



AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

The Founders' Account Joined and Enrolled

Week 2 of 4: The join · prepared for Tidepost, Inc.

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

January 30, 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
The week day by day	3
People move to IAM Identity Center	4
The pre-flight for the join	4
The one blocker	5
W3: The join and enrollment	6
Centralized root access	7
The billing transfer	7
The accounts Tidepost vended	9
Foundation scan checks this week.....	9
What did not go to plan.....	10
What happens next.....	10

Summary

The founders’ account, tp-prod, joined the organization on January 28 as the production member and was enrolled in Control Tower, and no workload moved. Dev Raman, Kofi Brandvold, Sasha Ilyin, and Gwen Tallis: this is week 2 of 4 of the Multi-Account Foundation, covering one change window (W3, 6 hours) and 19 hours of work, 35 of the 70 used so far. The nine-check pre-flight found one blocker on January 26, Gwen Tallis cleared it on January 27, and the window ran the next day. The rollback was ready and was not used.

The blocker was not about joining. It was about leaving: joining an organization needs no payment method, but leaving one does, and leaving is the rollback. The card on file was a founder’s and expired on January 31, so a rollback after that date would have failed. We found it on the first run, before anything depended on it.

Week 2 in eight numbers.

Week 2 at a glance	Result
People moved to IAM Identity Center	January 26
Change window	W3, January 28, 09:00 to 15:00 CST
Pre-flight checks, passed, and blockers	9, 8, and 1
Blocker cleared	January 27 by Gwen Tallis
Accounts in the organization	6 of 9 planned
Root credentials removed from tp-prod	January 29, by Tidepost
Cost and Usage Report export started	January 28
Foundation scan checks passed to date	4 of 11

The week day by day

Week 2, from the people move to the next window’s approval.

Date	Who	What
January 26	Kofi Brandvold	People provisioned into Identity Center over SCIM; join pre-flight first run finds one blocker
January 26	Dev Raman	W3 approved in writing
January 27	Gwen Tallis	Blocker cleared; pre-flight clean; Cost Explorer extract; execution role in tp-prod
January 28	Vantalect	W3: The join and enrollment
January 29	Kofi Brandvold	tp-staging and tp-policy-test provisioned; tp-prod root credentials removed; Policy Staging cases begin
January 30	Kofi Brandvold	Root recovery tested in tp-policy-test; Policy Staging finds the detection policy needs an exemption
January 30	Dev Raman	W4 approved in writing

People move to IAM Identity Center

On January 26 the people moved from IAM users to IAM Identity Center sign-in. The six permission sets and their groups were in place from week 1 and Kofi Brandvold moved the people. The groups were then assigned to tp-prod in W3, which is when a person could first sign in to the production account through Identity Center.

The IAM users are not deleted yet. Each one goes after its owner has signed in through Identity Center, so nobody loses access to an account they need; the plan retires them on February 10. That is how 18 IAM users in tp-prod on January 5 come down to one that stays, for a vendor that cannot use a role, which we cover at the end of the add-on.

The pre-flight for the join

The pre-flight is nine checks, each one a reason a join can go wrong. It ran for the first time on January 26 and a second time on January 27. Eight checks passed both times. One did not pass the first time.

The W3 pre-flight. The seventh check is the blocker; the second run on January 27 passed all 9.

No. Check	Result	Note
1Root email and MFA under Tidepost custody	Pass	Root email on the company group alias aws-prod@tidepost.example; two FIDO2 keys registered January 6 (C-1)
2No resource, key, or trust policy conditions on a source organization ID	Pass	There was no organization, so there was nothing to break; the search of bucket, key, and role policies found no organization condition
3No AWS RAM share the account depends on is scoped to an organization	Pass	No shares
4No service-managed StackSet would delete its stack instances	Pass	No service-managed StackSets
5No unplanned delegated administrator in the account	Pass	None
6Commitments, credits, and Marketplace agreements listed with a plan	Pass	No Savings Plan or Reserved Instance, the Activate credits ended in June 2025, and no active Marketplace subscription

No. Check	Result	Note
7The rollback can run: the account meets AWS's requirements to leave an organization (contact information, a current payment method, and a support plan chosen for the account)	Blocker, then cleared	Joining needs none of this, but leaving does, and leaving is the rollback. The card on file was a founder's and expired January 31, so a rollback after that date would have failed; the account's contact information still named a founder's personal email
8Enrollment: no existing AWS Config recorder or delivery channel, and the AWSControlTowerExecution role in place	Pass	Config was off; Tidepost created the role from the template on January 27
9The 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

The one blocker

The rollback could not have run. The rollback (leaving the organization) needs a current payment method and the account's own contact information; the card on file, a founder's, expired January 31. The account's contact information also still named a founder's personal email. Joining needs neither, so nothing would have stopped the window; the failure would have shown up only if we had needed to go back, after January 31, on a card that no longer worked.

