

使用Apple推送通知服务为BroadWorks NPS配置HTTP/2

目录

[要求](#)

[配置](#)

[设置HTTP/2的URL](#)

[配置身份验证密钥](#)

[为生产和开发环境添加令牌](#)

[如果使用XSP 22.0，则启用HTTP/2](#)

[重新启动BroadWorks](#)

[故障排除](#)

[参考](#)

[连接评估客户端](#)

2021年3月31日之后，通知推送服务器(NPS)必须使用HTTP/2接口与Apple推送通知服务(APNS)通信。HTTP/2接口可通过补丁ap354313和版本23.0在BroadWorks版本22.0上使用，仅支持HTTP/2。

如果运行BroadWorks版本22.0，则在应用ap354313后，可以使用以下说明配置HTTP/2。如果升级到23.0或更高版本，则需要执行以下步骤来为APNS配置HTTP/2。

要求

您必须在22.0+或23.0 XSP上。如果XSP仅运行NPS，而AS为21.sp1，则22.0/23.0 XSP与21.sp1堆栈并行运行是兼容的。有关详细信息，请参阅[BroadWorks兼容性表](#)。

您需要知道当前使用哪些客户端作为身份验证密钥ID，配置HTTP/2需要TeamID和身份验证密钥。在21.sp1上配置的应用可在以下位置找到：

```
XSP_CLI/Applications/NotificationPushServer/APNS/Production/Certificate> get
```

- 任何iOS应用非Cisco/BroadSoft应用必须配置为使用HTTP/2 APNS协议。
- 协作或SaaS BroadWorks应用需要迁移到HTTP/2。 [向APN的通知推送服务器添加HTTP/2支持](#)
对于SaaS客户端，请登录BAM门户→ Configuration → BroadWorks，向下滚动到以下部分：Notification Push Server（通知推送服务器），在下拉列表中选择正确的版本，然后按照说明操作。对于Connect Eval Clients，请向TAC打开票证，以请求身份验证密钥、身份验证密钥ID和TeamID。请注意，下面列出的应用ID、身份验证密钥ID和团队ID适用于无品牌客户端，如果使用品牌客户端，则需要从Apple为您的客户端获取此信息。

可以从Apple Developer门户获取其他客户端所需的令牌，请参阅此处的Apple文档：

https://developer.apple.com/documentation/usernotifications/setting_up_a_remote_notification_server/..

如果升级到或部署新的22.0、23.0或ADP，则需要必要的许可证。

另请参阅Xchange上提供的有关操作系统和升级要求的相关版本说明。

配置

确保Notification Push Server CLI中的URL对于HTTP/2 (用于生产和开发) 正确。

设置HTTP/2的URL

```
_CLI/Applications/NotificationPushServer/APNS/Production> get
url = https://api.push.apple.com/3/device
connectionPoolSize = 5
connectionTimeout = 1000
connectionIdleTimeoutInSeconds = 600
_CLI/Applications/NotificationPushServer/APNS/Development> get url =
https://api.development.push.apple.com/3/device connectionPoolSize = 5 connectionTimeout = 1000
connectionIdleTimeoutInSeconds = 600
```

可能需要针对您的特定系统调整上述设置。以上示例和以下建议可能提供一个起点。

- “ConnectionPoolSize”是NPS可以与APNS服务器建立的并发连接数。这将帮助NPS的吞吐量，并且可能不直接帮助超时问题。ConnectionPoolSize应增加到2以上，请注意，如果没有ap377409,NPS可能无法正确注册2以上的值。
- 建议将connectionTimeout设置为大于1000的值。

配置A验证密钥

```
_CLI/Applications/NotificationPushServer/APNS/AuthKey> add UTHPSAD667 Y2V5KSH586
/export/home/bwadmin/EVAL_Team-Y2V5KSH586-APNsAuthKey_ID-UTHPSAD667.p8
...Done
```

```
_CLI/Applications/NotificationPushServer/APNS/AuthKey> get
Auth Key Id      Team Id      Auth Key
=====
64D9E5NY4S      D775LZJG9V  *****    <- SaaS
L44B3C998K      698ZB8543V  *****    <- Connect Dev
UTHPSAD667      Y2V5KSH586  *****    <- Connect Eval
```

3 entry found.

为Produ添加令牌操作和开发环境

```
_CLI/Applications/NotificationPushServer/APNS/Production/Tokens> add com.broadsoft.connect.eval
authKeyId UTHPSAD667
...Done
```

```
_CLI/Applications/NotificationPushServer/APNS/Production/Tokens> get
App Id      Auth Key Id
=====
com.broadsoft.uc-one  64D9E5NY4S    <- SaaS
com.broadsoft.connect.eval  UTHPSAD667    <- Connect Eval
```

2 entries found.

如果 使用XSP 22.0

```
XSP_CLI/Applications/NotificationPushServer/APNS/GeneralSettings> set HTTP2Enabled true
```

注意：如果在23.0或ADP上，则不需要此步骤，因为无法禁用HTTP/2。

重新启动BroadWorks

```
restartbw
```

故障排除

对HTTP/2 POST的响应由通知推送服务器处理。来自APN的响应代码“200”表示APN成功接收了通知，并将尝试将通知推送到设备。详细错误消息会在通知推送服务器日志中捕获。

如果Apple返回错误代码，则Apple错误代码可在Apple文档中找到：

<https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/RemoteNotifi..>

如果使用ADP，则必须将AS设置为使用TLSv1.2。要设置此设置，请在AS上添加以下容器选项：

```
AS_CLI/Maintenance/ContainerOptions> add platform bw.apache.sslenabledprotocols "-ALL +TLSv1.2"
```

将AS设置为使用TLSv1.2后，停止BroadWorks，重新启动配置，然后在AS上再次启动BroadWorks。

```
stopbw  
configctl restart  
startbw
```

参考

HTTP/2 BroadWorks文档：<https://xchange.broadsoft.com/node/498995>

Exchange上有关替换以前的二进制APNS接口的警报：

<https://xchange.broadsoft.com/node/1053230>

UC-One解决方案指南：<https://xchange.broadsoft.com/node/1049202>

请参阅ap354313上22.0的补丁说明：<https://xchange.broadsoft.com/node/496044>

请注意，ap354313适用于平台以及AS、EMS、HZS、PS、NS、NFM、UMS和XSP，以便将Java更新为8.0_102b，这是22.0上的XSP与HTTP/2配合使用的要求，并不意味着UMS也必须在22.0上。

连接评估客户端

<https://apps.apple.com/in/app/uc-one-connect-evaluation/id1114743230>