1. Detailed Observations Cloud Configuration Review

# AWS misconfiguration

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Layer | Severity | | Likelihood | | Impact | |
| Configuration |  | Low |  | Low |  | Medium |

* + 1. **Observation**

During the analysis, it was detected that the following security settings were misconfigured.

|  |  |  |
| --- | --- | --- |
| Policy | Service | Description |
| Security contact information is registered | IAM | AWS allows customers to specify the contact information for the account’s security team.  **During the analysis, it was found that this information was not provided.**  It is recommended that security contact information be provided. |
| Security questions are registered in the AWS account | IAM | Security questions can be used to authenticate individuals calling AWS customer service for support.  **During the analysis, it was found that security questions were not established.**  It is recommended that security questions be established. |
| Access keys are rotated every 90 days or less | IAM | Rotating access keys will reduce the window of opportunity for an access key associated with a compromised or terminated account to be used.  **During the analysis, it was found that the following user's keys' last rotations were more than 90 days:**  svc-okta-424155111546 - 301 days ago  svc-smaf-product-stage - 148 days ago  svc-smaf-product-stg - 352 days ago  svc-smaf-user-readonly - 181 days ago  tower-init - 352 days ago  It is recommended that access keys should be rotated every 90 days or less to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen. |
| IAM Users Receive Permissions Only Through Groups | IAM | IAM users are granted access to services, functions, and data through IAM policies. There are three ways to define policies for a user:  1) Edit the user policy directly, aka an inline, or user, policy;  2) attach a policy directly to a user;  3) add the user to an IAM group that has an attached policy.  Only the third implementation is recommended.  Assigning IAM policy only through groups unifies permissions management to a single, flexible layer consistent with organizational functional roles. By unifying permissions management, the likelihood of excessive permissions is reduced.  **During the analysis, it was found that the following IAM users do not receive permissions through groups:**  **arn:aws:iam::424155111546:user/svc-smaf-product-stg**  **arn:aws:iam::424155111546:user/svc-smaf-product-stg**  **arn:aws:iam::424155111546:user/svc-okta-424155111546**  **arn:aws:iam::424155111546:user/tower-init**  **The following Policies are assigned directly to IAM users:**  **AmazonElastiCacheFullAccess**  **ApiGatewayFullAccess**  **AWSConfigRulesExecutionRole**  **AWSServiceRoleForAPIGateway**  **Smartfactory-product-stg-LocationService**  **okta-service-policy**  It is recommended that IAM Users can receive permissions through groups only. |
| IAM policies that allow full “\*:\*” administrative privileges are not attached | IAM | Standard security advice is to grant the least privilege - giving only the permissions required to perform a task. It’s more secure to start with a minimum set of permissions and grant additional permissions as necessary rather than starting with permissions that are too lenient and then trying to tighten them later. Providing full administrative privileges instead of restricting to the minimum set of permissions that the user is required to do exposes the resources to potentially unwanted actions.  **During the analysis, it was found that the “DeloitteVPCPeeringExceptionBoundaryPolicy”, “DeloitteConnectedEnvironmentBoundaryPolicy”, “DeloittePermissionsBoundaryPolicy” policies allow full “\*:\*” administrative privileges.**  It is recommended to review existing policies that allow full “\*:\*” administrative privileges. |
| A support role has been created to manage incidents with AWS Support | IAM | AWS provides a support center that can be used for incident notification and response, as well as technical support and customer services.  **During the analysis, it was found that the support role was not created to manage incidents with AWS Support.**  It is recommended to have a support role in managing incidents with AWS Support. |
