

# Catalyst SD-WAN AppQoE DRE - Topologia, configurazione, verifica

## Sommario

---

[Introduzione](#)

[Premesse](#)

[Ottimizzazione DRE](#)

[Connessioni dei controlli](#)

[Procedura per la creazione di un'installazione di AppQoE DRE con ISDN e ESN](#)

[1. Sistema \(interfacce e hardware\) e topologia](#)

[1.1. Topologia e interfacce](#)

[1.2. Requisiti del disco](#)

[1.3. Aggiunta di dispositivi al fabric SD-WAN](#)

[1.4. Dettagli su C8000v](#)

[2. Filiale: Configurazione ISDN di AppQoE](#)

[3. DC/Hub: Configurazione di AppQoE ESN](#)

[4. DC/Hub: Configurazione AppQoE SC](#)

[5. Politica centralizzata dei dati sul traffico](#)

[A. Filiale ISR](#)

[B. DC/Hub SC](#)

[Verifica - CLI](#)

[Ramo ISDN](#)

[DC/Hub SC](#)

[ESN DC/Hub](#)

[Verifica - Dashboard](#)

[Ramo ISDN](#)

[DC/Hub SC](#)

[ESN DC/Hub](#)

[calcolo LOAD](#)

[Prestazioni e scalabilità](#)

[Domande frequenti](#)

---

## Introduzione

In questo documento viene descritto come creare e configurare una configurazione per l'ottimizzazione dell'eliminazione della ridondanza dei dati (DRE).

## Premesse

Questo documento ha lo scopo di fornire un punto di partenza per linee guida su come creare e configurare una configurazione per DRE che fa parte di una [soluzione AppQoE \(Integrated](#)

[Application Quality of Experience](#)), offrendo una struttura di criteri e un monitoraggio coerenti end-to-end per una vasta gamma di scenari di utilizzo della distribuzione.

Elementi di base della soluzione AppQoE:

- Correzione progressiva errori (FEC) e duplicazione pacchetti (PD): Risolve i problemi di perdita di pacchetti. Vedere per FEC.
- Ottimizzazione TCP: Risoluzione dei problemi di latenza WAN. Per uno Use Case opzionale TCP a lato singolo, vedere.
- Ottimizzazione DRE: Risoluzione dei problemi di larghezza di banda ridotta. In genere, l'ottimizzazione DRE viene utilizzata insieme all'ottimizzazione TCP.

La documentazione [CCO DRE esistente](#) non contiene una descrizione completa del processo. Questo documento offre una descrizione dettagliata e completa della soluzione DRE.

Una spiegazione tecnica approfondita della funzionalità DRE esula dall'ambito di questo articolo. Per ulteriori informazioni sui dettagli tecnici e sulle funzionalità DRE, consultare [questa documentazione](#).

## Ottimizzazione DRE

DRE è una soluzione a due lati che rimuove i dati ridondanti mediante la memorizzazione nella cache dei modelli rilevati in precedenza. In combinazione con l'algoritmo Lempel-Ziv-Welch (LZW), che fornisce la compressione per ridurre la quantità di dati sulla WAN, la funzione DRE offre una soluzione completamente sicura e integrata con i proxy Unified Threat Defense (UTD) e Secure Sockets Layer (SSL).

Indipendente dalle applicazioni e dai protocolli, è una soluzione predisposta per il cloud che offre una riduzione del traffico WAN del 60-90%.

Sono supportati diversi scenari di distribuzione per ottenere una soluzione scalabile.

