

Catalyst SD-WAN AppQoE DRE – トポロジ、設定、検証

内容

[はじめに](#)

[背景説明](#)

[DRE最適化](#)

[コントロール接続](#)

[ISNおよびESNを使用したAppQoE DREセットアップを構築する手順](#)

[1. システム \(インターフェイスおよびハードウェア \) とトポロジ](#)

[1.1. トポロジとインターフェイス](#)

[1.2. ディスク要件](#)

[1.3. SD-WANファブリックへのデバイスの追加](#)

[1.4. C8000vの詳細](#)

[2. ブランチ : AppQoE ISNの設定](#)

[3. DC/Hub:AppQoE ESN構成](#)

[4. DC/Hub:AppQoE SC構成](#)

[5. 中央集中型トラフィックデータポリシー](#)

[A. ブランチISN](#)

[B. DC/ハブSC](#)

[検証 – CLI](#)

[ブランチISN](#)

[DC/ハブSC](#)

[DC/ハブESN](#)

[検証 – ダッシュボード](#)

[ブランチISN](#)

[DC/ハブSC](#)

[DC/ハブESN](#)

[負荷計算](#)

[パフォーマンスと拡張性](#)

[FAQ](#)

はじめに

このドキュメントでは、データ冗長性排除(DRE)最適化のセットアップを作成および設定する方法について説明します。

背景説明

このドキュメントの目的は、[統合アプリケーションQuality of Experience\(AppQoE\)ソリューション](#)の一部であるDREのセットアップを作成および設定する方法に関するガイダンスの出発点を提

供し、エンドツーエンドの一貫したポリシーフレームワークとモニタリングを提供して、多数の導入ユースケースに対応することです。

AppQoEソリューションの構成要素：

- 前方誤り訂正(FEC)およびパケット複製(PD)：パケット損失の問題に対処します。FECについては、[を参照してください](#)。
- TCP最適化：WAN遅延の問題に対処します。片面TCPオプトユースケースについては、[を参照してください](#)。
- DRE最適化：低帯域幅の問題に対応。通常、DRE最適化はTCP最適化とともに使用されません。

[既存のCCO](#) DREドキュメントには、完全なエンドツーエンドのプロセス説明は含まれていません。このドキュメントでは、DREソリューションのエンドツーエンドの説明を段階的に示します。

DREの機能に関する技術的な詳細な説明は、この文書の適用範囲外です。技術的な詳細とDRE機能の詳細については、[このドキュメント](#)を参照してください。

DRE最適化

DREは、以前に見られたパターンをキャッシュすることによって冗長データを削除するデュアルサイドソリューションです。DRE機能を、WAN経由のデータ量を削減する圧縮機能を提供するLempel-Ziv-Welch(LZW)アルゴリズムと組み合わせることで、Unified Threat Defense(UTD)およびSecure Sockets Layer(SSL)プロキシとの完全にセキュアな統合ソリューションが実現します。

アプリケーションやプロトコルに依存せず、WANトラフィックを約60 ~ 90 %削減するクラウド対応ソリューションです。

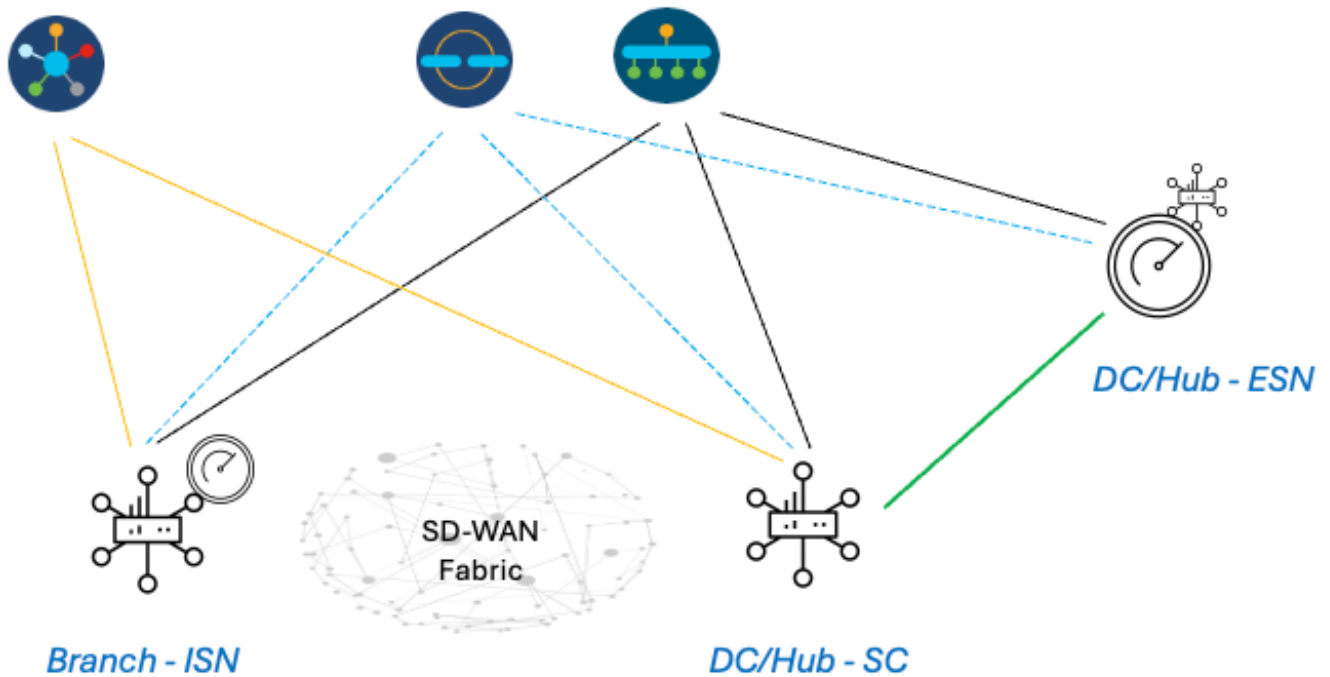
スケーラブルなソリューションを実現するために、さまざまな導入シナリオがサポートされています。

