

Clustered Hosting: A Better Hosting Technology

An XO™ White Paper

This document will demonstrate the benefits of XO™ Clustered Hosting and show how sites benefit from hardware redundancy, load-balanced traffic flow, resources-on-demand, elevated security and greater administrative ease for the same price as other services – all from a provider that, since 1997, has been leading the industry and has received a U.S. patent in clustering technology.

The software available for setting up a shared hosting server can enable a provider to establish a reasonably featured hosting service on a single server for several hundred (or even thousands) of accounts. Customers hosted on this server will be isolated to one server and share that server's resources, including disk, CPU, memory and Internet connection. Customers hosted on this server are vulnerable to many things that can impair service, including:

- High-traffic neighbors whose sites use a higher-than-expected share of the server's resources and squeeze out their neighbors
- Denial of Service attacks that congest a server's uplink, overload the shared local disk drives, or overwhelm the shared CPU
- Poorly written or malicious scripts that occupy processing power
- Any of the well-documented problems associated with shared hosting email management.

Exacerbating the problem of limited platform capabilities is the state of the shared hosting industry. Competition is at an all-time high, and most providers find it hard to differentiate their service from their competitors. To maintain profits with their service delivery platform, shared hosting service providers must *maximize* the number of customers on the platform and *minimize* the level of service and resources provided to them. These goals are exactly opposite of the needs of the hosting customer, who, as business increases, rightly wants the ability to drive more traffic to his or her Web site.

In some industries, high-volume customers are favored by business owners, but to a typical shared hosting provider, this type of customer is disruptive and needs to be isolated – or banished – to prevent the customer's high traffic

volume from causing churn among other customers.

Clustering allows traffic to be load-balanced over the computing base to ensure peak performance and availability even during peak traffic, and to spike to hundreds or thousands of times their normal volume because of special promotions or press coverage that drives huge volumes to their site. In fact, because of caching, the more usage a site gets, the more efficient XO Clustered Hosting becomes in serving that site.

Customers can grow from very small (one or two pages and negligible traffic) to large (thousands of pages, complex scripting and hundreds of gigabytes of traffic) without being forced to transition to another, higher-capacity platform.

Typical Hosting Provider Models

Standard hosting providers can choose among three types of service to sell. Customers that outgrow one solution must transition to another (more expensive service) or face diminishing service levels, capacity limitations or, in some cases, be thrown out by the service provider.

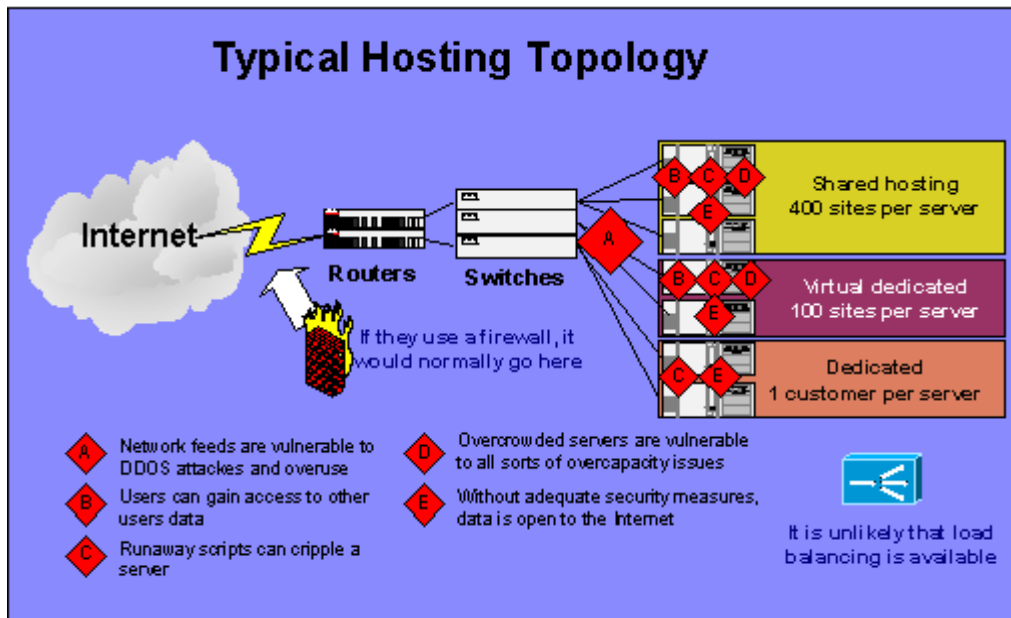
- **Shared hosting** is hosting for the masses. Hundreds (sometimes, thousands) of accounts are hosted on a single server, all competing for that server's resources. The sites on a server share the server's resources, including disk space, disk throughput, processor time, and bandwidth. To service providers, the accounts on this service should be small and lightly visited.
- A **Virtual Private Server (VPS)** is also a shared technology, but customers don't compete for resources as frantically. Customers are able to rent an allocation or slice of disk resources on that server, and those resources are reserved for them.
- The next step up is a **Dedicated Server**. Many customers take the step to a Dedicated Server thinking it to be the only protection against overloaded servers, bad performance and their server neighbor's poorly written scripts.

