



**Progress<sup>®</sup>**

# Kemp ECS Connection Manager

## Deployment Guide

UPDATED: 01 February 2022

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS\_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

# Table of Contents

---

<b>1 Introduction</b> .....	<b>6</b>
1.1 Intended Audience .....	6
1.2 Document Purpose .....	6
<b>2 Template</b> .....	<b>8</b>
<b>3 Dell EMC ECS</b> .....	<b>9</b>
<b>4 ECS Connection Manager Global Settings</b> .....	<b>10</b>
4.1 Layer 4 Considerations before Deployment .....	10
4.2 Enable Subnet Originating Requests Globally .....	11
4.3 Enable Check Persist Globally .....	12
<b>5 ECS Connection Manager Virtual Services with Layer 4</b> .....	<b>14</b>
5.1 Create a Virtual Service using a Template .....	14
5.2 S3 Virtual Services Layer 4 .....	15
5.2.1 S3 HTTP Layer 4 Virtual Service Recommended API Settings (optional) .....	15
5.2.2 S3 HTTPS Layer 4 Virtual Service Recommended API Settings (optional) .....	15
5.3 Atmos Virtual Services Layer 4 .....	16
5.3.1 Atmos HTTP Layer 4 Virtual Service Recommended API Settings (optional) .....	16
5.3.2 Atmos HTTPS Layer 4 Virtual Service Recommended API Settings (optional) .....	16
5.4 Swift Virtual Services Layer 4 .....	17
5.4.1 Swift HTTP Layer 4 Virtual Service Recommended API Settings (optional) .....	17
5.4.2 Swift HTTPS Layer 4 Virtual Service Recommended API Settings (optional) .....	17
5.5 ECS Connection Manager Virtual Services Layer 7 .....	18

---

5.5.1 Create a Virtual Service using a Template .....	18
5.5.2 S3 Virtual Services Layer 7 .....	19
5.5.2.1 S3 HTTP Layer 7 Virtual Service Recommended API Settings (optional) .....	19
5.5.2.2 S3 HTTPS Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional) .....	20
5.5.2.3 S3 HTTPS Offload Layer 7 Virtual Service Recommended API Settings (optional) ..	20
5.5.3 Atmos Virtual Services Layer 7 .....	21
5.5.3.1 Atmos HTTP Layer 7 Virtual Service Recommended API Settings (optional) .....	21
5.5.3.2 Atmos HTTPS Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional) .....	21
5.5.3.3 Atmos HTTPS Offload Virtual Service Recommended API Settings (optional) .....	22
5.5.4 Swift Virtual Services Layer 7 .....	23
5.5.4.1 Swift HTTP Layer 7 Virtual Service Recommended API Settings (optional) .....	23
5.5.4.2 Swift HTTPS Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional) .....	23
5.5.4.3 Swift HTTPS Offloaded Layer 7 Virtual Service Recommended API Settings (optional) .....	24
5.5.5 NFS Virtual Services Layer 7 .....	25
5.5.5.1 NFS TCP Virtual Service Recommended API Settings (optional) .....	26
5.5.5.2 NFS UDP PortMap Virtual Service Recommended API Settings (optional) .....	27
5.5.5.3 NFS UDP MountD Virtual Service Recommended API Settings (optional) .....	27
5.5.5.4 NFS UDP LockD Virtual Service Recommended API Settings (optional) .....	28
5.5.6 ECS Web Interface Virtual Services .....	28
5.5.6.1 ECS Web Interface Virtual Service Recommended API Settings (optional) .....	29

---

5.5.7 ECS XOR Virtual Services Layer 7 .....	29
5.5.7.1 ECS XOR Virtual Service Layer 7 .....	30
5.5.7.2 ECS XOR Offloaded Layer 7 Virtual Service Recommended API Settings (optional) .....	30
5.5.7.3 ECS XOR Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional) .....	32
5.5.8 Troubleshooting .....	34
5.5.8.1 Connections Rejected .....	34
<b>6 QoS/Rate Limiting .....</b>	<b>35</b>
6.1 Global Limits .....	35
6.2 Limiter Options .....	35
6.3 Client Limiting .....	36
6.4 URL Based Limiting .....	36
6.5 Per-Virtual Service Limiting .....	37
<b>7 References .....</b>	<b>38</b>
<b>Last Updated Date .....</b>	<b>39</b>

# 1 Introduction

The Dell EMC Elastic Cloud Storage (ECS) is a rack-based, flexible, and expandable object storage solution. You can configure the ECS through a web management interface frontend (HTTPS). In combination with a Kemp ECS Connection Manager, ECS can provide object storage using the protocols S3, Atmos, SWIFT, and Network File System (NFS) in addition to the web management interface. Other protocols such as CAS are also possible but are published without load balancers.

## 1.1 Intended Audience

Anyone interested in configuring the Kemp ECS Connection Manager to load balance Dell EMC ECS.

