

Vantalect



AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

Foundation Plan Readout

Before week 1: Plan readout · prepared for Tidepost, Inc.

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

January 16, 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

- The plan 2
- Where the organization starts 3
- Greenfield, and why 5
- The target organization 6
- Six change windows 7
- How write access works 9
- The guardrails 10
- The risk register 10
- The gate and the fee 13
- Decisions we need today 13
- The next four weeks 14

The plan

Tidepost gets a new AWS organization of 9 accounts, and the founders’ account joins it as production on January 28 without moving a single workload. Dev Raman: this is the Multi-Account Foundation’s plan, presented inside the Audit’s readout today because the Audit’s week-one scan and governance review were its discovery. The add-on runs four weeks, from January 20 to February 13, 2026, inside 70 consultant hours, through 6 change windows you approve one at a time.

The Foundation add-on as agreed at the readout.

Measure	Plan
Path	Greenfield
Accounts in the target organization	9
Change windows in the management account	6
Foundation scan checks in scope	12 of 13
Checks passing on the week-one scan (January 5)	1
Baseline policies, proven in Policy Staging first	11
Consultant hours, capped	70
Fee (already net; half on signature, half on the gate)	\$25,000

The week-one scan ran the thirteen foundation checks beside the Audit's own on January 5, 2026. One passed, and only because there was nothing to find: MAF-13 checks that our operator role is gone, and it did not exist yet. The scan, the inventory, and the governance review are chapters of the week-one scan and audit reports; this document is the plan built on them, and the policy set it attaches is in the appendix.

Where the organization starts

There is no organization. Production, staging, development, data science, and CI run in one account that is also its own payer, with root keys, 18 IAM users, and no trail anyone else holds. That is why 1 of 12 checks pass, and why every other one fails on the same fact.

The foundation scan on January 5, 2026, check by check. MAF-11 is out of scope: one VPC and no Transit Gateway.

Check	Passes when	Week one	Why
MAF-01 Landing zone	The landing zone is enrolled, active, and not drifted; all features are on in the organization	Fail	No organization and no landing zone
MAF-02 Accounts placed	Every in-scope account is in its target OU and enrolled	Fail	One standalone account; no organization to place it in
MAF-03 Organization trail	A multi-Region organization trail, logging, with log file validation, delivers to a bucket in the Log Archive account	Fail	No trail of any kind (C-9)
MAF-04 Security delegated	GuardDuty, Security Hub, IAM Access Analyzer, and the Config aggregator (and Inspector) are administered from the Audit account, with new accounts enrolled automatically	Fail	No security service enabled
MAF-05 Identity	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	Fail	No Identity Center; 18 IAM users, seven of them administrators with long-lived keys
MAF-06 Root	The management account's root user has MFA; centralized root access is on; member accounts hold no root password or access keys	Fail	Two active root access keys and no root MFA (C-1)
MAF-07 Guardrails	The agreed SCPs, RCPs, and declarative policies are attached at the agreed OUs, inherited by every in-scope account, and match the repository	Fail	No organization, so no SCP, RCP, or declarative policy
MAF-08 Controls	The agreed Control Tower controls are enabled on every target OU	Fail	No Control Tower
MAF-09 Vending	New accounts are vended through Account Factory, and one account vended in week five passes MAF-02 through MAF-08 untouched by hand	Fail	No Account Factory
MAF-10 Backup	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	Fail	No central backup; a snapshot cron job in the one account

Check	Passes when	Week one	Why
MAF-11 Network	Shared networking is owned by a Network account and shared through AWS RAM	Out of scope	One VPC and no Transit Gateway
MAF-12 Tagging	The agreed tag policy is attached and effective, with its compliance report readable from the management account	Fail	No tags on 94% of resources and no tag policy
MAF-13 No lingering access	Vantalect's operator role and any temporary assignment are gone from the management account	Pass	No role yet

Greenfield, and why

We recommend the greenfield path, and it is the only path: a retrofit needs an organization to keep. Dev Raman decided it today. The reasons, as recorded:

- No organization existed: the founders' account was its own payer, so there was nothing to retrofit.
- The account that would have been the payer runs production, and the management account holds no workloads.
- The founders' account joins as the production member, so no workload moves and no commitment or credit is lost (there were none: no Savings Plan, no Reserved Instance, and the Activate credits ran out in June 2025).

