Traffic Optimization with DRE

Table 1: Feature History

Feature Name	Release Information	Description
Traffic Optimization with DRE	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This release extends the DRE functionality to Cisco Catalyst SD-WAN. DRE is a compression technology that reduces the size of data transmitted over the WAN and enables more effective utilization of the WAN.
DRE Profiles	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides the flexibility to use resources for DRE based on your connection requirements by applying profiles such as S, M, L, and XL.
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature introduces support for deploying Cisco Catalyst 8000V instances, on supported routers, using UCS-E series blade server modules. With this feature, the supported routers can be configured as integrated service nodes, external service nodes, or hybrid clusters with both internal and external service nodes.
UCS-E Series Next Generation Support for Deploying Cisco Catalyst 8000V	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This feature introduces support for deploying Cisco Catalyst 8000V Edge Software on supported routers, using the UCS-E1100D-M6 server module.
SSL Proxy Support for TLS 1.3	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	With this feature, SSL proxy in AppQoE supports the TLS protocol version 1.3.

Feature Name	Release Information	Description
DRE Optimisation Using Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	With this feature you can enable DRE optimization using **AppQoE** feature under **Service Profile** in a configuration group in Cisco SD-WAN Manager.

Information About DRE

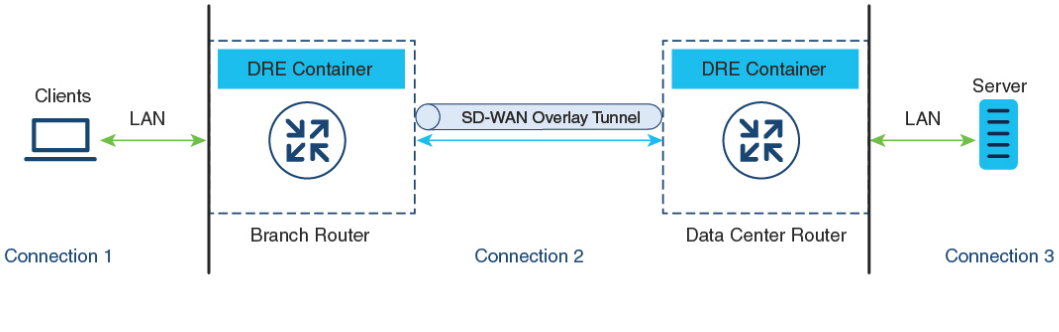
Overview of DRE

Data Redundancy Elimination (DRE) is a compression technology that reduces the size of data transmitted over the WAN. DRE reduces the size of transmitted data by removing redundant information before sending the data stream over the WAN. The DRE compression scheme is based on a shared cache architecture where each peer involved in compression and decompression shares the same redundancy cache. With the integration of DRE with Cisco Catalyst SD-WAN, DRE replaces repeated data in the stream with a much shorter reference, and then sends the shortened data stream across the SD-WAN overlay. The receiving end uses its local redundancy cache to reconstruct the data stream before passing it along to the destination client or server.

Note Cisco IOS XE Catalyst SD-WAN devices need to be deployed at both ends of the Cisco Catalyst SD-WAN overlay tunnel.

How DRE and TCP Optimization Work Together

Figure 1: Interception of TCP Traffic



When DRE is configured, the TCP traffic is intercepted and it's separated into three connections:

Connection Type	Network
Client to the branch Cisco IOS XE Catalyst SD-WAN device: This connection exists in Local Area Network (LAN)	LAN
Branch router to the data center router	Through Cisco Catalyst SD-WAN overlay tunnel
Remote branch or data center router to the server	LAN

TCP connections in the Local Area Network (LAN) continue to send the original data. However, TCP connections through the Cisco Catalyst SD-WAN overlay tunnel send data that is compressed by DRE. The DRE container in the Cisco IOS XE Catalyst SD-WAN device at one side of the tunnel compresses the data before it's sent over the overlay tunnel. The DRE container in the Cisco IOS XE Catalyst SD-WAN device at the other side of the tunnel decompresses the data before it's sent to the server at the remote branch or data center side.

Components of DRE

DRE Cache: DRE cache uses secondary storage so that it can store a large amount of data. DRE cache is stored on both sides of the WAN and is used by edge devices to decompress the data. DRE cache in both devices (branch and data center) is synchronized, which means that if a chunk signature is present on one side, the other side has it too.

DRE Compression: DRE uses the Lempel-Ziv-Welch (LZW) compression algorithm for compressing data. DRE operates on large streams of data, typically tens to hundreds of bytes or more, and maintains a much larger compression history.

Overview of DRE Profiles

DRE profiles is a feature introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. This feature provides the flexibility to allocate resources to the DRE service based on the size of your branches and the number of connections required. DRE profiles are combinations of resource requirements and allocations that enable resource assignment based on your connection requirements.

The following DRE profiles are supported:

- Small (S)
- Medium (M)
- Large (L)
- Extra-large (XL)

To see the profiles supported on the devices that support the DRE feature, see the *Supported DRE Profiles* section in this chapter.