| IAM Access analyzer is enabled for all regions | IAM | AWS IAM Access Analyzer helps identify the resources in organizations and accounts, such as Amazon S3 buckets or IAM roles, shared with an external entity. This lets to identify unintended access to resources and data. Access Analyzer identifies resources shared with external principals by using logic-based reasoning to analyze the resource-based policies in the AWS environment. IAM Access Analyzer monitors all policies for the S3 bucket, IAM roles, KMS(Key Management Service) keys, AWS Lambda functions, and Amazon SQS(Simple Queue Service) queues.  **During the analysis, it was found that the IAM Access analyzer is not enabled for all regions.**  It is recommended to enable Access analyzer is enabled for all regions. |
| VPC flow logging is enabled in all VPCs | VPC | VPC Flow Logs provide visibility into network traffic that traverses the VPC and can be used to detect abnormal traffic or insight during security workflows.  **During the analysis, it was found that the VPC flow logging is not enabled in all VPCs.**  It is recommended to enable VPC flow logging for all regions. |
| S3 Bucket Policy is set to deny HTTP requests | S3 | Amazon S3 allows both HTTP and HTTPS requests. To only allow access to Amazon S3 objects through HTTPS, explicitly denying access to HTTP requests is required. Bucket policies enabling HTTPS requests without explicitly denying HTTP requests will not comply with this recommendation.  **During the analysis, it was found that the following S3 Buckets allow HTTP requests:**  **smaf-nbi-stage-appdata**  **dcs-centralized-logging-bucket-af-south-1-rslnzkacjx**  **dcs-centralized-logging-bucket-ap-east-1-acdzhgjpiy**  **dcs-centralized-logging-bucket-me-south-1-clncbiprqw**  **dcs-centralized-logging-bucket-eu-south-1-dwlpgepobt**  It is recommended to deny HTTP requests. |
| MFA Delete is enabled on S3 buckets | S3 | Adding MFA delete to an S3 bucket requires additional authentication when changing the version state of a bucket or deleting and object version, adding another layer of security if security credentials are compromised or unauthorized access is granted.  Once MFA Delete is enabled on a sensitive and classified S3 bucket, it requires the user to have two forms of authentication.  **During the analysis, it was found that MFA Delete is not enabled on S3 buckets.**  It is recommended to enable “MFA Delete” on S3 buckets. |
| CloudTrail is enabled in all regions | CloudTrail | AWS CloudTrail is a web service that records AWS API calls for AWS account and delivers log files. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.  **During the analysis, it was found that CloudTrail is not enabled in all regions.**  It is recommended to enable global (Multi-region) CloudTrail logging. |
| CloudTrail trails are integrated with CloudWatch Logs | CloudTrail | Sending CloudTrail logs to CloudWatch Logs will facilitate real-time and historic activity logging based on user, API, resource, and IP address and provides an opportunity to establish alarms and notifications for anomalous or sensitive account activity.  **During the analysis, it was found that CloudTrail trails are not integrated with CloudWatch Logs.**  It is recommended that CloudTrail logs be sent to CloudWatch Logs. |
| S3 bucket access logging is enabled on the CloudTrail S3 bucket | CloudTrail | By enabling S3 bucket logging on target S3 buckets, capturing all events affecting objects within any target buckets is possible. Configuring logs to be placed in a separate bucket allows access to log information which can be helpful in security and incident response workflows.  **During the analysis, it was found that S3 bucket access logging is not enabled on the CloudTrail S3 bucket.**  It is recommended that bucket access logging be enabled on the CloudTrail S3 bucket. |
| Object-level logging for write events is enabled for the S3 bucket | S3 | Enabling object-level logging will help you meet data compliance requirements within your organization, perform comprehensive security analysis, monitor specific user behavior patterns in your AWS account, or take immediate actions on any object-level API activity within your S3 Buckets using Amazon CloudWatch Events.  **During the analysis, it was found that Object-level logging for write events is not enabled for S3 buckets.**  By default, CloudTrail trails don’t log data events, so it is recommended to enable Object-level logging for S3 buckets. |
| Object-level logging for reading events is enabled for the S3 bucket | S3 | Enabling object-level logging will help you meet data compliance requirements within your organization, perform comprehensive security analysis, monitor specific user behavior patterns in your AWS account, or take immediate action on any object-level API activity using Amazon CloudWatch Events.  **During the analysis, it was found that Object-level logging for reading events is not enabled for S3 buckets.**  By default, CloudTrail trails don’t log data events, so it is recommended to enable Object-level logging for S3 buckets. |
