

Fehlerbehebung APNS "400 - fehlerhafte Anforderung" Fehler

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Fehlerbehebung](#)

[Lösung](#)

[Überprüfung](#)

Einleitung

Dieses Dokument beschreibt die Fehlerbehebung bei APNS-Fehlern mit der Bezeichnung "400 Bad Request". Dieses bekannte Problem wurde im Cisco Bug [IDCSCvi01660](#) dokumentiert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- **Apple Push Notifications** Konfiguration.
- **Apple Push Notifications** Funktionalität.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Hardware- und Softwareversionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn in Ihrem Cluster Push-Benachrichtigungen aktiviert sind, senden Cisco Unified Communications Manager und der IM and Presence Service Push-Benachrichtigungen entweder über den Apple Cloud- oder den Google Cloud-Service an kompatible Cisco Jabber- oder WebEx-Clients, die auf iOS- oder Android-Geräten ausgeführt werden. Push-Benachrichtigungen

ermöglichen die Kommunikation Ihres Systems mit dem Client, auch nachdem dieser in den Hintergrundmodus (auch als "Suspended Mode" bezeichnet) gewechselt ist. Ohne Push-Benachrichtigungen kann das System möglicherweise keine Anrufe oder Nachrichten an Clients senden, die in den Hintergrundmodus gewechselt sind.

Zur Authentifizierung mit der Cisco Cloud generiert Ihr Cisco Communications Manager Server im Rahmen des Onboarding-Prozesses ein Token. Wenn Sie eine "400 Bad Request"-Nachricht erhalten, ist das Systemzugriffstoken für den Push-Benachrichtigungsdienst abgelaufen, und Sie müssen das Zugriffstoken manuell entsprechend der Dokumentation aktualisieren:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/push_notifications/cucm_b_push-notifications-deployment-guide/cucm_b_push-notifications-deployment-guide_chapter_01.html?bookSearch=true

Fehlerbehebung

Legen Sie die nächsten zu debuggenden Protokolle fest, und erfassen Sie diese mit dem Real Time Monitoring Tool:

Cisco Unified Communications Manager :

Cisco Push Notification Service

Cisco Management Agent-Service

Cisco Unified Communications Manager IM und Presence:

Cisco XCP-Konfigurations-Manager

Cisco XCP Router

Aus den Protokollen des Cisco Push Notification Service geht hervor, dass der CUCM mehrere 400 Antworten Beim Abrufen des Tokens, das APNS fehlschlägt, erhöhen sich die Zähler nicht:

```
2024-07-16 15:09:50,514 DEBUG [Timer-144] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:19:51,007 DEBUG [Timer-145] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:29:51,605 DEBUG [Timer-146] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:39:52,096 DEBUG [Timer-147] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:49:52,565 DEBUG [Timer-148] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:59:53,032 DEBUG [Timer-149] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400
```

Auf den Protokollen des Cisco XCP-Routers wird eine ungültige Antwort zu der Zeit angezeigt, zu der der Anruf getätigt wurde:

```
2024-07-16 17:21:43,464 DEBUG [Timer-1382] xmlframework.XCPConfigMgr - FetchAndStoreAccessToken: Calling createAccessToken() with granttype:refresh_token,
```

```
refreshToken:MTc2YzFhN2YtMDA1Ny00MTVILWJGZmMjcwYTU3MjY1NGI1NzItZmE0, accessTokenURL proxyUsername null 2024-07-16 17:21:43,468 INFO [Timer-1382] utilities.CloudOnboarding - TRACKING ID:::.....FOS_e8e8ee93-818f-4fe5-8a23-6b08a879b91b 2024-07-16 17:21:43,790 ERROR [Timer-1382] utilities.TomcatTrustManager - checkServerTrusted:entered 2024-07-16 17:21:43,791 ERROR [Timer-1382] utilities.TomcatTrustManager - checkServerTrusted:entered 2 2024-07-16 17:21:43,958 DEBUG [Timer-1382] xmlframework.XCPCConfigMgr - XCPCConfigMgr:Inside responseStatus() 2024-07-16 17:21:43,958 ERROR [Timer-1382] xmlframework.XCPCConfigMgr - 400 Bad Request: invalid_request, unsupported_grant_type, invalid_client, invalid_refresh_token, tokenlimit_reached 2019-07-16 17:21:43,958 DEBUG [Timer-1382] xmlframework.XCPCConfigMgr - XCPCConfigMgr:FetchAndStoreAccessToken: Inside Finally Block
```

Dies ist eine bekannte Cisco Bug-ID ([CSCvi01660](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvi01660)).

Lösung

Erstellen Sie ein Laborsystem, und aktualisieren Sie den Refresh-Token vom Labor auf das Produktionssystem.

Führen Sie nach der Bereitstellung des Laborsystems die folgenden Schritte aus:

Schritt 1:

Öffnen Sie auf Ihrem Call Manager-Publisher eine CLI-Sitzung, führen Sie den Befehl "run sql select * from machine account details" aus, und speichern Sie die gesamte Ausgabe in einer TXT-Datei:

```
admin:run sql select * from machineaccountdetails
pkid                               refreshtoken
  accesstokenurl                    alarmurl                    pushmsurl
=====
=====
=====
e40c24c0-cd4c-4256                 OGYyZGI2MWMtNjUwYy00Y2FiLThh
efreshToken https://idbroker.webex.com/idb/oauth2/v1/access_token https://push.webex.com/fos/api/v1/metrics https://fos-a.webex.com/fos/api/v1/alarm
```

Sobald alle Ergebnisse gespeichert sind, achten Sie besonders auf Ihr Call Manager pkid, zum Beispiel, unsere Laborumgebung ist "e40c24c0-cd4c-4256".

Führen Sie außerdem den Befehl "run sql select * from machine account details" in Ihrer Laborumgebung aus und speichern Sie alle Ausgaben in einer .txt-Datei.

Achten Sie besonders auf das Erfrischungstoken in Ihrer Laborumgebung, da dies das gültige Token ist, das wir verwenden, um das ungültige Token in Ihrer Produktionsumgebung zu ersetzen. In unserem Laborumfeld ist so etwas wie "OGYyZGI2MWMtNjUwYy00Y2FiLThh".

Phase 2:

Wir müssen Ihr aktuelles nicht funktionierendes Aktualisierungstoken durch das gültige

Labortoken ersetzen.

Nachdem Sie Ihr Produktions-PKID gespeichert haben, führen Sie diese SQL-Abfrage in Ihrem Produktions-Call Manager-Publisher aus:

führen Sie `sql update machineAccountDetails set refreshtoken='here goes the valid refresh token of your lab environment'` aus, wobei `pkid='here goes your production pkid'`.

Die vorherige SQL-Abfrage ändert Ihr nicht funktionierendes Token mit dem funktionierenden aus Ihrer Laborumgebung.

Schritt 3:

Nachdem Sie die Systemkontodetails mit dem Aktualisierungstoken für die Übung aktualisiert haben, starten Sie diese Dienste neu:

Cisco Unified Communications Manager ::

- Cisco Management Agent-Service (CMAS)
- Cisco Push Notification Service (CCMPNS)
- Tomcat

Cisco Unified Communications Manager IM und Presence:

- XCP-Konfigurationsmanager
- XCP-Router
- Tomcat

Diese Services müssen nach Geschäftsschluss neu gestartet werden, um Beeinträchtigungen des Service zu vermeiden.

Überprüfung

Führen Sie nun erneut `sql select * from machine account details` auf allen Knoten einschließlich der IMPs aus, und überprüfen Sie jetzt, ob Sie mein Aktualisierungstoken haben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.