UCS-E Series Server Support for Deploying Cisco Catalyst 8000V

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be configured as external service nodes on supported UCS E-Series server modules. These server modules reside in Cisco 4000 Series Integrated Services Routers (Cisco 4000 Series ISR) and Cisco Catalyst 8000 Series Edge Platforms. These routers come with integrated service nodes. However, you can use supported UCS E-Series servers to deploy Cisco Catalyst 8000V instances on these routers, therefore enabling them to act as hybrid clusters with integrated service nodes and external service nodes. This capability ensures that AppQoE services such as DRE, that require higher CPU, can run on routers that otherwise have lower CPU and RAM.

How Cisco Catalyst 8000V Works on Cisco UCS E-Series Servers

- You can install VMware vSphere ESXi 6.7 hypervisors on UCS-E series server modules that reside in Cisco 4000 Series ISR and Cisco Catalyst 8000 Series Edge Platforms.
- You can then install Cisco Catalyst 8000V on these servers.
- The installed Cisco Catalyst 8000V instances should be configured with the app-heavy profile. This ensures that more cores are allocated to the service plane. The app-heavy profile separates service plane and data plane cores, therefore improving service plane performance.

Overview of SSL Proxy

The Secure Sockets Layer (SSL) proxy feature in AppQoE provides a secure and transparent way of optimizing SSL traffic. An SSL Proxy serves as an intermediary between the client and server. It first decrypts the encrypted traffic, optimises it and then encrypts it back. This process ensures that all data remains secure while also allowing for optimization. For more information, see Overview of SSL/TLS Proxy.

The SSL proxy uses Transport Layer Security (TLS) as a protocol to secure and encrypt communication between the client and the server, and optimize the SSL traffic. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, SSL proxy supports TLS version 1.3. TLS version 1.3 is more widely deployed and is simpler, faster, and more secure than version 1.2.

Note In SSL proxy, the support for a TLS 1.3 version is enabled by default. When a TLS 1.3 version is not available, the SSL proxy switches to using the TLS 1.2 version.

For information about verifying the TLS version, see Verify SSL Proxy Support for TLS 1.3 Using CLI, on page 28

Benefits of SSL Proxy Support for TLS 1.3

The TLS 1.3 protocol is simpler, faster, and more secure than that of version 1.2, and is widely used.

Information About DRE Optimisation Using Configuration Groups

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can deploy and manage Cisco Catalyst SD-WAN network more efficiently by optimizing traffic based on sites and applications using configuration groups in Cisco SD-WAN Manager.

Supported Devices for DRE

Integrated Service Nodes and Controllers

Devices	Release	Memory Requirements
Cisco Catalyst 8300 Series Edge Platforms: • C8300-1N1S-6T • C8300-1N1S-4T2X • C8300-2N2S-6T • C8300-2N2S-4T2X	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and later	• RAM: 16 GB • Storage: 600 GB
Cisco Catalyst 8200 Series Edge Platforms: • C8200-1N-4T	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later	• RAM: 16 GB • Storage: 600 GB
Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V)	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and later	• RAM: 16 GB • Storage: 600 GB • vCPUs: 8

External Service Nodes and Controllers

Devices	Release	Memory Requirements
Cisco Catalyst 8000V	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	• RAM: 32 GB • Storage: 2 TB • vCPUs: 16
	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	• RAM: 16 GB • Storage: 600 GB • vCPUs: 8
C8500L-8S4X	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	• RAM: 32 GB • Storage: 2 TB
	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	• RAM: 16 GB • Storage: 600 GB

Disk Recommendations for DRE

We recommend using solid-state drive (SSD) disks for deploying DRE as well as other AppQoE services.

Configure the following recommended parameters from Cisco Integrated Controller Manager (IMC). Ensure that you configure these before installing the hypervisor because some of the settings may require disk formatting.

Table 2: Recommended Disk Parameters

Parameter	Value
RAID level	RAID10
Read Policy	Always Read Ahead
Disk Cache Policy	Disabled
Write Policy	Write Back Good BBU
Strip Size	256 KB
I/O Cache Policy	Direct

Disk Provisioning Recommendation for Cisco Catalyst 8000V Deployment

While deploying Cisco Catalyst 8000V instances, choose Thick Provision Eager Zeroed as the disk format.

For information on deploying Cisco Catalyst 8000V instances on supported hypervisors, see:

- ESXi
- KVM

Secondary Disk Recommendations for DRE

While deploying Cisco Catalyst 8000V instances, the extra disk space is added after the basic system partitions are allocated under the /bootflash partition. However, if there is a need to increase the disk size, you must reinstall the instances to realize more usable disk space. The disk for Cisco Catalyst 8000V can be expanded at any time in the hypervisor. However, after the disk is formatted, the Cisco Catalyst 8000V cannot take the additional space.

Configure the following recommended parameters from Cisco Integrated Controller Manager (IMC). Ensure that you configure these before installing the hypervisor because some of the settings may require disk formatting.

