CONFLUENT

Confluent Cloud Security Controls

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.

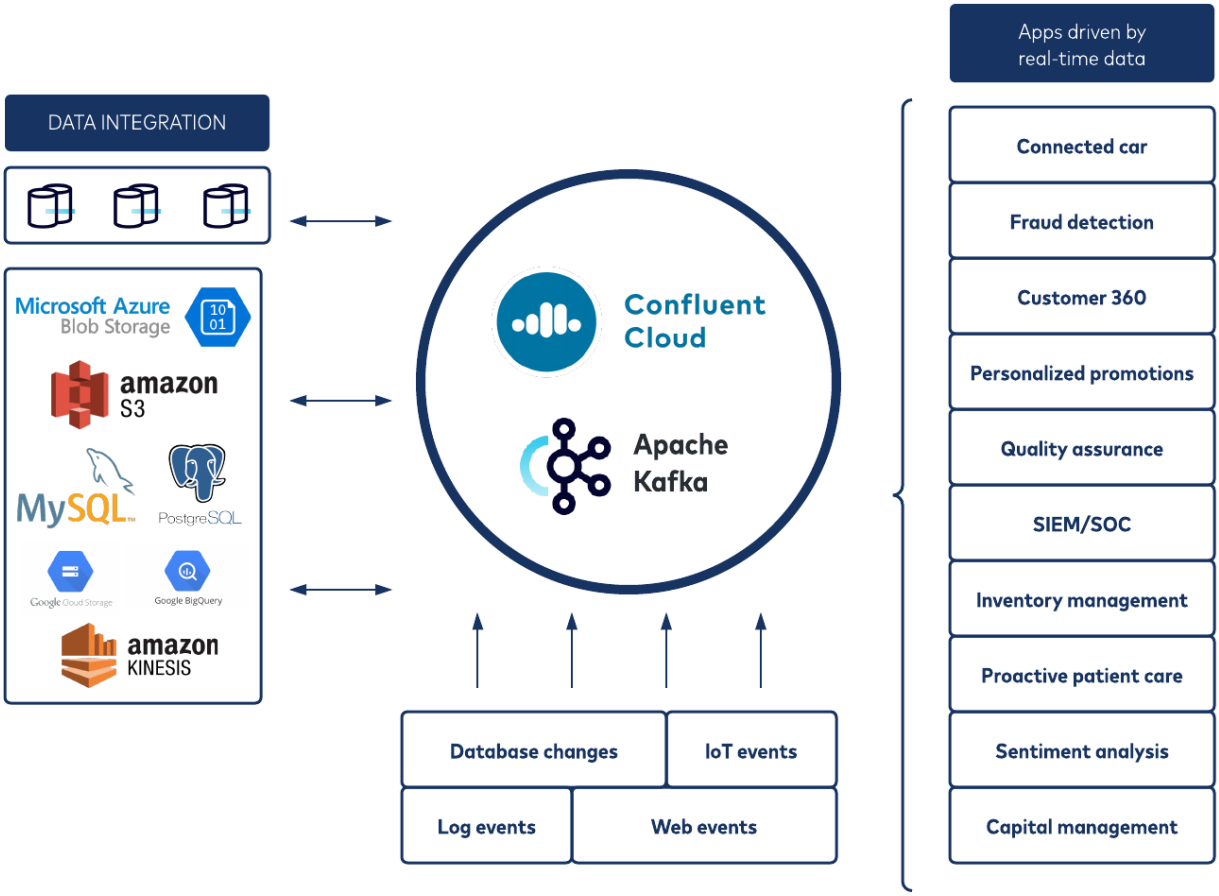
Confluent's security philosophy centers around layered security controls designed to protect and secure Confluent Cloud customer data. We believe in multiple logical and physical security control layers including access management, least privilege access, strong authentication, logging and monitoring,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

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 data streaming platform for connecting and processing your data everywhere it's needed. Confluent Cloud enables enterprises to transform Kafka into a central nervous system for all data in motion across their business with an elastically scaling, highly available, and secure data streaming platform for fast and easy development of real-time, event-driven applications.