## 1.2 Document Purpose

This deployment guide provides instructions on how to configure the Kemp ECS Connection Manager to load balance Dell EMC ECS services using Kemp application templates. This guide should only be used as a reference for the load balancing configuration of ECS services because each environment is unique and may have different requirements. This guide also outlines the load balancing configuration using custom ECS ports in the Kemp application templates, but default ports can also be leveraged based on the environment.

This guide outlines the configuration of Virtual Services (VSs) based on best practices. There are two approaches when publishing Dell EMC ECS through the Kemp ECS Connection Manager:

**Layer 4:** When SSL/TLS offloading is not required, Layer 4 may be used to pass the traffic back to the ECS nodes. Transparency is automatically enabled when using Layer 4. This sends the original source IP address to the Real Servers. For more information, see the [Transparency Feature Description](#). Using Layer 4 has the following requirements:

- The **ECS Connection Manager** must be set up in a two-arm configuration.
- ECS nodes must use the **ECS Connection Manager** as the default gateway.
- All connections to the ECS environment must be initiated from a different subnet.

**Layer 7:** When using SSL/TLS offloading or when the above requirements may not be met, you can leverage Layer 7. Layer 7 by default does not use transparency and therefore the IP address of the ECS Connection Manager is used when accessing the ECS environment. The X-Forwarded-For header is leveraged to provide the original source IP address in the ECS logs for troubleshooting purposes. When a secure connection is used, a certificate must be installed on the ECS Connection Manager to

## 1 Introduction

decrypt the traffic for the X-Forwarded-For header insertion. This traffic can then be re-encrypted or offloaded depending on the security requirements.

ECS Connection Manager allows for QoS/ Rate Limiting to be applied to provide granular controls to the traffic when layer 7 is used. For more information refer the section **QoS/Rate Limiting** in this document.

Contact Kemp Support for any questions regarding configuration options.

# 2 Template

Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. You can remove templates after use, and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

---

When we first create a High availability (HA) pair with ECS Connection Managers the pre-installed templates replicate between each other. This creates duplicate templates in the template list.

Before creating a HA pair with ECS Connection Managers, ensure that you have removed the pre-installed template from one of the ECS Connection Managers.

---

Download released templates from the following page: [LoadMaster Templates](#).

For more information and steps on how to import and use templates, refer to the [Virtual Services and Templates, Feature Description](#).



# 3 Dell EMC ECS

Dell EMC ECS is a software-defined object storage solution that can be deployed as a complete storage appliance or leverage supported standard hardware. Dell EMC ECS consists of the following components:

- ECS Portal and Provisioning Services
- Data Services
- Storage Engine
- Fabric
- Infrastructure
- Hardware

The following table provides a list of the Dell EMC ECS default ports and protocols used for accessing the storage:

ECS Protocol	Transport Protocol or Daemon Service	Port
S3	HTTP	9020
	HTTPS	9021
Atmos	HTTP	9022
	HTTPS	9023
Swift	HTTP	9024
	HTTPS	9025
NFS	Portmap	111
	Mountd, nfsd	2049
	Lockd	10000

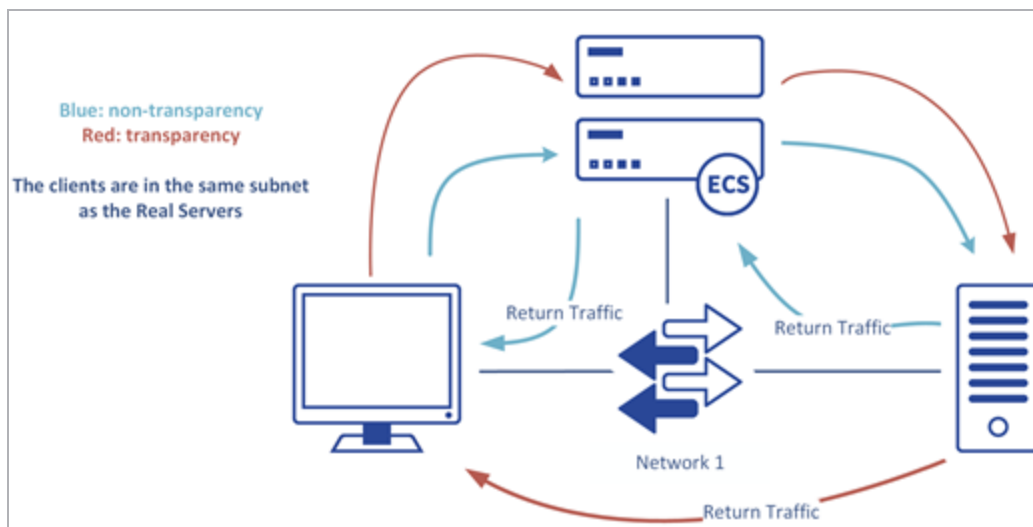
# 4 ECS Connection Manager Global Settings

Before setting up the Virtual Services, you must configure the following global settings to support the workload.