Table 3: Recommended Disk Parameters

Cloud Type	Disk Type	Disk Size	Instance Type
AWS	Throughput Optimized HDD (st1)	2 TB	c5.4xlarge (16 vCPUs, 32 GB memory)
Microsoft Azure	SSD Persistent disk	2 TB	custom (16 vCPUs, 32 GB memory)
Google Cloud Platform (GCP)	Premium SSD	2 TB	Standard F16s_v2 (16 vCPUs, 32 GB memory)

For information about deploying a Cisco Catalyst 8000V on different platforms, see the following:

- Deploy Cisco Catalyst 8000V on AWS
- Deploy Cisco Catalyst 8000V on Microsoft Azure
- Deploy Cisco Catalyst 8000V on GCP

For deploying Cisco Catalyst 8000V on AWS, Azure, or GCP platforms, include a cloud-init configuration and attach the secondary disk during deployment.

Supported DRE Profiles

The following table provides this information:

- Devices that support DRE feature and their default DRE profiles.
- DRE profiles supported on the devices.
- The UTD profile supported along with the DRE profile size configured.
- Minimum resource recommendation for the supported DRE profiles.

- The maximum connections that the DRE profiles provide on the supported devices.
- The FanOut values that correspond to the DRE profiles configured on the devices. FanOut refers to the number of peers that a device can communicate with to form the DRE service.

Table 4: DRE Profiles, Resource Requirements, and Supported Connections and FanOut

Devices and Default DRE Profile	DRE Profiles	Supported UTD Profile	Minimum Deployment Recommendations		Maximum Connections	FanOut
			RAM	Disk		
C8200-1N-4T (S)	S	—	8 GB	120 GB	750	35
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	S	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
C8300-2N2S-4T2X (M)	S	S, M	8 GB	120 GB	750	35
	M	S	8 GB	280 GB	5000	70
	L	—	16 GB	500 GB	10,000	256
C8500L-8G4X (M)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	32 GB	500 GB	22,000	256
	XL	—	32 GB	1600 GB	36,000	256
Cisco Catalyst 8000V—6 core (S)	S	—	8 GB	120 GB	750	35
Cisco Catalyst 8000V—8 core (S)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
Cisco Catalyst 8000V—12 core (S)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	16 GB	500 GB	10,000	256

Devices and Default DRE Profile	DRE Profiles	Supported UTD Profile	Minimum Deployment Recommendations		Maximum Connections	FanOut
			RAM	Disk		
Cisco Catalyst 8000V—16 core (S)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	32 GB	500 GB	22000	256
	XL	—	32 GB	1600 GB	36000	256

Note UCS E-Series servers only support 6 core, 8 core, and 12 core Cisco Catalyst 8000V instances. For more information, see Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.

The following table provides this information:

- The memory, disk, and cache allocated based on the DRE profile configured on the supported devices.

Table 5: Profile-wise Resource Allocation

Devices and Default DRE Profile	DRE Profiles	Resource Allocation (GB)		
		Memory	Disk	Cache Size
C8200-1N-4T (S)	S	2	80	60
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	2	80	60
	M	4	250	230
C8300-2N2S-4T2X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
C8500L-8G4X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180
Cisco Catalyst 8000V—6 core (S)	S	2	80	60
Cisco Catalyst 8000V—8 core (S)	S	2	80	60
	M	4	250	230

Devices and Default DRE Profile	DRE Profiles	Resource Allocation (GB)		
		Memory	Disk	Cache Size
Cisco Catalyst 8000V—12 core (S)	S	2	80	60
	M	4	250	230
	L	8	480	460
Cisco Catalyst 8000V—16 core (S)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180

Note UCS E-Series servers only support 6 core, 8 core, and 12 core Cisco Catalyst 8000V instances. For more information, see Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.

Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be deployed on UCS E-Series server modules that reside in Cisco 4000 Series Integrated Services Routers and Cisco Catalyst 8300 Series Edge Platforms.

From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, you can deploy Cisco Catalyst 8000V instances on UCS E-Series UCS-E1100D-M6 server modules that are installed in Cisco Catalyst 8000 Series Edge platforms.

Device Family	Device Model	Supported UCS-E Module and DRE Profiles
Cisco 4000 Series Integrated Services Routers	Cisco 4461	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	Cisco 4451	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	Cisco 4351	UCS-E160S-M3/K9 (S)
	Cisco 4331	UCS-E160S-M3/K9 (S)

Device Family	Device Model	Supported UCS-E Module and DRE Profiles
Cisco Catalyst 8300 Series Edge Platforms	C8300-2N2S-4T2X	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L) UCS-E1100D-M6 (S)
	C8300-2N2S-6T	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L) UCS-E1100D-M6 (S)
	C8300-1N1S-4T2X	UCS-E160S-M3/K9 (S)
	C8300-1N1S-6T	UCS-E160S-M3/K9 (S)