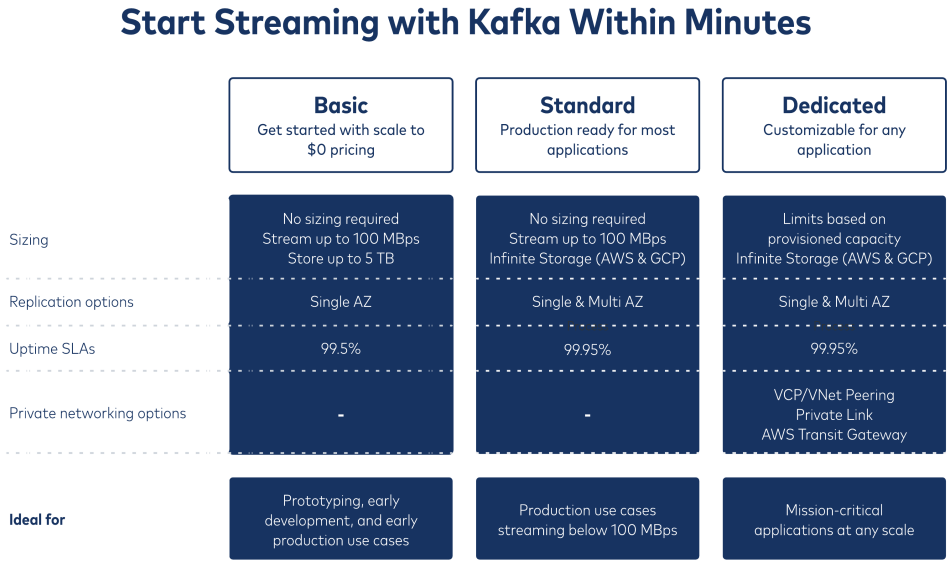
Confluent Cloud infinitely retains and democratizes access to all your event data in one place with simple development of data engineering pipelines and no infrastructure management. Simply point client apps or popular data services to Confluent Cloud and it takes care of the rest. Load is automatically 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:

- Set data in motion in minutes with on-demand provisioning of elastically scaling, cloud-native Apache Kafka clusters with scale-to-zero pricing for a truly serverless experience
- Stream confidently with enterprise-grade reliability, guaranteed uptime SLAs, multi-availability zone (AZ) replication for resilience, on-demand Kafka bug fixes, and zero-downtime upgrades
- Speed up app development with a rich, pre-built ecosystem of fully managed components including 50+ managed connectors, the industry's only governance suite for data in motion including Schema Registry, and real-time stream processing with ksqlDB
- Maintain flexibility with deployments available across clouds and on-premises that sync in real-time with Cluster Linking or Confluent Replicator

Confluent Cloud Cluster Types

Confluent Cloud offers a range of cluster types to address a multitude of customer use cases, cluster types can be mixed and matched in the same account.



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 Terminology

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.

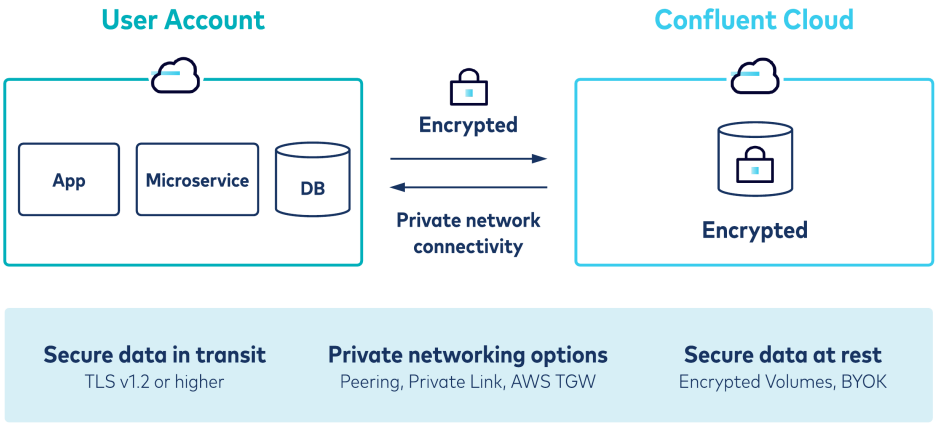
Cluster: A Confluent Cloud cluster is deployed inside an environment and provides Kafka API endpoints for developing streaming applications.