## 4.1 Layer 4 Considerations before Deployment

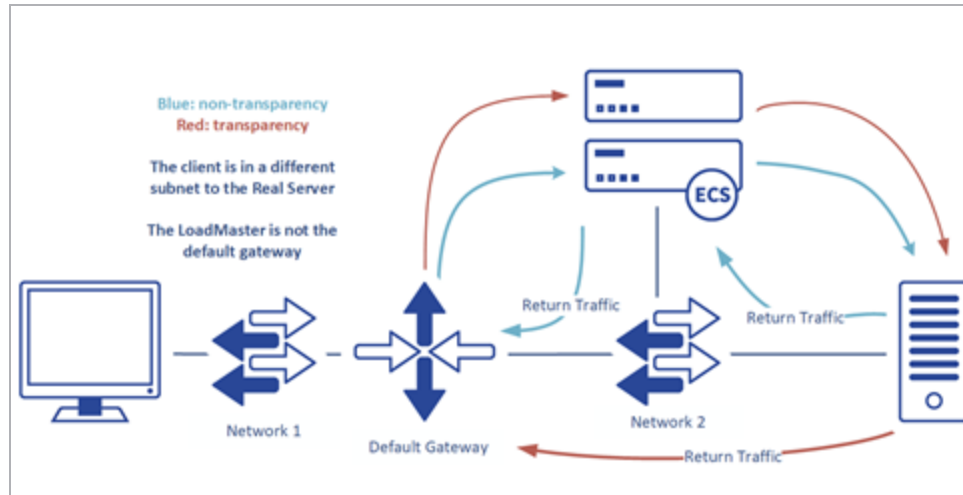
For this application, if you are using a Layer 4 service, it is automatically transparent. When using transparency, the following steps must be followed:

- If clients are on the same subnet as the Real Server, returning traffic to the ECS Connection Manager is instead sent to the client. This is asymmetric routing and causes the client to drop the connection because it is expecting it from the ECS Connection Manager, not the Real Server. The diagram below shows the flow of traffic when this rule is not followed.



- If the Real Servers' default gateway is not set to be the ECS Connection Manager's interface (the shared IP of the ECS Connection Managers are in High Availability (HA)), traffic returning to the ECS Connection Manager is instead sent to the gateway. This is asymmetric routing and causes the connection to drop because the connection should be sent from the ECS

Connection Manager, not the ECS Nodes. The diagram below shows the flow of traffic when this rule is not followed.



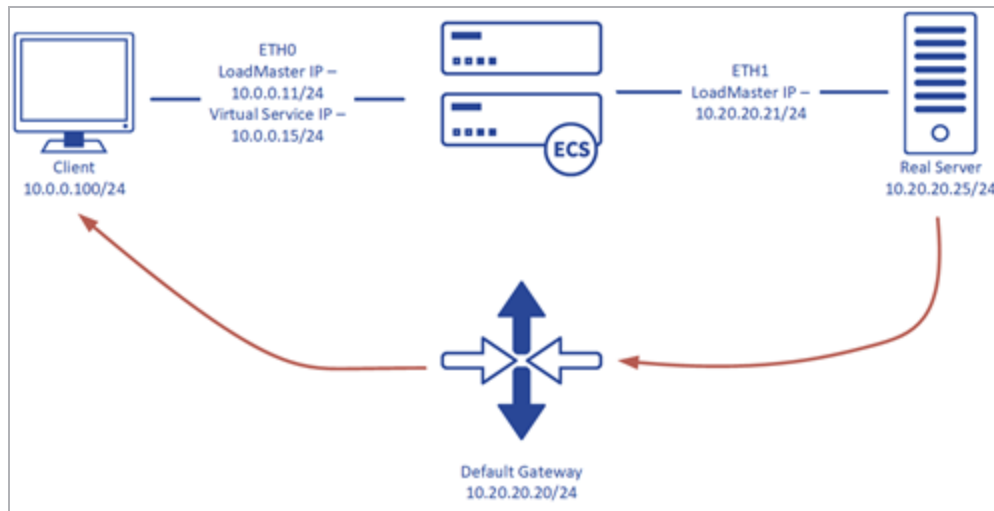
## 4.2 Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled.

Because this application can run at Layer 4, transparency is enforced. Transparency takes a higher priority than **Subnet Originating Requests**. Therefore, if transparency is enabled on the Virtual Service and **Subnet Originating Requests** is enabled globally, the Virtual Service still uses transparency. The Real Server sees traffic from this virtual service originating with the client's source IP address (transparency). Refer to the **Transparency Feature Description** document on the [Kemp Documentation page](#) for more details.



