



Progress[®]

Kemp ECS Connection Manager - Load Balancing Multi-Network Deployments

Technical Note

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

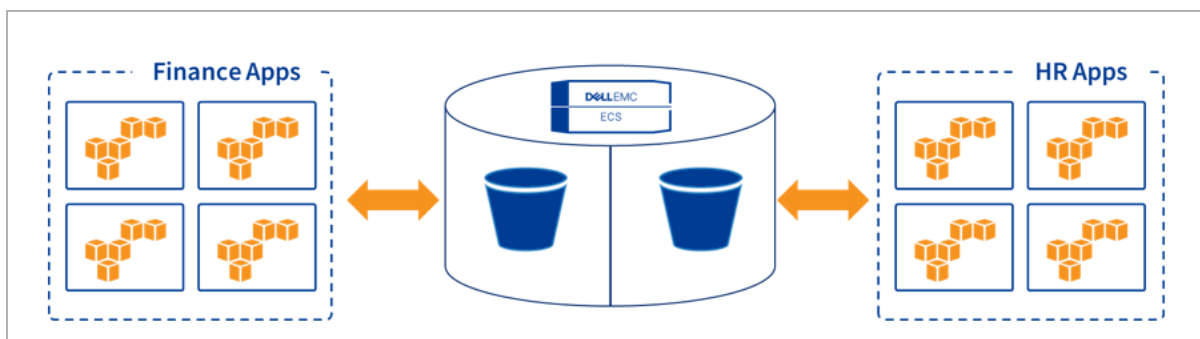
| | |
|--|----------|
| 1 Introduction | 4 |
| 2 Maintaining Network Isolation While Enabling Access | 5 |
| 3 Dynamic Name Resolution | 8 |
| Last Updated Date | 9 |

1 Introduction

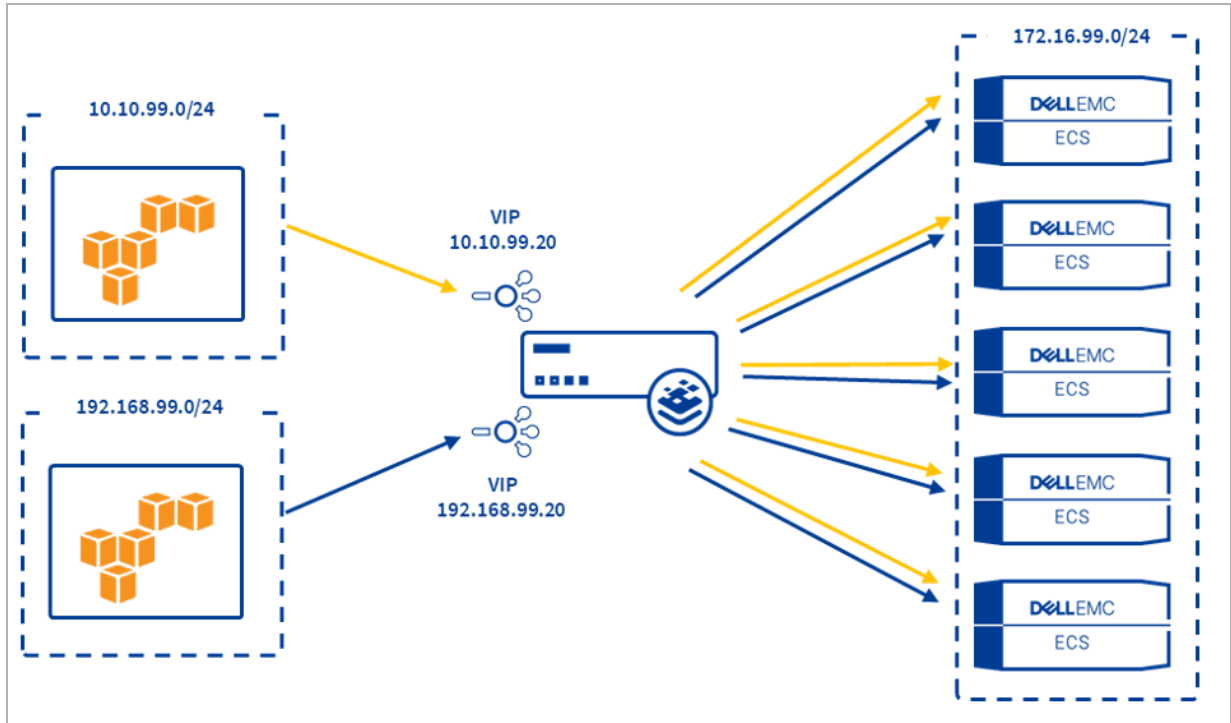
Dell EMC ECS is designed to deliver a secure storage solution by providing many different features including data isolation in some of the most protected environments. Data isolation and other advanced security features enable organizations to comply with their information security requirements. One area that can be challenging to address natively, however, is ensuring secure access to shared ECS object storage resources from multiple disparate network segments when it is not possible to address using firewall or routing rules. As ECS currently supports participation in a single network per service, the load balancer plays a key role in addressing this use case.

