VIVOCHA
SECURITY POLICY

INTRODUCTION

We operate a cloud-based digital platform—Software as a Service or SaaS—for you to engage your customers online using the most effective communication channel at the right time. We call it the Vivocha Services. We're committed to building reliable and secure systems that you can depend on for your business.

Security, privacy and compliance policies are some of the most common areas for questions we receive about Vivocha.com cloud service. Organizations using Vivovha.com are concerned about the safety of their data and that access to their data is reliable. This document aims to answer many of the frequently asked questions by IT security staff on these topics when they are considering Vivocha.com.

Rest assured that Vivocha uses advanced security technology to maximize the safety and security of your company information. Vivocha implements strict security controls aimed at protecting each user, application and system, with the confidentiality of your data and the integrity of your business as top priorities.

Security Framework

Vivocha is a software company and a services company. Security is layered into the application but physical security is just as important.

Vivocha.com leverages Amazon Web Services (AWS) for our computing infrastructure. AWS has achieved **ISO 27001 certification** and and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). They undergo annual SOC 1 audits and have been successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems.
For more detail on AWS security, please refer to http://aws.amazon.com/security/.

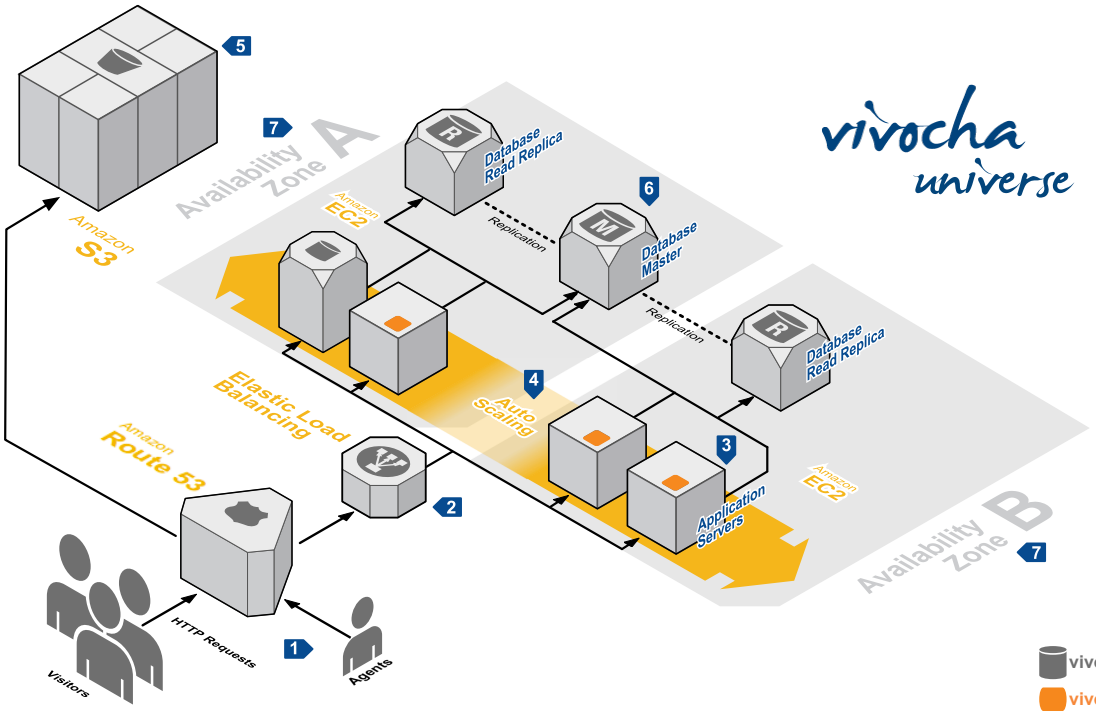
Vivocha Infrastructure Overview

The user's DNS requests are served by Amazon Route 53, a highly available Domain Name System (DNS) service. Network traffic is routed to Vivocha infrastructure running in Amazon Web Services.

