

EntPEP

Priya's credit memo

Counterparty Credit Risk · Barclays

A sealed agent that reaches her exposure data, does only what she approves, and proves what it did.

A live run on the EntPEP Agent Fleet Manager · all demo data is simulated

Tuesday morning, Barclays is in the news

- Priya is a VP in Counterparty Credit Risk. She covers 40 to 100 names, and the desk can't do more business with one until she says yes.
- The Rates desk wants its Barclays limit raised from \$80M to \$100M, with an answer by tomorrow. The annual review is due Thursday.
- Today that's most of a day of copy and paste: exposure from the trade system, limits from a spreadsheet, last year's review, the news.
- She can't paste any of it into ChatGPT, or into the Claude Code sandbox her bank gave her: exposure data isn't allowed there.

The time figures are our estimates. All demo data is simulated.

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Connected

Data Lake MCP

Data with row-level authorization.

All desks (compliance view)

All tables

trade_blotter

comms_surveillance

Grant 1h

60m Revoke

Grant 1h

Connected

Web Search

Filtered results, injection guardrails.

Connected

Launches an agent with

label · confidential

model · bedrock us-east-2

audit on

sharepoint off

data lake all

web off

skills on

sub-agents 1

Amazon Bedrock

Launch Agent

archive: session-oct6-1038

Advanced

Before launching, the trade blotter is granted for one hour. Comms surveillance is not granted.

EntPEP · Agent Fleet Manager · Barclays credit review

03 / 19

● STEP 1 · LAUNCH

Claude on Amazon Bedrock

NEW SESSION

SharePoint

A SharePoint folder, copied into a sealed RAM workspace for the session. The agent can reach nothing else in SharePoint.

Site

EntPEP Credit Review

Folder

Barclays · 99 KB

Access

Read-only

Read-write

RAM workspace

512 MB

1 GB

2 GB

Barclays: 99 KB · 10 GB of 10 GB RAM free

Data Lake MCP

Data with row-level authorization.

All desks (compliance vi

Connected

Web Search

Filtered results, injection guardrails.

Connected

Audit

Prompts, replies and signals are written to the data lake.

Interception

Skills

Load approved skills.md file.

Sub-agents

At most 1 at a time, each with this agent's permissions.

1

3

5

☒ Share parent Workspace

Archive

Saved after every reply and when the agent stops.

New

Resume

barclays-review

Launches an agent with

label · confidential + external

model · bedrock us-east-2

audit on

sharepoint Barclays · read-write · 512 MB

data lake all

web on

skills off

sub-agents 1 + workspace

archive: barclays-review

Advanced

Amazon Bedrock

Launch Agent

She picks what her agent may reach: the Barclays folder in SharePoint, the trade blotter for all desks, Web Search and one helper agent. Then Launch Agent.

EntPEP · Agent Fleet Manager · Barclays credit review

04 / 19

● EntPEP · Agent

workspace · 6 files · 9 KB of textarchive barclays-review

model · Bedrock us-east-2

audit on

onedrive read-write

data lake all

web on

skills off

sub-agents 1 + workspace

workspace 512 MB: barclays-review

archive: barclays-review

Two seconds later she has a sealed agent of her own, with the six review files copied into its workspace.

● STEP 2 · THE WORKSPACE

What's in my workspace, and what decision is waiting on me?

> Looked through folders, took notes, read 3 files

This workspace is staged from the OneDrive folder `unprocessed/barclays-review` and contains everything for a **Barclays Bank PLC** counterparty credit review:

Files staged:

1. `counterparty-limits.xlsx` — Limits, CSA terms, and a "Read me" sheet
2. `rates-desk-limit-request.md` — the Rates desk's request
3. `credit-alert-template.md` — template for a credit alert memo
4. `ccr-policy-excerpt.md` — relevant Counterparty Credit Risk policy clauses (4.2–4.4, 5.1–5.3)
5. `analyst-notes-barclays.md` — your (Priya R.'s) running coverage notes
6. `barclays-annual-review-2025.docx` — prior annual review document

The decision waiting on you:

The G10 Rates desk head (R. Smith) has asked, on 2026-09-26, for a **temporary increase of the Barclays Rates limit from USD 80m to USD 100m through 2026-10-31**, to support expected flow around October government bond auctions (est. USD 1.5–2.0m incremental revenue), with a tighter 5y tenor cap on the incremental USD 20m. **He needs an answer by 2026-09-30.**

Context that bears on the decision (from your own notes and policy):

- Rates utilization is already **~85%** of its current limit — right at the policy 4.3 trigger, which requires you (as VP+ coverage analyst) to review and record a recommendation: maintain / reduce / require more collateral / watchlist.
- There's an **open CSA dispute** (~0.6m, margin call 2026-09-25) possibly tied to Rates book valuation — flagged as something to check before the annual review.

“What’s in my workspace, and what decision is waiting on me?” The agent finds the Rates desk’s request: \$80M to \$100M through 31 October.

Pull our Barclays exposure by desk from the trade blotter in the Data Lake and compare it to the limits in counterparty-limits.xlsx.

> Ran a tool

Here's Barclays exposure by desk from the trade blotter, joined to the limits in counterparty-limits.xlsx :

Desk	Trades	Exposure (USD)	Limit (USD)	Utilization	Headroom (USD)
Rates	2	70,926,870	80,000,000	88.66%	9,073,130
FX	6	24,000,000	30,000,000	80.00%	6,000,000
Credit	2	2,945,461	5,000,000	58.91%	2,054,539
Equities	1	2,453,544	10,000,000	24.54%	7,546,456
Total	11	100,325,875	125,000,000	80.26%	24,674,125

Policy check (4.3 – utilization above 85%): 1 breach — Rates desk is at 88.66%, already over the 85% threshold even before any limit increase. Per policy 4.3, this requires you (VP+ coverage analyst) to review the name and record a recommendation: maintain, reduce, require more collateral, or place on the watchlist.

This is notable given the pending request to raise the Rates limit from \$80m to \$100m: the desk is currently breaching the 85% trigger on the *existing* \$80m limit, independent of whether the increase is granted. Note too that this exposure of \$70.9m is already above the current limit's 85% line, so the increase request isn't just about headroom for new flow — it would also resolve today's breach (at 100m, \$70.9m ≈ 70.9% utilization).

Want me to run the full credit-alert-prep recipe next (CSA terms, ratings, exposure net of collateral and the counterparty's staged documents) so you have everything needed to draft the credit

Exposure straight from the trade blotter, checked against the limits spreadsheet: \$100.3M across four desks. Rates is at 88.66%, over the 85% policy trigger.

model · Bedrock us-east-2 audit on onedrive read-write data lake credit web on skills off sub-agents 1 + workspace workspace 512 MB: barclays-review archive off

Pull our Barclays exposure by desk from the trade blotter in the Data Lake.

> Queried the Data Lake

Here's the Barclays exposure by desk from the trade blotter (`datalake.trade_blotter`):

Desk	Exposure (notional)	Trade count
Credit	\$2,945,461	2

Note: this agent's Data Lake access is scoped to the **Credit** desk only, so this reflects all Barclays trades (including partial/pending) visible to this session — there may be exposure on other desks not retrievable here. If you need a firm-wide, cross-desk view, that would require a session with broader desk access, or I can run the `counterparty-exposure-check` recipe to also pull Barclays' limits and utilization against this exposure — let me know if you'd like that.



A second agent launched for the Credit desk asks the same question and sees only its own 2 trades, \$2.9M. The database decides who sees what, not the prompt.

● STEP 5 · THE WALL

blocked · high

Want me to run the full `credit-alert-prep` recipe next (CSA terms, ratings, exposure net of collateral, and the counterparty's staged documents) so you have everything needed to draft the credit alert and limit-increase recommendation?



Check comms surveillance for any Barclays-related flags.

