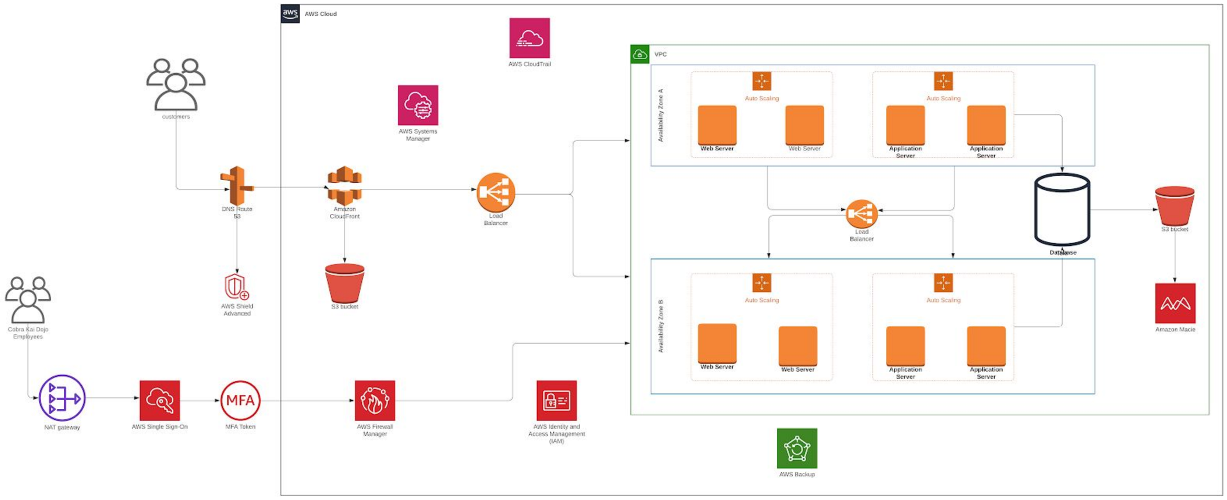
FINAL PROJECT REPORT
ENPM809J- Cloud Security
Mrugandha Namjoshi

COBRA KAI

Introduction-

After proposing hosting of the Cobra Kai application on the Amazon Web Services (AWS), I would like to give a walkthrough for the services that can be used to successfully migrate the application in the cloud. This migration will make the application more secure and sturdy and can help in reducing IT costs, and enabling benefits like application scalability and many more.

This was a high-level representation of how the Cobra Kai application will look after migrating it to AWS.



Considering the current issues, the document will describe use of several services provided by AWS to overcome those issues and make the application more resilient and highly secure.

For Migrating the Cobra Kai Application to AWS we need to follow the below mentioned steps:

1. Assess cloud migration strategies and readiness.
2. Discover portfolio and plan for migration.
3. Plan and design application migration strategy.
4. Perform and validate application migration to the cloud.
5. Optimize applications and operations after migration

Tools Used to implement the services in order to overcome the current issues in Cobra Kai Application are as follows:

Problem 1: Patching Strategy

Patch Management:

Patch management is the process of distributing and applying updates to software.These patches are regularly important to address mistakes (likewise alluded to as "weaknesses" or "bugs") in the product. At the point when a weakness is found after the arrival of a bit of programming, a patch can be utilized to fix it.

Patch Management Life Cycle:

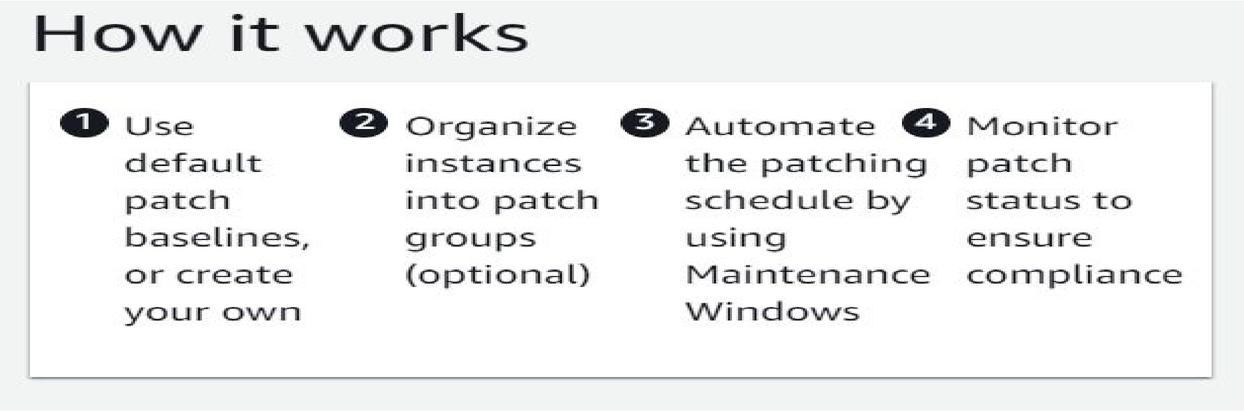
- Update vulnerability details from software vendors.
- Scan the enterprise network for vulnerability.
- Examine the Vulnerability and identify the missing patches.
- Deploy patches and validate patch installation.
- Produce Status Report on the most recent patch updates.

Recommendation:

For the Kobra Kai application, we can make use of AWS System Manager that will help in providing a unified user interface, so that we can view the operational data from the multiple AWS services. System Manager can help in grouping resources like the EC2 instance and the S3 buckets, therefore here in the case of occurrence of malfunctioning in the availability zone A and B, Amazon S3 buckets will have the backup data.

Process of patching by AWS System Manager:

How it works:



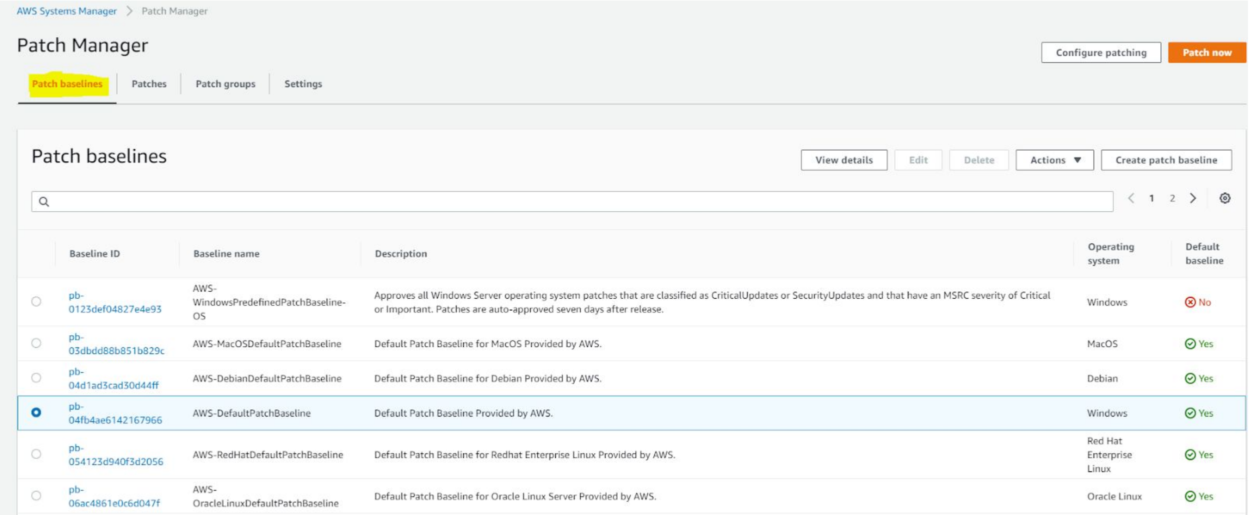
How it works

1. Use default patch baselines, or create your own
2. Organize instances into patch groups (optional)
3. Automate the patching schedule by using Maintenance Windows
4. Monitor patch status to ensure compliance

Using patch baselines:

A **patch baseline** defines which patches ought to and shouldn't be introduced on your instances. We can specify approved or rejected patches one after another. We can also create an auto-approval rule to specify that certain types of updates (for example, critical updates) should be automatically approved.

