Security In a Multi-tenant Environment

Learn about protecting your data on the cloud - a) data in transit b) data at rest c) protecting your credentials d) securing your Application.

Security Best Practices for the Cloud In a multi-tenant environment.

We as cloud architects often express concerns about security. Security should be implemented in every layer of the cloud application architecture. Physical security is typically handled by your service provider, which is an additional benefit of using the cloud. Network and application-level security is your responsibility and you should implement the best practices as applicable to your business. It is recommended to take advantage of these tools and features mentioned to implement basic security and then implement additional security best practices using standard methods as appropriate or as they see fit.

Protect your data in transit

If you need to exchange sensitive or confidential information between a browser and a web server, configure SSL on your server instance. You'll need a certificate from an external certification authority like VeriSign or Entrust. The public key included in the certificate authenticates your server to the browser and serves as the basis for creating the shared session key used to encrypt the data in both directions.

Creating a Virtual Private Cloud by making a few command line calls (using VPC). This will enable you to use your own logically isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPSec VPN connections. You can also setup an OpenVPN server on an Amazon EC2 instance and install the OpenVPN client on all user PCs.

Protect your data at rest

If you are concerned about storing sensitive and confidential data in the cloud, you should encrypt the data (individual files) before uploading it to the

cloud. For example, encrypt the data using any open source or commercial

PGP based tools before storing it as Amazon S3 objects and decrypt it after download.

This is often a good practice when building HIPAA-Compliant applications that need to store Protected Health Information (PHI). On Amazon EC2, file encryption depends on the operating system. Amazon EC2 instances running Windows can use the built-in Encrypting File System (EFS) feature.

This feature will handle the encryption and decryption of files and folders automatically and make the process transparent to the users . However, despite its name, EFS doesn't encrypt the entire file system; instead, it encrypts individual files. If you need a full encrypted volume, consider using the open-source TrueCrypt product; this will integrate very well with NTFS-formatted EBS volumes. Amazon EC2 instances running Linux can mount EBS volumes using encrypted file systems using variety of approaches (EncFS, Loop-AES , dm-crypt, TrueCrypt).

Likewise, Amazon EC2 instances running OpenSolaris can take advantage of ZFS Encryption Support. Regardless of which approach you choose, encrypting files and volumes in Amazon EC2 helps protect files and log data so that only the users and processes on the server can see the data in clear text, but anything or anyone outside the server see only encrypted data. No matter which operating system or technology you choose, encrypting data at rest presents a challenge: managing the keys used to encrypt the data. If you lose the keys, you will lose your data forever and if your keys become compromised, the data may be at risk.

Therefore, be sure to study the key management capabilities of any products you choose and establish a procedure that minimizes the risk of losing keys. Besides protecting your data from eavesdropping, also consider how to protect it from disaster. Take periodic snapshots of Amazon EBS volumes to ensure it is highly durable and available. Snapshots are incremental in nature and stored on Amazon S3 (separate geo-location) and can be restored back with a few clicks or command line calls.

Protect your AWS credentials

AWS supplies two types of security credentials: AWS access keys and X.509

certificates. Your AWS access key has two parts: your access key ID and your secret access key. When using the REST or Query API, you have to use your secret access key to calculate a signature to include in your request for authentication. To prevent in-flight tampering, all requests should be sent over HTTPS. If your Amazon Machine Image (AMI) is running processes that need to communicate with other AWS web services, one common design mistake is embedding the AWS credentials in the AMI.

Instead of embedding the credentials, they should be passed in as arguments during launch and encrypted before being sent over the wire. If your secret access key becomes compromised, you should obtain a new one by rotating to a new access key ID. As a good practice, it is recommended that you incorporate a key rotation mechanism into your application architecture so that you can use it on a regular basis or occasionally (when disgruntled employee leaves the company) to ensure compromised keys can't last forever. Alternately, you can use X.509 certificates for authentication to certain AWS services.

The certificate file contains your public key in a base64-encoded DER certificate body. A separate file contains the corresponding base64-encoded PKCS private key. AWS supports multi-factor authentication as an additional protector for working with your account information on AWS Management Console.

Manage multiple Users and their permissions with IAM AWS Identity and Access Management (IAM) enables you to create multiple Users and manage the permissions for each of these Users within your AWS Account. A User is an identity (within your AWS Account) with unique security credentials that can be used to access AWS Services.

IAM eliminates the need to share passwords or access keys, and makes it easy to enable or disable a User's access as appropriate. IAM enables you to implement security best practices, such as least privilege, by granting unique credentials to every User within your AWS account and only grant permission to access the AWS Services and resources required for the Users to perform their job.

