

AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

Foundation Re-Scan

Week 4 of 4: Re-scan · prepared for Tidepost, Inc.

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

February 13, 2026 · AWS Multi-Account Foundation: The Build, as an add-on to the Audit (four weeks)

SAMPLE DELIVERABLE

This is a sample deliverable. Tidepost, Inc. is a fictional company: its people, products, users, accounts, investors, and figures are invented for this sample, and any resemblance to a real company, person, product, or publication is coincidental. AWS prices are list prices from the AWS Price List API retrieved on October 13, 2026, and from the public AWS Price List bulk API on October 18, 2026.

Contents

Summary	2
How the re-scan was run.....	3
Before and after	4
Check by check	6
The MAF-05 waiver	10
MAF-11 is out of scope.....	11
The gate	12
The week’s window: W6	12
Cross-account backup and the vault lock.....	14
The week, day by day	14
What happens next.....	14

Summary

The gate is met. Dev Raman, Sasha Ilyin, Kofi Brandvold, and Gwen Tallis: of the 12 checks the foundation scan scores, 11 pass outright and 1 is waived in writing, and none fails. In week one, on January 5, 2026, 1 passed and 11 failed. The gate agreed at the readout counts a check waived in writing as passed, so all 12 count, and the second half of the add-on’s fee is invoiced.

We ran the same scan the same way on February 13, 2026, after Tidepost deleted the operator role, against all 9 accounts, reading them from the read-only roles. Nothing about the checks changed between the two runs: the same 13 checks, the same pass conditions, and a result read from the accounts, not from our notes.

The week at a glance. The scan measures the foundation as built; it is not an audit opinion.

Week 4 at a glance	Result
Checks in scope	12
Passing, week one (Jan 5)	1
Passing at the end (Feb 13)	11
Waived in writing at the end	1
Failing at the end	0
Counted as passed, for the gate	12 of 12
Out of scope and not scored	MAF-11
Window used this week	W6, Feb 10, 5 hours
Consultant hours this week	15
Consultant hours to date	68 of 70

The gate

Every check of the foundation scan agreed at the readout passes at the end, and a check waived in writing counts as passed. The gate is **met**: 11 passing plus 1 waived in writing is 12 of 12. Beyond that gate, no particular result is guaranteed, and Vantalect is not Tidepost's auditor: nothing here predicts what a SOC 2 report will say.

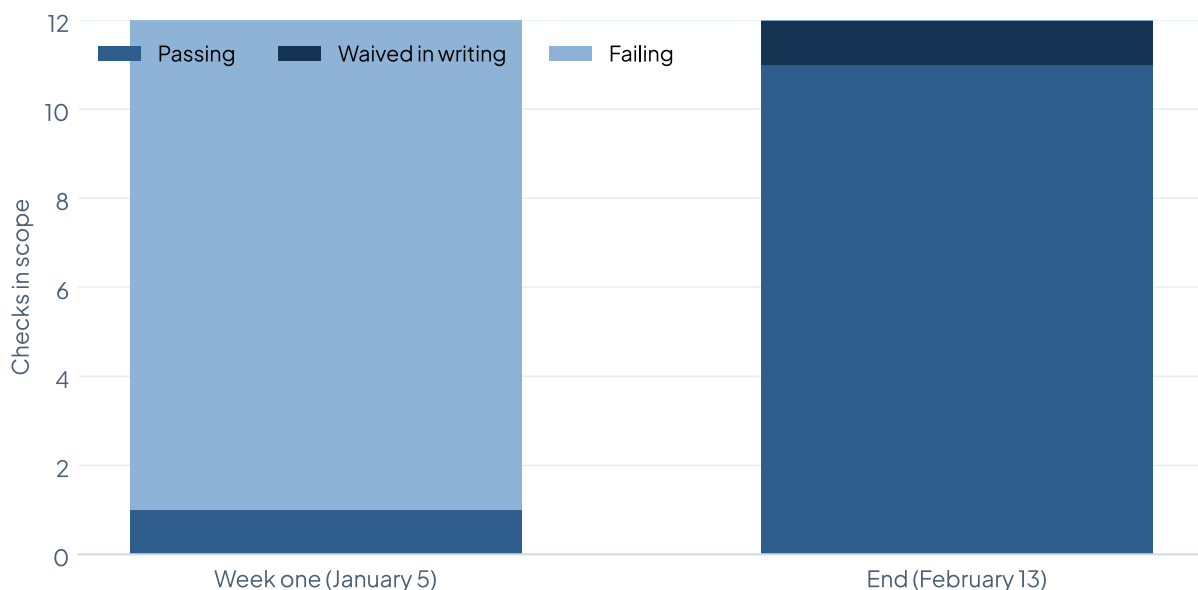
How the re-scan was run

A re-scan that is easier the second time is not a result, so the method matters more than the number.

