

AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

Guardrails, Vending, and Shared Services

Week 3 of 4: Guardrails and vending · prepared for Tidepost, Inc.

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

February 6, 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	4
Policy Staging: the cases and the one correction	4
The correction.....	5
The SCP quota and why the baseline is three SCPs	6
W4: Policies to Sandbox and NonProd	7
W5: Policies to Prod, and the vended account	8
Attachments, OU by OU	9
What each policy does to Tidepost today	11
The eight elective controls.....	11
The Suspended move test	12
Tidepost's accounts: tp-dev	12
The vended account: tp-sandbox-ml	12
The break-glass role	13
The draft backup and tag policies.....	13
Foundation scan checks this week.....	14
What did not go to plan	15
What happens next.....	15

Summary

The baseline policies are on every OU that holds an account, no policy caused an access denial after any attachment, and the first account vended through Account Factory passed the foundation scan untouched. Dev Raman, Kofi Brandvold, and Sasha Ilyin: this is week 3 of 4 of the Multi-Account Foundation, covering 2 change windows (W4 and W5, 7 hours between them) and 18 hours of work, 53 of the 70 used so far. Across the two windows, 8 pre-flight checks ran with no blockers.

Production was the risky attachment, and it went last: 45 hours of watching after the non-production OUs, then W5. The one correction of the week was found before any of that, in tp-policy-test.

Week 3 in nine numbers.

Week 3 at a glance	Result
Change windows	W4 (February 3, 3 hours) and W5 (February 5, 4 hours)
Policy Staging cases, across all 11 policies	29
Policies corrected after staging	1 (tp-scp-baseline)
Hours between the NonProd and Prod attachments	45, with 0 policy-caused denials
Policy-caused denials after the Prod attachment (through February 6)	0
OUs newly enforcing policies, besides Policy Staging	7
Elective Control Tower controls enabled	8, on 5 OUs
Accounts in the organization	8 of 9 planned
Foundation scan checks passed to date	7 of 11

The week day by day

Week 3, from the corrected policy to the next window's approval.

Date	Who	What
February 2	Kofi Brandvold	Corrected detection policy merged
February 3	Vantalect	W4: Policies to Sandbox and NonProd
February 3	Dev Raman	W5 approved in writing
February 3	Kofi Brandvold	tp-dev provisioned after the window closed
February 4	Kofi Brandvold	Tidepost's engineers move the developer instances into tp-dev; the break-glass role created in tp-prod, with the vendor key rotation role
February 5	Vantalect	W5: Policies to Prod, and the vended account
February 6	Dev Raman	W6 approved in writing

Policy Staging: the cases and the one correction

Every policy is tried against test cases in `tp-policy-test` before it reaches an OU with accounts in it. The account sits in the Policy Staging OU, and the cases began on January 29. There are 29 across the 11 policies. Each case is a call that should be denied, a call that should be allowed, or, for the tag policy, a call that should be reported; the allow cases matter as much as the deny cases, because a policy that blocks everything also passes every deny test.

Policy Staging cases per policy. The last baseline run before the window was February 2.

Policy	Name	Kind	Cases
POL-S1	tp-scp-baseline	SCP	9
POL-S2	tp-scp-no-member-root	SCP	2
POL-S3	tp-scp-no-iam-users	SCP	5

Policy	Name	Kind	Cases
POL-S4	tp-scp-suspended-deny-all	SCP	1
POL-R1	tp-rcp-s3-perimeter	RCP	3
POL-R2	tp-rcp-kms-perimeter	RCP	1
POL-R3	tp-rcp-sts-perimeter	RCP	2
POL-D1	tp-decl-ec2-imsds	declarative (EC2)	1
POL-D2	tp-decl-ec2-no-public-sharing	declarative (EC2)	2
POL-T1	tp-tag-baseline	tag policy	2
POL-B1	tp-backup-prod	backup policy	1

The correction

tp-scp-baseline denied Control Tower's own repair, and staging caught it on January 30. The baseline SCP's detection statement denied Control Tower's own Config update during a drift repair. The statement exists to stop anyone stopping or deleting CloudTrail, AWS Config, GuardDuty, or Security Hub, and it caught the one role that has to touch them. On a live OU that would have been a drift repair failing with an access-denied error nobody expected.

