Vantalect

AWS MULTI-ACCOUNT · ORGANIZATIONS · CONTROL TOWER

AWS Multi-Account Foundation

Every AWS account in its place, designed in two weeks. Built in six.

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

November 6, 2026

The problem

Production, staging, and the intern's experiment share one account, and your auditor just asked how you separate them. Or the accounts multiplied by hand and every policy is an exception.

This engagement puts your AWS accounts in the structure AWS recommends: a landing zone, every account in its place, guardrails every new account inherits, and one way to make the next one. We design it in two weeks and build it in six.

The Blueprint

Two weeks

$25,000

Up to 40 consultant hours

Your AWS accounts, read from the inside, and the organization they should become. We inventory every account, run the foundation scan, and design the OU tree, the guardrails, and the move plan, for a new organization, an existing one, or a move into a new one.

GUARANTEED

The Build

Six weeks

$35,000

Up to 110 consultant hours

The Blueprint in the first two weeks. Then weeks three through five stand up the landing zone, move every account into its place in approved change windows, and put the guardrails in. Week six runs the same scan again and hands it over.

The second half of the fee is invoiced only when every agreed check of the foundation scan passes at week six and every in-scope account is in its target OU.

Who it is for

- A CTO, VP of Engineering, head of platform, or CISO whose production runs on AWS
- Production in one account, a handful of accounts made by hand, or an organization that grew without guardrails
- A SOC 2 or ISO 27001 audit, a financing, an acquisition, or a payer change on the calendar
- Budget authority for a fixed-price engagement without a procurement cycle

It is not the right engagement if you want workloads moved between accounts (accounts move with their resources intact), or if you cannot grant a read-only role in your own accounts. The structure it builds is described in public at vantalect.com/multi-account/best-practices. To audit your accounts for security findings first, see the AWS Security, Compliance & Governance Audit at vantalect.com/security-audit.

Week by week

All three paths end in an organization built right and pass the same scan: greenfield (a new organization, with AWS Control Tower and new accounts), retrofit (an existing organization), or migration (accounts, with their resources intact, moved from old organizations into a new one). The Blueprint chooses, in writing, at the week-two readout.

The Blueprint, two weeks.

Week	What happens
1. Inventory and scan	The read-only role goes into every account and the management account on day one. Every account, policy, trail, identity assignment, commitment, and organization-scoped dependency is inventoried, and the foundation scan runs.
2. Design and plan	The target OU tree and account map, the guardrail, identity, logging, network, backup, vending, and tagging designs, the path, the move plan by wave and change window, and the risk register. A design review, then the sponsor readout.

The Build, six weeks.

Week	What happens
1 and 2. Inventory, scan, design, plan	The Blueprint's two weeks, with no changes yet. The week-one scan is the baseline, and at the readout your sponsor approves the account map, the checks, the path, and the first change window.
3. Landing zone and core accounts	AWS Control Tower set up or upgraded; the Security OU with the Log Archive and Audit accounts; the organization trail; the security services delegated to Audit; IAM Identity Center connected to your identity provider.
4. Accounts moved	People move to single sign-on first. Then accounts move in waves, a pilot of sandbox and non-production accounts first, each behind its pre-flight checks, each landing in its target OU, enrolled.
5. Guardrails, vending, and shared services	Policies proven in a Policy Staging OU, then attached OU by OU. Account vending proven by vending one real account. Central backup, the network account, and the tag policy where in scope.
6. Re-scan and hand over	The same scan as week one, run the same way, the runbooks, and the handover. Our operator role is deleted, and the re-scan proves it.

The add-on: The Build after a Security Audit

When our AWS Security, Compliance & Governance Audit has already read your organization, its inventory and governance review replace the Blueprint's discovery. Taken with or after the Audit or the Hardening, the Build runs in four weeks for $25,000, up to 70 hours (about 30 live), under its own statement of work. The same thirteen-check scan decides the second half of the fee, and the fee is refunded in full if the security engagement ends before its readout, other than for your breach, or the add-on has not begun within sixty days. It is priced net: it takes no bundle discount and does not count toward one.

What you receive

The Blueprint

1. **The inventory.** Every account with its OU, owner, root email and MFA custody, support plan, commitments, credits, Marketplace agreements, IAM users and keys, delegated administrators, and what would break in a move.
2. **The foundation scan.** All thirteen checks, run read-only against your organization as it is, with the raw results.
3. **The target design.** The OU tree, the account map, the core accounts, and the guardrail, identity, logging, network, backup, vending, and tagging designs, each tied to AWS's guidance.
4. **The policy set.** The baseline service control, resource control, declarative, and tag policies and the Control Tower controls, as code, with what each blocks.
5. **The move plan.** The path, the waves, the change windows, and each window's actions, pre-flight checks, and rollback.
6. **The risk register.** Billing, commitments, Marketplace, support, quotas, dependencies, root custody, and the policy blast radius, each sized for you.
7. **The sponsor readout.** A short written document, presented in the closing meeting.

The Build

Everything in the Blueprint, then eight more:

8. **The landing zone,** set up or upgraded and enrolled, with the Security OU, Log Archive, Audit, and one organization trail.
9. **Every in-scope account in its place,** in its target OU and enrolled, wave by wave.
10. **Guardrails at every OU,** proven in Policy Staging first and inherited by every account below.
11. **Identity on single sign-on,** with long-lived IAM users retired from workload accounts.
12. **Detection delegated** to the Audit account, with every new account enrolled automatically.

