Vantalect



AWS INCIDENT RESPONSE · SAMPLE DELIVERABLE

Containment and Eradication Actions

DISTRIBUTION: OPERATIONAL

Days 1 to 6: Contain · prepared for Wrenfield Bancorp, Inc.

Prepared by Charles Sieg · charles.sieg@vantalect.com · vantalect.com

July 9, 2026 · AWS Incident Response: The Response (July 4 to 9, 2026)

SAMPLE DELIVERABLE

This is a sample deliverable. Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

Contents

What this report covers **3**

How fast, in elapsed time **4**

The action register **5**

- Actions A-01 to A-04 6
- Actions A-05 to A-08 7
- Actions A-09, A-36, A-37, and A-38 8
- Actions A-39, A-10, A-11, and A-12 9
- Actions A-40, A-13, A-14, and A-32 10
- Actions A-33, A-34, A-35, and A-15 11
- Actions A-16 to A-19 13
- Actions A-41, A-42, A-20, and A-43 15
- Actions A-21, A-44, A-45, and A-22 16
- Actions A-23 to A-26 17
- Actions A-27 to A-30 19
- Actions A-46, and A-31 21

Credentials disabled and sessions revoked **22**

Jobs canceled and settings reversed **25**

The recovery vault **29**

What we deliberately did not do, and why **32**

Appendix: the guardrail policies as code **33**

- The containment SCP, as attached at 01:22 33
- The containment SCP, as updated at 02:58 35
- What the first policy did not deny, and what the attacker did in that window 37
- The resource control policy, as attached at 03:20 39
- The vault's deny-all SCP 40
- The session-revoking inline policy 43
- Our incident role's trust policy 44
- The lock configurations 45

Notice **46**

Distribution

This report is for the bank's incident and platform teams. It is not part of the counsel track and holds no legal analysis.

What this report covers

Every action we and the bank took to contain and eradicate the attacker, from Saturday, July 4, 01:16 EDT to Thursday, July 9, 09:00 EDT, is in the register below, with who approved it, what was read before the change, how we checked it, and how to undo it. The incident role was deployed 42 minutes after we joined the bridge, and the containment policy was attached 4 hours 18 minutes after the attacker's first write-capable call. Both numbers are in the elapsed-time table.

Operational means the bank's incident and platform teams. The report is not part of the counsel track and holds no legal analysis. It says what changed in the estate, in the order it changed, so a responder can repeat it, check it, or reverse it. It makes no statement about notification, privilege, or any regime. Those are in the counsel-track reports.

What it does not cover. It does not describe the attack (the Investigation's narrative does), the root causes, the evidence's custody, or the notification clocks. It lists no hours. The guardrail policies are in the appendix as code. Times are Eastern Daylight Time (EDT, UTC-4). Every EV- number is an event in the organization trail that a responder can look up.

How approval worked. Mireille Danvers, the sponsor, approved every containment and eradication action on the bridge, before it was taken, except the workload decisions in A-09, A-19, and A-29, which Rafael Quintero and Lucía Brandt approved. Rafael Quintero also approved A-15 and A-16 with the sponsor. Imani Castell executed every change in AWS through the bank's identity provider with MFA, in the management account, through the bank's break-glass role in the workload accounts, and through the account-access or copy roles in the two new accounts. The break-glass role is exempt from the containment policy by name, and we reviewed each change. Lucía Brandt executed the loan platform's own offline and online steps (A-09 and A-29), and Mireille Danvers executed the written declaration (A-31). We made no change in the bank's accounts. Our role read (A-36 is its capture of the share, the key policies, and the grants), and in the evidence account it can only add new objects. The removals that closed the exfiltration path (A-37 to A-39) were made by Imani Castell in the break-glass role.

How fast, in elapsed time

The containment policy went on 4 hours 18 minutes after the first write-capable call, and the closing steps followed within minutes of each alert. The table gives each interval from the recorded times.

Elapsed times between the recorded events, computed from the times as shown to the minute. The incident role's 42-minute figure is measured from our joining the bridge, not from activation. The share's 137 minutes run from the `ModifyDBSnapshotAttribute` that added the account to the one that removed it.

Interval	From (EDT)	To (EDT)	Elapsed
First write-capable call to the containment SCP	Friday, July 3, 21:04 EDT	Saturday, July 4, 01:22 EDT	4 hours 18 minutes
GuardDuty finding to the containment SCP	Friday, July 3, 22:44 EDT	Saturday, July 4, 01:22 EDT	2 hours 38 minutes
The page to the containment SCP	Friday, July 3, 23:18 EDT	Saturday, July 4, 01:22 EDT	2 hours 4 minutes
Emergency activation to the containment SCP	Saturday, July 4, 00:52 EDT	Saturday, July 4, 01:22 EDT	30 minutes
We join the bridge to the incident role deployed	Saturday, July 4, 00:58 EDT	Saturday, July 4, 01:40 EDT	42 minutes
The outside account is added to the database snapshot's share to the share removed	Friday, July 3, 23:51 EDT	Saturday, July 4, 02:08 EDT	137 minutes
The SCP to the exfiltration path closed (the last of five steps)	Saturday, July 4, 01:22 EDT	Saturday, July 4, 02:10 EDT	48 minutes
The SCP to the stolen key inactive	Saturday, July 4, 01:22 EDT	Saturday, July 4, 01:24 EDT	2 minutes
The SCP to the attacker's batch job canceled	Saturday, July 4, 01:22 EDT	Saturday, July 4, 01:28 EDT	6 minutes
Pursuit's alert on the second key to the SCP update	Saturday, July 4, 02:50 EDT	Saturday, July 4, 02:58 EDT	8 minutes
The attacker's `AssumeRole` of `OrgAccessBackup` to the RCP	Saturday, July 4, 01:36 EDT	Saturday, July 4, 03:20 EDT	1 hour 44 minutes

The action register

The register holds 46 actions, in the order they were taken, on the landscape pages that follow. Each row names the approver and the executor, what was read or saved before the change, what we checked after it, the way back, and the result. Stage numbers are those of the situation reports. Every change in a workload account went through the bank's break-glass role, which the containment policy exempts by name, and the changes in the two new accounts went through the account-access or copy roles. Rows A-32 to A-35 are the evidence account's own controls. They sit among the Stage 1 rows by time. The organization trail export we hold has no event for them, so their evidence column points to the custody log.

Actions A-01 to A-04

Register rows A-01 to A-04: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-01	Sat 01:16:31	1	Create the containment SCP `wf-incident-containment` from our template	`wf-management`; policy `p-wrnfcontain01`	Mireille Danvers	Imani Castell	Template reviewed on the bridge; the Workloads OU's policy list read	Policy text read back and matched to the draft	Delete the policy (not yet attached)	Created. `EV-00536`
A-02	Sat 01:22:15	1	Attach the SCP to the Workloads OU	OU `ou-wrnf-wl000001` (ten workload accounts)	Mireille Danvers	Imani Castell	Organization trail unaltered in `wf-log-archive`; attacker events read	First denial 01:24:35 (`EV-00544`); also 01:31 (`EV-00566`) and 01:39 (`EV-00570`)	Detach the policy from the OU	Attached. `AssumeRole` is not denied by design, so sessions ran on (A-03, A-04). At 01:36 the attacker assumed `OrgAccessBackup` as an administrator (`EV-00569`); the SCP blocked only the delete after it. `EV-00537`
A-03	Sat 01:24:30	1	Set the stolen key `AKIAWRFNEXAMPLE00001` to Inactive	`wf-tools`; IAM user `svc-artifact-sync`	Mireille Danvers	Imani Castell	Key's last-used data and its trail calls read and saved	No call by the key after 01:24:30	Set Active (not advised; the key is stolen)	Inactive. `EV-00543`
A-04	Sat 01:26:05 to 01:26:41	1	Revoke active sessions of `wf-deploy-pipeline` with an inline deny policy `AWSRevokeOlderSessions` (10 accounts)	Role `wf-deploy-pipeline`, every workload account	Mireille Danvers	Imani Castell	Role trust and policies read in each account	No `AssumeRole` of the role by the attacker after 01:24:05	Delete the inline policy in each account (new sessions were never affected)	Applied 01:26. `EV-00555` to `EV-00564`

