

AWS SEA Central Logging Structures

Accelerator Central Logging Buckets:

Bucket Type	Bucket Name	Purpose
AES Encrypted Bucket	pbmaccel-logarchive-phase0-aescacental1-1py9vr4cdwuxu	ALB Logs - ALB's do not support logging to a KMS bucket
KMS Encrypted Bucket	pbmaccel-logarchive-phase0-cacental1-1tr23emhncdzo	All other AWS logs

Notes:

- Every customer has two logging buckets
- Customers could use any account name for their central logging account
- Bucket name format is: {Accel-Prefix}-{Account-Name}-{Accel-Phase}-xxx{Region}-{Random}
 - {Accel-Prefix} should always be 'pbmaccel' for Canada
 - {Accel-Phase} should always be 'phase0'
 - {region} should always be 'cacental1' for Canada
 - {account} is likely to be 'log-archive'
 - xxx is either "aes" or "" (nothing)

Accelerator Bucket Folders:

Log Type	Folder Path	Example
ELB (in AES bucket)	{account#}/elb-{elbname}/AWSLogs/{account#}/*	s3://pbmaccel-logarchive-phase0-aescacental1-1py9vr4cdwuxu

Log Type	Folder Path	Example
VPC Flow Logs	{account#}/{vpc-name}/AWSLogs/{account#}/vpcflowlogs/{region}/{year}/{month}/{day}/*	s3://pbmmaccel-logarchive-phase0-cacen
Macie Reports	{account#}/macietestobject	s3://pbmmaccel-logarchive-phase0-cacen
Cost and Usage Reports	{account#}/cur/Cost-and-Usage-Report/*	s3://pbmmaccel-logarchive-phase0-cacen
Config History	AWSLogs/{account#}/Config/{region}/{year}/{month}/{day}/ConfigHistory/*	s3://pbmmaccel-logarchive-phase0-cacen
Config Snapshot	AWSLogs/{account#}/Config/{region}/{year}/{month}/{day}/ConfigSnapshot/*	s3://pbmmaccel-logarchive-phase0-cacen
GuardDuty	AWSLogs/{account#}/GuardDuty/{region}/{year}/{month}/{day}/*	s3://pbmmaccel-logarchive-phase0-cacen
CloudWatch Logs	CloudWatchLogs/{year}/{month}/{day}/{hour}/*	s3://pbmmaccel-logarchive-phase0-cacen
CloudTrail Digest	{org-id}/AWSLogs/{org-id}/{account#}/CloudTrail-Digest/{region}/{year}/{month}/{day}/*	s3://pbmmaccel-logarchive-phase0-cacen
CloudTrail Insights	{org-id}/AWSLogs/{org-id}/{account#}/CloudTrail-Insights/{region}/{year}/{month}/{day}/*	s3://pbmmaccel-logarchive-phase0-cacen
CloudTrail	{org-id}/AWSLogs/{org-id}/{account#}/CloudTrail/{region}/{year}/{month}/{day}/*	s3://pbmmaccel-logarchive-phase0-cacen

Notes:

- Account number is sometimes duplicated in path because logs replicated from another account always need to start with the source account number
- Macie reports will only appear in the {account#} for the central security account, and only if a customer schedules PII discovery reports
- All CloudWatch Logs from all accounts are mixed in the same folder, the embedded log format contains the source account information as documented here: <https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/ValidateLogEventFlow.html>
- With the exception of CloudWatch Logs, all logs are in the original format provided by the log source/service.

[...Return to Accelerator Table of Contents](#)