

AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

The Policy Set as Code

Week 2 of the Audit: Design (appendix) · prepared for
Tidepost, Inc.

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

January 15, 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

- How to read this appendix 2
- The quota that shapes the set 3
- Service control policies 4
 - POL-S1: tp-scp-baseline 6
 - POL-S2: tp-scp-no-member-root 7
 - POL-S3: tp-scp-no-iam-users..... 8
 - POL-S4: tp-scp-suspended-deny-all 9
- Resource control policies 9
 - POL-R1: tp-rcp-s3-perimeter 11
 - POL-R2 and POL-R3..... 11
- Declarative policies 12
 - POL-D1: tp-decl-ec2-imds 12
- Tag policy and backup policy 13
 - POL-T1: tp-tag-baseline 13
 - POL-B1: tp-backup-prod 13
- Where each policy is attached 14
- The staging cases..... 17
- The Control Tower controls 19

How to read this appendix

The foundation’s policy set is 11 policies, written as code, and every one was designed to stop something specific while breaking nothing Tidepost runs today. This appendix is for Kofi Brandvold (Head of Platform), who owns the repository the policies live in, and Sasha Ilyin (Head of Security and Compliance), who reviews every change to them. It holds the complete set that the Foundation plan readout summarizes: for each policy, what it blocks, what it exempts, who it affects today, and the cases it must pass in Policy Staging before any other OU receives it.

The set is 4 service control policies, 3 resource control policies, 2 declarative policies, 1 tag policy, and 1 backup policy, plus 40 Control Tower control enablements. Because this appendix is delivered with the Audit's week two, the facts below are written as they stand at the end of the engagement: where a policy later reached an OU, the date is given, so the document stays true when you return to it.

- **Everything is in tidepost-foundation.** Each policy is a JSON file reviewed by pull request, validated with IAM Access Analyzer, and attached only in an approved change window, after the window's pre-flight compares the content to be attached with the merged file by hash.
- **The management account is never governed by them.** SCPs and RCPs never apply to the management account, so tp-management is protected by its root user's two FIDO2 keys, the operator role's explicit denies, and the alarm on every sign-in, not by this set.
- **Placeholders.** Values in angle brackets, such as <org-id>, are the only things to fill in. The JSON shown for each kind is representative of that policy's blocks and exemptions as the tables state them; the file in the repository is the one that is attached.
- **Detaching is the rollback.** One management-account call per policy per OU undoes any attachment. The one setting below that becomes permanent is the backup vault's lock, and it is not a policy.

The policy set by kind. Every policy has an ID, a file in the repository, and staging cases.

Kind	PoliciesIDs
Service control policies	4POL-S1, POL-S2, POL-S3, POL-S4
Resource control policies	3POL-R1, POL-R2, POL-R3
Declarative policies (EC2)	2POL-D1, POL-D2
Tag policy	1POL-T1
Backup policy	1POL-B1
Total	11

The quota that shapes the set

AWS allows 5 service control policies on each root, OU, or account. 2 of them are always taken on a registered OU, by FullAWSAccess and by Control Tower's SCP for its preventive controls, so the baseline is 3 SCPs. The rule that follows is the one to remember: **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; RCPFullAWSAccess takes one, and the baseline is 3.

SCPs attached to each OU, counting the 2 fixed ones. Exceptions carries one fewer baseline SCP (the IAM-user policy); Suspended carries only the deny-all.

OU	SCPs attached	Of the limit	Headroom
Policy Staging	5	5	0
Sandbox	5	5	0
Workloads/NonProd	5	5	0
Workloads/Prod	5	5	0
Security	5	5	0
Infrastructure	5	5	0
Exceptions	4	5	1
Suspended	3	5	2

Service control policies

Three baseline SCPs are attached to every OU that holds accounts (Exceptions excepts the IAM-user policy), and a fourth, the deny-all, sits on Suspended alone. Policy POL-S1 is the only SCP with several statements; a statement added later joins it rather than becoming a fourth baseline attachment.

The service control policies. "Affects today" is who or what the policy stops on the day it is attached.

