AWS Secure Environment Accelerator Deployment Capabilities

- Deploys, creates, manages and updates the following objects across a multi-region, multi-account AWS environment

TASK	Accelerator - What hap
AWS Accounts	
- Creates mandatory accounts (accounts which other accounts are dependent on)	organization manageme
- Creates workload accounts (individually or in bulk), base personality determined by ou placement	organization manageme
- Supports native AWS Organization account and OU activities (OU and account rename, move account between OU's, create accounts, etc.)	organization manageme
- Applies a Deny All SCP on any newly created account(s) until successfully guardrailed	organization manageme
- Allows bulk parallel account creation, configuration, updates and guardrail application	creates, guardrails and
- Performs 'account warming' to establish initial limits, when required	state Machine region on
- Checks limit increases, when required (complies with initial limits until increased)	per account, per region
- Automatically submits limit increases, when required	state Machine region on
Networking	
- Creates Transit Gateways and TGW route tables incl. static routes	in the defined region(s),
- Creates centralized and/or local account (bespoke) VPC's	in the defined region(s),
- Creates Subnets, Route tables, NACLs, Security groups, NATGWs, IGWs, VGWs, CGWs (per customer specs)	part of any VPC, in the
- Deletes default VPC's (worldwide)	in all regions, in all acc
- Creates VPC Endpoints (Gateway and Interface)	part of any VPC, in the
- Configures centralized endpoints (R53 zones populated, shared and attached to local and cross-account VPC's)	configures regional centr
- Creates Route 53 Private and Public Zones	in the defined account(s
- Creates Resolver Rules and Resolver (inbound/outbound) Endpoints	part of a specific VPC(s
...including MAD R53 DNS resolver rule creation	created in same region a
- Automatically creates R53 VPC Endpoint Overloaded Zones	same region(s), same ac
Cross-Account Object Sharing	
- VPC and Subnet sharing, including account level retagging/naming (and per account security group 'replication')	VPC's are shared to acc
- VPC peering and TGW attachments (local and cross-account)	in the defined region, no

TASK	Accelerator - What hap
- Managed Active Directory sharing	state machine region on
- Automated TGW inter-region peering	cross-region, cross-accou
- Shares SSM remediation documents	from defined account(s)
Zone sharing and VPC associations	
- Public Hosted Zones	no sharing, no associati
- Private Hosted Zones - i.e. Cloud DNS domains	associated worldwide to
- Endpoint Private Hosted Zones	associate within region,
- On-premise resolver rules	associate within region,
- MAD resolver rule association	same region as the MAI
Identity	
- Creates Directory services (Managed Active Directory and Active Directory Connectors)	in a specific VPC, in th
- Creates Windows admin bastion host auto-scaling group	once per above MAD (c
- Set Windows domain password policies (initial installation only)	once per above MAD (c
- Set IAM account password policies	once per account, globa
- Creates Windows domain users and groups (initial installation only)	once per above MAD (c
- Creates IAM Policies, Roles, Users, and Groups	once per account, globa
Cloud Security Services	
- Enables and configs the following AWS services, worldwide w/central specified admin account:	(each service can have s
- Guardduty w/S3 protection	enabled all regions, all a
- Security Hub (Enables specified security standards, and disables specified individual controls)	enabled all regions, all a
- Firewall Manager	enabled once per accou
- CloudTrail w/Insights and S3 data plane logging	enabled all regions (usi
- Config Recorders/Aggregator	enabled all regions, all r
- Macie	enabled all regions, adm
- IAM Access Analyzer	enabled once per accou
- Enables CloudWatch access from central specified admin account	enabled once per accou
- Deploys customer provided SSM remediation documents (four provided out-of-box today)	customized per OU, def
...remediates S3 buckets without KMS CMK encryption and ALB's without centralized logging	customized per OU, all
- Deploys AWS Config rules (managed and custom) including AWS Conformance packs (NIST 800-53 deployed by default + 2 custom)	customized per OU, all
Other Security Capabilities	
- Creates, deploys and applies Service Control Policies	at the top OU level only
- Creates Customer Managed KMS Keys w/automatic key rotation (SSM, EBS, S3)	SSM and EBS keys are
- Enables account level default EBS KMS CMK encryption	set if a VPC exists in th
- Enables S3 Block Public Access	once per account, globa
- Configures Systems Manager Session Manager w/KMS CMK encryption and centralized logging	set if a VPC exists in th
- Imports or requests certificates into AWS Certificate Manager	State Machine region or
- Deploys both perimeter and account level ALB's w/Lambda health checks, certs & TLS policies	State Machine region or
- Deploys & configures 3rd party firewall clusters and management instances	in the defined region(s),
- Configuration is fully managed and maintained in AWS CodeCommit - full multi-account configuration history	organization manageme
...breaking configuration changes block Accelerator execution	Indempotent - extensive

