HTTPS方式登录UI 使用说明

产品版本：ZStack 3.10.0

文档版本：V3.10.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴科技商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受云轴科技公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，云轴科技公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 介绍

ZStack支持HTTPS方式登录UI管理界面，进一步提升系统安全性。

- HTTPS方式默认不启用。
- 启用HTTPS后，系统默认支持5443端口，且支持自定义指定其它端口登录。
- 启用HTTPS后，如使用HTTP方式的5000端口登录，将会自动重定向到HTTPS方式。目前仅支持HTTP的5000端口自动重定向到HTTPS。
- 系统默认支持**PKCS12**格式证书。目前仅提供PKCS12/JKS格式证书支持，如使用其它格式证书，请自行格式转换。

以下分单管理节点和多管理节点物理机高可用两个场景，分别介绍HTTPS方式登录UI的使用方法。

2 单管理节点场景

2.1 默认HTTPS方式

背景信息

初始状态下，支持使用系统默认证书以HTTPS方式登录UI。

操作步骤

1. 在管理节点执行以下命令，停止管理节点服务和UI服务

```
zstack-ctl stop
```

2. 确保VNC控制台支持HTTPS功能。

a) 执行以下命令，查看证书的路径和私钥密码（初始状态下均为系统默认值）。

```
zstack-ctl show_ui_config
```

例如：

```
[root@localhost ~]# zstack-ctl show_ui_config
db_url = jdbc:mysql://10.0.233.184:3306
db_username = zstack_ui
db_password = zstack.ui.password
mn_host = 127.0.0.1
mn_port = 8080
webhook_host = 127.0.0.1
webhook_port = 5000
server_port = 5000
log = /usr/local/zstack/apache-tomcat/logs
enable_ssl = false
ssl_keyalias = zstackui
ssl_keystore = /usr/local/zstack/zstack-ui/ui.keystore.p12 //证书路径
ssl_keystore_type = PKCS12
ssl_keystore_password = password //私钥密码
```

b) 由于UI默认支持PKCS12格式证书，VNC控制台代理默认支持x509格式证书，如希望VNC控制台代理也能使用UI证书，需将PKCS12格式证书转换成x509格式。

```
openssl pkcs12 -in /path/to/mykeystore.p12 -out ui.keystore.pem -nodes
```

其中，/path/to/mykeystore.p12是PKCS12格式的证书，ui.keystore.pem是转换后x509格式的证书。

例如：

```
[root@localhost ~]# openssl pkcs12 -in /usr/local/zstack/zstack-ui/ui.keystore.p12 -out ui
.keystore.pem -nodes
Enter Import Password:
```

```
MAC verified OK
```

c) 进入/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties修改**zstack.properties**配置文件，将证书路径设置为绝对路径（绝对路径指向证书私钥密码文件）。

```
consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem
```

3. 执行以下命令，将基于默认配置自动生成证书，并使用默认证书以HTTPS方式登录UI，端口默认为5443。

```
zstack-ctl config_ui --enable-ssl True
```

4. 在管理节点执行以下命令，启动管理节点服务和UI服务

```
zstack-ctl start
```

5. 使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*https://your_domain_name:5443*），输入默认用户名和密码（*admin/password*），即可以默认HTTPS方式成功登录。

6. 设置控制台代理地址。

登录UI界面，ZStack私有云主菜单，点击**平台管理** > **控制台代理**按钮，将控制台代理设置为*your_domain_name*，确保控制台正常打开。

2.2 自定义HTTPS方式

背景信息

初始状态下，支持使用自定义证书以HTTPS方式登录UI。

操作步骤

1. 准备好自定义证书，可使用相关工具生成自签证书，也可购买正规CA签发证书。

如使用Keytool（Java数据证书管理工具）生成自签证书：

```
mkdir certs

keytool -genkey -alias tomcat  -storetype PKCS12 -keyalg RSA -keysize 2048 -keystore ./certs/keystore.p12 -validity 365
```

例如：

```
[root@localhost ~]# mkdir certs
[root@localhost ~]# keytool -genkey -alias tomcat  -storetype PKCS12 -keyalg RSA -keysize 2048 \
-keystore ./certs/keystore.p12 -validity 365
输入密钥库口令:
再次输入新口令:
```

```
您的名字与姓氏是什么?
  [Unknown]:  Jack Chen
您的组织单位名称是什么?
  [Unknown]:  ZStack
您的组织名称是什么?
  [Unknown]:  DOC
您所在的城市或区域名称是什么?
  [Unknown]:  SH
您所在的省/市/自治区名称是什么?
  [Unknown]:  SH
该单位的双字母国家/地区代码是什么?
  [Unknown]:  CN
CN=Jack Chen, OU=ZStack, O=DOC, L=SH, ST=SH, C=CN是否正确?
  [否]:  是
[root@localhost certs]# ls
keystore.p12
```