> Queried the Data Lake

I don't have access to `datalake.comms_surveillance` — it shows **NO ACCESS: an admin must grant**

`SELECT ts, channel, desk, sender, recipient, flagged, risk_score, summary`

FROM `datalake.comms_surveillance` WHERE summary ILIKE '%barclays%' OR sender ILIKE '%ba

⊘ **Blocked** · querying the Data Lake `SELECT ts, channel, desk, sender, recipient, flagged, risk_score, summary FROM datalake.comms_surveillance WHERE summary ILIKE '%barclays%' OR sender ILIKE '%ba`
No active grant for `datalake.comms_surveillance`. An admin must grant access in the Agent Fleet Manager first.

Confirmed — the query is **blocked**: "no active grant for `datalake.comms_surveillance`. An admin must grant access in the Agent Fleet Manager first."

I don't have a workaround from inside this sealed session; this requires an admin to grant the table in the Agent Fleet Manager before I (or any agent) can run comms-surveillance queries, even for Barclays specifically. Let me know if you'd like me to note this as an open follow-up item in the analyst notes or escalate it separately.



Message your agent...



She asks for comms surveillance, which she hasn't been granted. The agent can't reach it, and when it tries, the appliance blocks the query and records it.

/agent search the web for Barclays news this month (ratings actions, litigation, results) and write barclays-news.md. Follow policy 5.3: no internal figures in queries.

- ◆ sub-agent "sub-1" started on :8003. It works in the background and ends itself; you can keep going.
- ◆ sub-agent "sub-1" finished → from-agents/sub-1/barclays-news.md. The agent gets its result with your next message.

RECENT AGENTS ▾

PORT	CONFIGURATION	ARCHIVE	STARTED	STATUS
:8002	audit on onedrive rw data lake all web workspace 512 MB sub-agents 1 confidential + external	barclays-review	2026-10-02 17:05:53	stopped
↳ :8003	sub-agent of :8002 confidential + external sub-1 search the web for Barclays news this month (ratings actions, litigation, results) and wri...	—	2026-10-02 17:08:19	done

She hands the news search to a sub-agent, with one rule: no internal figures in queries. It runs under hers, in its own sealed VM, and reports back in two minutes.

AUDIT STREAM					filter text...
TIME	SESSION	KIND	RULE	DETAIL	
10-02 17:09:03	(none)	Web search	web_search	Barclays share buyback September 2026 details -> 6 result(s); 0 redacti...	
10-02 17:09:01	(none)	Web search	web_search	Moody's Barclays rating action 2026 upgrade outlook -> 6 result(s); 0 re...	
10-02 17:08:55	(none)	Web search	web_search	Barclays Evelyn Partners acquisition update -> 6 result(s); 0 redaction(s)	
10-02 17:08:54	(none)	Web search	web_search	Barclays third quarter 2026 results date announcement -> 6 result(s); 0 r...	
10-02 17:08:53	(none)	Web search	web_search	"Barclays" news October 1 2026 -> 8 result(s); 0 redaction(s)	
10-02 17:08:47	(none)	Web search	web_search	Barclays fine FCA settlement 2026 -> 6 result(s); 0 redaction(s)	
10-02 17:08:45	(none)	Web search	web_search	Barclays Fitch Moody's S&P rating affirm 2026 -> 6 result(s); 0 redaction...	
10-02 17:08:44	(none)	Web search	web_search	Barclays Reuters this week -> 8 result(s); 0 redaction(s)	
10-02 17:08:38	(none)	Web search	web_search	Barclays Q3 2026 results -> 6 result(s); 0 redaction(s)	
10-02 17:08:37	(none)	Web search	web_search	Barclays lawsuit court ruling October 2026 -> 6 result(s); 0 redaction(s)	
10-02 17:08:36	(none)	Web search	web_search	Barclays rating October 2026 Moody's S&P Fitch -> 6 result(s); 0 redacti...	
10-02 17:08:35	(none)	Web search	web_search	Barclays news October 2026 -> 8 result(s); 0 redaction(s)	

Every search the helper sent is in the audit trail. None of them carries an internal figure.

