As a growing number of organizations leverage the strength and flexibility of web-based applications for the core function of their business, high availability (HA) infrastructure is becoming a required component of their systems architecture.

**Typical, HA architectures include the following components:**

- Dedicated HA firewalls – Delivers peace of mind and application security
- HA load balancing – Provides traffic management
- Bare-metal backup – Allows for reliable data and systems protection and speedy recovery at time of disaster
- Advanced monitoring platform – Monitors your system performance and notifies you before an issue occurs
- Configurable systems and patching – Keeps your applications up to date while reducing management costs

Along with other technological components that might be required to architect your systems for availability, organizations also face the challenge of having the resources available to build and test the infrastructure.

Many organizations rely on managed hosting providers to deliver these highly available systems for Internet connectivity, physical security, and additional computing resources. These providers can help address technical issues, outages, and sudden increases in traffic.

This paper provides you with best practice considerations for working with a managed hosting provider to architect an application infrastructure for maximum availability.
UNDERSTAND THE RULES OF THE HOSTING GAME.
Many managed hosting providers use similar technologies as you would if building a system in your internal data center. However, they may implement them in a different way. Why? Standardizing on certain configurations makes supporting numerous customers, devices, and systems both efficient and economical.

RECOMMENDATION:
If you know you will be outsourcing your server infrastructure with a hosting company, talk to your provider and get their architecture input before you build. It will save time and money later.

For example, consider a hosting company that offers hard drives for servers. A typical hosting company may have two or three tiers of storage available such as SATA (less expensive) or fibre channel (more expensive) with only a few storage sizes available. Having fewer products in their catalog allows hosting companies to carry lower inventory and therefore, offer you better pricing. Keep in mind that the more custom your system requirements, the more variable the pricing. If your requirements are standard and in alignment with your hosting company’s structure, you may receive more competitive pricing.

When you engage with a managed hosting provider don’t be surprised if the architecture offered by their sales engineers is different than you anticipated. The engineers know how to architect within the hosting company’s best practices.
ARCHITECTING THE SECURITY LAYER

Whether you use IIS, Apache, or some other web server technology, it is important to think critically about security, performance, and compliance. For Internet-facing applications, security planning is essential. Many managed hosting providers offer a shared firewall tier configured to offer typical security performance. Due to the shared nature of the device, the firewall cannot be configured to your exact needs. However, a dedicated firewall appliance allows you to customize and lockdown all but the most needed ports. A dedicated firewall appliance will also allow you to monitor both inbound and outbound traffic for better platform management. Most service providers have various levels of firewall devices. You can choose which works best for your organization based on your performance and pricing requirements.

Any firewalls chosen should be set up in a highly available configuration so if one firewall fails, all traffic is redirected through the available device while the broken device is replaced. These highly available firewalls “talk” to each other over a separate Ethernet connection to determine if the other device is present and functioning, providing you an easy and relatively inexpensive option to add a layer of redundancy and availability for the security layer.

CONSIDERATIONS FOR THE WEB TIER

Many web servers hold the responsibility of providing content to the end client. Because the web server is the public front end to the application, it is vulnerable to hacking and other malicious action even when protected by high availability firewalls. Taking appropriate measures to ensure full-stack security is the responsibility of both your developers and your hosting provider’s systems engineers who will help architect the appropriate server configuration for your applications. The use of web application firewalls (WAF) provides another layer of protection for your public-facing systems, safeguarding against hacking, pattern recognition intrusion, and cross-site scripting. Web application firewalls are mandatory if your applications have compliance needs. And, they will greatly increase the speed of passing a security audit.
SECURITY-FOCUSSED ARCHITECTURE
Employing the high availability firewalls as a way to help secure an application, architects should require that all server traffic cross the firewall. By using the firewall to manage traffic, security architects can specify the particular ports and traffic type that can move between servers. This allows for granular traffic flow rules which provide tighter security for the running application.

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Port</th>
<th>Service</th>
<th>Zone/Tier</th>
<th>Action</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.10.25</td>
<td>10.1.10.26</td>
<td>53 UDP/TCP</td>
<td>DNS</td>
<td>Web Tier</td>
<td>Allow</td>
<td>Yes</td>
</tr>
<tr>
<td>10.1.10.25</td>
<td>10.1.10.26</td>
<td>445 UDP/TCP</td>
<td>MS CIFS</td>
<td>App Tier</td>
<td>Allow</td>
<td>No</td>
</tr>
</tbody>
</table>

Example firewall rule
Figure 1.1 shows an example of facilitating stronger systems protection by setting server-specific rules to lock down security at the port and server level. Flat architectures can still enable firewall controls, but more ports are open to all services. If possible, a tier architecture is recommended.