HTTP requests are first handled by Elastic Load Balancing, which automatically distributes incoming application traffic across multiple EC2 instances across Availability Zones. Vivocha Web Servers (www.vivocha.com) and Vivocha Application Servers (Worlds) are deployed on Amazon EC2 instances.

With Auto Scaling we can ensure that the number of EC2 instances we're using increases seamlessly during demand spike to maintain performances.

Resources and static contents used by the Vivocha applications are stored on Amazon Simple Storage Service (S3), a highly durable storage infrastructure designed for mission-critical and primary data storage.



System Overview

1. The user's DNS requests are served by Amazon **Route 53**, a highly available Domain Name System (**DNS**) service. Network traffic is routed to Vivocha infrastructure running in Amazon Web Services.
2. HTTP requests are first handled by **Elastic Load Balancing** which automatically distributes incoming application traffic across multiple **EC2** instances across Availability Zones.
3. Vivocha Web Servers (**www.vivocha.com**) and Vivocha Application Servers (**Worlds**) are deployed on Amazon EC2 instances.
4. With **Auto Scaling** we can ensure that the number of EC2 instances we're using increases seamlessly during demand spike to maintain performances.
5. **Resources and static contents** used by the Vivocha applications are stored on Amazon Simple Storage Service (**S3**), a highly durable storage infrastructure designed for mission-critical and primary data storage.
6. **Database replication** ensures redundancy, backup, and automatic failover. A three-member replica sets provide enough redundancy to survive most network partitions and other system failures. Additionally, these sets have sufficient capacity for many distributed read operations.
7. **Availability Zones** (AZs) are distinct geographic locations that are engineered to insulate against failures in other AZs. Multiple AZs are combined into different **Regions**. Vivocha applications are deployed in different AZs and different regions to ensure high availability.

Database replication ensures redundancy, backup, and automatic failover. A three-member replica sets provide enough redundancy to survive most network partitions and other system failures. Additionally, these sets have sufficient capacity for many distributed read operations.

Availability Zones (AZs) are distinct geographic locations that are engineered to insulate against failures in other AZs. Multiple AZs are combined into different Regions (United States, EU). Vivocha applications are deployed in different AZs and different regions to ensure high availability.

Physical Security of Facilities

Vivocha.com employees do not have physical access of any kind to our production facilities, as all of our infrastructure is in the cloud at AWS.

Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow to remain resilient in the face of most failure modes, including natural disasters or system failures.

Our Infrastructure provider - Amazon - has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical locations have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Authorized staff must pass two-factor authentication no fewer than three times to access Amazon Web Services Security data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center 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 centers by Amazon employees is logged and audited routinely.

Environmental Safeguards

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

Management

Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Network Security

The Amazon EC2 inbound firewall is configured in a default deny mode and Vivocha.com explicitly opens 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 to permit only the absolute minimum connectivity required to provide the Vivocha.com services. Changes to firewall access rules require Vivocha.com's X. 509 certificate and key for authorization.

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. Vivocha.com then uses 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.
- **Port Scanning**: Port scans by Amazon EC2 customers are a violation of the Amazon EC2 Acceptable Use Policy (AUP). Violations of the AUP are taken seriously, and every reported violation is investigated. When Port scanning is detected it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed.

Packet sniffing by other tenants: It is not possible for a virtual instance running in promiscuous mode to receive or “sniff” traffic that is intended for a different virtual instance. The hypervisor will not deliver any traffic to instances that is not addressed to them. This includes two virtual instances that are owned by the same customer, even if they are located on the same physical host. Attacks such as ARP cache poisoning do not work within EC2.

The Operations Team has the ability to change firewall rules.

Additional information on AWS specific security measures can be found at http://media.amazonwebservices.com/AWS_Security_Whitepaper.pdf

Host Security

We are leveraging AWS for all of our computing infrastructure. AWS owns the physical hardware. AWS provides security groups to limit access to devices. We fully utilize security groups to limit access to our computing resources.