Actions A-05 to A-08

Register rows A-05 to A-08: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-05	Sat 01:28:05	1	Cancel the attacker's S3 Batch Operations job	`wf-prod-imaging`; job `45eb31f1-d889-53b5-ac3d-236b4a64dea8`	Mireille Danvers	Imani Castell	`DescribeJob` output and the inventory manifest saved. The job's report was disabled, so there is no completion report	Job status canceled; counters stopped	None. A canceled job cannot resume	Canceled after 3 hours 47 minutes. `EV-00565`
A-06	Sat 01:31:40	1	Create the self-managed StackSet `VantalectIncidentResponse`, execution role `wf-break-glass`	`wf-management`	Mireille Danvers	Imani Castell	Template and trust read by the bank: one named principal, MFA, source identity. The execution role is exempt from the SCP	StackSet listed; instances follow in A-08	Delete the stack instances, then the StackSet	Created. `EV-00567`
A-07	Sat 01:35:12	1	Remove the attacker's lifecycle rule from the imaging archive	`wf-prod-imaging`; bucket `wf-imaging-archive-prod`	Mireille Danvers	Imani Castell	Rule text saved: expire noncurrent versions after one day	Bucket lifecycle read back: no rules	Re-put the attacker's rule (not wanted)	Removed. `EV-00568`
A-08	Sat 01:39:30 to 01:40:31	1	Deploy our incident role `VantalectIncidentResponse` to 19 accounts by stack instances, and to `wf-management` by a separate stack (20 roles created)	Every account, us-east-1	Mireille Danvers	Imani Castell	Trust reviewed: named principal `charles-sieg`, MFA, source identity. CloudFormation assumes the exempt `wf-break-glass` in each account	First reads 01:44 to 01:54 in six accounts (`EV-00613` to `EV-00624`). `wf-management` got its copy from the separate stack	Delete the stack instances, and the separate stack in `wf-management`	Deployed 01:39 to 01:40, 42 minutes after we joined the bridge. `EV-00571` to `EV-00612`

Actions A-09, A-36, A-37, and A-38

Register rows A-09, A-36, A-37, and A-38: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-09	Sat 01:50	1	Take loan origination offline to freeze its state	`wf-prod-lending`; the application tier	Rafael Quintero and Lucía Brandt	Lucía Brandt	Database instance settings and the application queue read	Platform health shows offline; no new applications written	Return to service after integrity checks (A-29)	Offline. No API event; the bank's decision
A-36	Sat 02:03:10 to 02:05:00	1	Capture the snapshot's sharing attributes, the three attacker key policies, and the grants on each key, before any change (7 reads)	Lending, imaging, and data accounts; the snapshot and three attacker keys	Mireille Danvers	Charles Sieg (Vantalect)	Nothing changed yet; our role only reads	Outputs saved and hashed for the custody log (no evidence account until 03:12)	Not applicable (read-only)	Captured 02:03 to 02:05. `EV-00625` to `EV-00631`
A-37	Sat 02:08:20	1	Remove account `777788889999` from the snapshot's restore attribute (`ModifyDBSnapshotAttribute`, remove)	`wf-prod-lending`; snapshot `wf-los-prod-bk-20260703`	Mireille Danvers	Imani Castell	Share captured 02:03:10 (A-36); the add was 23:51:12 (`EV-00520`)	Sharing attributes read back	Add the account back (not wanted)	Removed 02:08:20. The share was open 137 minutes. `EV-00632`
A-38	Sat 02:09:05 to 02:09:45	1	Replace each attacker key's policy with one that names only the owning account, which drops the statement for `777788889999` (3 keys)	Lending, imaging, and data production accounts; the three attacker keys	Mireille Danvers	Imani Castell	The three policies captured 02:03:40 to 02:04:10 (A-36)	Policies read back: no outside principal	Re-put the captured policy (not wanted)	Applied 02:09:05, 02:09:25, and 02:09:45. `EV-00633` to `EV-00635`

Actions A-39, A-10, A-11, and A-12

Register rows A-39, A-10, A-11, and A-12: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-39	Sat 02:10:30	1	Revoke the attacker's KMS grant on the lending key. The RDS service grant was already retired at 00:51:06 (`EV-00531`)	`wf-prod-lending`; the lending attacker key	Mireille Danvers	Imani Castell	Grant list captured 02:04:30 (A-36)	Grant list read back: no grant for the attacker	None. A revoked grant cannot be restored	Revoked 02:10:30. The exfiltration path was closed. `EV-00636`
A-10	Sat 02:58:12	1	Update the SCP: deny everything for the attacker's user and two roles, and close the gaps the first policy left (IAM persistence, `GetFederationToken`, Recycle Bin changes, recovery-point deletes, object deletes in the imaging archive bucket, use of the three attacker keys)	`p-wrnfcontain01`; `aws-support-sync`, `OrgAccessBackup`, `s3-batch-replication`	Mireille Danvers	Imani Castell	The user, key, and two roles the attacker created, read from the trail (Pursuit live from 02:20, its alert on the second key at 02:50)	The attacker's `ListUsers` at 02:59 and 03:00 denied (`EV-00643`, `EV-00644`)	Remove the statement `DenyAttackerPrincipals` and the three statements added after it	Updated. `EV-00642`
A-11	Sat 03:01:10	1	Set the second key `AKIAWRFNEXAMPLE00002` to Inactive	`wf-prod-data`; IAM user `aws-support-sync`	Mireille Danvers	Imani Castell	Use from `203.0.113.47` at 02:47 to 02:50 saved (`EV-00637` to `EV-00641`)	No allowed call by the user after 02:50; none at all after 03:00	Set Active (not advised)	Inactive. `EV-00646`
A-12	Sat 03:11:20 to 03:14:40	1	Create the Incident OU and the evidence account, and move the account into the OU	OU `ou-wrnf-ir000001`; account `wf-ir-forensics` (`584729107701`)	Mireille Danvers	Imani Castell	Nothing to preserve: a new, empty account	Account active and in the OU	Close the account (not wanted once evidence is in it)	Created 03:11 to 03:14. `EV-00647` to `EV-00649`

Actions A-40, A-13, A-14, and A-32

Register rows A-40, A-13, A-14, and A-32: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-40	Sat 03:15:10 to 03:16:40	1	Enable the resource control policy type at the root, and list the outside trusts the RCP will cut (Access Analyzer)	`wf-management` root; analyzer `wf-org-external-access` in `wf-audit`	Mireille Danvers	Imani Castell	Not applicable (type not yet enabled)	Two outside trusts: the attacker's `OrgAccessBackup` and our role (exempt). No other to cut	Detach the RCP (A-13), then disable the policy type	Enabled 03:15:10; listed 03:16:40. `EV-00650` to `EV-00652`
A-13	Sat 03:19:05 to 03:20:14	1	Create and attach the RCP `wf-deny-outside-access` (outside principals: STS role sessions, `kms:*`, `s3:*`)	Workloads OU; policy `p-wrnfrcp00001`	Mireille Danvers	Imani Castell	The 01:36 `AssumeRole` (`EV-00569`) saved; outside trusts listed (A-40)	Policy and attachment read back. Its effect is shown by its text and the absence of any allowed outside use after 03:20, not by a logged deny: a denied request is logged only in the caller's account	Detach the policy	Attached 03:20:14. `EV-00653` to `EV-00654`
A-14	Sat 03:40:12 to 03:41:03	1	Create the evidence bucket and set Object Lock in compliance mode, seven years	`wf-ir-forensics`; bucket `wf-ir-evidence`	Mireille Danvers	Imani Castell	Not applicable (new bucket)	Lock configuration read back	None, by design: compliance mode cannot be shortened	Created 03:40, locked 03:41. `EV-00656` to `EV-00657`
A-32	Sat 03:46	1	Create the evidence key `alias/wf-ir-evidence`, origin AWS KMS, administered by the bank	`wf-ir-forensics`; key `alias/wf-ir-evidence`	Mireille Danvers	Imani Castell	Not applicable (new key)	Key policy read back	Scheduling deletion is limited to the bank's custodian role; not planned	Created 03:46. No event for this change in the organization trail export we hold. The custody log records it.

