Clavister Feature Spotlight

Clavister Server Load Balancing

Increase performance and manage dynamic business needs using server load balancing

Top Features

- Reduced workload on servers and applications
- Faster responses to users' requests
- Elastic scalability of server farm capacity
- Load balancing customizable through several customizable algorithms
- Increased revenues through prioritization of commercial systems
- Decreased costs of maintenance and operation
- Improved fault-tolerance - 24/7 service availability
- Agent-free technology – No need for additional host-based applications
- Simplified administration without any need for service interruptions during restarts

Introduction

Server Load Balancers are very commonly used in data centers and an essential component in making sure that applications are available at all times and that administration and maintenance becomes significantly less complicated.

The typical owner or user of load balancers are service providers or large enterprises. The reason why load balancers are common in these scenarios is not necessarily based on that smaller data centers or customers does not need it but simply because load balancers are expensive and often exceeds their budgets.

In order to maximize the value for the users of Clavister's products we have integrated Server Load Balancing (SLB) as an integrated feature into the Clavister security gateways. This value adding feature complements the robust security gateway and turns it into an intelligent, high-availability load-balancer.

Flexible Configuration for Dynamic Business Needs

To meet the needs of customers and networks of all kinds the SLB feature included in the Clavister Security Gateway is closely integrated with the core functionality and is activated/deactivated as a part of a policy set, thus making it highly flexible and configurable.

As with all load balancers the Clavister security gateway subsystem for server load Balancing has the following key features:

- Load distribution
- Server Monitoring

Server Health Monitoring

Performing various checks to determine the health of servers and applications is one of the most important aspect of the server load balancing feature. Clavister security gateway can perform certain network-level checks at different OSI layer, which makes server monitoring both flexible and powerful.

The health checks are done both to determine the availability of the server and entire chain of applications and its dependencies. Additionally the health checks can be used to measure the responsiveness and performance of the service (latency).

When a server/application fails to meet the defined policy, it is removed from the active server/application lists and traffic is not routed to it until the server or application is restored.
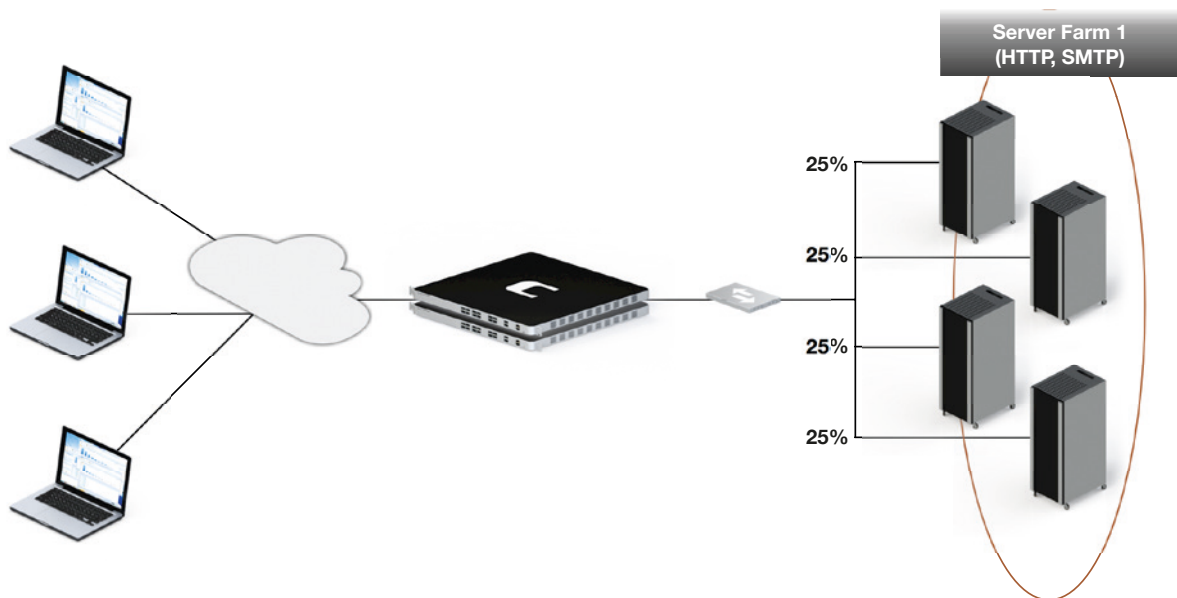
ICMP Ping

Clavister security gateway pings the real server IP address. A ping is used to check whether the server is available. This is also known as "heartbeat".

