

Sprint 3 Requirements: Enhanced Security with AWS Cloud HSM

Team Name: Data Defenders

Team Leader: Takala

Project Manager: Awa

Technical Lead: Jaelin

Technical Lead Support: Mariana

Technical Documentation:

CloudHSM Deployment & Configuration

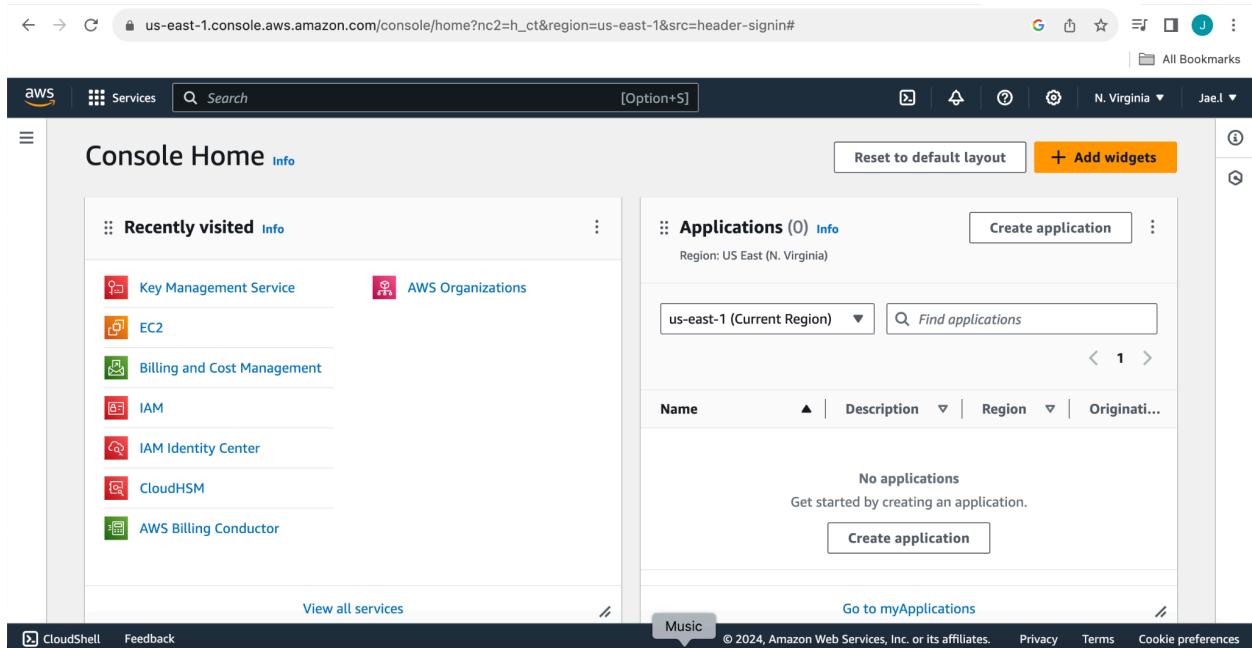
1. **Deploying an AWS CloudHSM Cluster:**

- Choose appropriate CloudHSM instance type and configuration.
- Create and initialize the CloudHSM cluster.
- Configure networking and security groups.
- Set up high availability and fault tolerance.

CloudHSM Cluster Deployment and Configuration

Creating a Cluster

1. **Sign in to the AWS Management Console:** Go to the AWS Management Console and sign in to your AWS account. <https://console.aws.amazon.com/>



2. **Open CloudHSM in the Console:** Navigate to the CloudHSM service from the list of available AWS services.

The screenshot shows the AWS CloudHSM search results. The search bar at the top contains the query 'cloudhsm'. Below the search bar, there's a sidebar with recent services like Key Management, IAM Identity Center, IAM, EC2, and CloudWatch Metrics. The main content area is titled 'Search results for 'cloudhsm'' and shows a 'Services' section with one result: 'CloudHSM' (Managed Hardware Security Modules in the Cloud). Below that is a 'Features' section with three items: 'Backups' (CloudHSM feature), 'Clusters' (CloudHSM feature), and 'Amazon VPC Lattice' (VPC feature). A blue sidebar on the right provides information about CloudHSM, including how to generate a custom key and a link to the AWS CloudHSM User Guide.