- **The same script, the same way.** The same read-only script, run the same way, from the read-only roles in every account. It reads; it changes nothing. The only difference between the runs is what exists to be read.
- **One account, then 9.** In week one there was a single standalone account, the founders' account, and no organization. At the end there are 9 accounts in an organization of 9 OUs (2 of them empty by design), and the scan reads every account.

- **The operator role is gone first.** VantalectFoundationOperator was deleted by Kofi Brandvold on February 13, 2026, before the final run. That is check MAF-13, and it is why the last run is the cleanest evidence we can give: it was taken with no Vantalect access to the management account at all.
- **Twelve checks are scored.** MAF-11 is described below and not scored, in the week-one baseline and at the end alike.
- **A waived check is not hidden.** The one waiver is reproduced in full in [The MAF-05 waiver](#), and the result table says "waived" beside it, not "pass".

Before and after



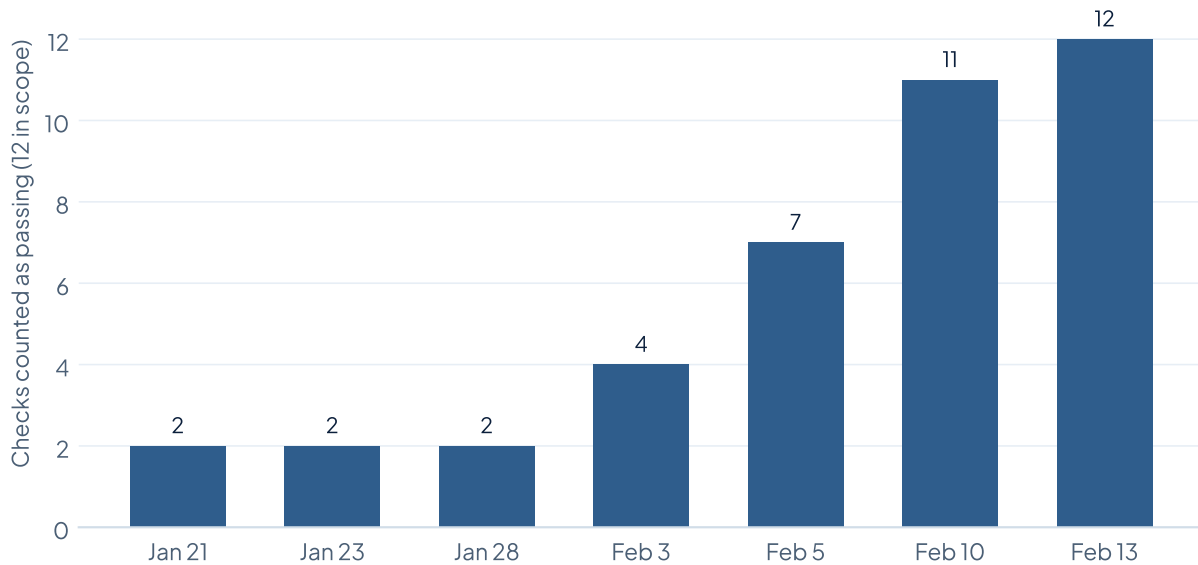
The 12 scored checks at week one and at the end. The one passing check in week one passes only because there was no role yet.



The result at the end, grouped by the five check families. Each bar sums to the number of checks in the family.

The checks by family. Identity and root holds the only waiver; the one week-one pass is MAF-13, in the same family.

Family	Checks	Passing, week one	Passing, end	Waived, end
Landing zone and accounts	3	0	3	0
Logging and detection	2	0	2	0
Identity and root	3	1	2	1
Guardrails and controls	2	0	2	0
Backup and tagging	2	0	2	0



Checks counted as passing as the work landed. A check counts from the day its work was in place; MAF-13 counts only after the role was deleted.

The climb has three steps, and each is a window. The landing zone and the organization trail came first (two checks, January 21, 2026), the guardrails, controls, and the vended account followed in the policy windows (7 by February 5, 2026), and backup, tagging, accounts placed, and identity closed on February 10, 2026 (11). The twelfth is the deleted role, on February 13, 2026. The over-time series starts on the landing zone's first day; before it, week one's single pass is the check that has nothing to fail while no role exists.

