CONFLUENT

Confluent Cloud Security Controls

Peter Gustafsson, v1.0

Table of Contents

Introduction

Confluent takes the security of our services very seriously. This is clear from the many investments we have made and continue to make toward improving authentication, authorization, auditing, and the data confidentiality features of those services. While technical security measures are important, equally important are the processes and people involved in keeping both the platform secure and your data as safe as possible.

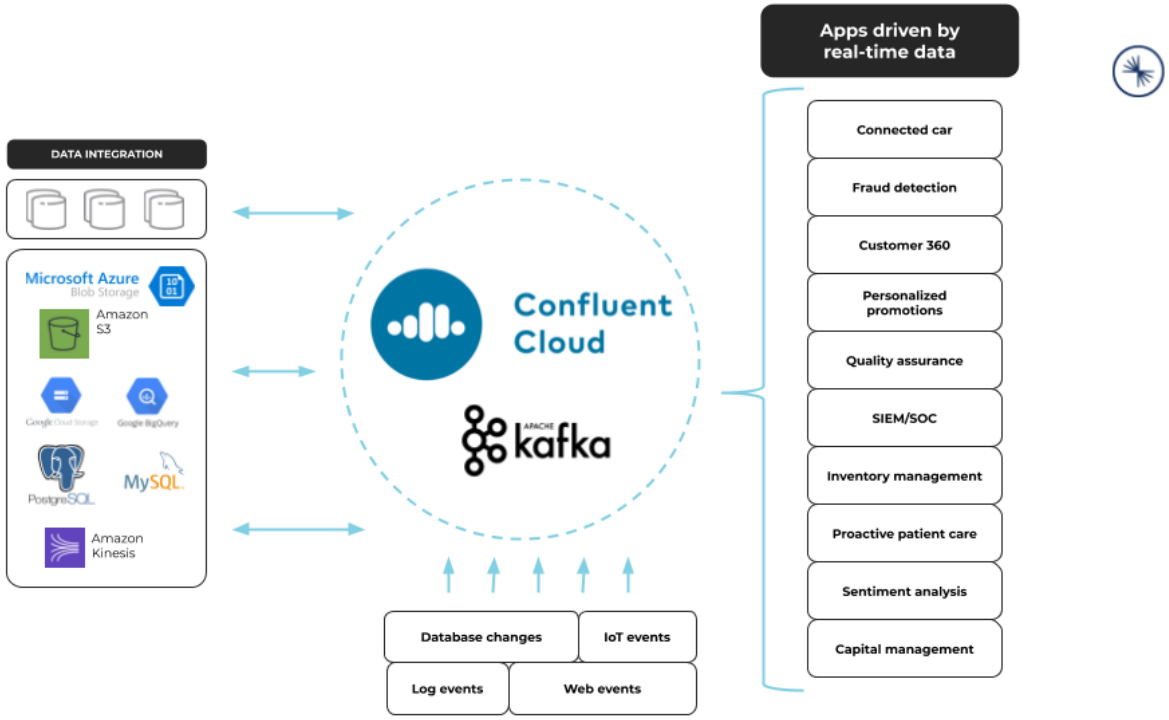
Confluent's security philosophy centers around layered security controls designed to protect and secure Confluent Cloud customer data. We believe in multiple logical and physical security control layers including access management, least privilege access, strong authentication, logging and monitoring, vulnerability management, and bug bounty programs.

Part of our information security strategy is proactive monitoring and management to identify critical security issues. When issues are identified, each issue is evaluated and quickly addressed. We rely on industry standard information security best practices and compliance frameworks to support our security initiatives. Our goal is to make users feel confident using our service for their most sensitive workloads.

We truly believe that transparency around our controls environment and the standards and processes we adhere to is of utmost importance. This document aims to provide clarity and a deeper understanding of all the available security controls in Confluent Cloud.

What is Confluent Cloud?

Built and operated by the original creators of Apache Kafka®, Confluent Cloud is the industry's only fully managed, cloud-native event streaming service powered by Kafka. Confluent Cloud enables enterprises to transform Kafka into a central nervous system for all event data with an elastically scalable, highly reliable, and secure event streaming service to quickly build real-time, event-driven applications.



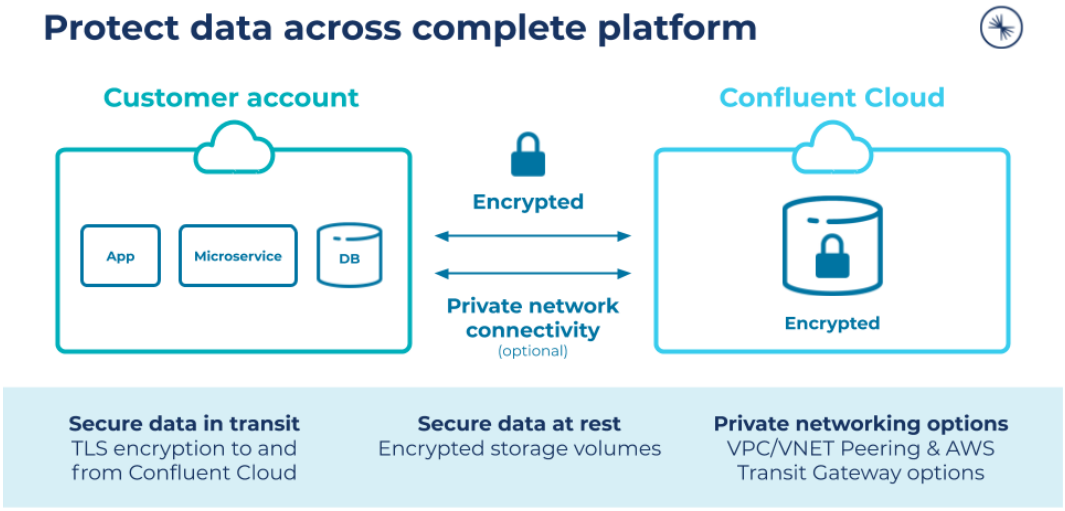
With no infrastructure to provision, monitor, or manage, Confluent Cloud infinitely retains and democratizes access to all your event data in one place without complex data engineering pipelines. Simply point client apps or popular data services to Confluent Cloud and it takes care of the rest. Load is automatically distributed across brokers, consumer groups automatically rebalance when a consumer is added or removed, the state stores used by applications using the Kafka Streams APIs are automatically backed up to Confluent Cloud, and failures are automatically mitigated.

