instaclustr

SECURITY FEATURES OVERVIEW

Security has been at the forefront of Instaclustr's system and operations since day one. We understand that you are trusting us with your valuable data and take that trust very seriously. As part of our security focus, we are nearing completion of our first audit against the Trust Service Principles of the Service Organisation Controls (SOC 2).

Preparation for this audit has caused us to undertake a ground-up evaluation of our security controls and undertake improvements in several areas where we thought there was opportunity to strengthen our security posture through additional defence in depth. With the culmination of this project focus, it is a timely point to stocktake the key security protections that are in place when you run your cluster with Instaclustr.

This article provides an overview of our key technical security features but of course these features are supported by a full range of security processes such as staff background checks, configuration management, regular risk assessments and procedural compliance testing.

Cassandra and Spark Cluster Security

- Each client cluster is created in a separate network environment (eg VPC in AWS) with no shared instances
- Encrypted EBS (using client controlled keys) supported for AWS & disk encryption on by default for GCP
- Internode encryption (with cluster-specific certs) enabled by default
- Check box option when provisioning to enable client authentication and client to cluster encryption (client requirement for SOC2 compliance)
- Client controlled firewall whitelist
- Use private IPs to connect to Cassandra and Spark in your cluster (using VPC peering in AWS and similar approaches in other providers)
- Spark Jobserver is available to provide encrypted and authenticated access to Spark services
- Out of the box default 'cassandra' user is disabled on all clusters with non-default super user created on cluster provisioning

- Communication from client nodes to our central infrastructure is via a single channel with the connection initiated by the nodes
- Whitelist monitoring of open ports and running processes (basic intrusion detection)
- Rapidly rotated and per-cluster password for Instaclustr admin access to Cassandra.

Security in our Management Console

- Two factor authentication
- Multiple users per account with different access levels
- Two factor cluster deletion confirmation (requires separate confirmation via Instaclustr support before cluster is deleted)
- Central management infrastructure has no access to data in customer clusters
- Per-user access keys are separately available for our provisioning and monitoring APIs with the provisioning API disabled by default
- Sensitive data is encrypted before being stored in our management database
- No credit card details are stored in our management infrastructure - they are passed directly to our credit card services provider.

Security in our Operations Environment

- All admin access to customer clusters is via two-stage bastion server using short-lived SSH certs for customer node access
- All admin access to customer nodes logged including any commands issued via CQLSH and traceable to incident or request ticket
- Admin access to our management environment is broadcast to a open internal Slack channel where it is monitored and linked to approved release or incident tickets
- An Intrusion Detection System monitors all servers
- A management tool, icadmin, is used as the preferred method of undertaking operations on customer cluster rather than manual configuration changes
- Two factor authentication is required for access to all admin systems.