- この統合ソリューションは、Integrated Service Node(ISN)と呼ばれるブランチサービスを導入するためのワンボックスソリューションを提供します。
- 外部サービスノード(ESN)は、外部サービスノード展開 (通常はデータセンターとハブ) のエッジルータやサービスコントローラ(SC)を代行受信しないように分離されています。アプリケーショントラフィックに基づくフローのリダイレクトは、データポリシーを使用して実現されます。

コントロール接続



注:ESNは、コントローラ（以前のvSmart）と制御接続を形成しません。 ESNはSD-WAN Managerへの制御接続を備えています。



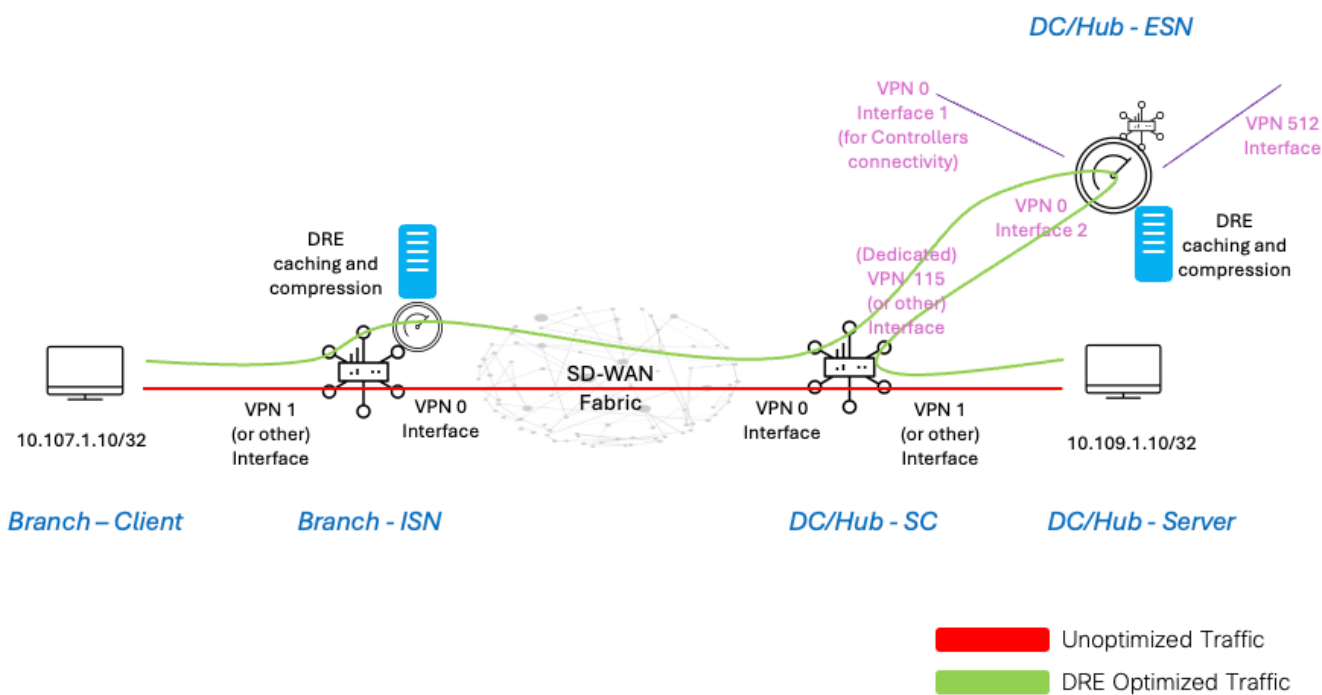
ISNおよびESNを使用したAppQoE DREセットアップを構築する手順

1. システム (インターフェイスおよびハードウェア) とトポロジ

1.1. トポロジとインターフェイス

ESNには次のインターフェイスが必要です。

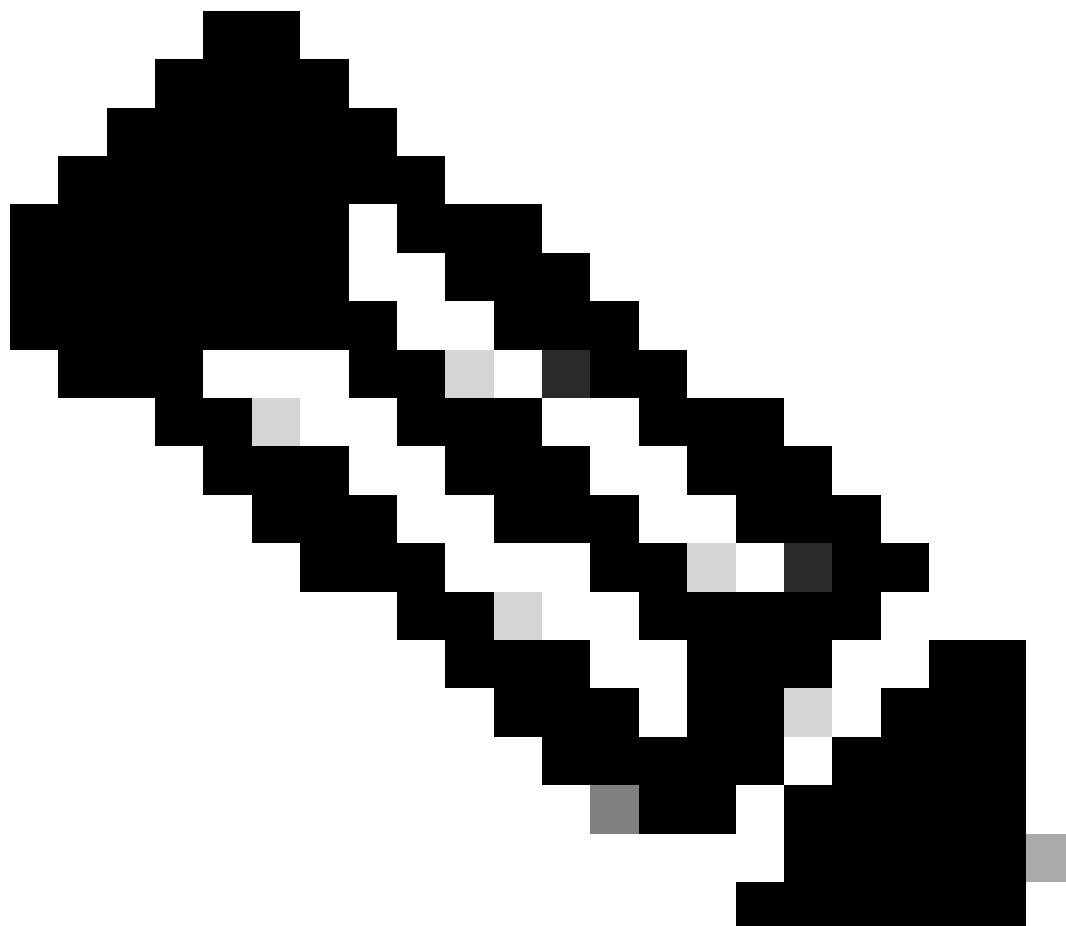
- コントローラ(ManagerおよびValidator (一時的))へのVPN0インターフェイス接続。
ESNからコントローラへの接続は、直接またはSC経由で行うことができます。ESNに追加のWAN回線が不要になるため、SCを使用することをお勧めします。
- サービスコントローラへの接続用の別のVPN0インターフェイス。
- オプション : VPN512管理インターフェイス。



1.2.ディスク要件

ラボのセットアップでは、DRE最適化が動作するのに150 GBのディスクで十分です。

これは、ラボ環境での機能検証にのみ有効で、実稼働用ではありません。正確なディスクおよびその他の推奨事項については、[このCCOリンク](#)を確認してください。



注：この追加のディスク要件は、ISNおよびESNに対してのみ適用されます。SCでは必要ありません。

1.3. SD-WANファブリックへのデバイスの追加

- テンプレートの使用（20.6/17.6以降で使用可能）：AppQoe機能テンプレート。追加テンプレートとしてデバイステンプレートに指定できます。
- 構成グループの使用（20.14/17.14以降で使用可能）：構成グループのサービス/LANプロファイルで使用可能なAppQoE機能パーセル。

1.4. C8000vの詳細

