iQuila Enterprise Server Deployment Guide

IQ22097r3

This Document Applies to:

iQuila Enterprise

iQuila Enterprise Server Deployment Guide

iQuila Server easily be deployable in large-scale environments.

iQuila Enterprise is a full Layer 2 platform that has full support for 801.2q VLANs.

iQuila Enterprise Server System Requirements.

Software Requirements:

Operating System	Version
Microsoft Windows	Windows 10 Server 2016 Server 2019
CentOS	8 (preferred)
Ubuntu	20 LTS
Hyper-V	Server 2016 or above
VMWare	5.7 or above

**Note: For Ubuntu, only long-term support (LTS) releases are supported.*

Hardware requirements:

iQuila Enterprise Server hardware requirements are largely specific to your bandwidth utilization. For example, if you run an iQuila server to connect only a few remote offices with a given number of VLANs, then the requirements are much less when compared to running hundreds of remote iQuila Bridge's and Clients, that redirect all Internet traffic. Traffic passing through a VEN connection utilizes processing capacity for encrypting and decrypting on both the client and the server-side.

To correctly estimate the sizing of your iQuila Server, you must estimate how much sustained bandwidth you need to route through the iQuila server, and estimate the CPU size accordingly. Memory size and disk space are more predictable.

iQuila Enterprise Server supports dedicated and virtualized environments.

Processor:

iQuila Server automatically uses AES-NI for the default AES-256 encryption. A non-AES-NI CPU severely lowers the speed of the encryption/decryption process. As a very rough estimate, you should quadruple your estimates for CPU sizing, if AES-NI is not supported on your intended deployment platform.

These estimates are only a rough guide, as they do not account for variations in capabilities between different CPUs. Nor do they account for throttling from physical limitations such as overheating, or virtual limitations such as running on a shared platform.

Memory:

iQuila requires approximately 4GB of RAM for its core services, then 1.5MB of RAM per concurrent connection. Each Virtual Switch uses approximately 5MB of RAM.

Bandwidth:

Bandwidth requirements are completely dependent on how much total data you want to route through your iQuila VEN tunnels. If you have a server with a 1Gbps network connection, and you have 100 connections, that equates to 10Mbps per user if they all use the full potential bandwidth at the same time. Usually, however, not everyone requires that level of simultaneous bandwidth. For example, if only half of the users are connected and the other half is idling, then that would mean the bandwidth is approximately 20Mbps per user. Unfortunately, there is no way for us to estimate how your users will use the connection; this should be taken into consideration when estimating.

Hard Disk:

Hard disk requirements are minimal. The only data that it is necessary to store on disk are connection, program logs, user certificates and settings. The logs may accumulate over time and should be rotated or cleaned using the instructions on our logging page. 64GB of disk space should be more than adequate.

Recommended Network Adapters:

In-house testing carried out at iQuila has shown the following network adapters to possess very high-performance worthy of recommendation. Please note, however, that other network adapters generally pose no problems for use with a local bridge. We recommend considering a change to one of the following network adapters if, the network adapter you are currently using lacks sufficient performance and is unable to function as required during local bridging.

Manufacturer	Product Series	Link Type
Intel	Intel PRO or Gigabit Adapter series	100Base-TX,1000Base-T, 1000Base-SX, 1000Base-LX, 10GBase-SR, 10GBase-LR
Broadcom	Broadcom NetXtreme series	100Base-TX
Hewlett Packard	593717-B21	10GBase-TX
Hewlett Packard	458492-B21	100/1000Mbps
Hewlett Packard	H221	10Gbps

Running iQuila Enterprise in a Cluster.

iQuila Enterprise Server supports advanced clustering functions controlled with advanced AI.

What is Clustering?

Server clustering refers to a group of servers working together on one system to provide users with higher availability. These clusters are used to reduce downtime and outages by allowing another server to take over, in the event of an outage.

Here is how it works. A group of servers is connected to a single system. The moment one of these servers experiences a service outage, the workload is redistributed to another server before any downtime is experienced by the client. Overall, clustering servers offer clients a higher level of availability, reliability, and scalability than any one server could possibly offer.

In a clustered server environment, each server is responsible for the ownership and management of each of its own connections and has a copy of the iQuila system database being used to run the other servers in the cluster. The servers in the cluster are programmed to work together to increase the protection of data and maintain the consistency of the cluster configuration over time.

iQuila Enterprise Server features the clustering function, which gathers the iQuila Servers into one cluster, to enable the handling of a large amount of processing where a single computer would normally not be capable. This enables tens of thousands of concurrent connections, and if a member of the cluster were to fail, all the connections the member was handling are seamlessly taken up by another member in the cluster.

The iQuila Server Administrator can connect to the cluster controller and perform cluster member server administration simply without having to be aware of the individual member servers.

Cluster Controllers

What is a Cluster Controller?

The cluster controller is the iQuila Enterprise server forming the core of the entire cluster. The server representing the cluster, when it is created, is known as the cluster controller and an iQuila Client, Server, or Bridge attempting to connect to the cluster designates the cluster controller's IP address or hostname as the destination IP address or hostname.

