

Configure NGINX Proxy for Integration with an Agent Assist Solution

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background](#)

[Configure](#)

[Deployment](#)

[NGINX Installation Details](#)

[Configuration Steps](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure a NGINX proxy server for an integration with a Cisco Agents Assist solution.

Contributed by Gururaj B. T. and Ramiro Amaya, Cisco Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Border Element (CUBE)
- Webex Contact Center Artificial Intelligence Services (WCCAI)
- NGINX Proxy
- Security certificates exchange

Components Used

The information in this document is based on these software versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

In an Agent Answers deployment CUBE communicates with WSConnector service deployed as part of WCCAI services. In order for the communication to be established CUBE needs Internet access. Some of the enterprises have restriction to provide the direct Internet access to the solution components. In this scenario Cisco recommends the usage of proxy which has the support for WebSocket. This document explains the required configuration for NGINX proxy which has the support for websocket.

Configure

Deployment

CUBE ----<websocket>---NGINX Proxy ----<websocket>---WSconnector

Currently CUBE does not support CONNECT method to tunnel the TCP connection from CUBE to WSConnector. Cisco recommends the hop-by-hop connection through proxy. With this deployment NGINX has a secured connection from CUBE on the incoming leg and another secured connection on the outbound leg towards WSConnector

NGINX Installation Details

OS details : Cent OS centos-release-7-8.2003.0.el7.centos.x86_64
NGINX Version : nginx/1.19.5

Configuration Steps

Step 1. Installation of NGINX: Follow the installation steps from NGINX portal. Follow this link: [NGINX Admin Guide](#).

Step 2. NGINX Self Signed Certificate and Key creation. Execute this command on the NGINX proxy server:

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

Step 3. Edit the **nginx.conf** file.

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

events {
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;
# forward proxy for non-CONNECT request
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 Certificate>;
proxy_ssl_protocols 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 5m;
ssl_ciphers HIGH:!aNULL:!MD5;
ssl_prefer_server_ciphers on;
}
}

```

Step 4. To check the status of the NGINX proxy, execute the command: **systemctl status nginx**

Verify

Here are some commands that you can use to verify the NGINX configuration.

a. To check that the NGINX configuraion is correct.

nginx -t

b. To restart the nginx server

systemctl restart nginx

c. To check the nginx version

nginx -V

d. To stop the nginx

systemctl stop nginx

e. To start the nginx

systemctl start nginx

Troubleshoot

There are not steps to troubleshoot this configuration.

Related Information

- [NGINX Admin Guide](#)
- [Useful NGINX Command Examples](#)
- [How to create a self-signed ssl certificate for NGINX](#)
- [Technical Support & Documentation - Cisco Systems](#)