Actions A-33, A-34, A-35, and A-15

Register rows A-33, A-34, A-35, and A-15: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-33	Sat 03:52	1	Attach the SCP `wf-evidence-deny-all` to the Incident OU: deny all actions except the custodian role	OU `ou-wrnf-ir000001`; policy `p-wrnfevid00001`	Mireille Danvers	Imani Castell	Not applicable (new policy)	Policy read back on the OU	Detach the policy; only the management account can	Attached 03:52. No event for this change in the organization trail export we hold. The custody log records it.
A-34	Sat 03:52	1	Put the one exempt role in the evidence account: `wf-evidence-custodian` (the bank). Vantalect holds no role in the account	`wf-ir-forensics`	Mireille Danvers	Imani Castell	Not applicable (new role)	Rights read back: the custodian role can add objects, set or release a legal hold on counsel's written instruction, and administer the key; no other principal can act in the account	Delete the role	In place by 03:52. No event for this change in the organization trail export we hold. The custody log records it.
A-35	Sat 03:56	1	Turn on S3 server access logging for `wf-ir-evidence`, to a separate log bucket in `wf-ir-forensics` (the log bucket must be in the same account and Region)	`wf-ir-forensics`; bucket `wf-ir-evidence`	Mireille Danvers	Imani Castell	Not applicable (new bucket)	Logging setting read back	Turn the logging off (not planned)	On 03:56; first item sealed 04:02. No event for this change in the organization trail export we hold. The custody log records it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-15	Sat 04:29:20 to 04:34:10	1	Create the Recovery OU and the vault account, and attach the deny-all SCP `wf-vault-deny-all`	OU `ou-wrnf-rc000001`; account `wf-recovery-vault` (`584729107714`); `p-wrnfvault0001`	Mireille Danvers and Rafael Quintero	Imani Castell	Not applicable (new account)	Policy listed on the OU; account active	Detach the policy; close the account	Created 04:29 to 04:34. `EV-00658` to `EV-00663`

Actions A-16 to A-19

Register rows A-16 to A-19: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-16	Sat 04:40:10	1	Create the vault keys, origin AWS KMS, held by the bank (3 keys)	`wf-recovery-vault`; alias `alias/wf-vault`	Mireille Danvers and Rafael Quintero	Imani Castell	Not applicable (new keys)	Key origin and state read: AWS KMS, enabled	Schedule key deletion (the seven-day minimum wait)	Created 04:40. `EV-00667` to `EV-00669`
A-17	Sat 07:40:05 to 07:41:38	2	Restore the deleted volume snapshots from the Recycle Bin (46 snapshots)	`wf-prod-lending` and `wf-prod-data`	Mireille Danvers	Imani Castell	The deletion events and the session change between them (`EV-00454` to `EV-00500`) and the Recycle Bin listing preserved	Every restored snapshot listed as available	Delete the restored snapshots (not wanted)	Restored 07:40 and 07:41. `EV-00673` to `EV-00719`
A-18	Sun 05:10:00 to 07:50:00	3	Restore the month-end database snapshots from the central backup account (9 snapshots)	`wf-backup` to `wf-prod-lending`; key `alias/wf-rds`	Mireille Danvers	Imani Castell	The deletion events (`EV-00444` to `EV-00452`) preserved; the copies in `wf-backup` listed	Every restored snapshot available	Delete the restored copies (the originals in `wf-backup` remain)	Sunday 05:10 to 07:50, one every 20 minutes. `EV-00722` to `EV-00732`

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-19	Sun 08:50:11 to Tue 10:58:40	3	Create role `s3-batch-restore` and the bank's 31 sequential S3 Batch slice jobs that copy noncurrent bank-key versions back as current (31 slice jobs)	`wf-prod-imaging`; bucket `wf-imaging-archive-prod`	Rafael Quintero and Lucía Brandt	Imani Castell	The attacker's `DescribeJob` output (progress summary, status history, manifest location), the inventory manifest, and the version listing saved first. No completion report exists	Counters read after each slice. Tuesday 14:00: the slice jobs' completion reports read, and, after a canary object written at 13:20 showed that the bucket's S3 Metadata live inventory table covered writes through 13:20 (after the last slice finished at 12:40), two Athena count queries over that table (the three queries are `EV-01034`, `EV-01036`), per the bank, found no current version under an attacker key (bank-reported; the query results are not independently preserved). S3 Inventory is a scheduled report and cannot be run on demand; its next report would confirm encryption-type coverage, not which KMS key encrypted each version	Cancel the running slice (the versions stay where they are)	First slice Sunday 08:58; last created Tuesday 10:58; done Tuesday 12:40 (329.6 objects a second). `EV-00735` to `EV-01029`

Actions A-41, A-42, A-20, and A-43

Register rows A-41, A-42, A-20, and A-43: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-41	Sun 09:30:00 to 09:30:50	3	Let the vault copy role read the bank's three source keys for a copy (key-policy grant) (3 keys)	`wf-prod-lending` (two keys) and `wf-prod-data` (one key); role `wf-vault-copy-in`	Mireille Danvers and Rafael Quintero	Imani Castell	Current key policies read and saved	Policies read back: one added statement for the copy role	Re-put the saved key policy (the source keys are in the bank's accounts)	Applied Sunday 09:30. `EV-00741` to `EV-00744`
A-42	Sun 10:00:00	3	Share each source database snapshot with the vault account (10 snapshots)	`wf-prod-lending`; account `584729107714`	Mireille Danvers and Rafael Quintero	Imani Castell	Sources: nine month-end snapshots and `wf-los-prod-manual-20260703-2122`	Sharing attribute read back on each: the vault account only	Remove the account from the attribute	Shared Sunday 10:00 to 10:04. `EV-00745` to `EV-00754`
A-20	Sun 12:00:00 to Mon 16:03:00	3	Copy the live snapshot first, then each month-end database snapshot, into the vault under a vault key (not locked) (10 copies)	`wf-recovery-vault`; role `wf-vault-copy-in`	Mireille Danvers	Imani Castell	Source snapshot metadata saved	Each copy available under a vault key; size and engine match the source	No lock. The vault SCP denies deletes, so an SCP change comes first	Sunday 12:00 to Monday 16:03. `EV-00759` to `EV-00990`
A-43	Sun 22:00:00 to 22:02:15	3	Share each restored volume snapshot with the vault account (46 snapshots)	`wf-prod-lending` and `wf-prod-data`; account `584729107714`	Mireille Danvers and Rafael Quintero	Imani Castell	The restored snapshots listed (A-17); their keys are the bank's	Sharing attribute read back on each	Remove the account from the attribute	Shared Sunday 22:00 to 22:02. `EV-00788` to `EV-00834`

