**Current Cloudtrail Setup Details across IDAutomation Account**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Account Name | Trail Log Location | Log File Validation | Multi Region Trail | API Activity | CloudWatch Log Destination |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Review of jamf-external-cloudtrail-logs Bucket**

The bucket access policy appears to follow least privilege by:

* Only allowing “PutObject” permissions needed for log delivery
* No broad or wildcard principals (e.g., "\*”)
* Access restricted to known IDAutomation source accounts
* No cross-account exposure except required logging permissions

Adding the snippet of the permission below for reference.

**Evidence for forwarded logs from IDAuto accounts**

**Table of IDAutomation accounts with CloudTrail Status and Logging Destination Info**

|  |  |  |
| --- | --- | --- |
| Account Details | Cloudtrail Status | Logging Destination |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Gaps and Issues**

* Data from some accounts from the account list is not showing up in the jamf-external-cloudtrail-logs bucket.
* On the engineering-sandbox I can see that cloudwatch logging is not enabled for the cloudtrail.
* CloudTrail log file SSE-KMS encryption not enabled as CloudTrail logs may contain sensitive operational and security metadata. Without KMS encryption, unauthorized users with access to the bucket could read raw log data. KMS also ensures Compliance with industry and regulatory standards.