

AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

Landing Zone and Core Accounts

Week 1 of 4: Landing zone · prepared for Tidepost, Inc.

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

January 23, 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 work runs	3
W1: Landing zone	4
W2: IAM Identity Center and the identity provider	5
The accounts and the OUs	6
Logging and detection	7
Identity	8
The draft policies on Policy Staging	9
Foundation scan checks this week	10
What did not go to plan	11
What happens next	12
The week day by day	13

Summary

The landing zone is active and in sync, the organization trail has been logging since January 21, and IAM Identity Center has been connected to the identity provider since January 23. Dev Raman, Kofi Brandvold, and Sasha Ilyin: this is week 1 of 4 of the Multi-Account Foundation, covering 2 change windows (W1 and W2) and 16 of the 70 hours in the add-on. Across the two windows, 6 pre-flight checks ran with no blockers. Nothing was rolled back.

This is a greenfield build. Tidepost had no AWS organization on January 5, 2026: the founders' account, now tp-prod, was its own payer. You created tp-management on January 12, and this week we built the organization around it. No workload moved, and none will move in the add-on.

Week 1 in eight numbers.

Week 1 at a glance	Result
Change windows	2 (9 hours in the windows)
Hours used this week, and to date	16, and 16 of 70
Pre-flight checks, and blockers	6, and 0
Accounts in the organization	3 of 9 planned
Organizational units created	9 (2 empty by design: Suspended and Exceptions)
Governed Regions	us-east-1 and us-west-2
IAM Identity Center permission sets	6
Draft policies on Policy Staging	8 (3 SCPs, 3 RCPs, 2 declarative policies)
Foundation scan checks passed to date	2 of 11

The one thing to know: **week 1 builds the place everything else lives, and it touches no running system.** The two core accounts are new and empty, and the draft policies sit on an OU with no workload. The real change, putting tp-prod into the organization, is week 2, and its window is the one that carries risk.

How the work runs

Every change to your accounts happens in an approved window, through one role that you own. The role is `VantalectFoundationOperator` in `tp-management`. Kofi Brandvold created it on January 20, 2026 from a template Charles Sieg sent on January 16, so you read it before it existed.

The operator role. Vantalect cannot change a setting in this table; the role belongs to Tidepost.

Property	Setting
Who can assume it	Charles's named principal only; MFA required; a source identity naming him; aws:CurrentTime bounds from the window's start to one hour before its end, the condition AWS checks when a session starts; sessions of at most one hour, so the last one ends when the window does
Explicit denies	closing accounts; deleting the organization; changing payment methods or billing contacts; creating IAM users or access keys; leaving the organization
How we are seen	Every call lands in the organization trail with his source identity; an EventBridge rule posts each AssumeRole to the platform channel
Member accounts	Vantalect holds no write access to any member account; everything inside members goes through tidepost-foundation and tidepost-cdk pull requests
Removal	Deleted by Kofi Brandvold on February 13, 2026, before the final scan (MAF-13)

Six windows cover the add-on. Dev Raman and Kofi Brandvold approve each in writing, two business days ahead, and the role's `aws:CurrentTime` bounds run from the window's start to one hour before its end. AWS checks that condition only when a session starts, and a session lasts at most one hour, so the last one ends as the window closes and an unapproved hour cannot be used even by mistake. The two for this week:

The windows of week 1. Each action list is in the sections that follow.

Window	Date and time	What it did	Approved	Pre-flight	Blockers
W1	January 21, 09:00 to 15:00 CST	Landing zone: 5 actions	January 16	3	0
W2	January 23, 09:00 to 12:00 CST	IAM Identity Center and the identity provider: 4 actions	January 21	3	0

W1: Landing zone

January 21, 2026, 09:00 to 15:00 CST (6 hours). Approved on January 16, 2026 by Dev Raman and Kofi Brandvold, in writing, by email, two business days ahead. The operator role's time conditions were set to exactly this window. Result: **Landing zone ACTIVE and in sync; both core accounts created; the trail logging.**

What we did, in order:

- Set up Control Tower in `tp-management: home Region us-east-1`, governed Regions `us-east-1` and `us-west-2`.