| The default security group of every VPC restricts all traffic | VPC | Configuring all VPC default security groups to restrict all traffic will encourage least privilege security group development and mindful placement of AWS resources into security groups, reducing the exposure of those resources.  **During the analysis, it was found that the default security group of every VPC does not restrict all traffic.**  It is recommended that the default security group restrict all traffic. |
| No Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports | VPC | Public access to remote server administration ports, such as 22 and 3389, increases the resource attack surface and unnecessarily raises the risk of resource compromise.  **During the analysis, it was found the default Network ACL allows ingress from 0.0.0.0/0 to remote server administration ports.**  It is recommended that no NACL allows unrestricted ingress access to remote server administration ports, such as SSH to port 22 and RDP to port 3389. |
| Database Instance is listening on to a standard/default port | RDS | Configuring database instances to listen to non-default ports can prevent malicious traffic from reaching the targeted instance.  **During the analysis, it was found that the following databases are listening to the standard/default 3306 port: smaf-nbiperf-aws-infra-stage-stack-rds-instanceone-fvu082sem744  smaf-nbi-aws-infra-stage-stack-rdsauro-instanceone-stufoqurr6fl**  It is recommended to review the possibility of switching to the non-standard port. |
| Event Subscriptions for Instance Level Events are not enabled for DB Instances | RDS | When an event occurs in the RDS DB Instance, the RDS Event Subscription sends alerts via the Amazon Simple Notification Service (SNS). This gives the administrator prompt notice of any important occurrences.  **During the analysis, there was no found event subscription associated with the following DB Instances:  smaf-nbiperf-aws-infra-stage-stack-rds-instanceone-fvu082sem744  smaf-nbi-aws-infra-stage-stack-rdsauro-instanceone-stufoqurr6fl**  It is recommended to create an Event Subscription for RDS DB Instances. |
| CMK is not used to protect RDS DB Cluster encryption key. | RDS | Data-at-rest encryption using a customer master key is supported by Amazon RDS (CMK). By real-time encrypting and decrypting the underlying storage for the cluster's database instances, automatic backups, Read Replicas, and snapshots, enabling encryption for database clusters can help safeguard data against the risk of malicious activity. Because the CMK is entirely maintained by the user rather than Amazon, using it to encrypt the DB Cluster offers superior security.  **During the analysis, it was found that encryption is disabled for the following RDS DB Clusters using CMK:**  **smaf-nbiperf-aws-infra-stage-stack-globaldbcluster-lkculzn7a2pi smaf-nbi-aws-infra-stage-stack-rds-globaldbcluster-1vfofkdzvvon**  It is recommended to use CMK to protect RDS DB Cluster encryption key. |
| Event Subscriptions for cluster Level Events are not enabled for DB Clusters. | RDS | When an event occurs in the RDS DB Cluster, the RDS Event Subscription sends alerts via the Amazon Simple Notification Service (SNS). This gives the administrator prompt notice of any important occurrences.  **During the analysis, it was found that there were not found event subscriptions associated with the following DB Clusters: smaf-nbiperf-aws-infra-stage-stack-globaldbcluster-lkculzn7a2pi smaf-nbi-aws-infra-stage-stack-rds-globaldbcluster-1vfofkdzvvon**  It is recommended to create an Event Subscription for RDS DB Clusters. |
| MYSQL DB Instance backup Binary logs configuration is enabled. | RDS | Events like table formation operations or changes to table data are recorded in the binary logs as writes or updates to the database data. For replication from a Mater MySQL server to a slave MySQL server, they are crucial. Also, it is essential for the complete current recovery of the databases from the backup. Various versions of MySQL utilize different binary log formats. Thus, it is crucial to pick the right one.  **During the analysis, it was found that the binary log format is not configured (set to "OFF") for the following MYSQL DB Clusters: smaf-nbiperf-aws-infra-stage-stack-globaldbcluster-lkculzn7a2pi smaf-nbi-aws-infra-stage-stack-rds-globaldbcluster-1vfofkdzvvon**  It is recommended to enable MYSQL DB Instance backup Binary logs. |