With Confluent Cloud you can:

- Start streaming with Kafka in minutes with on-demand provisioning, elastic scaling, and scale-to-zero pricing for a serverless Kafka experience
- Stream with confidence with enterprise-grade reliability, guaranteed uptime SLAs, multi-availability zone (AZ) replication for resilience, on-demand Kafka bug fixes, and upgrades without downtime
- Speed up app development with a rich pre-built ecosystem of fully managed components such as Schema Registry, Kafka Connect, and ksqlDB
- Reduce the TCO of Apache Kafka up to 60% by moving to a fully-managed service
- Build a hybrid Kafka service leveraging Confluent Platform on your on-premises environment with a persistent bridge to Confluent Cloud with Confluent Replicator

Internal Confluent Cloud Infrastructure Security

Data security is essential when it is transported in and out of the service as well as when the data is persisted to disk. Confluent provides industry standard and audited protection mechanisms to ensure customers can confidently store data in Confluent Cloud. To further protect data, network-level isolation is available through VPC/VNet isolation and private networking options.



Datacenters

Confluent Cloud runs on top of the three largest public cloud providers: Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.

Customer data is stored in Confluent Cloud clusters; customers can choose if these are to be single-tenant or multi-tenant clusters, and both cluster types are run on virtual machines managed on a Kubernetes environment.

Cloud provider datacenters are compliant with a large number of physical and information security standards. For additional information, please refer to the compliance page of your selected cloud provider:

- AWS compliance

- Azure compliance
- GCP Compliance

Note: Confluent Cloud cluster types Basic and Standard are always multi-tenant systems. For more information on cluster types, please refer to Confluent Cloud™: Managed Apache Kafka® Service for the Enterprise.

Network Isolation

Terminology

Network ports: Confluent Cloud uses the following network ports with the components listed below.

- tcp/9029 for brokers
- tcp/443 for admin GUI/CLI/API
- Network ports can not be changed.
- TLS v1.2 is mandated and can not be disabled, TLS 1.0 and V1.1 are not allowed.

Confluent Cloud Organization/CloudOrg/OrgID: A unique identifier (UUID) for a Confluent Cloud organization that can contain other Confluent Cloud resources such as ***environments***, billing information, users, or ***clusters***.

Environment: An environment-specific namespace for one or more Kafka clusters and one or zero Schema Registries. If enabled, Schema Registry runs in a customer-specific namespace on a multi-tenant Schema Registry cluster. The Schema Registry provides a serving layer for your metadata enabling Kafka clients to store and retrieve schemas.

Cluster: A Confluent Cloud cluster is deployed inside an environment and provides Kafka API endpoints for developing streaming applications.

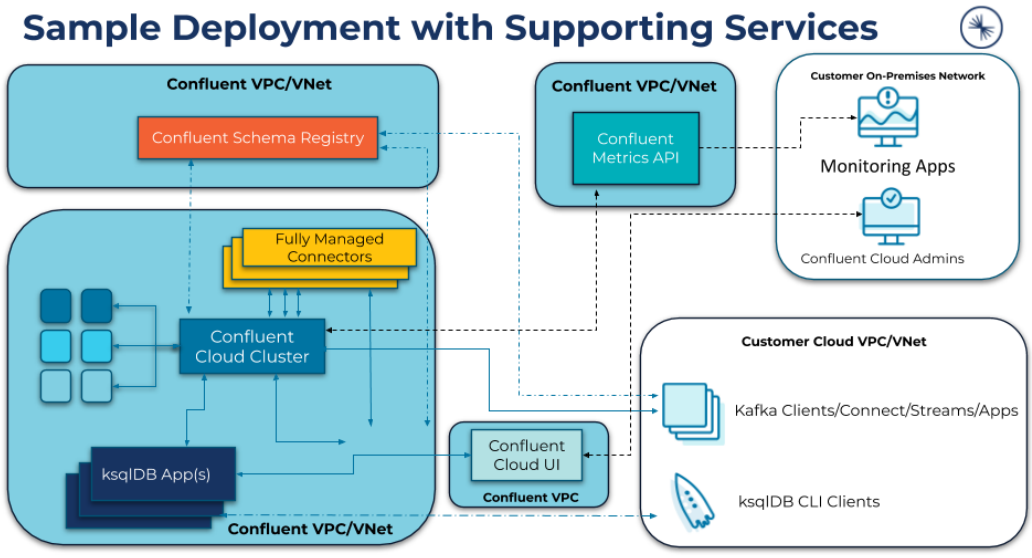
Confluent Cloud Cluster Types

	Basic Get started with no minimums	Standard Production-ready for most applications	Dedicated Customizable for any application
Sizing	No sizing required Stream up to 100MBps Store up to 5TB	No sizing required Stream up to 100MBps Store up to 5TB	Limits based on provisioned capacity
Replication options	Single AZ	Single & Multi AZ	Single & Multi AZ
Uptime SLAs	99.5%	99.95%	99.95%
Private networking options	-	-	VPC/VNet Peering AWS Transit Gateway
Ideal for	Prototyping, early development, and some production use cases	Most production use cases	MIssion-critical applications at any scale

Mix and match any cluster type across your organization

Confluent Cloud Basic/Standard/Dedicated: These are the available **cluster types**. Basic and Standard clusters are multi-tenant clusters. Dedicated runs on per-customer dedicated compute resources and supports the most features and custom options.