In the diagram above, you can see the following details:

- Client: 10.0.0.100/24
- Virtual Service on **eth0**: 10.0.0.15/24
- Real Server on **eth1**: 10.20.20.25/24

With **Subnet Originating Requests** enabled, the Real Server sees traffic originating from 10.20.20.21 (ECS Connection Manager eth1 address) and responds correctly.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (ECS Connection Manager Virtual Service address on **eth0**) and responds to **eth0** causing asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If the **Subnet Originating Requests** option is disabled globally, you can choose whether or not to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the ECS Connection Manager Web User Interface (WUI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

### 4.3 Enable Check Persist Globally

It is recommended that you change the **Always Check Persist** option to **Yes – Accept Changes**. Use the following steps:

1. Go to **System Configuration > Miscellaneous Options > L7 Configuration**.

Allow connection scaling over 64K Connections	<input type="checkbox"/>	
Always Check Persist	<input type="text" value="No"/>	
Add Port to Active Cookie	<input type="checkbox"/>	
Conform to RFC	<input checked="" type="checkbox"/>	
Close on Error	<input type="checkbox"/>	
Add Via Header In Cache Responses	<input type="checkbox"/>	
Real Servers are Local	<input type="checkbox"/>	
Drop Connections on RS failure	<input type="checkbox"/>	
Drop at Drain Time End	<input type="checkbox"/>	
L7 Connection Drain Time (secs)	<input type="text" value="300"/>	<b>Set Time</b> (Valid values:0, 60 - 86400)
L7 Authentication Timeout (secs)	<input type="text" value="30"/>	<b>Set Timeout</b> (Valid values:30 - 300)
L7 Wait after POST(ms)	<input type="text" value="2000"/>	<b>Set Post Wait</b> (Valid values:1 - 2000)
L7 Client Token Timeout (secs)	<input type="text" value="120"/>	<b>Set Timeout</b> (Valid values:60 - 300)
Additional L7 Header	<input type="text" value="X-Forwarded-For"/>	
100-Continue Handling	<input type="text" value="RFC-7231 Compliant"/>	
Allow Empty POSTs	<input type="checkbox"/>	
Allow Empty HTTP Headers	<input type="checkbox"/>	
Force Complete RS Match	<input type="checkbox"/>	
Least Connection Slow Start	<input type="text" value="0"/>	<b>Set Slow Start</b> (Valid values:0 - 600)
Share SubVS Persistence	<input type="checkbox"/>	
Log Insight Message Split Interval	<input type="text" value="10"/>	<b>Set Log Split Interval</b> (Valid values:1 - 100)
Include User Agent Header in User Logs	<input type="checkbox"/>	
Use CEF Log Format	<input type="checkbox"/>	
SSO Maximum Threads	<input type="text" value="128"/>	<b>Set SSO Max Threads</b> (Valid values:64 - 512)
NTLM Proxy Mode	<input checked="" type="checkbox"/>	

2. Click the **Always Check Persist** drop-down arrow and select **Yes – Accept Changes**.

# 5 ECS Connection Manager Virtual Services with Layer 4

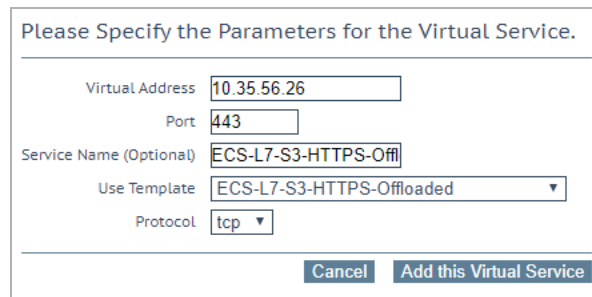
This step-by-step setup of Virtual Services leverages the Kemp application template for Dell EMC ECS with Layer 4. Layer 4 has the following requirements:

- The ECS Connection Manager must be set up in a two-arm configuration.
- ECS nodes must use the Kemp ECS Connection Manager as the default gateway.
- All connections to the ECS environment must be initiated from a different subnet.

The table in each section outlines the settings configured by the application template. You can use this information to manually configure Virtual Services or use the Kemp ECS Connection Manager Application Programming Interface (API) and automation tools.

## 5.1 Create a Virtual Service using a Template

To configure a Virtual Service using the application template, perform the following steps:



Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text" value="10.35.56.26"/>
Port	<input type="text" value="443"/>
Service Name (Optional)	<input type="text" value="ECS-L7-S3-HTTPS-Offl"/>
Use Template	<input type="text" value="ECS-L7-S3-HTTPS-Offloaded"/>
Protocol	<input type="text" value="tcp"/>

1. In the main menu of the **ECS Connection Manager** WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.
3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Expand the **Real Servers** section.
6. Click **Add New**.

7. Type the **Real Server Address** (you can use an IP address or FQDN).
8. Confirm that the correct port is entered.
9. Click **Add This Real Server**.

## 5.2 S3 Virtual Services Layer 4

The following section outlines the Layer 4 configuration options for using S3 with Dell EMC ECS.

### 5.2.1 S3 HTTP Layer 4 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
VStype	http
ForceL7	0
Schedule	lc
CheckType	tcp
CheckPort	9020

### 5.2.2 S3 HTTPS Layer 4 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
ForceL7	0
Schedule	lc

API Parameter	API Value
CheckType	tcp
CheckPort	9021

### 5.3 Atmos Virtual Services Layer 4

The following section outlines the Layer 4 configuration options for using Atmos with Dell EMC ECS.