3. **Create a Cluster:** Click on "Create cluster" to start the process of creating a new cluster.

The screenshot shows the AWS CloudHSM home page. The main title is 'AWS CloudHSM' with the subtitle 'Managed hardware security module (HSM) in the AWS Cloud'. Below the title, there's a paragraph about CloudHSM providing cloud-based HSMs for generating encryption keys. On the right side, there's a large call-to-action button labeled 'Create CloudHSM cluster' with the sub-instruction 'Begin using AWS Cloud HSM. Learn more'. Below this button is a 'Pricing' section.

4. **Configure the cluster:**

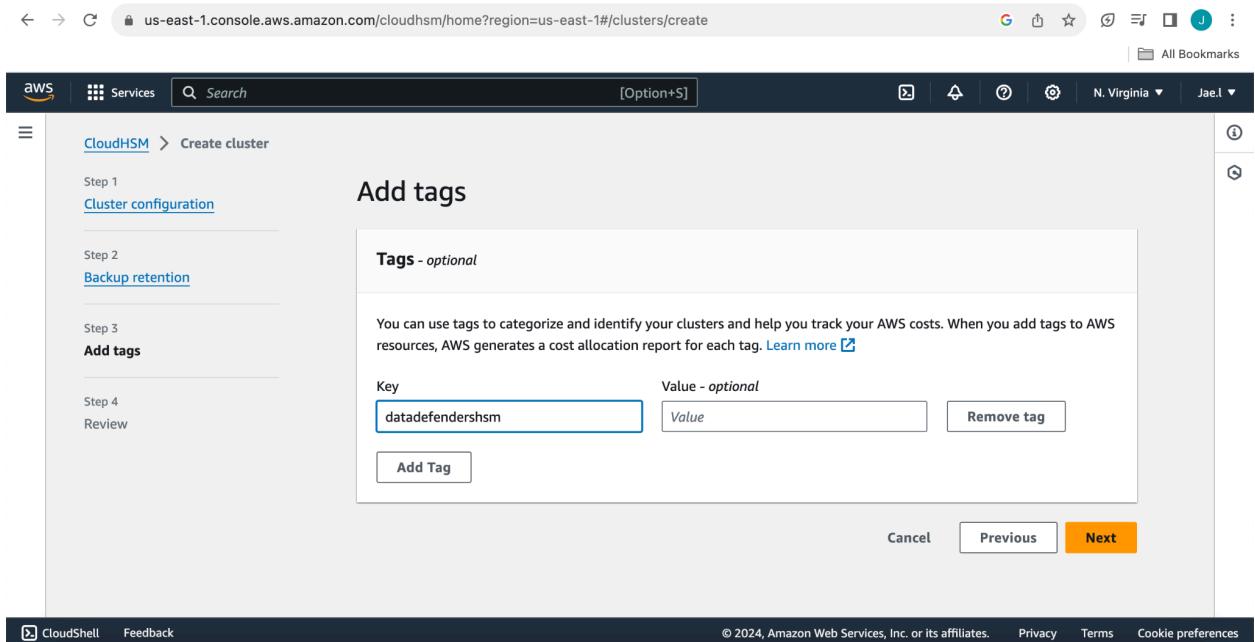
- Select the appropriate subnet and VPC (Virtual Private Cloud) for your HSMs.
- Choose the AWS Region where you want to create the cluster.