Confluent Cloud Architecture



The Confluent Cloud architecture is uniform across all cloud providers. All resources are run inside managed Confluent VPCs/VNets and the service can be exposed through various connectivity options. These options are:

- Secured internet endpoints (AWS, GCP, and Azure)
- VPC/VNet Peering (AWS, GCP, and Azure)
- Private link (AWS and available soon on Azure)
- Transit Gateway (AWS only)

Amazon Web Services Topology

Secured Public Endpoints

Using secured public endpoints in AWS is straightforward as they are announced and accessible over the public internet as well as from inside an AWS VPC. It should be noted that public endpoint access from applications deployed inside an AWS VPC will never traverse the public internet, just the AWS public backbone.

VPC Peering

Confluent Cloud in AWS also supports peering with your own VPC estate in AWS. This means the traffic never traverses the public backbone of the cloud provider or the public internet.

Before deploying a cluster using VPC peering, you need to choose a private Classless Inter-domain Routing (CIDR) range to use for the cluster. This CIDR range can not overlap with existing ranges in the same routing domain.

Customers worried about peering extending the network trust boundary to the peered VPC can configure mitigating controls. This includes setting up security groups to not allow any inbound access to instances in their VPC.

AWS Transit Gateway

AWS Transit Gateway (TGW) allows you to connect multiple VPCs (even containing Private Link connections) and remote networks using a single gateway. Remote networks can be other clouds via IPSec connections or more commonly on premise networks connecting to the TGW using AWS Direct Connect or VPN. The TGW provides transitive connectivity across all connected VPCs and remote networks. TGW allows you to control routing and thus provides a single point of connectivity control.

AWS PrivateLink

AWS PrivateLink only allows connections to be initiated from your VPC toward Confluent Cloud, basically a one-way channel for setting up connectivity. This reduces the security boundary and lowers the risk compared to VPC peering. PrivateLink can also simplify the network architecture allowing you to use the same set of security controls across your organization. Additionally there is no need to coordinate CIDR ranges as with VPC peering making deployments easier and faster. PrivateLink also provides transitive connectivity from other peered VPCs, Direct Connect, and VPN connections from on-premises datacenters.

DNS

Domain name system (DNS) names are managed by Confluent. When peering with Confluent Cloud, hostnames will be resolved to their private IP addresses from the CIDR ranges allocated to Confluent Cloud during provisioning. For secured public endpoints, hostnames will resolve to publicly routed IP addresses allocated from the cloud provider regional ranges.

When deploying PrivateLink endpoints, customers are required to override the AWS auto-generated DNS names for the endpoints with the hostnames provided by Confluent. The DNS names for the override are provided as part of the self-serve workflow when provisioning cluster network connectivity in the Confluent Cloud Dashboard.

Google Cloud Platform Topology

Secured Public Endpoints

Using secured public endpoints in GCP is straightforward as they are announced and accessible over the public internet as well as from inside an GCP VPC. It should be noted that public endpoint access from applications deployed inside of a GCP VPC will never traverse the public internet, just the GCP public backbone.

VPC Peering

Confluent Cloud in GCP also supports peering with your own VPC estate in GCP. This means the traffic never traverses the public backbone of the cloud provider or the public internet.

Before deploying a cluster using VPC peering, you need to choose a private CIDR range to use for the cluster. This CIDR range can not overlap with existing ranges in the same routing domain.

Customers worried about peering extending the network trust boundary to the peered VPC can configure mitigating controls. This includes setting up security groups to not allow any inbound access to instances in their VPC.

DNS

DNS is managed by Confluent. When peering with Confluent Cloud, hostnames will be resolved to their private IP addresses from the CIDR ranges allocated to Confluent Cloud during provisioning. For secured public endpoints, hostnames will resolve to publicly routed IP addresses allocated from the cloud provider regional ranges.

Microsoft Azure

This section describes how to connect your Kafka clients securely to a Confluent Cloud cluster running in Azure.

Secured Public Endpoints

Using secured public endpoints in Azure is straightforward as they are announced and accessible over the public internet as well as from inside an Azure VNet. It should be noted that public endpoints accessed from applications deployed inside of an Azure VNet will never traverse the public internet, just the Azure public backbone.

VNet Peering

Confluent Cloud in Azure also supports peering with your own VNet estate in Azure. This means the traffic never traverses the public backbone of the cloud provider or the public internet.

Before deploying a cluster using VNet peering, you need to choose a private CIDR range to use for the cluster. This CIDR range can not overlap with existing ranges in the same routing domain.

Customers worried about peering extending the network trust boundary to the peered VNet can configure mitigating controls. This includes setting up security groups to not allow any inbound access to instances in their VNet.

Azure PrivateLink

Azure PrivateLink is on the Confluent Cloud roadmap.

DNS

DNS is managed by Confluent. When peering with Confluent Cloud, hostnames will be resolved to their private IP addresses from the CIDR ranges allocated to Confluent Cloud during provisioning. For secured public endpoints, hostnames will resolve to publicly routed IP addresses allocated from the cloud provider regional ranges.

Cloud Provider Region Selection

Customers are able to choose the geographic region of their clusters for data residency and other reasons. Confluent will never move customer data out of the selected region.