ID	Policy	Blocks	Exempts	Affects today
POL-S1	tp-scp-baseline	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).	The Control Tower execution role, from the detection statement (added February 3 after Policy Staging showed it denying a drift repair) and from the Region statement, with the other Control Tower roles (aws-controltower-*), so the landing zone's own calls are never denied; the break-glass role, from the detection, Region, and instance-metadata-change statements; global services (IAM, Organizations, Route 53, CloudFront, Support, Billing), from the Region statement	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)
POL-S2	tp-scp-no-member-root	Any action by the root user of a member account signed with root credentials.	Root sessions started centrally from tp-management with sts:AssumeRoot (the aws:AssumedRoot condition key), each scoped to one privileged task	No one; tp-prod's root credentials were removed on January 29, and new accounts are created without them
POL-S3	tp-scp-no-iam-users	Creating IAM users, console passwords, and access keys.	The break-glass role; the vendor key rotation role in tp-prod, for the vendor user's access keys only; the Exceptions OU does not carry this policy	The video analytics vendor's IAM user in tp-prod: its key is rotated only through the rotation role (the MAF-05 waiver)
POL-S4	tp-scp-suspended-deny-all	Every action in an account moved to the Suspended OU.	The Control Tower execution role, so the landing zone can still govern and repair the account	No one; the OU is empty

POL-S1: tp-scp-baseline

Four statements. The detection statement carries a correction found in Policy Staging: on January 30, 2026 it denied Control Tower's own Config update during a drift repair, and the exemption for the Control Tower execution role was merged on February 2, 2026, before any other OU received the policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyLeavingTheOrganization",
      "Effect": "Deny",
      "Action": "organizations:LeaveOrganization",
      "Resource": "*"
    },
    {
      "Sid": "DenyDisablingDetection",
      "Effect": "Deny",
      "Action": [
        "cloudtrail:StopLogging",
        "cloudtrail>DeleteTrail",
        "config:StopConfigurationRecorder",
        "config>DeleteConfigurationRecorder",
        "config>DeleteDeliveryChannel",
        "guardduty>DeleteDetector",
        "guardduty:DisassociateFromAdministratorAccount",
        "securityhub:DisableSecurityHub",
        "securityhub:DisassociateFromAdministratorAccount"
      ],
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:role/AWSControlTowerExecution",
            "<break-glass-role-arn>"
          ]
        }
      }
    },
    {
      "Sid": "DenyOutsideGovernedRegions",
      "Effect": "Deny",
      "NotAction": [
        "iam:*",
        "organizations:*",
        "route53:*",
        "cloudfront:*",
        "support:*",
        "billing:*"
      ],
      "Resource": "*",
    }
  ]
}
```

```

    "Condition": {
      "StringNotEquals": {
        "aws:RequestedRegion": ["us-east-1", "us-west-2"]
      },
      "ArnNotLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::*:role/AWSControlTowerExecution",
          "arn:aws:iam::*:role/aws-controltower-*",
          "<break-glass-role-arn>"
        ]
      }
    },
    {
      "Sid": "RequireIMDSv2",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2::*:instance/*",
      "Condition": {
        "StringNotEquals": {"ec2:MetadataHttpTokens": "required"}
      }
    },
    {
      "Sid": "KeepIMDSv2OnExistingInstances",
      "Effect": "Deny",
      "Action": "ec2:ModifyInstanceMetadataOptions",
      "Resource": "arn:aws:ec2::*:instance/*",
      "Condition": {
        "StringNotEquals": {"ec2:MetadataHttpTokens": "required"},
        "ArnNotLike": {"aws:PrincipalArn": "<break-glass-role-arn>"}
      }
    }
  ]
}

```

The IMDS statement is two entries so a launch and a later change are both covered; together they are the fourth block in the table above. The second denies a metadata change only when it would leave tokens optional, so turning the hop limit or the endpoint up or down still works. The Region statement exempts the Control Tower roles as well as break-glass, so the landing zone's own calls are never denied. The file stays well under the 5,120-character limit for an SCP, with room for the statements the next engagements add.

POL-S2: tp-scp-no-member-root

The policy denies every action signed with a member account's root credentials. A root session started centrally from tp-management carries the `aws:AssumedRoot` key, so it passes, scoped to the one task it was started for.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyMemberRootCredentials",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {"aws:PrincipalArn": "arn:aws:iam::*:root"},
        "Null": {"aws:AssumedRoot": "true"}
      }
    }
  ]
}
```