The screenshot shows the AWS CloudHSM cluster creation interface. The top navigation bar includes the AWS logo, services menu, search bar, and region selection (N. Virginia). The main content area is titled "VPC" and displays a dropdown menu for selecting a VPC, currently set to "Default VPC ('vpc-071d8ba7a3685b6f8')". Below this is a link to "Create a new VPC". A section titled "Availability Zone(s)" contains two rows of dropdown menus for selecting subnets. The first row shows "us-east-1a" with "subnet-0a608d19e6c29c7a9" and "us-east-1b" with "subnet-0364ed27644866914". The second row shows "us-east-1c" with "Select a subnet..." and "us-east-1d" with "Select a subnet...". On the left sidebar, steps 2 through 4 are listed: "Backup retention", "Add tags", and "Review". The bottom navigation bar includes CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

- Specify the "Cluster Backup Configuration" (Enable automatic backups or not).
- Specify the "Cluster Retention Period" : A 10 day backup retention period was selected

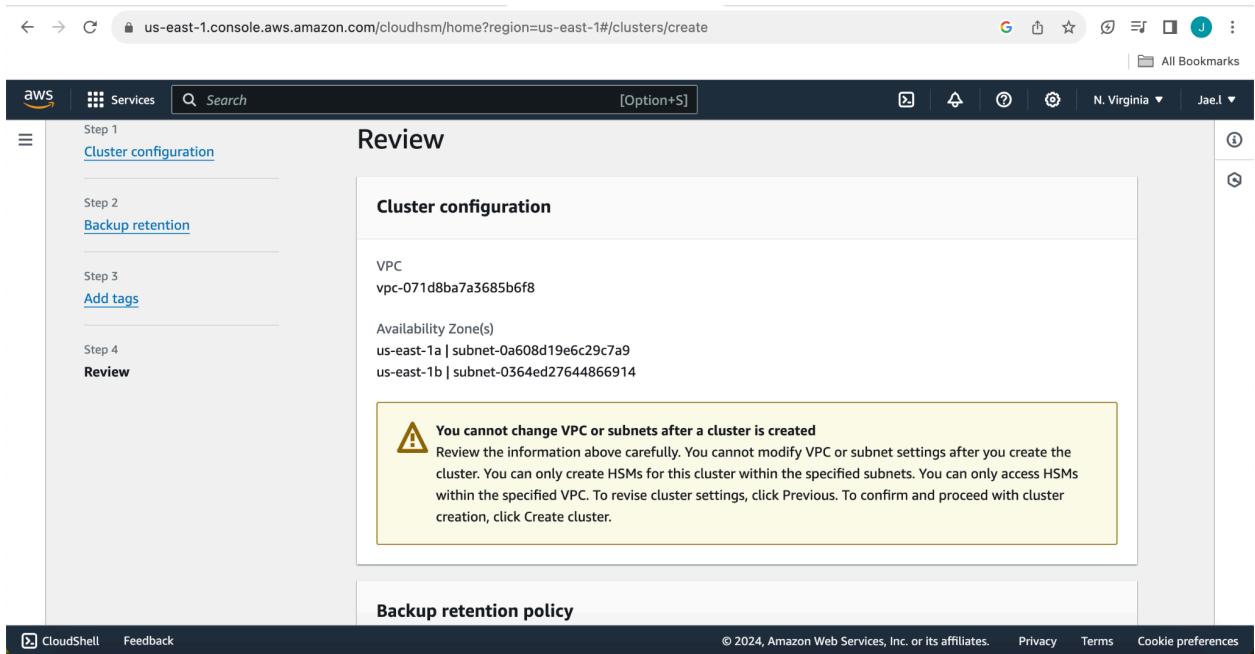
The screenshot shows the "Backup retention" step of the cluster creation process. The top navigation bar is identical to the previous screenshot. The main content area is titled "Backup retention" and contains a section for "Backup retention period". It states that backups will be automatically deleted after this period and that the value can be changed at any time. A text input field shows the value "35", which is highlighted with a blue border. Below the input field is a placeholder text "Enter a period between 7 and 379 days". At the bottom right are "Cancel", "Previous", and "Next" buttons, with "Next" being highlighted in orange. On the left sidebar, the "Cluster configuration" step is currently selected. The bottom navigation bar includes CloudShell, Feedback, System Settings, and links to Privacy, Terms, and Cookie preferences.