IAM is secure by default; new Users have no access to AWS until permissions are explicitly granted. IAM is natively integrated into most AWS Services. No

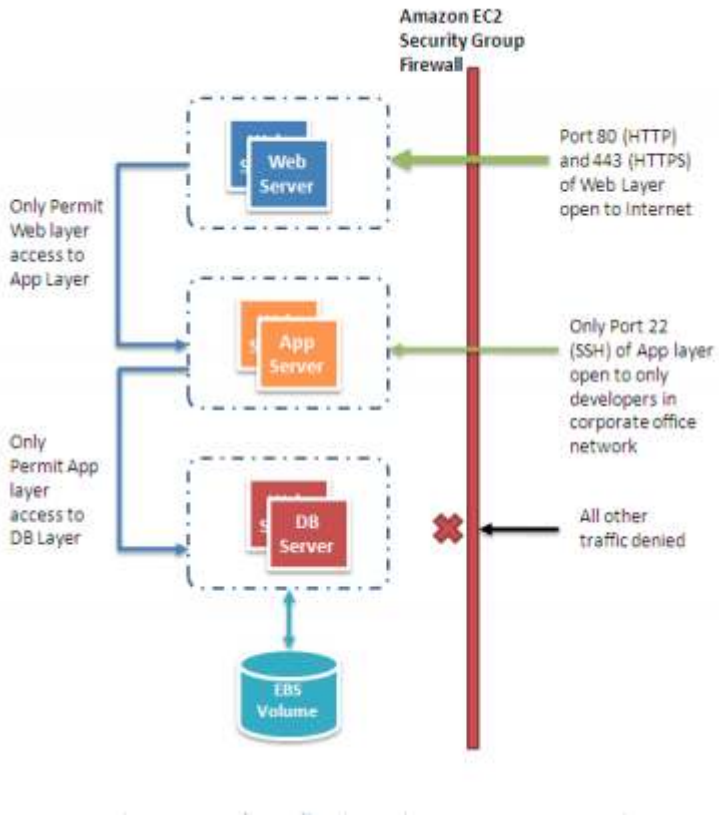
service APIs have changed to support IAM, and applications and tools built on top of the AWS service APIs will continue to work when using IAM.

Applications only need to begin using the access keys generated for a new User.

You should minimize the use of your AWS Account credentials as much as possible when interacting with your AWS Services and take advantage of IAM User credentials to access AWS Services and resources.

Secure your Application

Every Amazon EC2 instance is protected by one or more security groups 43, named sets of rules that specify which ingress (i.e., incoming) network traffic should be delivered to your instance. You can specify TCP and UDP ports, ICMP types and codes, and source addresses. Security groups give you basic firewall-like protection for running instances. For example, instances that belong to a web application can have the following security group settings:



Another way to restrict incoming traffic is to configure software-based firewalls on your instances. Windows instances can use the built-in firewall. Linux instances can use netfilter and iptables. Over time, errors in software are discovered and require patches to fix.

You should ensure the following basic guidelines to maximize security of your

application:

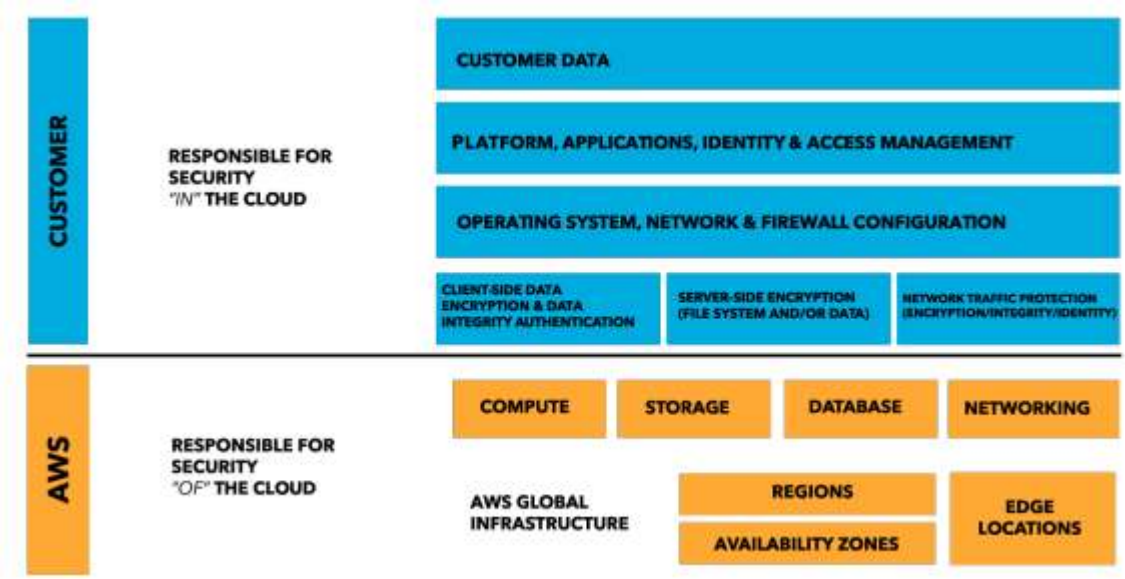
1. Regularly download patches from the vendor's web site and update your AMIs
   Redeploy instances from the new AMIs and test your applications to ensure the patches don't break anything. Ensure that the latest AMI is deployed across all instances
2. Invest in test scripts so that you can run security checks periodically and automate the process
3. Ensure that the third-party software is configured to the most secure settings
4. Never run your processes as root or Administrator login unless absolutely necessary