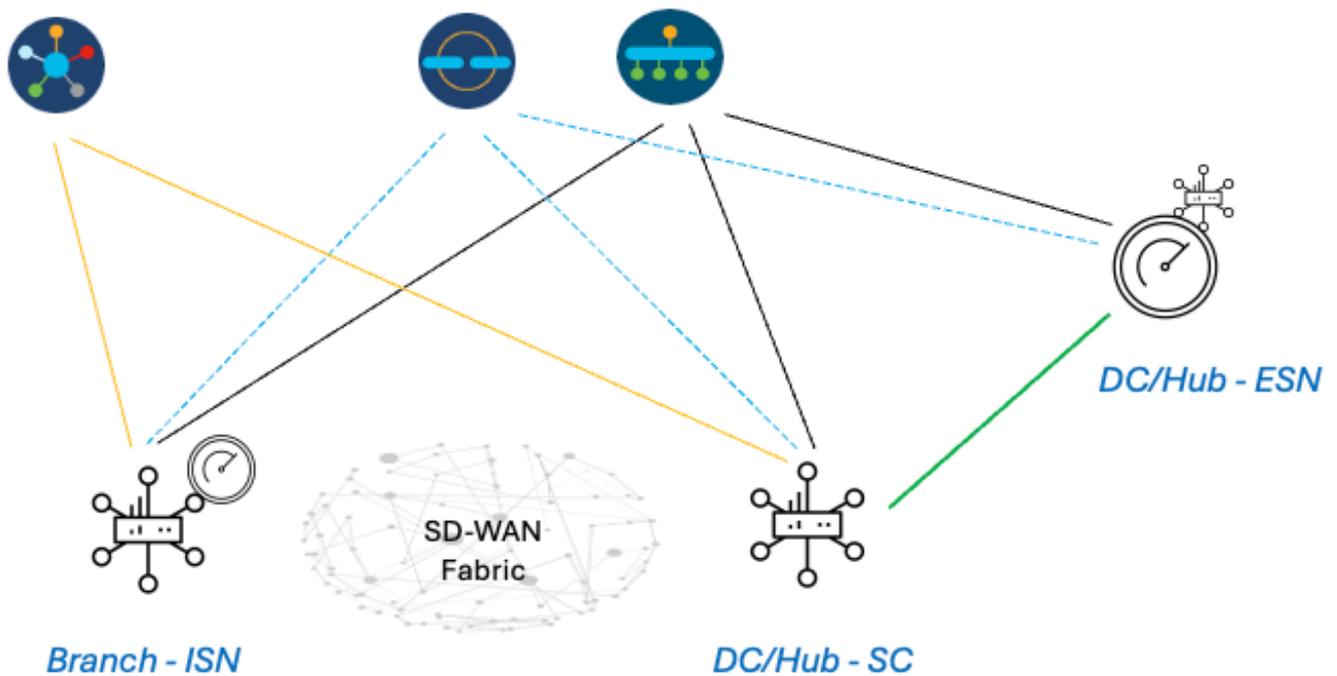
- La soluzione integrata fornisce una soluzione completa per l'installazione dei servizi di filiale, definita ISDN (Integrated Service Node).
- I nodi di servizio esterni (ESN, External Service Nodes) vengono disaccoppiati dall'intercettazione dei router periferici o dei controller di servizio (SC, Service Controller) nell'implementazione dei nodi di servizio esterni, in genere nei centri dati e negli hub. Il reindirizzamento dei flussi in base al traffico delle applicazioni viene eseguito utilizzando un criterio dati.

## Connessioni dei controlli



Nota: ESN non forma alcuna connessione di controllo con il controller (precedentemente noto come vSmart). ESN dispone di una connessione di controllo a SD-WAN Manager.

---



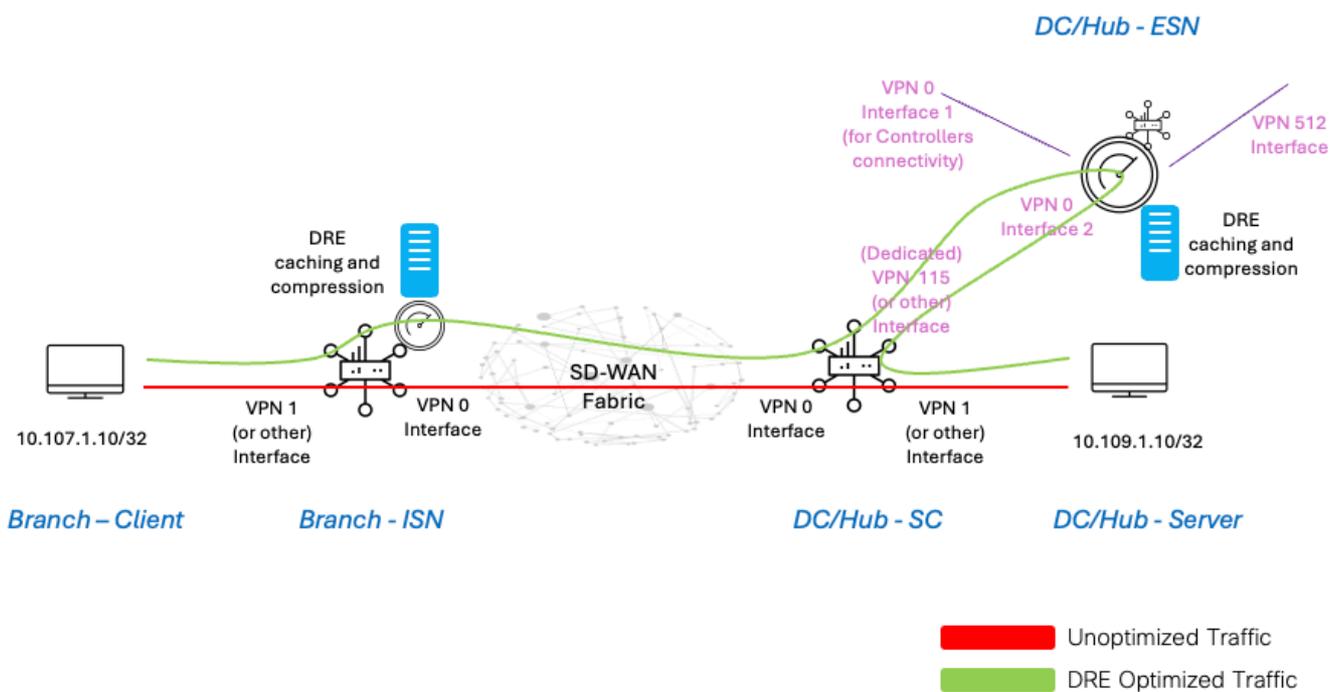
## Procedura per la creazione di un'installazione di AppQoE DRE con ISDN e ESN