Check by check

Each row is one check, with what week one found and why, what the end found and why, and the day its work was in place. The pass condition for every check is in [What each check requires. A check passes only when its whole condition holds in every account it covers.](#)

Every scored check, week one against the end. All twelve are on the same scan, run the same way.

Check	Week one	Why, week one	End	Why, end	In place
MAF-01 Landing zone	Fail	No organization and no landing zone	Pass	Landing zone ACTIVE and in sync since January 21; FeatureSet ALL	Jan 21
MAF-02 Accounts placed	Fail	One standalone account; no organization to place it in	Pass	All nine accounts in their target OUs and enrolled; the last, tp-backup, on February 10	Feb 10
MAF-03 Organization trail	Fail	No trail of any kind (C-9)	Pass	Organization trail logging since January 21 into tp-log-archive; tp-prod's events from the join on January 28	Jan 21
MAF-04 Security delegated	Fail	No security service enabled	Pass	Delegated to tp-audit January 21; tp-prod enrolled automatically after the join, active January 29	Jan 29
MAF-05 Identity	Fail	No Identity Center; 18 IAM users, seven of them administrators with long-lived keys	Waived in writing	Identity Center connected January 23; 17 of 18 IAM users retired; one remains for a vendor that cannot assume a role, waived in writing February 11	Feb 10
MAF-06 Root	Fail	Two active root access keys and no root MFA (C-1)	Pass	tp-management root has two FIDO2 keys; centralized root access on January 28; tp-prod's root credentials removed January 29	Jan 29
MAF-07 Guardrails	Fail	No organization, so no SCP, RCP, or declarative policy	Pass	Eight baseline policies on every OU with accounts by February 5; hashes match the repository	Feb 5
MAF-08 Controls	Fail	No Control Tower	Pass	Eight elective controls on five OUs by February 5: the four that held accounts, and Infrastructure, empty until tp-backup on February 10	Feb 5
MAF-09 Vending	Fail	No Account Factory	Pass	tp-sandbox-ml vended February 5 and passed MAF-02 through MAF-08 untouched by hand	Feb 5
MAF-10 Backup	Fail	No central backup; a snapshot cron job in the one account	Pass	Backup policy on Workloads/Prod, tp-backup delegated, vaults in two Regions, vault lock in compliance mode	Feb 10

Check	Week one	Why, week one	End	Why, end	In place
MAF-12 Tagging	Fail	No tags on 94% of resources and no tag policy	Pass	Tag policy on Prod, NonProd, and Sandbox February 10; the report reads from tp-management	Feb 10
MAF-13 No lingering access	Pass	No role yet	Pass	The role was deleted February 13 before the final run	Feb 13

What each check requires. A check passes only when its whole condition holds in every account it covers.

Check	Family	Passes when
MAF-01 Landing zone	Landing zone and accounts	The landing zone is enrolled, active, and not drifted; all features are on in the organization
MAF-02 Accounts placed	Landing zone and accounts	Every in-scope account is in its target OU and enrolled
MAF-03 Organization trail	Logging and detection	A multi-Region organization trail, logging, with log file validation, delivers to a bucket in the Log Archive account
MAF-04 Security delegated	Logging and detection	GuardDuty, Security Hub, IAM Access Analyzer, and the Config aggregator (and Inspector) are administered from the Audit account, with new accounts enrolled automatically
MAF-05 Identity	Identity and root	IAM Identity Center is the organization's instance and is connected to the identity provider; no workload account has an IAM user with a console password or an active access key, except in the Exceptions OU with a written exception
MAF-06 Root	Identity and root	The management account's root user has MFA; centralized root access is on; member accounts hold no root password or access keys
MAF-07 Guardrails	Guardrails and controls	The agreed SCPs, RCPs, and declarative policies are attached at the agreed OUs, inherited by every in-scope account, and match the repository
MAF-08 Controls	Guardrails and controls	The agreed Control Tower controls are enabled on every target OU
MAF-09 Vending	Landing zone and accounts	New accounts are vended through Account Factory, and one account vended in week five passes MAF-02 through MAF-08 untouched by hand
MAF-10 Backup	Backup and tagging	A backup policy is attached to the agreed OUs, AWS Backup is administered from a delegated account, and copies land in a central vault in a separate account
MAF-12 Tagging	Backup and tagging	The agreed tag policy is attached and effective, with its compliance report readable from the management account
MAF-13 No lingering access	Identity and root	Vantalect's operator role and any temporary assignment are gone from the management account

Three of the results deserve a sentence each, because they are the ones a reviewer asks about.

