Clarity Solutions Hardware Recommendations

CLARITY

Clarity eCommerce & Connect Framework Server Recommendations

Summary

The Clarity Connect Framework (Connect) and Clarity eCommerce Framework (CEF) work in conjunction with each other to provide a seamless experience for end users that's enriched with securely integrated data from selected line-of-business applications (CRM, ERP, etc.).

The Connect and CEF applications were architected to handle the myriad of physical infrastructure needs each of our Clients have. As a result, these two platforms can be physically located in different environments and respectively hardened to allow them to meet the Client team's security and performance requirements.

This document will provide very high-level recommendations for the Connect and CEF application's hosting hardware requirements. Many of the recommended configurations and detailed technical specifications are dependent on the frequency and amount of expected traffic to each of the applications. Additional information is also available during the project discovery process, during which a customized network diagram and security analysis can be generated.

Clarity eCommerce & Connect Framework Server Recommendations

Clarity Connect Framework (Connect)

Connect serves to integrate data between line-of-business applications and the CEF or web applications. Connect runs as a standalone application. CEF can thus be hosted externally or in a DMZ for example, while Connect can also be hosted externally, or internally within a LAN or behind a separate firewall, if desired.

Most Clients will configure Connect to run behind some level of increased physical security (if the LOB application is on premises). Many Clients will install Connect on a server that also runs other connector/integrations, etc. It's possible to implement Connect though on the same physical hardware instance(s) as CEF (although this isn't recommended for security and redundancy purposes).

With regards to hardware / networking resource allocation, typically the needs of the Connect are roughly 25% that of CEF. In general, a very minimal instance of Windows Server (following the recommendations here: CEF and Connect Server Requirements).

Clarity eCommerce & Connect Framework Server Recommendations

Clarity eCommerce Framework (CEF)

CEF can typically be heavily optimized within the software itself for improved performance and reduced hardware requirements. However, with the cost of hardware being relatively lower and lower vs. the cost of optimizing software, we typically recommend rather more emphasis on hardware to assist with performance as a lower cost/ higher payoff option.

This tends to position Clients well for future growth as well and the team will be able to implement many if not all of the most common caching and performance related software configurations through a standard checklist used to that end.

Overview of Hardware Recommendations

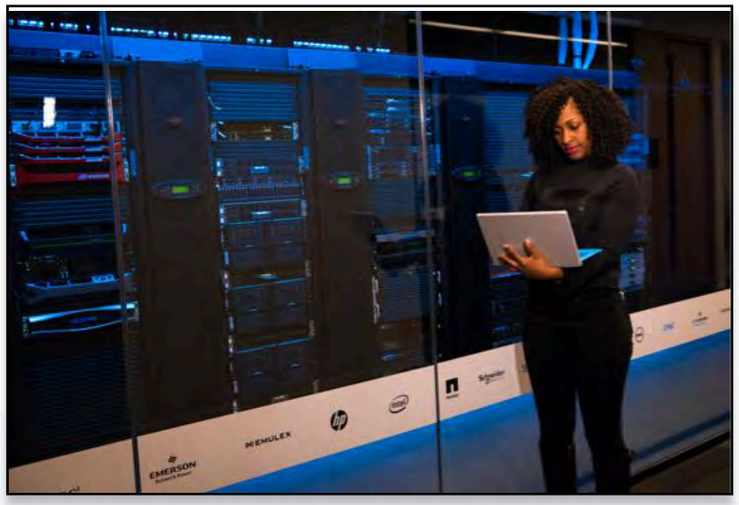
Please see below for hardware recommendations noting that these recommendations are very high level with the traffic estimate data below as well as general experience with CEF driving the recommendations. This is by no means intended as a final set of recommendations, but is intended to begin the discussions. In addition to the hardware items below there are CDN (content delivery network) providers, as well as security and monitoring providers that the team would like to review and recommend as well to further enable a very responsive and secure experience for site visitors and administrators.

Overview of Hardware Recommendations

Estimates of current traffic

- Current Analytics not provided yet, need the following:
  - Total Visits and Unique Visits in past 12 months
  - Peak months (if there are 2-3 then let's review those)
  - Peak traffic per day
  - Peak time of day and traffic during that period (total and unique)
  - Location of traffic (%'s by location for 12 month and monthly data)

- Current Hardware usage needed:
  - Current hard drive space used for media or other files
  - CDN service(s) needed
  - Security auditing services
  - Specifications for current networking configuration



Scenario 1

Medium Traffic Load CMS external

High-Level Recommendations for Production Server Hardware – Cloud & Virtualized

400,000
visits for past

280,000
unique visitors

Up to 2,000
per day

35,000
per month

Global traffic

High-Level Recommendations

Single Server with Failover option - [Cloud Hostin

Summary:

Web server with local file and SQL server.