#### 5.3.1 Atmos HTTP Layer 4 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
VStype	http
ForceL7	0
Schedule	lc
CheckType	tcp
CheckPort	9022

#### 5.3.2 Atmos HTTPS Layer 4 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
ForceL7	0
Schedule	lc



API Parameter	API Value
CheckType	tcp
CheckPort	9023

## 5.4 Swift Virtual Services Layer 4

The following section outlines the Layer 4 configuration options for using Swift with Dell EMC ECS.

### 5.4.1 Swift HTTP Layer 4 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
VStype	http
ForceL7	0
Schedule	lc
CheckType	tcp
CheckPort	9024

### 5.4.2 Swift HTTPS Layer 4 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. These settings can be used with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
ForceL7	0
Schedule	lc

API Parameter	API Value
CheckPort	9025

## 5.5 ECS Connection Manager Virtual Services Layer 7

This step-by-step setup of Virtual Services leverages the Kemp application template for Dell EMC ECS with Layer 7. Layer 7 does not have the same requirements as the Layer 4 configuration above:

- The ECS Connection Manager can be set up with one-arm or two-arm configurations.
- ECS nodes do not require the use of the ECS Connection Manager as the default gateway.
- Connections to the ECS environment can be initiated from the same subnet or a different subnet.

In addition, Layer 7 by default does not use transparency and therefore the IP address of the ECS Connection Manager is used when accessing the ECS environment. X-Forwarded-For header is leveraged to provide the original source IP address in the ECS logs for troubleshooting purposes. When a secure connection is used, a certificate must be installed on the ECS Connection Manager to decrypt the traffic for the X-Forwarded-For header insertion. This traffic can then be re-encrypted or offloaded depending on the security requirements. The ECS environment requires some configuration for X-Forwarded-For to be leveraged. Consult with Dell EMC to enable this feature in ECS.

The table in each section outlines the settings configured by the application template. You can use this information to manually configure Virtual Services or using the Kemp ECS Connection Manager API and automation tools.

### 5.5.1 Create a Virtual Service using a Template

To configure a Virtual Service using the application template, perform the following steps:

Please Specify the Parameters for the Virtual Service.

Virtual Address

Port

Service Name (Optional)

Use Template

Protocol

1. In the main menu of the **ECS Connection Manager** WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.
3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Required only for TLS/SSL offload and re-encrypt: Expand the **SSL Properties** section.
6. Required only for TLS/SSL offload and re-encrypt: Select the certificate to use in the **Available Certificates** and click the arrow (>) to move it to **Assigned Certificates**.
7. Expand the **Real Servers** section.
8. Click **Add New**.
9. Type the **Real Server Address**.
10. Confirm that the correct port is entered.
11. Click **Add This Real Server**.

### 5.5.2 S3 Virtual Services Layer 7

The following section outlines the Layer 7 configuration options for using S3 with Dell EMC ECS.

#### 5.5.2.1 S3 HTTP Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp
CheckPort	9020

### 5.5.2.2 S3 HTTPS Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
SSLReencrypt	1
AddVia	1
TLSType	1
CipherSet	BestPractices
CheckType	tcp
CheckPort	9021

### 5.5.2.3 S3 HTTPS Offload Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1

API Parameter	API Value
AddVia	1
TLSType	1
CipherSet	BestPractices
CheckType	tcp
CheckPort	9020

### 5.5.3 Atmos Virtual Services Layer 7

The following section outlines the Layer 7 configuration options for using Atmos with Dell EMC ECS.

#### 5.5.3.1 Atmos HTTP Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
VSType	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp
CheckPort	9022

#### 5.5.3.2 Atmos HTTPS Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	443

API Parameter	API Value
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
SSLReencrypt	1
AddVia	1
TLSType	1
CipherSet	BestPractices
CheckMethod	tcp
CheckPort	9023

### 5.5.3.3 Atmos HTTPS Offload Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. These settings can be used with scripts and automation tools. SSL/TLS certificates should be added before creating this VS. For further information on certificates, refer to the [SSL Accelerated Services Feature Description](#).

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
AddVia	1
TLSType	1

API Parameter	API Value
CipherSet	BestPractices
CheckType	tcp
CheckPort	9022

#### 5.5.4 Swift Virtual Services Layer 7

The following section outlines the Layer 7 configuration options for using Swift with Dell EMC ECS.

##### 5.5.4.1 Swift HTTP Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	80
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp
CheckPort	9024

##### 5.5.4.2 Swift HTTPS Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. These settings can be used with scripts and automation tools.