- Create the Security OU with tp-log-archive and tp-audit through the landing zone.
- Create the other OUs: Infrastructure, Workloads with Prod and NonProd, Sandbox, Policy Staging, and the empty Suspended and Exceptions.
- Confirm the organization trail into tp-log-archive: multi-Region, logging, log file validation on.
- Register tp-audit as delegated administrator for GuardDuty, Security Hub, IAM Access Analyzer, AWS Config, and Inspector.

W1 pre-flight: 3 checks, 0 blockers.

Pre-flight check	Result	Note
tp-management root user: two FIDO2 keys, held by Noor Castellanos and Sasha Ilyin in separate places	Pass	Both keys signed in before the window opened
All features are on in the organization, and the Regions were agreed at the January 16 readout	Pass	FeatureSet is ALL
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

Rollback, as written before the window: Decommission the landing zone from the console (no workload exists in the organization). The operator role cannot close accounts, so tp-log-archive and tp-audit stay as empty accounts.

W2: IAM Identity Center and the identity provider

January 23, 2026, 09:00 to 12:00 CST (3 hours). Approved on January 21, 2026 by Dev Raman and Kofi Brandvold, in writing, by email, two business days ahead. The operator role's time conditions were set to exactly this window. Result: **Identity Center connected; six permission sets; the draft policies on Policy Staging.**

What we did, in order:

- Enable IAM Identity Center as the organization instance in us-east-1 (the landing zone was set up without managing it, so its configuration lives in tidepost-foundation).
- Connect the identity provider (SAML sign-in, SCIM provisioning) and create the six permission sets.
- Assign the permission sets to groups on tp-management, tp-log-archive, and tp-audit.
- Enable the resource control policy and EC2 declarative policy types, then attach the draft baseline policies (three SCPs, three RCPs, two declarative policies) to the empty Policy Staging OU.

W2 pre-flight: 3 checks, 0 blockers.

Pre-flight check	Result	Note
Kofi Brandvold holds the identity provider's admin console during the window	Pass	A test group synced through SCIM the day before
A path into tp-management that does not use the identity provider	Pass	The break-glass user bg-admin exists with its hardware key sealed (January 22)
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

Rollback, as written before the window: Disable the identity provider connection and sign in with the break-glass user; assignments are removed in one call per permission set. Detaching the draft policies from Policy Staging is one call each.

The accounts and the OUs

3 accounts exist at the end of the week, and the 6 that join them are already named, each with its target OU. tp-management is yours and was created in the console; the other two came out of the landing zone's set-up.

Accounts in the organization on January 23, 2026. IDs are shortened to their last four digits.

Account	ID	OU	Purpose	Created
tp-management	...7702	Root	Payer, Control Tower, IAM Identity Center, and the Cost and Usage Report data export	January 12 by Tidepost
tp-log-archive	...7715	Security	The organization trail and AWS Config history	January 21 by the landing zone, in W1
tp-audit	...7723	Security	Delegated GuardDuty, Security Hub, IAM Access Analyzer, the Config aggregator, and Inspector	January 21 by the landing zone, in W1

The accounts still to come, with the dates they are planned for: tp-prod (January 28), tp-staging (January 29), tp-policy-test (January 29), tp-dev (February 3), tp-sandbox-m1 (February 5), tp-backup (February 10). Tidepost creates or joins most of them itself; the rest we vend through Account Factory.

The organizational units. Two are empty by design and stay empty unless an account needs them.

OU	Parent	Created	Holds at the end of the week
Security	Root	January 21	tp-log-archive, tp-audit
Infrastructure	Root	January 21	No account yet
Workloads	Root	January 21	No account yet
Workloads/Prod	Workloads	January 21	No account yet
Workloads/NonProd	Workloads	January 21	No account yet
Sandbox	Root	January 21	No account yet
Policy Staging	Root	January 21	No account yet
Suspended	Root	January 21	No account yet
Exceptions	Root	January 21	No account yet

The Security OU holds the two accounts no workload runs in. tp-log-archive receives the organization trail and AWS Config history; tp-audit is where detection is administered. Keeping them apart means a compromised workload account cannot reach the logs about itself.