API keys: API keys can be divided into two classes

- Cloud API keys: These grant access to the Confluent Cloud Control Plane APIs, such as for provisioning and metrics integrations.
- Cluster API keys: These grant access to a single cluster, such as a specific Kafka or Schema Registry cluster.

Internal Confluent Cloud Infrastructure Security

Data security is essential when it is transported in and out Confluent Cloud 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, 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 data centers are compliant with a large number of physical and information security standards resulting in Confluent Cloud inheriting the same best in class security controls. For additional information, please refer to the compliance page of your selected cloud provider:

- AWS compliance
- Azure compliance
- Google Cloud Compliance

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

Networking

Confluent Cloud runs on public cloud provider infrastructure and the cloud specific networking details are covered further down, security controls and details that are generic to the service across clouds are covered here.

Network Ports

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

- tcp/9092 for Kafka service endpoints
- tcp/443 for admin GUI/CLI/API, ksqlDB endpoints, Schema Registry endpoints, Metrics API endpoints

TLS v1.2 is mandated and can not be disabled, TLS 1.0 and V1.1 are not allowed.

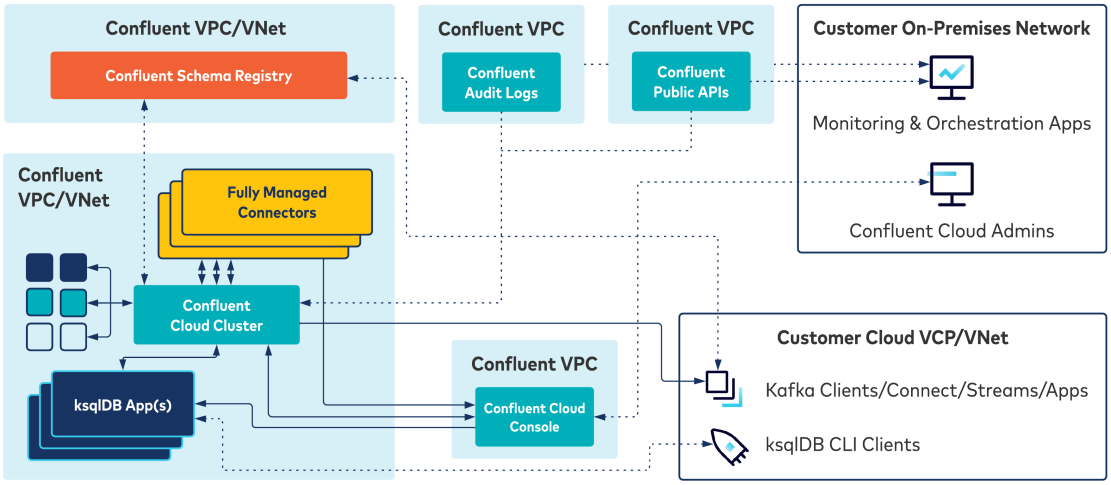
Denial of Service Protection (DoS)

Confluent Cloud clusters with public endpoints are protected by a proxy layer that prevents some types of DoS attacks like syn flooding and other network-level attacks. Confluent Cloud clusters using peering, Private Link or AWS Transit Gateway are not accessible from the public internet at all.

In general the cloud provider networks have inherent protections against large scale DoS attacks enabling them to absorb and divert flows to protect their services.

Confluent Cloud Architecture

Sample Deployment with Supporting Services



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 network connectivity options. These options are:

- Secured public endpoints (AWS, Google Cloud, and Azure)
- VPC/VNet Peering (AWS, Google Cloud, and Azure)
- Private link (AWS and Azure)
- Transit Gateway (AWS only)

Amazon Web Services Networking

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, the traffic will be carried on the AWS 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 access vector risk compared to VPC peering and Transit Gateway. 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 or Transit Gateway connections making deployments easier and faster. PrivateLink also provides for transitive connectivity with peered VPCs as well as for Direct Connect and VPN connections to on-premises data centers.

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 required DNS information for the override is provided as part of the Confluent Cloud self-serve workflow.