Actions A-21, A-44, A-45, and A-22

Register rows A-21, A-44, A-45, and A-22: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-21	Mon 02:00:00	3	Copy the restored volume snapshots into the vault under a vault key (46 snapshots)	`wf-recovery-vault`; role `wf-vault-copy-in`	Mireille Danvers	Imani Castell	Restored snapshots' metadata saved	Each copy available; size and encrypted flag match the source	Delete before the lock (A-44); the vault SCP denies it, so an SCP change first	Monday 02:00 to about 05:22. `EV-00847` to `EV-00902`
A-44	Mon 05:45:00	3	Lock each volume snapshot copy: compliance mode, 14 days, cooling-off 72 hours (`LockSnapshot`) (46 snapshots)	`wf-recovery-vault`; the 46 volume snapshot copies	Mireille Danvers	Imani Castell	All 46 copies verified (A-21)	Each lock read back: state compliance, in cooling-off	Unlock only in the cooling-off, after an SCP change (the SCP denies unlock)	Locked Monday 05:45 to 05:48. `EV-00904` to `EV-00949`
A-45	Mon 06:10:00 to 14:20:00	3	Create Backup vault `wf-recovery`, restore `wf-los-vault` from the live snapshot, create the service role `wf-backup-service` and exempt it in the vault SCP, and back the database up into the vault (one recovery point)	`wf-recovery-vault`; backup vault `wf-recovery`; database `wf-los-vault`	Mireille Danvers and Rafael Quintero	Imani Castell	Not applicable (new Backup vault and database). Deletion protection set on the database	Backup job started; the vault holds one recovery point of the live database	Delete the recovery point until the cooling-off ends (A-22)	Vault 06:10; database 06:40; role and SCP exemption 13:30 to 13:40; backup job 14:20. `EV-00950` to `EV-00982`
A-22	Mon 19:30:05	3	Set Vault Lock on the Backup vault: compliance mode, minimum 14 days, cooling-off 3 days. It covers recovery points in `wf-recovery`, today the one in A-45	`wf-recovery-vault`; backup vault `wf-recovery`	Mireille Danvers	Imani Castell	The recovery point exists (A-45)	Lock configuration read back	Delete the configuration until the cooling-off ends; none after	Set Monday 19:30. `EV-00998`

Actions A-23 to A-26

Register rows A-23 to A-26: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-23	Wed 10:00:30 to 10:01:20	4	Detach the administrator policy, delete the second key, and delete the user `aws-support-sync`	`wf-prod-data`	Mireille Danvers	Imani Castell	User, policy, key metadata, and last-used data exported and hashed; trail events preserved	`GetUser` returns no such entity	None (deleted). The export holds the configuration	Deleted Wednesday 10:00 to 10:01. `EV-01045` to `EV-01047`
A-24	Wed 10:01:45 to 10:02:10	4	Detach the administrator policy and delete the role `OrgAccessBackup`	`wf-prod-lending`	Mireille Danvers	Imani Castell	Role trust and policy exported and hashed	`GetRole` returns no such entity	None (deleted). The export holds the configuration	Deleted 10:01 to 10:02. `EV-01048` to `EV-01049`
A-25	Wed 10:02:35 to 10:03:00	4	Delete the role policy and the role `s3-batch-replication`	`wf-prod-imaging`	Mireille Danvers	Imani Castell	Role policy `copy-all` and trust exported and hashed. The job has no report (disabled); its `DescribeJob` output was saved (A-05)	`GetRole` returns no such entity	None (deleted). The export holds the configuration	Deleted 10:02 to 10:03. `EV-01050` to `EV-01051`

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-26	Wed 10:03 to 10:04	4	Call `DisableKey` on each of the three attacker keys and read each key with `DescribeKey`; hold the keys as they are, with no deletion. Material expired Tuesday 18:00 (PendingImport) (3 rejected calls)	Lending, imaging, and data production accounts; alias `alias/wf-backup-2026`	Mireille Danvers	Imani Castell	Key policies, grants, aliases, and metadata exported and hashed	Each `DisableKey` was rejected with `KMSInvalidStateException` (KMS does not accept it for a key in PendingImport). The `DescribeKey` after each returns `PendingImport`, not enabled. No change made. Outside statements removed July 4 (A-38)	Not applicable (no change made)	Three calls rejected; keys held in PendingImport for counsel. `EV-01052` to `EV-01057`

Actions A-27 to A-30

Register rows A-27 to A-30: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-27	Wed 10:05:00 to 10:08:00	4	Narrow the trust of `wf-deploy-pipeline` to the Jenkins role, with a source identity condition (10 accounts)	Role `wf-deploy-pipeline`, every workload account	Mireille Danvers	Imani Castell	Prior trust policy exported in each account	New trust policy read back in each account	Re-put the prior trust from the export (not advised)	Applied 10:05 to 10:08. `EV-01058`, `EV-01066` to `EV-01074`
A-28	Wed 10:10:00 to 10:11:00	4	Delete `svc-artifact-sync` and its key, and create the OIDC provider that replaces them	`wf-tools`	Mireille Danvers	Imani Castell	User, key metadata, and last-used data exported and hashed	Provider listed; the pipeline's first run with it is the bank's check	None for the user and key (deleted); delete the provider to undo	Applied 10:10 to 10:11. `EV-01075` to `EV-01077`
A-29	Wed 16:00	4	Return loan origination to service after integrity checks	`wf-prod-lending`	Rafael Quintero and Lucía Brandt	Lucía Brandt	The bank's integrity checks passed	Queued applications being processed	Take offline again	Online after 110 hours 10 minutes. No API event; the bank's decision

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-30	Wed 16:30:00 to 18:25:00	4	Create the vault's Object Lock bucket, put a replication rule on the imaging archive toward it, build a manifest of the current versions under the bank's key with an Athena `UNLOAD` over the live inventory table (18:12), and start an S3 Batch Replication job over it (18:25, `s3ReplicateObject`)	`wf-recovery-vault` bucket `wf-imaging-archive-vault`; source `wf-imaging-archive-prod`	Mireille Danvers	Imani Castell	The source bucket's version listing saved	Rule read back. It copies new writes only. The job's description names 286,000,000 current versions, and its completion report is enabled. The job was still running when this report was written	Remove the replication rule. Copies already written stay in the bucket. Object Lock is enabled on it, but no default retention or per-object retention was set, so the copies are not locked	Rule put Wednesday 17:05; replication job started 18:25 and running. Its finish and result: open item. `EV-01090` to `EV-01101`

Actions A-46, and A-31

Register rows A-46, and A-31: what was changed, who approved and made the change, what was read before it and checked after it, and how to undo it.

ID	Time (EDT)	Stage	Action	Account and resource	Approver	Executor	Evidence before	Verification after	Rollback	Result
A-46	Wed 16:45:00	4	Update the vault SCP once setup is done: `OrganizationAccountAccessRole` (full administrator rights, trusted by the management account) and the backup service role `wf-backup-service` are no longer exempt, so each is denied by name and only the two copy roles can act in the vault	`p-wrnfvault0001` on the Recovery OU; the roles `wf-vault-copy-in` and `wf-vault-copy-out` stay exempt, each with MFA and two-person approval	Mireille Danvers	Imani Castell	The last call that needed the setup role (the archive key's alias, 16:20) was done, and the bucket and its policy were written by `wf-vault-copy-in`	Policy read back: statement one exempts the two copy roles only. Anyone with administrator access in the management account can still change this SCP (R-3)	Add the role back to the exemption list in the management account	Updated Wednesday 16:45. `EV-01092`
A-31	Thu 09:00	5	Declare containment in writing	The Response	Mireille Danvers	Mireille Danvers	This register and the last situation report	Not applicable	Not applicable. The Response ends	Declared. No API event; the bank's written declaration

Credentials disabled and sessions revoked

Every credential and role the attacker held was cut off by 03:20 on Saturday, and every one was deleted or removed by Wednesday at 10:11. The attacker's account lost the use of the three KMS keys on Saturday at 02:09, when the bank removed its statement from each key policy (A-38), and its grant at 02:10:30 (A-39). The keys themselves were kept for counsel. Temporary credentials the attacker's sessions had already been issued either expired or were covered by the deny policies below.

Credentials and principals the attacker held or made, and ours (part 1): what stopped each, what removed it, and where the proof is.

