钴矿

作者：HelpSystems

安装指南
Cobalt Strike 4.6

版权条款和条件

202205051008

在你开始之前

在安装Cobalt Strike之前，请阅读本节。

系统要求

任何承载Cobalt Strike客户端和/或服务器组件的系统都需要以下项目。

爪哇

Cobalt Strike的GUI客户端和团队服务器需要以下Java环境之一。

- Oracle Java 1.8
- Oracle Java 11
- OpenJDK 11. (参见第4页的*安装OpenJDK*说明)

> **注意：**
> 如果你的组织没有允许商业使用Oracle Java的许可，我们鼓励你使用OpenJDK 11。

支持的操作系统

Cobalt Strike Team Server支持符合Java要求的Linux系统，并已在以下基于Debian的Linux发行版上进行了测试（其他版本可能可以使用，但没有经过测试）。

- 蝶变
- 乌班图
- Kali Linux

Cobalt Strike客户端在以下系统上运行。

- Windows 7及以上版本
- MacOS X 10.13及以上版本
- 基于GUI的Linux，例如。蝶变、Ubuntu和Kali Linux（其他版本可能适用，但没有经过测试）。

硬件设施

除了一个公认的操作系统外，还应满足以下最低要求。

- 2 GHz以上的处理器
- 2GB内存
- 500MB以上的可用磁盘空间

在亚马逊的EC2上，至少要使用一个高CPU的中等（c1.medium，1.7GB）实例。

Linux glibc

请注意，某些Linux发行版可能缺少或没有 glibc的正确版本。如果你遇到了这个问题，请查阅HelpSystems门户网站上的知识文章，glibc在较早的Linux发行版中缺失。

安装OpenJDK

Cobalt Strike已通过OpenJDK 11测试，其启动器与正确安装的OpenJDK 11环境兼容。

Linux (Kali 2018.4, Ubuntu 18.04)

1. 更新APT。
   ```
   sudo apt-get update
   ```
2. 用APT安装OpenJDK 11。
   ```
   sudo apt-get install openjdk-11-jdk
   ```
3. 将OpenJDK 11作为默认值。
   ```
   sudo 更新-java-alternatives -s java-1.11.0-openjdk-amd64
   ```

Linux (其他)

1. 卸载当前的OpenJDK包。
2. 下载OpenJDK for Linux/x64的网址是：https://jdk.java.net/archive/。
3. 提取OpenJDK的二进制文件。
   ```
   tar zxvf openjdk-11.0.1_linux-x64_bin.tar.gz
   ```
4. 将OpenJDK文件夹移到**/usr/local**。
   ```
   mv jdk-11.0.1 /usr/local
   ```
5. 在 **~/.bashrc** 中加入以下内容。
   ```
   JAVA_HOME="/usr/local/jdk-11.0.1"
   PATH=$PATH：$JAVA_HOME/bin
   ```
6. 刷新你的**~/.bashrc**以使新的环境变量生效。
   ```
   源于~/.bashrc
   ```

MacOS X

1. 下载OpenJDK for macOS/x64的网站：https://jdk.java.net/archive/。
2. 打开一个终端，浏览到**Download/**文件夹。
3. 提取档案。

```
tar zxvf openjdk-11.0.1_osx-x64_bin.tar.gz
```

4. 将解压后的档案移到**/Library/Java/JavaVirtualMachines/**。

```
sudo mv jdk-11.0.1.jdk/ /Library/Java/JavaVirtualMachines/
```

MacOS X上的java命令将使用/Library/Java中最高的Java版本作为默认。

小费。
如果您看到**JRELoadError消息**，这是因为Cobalt Strike包含的JavaAppLauncher存根从设定的路径加载一个库，以在存根进程中运行JVM。发布以下命令来解决这个错误。

```
sudo ln -fs /Library/Java/JavaVirtualMachines/jdk-11.0.2.jdk
/Library/Internet/ Plug-Ins/JavaAppletPlugin.plugin
```