API Parameter	API Value
port	443
prot	tcp
VStype	http

API Parameter	API Value
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
SSLReencrypt	1
AddVia	1
TLSType	1
CipherSet	BestPractices
CheckType	tcp
CheckPort	9025

#### 5.5.4.3 Swift HTTPS Offloaded Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools. SSL/TLS certificates should be added before creating this VS. For further information on certificates, refer to the [SSL Accelerated Services Feature Description](#).

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
AddVia	1
TLSType	1
CipherSet	BestPractices
CheckType	tcp



API Parameter	API Value
CheckPort	9024

### 5.5.5 NFS Virtual Services Layer 7

The following section outlines the configuration options for using NFS with Dell EMC ECS. NFS requires four Virtual Services set up by the application template. You must use port following to ensure traffic is sent to the same ECS node.

Please Specify the Parameters for the Virtual Service.

Virtual Address:

Port:

Service Name (Optional):

Use Template:

Protocol:

1. Deploy NFS Virtual Services using the application template.
2. Configure port following for the ECS-NFS-L7-UDP-Portmap Virtual Service:
  - a) In the main menu of the **ECS Connection Manager** WUI, go to **Virtual Services > View/Modify Services**.
  - b) Click **Modify** for the ECS-NFS-L7-UDP-Portmap Virtual Service.
  - c) Expand **Advanced Properties**.

▼ **Advanced Properties**

Not Available Server:  Port:

Port Following Follow:

Service Specific Access Control:

- d) Select the ECS-NFS-L7-TCP Virtual Service in the **Port Following** drop-down list.
3. Configure port following for the ECS-NFS-L7-UDP-MountD Virtual Service:
  - a) In the main menu of the **ECS Connection Manager** WUI, go to **Virtual Services > View/Modify Services**.
  - b) Click **Modify** for the ECS-NFS-L7-UDP- MountD Virtual Service.
  - c) Expand **Advanced Properties**.

- d) Select the ECS-NFS-L7-TCP Virtual Service in the **Port Following** drop-down list.
- 4. Configure port following for the ECS-NFS-L7-UDP-LockD Virtual Service:
  - a) In the main menu of the **ECS Connection Manager** WUI, go to **Virtual Services > View/Modify Services**.
  - b) Click **Modify** for the ECS-NFS-L7-UDP- LockD Virtual Service.
  - c) Expand **Advanced Properties**.

- d) Select the ECS-NFS-L7-TCP Virtual Service in the **Port Following** drop-down list.

**5.5.5.1 NFS TCP Virtual Service Recommended API Settings (optional)**

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	111
prot	tcp
VStype	gen
SubnetOriginating	1
ExtraPorts	2049, 10000
Persist	src
PersistTimeout	86400
Schedule	lc
AddVia	1

CheckType	tcp
CheckPort	111

#### 5.5.5.2 NFS UDP PortMap Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	111
prot	udp
SubnetOriginating	1
ForceL7	1
Persist	src
PersistTimeout	86400
Schedule	lc
CheckType	icmp

#### 5.5.5.3 NFS UDP MountD Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	2049
prot	udp
SubnetOriginating	1
ForceL7	1
Persist	src
PersistTimeout	86400
Schedule	lc
CheckType	icmp

#### 5.5.5.4 NFS UDP LockD Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. You can use these settings with scripts and automation tools.

API Parameter	API Value
port	10000
prot	udp
SubnetOriginating	1
ForceL7	1
Persist	src
PersistTimeout	86400
Schedule	lc
CheckType	icmp

#### 5.5.6 ECS Web Interface Virtual Services

The following section outlines the configuration options for using ECS Web Interface with Dell EMC ECS.

Please Specify the Parameters for the Virtual Service.

Virtual Address

Port

Service Name (Optional)

Use Template

Protocol

1. In the main menu of the **ECS Connection Manager** WUI, go to **Virtual Services > Add New**.
2. Type a valid **Virtual Address**.
3. Select the appropriate template in the **Use Template** drop-down list.
4. Click **Add this Virtual Service**.
5. Required only for TLS/SSL offload and re-encrypt: Expand the **SSL Properties** section.

6. Required only for TLS/SSL offload and re-encrypt: Select the certificate to use in the **Available Certificates** and click the arrow (>) to move it to **Assigned Certificates**.
7. Expand the **Real Servers** section.
8. Click **Add New**.
9. Type the **Real Server Address**.
10. Confirm that the correct port is entered.
11. Click **Add This Real Server**.