In a typical shared hosting environment, the customer's site will live on a single server among many "neighbors" – other Web sites – located on that server. This customer will have

no recourse against the malfeasance of his neighbors that bring harm to their shared server. Essentially, each server is a lifeboat to the customers that are homed to that server. The

more customers, the more vulnerable that server will be to overuse. As long as no one rocks the boat, there won't be a problem, but many things *can* rock the boat:

Problem	Cause	Impact	Potential Solution
Resource problems (Disk, RAM, CPU, or bandwidth)	Provider sold too many accounts on the server	<ul style="list-style-type: none"> Degraded level of service Server crashing Web site 	Move accounts to new server; add processors or RAM to server. Both require downtime and possible customer involvement with re-addressing or modification of scripts due to hard-coded file locations changing.
	Runaway or malicious script running on your server (<i>not necessarily your script</i>)	<ul style="list-style-type: none"> Server crashing Security risks 	Stop process or reboot server. Preventative measures can be limiting the CPU cycles that a script can use or limiting the types of scripts allowed
	Denial of Service attack to a site on your server (<i>not necessarily your site</i>)	<ul style="list-style-type: none"> Server unavailable for your traffic. 	Firewall or other protocol filters; higher bandwidth Internet pipes
Security Problems	Site hacked by a customer on the same server	<ul style="list-style-type: none"> Data security breach Loss of confidential information 	Using the typical open-source or commercial off-the-shelf solutions. No stock solution to protecting customers inside the operating system – this requires custom software solutions.
	Site hacked from outside	<ul style="list-style-type: none"> Data security breach Loss of confidential information 	Firewall or other protocol filters; tightly locked down server systems; aggressive patching procedures (which often result in customer downtime since no ability to fail over during maintenance exists)
Email problems	Increased storage of an aged user base	<ul style="list-style-type: none"> Server overloaded (see above) 	Move users to a new box; take the box down to add storage or delete email.
	Email spikes, loops, and bombs constrained to a single server, causing mail to be delayed or lost for other customers	<ul style="list-style-type: none"> Mail delays Mail loss 	Move customers to a new box.
	Non-redundant local storage causes data loss after routine drive failure.	<ul style="list-style-type: none"> Mail loss 	Cry. Repeat.



The typical hosting service model has many single points of failure.

XO™ Clustered Hosting

Clustering technology is designed to eliminate the problems inherent with typical shared hosting infrastructures. This technology provides customers with a “clustered” handling of security, load balancing, and necessary Web site resources.

The XO Clustered Hosting platform is data-driven, which means that no human interaction is needed to provision a new account to the platform. Immediately upon account purchase, the customer can begin using hosting resources such as DNS Manager, email services (Web Mail, POP3 and IMAP), FTP, FrontPage™, MySQL™ and Shell access.