Confluent Cloud is available in a large number of cloud provider regions across the world. For an updated list, please refer to the Cloud Providers and Regions page in the docs.

Encryption in Transit

For encryption in transit, TLS and SASL over TLS is mandated and cannot be disabled. Traffic from clients to Confluent Cloud is authenticated and encrypted in transit and clients using earlier versions of TLS than v1.2 are not permitted to connect.

Encryption at Rest

Data at rest uses essentially the same default transparent AES-256 based disk encryption across AWS, GCP, and Azure. The transparent disk encryption is well suited for Kafka since Kafka serializes data into raw bytes before it is being persisted to disk.

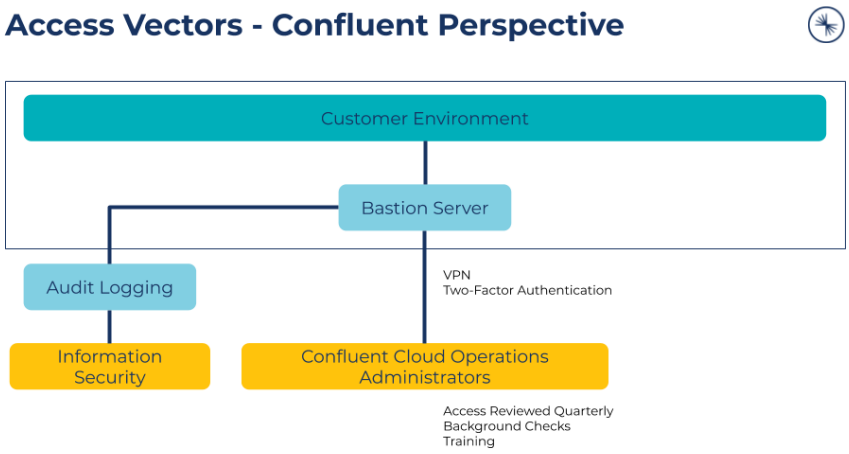
Encryption Key Management

Confluent Cloud uses one master key per account/project/tenant using the default cloud provider disk encryption mechanism described above. Confluents support for bring your own key (BYOK) is detailed later in this paper.

Confluent Employee Access Vectors

Confluent maintains an Access Management Standard that is updated at least annually and that

dictates access control internally based upon the principles of least privilege, need to know, and segregation of duties. Access reviews occur at time of hire, change of role, and termination as well as periodically through each calendar year. A list of preapproved administrators is maintained and regularly reviewed. Access to all production environments is only allowed for the preapproved individuals and requires multi-factor authentication.



Security events are logged centrally in support of investigation and review. VPN, with split tunneling prohibited, is required with two-factor authentication for access to our cloud bastion hosts for management of Confluent Cloud systems. Access is automatically revoked when someone leaves the company or changes roles. Periodic re-authentication with our single sign-on (SSO) platform is required. Bastion hosts that utilize appropriate security measures (host hardening, etc.) are the only enabled remote administration point of access for the small group of Confluent Cloud Operations Administrators on the Confluent Cloud production environment.

Internal Confluent Cloud Service Security

Configuration Management

The Confluent engineering team leverages infrastructure-as-code tools such as Terraform to configure all aspects of our cloud architecture with the same code review and release process that we use to build the applications and supporting processes that run the Confluent Cloud and Confluent Platform services. All changes are peer-reviewed before being rolled out to the first development pre-production environment where they are tested for extended functionality, and then moved to the next environment, staging, where they are tested at scale before finally being promoted to production.

Our Configuration Management Standard includes hardening procedures such as default password change, timely patching, administrative privileges limitation, and unnecessary account or service removal/deletion. We further restrict access to the images with only necessary Kafka protocol ports exposed outside of Confluent managed VPCs.

Separation of Production and Non-Production Environments

Confluent Cloud maintains strict separation between production and non-production environments. No customer data is ever utilized for non-production purposes, and non-production environments are used for development, testing, and staging only.

Confluent enforces the principle of least privilege and separation of duties. To this effect, developers only have access to development environments and production access is limited to authorized personnel only.

Firewalls and Bastion Hosts

Confluent Cloud infrastructure is only accessible via bastion hosts requiring multi-factor authentication in addition to a default key-based authentication. Access to production environments are subject to senior management approval. Firewalls are in place to segment and isolate various components of Confluent Cloud as well as to prevent unauthorized access.

Logging and Alerting

Confluent's information security team utilizes a centralized SIEM that merges multiple data sources for granular analysis as well as threat detection solutions/services to monitor and identify anomalous behavior, security events of interest, and indications of data breach. InfoSec reacts to identified deviations in line with Confluent's incident response plan.

Log Retention

Internal logs are immutable within our logging infrastructure by all users. Logs are stored for 12 months and are not shared with customers unless required as part of a security incident management process. Log deletion is a restricted authorized activity.

Secure Deletion of Data

When a customer deletes a Confluent Cloud cluster, the data becomes unavailable immediately. Maximum retention time can be configured on a per-topic basis. All data can be deleted by a customer or by our support team when requested at any time. Confluent will not store any data upon terminating the agreement. Confluent will delete all proprietary information within seven days but retain contact information of people that we engaged with as part of the purchase and deployment process in our CRM.

For disk deletion, we leverage the mechanisms offered by our cloud service providers:

- AWS
- Microsoft
- GCP

Input Validation

Input validation is done for data submitted to the web UI using source code checks, as part of code peer reviews, and through internal and external security testing.

