

LincTV MDM Server: Security & Architecture

Executive Summary

Lincata employs a modern, cloud-native multi-tenant architecture built on Amazon Web Services (AWS). Our infrastructure is designed with a "Security First" mindset, utilizing Defense in Depth principles to ensure strict tenant isolation, data privacy, and high availability. By leveraging Infrastructure as Code (IaC), we ensure that every deployment is consistent, auditable, and secure by design.

Dedicated Resources with Strict Tenant Isolation

Tenants receive a unique subdomain on *.linctv.co and run on a dedicated stack of compute resources within a Lincata managed Virtual Private Cloud (VPC).

Within our VPC, we enforce strict logical isolation of dedicated tenant resources:

- **Dedicated Network Segments:** Each tenant is provisioned with a unique, non-overlapping set of subnets.
- **Network ACLs (NACLs):** We utilize Network Access Control Lists as a stateless firewall at the subnet boundary. These are rigorously configured to explicitly allow traffic only within a specific tenant's resources, effectively blocking any cross-tenant communication at the network packet level.
- **Security Groups:** Stateful firewalls surround every compute and database resource, enforcing a "least privilege" network access model (e.g., the Database accepts connections only from the App Server, never from the public internet).

Network Security & Perimeter Defense

Our network topology is designed to minimize the attack surface by keeping critical infrastructure hidden from the public internet:

- **Private-by-Default:** Application logic (ECS Fargate), Databases (Aurora PostgreSQL), and Caches (Redis) run exclusively in Private Subnets. They have no public IP addresses and cannot be reached directly from the outside world.
- **Secure Edge Delivery:** All incoming traffic is routed through AWS CloudFront, a global Content Delivery Network (CDN). This acts as our first line of defense, providing DDoS protection and enforcing HTTPS/TLS encryption before traffic ever reaches our servers.
- **Web Application Firewall (WAF):** We deploy AWS WAF at the edge to enforce IP whitelisting and filter malicious traffic patterns before they enter our network.
- **VPC Endpoints:** Communication between our application and AWS services (such as S3, SES, and Secrets Manager) occurs via private VPC Interface Endpoints. This ensures that internal traffic remains within the AWS private network backbone and never traverses the public internet.

Data Protection

We adhere to strict encryption standards to protect data throughout its lifecycle:

- **Encryption at Rest:** All persistent storage layers—including Aurora Databases, ElastiCache Redis clusters, and S3 Buckets—are encrypted using industry-standard AES-256 encryption.
- **Encryption in Transit:** All data moving between clients, load balancers, applications, and databases is encrypted via TLS 1.2+.
- **Secrets Management:** Sensitive information such as database credentials and API keys are never stored in source code. We utilize AWS Secrets Manager to securely inject ephemeral credentials into application containers only at runtime.

Secure Content Delivery

- **Signed URLs:** Access to private media and sensitive documents is controlled via CloudFront Signed URLs. This ensures that only authenticated users with valid session tokens can access specific files, preventing unauthorized sharing of direct links.
- **Origin Access Control (OAC):** Our storage buckets are completely private. CloudFront is granted access via OAC, ensuring that users cannot bypass the CDN's security controls to access raw files directly from S3.

Operational Reliability

- **Serverless Compute:** We utilize AWS Fargate for our application workload. This removes the security risks associated with managing and patching underlying server operating systems.
- **Immutable Infrastructure:** All infrastructure changes are managed via Terraform. This prevents "configuration drift" and ensures that security policies are applied consistently across all environments, from testing to production.

Infrastructure Architecture Diagram