POL-S3: tp-scp-no-iam-users

Two principals are exempted, and the Exceptions OU does not carry this policy, so a written exception for a whole account has somewhere to live. The break-glass role is exempt outright. TidepostVendorKeyRotation in tp-prod is exempt only for access keys on the video analytics vendor's user, and the second statement denies it any other user. That vendor user is the one exception today, and it sits in tp-prod, outside the Exceptions OU, so MAF-05 is waived rather than passed (the waiver is in the re-scan report).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIAMUsersAndLogins",
      "Effect": "Deny",
      "Action": [
        "iam:CreateUser",
        "iam:CreateLoginProfile",
        "iam:UpdateLoginProfile"
      ],
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {"aws:PrincipalArn": "<break-glass-role-arn>"}
      }
    },
    {
      "Sid": "DenyAccessKeys",
      "Effect": "Deny",
      "Action": "iam:CreateAccessKey",
      "Resource": "*",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalArn": [

```

```

        "<break-glass-role-arn>",
        "<vendor-key-rotation-role-arn>"
    ]
  }
},
{
  "Sid": "RotationRoleOnlyForTheVendorUser",
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "NotResource": "<vendor-user-arn>",
  "Condition": {
    "ArnLike": {"aws:PrincipalArn": "<vendor-key-rotation-role-arn>"}
  }
}
]
}

```

POL-S4: tp-scp-suspended-deny-all

The deny-all sits on the Suspended OU only. Moving an account there is the fifth runbook in the handover report: the policy applies at once, and the Control Tower execution role stays able to govern and repair the account. Today it affects no one: the OU is empty.

Resource control policies

A resource control policy sets the ceiling on what can be done to a resource, whoever asks. These three are the organization's data perimeter. They use the new organization's ID, so they were written after the organization existed and not copied from anywhere.

The resource control policies. The exemptions are by account ID or by source ARN, never by a blanket allow.

ID	Policy	Blocks	Exempts	Affects today
POL-R1	tp-rcp-s3-perimeter	Access to S3 buckets by principals outside the organization.	AWS services acting for the organization; CloudFront origin access control, admitted by source ARN (the distributions in tp-prod)	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
POL-R2	tp-rcp-kms-perimeter	Use of KMS keys by principals outside the organization.	AWS services acting for the organization	No one
POL-R3	tp-rcp-sts-perimeter	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.	AWS services acting for the organization; the four vendor accounts whose roles carry external IDs (M-14), by account ID; the account that holds Vantalect's scan principal, for the read-only role only, until Tidepost deletes the role	Four vendor roles in tp-prod and the scan's read-only roles, both on the exemption list; any other outside account is denied

POL-R1: tp-rcp-s3-perimeter

The S3 perimeter has two statements. The first denies any principal outside the organization, and lets AWS services through. The second narrows the service exemption for CloudFront: origin access control is admitted only when the request's source ARN is a distribution in tp-prod, so another account's distribution cannot read a Tidepost bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOrganizationIdentities",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {"aws:PrincipalOrgID": "<org-id>"},
        "BoolIfExists": {"aws:PrincipalIsAWSService": "false"}
      }
    },
    {
      "Sid": "AdmitCloudFrontByDistributionArn",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {"aws:PrincipalServiceName": "cloudfront.amazonaws.com"},
        "ArnNotLike": {
          "aws:SourceArn": "arn:aws:cloudfront::<tp-prod-account-id>:distribution/*"
        }
      }
    }
  ]
}
```

POL-R2 and POL-R3

tp-rcp-kms-perimeter has the same shape as the first statement above, applied to kms:*. tp-rcp-sts-perimeter applies it to sts:AssumeRole and carries the exemption list: the four vendor accounts whose roles carry external IDs, by account ID, and the account that holds Vantalect's scan principal for the read-only role only, until Tidepost deletes the role. Web identity and SAML federation are not in the statement; the roles that federation reaches are governed by their own trust policies.