### 1. Sistema (interfacce e hardware) e topologia

#### 1.1. Topologia e interfacce

ESN richiede le seguenti interfacce:

- Connettività dell'interfaccia VPN0 ai controller (gestione e convalida (temporanea)). La connettività tra ESN e i controller può avvenire direttamente o tramite SC. La raccomandazione è tramite SC in quanto ciò evita la necessità di un circuito WAN aggiuntivo sull'ESN.
- Un'altra interfaccia VPN0 per la connettività al controller del servizio.
- Facoltativo: Interfaccia di gestione VPN512.



## 1.2. Requisiti del disco

Per un'installazione in laboratorio, un disco da 150 GB è sufficiente per l'ottimizzazione del DRE.

Ciò è valido solo per la verifica funzionale in un ambiente di laboratorio e non per la produzione. Per consigli precisi su disco e altro, controllare [questo collegamento CCO](#).



Nota: Questo requisito aggiuntivo del disco è valido solo per gli ISDN e ESN. Non è richiesto su SC.

---

### 1.3. Aggiunta di dispositivi al fabric SD-WAN

- Utilizzo di modelli (disponibili a partire da 20.6/17.6): Modello di funzionalità AppQoe che può essere specificato nel modello di dispositivo come modello aggiuntivo.
- Uso dei gruppi di configurazione (disponibili a partire dalla versione 20.14/17.14): Pacchetto funzionalità AppQoE disponibile nel profilo Servizio/LAN nel gruppo di configurazione.

### 1.4. Dettagli su C8000v

Se si utilizza c8kv, assicurarsi di abilitare la configurazione del profilo CPU con elevato numero di applicazioni. [Questo](#) è un articolo utile.

## 2. Filiale: Configurazione ISDN di AppQoE

Creare un modello di funzionalità AppQoE (utilizzando i modelli illustrati di seguito) per il modello di dispositivo.

### 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

Quindi, specificare questo modello di funzionalità nel modello di dispositivo.

### Additional Templates

AppQoE

DRE-IntNode-template

### 3. DC/Hub: Configurazione di AppQoE ESN

Creare una AppQoS Feature Template maschera per il modello di dispositivo.

## Configuration

**Device Templates**   **Feature Templates**

Feature Template > AppQoS > [REDACTED] DRE-feature-template

**Device Type**   C8000v

**Template Name**   [REDACTED] DRE-feature-template

**Description**   Feature Template for DRE

Control Components    Service Node

---

**Service Node**

**External Service Node**    Enable

---

**Advanced**

**DRE Optimization**   ⓘ  

**Resource Profile**   ⓘ    default

**SSL Decryption**   ⓘ    Enable

Quindi, specificare questo modello di funzionalità nel modello di dispositivo.

## Additional Templates

AppQoE \*

[REDACTED]-DRE-feature-template ▼

### 4. DC/Hub: Configurazione AppQoE SC

Creare un modello di funzionalità AppQoE per il modello di dispositivo.

#### 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: [Globe icon] 10.115.1.5

Service VPN: [Globe icon] 115

---

#### Service Nodes

[Info icon]

Service Node Group Name	Service Node IP Addresses
[Globe icon] SNG-APPQOE	1 Service Node IP Addresses

10.115.1.10

Quindi, specificare questo modello di funzionalità nel modello di dispositivo.

## Additional Templates

AppQoE

DRE-DC2-ServContr-...

### 5. Politica centralizzata dei dati sul traffico

- Sono necessarie due politiche diverse: una per l'ISN (Internal Service Node) e la seconda per SC (Service Controller).
- La direzione dei criteri deve essere 'Tutti' per entrambi.
- Service-node-group deve essere vuoto per ISN e specificato per SC.
- L'ottimizzazione DRE viene in genere utilizzata insieme all'ottimizzazione TCP. Quando DRE è abilitato, consente anche l'ottimizzazione TCP.

In questo esempio, viene definito un client Web in un percorso di succursale e un server Web nel sito controller di dominio. È possibile modificare il client in base al traffico di interesse.

#### A. Filiale ISR

#### Interfaccia utente - Modello

Sequenza 1 - Dal client 10.107.1.10 al server 10.109.1.10:

The screenshot shows the configuration interface for a custom sequence rule. The 'Match' tab is active, displaying the following match conditions:

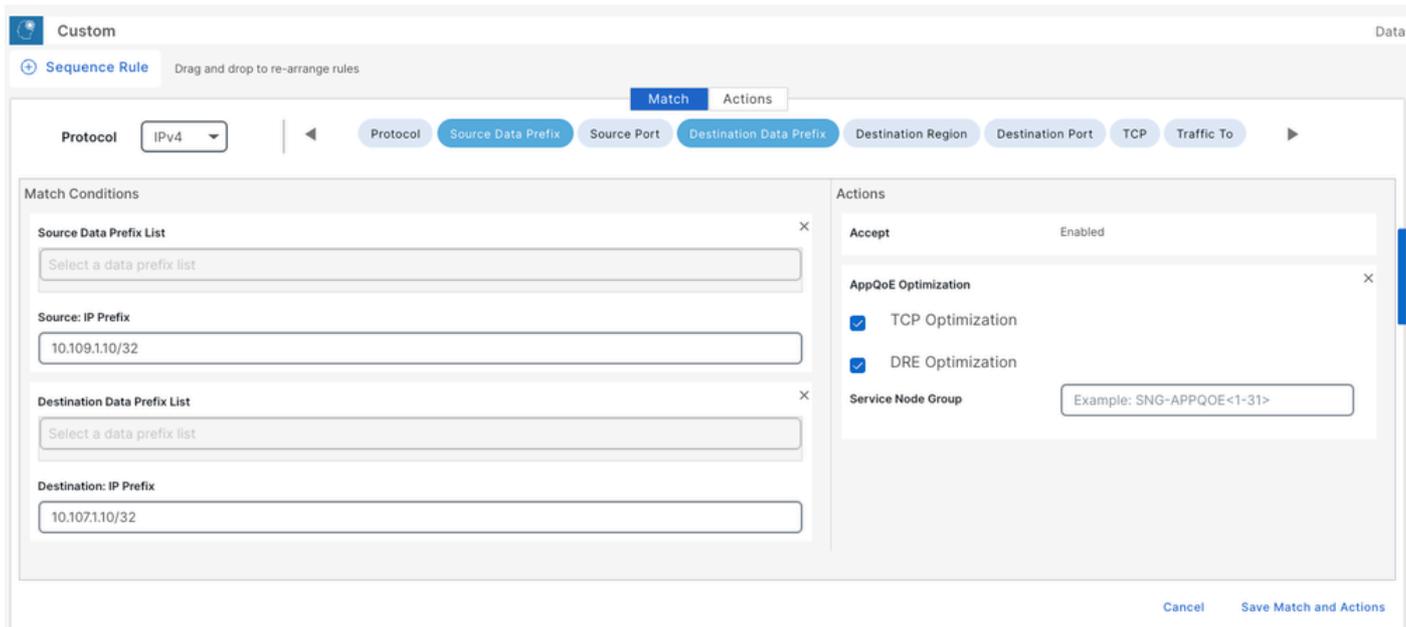
- Source Data Prefix List: Select a data prefix list
- Source: IP Prefix: 10.107.1.10/32
- Destination Data Prefix List: Select a data prefix list
- Destination: IP Prefix: 10.109.1.10/32

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

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

Buttons for 'Cancel' and 'Save Match and Actions' are visible at the bottom right.

Sequenza 2 - dal server al client:



CLI:

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

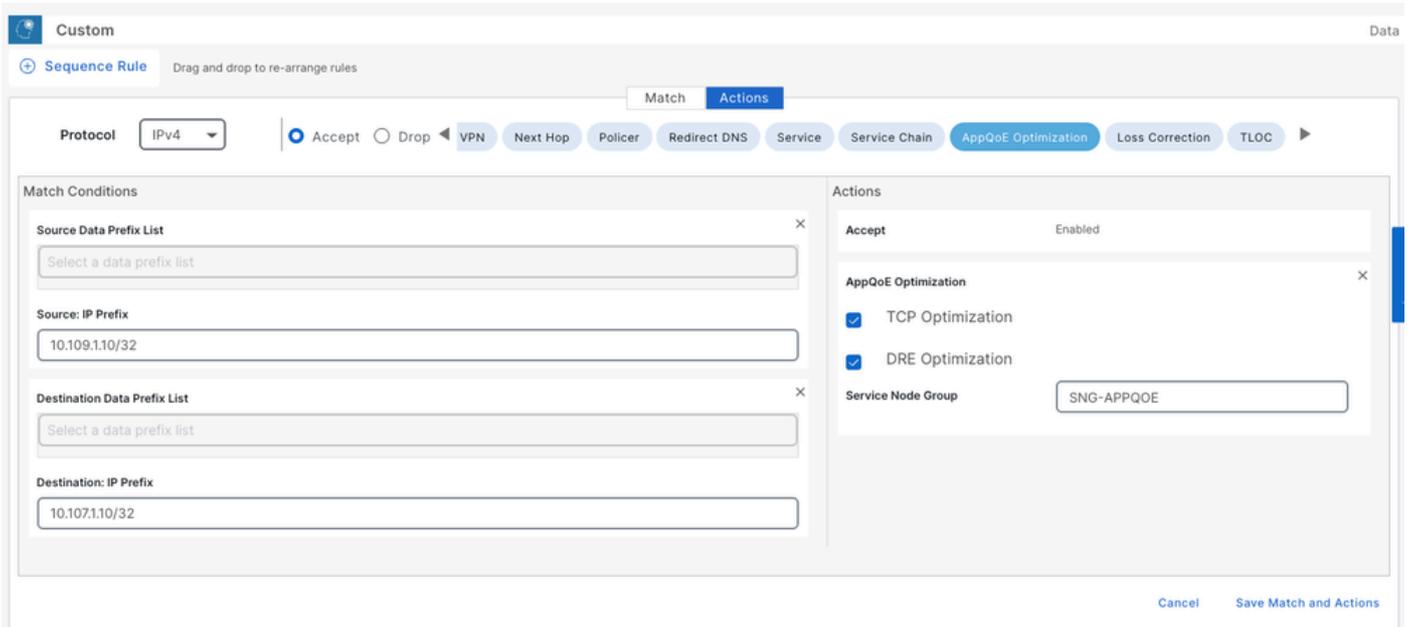
```
from-vsmart data-policy _CorpVPN_DRE-data-policy-ISN-2
direction all
vpn-list CorpVPN
sequence 1
match
source-ip 10.107.1.10/32
destination-ip 10.109.1.10/32
action accept
tcp-optimization
dre-optimization
sequence 11
match
source-ip 10.109.1.10/32
destination-ip 10.107.1.10/32
action accept
tcp-optimization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

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

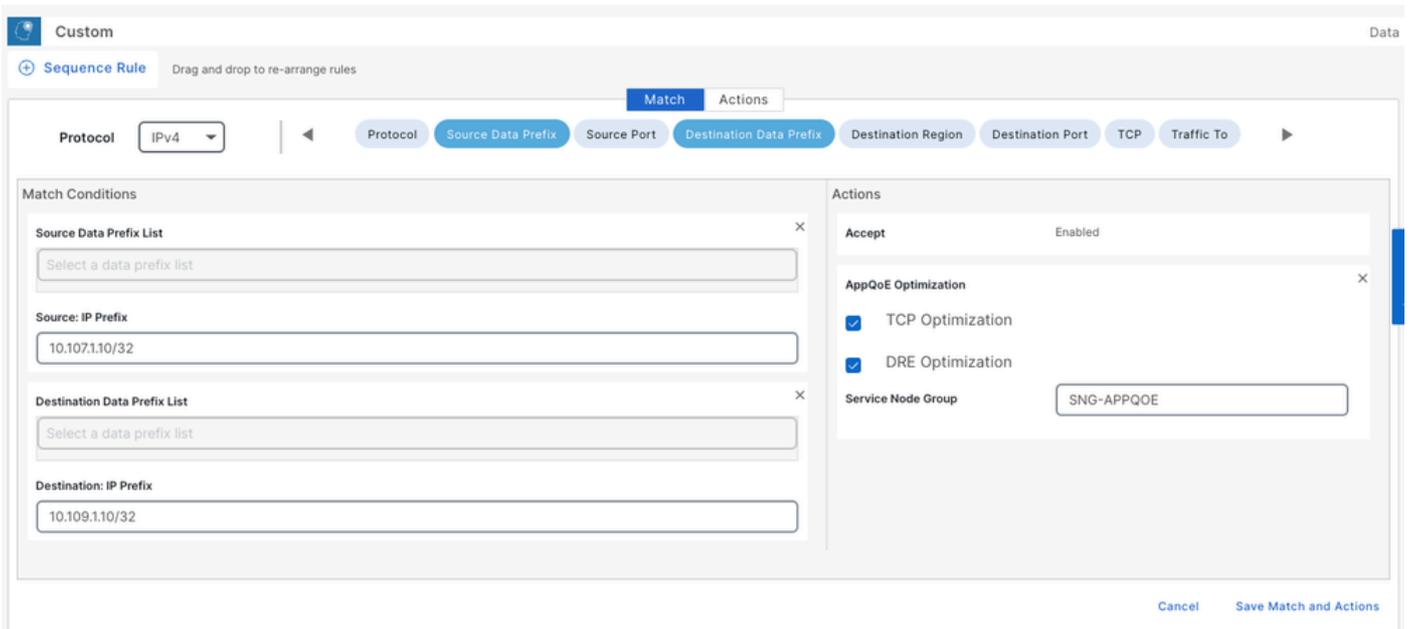
B. DC/Hub SC

Interfaccia utente - Modello

Sequenza 1 -



## Sequenza 2 -



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

```

## Verifica - CLI

### Ramo ISDN

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/Hub 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