TASK	Accelerator - What hap
Centralized Logging	
- Deploys an rsyslog auto-scaling cluster behind an NLB, all syslogs forwarded to CWL	State Machine region or
- Centralizes logging to a single centralized S3 KMS CMK encrypted bucket (enables, configures and centralizes) incl:	Sets S3 ownership flag,
- VPC Flow logs (w/Enhanced metadata fields and optional CWL destination)	part of a specific VPC,
- Organizational Cost and Usage Reports	once per organization, g
- CloudTrail Logs including S3 Data Plane Logs (also sent to CWL)	directly back to log-arch
- All CloudWatch Logs (includes rsyslog logs) (and setting Log group retentions)	State machine region, p
- Config History and Snapshots	directly back to log-arch
- Route 53 Public Zone Logs, DNS Resolver Query Logs	to CloudWatch Logs in
- GuardDuty Findings	directly back to log-arch
- Macie Discovery results	directly back to security
- ALB Logs	State Machine region or
- SSM Session Logs	All regions currently ser
Extensibility	
- Populates each accounts Parameter Store with the Accelerator deployed objects (allows customer IaC to extend/leverage)	each account, defined re
- Every execution outputs the execution status and a list of successfully guardrailed accounts to a SNS topic	allows 3rd party framew
...which emails a customer defined email address	...or hooking to the ema
- Deploys roles with customized access (read-only,write) to the log-archive buckets (enabling customer SIEM deployments, SSM, EC2 CWL)	defined account, global
- Designed for Day 1, 2 and day 10. Customers get new features without any customization effort no matter the deployed architecture	Upgradable from any ve
Alerting	
- Deploys global High, Medium, Low, Ignore priority SNS topics and email subscriptions	in the defined account,
- Deploys customer defined CloudWatch Log Metrics and Alarms w/priorities (19 out-of-box)	in the organization man
- Creates and configures AWS budgets w/alerting (customizable per OU and per account)	once per account, globa

---

General

- ”defined” region, ”defined” account, means ”customer defined”, either at installation, upgrade, or any time they decide to reconfigure
- all items are created per customer defined parameters and configurations and are fully customizable without changing a single line of code
- security services are enabled and deployed globally, but, each service can be disabled per region. A single region deployment is possible.
- customer can enable/disable features, or change the configuration of each feature in the Accelerator config file
- customers can evolve their configurations over time, as they evolve and as their requirements change, without the requirement for code changes or professional services

Region support

- All AWS commercial regions are supported. Lack of availability of CodeBuild, CodeCommit, or AWS Organizations in the Accelerator primary or installation region will prevent installation directly in that region. In these cases, customers can select a different installation region and the Accelerator can remotely deploy configurations and guardrails to that unsupported installation region.
- Prior to v1.2.5, we utilized a single StackSet, which blocked several additional installation regions. The Accelerator no longer leverages any StackSets, unblocking installing directly in several additional regions.
- As most features can be toggled on/off (per region), we expect most regions should be supportable both as a primary (or installation) region with the three above noted exceptions, and in these cases should still be fully supported as a managed (or secondary) region.

...Return to Accelerator Table of Contents