- **MAF-02, accounts placed, closed on February 10, 2026.** It needs every in-scope account in its target OU and enrolled, and the last account to arrive was tp-backup, placed that day in the window below. Until then the check was honestly failing.
- **MAF-09, vending, is proven on a real account.** tp-sandbox-m1 was vended through Account Factory on February 5, 2026 and its vending record reads: "Passed MAF-02 through MAF-08 untouched by hand." That is 7 checks, from MAF-02 to MAF-08, passed with no manual step.
- **MAF-13, no lingering access, is the check that was passing and then not.** It passed in week one only because the role did not exist yet. It failed in the middle, as it should, and it passes now because Tidepost deleted the role.

The MAF-05 waiver

MAF-05 asks that no workload account hold an IAM user with a console password or an active access key, except in the Exceptions OU with a written exception. Week one found 18 IAM users in tp-prod, seven of them administrators with long-lived keys. 17 are gone. One remains, and it is waived.

Where the 18 IAM users went. Retiring the last fourteen waited until each person had signed in through Identity Center.

Group retired	UsersOn	By	How
Administrator users who had left the company	2January 6, 2026	Kofi Brandvold	Deleted on notice (C-7)
The CI user and its two access keys	1January 20, 2026	Kofi Brandvold	GitHub Actions moved to OIDC federation with a deploy role per repository (H-14)
People who are current staff (5 administrators and 9 others)	14February 10, 2026	Kofi Brandvold	People moved to Identity Center on January 26 and were assigned to tp-prod on January 28; each user's password and keys were deleted after that person signed in through Identity Center
Remaining	1		The video analytics vendor's user: Waived in writing on February 11 (MAF-05)

Waiver for MAF-05

Signed by: Sasha Ilyin, Head of Security and Compliance, on February 11, 2026.

What is waived: One IAM user with an access key in tp-prod, for a video analytics vendor whose system cannot assume a role. Its scope is read access to one prefix of the renditions bucket. The user sits in tp-prod, in the Prod OU, not in the Exceptions OU, so MAF-05 cannot pass: moving the user would mean moving the production account out of Prod. That is why the check is waived rather than passed.

Why it is not fixed: The vendor's system cannot assume a role; asked, it has no plan to.

Controls: the key is rotated every 90 days through TidepostVendorKeyRotation, a role in tp-prod that can change only this user's keys and has its own exemption in the IAM-user policy, so a rotation never opens the break-glass credential. Kofi Brandvold owns the rotation and the role, which can create, deactivate, and delete access keys for the video analytics vendor's IAM user, and nothing else. The next rotation is due May 12, 2026.

Review: At each quarterly access review.

The waiver counts as passed under the gate, and it should: the exception is written, bounded to one prefix of one bucket, rotated on a date, and signed by the person who owns security risk. It is a waiver, not a pass, because the user is not where the organization expects an exception to sit: it is in tp-prod, and the Exceptions OU is for accounts, not for one user inside the production account. The IAM-user policy gives the rotation its own narrow exemption, a role that can change only this user's keys, so a rotation needs no policy change, never opens the break-glass credential, and does not set off the break-glass alarm.

MAF-11 is out of scope

MAF-11 (Network) asks that shared networking is owned by a Network account and shared through AWS RAM. It is not scored, in week one or at the end, and the reason is plain: Tidepost has one VPC and no Transit Gateway, so there is no shared network to own and nothing for a Network account to hold. The week-one note reads: "One VPC and no Transit Gateway." None of the 9 accounts is a Network account.

Leaving it unscored is not hiding a failure. A check that asks who owns a shared network cannot pass or fail where there is none, and scoring it would make the gate harder to read. It reopens when Tidepost’s workloads move into separate accounts and need to reach each other privately. The deferred data accounts, described in the handover report, are the likely occasion.

The gate

The gate computation, on February 13, 2026. The gate’s own statement: Every check of the foundation scan agreed at the readout passes at the end, and a check waived in writing counts as passed.