2. 在管理节点执行以下命令，停止管理节点服务和UI服务

```
zstack-ctl stop
```

3. 确保VNC控制台支持HTTPS功能。

   a) VNC控制台代理默认支持x509格式证书，如有需要，进行证书格式转换。

   如将PKCS12格式证书转换成x509格式：

   ```
   openssl pkcs12 -in /path/to/mykeystore.p12 -out ui.keystore.pem -nodes
   ```

   其中，/path/to/mykeystore.p12是PKCS12格式的证书，ui.keystore.pem是转换后x509格式的证书。

   例如：

   ```
   [root@localhost ~]# openssl pkcs12 -in /root/certs/keystore.p12 -out ui.keystore.pem -
   nodes
   Enter Import Password:
   MAC verified OK
   ```

   b) 修改**zstack.properties**配置文件，将证书路径设置为绝对路径（绝对路径指向证书私钥密码文件）。

   ```
   consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem
   ```

4. 执行以下命令，自定义证书别名、证书路径、证书类型、私钥密码、HTTPS登录端口等信息，并使用自定义证书以HTTPS方式登录UI。

```
zstack-ctl config_ui --enable-ssl True \
--ssl-keyalias=*** --ssl-keystore=*** --ssl-keystore-type=*** \
--ssl-keystore-password=*** --server-port=*** --webhook-port=***
//将自定义参数信息记录到zstack.ui.properties配置文件
//包括设置：启用HTTPS功能、证书别名、证书路径、证书类型、私钥密码、HTTPS登录端口
```

```
zstack-ctl show_ui_config //可查看自定义参数信息

zstack-ctl stop_ui
zstack-ctl start_ui //每次以HTTPS方式登录UI
```

例如：

```
[root@localhost ~]# zstack-ctl config_ui --enable-ssl True \
--ssl-keyalias=tomcat --ssl-keystore=/root/certs/keystore.p12 --ssl-keystore-type=PKCS12
 \
--ssl-keystore-password=password --server-port=8888
[root@localhost ~]# zstack-ctl show_ui_config
db_url = jdbc:mysql://10.0.233.184:3306
db_username = zstack_ui
db_password = zstack.ui.password
mn_host = 127.0.0.1
mn_port = 8080
webhook_host = 127.0.0.1
webhook_port = 5000
server_port = 8888
log = /usr/local/zstack/apache-tomcat/logs
enable_ssl = true
ssl_keyalias = tomcat
ssl_keystore = /usr/local/zstack/zstack-ui/ui.keystore.p12.cp
ssl_keystore_type = PKCS12
ssl_keystore_password = password
[root@localhost ~]# zstack-ctl stop_ui
successfully stopped the UI server
[root@localhost ~]# zstack-ctl start_ui
successfully started UI server on the local host, PID[32166], https://10.0.233.184:8888
```

5. 在管理节点执行以下命令，启动管理节点服务和UI服务。

```
zstack-ctl start
```

6. 使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*https://your_domain_name:your_server_port*），输入默认用户名和密码（*admin/password*），即可以自定义HTTPS方式成功登录。

注:

若使用FireFox浏览器无法正常打开VNC控制台，请按如下步骤解决：

1. 使用FireFox浏览器访问*https://your_domain_name:4900*；
2. 根据FireFox浏览器的提示，将*https://your_domain_name:4900*添加到安全例外（Exception）；
3. 使用FireFox浏览器打开VNC控制台。

更多详情可参考*FireFox*官网文章。

7. 设置控制台代理地址。

登录UI界面，ZStack私有云主菜单，点击**平台管理** > **控制台代理**按钮，将控制台代理设置为*your_domain_name*，确保控制台正常打开。

2.3 恢复HTTP方式登录UI

操作步骤

1. 执行以下命令，将**zstack.ui.properties**中关于HTTPS功能的相关参数恢复到系统默认值。

```
zstack-ctl config_ui --restore
```

2. 执行zstack-ctl stop_ui及zstack-ctl start_ui即可。

   例如：

```
[root@localhost ~]# zstack-ctl config_ui --restore
[root@localhost ~]# zstack-ctl show_ui_config
db_url = jdbc:mysql://10.0.233.184:3306
db_username = zstack_ui
db_password = zstack.ui.password
mn_host = 127.0.0.1
mn_port = 8080
webhook_host = 127.0.0.1
webhook_port = 5000
server_port = 5000
log = /usr/local/zstack/apache-tomcat/logs
enable_ssl = false
ssl_keyalias = zstackui
ssl_keystore = /usr/local/zstack/zstack-ui/ui.keystore.p12
ssl_keystore_type = PKCS12
ssl_keystore_password = password
[root@localhost ~]# zstack-ctl stop_ui
successfully stopped the UI server
[root@localhost ~]# zstack-ctl start_ui
successfully started UI server on the local host, PID[43261], http://10.0.233.184:5000
```