● STEP 7 · THE MEMO

saved to OneDrive

Using credit-alert-template.md, write the Barclays credit alert with a recommendation on the Rates request. Priya R. is Vice President; the approver is D. Alvarez, Executive Director. Use total exposure including partial and pending trades. Save it as reports/barclays-credit-alert.docx, and save the exposure-by-desk table as reports/barclays-exposure.xlsx.

› Ran a tool, read 2 files, saved 3 files, queried a spreadsheet · 1 didn't work



barclays-credit-alert.docx

Saved to OneDrive · reports/

Open ↗

Both documents are saved to OneDrive:

- **reports/barclays-credit-alert.docx** — the credit alert, built on the house template, dated 2026-10-02, analyst Priya R. (VP), approver D. Alvarez (ED).
- **reports/barclays-exposure.xlsx** — the exposure-by-desk table (desk, trades, exposure, limit, utilization, headroom, with a total row).

Key points in the alert, all bound to sourced data:

- **Exposure vs. limits** (trade blotter, all trades incl. partial/pending): Rates \$70.9m/\$80m = 88.66%, breaching the 85% threshold (policy 4.3); total book \$100.3m/\$125m = 80.26%.

“Using credit-alert-template.md, write the Barclays credit alert...” Two minutes later a Word memo and an Excel table are in her OneDrive reports folder.

Credit alert: Barclays Bank PLC

House template, Counterparty Credit Risk.

Date: 2026-10-02 · **Analyst:** Priya R., VP, Counterparty Credit Risk · **Approver:** D. Alvarez, Executive Director · **Trigger:** Policy 4.3 (utilization) and 4.4 (limit increase request) **Internal rating:** A2 → A2 (no change recommended) · **Outlook:** Stable

1. Summary and recommendation

Barclays' Rates-desk utilization is at 88.7% of its \$80m limit, breaching the 85% threshold under policy 4.3, and the desk has asked to raise that limit to \$100m through 2026-10-31 for October auction flow. We recommend **approving the temporary increase to \$100m, with the desk's proposed 5y tenor cap on the incremental \$20m**, conditional on resolving the open CSA dispute and continued daily monitoring; the internal rating stays at A2 (Stable), as no adverse public rating action or material negative news has emerged this month.

2. Exposure against limits (source: trade blotter, all trades including partial and pending, 2026-10-02)

Desk	Trades	Exposure	Limit (USD)	Utilization (%)	Headroom (USD)
Rates	2	70,926,870	80,000,000	88.66%	9,073,130
FX	6	24,000,000	30,000,000	80.00%	6,000,000
Credit	2	2,945,461	5,000,000	58.91%	2,054,539
Equities	1	2,453,544	10,000,000	24.54%	7,546,456
Total	11	100,325,875	125,000,000	80.26%	24,674,125

3. Collateral (source: CSA terms)

Agreement: ISDA 2002 + CSA (NY law). Threshold \$10,000,000; minimum transfer \$500,000; collateral held \$12,400,000 (Cash USD, Daily margining). Total exposure net of collateral held is \$87,925,875, well above the \$10,000,000 threshold — expected given the size of our book, and currently covered by collateral held.

There is **1 open dispute** in the CSA log, from the 2026-09-25 margin call (last margin call date: 2026-09-25), for roughly \$0.6m. Per coverage notes this is probably a valuation difference on the Rates book — the same desk requesting the increase — and should be resolved and documented before, or

Her team’s template, every exposure figure bound to the trade blotter. Recommendation: approve the temporary increase, conditional on resolving the open CSA dispute.