Overview of Cluster Controller Load Sharing:

When the cluster controller receives a VEN connection from a VEN source client it performs user authentication in the same manner as a regular VEN connection. After successful user authentication, the cluster controller decides automatically which cluster member server is to perform the processing load sharing by redirecting the connection to that cluster member server. The iQuila Server which is the cluster controller can also be a load-sharing destination. The AI load-sharing algorithm compares the load of each iQuila Server and automatically determines the assignment destination of a newly connected VEN session. At this time, it uses integers referred to as points in the cluster member list. By pre-setting the [Function Standard Ratio in Cluster] settings entry for the cluster controller and cluster member servers, it is also possible to manually adjust the parameters for load sharing.

The load sharing discussed here is an overview, and more detailed control is performed depending on the type of Virtual Switch to which the actual VEN connection is made.

Functions not available in Cluster-Mode:

Using the iQuila Enterprise Servers in cluster mode makes certain functions unavailable as these functions are not designed for clustering technologies.

- IPsec/L2TP, L2TPv3, EtherIP, MS-SSTP, Open VPN
- Outbound Cascade Connections.
- NAT on Static Virtual Switches
- NAT Virtual Gateway on Dynamic Virtual Switches
- Layer 3 Switching with Dynamic Virtual Switches

*If you require a connection from some of the functions that are not available when clustering is enabled, a separate instance of the iQuila server can be run and the relevant Virtual Switches cascaded into the iQuila Cluster setup, these tasks can be automated using the iQuila API.

Load Balancing:

When making a normal VEN connection from the iQuila Client and a cascade connection from the iQuila Client / iQuila Server / iQuila Bridge to a cluster, designate the cluster controller's IP address and port number and the name of the destination Virtual Switch.

The cluster controller iQuila Server receiving the connection from the VEN source carries out authentication of that connection then selects the cluster member to which to assign that VEN session.

Fault Tolerance:

The iQuila Enterprise Server clustering not only offers load balancing but also supports fault tolerance.

When an iQuila cluster member server within the cluster terminates suddenly due to hardware, software, or device driver malfunction, or when a situation arises whereby it has to temporarily terminate its iQuila Server process to update the iQuila Server or operating system, the cluster member server loses connection with the cluster controller. In this case, the cluster controller automatically deems it as having disengaged from the cluster and automatically excludes it from the load balancing.

Static Virtual Switches:

When iQuila Server is set in Clustering mode and a new Virtual Switch is created there is an option to select two types of Virtual Switches, static Virtual Switch, and dynamic Virtual Switch. Once a Virtual Switch has been created it is not possible to change the type of the Virtual Switch.

When a static Virtual Switch is created the Switch’s, instance is created on every member in the cluster, this Virtual Switch will continue to run on all iQuila Servers for as long as the cluster is operating.

When a connection source (usually an end user iQuila Client), wishing to make a remote access connection is connected to the cluster controller, the cluster controller uses the aforementioned AI algorithms, to select one of the iQuila Servers and redirects the connection to the static Virtual Switch instance within that iQuila Server.

By configuring a local bridge connection between the physical Network Adapters connected to each of the iQuila Servers for each static Virtual Switch instance created in each iQuila Server in the cluster, and by connecting all of the local bridging destination physical LANs to the in-house LAN destination to which the remote access is desired (either a direct Layer 2 connection or a Layer 3 connection using

a router and NAT is acceptable), the iQuila Client user can remotely access this in-house LAN regardless of which iQuila Server the connection is assigned to.

The clustering enables the creation of the large-scale remote access iQuila service required to process a large volume of simultaneous connections.

Dynamic Virtual Switches:

When a dynamic Virtual Switch has been created within a cluster but does not have any sessions connected to it, that Virtual Switch's instance (entity) does not exist on any of the iQuila Member Servers in the cluster. When the first session designating that Virtual Switch makes a VEN connection, the controller selects the iQuila Member Server which should launch that Virtual Switch's instance for the first time, then creates the Virtual Switch instance for that iQuila Member Server and redirects the VEN session to that server. For the second and subsequent sessions to that Virtual Switch, they are automatically redirected to the iQuila Member Server running that Virtual Switch instance such that regardless of how many iQuila Servers there are, VEN sessions connected to the same Virtual Switch are always connected to the same iQuila Server. When no one is connected to a dynamic Virtual Switch, its instance automatically stops running and releases the CPU and memory reserved for it.

The dynamic Virtual Switch makes it possible to create a large-scale Virtual Switch hosting service capable of hosting a very large number of Virtual Switches.

Please note, it is not possible to bridge dynamic Virtual Switches to a network port, in the case where you need to bridge a dynamic Virtual Switch you would need to run a separate iQuila Server running as a bridge.

Clustering Networking:

iQuila Enterprise server can be configured using Linux system on Public IP address or can sit behind a NAT/Firewall running Linux or Windows. Each server should have a minimum of 3 network cards, one for internet VEN communications, one for clustering configuration, and a 3rd dedicated for any bridging requirements to the local LAN. Depending on load further network cards may be added to create local bridges. When creating a local bridge in a cluster, each member of the cluster requires a bridge connection to the local LAN.

Although the clustering connections are encrypted, for better performance all nodes should be located on the same LAN segment. If planning a geographically distributed cluster for better performance and security, the clustering network should be situated on the same Layer 2 network, this can be either an iQuila Layer 2 network or existing Layer 2 circuits.

iQuila API:

iQuila supports a full API. Utilizing the iQuila API enables the management of one or more clusters and multiple single instances of iQuila from a central portal. For full detail on iQuila API please consult the API documentation.