Google Cloud Networking

Secured Public Endpoints

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

VPC Peering

Confluent Cloud in Google Cloud also supports peering with your own VPC estate in Google Cloud. 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 Networking

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 Private Link

Azure Private Link only allows connections to be initiated from your VNet toward Confluent Cloud, basically a one-way channel for setting up connectivity. This reduces the security boundary and lowers the access vector risk compared to VNet peering. Private Link 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 VNet peering making deployments easier and faster. Private Link also provides for transitive connectivity with other peered VNets as well as for Express Route and VPN connections to on-premises datacenters.

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.

When deploying Private Link endpoints, customers are required to override the Azure auto-generated DNS names for the endpoints with the hostnames provided by Confluent. The required DNS information for the override is provided as part of the Confluent Cloud self-serve workflow.

Cloud Provider Region Selection

For customer message data produced to a topic and transmitted through Kafka, Customers are able to choose the geographic region of their clusters for data residency and sovereignty requirements. Confluent does not move such 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 documentation.

Encryption in Transit

Encryption using TLS 1.2 is required for all client connections to Confluent Cloud and HTTP Strict Transport Security (HSTS) is enabled.

Encryption at Rest

Data at rest uses essentially the same default transparent AES-256 based disk encryption across AWS, Google Cloud, 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. Confluent's 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. Two-factor authentication is required for access to our cloud bastion hosts and cloud consoles 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 and cloud administration consoles are the only enabled remote administration points of access for engineers on the Confluent Cloud production environment.

Authorization and multi-factor authentication are required in order to access bastion hosts or the cloud administration consoles.

Internal Confluent Cloud Service Security

Configuration Management

The Confluent engineering team leverages infrastructure-as-code tools 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, security 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, access to production environments are limited to authorized personnel only.

Network Access Controls and Bastion Hosts

Confluent Cloud infrastructure access requires multi-factor authentication in addition to a default key-based authentication. Access to production environments are subject to an approval process based on need-to-know, separation of duties and least privilege. Additionally employees undergo background checks, where allowable by law. Network access controls are in place to segment production networks to prevent unauthorized access.

Time Synchronization

Confluent Cloud leverages cloud provider NTP server pools to do time synchronisation across the infrastructure.

Logging and Alerting

Confluent's information security team utilizes a centralized Security Information and Event Management (SIEM) system 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 in our internal SIEM system are retained for at least 12 months

Log deletion is a restricted authorized activity.

Secure Deletion of Data

When a customer deletes a Confluent Cloud cluster, messages stored in topics immediately becomes unaccessible via the Kafka APIs. 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. Upon termination of the agreement, Confluent will no longer write new data and existing customer data will no longer be stored after seven days.

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

- AWS
- Google Cloud
- Microsoft

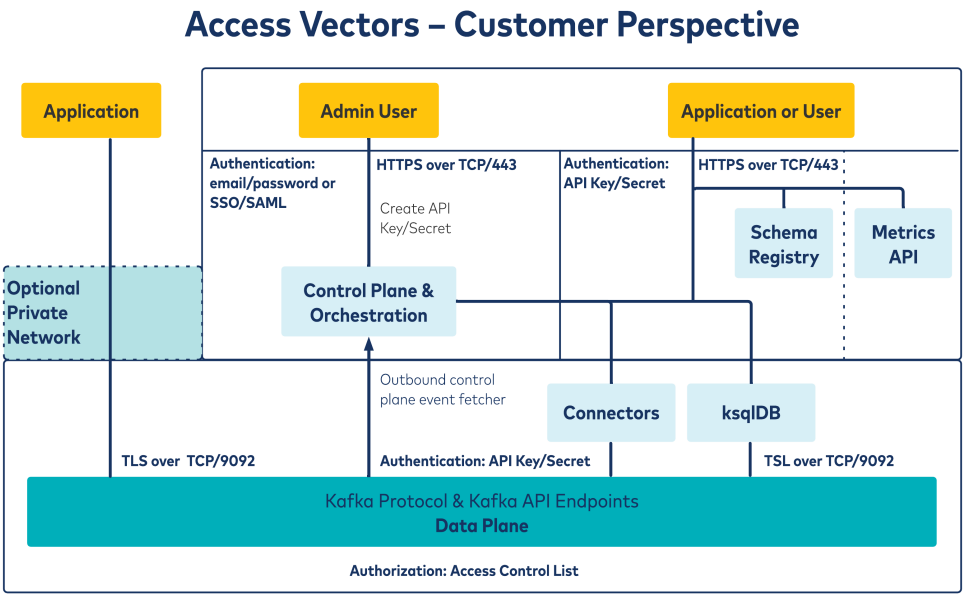
Available Customer Security Controls

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.