The fix is an exemption: the Control Tower execution role is exempt from the detection statement. Kofi Brandvold's team merged it on February 2 and we re-ran its staging cases, and the corrected policy went out in W4. The policy has 9 staging cases; the allow case for a Control Tower drift repair is the one this correction exercises:

- deny: organizations:LeaveOrganization from a member account.
- deny: cloudtrail:StopLogging on the organization trail.
- deny: config:StopConfigurationRecorder.
- allow: a Control Tower drift repair that updates the Config recorder.
- deny: ec2:RunInstances in eu-west-1.
- allow: backup:StartCopyJob into us-west-2.
- deny: ec2:RunInstances with HttpTokens optional.
- allow: ec2:ModifyInstanceMetadataOptions that keeps HttpTokens required.
- allow: a Control Tower role's call in eu-west-1.

The policy’s other exemptions did not change: the break-glass role is exempt from the detection, Region, and instance-metadata-change statements, and global services are exempt from the Region statement. What each policy affects today is in the policy set’s appendix; for this one: No one: nothing runs outside us-east-1, us-west-2 holds backup copies, the Hardening’s detective services are not touched, and every launch template requires IMDSv2 since January 22 (H-2).

The SCP quota and why the baseline is three SCPs

AWS allows 5 SCPs on any root, OU, or account, and 2 of them are taken before we add one. FullAWSAccess and Control Tower’s SCP for its preventive controls occupy a slot on every registered OU. That leaves 3 for the baseline, so the baseline is exactly 3 SCPs, and a design that needed a fourth would not have fit.

The rule that follows: **a new statement joins one of the three baseline SCPs; it never becomes a fourth attachment.** Resource control policies have the same limit of 5, with RCPFullAWSAccess fixed and 3 in the baseline.

SCP slots on each OU once the attachments below are in. A full OU has no room for a fourth baseline SCP.

OU	SCP slots attachedOf the limit of 5
Policy Staging	5Full
Sandbox	5Full
Workloads/NonProd	5Full
Workloads/Prod	5Full
Security	5Full
Infrastructure	5Full
Exceptions	44 of 5; the IAM-user policy is deliberately absent
Suspended	33 of 5; the deny-all policy plus the two fixed

The three baseline SCPs are tp-scp-baseline (four statements), tp-scp-no-member-root, and tp-scp-no-iam-users. The deny-all policy tp-scp-suspended-deny-all sits only on Suspended, which is why that OU has 3 rather than 5.

W4: Policies to Sandbox and NonProd

February 3, 2026, 09:00 to 12:00 CST (3 hours). Approved on January 30, 2026 by Dev Raman and Kofi Brandvold, in writing, by email, two business days ahead. Result: **Baseline policies and controls on Sandbox and NonProd; the watch began at the window’s end.**

- 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.

W4 pre-flight: 4 checks, 0 blockers.

Pre-flight check	Result	Note
Policy content in the repository equals the content to be attached (hash compared)	Pass	Merged February 2
IAM Access Analyzer policy validation on every policy	Pass	No errors and no security warnings
All Policy Staging cases pass	Pass	Including the three re-run on the morning of the window
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: Detach each policy from the OU: one management-account call per policy per OU. Disabling a control is one call.

The watch began when the window ended. The rule is that CloudTrail is queried for access denied by a policy for at least 24 hours after each attachment before the next, more critical OU. We waited 45 hours before W5. The query found no denials caused by a policy.

W5: Policies to Prod, and the vended account

February 5, 2026, 09:00 to 13:00 CST (4 hours). Approved on February 3, 2026 by Dev Raman and Kofi Brandvold, in writing, by email, two business days ahead. Result: **Baseline on every OU; tp-sandbox-ml vended and passing MAF-02 through MAF-08 untouched by hand.**

- 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).

W5 pre-flight: 4 checks, 0 blockers.

Pre-flight check	Result	Note
At least 24 hours since the NonProd attachment without a policy-caused access denial	Pass	45 hours, from the end of the February 3 window; zero denials
Policy content in the repository equals the content attached to Sandbox and NonProd	Pass	Hashes match
The break-glass role and the vendor key rotation role exist in tp-prod, and the IAM-user policy exempts each	Pass	Created by Tidepost's pipeline on February 4
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: 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.

Attachments, OU by OU

8 OUs carry a policy at the end of the week, attached in two windows. The order is the risk order: the test OU first (in week 1), then the two non-production OUs, then the OUs that hold production and shared services, then the two OUs that hold no account.

Attachments made in week 3. Policy Staging also carries the eight draft policies attached in week 1 (January 23).