Step	Result
Checks in scope	12
Passing at the end	11
Waived in writing	1
Failing at the end	0
Counted as passed	12 of 12
Gate	Met

The add-on’s fee is \$25,000, invoiced in two halves: \$12,500 at signature and \$12,500 on the gate. The gate is met, so the second invoice is issued on February 13, 2026. The work product is Tidepost’s: the code in tidepost–foundation and tidepost–cdk, the policies, the runbooks, the scan results, and the recordings. The add-on used 68 of its 70 hours.

The week’s window: W6

W6 was the only window this week, on February 10, 2026 from 09:00 to 14:00 CST (5 hours). It was in writing, by email, two business days ahead, on February 6, 2026, by Dev Raman and Kofi Brandvold. It built the last account and turned on the last two policies.

W6, Backup and tag policies; the backup account. Every sign-in to the operator role during the window was posted to the platform channel.

Step	What happened
1	Create tp-backup through Account Factory in the Infrastructure OU, with us-east-1 and us-west-2 enabled
2	Turn on AWS Backup cross-account management and cross-account backup in tp-management, and delegate AWS Backup administration to tp-backup
3	Point the backup policy's copy actions at tp-central-vault and tp-central-vault-west, and attach it to Workloads/Prod
4	Attach the tag policy to Workloads/Prod, Workloads/NonProd, and Sandbox

The 4 pre-flight checks, run before the window opened. Blockers: 0.

Pre-flight check	Result	Note
The backup and tag policies passed their Policy Staging cases	Pass	A tagged test volume in tp-policy-test backed up and copied to its own us-west-2 test vault on February 6 and 9; a value outside the list refused on an instance; the tag compliance report read from tp-management
tp-backup's root email is a company group alias, and the account is created with no root password (centralized root access)	Pass	aws-backup@tidepost.example
IAM Access Analyzer policy validation on both policies	Pass	No errors
The operator role's time conditions run from the window's start to one hour before its end	Pass	Read from the role's trust policy; the one-hour session limit covers the last hour

Outcome. tp-backup created and delegated; the backup and tag policies attached; the test volume's next backup copied into both central vaults. **Rollback.** Detach the backup and tag policies. tp-backup stays. Tidepost can remove the vault lock until the cooling-off period ends on February 13.

Cross-account backup and the vault lock

tp-backup sits in the Infrastructure OU and holds two vaults, tp-central-vault and tp-central-vault-west, with the vault lock in compliance mode and a minimum retention of 7 days. The lock is the one irreversible thing this engagement did, so it has a cooling-off period: it was set on February 10, 2026, Tidepost can remove it for 3 days, and from February 13, 2026 nobody can, including Tidepost and including us. That date is the day the operator role was deleted, so the lock became permanent the moment Vantalect's access ended.

The backup policy selects resources tagged backup=required, and no resource carries that tag yet, so it selects nothing until Tidepost tags one, which the Well-Architected Remediation does. What was proven is the path: a tagged test volume in tp-policy-test backed up and copied on February 6, 2026 and February 9, 2026, and the window's first run copied into both central vaults.

The watch for policy-caused denials after the backup and tag policies ran through February 11, 2026 and found 0.

The week, day by day

The week's events. Everything inside a member account went through a pull request, and Vantalect's only access this week was the W6 window.

Date	Who	What
February 10, 2026	Vantalect	W6: Backup and tag policies; the backup account
February 11, 2026	Sasha Ilyin	MAF-05 waiver signed
February 12, 2026	Kofi Brandvold	Handover workshop, recorded
February 13, 2026	Vantalect	Operator role deleted; final scan; closing readout

What happens next

1. Read the handover report: the five runbooks, the break-glass custody, and what stays with Tidepost.
2. Put May 12, 2026 on the calendar: the waived vendor key is due for rotation, through TidepostVendorKeyRotation.

3. Rerun the scan yourselves, from the read-only roles, in the first week of each month for a quarter, and compare it against this report. If a check that passes here starts to fail, find out which change caused it that week.

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

AWS, Amazon Web Services, AWS Graviton, AWS Inferentia, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Kubernetes is a registered trademark of The Linux Foundation. Redis is a registered trademark of Redis Ltd. Valkey is a trademark of the Linux Foundation. OpenSearch is a registered trademark of Amazon.com, Inc. SOC 2 is a registered trademark of the American Institute of Certified Public Accountants. CIS Benchmarks is a trademark of the Center for Internet Security, Inc. GitHub is a trademark of GitHub, Inc. Jupyter is a trademark of LF Charities. Vantalect is not affiliated with or endorsed by any of them. Tidepost, Inc. is fictional.