

排除CommPilot錯誤

"SSL_ERROR_NO_CIPHER_OVERLAP" ; 故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[背景資訊](#)

[BroadWorks配置](#)

[功能實驗室示例](#)

[組態](#)

[驗證](#)

[連線稽核](#)

[有錯誤的實驗示例](#)

[問題](#)

[組態](#)

[驗證](#)

[連線稽核](#)

[解析](#)

[解析度驗證](#)

簡介

本檔案介紹如何設定BroadWorks和對其進行疑難排解，以避免「SSL_ERROR_NO_CIPHER_OVERLAP」錯誤。

必要條件

需求

思科建議您瞭解BroadWorks平台。

背景資訊

BroadWorks配置

對於Broadworks版本22及更高版本，可以通過在不同配置級別看到的情景通過CLI配置協定和密碼。

。

```
'Interface/Port specific - low level'
```

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols
```

```
CLI/Interface/Http/HttpServer/SSLSettings/Ciphers
```

```
'All interfaces - mid level'  
CLI/Interface/Http/SSLCommonSettings/Protocols  
CLI/Interface/Http/SSLCommonSettings/Ciphers
```

```
'Generic system level - high level'  
CLI/System/SSLCommonSettings/JSSE/Protocols  
CLI/System/SSLCommonSettings/JSSE/Ciphers
```

名為SSLCommonSettings的上下文引用了SSL層次結構中不太特定的項，名為SSLSettings的上下文引用了層次結構中比較特定的項。

功能實驗室示例

組態

繫結到特定介面和埠且未定義密碼的低級配置：

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443  
Protocol Name  
=====
```

```
TLsv1.1  
TLsv1.2  
TLsv1  
  
CLI/Interface/Http/HttpServer/SSLSettings/Ciphers> get 172.16.30.146 443  
Cipher Name  
=====
```

0 entry found.

驗證

使用 curl 指令：

```
$ curl -v -k https://172.16.30.146  
* About to connect() to 172.16.30.146 port 443 (#0)  
* Trying 172.16.30.146...  
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)  
* Initializing NSS with certpath: sql:/etc/pki/nssdb  
* skipping SSL peer certificate verification  
* SSL connection using TLS_RSA_WITH_AES_256_CBC_SHA256 <-----  
* Server certificate:  
* subject:  
E=broadworks_tac@cisco.com,CN=*.calo.cisco.com,OU=BroadworksTAC,O=TestIssuer,ST=Veracruz,C=MX  
* start date: Apr 04 20:39:56 2022 GMT  
* expire date: Apr 04 20:39:56 2023 GMT  
* common name: *.calo.cisco.com  
* issuer: CN=Root CA test,OU=BroadworksTAC,O=TestIssuer,L=Teocolutla,ST=Veracruz,C=MX  
>GET / HTTP/1.1  
>User-Agent: curl/7.29.0  
>Host: 172.16.30.146  
>Accept: /*/*  
>  
<HTTP/1.1 302 Found
```

在這裡，它已成功通過TLSv1.2與密碼TLS_RSA_WITH_AES_256_CBC_SHA256連線。

連線稽核

要驗證接受的協定和密碼，請執行以下操作：

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 04:26 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.00013s latency).
PORT STATE SERVICE VERSION
443/tcp open ssl/https?
| ssl-enum-ciphers:
| TLSv1.0:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
| TLSv1.1:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - strong
| TLS_ECDHE_RSA_WITH_RC4_128_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_RSA_WITH_AES_256_CBC_SHA - strong
| TLS_RSA_WITH_AES_256_CBC_SHA256 - strong
| TLS_RSA_WITH_RC4_128_SHA - strong
| compressors:
| NULL
|_ least strength: strong
```

有錯誤的實驗示例

問題

觀察到錯誤 — 通過瀏覽器顯示「SSL_ERROR_NO_CIPHER_OVERLAP」。

```
# curl -v https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
```

```
* Initializing NSS with certpath: sql:/etc/pki/nssdb * CAfile: /etc/pki/tls/certs/ca-bundle.crt
CApath: none
* NSS error -12286 (SSL_ERROR_NO_CYPHER_OVERLAP)
* Cannot communicate securely with peer: no common encryption algorithm(s).
* Closing connection 0 curl: (35) Cannot communicate securely with peer: no common encryption
algorithm(s).
```

組態

與特定介面和埠繫結的低級配置，使用TLSv1.2協定集和TLSv1.0密碼
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256設定：

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
=====
TLSv1.2
```

```
CLI/Interface/Http/SSLCommonSettings/Ciphers> get
Cipher Name
=====
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
```

驗證

使用 curl 指令：

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* NSS error -12286 (SSL_ERROR_NO_CYPHER_OVERLAP)
* Cannot communicate securely with peer: no common encryption algorithm(s).
* Closing connection 0
curl: (35) Cannot communicate securely with peer: no common encryption algorithm(s).
```

連線稽核

要驗證接受的協定和密碼，請執行以下操作：

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146

Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 05:31 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.000049s latency).
PORT STATE SERVICE VERSION
443/tcp open https?
| ssl-enum-ciphers:
|_ TLSv1.2: No supported ciphers found
從工具的結果可以看到TLSv1.2協定可用，但沒有受支援的密碼。
```

解析

刪除TLSv1.1密碼的 CLI/Interface/Http/SSLCommonSettings/Ciphers ，然後再次開啟所有TLSv1.2密碼（或新增TLSv1.2密碼）。

```
CLI/Interface/Http/HttpServer/SSLSettings/Protocols> get 172.16.30.146 443
Protocol Name
=====
TLSv1.2
```

```
CLI/Interface/Http/HttpServer/SSLSettings/Ciphers> get 172.16.30.146 443
Cipher Name
=====
0 entry found.
```

```
CLI/Interface/Http/SSLCommonSettings/Ciphers> get
Cipher Name
=====
0 entry found.
```

解析度驗證

```
$ curl -v -k https://172.16.30.146
* About to connect() to 172.16.30.146 port 443 (#0)
* Trying 172.16.30.146...
* Connected to 172.16.30.146 (172.16.30.146) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 <-----
* Server certificate:
* subject:
E=broadworks_tac@cisco.com,CN=*.calo.cisco.com,OU=BroadworksTAC,O=TestIssuer,ST=Veracruz,C=MX
* start date: Apr 04 20:39:56 2022 GMT
* expire date: Apr 04 20:39:56 2023 GMT
* common name: *.calo.cisco.com
* issuer: CN=Root CA test,OU=BroadworksTAC,O=TestIssuer,L=Tecolutla,ST=Veracruz,C=MX
>GET / HTTP/1.1
>User-Agent: curl/7.29.0
>Host: 172.16.30.146
>Accept: */*
>
<HTTP/1.1 302 Found
```

```
$ nmap -sV --script ssl-enum-ciphers -p 443 172.16.30.146
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2022-05-09 05:44 EDT
Nmap scan report for r23xsp01.calo.cisco.com (172.16.30.146)
Host is up (0.000063s latency).
PORT STATE SERVICE VERSION
443/tcp open https?
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - strong
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。