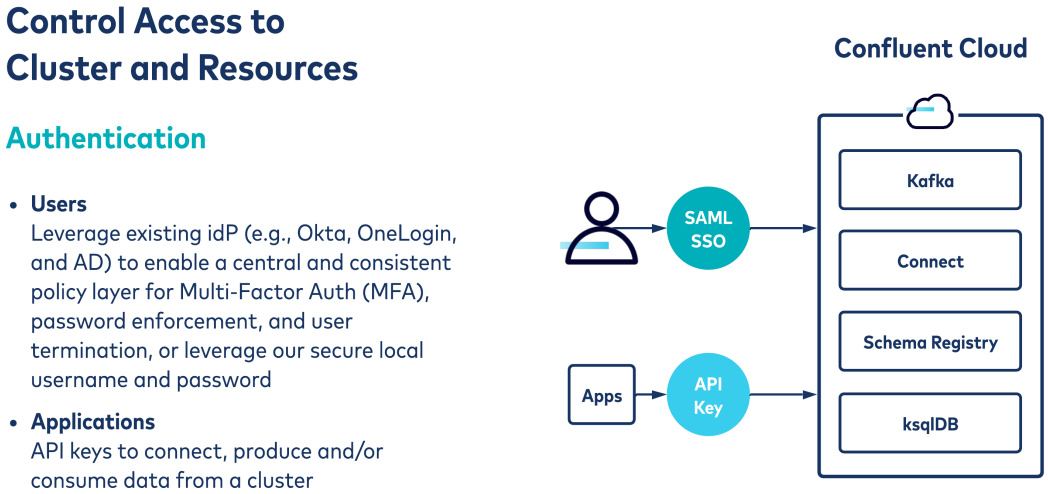
The Kafka admin APIs and the producer/consumer APIs in the data plane are exposed over tcp/9092 with mandatory TLS protection. Data plane endpoints are accessible by Kafka clients authenticating using API key and API secret key as credentials over SASL/PLAIN. The Confluent Cloud UI also allows for data plane access using JWT tokens issued by the control plane for authenticated admin users with the proper RBAC permissions.



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 admin users manage all resources including the initial user setup. The web UI and CLI supports authentication with username/password and SSO via any SAML identity provider such as Okta, OneLogin, Azure AD, etc. Administrator users are added by way of the control plane interfaces. Confluent recommends SSO integration for all production environments.

User passwords are held by our identity management solutions provider Auth0, the auth0 stored credentials are protected using the industry standard *bcrypt* one-way salted hashing algorithm before being persisted.

By default administrator users have full super-user permissions to all resources in the Confluent Cloud organization Confluent recommends using Control Plane Role-Based Access Control (RBAC) to further

manage administrator permissions and roles.

Data Plane

Confluent Cloud clusters provide TLS endpoints mandating authentication using SASL/PLAIN for encrypted and authenticated application access. 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 Secret Keys are hashed using *bcrypt* before being stored in the service and can not be retrieved once generated.

Confluent Cloud REST APIs

Access to the non-Kafka REST APIs are controlled by Cloud API keys. Cloud API keys consist of an API key + API secret key combination used as credentials. API keys are tied to either a service account or user account principle and inherit their existing permissions as configured through role-based access control (RBAC) and/or access control lists (ACLs).

Confluent Cloud REST APIs are protected using multiple rate limiting functions; breaching limits will result in error messages or dropped requests to safeguard availability.

Confluent Cloud Role Based Access Control (RBAC)

Confluent Cloud Role Based Access Control (RBAC) enables delegation and control of permissions to Confluent Cloud admin users as well as for service accounts. Confluent Cloud RBAC roles can be used to control access to an organization, its environments, the clusters within each environment, and the Kafka resources on those clusters. Principles can be assigned multiple roles.