Restrictions for DRE

- DRE is a dual-side solution. Therefore, flow symmetry is required to configure DRE optimization. DRE isn't supported for asymmetric flows.
- DRE is supported only if integrated service nodes or external service nodes are deployed at both ends of a Cisco Catalyst SD-WAN overlay tunnel.
- DRE isn't supported on devices that are configured as service controllers.
- In a scenario where Unified Threat Defense (UTD) is installed on a router and there is a data policy to redirect the traffic to an external service node, if the traffic is learned by UTD for a given VRF, then the same traffic cannot be redirected to an external service node.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a the default mode for SSL proxy is single-side. However, because DRE is a dual-side solution, it requires SSL on both, the sending and the receiving end, of the traffic. To optimize SSL performance for this dual-side use case, enable dual-side SSL optimization using the `dual-side optimization enable` command in Cisco SD-WAN Manager CLI templates. We don't recommended enabling dual-side SSL if you use GRE tunnels over the WAN.
- From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, SMB 311 auto bypass of encrypted traffic is enabled to the DRE. You can continue to manually enable the SMB311 encrypted traffic bypass policy to DRE, for the service nodes running on the devices prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.
- DRE optimization is not supported for Cisco Catalyst 8000V when deployed on Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) on CSP devices.

Restrictions for Installing Cisco Catalyst 8000V on UCS E-Series Servers

Note UCS E-Series Server support is applicable for installing Cisco Catalyst 8000V as an external service node starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a only.

- Only the VMware vSphere ESXi (release 6.7) hypervisor is supported for deploying Cisco Catalyst 8000V instances on UCS-E Series server modules.
- Hyperthreading should be disabled on VMware vSpehere ESXi hypervisor.
- Hyperthreading is not supported for the app-heavy core allocation profile for Cisco Catalyst 8000V deployed on UCS E-Series servers.
- Cisco Catalyst 8000V instances on UCS-E series server modules can only have 6, 8, or 12 cores.
- Cisco Catalyst 8000V instances on UCS-E series server modules should be configured with the app-heavy core allocation profile to enable them to run the DRE service.
- Only one Cisco Catalyst 8000V instance can be installed on a supported UCS E-Series server.
- To change the DRE profile applied to a device, you need to uninstall DRE, reinstall it, and then apply the new DRE profile.

Note Uninstalling DRE results in loss of cache data.

Configure DRE

Before You Begin

Cisco Catalyst 8000V instances on UCS and USC E-Series servers should be configured with the app-heavy resource allocation profile. This profile allows the Cisco Catalyst 8000V instances to participate in DRE optimization. Ensure to reload the device in order to apply the core allocation.

The following example shows how to configure a device as app-heavy using the Cisco SD-WAN Manager CLI Add-on feature template:

```
Device(config)# platform resource app-heavy
```

Upload DRE Container Image to the Software Repository

Prerequisite

Download the DRE container image from Cisco software downloads page. To download the DRE container image navigate to Catalyst 8000V Edge Software page and select IOS XE SD-WAN Software. You can use the same container image across the Cisco 8000 platform.

Upload the Container Image to Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Under **Upload Virtual Image**, choose **Manager**.
4. Browse to the downloaded container image on your local machine, and then click **Upload**.

When the upload is complete, the image appears in the **Virtual Images** window.

Upgrade DRE Container Virtual Image

To upgrade the container image, see Upgrade Software Image on a Device.

Enable DRE Optimization

Configure AppQoE Template for DRE

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose a device that is supported for DRE.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose on of the following device roles:
   - **Controller:** Choose **Controller** if you want to configure the device as a controller with an integrated service node. For devices that support an integrated service node, the **Enable** checkbox is available. This option is grayed out for devices that don't support the integrated service node functionality.
   - **Service Node:** Choose the **Service Node** option if you want to configure the device as an external service node. The **External Service Node** check box is enabled by default.

     The **Service Node** option is not visible if the device that you chose cannot be configured as an external service node.
7. Under **Advanced**, enable **DRE Optimization**.

8.

Note The Resource Profile field is applicable for DRE profiles. The DRE profiles feature was introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a. Therefore, this option is not available in previous releases.

(Optional) In the **Resource Profile** field, choose **Global** from the drop-down list. Next, choose a profile size from the options available.

If you don't configure the **Resource Profile**, the default DRE profile size for the device is applied. For more information on the default profiles, see Supported DRE Profiles.

9. (Optional) To optimize HTTPS, FTPS, or any other encrypted traffic, enable **SSL Decryption**.

Note If you enable **SSL Decryption**, you must configure an SSL/TLS decryption security policy so that the TLS service can decrypt the traffic before it is sent to the DRE container, and then encrypted again after the traffic is optimized.

10. Click **Save**.

Create Security Policy for SSL Decryption

This procedure applies if you enable SSL decryption at the time of configuring the AppQoE feature template to enable DRE optimization.

Configure CA for SSL Proxy

To configure certificate authority for SSL proxy, see Configure CA for SSL/TLS Proxy.

