Intro to Cloud Security

Show Split View | Cloud Details | Awards | Help

Learn fundamental concepts regarding securing a cloud environment.

✖

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Loading... *Loading...* *Loading...* *Loading...*

94%

Task 1 ✓ Introduction

Task 2 ✓ Architectural Concepts of Cloud

Task 3 ✓ Cloud Security Concepts

Task 4 ✓ Cloud Security Risks Concerning Deployment Models

Task 5 ✓ Security Through Access Management

Task 6 ✓ Security Through Policies

Task 7 ✓ Security Through Network Management

Task 8 ✓ Security Through Storage Management

Task 9 ✓ Cloud Security - Some Additional Concepts

Disaster Recovery (DR) & Backup

Cloud is considered an excellent source for establishing Disaster Recovery and Backup sites. In cloud computing environments, there is a famous terminology known as **Cloud Disaster Recovery (CDR)**, a combination of approaches, tools & techniques that ensures backup data, resources and other applications on cloud infrastructure. In case of any disaster, cloud service providers provide backups of on-premises environments to ensure the regular continuity of business operations. Following are the essential concepts in terms of Disaster & Recovery in cloud computing through the following three approaches:

- **Cold DR**: This is the most straightforward approach and inexpensive but has the largest RTO (Recovery Time Objective). It entails storing data and saving images & snapshots of machines. All snapshots must be recovered to resume business operations in a disaster situation.
- **Warm DR**: It works on the principle of near real-time synchronisation of actual data and applications with disaster sites. A copy of all data and services is being maintained at the DR setup, hosted on a cloud environment. This data is just being kept as a backup to resume business operations in a disaster scenario. When a disaster occurs, the DR site is configured to resume operations. RTO, in this case, is the time required for configuring the DR site to become operational.
- **Hot DR**: It has practically zero RTO but is the most expensive. In this approach, the actual and DR sites work in parallel and share the workload through load balancers. In case of disaster, all workload is shifted to the DR site.

Security through Monitoring & Logging

It is accurate to say that monitoring and logging are the hallmarks of maintaining security, and cloud computing is no exception. Nowadays, cloud service providers provide excellent approaches to logging and monitoring. Customers can take advantage of this option to keep an oversight on all the operations of their cloud environment. Following are some generic logging and monitoring approaches in a cloud computing environment:

- **Real-time Logging**: Almost all cloud service providers monitor and log all identities and resources.
- **Monitoring & Logging of API Calls**: All cloud instances have the provision for recording API calls made to cloud infrastructure. Typical logs include the source IP address of the user or service, time, etc.
- **Credential Reports**: Another essential thing that cloud service provider monitors are user accounts logs. Common logged factors include user account, account last used date, password last change data and password last used date, etc.