c8kvを使用している場合は、アプリケーション負荷の高いCPUプロファイル設定が有効になっていることを確認します。[これ](#)は役に立つ記事だ。

2. ブランチ：AppQoE ISNの設定

デバイスモデルのAppQoE機能テンプレートを作成します（ここに示すテンプレートを使用）。

Configuration

Device Templates

Feature Templates

Feature Template

>

AppQoE

>

DRE-IntNode-template

Device Type

C8000v

Template Name

DRE-IntNode-template

Description

Feature Template for Integrated Node

Control Components

Service Node

Control Components

Integrated Service Node

Enable

Controller IP address

192.168.2.1

Service Node IP 1

192.168.2.2

Advanced

DRE Optimization

Resource Profile

default

SSL Decryption

Enable

次に、この機能テンプレートをデバイステンプレートに指定します。

Additional Templates

AppQoE

DRE-IntNode-template

3. DC/Hub:AppQoE ESN構成

デバイスモデルのAppQoE機能テンプレートを作成します。

Configuration

Device Templates

Feature Templates

[Feature Template](#) > [AppQoS](#) > [DRE-feature-template](#)

Device Type C8000v

Template Name [DRE-feature-template](#)

Description [Feature Template for DRE](#)

☐ Control Components ☒ Service Node

Service Node

External Service Node ☒ Enable

Advanced

DRE Optimization [i](#)



Resource Profile



default

SSL Decryption [i](#)