Gwen Tallis fixed both on January 27: the company card went on file and the finance alias became the account's contact. Support plans are per account: tp-prod keeps Business Support+, and an account that has to leave needs a plan, contact information, and a payment method of its own. The window was approved on January 26, the same day as the first run, on the condition that the second run was clean. It was.

Two other pieces of preparation happened that day:

- January 27, Kofi Brandvold: created the AWSControlTowerExecution role in tp-prod from the template Vantalect sent.
- January 27, Gwen Tallis: exported twelve months of Cost Explorer data (by service and usage type) to a bucket in tp-management, because the new payer cannot see the account's earlier history.

W3: The join and enrollment

January 28, 2026, 09:00 to 15:00 CST (6 hours). Approved on January 26, 2026 by Dev Raman and Kofi Brandvold, in writing, by email, two business days ahead. Result: **tp-prod joined as the production member and enrolled; the data export started; no workload moved.**

What we did, in order:

- Invite tp-prod (the founders' account) to the organization, accepted by Tidepost in tp-prod.
- Place tp-prod in Workloads/Prod and enroll it in Control Tower.
- Turn on centralized root access (root credentials management and root sessions).
- Start the CUR 2.0 data export in tp-management, from the join.
- Assign the Identity Center groups to tp-prod.

The account was invited, not created. The founders' account (opened March 4, 2024) was invited by tp-management and the invitation was accepted by Tidepost inside tp-prod, so Vantalect never had write access to it. It landed in Workloads/Prod, was enrolled in Control Tower, and the organization trail started carrying its events, which replaces the account trail (finding C-9). The delegated security services in tp-audit enrolled it automatically and they became active on January 29. No workload moved: the join changes who the account belongs to, and the account itself keeps running as it was.

The rollback, as written before the window: Tidepost removes tp-prod from the organization (the pre-flight confirms it can stand alone: contact information, a current payment method, and a support plan), and billing returns to tp-prod's own invoice. The operator role cannot do this; it is the client's call. It was not used. From January 29, when tp-prod's root credentials were removed, the rollback starts one step earlier: an account outside the organization needs its own root user, so Tidepost first starts a central root session (sts:AssumeRoot) that turns on root password recovery for tp-prod, then resets the root password through the account's root email. That path was tested in tp-policy-test on January 30.

Centralized root access

Nobody holds a root password for a member account anymore. Every root email is a company group alias, so no root email depends on one person's mailbox: the address for tp-prod is aws-prod@tidepost.example and for tp-management it is aws-management@tidepost.example. tp-management's root user has two FIDO2 keys, held by Noor Castellanos and Sasha Ilyin in separate places. Vantalect never holds a root credential.

Root custody, from the registered keys to the tested recovery path.

Date	What	By
January 6	Two FIDO2 keys registered on tp-prod's root user, replacing two active root access keys with no MFA (finding C-1)	Tidepost
January 28	Centralized root access turned on in W3: root credentials management and root sessions, from tp-management	Vantalect, in the window
January 29	tp-prod's root credentials removed	Tidepost (Kofi Brandvold)
January 30	Recovery path tested in tp-policy-test: Turned on root password recovery in tp-policy-test from a central root session (sts:AssumeRoot), reset the password through the account's group alias, then deleted it again from a second root session: the path an account would need to stand alone	Tidepost (Kofi Brandvold)

New accounts are created with no root password. The test on January 30 matters because removing a root credential is only safe if you know how to get one back: it proved the path an account would need to stand on its own, with no stored root password.

The billing transfer

Joining the organization moves tp-prod's bill to tp-management, and nothing was lost doing it.

Joining needs no payment method; leaving does, which is why the blocker above was about the rollback. Gwen Tallis owns this part.

What changes in billing at the join.