Logging and detection

Logging is on first because every later step is visible in it. The organization trail is multi-Region, with log file validation on, and delivers to tp-log-archive. It has been logging since January 21; before that you had no trail of any kind (finding C-9). When tp-prod joins in week 2, its events join the same trail.

tp-audit is the delegated administrator for five services, so a new account is enrolled in each without anyone repeating the set-up:

The five delegated security services.

Service	Administered from	Registered
Amazon GuardDuty	tp-audit	January 21 (W1)
AWS Security Hub CSPM	tp-audit	January 21 (W1)
IAM Access Analyzer	tp-audit	January 21 (W1)
AWS Config aggregator	tp-audit	January 21 (W1)
Amazon Inspector	tp-audit	January 21 (W1)

The check that covers this, MAF-04, does not pass yet: it needs tp-prod enrolled, and tp-prod joins in week 2.

Identity

People sign in to AWS through IAM Identity Center from January 23, with 6 permission sets mapped to groups. The identity provider connects over SAML for sign-in and SCIM for provisioning. Kofi Brandvold held the identity provider’s admin console during the window, and a test group had synced through SCIM the day before. In this week the groups are assigned on tp-management, tp-log-archive, and tp-audit; the scopes on other accounts attach as those accounts arrive.

The permission sets. The people move on January 26, 2026, not this week.

Permission set	Group	Who	Scope once the accounts exist
PlatformAdministrator	aws-platform-admins	Kofi Brandvold	Every account; administrator, MFA required
Developer	aws-developers	Marcus Oyelaran, Bea Okafor	tp-dev and tp-staging with power-user access; read-only in tp-prod
MachineLearning	aws-ml	Yuki Sorensen	tp-sandbox-ml with power-user access; read-only in tp-prod
DataEngineer	aws-data	Lior Haddad	Read and query on the telemetry stores in tp-prod; power-user in tp-dev
SecurityAudit	aws-security-audit	Sasha Ilyin, Amara Delacroix	Read-only everywhere; tp-audit and tp-log-archive
BillingViewer	aws-billing	Gwen Tallis	Billing and Cost Explorer in tp-management

Identity Center is configured outside the landing zone's own set-up, because the landing zone was created without managing it. Its configuration therefore lives in `tidepost-foundation`, as code you review, rather than in a console setting nobody can see.

The break-glass path exists before anyone depends on the identity provider. Kofi Brandvold created the IAM user `bg-admin` in `tp-management` on January 22 and sealed its hardware key, with custody split between Sasha Ilyin and Noor Castellanos. Every sign-in and every `AssumeRole` posts to the platform channel and opens a ticket. The matching role, `TidepostBreakGlass`, goes into every member account, and the policy that would otherwise forbid IAM users exempts it. W2's pre-flight checked that `bg-admin` existed before the identity provider was connected, because a federation outage with no other way in is how people lock themselves out of their own organization.

The draft policies on Policy Staging

8 draft policies are attached to Policy Staging, the one OU that never holds a workload. They are the policies from the set we delivered with the Audit, now in `tidepost-foundation` as code and attached on January 23 (W2). Nothing is enforced on anything that runs: `tp-management` is exempt from every SCP and RCP by design, the new accounts carry no workload, and `tp-policy-test`, the account that will exercise them, does not exist until you provision it in week 2.

The draft policies, attached to Policy Staging in W2.