Hard drive:

Raid 5, at least 50GB for OS partition. 20GB for application partition, 20GB for file partition, 20GB for database partition (all partitions can be combined if desired).

CPU:

4 virtual cores.

RAM:

4 GB

Minimum Recommended Environment:

Windows Server 2012 R2,IIS 8.5,.NET Framework 4.7

Connect Server(s) - [Internal Network]

Summary:

Connect server (with the option to scale as needed).

Hard drive:

Raid 5, at least 20GB for db and files* & 50GB + OS.

CPU:

Recommended 2 cores for VM.

RAM:

4 GB

Minimum Recommended Environment:

Windows Server 2012 R2,IIS 8.5,.NET Framework 4.7

Scenario 1. – Medium Traffic Load – CMS external

Estimated Configuration / Setup Time

Infrastructure team:

2-4 hours

Security team:

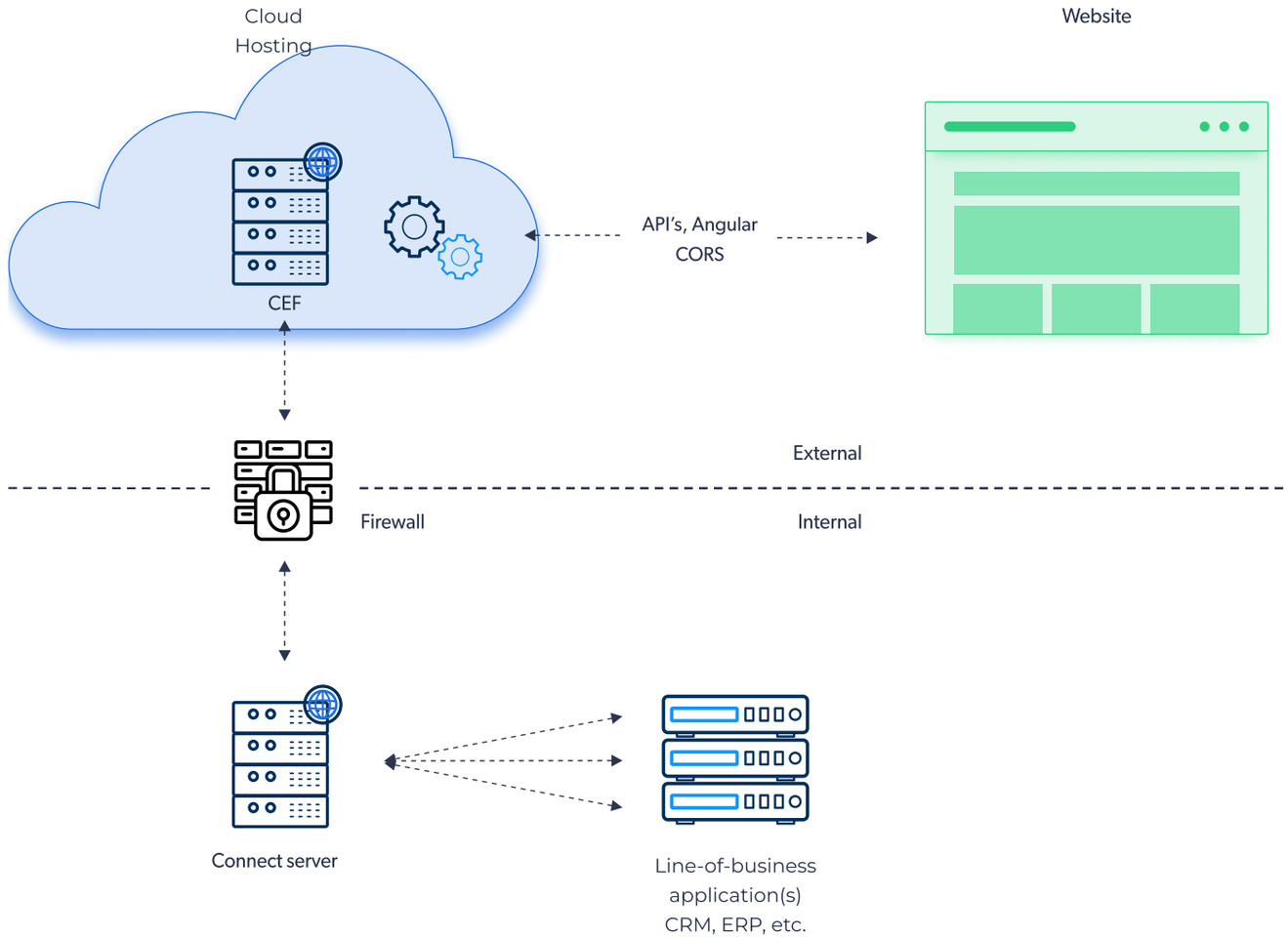
2-4 hours

CEF team:

2-4 hours

Minimum Recommended Environment:

Windows Server 2012 R2,SQL Server 2014,
.NET Framework 4.7



Scenario 2

Larger Traffic Load CMS included

High-Level Recommendations for Production Server Hardware – Minimums

1,661,706
visits for past

1,155,000
unique visitors

10,000
per day

150,000
per month

Vast majority of traffic is US based.

* just eCommerce

Scenario 2. – Larger Traffic Load – CMS included

High-Level Recommendations

Web Server(s)

Summary:

Load Balanced w/2 web-heads (or more).

Hard drive:

Raid 5, at least 60GB for OS partition. Application files & DB on separate servers.

CPU:

4 virtual cores.

RAM:

8GB each.

Minimum Recommended Environment:

Windows Server 2012 R2,IIS 8.5,.NET Framework 4.7

File Server(s)

Summary:

Synchronized failover preferred (2 machines, 1 active).

Hard drive:

Raid 5, at least 10GB recommended for application partition*, 50GB + OS.

CPU:

Recommended 4 cores for active VM, at least 2 cores for failover.

RAM:

6GB for active VM and 4GB for failover.

Minimum Recommended Environment:

Windows Server 2012 R2

Scenario 2. – Larger Traffic Load – CMS included

High-Level Recommendations

Database Server(s)

Summary:

Always on/failover preferred (2 machines, 1 active).

Hard drive:

Raid 5, partitions for db (20GB), logs (20GB), backup (50GB)* & 50GB + OS.

CPU:

Recommended 6 cores for active VM, 2 cores for failover.

RAM:

16GB for active VM & 8GB for failover.

Minimum Recommended Environment:

Windows Server 2012 R2,SQL Server 2014,.NET Framework

Connect Server(s)

Summary:

Connect server (with the option to scale as needed).

Hard drive:

Raid 5, at least 20GB for db and files* & 50GB + OS.

CPU:

Recommended 2 cores for VM.

RAM:

4GB.

Minimum Recommended Environment:

Windows Server 2012 R2,SQL Server 2014,.NET Framework

Scenario 2. – Larger Traffic Load – CMS included

Estimated Configuration / Setup Time

Infrastructure team:

12-18 hours

Security team:

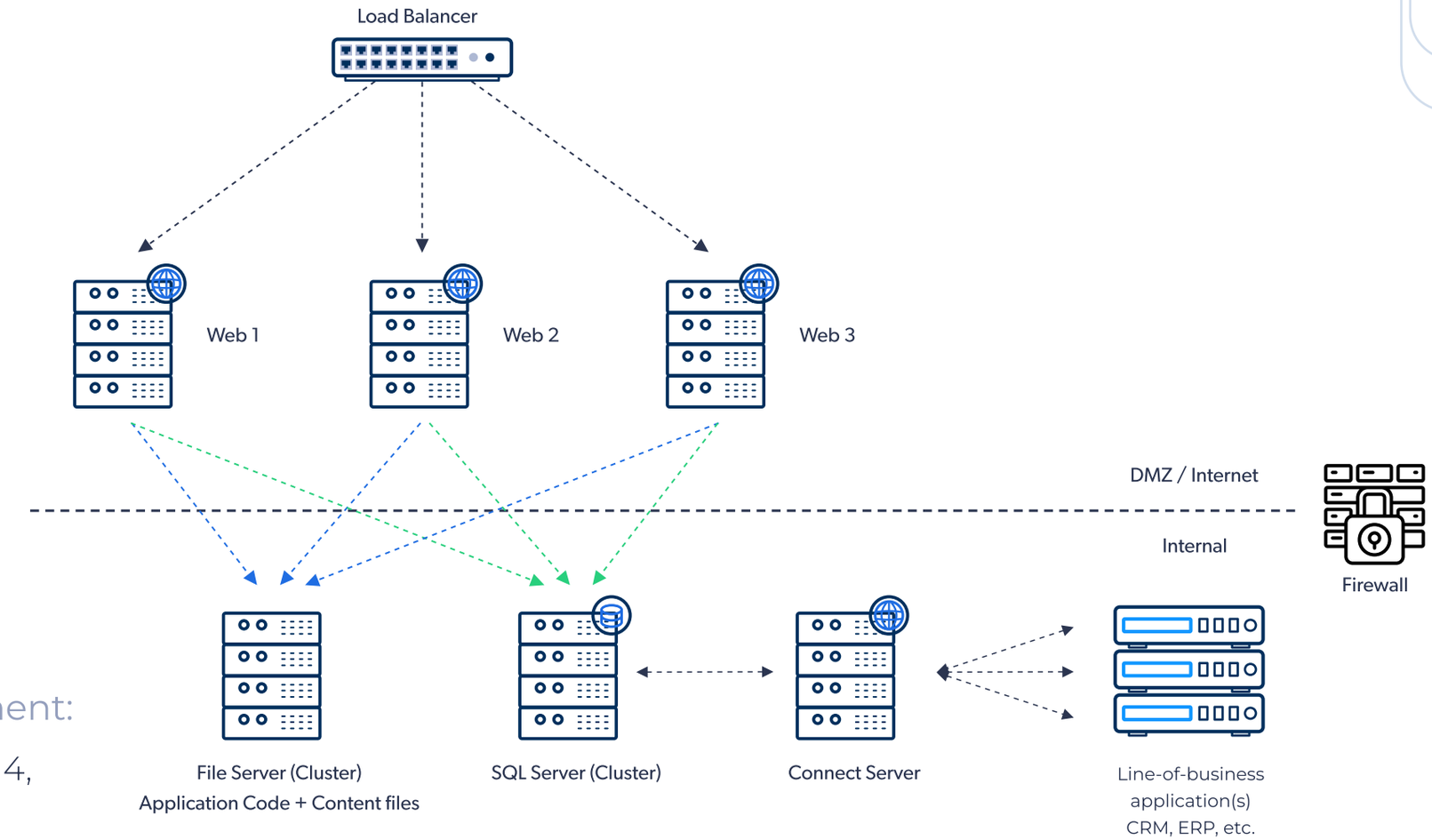
6-8 hours

CEF team:

5-8 hours

Minimum Recommended Environment:

Windows Server 2012 R2,SQL Server 2014, .NET Framework 4.7



CEF and Connect Server Requirements

In order to setup a CEF or Connect application you need to have the following requirements met:

CEF, Connect

Recommended Environment

Windows Server 2016+ // IIS 10+ // SQL Server 2017+ // .NET

Supported Web Servers

Microsoft IIS 7.0+

Supported .NET Framework

4.7+

Supported Database Servers

Microsoft SQL Server 2008/Express
Microsoft SQL Server 2008 R2/ Express
Microsoft SQL Server 2012/Express
Microsoft SQL Server 2014/Express
Microsoft SQL Server 2016/Express
Microsoft SQL Server 2017/Express
Microsoft SQL Server 2019/Express

Supported Operating Systems

Windows 10+ (Local development)
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016

Common Questions and Answers

The section below provides answers to common Client questions regarding hosting and platform architecture.

Common Questions and Answers

Is the Website contained in a single standard ASP.NET 4.x Web application? If so, does it support MS Web Deploy 4.5?

The website is contained within a single ASP.NET 4.x web application but it does contain several virtual directories depending on the modules installed for the instance. The application does support web deploy but we've very heavily tested and validated using Microsoft VSTS build and release tools if that's supported in the Client team's environment. We also provide an installer for the web application that will deploy the Client's specific web application with customizations.

*NOTE: Be sure to ask about DevOps or CI-CD configurations for production

What type of application(s) is the Connect Server composed of? I.e. Is it a Windows service? How is it deployed?

It's an IIS application, it's based on the hangfire.io platform. It's typically deployed via an installer application we will provide for the Client's project that includes the specific connectors and customizations for the project's specific

Common Questions and Answers

Is there any use of SQL Server beyond ANSI relational-database? Meaning, are there any agent jobs, use of full text search, CLR integration, or other feature that is a hosting/ environment consideration, especially when considering multi-tenancy cloud-based SQL options?

There aren't any necessary requirements as listed above for SQL beyond the ANSI relational- database. We've successfully deployed the platform in an Azure environment for example and can help provide the steps to configure and complete that type of deployment or we can directly complete that deployment or similar if that would be helpful.

What kind of credential store and respective encryption does the Clarity Connect service use for user/password secrets for connecting to integration APIs (and back to the Website)?

