**Automate data at rest protection**

Automating data at rest protection involves regularly checking if AWS resources are encrypted. AWS Config is a valuable service for this purpose, as it allows you to define and enforce compliance rules for your AWS resources. Here's a step-by-step guide on how to use AWS Config to check if related AWS resources are encrypted:

**Prerequisites**

1. AWS Config Enabled:

Ensure that AWS Config is enabled in your AWS account. If not, go to the AWS Config console and set up AWS Config.

**Setting up AWS Config Rules:**

**1. Navigate to AWS Config Console**

Go to the AWS Management Console and navigate to the AWS Config service.

**2. Create a New Config Rule**

- Click on "Rules" in the left navigation pane.

- Click "Add Rule."

**3. Select AWS Managed Rule**

- Choose "Encrypted volumes" or a similar AWS Managed Rule that fits your use case.

**4. Configure Rule Parameters**

- Set parameters such as the AWS resource type (e.g., EBS volumes, RDS databases) and other rule-specific settings.

**5. Scope Rule to Specific Resources**

- Specify the resources you want the rule to apply to (e.g., by resource tag, AWS region, etc.).

**6. Review and Create**

- Review your rule configuration and click "Create rule."

**Monitoring Compliance**

**1. View Compliance Dashboard**

- Navigate to the AWS Config console.

- Click on "Rules" in the left navigation pane.

- Select the rule you created.

**2. View Non-Compliant Resources**

- AWS Config will display a list of compliant and non-compliant resources based on your rule. Focus on the non-compliant resources to identify where encryption is not properly configured.

**Notifications and Remediation**

**1. Set up SNS Notifications**

- Optionally, configure AWS Simple Notification Service (SNS) to send notifications when non-compliant resources are detected.

**2. Automate Remediation**

- For certain AWS Config rule violations, you can set up AWS Systems Manager Automation documents or AWS Lambda functions to automatically remediate non-compliant resources. For example, you can create a Lambda function to encrypt an unencrypted EBS volume.

**Continuous Monitoring**

**1. Review AWS Config Snapshots**

- Regularly review AWS Config snapshots in your S3 bucket to get a historical view of resource configurations.

**2. Adjust Rules as Needed**

- Periodically review and adjust your AWS Config rules based on changes in your environment or new compliance requirements.

**Considerations**

**1. Custom Rules**

If AWS Managed Rules do not cover your specific use case, consider creating custom AWS Config rules using AWS Lambda functions.

**2. Audit Trail**

Leverage AWS Config to maintain an audit trail of configuration changes, helping in forensic analysis and compliance reporting.

By following these steps, you can automate the process of checking if AWS resources are encrypted at rest using AWS Config. This ensures continuous compliance with your organization's data protection policies.