Item	What we found	What it meant for the join
January invoice	January splits at the join: January 1 to 27 on tp-prod's own invoice, January 28 to 31 on tp-management's	Two invoices for January, split at the join, with nothing missing between them
Cost history	The new payer cannot see the account's earlier Cost Explorer history	Twelve months of Cost Explorer data by service and usage type exported on January 27 by Gwen Tallis, to a bucket in tp-management
Cost and Usage Report	None existed to carry over	tidepost-cur2 starts in tp-management on January 28: CUR 2.0, Parquet, hourly, with resource IDs
Budgets, cost categories, cost allocation tags	None existed	Nothing to carry over
Savings Plans and Reserved Instances	None existed	Nothing to lose
Credits	The Activate credits ran out in June 2025	Nothing to lose
Marketplace	No active subscription, listed from the Marketplace and License Manager consoles on January 26	No vendor to ask for a new offer
Support plans	Per account: tp-prod keeps Business Support+, new accounts start on Basic Support	Production cases keep their plan

Why the commitments check exists. A Savings Plan or a Reserved Instance belongs to the account that bought it, and its discount is shared across the payer's whole consolidated billing family. A join or a leave changes who benefits from a discount. In your case there were none, so there was nothing to lose. Vantalect buys, sells, and exchanges no commitment in this engagement.

The join was not held to a month boundary, because there was nothing the split could cost. Cost reporting uses the export from here: CUR 2.0, Parquet, hourly, with resource IDs.

The accounts Tidepost vended

Tidepost created `tp-staging` and `tp-policy-test` itself on January 29, through Account Factory. Vantalect did not provision them and has no access to either. Both landed in the OUs built in week 1.

The two accounts vended this week.

Account	ID	OU	Purpose	Provisioned
tp-staging	...7746	Workloads/NonProd	Staging, empty until the June rebuild (EC2-1a)	January 29, by Tidepost through Account Factory
tp-policy-test	...7774	Policy Staging	Proving every policy before it is attached	January 29, by Tidepost through Account Factory

`tp-staging` stays empty until the staging rebuild in June (change EC2-1a in the cost engagement); moving staging and the data workloads out of `tp-prod` is workload migration, outside the add-on. `tp-policy-test` is where the Policy Staging cases begin the same day, and week 3's report covers them.

Foundation scan checks this week

4 of the 11 checks that can pass before the final scan are passing, up from 2 at the end of week 1. MAF-04 and MAF-06 passed on January 29.

The foundation scan checks at the end of week 2.

Check	Title	Status on January 30	What moved this week
MAF-01	Landing zone	Passing since January 21	No change
MAF-02	Accounts placed	Open	6 of 9 accounts placed
MAF-03	Organization trail	Passing since January 21	<code>tp-prod</code> events join the organization trail from the join
MAF-04	Security delegated	Passing since January 29	Passed: <code>tp-prod</code> enrolled automatically after the join, active January 29

Check	Title	Status on January 30	What moved this week
MAF-05	Identity	Open	People moved January 26 and assigned to tp-prod January 28; IAM users still to retire
MAF-06	Root	Passing since January 29	Passed: centralized root access on, tp-prod root credentials removed
MAF-07	Guardrails	Open	Draft policies under test in tp-policy-test; none on an OU with accounts
MAF-08	Controls	Open	No change
MAF-09	Vending	Open	No change
MAF-10	Backup	Open	No change
MAF-12	Tagging	Open	No change
MAF-13	No lingering access	Judged at the final scan	No change

What did not go to plan

One pre-flight check failed, and it was cleared before the window. The first run on January 26 found the blocker, and the window did not run until the second run on January 27 was clean, which was the condition of its approval. The fix was a card and a contact, and the window kept its date.

Two things are still less finished than they look:

- **The IAM users are still there.** People sign in through Identity Center, but the old users stay until each person has proved the new path, so MAF-05 stays open.
- **tp-prod is production and the old staging.** Joining did not separate them. tp-staging exists and is empty; the move out of tp-prod is Tidepost's own work on its own calendar.

What happens next

Week 3 is the first week the guardrails reach accounts. The draft policies from week 1 have been under test in tp-policy-test since January 29, and the first correction came out of that on January 30: tp-scp-baseline needed an exemption for Control Tower's own role. The fix merges on February 2, ahead of the next window.

The next steps.

When	Who	What
January 30	Dev Raman and Kofi Brandvold	Approve W4 in writing, two business days ahead
February 3	Vantalect and Tidepost	W4: Policies to Sandbox and NonProd, 09:00 to 12:00 CST
February 5	Vantalect and Tidepost	W5: Policies to Prod, and the vended account, 09:00 to 13:00 CST

What we need from you: Dev Raman and Kofi Brandvold, the W4 approval by January 30.

© 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.