XC FRONTIER

POWERED BY XCONTENT

UNDERSTANDING XC|FRONTIER

Understanding XCFrontier

In contrast to how most of the world understands current computing methods, our XCFrontier technology powered by XContent, is based on the concept of "Centralised Computing". This provides an input medium for the end-user and allows the processing to take place in a datacentre.

Decentralized computing is efficient in LAN based environments, where the server is relatively close to the end-user computer but this becomes more of a problem when one starts engaging with cloud-based computing. This is pronounced when you look at PaaS (Platform as a Service), where that specific server is often located many kilometres from the end-user device.

XCFrontier by default requires a scalable and powerful server in the datacentre that will take over the processing side of the smaller end-user computing device. This server will handle all the clients processing requirements and will allow the end-user, no matter where they are situated, the ability to provide input and receive information back.

This method of computing provides many benefits. One of these is lower bandwidth utilisation due to the fact that only a small amount of input and output data is passed through to the server and back to the users.

The data displayed is nothing more than an image pixilation change which is more secure since you communicate constantly in a compressed and encrypted 168-bit 3DES DataStream. This does not happen in most decentralized computing processes. Since this DataStream is already compressed and encrypted, we do not require a VPN tunnel, which in a decentralized computing environment, is critical.

Additional benefits include:

- simpler administration of the end-user environment, where we utilise our own in-memory desktop sharing solution (similar to applications like TeamViewer)

- centralised storage of documents and other data

- with cloud services such as Azure, we can provide Scale Sets with High Availability and dynamic extreme processing solutions at no extra cost

- decreased PaaS and localised data-centre server costs

Below is a breakdown of our requirements for the technology:

XCFrontier Base Server requirements need the following server specification:

Operating System and backend (Base System, no Users)

- Windows Server 2016 / 2019
- 4 Cores
- 8 GB Ram
- 256 GB SSD OS drive (no storage)
- 1 TB for Storage (if required)- OneDrive sync, etc.
- Gigabit Network Card

Requirements per standard end-user (may be revised depending on workload and requirements, for example Call Centre agents require less than half of these requirements)

© 2020 XContent (Pty) Ltd. South-Africa, All Rights Reserved

For 1 Office (Word, Excel, Outlook, Teams) bound per User:

- Ram: 1.5 GB
- Cpu:1/2 CPU

Our recommended best practice for CONCURRENT CONNECTIONS is as follows (these may differ depending on the number of users and applications required)

Therefore for:

4 concurrent connections:

- Ram: 4GB x 4 users + 4 GB for Base System = 8GB
- CPU: 2 Cores + 4 Cores = 6 Cores

Or

100 concurrent connections:

- Ram: 150GB x 100 User + 4 GB for Base System = 154GB Ram
- CPU: 50 CPU Core's for Users + 4 Cores = 54 CPU Cores

Or

1000 concurrent connections:

- Ram 1500GB x 1000 Users = 4GB = 1504GB Ram (Or 1.5 TB)
- CPU: 500 Core's for Users + 4 Cores = 504 CPU Cores

System Security Protocols:

- True 168 Bit key Encryption using the 3DES cipher between Client and Server
- Forced High Security Connection – CredSSP (SSL with NLA) (Secure Socket Layer with Network Level Authentication)
- Full TLS (Transport Layer Security) – This is used by the server and client for authentication prior to a remote connection being established
- Federal Information Processing Standard (FIPS) Encryption - This security level is FIPS-Compliant, meaning that all communication between the server and the client is encrypted and decrypted with the FIPS encryption algorithms
- XCFrontier Client and server use port 8443
- In Azure, we now have an option to increase security to enable a Dynamic VPN tunnel, encapsulating the XCFrontier Data Stream from the EUC client to the XCFrontier server with virtually no performance degradation. This architecture allows us to close ALL public facing Ports completely, removing the server infrastructure from the outside world, yet for our clients, the system would be available from anywhere in the world!

As has been described above, Security is critical to all our designs. We will not launch new functionality or versions of XCFrontier unless the feature conforms to the most stringent security standards.

For Azure Deployment:

- 2 Hour Build Time
- VPN must be created between the Azure datacentre and Client on-site datacentre

Client requirements for XCFrontier end-user-computing (EUC):

- Windows 10 (Dedicated Terminal mode and Windows Mode)
- 220MB Ram for XCFrontier Client
- 5 MB Disk space
- Linux (Dedicated Terminal mode) (50 MB Ram)
- XContent can provide hardware for both Windows 10 and Linux Thin Client devices.

Bandwidth Requirements:

For EUC clients, we require a stable internet link with a minimum speed of 1Mbps. This requirement is especially for voice; we have monitored a constant bandwidth requirement of 50 Kbps or 512 Kbps combined up and down.

© 2020 XContent (Pty) Ltd. South-Africa, All Rights Reserved