Credential or principal	Account	Disabled, denied, or revoked	Then	Evidence
IAM user `svc-artifact-sync`, key `AKIAWRFNEXAMPLE00001`	`wf-tools`	Key Inactive Saturday 01:24 (A-03)	Key and user deleted Wednesday 10:10 (A-28)	`EV-00543`; `EV-01075`, `EV-01076`
Sessions of role `wf-deploy-pipeline`	Every workload account	Older sessions revoked Saturday 01:26 (A-04), by an inline deny on token issue time	Trust narrowed Wednesday 10:05 to 10:08 (A-27)	`EV-00555` to `EV-00564`; `EV-01058`, `EV-01066` to `EV-01074`
IAM user `aws-support-sync`, key `AKIAWRFNEXAMPLE00002`	`wf-prod-data`	Denied everything by the SCP Saturday 02:58 (A-10); key Inactive 03:01 (A-11). Temporary credentials from `GetSessionToken` (`EV-00640`) act as the user, so the same deny covers their authorized resource actions; the SCP does not prevent `GetSessionToken` issuance	Policy detached, key and user deleted Wednesday 10:00 to 10:01 (A-23)	`EV-00642`, `EV-00646`; `EV-01045` to `EV-01047`
Role `OrgAccessBackup` (trusts `777788889999`)	`wf-prod-lending`	Assumed successfully at 01:36 (administrator session, `EV-00569`); the SCP blocked only the 01:39 delete (`EV-00570`). Denied by the SCP from 02:58; new assumptions from outside denied by the RCP from 03:20 (A-13). A denied cross-account `AssumeRole` is not logged in the bank's trail, so none appears there	Policy detached and role deleted Wednesday 10:01 to 10:02 (A-24). The role's outside trust was still present on July 4 (A-40)	`EV-00642`, `EV-00654`; `EV-01048`, `EV-01049`

Credentials and principals the attacker held or made, and ours (part 2).

Credential or principal	Account	Disabled, denied, or revoked	Then	Evidence
Role `s3-batch-replication`	`wf-prod-imaging`	Denied by the SCP Saturday 02:58 (A-10)	Role policy and role deleted Wednesday 10:02 to 10:03 (A-25)	`EV-00642`; `EV-01050`, `EV-01051`
The three attacker KMS keys	Lending, imaging, and data production accounts	The statement naming `777788889999` was dropped from each key policy Saturday 02:09 (A-38), and the attacker's grant was revoked at 02:10:30 (A-39). Imported material expired Tuesday 18:00 (the attacker's own `ValidTo`), so each key is in PendingImport	Kept as they are for counsel, with deletion not scheduled (A-26). The bank's `DisableKey` calls on Wednesday 10:03:30 to 10:04:20 were each rejected with `KMSInvalidStateException`, because a key in PendingImport cannot be disabled; no key change succeeded on Wednesday. The captured policies, not a live statement, are the evidence	`EV-00633` to `EV-00636`; `EV-01037` to `EV-01039`; rejected calls `EV-01052`, `EV-01054`, `EV-01056`
Our own incident role `VantalectIncidentResponse`	Every account	Not disabled. It trusts one named principal, requires MFA and a source identity, and stays for the Investigation	Removal is part of the closure sweep if the bank engages the Recovery, and otherwise on the bank's request	`EV-00574` to `EV-00612`

Jobs canceled and settings reversed

The attacker's job was canceled, the share and the key access were removed, and every change that could be reversed was reversed. 6 items are left as they are, and the last table says which and why.

The jobs and settings the attacker changed, and what we or the bank did about each (part 1).

What	Where	What was done	State
The attacker's S3 Batch Operations job	`wf-prod-imaging`	Canceled Saturday 01:28 (A-05). Its partial output was left untouched until preserved	Not reversible. The bank rewrote the affected objects itself (A-19)
The attacker's lifecycle rule on the imaging archive	`wf-imaging-archive-prod`	Removed Saturday 01:35 (A-07)	Reversed. No noncurrent version was ever expired by it
The share of the loan database snapshot copy `wf-los-prod-bk-20260703` with `777788889999`	`wf-prod-lending`	Removed Saturday 02:08:20 (A-37), after the sharing attributes were captured. The share had been open 137 minutes	Reversed. Nothing left in the snapshot's sharing

The jobs and settings the attacker changed (part 2).

What	Where	What was done	State
The attacker's account in the three attacker key policies, and its KMS grant	Lending, imaging, and data production accounts	Statements dropped Saturday 02:09 (A-38); grant revoked 02:10:30 (A-39)	Reversed. The captured policies and grant list are the record
The deleted volume snapshots	Lending and data production accounts	Restored from the Recycle Bin Saturday 07:40 and 07:41 (A-17)	Reversed
The deleted month-end database snapshots	`wf-prod-lending`	Restored from `wf-backup` Sunday 05:10 to 07:50 (A-18)	Reversed

The jobs and settings the attacker changed (part 2).

What	Where	What was done	State
Objects under the attacker's keys	`wf-imaging-archive-prod`	Rewritten as current versions under the bank's key by the bank's own 31 slice jobs (A-19)	Reversed, bank-reported: none current under an attacker key at expiry, read on Tuesday 14:00 from the slice jobs' completion reports and the live inventory table (A-19); the query results are not independently preserved. The next scheduled S3 Inventory report would confirm encryption-type coverage, not key identity
Loan origination taken offline	`wf-prod-lending`	Back online Wednesday 16:00 (A-29)	Reversed
The vault SCP's exemptions of `OrganizationAccountAccessRole` (full administrator rights, trusted by the management account) and, from 13:40 on July 6, of the backup service role `wf-backup-service`	`wf-recovery-vault`, Recovery OU	Both dropped from the exemption list at 16:45 on July 8 (A-46), once the last setup call was done and the backup job had long finished. Each role is denied by name; the two copy roles, each with MFA and two-person approval, are the only principals left	In place. Anyone with Organizations rights in `wf-management` can still change this SCP (R-3 in the Investigation)

The items the Response did not reverse, and the reason for each (part 1).

Left as it is, on July 9	Why, and who decides
Deletion protection on `wf-los-prod` was turned off by the attacker at 00:47 (`EV-00529`)	No change back appears in the trail through July 9. The SCP's deny on `rds:DeleteDBInstance` and `rds:ModifyDBInstance` stands in its place. The bank decides when to set it again; the Recovery plans it for week three.
The attacker-key database snapshot copy `wf-los-prod-bk-20260703` still exists	It is no longer shared: the share was removed Saturday at 02:08:20 after 137 minutes (A-37). The copy is kept as it is until counsel directs, and the SCP denies deleting it. The Recovery plans its removal, after preservation, for week three.
The legacy trail `wf-lending-legacy-trail` was deleted by the attacker at 22:14 (`EV-00501`)	Not recreated. The organization trail is the record. The bank decides whether to restore the legacy trail; the Recovery takes up the decision in week three.
The attacker-key copies of the volume snapshots and of the database snapshot	Kept as evidence. Their keys' material expired Tuesday at 18:00 and the keys are in PendingImport. The bank's `DisableKey` calls on Wednesday were rejected for that state (A-26), so the keys stay as they are. Deletion waits for counsel's direction.

The items the Response did not reverse (part 2).

Left as it is, on July 9	Why, and who decides
The broad `kms:CreateGrant` deny in the containment SCP	A narrower deny is recommended (the appendix gives the reason). The gaps the first policy left were closed by the 02:58 update; the appendix lists them. The bank decides on the grant deny in the Recovery.
The vault copy of the imaging archive's existing objects is not complete	The rule (A-30) copies new writes only. For the existing objects the bank started an S3 Batch Replication job on Wednesday at 18:25 (`EV-01101`) over a manifest of the current versions under the bank's key, with its completion report enabled. It was still running when this report was written, and a job of that size runs for days. Versions that are not current, among them the versions under the attacker keys, are not in the manifest. Its result, any failed tasks, and a read-back of the vault bucket are open. The bank decides what check closes the item.

The recovery vault

The vault is a separate account that the attacker's account, the deploy role, and our own role cannot enter. What protects each kind of copy differs, and only some of it is a lock. Its design is the answer to the question "what if the attacker comes back." Every copy sits under a key the bank holds, and the vault's SCP denies deleting any copy. The 46 volume snapshot copies are also locked, and one recovery point of the live database is under Vault Lock. The 10 database snapshot copies are plain snapshots and are not locked. The weakest link is in the design table below, and the bank has not yet decided what to do about it.

The vault's design, what protects each kind of copy, the reason for each part, and the open decision on the setup role.

