



ProductWorld
Online Product Communities

SECURITY ON AMAZON WEB SERVICES

ELASTIC CLOUD COMPUTING- EC2

Hosting

ProductWorld hosts its services on the Amazon Web Services platform Elastic Cloud Computing EC2. EC2 delivers a highly scalable cloud computing platform with high availability and dependability. The issues of end-to-end security and end-to-end privacy within the cloud computing world are more sophisticated than within a single data centre not facing the Internet. Ensuring the confidentiality, integrity, and availability of customer's systems and data is of the utmost importance to ProductWorld, as is maintaining trust and confidence. This document is intended to answer customer questions such as "How does ProductWorld use AWS to ensure your data is secure?"

Certifications and Accreditations

AWS is working with a public accounting firm to ensure continued Sarbanes Oxley (SOX) compliance and attain certifications such as recurring Statement on Auditing Standards No. 70: Service Organizations, Type II (SAS70 Type II) certification. These certifications provide outside affirmation that AWS has established adequate internal controls and that those controls are operating efficiently. AWS will continue efforts to obtain the strictest of industry certifications in order to verify its commitment to provide a secure, world-class cloud computing environment. The AWS platform also permits the deployment of solutions which meet industry-specific certification requirements.

Physical Security

Amazon has many years of experience in designing, constructing, and operating large-scale data centres. This experience has been applied to the AWS platform and infrastructure. AWS data centres are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data centre access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centres by Amazon employees is logged and audited routinely.

Backups

ProductWorld has a rigorous back-up routine and completes a back-up of all data in the Amazon storage service called S3. S3 itself is redundantly stored in multiple physical locations. The backup routine ensures an operating copy of the data plus 2 independent backups of the data in different locations are stored.



Elastic Compute Cloud (EC2) Security

Security within EC2 is provided on multiple levels: The operating system (OS) of the host system, the virtual instance operating system or guest OS, a stateful firewall and signed API calls. Each of these items builds on the capabilities of the others. The goal is to ensure that data contained within EC2 cannot be intercepted by non-authorized systems or users and that EC2 instances themselves are as secure as possible without sacrificing the flexibility in configuration that customers demand. Further details are provided below:

- **Host Operating System:** ProductWorld uses its individual cryptographically strong SSH keys to gain access to a bastion host. These bastion hosts are specifically built systems that are designed and configured to protect the management plane of the cloud. Once connected to the bastion, authorized administrators are able to use a privilege escalation command to gain access to an individual host. All such accesses are logged and routinely audited. When an AWS employee no longer has a business need to administer EC2 hosts, their privileges on and access to the bastion hosts are revoked.
- **ProductWorld AWS Operating System:** All virtual instances are completely controlled by ProductWorld. ProductWorld has full root access and all administrative control over additional accounts, services, and applications. Amazon AWS administrators do not have access to ProductWorld instances, and cannot log into the guest OS.
- **Firewall:** Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny mode and the Amazon EC2 customer must explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block).

The firewall is configured in groups permitting different classes of instances to have different rules, for example the case of a traditional three-tiered web application. The group for the web servers would have port 80 (HTTP) and port 443 (HTTPS) open to the world. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. Highly secure applications can be deployed using this expressive mechanism.

The firewall is controlled not by the host/instance itself, but requires the ProductWorld's X.509 certificate and key to authorize changes, thus adding an extra layer of security. The default state is to deny all incoming traffic.

- **API:** Calls to launch and terminate instances, change firewall parameters, and perform other functions are all signed by an X.509 certificate or ProductWorld's Secret Access Key. Without access to the ProductWorld's Secret Access Key or X.509 certificate, Amazon EC2 API calls cannot be made on their behalf. In addition, API calls can be encrypted in transit with SSL to maintain confidentiality.

The Hypervisor

Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor, taking advantage of paravirtualization. Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, it is possible to run the guest OS with no elevated access to the CPU. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in strong security separation between the two.



Instance Isolation

Different instances running on the same physical machine are isolated from each other utilizing the Xen hypervisor. Amazon is an active participant and contributor within the Xen community, which ensures awareness of potential pending issues. In addition, the aforementioned firewall resides within the hypervisor layer, between the physical interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no additional access to that instance, and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

ProductWorld instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically wipes every block of storage used by ProductWorld, and guarantees that one customer's data is never exposed to another.

Network Security

The AWS network provides significant protection against traditional network security issues. The following are a few examples:

- **Distributed Denial Of Service (DDoS) Attacks:** AWS API endpoints are hosted on the same Internet-scale, world class infrastructure that supports the Amazon.com retail site. Standard DDoS mitigation techniques such as syn cookies and connection limiting are used. To further mitigate the effect of potential DDoS attacks, Amazon maintains internal bandwidth which exceeds its provider-supplied Internet bandwidth.
- **Man In the Middle (MITM) Attacks:** All of the AWS APIs are available via SSL-protected endpoints which provides server authentication. Amazon EC2 AMIs automatically generate new SSH host keys on first boot and log them to the console. Customers can then use the secure APIs to call the console and access the host keys before logging into the instance for the first time.
- **IP Spoofing:** Amazon EC2 instances cannot send spoofed traffic. The Amazon -controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.



ProductWorld
Online Product Communities

ProductWorld
Rubicon Centre
Bishopstown
Cork
Ireland

www.productworld.com
sales@productworld.com

v1 Feb 2010