Patch Manager has a pre-characterized (default) patch standard:



Patch baselines

	Baseline ID	Baseline name	Description	Operating system	Default baseline
○	pb-0123def04827e4e93	AWS-WindowsPredefinedPatchBaseline-OS	Approves all Windows Server operating system patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of Critical or Important. Patches are auto-approved seven days after release.	Windows	⊗ No
○	pb-03dbdd88b851b829c	AWS-MacOSDefaultPatchBaseline	Default Patch Baseline for MacOS Provided by AWS.	MacOS	✓ Yes
○	pb-04d1ad3cad30d44ff	AWS-DebianDefaultPatchBaseline	Default Patch Baseline for Debian Provided by AWS.	Debian	✓ Yes
●	pb-04fb4ae6142167966	AWS-DefaultPatchBaseline	Default Patch Baseline Provided by AWS.	Windows	✓ Yes
○	pb-054123d940f3d2056	AWS-RedHatDefaultPatchBaseline	Default Patch Baseline for Redhat Enterprise Linux Provided by AWS.	Red Hat Enterprise Linux	✓ Yes
○	pb-06ac4861e0c6d047f	AWS-OracleLinuxDefaultPatchBaseline	Default Patch Baseline for Oracle Linux Server Provided by AWS.	Oracle Linux	✓ Yes

Creating a patch baseline:

We can make our own custom patch baselines, here we can pick which patches to auto-support by using the Operating system, Product name, Classification and Severity.

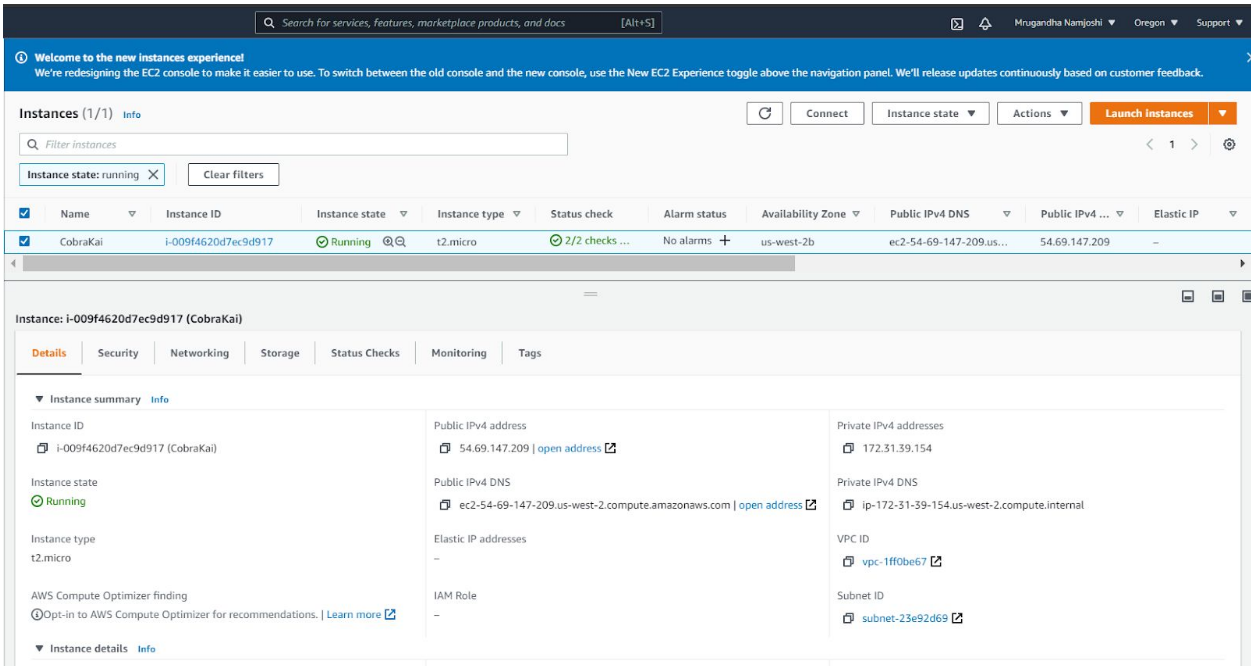
Patch groups:

Patch group is a discretionary method for characterizing which patch pattern should be utilized for what occurrences. For instance, one can establish patch groups for various conditions, for example, development, test, and production. One can likewise make essential and optional failover bunch groupings

Maintenance Windows:

AWS Systems Manager Maintenance Windows lets you characterize a schedule for when to perform possibly troublesome activities on your instances, for example, patching an operating system (OS), refreshing drivers, or installing software.

Created AWS EC2 instance:



Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi ▼
Oregon ▼
Support ▼

Welcome to the new instances experience!
We're redesigning the EC2 console to make it easier to use. To switch between the old console and the new console, use the New EC2 Experience toggle above the navigation panel. We'll release updates continuously based on customer feedback.

Instances (1/1) Info

Instance state: running ✕

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	CobraKai	i-009f4620d7ec9d917	✓ Running	t2.micro	✓ 2/2 checks ...	No alarms +	us-west-2b	ec2-54-69-147-209.us...	54.69.147.209	–

Instance: i-009f4620d7ec9d917 (CobraKai)

▼ Instance summary Info

Instance ID
i-009f4620d7ec9d917 (CobraKai)

Instance state
✓ Running

Instance type
t2.micro

AWS Compute Optimizer finding
ⓘOpt-in to AWS Compute Optimizer for recommendations. | Learn more

Public IPv4 address
54.69.147.209 | open address

Public IPv4 DNS
ec2-54-69-147-209.us-west-2.compute.amazonaws.com | open address

Elastic IP addresses
–

IAM Role
–

Private IPv4 addresses
172.31.39.154

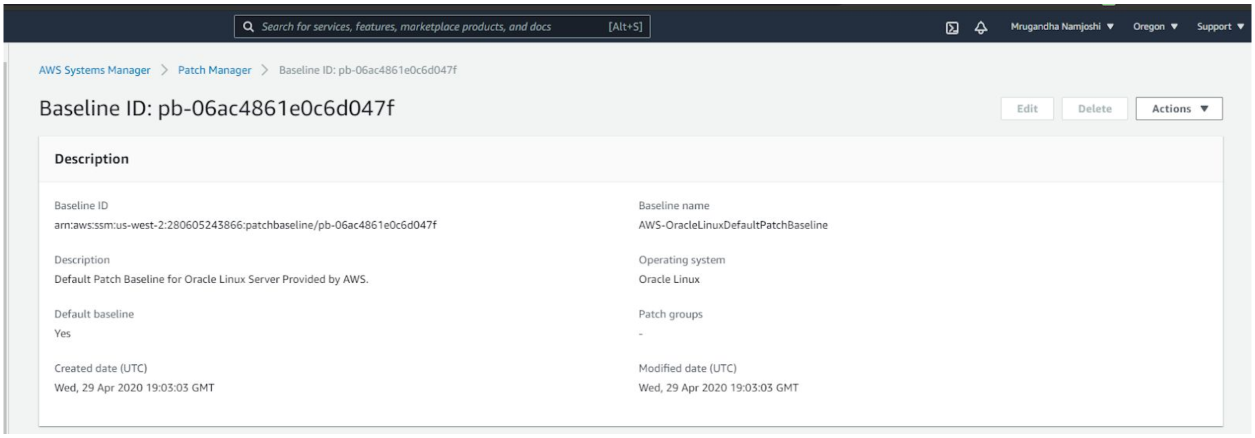
Private IPv4 DNS
ip-172-31-39-154.us-west-2.compute.internal

VPC ID
vpc-1ff0be67

Subnet ID
subnet-23e92d69

▼ Instance details Info

Baseline ID:


Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi ▼
Oregon ▼
Support ▼
AWS Systems Manager > Patch Manager > Baseline ID: pb-06ac4861e0c6d047f
Edit
Delete
Actions ▼

Baseline ID: pb-06ac4861e0c6d047f

Description

Baseline ID
arn:aws:ssm:us-west-2:280605243866:patchbaseline/pb-06ac4861e0c6d047f

Baseline name
AWS-OracleLinuxDefaultPatchBaseline

Description
Default Patch Baseline for Oracle Linux Server Provided by AWS.