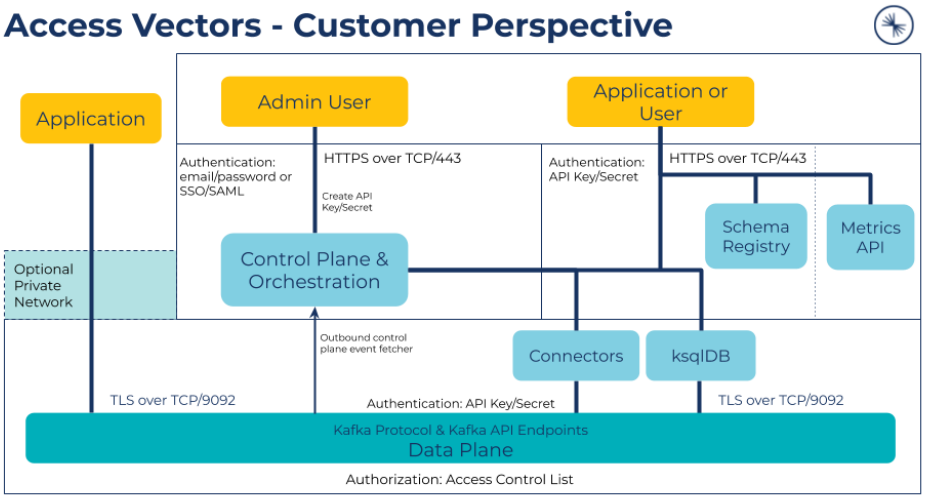
Available Customer Security Controls

Customer Access Vectors

Confluent Cloud exposes various endpoints as part of the service. The service separates into a control plane and a data plane, these are separated from each other and host their own authenticated endpoints. Control plane endpoints, as well as Schema Registry and the Metrics API are exposed over tcp/443 using API keys and secret keys as credentials. Access to the admin interfaces are authenticated using username/password or an SSO integration.

Important to note is that control plane events are fetched by the data plane using an outbound connection towards the control plane, there is no direct inbound access allowed to the data plane via the control plane.

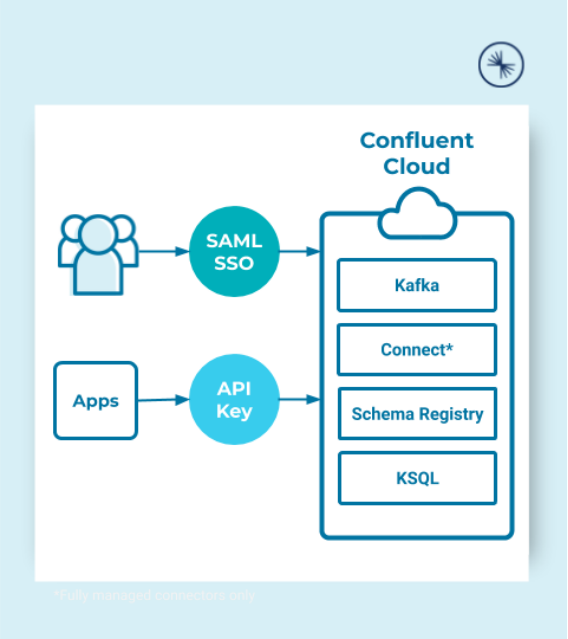
The Kafka admin APIs and the producer/consumer APIs in the data plane are exposed over tcp/9092 with mandatory TLS protection. Data plane endpoints are authenticated with SASL/PLAIN using API keys and secret keys as credentials.



Confluent Cloud Authentication and User Management

In this section, two Confluent Cloud components will be discussed:

- Confluent Cloud control plane (web UI, Confluent Cloud CLI, and APIs)
- Confluent Cloud data plane (produce and consume)



** for managed Kafka Connect only*

Control Plane

The Confluent Cloud web UI is where administrator **users** can manage clusters including the initial user setup. The web UI and CLI supports authentication with username/password and SSO via a SAML identity provider such as Okta, Azure AD, OneLogin, etc. Administrator users are added by way of the control plane interfaces either as local and/or SSO-enabled users. Confluent recommends SSO integration for all production environments.

User credentials for local, non-SSO-enabled users, are protected using the audited industry standard *bcrypt* one-way hashing algorithm before being stored.

Administrators have full super-user permissions to all resources in the Confluent Cloud organization. Control plane Role-Based Access Control (RBAC) is on the roadmap.

Data Plane

Confluent Cloud clusters have mandatory authentication enabled using SASL/PLAIN over TLS for applications. Service accounts and API keys are used as application credentials and are managed via the

control plane interfaces. No unauthenticated access is allowed to the service. API keys are hashed using *bcrypt* before being stored in the service and can not be retrieved once generated.