## ESN DC/Hub

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

## Verifica - Dashboard

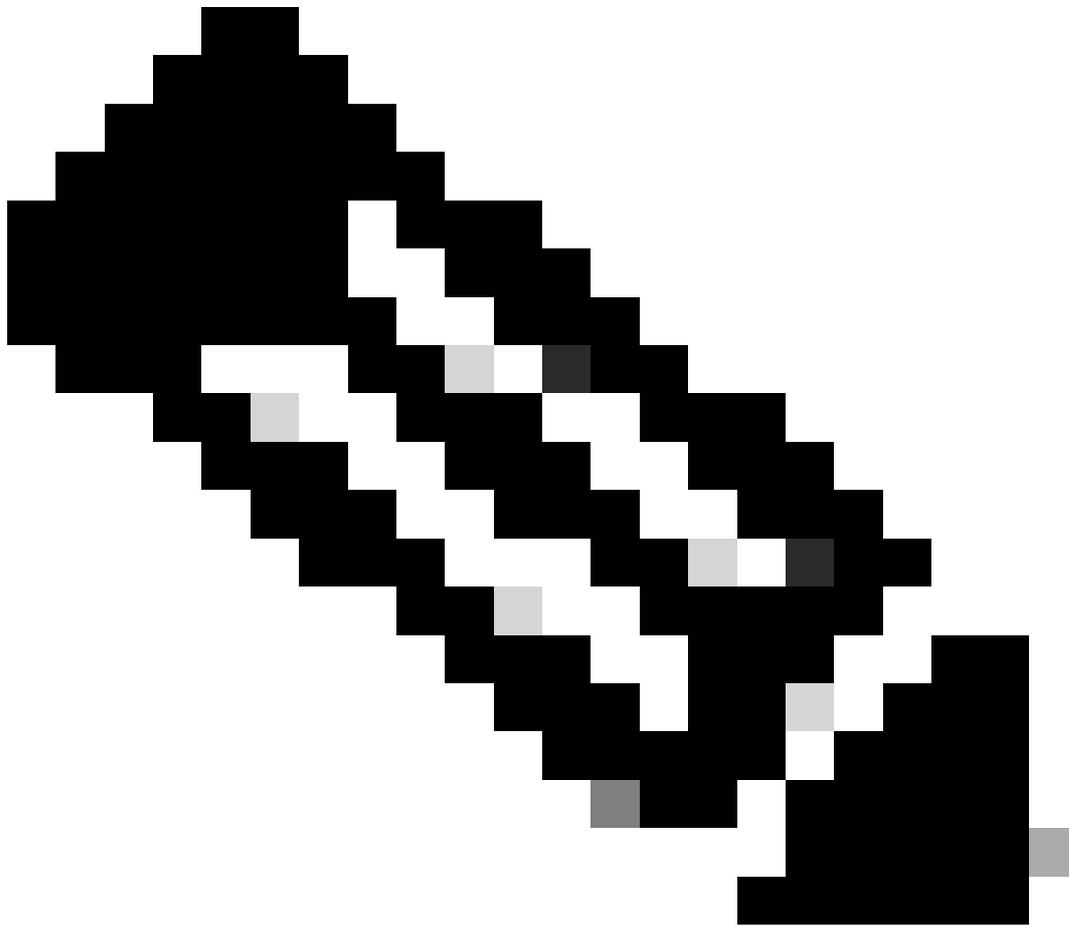
Per visualizzare i dati AppQoE DRE nel dashboard del dispositivo SD-WAN Manager, verificare che:

- L'ora di controller e dispositivi viene sincronizzata configurando Network Time Protocol (NTP). È inoltre possibile utilizzare il comando `clock set` per impostare l'orologio manualmente.
- Aggiungere le seguenti CLI alla configurazione del dispositivo (ISN/SC/ESN):

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

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

---



Nota: Per visualizzare questi dashboard, è necessario abilitare la risoluzione dei problemi su richiesta. Si noti che le schermate del dashboard mostrate di seguito non mostrano informazioni in tempo reale.

---

Per ottenere i dati più recenti, è possibile passare a [Tools > On Demand Troubleshooting](#), scegliere il Dispositivo appropriato e 'DPI' come Tipo di dati e recuperare le statistiche DPI per le ultime 3 ore, come mostrato di seguito:

The screenshot shows a configuration page for data backfill. The device selected is 'BR7-DRE-intNode-70.7.71-vedge'. The data type is set to 'DPI'. The time period is 'Last 3 hours'. The start and end dates and times are configured. Below the configuration is a table with the following data:

ID	Device ID	Data Type	Creation Time	Expiration Time	Data Backfill Start Time	Data Backfill End Time	Status	Action
1d7c7605-0e17-43d3-97e6-59c69ec6ac12	1.11.222	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, 8:44:33 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.

## Ramo ISDN

Sono stati scaricati circa 900 MB di dati (3 x 200 MB e 3 x 100 MB) - Traffico originale (GIALLO).

L'ottimizzazione ha prodotto solo 8,07 MB di traffico inviato sulla WAN, circa il 90% di riduzione dell'utilizzo della larghezza di banda - traffico ottimizzato (BLUE).