13. **One way to make the next account,** proven by vending one real account.
14. **The week-six re-scan** against week one: same checks, same method. It decides the second invoice.
15. **The operations runbooks and the handover workshop,** and its recording.

How the result is measured

The foundation scan is thirteen read-only checks, run by a script you can read: the landing zone, account placement, the organization trail, delegated security, identity, root, guardrails, controls, vending, backup and network where in scope, tagging, and that no access of ours lingers. The checks in scope and the account map are agreed at the week-two readout.

> **The guarantee**
>
> The second half of the Build fee is invoiced only when every check of the foundation scan agreed at the week-two readout passes at week six, verified by the same scan run the same way, and every in-scope account is in its target OU. If the gate is not met, the second invoice is not issued and you keep everything delivered.
>
> A check you waive in writing counts as passed, as does one whose change you declined, or approved but had not applied by the re-scan.

Beyond that gate, no particular result is guaranteed. The engagement builds the structure auditors expect to see; it is not an audit opinion, an attestation, or a certification of compliance.

Terms at a glance

Fees, hours, and scope. Invoices are due within fifteen days.

Term	The Blueprint	The Build
Fee	$25,000, fixed	$35,000, fixed
Length	Two weeks	Six weeks
Consultant hours included	Up to 40	Up to 110
Time live with your team (estimate)	About 8 hours	About 38 hours, every change window included
Invoicing	As the statement of work sets out	Half at signature, half only if the guarantee is met

Term	The Blueprint	The Build
Beyond the cap	$450 per hour, by written change order agreed before the hour is spent, invoiced monthly	Same
Scope	One target AWS organization by greenfield build, retrofit, or migration, with 50 accounts included, then $50, $30, or $20 more per account by band	Same, plus policies and account customizations in up to two infrastructure-as-code repositories
Bundle	10% off each with one other AWS engagement, 15% off each with two or more	The same

A second target organization, re-platforming workloads between accounts, an on-site day, and support after the closing readout are outside scope, available only by written change order. Either party may end an engagement with five business days' written notice; you then pay for hours spent to date at $450 per hour, capped at the fee, and keep everything delivered. In the Build, ending it after week two costs at least the Blueprint's fee, and if we end it before its measurement gate is decided, you pay no more than the first half.

> **Access, and what stays with you**
>
> Read-only roles everywhere, from a CloudFormation StackSet we hand you. In the Build, write access exists only in the management account, only in change windows you approve in writing, through a role you create whose trust policy admits only Charles, requires MFA, and expires with the window. Closing accounts, billing changes, and creating IAM users are denied outright. Member accounts change only as code, through your pipeline. Root credentials, account emails, and payment methods stay with you, and you own outright everything delivered.

What we need from you

- The read-only role in every in-scope account and the management account within three business days of signature. The schedule starts on the agreed date, or when the role exists, whichever is later, and slides by the same number of business days if an obligation is not met.
- A platform lead at least four hours a week, and a finance or billing contact in week one for commitments, credits, Marketplace agreements, and the support plan.
- Your sponsor available for thirty minutes a week and for the readouts.
- In the Build, each change window approved in writing at least two business days ahead, the management account's owner in every window, and, on the greenfield and migration paths, the new management account created by you before week three.
- Your permission to record the sessions.

What comes with every engagement

- **Charles, personally.** Charles Sieg delivers every engagement inside your accounts, with your engineers and no hand-off to a junior team. He holds AWS Certified Solutions Architect and DevOps Engineer at the professional level and Security at the specialty level.
- **Pavilion, your private workspace.** Set up in week one: the calendar, every recording with its transcript and summary, the account map and move plan, each window's approval, the decisions, and the action items.
- **Every session recorded,** with your permission, with transcripts and recaps.
- **A start within two weeks** of signature, once the access it needs exists.

Questions clients ask

Greenfield, retrofit, or migration: how do we know?

The Blueprint decides, in writing. No organization yet means greenfield. Keep yours (a retrofit) when its management account runs no workloads and its payer is staying; migrate into a new one when the management account runs production, the organization belongs to someone else, or two or more must become one.

Will moving accounts break production?

An account moves with its resources intact. Policies that name the organization, resource shares, and StackSets can break, so a pre-flight scan finds each one before its wave, the fix goes in first, and every wave has a rollback.

What happens to our Savings Plans and credits?

They stay with the account that bought them. In a migration the plan keeps them applying, usually by bringing each old management account in as a member; we never buy, sell, or exchange a commitment.

Do you ever hold root credentials?

No, for any account. Root emails move to aliases on your domain, and the management account's root user gets hardware keys held by two of your officers.

Start with an email

Write to **charles.sieg@vantalect.com** and tell us how many accounts you have, whether you have an organization today, and what prompted the question. Charles replies within one business day, and the first call is fifteen minutes.

The full description is at **vantalect.com/multi-account**, and the standard terms are at **vantalect.com/terms**.

© 2026 Vantalect, LLC. Prices and terms as of November 6, 2026; the terms at vantalect.com/terms govern.

AWS, Amazon Web Services, AWS Control Tower, AWS Organizations, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. SOC 2 is a registered trademark of the American Institute of Certified Public Accountants. ISO is a registered trademark of the International Organization for Standardization. Terraform is a registered trademark of HashiCorp, Inc. Zoom is a trademark of Zoom Video Communications, Inc. Vantalect is not affiliated with or endorsed by any of them.