AWS Well Architected

Your company’s new dev team requires access to SAML enabled applications on AWS. The system admin would like to rely solely on the company’s on- premise Active Directory to use existing user credentials. A user portal for logins and MFA is required for easy access and added security.

How would you design a solution for federating users into AWS?

A. Configure AWS Managed Microsoft AD to provide user authentication and set up user access via an AWS sign-in endpoint for SAML and Microsoft ADFS

B. Connect to your corporate AD server by using Simple AD for user authentication and set up user access via AWS SSO.

Does AWS SSO provide a user portal for easy login where users would not have to create new credentials? Does Simple AD support SAML? Does Simple AD support MFA?

Fail to meet MFA requirement

**C. Use your corporate AD server by configuring AD Connector for user authentication and set up user access via AWS SSO**

Can AD Connector forward sign-in requests to your on-premise AD for authentication?

Does AWS SSO provide a user portal for easy login where users would not have to create new credentials?

Meet all requirements

D. Create IAM users and groups that are mapped to the corporate AD user roles and use MFA for authentication

One of your hybrid clients is having latency issues with their new video and voice application hosted on EC2 instances. An internet -based VPN connection is being used for encryption. They are based in San Francisco and currently operate in us-west-1. They want to spin up more instances into ap-southeast-1, and are concerned that latency will increase for their real-time data applications.

What do you recommend to improve latency and also provide in-transit data protection?

B. Use AWS VPN CloudHub to access instances in both regions via a private virtual interface. Use AWS KMS for encryption.

Can AWS KMS protect data in-transit?

Fails to address the low latency multi-region and in-transit data protection requirement

D. Use an AWS Direct Connect to access instances in both regions via a private virtual interface. Use an AWS managed VPN for encryption.

Incorrect architecture to meet encryption requirement

A company has multiple AWS accounts to separate the dev and test resources. They want to automate their end-to-end account creation process. The security officer pointed out that AWS CloudTrail logging must be enabled on all accounts and regions. Users including those with administrative privileges should not be able to perform any actions on CloudTrail trails.

How would you automate account creation and centrally enforce the security requirement on all accounts?

1. **Use AWS Organizations to manage and create accounts and AWS CloudFormation for configuration. Use a service control policy (SCP) to filter out API for CloudTrail**

Can AWS Organizations manage and automatically create accounts via its API?

Can AWS CloudFormation be used to configure the account with the needed resources, including creating CloudTrail trails?

Can SCP be used to filter out API for an account?

Meets all requirements

1. Use AWS managed Microsoft AD to manage and create accounts and AWS CloudFormation for configuration. Move all users under an IAM group denying CloudTrail API

Can AWS Managed Microsoft AD be used to manage or create AWS accounts?

Is moving all users, including administrators to a single group with the same permission desirable?

Fails to meet management and automation requirement

An education company delivers course materials to their students as PDF downloads. Recently there have been more downloads than students in their classes and the company wants to limit each PDF to being downloaded to class members.

The current architecture has students sign in to a website that runs on EC2 instances. The website provides links to publicly accessible files in Amazon S3. The company wants to use CloudFront to limit downloads

1. Configure CloudFront with an origin access identity for Amazon S3 and remove public read actions from the S3 bucket policy. Configure Amazon S3 as a trusted signer for CloudFront. Have the web servers return a CloudFront signed URL

What is an OAI? What is a trusted signer? **Amazon S3 cannot be a trusted signer for CloudFront**. What is a CloudFront signed URL?

1. Configure CloudFront with an origin access identity (OAI) for S3. Create an EC2 role for the web servers that explicitly denies all S3 actions. Have the web servers return a CloudFront signed URL

Can public access to s3 be denied using EC2 role? Can S3 hosted web servers return CloudFront signed URL? This will not restrict downloads

1. Create a CloudFront behaviour with the AWS account as a trusted signer. Update the S3 bucket policy to remove all S3 URL

What is a CloudFront behaviour? Can AWS accounts be trusted signers? Will removing all public read actions be effective? Web servers returning S3 URL are the current issue

1. **Configure CloudFront with an OAI for S3 and remove public read actions from the S3 bucket policy. Create a CloudFront behaviour with the AWS account as a trusted signer. Have the web servers return a CloudFront signed URL**

Can S3 be configured to be an OAI for Amazon CloudFront? What happens when public read actions are removed from S3 buckets? How is a CloudFront signed URL different than a S3 URL?

Meet all requirements

You are working with a company that wants to create a new game using AWS Mobile Hub. Backend systems will use multiple AWS Regions. Player data, including scores, will be stored in the region closest to users when the game is first launched. Each region is to host its own scoreboard.