用你的Java路径替换**jdk-11.0.2.jdk**。下一个Cobalt Strike版本将使用MacOS X的Java应用存根，更加灵活。

窗户

1. 下载OpenJDK for Windows/x64的网址是：https://jdk.java.net/archive/。
2. 提取档案到**c:\program files\jdk-11.0.1**。
3. 将**c:\program files\jdk-11.0.\bin**添加到用户的PATH环境变量。
   a. 进入**控制面板->系统->更改设置->高级->环境变量....**
   b. 在**用户变量**中突出显示**用户的路径**。
   c. 按**编辑**。
   d. **按新**。
   e. 类型：**c:\program files\jdk-11.0.1\bin**。
   f. 在所有的对话框中按**确定**。

Wayland桌面 - 不支持

Wayland是X Windows系统的现代替代品。作为一个项目，Wayland已经取得了巨大的进步，一些桌面环境将其作为他们的默认窗口系统。不过，不要被采用的情况所迷惑。并非所有的应用程序或应用环境都能在Wayland上100%完美运行。仍然有一些错误和问题需要解决。

Java（或Wayland）中存在一些错误，在正常使用期间，当在Wayland桌面中运行时，可能会导致图形化的Java应用程序崩溃。这些错误影响了Cobalt Strike的用户。**HelpSystems不支持在Wayland桌面上使用Cobalt Strike。**

我在使用Wayland吗？

输入echo $XDG_SESSION_TYPE来了解你是在wayland还是x11上。

如何在Kali Linux上禁用Wayland？

最新版本的Kali Linux 2017 Rolling默认使用Wayland桌面。要把它改回X11。

1. 用你喜欢的文本编辑器打开**/etc/gdm3/daemon.conf**。
2. 找到**[daemon]**部分。
3. 添加**WaylandEnable=false**并重新启动系统。

安装Cobalt Strike

遵循这些说明来安装Cobalt Strike。

> **注意：**
> Cobalt Strike**分发包**（步骤1和3）包含操作系统特定的Cobalt Strike启动器、支持文件和更新程序。它不包含Cobalt Strike程序本身。运行**更新程序**（步骤4）下载Cobalt Strike产品并执行最后的安装步骤。

1. 下载支持的操作系统的Cobalt Strike发行包。(提供了一个带有下载链接的电子邮件)
2. 设置一个推荐的Java环境。(见第4页 *安装OpenJDK*的说明)
3. 提取、挂载或解压发行包。根据操作系统，执行下列操作之一。
    a. 对于Linux。
        i. 提取**cobaltstrik-dist.tgz**。
        ```
        tar zxvf cobaltstrik-dist.tgz
        ```
    b. 用于MacOS X。
        i. 双击**cobaltstrik-dist.dmg**文件以加载它。
        ii. 将**Cobalt Strike**文件夹拖到**应用程序**文件夹。
    c. 对于Windows。
        i. 在安装Cobalt Strike之前，请禁用反病毒软件。
        ii. 使用你喜欢的压缩工具将**cobaltstike.zip**文件解压到安装位置。
4. 运行更新程序以完成安装。根据操作系统，执行以下操作之一。
    a. 对于Linux。
        i. 输入以下命令。
        ```
        cd /path/to/cobaltstrike
        ./update
        ```

b. 用于MacOS X。
    i. 导航到**Cobalt Strike**文件夹。
    ii. 双击**更新`Cobalt Strike.`命令**。
c. 对于Windows。
    i. 导航到**Cobalt Strike**文件夹。
    ii. 双击**`update.bat`**。

请确保你用你的许可证密钥更新你的团队服务器和客户端软件。Cobalt Strike通常以每个用户为单位进行授权。团队服务器不需要单独的许可证。

完成后

祝贺您!Cobalt Strike现在已经安装完毕。请阅读以下内容，了解更多信息和您的下一步行动。

接下来的步骤

有关启动Cobalt Strike团队服务器和Cobalt Strike客户端的信息，请参考用户指南。