☐ Enable

次に、この機能テンプレートをデバイステンプレートに指定します。

Additional Templates

AppQoE *

[REDACTED]-DRE-feature-template ▼

4. DC/Hub:AppQoE SC構成

デバイスモデルのAppQoE機能テンプレートを作成します。

Configuration

Device Templates Feature Templates

Feature Template > AppQoE > [REDACTED]-DRE-DC2-ServContr-Template

Device Type C8000v

Template Name [REDACTED]-DRE-DC2-ServContr-Template

Description DRE AppQoE Template for DRE Service Controller

☒ Control Components ☐ Service Node

Control Components

Integrated Service Node

☐ Enable

Controller IP address



10.115.1.5

Service VPN



115

Service Nodes



Service Node Group Name



SNG-APPQOE

Service Node IP Addresses

1 Service Node IP Addresses

10.115.1.10

次に、この機能テンプレートをデバイステンプレートに指定します。

Additional Templates

AppQoE

DRE-DC2-ServContr-...

5. 中央集中型トラフィックデータポリシー

- 2つの異なるポリシーが必要です。1つは内部サービスノード(ISN)用、もう1つはサービスコントローラ(SC)用です。
- ポリシーの方向は両方とも'All'である必要があります。
- ISNの場合はService-node-groupを空白にし、SCに指定する必要があります。
- DRE最適化は、通常、TCP最適化とともに使用されます。DREを有効にすると、TCP最適化も有効になります。

この例では、ブランチロケーションのWebクライアントが定義され、DCサイトのWebサーバが定義されています。そのため、対象のトラフィックに合わせて調整できます。

A. ブランチISN

UI - テンプレート

シーケンス1 - クライアント10.107.1.10からサーバ10.109.1.10:

The screenshot displays the 'Custom' configuration page for a 'Sequence Rule'. The 'Match' tab is active, showing the following settings:

- Protocol:** IPv4
- Action:** Accept (selected), Drop
- Match Conditions:**
 - Source Data Prefix List:** Select a data prefix list
 - Source: IP Prefix:** 10.107.1.10/32
 - Destination Data Prefix List:** Select a data prefix list
 - Destination: IP Prefix:** 10.109.1.10/32

The 'Actions' tab is also visible, showing the following settings:

- Accept:** Enabled
- AppQoE Optimization:**
 - ☒ TCP Optimization
 - ☒ DRE Optimization
- Service Node Group:** Example: SNG-APPQOE<1-31>

Buttons at the bottom include 'Cancel' and 'Save Match and Actions'.

シーケンス2 - サーバからクライアントへ :

Custom Data

Sequence Rule Drag and drop to re-arrange rules

Match Actions

Protocol IPv4 | Protocol Source Data Prefix Source Port Destination Data Prefix Destination Region Destination Port TCP Traffic To

Match Conditions

Source Data Prefix List ×

Select a data prefix list

Source: IP Prefix

10.109.1.10/32

Destination Data Prefix List ×

Select a data prefix list

Destination: IP Prefix

10.107.1.10/32

Actions

Accept Enabled

AppQoS Optimization ×

☒ TCP Optimization

☒ DRE Optimization

Service Node Group Example: SNG-APPQOE<1-31>

[Cancel](#) [Save Match and Actions](#)

CLI :

```
ISN# show sdwan policy from-vsmart
```

```
from-vsmart data-policy _CorpVPN_DRE-data-policy-ISN-2
direction all
vpn-list CorpVPN
sequence 1
match
source-ip 10.107.1.10/32
destination-ip 10.109.1.10/32
action accept
tcp-optimization
dre-optimization
sequence 11
match
source-ip 10.109.1.10/32
destination-ip 10.107.1.10/32
action accept
tcp-optimization
dre-optimization
default-action accept
```

```
from-vsmart lists vpn-list CorpVPN
vpn 1
```

B. DC/ハブSC

UI – テンプレート

シーケンス1 -

Custom Data

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Protocol IPv4 | ☒ Accept ☐ Drop | VPN Next Hop Policer Redirect DNS Service Service Chain AppQoE Optimization Loss Correction TLOC

Match Conditions

Source Data Prefix List ×

Select a data prefix list

Source: IP Prefix

10.109.1.10/32

Destination Data Prefix List ×

Select a data prefix list

Destination: IP Prefix

10.107.1.10/32

Actions

Accept Enabled

AppQoE Optimization ×

☒ TCP Optimization

☒ DRE Optimization

Service Node Group SNG-APPQOE

[Cancel](#) [Save Match and Actions](#)

シーケンス2 -

Custom Data

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Protocol IPv4 | Protocol Source Data Prefix Source Port Destination Data Prefix Destination Region Destination Port TCP Traffic To

Match Conditions

Source Data Prefix List ×

Select a data prefix list

Source: IP Prefix

10.107.1.10/32

Destination Data Prefix List ×

Select a data prefix list

Destination: IP Prefix

10.109.1.10/32

Actions

Accept Enabled

AppQoE Optimization ×

☒ TCP Optimization

☒ DRE Optimization

Service Node Group SNG-APPQOE

[Cancel](#) [Save Match and Actions](#)