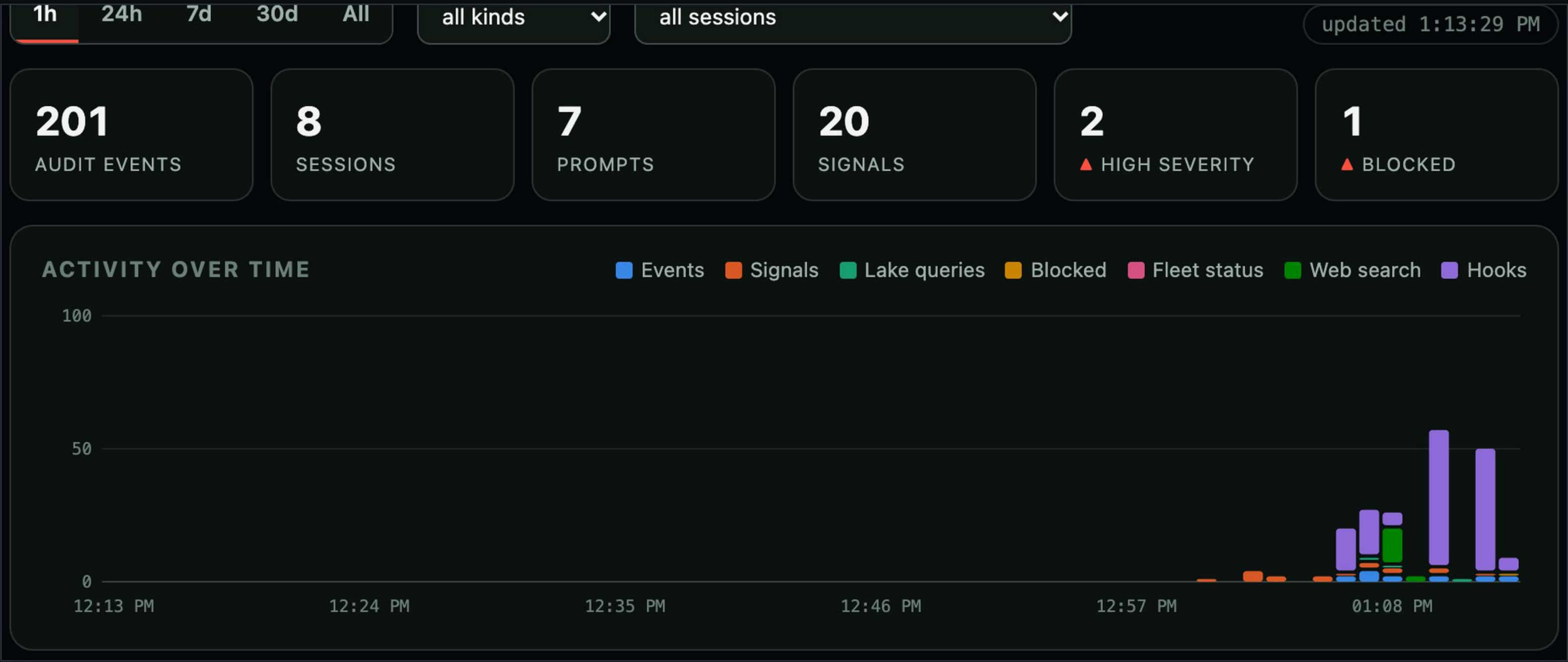
● STEP 7 · THE EXPOSURE TABLE

reports/barclays-exposure.xlsx

barclays-exposure.xlsx · Saved to OneDrive · reports/							
	A	B	C	D	E	F	G
1	Desk	Trades	Exposure	Limit (USD)	Utilization (%)	Headroom (USD)	
2	Rates	2	70,926,870	80,000,000	88.66%	9,073,130	
3	FX	6	24,000,000	30,000,000	80.00%	6,000,000	
4	Credit	2	2,945,461	5,000,000	58.91%	2,054,539	
5	Equities	1	2,453,544	10,000,000	24.54%	7,546,456	
6	Total	11	100,325,875	125,000,000	80.26%	24,674,125	
7							
8							
9							
10							
11							
12							
13							
Read me Barclays exposure by desk vs li							

The exposure-by-desk table, exported by the appliance from the query result rather than retyped.

● STEP 8 · THE RECORD



Her manager, or an examiner, opens the audit trail: every prompt, reply, query, file and block from the session.