Operating system
Oracle Linux

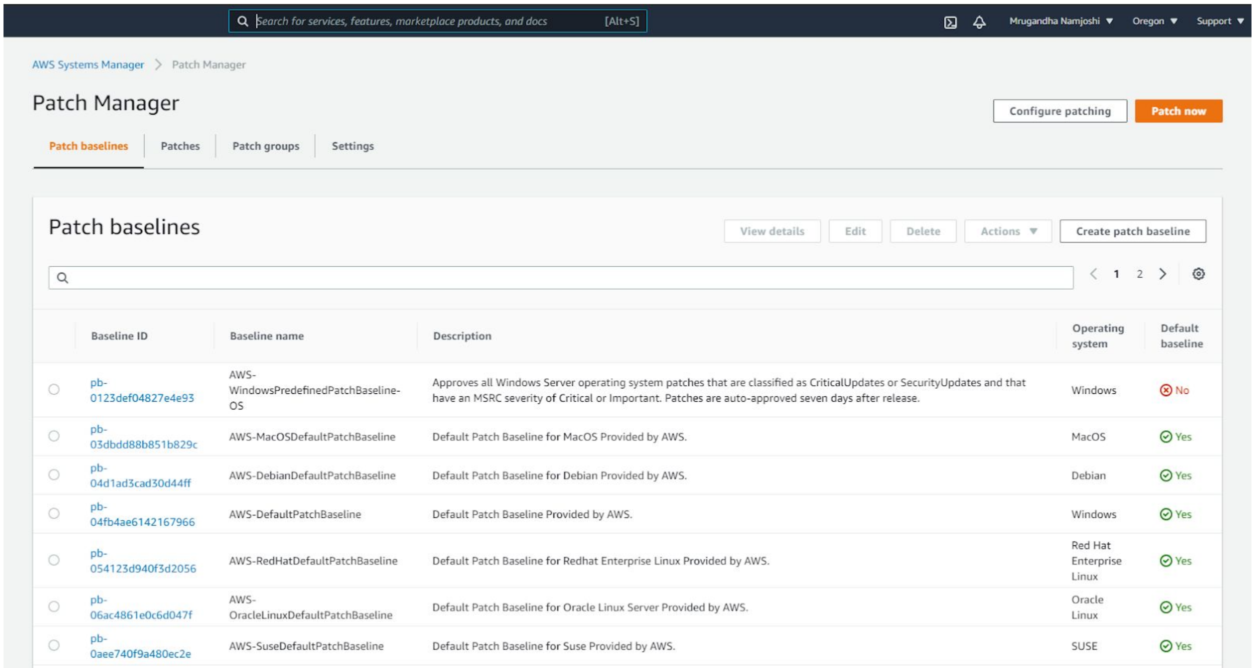
Default baseline
Yes

Patch groups
-

Created date (UTC)
Wed, 29 Apr 2020 19:03:03 GMT

Modified date (UTC)
Wed, 29 Apr 2020 19:03:03 GMT

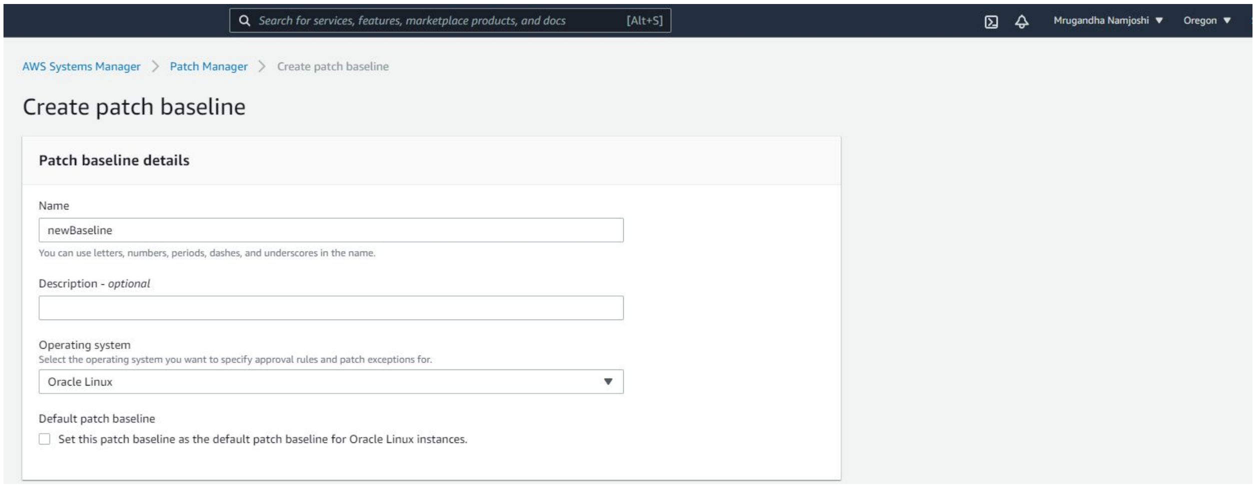
Patch Manager:



Patch baselines

	Baseline ID	Baseline name	Description	Operating system	Default baseline
○	pb-0123def04827e4e93	AWS-WindowsPredefinedPatchBaseline-OS	Approves all Windows Server operating system patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of Critical or Important. Patches are auto-approved seven days after release.	Windows	⊗ No
○	pb-03dbdd88b851b829c	AWS-MacOSDefaultPatchBaseline	Default Patch Baseline for MacOS Provided by AWS.	MacOS	✓ Yes
○	pb-04d1ad3cad30d44ff	AWS-DebianDefaultPatchBaseline	Default Patch Baseline for Debian Provided by AWS.	Debian	✓ Yes
○	pb-04fb4ae6142167966	AWS-DefaultPatchBaseline	Default Patch Baseline Provided by AWS.	Windows	✓ Yes
○	pb-054123d940f3d2056	AWS-RedHatDefaultPatchBaseline	Default Patch Baseline for Redhat Enterprise Linux Provided by AWS.	Red Hat Enterprise Linux	✓ Yes
○	pb-06ac4861e0c6d047f	AWS-OracleLinuxDefaultPatchBaseline	Default Patch Baseline for Oracle Linux Server Provided by AWS.	Oracle Linux	✓ Yes
○	pb-0aee740f9a480ec2e	AWS-SuseDefaultPatchBaseline	Default Patch Baseline for Suse Provided by AWS.	SUSE	✓ Yes

Creating a baseline


Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi
Oregon
AWS Systems Manager > Patch Manager > Create patch baseline

Create patch baseline

Patch baseline details

Name: newBaseline

You can use letters, numbers, periods, dashes, and underscores in the name.

