iQuila FAQ
on Enterprise Clustering

iQ22085r2

Clustering

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

What is Clustering?

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

How it works. A group of servers are connected to a single system. The moment one of these servers experiences a service outage, the workload is redistributed to other server(s) 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 Servers feature this clustering function. This gathers the iQuila Servers into one cluster, enabling the handling of a large amount of processing power, where a single computer would normally not be capable of. This enables tens of thousands of concurrent connections to be made, and if a member of the cluster was to fail, all connections this member was handling, are seamlessly taken up by another member in the cluster.

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

Cluster Controllers.

What is a Cluster Controller?
The cluster controller is the iQuila server forming the core of the entire cluster. The server representing the cluster when it's created, is known as the cluster controller. And a 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 and 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 the same time, it uses integers, referred to as points, in the cluster member list. By pre-setting the [Function Standard Ratio in Cluster] settings 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. A more detailed control is performed depending on the type of Virtual Switch to which the actual VEN connection is made.

Setting an iQuila Server as a Cluster Controller:

The iQuila Server operates as a standalone server in the default operating mode. Changing this operating mode to a cluster controller allows the iQuila Server to run in cluster controller mode. This and all other settings related to clustering can only be performed, by the iQuila Server Administrator.

To set the iQuila Server to cluster controller mode, click on the [Clustering Configuration] button in the iQuila Server Manager. Next select [Cluster controller] in the dialogue box which appears and click [OK]. In the command line utility, use the [ClusterSettingController] command.

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

Functions not available in Cluster-Mode

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

It is therefore recommended to make a backup before changing the server's operating mode as any configuration to these setting may be lost.

Creating & Administering Virtual Switches:

Virtual Switches are created for the cluster controller in the iQuila Server clustering environment. Where necessary, the cluster member servers create temporary, Virtual Switch instances, upon instructions from the cluster controller, but it is not a necessary to directly create Virtual Switches for the cluster member servers. Virtual Switch creation, setting and administration of all Virtual Switches, can only be carried out by the cluster controller in a clustering environment.

Cluster Member Servers.

What is a Cluster Member Server?

The term "cluster member server" refers to any iQuila Server which forms a part of the cluster configuration other than the cluster controller. By connecting an iQuila Server to the cluster controller, the cluster member server is placed under the control of the iQuila cluster controller, and shares processing within the cluster.

When adding a cluster member server to an existing server, the cluster controller's hostname or IP address, port number (one of the listener ports made available by the cluster controller) and administration password are required. Each member server should have a Public IP Address either configured on the iQuila server, or passed via NAT to the iQuila Member server.

Setting a VEN Server as a Cluster Member Server:

The iQuila Server operates as a standalone server in the default operating mode. Changing this operating mode to a cluster member server allows the iQuila Server to run in cluster member server mode.

To set the iQuila Server to cluster member server mode, click on the [Clustering Configuration] button in the iQuila Server Manager. Next, select [Cluster Member Server] in the dialogue box which appears and click [OK]. In the command line utility, use the [ClusterSettingMember] command.

The entries required at this time are as follows.

Entry	Description
Controller Host Name or IP Address	The Hostname for IP address of the iQuila Cluster Controller Server
Port Number of Controller	Designates the TCP/IP port of the destination cluster controller.
Administration Password	The administration password of the iQuila cluster controller. Participation as a member in the cluster is either allowed or denied depending on whether the hash value of the inserted administration password is matched by challenge-response authentication. It is also necessary to change the cluster connection settings' administration password of the cluster member servers when the cluster controller administration password is changed. This password is not the same as the iQuila Server administration password of the cluster member server.
Public IP Address	The public IP address of this cluster member filed with the cluster controller. The IP address designated here is used as the redirect address when this cluster member server is selected by the cluster controller as a VEN connection session load sharing destination from a new VEN source. When no address is entered, the network interface IP address used when the cluster connecting to the cluster controller is automatically used. If wishing to use a different public IP address to that of the network interface when cluster connecting to the cluster controller, that address should be designated.

Public Port List	The public port number of this cluster member filed with the cluster controller. Typically, the list of the listener port made public by the cluster member server is designated. More than one public port number must to be designated, and multiple port numbers can be designated by separating them with a comma.

Cluster Connecting to a Cluster Controller with a Cluster Member Mode iQuila Server:

iQuila Servers running in cluster member mode are constantly connected to the cluster controller by a special control TCP/IP connection known as a "cluster connection". The cluster member server attempts to maintain the control cluster connection between the designated cluster controller for as long as possible. In addition, if the cluster connection is disconnected or fails to connect, ongoing repeated attempts are made at an interval of a few seconds until the connection is successful.

