

エージェントアシストソリューションとの統合のためのNGINXプロキシの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景](#)

[設定](#)

[導入](#)

[NGINXのインストールの詳細](#)

[設定手順](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Agents Assistソリューションとの統合のためにNGINXプロキシサーバを設定する方法について説明します。

著者：シスコエンジニア、Gruraj B. T.およびRamiro Amaya

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Border Element (CUBE)
- Webex Contact Center Artificial Intelligence Services(WCCAI)
- NGINXプロキシ
- セキュリティ証明書交換

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Unified Border Element (CUBE)
- Webex Contact Center Artificial Intelligence Services(WCCAI)
- NGINXプロキシ
- Webソケットコネクタ(WSCconnector)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

Agent Answers展開では、CUBEはWCCAIサービスの一部として展開されたWSConnectorサービスと通信します。通信を確立するには、CUBEにインターネットアクセスが必要です。一部の企業では、ソリューションコンポーネントへの直接インターネットアクセスを提供することに制限があります。このシナリオでは、WebSocketをサポートするプロキシの使用を推奨します。このドキュメントでは、websocketをサポートするNGINXプロキシに必要な設定について説明します。

設定

導入

CUBE —<websocket>—NGINXプロキシ – <websocket>—WSconnector

現在、CUBEはCUBEからWSConnectorへのTCP接続をトンネルするためのCONNECTメソッドをサポートしていません。シスコでは、プロキシ経由のホップ間接続を推奨しています。この導入により、NGINXは着信ログのCUBEからセキュアな接続を確立し、発信ログのWSConnectorに対する別のセキュアな接続を確立します。

NGINXのインストールの詳細

OSの詳細：Cent OS centos-release-7-8.2003.0.el7.centos.x86_64

NGINXバージョン：NGINX/1.19.5

設定手順

ステップ1:NGINXのインストール：NGINXポータルのインストール手順に従います。 次のリンクを参照してください。[NGINX管理ガイド](#)』を参照してください。

ステップ2:NGINX自己署名証明書とキーの作成。NGINXプロキシサーバで次のコマンドを実行します。

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

ステップ3: nginx.confファイルを編集します。

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

```
イベント{  
worker_connections 1024;
```

```

}
http{
include mime.types;
default_type application/octet-stream;
sendfile on;
keepalive_timeout 65;
server{
listen 8096 ssl、
server_name ~ +;
# dns resolver used by forward proxying
resolver <DNS_Server IP:PORT>;
proxy_read_timeout 86400s;
proxy_send_timeout 86400s;
client_body_timeout 86400s;
keepalive_timeout 86400s;
非CONNECT要求の転送プロキシ数
location / {
proxy_pass https://$http_host;
proxy_http_version 1.1;
proxy_set_header アップグレード $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 Certificate>;
proxy_ssl_protocols TLSv1.2;
}
#ssl
ssl_certificate <nginx_selfsigned_certificate_path>;
ssl_certificate_key <nginx_certificate_key_path>;
ssl_session_cache shared:SSL:1m;
ssl_session_timeout 5m;
ssl_ciphers HIGH:!aNULL:!MD5;
ssl_prefer_server_ciphers on;
}
}

```

ステップ4:NGINXプロキシのステータスを確認するには、次のコマンドを実行します。 **systemctl status nginx**

確認

NGINX設定の確認に使用できるコマンドを次に示します。

a.NGINXの設定が正しいことを確認します。

nginx -t

b.nginxサーバを再起動するには

systemctl restart nginx

c. nginxバージョンを確認するには

nginx -V

d.nginxを停止するには

```
systemctl stop nginx  
e.nginxを開始するには  
systemctl start nginx
```

トラブルシューティング

この設定をトラブルシューティングする手順はありません。

関連情報

- [NGINX管理者ガイド](#)
- [便利なNGINXコマンドの例](#)
- [NGINX用の自己署名SSL証明書を作成する方法](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)