Typical tier configurations include web, application, and database — all with tier-specific firewall rules. This limits communication traffic to only the absolute essential for maximum security.
MANAGING LOAD-BALANCED TRAFFIC FLOW

Traditional web architectures can be scaled by using hardware-based load balancing to manage traffic flow to each of the configured web servers at the web tier. Many hosting service providers will offer dedicated, load-balancing configurations and models based on the traffic volume needed for the application. Hosting providers also offer affordable shared or multi-tenant load balancing configured in “one-armed” mode for smaller or simple traffic management.

If you have more specific load balancing needs, such as SSL offloading, then you should look at a pair of dedicated appliances configured as an high availability pair to offer redundancy against physical component failure. Similar to the HA firewall configurations, the HA load balancers monitor each other’s status. If one server has an issue, the other is triggered to take the full traffic load.

KEY CONSIDERATIONS:
- Understand session requirements
- Shared or dedicated hardware?
- Is SSL offloading required?
- Know traffic load requirements
- Do you need traffic management at the application tier?

PLANNING FOR THE WORKLOAD

Properly planning the appropriate size and systems configuration for the web services tier is one of the most challenging tasks on the high availability checklist. If your application is currently in use, then planning is easier since the application already has a specific architecture and historic traffic load. The environment can be reengineered at the managed hosting provider’s data center, the application can be tested, and a simple DNS change can have the new application up and running. New applications with no production history can create challenges during architecture. You can ease planning for this scenario by using cloud-based servers that adjust resources as needed by allowing users to configure RAM, CPU, and storage. A secondary benefit is that you only pay for the resources you use—not idle servers.
The uptime and availability of applications and web assets is critical to your success. Managed hosting providers offering both dedicated and shared load balancers provide a secure, cost-effective solution.

VIRTUAL SERVERS, PHYSICAL SERVERS, OR BOTH?

When you need both the brute force of dedicated big iron servers and you need the flexibility of modern, cloud-based virtual machines, the ability to mix environments in a hybrid configuration solves your complex hosting requirements with a solution that is tailored to fit your business needs.

From year to year, standard solutions may not deliver the security, performance, or scalability you need to meet growing business demands. Hybrid hosting provides flexibility, allowing you to instantly adjust infrastructure — whether dedicated or cloud-based — without compromising security or reliability.

The hybrid approach eliminates the need for spreading your infrastructure across disconnected, self-managed data centers and disparate hosting providers and eliminates the costs associated with maintaining underutilized infrastructures.

Hybrid hosting solutions connect a collocated and/or dedicated server environment (private, secure, and compliant) to a private or public cloud environment. Understanding your environment and its performance requirements will help you determine what type of systems architecture works best for your application. Collaborate with the managed hosting provider’s systems engineers to help them understand your unique needs so they can recommend the most cost-effective configuration for you.

REDUNDANCY AT EACH TIER

Whether your server environment is physical or virtual, it is vital to have redundancy at each tier of your architecture. Having multiple web servers can make code management a logistical challenge, but there are ways to easily manage these hurdles. The easiest and recommended method is to use a NAS share for all collateral and web content. This method allows you to update content in one location and have your web servers all pull data from the same data store. If your application requires a physical install on the local server you should consider a simple plan that consists of the following:

- Drop one of the web servers temporarily out of the load balanced pool
- Push the updated code to that box
- Test availability using the IP, not the DNS name
- Redirect all traffic on the load balancer to the newly updated server
- Update the remaining servers following the same process
THE HIGH AVAILABILITY DATABASE
Almost all web-based applications today have a critical database component that must be considered as you architect your hosted systems for high redundancy and availability. Whichever database you choose to drive your application, you should understand that managed hosting providers can typically support only the most common brands and configurations due to the nature of their support organizations. However, some providers offer professional database services for extra fees.

DATABASE RECOMMENDATIONS:
- Don’t use uncommon databases for your application
- Design your database to support high availability from the ground up
- Use standard configurations

Understanding if your application is write or read intensive will help systems engineers choose the best and most cost effective storage solutions for your application. Understanding and anticipating IOPS (input/output operations per second) will greatly speed up the provisioning of the storage for your hosted application. **NOTE:** If you are using a Microsoft SQL Server Cluster keep in mind that you will need Active Directory (AD) to manage the cluster communication and, in the spirit of redundancy, you need two AD servers in case of outage. The best practice is to have AD servers on two different and isolated platforms; for example, one virtual AD server and one physical AD server.

REDUNDANT STORAGE
Anytime you are using physical servers for your hosted application you should ensure that the operating system drive is at minimum RAID1 for redundancy. You will also need to choose the appropriate drive size to handle local storage and any local caching, if needed. Most hosting service providers have varied tiers of high availability storage that can be expanded at the LUN (logical unit number) level. Some hosting providers can dynamically migrate your data between storage tiers to adjust for load and performance needs at peak and off-peak times. Take time to understand the various types of storage offered by your managed hosting provider and leverage their systems engineering teams to help choose the best offering based on your applications’ unique needs.
MANAGEMENT OF YOUR SYSTEMS
Now that you have addressed your core architecture, some of the smaller but still important functions need to be considered. Monitoring your application is critical to understanding performance at both peak and off-peak times. Understanding the performance characteristics of your application will help you plan the best time to perform mandatory systems backups and nightly database maintenance required to keep your application performing optimally. Most hosting service providers offer detailed monitoring packages along with scripted synthetic transaction monitoring (STM) that validate not only that the servers and services are running, but that the user experience is ideal. A synthetic transaction simulates a typical user experience and monitors the performance. If the experience is slow then you are notified of the potential systems or application issue affecting the users online experience. This allows you to identify and fix issues before the end user notices.