Declarative policies

A declarative policy sets an account attribute at the service, so it holds whatever a member account tries. Neither policy exempts anyone.

The EC2 declarative policies.

ID	Policy	Blocks	Exempts	Affects today
POL-D1	tp-decl-ec2-imds	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.	Nothing	New launches only; existing instances are the Hardening's H-2
POL-D2	tp-decl-ec2-no-public-sharing	Sharing an EBS snapshot or an AMI publicly (snapshot and image block public access, which a member account cannot turn off).	Nothing	No one

POL-D1: tp-decl-ec2-imds

The metadata default is the other half of the IMDS control. POL-S1 refuses a launch that asks for IMDSv1; this policy makes IMDSv2 the answer when a launch asks for nothing, and keeps a member account from changing the default back.

```
JSON
{
  "ec2_attributes": {
    "instance_metadata_defaults": {
      "http_tokens": {"@@assign": "required"}
    }
  }
}
```

Tag policy and backup policy

POL-T1: tp-tag-baseline

What it refuses: Tagging an EC2 instance, an EBS volume, or an RDS database with an environment, team, or backup value outside the allowed list (enforced for those three types). It does not require a tag: an untagged resource, or a wrong value on any other type, is reported in the compliance report, not refused.

The tag policy's keys. Activating them as cost allocation tags waits until they appear on resources, and belongs to the Well-Architected Remediation (COST01).

Tag key	Allowed values
environment	prod, staging, dev, sandbox
team	platform, ml, data, trust-and-safety, mobile, backend
service	Any value; the policy standardizes only the key's capitalization
backup	required, none

POL-B1: tp-backup-prod

Does not block. Backs up every resource tagged backup=required daily, keeps each recovery point 35 days, and copies each to the central vaults in tp-backup (us-east-1 and us-west-2); no resource carries the tag until the Well-Architected Remediation (RELO9).

The backup policy's destination and its vault lock. The lock can be removed until the cooling-off period ends; after that it cannot.

Setting	Value
Backup account	tp-backup
Central vaults	tp-central-vault (us-east-1), tp-central-vault-west (us-west-2)
Selection	Resources tagged backup=required; none are tagged until the Well-Architected Remediation
Vault lock	Compliance mode, minimum retention 7 days
Cooling-off	3 days: set February 10, 2026, immutable from February 13, 2026
AWS Backup administration delegated	February 10, 2026

Where each policy is attached

The attachment matrix. No policy is attached at the Root or at Workloads, so a new OU under them inherits nothing until it is placed deliberately.

OU	Policies in place at the end	SCPs (with the fixedFirst attached two)	Last attached
Policy Staging	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2, POL-T1, POL-B1	5 of 5January 23, 2026	February 5, 2026
Sandbox	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2, POL-T1	5 of 5February 3, 2026	February 10, 2026
Workloads/NonProd	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2, POL-T1	5 of 5February 3, 2026	February 10, 2026
Workloads/Prod	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2, POL-T1, POL-B1	5 of 5February 5, 2026	February 10, 2026
Security	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2	5 of 5February 5, 2026	February 5, 2026
Infrastructure	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2	5 of 5February 5, 2026	February 5, 2026
Exceptions	POL-S1, POL-S2, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2	4 of 5February 5, 2026	February 5, 2026
Suspended	POL-S4	3 of 5February 5, 2026	February 5, 2026

The matrix is the end state. The order they arrived in is the rollout, and it is the reason the set broke nothing: every policy was proven in Policy Staging first, then reached the lower-risk OUs, then Prod, after a watch.

The attachment history, in order. Each row is one change window, and one management-account call per policy per OU.

