Configure Host Entry for SDWAN vBond Controller

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Scope
- Considerations

Problem: DNS Scenarios with FQDN Entry

- Scenario 1. DNS Entry with FQDN, Resolution Works
- Scenario 2. DNS Entry with FQDN, Resolution Fails

Solution: Configure DNS Entry with Static IP

- Configuration for vEdge
- Configuration for Controllers
- Configuration for Cisco Edge Router
- Additional Configuration
- Common Configuration Issues

Related Information

Introduction

This document describes how to configure the host entry for Software Defined Wide Area Network (SD-WAN) Authenticator.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco SD-WAN Authenticator
- Cisco Software-defined Wide Area Network (SD-WAN)

Components Used

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

- Manager Software 20.12.8.1
- Controller Software 20.12.8.1
- Authenticator Software 20.12.8.1
- Cisco Edge (cEdge) Router Software 17.12.8
- Viptela Edge (vEdge) Router Software 20.9.10

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.

Scope

Configure the vBond host entry when there are Domain Name Server (DNS) issues such as, but not limited to:

- DNS connectivity
- Cannot translate Fully Qualified Domain Name (FQDN)

Considerations

This document assumes:

- WAN SD-WAN Edge routers are fully functional
- Basic Configuration is applied to the controllers
- Controllers and Edge Routers have connectivity between them
- The network has Authenticator, Manager, and Controllers that are up and in a healthy state

---

Problem: DNS Scenarios with FQDN Entry

Scenario 1. DNS Entry with FQDN, Resolution Works

This is an example of a common configuration with FQDN:

```
vedge# show running-config system vbond
system
 vbond vbond.lab.sdwan
!
```

```
vedge# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 primary
!
```

This is the expected result when DNS translation works properly:

```
vedge# nslookup vbond.lab.sdwan
nslookup in VPN 0:
Server:    192.168.1.11
Address 1: 192.168.1.11

Name:      vbond.lab.sdwan
Address 1: 192.168.2.1 vbond.lab.sdwan
Address 2: 192.168.2.2 vbond.lab.sdwan

vedge# ping vbond.lab.sdwan
Ping in VPN 0
PING vbond.lab (192.168.2.1) 56(84) bytes of data.
64 bytes from vbond.lab (192.168.2.1): icmp_seq=1 ttl=63 time=26.1 ms
```

Scenario 2. DNS Entry with FQDN, Resolution Fails

This configuration is the same as the previous scenario:

```
vedge# show running-config system vbond
system
 vbond vbond.lab.sdwan
!
vedge# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 primary
!
```

This time, DNS resolution fails:

```
vedge#nslookup vbond.lab.sdwan
nslookup in VPN 0:
Server: 192.168.1.11
Address 1: 192.168.1.11
nslookup: can't resolve 'vbond.lab.sdwan'
vedge#
vedge# ping vpn 0 vbond.lab.sdwan
Ping in VPN 0
ping: vbond.lab.sdwan: Name or service not known
```

```
vedge#
```

Solution: Configure DNS Entry with Static IP

Configuration for vEdge

Configure the host command with FQDN and vBond IPs:

```
vedge# show running-config vpn 0 host
vpn 0
 host vbond.lab.sdwan ip 192.168.2.1 192.168.2.2
!
vedge#
```

Run the **nslookup** command for validation purposes:

```
vedge# nslookup vbond.lab.sdwan
nslookup in VPN 0:
Server: 192.168.1.11
Address 1: 192.168.1.11

Name: vbond.lab.sdwan
Address 1: 192.168.2.1 vbond.lab.sdwan
Address 2: 192.168.2.2 vbond.lab.sdwan
```

 **Tip**: You can analyze logs of vDebug file from admin-tech if vBond resolution fails.

Configuration for Controllers

The configuration is the same as vEdge devices. This is an example of the controller:

```
vsmart# show running-config system vbond
system
 vbond vbond.lab.sdwan
!
vsmart# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 primary
!
```

```
vsmart# show running-config vpn 0 host
vpn 0
 host vbond.lab.sdwan ip 192.168.2.1 192.168.2.2
!
vsmart#
```

Configuration for Cisco Edge Router

This is the configuration for the Cisco Edge Router:

```
cedge#show sdwan run system | include vbond
vbond vbond-list
cedge#
cedge#show sdwan run | include host
ip host vbond-list 192.168.2.1 192.168.2.2
cedge#
```

Run ICMP for validation purposes:

```
cedge#ping vbond-list
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.149, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 27/29/31 ms
cedge#
```

Additional Configuration

Set the primary and secondary DNS server as a redundancy method. This is in case one server fails and the other forms a DNS resolution.

The next example applies to vEdge, Manager, and Controller:

```
VM# show running-config vpn 0 dns
vpn 0
 dns 192.168.1.11 secondary
 dns 192.168.1.12 primary
!
```

The next example applies for cEdge:

```
cedge#show run | i name
ip name-server 192.168.30.32 192.168.48.89
cedge#
```

Common Configuration Issues

- Wrong Authenticator IP addresses.
- Inconsistent name resolution among controllers and WAN Edge routers.
- Use the same IP address in the Authenticator. Each Authenticator must have its own IP address configured as the **vBond local** command.
- You can have multiple WAN interfaces such as Gigabitethernet1 and Gigabitethernet2, however, the DNS server is only reachable via Gigabitethernet1, therefore, the control connection fails.

Related Information

- Host Entry for Version SD-WAN Version 20.15
- Collect Admin-Tech
- Technical Support & Documentation - Cisco Systems