Confluent Cloud RBAC is applied across the GUI, the Confluent CLI as well as the Confluent Cloud REST APIs as a security control common across all user interfaces. RBAC is the recommended method to control permissions in a Confluent Cloud environment, superseding the classic Kafka access control lists (ACLs). Kafka ACLs and Confluent Cloud RBAC can be used simultaneously if required although RBAC is considered best practise.

For details on roles, resource scoping and setup please refer to the documentation.

Confluent Cloud Access Control Lists (ACLs)

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 documentation for additional details.

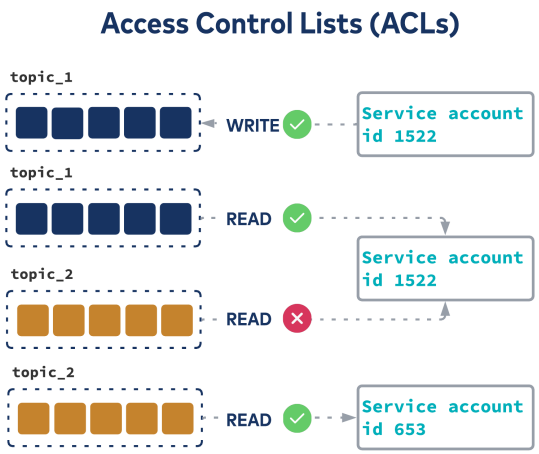
Limiting a producer/consumer application to only produce/consume to a certain topic is a common use case. Applications are issued service accounts that are mapped to ACLs as well as the API key and secret key credentials.

Confluent Cloud supports ACLs and RBAC to be used simultaneously although using RBAC is considered best practise where applicable.

Control Access to Cluster and Resources

Authorization

Enforce granular controls over application access to and management of topics and consumer groups with familiar Kafka ACLs



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 and GCP dedicated clusters. For key rotation only automatic rotation is supported, importing key material is not supported and the key and the Confluent Cloud cluster must be in the same region.

Support for customer managed keys on Azure is on the roadmap.

AWS

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 the Confluent AWS Account with permissions to access and use the supplied key, further details and sample KMS key policy available in the documentation. The sample KMS policy can be further augmented with additional conditions such as source VPC validation to meet requirements above what is covered in the sample policy. 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.

GCP

During cluster creation the Google Cloud resource name is supplied, a service account with the proper permissions is used to fetch the key from the Google Cloud KMS. For details on required IAM permissions and further details refer to the documentation.

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.

Audit Logs

Confluent Cloud audit logs include three types of events that can be audited:

- Authentication events: Event log events occur when a client connects to a Kafka cluster
- Authorization events: When a Kafka cluster verifies authorization
- Organizational events: This is sent when a Confluent Cloud service performs an operation or action

The audit logs are stored in a Kafka topic. This means that the logs are immutable and persisted to disk. Logs can then be accessed using standard Kafka APIs and exported into a log management or SIEM solution, which can be achieved either by custom integration or using existing Confluent connectors.

More details on Confluent Cloud Audit Logs are available in the documentation.

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.

Confluent BC/DRP documentation can be requested using the automated request form at our Trust and Security Page.

Availability

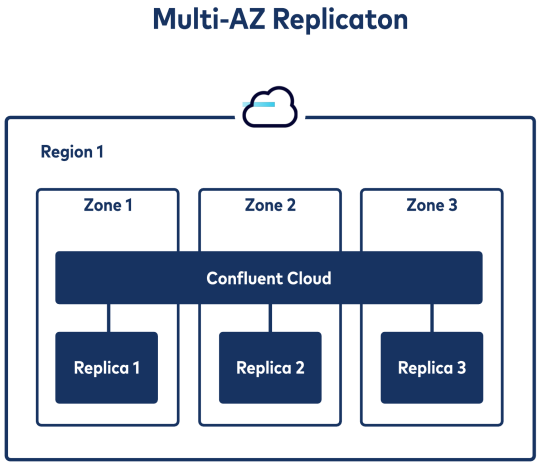
Confluent Cloud is built leveraging the cloud provider availability zone (AZ) concept. In each cloud provider region, clusters are stretched across three (3) AZs, effectively distributing the Kafka nodes across the AZs for maximum availability. Setting `replication-factor = 3` and `min.insync.replicas = 2`, effectively ensures 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 and Cluster Linking. Losing two AZs will disable writing of data to the cluster, reading data from the cluster is still possible with only one AZ operational.