This is the most basic form of health checks and is used in order to determine if the server is running but does not really ensure that the applications running on top of the server and its OS are responsive.

TCP Connection

Clavister security gateway attempts to connect or bind to configured ports where applications are running. For example, if the server runs a Web application on port 80, Clavister security gateway attempts to establish a connection or attempts to bind to that port. The Clavister security gateway sends a TCP SYN request to port 80 on each physical server and checks for a TCP SYN/ACK in return. If the connection or bind fails, Clavister security gateway marks the port 80 to be down on that server.

This form of health checks is more advanced than ICMP Ping and can help determine the health of the application such as the web-server. It does not detect if the scripts on the web server is working or if any dependencies, such as SQL servers, are available.

HTTP Application Requests

The HTTP Application Requests feature is a very powerful form of health check and can determine if the actually application and its dependencies such as SQL Servers, business applications and similar are available and responsive.

There are two main parts of the HTTP Application Request feature, one is the custom Request URL and the other is the Expected Response.

The feature operates by allowing you to create a custom HTTP GET request which is sent to the servers in the server farm. On the web server you place a custom script file in which you can establish connections to your dependency servers such as SQL servers, run a few basic SQL requests and based on the result of the scripts you output either an error code or the data that you entered into the "Expected Response" part of the configuration of the health check.

In your policies for the health check you can build powerful rules that will define if the server is to be considered as healthy or not, this includes monitoring average latency, maximum number of failed monitoring events and more.

Questions and Answers

When does Server Load Balancing in Clavister Security Gateway make sense?

Clavister Security Gateway with Server Load Balancing is the answer to three key issues when it comes to server clustering; Availability, Scalability and Simplified Administration.

Availability

Q: How does Server Load Balancing provide increased availability?

A: Clavister Security Gateway provides increase availability by adding redundancy and eliminating single point of failures. It adds the possibility to guarantee availability to critical systems and services.

Q: What happens if the Clavister Security Gateway itself stops functioning for some reason?

A: Clavister Security Gateway is built for resilient solutions and provides the capability to have redundant gateways which automatically takes over the role as active gateway in the rare case of hardware failure.

Q: How many servers can you add to a cluster provisioned by the Clavister Security Gateway?

A: Clavister Security Gateway is built to function even in the extreme scenarios and there is no exact limit to how many servers you can place in a server farm, however there are of course practical limits, such as financial limits.

Q: What happens if a server or application in the cluster ceases to work?

A: If a server or application provisioned by Clavister Security Gateway ceases to work the Health Monitoring mechanism detects the problem and automatically stops routing traffic to the malfunctioning host and balances the load to the other servers.

Scalability

Q: In what way does Server Load Balancing provide scalability?

A: Clavister Security Gateway increase scalability by allowing the administrator to easily add more servers to a cluster and to expand with the growing need for performance and availability.

Q: What value does this scalability provide to our company?

A: By enabling your company to easily expand the server farm you can balance the need for performance against current financial means. This type of scalability also makes it possible to purchase less expensive main-stream servers instead of expensive cutting- edge technology servers in order to stay ahead.

Simplified Administration

Q: Administration is a time-consuming task for us since service availability must be guaranteed at all times, does the Clavister Security Gateway help us simplifying this task?

A: Yes, as there are no single points of failure you can easily disable one or more servers to perform maintenance whilst providing the critical service without any interruptions.

Clavister Server Load Balancing Key Benefits

- Reduced workload on servers and applications

- Faster responses to users' requests

- Elastic scalability of server farm capacity

- Load balancing customizable through several customizable algorithms

- Increased revenues through prioritization of commercial systems

- Decreased costs of maintenance and operation

- Improved fault-tolerance - 24/7 service availability

- Agent-free technology – No need for additional host-based applications

- Simplified administration without any need for service interruptions during restarts

For more information about Clavister products and services, please visit us at: www.clavister.com.

Where to Buy Clavister

For more information about where to buy Clavister products, visit www.clavister.com/partners. Additional resources and customer testimonials can be found at www.clavister.com/support/resources.

About Clavister
Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

CLAVISTER

WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
■ **Phone:** +46 (0)660 29 92 00 ■ **Fax:** +46 (0)660 122 50 ■ **Web:** www.clavister.com