| Lambda function has tracing enabled | Lambda | With every call to the Lambda function, Amazon automatically generates logs and metrics using CloudWatch. Nevertheless, this might not be practical for tracking the lambda function's upstream calls or the event source that called it. When enabled, Amazon X-Ray tracing gathers information about client requests for the application servers and offers tools for viewing, filtering, and delving into that information to find problems.  **During the analysis, it was found that only the following 2 of 1414 Lambda functions have tracing enabled: smaf-nbi-sys-cc-ddb-service-stage-sta-InvokeLambda-Q8IPlUWtFcMh smaf-nbiperf-sys-cc-ddb-service-stage-InvokeLambda-ZgOm48HJVIwH**  It is recommended to enable tracing. |
| Lambda Function is not using An IAM role for more than one Lambda Function | Lambda | POLP (Principal of Least Privilege) will be broken if the same IAM Role is used with several Lambda functions. Because the access advisor is useless in that situation, keeping track of permissions on the roles is similarly challenging to maintain. Even when the privileges granted are the same, it is best practice to grant resources the fewest possible rights, and each function is given a different IAM Role.  **During the analysis, it was found that the following IAM role used by the Lambda Function is shared among multiple functions: arn:aws:iam::424155111546:role/lambda\_exec\_role**  It is recommended not to use the same role by more than one Lambda function. |
| Lambda Runtime Version is the latest and not custom | Lambda | Older runtime environments are more likely to include undiscovered flaws that could lead to errors or give attackers opportunities to exploit them.  **During the analysis, it was found that Lambda Functions use the following old Runtime Environment version: nodejs12.x nodejs14.x**  It is recommended to utilize the most recent versions of the runtime and the Lambda Function. Make sure that the identified flaws and vulnerabilities from the earlier version have been fixed by using the most recent runtime |
| Lambda Environment Variables at rest are encrypted with CMK | Lambda | AWS Lambda variables can be used to create dynamic and regularly changing settings to alter a Lambda Function's behavior without actually modifying the function code. These variables should be safeguarded when being saved since they may contain sensitive information like database connection details. Amazon default key management is improved when a CMK is used instead of the KMS key used to encrypt the variables.  **During the analysis, it was found that** **Aws/Lambda (default) key is used to encrypt Lambda environment variables at rest.**  It is recommended to encrypt Lambda Environment Variables at rest with CMK. |
| Lambda Environment Variables are encrypted using AWS encryption helpers for encryption in transit | Lambda | Dynamic and often changing variables can be configured using AWS Lambda variables to alter the function's behavior without changing the function code. These variables should be secured using Amazon Lambda helpers for encryption in transit because they may contain sensitive information like database connection details. If the variable is unencrypted, any user accessing Lambda Function can read it in plain text.  **During the analysis, it was found that the Environment Variables of the Lambda Functions are not encrypted.**  It is recommended to encrypt Lambda Environment Variables in transit. |
| VPC access for Lambda Function is not set to default | Lambda | To have better control over the network between the resources, AWS resources can be used inside a VPC.  **During the analysis, it was found that the following Lambda functions use default VPC: nbi-s3foldercreator-stage nbi-cloudfront-lambdafunc-stage lambda-logging-stage-nbiperf nbiperf-s3foldercreator-stage nbiperf-cloudfront-lambdafunc-stage lambda-logging-stage-nbi**  It is recommended not to use the default VPC. |
| Access keys unused for 90 days or greater are disabled | IAM | AWS IAM users can access AWS resources using different types of credentials, such as passwords or access keys.  **During the analysis, it was found that the following IAM users lasted used access keys more than 90 days ago: arn:aws:iam::424155111546:user/svc-smaf-product-stage arn:aws:iam::424155111546:user/tower-init**  It is recommended that all users' access keys unused in 90 or greater days be removed or deactivated. |
