instaclustr

SECURITY FEATURES OVERVIEW

Security management, integrated engineering, and independent certification

Security has been at the forefront of Instaclustr's systems and operations since day one. We understand that you trust us with your valuable data and we take that responsibility very seriously. As part of our security focus, several of our offerings are PCI certified and we have been SOC 2 compliant for several years. Both of these certifications require individual, regular external compliance audits.

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

Cluster Security: Cassandra, Spark, Kafka

- Each client cluster is created in a separate network environment (e.g. VPC in AWS) with no shared instances—(run in your own account customers may choose to create multiple clusters in a single VPC)
- Encrypted EBS (using client controlled keys) supported for AWS, and disk encryption on by default for GCP and Azure
- Option to provision Private Network cluster on AWS where nodes have no public IPs, and admin access is via a bastion box automatically provisioned within the VPC (required for PCI)
- 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 SOC 2 compliance)
- Client controlled firewall whitelist
- Use of private IPs to connect to your cluster (using VPC peering in AWS, and similar approaches for other providers)
- Cluster hosted REST/HTTP interfaces all support HTTPS, and most services support automatic provisioning of externally signed certificates for cluster-specific DNS names

- Out of the box default 'Cassandra' user is disabled on all Cassandra clusters, with non-default super user created on cluster provisioning
- All communication from client nodes to our central infrastructure is initiated by the nodes (no inbound firewall rules other than SSH from operations environment)
- Whitelist monitoring of open ports and running processes (basic intrusion detection)
- Rapidly rotated and per-cluster password for Instaclustr admin access to Cassandra
- Operating system hardened to CIS standards
- Access logged and shipped to controlled central log management infrastructure
- Restricted outbound firewall rules for PCI compliant clusters.

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

- Bastion servers, which provide access to our management servers and customer clusters, are accessed via VPN and VNC with copy out disabled to prevent egress of data from the management 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 are traceable to incident or request ticket
- Admin access to our management environment is broadcast to an 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
- Central management systems are hardened to applicable CIS standards
- Outbound network access is restricted to defined, necessary services.

About Instaclustr

Instaclustr delivers reliability at scale through our integrated data platform of open source technologies such as Apache Cassandra®, Apache Kafka®, Apache Spark™, Elasticsearch and Redis.

Our expertise stems from delivering more than 70 million node hours under management, allowing us to run the world's most powerful data technologies effortlessly.

We provide a range of managed, consulting, and support services to help our customers develop and deploy solutions around open source technologies. Our integrated data platform, built on open source technologies, powers mission critical, highly available applications for our customers and help them achieve scalability, reliability, and performance for their applications.