3. 使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*https://your_machine_ip:5000*），输入默认用户名和密码（*admin/password*），即可恢复默认HTTP方式成功登录。
4. 设置控制台代理地址

   登录UI界面，ZStack私有云主菜单，点击**平台管理** > **控制台代理**按钮，将控制台代理设置为*your_machine_ip*，确保控制台正常打开。

后续操作

至此，HTTPS方式登录UI的使用方法介绍完毕。

3 多管理节点物理机高可用场景

本章节主要介绍双管理节点物理机高可用场景下，如何使用自定义HTTPS方式登录UI，以及如何恢复HTTP方式登录UI。

3.1 自定义HTTPS方式登录UI

背景信息

在双管理节点物理机高可用场景下，使用自定义证书以HTTPS方式登录UI。

操作步骤

1. 准备多域名HTTPS证书。
   - 提前准备一个多域名HTTPS证书，例如：**.zstack.io*；
   - 将两个管理节点以及VIP分别绑定一个域名，例如：*mna.zstack.io*（管理节点A）、*mnb.zstack.io*（管理节点B）、*mn.zstack.io#VIP#*。
2. 停止管理节点服务和UI服务，并关闭*zsha2*服务。

   分别在两个管理节点执行以下命令，停止管理节点服务和UI服务，并关闭*zsha2*服务。

   ```
   [root@localhost ~]# zsha2 stop-node
   ```
3. 确保VNC控制台支持HTTPS功能。

   两个管理节点均需确保VNC控制台支持HTTPS功能。详情可参考单管理节点场景自定义HTTPS方式章节步骤三。
4. 参数配置。

   分别在两个管理节点自定义证书别名、证书路径、证书类型、私钥密码、HTTPS登录端口等信息，并使用自定义证书以HTTPS方式登录UI。详情可参考单管理节点场景自定义HTTPS方式章节步骤四。
5. 启动管理节点服务和UI服务，并启动*zsha2*服务。

   分别在两个管理节点执行以下命令，启动管理节点服务和UI服务，并启动*zsha2*服务。

   ```
   [root@localhost ~]# zsha2 start-node
   ```
6. 以自定义HTTPS方式登录UI。

   使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*https://your_domain_name:your_server_port*），输入默认用户名和密码（*admin/password*），即可以自定义HTTPS方式成功登录。

注:

若使用FireFox浏览器无法正常打开VNC控制台，请按如下步骤解决：

1. 使用FireFox浏览器访问*https://your_domain_name:4900*；
2. 根据FireFox浏览器的提示，将*https://your_domain_name:4900*添加到安全例外（Exception）；
3. 使用FireFox浏览器打开VNC控制台。

更多详情可参考*FireFox*官网文章。

7. 设置控制台代理地址。

   分别登录两个管理节点UI界面，在ZStack私有云主菜单，点击**平台管理** > **控制台代理** > **设置控制台代理地址**按钮，将控制台代理设置为*your_domain_name*，例如：mna.zstack.io（管理节点A）、mnb.zstack.io（管理节点B），确保控制台正常打开。

3.2 恢复HTTP方式登录UI

背景信息

在双管理节点物理机高可用场景下，恢复HTTP方式登录UI。

操作步骤

1. 停止管理节点服务和UI服务，并关闭*zsha2*服务。

   分别在两个管理节点执行以下命令，停止管理节点服务和UI服务，并关闭*zsha2*服务。

   ```
   [root@localhost ~]# zsha2 stop-node
   ```

2. 关闭HTTPS功能。

   分别在两个管理节点执行以下命令，将**zstack.ui.properties**中关于HTTPS功能的相关参数恢复到系统默认值。

   ```
   [root@localhost ~]# zstack-ctl config_ui --restore
   ```

3. 重新配置webhook-host。

   分别在两个管理节点执行以下命令，将webhook-host地址配置为双管理节点VIP地址。

   ```
   [root@localhost ~]# zstack-ctl config_ui --webhook-host VIP
   ```

4. 启动管理节点服务和UI服务，并启动*zsha2*服务。

分别在两个管理节点执行以下命令，启动管理节点服务和UI服务，并启动*zsha2*服务。

```
[root@localhost ~]# zsha2 start-node
```

5. 以HTTP方式登录UI。

   使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*https://your_machine_ip:5000*），输入默认用户名和密码（*admin/password*），即可恢复默认HTTP方式成功登录。

6. 设置控制台代理地址。

   分别登录两个管理节点UI界面，在ZStack私有云主菜单，点击**平台管理** > **控制台代理** > **设置控制台代理地址**按钮，将控制台代理设置为*your_machine_ip*，确保控制台正常打开。

后续操作

至此，在双管理节点物理机高可用场景下，HTTPS方式登录UI的使用方法介绍完毕。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、Shared Mount Point、Shared Block类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。支持ImageStore、Sftp（社区版）、Ceph类型。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一时间点某一磁盘的数据状态文件。包括手动快照和自动快照两种类型。