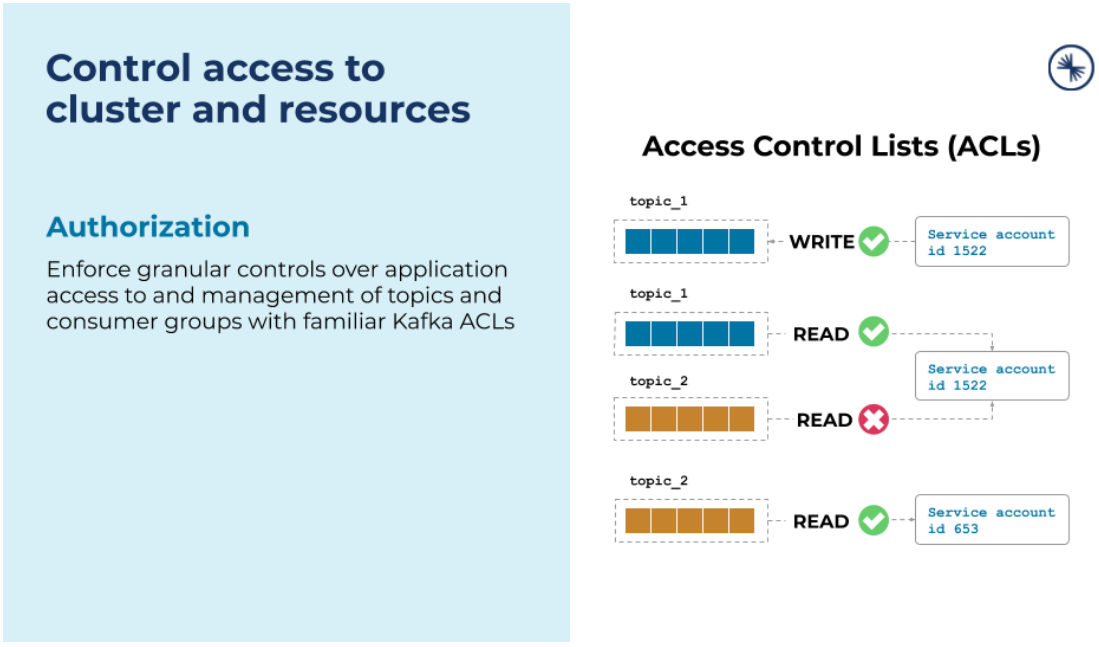
API Access

Access to the non-Kafka APIs, like the Control Plane and Metrics APIs, are controlled by Global API keys. Global API keys consist of an API Key + API Secret Key combination used as credentials.

Confluent Cloud Resource Access Control

Confluent Cloud can, in addition to Kafka clusters, also host Kafka Connect, ksqlDB, and Schema Registry resources. Access to these resources follow the same API key and secret key authentication mechanisms described earlier. In addition, Confluent Cloud supports Kafka Access Control Lists (ACLs) to provide granular control of what actions an application is allowed across certain topics. Please refer to the docs for additional details.

Limiting a producer/consumer application to only produce/consume to a certain topic is a common use case. Applications are issued service accounts that are mapped to ACLs as well as the API key and secret key credentials.



Customer Managed Encryption Keys (BYOK)

Customers can bring their own keys to Confluent Cloud as an alternative to further secure the data at rest. Customer managed encryption keys are available on AWS dedicated clusters.

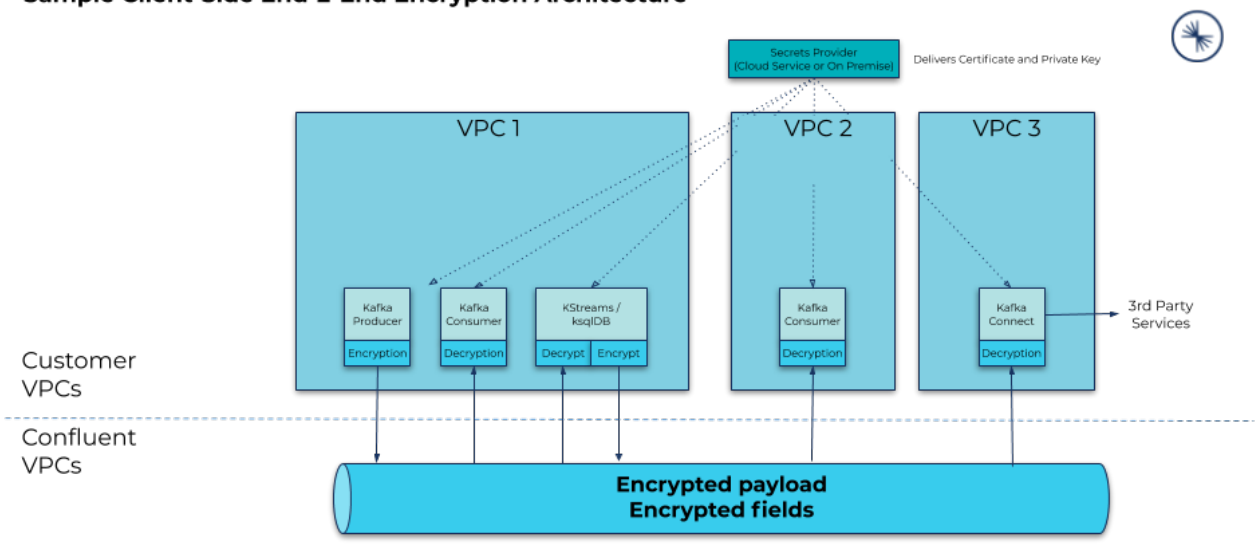
During cluster creation the AWS Amazon resource name (ARN) for the unique customer master key is supplied as an input to the provisioning of the cluster. This requires the customer to provide *read access* on the supplied key to the Confluent AWS account. Data encryption keys (DEKs) derived from the customer master key are then used to encrypt all data at rest; the DEKs are encrypted with the master key for protection, this process is known as envelope encryption.

Support for customer managed keys in GCP and Azure is on the roadmap.

Client-Side End-to-End Encryption

Confluent can provide field-level encryption and tokenization framework as part of a professional services engagement. This encryption framework is not covered by Confluent standard support offerings, rather it is framework delivered and supported through a professional services engagement. The framework includes components like custom serializer/deserializer, support of ksqlDB, integration to on-premises key managers as well as AWS, GCP and Azure key management services.

Sample Client-Side End-2-End Encryption Architecture



Also possible:

Clear Payload w. Encrypted Fields & Fully Clear Events

For more information about Client-Side End-to-End Encryption, please contact your local Confluent sales team or email info@confluent.io.

Auditing

Control Plane Auditing

Confluent Cloud audit logging for management authorization events is currently in Preview.

Confluent Cloud allows administrators to audit all actions and events triggered in the control plane at the organization, environment, and cluster level. The audit logs are stored in a Kafka topic. This means the logs are immutable and persisted to disk. Logs can then be accessed by the normal Kafka APIs.