Our production environment is completely separate from the other environments, including development and QA. The development and QA environments are in the west-2 region (Oregon, USA), the production environments are currently in the east-1 (North Virginia, USA) and eu-1 (Ireland, Europe) regions.

AWS provides Identity Access Management (IAM) to control access to AWS resources. We use AWS IAM to manage separate, restrictive AWS credentials for each of our environments. This limits the AWS services available to each environment and compartmentalizes them.

We also use AWS IAM to delegate monitoring and management capabilities to operations staff and prevent destructive actions.

SSH keys are required to gain console access to our servers, in any of the environments.

Individually identifiable RSA key pairs are used for SSH access, and root login is disabled. This insures that there is a complete audit trail via sudo from a specific action back to the specific individual who triggered that action.

We adhere to strong password policies and require that all RSA private keys be encrypted with a compliant password.

Automated processes are in place on each host that monitoring for unauthorized login attempts, with the offending IP address being automatically blacklisted and an alert being generated.

Hardened Operating System

Vivocha runs on hardened Linux servers. Externally exposed critical patches are addressed within 24 hours.

Internal and Third Party Testing
Vivocha routinely runs internal and external vulnerability scans and penetration tests. Third party firms are utilized to perform in-depth quarterly security reviews.

Password Policies
Administrative controls allow the definition of password policies for length, expiry, and complexity to mirror your corporate password policies.

Business Continuity
Your data is backed up multiple times a day. Backups are transferred offsite over SSH and properly deleted after six months.

The servers are built using repeatable build processes. All changes to the production environment pass through a peer-review change management process, with all changes logged to a central ticket system.

Secure Connections
All connections to Vivocha.com session controlled APIs are secured via SSL/TLS. Any attempt to connect over HTTP is redirected to HTTPS.

Application Security

Vivocha utilizes secure development best practices that integrate security reviews throughout design, prototype, and deployment.

Encryption

We have implemented strong encryption via SSL in our application. By using encryption, we minimize the chances of someone possibly intercepting username/password combinations and/or other sensitive information.

Areas where we utilize SSL include:

- All application logins require SSL. Any area which requires a user to log into our system also requires that SSL is used.
- The administrative, agent, analytics and API interfaces all leverage and requires SSL throughout.

- Any communication session through Vivocha.com (chat, voice, video, co-browsing sessions) requires SSL throughout.

Some static assets (javascript libraries and css style sheets) have optional SSL access.

Brute Force Attack Prevention

In order to minimize brute force login attacks, we automatically disable accounts for a five-minute period after five consecutive failed attempts have been registered. If we ever determine that this is a possible area of concern, we can easily increase the lockout period or decrease the number of consecutive failures via configuration.

XSS

All communication messages (user chat text and API generated chat events) and user provided data are sanitized to prevent XSS

CSRF

Vivocha.com requires authenticity tokens in all sensitive JSON requests with corresponding verification on inbound requests.

SQL Injection

Vivocha.com is immune to SQL injection attacks, as we don't use any form of SQL in our systems.

Attachment filenames

Attachments are saved to a generated GUID temp file before uploading to S3. This avoids issues associated with saving/overwriting files with relative file paths.

Passwords

All user passwords are hashed using the MD5 algorithm with salt. Hashing passwords is actually more secure than encrypting them, because that means we don't have access to the original passwords, nor does anyone else. So even if our database is compromised, everyone's passwords will stay secure.

Complex passwords with a minimum password length of 8 characters are required for all users by default.

Data Storage & Retention Policies

Data is generally stored in a MongoDB Database. File attachments are stored within S3. All data (other than passwords and authentication strings) is stored in clear text.

We support optional end-to-end encryption of communication messages (chat transcripts), via our APIs: in this scenario, Vivocha.com does not store the encryption key used, and has no means of decrypting the stored data.