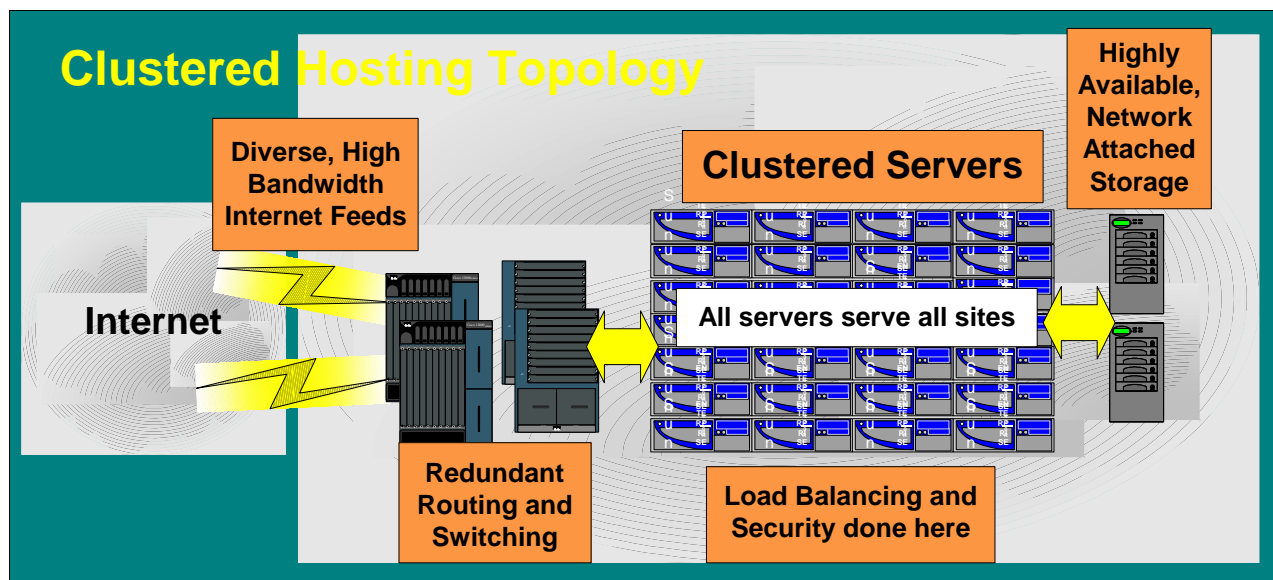
Since customers can add additional allocations for disk, traffic, and processor cycles, these allocations – received at sign-up – are a function

of the monthly charge and not a physical limitation of the platform.

XO™ Clustered Hosting “virtualizes” the resources beyond the limits of one physical box.

Customers are not limited to one server. They share the processing power of many servers and their applications are distributed in real-time. This means that they can purchase as much computing power as they want from a virtually inexhaustible source, since even the largest customer never consumes more than a fraction of a percent of the total server pool. Customer account changes (to add new resources or change settings) are propagated immediately to every server in the cluster.

This is different from typical shared hosting architectures that usually require changes to a configuration file that becomes live after the server is rebooted during off hours, or are pushed on a cyclic basis every few hours.



Clustered Hosting serves Web sites, email and DNS from a secure, reliable, redundant, load-balanced platform.

As this graphic shows, traffic is dynamically load-balanced across all of the web servers, so the impact of an increased load is diluted. Capacity management can be achieved by adding additional servers to the cluster, and this can be done in a matter of hours with no impact to existing customers. By being served from a cluster of servers instead of confined to one, your neighbor's usage does not impact your Web site response time or available resources.

XO™ Clustered Hosting preserves the benefits of Windows hosting services within the robust, clustered framework. Windows / IIS provides a highly robust and feature-rich hosting environment, but experiences the same limitations as other hosting options when implemented in a shared environment, including local vulnerabilities, scalability and capacity management limitations, and hardware points of failure around single servers and local storage. XO Clustered Hosting allows Windows servers to share in the benefits of enhanced security, network storage and real-time fail-over.

XO Clustered Hosting is operating-system agnostic. It was designed to deliver its load-balanced secure service to both Windows and UNIX applications, and both end-user solutions share the benefits of the years of development and engineering within XO Clustered Hosting. 'Shared' Windows solutions without this level of investment and architecture suffer from the same problems described above.

Clustering ensures that web servers are available to handle huge spikes in traffic. If a site handles traffic of more than 100GB a day or a month, each request will be served appropriately.

XO Clustered Hosting places controls and protections on the scripts that customers run as part of their Web sites. A poorly-written script can cripple a server. XO Clustered Hosting secures and assigns script processes to individual accounts by isolating script processes within the "Virtual Domain Environment" (VDE).

The VDE measures script processing time in Resource Units (RUs), which is a measure of CPU run time. RUs are generously allocated and can be added in real time by the account's administrator. The VDE protects accounts from their neighbors and helps administrators recognize the resources used by their script processes. While a poorly written script can cripple a normal shared server, the VDE isolates script's process to the individual account's resources and isolates scripts with loops and critical flaws to the account which owns them. This ensures that a bad developer doesn't harm anybody but his own account and solves the problem of the bad developer "neighbor."

The VDE's purpose is much like the process isolation mechanisms of a Virtual Dedicated Server (VDS); however, it has significant differences.

- A VDS runs on one server and partitions the one server's resources. An account on a VDS can only use the portion of a server's resources it has been allocated. In comparison, the VDE that has access to the computing power of the entire cluster. Customers can consume multiple processors' worth of CPU when needed and no idle resources when not in use. The VDE runs on all servers in the cluster and is dynamically scalable; unlike traditional virtual dedicated servers, there is no static configuration per site and no startup time to transition to the VDE for individual site events.
- VDS solutions are vulnerable to maximum load failures at large load times, and typically are not sufficient for a site which either consumes huge processing resources or may expect a spike due to a successful ad campaign or press release.