Data Plane Auditing

Data plane auditing is under development and is coming soon.

IP Address Whitelisting

Whitelisting is on the Confluent Cloud roadmap.

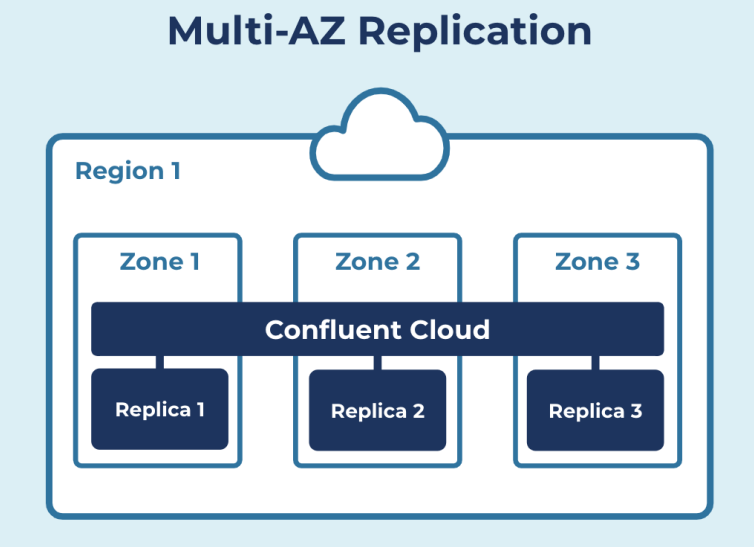
Business Continuity and Disaster Recovery

Confluent Cloud runs on infrastructure with a high level of availability and a resilient IT architecture. Confluent Cloud was designed to handle system, availability zone, and hardware failures with minimal or no customer impact.

In order to maintain an actionable Business Continuity and Disaster Recovery Plan (BCDRP), Confluent will conduct periodic (at least annually) testing and exercises to review incident management procedures, update plan documentation, and conduct system recovery testing. Confluent's BCDRP is based upon a business impact analysis (BIA) that is conducted at least annually and addresses a range of potential disruption scenarios and key recovery activities required for each disruption.

Availability

Confluent Cloud is built leveraging the cloud provider availability zone (AZ) concept. In each cloud provider region, clusters are stretched across three (3) AZs, effectively distributing the Kafka nodes across the AZs for maximum availability. Setting `replication-factor = 3` and `min.insync.replicas = 2`, effectively ensures the write operations can be performed even if one whole AZ goes down. Any cross-region replication requirements would be the responsibility of the customer to implement, Confluent provides tooling for this through Confluent Replicator.



Losing two AZs will deny writing of data to the cluster but reading data from the cluster is still possible.

Further, Confluent Cloud makes sure the number of nodes in each AZ cater for the need to do rolling restarts without affecting the availability of the service.

Availability statistics are published continuously on Confluent Cloud's status page.

Infrastructure Service Recovery

Confluent Cloud runs workloads on infrastructure provided by Azure, GCP, and AWS. Hence, data availability is also subject to the BCP and DR process of those infrastructure providers. For more information about the cloud providers' certifications and audit reports, see:

- AWS cloud compliance
- GCP cloud compliance and regulations resources
- Azure cloud compliance

Continuous Backups

Confluent backs up the details of customer accounts and configurations so that it can recover them in the event of a full cloud region outage or other catastrophic failures. Confluent does not archive or back up customer data.

Backing up data external to the service is possible but is the responsibility of the customer.

Incident Response

Confluent has a formal Incident Management Policy and procedure and communicates and trains the appropriate personnel on a periodic basis. Security incidents are handled by Confluent staff in either our IT/Facilities department (for physical security incidents) or in our Customer Operations/Support department (for software, computer, and network security incidents). Procedures include liaisons and points of contacts with local authorities in accordance with contracts and relevant regulations. Incident response is active 24x7x365 to detect, manage, and resolve any detected incidents.

Companywide Executive Review

The Security Steering Committee meets biannually to review reports, to identify control deficiencies and material changes in the threat environment, and to make recommendations for new or improved controls and threat mitigation strategies to executive management.

Support Coverage

Confluent support plans include options for 24x7 support with SLAs for response time depending on case severity and plan tier, with Premier and Enterprise support offering a 30-minute response SLA for P1s. Confluent Cloud Dedicated provides standard business support to all customers. This gives customers 24x7, follow-the-sun support with a SLA for a response time of 1 hour.

The support team has the backing of, and ability to escalate to, the majority of the Kafka committers, including the original architect and engineers. This ensures that you have the expertise to solve any Kafka problem, and confidence that patches will not lead you to a custom fork that would leave your production deployment exposed.

Our world-class support team is available via our enterprise support portal. Customers can also choose to purchase Premier support which offers a first response SLA of 30 minutes. Additional information at Confluent Cloud Support – Managed Kafka® as a Service.

Compliance

Confluent maintains a number of compliance certifications listed in this section, for additional information or to contact our compliance team please refer to our Trust and Compliance Page.

SOC 1, 2, and 3

- SOC 1 Type 2 is a regularly refreshed report that focuses on user entities' internal control over financial reporting. We currently offer SOC 1 Type 2 reports for Confluent Cloud and Confluent Platform.
- SOC 2 Type 2 is a regularly refreshed report that focuses on non-financial reporting controls as they relate to security, availability, and confidentiality. We currently offer SOC 2 Type 2 reports for Confluent Cloud and Confluent Platform.
- SOC 3 is a general use report that focuses on non-financial reporting controls as they relate to security, availability, and confidentiality. We currently offer SOC 3 reports for Confluent Cloud and Confluent Platform.