Description - *optional*

Operating system

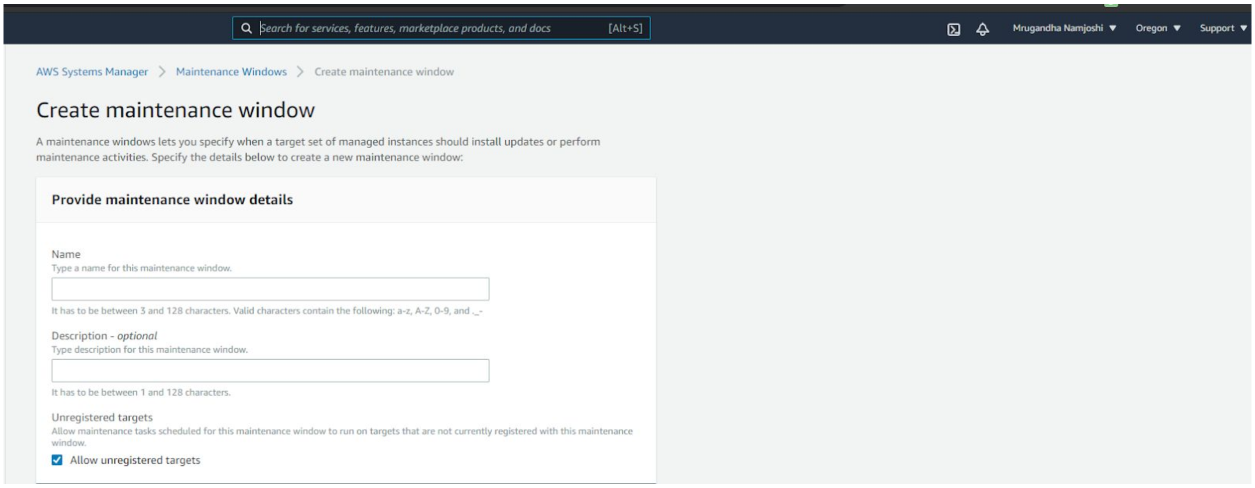
Select the operating system you want to specify approval rules and patch exceptions for.

Oracle Linux

Default patch baseline

□ Set this patch baseline as the default patch baseline for Oracle Linux instances.

Creating Maintenance Window:


Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi
Oregon
Support
AWS Systems Manager > Maintenance Windows > Create maintenance window

Create maintenance window

A maintenance windows lets you specify when a target set of managed instances should install updates or perform maintenance activities. Specify the details below to create a new maintenance window:

Provide maintenance window details

Name

Type a name for this maintenance window.

It has to be between 3 and 128 characters. Valid characters contain the following: a-z, A-Z, 0-9, and ._-

Description - *optional*

Type description for this maintenance window.

It has to be between 1 and 128 characters.

Unregistered targets

Allow maintenance tasks scheduled for this maintenance window to run on targets that are not currently registered with this maintenance window.

☑ Allow unregistered targets

Problem 2: DDoS Attack Prevention

Distributed denial-of-service Attack:

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Recommendation:

In the case of any DDoS attacks by the rivals, AWS shield advanced will help our application to withstand that attack. AWS shield advanced provides customized detection based on the traffic patterns in our protected elastic IP address. AWS Shield Advanced accompanies DDoS cost insurance, to protect against scaling charges coming about because of DDoS-related utilization spikes.. It is integrated with AWS WAF, that is a web-application firewall.

AWS shield advanced:

Tailored detection based on application traffic patterns:

AWS Shield Advanced provides customized detection based on traffic patterns to your protected Elastic IP address, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator or Amazon Route 53 resources. Using additional region- and resource-specific monitoring techniques, AWS Shield Advanced detects and alerts you of smaller DDoS attacks.

Advanced attack mitigation:

AWS Shield Advanced provides more sophisticated automatic mitigations for attacks targeting your applications running on protected Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 resources.

Elastic Load Balancing:

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, containers, and IP addresses, and multiple Availability Zones, which minimizes the risk of overloading a single resource.

DNS Route 53:

One of the most common targets of DDoS attacks is the Domain Name System (DNS). Amazon Route 53 is a highly available and scalable DNS service designed to route end users to infrastructure running inside or outside of AWS. Route 53 makes it possible to manage traffic globally through a variety of routing types and provides out-of-the box shuffle sharding and Anycast routing capabilities to protect domain names from DNS-based DDoS attacks.

Advanced DDoS protection

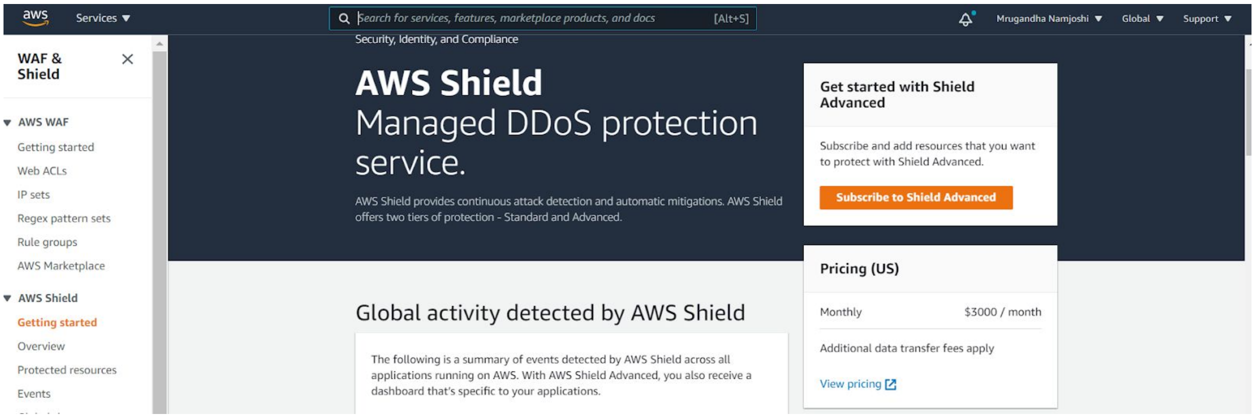
Get additional DDoS protection and attack mitigation

24/7 DDoS response team

During an attack, get help with mitigation from a team of DDoS experts

Visibility and reporting

Monitor and analyze DDoS events with metrics and detailed reports



Security, Identity, and Compliance

AWS Shield

Managed DDoS protection service.

AWS Shield provides continuous attack detection and automatic mitigations. AWS Shield offers two tiers of protection - Standard and Advanced.

Get started with Shield Advanced

Subscribe and add resources that you want to protect with Shield Advanced.

Pricing (US)

Monthly	$3000 / month

Additional data transfer fees apply

Global activity detected by AWS Shield

The following is a summary of events detected by AWS Shield across all applications running on AWS. With AWS Shield Advanced, you also receive a dashboard that's specific to your applications.

Problem 3: Slow streaming, Downloads and order processing:

Recommendation:

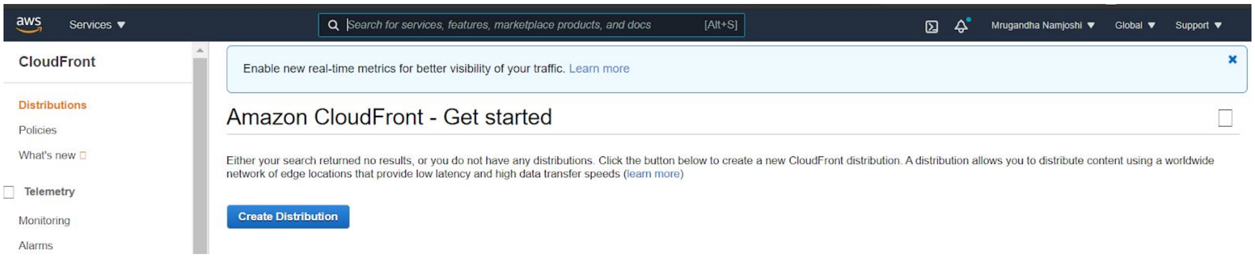
In the event of slow streaming and downloading of data and videos, Amazon CloudFront, a fast Content Delivery Network (CDN) service, helps in securely delivering data, videos and applications and APIs to customers globally with low latency and high transfer speed.Customers will have easy access to the data without any interruptions. AWS CloudFront works smoothly with other services like Amazon S3 and Elastic Load Balancing.