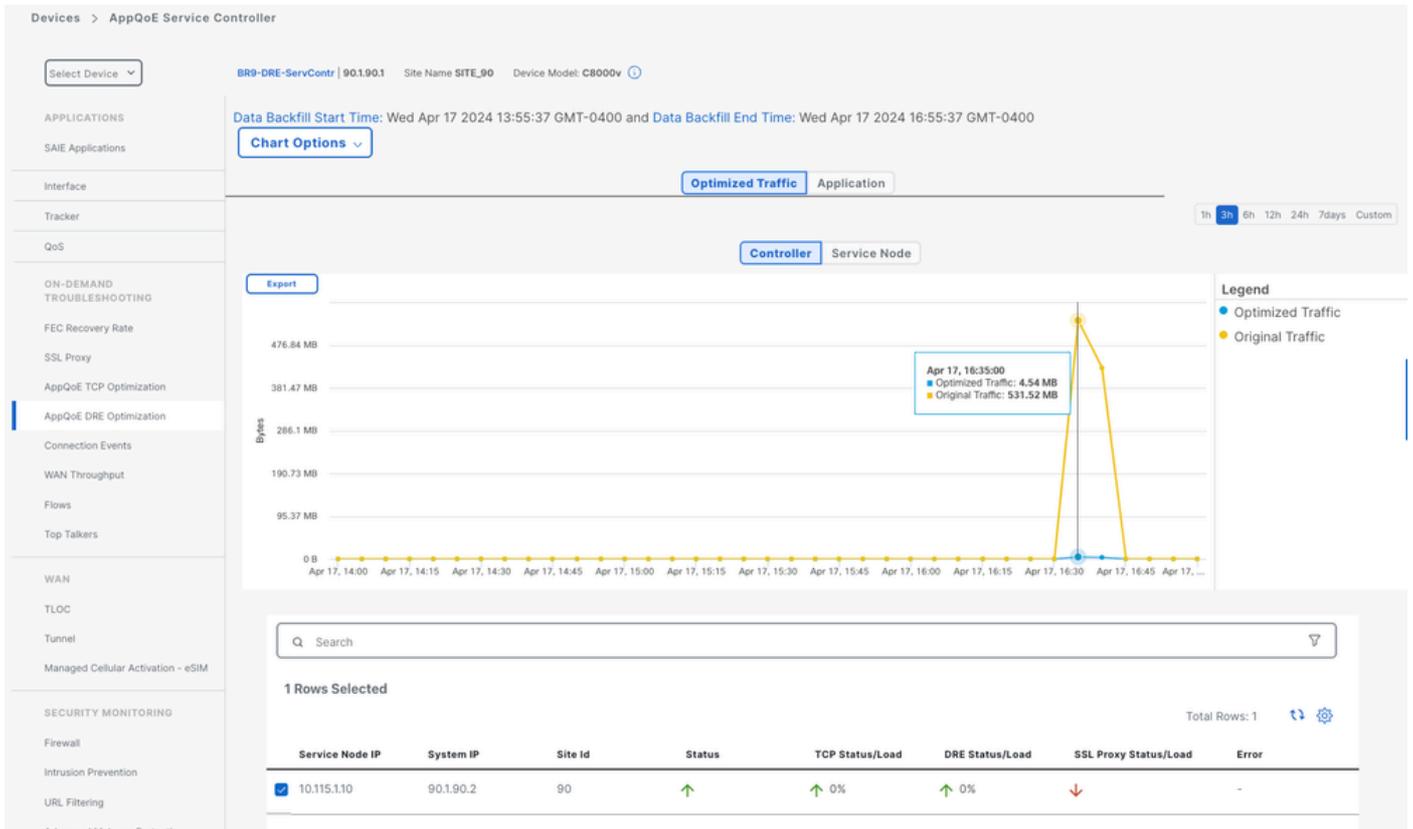
The screenshot shows the 'AppQoE Integrated Service Node' configuration page. The device is 'BR7-DRE-intNode | 70.7.71'. The data backfill start and end times are 'Wed Apr 17 2024 13:54:41 GMT-0400' and 'Wed Apr 17 2024 16:54:41 GMT-0400'. The chart shows traffic volume over time, with a significant spike at 16:35:00. The legend indicates 'Optimized Traffic' (blue) and 'Original Traffic' (yellow).