Monitoring & Logging into AWS

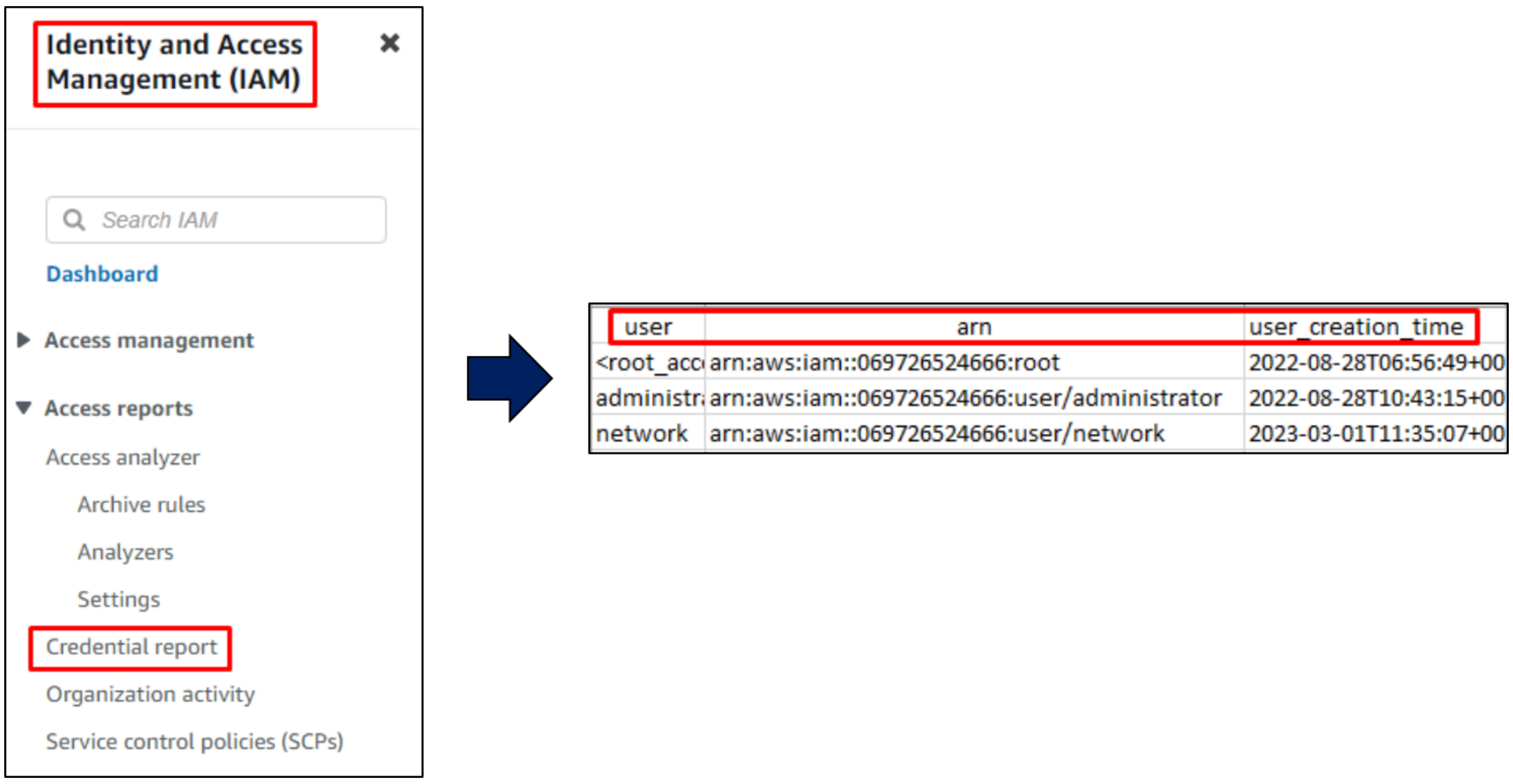
The following components manage monitoring and logging in AWS:

- Identity & Access Management: Basic logging features related to access management, e.g. logs credential reports of user accounts.
- CloudTrail: Logs all API calls made to AWS resources.
- CloudWatch: Monitors the entire cloud infra and informs about applications status performance changes, ensuring better resource utilisation.
- GuardDuty: Ensures continuous monitoring of malicious activity and unauthorised behaviour.

Practical Exercise

In this exercise, we will generate Credential Report for the AWS account. IAM provides an excellent feature of generating a credential report that lists all users and the status of their credentials, including passwords, Multi-Factor Authentication Status, usage & change history.

- Login to your AWS account by visiting `console.aws.amazon.com` & Navigate to `IAM` in the services menu.
- In the navigation pane, choose `Credential Report` & click "Download Report" on the next page.



user	arn	user_creation_time
<root_acc	arn:aws:iam::069726524666:root	2022-08-28T06:56:49+00
administr	arn:aws:iam::069726524666:user/administrator	2022-08-28T10:43:15+00
network	arn:aws:iam::069726524666:user/network	2023-03-01T11:35:07+00

Click to enlarge the image.

- The report will be downloaded in CSV format and contain various vital fields, such as `password_last_used, password_last_changed, user_creation_time, etc` .

Updates & Patching

Updating & patching is an essential parts of the calculus of the entire security paradigm. In cloud computing environments, “Automated & Scheduled Patch Management” ensures that security and other related updates are routinely applied.

Patch Management in AWS

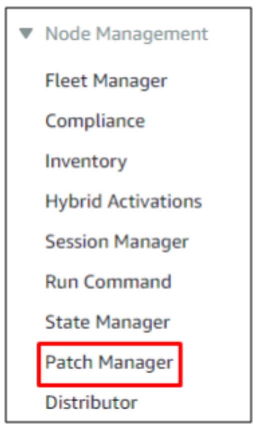
Patch management in AWS is managed by a component called “Systems Manager”. Patch Management in AWS has the following concepts:

- Patch manager ensures automatic & scheduled updating of cloud resources and can be used to update operating systems and applications.
- Provides scanning option to scan complete infrastructure regarding missing patches.