Company leaders want scoreboards in each region to deploy high scores from both the Region and those achieved globally. In each region, how should the backend store player score information?

1. Write scores to a Multi-AZ table in an Amazon Aurora instance in the local region. Replicate the score table among regions using Aurora replication.
2. **Write scores to a DynamoDB table in the local region. Enable DynamoDB streams, create a worker tier to consume the stream and relay the data to DynamoDB tables in all other regions**

Is DynamoDB good for storing click stream data? Can DynamoDB Streams synchronize data between DynamoDB tables? What is the data retention limit for DynamoDB Streams?

Meets all the requirements

1. Write scores to a DynamoDB table in the local region. Create a worker tier to read recent writes from the table and relay the data to DynamoDB tables in all other regions

Is a worker tier enough to replicate DynamoDB tables? How much logic is needed to identify and define what a recent write is? How much overhead would be added to DynamoDB throughput per table to do the work?

Works but the worker tier needs intelligence to identify recent writes and throughput will be high because of the constant queries

1. Write scores to a DynamoDB table in every region directly
2. Write scores to a Multi-AZ ElasticCache Redis cluster in the local region. Write the code for the scoreboard to pull data from the Redis read replicas

You have a client that has an application with components written in various languages, including Python, Ruby, node js, and PHP

Data is stored in an Amazon RDS MySQL database. Logs from the components contain different fields and information. Your task is to centralize the logs and use them to produce a coherent weekly report of usage patterns. What approach should you take?

1. Use Amazon Simple Workflow Service (Amazon SWF) to move the logs into Amazon Redshift. Query Amazon Reshift using various BI tools
2. Have each application component store its logs in Amazon Kinesis. Move the logs into Amazon Redshift in real time. Query Amazon redshift using various BI tools

Is Amazon Kinesis appropriate for sending log data? Is Amazon Redshift designed to ingest data in real time? Amazon redshift not designed for continuous ingestion of real time data

1. **Have each application put its logs in Amazon S3. Process the logs using Amazon EMR and store the results in Amazon redshift for long term analysis using various BI tools**

Is Amazon s3 good for log storage? Can Amazon EMR effectively and efficiently process log files

? Is Amazon Redshift a good tool for data storage and BI processing? Meets all the requirements

1. Use AWS data Pipeline to move logs from the application servers into an Amazon EMR cluster once per week. Process the logs using Amazon EMR and then move the results in Amazon redshift for long term analysis using various BI tools

A software company is considering Elastic Beanstalk to deploy new versions of their applications into their production environment consisting of a Multi-AZ RDS setup. Application availability during deployment and a low -cost solution are top priorities. After the deployment, the company is required to delete the source application code used by Elastic Beanstalk. What would you recommend for a deployment solution?

1. Run an immutable deployment to minimize application downtime and manually delete the source bundle after the deployment
2. Run a rolling deployment with an additional batch to minimize application downtime and allow Elastic beanstalk to automatically delete the source bundle

Will a rolling deployment with an additional batch minimize application downtime? Does Elastic Beanstalk automatically delete the source bundle?

1. **Run a rolling deployment to minimize application downtime and manually delete the source bundle after the deployment**

Will a standard rolling deployment minimize application downtime at the lowest cost? Matches the requirement

1. Run the default deployment option to minimize application downtime and allow Elastic Beanstalk to automatically delete all previous versions of the application

Your customer runs an event management SaaS application that uses Amazon EC2, Auto Scaling, Elastic Load Balancing and Amazon RDS. Software is installed on instances at first boot, using Puppet and Chef, which is also used to deploy software updates multiple times per week. A major software overhaul – a new, much larger version of the software – has been deployed to running EC2 instances and some instances are being terminated during the update process.

What actions could be taken to prevent instances from being terminated during updates?

1. Use the zero downtime feature of Elastic Beanstalk to deploy new software releases to your existing instances
2. **Use CodeDeploy to create an application and a deployment targeting the Auto Scaling group. Use CodeDeploy to deploy and update the application in the future**

Can CodeDeploy remove an instance from an ELB load balancer? Can CodeDeploy suspend health checks on an ELB load balancer and then, after the install, reinstate them?

AWS CodeDeploy can run pre-install tasks to remove an instance from an ELB load balancer, suspend health checks before install, then reinstate

1. **Suspend the Auto Scaling process. Once suspended, deregister the instance from the ELB, update the application, and register it with the ELB on successful update**

What happens if the Auto Scaling process remains active while updating the instance?