Apr 17, 16:35:00  
 Optimized Traffic: 8.07 MB  
 Original Traffic: 939.36 MB

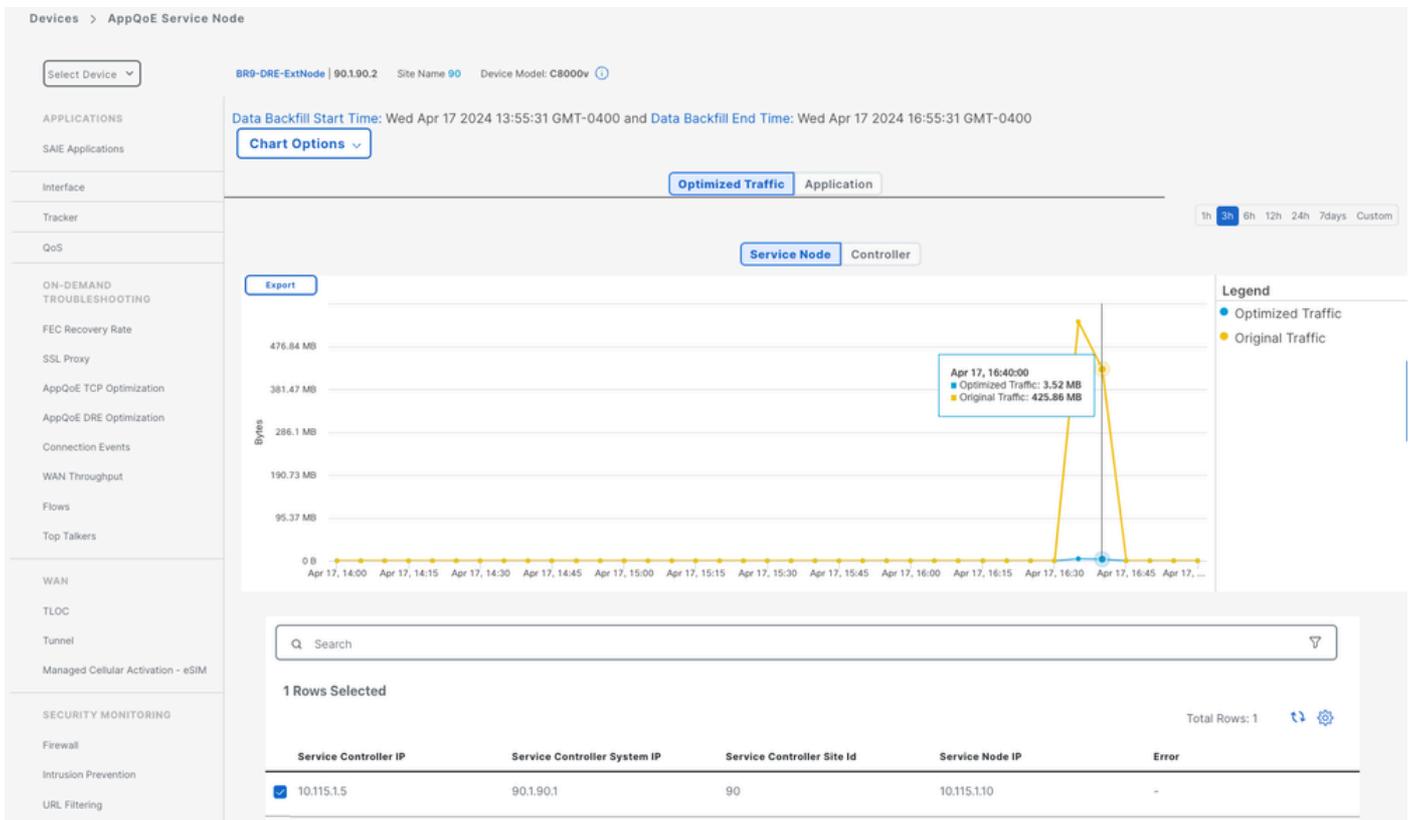
Service Node IP	System IP	Site Id	Status	TCP Status/Load	DRE Status/Load	SSL Proxy Status/Load	Error
192.168.2.2	70.7.71	70	↑	↑ 0%	↑ 0%	↓	-

## DC/Hub SC

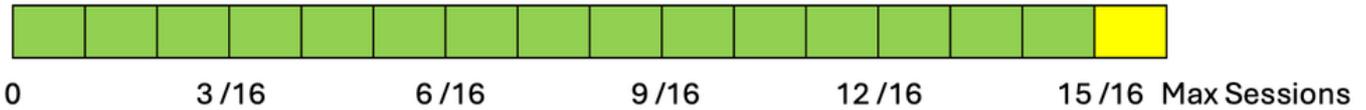
Se sono presenti più ESN, nella Controller scheda verranno visualizzati i dati cumulativi e nella Service Node scheda verranno visualizzati i singoli dati ESN.



## ESN DC/Hub



calcolo LOAD



Esempio:

Ad esempio, Max session supportato per l'ottimizzazione TCP è = 40000.

(il valore Max sessions è disponibile nell'output `show sdwan appqoe rm-resources` CLI sul nodo del servizio).

Il valore Max sessions è specifico del dispositivo.

$40000/16 = 2500$ , dimensioni di ciascun blocco.

Se il numero corrente di sessioni è, ad esempio 3000, questo numero rientra nel secondo blocco.

$LOAD = (2/16) \times 100 = 12\%$  (senza decimali).

Lo stesso vale per il proxy DRE e SSL. I corrispondenti valori Max session vengono considerati nel calcolo.

<#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

Quando il numero di connessioni correnti raggiunge circa il 95% del numero massimo di sessioni, il nodo di servizio viene contrassegnato come FULL (stato giallo) e AppQoE viene ignorato per i nuovi flussi, per questo nodo di servizio.

## Prestazioni e scalabilità

Fare riferimento a [SD-WAN TCP Optimization and DRE - Performance and Scale](#) (Ottimizzazione TCP e DRE SD-WAN - Prestazioni e scalabilità).

## Domande frequenti

Q: Un'applicazione di trasferimento file utilizza SOAP su HTTP, con WS-Security (WSS) applicato a livello di messaggio.

Il protocollo DRE può essere ancora efficace in questo scenario o la crittografia a livello di

messaggio tramite WSS è fondamentalmente incompatibile con esso?

A: WS Security non utilizza la crittografia a livello TLS. Pertanto, non funziona con DRE.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).