CPB-2026-003

Cloud audit logging 2026: capabilities and event models across seven cloud providers

A documentation-based assessment of control-plane audit logging, identity, retention, export and integrity at seven cloud providers, with a common event model.

VERSION
1.0

PUBLISHED
6 November 2026

UPDATED
6 November 2026

ONLINE VERSION
https://www.cloudproviderbenchmarks.com/reports/cloud-audit-logging-2026/

Contents

Executive summary

1. Scope

2. Provider-level capability

3. Feature assessment

4. Common event model

5. Findings by provider

6. Recommendations for buyers

7. Conclusion

Limitations

Version history

Sources

DIRECT ANSWER

The services compared are AWS CloudTrail, PortvMind vTrail, Google Cloud Audit Logs and the Azure Activity Log. CloudTrail, Google Cloud Audit Logs and the Azure Activity Log provide documented, default-on control-plane audit logging with export and retention. vTrail records identity-attributed management operations, with retention, export and integrity not yet publicly documented. DigitalOcean, Vultr and Hetzner are unverified.

EXECUTIVE SUMMARY

This report assesses customer-facing audit logging at AWS, PortvMind Cloud, Google Cloud, Microsoft Azure, DigitalOcean, Vultr and Hetzner using nine qualitative features and maps PortvMind's vTrail event model to CloudTrail, Google Cloud Audit Logs and DMTF CADF. The three hyperscalers document mature services with default control-plane logging, optional data-access logs, retention and export. PortvMind documents control-plane coverage, identity and request metadata through vTrail. For DigitalOcean, Vultr and Hetzner a customer-facing control-plane audit log could not be verified from public documentation.

KEY FINDINGS

01 All three hyperscalers record control-plane events by default; data-access events are opt-in and generally charged.

02 Default retention is 90 days (CloudTrail event history, Azure Activity Log) or 400 days (Google Admin Activity).

03 Only CloudTrail documents cryptographic integrity validation; Google and Azure rely on locked buckets or immutable storage at the destination.

04 vTrail's field set covers who, what, when, where and outcome, plus request duration and gateway route identifiers that CloudTrail does not record.

05 Public audit-logging documentation was insufficient to verify the feature at DigitalOcean, Vultr and Hetzner.

1. Scope

The report covers customer-facing audit logs of management (control-plane) activity: who did what, to which resource, when, from where and with what result. Security-operations products built on top (SIEMs, threat detection) are out of scope. Method: cloud auditing methodology.

2. Provider-level capability

Audit and network-security capabilities, all providers

CRITERION	PORTVMIND	AWS	AZURE	GOOGLE CLOUD
Networking				
Private networks / VPC Isolated tenant networks with custom CIDR ranges.	● Yes Isolated networks with custom CIDR.	● Yes	● Yes	● Yes
Security groups / cloud firewall Stateful, API-managed network access rules.	● Yes	● Yes	● Yes	● Yes VPC firewall rule policies.
Security & auditing				
Control-plane audit logging A provider service that records management (API/console) operations against cloud resources.	● Yes vTrail (provider-supplied capability information).	● Yes AWS CloudTrail.	● Yes Azure Monitor Activity Log.	● Yes Cloud Audit Log
User identity attribution in audit events Each audit event identifies the authenticated principal that performed the operation.	● Yes vTrail records the authenticated user, project and scope (provider-supplied).	● Yes	● Yes	● Yes

3. Feature assessment

The nine features below are assessed for providers with a documented audit-logging service.

Documented features of cloud audit logging services

FEATURE	VTRAIL PortvMind Cloud	AWS CLOUDTRAIL Amazon Web Services	AZURE MONITOR ACTIVITY LOG Microsoft Azure
Control-plane audit scope Records management operations (create, modify, delete) performed through the API or console.	● Yes Cloud management API operations.	● Yes Management events recorded by default.	● Yes Azure Resource Manager write/delete/action operations.
Identity attribution Identifies the authenticated user, project/account and scope behind each operation.	● Yes User ID, user name, project ID and auth scope.	● Yes userIdentity block (principal, account, session).	● Yes Caller and claims.
Request metadata Captures request ID, HTTP method, path, status code, source IP and user agent.	● Yes Request ID, HTTP method, path, status, client IP, user agent, request time.	● Yes eventTime, requestID, sourceIPAddress, userAgent, errorCode.	◐ Partial Correlation ID, operation, status and caller IP in HTTP request details where available.
Data-plane (data access) events Optional recording of data-level reads and writes (for example object reads).	*? Unverified*	● Yes Data events (for example S3 object-level) are optional and charged.	◐ Partial Via resource logs and diagnostic settings, not the Activity Log itself.
Event search and filtering Console or API search by user, time range, resource or operation.	*? Unverified*	● Yes Event history lookup; SQL queries in CloudTrail Lake.	● Yes Portal filtering and Log Analytics (KQL).
Configurable retention Documented default retention and options to extend it.	*? Unverified*	● Yes 90-day event history; longer retention via trails to S3 or CloudTrail Lake.	● Yes 90 days in the platform; longer through Log Analytics or Storage.
Export and streaming Delivery to object storage, log analytics or SIEM pipelines.	*? Unverified*	● Yes S3, CloudWatch Logs, EventBridge.	● Yes Diagnostic settings to Log Analytics, Storage and Event Hubs.
Log integrity validation Cryptographic or immutability controls that detect tampering.	*? Unverified*	● Yes Log file integrity validation with digest files.	◐ Partial Immutable storage policies on the export destination.
Pricing model Whether baseline audit history is included and how extended capabilities are charged.	*? Unverified*	● Yes Event history and one copy of management events free; data events and Lake charged.	● Yes 90-day Activity Log included; ingestion into Log Analytics is charged.
Information source	Supplied by provider team	Official documentation	Official documentation

4. Common event model

Combining audit data from several providers requires a common model. The table maps the fields of vTrail’s event model to CloudTrail, Google Cloud Audit Logs and CADF.