When seeking to confirm whether the cluster member server is properly connected to the cluster controller, connect to the cluster member server with the iQuila Server Manager and click [Clustering Status] to display the following information. In the command utility, use the [ClusterConnectionStatusGet] command.

Entry	Description
Connection Status	Displays [Online] when the cluster connection is in normal status. If the cluster connection shows errors, the cause of the error is then displayed.
Connection Start Time	The time & date at which the cluster connection commenced.
Time of First Successful Connection	Time & date of first successful connection to cluster controller.
Time of Current Successful Connection	Time & date of the currently connected cluster connection.
Connection Attempts	Displays the number of attempts to connect to the cluster controller to date.
Successful Connections	Displays the number of connection attempts to date which were successful.
Failed Connections	Displays the number of connection attempts to date which failed.

Cluster controller connection status display window:

Obtaining list of iQuila Servers connected to Cluster Controller & Displaying Details

Connect to the cluster controller with the iQuila Server Manager and click the [Clustering Status] button to display a list of all cluster controllers and cluster member servers connected to that cluster controller. In the command line utility, use the [ClusterMemberList] command.

The entries listed here are as follows.

Entry	Description
Type	Either [Controller] or [Member].
Connection Time	Time & date that member started operating as a member of the cluster after cluster connection to the cluster controller.
Host	Host name of cluster controller or cluster member server.
Points	Value indicating the load status of the cluster member server. The higher this value, the lower the load and the higher the likelihood that the member will be designated has the load share destination for a new VEN session.
Sessions	Displays the number of VEN sessions being processed by the iQuila Server.
TCP Connections	Displays the number of TCP/IP connections being processed by the iQuila Server.
Dynamic Virtual Switches	Displays the number of instances of Virtual Switches operating on the iQuila Server.

By selecting the desired cluster member server shown in the iQuila Server Manager and clicking on [Cluster Member Server Information] enables detailed information on that cluster member server to be viewed. In the Command line utility, use the [ClusterMemberInfoGet] command.

While cluster connection communication between a cluster controller and cluster member servers is TCP/IP protocol-based, this differs from the iQuila Enterprise protocol in that it is implemented by a proprietary dedicated synchronous and asynchronous RPC (remote proxy call). The System Administrator does not require an in-depth knowledge of this protocol. SSL encryption is used on the protocol contents and a hashed password is used for authentication. However, it does not feature functions such as the sophisticated server certificate authentication of the iQuila Enterprise protocol VEN. It is recommended to perform the cluster connection between the cluster controller and cluster members using a physically secure LAN locally or using another Instance of iQuila to extend the LAN.

Load Balancing.

When making a normal VEN connection from the iQuila Client and a cascade connection from the iQuila Client / iQuila Server / 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. The following algorithms are used in this case.

When the Virtual Switch Designated as the VEN Destination is Static:

The cluster controller redirects the connection to the iQuila Server with the highest point value among all of those currently available.

When the Virtual Switch Designated as the VEN Destination is Dynamic:

The redirect iQuila Server is selected according to the following procedure.

When the VEN session connected to that Virtual Switch does not yet exist on one of the iQuila Servers in the cluster, the connection is redirected to the VEN Server with the highest point value.

When the VEN session connected to that Virtual Switch already exists on one of the iQuila Servers in the cluster, the connection is redirected to that iQuila Server.

Load Balancing using Performance Standard Ratio:

Weighting by Performance Standard Ratio

As previously mentioned, when the cluster controller selects the server with the lowest load from among the iQuila Servers in the cluster, it selects the iQuila Server with the highest point value.

The points used here are approximately determined by the following formula.

Points = (4096 - Number of Concurrent VEN Sessions * 100 / weight) • * 100000 • / 4096

The above formula enables a definition of the performance standard ratio of each iQuila Server by setting "weighting" parameters for each server. By setting the values of the [Function Standard Ratio in Cluster] settings entry in the iQuila Server's [Configure Clustering], it is possible to change the weight parameter freely. The default setting of the weight parameter is 100.

The [Function Standard Ratio in Cluster] value sets how the subject iQuila Server performs against a value of 100 for a normally performing iQuila Server. For example, where two servers have respective [Function Standard Ratio in Cluster] values of 100 and 200, this means that the latter server is capable of processing twice the amount of VEN sessions as the former server. The iQuila cluster controller determines how many VEN sessions the entire iQuila Server should be able to process based largely on the value set here and distributes load accordingly.