ID	Policy	Kind	What it blocks
POL-S1	tp-scp-baseline	SCP	Four statements: a member account leaving the organization; stopping or deleting CloudTrail, AWS Config, GuardDuty, or Security Hub; any call in a Region other than us-east-1 and us-west-2, except global services; and launching an instance, or changing one, with IMDSv1 allowed (ec2:MetadataHttpTokens must be required).
POL-S2	tp-scp-no-member-root	SCP	Any action by the root user of a member account signed with root credentials.
POL-S3	tp-scp-no-iam-users	SCP	Creating IAM users, console passwords, and access keys.
POL-R1	tp-rcp-s3-perimeter	RCP	Access to S3 buckets by principals outside the organization.
POL-R2	tp-rcp-kms-perimeter	RCP	Use of KMS keys by principals outside the organization.
POL-R3	tp-rcp-sts-perimeter	RCP	sts:AssumeRole into a role in the organization by a principal outside it. Web identity and SAML federation (GitHub Actions, Identity Center) are governed by their own trust policies and are not in this statement.
POL-D1	tp-decl-ec2-imds	declarative (EC2)	Changing the account's instance metadata default: every new launch gets IMDSv2 required unless its own call asks for IMDSv1, and tp-scp-baseline denies that call. No one in a member account can change the default.
POL-D2	tp-decl-ec2-no-public-sharing	declarative (EC2)	Sharing an EBS snapshot or an AMI publicly (snapshot and image block public access, which a member account cannot turn off).

Each one gets proven against test cases in tp-policy-test before it goes anywhere with an account in it; that is week 2 and week 3. The rule is that no policy reaches an OU with an account in it until it has been tried against a test account first.

Foundation scan checks this week

2 of the 11 checks that can pass before the final scan are passing. MAF-13, no lingering access, is judged at the end: the operator role exists on purpose until February 13. MAF-11, the shared network, is out of scope for the add-on.

The foundation scan checks, MAF-01 to MAF-13 (MAF-11 not scored), at the end of week 1.

Check	Title	Status on January 23	What moved this week
MAF-01	Landing zone	Passing since January 21	Passed in W1: landing zone active and in sync, all features on
MAF-02	Accounts placed	Open	3 of 9 accounts placed
MAF-03	Organization trail	Passing since January 21	Passed in W1: organization trail logging into tp-log-archive
MAF-04	Security delegated	Open	Five services delegated to tp-audit in W1; passes when tp-prod is enrolled
MAF-05	Identity	Open	Identity Center connected in W2; passes after the people move and the IAM users retire
MAF-06	Root	Open	tp-management root has two FIDO2 keys; centralized root access and tp-prod come in week 2
MAF-07	Guardrails	Open	Eight draft policies on Policy Staging; 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

Nothing failed this week, but three things are less finished than the green results suggest. No pre-flight check failed and neither window recorded a blocker.

- **Identity Center is not under the landing zone.** The landing zone was set up without managing it, so its configuration lives in tidepost-foundation and must be kept in sync by pull request. That is deliberate and it is one more thing to keep current.

- **The landing-zone rollback is weaker than it looks.** Decommissioning the landing zone is a console action, but the operator role cannot close accounts, so tp-log-archive and tp-audit would stay as empty accounts. We accepted that because no workload is in the organization yet.
- **Two checks that sound done are not.** The security services are delegated, but MAF-04 needs tp-prod enrolled. Identity Center is connected, but MAF-05 needs the people moved and the IAM users retired. Counting either as passed would overstate the week.

What happens next

Week 2 is the week with the risk: the founders' account joined and enrolled. The window, W3, is January 28, 2026 (09:00 to 15:00 CST).

The next steps.

When	Who	What
January 26	Kofi Brandvold	People move to Identity Center; the join pre-flight runs for the first time
January 26	Dev Raman and Kofi Brandvold	Approve W3 in writing, two business days ahead
January 28	Vantalect and Tidepost	W3: The join and enrollment

What we need from you: Dev Raman and Kofi Brandvold, the W3 approval by January 26, and Gwen Tallis on standby for any billing question the join pre-flight raises.

The week day by day

Week 1, from kickoff to the second window.

Date	Who	What
January 20	Kofi Brandvold	Kickoff; the operator role created in tp-management from the template Vantalect sent January 16
January 21	Vantalect	W1: Landing zone
January 21	Dev Raman	W2 approved in writing
January 22	Kofi Brandvold	Break-glass user created and its hardware key sealed
January 23	Vantalect	W2: IAM Identity Center and the identity provider

© 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.