

Atlassian产品使用https访问

场景

需要使用https的协议访问jira, confluence, bitbucket。

此时需要配置https的相应证书，证书看需要配置到哪一层。包括直接配置在jira, confluence, bitbucket，还是在前端增加nginx, 配置在nginx中。

一般配置https时，需要开启 443 或者 8443 端口。

如：Confluence访问地址为：<http://confluence.hktxcn.com> 现需要通过https来进行访问，即地址为：<https://confluence.hktxcn.com>

- Confluence的IP地址为： 10.10.1.1 端口号为8090
- Nginx的IP地址为： 20.20.1.1 端口号为80

使用Nginx进行配置

配置nginx的server内容

红色是配置的内容

```
server {  
    listen 80;  
    server_name confluence.hktx.cn;  
  
    listen 443 default ssl;  
    ssl_certificate /usr/local/etc/nginx/ssl/nginx.crt; ##私钥证书  
    ssl_certificate_key /usr/local/etc/nginx/ssl/nginx.key; ##私钥证书的key  
  
    ssl_session_timeout 5m;  
  
    location / {  
        client_max_body_size 100m;  
        proxy_set_header X-Forwarded-Host $host;  
        proxy_set_header X-Forwarded-Server $host;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
        proxy_pass http://10.10.1.1:8090;  
    }  
}
```

配置jira\confluence的server.xml内容

通常情况下，可以将原来配置的Connector 进行屏蔽，可以在server.xml的配置文件下方找到另外的一个Connector

填写以下内容（以jira为例），server.xml文件位于安装目录下的conf目录中。

```
<Connector port="8080" relaxedPathChars="[]|" relaxedQueryChars="[]|{}^&#x5c;&#x60;&quot;&lt;&gt;"  
    maxThreads="150" minSpareThreads="25" connectionTimeout="20000" enableLookups="false"  
    maxHttpHeaderSize="8192" protocol="HTTP/1.1" useBodyEncodingForURI="true" redirectPort="8443"  
    acceptCount="100" disableUploadTimeout="true" bindOnInit="false" secure="true" scheme="https"  
    proxyName="confluence.hktx.cn" proxyPort="443"/>
```

配置bitbucket的bitbucket.properties的server.xml内容

bitbucket.properties文件通常情况下位于文件目录下的 shared 目录,可以在以下文件增加以下信息

```
server.port=443  
  
server.ssl.enabled=true  
  
server.scheme=https
```

在应用中进行配置

配置jira\confluence的server.xml内容

通常情况下，可以将原来配置的Connector 进行屏蔽，可以在server.xml的配置文件下方找到另外的一个Connector

填写以下内容（以jira为例），server.xml文件位于安装目录下的 conf目录中。

```
<Connector port="8443" maxHttpHeaderSize="8192"
  maxThreads="150" minSpareThreads="25"
  protocol="org.apache.coyote.http11.Http11Nio2Protocol"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLSv1.2"
  sslEnabledProtocols="TLSv1.2" SSLEnabled="true"
  URIEncoding="UTF-8" keystorePass="<MY_CERTIFICATE_PASSWORD>" ##证书密码
  keystoreFile="<MY_CERTIFICATE_LOCATION>" /> ##证书位置
```

通常情况下，keystoreFile的文件类型应当为 .keystore

配置bitbucket的bitbucket.properties的server.xml内容

bitbucket.properties文件通常情况下位于文件目录下的 shared 目录,可以在以下文件增加以下信息

```
server.port=8443
server.ssl.enabled=true
server.ssl.key-store=/path/to/keystore/bitbucket.jks
server.ssl.key-store-password=<password value>
server.ssl.key-password=<password value>
```