Settings to Prevent the Cluster Controller Itself from Processing VEN Communication:

The cluster controller may select itself as the iQuila Server to process a VEN connection from a VEN source. When the cluster controller decides the iQuila Server to which to allocate a new VEN session, the decision is based on the cluster's iQuila Server point values determined by the algorithms, so both the cluster controller and the cluster members are judged according to an equal standard.

However, when a large volume of VEN connection sessions representing a significantly large load for the entire server has to be processed, it is possible to reduce the load on the cluster controller itself by having it only assume the role of processing the redirection of VEN sessions to each of the cluster members. To enable this setting, open the [Configure Clustering] settings entry and enable the [Controller functions only (It does not process VEN communication itself)] checkbox. This prevents the cluster controller from selecting itself when deciding which iQuila Server to assign a new VEN session to.

Fault Tolerance:

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

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 in order to update its 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.

In addition, all VEN sessions which were connected to the cluster member server which has ceased to function are automatically taken over by other cluster member servers. This processing is carried out automatically without the need for any special handling by the VEN Client. Therefore, even when a part of the multiple iQuila Server computers used by an ISP or a large company terminate due to a malfunction or have to shut down for maintenance, this mechanism enables the entire network to continue operating without stopping as long as other computers remain in the cluster.

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 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 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 a 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.

Connecting directly to an iQuila Member Servers (Static Virtual Switch):

As mentioned above, a VEN connection to a static mode Virtual Switch is automatically load shared, so it is not possible to know which iQuila Member Server the connection is to until it has been established.

Virtual Switch Administrators may, however, need to connect to the static Virtual Switch instance of an arbitrary iQuila Server in a cluster for administration purposes and testing. In this event, when creating the connection settings in the iQuila Client or Cascade Connection, designate the address of the iQuila Member Server and the name of the Virtual Switch to which direct connection is required instead of designating the cluster controller as the connection destination iQuila Server. In addition, designate the password required to connect as an Administrator user. This exception makes it possible for a VEN connection to be made directly to the desired iQuila Server's static Virtual Switch without going via the cluster controller router.

Administering the iQuila Servers Entire Cluster.

Once a cluster is created, the entire iQuila Server Administrator and Virtual Switch Administrators need only make an administration connection to the controller to be able to collectively administer the status and VEN sessions of all the Virtual Switches operating in the cluster. The administration of the iQuila Server and Virtual switches is carried out using the iQuila Server Manager or command-line utility in the same manner as when not using the clustering function.

By connecting to the cluster controller, iQuila Server Administrators can administer all the Virtual Switches in the cluster. Each Virtual Switch Administrator can administer the Virtual Switch for which they have authority.

The only situations in which it is necessary for iQuila Server Administrators to make a direct administration connection to cluster member servers other than the cluster controller are the following.

❖ When confirming which Virtual Switch instances (entities) are operating within the cluster member servers.

❖ When editing the cluster member server's [Encryption and Communication Setting] entries, obtaining the contents of the Configuration file or acquiring the server's status.

❖ Virtual Switch Administrators can only perform administration connections to the cluster controller, and not to the cluster member servers.

Local Bridge & Virtual Layer 3 Switch Settings:

Local bridge and virtual layer three switch settings are conducted for each iQuila Server. However, entire iQuila Server Administrator authority is required for these settings.

Changing Virtual Switch Types:

After creating the Virtual Switch, the type (dynamic Virtual Switch or static Virtual Switch) cannot be changed. As such, be sure to select a suitable type when creating the Virtual Switch.

Functions not Available Simultaneously with Clustering:

When the clustering function is enabled, the following functions are disabled.

❖ Outgoing Cascade Connections

❖ Virtual NAT with Static Virtual Switches

❖ Virtual NAT Gateway on Dynamic Virtual Switches

❖ Layer 3 Switching with Dynamic Virtual Switches

(Virtual DHCP Server function work)

The local bridging and virtual layer three switch functions can be used normally. However, local bridging and virtual layer 3 switching of Virtual Switch instances (entities) designated as local bridge definitions or virtual layer 3 switch virtual interface definitions can only operate between that iQuila Server on which they exist. In the case of static mode Virtual Switches, a defined static Virtual Switch instance normally exists, in principle, on all iQuila Servers. However, in the case of dynamic Switches, there can only be one iQuila Server in the cluster on which an instance can exist at the same time so the local bridging and virtual layer 3 switching functions are typically not available for dynamic Virtual Switches.

Contents