CLI :

```
SC# show sdwan policy from-vsmart
```

```
from-vsmart data-policy _CorpVPN_DRE-data-policy-SC_ESN-2
direction all
vpn-list CorpVPN
sequence 1
match
source-ip 10.107.1.10/32
destination-ip 10.109.1.10/32
action accept
tcp-optimization
dre-optimization
service-node-group SNG-APPQOE
```

```
sequence 11
match
  source-ip 10.109.1.10/32
  destination-ip 10.107.1.10/32
action accept
  tcp-optimization
  dre-optimization
  service-node-group SNG-APPQOE
default-action accept

from-vsmart lists vpn-list CorpVPN
vpn 1
```

検証 – CLI

ブランチISN

ISN# show sdwan appqoe dreopt status

```
DRE ID                : 52:54:dd:2a:74:d7-018eafaa99e1-f9ff51aa
DRE uptime            : 04:10:59:59
Health status         : GREEN
Health status change reason : None
Last health status change time : 04:10:59:59
Last health status notification sent time : 1 second
DRE cache status      : Active
Disk cache usage       : 2%
Disk latency           : 25 ms
Active alarms:
  None
```

Configuration:

```
Profile type          : S
Maximum connections   : 750
Maximum fanout        : 35
Disk size             : 60 GB
Memory size           : 2048 MB
CPU cores             : 1
Disk encryption       : ON
```

ISN# show sdwan appqoe flow active
T:TCP, S:SSL, U:UTD, D:DRE

Flow ID	VPN ID	Source IP	Port	Destination IP	Port	Tx Bytes	Rx Bytes	Services
54382538667	1	10.107.1.10	55340	10.109.1.10	80	263663268	640416	TD

ISN# show sdwan appqoe dreopt statistics

```
Total connections      : 4
Max concurrent connections : 1
Current active connections : 1
Total connection resets : 0
```

Total original bytes : 3570 MB
Total optimized bytes : 1633 MB
Overall reduction ratio : 54%
Disk size used : 2%
Cache details:
Cache status : Active
Cache Size : 59132 MB
Cache used : 2%
Oldest data in cache : 01:22:02:49
Replaced(last hour): size : 0 MB

DC/ハブSC

SC# show service-insertion type appqoe service-node-group

Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 1

Service Node (SN) : 10.115.1.10
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
System IP : 10.1.90.2
Site ID : 90
Time current status was reached : Sat Apr 6 07:26:16 2024

Cluster protocol VPATH version : 2 (Bitmap recvd: 3)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1714282683
Cluster protocol last received sequence number: 1931795
Cluster protocol last received ack number : 1714282682

Health Markers:

AO Load State

tcp GREEN 0%
ssl RED/NOT AVAILABLE
dre GREEN 0%
http RED/NOT AVAILABLE
utd chnl RED/NOT AVAILABLE

DC/ハブESN

ESN# show sdwan appqoe dreopt status

DRE ID : 52:54:dd:c3:40:17-018eb15f4fc3-49ee2d0f
DRE uptime : 04:11:28:50
Health status : GREEN
Health status change reason : None
Last health status change time : 04:11:28:50

Last health status notification sent time : 1 second
DRE cache status : Active
Disk cache usage : 2%
Disk latency : 10 ms
Active alarms:
None

Configuration:

Profile type : S
Maximum connections : 750
Maximum fanout : 35
Disk size : 60 GB
Memory size : 2048 MB
CPU cores : 1
Disk encryption : ON

ESN# show sdwan appqoe flow active
T:TCP, S:SSL, U:UTD, D:DRE

Flow ID	VPN ID	Source IP	Port	Destination IP	Port	Tx Bytes	Rx Bytes	Services
20022800299	1	10.107.1.10	55340	10.109.1.10	80	2998777	1074725760	TD

ESN# show sdwan appqoe dreopt statistics

Total connections : 4
Max concurrent connections : 1
Current active connections : 1
Total connection resets : 0
Total original bytes : 4294 MB
Total optimized bytes : 1634 MB
Overall reduction ratio : 61%
Disk size used : 2%
Cache details:
Cache status : Active
Cache Size : 59132 MB
Cache used : 2%
Oldest data in cache : 01:22:04:08
Replaced(last hour): size : 0 MB

