tls/private/localhost.key
```

注意

- **ServerName** 必须与与 SSL 证书关联的通用名称(CN)匹配。如果 **ServerName** 与 CN 不匹配，客户端浏览器会显示域名不匹配的错误。
- **SSLCertificateFile** 指定 SSL 证书文件的路径。
- **SSLCertificateKeyFile** 指定与 SSL 证书关联的私钥文件的路径。

3. 验证 **Listen** 指令是否与部署的 **httpd** 服务的主机名或 IP 地址匹配。
4. 要重启 Apache HTTP 服务器，请输入以下命令：

```
# service jbcs-httpd24-httpd restart
```

7.3. 使用带有 APACHE HTTP 服务器的 OCSP

您可以使用在线证书状态协议(OCSP)与 Apache HTTP 服务器安全连接。

先决条件

- 您已为 SSL 连接配置了 Apache HTTP 服务器。

流程

1. 配置证书颁发机构。

注意

确保您的 CA 可以发布 OCSP 证书。CA 必须能够将以下属性附加到证书中：

```
[ usr_cert ]
...
authorityInfoAccess=OCSP;URI:http://<HOST>:<PORT>
...
[ v3_OCSP ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSP Signing
```

在前面的示例中，将 ***HOST*** 和 ***PORT*** 替换为您要配置的 OCSP 响应器的详细信息。

2. 配置 OCSP 响应程序。

其他资源

- 管理证书和证书颁发机构.
- 配置 OCSP 响应器.

7.4. 配置 APACHE HTTP 服务器以验证 OCSP 证书

您可以通过在 **ssl_conf** 文件中定义 OCSP 设置，将 Apache HTTP 服务器配置为验证 OCSP 证书。

先决条件

- 您已配置了证书颁发机构(CA)。
- 您已配置了 OCSP Responder。

流程

1. 打开 ***JBCS_HOME*/httpd/conf.d/ssl.conf** 文件。
2. 为您的部署指定适当的 OCSP 配置详情。
   例如：

```
# Require valid client certificates (mutual auth)
SSLVerifyClient require
SSLVerifyDepth  3
# Enable OCSP
SSLOCSPEnable on
SSLOCSPDefaultResponder http://<HOST>:<PORT>
SSLOCSPOverrideResponder on
```

注意

前面的示例演示了如何启用客户端证书的 OCSP 验证。在前面的示例中，将 < ***HOST>*** 和 & ***lt;PORT*** > 替换为默认 OCSP Responder 的 IP 地址和端口。

7.5. 验证 APACHE HTTP 服务器的 OCSP 配置

您可以使用 OpenSSL 命令行工具验证 Apache HTTP 服务器的 OCSP 配置。

流程

- 在命令行中以以下格式输入 **openssl** 命令：

```
# openssl ocsp -issuer cacert.crt -cert client.cert -url http://HOST:PORT -CA ocsp_ca.cert -
VAfile ocsp.cert
```

  在前面的命令中，确保指定以下详情：

  - 使用 **-issuer** 选项指定 CA 证书。
  - 使用 **-cert** 选项指定您要验证的客户端证书。
  - 使用 **-url** 选项指定 HTTP 服务器验证证书(OCSP)。
  - 使用 **-CA** 选项指定用于验证 Apache HTTP 服务器服务器证书的 CA 证书。
  - 使用 **-VAfile** 选项指定 OCSP 响应器证书。

更新于 2024-02-06