Configure Security Policy for SSL Decryption

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. Choose **Application Quality of Experience** and click **Proceed**.
4. Click **Add TLS/SSL Decryption Policy** and choose **Create New**.
5. Click **Enable SSL Decryption**. Alternatively, toggle the **SSL Decryption** option to enable it.
6. Enter **Policy Name** and other requested details.
7. Click **Save TLS/SSL Decryption Policy**. Your new policy appears in the window.
8. Click **Next**.
9. Enter **Security Policy Name** and **Security Policy Description**.
10. To view the CLI configuration for the policy, click **Preview**. Otherwise, click **Save**.

Update Device Template

For the DRE configuration to take effect, attach the AppQoE policy with DRE enabled, to the device template of the device for which you created the AppQoE policy with DRE.

1. To create a new device template or update an existing one, see Create a Device Template from Feature Templates
2. In the **Additional Templates** area, for **AppQoE**, choose the template you created in the Configure AppQoE Template for DRE section.

Note To deactivate the DRE service, detach the AppQoE template from the device template.

Create a Centralized Policy for TCP and DRE Optimization

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Under **Centralized Policy**, click **Add Policy**.

Note For more information, see Configure Centralized Policies Using Cisco SD-WAN Manager.

3. In the policy configuration wizard, click **Next** until you are on the **Configure Traffic Rules** window.
4. Click **Traffic Data**, and then click **Add Policy**.
5. Enter a name and description for your policy.
6. Click **Sequence Type** and from the **Add Data Policy** dialog box, choose **Custom**.
7. Click **Add Sequence Rule**.
8. Under the **Match** option, you can choose any match conditions that are applicable to a data policy, such as, Source Data Prefix, Application/Application Family List, and so on.
9. Under the **Actions** option, choose **Accept**. Choose **TCP Optimization** and **DRE Optimization** from the options.

   From Cisco Catalyst SD-WAN Manager Release 20.14.1, AppQoE clusters can handle both IPv4 and IPv6 traffic.

Note Not all actions are available for all match conditions. The actions available to you depend on the match conditions you choose. For more information, see Configure Traffic Rules.

10. Click **Save Match And Actions**.
11. Click **Save Data Policy**.
12. Apply the centralized data policy to the edge devices at the sites between which DRE optimization should be triggered for traffic flows. For more information, see Apply Policies to Sites and VPNs.
13. Activate the centralized policy. For more information, see Activate a Centralized Policy.

Configure DRE using Configuration Groups

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can enable DRE optimisation using Cisco SD-WAN Manager by configuring **AppQoE** feature under **Service Profile** in a configuration group. For more information see, AppQoE.

To optimize HTTPS, FTPS, or any other encrypted traffic, configure and deploy **TLS/SSL Decryption** from policy groups. For more information see, Embedded Security Additional Settings.

Configure DRE Using the CLI

Install DRE Container Package

To install the DRE container package, use the following command:

```
app-hosting install appid < name > package bootflash:<name>.tar
```

Configure Virtual Port Group and Map it to DRE

The following example shows how to configure a virtual port group and map it to the DRE service, and then start the DRE service:

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre


Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

Configure Virtual Port Group and Map it to DRE, and Assign a DRE Profile

Note The DRE Profiles feature is available starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a only. This feature is not applicable to releases before Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

The following example shows how to configure a virtual port group, map it to the DRE service and assign a DRE profile to the device. This example shows the small (S) profile being assigned.

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre
Device(config-app-hosting)# app-resource profile-package small


Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

Activate DRE Service

The following example shows how to activate DRE service for the application named Bangalore:

```
Device# app-hosting activate appid Bangalore
```

Note Use the **app-hosting activate appid** command if you've already configured the DRE application, but haven't enabled it. Alternatively, you can use the **start** command in application hosting gateway configuration mode, as shown in the example in the preceding section.

Uninstall DRE

Follow these steps to deactivate and uninstall the DRE service.

1. Use the following command in privileged EXEC mode to stop the DRE service.

   ```
   Device# app-hosting stop appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be stopped.

2. Use the following command in privileged EXEC mode to deactivate the DRE service.

   ```
   Device# app-hosting deactivate appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be deactivated.

3. Use the following command in privileged EXEC mode to uninstall the DRE service.

   ```
   Device# app-hosting uninstall appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be uninstalled.

Configure Cisco Catalyst 8000V on UCS-E Series Server Modules for DRE Optimization

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cisco Catalyst 8000V instances can be installed as external service nodes on supported UCS E-Series servers that reside in specific router models. This functionality enables the routers to act as hybrid clusters with integrated as well as external service nodes.

Configuration Workflow

1. Configure the UCS E-Series server on the supported router.
2. Deploy Cisco Catalyst 8000V on the supported UCS E-Series server.
3. In Cisco SD-WAN Manager, configure AppQoE feature template for Cisco Catalyst 8000V instances on UCS E-Series servers.
4. In Cisco SD-WAN Manager, configure the AppQoE feature template for the service controllers, and add additional configuration using Cisco SD-WAN Manager CLI template and CLI Add-on feature template.

Configure UCS E-Series Server

Before You Begin

Insert the UCS E-Series server module into the supported device and connect two interfaces (TE2 and TE3) from the front panel. For more information, see UCS-E Series Servers Hardware Installation Guide.

Configure UCS E-Series Server on the Supported Router

The following is sample configuration to enable UCS E-Series server on a supported router:

```
Device(config)# ucse subslot 1/0
Device(config-ucse)# imc access-port shared-lom <ge1/te2/te3>
Device(config-ucse)# imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x
Device(config-ucse)# exit
Device(config)# interface ucse1/0/0
Device(config-if)# ip address x.x.x.1 255.255.255.0
```

Deploy Cisco Catalyst 8000V on UCS E-Series Server

Before You Begin

- Install the hypervisor on the UCS-E server module.
- Download the Cisco Catalyst 8000V 17.6.1 OVA file from the Cisco software download page for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, and install it..

Configure IP Addresses for Cisco Catalyst 8000V

The following is a sample for configuring IP addresses for Cisco Catalyst 8000V on the UCS E-Series server:

```
Device(config)# interface GigabitEthernet1
Device(config-if)# description Mgmt
Device(config-if)# ip addeess x.x.x.x x.x.x.x
Device(config)# int GigabitEthernet2
Device(config-if)# description WAN-CONTROLLER
Device(config-if)# ip address x.x.x.x x.x.x.x
Device(config-if)# exit
Device(config)# int GigabitEthernet3
Device(config-if)# description UCSE-INTF
Device(config-if)# ip addeess x.x.x.x x.x.x.x
```

Configure AppQoE Feature Template for Cisco Catalyst 8000V Instances

Before You Begin

Cisco Catalyst 8000V instances on UCS E-Series servers should be configured with the app-heavy resource allocation profile. This profile allows the Cisco Catalyst 8000V instances to participate in DRE optimization. Ensure to reload the device in order to apply the core allocation.

The following example shows how to configure a device as app-heavy using the Cisco SD-WAN Manager CLI Add-on feature template:

```
Device(config)# platform resource app-heavy
```

Enable DRE Optimization for Cisco Catalyst 8000V Instances

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose **C8000v**.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose the **Service Node** option.
7. Under the **Advanced** section, enable **DRE Optimization**.
8. Click **Save**.

Configure the Controller Cluster Types

Add UCS E-Series Server Configuration in Cisco SD-WAN Manager

In Cisco SD-WAN Manager, create a CLI Add-on feature template and update it with UCS E-Series server configuration.

The following is sample configuration for UCS E-Series servers that can be added to the CLI Add-on feature template:

```
ucse subslot 1/0
imc access-port shared-lom te2
imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x

interface ucse1/0/0
vrf forwarding 5
```

Option 1: Configure Service Controller as the Cluster Type

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. In the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Leave the **Integrated Service Node** check box unchecked.

7. In the **Controller IP address** field, enter the IP address of the controller.

   Alternatively, choose **Default** from the drop-down list. The AppQoE controller address is chosen by default.

8. In the **Service VPN** field, enter the service VPN number.

   Alternatively, choose **Default** from the drop-down list. The AppQoE service VPN is chosen by default.

9. In the **Service Nodes** area, click **Add Service Nodes** to add service nodes to the AppQoE service node group.

10. Click **Save**.

11. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

    - CLI Add-on feature template with the UCS E-Series server configuration
    - AppQoE feature template

    For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as the integrated service node separately. For more information, see Enable DRE Optimization.

Option 2: Configure Hybrid as the Cluster Type

Routers that have Cisco Catalyst 8000V instances deployed on their UCS E-Series servers can be configured with cluster types as service-controllers or hybrid.

1. From theCisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **Feature**.

3. From the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.

4. Under **Other Templates**, click **AppQoE**.

5. Enter **Template Name** and **Description**.

6. For the **Integrated Service Node** field, check the **Enable** check box.

7. Click **Save**.

8. Create a CLI template to add the cluster-type hybrid configuration.

   The following is a sample configuration to configure the cluster type as hybrid on the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

```
interface VirtualPortGroup2
 vrf forwarding 5
 ip address 192.168.2.1 255.255.255.0

interface ucse1/0/0
 vrf forwarding 5
 ip address 10.40.17.1 255.255.255.0
```

```
service-insertion service-node-group appqoe SNG-APPQOE
 service-node 192.168.2.2
service-insertion service-node-group appqoe SNG-APPQOE1
 service-node 10.40.17.5
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 10.40.17.1 vrf 5