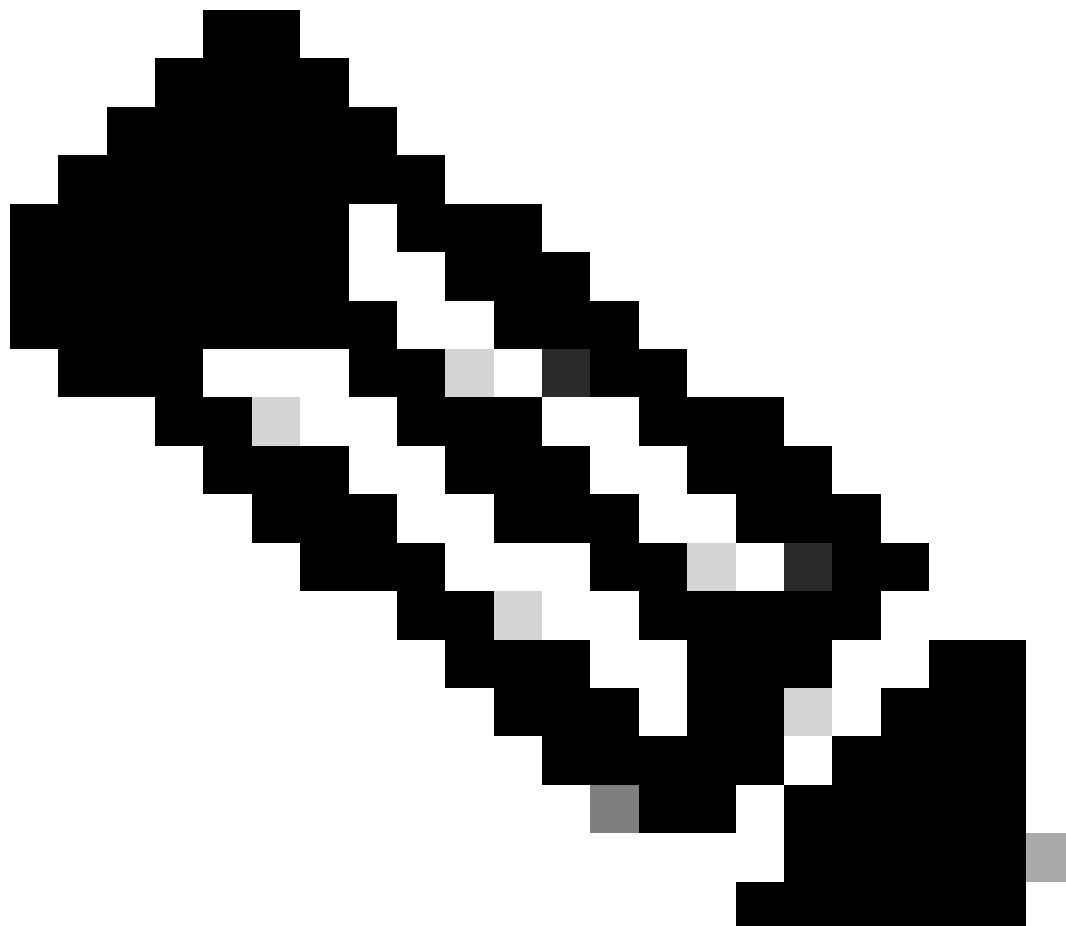
検証 – ダッシュボード

SD-WAN ManagerデバイスダッシュボードでAppQoE DREデータを表示するには、次の点を確認します。

- ・コントローラとデバイスの時刻は、ネットワークタイムプロトコル(NTP)を設定することで同期されます。また、Clock setコマンドを使用して、クロックを手動で設定することもできます。
- ・デバイス設定(ISN/SC/ESN)に次のCLIを追加します。

```
policy ip visibility features multi-sn enable
```

```
policy ip visibility features dre enable
policy ip visibility features sslproxy enable - (for SSL traffic)
```



注：これらのダッシュボードを表示するには、オンデマンドトラブルシューティングを有効にする必要があります。ここに示すダッシュボード画面には、リアルタイムの情報は表示されないことに注意してください。

最新のデータを取得するには、Tools > On Demand Troubleshootingに移動し、適切なデバイスを選択して、Data Typeとして「DPI」を選択し、次に示すように、過去3時間のDPI統計情報を取得できます。

Monitor BR7-DRE-intNode-70.7.71-vedge Select Data Type

Configuration

Tools

Maintenance

Administration

Workflows

Reports

Analytics

Explore

Data Backfill Time Period

☐ Last 1 hour ☐ Last 3 hours ☐ ConnectionEvents

Start Date Start time AM End Date End time AM

Save Clear

Search Table

As of: Apr 18, 2024 05:48 PM

ID	Device ID	Data Type	Creation Time	Expiration Time	Data Backfill Start Time	Data Backfill End Time	Status	Action
1d7c7605-0e17-43d3-97e6-59c69ec6ac12	1.1.1.222	ConnectionEvents	Feb 15, 2022, 12:36:05 AM	Feb 15, 2022, 3:36:05 AM	Feb 14, 2022, 11:36:05 PM	Feb 15, 2022, 12:36:05 AM	COMPLETED	...
a92e3d95-9ac9-4a87-a36d-311012d9c0f9	70.7.71	DPI	Apr 18, 2024, 5:44:33 PM	Apr 18, 2024, 6:44:33 PM	Apr 18, 2024, 2:44:33 PM	Apr 18, 2024, 5:44:33 PM	COMPLETED	...

2 Records

Items per page: 25 1 - 2 of 2

ブランチISN

約900 MBのデータがダウンロードされました (3個の200 MBファイルと3個の100 MBファイル) – オリジナルトラフィック (黄色)。

最適化により、WAN経由で送信されるトラフィックは8.07 MBのみとなり、帯域幅使用量は約90 %削減されました。Optimized Traffic(BLUE)。

Devices > AppQoS Integrated Service Node

Select Device

BR7-DRE-intNode | 70.7.71 Site Name 70 Device Model: C8000v

DATA Backfill Start Time: Wed Apr 17 2024 13:54:41 GMT-0400 and Data Backfill End Time: Wed Apr 17 2024 16:54:41 GMT-0400