OU	Date	Window	Attached	SCPs on the OU
Sandbox	February 3	W4	tp-scp-baseline, tp-scp-no-member-root, tp-scp-no-iam-users, tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter, tp-decl-ec2-imds, tp-decl-ec2-no-public-sharing	5
Workloads/NonProd	February 3	W4	tp-scp-baseline, tp-scp-no-member-root, tp-scp-no-iam-users, tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter, tp-decl-ec2-imds, tp-decl-ec2-no-public-sharing	5
Workloads/Prod	February 5	W5	tp-scp-baseline, tp-scp-no-member-root, tp-scp-no-iam-users, tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter, tp-decl-ec2-imds, tp-decl-ec2-no-public-sharing	5
Security	February 5	W5	tp-scp-baseline, tp-scp-no-member-root, tp-scp-no-iam-users, tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter, tp-decl-ec2-imds, tp-decl-ec2-no-public-sharing	5
Infrastructure	February 5	W5	tp-scp-baseline, tp-scp-no-member-root, tp-scp-no-iam-users, tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter, tp-decl-ec2-imds, tp-decl-ec2-no-public-sharing	5
Exceptions	February 5	W5	tp-scp-baseline, tp-scp-no-member-root, tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter, tp-decl-ec2-imds, tp-decl-ec2-no-public-sharing	4
Suspended	February 5	W5	tp-scp-suspended-deny-all	3
Policy Staging	February 5	W5	tp-tag-baseline, tp-backup-prod	5

Two OUs differ on purpose. Exceptions carries the baseline minus tp-scp-no-iam-users, because it is the only OU where an IAM user is allowed, and only with a written exception. Suspended carries only tp-scp-suspended-deny-all. Both are empty, so neither affects a running system today.

What each policy does to Tidepost today

For nearly everyone: nothing. That is the point of proving them first. The table reads the policy set's own "affects today" column.

The effect of each baseline policy on Tidepost's accounts.

Policy	Affects today
tp-scp-baseline	No one: nothing runs outside us-east-1, us-west-2 holds backup copies, the Hardening's detective services are not touched, and every launch template requires IMDSv2 since January 22 (H-2)
tp-scp-no-member-root	No one; tp-prod's root credentials were removed on January 29, and new accounts are created without them
tp-scp-no-iam-users	The video analytics vendor's IAM user in tp-prod: its key is rotated only through the rotation role (the MAF-05 waiver)
tp-rcp-s3-perimeter	No one: the media buckets are read through CloudFront; the video analytics vendor reads its one renditions prefix as an IAM user in tp-prod, a principal inside the organization, so the perimeter admits it (its limits are the MAF-05 waiver's); and the marketing vendor's share (C-3) was closed on January 6
tp-rcp-kms-perimeter	No one
tp-rcp-sts-perimeter	Four vendor roles in tp-prod and the scan's read-only roles, both on the exemption list; any other outside account is denied
tp-decl-ec2-imds	New launches only; existing instances are the Hardening's H-2
tp-decl-ec2-no-public-sharing	No one

The eight elective controls

Eight detective controls are on five OUs: the four that hold accounts, and Infrastructure, which gets its first account, tp-backup, in week 4. The landing zone's own mandatory controls were already on every registered OU. The elective ones detect and report; none of them blocks.

- Detect public read access to S3 buckets
- Detect public write access to S3 buckets
- Detect unencrypted EBS volumes attached to instances
- Detect RDS instances that are publicly accessible

- Detect unencrypted RDS storage
- Detect unrestricted incoming SSH
- Detect a root user without MFA
- Detect IAM console users without MFA

Sandbox and Workloads/NonProd got them with the policies in W4 on February 3. Workloads/Prod, Security, and Infrastructure got them in W5 on February 5. Disabling a control is one call.

The Suspended move test

On February 5, `tp-policy-test` spent fifteen minutes in the Suspended OU and then went back. The point was to prove the deny-all policy does what its name says, on an account where nothing mattered, before the first real account needed it. The case is deny: any call from `tp-policy-test` while it is moved into Suspended, and the Control Tower execution role stays exempt so the landing zone can still govern and repair a suspended account.

Tidepost's accounts: `tp-dev`

`tp-dev` was provisioned by Tidepost on February 3, in the afternoon, after the day's window had closed. Vantalect had no part in it. It landed in Workloads/NonProd, where the baseline had been attached that morning, so it inherited the policies from its first minute. Tidepost's engineers moved the developer instances into it on February 4; its infrastructure code lives in `tidepost-cdk`.

The vended account: `tp-sandbox-ml`

`tp-sandbox-ml` was vended through Account Factory in W5 and passed MAF-02 through MAF-08 untouched by hand. That is the proof behind MAF-09: a new account, created by the machinery and not a person, that satisfies the checks without anyone repairing it afterward. It sits in the Sandbox OU and is owned by Yuki Sorensen's team. Nobody has touched it since.

The Service Quotas template is the reason a vended account is usable on day one rather than waiting on a quota request. It applies the agreed quotas to every vended account:

The Service Quotas template. A vended account starts at the AWS defaults, and the template raises them to these values.