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.

Resiliency to Cloud Provider Failures

Single Region

- **Zero downtime**
  Protection against single zone failures with multi-AZ replication
- **Synchronous replication**
  Replication across three availability zones for high availability and durability
- **Data residency**
  Confluent never moves customer data outside the cloud region selected by the customer



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

Infrastructure Service Recovery

Confluent Cloud runs workloads on infrastructure provided by Azure, Google Cloud, 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
- Google Cloud 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 utilize traditional backup media including magnetic tapes, optical drives, or periodic data media removal and rotation.

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. A Priority One (P1) Issue means the (i) Cloud Service is severely impacted or completely shut down, or (ii) Cloud Service operations or mission-critical applications are down. More details on priority definitions can be found in our Support Services Policy.

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 choose a range of support tiers where the Premier support tier offers a first response SLA of 30 minutes. Additional information on support offerings available at Confluent Cloud Support – Managed Kafka® as a Service.

Service SLAs

Confluent Cloud maintains a guaranteed 99.95% SLA with a credit-based compensation process. You can refer to the Confluent Cloud Service Level Agreement for more details.

Confluent Cloud ksqlDB maintains a guaranteed 99.9% SLA with a credit-based compensation process. You can refer to the Confluent Cloud ksqlDB Service Level Agreement for more details.

For the Confluent Cloud Schema Registry service, there is also an SLA available.

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 Security 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 use the automated request form at our Trust and Security Page.

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 use the automated request form at our Trust and Security Page.

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 using the automated request form at our Trust and Security Page.

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.

TISAX

The Trusted Information Security Assessment Exchange (TISAX) is an assessment and exchange mechanism for information security in the automotive industry. TISAX assessments are conducted by accredited audit providers that demonstrate a company's qualification at regular intervals. The certification is based on key aspects of information security, such as connections to third parties and data protection.

TISAX and TISAX results are not intended for the general public, the Confluent results (Scope-ID: S4PCMP; Assessment-ID: AV56AB-2) are exclusively available through the ENX Portal

Privacy

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. Article 28 of the GDPR requires all data controllers enter into binding agreements with their data processors. These agreements, known as Data Processing Addenda or DPAs, establish the roles and responsibilities of processors when processing personal data on the controller's behalf. Article 28 also requires that processors enter into DPAs with their subprocessors (e.g., vendors who provide services to processors to enable the processing).

In addition, 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. The CCPA requires that service providers, like Confluent, agree to certain written contractual restrictions with their customers.

These include commitments not to sell personal information, to use personal information only to perform under the agreement, and to pass through similar obligations to sub-service providers. Confluent is committed to supporting its customers in their GDPR and CCPA compliance efforts. Because Confluent acts as a data processor and as a service provider of customer message data produced to a topic and transmitted through Kafka via the Cloud Service, Confluent uses its Confluent Cloud Data Processing Addendum to address both CCPA and GDPR requirements.

Confluent is committed to being transparent about the data we handle and how we handle it. In the event that Confluent acts as a data controller with regard to personal information, Confluent handles such personal information according to Confluent's Privacy Policy.

Trust & 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 Chief Information Security Officer 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 employs a Software Development Lifecycle (SDLC) program that includes a standardized vulnerability management process and subscribes to manufacturer-related vulnerability advisories as well as US-CERT. The SDLC program and processes aligns with NIST 800-160, ISO 27001 Anex A.14 and CIS Control 18 and is alidated by third party assessment firms and exemplified by our compliance certifications.

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. Open Source management tools are used to scan licenses of dependencies, Docker packages and jar dependencies are scanned using vulnerability management tools. In addition,

Confluent utilizes a variety of commercial and open source tools to scan for vulnerabilities and misconfigurations.

Notifications and Communication

Confluent will notify a customer in writing within seventy-two (72) hours of a confirmed unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to customer message data transmitted through Confluent Cloud.

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.

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 available in the documentation.

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.