|  |  |  |  |
| --- | --- | --- | --- |
| Version | 1.0 |  |  |
| Customer(s) Name | Caribou Therapeutics | Change Request Number |  |
| Requested By | Abinand D | Date of Implementation |  |
| Presented To |  | Change Type  (Standard, Emergency, Normal) | Normal |

|  |  |
| --- | --- |
| Technical Category | Data Encryption on EBS volumes – Caribou Shared Services |
| Change Owner (Technical) | Abinand D |
| Change Owner (Business) |  |
| Change Implementer | Abinand D |
| Change Type | Standard |

|  |
| --- |
| **Reason for Change** |
| The primary reason for this change is to enhance data security by encrypting both root and data volumes attached to EC2 instances in Caribou AWS accounts. Encryption ensures that data at rest is secure, protecting sensitive information from unauthorized access while maintaining seamless access for authorized users. |

|  |
| --- |
| **Downtime : 45 – 60 mins for Encrypting 1 EBS volume** |

|  |
| --- |
| **Scope** |
| **Root Volume Encryption:** Encrypting the root volumes of existing EC2 instances using AWS KMS keys without altering instance configurations.  **Data Volume Encryption:** Encrypting data volumes attached to EC2 instances by creating encrypted copies using snapshots and KMS keys, then reattaching them to the instances.  This procedure applies to all instances on AWS within Caribou AWS accounts. Attached document has the required EBS volumes of the instances that are to be encrypted.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Account** | **Name** | **Volume ID** | **Type** | **Volume** | | Caribou-Shared-Services | – | [vol-03a30c3419950d7c9](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-03a30c3419950d7c9) | gp3 | Root volume | | Caribou-Shared-Services | – | [vol-0c86e4cf65668ba21](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-0c86e4cf65668ba21) | gp2 | Available | | Caribou-Shared-Services | – | [vol-06cf55efcda8cd539](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-06cf55efcda8cd539) | gp2 | Available | | Caribou-Shared-Services | – | [vol-0a4391fefc335e854](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-0a4391fefc335e854) | gp3 | Root volume | | Caribou-Shared-Services | CB-Rapid7IVM-DSE | [vol-0aa006d8cb36557f9](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-0aa006d8cb36557f9) | gp3 | Root volume | | Caribou-Shared-Services | – | [vol-07b9006f622eac6ff](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-07b9006f622eac6ff) | gp3 | Root volume | | Caribou-Shared-Services | WAMStudio | [vol-0698a2834dcaf7069](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-0698a2834dcaf7069) | gp2 | Root volume | | Caribou-Shared-Services | – | [vol-0efa9b73f388b55c4](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-0efa9b73f388b55c4) | gp2 | Root volume | | Caribou-Shared-Services | – | [vol-02c76a17c7adc2846](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-02c76a17c7adc2846) | gp3 | Root volume | | Caribou-Shared-Services | – | [vol-0658fc7f3712335aa](https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2#VolumeDetails:volumeId=vol-0658fc7f3712335aa) | gp3 | Root volume | |

|  |
| --- |
| **Pre-requisites / Support (If any)** |
| * **AWS Access**: Appropriate permissions to create snapshots, create encrypted volumes, and replace root volumes in the AWS EC2 Dashboard. * **KMS Key**: A KMS key must be available for encryption. Ensure the key is accessible and properly configured. * **Volume Creation**: Sufficient storage and permissions to create snapshots of both root and data volumes. * **Backup**: Ensure AMI backup is taken prior the activity before proceeding with the volume encryption. |
|  |

|  |
| --- |
| **Change Implementation Procedure** |
| The implementation procedure is divided into two parts: Root Volume Encryption and Data Volume Encryption.  **Root Volume Encryption**   * **Create Snapshot:** Create a snapshot of the current unencrypted root volume from the EC2 Dashboard.  A screenshot of a computer    AI-generated content may be incorrect. * **Copy Snapshot:** Copy the snapshot and enable encryption using a KMS key during the copy process.  A screenshot of a computer    AI-generated content may be incorrect.  A screenshot of a computer    AI-generated content may be incorrect. * **Replace Root Volume**: Use the Replace Root Volume feature to attach the encrypted snapshot as the new root volume of the instance.  A screenshot of a computer    AI-generated content may be incorrect.  A screenshot of a computer    AI-generated content may be incorrect. * **Verify Encryption**: Confirm the root volume is encrypted by checking the Encryption status  in the EC2 Dashboard.   **Data Volume Encryption**   * **Detach Volume**: Detach the unencrypted data volume from the EC2 instance. * **Create Snapshot:** Create a snapshot of the unencrypted data volume from the EC2 Dashboard. * **Create New Volume:** Create a new volume from the encrypted snapshot in the same Availability Zone as the instance.  A screenshot of a computer    AI-generated content may be incorrect. * **Attach Volume:** Attach the new encrypted volume to the instance using the same or updated device name.  A screenshot of a computer    AI-generated content may be incorrect. * **Mount Volume:** Connect to the instance via SSH or Session Manager, identify the new encrypted volume using commands like lsblk or fdisk -l, and mount it to the desired directory (e.g., /mnt/data). * **Update Configuration:** Update /etc/fstab to ensure the volume mounts automatically on reboot. * **Verify Encryption and Data Accessibility:** Confirm the volume is encrypted by checking the Encryption status in the EC2 Dashboard and verify that the data is accessible on the instance. |
|  |

|  |
| --- |
| **Back-out Plan** |
| In case of issues during the encryption process, follow these steps to revert to the original state:  **Root Volume**:   * + If the root volume encryption fails, use the original unencrypted volume to replace the root volume again.   + Ensure the instance is in stopped before replacing the root volume to avoid data loss.   **Data Volume**:   * + Detach the newly encrypted data volume and reattach the original unencrypted volume.   + If the original volume is unavailable, restore data from the unencrypted snapshot.   **Instance State**: If the instance becomes inaccessible, stop the instance and restore it from the last known good configuration or snapshot. |
|  |

|  |
| --- |
| **Validation** |
| **Root Volume**:   * Check the Encryption status in the EC2 Dashboard to confirm the root volume is encrypted. * Verify that the instance boots up correctly and all configurations are intact.   **Data Volume**:   * + Confirm the Encryption status in the EC2 Dashboard for the data volume.   + Verify that the data is accessible on the instance and that applications are functioning as expected.   + Ensure the volume mounts automatically on reboot by checking /etc/fstab. |
| **Effect of NOT Approving this Change** |
| NA |

|  |
| --- |
| **Reason for Rejection (if applicable)** |
|  |