Date	Window	OU	Policies attached
January 23, 2026	W2	Policy Staging	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 3, 2026	W4	Sandbox	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 3, 2026	W4	Workloads/NonProd	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 5, 2026	W5	Workloads/Prod	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 5, 2026	W5	Security	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 5, 2026	W5	Infrastructure	POL-S1, POL-S2, POL-S3, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 5, 2026	W5	Exceptions	POL-S1, POL-S2, POL-R1, POL-R2, POL-R3, POL-D1, POL-D2
February 5, 2026	W5	Suspended	POL-S4
February 5, 2026	W5	Policy Staging	POL-T1, POL-B1
February 10, 2026	W6	Workloads/Prod	POL-T1, POL-B1
February 10, 2026	W6	Workloads/NonProd	POL-T1
February 10, 2026	W6	Sandbox	POL-T1

The watch rule between steps: CloudTrail queried for access denied by a policy, for at least 24 hours after each attachment before the next, more critical OU. After the NonProd and Sandbox attachment (window W4) and before Prod (window W5) there were 0 policy-caused denials; after Prod, through February 6, 2026, 0; after the backup and tag policies, through February 11, 2026, 0.

The staging cases

Policy Staging holds one account, `tp-policy-test`. The first cases ran on January 29, 2026, and the baseline's last full run was February 2, 2026. In all, Tidepost's set has 29 cases across 11 policies, each stated as an expected result so it can be rerun from the repository.

Every staging case by policy. A case names the call, and whether it must be denied, allowed, or reported.

ID	Policy	CasesExpected results
POL-S1	tp-scp-baseline	9deny: 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
POL-S2	tp-scp-no-member-root	2deny: an action signed by a member account's root user; allow: a central root session that turns on root password recovery in tp-policy-test
POL-S3	tp-scp-no-iam-users	5deny: iam:CreateUser from a developer permission set; deny: iam:CreateAccessKey for an existing user; allow: iam:CreateAccessKey through the break-glass role; allow: iam:CreateAccessKey for the vendor's user through the rotation role; deny: iam:CreateAccessKey for any other user through the rotation role
POL-S4	tp-scp-suspended-deny-all	1deny: any call from tp-policy-test while it is moved into Suspended
POL-R1	tp-rcp-s3-perimeter	3deny: s3:GetObject by a principal in another AWS account; allow: s3:GetObject by CloudFront with the distribution's source ARN; deny: s3:GetObject by CloudFront with another account's distribution
POL-R2	tp-rcp-kms-perimeter	1deny: kms:Decrypt by a principal in another AWS account
POL-R3	tp-rcp-sts-perimeter	2deny: sts:AssumeRole from an AWS account not on the list; allow: sts:AssumeRole from a listed vendor account with its external ID
POL-D1	tp-decl-ec2-imds	1a launch with no metadata options gets HttpTokens required
POL-D2	tp-decl-ec2-no-public-sharing	2deny: making a snapshot public; deny: making an AML public
POL-T1	tp-tag-baseline	2deny: tagging an instance environment=production; report: an S3 bucket tagged environment=production is noncompliant
POL-B1	tp-backup-prod	1a test volume tagged backup=required is backed up and copied

Two staging results are worth recording. The detection statement’s correction on January 30, 2026 is described under [POL-S1: tp-scp-baseline](#). And the same day, Kofi Brandvold ran the root recovery 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. The backup policy’s tag cases ran on February 6, 2026 and February 9, 2026.

The Control Tower controls

The landing zone’s own controls, on every registered OU are on, with no choice involved. On top of them, 8 elective detective controls are enabled on the OUs that hold accounts.

The elective controls, enabled on each OU below. 40 enablements in all.

Elective control

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

When the elective controls reached each OU.

OU	Controls enabled on
Sandbox	February 3, 2026
Workloads/NonProd	February 3, 2026
Workloads/Prod	February 5, 2026
Security	February 5, 2026
Infrastructure	February 5, 2026

What is not here

The management account is ungoverned by every policy above, VPC Block Public Access is not attached (it would block the public load balancers without exclusions, so it waits for the change-a-policy runbook), and nothing in this set requires a tag: untagged resources are reported, not refused. Each of those is a decision the owners can revisit through a pull request.

© 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.