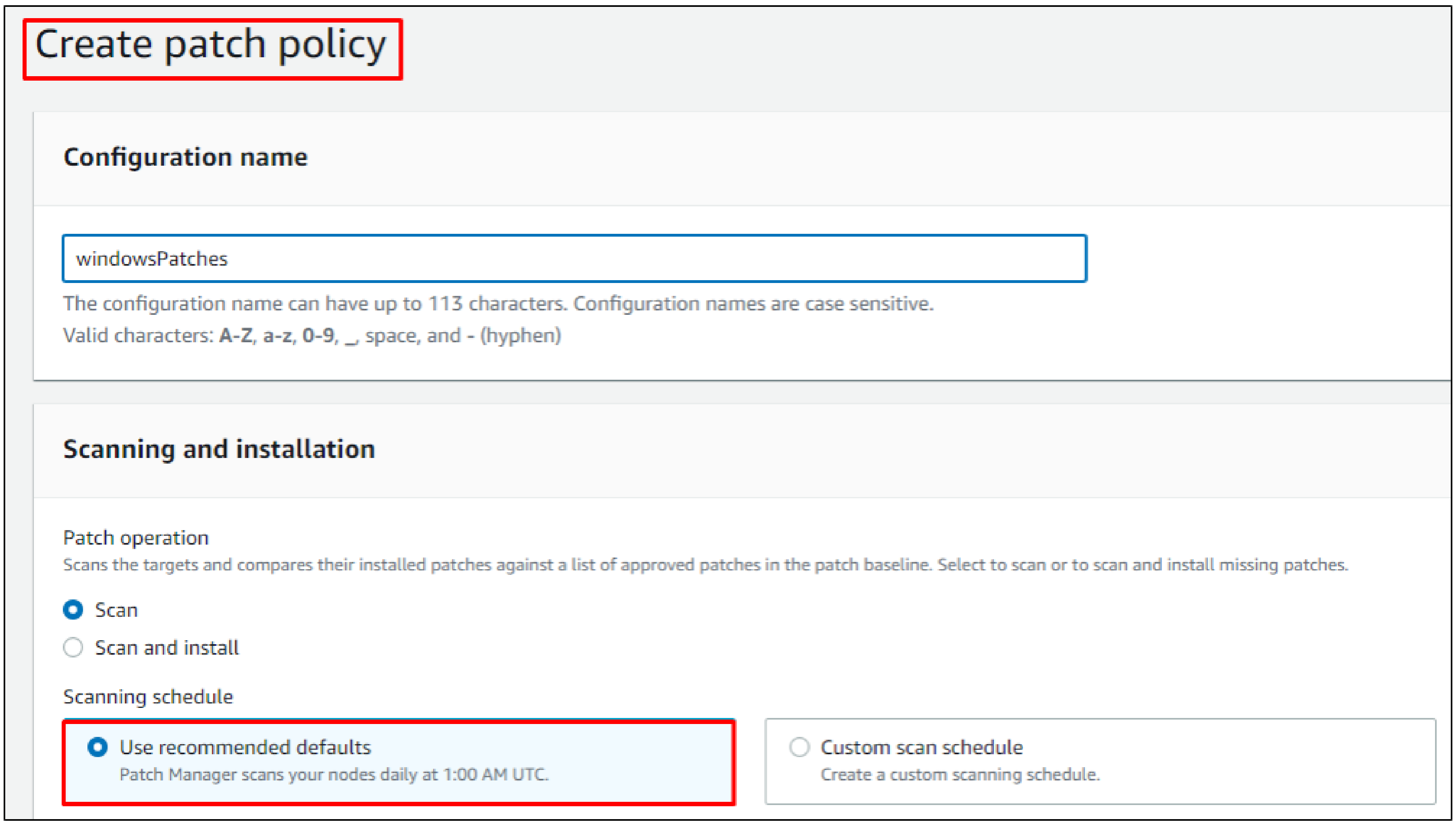
Practical Exercise

In this exercise, we will gain an understanding of AWS Patch Manager.

- Log in to your AWS account & Open `Systems Manager` from the services menu.
- Open `Patch Manager` in the left window under Node Management and click on `Create Patch Policy` .



- There are two types of patching mechanisms, i.e., Patches without a Schedule and Scheduled Patching.



Create patch policy

Configuration name

windowsPatches

The configuration name can have up to 113 characters. Configuration names are case sensitive.
Valid characters: **A-Z, a-z, 0-9, _**, space, and **-** (hyphen)

Scanning and installation

Patch operation
Scans the targets and compares their installed patches against a list of approved patches in the patch baseline. Select to scan or to scan and install missing patches.

● Scan
○ Scan and install

Scanning schedule

● Use recommended defaults
Patch Manager scans your nodes daily at 1:00 AM UTC.

○ Custom scan schedule
Create a custom scanning schedule.

- We will enter the configuration name and select options like **scan** or **scan and install patches** immediately. In the next section, we must enter all the necessary details for patching.

Answer the questions below

Is it a good practice to keep Disaster Recovery Backups of a server in the same vicinity or data centre (yea/nay)?