- Optionally, add tags to your cluster for easier identification.



5. Review and Create:

- Review the configuration details to ensure everything is correct.
- If everything looks good, click on the "Create cluster" button to initiate the creation process.



6. Wait for Cluster Creation: AWS CloudHSM will now provision the resources and create the cluster. This process may take several minutes.

The screenshot shows the AWS CloudHSM console with a message at the top stating "Your CloudHSM cluster 'cluster-abbye4366oq' is being created. It might take a few minutes for it to enter the Uninitialized state. You must initialize the cluster from the Clusters page once it moves to the Uninitialized state." Below this, the "Clusters" page is displayed with a single row in the table:

Cluster ID	State	Number of HSMs
cluster-abbye4366oq	Create in progress	0

7. Accessing the Cluster: Once the cluster creation process is finished, you can access your HSMs using the CloudHSM client software or AWS SDKs/APIs.

The screenshot shows the AWS CloudHSM console with a message at the top stating "Your CloudHSM cluster 'cluster-abbye4366oq' has been created". Below this, the "Clusters" page is displayed with a single row in the table:

Cluster ID	State	Number of HSMs
cluster-abbye4366oq	Uninitialized	0

8. Initialize HSMs: Before you can start using your HSMs, you'll need to initialize them. This involves setting up the HSM administrator user and configuring other necessary settings.

- Select your cluster, select “initialize” from the actions menu

The screenshot shows the AWS CloudHSM console. A green banner at the top says "Your CloudHSM cluster 'cluster-abbye4366oq' has been created". Below it, the "Clusters" page lists one cluster: "cluster-abbye4366oq" with Cluster ID "cluster-abbye4366oq", State "Uninitialized", and 0 HSMs. An "Actions" dropdown menu is open over the cluster row, with "Initialize" highlighted. The browser address bar shows "us-east-1.console.aws.amazon.com/cloudhsm/home?region=us-east-1#/clusters".

- Select your availability zone to provision your first HSM in the cluster

The screenshot shows the "Create an HSM in the cluster" step 1 page. It has three steps listed: Step 1 "Create an HSM in the cluster", Step 2 "Download certificate signing request", and Step 3 "Upload certificates". The main area is titled "First HSM" and contains instructions: "To initialize the cluster, you must first create an HSM in the cluster." and "Choose the Availability Zone to create this HSM. [Learn more](#)". A dropdown menu shows "us-east-1a | subnet-0a608d19e6c29c7a9". At the bottom are "Cancel" and "Create" buttons. The browser address bar shows "us-east-1.console.aws.amazon.com/cloudhsm/home?region=us-east-1#/clusters/cluster-abbye4366oq/initializeCluster".

6. Deploy Client Software: Install the CloudHSM client software on the systems that need to interact with the HSMs. This software allows applications to communicate securely with the HSM cluster.

2. Configuring CloudHSM:

- Partition and manage CloudHSM partitions.
- Create and manage HSM users and roles.
- Configure backup and restore procedures.
- Explain key concepts: secure partition initialization, cryptographic officers, quorum authentication.
- Discuss best practices for securing and hardening CloudHSM.
- Provide examples of integrating CloudHSM with applications for cryptographic operations.

KMS Integration with CloudHSM

1. Integrating AWS KMS with CloudHSM:

- Create a custom key store in KMS linked to your CloudHSM cluster.

- Insert rotation period days and save

The screenshot shows the AWS KMS console with the URL <https://us-east-1.console.aws.amazon.com/kms/home?region=us-east-1#/kms/keys/97ecbb0c-7e75-49a5-9d56-f3e863ea428f/editKeyRotation>. The left sidebar shows 'Customer managed keys' selected under 'Custom key stores'. The main content area is titled 'Edit automatic key rotation' and contains a section for 'Automatic key rotation'. It has a 'Key rotation' toggle set to 'Enable' (radio button selected) and a 'Rotation period (in days)' input field set to '90'. A note below the input says 'Rotation period defines the number of days between each automatic rotation'. At the bottom right are 'Cancel' and 'Save' buttons, with 'Save' being highlighted.