Conceptual cloud audit event data model

For research documentation; does not represent production audit records.

FIELD	TYPE	DESCRIPTION	AWS CLOUDTRAIL	GOOGLE CLOUD AUDIT LOGS
event_time	string (RFC 3339)	When the operation was received, in UTC.	eventTime	timestamp
request_id	string	Unique request identifier used to correlate gateway, service and resource logs.	requestID	insertId / operation.id
http_method	string	HTTP verb of the API call (GET, POST, PUT, PATCH, DELETE).	–	httpRequest.requestMethod
full_path	string	Requested API path, identifying the target resource.	eventSource + eventName	protoPayload.methodName / resourceName
http_status	integer	Response status code — the outcome of the operation.	errorCode (on failure)	protoPayload.status.code
client_ip	string (IP)	Source IP address of the caller.	sourceIPAddress	protoPayload.requestMetadata.callerIp
user_agent	string	Client software (console, CLI, SDK, Terraform).	userAgent	protoPayload.requestMetadata.callerSupplied

FIELD	TYPE	DESCRIPTION	AWS CLOUDTRAIL	GOOGLE CLOUD AUDIT LOGS
auth_user_id	string	Stable identifier of the authenticated user.	userIdentity.principalId	protoPayload.authenticationInfo.principalSu
auth_user_name	string	Human-readable user name at the time of the request.	userIdentity.userName / arn	protoPayload.authenticationInfo.principalEm
auth_project_id	string	Project (tenant) the token was scoped to.	recipientAccountId	resource.labels.project_id
auth_scope	string	Authorisation scope or role context of the token.	userIdentity.sessionContext	protoPayload.authorizationInfo
service_id	string	Backend cloud service that handled the request (compute, network, storage).	eventSource	protoPayload.serviceName
route_id	string	API gateway route that matched the request.	–	–
request_time	number (ms)	End-to-end request processing time.	–	httpRequest.latency

Empty template (JSON)

```
{
  "event_time": "",
  "request_id": "",
  "http_method": "",
  "full_path": "",
  "http_status": null,
  "client_ip": "",
  "user_agent": "",
  "auth_user_id": "",
  "auth_user_name": "",
  "auth_project_id": "",
  "auth_scope": "",
  "service_id": "",
  "route_id": "",
  "request_time": null
}
```

Two vTrail fields stand out: `request_time` (request duration), which only Google Cloud exposes through `httpRequest.latency`, and `route_id`, which identifies the API-gateway route and has no equivalent in the other formats. `http_method` is also absent from CloudTrail records, which express the operation as `eventSource` and `eventName`.

5. Findings by provider

AWS CloudTrail. Default management events with 90-day event history; trails to S3 and CloudWatch Logs; optional, charged data events; CloudTrail Lake for SQL; signed digest files for integrity.

Google Cloud Audit Logs. Admin Activity always on and retained 400 days; Data Access mostly off by default; sinks to Storage, BigQuery and Pub/Sub; locked buckets prevent retention changes.

Azure Activity Log. Subscription-level control-plane events for 90 days; diagnostic settings export to Log Analytics, Storage and Event Hubs; data-plane via resource logs.

PortvMind vTrail. Management API operations with user, project, scope and full request metadata. Retention, export, search, integrity and pricing are unverified.

DigitalOcean, Vultr, Hetzner. Public documentation reviewed was insufficient to verify a customer-facing control-plane audit log. Values will be updated when documentation is found or published.

6. Recommendations for buyers

1. Ask every provider for its audit-log retention period, export mechanism and integrity controls in writing.
2. Export audit events to storage you control, with write-once protection.
3. Normalise events from multiple providers to a common schema before building detections.
4. Test the trail by performing known actions and confirming they appear correctly attributed.

7. Conclusion

Audit logging has converged among hyperscalers; smaller providers vary widely in what they document. vTrail gives PortvMind Cloud a detailed control-plane event model, and its assessment will be completed when its operational features are publicly documented.

Limitations

- Assessments are based on public documentation and provider-supplied information; no logging pipeline was tested.
- Feature availability may vary by region, edition or account type.
- vTrail information is provider-supplied.
- 'Unverified' means insufficient documentation, not absence of the feature.

Version history

1.0	6 November 2026	First edition.

Sources

[1] AWS CloudTrail User Guide — AWS Official documentation
accessed: 6 November 2026

[2] CloudTrail record contents — AWS Official documentation
accessed: 6 November 2026

[3] Cloud Audit Logs overview — Google Cloud Official documentation
accessed: 6 November 2026

[4] Azure Monitor activity log — Microsoft Official documentation
accessed: 6 November 2026

[5] keystonemiddleware — Audit middleware — OpenStack Official documentation
accessed: 6 November 2026

[6] DMTF Cloud Auditing Data Federation (CADF) — DMTF Official documentation

accessed: 6 November 2026

[7] NIST SP 800-92: Guide to Computer Security Log Management — NIST Official documentation
accessed: 6 November 2026

[8] PortvMind Cloud — PortvMind Supplied by provider team
accessed: 6 November 2026