Part	Design	Why
Account	`wf-recovery-vault` (`584729107714`), in the Recovery OU, created Saturday, July 4, 04:30 EDT	A new account holds nothing the attacker ever touched
Guardrail	The SCP `wf-vault-deny-all` on the OU. Statement one denies everything except the roles `wf-vault-copy-in` and `wf-vault-copy-out`. As created it also exempted the account's `OrganizationAccountAccessRole`, which the bank's administrator used for the setup calls, and from 13:40 on July 6 it exempted the backup service role `wf-backup-service` too, so that AWS Backup could take the live database's recovery point (`EV-00981`, A-45). The update at 16:45 on July 8 (`EV-01092`, A-46) removed both, so each is denied by name. Statement two denies, for everyone, deleting or unsharing a snapshot, unlocking one, and changing a key, its policy, or a grant	Only the two copy roles can act, each with MFA and two-person approval (the CISO approves and the platform engineer executes), and neither can delete a copy or change a key
Keys	Three keys, origin AWS KMS, held by the bank. No imported material	An imported-material key is how the attacker locked the archive
Our access	None. The vault was created after our StackSet ran	Nothing in the vault depends on us
Volume snapshot copies (46)	Snapshot lock in compliance mode, 14 days, cooling-off 72 hours (A-44), taken Monday 05:45 to 05:48	A locked copy cannot be deleted by a stolen administrator once the cooling-off ends
Database snapshot copies (10)	**Not locked.** Plain snapshots, protected only by the vault SCP and keys the bank holds	RDS snapshots have no lock of their own. Nobody should rely on a lock that is not there
Backup recovery point	AWS Backup vault `wf-recovery` with Vault Lock: compliance mode, 14 days minimum, cooling-off 3 days. It covers one recovery point of the live database (A-45). After Thursday, July 9, 19:30 EDT no one can remove the lock, including us	Vault Lock covers only recovery points in that Backup vault
Weakest link	Anyone with Organizations rights in `wf-management` can change the SCP, and an SCP never applies to the management account itself. Until 16:45 on July 8 the exempt `OrganizationAccountAccessRole` (full administrative permissions, trusted by the management account) was a second way in for anyone with administrator access there, and from 13:40 on July 6 the exempt `wf-backup-service` could act in the vault too (statement two still denied it deletes and key changes); A-46 closed both	The ten database copies rest on the SCP. The vault design leaves the two copy roles as the only principals that can act, each with MFA and two-person approval; the remaining risk is a person with Organizations rights, which no guardrail covers

Part	Design	Why
Evidence	Not in the vault. Evidence is in `wf-ir-evidence`, in a different account with its own Object Lock	A copy for recovery and a copy for the record should not share a failure

The copy-and-verify record. Before each copy the bank shared the source with the vault account and let the copy role read the source key (A-41 to A-43). A restore test of the application from the vault was not part of the Response. It is proposed for the Recovery.

What was copied	Source	When (EDT)	How it was verified	What protects the copy
Month-end database snapshots (nine)	`wf-backup`, restored into `wf-prod-lending` (A-18); shared with the vault account (A-42)	Sunday 15:07 to Monday 16:03	Vault copy role; snapshot available under a vault key; size and engine match	Plain snapshots, not locked. The vault SCP and keys the bank holds
The live database snapshot of `wf-los-prod`	`wf-prod-lending`, `wf-los-prod-manual-20260703-2122`	Sunday 12:00	The same checks; the attacker-key copy is not the one copied	Plain snapshot, not locked. The vault SCP and keys the bank holds
Volume snapshots (46)	Restored from the Recycle Bin (A-17); shared with the vault account (A-43)	Monday 02:00 to about 05:22	Vault copy role; snapshot available under a vault key; size and encrypted flag match	Snapshot lock, compliance mode, 14 days, cooling-off 72 hours (A-44)
A recovery point of the live database	`wf-los-vault`, restored in the vault account (A-45)	Monday 06:10 to 14:20	Backup job started into `wf-recovery`	Vault Lock, compliance mode, 14 days minimum (A-22)
The imaging archive	`wf-imaging-archive-prod`	Rule put Wednesday 17:05; replication job started 18:25 and running	Rule read back. It copies new writes only; the existing current versions under the bank's key are in an S3 Batch Replication job (A-30), whose result is an open item	**Not locked.** Object Lock is enabled on the bucket, but no default retention or per-object retention is configured or shown. Keys the bank holds

What the verification does and does not show. Each copy was checked by its state and metadata: the copy is available, it is under a vault key, and its size matches the source. That shows the copies exist and are intact as objects. It does not show that the database restores cleanly. The one restore we know of is the bank's restore of a snapshot copy as `wf-los-vault`, which gave the Backup job its source (A-45); it was not a test of the loan application. "Copied" is the claim for every copy. "Locked" is true of the 46 volume snapshot copies and the one recovery point only, and it is not true of the 10 database snapshot copies.

What we deliberately did not do, and why

We left 9 things undone on purpose, and each was a decision on the bridge. A responder reading this later should not have to guess whether a gap was an oversight.

- **We did not pay, offer to pay, or discuss paying.** No payment was made. The demand, its deadline, and the attacker's indicators belong to counsel, who screens them for sanctions before anyone considers anything else.
- **We did not contact the attacker or open the contact in the note.** Any contact is a decision for the bank and counsel. It would also tell the attacker which of their identities we had seen. The contact is withheld from this report.
- **We did not delete the attacker's user, key, or roles before preservation.** Deleting an identity destroys the best evidence of how it was made and used. We exported and hashed each one first, then removed it (A-23 to A-25).
- **We did not delete the attacker's three keys.** The keys in PendingImport keep the key history for counsel. Deletion cannot be undone. The bank's `DisableKey` calls on Wednesday were rejected for that state, so the keys are as they were when the material expired. The outside statement is already out of each policy (A-38), and the captured policies hold its text.
- **We did not touch the S3 Batch job's records until they were preserved.** The job's `DescribeJob` output (progress summary, status history, manifest location), the inventory manifest it used, and the version listing show which objects were changed. The job had its report disabled, so there is no completion report. The bank's rewrite started after all three were saved.
- **We did not leave the snapshot share open, or the attacker's account in the key policies, to keep them as evidence.** The evidence is the add and remove events, the capture taken first (A-36), and the key-policy history, not a live share. An open share would have let the attacker retry or finish a copy. We captured, then removed everything within six minutes of the capture ending (A-37 to A-39), all through SCP-exempt roles in Stage 1.

- **We did not delete the attacker-key copies of the snapshots.** They are the evidence of what was shared. Deletion cannot be undone and waits for counsel's direction.
- **We did not stop or restart any host, and we did not image any disk.** No host access was found. The loan platform's application and load-balancer logs show no attacker traffic, so stopping instances would have destroyed state to no purpose.
- **We did not attach the containment SCP to the management account or to the Security, Infrastructure, or Sandbox OUs.** An SCP does not apply to the management account. The attacker's destructive work was in the workload accounts, and a broader deny risked stopping the bank's own logging and backups.

Appendix: the guardrail policies as code

These are the policies as they stood on July 9. The containment SCP, its 02:58 update, the resource control policy, the vault's deny-all SCP, the session-revoking inline policy, and our incident role's trust policy are each valid JSON, printed exactly as the facts hold them. The identifiers are the bank's fictional organization (`o-wrnfld4x7q`) and our account (`111122223333`). The call that attached each one is named, so a responder can compare the text to the trail.