Depending on the Client scenario this can vary widely from a robust HIPAA compliant instance to a more standard implementation. As a minimum (in a standard implementation), the credential store would consist of a static API key, username and password encrypted within the Connect application. The data transmission between the Connect application and the website will require this authentication information and is sent over an SSL encrypted and typically IP restricted connection. There are more robust options for the communication between the Connect application and the website API endpoints such as a direct VPN connection or similar formats.

Common Questions and Answers

What kind of credential store and respective encryption does the Clarity Connect service use for user/password secrets for connecting to integration APIs (and back to the Website)? <CONT.>

Typically the communication between the Connect application and line-of-business applications will follow the standard methods for those application endpoints. Our team will typically provide minimum recommended hardening suggestions and will provide additional hardening to suit the specific integration needs for the Client team. Since the underlying application is a .Net IIS based application it can leverage the myriad options available to harden and secure both eCommerce API and internal line-of-business API integrations.

As a caveat, by the nature of the sensitivity of information being sent back and forth by the Clarity Connect application we typically recommend that the Connect application is physically located on a LAN (behind a physical firewall infrastructure). Sometimes this doesn't make the most sense to do and if not we can heavily harden the device that it will reside on and ensure restrictions are in place to appropriately remove security openings, or if all integrated applications are cloud-based.

Common Questions and Answers

Are there typically scenarios whereby the Client LOB applications would be pushing data/content to Clarity Connect (as opposed to only having Clarity Connect performing on-demand and scheduled pull requests)? In other words, is the integration uni-directional or bi-directional?

Typically, the integration(s) we setup are bidirectional in nature. In other words, they do typically push/pull from more than one system. With that said, it's also possible to configure the access to the APIs such that they can be called directly from LOB applications. We also have live connection model that can serve as a real-time integration for specific real-time oriented integration points and workflows.

What is used for search? Is this hosted external and managed by Clarity?

The search functionality is supported by the application natively. It leverages Lucene indexing and common best practices such as Levenshteinian fuzzy matching (basically intelligent approximate string matching), restrictive matching and results relevance, etc. It also offers indexing of documents, other portals and file repositories if needed and is extensible to incorporate

Common Questions and Answers

Aside from client requested custom scenarios, for customer and admin authentication and authorization, do you use ASP.NET Identity? Else, what role-based identity and membership provider do you use (or what options are at your disposal, and which is Clarity's recommendation)?

Yes, we have ASP.Net identity integrated into the core eCommerce platform for customer and admin authentication and authorization. Although that is the default / recommended option for most scenarios, we also typically see ADFS (also SAML 2.0) used for single sign-on scenarios and support that as well as the following options (noting some additional configuration may be necessary for more advanced options - this is a bit of a laundry list too but these options are all available with some additional configuration but the ASP.Net or ADFS would be typical scenarios):

- Custom Credentials - By inheriting CredentialsAuthProvider and providing your own Username/Password TryAuthenticate implementation
- Credentials - For authenticating with username/password credentials by posting to the/auth/credentials service
- Digest Auth - Allowing users to authenticate with HTTP Digest Authentication
- AspNetWindowsAuthProvider - Allowing users to authenticate with Windows Authentication
- Twitter OAuth - Allow users to Register and Authenticate with Twitter
- Facebook OAuth - Allow users to Register and Authenticate with Facebook
- API Keys - Allowing users to authenticate with API Keys
- JWT Tokens - Allowing users to auth with JWT Tokens

Common Questions and Answers

- GitHub OAuth - Allow users to Register and Authenticate with GitHub
- Google OAuth2 - Allow users to Register and Authenticate with Google OAuth2
- Instagram OAuth2 - Allow users to Register and Authenticate with Instagram OAuth2
- Yammer OAuth - Allow users to Register and Authenticate with Yammer
- Yandex OAuth - Allow users to Register and Authenticate with Yandex
- Odnoklassni OAuth - Allow users to Register and Authenticate with Odnoklassni
- VK OAuth - Allow users to Register and Authenticate with VK
- Microsoft Live OAuth2 - Allow users to Register and Authenticate with Microsoft Live OAuth2
- Google OpenId - Allow users to Register and Authenticate with Google
- Yahoo OpenId - Allow users to Register and Authenticate with Yahoo
- MyOpenId - Allow users to Register and Authenticate with MyOpenId
- OpenId - Allow users to Register and Authenticate with any custom OpenId provider
- LinkedIn OAuth2 - Allow users to Register and Authenticate with LinkedIn OAuth2
- Basic Auth - Allowing users to authenticate with HTTP Basic Auth