

# Konfigurieren des NGINX-Proxys für die Integration mit einer Agent Assist-Lösung

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Konfigurieren](#)

[Bereitstellung](#)

[NGINX-Installationsdetails](#)

[Konfigurationsschritte](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie einen NGINX-Proxyserver für eine Integration mit einer Cisco Agents Assist-Lösung konfigurieren.

Unterstützt von Gururaj B. T. und Ramiro Amaya, Cisco Engineers.

## Voraussetzungen

### Anforderungen

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

- Cisco Unified Border Element (CUBE)
- WebEx Contact Center Artificial Intelligence Services (WCCAI)
- NGINX-Proxy
- Austausch von Sicherheitszertifikaten

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco Unified Border Element (CUBE)
- WebEx Contact Center Artificial Intelligence Services (WCCAI)
- NGINX-Proxy
- Web-Socket-Anschluss (WSConnector)

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 potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrund

In einer Agent Answers-Bereitstellung kommuniziert CUBE mit dem WSConnector-Service, der als Teil der WCCAI-Services bereitgestellt wird. Damit die Kommunikation hergestellt werden kann, benötigt CUBE Internetzugang. Einige der Unternehmen haben Einschränkungen, den direkten Internetzugang zu den Lösungskomponenten bereitzustellen. In diesem Szenario empfiehlt Cisco die Verwendung des Proxys, der WebSocket unterstützt. In diesem Dokument wird die erforderliche Konfiguration für den NGINX-Proxy erläutert, der WebSocket unterstützt.

## Konfigurieren

### Bereitstellung

CUBE —<websocket>—NGINX Proxy —<websocket>—WSconnect

Derzeit unterstützt CUBE keine CONNECT-Methode zum Tunnel der TCP-Verbindung von CUBE zu WSConnector. Cisco empfiehlt die Hop-by-Hop-Verbindung über den Proxy. Mit dieser Bereitstellung verfügt NGINX über eine gesicherte Verbindung von CUBE am Eingangs- und am Ausgangs-Bein zum WSConnector.

### NGINX-Installationsdetails

Betriebssystem-Details: Cent OS centos-release-7-8.2003.0.el7.centos.x86\_64

NGINX-Version: Nginx/1.19.5

### Konfigurationsschritte

Schritt 1: Installation von NGINX: Befolgen Sie die Installationsschritte im NGINX-Portal. Folgen Sie diesem Link: [Administratoranleitung für NGINX](#).

Schritt 2: Selbstsigniertes NGINX-Zertifikat und Schlüsselerstellung. Führen Sie diesen Befehl auf dem NGINX-Proxyserver aus:

```
sudo openssl req -x509 -knoten -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```

Schritt 3: Bearbeiten Sie die Datei `nginx.conf`.

```
worker_process 1;  
error_log logs/error.log debug;
```

```
event {  
worker_connections 1024;
```

```

}
http {
    schließen mime.types ein;
    default_type application/octet-stream;
    sendfile on;
    Keepalive_timeout 65;
    server{
        listen Sie 8096 ssl;
        server_name ~.+
        Anzahl der DNS-Resolver für Weiterleitungsproxen
        resolver <DNS_Server IP:PORT>;
        proxy_read_timeout 86400s;
        proxy_send_timeout 86400s;
        client_body_timeout 86400s;
        Keepalive_timeout 86400s;
        # Weiterleitungsproxy für Nicht-CONNECT-Anfrage
        location / {
            proxy_pass https://$http_host;
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade
            proxy_set_header Connection $connection_upgrade;
            proxy_set_header Host $host;
            proxy_ssl_certificate <nginx_selfsigned_certificate>
            proxy_ssl_certificate_key <nginx_certificate_key_path>
            proxy_ssl_trusted_certificate <WsConnector CA-Zertifikat>;
            proxy_ssl_logs TLSv1.2;
        }
        #ssl on;
        ssl_certificate <nginx_selfsigned_certificate_path>
        ssl_certificate_key <nginx_certificate_key_path>
        ssl_session_cache shared:SSL:1m;
        ssl_session_timeout 5 m;
        ssl_ciphers HIGH:!aNULL:!MD5;
        ssl_prefer_server_ciphers on;
    }
}

```

Schritt 4: Um den Status des NGINX-Proxys zu überprüfen, führen Sie den folgenden Befehl aus:  
**systemctl status nginx**

## Überprüfung

Hier sind einige Befehle, mit denen Sie die NGINX-Konfiguration überprüfen können.

antwort: So überprüfen Sie, ob die NGINX-Konfiguration korrekt ist.

**nginx -t**

b) So starten Sie den Nginx-Server neu

**systemctl restart nginx**

c) So prüfen Sie die Nginx-Version

**Nginx-V**

d) So stoppen Sie den Nginx

```
systemctl stop nginx  
e So starten Sie den Nginx  
systemctl start nginx
```

## Fehlerbehebung

Es gibt keine Schritte zur Fehlerbehebung für diese Konfiguration.

## Zugehörige Informationen

[NGINX-Administratorhandbuch](#)

[Nützliche Beispiele für NGINX-Befehle](#)

[Erstellen eines selbstsignierten SSL-Zertifikats für NGINX](#)

[Technischer Support und Dokumentation für Cisco Systeme](#)