All the standard security practices pre-cloud era like adopting good coding practices, isolating sensitive data are still applicable and should be implemented. In retrospect, the cloud abstracts the complexity of the physical security from you and gives you the control through tools and features so that you can secure your application.

Cloud Security - Shared Security Responsibility Model

Before we go into the details of how AWS secures its resources, we should talk about how security in the cloud is slightly different than security in your on premises data centers. When you move computer systems and data to the cloud, security responsibilities become shared between you and your cloud service provider.

In this case, AWS is responsible for securing the underlying infrastructure that supports the cloud, and you're responsible for anything you put on the cloud or connect to the cloud. This shared security responsibility model can reduce your operational burden in many ways, and in some cases may even improve your default security posture without additional action on your part.



The amount of security configuration work you have to do varies depending on which services you select and how sensitive your data is. However, there are certain security features—such as individual user accounts and credentials, SSL/TLS for data transmissions, and user activity logging—that you should configure no matter which AWS service you use.

AWS Security Responsibilities

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

Protecting this infrastructure is AWS's number one priority, and while you can't visit our data centers or offices to see this protection firsthand, we provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations. Note that in addition to protecting this global infrastructure, AWS is responsible for the security configuration of its products that are considered managed services. Examples of these types of services include Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces, and several other services.

These services provide the scalability and flexibility of cloud-based resources with the additional benefit of being managed. For these services, AWS will handle basic security tasks like guest operating system (OS) and database

patching, firewall configuration, and disaster recovery. For most of these managed services, all you have to do is configure logical access controls for

the resources and protect your account credentials. A few of them may require additional tasks, such as setting up database user accounts, but overall the security configuration work is performed by the service.

Customer Security Responsibilities

With the AWS cloud, you can provision virtual servers, storage, databases, and desktops in minutes instead of weeks. You can also use cloud-based analytics and workflow tools to process your data as you need it, and then store it in your own data centers or in the cloud. Which AWS services you use will determine how much configuration work you have to perform as part of your security responsibilities. AWS products that fall into the well-understood category of Infrastructure as a Service (IaaS)—such as Amazon EC2, Amazon VPC, and Amazon S3 are completely under your control and require you to perform all of the necessary security configuration and management tasks.

For example, for EC2 instances, you're responsible for management of the guest OS (including updates and security patches), any application software or utilities you install on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

These are basically the same security tasks that you're used to performing no matter where your servers are located. AWS managed services like Amazon RDS or Amazon Redshift provide all of the resources you need in order to perform a specific task—but without the configuration work that can come with them.

With managed services, you don't have to worry about launching and maintaining instances, patching the guest OS or database, or replicating databases AWS handles that for you. But as with all services, you should protect your AWS Account credentials and set up individual user accounts with Amazon Identity and Access Management (IAM) so that each of your users has their own credentials and you can implement segregation of duties.

We also recommend using multi-factor authentication (MFA) with each account, requiring the use of SSL/TLS to communicate with your AWS resources, and setting up API/user activity logging with AWS CloudTrail. AWS Global Infrastructure Security AWS operates the global cloud infrastructure

that you use to provision a variety of basic computing resources such as processing and storage. The AWS global infrastructure includes the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. The AWS global infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. As an AWS customer, you can be assured that you're building web architectures on top of some of the most secure computing infrastructure in the world.

AWS as well as Azure have Compliance Programs to customers understand the robust controls in place to maintain security and data protection in the cloud.

As systems are built on top of any infrastructure, compliance responsibilities will be shared.

By tying together governance-focused, audit friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

The IT infrastructure that is provided to customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

• SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70) • SOC 2 • SOC 3 • FISMA, DIACAP, and FedRAMP • DOD CSM Levels 1-5 • PCI DSS Level 1 • ISO 9001 / ISO 27001 • ITAR • FIPS 140-2 • MTCS Level 3