Greenfield usually means moving accounts out of an old organization, with the billing split, the lost commitments, and the broken organization conditions that come with it. Tidepost's version is the gentle one. The founders' account is invited into the new organization and accepts; it keeps its resources, quotas, and IAM; and it lands in Workloads/Prod. The new management account, tp-management, which Tidepost created on January 12, 2026, becomes the payer and runs no workload.

Not in the plan. Moving the staging and data workloads out of tp-prod is workload migration, a change order or another statement of work. The add-on vends the accounts; Tidepost moves into them on its own calendar (the data accounts wait for the third quarter).

The target organization

9 accounts in 9 OUs (2 of them empty by design), with production alone in Workloads/Prod and nothing running in the management account.

The account map. Every root email is a company group alias; no account is created with a root password.

Account	OU	Purpose	Created by
tp-management	Root	Payer, Control Tower, IAM Identity Center, and the Cost and Usage Report data export	Tidepost, January 12
tp-log-archive	Security	The organization trail and AWS Config history	Vantalect, in W1
tp-audit	Security	Delegated GuardDuty, Security Hub, IAM Access Analyzer, the Config aggregator, and Inspector	Vantalect, in W1
tp-backup	Infrastructure	The central backup vault (vault lock in compliance mode) and delegated AWS Backup	Vantalect, in W6
tp-prod	Workloads/Prod	Production, and until June the old staging: the founders' account, joining as the production member	Tidepost, March 4, 2024 (joins in W3)
tp-staging	Workloads/NonProd	Staging, empty until the June rebuild (EC2-1a)	Tidepost, through Account Factory
tp-dev	Workloads/NonProd	Developer instances, moved by Tidepost's engineers on February 4	Tidepost, through Account Factory
tp-sandbox-ml	Sandbox	Notebooks and experiments; vended through Account Factory untouched by hand (MAF-09)	Vantalect, in W5
tp-policy-test	Policy Staging	Proving every policy before it is attached	Tidepost, through Account Factory

Two OUs start empty on purpose. Suspended holds an account on its way out, under a deny-all policy. Exceptions holds an account that needs something the baseline forbids, such as an IAM user, and nothing goes there without a written exception. The governed Regions are us-east-1

and us-west-2, and the Region policy allows both. Keeping us-west-2 to backup copies is a convention, not a guardrail: nothing in the policy set stops a workload launching there, so the platform team checks it at each monthly review.

Six change windows

Every change to the management account happens in a window you approve in writing at least two business days ahead, and nothing outside the window's list is done in it. Dev Raman and Kofi Brandvold approve each one. W1 is approved today.

W1, Landing zone: January 21, 09:00 to 15:00 Central, 3 pre-flight checks.

- 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
- Rollback: 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, 09:00 to 12:00 Central, 3 pre-flight checks.

- 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
- Rollback: 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.

W3, The join and enrollment: January 28, 09:00 to 15:00 Central, 9 pre-flight checks.

- 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
- Rollback: 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.

W4, Policies to Sandbox and NonProd: February 3, 09:00 to 12:00 Central, 4 pre-flight checks.

- Update tp-scp-baseline with the Control Tower role exemption found in Policy Staging, and re-run its staging cases
- Attach the baseline SCPs, RCPs, and declarative policies to Sandbox and Workloads/NonProd from Policy Staging
- Enable the eight elective Control Tower controls on both OUs
- Start the denial watch: CloudTrail queried for access denied by a policy
- Rollback: Detach each policy from the OU: one management-account call per policy per OU. Disabling a control is one call.

W5, Policies to Prod, and the vended account: February 5, 09:00 to 13:00 Central, 4 pre-flight checks.