| IAM policies are attached only to groups or roles | IAM | By default, IAM users, groups, and roles have no access to AWS resources. IAM policies are how users, groups, or roles are granted privileges.  **During the analysis, it was found that the following IAM Users have a direct policy attachment arn:aws:iam::424155111546:user/tower-init arn:aws:iam::424155111546:user/svc-smaf-product-stg arn:aws:iam::424155111546:user/svc-okta-424155111546**  It is recommended that IAM policies be applied directly to groups and roles but not users. |
| Access logging is enabled for S3 buckets | S3 | S3 Bucket Access Logging generates a log that contains access records for each request made to your S3 bucket. An access log record contains details about the request, such as the request type, the resources specified in the request worked, and the time and date the request was processed. It is recommended that bucket access logging be enabled on the CloudTrail S3 bucket.  **During the analysis, it was found that access logging is not enabled for the following S3 buckets:  dcs-s3-access-log-424155111546-us-east-1 dcs-centralized-logging-bucket-[region]**  It is recommended to enable access logging for S3 buckets. |
| Versioning is enabled for S3 buckets | S3 | Versioning is a means of keeping multiple variants of an object in the same bucket. Versioning is used to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, it can easily recover from unintended user actions and application failures.  **During the analysis, it was found that versioning is not enabled for S3 buckets.**  It is recommended to enable versioning for S3 buckets. |
| No AWS default KMS Key is used to protect Secrets | Secrets Manager | AWS Secrets Manager service provides secure information management such as database credentials, passwords, third-party API keys, and arbitrary text. This information is termed as secret and can be retrieved from centralized storage whenever needed.  **During the analysis, it was found that CMK was not used for encryption at rest for the secret: smaf-db-service-nbi-entitymanagement-stage smfa-stage-gyILwG smaf-db-service-nbi-crewscheduling-stage smaf-db-service-nbi-commonservice-stage smaf-db-service-nbi-factoryhealthconfig-stage  smaf-db-service-nbi-organization-stage  smaf-db-service-nbi-rolemanagement-stage  smaf-tenant-credentials smfa-stage smaf-db-service-nbi-entities-stage**  KMS CMK is recommended to encrypt the secrets when stored at rest. |
| Only Root user of the AWS Account should be allowed full access to the CMK | KMS | AWS KMS Customer Managed Keys (CMKs) access control is primarily accomplished using Key policies and can be used with IAM policies and Grants. Unlike many AWS services, the AWS account's root user does not have access to CMK implicitly.  **During the analysis, it was found that arn:aws:sts::424155111546:assumed-role/dcs-logging-plugin-role/DCSLoggingAutomation policy has full access to the keys, except the following ones:**  **5a45ce2c-3a3c-4f71-a20b-3fcffc8b50ce**  **bc7a9343-130a-40d5-b9d1-5002b2102afd**  **762f70b2-d02c-4e61-ad1d-d542748482a8**  **bd1ea10e-4f41-4092-8c4c-9d360fc5200f**  **321a7ad7-a05c-4352-a9b1-26c9a67390df**  It is recommended to allow access to AWS account's root user to reduce the risk of CMK becoming unmanageable in case the account with such privileges is either not accessible or deleted. Further, to enable IAM policies for the CMK, the Root user of the AWS account must have full access to the key. |
| Permission to delete the key is not granted to any Principal other than the Root user of AWS Account | KMS | The deletion of AWS KMS CMK is destructive. Deleting CMK results in the deletion of the associated key material and metadata. If the effect radius is not monitored correctly, deleting a CMK could lead to the unavailability of data, as any data encrypted with this key cannot be decrypted.  **During the analysis, it was found that the Delete privilege was assigned to Principals other than the AWS account's Root user. The following insecure policy was identified arn:aws:sts::424155111546:assumed-role/dcs-logging-plugin-role/DCSLoggingAutomation**  It is recommended to remove the "kms:ScheduleKeyDeletion" privilege from any Principal other than the AWS account's root user. |
| Ensure to enable config for the global resources like IAM for Config Service | Config | AWS Config enables assess, audit, and evaluate the configurations of AWS resources. Config continuously monitors and records AWS resource configurations and allows to automate the evaluation of recorded configurations against desired configurations.  **During the analysis, it was found that Config for global resources like IAM is not enabled for Config Service.**  It is recommended to enable config for the global resources like IAM for Config Service. |