Quota	ValueAccount	Basis
Running On-Demand Standard instances (vCPUs)	256tp-dev	22 developer m5.2xlarge, 8 vCPUs each, is 176
ml.g5.12xlarge for notebook instance usage	2tp-sandbox-ml	One in use
ml.g5.2xlarge for notebook instance usage	5tp-sandbox-ml	Four in use

The break-glass role

TidepostBreakGlass now exists in tp-prod, created by Tidepost's pipeline on February 4. The IAM-user policy exempts it outright, so it is the path for the rare case where an IAM user or key has to change. The one routine key change, the video analytics vendor's rotation, has its own narrower role, TidepostVendorKeyRotation, created the same day: the policy exempts it only for that user's access keys. Every sign-in and every AssumeRole posts to the platform channel and opens a ticket. Custody of the matching user, bg-admin, sits with Sasha Ilyin and Noor Castellanos. The role is exempt from the detection, Region, and instance-metadata-change statements of the baseline for the same reason: when it is needed, nothing should stop it.

W5's pre-flight checked that it existed before the policy reached Workloads/Prod. The attachment would otherwise have left tp-prod with IAM users it could not change.

The draft backup and tag policies

The tag and backup policy types are on, and both policies are attached to Policy Staging only. They did not leave staging this week. tp-tag-baseline and tp-backup-prod are drafts, and the backup policy copies to a test vault in tp-policy-test's us-west-2, because tp-backup does not exist yet.

The tag policy sets allowed values on 4 keys and enforces them on EC2 instances, EBS volumes, and RDS databases only; anywhere else it reports. The backup policy backs up resources tagged backup=required and selects none today. Staging cases for both run on February 6 and again on February 9, ahead of the window that moves them: W6, February 10.

Foundation scan checks this week

7 of the 11 checks that can pass before the final scan are passing, up from 4 at the end of week 2. MAF-07, MAF-08, and MAF-09 passed on February 5. MAF-13 is judged at the final scan; MAF-11, the shared network, is out of scope.

The foundation scan checks at the end of week 3.

Check	Title	Status on February 6	What moved this week
MAF-01	Landing zone	Passing since January 21	No change
MAF-02	Accounts placed	Open	8 of 9 accounts placed (tp-dev, tp-sandbox-ml)
MAF-03	Organization trail	Passing since January 21	No change
MAF-04	Security delegated	Passing since January 29	No change
MAF-05	Identity	Open	Unchanged: the IAM users are still to retire
MAF-06	Root	Passing since January 29	No change
MAF-07	Guardrails	Passing since February 5	Passed: baseline on every OU with accounts, hashes match the repository
MAF-08	Controls	Passing since February 5	Passed: eight elective controls on the four OUs that hold accounts and on Infrastructure, ready for tp-backup
MAF-09	Vending	Passing since February 5	Passed: tp-sandbox-ml vended and untouched by hand
MAF-10	Backup	Open	Draft backup policy in Policy Staging; tp-backup not yet created
MAF-12	Tagging	Open	Draft tag policy in Policy Staging; not yet on a workload OU
MAF-13	No lingering access	Judged at the final scan	No change

What did not go to plan

One policy was wrong, one account missed its window, and none of it reached production.

- **tp-scp-baseline was wrong.** It denied Control Tower's own repair, found on January 30 in staging, fixed on February 2, and re-tested before W4. The cost was a policy revision, not an outage, which is what staging is for.
- **tp-dev was provisioned after the window.** It is Tidepost's account, created in the afternoon of February 3, so it was never part of the W4 change; it inherited the policies that were already attached.
- **The SCP quota narrowed the design.** The baseline holds 3 SCPs because 5 is the limit and 2 slots are fixed. Every new rule becomes a statement in one of the three, not a fourth policy, and Exceptions and Suspended are the only OUs with spare room.
- **One vendor's key is affected.** tp-scp-no-iam-users stops anyone creating IAM users or keys. The video analytics vendor's IAM user in tp-prod: its key is rotated only through the rotation role (the MAF-05 waiver). The written waiver for MAF-05 comes later in the add-on.

What happens next

Week 4 closes the foundation: backup, tags, re-scan, and handover. W6 is February 10, 2026, 09:00 to 14:00 CST.

The next steps.

When	Who	What
February 6	Dev Raman and Kofi Brandvold	Approve W6 in writing, two business days ahead
February 10	Vantalect and Tidepost	W6: Backup and tag policies; the backup account, 09:00 to 14:00 CST
February 13	Vantalect and Tidepost	The re-scan, the closing readout, with the operator role deleted by Tidepost first

What we need from you: Dev Raman and Kofi Brandvold, the W6 approval by February 6.

© 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.