PATCHING YOUR SERVERS FOR SECURITY
Patching servers for protection from exploits and to address ongoing issues is another key item required in managing your systems. Most managed hosting providers allow for scheduling so that patches are applied during standard maintenance windows. **NOTE:** Make sure that patches are applied one server at a time. If all the servers are patched at the same time and reboot is required, they all might simultaneously reboot and create an unwanted outage.

YOU STILL NEED SYSTEMS BACKUPS
Just because you have a highly available configuration throughout your entire stack does not guarantee protection of your valuable data. Every managed hosting provider offers some sort of back-up service to protect systems.

Consider your backup options for all of your data whether it’s a database, NAS, SAN, physical server, or virtual server. Also consider recovery after a catastrophic outage. Backups can be complicated, so work with a managed hosting provider that can offer one tool that gives you both bare-metal and file-based backups. These solutions typically offer you the option to keep a local copy of the data and also move a copy to a geographically-remote location.

**BACKUP CONSIDERATIONS:**
- Bare-metal backups allow you to recover significantly faster
- Understand system state
- File-based backups can take over 24 hours to recover a server
- Backup to a remote location

**NOTE:** Always choose a bare-metal backup for your servers (virtual or physical). A bare-metal backup maintains a snapshot of the system state at time of back-up so you can restore the server to the exact condition it was in at the time of backup. A file-based backup requires you to rebuild the server to a functional state before you can reload the agent and restore the files.
TESTING: THE MOST IMPORTANT ITEM ON THE CHECKLIST
Once you have the ideal, highly available architecture identified and the contract is signed, how do you know it’s truly highly available? The answer is simple: test it. For a typical, high availability solution, your managed hosting provider should work with you to write up a test plan then run it until all the “gotchas” are resolved. **NOTE:** This means pulling cables, turning off ports, forcing database clusters to fail, and more. Testing every three to six months or after any major change is the key to ensuring your application is truly 100% highly available—giving you peace of mind that your business is always on.

**KEY TOPIC SUMMARY**

**Systems Monitoring and Maintenance:** *(Monitoring and patching)*
Monitoring your servers individually as well as monitoring them as a collective application is key to systems management. Much of your ongoing and future planning will be reliant on the business intelligence that in-depth monitoring offers. Regularly scheduled systems patching is a key component to protect your systems against new exploits and malicious attacks. Patching should be a standard systems management practice with any environment.

**Data Protection:** *(Bare-metal and file-based backup)*
Backing up your data is a critical component of your architecture. Always use a bare-metal backup for both your physical and virtual servers to ensure a speedy recovery in the event of a catastrophic disaster. Use file-based backups for NAS or data repositories and consider having your managed hosting provider move a copy of your data offsite to a geographically-diverse location.

**Servers:** *(Physical or virtual)*
Managed hosting providers can offer you physical, virtual, or hybrid offerings as the underlying platform for your application. Plan for redundancy at each tier using the most appropriate systems based on your needs. Consider using load-balanced, scalable, and flexible virtual machines for web and application tiers and fiber-channel-connected physical servers for demanding database tiers.
Security: (Physical firewalls and web application firewalls)
The security and protection of your confidential data is critical to the future of your business. It is crucial to consider every aspect of the security layer of your solution. Work with your managed hosting provider’s systems engineers to architect a tiered approach to locking down communications traffic. Use a web application firewall to offer secondary protection at the web server level.

Service Level Agreements (SLA)
Service level agreements are especially important for architecture that has 100% availability guarantees. SLAs demonstrate your managed service provider’s commitment to the 100% guarantee. Your managed hosting provider should offer an overall, solution-level SLA that covers all components against outage and ensures their commitment to your 100% availability.

Hosting.com is a leading provider of cloud hosting and recovery solutions to a global customer base. We measure our success through our ability to provide clients with an Always On solution to support their mission-critical applications. To accomplish this, we collaborate with our clients to build custom solutions architected and certified with the appropriate levels of availability and recovery necessary to meet unique business needs. Our North American data centers in Dallas, Denver (Corporate Headquarters), Irvine, Louisville, Newark, and San Francisco are SOC 3 certified and PCI Level 1 certified. Hosting.com’s geographically-dispersed datacenters and Cloud Super Sites coupled with the industry’s top networking and connectivity technologies provide clients with the highest levels of security, reliability, and support. To learn more about Hosting.com, visit www.hosting.com.