Chart Options

Optimized Traffic Application

Controller Service Node

Export

Bytes

Apr 17, 16:35:00

Optimized Traffic: 8.07 MB

Original Traffic: 939.36 MB

Legend

Optimized Traffic

Original Traffic

Search

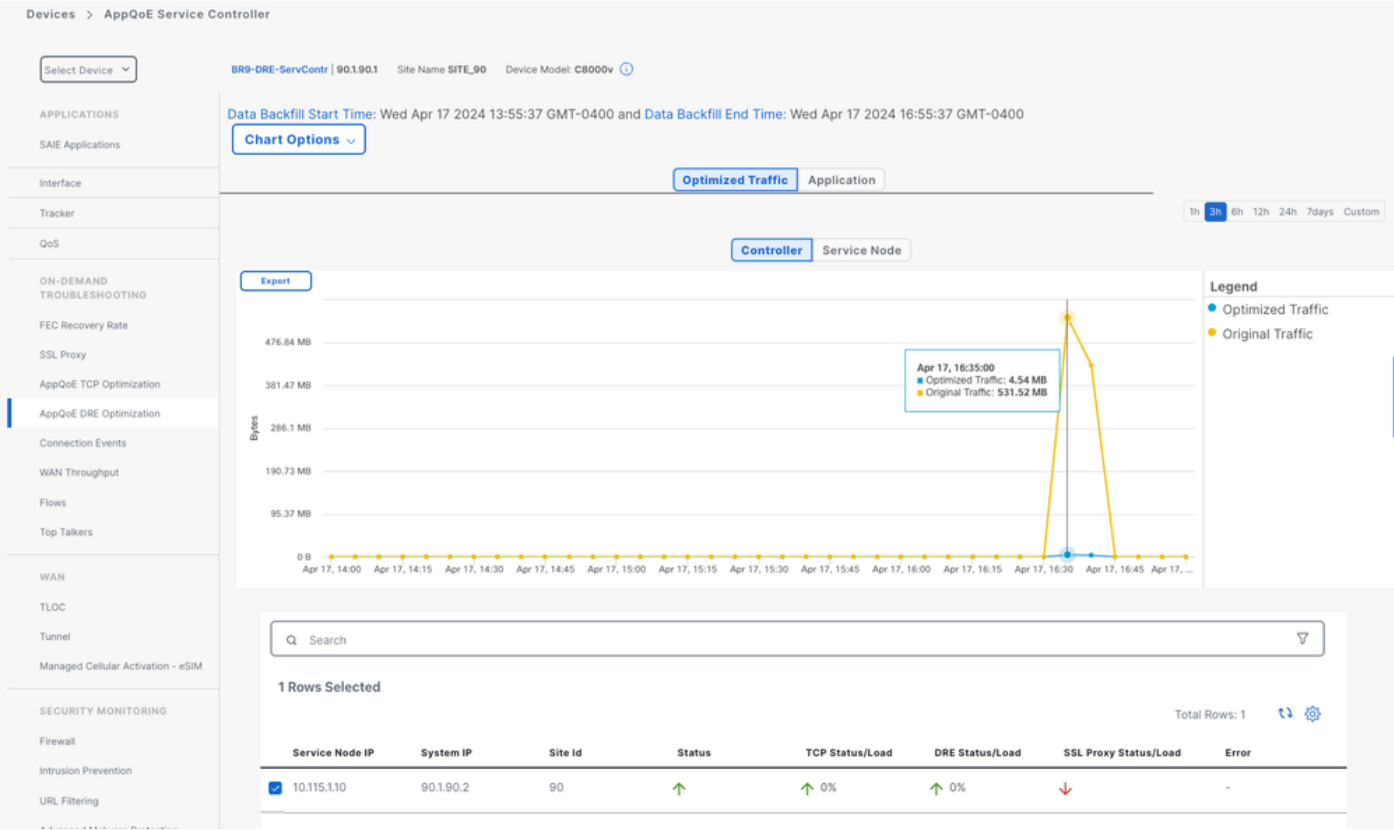
1 Rows Selected

Total Rows: 1

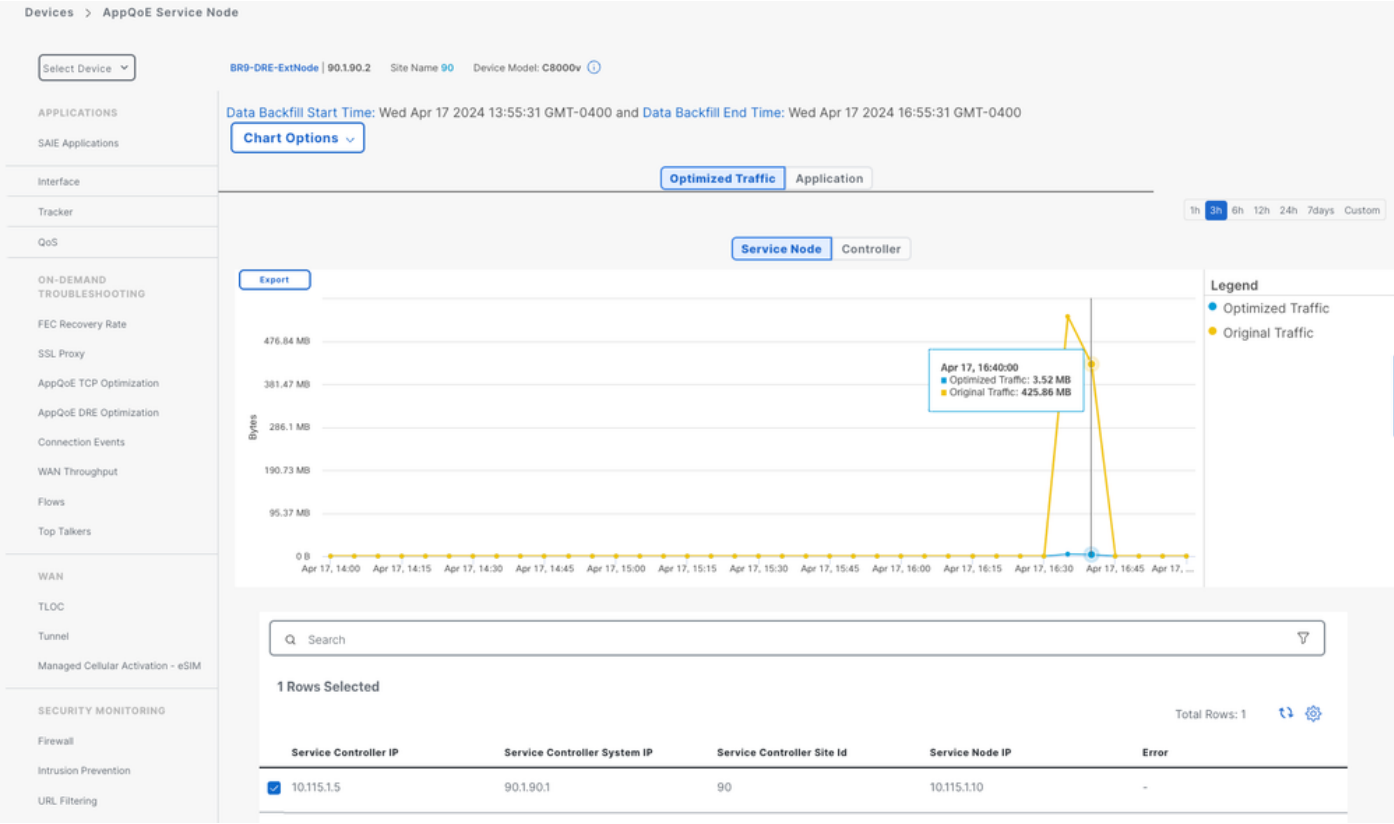
Service Node IP	System IP	Site Id	Status	TCP Status/Load	DRE Status/Load	SSL Proxy Status/Load	Error
☒ 192.168.2.2	70.7.71	70	↑	↑ 0%	↑ 0%	↓	-

DC/ハブSC

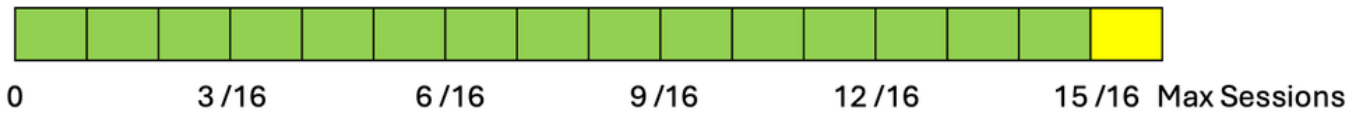
複数のESNが存在する場合は、「Controllertab」に累積データが表示され、「Service」に個々のESNデータが表示されます。



DC/ハブESN



負荷計算



例：

たとえば、TCP最適化でサポートされる最大セッション数は= 40000です。

(最大セッションの値は、サービスノードのshow sdwan appqoe rm-resources CLI出力で確認できます)。

Max sessionsの値はデバイス固有であることに注意してください。

$40000/16 = 2500$ 、各ブロックのサイズ。

現在のセッション数が3000の場合は、2番目のブロックに入ります。

$LOAD = (2/16) \times 100 = 12\%$ (小数点なし) 。

DREおよびSSLプロキシについても同じです。対応する最大セッションの値が、計算の対象となります。

<#root>

Router#show sdwan appqoe rm-resources

```
=====
RM Resources
=====
```

RM Global Resources :

```