service-insertion service-context appqoe/1
 cluster-type hybrid
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
 service-node-group SNG-APPQOE1
 vrf global
 enable
```

9. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:
   - AppQoE feature template
   - CLI Add-on feature template with the UCS E-Series server configuration
   - CLI template with the hybrid cluster configuration

   For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as integrated service node separately. For more information, see Enable DRE Optimization.

Monitor DRE

To view the AppQoE DRE data on Cisco SD-WAN Manager, ensure that you:

- Synchronize the controller and device time by configuring Network Time Protocol (NTP). You can also set the clock manually using the **clock set** command.
- Add the following commands to the device configuration:
  - **policy ip visibility features multi-sn enable**
  - **policy ip visibility features dre enable**
  - **policy ip visibility features sslproxy enable** (for SSL traffic)

From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. Enable **On-demand Troubleshooting** to view the dashboards. The dashboard screens do not display real-time information. You can also retrieve the DPI statistics by selecting the device from the drop-down menu and choosing the **Data Type** as **DPI**.

You can monitor the traffic or applications optimized by DRE using Cisco SD-WAN Manager.

From Cisco vManage Release 20.9.x, you can use **On-Demand Troubleshooting** to monitor traffic or applications optimized by DRE.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier releases: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Click the hostname of the device you want to monitor.
3. Under **On-Demand Troubleshooting**, choose **AppQoE DRE Optimization**.
4. Enable **On-Demand Troubleshooting** to view details of the selected device.
5. Choose **Optimized Traffic** or **Application**, depending on what you want to monitor.
6. Choose **Controller** or **Service Node**.

   If the chosen device has an integrated service node, you can view the data for either the controller role or the service node role. If the chosen device is an external AppQoE service node, you can view the monitoring data for the external service node, as well as the controller that it's connected to.

Chart and Table View Options

The monitoring data for your selected device displays in the form of a chart, followed by a table. You can view the data in form of a graph or bar chart by toggling between the two options.

- From the **Chart Options** drop-down list, you can view the data by **Bytes** or **Percentage Reduction**.
- You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

Verify and Monitor and Troubleshoot DRE Using CLI

DRE Optimization Status

The following is a sample output of the **show sdwan appqoe dreopt status** command:

```
Device# show sdwan appqoe dreopt status

DRE ID                                          : 52:54:dd:d0:e2:8d-0176814f0f66-93e0830d

DRE uptime                                      : 18:27:43

Health status                                   : GREEN

Health status change reason                     : None

Last health status change time                  : 18:25:29

Last health status notification sent time       : 1 second

DRE cache status                                : Active

Disk cache usage                                : 91%

Disk latency                                    : 16 ms

Active alarms:

  None


Configuration:
```

```
  Profile type                              : Default
  Maximum connections                       : 750
  Maximum fanout                            : 35
  Disk size                                 : 400 GB
  Memory size                               : 4096 MB
  CPU cores                                 : 1
  Disk encryption                           : ON
```

To view the status in more detail, use the **show sdwan appqoe dreopt status detail** command.

```
Device# show sdwan appqoe dreopt statistics detail
Total connections                 : 325071
Max concurrent connections        : 704
Current active connections        : 0
Total connection resets           : 297319
Total original bytes              : 6280 GB
Total optimized bytes             : 2831 GB
Overall reduction ratio           : 54%
Disk size used                    : 93%
Cache details:
  Cache status                      : Active
  Cache Size                        : 406573 MB
  Cache used                        : 93%
  Oldest data in cache              : 17:13:53:40
  Replaced(last hour): size         : 0 MB
  Cache created at                  : 27:14:13:43
  Evicted cache in loading cache    : 149610430464
Connection reset reasons:
  Socket write failures                           : 0
  Socket read failures                            : 0
  DRE decode failures                             : 0
  DRE encode failures                             : 0
  Connection init failures                        : 0
  WAN unexpected close                            : 297319
  Buffer allocation or manipulation failed        : 0
```

```
  Peer received reset from end host                   : 0
  DRE connection state out of sync                    : 0
  Memory allocation failed for buffer heads           : 0
  Other reasons                                       : 0
Connection Statistics:
  Alloc                                               : 325071
  Free                                                : 325071
Overall EBP stats:
  Data EBP received                                   : 1921181978
  Data EBP freed                                      : 1921181978
  Data EBP allocated                                  : 218881701
  Data EBP sent                                       : 218881701
  Data EBP send failed                                : 0
  Data EBP no flow context                            : 0
  Data EBP requested more than max size               : 46714730
```

DRE Auto-bypass Status

The following example shows the auto-bypass status of DRE optimization.

```
Device# show sdwan appqoe dreopt auto-bypass

      Server IP   Port       State    DRE LAN BYTES    DRE WAN BYTES    DRE COMP   Last
Update   Entry Age
-------------------------------------------------------------------------------------------------------

      10.0.0.1    9088       Monitor      48887002724      49401300299   0.000000
13:41:51   03:08:53
```

DRE Optimization Statistics

The following example shows DRE optimization statistics.

```
Device# show sdwan appqoe dreopt statistics

Total connections                 : 3714
Max concurrent connections        : 552
Current active connections        : 0
Total connection resets           : 1081
Total original bytes              : 360 GB
Total optimized bytes             : 164 GB
Overall reduction ratio           : 54%
```

```
Disk size used                    : 91%

Cache details:

  Cache status                      : Active

  Cache Size                        : 407098 MB

  Cache used                        : 91%

  Oldest data in cache              : 03:02:07:55

  Replaced(last hour): size         : 0 MB
```

The following example shows DRE optimization statistics for a peer device.