Amazon CloudFront:

Amazon CloudFront distributes traffic across multiple edge locations and filters requests to ensure that only valid HTTP(S) requests will be forwarded to backend hosts. CloudFront also supports geo-blocking, which you can use to prevent requests from particular geographic locations from being served.

Amazon CloudFront Key Features:

- Faster Performance. Network optimizations for optimal performance.
- Security protection against Network and Application Layer Attacks.
- Programmable and DevOps Friendly full-featured APIs and DevOps Tools.
- Cost effective pay-as-you-go publicly available pricing and discounted pricing.

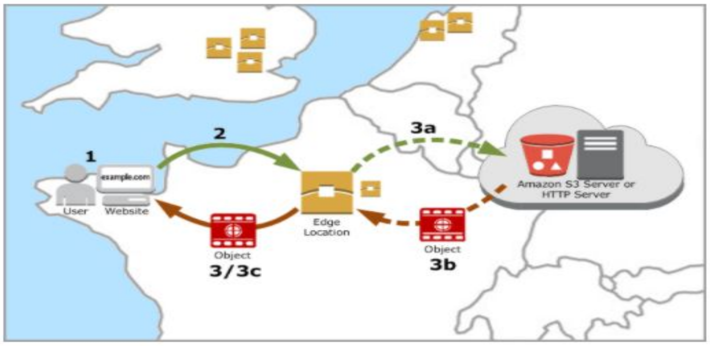


Enable new real-time metrics for better visibility of your traffic. Learn more

Amazon CloudFront - Get started

Either your search returned no results, or you do not have any distributions. Click the button below to create a new CloudFront distribution. A distribution allows you to distribute content using a worldwide network of edge locations that provide low latency and high data transfer speeds (learn more)

CloudFront delivers content to your users:



Problem 4: Account Permission

Account Permission Strategy:

It is an approach intended to offer approval to various clients that empowers them to get to explicit assets on the organization, for example, information records, applications, printers and scanners.

Recommendation:

Currently every user group has the ability to run the privileged commands on the web server if they want to, but that is highly insecure and thus we should have a good account permission strategy. Use of AWS Identity & Access Management (IAM) will allow us to manage access to AWS services and resources securely.

AWS Identity & Access Management (IAM):

AWS Identity and Access Management, helps you set up users and groups, and shows you how to protect your resources with access control policies. Also shows how to connect to other identity services to grant external users access to your AWS resources.

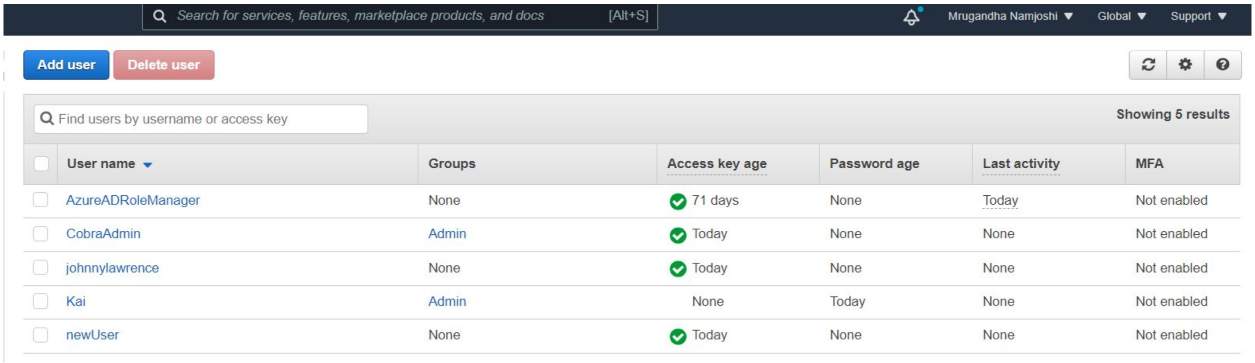
Working of IAM for securing resources on AWS:

Using IAM, we can create and manage several user groups and according to their different user roles, they will be given access to various services in AWS.

IAM allows us to:

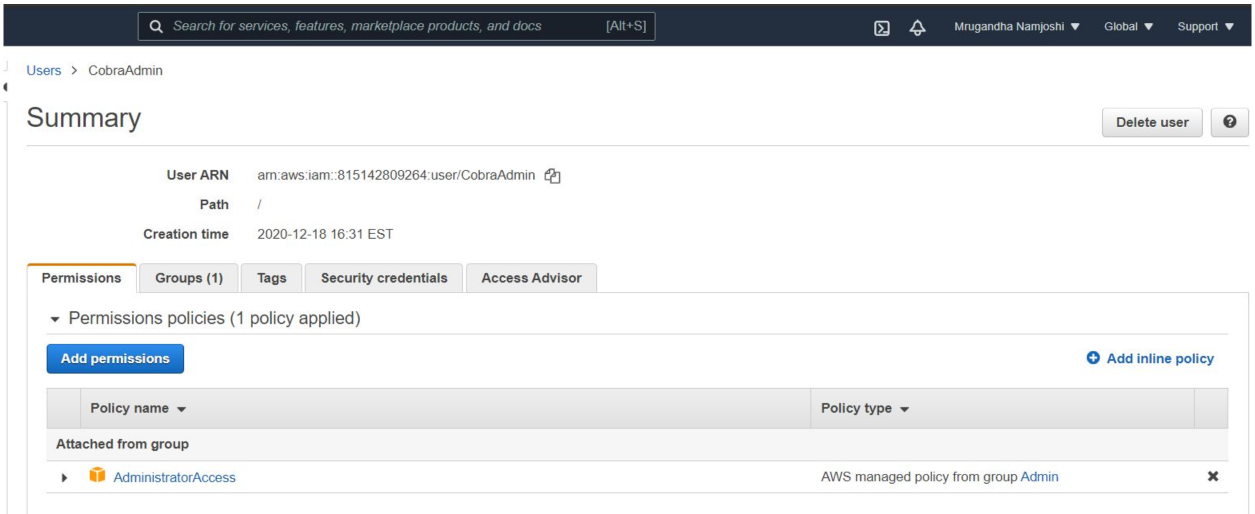
- **Manage IAM users and their access** – We can create users in IAM, assign them individual security credentials (in other words, access keys, passwords, and multi-factor authentication devices), or request temporary security credentials to provide users access to AWS services and resources.
- **Manage IAM roles and their permissions** – We can create roles in IAM and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. We can also define which entity is allowed to assume the role.
- **Manage federated users and their permissions –** You can enable identity federation to allow existing identities (users, groups, and roles) in your enterprise to access the AWS Management Console, call AWS APIs, and access resources, without the need to create an IAM user for each identity.

Creating a User:


Search for services, features, marketplace products, and docs
[Alt+S]
Mrugandha Namjoshi ▼
Global ▼
Support ▼
Add user
Delete user
Find users by username or access key
Showing 5 results

User name	Groups	Access key age	Password age	Last activity	MFA
AzureADRoleManager	None	✓ 71 days	None	Today	Not enabled
CobraAdmin	Admin	✓ Today	None	None	Not enabled
johnnylawrence	None	✓ Today	None	None	Not enabled
Kai	Admin	None	Today	None	Not enabled
newUser	None	✓ Today	None	None	Not enabled

Adding Permissions:



Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi ▼
Global ▼
Support ▼
Users > CobraAdmin