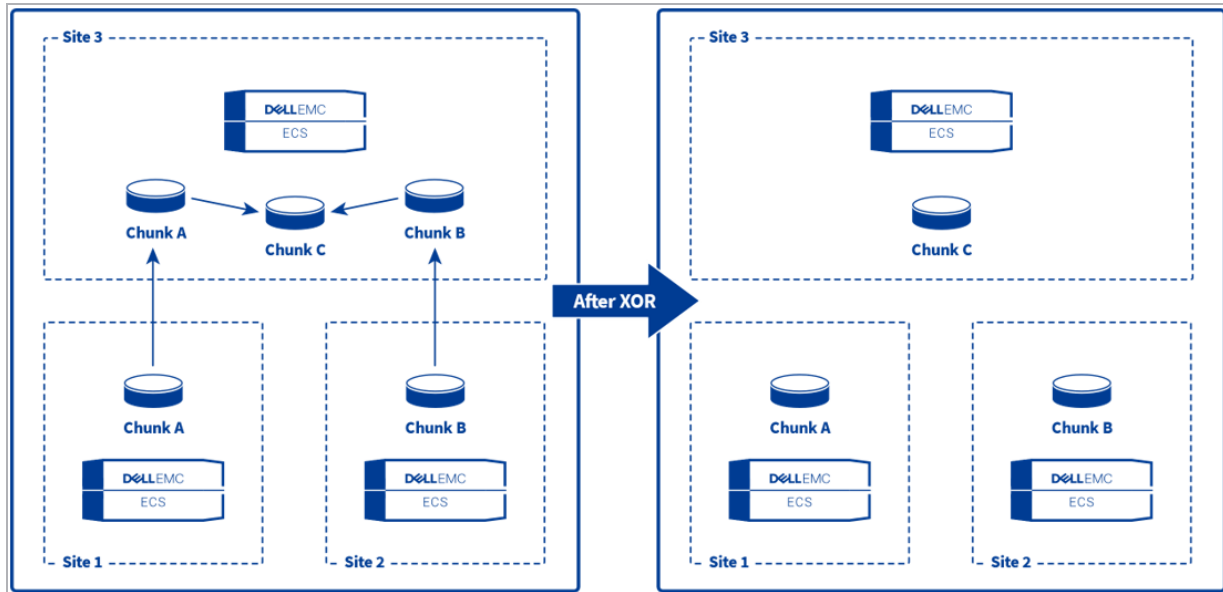
#### 5.5.6.1 ECS Web Interface Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. These settings can be used with scripts and automation tools. SSL/TLS certificates should be added before creating this VS. For further information on certificates, refer to the [SSL Accelerated Services Feature Description](#).

API Parameter	API Value
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	lc
SSLAcceleration	1
SSLReencrypt	1
TLStype	1
CipherSet	BestPractices
CheckType	https

#### 5.5.7 ECS XOR Virtual Services Layer 7

Dell EMC ECS XOR storage efficiency leverages the optimized scheduling component of the ECS Connection Manager. This method uses a URL Hash algorithm to distribute writes evenly across multiple sites and sends all reads to the site owning the object. This reduces ECS system overhead and WAN bandwidth providing greater performance and optimization of S3 traffic.



### 5.5.7.1 ECS XOR Virtual Service Layer 7

The following section outlines the configuration options for using XOR with Dell EMC ECS. XOR deployments requires a single Virtual Service and a SubVS for each Virtual Data Center (VDC). The top-level Virtual Service and three SubVSs are set up by the application template. Additional SubVSs can be added if the environment has more than three VDCs.

1. Deploy the XOR Virtual Services using the application template.
2. Add additional SubVSs, if applicable.
3. Add the ECS nodes for each of the VDCs (sites).

### 5.5.7.2 ECS XOR Offloaded Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. These settings can be used with scripts and automation tools. SSL/TLS certificates should be added before creating this VS. For further information on certificates, refer to the [SSL Accelerated Services Feature Description](#).

API Parameter	API Value
	ECS-L7-S3-XOR-Offloaded
	(Top-Level Virtual Service)
port	443

API Parameter	API Value
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	uhash
SSLAcceleration	1
SSLReencrypt	0
TLStype	1
CipherSet	BestPractices
CheckType	https
VDC 1 Offloaded (SubVS)	
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp
CheckPort	9020
VDC 2 Offloaded (SubVS)	
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp

API Parameter	API Value
CheckPort	9020
VDC 3 Offloaded (SubVS)	
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp
CheckPort	9020

#### 5.5.7.3 ECS XOR Re-Encrypted Layer 7 Virtual Service Recommended API Settings (optional)

This table outlines the API parameters and values set using the Kemp application template. These settings can be used with scripts and automation tools. SSL/TLS certificates should be added before creating this VS. For further information on certificates, refer to the **SSL Accelerated Services Feature Description** on the [KEMP Documentation Page](#).

API Parameter	API Value
ECS-L7-S3-XOR-ReEncrypted (Top-Level Virtual Service)	
port	443
prot	tcp
VStype	http
SubnetOriginating	1
Schedule	uhash
SSLAcceleration	1
SSLReencrypt	1
TLStype	1



API Parameter	API Value
CipherSet	BestPractices
CheckType	https
VDC 1 ReEncrypted (SubVS)	
VStype	http
SubnetOriginating	1
Schedule	Lc
AddVia	1
CheckType	tcp
CheckPort	9021
VDC 2 ReEncrypted (SubVS)	
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1
CheckType	tcp
CheckPort	9021
VDC 3 ReEncrypted (SubVS)	
VStype	http
SubnetOriginating	1
Schedule	lc
AddVia	1

API Parameter	API Value
CheckType	tcp
CheckPort	9021

### 5.5.8 Troubleshooting

Refer to the section below for details on some common issues seen when load balancing the Dell EMC ECS workload.