The production MongoDB database is configured with high availability with data replicated to multiple, redundant instances. The database is backed up on a nightly basis with encrypted backup copies being shipped to secure offsite storage.

Vivocha.com is a multi-tenant SaaS solution: customer data is co-mingled on the same database collections, but all data is scoped by an account ID to ensure that one account cannot access data of another account. Unit, functional, and integration tests are run continuously on our servers to ensure that it‘s not possible for account data to leak.

In addition to our usage of this data in production we also occasionally take a copy of the data and load it in our testing environments. These copies are scrubbed of any sensitive or personally-identifiable information before being used for testing or development purposes.

Access controls to service data

Having contracted with Vivocha for the service you provide Vivocha with access to your production, development or test environment, which may include personal information about your employees, customers, partners or suppliers (collectively "end users").

Vivocha's access to services data is based on job role/responsibility. Vivocha will safeguard data you send to our organization in the same manner in which we protect our own similar confidential information.

Vivocha.com staff does not access or interact with customer data or applications as part of normal operations. There may be cases where Vivocha.com is requested to interact with customer data or applications at the request of the customer for support purposes or where required by law.

Below are the conditions under which Vivocha may access, collect and/or use services data.

- **To Provide Services**: Services data may be accessed and used to fulfill the requirements specified in your order for support, consulting,or other services.
- **To Maintain and Upgrade a System**: Technical staff may require periodic access to services data to monitor system performance, test systems and develop and implement upgrades to systems. Any temporary copies of services data created as a necessary part of this process are only maintained for time periods relevant to those purposes.
- **To Address Performance and Fix Issues**: On occasion, Vivocha may develop new versions, patches, updates, and other fixes to its programs and services (such as security patches addressing newly discovered vulnerabilities). In accordance with the terms of your order for services and/or with notice to you, we may access and/or use a copy of your test, development or production environment, including services data, to test such new versions, patches, updates and fixes and validate that they work in your environment(s).

- **As a Result of Legal Requirements:** Vivocha may be required to provide personally identifiable information to comply with legally mandated reporting, disclosure or other legal process requirements.

Vivocha may transfer and access services data globally as required for the purposes specified above. If Vivocha hires subcontractors to assist in providing services, their access to services data will be consistent with the terms of your order for services and this services privacy policy.

Vivocha does not use services data except as stated above or in your order. Vivocha may process services data, but does not control your information collection or use practices for services data. If you provide any services data to Vivocha, you are responsible for providing any notices and/or obtaining any consents necessary for Vivocha to access and use services data as specified in this policy and your order.

Each Vivocha Employee and subcontractor must sign a confidentiality agreement, specifically covering access to services data.

Penetration Testing

Vivocha.com strives to provide a robust and trustworthy service for our customers. We take security very seriously and continually monitor our services for suspected attack. We also understand that security is a partnership between us and our customers. A critical phase of any secure application deployment involves testing applications for potential vulnerabilities.

Our Terms and Conditions (http://www.vivocha.com/tos) describes permitted and prohibited behavior on Vivocha.com and includes descriptions of prohibited security violations and network abuse. However, because penetration testing frequently is indistinguishable from these activities, we have established a policy for customers to request permission to conduct penetration tests: please send an email to support@vivocha.com, providing as much details as possible, including the nature of the tests that you want to perform, where the tests would be performed from and who will be conducting them, and contact details of who will be responsible for them on your side. Our staff get in contact with you as soon as possible to discuss you request and eventually grant you our authorization.

No further action on your part is required after you receive our authorization. You may conduct your testing through the conclusion of the period agreed. If you need more time for additional testing, contact our support staff again asking to extend your test period to the new date. You are not authorized for an extension unless you receive a new authorization from us.

References

Overview of AWS Security Practices Whitepaper, March 2013

(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

AWS Risk and Compliance Whitepaper, January 2013

(media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)