2 Maintaining Network Isolation While Enabling Access

Nearly every organization's network topology consists of multiple VLANs and subnets to support some level of network isolation. These boundaries are typically determined by tenant, business unit, location, or security compliance policies. Regardless of the reason for network isolation, the end goal is typically to keep assets and users in one network zone isolated from those in others. The challenge arises when common network resources such as storage must be accessed from across these boundaries.



An application load balancer (a common requirement for ECS deployments) can provide the required access to the storage while still maintaining the highest level of security. Using the ECS Connection Manager's multi-interfaces or multi-VLAN capabilities, applications on isolated network segments can access the ECS storage through a dedicated Virtual IP Address (VIP) that is local to each network without the need for creating additional routes or compromising security posture at the firewall level. Essentially, as long as the ECS Connection Manager has a network interface created in each client application subnet, a local published endpoint can be created that points to the same backend pool of ECS resources. As shown in the below diagram, two Virtual Service endpoints for ECS have been created, on different networks on a single ECS Connection Manager, both pointing to the same backend ECS pool.



As a basic Layer 4 firewall, the ECS Connection Manager is designed to deny all connections and only permit explicitly allowed traffic to defined resources. Since it serves as a proxy and termination endpoint in most deployment scenarios, network routing is also not required between the client applications and the backend ECS nodes, if not allowed based on security policies.

| Access Lists for tcp/10.10.99.20:443 (Id:1) | | |
|---|------------------------------|-----------------------------------|
| Blacklist (Blocked) addresses | Comment | Operation |
| 10.10.99.200/32 | Firewall NAT | Delete |
| Add Blocked Address(es) | | |
| IP Address <input type="text"/> | Comment <input type="text"/> | Block Address(es) |
| Whitelist (Allowed) addresses | Comment | Operation |
| 10.10.99.56/32 | Application1 | Delete |
| 10.10.99.78/32 | Application2 | Delete |
| 10.10.99.99/32 | Application3 | Delete |
| Add Allowed Address(es) | | |
| IP Address <input type="text"/> | Comment <input type="text"/> | Allow Address(es) |

Additional security measures such as blacklisting and whitelisting can also be leveraged on deployed ECS Connection Manager to further support a segmentation strategy.

| Virtual IP Address | Prot | Name | Layer | Certificate Installed | Status | Real Servers | Operation |
|--------------------|------|-----------------------------|-------|-----------------------|--------|--|---|
| 10.10.99.20:443 | tcp | ECS-L7-S3-HTTPS-ReEncrypted | L7 | s3.kemp.ax | ✔ Up | ✔ 172.16.99.101:9021 ✔ 172.16.99.102:9021 | Modify Delete |
| 192.168.99.20:443 | tcp | ECS-L7-S3-HTTPS-Offloaded | L7 | s3.kemp.ax | ✔ Up | ✔ 172.16.99.101:9020 ✔ 172.16.99.102:9020 | Modify Delete |

With the use of multiple VIPs, each subnet will terminate storage connections locally to access the shared storage environment residing on a remote network segment. Each VIP or Virtual Service can be independently configured to allow for different configuration options. Some highly secure networks may require encryption end to end while other less secure networks allow for TLS offloading.

3 Dynamic Name Resolution

In addition to providing secure connectivity to the shared storage across these isolated networks, ECS Connection Manager’s Global Balancing can provide seamless name resolution across a multi-network segment infrastructure and dynamically direct traffic to the proper virtual IP address. While some environments will have dedicated DNS infrastructure to support each of these networks, ECS Connection Manager can centralize resolution and direct clients from different network segments to different endpoint targets. By setting the locations, health checking and associated virtual IP addresses for each of the networks, ECS Connection Manager determines where to direct requests based on where the query originates from.

Configure s3.kemp.ax.

Selection Criteria

Fail Over

Public Requests

Private Requests

Site Failure Handling Failure Delay (minutes) [Set Failure Delay](#)

Enable Local Settings

Unanimous Cluster Health Checks

| IP Address | Cluster | Checker | Availability | Parameters | Operation |
|---------------|---|---|---|--------------------------------|--|
| 10.10.99.20 | <input type="text" value="Site 1 - Finance"/> | <input type="text" value="Cluster Checks"/> | ✔ Up | Show Locations | Disable Delete |
| 192.168.99.20 | <input type="text" value="Site 2 - Human Resources"/> | <input type="text" value="Cluster Checks"/> | ✔ Up | Show Locations | Disable Delete |

By leveraging the native capabilities of the ECS Connection Manager to proxy ECS, Dell EMC object storage deployments can be configured to successfully support environments with requirements for network isolation between applications while simplifying access to business-critical resources.

Last Updated Date

This document was last updated on 01 February 2022.