- Attach the baseline policies and controls to Workloads/Prod, Security, and Infrastructure, after the watch
- Attach the baseline minus the IAM-user policy to Exceptions, and the deny-all policy to Suspended (both OUs are empty)
- Vend tp-sandbox-ml through Account Factory into Sandbox
- Move tp-policy-test into Suspended for fifteen minutes to prove the deny-all policy, then back to Policy Staging
- Enable the tag policy and backup policy types, and attach the draft backup and tag policies to Policy Staging (the draft backup policy copies to a test vault in tp-policy-test's us-west-2, because tp-backup does not exist yet)
- Rollback: Detach the policies from Workloads/Prod, Security, and Infrastructure (one call each); a vended account stays, because the operator role cannot close accounts, and Tidepost can suspend it.

W6, Backup and tag policies; the backup account: February 10, 09:00 to 14:00 Central, 4 pre-flight checks.

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

The join window (W3) carries the most checks, because it is the one that changes who pays the bill: root email and MFA custody, organization conditions, resource shares, StackSets, delegated administrators, commitments and Marketplace agreements, the account's ability to stand alone again (which the rollback needs), and Control Tower's enrollment prerequisites.

How write access works

Read-only everywhere, and write access only in the management account, only inside an approved window, through a role Tidepost owns. Control Tower's set-up needs administrator-level permissions there, so the control is approval and time rather than a narrow policy.

- **The role is yours, and it expires.** Kofi Brandvold creates `VantalectFoundationOperator` in tp-management from the template we send today, after reading it. Its trust policy: 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. You set the dates for each window, and no session can start late enough to outlive one, so access outside a window is impossible rather than forbidden.
- **Some things are denied outright:** closing accounts, deleting the organization, changing payment methods or billing contacts, creating IAM users or access keys, leaving the organization. Account emails, root credentials, and payment methods stay with Tidepost.
- **Everything is seen.** Every call lands in the organization trail with his source identity; an EventBridge rule posts each AssumeRole to the platform channel.

- **Member accounts change only as code.** Vantalect holds no write access to any member account; everything inside members goes through tidepost-foundation and tidepost-cdk pull requests.
- **It ends.** On February 13 Tidepost deletes the role, and MAF-13 in the final scan proves it.

The guardrails

The policy set is 11 policies: 4 SCPs, 3 RCPs, 2 EC2 declarative policies, a tag policy, and a backup policy, each proven in Policy Staging before any other OU sees it. The appendix has each one as code, with what it blocks and who it would affect today.

The baseline is three SCPs rather than one per purpose because AWS allows at most 5 SCPs on an OU, and FullAWSAccess and Control Tower's own SCP take two of them on every OU the landing zone governs. A new statement joins one of the three baseline SCPs; it never becomes a fourth attachment. The rollout order is fixed: Policy Staging, then Sandbox and NonProd, then Prod, Security, and Infrastructure after at least a day with no access denied by a policy. SCPs and RCPs never apply to the management account, which is why it runs nothing.

The risk register

The register holds 10 risks sized for Tidepost: 1 high, 4 medium, and 5 low. Most of what makes a greenfield move dangerous is absent here, and the register says so rather than inflating it.

The risk register as agreed at the readout.

ID	Risk	Size	Owner	As found	Plan
FR-1	Billing transfer	Medium	Gwen Tallis	One account that joins mid-month, with no commitments or credits, no budgets, no cost allocation tags, and no Cost and Usage Report to carry over	Gwen Tallis exports twelve months of Cost Explorer data the day before the join, because the new payer cannot see the account's history; the CUR 2.0 data export starts in tp-management at the join; January's invoice splits at the join. The join is not held to a month boundary, because nothing in the account depends on one.
FR-2	Reserved Instances and Savings Plans	Low	Gwen Tallis	None exist; the Activate credits ran out in June 2025	Nothing to protect at the join. A commitment bought later is bought after the join, with discount sharing left on across the organization (the default).
FR-3	Marketplace subscriptions	Low	Gwen Tallis	No active subscription in the inventory	Listed again from the Marketplace and License Manager consoles the week of the join; an agreement found then waits on its vendor.
FR-4	Support plans	Medium	Gwen Tallis	Support plans are per account: tp-prod has Business Support+ on its own usage, the new accounts start on Basic Support, and an account that has to leave again needs a plan, contact information, and a current payment method of its own	Business Support+ stays on tp-prod, and the new accounts start on Basic Support. The pre-flight confirms tp-prod could stand alone again (contact information, a current payment method, a support plan), because leaving is the join's rollback.
FR-5	Service quotas	Low	Kofi Brandvold	Quotas move with the account; a vended account starts at the defaults	A Service Quotas organization template carries the raised quotas to every vended account; the vended sandbox account proves it.