The containment SCP, as attached at 01:22

Attached to the Workloads OU by `EV-00537`, created by `EV-00536`. It denies the destructive and persistence actions for every principal except the incident role and the bank's break-glass role. The key-origin rule is its own statement so that its condition applies to `kms:CreateKey` only.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDestructiveAndPersistence",
      "Effect": "Deny",
      "Action": [
        "kms:ImportKeyMaterial",
        "kms:DeleteImportedKeyMaterial",
        "kms:ScheduleKeyDeletion",
        "kms:PutKeyPolicy",
        "kms:CreateGrant",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute",
        "rds:DeleteDBInstance",
        "rds:ModifyDBInstance",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
```

```
        "cloudtrail:DeleteTrail",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "iam:CreateUser",
        "iam:CreateAccessKey",
        "iam:CreateRole",
        "s3:CreateJob"
      ],
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    },
    {
      "Sid": "DenyKeysNotCreatedByAwsKms",
      "Effect": "Deny",
      "Action": "kms:CreateKey",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "kms:KeyOrigin": "AWS_KMS"
        },
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    }
  ]
}
```

Operational effects the bank accepted for the Response. The denies on `kms:CreateGrant` and `iam:CreateRole` apply to every principal in the ten Workloads accounts except the two exempt roles. Every encrypted EBS volume launch or attachment needs a grant, so users could not launch or attach one. The same holds for RDS restores and copies of encrypted snapshots, EBS `CopySnapshot` into an encrypted target, and AWS Backup jobs that use a customer-managed service role (a service-linked role is not affected the same way). No new IAM role could be created either, apart from the StackSet's, which passed because its execution role was the exempt `wf-break-glass` (A-06 and A-08). The bank accepted all of this, and the trail holds no denied call by a bank application. **What we would do now:** scope the `kms:CreateGrant` deny to the ARNs of the three attacker keys, or deny it only where `kms:GrantIsForAWSResource` is not true, so AWS services acting for the bank's own resources keep working. That is a recommendation, not a change made.

The containment SCP, as updated at 02:58

Updated by `EV-00642`. It adds four statements; the first two are unchanged. The third denies every action for the attacker's user and two roles, wherever they appear. The other three close what the 01:22 policy left open (the next section): the fourth denies the IAM persistence actions, `sts:GetFederationToken` (it also lists `sts:GetSessionToken`, but an SCP cannot block that call, which is an authentication operation), the Recycle Bin rule changes, and `backup:DeleteRecoveryPoint`; the fifth denies `s3:DeleteObject` and `s3:DeleteObjectVersion` in `wf-imaging-archive-prod` only; the sixth denies `kms:Encrypt`, `kms:GenerateDataKey*`, and `kms:ReEncrypt*` on the three attacker key ARNs only. The fourth to sixth keep the same two exemptions.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDestructiveAndPersistence",
      "Effect": "Deny",
      "Action": [
        "kms:ImportKeyMaterial",
        "kms:DeleteImportedKeyMaterial",
        "kms:ScheduleKeyDeletion",
        "kms:PutKeyPolicy",
        "kms:CreateGrant",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute",
        "rds:DeleteDBInstance",
        "rds:ModifyDBInstance",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "cloudtrail:DeleteTrail",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "iam:CreateUser",
        "iam:CreateAccessKey",
        "iam:CreateRole",
        "s3:CreateJob"
      ],
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    },
```

```
    {
      "Sid": "DenyKeysNotCreatedByAwsKms",
      "Effect": "Deny",
      "Action": "kms:CreateKey",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "kms:KeyOrigin": "AWS_KMS"
        },
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    },
    {
      "Sid": "DenyAttackerPrincipals",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:user/aws-support-sync",
            "arn:aws:iam::*:role/OrgAccessBackup",
            "arn:aws:iam::*:role/s3-batch-replication"
          ]
        }
      }
    },
    {
      "Sid": "DenyPersistenceAndRecoveryPointDeletion",
      "Effect": "Deny",
      "Action": [
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateLoginProfile",
        "iam:UpdateLoginProfile",
        "sts:GetFederationToken",
        "rbin:DeleteRule",
        "rbin:UpdateRule",
        "rbin:UnlockRule",
        "backup:DeleteRecoveryPoint"
      ],
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    },
```

```
    {
      "Sid": "DenyObjectAndVersionDeletesInTheAffectedBucket",
      "Effect": "Deny",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::wf-imaging-archive-prod/*"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    },
    {
      "Sid": "DenyUseOfTheAttackerKeys",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:ReEncrypt*"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:584729104402:key/b9885f41-4ff8-5cbf-9f54-7753a6180289",
        "arn:aws:kms:us-east-1:584729104415:key/6d9bd1af-48a0-5150-b619-9ab79ca2b680",
        "arn:aws:kms:us-east-1:584729104423:key/33767b29-2aaa-5253-83bf-0d1d670c1e43"
      ],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/VantalectIncidentResponse",
            "arn:aws:iam::*:role/wf-break-glass"
          ]
        }
      }
    }
  ]
}
```

What the first policy did not deny, and what the attacker did in that window

The policy attached at 01:22:15 left these actions open, and the 02:58 update above closed them. The attacker had two windows in which they could have used them: the user `aws-support-sync` from July 3, 22:31 EDT to the 02:58 update, and the role `OrgAccessBackup` from its assumption at 01:36:52 EDT. The last column is what the trail shows for the attacker's sessions after the SCP went on at 01:22:15. **Of these gaps the attacker used one, `sts:GetSessionToken`; the trail shows no object delete, no version delete, no KMS use of the attacker keys, no IAM write, no Recycle Bin call, and no recovery-point delete in the window.**

Actions the 01:22 policy did not deny, what each would protect, and what the trail shows. The 02:58 update denies them, with the KMS statement scoped to the three attacker key ARNs and the S3 deletes to `wf-imaging-archive-prod`, and with the same two exemptions.

Actions not denied until 02:58	What they would protect	Used in the window?
`s3:DeleteObjectVersion`, `s3:DeleteObject` in `wf-imaging-archive-prod`	The noncurrent bank-key versions, the only clean copies of the archive	None in the trail. The bank's rewrite later copied the noncurrent bank-key versions back (A-19), which is consistent with none having been deleted
`kms:Encrypt`, `kms:GenerateDataKey*`, `kms:ReEncrypt*` on the three attacker key ARNs	Per-object re-encryption could resume after the job was canceled	None in the trail. The one `ReEncrypt` (`EV-00525`, 00:07:02) came before the SCP
`rbin:DeleteRule`, `rbin:UpdateRule`, `rbin:UnlockRule`	The Recycle Bin rule that held the 46 deleted snapshots until the bank restored them (A-17)	None in the trail. The trail holds no `rbin` call by anyone
`iam:UpdateAssumeRolePolicy`, `iam:PutRolePolicy`, `iam:AttachRolePolicy`, `iam:CreateLoginProfile`, `iam:UpdateLoginProfile`	New persistence: a changed trust, a new policy, or a console password	None in the trail after 01:22:15. Earlier, before the SCP, the attacker made one `PutRolePolicy` (`EV-00392`) and one `AttachRolePolicy` (`EV-00514`)
`sts:GetFederationToken`, and `sts:GetSessionToken` (which no policy can deny)	Temporary credentials that outlive a deleted key's use	One `GetSessionToken` by `aws-support-sync` at 02:49:31 EDT (`EV-00640`), issued because no policy can block it; a call at 02:50 used it. The 02:58 update denied the named user and its temporary sessions every authorized resource action, and its long-lived key was deactivated at 03:01. The SCP does not prevent `GetSessionToken` issuance. No `GetFederationToken`
`backup:DeleteRecoveryPoint`	The bank's recovery points in `wf-backup`	None in the trail

What this does and does not show. The `OrgAccessBackup` session held administrator rights from 01:36 EDT and its only call in the trail is the `DeleteDBInstance` that the SCP denied (`EV-00570`). "None in the trail" means none in the organization trail export we hold. Object-level deletes would be data events, and we claim no more than the export shows.