Max Services Memory (KB)      : 12221390
Available System Memory(KB)   : 0
Used Services Memory (KB)     : 24442780
Used Services Memory (%)      : 0
System Memory Status          : GREEN
Num sessions Status           : GREEN
Overall HTX health Status     : GREEN
```

Registered Service Resources :

TCP Resources:

```
Max Sessions                   : 40000
```

Used Sessions : 0
Memory Per Session : 64

SSL Resources:

Max Sessions : 40000

Used Sessions : 0
Memory Per Session : 50

DRE Resources:

Max Sessions : 22000

Used Sessions : 0
Memory Per Session : 50

HTTP Resources:

Max Sessions : 0
Used Sessions : 0
Memory Per Session : 0

現在の接続数がMaxセッションの約95 %に達すると、サービスノードはFULL (黄色のステータス) としてマークされ、このサービスノードの新しいフローに対してAppQoEがバイパスされます。

パフォーマンスと拡張性

『[SD-WAN TCP Optimization and DRE - Performance and Scale](#)』を参照してください。

FAQ

Q：ファイル転送アプリケーションでは、SOAP over HTTPを使用し、WS-Security(WSS)がメッセージレベルで適用されています。

DREはこのシナリオでも有効ですか。または、WSSを使用したメッセージレベルの暗号化には根本的な互換性がないのですか。

A: WSセキュリティではTLSレベルの暗号化は使用されません。したがって、DREでは機能しません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。