

Problembehandlung bei CommPilot-Fehler "SSL_ERROR_NO_CIPHER_OVERLAP"

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Hintergrundinformationen](#)

[BroadWorks-Konfiguration](#)

[Beispiel für ein funktionales Labor](#)

[Konfiguration](#)

[Verifizierung](#)

[Verbindungs-Audit](#)

[Beispiel mit Fehler](#)

[Problem](#)

[Konfiguration](#)

[Verifizierung](#)

[Verbindungs-Audit](#)

[Auflösung](#)

[Auflösungsüberprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie BroadWorks konfigurieren und Fehler beheben, um den Fehler "SSL_ERROR_NO_CIPHER_OVERLAP" zu vermeiden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der BroadWorks-Plattform verfügen.

Hintergrundinformationen

BroadWorks-Konfiguration

Bei Broadworks-Versionen 22 und höher können die Protokolle und Chiffren über die CLI konfiguriert werden. Dies geschieht über die Kontexte, die auf verschiedenen Konfigurationsebenen angezeigt werden.

```
'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
```

Ein Kontext mit dem Namen `SSLCommonSettings` verweist auf ein weniger spezifisches Element aus der SSL-Hierarchie, und ein Kontext mit dem Namen `SSLSettings` verweist auf ein spezifischeres Element aus der Hierarchie.

Beispiel für ein funktionales Labor

Konfiguration

Low-Level-Konfiguration mit spezifischer Schnittstelle und Port ohne definierte Chiffren:

```
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.
```

Verifizierung

Überprüfen Sie die Konfiguration mit dem `curl` command:

```
$ 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
```

Hier wurde eine erfolgreiche Verbindung über TLSv1.2 mit der Chiffre

TLS_RSA_WITH_AES_256_CBC_SHA256 hergestellt.

Verbindungs-Audit

So überprüfen Sie die akzeptierten Protokolle und Chiffren:

```
$ 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
```

Beispiel mit Fehler

Problem

Fehler festgestellt - "SSL_ERROR_NO_CIPHER_OVERLAP" über den Browser.

```
# 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).
```

Konfiguration

Low-Level-Konfiguration, verknüpft mit der spezifischen Schnittstelle und dem Port, wobei das TLSv1.2-Protokoll mit dem TLSv1.0-Cipher TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256-Satz festgelegt ist:

```
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
```

Verifizierung

Überprüfen Sie die Konfiguration mit dem `curl` command:

```
$ 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).
```

Verbindungs-Audit

So überprüfen Sie die akzeptierten Protokolle und Chiffren:

```
$ 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
```

Aus den Ergebnissen des Tools geht hervor, dass das TLSv1.2-Protokoll verfügbar ist, es jedoch keine unterstützten Chiffren gibt.

Auflösung

Löschen Sie den TLSv1.1-Chiffren unter **CLI/Interface/Http/SSLCommonSettings/Ciphers** , und öffnen Sie dann alle TLSv1.2-Verschlüsselungen erneut (oder fügen Sie eine TLSv1.2-Verschlüsselung hinzu).

```
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.
```

Auflösungsüberprüfung

```
$ 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
```

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.