```
Device# show sdwan appqoe dreopt statistics peer

  Peer No.  System IP          Hostname    Active connections    Cummulative connections
-------------------------------------------------------------------------------------------

         0  209.165.201.1       dreopt                    0                       3714
```

DRE Decryption Status

The following example shows how to send a decryption request to DRE and verify if the request was successfully received.

```
Device# show sdwan appqoe dreopt crypt

Status: Success

Atempts: 1

1611503718:312238        DECRYPT REQ SENT

1611503718:318198        CRYPT SUCCESS

ENCRYPTION:

-------------------------------------------------

BLK NAME        :  No of Oper  | Success | Failure

-------------------------------------------------

SIGNATURE BLOCK |     210404     210404          0

SEGMENT BLOCK   |     789411     789411          0

SECTION BLOCKS  |      49363      49363          0

-------------------------------------------------

DECRYPTION:

-------------------------------------------------

BLK NAME        :  No of Oper  | Success | Failure

-------------------------------------------------
```

```
SIGNATURE BLOCK |     188616     188616          0

SEGMENT BLOCK   |          1          1          0

SECTION BLOCKS  |     366342     366342          0

-------------------------------------------------
```

Troubleshoot DRE

The following sample output displays the statistics for the auto discovery of peer devices. When connections are not optimized by DRE, run this command and share the output with Cisco Technical Support.

```
Device# show sdwan appqoe ad-statistics

============================================================

              Auto-Discovery Statistics

============================================================

 Auto-Discovery Option Length Mismatch       : 0

 Auto-Discovery Option Version Mismatch      : 0

 Tcp Option Length Mismatch                  : 6

 AD Role set to NONE                         : 0

 [Edge] AD Negotiation Start                 : 96771

 [Edge] AD Negotiation Done                  : 93711

 [Edge] Rcvd SYN-ACK w/o AD options          : 0

 [Edge] AOIM sync Needed                     : 99

 [Core] AD Negotiation Start                 : 10375

 [Core] AD Negotiation Done                  : 10329

 [Core] Rcvd ACK w/o AD options              : 0

 [Core] AOIM sync Needed                     : 0
```

The following sample output displays the statistics for one time exchange of information between peer devices.

```
Device# show sdwan appqoe aoim-statistics

============================================================

              AOIM Statistics

============================================================

 Total Number Of Peer Syncs      : 1

 Current Number Of Peer Syncs in Progress      : 0

 Number Of Peer Re-Syncs Needed      : 1

 Total Passthrough Connections Due to Peer Version Mismatch   : 0

 AOIM DB Size (Bytes): 4194304
```

```
 LOCAL AO Statistics

---------------------------------------

 Number Of AOs      : 2

 AO             Version   Registered

 SSL             1.2        Y

 DRE             0.23       Y


 PEER Statistics

---------------------------------------

 Number Of Peers      : 1

 Peer ID: 203.203.203.11

 Peer Num AOs      : 2

 AO             Version   InCompatible

 SSL             1.2        N

 DRE             0.23       N
```

The following example shows how to clear DRE cache. Clearing cache restarts the DRE service.

```
Device# clear sdwan appqoe dreopt cache

DRE cache successfully cleared
```

Monitor SSL Proxy

To view the AppQoE data on Cisco SD-WAN Manager, ensure that you:

- Synchronize the controller and device time by configuring Network Time Protocol (NTP). You can also set the clock manually using the **clock set** command.
- Add the **policy ip visibility features sslproxy enable** command to the device configuration:

From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. Enable **On-demand Troubleshooting** to view the dashboards. The dashboard screens do not display real-time information. You can also retrieve the DPI statistics by selecting the device from the drop-down menu and choosing the **Data Type** as **DPI**.

You can monitor the traffic optimized by SSL Proxy using Cisco SD-WAN Manager.

From Cisco vManage Release 20.9.x, you can use **On-Demand Troubleshooting** to monitor traffic optimized by SSL Proxy.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.1 and earlier releases: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Click the hostname of the device you want to monitor.
3. Under **On-Demand Troubleshooting**, choose **SSL Proxy**.
4. Enable **On-Demand Troubleshooting** to view details of the selected device.
5. Choose **Traffic View** type from the drop-down menu to view data in graph or tabular format.

   You can also click **Filter** to choose by VPN, local or remote TLOC, traffic source and more.

Chart and Table View Options

The monitoring data for your selected device displays in the form of a chart, followed by a table. You can view the data in form of a graph or bar chart by toggling between the two options.

You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

Verify SSL Proxy Support for TLS 1.3 Using CLI

The following is a sample output from the **show ssl proxy statistics** command showcases SSL statistics and TLS flow counters. The count for the TLS flow counter for version 1.3 is shown as 8.

```
Device# show sslproxy statistics
=========================================================
SSL Statistics:
=========================================================
Flow Selected SSL/TLS version:
TLS 1.0 Flows : 0
TLS 1.1 Flows : 0
TLS 1.2 Flows : 0
TLS 1.3 Flows : 8
```