#### 5.5.8.1 Connections Rejected

When using a non-default TCP port or offloading for ECS services, you must ensure the Real Server port is correct. This is a common mistake when configuring the Real Servers when the Virtual Service port is different from the Real Server port. See the table in the Dell EMC ECS section of this document for the required Real Server ports for Dell EMC ECS.

# 6 QoS/Rate Limiting

In ECS Connection Manager firmware version 7.2.52, the QoS/Rate Limiting feature was introduced. ECS Connection Manager implements QoS (Quality of Service) to rate limit traffic for Dell ECS therefore providing granular control of resource allocation. This feature will protect the ECS solution against rogue applications that generate excessive requests and provide fair and balanced allocation of services across multiple workloads.

QoS configurations can be applied in several different ways on ECS Connection Manager to deliver the necessary protection and provide optimal performance for the storage solution. The QoS options are provided below.

For more information on these options and configuration details visit Kemp's support site to review the [Rate Limiting Feature Description](#).

## 6.1 Global Limits

Global limits apply QoS to all requests sent to ECS Connection Manager.

- **Maximum Concurrent Connections:** Limit the maximum number of simultaneous connections allowed to ECS Connection Manager.
- **Global Connections Limit:** Limit the maximum number of connection attempts per second (CPS).
- **Global HTTP Requests Limit:** Limit the maximum number of HTTP requests attempts per second (RPS).
- **Global Bandwidth Limit:** Limit the maximum bandwidth for ECS Connection Manager.

## 6.2 Limiter Options

Limiter Options controls the behaviour of QoS on ECS Connection Manager.

- **Error Response:** By default, the ECS Connection Manager drops any connections when the limit is reached. A more graceful response (429 - Too Many Connections or 503 - Service Unavailable) can be sent back to the client or application requesting access.
- **Fail on RS/Sub-VS Rate Limiting:** If rate limiting is activated for a Real Server (RS) or SubVS, the ECS Connection Manager tries to select a different RS/SubVS to use for the connections.

Enabling this will force the request to fail with the selected Error Response selected.

- **Generate Limiter Statistics:** Generates a global summary syslog message every five seconds containing state of the limiting subsystem.
- **Client Message Repeat Delay:** Set the minimum time after a client is no longer limited before a new message is generated.

## 6.3 Client Limiting

Client Limiting allows rate limiting to be applied based on the source IP address or network of the client or application accessing the storage.

- **Maximum Client Concurrent Limit:** Limit the maximum number of simultaneous connections allowed by a single client or application. A default (global) setting must be set prior to applying limits based on specific IP addresses or networks.
- **Client Connections/sec Limit:** Limit the maximum number connections per second (CPS) allowed by a single client or application. A default (global) setting must be set prior to applying limits based on specific IP addresses or networks.
- **Client Requests/sec Limit:** Limit the maximum number requests per second (RPS) allowed by a single client or application. A default (global) setting must be set prior to applying limits based on specific IP addresses or networks.
- **Client Bandwidth Limit:** Limit the maximum bandwidth allowed by a single client or application. A default (global) setting must be set prior to applying limits based on specific IP addresses or networks.

## 6.4 URL Based Limiting

URL Based Limiting allows rate limiting to be applied based on the HTTP header of the request. ECS Connection Manager uses Regular Expression (RegEx) to identify these characteristics.

- **Request URL:** Limit the number of attempts based on the request URL (ECS Bucket Name).
- **Host:** Limit the number of attempts based on the domain name of the request (ECS Namespace).
- **User Agent:** Limit the number of attempts based on the User Agent of the request (Operating System, software vendor, or software version).

- **Method:** Limit the number of attempts based on the HTTP request method. (GET, PUT, DELETE).

## 6.5 Per-Virtual Service Limiting

In addition to being able to configure QoS on a global level, you can also configure limits on a Virtual Services and Sub Virtual Service level.

**Connections per second:** Limit the maximum number connections per second (CPS) allowed for a Virtual Service of Sub Virtual Service.

**HTTP Requests per second:** Limit the maximum number requests per second (RPS) allowed for a Virtual Service of Sub Virtual Service.

**Concurrent Connections:** Limit the maximum concurrent connections allowed for a Virtual Service of Sub Virtual Service.

**Bandwidth Limit (Kilobits/sec):** Limit the maximum bandwidth allowed for a Virtual Service of Sub Virtual Service.

# 7 References

Some resources on Dell EMC ECS are listed below:

[Dell EMC ECS Solutions](#)

Useful, related Kemp documents are listed below:

[SSL Accelerated Services, Feature Description](#)

[Transparency, Feature Description](#)

[RESTful API, Interface Description](#)

# Last Updated Date

This document was last updated on 01 February 2022.