To request SOC reports, please contact your Confluent representative or email info@confluent.io.

ISO 27001

ISO/IEC 27001:2013 (also known as ISO27001) is the international standard that sets out the specification for an ISMS (information security management system). Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology. An independently accredited certification to the Standard is recognised around the world as an indication that our ISMS is aligned with information security best practice.

To request our latest ISO 27001 certificate, please contact your Confluent representative or email info@confluent.io.

PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) is an information security standard designed to ensure that companies processing, storing, or transmitting payment card information maintain a secure environment. Customers shall not transmit cardholder or sensitive authentication data (as those terms are defined in the PCI DSS standards) unless such data is message-level encrypted by the customer.

Confluent's Attestation of Compliance (AOC) can be requested by contacting your Confluent representative or email info@confluent.io.

CSA Star Level 1

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA's self-assessment tool is the Consensus Assessments Initiative Questionnaire (CAIQ). Confluent's CAIQ can be found here.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates protecting the privacy and security of health information. Confluent can support HIPAA-related customer data after a Business Associate Agreement (BAA) has been properly executed with Confluent.

Privacy

Confluent is committed to being transparent about the data we handle and how we handle it. Confluent's Privacy Policy can be found here.

GDPR Readiness

The General Data Protection Regulation (GDPR) regulates the use and protection of personal data originating from the European Economic Area (EEA) and provides individuals rights with regard to their data. Confluent is committed to supporting our customers in their GDPR compliance efforts. Confluent's Data Processing Addendum for Confluent Cloud customers can be found here.

CCPA Readiness

The California Consumer Privacy Act (CCPA) creates consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. Confluent is committed to supporting its customers in their CCPA compliance efforts. Confluent's Data Processing agreement for Confluent Cloud customers addresses both GDPR and CCPA requirements and can be found here.

Information Security Program Overview

Confluent has Information Security Policies and Standards that are based on industry best practices and standards (e.g., NIST SP 800-53 and ISO 27000-series). Confluent Information Security Policies and Standards are updated and reviewed at least annually and are made available to employees via the intranet. Confluent maintains a Security Steering Committee consisting of the Head of Information Security and Chief Legal Counsel. The Security Steering Committee meets biannually to review reports, to identify control deficiencies and material changes in the threat environment, and to make recommendations for new or improved controls and threat mitigation strategies to executive management. Risks are maintained within the Confluent Governance Risk & Compliance (GRC) system.

Security functions are spread across the organization including Information Security, Legal, Engineering, Business Operations, and Customer Support.

Confluent conducts risk assessments of various kinds throughout the year, including self- and third-party assessments and tests, automated scans, and manual reviews. Results of assessments, including formal reports as relevant, are reported to head of the Confluent Security Steering Committee. All risks are evaluated to assess impact, likelihood of occurrence, and other factors.

Confluent is committed to working with industry experts and security researchers to ensure our products are the most secure they can be for our customers. Confluent partners with HackerOne in order to continuously improve our security posture. If you would like to be invited into our bug bounty program, please send a request to bugbounty@confluent.io.

Application Security

Confluent has a standardized vulnerability management process and subscribes to manufacturer-related vulnerability advisories as well as US-CERT. Vulnerability scanning includes periodic internal and external scans by third-party penetration testing specialists. The latest applicable patches and updates are applied promptly after becoming available and being tested in Confluent's pre-production environments.

Potential impacts of vulnerabilities are evaluated. Vulnerabilities that trigger alerts and have published exploits are reported to the Security Steering Committee, which determines and supervises appropriate remediation action. FOSSA is used to scan licenses of dependencies and Twistlock for Docker package and jar dependency vulnerability management. In addition, Confluent utilizes a variety of tools that are open source and commercial such as InsightVM (Rapid7), Twistlock (Palo Alto Networks), FindBugs, and Prisma to scan for vulnerabilities and misconfigurations.

Notifications and Communication

Confluent will notify the customer in writing within seventy-two (72) hours of confirmed unauthorized access to content. Such notification will summarize the known details of the breach and the status of Confluent's investigation. Confluent will take appropriate actions to contain, investigate, and mitigate any such breach. This is in line with article 33(2) for the GDPR regulation where the regulation states: "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

Patching and Change Management

Patching is performed continuously on a need-to-update basis. Automated tools are used in conjunction with monitoring advisory and security bulletins. Confluent Cloud is continuously upgraded as new versions are released and deployed to production.

All changes are tracked with tickets, and peer-reviewed before being rolled out first to the development pre-production environment, where they are tested for extended functionality before moving to the next environment, staging, where they are tested at scale before finally being promoted to production. All releases have a corresponding QA test plan and internal release notes.

The Confluent Cloud upgrade policy is documented here.

Resources

Kafka expertise from the inventors of Kafka. Start your event streaming journey with Confluent. For more information, please visit confluent.io or contact us at info@confluent.io.

Confluent Cloud Security Addendum

Confluent Cloud DPA

Confluent Cloud Free Trial – Sign Up

Streaming Resources – Apache Kafka Resources, Tools, and Best Practices

Confluent, founded by the original creators of Apache Kafka®, pioneered the enterprise-ready event streaming platform. With Confluent, organizations benefit from the first event streaming platform built for the enterprise with the ease of use, scalability, security, and flexibility required by the most discerning global companies to run their business in real time. Companies leading their respective industries have realized success with this new platform paradigm to transform their architectures to streaming from batch processing, spanning on-premises and multi-cloud environments. Confluent is headquartered in Mountain View and London, with offices globally. To learn more, please visit www.confluent.io. Download Confluent Platform and Confluent Cloud at www.confluent.io/download.