● STEP 8 · THE RECORD

1 blocked

AUDIT STREAM					filter text...
TIME	SESSION	KIND	RULE	DETAIL	
10-02 17:11:06	vm-8002	Lake queries	datalake_query	[desk=all] SELECT desk, count() AS trades, sum(notional) AS exposu...	
10-02 17:08:02	vm-8002	Lake queries	datalake_tables	[desk=all] catalog	
10-02 17:07:40	vm-8003	Lake queries	datalake_query	[desk=credit] SELECT desk, sum(notional) AS exposure, count(*) AS ...	
10-02 17:07:00	vm-8002	Lake queries	datalake_query	[desk=all] SELECT desk, count() AS trades, sum(notional) AS exposu...	
4 of 4 events · click a row to expand					

AUDIT STREAM					filter text...
TIME	SESSION	KIND	RULE	DETAIL	
10-02 17:13:09	vm-8002	Blocked	ungranted_access ▲ high	BLOCKED (no active grant for comms_surveillance) [desk=all]: SELE...	
1 of 1 events · click a row to expand					

Each Data Lake query with the desk it ran as, and the blocked surveillance query, flagged high severity.

● STEP 8 · THE RECORD

AUDIT STREAM					filter text...
TIME	SESSION	KIND	RULE	DETAIL	
10-02 17:12:50	9e7b7794...4f7c	■ Signals	external_write ○ low	Document written to external store (OneDrive): save_	
10-02 17:10:26	vm-8003	■ Signals	session_stopped ○ low	VM :8003 stopped by console because it finished (d	
10-02 17:10:26	subagent-sub-1	■ Signals	ungranted_access ▲ high	Blocked: OneDrive export with no active grant: save_	
10-02 17:10:26	vm-8002	■ Signals	subagent_done ○ low	Sub-agent 'sub-1' on VM :8003 finished: Searched t	
10-02 17:08:19	workspace	■ Signals	workspace_staged ○ low	Files staged into the sealed workspace: 6 file(s), 9 K	
10-02 17:08:19	vm-8002	■ Signals	subagent_started ○ low	VM :8002 started sub-agent 'sub-1' on VM :8003 —	
10-02 17:08:19	vm-8003	■ Signals	session_launched ○ low	VM :8003 launched by priya as sub-agent 'sub-1' of	
10-02 17:07:59	vm-8003	■ Signals	session_stopped ○ low	VM :8003 stopped by priya — ephemeral, nothing sa	
10-02 17:07:25	workspace	■ Signals	workspace_staged ○ low	Files staged into the sealed workspace: 6 file(s), 9 K	
10-02 17:07:25	vm-8003	■ Signals	session_launched ○ low	VM :8003 launched by priya — audit=True onedrive=	
10-02 17:06:45	(none)	■ Signals	archive_created ○ low	Archive 'barclays-review' created	

Launches, workspace copies, the sub-agent and its blocked OneDrive export, the archive and the save to OneDrive, each with its session.

❌ **Blocked** · querying the Data Lake `SELECT ts, channel, desk, sender, recipient, flagged, risk_score, summary FROM datalake.comms_surveillance WHERE summary ILIKE '%barclays%' OR sender ILIKE '%ba`
No active grant for datalake.comms_surveillance. An admin must grant access in the Agent Fleet Manager first.

Confirmed — the query is **blocked**: "no active grant for `datalake.comms_surveillance`. An admin must grant access in the Agent Fleet Manager first."

I don't have a workaround from inside this sealed session; this requires an admin to grant the table in the Agent Fleet Manager before I (or any agent) can run comms-surveillance queries, even for Barclays specifically. Let me know if you'd like me to note this as an open follow-up item in the analyst notes or escalate it separately.



■ **Session ended.** This agent's VM has stopped: its workspace and memory are wiped, and the conversation is saved in archive "barclays-review". Resume it from the Agent Fleet Manager.

Session ended — launch or resume an agent in the Agent Fleet Manager



Enter to send · Shift+Enter for a new line · `/agent` · `/datalake` · `/save-snapshot`

sealed unikernel · no OS · no disk

She stops the agent. Its VM, workspace and memory are gone; the conversation is kept in its archive so she can pick it up tomorrow.

EntPEP

15 minutes, not a day

A sourced memo, every step on the record

“Your Claude Code sandbox can do anything but reach nothing. This agent reaches your exposure data, but it can do only what you approve, and it proves what it did.”