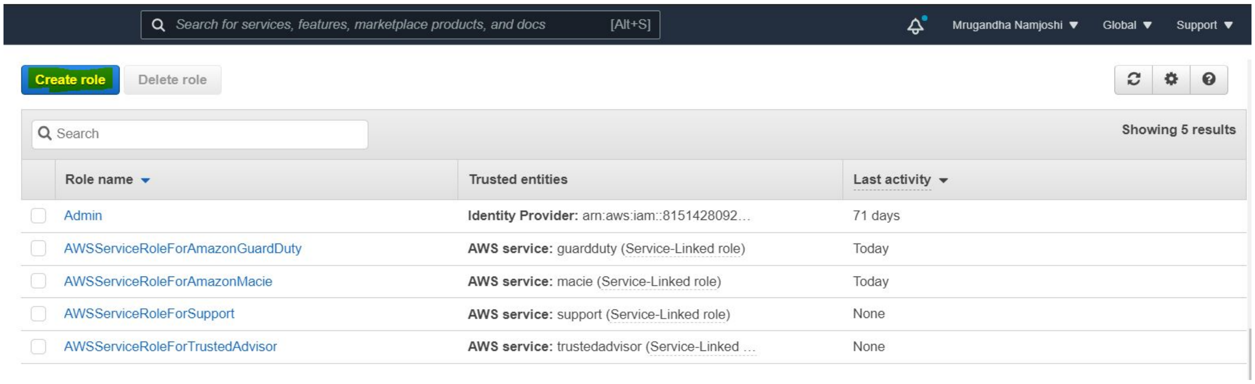
Summary

User ARN	arn:aws:iam::815142809264:user/CobraAdmin
Path	/
Creation time	2020-12-18 16:31 EST

Permissions policies (1 policy applied)

Policy name	Policy type	
Attached from group		
AdministratorAccess	AWS managed policy from group Admin	✖

Roles can be created:

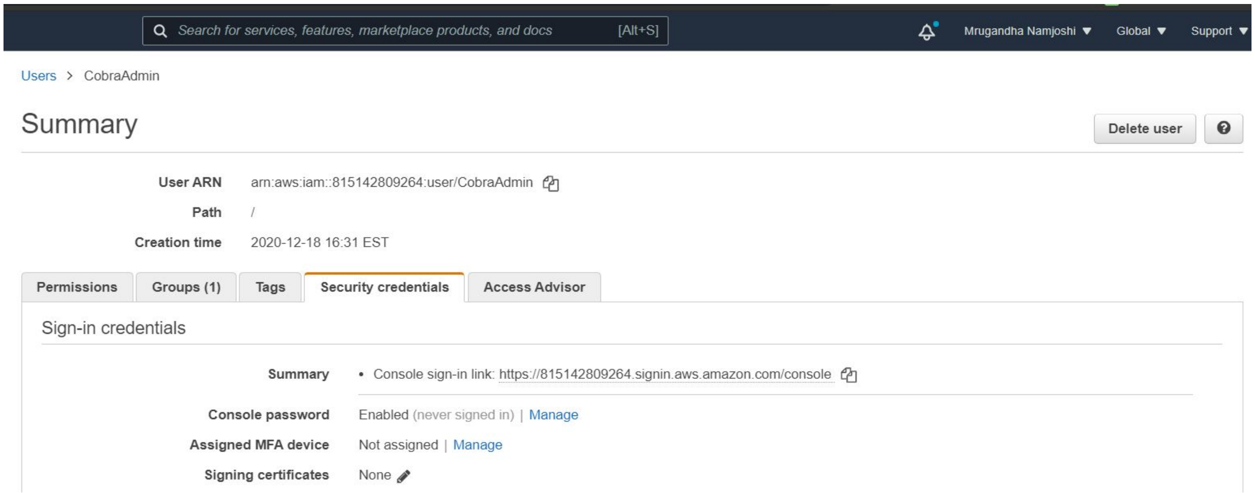


Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi ▼
Global ▼
Support ▼
Create role
Delete role
Search

Showing 5 results

	Role name	Trusted entities	Last activity
□	Admin	**Identity Provider:** arn:aws:iam::8151428092…	71 days
□	AWSServiceRoleForAmazonGuardDuty	**AWS service:** guardduty (Service-Linked role)	Today
□	AWSServiceRoleForAmazonMacie	**AWS service:** macie (Service-Linked role)	Today
□	AWSServiceRoleForSupport	**AWS service:** support (Service-Linked role)	None
□	AWSServiceRoleForTrustedAdvisor	**AWS service:** trustedadvisor (Service-Linked …	None

Setting up MFA for IAM user:



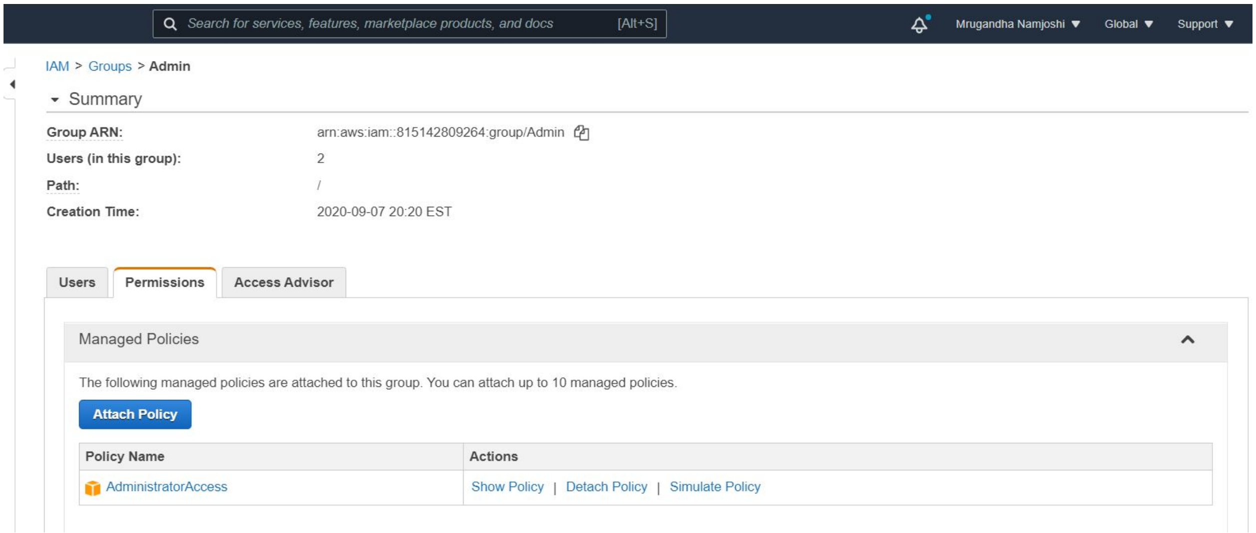
Summary

User ARN	arn:aws:iam::815142809264:user/CobraAdmin
Path	/
Creation time	2020-12-18 16:31 EST

Sign-in credentials

Summary	• Console sign-in link: https://815142809264.signin.aws.amazon.com/console
Console password	Enabled (never signed in) | Manage
Assigned MFA device	Not assigned | Manage
Signing certificates	None

Admin Policies:



Summary

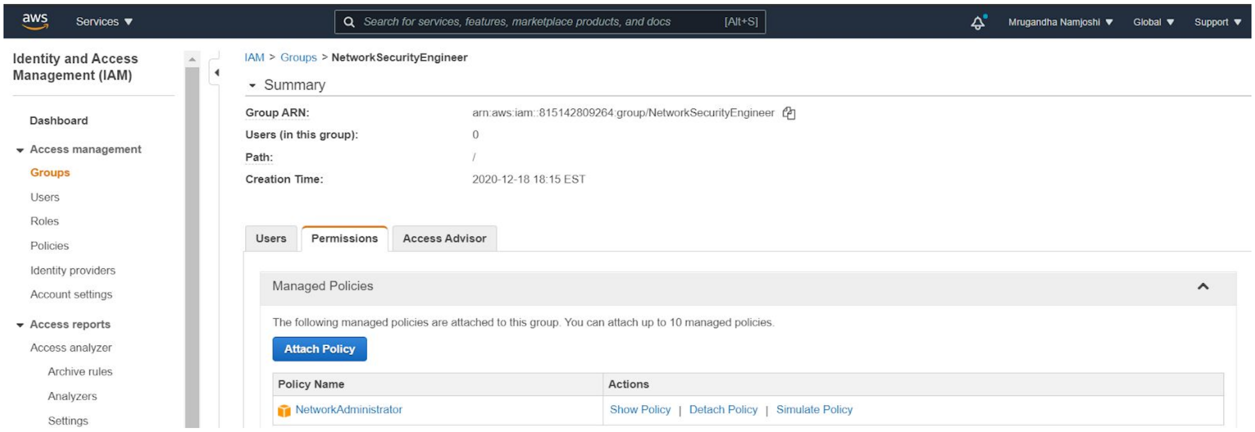
Group ARN:	arn:aws:iam::815142809264:group/Admin
Users (in this group):	2
Path:	/
Creation Time:	2020-09-07 20:20 EST