ID	Risk	Size	Owner	As found	Plan
FR-6	Account-level dependencies	Low	Kofi Brandvold	There was no source organization, so no policy conditioned on a source organization ID	The pre-flight searches tp-prod's bucket, key, and role policies, its RAM shares, StackSets, and delegated administrators before the join; the RCPs are written against the new organization ID.
FR-7	Root email and MFA custody	Medium	Sasha Ilyin	tp-prod held two active root keys and no MFA on January 5	Root emails on company group aliases; tp-management's root already has two FIDO2 keys in separate custody; centralized root access turns on at the join and tp-prod's root credentials are removed after it; the recovery path is tested in Policy Staging. Vantalect never holds a root credential.
FR-8	SCP and RCP blast radius	High	Kofi Brandvold	Production runs in one account; a wrong deny stops it, and the error surfaces only as access denied	Every policy proven in Policy Staging, then attached to Sandbox and NonProd, then to Prod after at least 24 hours without a policy-caused denial. Three baseline SCPs, because FullAWSAccess and Control Tower's SCP take two of the five each OU allows. Detaching is the rollback.
FR-9	Control Tower enrollment	Low	Kofi Brandvold	One existing account to enroll, with Config off	The pre-flight checks tp-prod for an AWS Config recorder or delivery channel and for the execution role; tp-prod's own enrollment is the pilot.
FR-10	SOC 2 timing	Medium	Sasha Ilyin	The observation window opens April 1	The organization trail and the log archive go in during week one, so every control the Foundation provides has a start date before April 1.

The one high risk is the blast radius. Production runs in one account, so a deny with a wrong condition stops it, and the only symptom is access denied. That is why the guardrails reach Prod last and why each attachment has a one-call rollback.

The billing transfer is medium and mostly bookkeeping. There is no commitment, credit, budget, or cost allocation tag to carry, so the join does not wait for a month boundary. Gwen Tallis exports the account's twelve months of Cost Explorer data before the join, because once tp-management is the payer it sees the account's costs only from the join.

The gate and the fee

Every check of the foundation scan agreed at the readout passes at the end, and a check waived in writing counts as passed. The 12 checks in scope are agreed today; MAF-11 is out because Tidepost has one VPC and no shared network to own. The fee is \$25,000, already net of the Audit's discovery: \$12,500 was invoiced at signature, and \$12,500 is invoiced only when the gate is met.

Decisions we need today

The decisions that start week one.

No. Decision	Who
1 Agree the greenfield path and the account map	Dev Raman
2 Agree the 12 checks in scope, with MAF-11 out	Dev Raman
3 Approve W1 (January 21) in writing	Dev Raman and Kofi Brandvold
4 Create VantalectFoundationOperator from the template before the January 20 kickoff	Kofi Brandvold
5 Name the finance contact for the Cost Explorer export and the payment information the join's rollback needs	Gwen Tallis
6 Agree that moving workloads out of tp-prod stays outside the add-on, on Tidepost's own calendar	Dev Raman

The next four weeks

The add-on by week. Week one starts on January 20, the day after Martin Luther King Jr. Day.

WeekDates	What happens	Windows
1January 20 to January 23	Landing zone and core accounts	W1, W2
2January 26 to January 30	The founders' account joins and is enrolled	W3
3February 2 to February 6	Guardrails, vending, and shared services	W4, W5
4February 9 to February 13	Backup, tags, re-scan, and handover	W6

Sasha Ilyin owns the SOC 2 timeline, and the plan respects it: the organization trail and the log archive arrive in week one, so every control the Foundation provides has a start date well before the observation window opens on April 1, 2026. We are not Tidepost's auditor, and nothing here predicts what the auditor will conclude.

© 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.