The resource control policy, as attached at 03:20

Enabled as a policy type at the root by `EV-00650`, created by `EV-00653` (`wf-deny-outside-access`), and attached to the Workloads OU by `EV-00654`. It has three statements. The first denies the STS actions that start or tag a role session (`sts:AssumeRole`, `sts:SetContext`, `sts:SetSourceIdentity`, `sts:TagSession`, and never `AssumeRoleWithSAML` or `AssumeRoleWithWebIdentity`) to any principal outside the organization, except AWS service principals and one named principal in our account, `charles-sieg`. The second denies `kms:*` and the third `s3:*` to any principal outside the organization, with no responder exemption, because our role is inside the bank's account while it is in use. A resource control policy applies to the resource being reached, so it stops an outside principal that a service control policy cannot see.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAssumeRoleFromOutsideTheOrganization",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext",
        "sts:SetSourceIdentity",
        "sts:TagSession"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:PrincipalOrgID": "o-wrnfld4x7q"
        },
        "BoolIfExists": {
          "aws:PrincipalIsAWSService": "false"
        },
        "ArnNotLikeIfExists": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:user/charles-sieg"
          ]
        }
      }
    },
    {
      "Sid": "DenyKmsFromOutsideTheOrganization",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "kms:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:PrincipalOrgID": "o-wrnfld4x7q"
        },
```

```
        "BoolIfExists": {
          "aws:PrincipalIsAWSService": "false"
        }
      }
    },
    {
      "Sid": "DenyS3FromOutsideTheOrganization",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:PrincipalOrgID": "o-wrnfld4x7q"
        },
        "BoolIfExists": {
          "aws:PrincipalIsAWSService": "false"
        }
      }
    }
  ]
}
```

What it did to the outside trusts that already existed. Before attaching it the bank listed them with Access Analyzer (`EV-00652`, 03:16:40). The listing held two: the attacker's `OrgAccessBackup` trust, which was still present on July 4 and was deleted on July 8 (A-24), and our incident role, which the named-principal exemption keeps working. The bank had no other outside trust to cut.

What the trail can show of it. A denied cross-account `AssumeRole` is not logged in the role owner's account, so the bank's trail holds no denied `AssumeRole` from the attacker. The same holds for a denied `Decrypt` of the lending attacker key: a request that a key policy or a resource control policy denies is logged only in the caller's account, which the bank does not hold. The attacker's account may have tried the key after the policy went on, and the bank's trail cannot show a try either way. What the trail does show is the policy's text and attachment (`EV-00653` and `EV-00654`), and that no outside use of the key was allowed after 03:20: the last call from the attacker's account is the grant retirement at 00:51 on Saturday, before the policy.

The vault's deny-all SCP

Created by `EV-00662`, attached to the Recovery OU by `EV-00663`. As created, statement one denied every action for every principal except the two copy roles and the account's `OrganizationAccountAccessRole`, which the bank's administrator used for the setup calls (`EV-00667`, `EV-00998`, and the archive key's alias on July 8 at 16:20). Statement two, `DenyDeletionAndKeyChangesForEveryone`, has no condition: nobody can delete a snapshot, change its sharing, unlock it, schedule a key's deletion, disable a key, change a key policy, or revoke a grant. `kms:CreateGrant` is left out on purpose, because a cross-account copy needs it. The first form is printed here.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyEverythingExceptTheCopyAndSetupRoles",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/wf-vault-copy-in",
            "arn:aws:iam::*:role/wf-vault-copy-out",
            "arn:aws:iam::*:role/OrganizationAccountAccessRole"
          ]
        }
      }
    },
    {
      "Sid": "DenyDeletionAndKeyChangesForEveryone",
      "Effect": "Deny",
      "Action": [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:UnlockSnapshot",
        "kms:ScheduleKeyDeletion",
        "kms:DisableKey",
        "kms:PutKeyPolicy",
        "kms:RevokeGrant"
      ],
      "Resource": "*"
    }
  ]
}
```

The vault's deny-all SCP, as updated at 13:40 on July 6

Updated by `EV-00981`, ten minutes after the bank created the role `wf-backup-service` for AWS Backup (`EV-00978`) and before the backup job that took the live database's recovery point (A-45). AWS Backup takes a backup by assuming an ordinary IAM role that is passed to it; this is not a service-linked role, so the SCP applies to its session like any other role's, and the backup would have been denied. The one change is in statement one: `wf-backup-service` is added to the exemption list. Statement two still applies to it: it cannot delete a snapshot, share one, unlock one, or change a key. This form stood until 16:45 on July 8.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Sid": "DenyEverythingExceptTheCopyAndSetupAndBackupRoles",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/wf-vault-copy-in",
            "arn:aws:iam::*:role/wf-vault-copy-out",
            "arn:aws:iam::*:role/OrganizationAccountAccessRole",
            "arn:aws:iam::*:role/wf-backup-service"
          ]
        }
      }
    },
    {
      "Sid": "DenyDeletionAndKeyChangesForEveryone",
      "Effect": "Deny",
      "Action": [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:UnlockSnapshot",
        "kms:ScheduleKeyDeletion",
        "kms:DisableKey",
        "kms:PutKeyPolicy",
        "kms:RevokeGrant"
      ],
      "Resource": "*"
    }
  ]
}
```

The vault's deny-all SCP, as updated at 16:45 on July 8

Updated by `EV-01092` once setup was done (the last call that needed the setup role was the archive key's alias at 16:20, and the bucket and its policy were written by `wf-vault-copy-in`). Two exemptions are removed from statement one: the account's `OrganizationAccountAccessRole` and the backup service role `wf-backup-service` (its backup job had completed on July 6, `EV-00987`), so each is denied by name. The setup role has full administrative permissions and trusts the management account's root, so while it was exempt anyone with administrator access in `wf-management` could enter the vault. Only the two copy roles remain, each assumed with MFA and with two-person approval. Anyone with Organizations rights in the management account can still change this SCP; no guardrail covers that, and the bank decides who holds those rights.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "DenyEverythingExceptTheCopyAndSetupRoles",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/wf-vault-copy-in",
            "arn:aws:iam::*:role/wf-vault-copy-out"
          ]
        }
      }
    },
    {
      "Sid": "DenyDeletionAndKeyChangesForEveryone",
      "Effect": "Deny",
      "Action": [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:UnlockSnapshot",
        "kms:ScheduleKeyDeletion",
        "kms:DisableKey",
        "kms:PutKeyPolicy",
        "kms:RevokeGrant"
      ],
      "Resource": "*"
    }
  ]
}
```

The session-revoking inline policy

Put on `wf-deploy-pipeline` in each workload account by `EV-00555` to `EV-00564`. It denies every action to a session whose token was issued before 01:26 EDT (05:26 UTC) on July 4, and it does not touch a session issued after that time.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "DateLessThan": {
          "aws:TokenIssueTime": "2026-07-04T05:26:00Z"
        }
      }
    }
  ]
}
```

Our incident role's trust policy

Created in every account by `EV-00574` to `EV-00612`: by the self-managed StackSet in 19 accounts, and in `wf-management` by a separate stack. It lets one named principal assume the role, the IAM user `charles-sieg` in our account (not the account root), and only with MFA and the source identity `charles.sieg`. The second action is what allows the caller to set a source identity. The caller asserts the source identity, so on its own it limits nothing; the named principal is what limits who can assume the role. The MFA condition needs MFA context on the session. In an incident or a drill we produce it by calling `sts:GetSessionToken` with that IAM user's MFA device and assuming the role with the resulting session. An Identity Center session carries no MFA context and cannot meet the condition. The containment SCP exempts the role by name.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/charles-sieg"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "Bool": {
          "aws:MultiFactorAuthPresent": "true"
        },
        "StringEquals": {
          "sts:SourceIdentity": "charles.sieg"
        }
      }
    }
  ]
}
```

The lock configurations

The evidence bucket's default Object Lock retention (`EV-00657`), the vault's Vault Lock (`EV-00998`), and the snapshot lock on the 46 volume snapshot copies (`EV-00904` to `EV-00949`) are settings and not policies, but they are the controls that make the evidence and the locked copies unremovable, so they are here.

```json
{
  "ObjectLockEnabled": "Enabled",
  "Rule": {
    "DefaultRetention": {
      "Mode": "COMPLIANCE",
      "Years": 7
    }
  }
}
```

```json
{
  "BackupVaultName": "wf-recovery",
  "MinRetentionDays": 14,
  "ChangeableForDays": 3
}
```

```JSON
{
  "LockMode": "compliance",
  "LockDuration": 14,
  "CoolOffPeriod": 72
}
```

Notice

Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

© 2026 Vantalect, LLC. Sample deliverable; Wrenfield Bancorp, Inc. is fictional.

AWS, Amazon Web Services, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. MITRE ATT&CK is a registered trademark of The MITRE Corporation. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Other product names are trademarks of their owners. Vantalect is not affiliated with or endorsed by any of them. Wrenfield Bancorp, Inc. is fictional.