Auto Scaling is causing instances to terminate. While updating, suspend it and after the updates complete, restart

1. Use the AWS Management Console to enable termination protection for the current processes
2. Run “AWS auto scaling detach-load-balancers” before updating your application

What happens to traffic when load balancers are detached from the Auto Scaling group? Does the load balancer control the size and shape of the Auto Scaling group? Detaching load balancers stops all traffic to all instances in the Auto Scaling group

One of your clients runs free video streaming services on AWS. Videos are stored in Amazon S3 and distributed publicly via S3 URLs. The client is moving towards a paid subscription model. Videos should now only be available to paid subscribers. Also, since this will now be paid content, security controls require to be encrypted at rest.

What is the best way to meet the new requirements for paid services?

1. Use a Cloud HSM appliance cluster for data encryption, create IAM users and groups to only provide the paid subscribers access to the videos on Amazon S3

Are CloudHSM appliances used to encrypt data? It is possible to create IAM users for each paid subscriber and allow access . Is that the best way compared to other options?

1. **Use AWS KMS to encrypt and decrypt videos, create a CloudFront distribution, configure OAI for user access, and deny direct access to Amazon S3 URLs**

Can AWS KMS be used to encrypt data on an S3 bucket via SSE\_KMS? Is configuring an OAI the best way to restrict user access in comparison to Amazon S3 URLs? yes

1. Use SSE-C to encrypt and decrypt videos, create a CloudFront distribution and store the encryption keys in CloudFront so that only authenticated users have access

Is SSE\_C a supported encryption method for Amazon S3 buckets? Where is the key used n SSE-C stored? Fails to meet the user restriction requirement

1. Create a CloudFront distribution, use SSL\TLS encryption between the paid subscribers and CloudFront, and deny access via Amazon S3 URLs

Does using SSL\TLS encrypt data in-transit? At rest? What impact does denying access via Amazon S3 URLs have? Fails to meet data encryption at rest and user access restriction

A company has been manually deploying package updates to all their applications running on Amazon EC2 instances. Due to the increasing amount of management overhead, the company is looking for a solution to automate application deployment and updates. These applications are critical and warrant the least amount of downtime during updates

Which solution provides the automation needed?

1. Create a golden image from a custom AMI containing all the required application package updates
2. Modify the EC2 user data property in an AWS CloudFormation template and update the stack
3. **Use AWS CloudFormation to create and deploy a Chef server and bootstrap the EC2 instances with the Chef client software**

Can Chef be combined with CloudFormation to manage deployments? What does it mean to bootstrap EC2 instances with Chef client software? Matches the requirements

1. Use the UpdateStack API call in AWS CloudFormation to update the stack with a new version of the application

What happens to applications running on instances when a stack is updated? Not mentioned is the cfn-hup helper. What is it? If it were present, would it improve the answer? Fails to meet the least downtime requirement

Your client’s CloudWatch logs configuration receives logs and data from on-premises monitoring systems and agents installed in operating systems. A new team wants to use CloudWatch to also monitor Amazon EC2 instance performance and state changes of EC2 instances, such as instance creation, instance power-off, and instance termination. This solution should also be able to notify the team of any state changes for troubleshooting

What should you do to monitor EC2 instance state changes and performance?

**Use Amazon Cognito for mobile user sign-in. use an Auto Scaling group of EC2 instances across multiple AZ to serve the images, Amazon ElasticCache with a Redis replication group to cache, multi AZ RDS to store user information**

Use Amazon web identity federation for mobile user sign-in, an Auto Scaling group of EC2 instances across multiple AZ to serve images, an Amazon ElastiCache cluster using Mencached as a caching layer, and multi-AZ RDS instance

Which is more cost effective building out a web identity federation or using Amazon Cognito? Is this option highly available? Identity federation matches the requirement but requires a significant number of development cycles

Create IAM users for the application. Use Amazon Cognito to map policies to the IAM users and cache identities across AZ. Use an Auto Scaling group of EC2 instances across multiple AZ to serve images, an Amazon ElastiCache with a Redis replication group to cache and multi-AZ RDS to store user information

IAM users should not be used for application authentication. Each AWS account can have 5000 IAM users

AWS Managed VPN – a hardware VPN connection from client premises network equipment on a remote network to AWS managed network equipment attached to client’s Amazon VPC

AWS VPN CloudHub – a hub and spoke model for connecting multiple remote branch offices to an Amazon VPC

Software VPN – a VPN connection from client’s equipment on a remote network to a user managed software VPN appliance running inside client’s Amazon VPC

Whitepapers

AWS Security Best Practices

AWS well- architected framework

Architecting for the cloud

Microservices on AWS

AWS overview of Security Processes

CI and CD on AWS accelerating software delivery with DevOps

Using AWS for disaster recovery

AWS compute, management tools, storage, networking and content delivery, analytics, identity and compliance and application integration

AWS architecture centre