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy

Network Engineer Policies:



Summary

Group ARN:	arn:aws:iam::815142809264:group/NetworkSecurityEngineer
Users (in this group):	0
Path:	/
Creation Time:	2020-12-18 18:15 EST

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

Policy Name	Actions
NetworkAdministrator	Show Policy | Detach Policy | Simulate Policy

Problem 5: Backup Strategy

Why do we need a backup Strategy-

Backup Strategy is storing copies of data so that, in the case of loss or damage of the original data we can utilize the extra copies of data that is stored in backup.

Recommendation:

In case of break-down in the VPC(Virtual Private Cloud), **AWS Backup** service will be used.

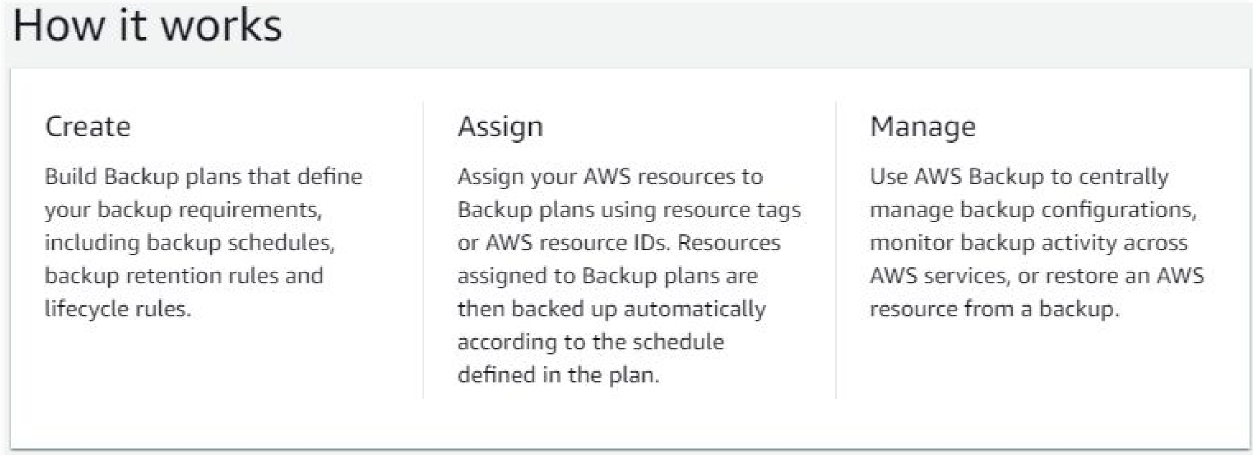
AWS Backup:

AWS Backup, is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services.It helps in automating the backup process and saves time and money.

Benefits of AWS Backup:

- Centrally manage backups
- Automate backup processes
- Improve backup compliance

As Stated by AWS document-



How it works

Create

Build Backup plans that define your backup requirements, including backup schedules, backup retention rules and lifecycle rules.

Assign

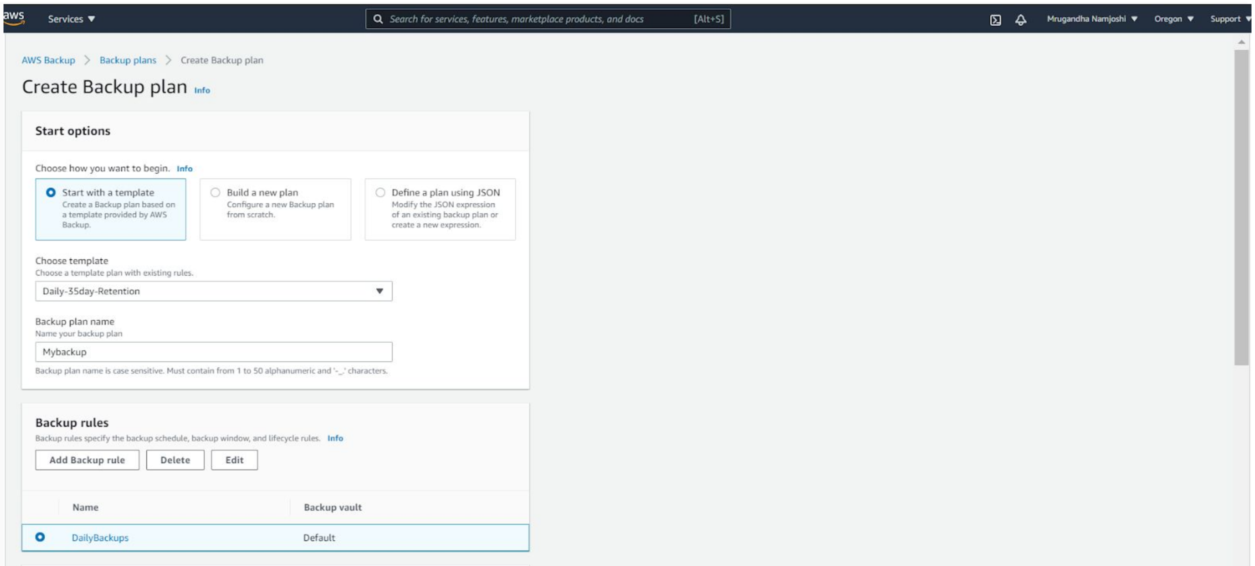
Assign your AWS resources to Backup plans using resource tags or AWS resource IDs. Resources assigned to Backup plans are then backed up automatically according to the schedule defined in the plan.

Manage

Use AWS Backup to centrally manage backup configurations, monitor backup activity across AWS services, or restore an AWS resource from a backup.

Creating a Backup Plan:

- AWS Console -> AWS Backup -> Create Backup plan. In which we can define rules, retention period, region, and other options as per need


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi ▼
Oregon ▼
Support ▼

AWS Backup > Backup plans > Create Backup plan

Create Backup plan Info

Start options

Choose how you want to begin. Info

● Start with a template
Create a Backup plan based on a template provided by AWS Backup.

○ Build a new plan
Configure a new Backup plan from scratch.