- Generate and manage KMS customer master keys (CMKs) in CloudHSM.
- Configure KMS to use CloudHSM for cryptographic operations.

:

Benefits of Using CloudHSM:

- **Enhanced Security:** Dedicated hardware security modules (HSMs) ensure cryptographic keys never leave the hardware, safeguarding against unauthorized access.
- **Regulatory Compliance:** CloudHSM meets stringent compliance requirements like PCI DSS, HIPAA, and GDPR by offering tamper-resistant hardware and strict access controls.
- **Performance Improvements:** Offloading cryptographic operations to CloudHSM accelerates performance, reducing latency and enhancing application responsiveness.

Code examples for working with KMS keys integrated with Cloud HSM using AWS CLI commands:

1. Creating a Custom Key Store in KMS Linked to CloudHSM:

```
```bash
aws kms create-custom-key-store --custom-key-store-name MyCustomKeyStore
--cloud-hsm-cluster-id <cloudHSM-cluster-id>
````
```

2. Generating a KMS Customer Master Key (CMK) in CloudHSM:

```
```bash
aws kms create-key --origin CLOUDHSM --custom-key-store-id <custom-key-store-id>
````
```

3. Enabling Automatic Key Rotation for the CMK:

```
```bash
aws kms enable-key-rotation --key-id <CMK-key-id>
````
```

These commands demonstrate the creation of a custom key store in KMS linked to Cloud HSM, the generation of a CMK within Cloud HSM, and the enabling of automatic key rotation for the CMK to enhance security. Adjust the parameters accordingly to your AWS environment.

Key Considerations for Integration:

- **Availability:** Deploy cloud HSM clusters across multiple availability zones for fault tolerance.
- **Durability:** Regularly back up cloud HSM partitions to prevent data loss.
- **Performance Implications:** Optimize cloud HSM configurations based on application requirements to balance performance and cost.

Best Practices for Monitoring and Auditing KMS Key Usage:

- 1. Enable AWS Cloud Trail Logging:** Log all KMS API calls to track key usage.

Example:

```
``bash
``
```

- 2. Set Up CloudWatch Alarms:** Monitor key usage metrics for anomalies.

Example:

```
``bash
```

```
aws cloudwatch put-metric-alarm --alarm-name kms-key-usage --metric-name KeyUsageCount
--namespace AWS/KMS --statistic Sum --period 300 --threshold 100 --comparison-operator
GreaterThanOrEqualToThreshold --evaluation-periods 1 --alarm-actions <sns topic ARN>
``
```

- 3. Regularly Review Audit Logs:** Analyze CloudTrail logs for unauthorized access.

Example:

```
``bash
```

```
aws clouptrail lookup-events --lookup-attributes
AttributeKey=EventName,AttributeValue=Decrypt
``
```

- 4. Implement Least Privilege Access:** Restrict permissions to only necessary actions.

Example:

```
``bash
```

```
aws iam attach-role-policy --role-name <role-name> --policy-arn
arn:aws:iam::aws:policy/ReadOnlyAccess
``
```

- 5. Encrypt CloudTrail Logs:** Encrypt logs using KMS-managed keys for data integrity.

Example:

```
``bash
```

```
aws clouptrail update-trail --name my-kms-trail --kms-key-id <kms-key-id>
``
```

- 6. Enable Key Usage Tags:** Tag keys for categorization and tracking.

Example:

```
``bash
```

```
aws kms tag-resource --key-id <key-id> --tags Key=Environment,Value=Production
``
```

- 7. Perform Regular Security Audits:** Review key usage, access policies, and configurations.

Example:

```
``bash
```

```
aws kms list-keys
``
```

- 8. Implement Multi-Factor Authentication (MFA):** Require MFA for critical operations.

Example:

```
``bash
```

```
aws kms enable-key-rotation --key-id <key-id> --multi-region
```

..

By implementing these practices, you can ensure effective monitoring and auditing of KMS key usage, maintaining security and compliance standards.