Disk space and bandwidth are also restricted so that users cannot use more than their allotment. However, if an account needs more of any of these resources, it is available to them in real time through the administrative interface. All accounts include notifications as resource use reaches limits. Additionally, real-time log and usage reporting ensures account administrators understand their resource utilization at any time.

Security is a fundamental part of XO Clustered Hosting, not an afterthought.

There are multiple tiers of security protections integrated into the XO Clustered Hosting platform. In a typical hosting environment, the security layer is usually not integrated in the platform. The stock solutions used for shared hosting do not solve core issues around integrating security between the application and the operating system. At best, most typical hosts will implement a firewall solution, and weaknesses inherent with the operating system will remain exploitable to those that penetrate the firewall. In popular vernacular: they have a hard, crunchy outside and a soft, chewy inside.

XO Clustered Hosting is designed from the ground up to provide Web services securely and efficiently. Its network layer protections employ intelligent routing, redundant switching fabric and built in firewall and proxy technology. XO protects against the traditional sorts of attacks aimed at IIS and/or Apache and thus avoids the constant scramble that traditional hosts have to do whenever a new vulnerability is announced:

the race to see if systems can be patched before exploit scripts are published.

Our internal designs also prevent the sorts of internal attacks that are endemic on shared platforms where customers have root access and can, for example, exploit file permissions that are incorrectly set by other account holders or use the frequent internal holes inside operating systems.

XO Clustered Hosting provides considerable advantages over traditional hosting architectures in mitigating Denial of-Service and other network attacks because such attacks can be dispersed over a large pool of servers, and if individual hardware components are impacted by such attacks, they automatically fall out of traffic handling during the attack.

As discussed above, the VDE grants sites the right to use the entirety of the hosting cluster's file serving resources for scripts while account limits protect the platform and the community of users from the impacts of a poorly designed script or site. Essentially, the VDE enforces the social impact of "neighbors'" poor design skills.

Lastly, XO provides the ability for the customer to secure themselves better. Traditionally, a hosting provider will provide a single login for file system access which must be shared by all the people with access needs. These shared passwords are disasters waiting to happen; they are usually weak and rarely changed properly when staffing changes.

XO Clustered Hosting allows for unlimited access levels to be created and managed by account administrators, which enables users to have finely-tuned access rights only to the set of files or resources they need. When a user is no longer allowed access, one configuration change will disable all their rights without impacting others. Thus people are not forced to have greater privileges than they need, which leads to weak security.

The New Hosting Marketplace

Web site administrators looking for reliable hosting for sites doing 1GB daily or more than 100GB of monthly traffic should investigate the benefits of XO Clustered Hosting.

Platform Scalability and Performance

- Accounts are not resident on any single server; they share the computing power of the cluster, so resources are virtually limitless.
- Clustering ensures that web servers are available to handle huge spikes in traffic and processing demands from successful sites.
- Poorly-written scripts won't cripple neighboring accounts. Scripts are isolated, monitored and restricted to the account's available CPU cycles.
- Storage, bandwidth and CPU are spread across the cluster, ensuring web site responsiveness and scalability.

Account control

- Real-time provisioning of accounts, resources and service changes
- Account administrators have single login online access to all of the functions that they need, like adding users and resources, uploading changes, modifying publishing rights and DNS, managing databases, etc.
- Reports are available online to see bandwidth and disc usage, site hits and other critical account management statistics.

Redundancy

- All functions have inherent failover because all servers serve all functions. Functions such as load balancing and firewall are all in redundant configuration.

- Services are not local to a server, so loss of a server is not fatal to the overall service.

Security

- Firewall protection and access control are natively integrated into the platform
- Accounts are isolated from one another. Your service and data are safe.
- Scripts operate in a virtual development environment. Rogue scripts do not have the opportunity to take down servers.

Price

- XO Clustered Hosting is a fraction the cost of dedicated or VPS solutions and equal to the cost of lesser shared hosting services.

About XO Communications

XO Communications is a leading provider of national and local telecommunications services to businesses, large enterprises and telecommunications companies. XO offers a complete portfolio of services, including local and long distance voice, dedicated Internet access, private networking, data transport, and Web hosting services as well as bundled voice and Internet solutions.

XO provides these services over an advanced, national facilities-based IP network and serves more than 70 metropolitan markets across the United States. For more information, visit www.xo.com.