| Trail is configured on the organization level | CloudTrail | AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Using AWS CloudTrail, a user in a management account can create an organization trail that logs all events for all AWS accounts in that organization.  **During the analysis, it was found that Trail is not configured on the organization level.**  It is recommended to configure Trail on the organization level. |
| Each trail includes the global services | CloudTrail | For most global services, events are logged as occurring in US East (N. Virginia) Region, but some global service events are logged as appearing in other regions, such as US East (Ohio) Region or US West (Oregon) Region.  **During the analysis, it was found that trails are not configured to log global service events.**  It is recommended to include global service events logging to trail. |
| Every security groups rule has a description | VPC | Security Group Rule descriptions help to get an insight into the rule's configuration. It gives an idea of who has access and what prompted the rule's creation.  **During the analysis, it was found that Security groups' rules do not have a description.**  It is recommended to create security groups' rule descriptions. |
| Customer-managed KMS key policy does not contain a wildcard (\*) principal | KMS | Key policies are the primary way to control access to AWS KMS keys. The statements in the key policy document determine who has permission to use the KMS key and how they can use it.  **During the analysis, it was found that arn:aws:sts::424155111546:assumed-role/dcs-logging-plugin-role/DCSLoggingAutomation policy contains Wildcard Principal on the keys, except the following ones: 5a45ce2c-3a3c-4f71-a20b-3fcffc8b50ce bc7a9343-130a-40d5-b9d1-5002b2102afd 762f70b2-d02c-4e61-ad1d-d542748482a8 bd1ea10e-4f41-4092-8c4c-9d360fc5200f 321a7ad7-a05c-4352-a9b1-26c9a67390df**  It is recommended to remove wildcard (\*) principals from Customer managed KMS key policy. |
| Glue Data Catalog Encryption is enabled with SSE-KMS with customer-managed keys | Glue | When encryption is turned on, all future Data Catalog objects are encrypted. The default key is the AWS Glue AWS KMS key created for your account by AWS.  **During the analysis, it was found that AWS Glue Data Catalog Encryption is disabled.**  It is recommended to enable Glue Data Catalog Encryption with SSE-KMS with customer-managed keys. |
| EBS default encryption is enabled with customer-managed key | EC2 | Encryption operations occur on the servers hosting EC2 instances, ensuring the security of data-at-rest and data-in-transit between an instance and its attached EBS storage.  **During the analysis, it was found that AWS EBS default encryption is either disabled or used AWS managed key.**  It is recommended to enable EBS default encryption with a customer-managed key. |
| Trail is configured to log Data events for s3 buckets | CloudTrail | Choosing All current and future S3 buckets enables data event logging for all buckets currently in AWS account and any buckets created after creating the trail. It also allows the logging of data event activity performed by any user or role in the account, even if performed on a bucket that belongs to another AWS account.  **During the analysis, it was found that trail is not configured to log data events for all s3 buckets.**  It is recommended to enable Trail to log Data events for s3 buckets. |
| GuardDuty is enabled for specific org/region | GuardDuty | Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following Data sources: VPC Flow Logs, AWS CloudTrail management event logs, CloudTrail S3 data event logs, and DNS logs.  **During the analysis, it was found that AWS GuardDuty is disabled.**  It is recommended to enable GuardDuty to specific org/regions. |
| All IAM users are members of at least one IAM group | IAM | This policy ensures that all IAM users have at least one group member.  **During the analysis, it was found that the following IAM users are not members of at least one IAM group: svc-okta-424155111546 tower-init**  It is recommended to avoid assigning identity-based policies to individual IAM users or defining inline policies when creating an IAM user. Instead, you can assign policies to a group of IAM users or write inline policies when creating an IAM group |

* + 1. **Implication and Impact**

These incorrect settings could lead to a compromise of the confidentiality, integrity and availability of the data held within the platform.

* + 1. **Recommendations**

Management should consider carefully reviewing and implementing the recommendation mentioned above.