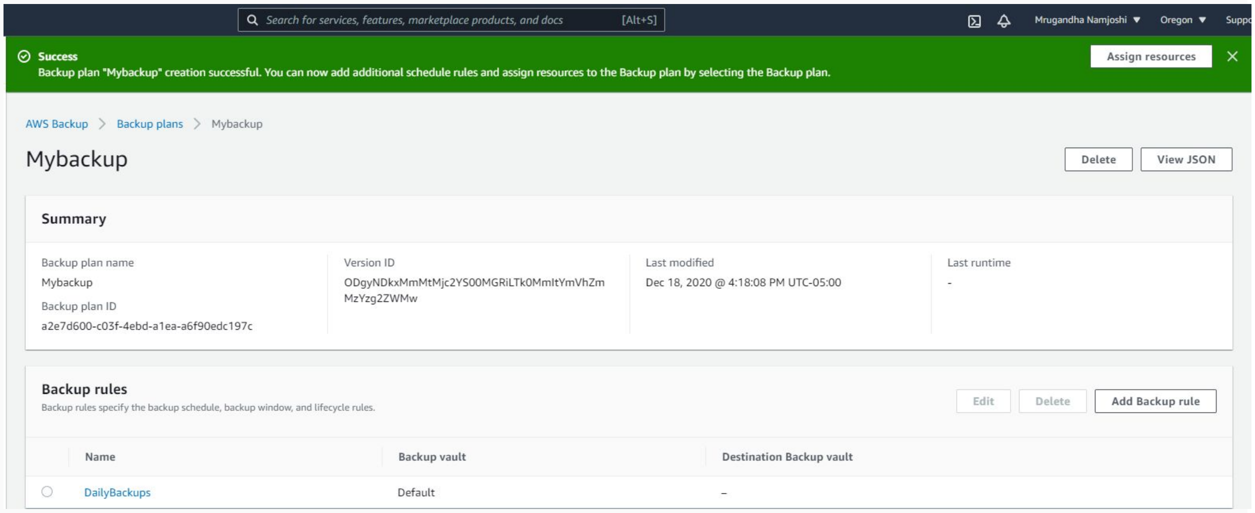
○ Define a plan using JSON
Modify the JSON expression of an existing backup plan or create a new expression.

Choose template
Choose a template plan with existing rules.
Daily-35day-Retention ▼

Backup plan name
Name your backup plan
Mybackup
Backup plan name is case sensitive. Must contain from 1 to 50 alphanumeric and '-_.' characters.

Backup rules
Backup rules specify the backup schedule, backup window, and lifecycle rules. Info

	Name	Backup vault
●	DailyBackups	Default


Search for services, features, marketplace products, and docs [Alt+S]
Mrugandha Namjoshi ▼
Oregon ▼
Supp

Success
Backup plan "Mybackup" creation successful. You can now add additional schedule rules and assign resources to the Backup plan by selecting the Backup plan.

AWS Backup > Backup plans > Mybackup

Mybackup

Summary

Backup plan name
Mybackup

Backup plan ID
a2e7d600-c03f-4ebd-a1ea-a6f90edc197c

Version ID
ODgyNDkxMmMtMjc2YS00MGRiLTk0MmItYmVhZmMzYzg2ZWMw

Last modified
Dec 18, 2020 @ 4:18:08 PM UTC-05:00

Last runtime
-

Backup rules
Backup rules specify the backup schedule, backup window, and lifecycle rules.

	Name	Backup vault	Destination Backup vault
○	DailyBackups	Default	-

Problem 6: Personal Information

Recommendation:

In order to keep the sensitive information of the users safe, **Amazon Macie service** is used. It uses machine Learning and pattern learning to discover and protect the user data.Amazon Macie is linked to the S3 buckets, where it applies techniques to these buckets in order to identify and alert about any sensitive data, such as personally identifiable information (PII).

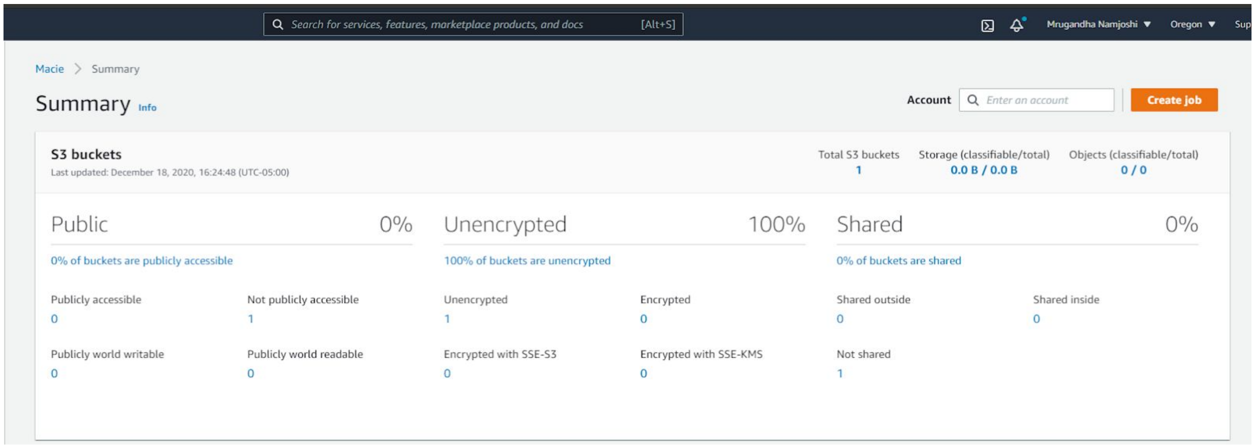
Amazon Macie features:

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.

Features of Amazon Macie:

- Detailed and actionable security and sensitive data discovery findings
- Custom-defined sensitive data types
- One-click deployment with no upfront data source integration
- Multi-account support and integration with AWS Organizations
- Fully managed sensitive data types

After enabling Amazon Macie:



Summary

S3 buckets
Last updated: December 18, 2020, 16:24:48 (UTC-05:00)

Total S3 buckets	Storage (classifiable/total)	Objects (classifiable/total)
1	0.0 B / 0.0 B	0 / 0

Public 0%
0% of buckets are publicly accessible

Publicly accessible	Not publicly accessible
0	1
Publicly world writable	**Publicly world readable**
0	0

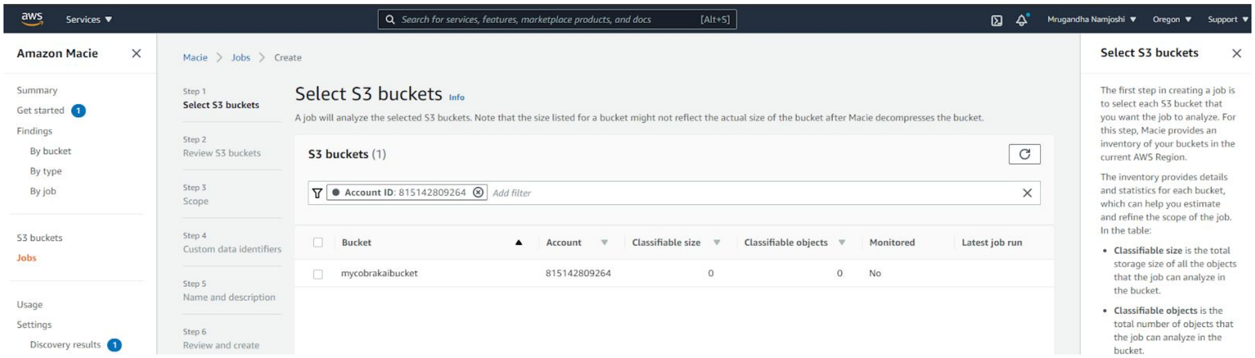
Unencrypted 100%
100% of buckets are unencrypted

Unencrypted	Encrypted
1	0
Encrypted with SSE-S3	**Encrypted with SSE-KMS**
0	0

Shared 0%
0% of buckets are shared

Shared outside	Shared inside
0	0
Not shared	
1	

S3 Bucket:



Select S3 buckets

A job will analyze the selected S3 buckets. Note that the size listed for a bucket might not reflect the actual size of the bucket after Macie decompresses the bucket.

S3 buckets (1)

Account ID: 815142809264

□	Bucket ▲	Account ▼	Classifiable size ▼	Classifiable objects ▼	Monitored	Latest job run
□	mycobrakaibucket	815142809264	0	0	No	

Select S3 buckets

The first step in creating a job is to select each S3 bucket that you want the job to analyze. For this step, Macie provides an inventory of your buckets in the current AWS Region.

The inventory provides details and statistics for each bucket, which can help you estimate and refine the scope of the job. In the table:

- **Classifiable size** is the total storage size of all the objects that the job can analyze in the bucket.
- **Classifiable objects** is the total number of objects that the job can analyze in the bucket.