Security in ClickHouse Cloud

San Tran

Dec, 2023

ClickHouse

Speakers

San Tran

Application/Product security dude

01 ClickHouse Cloud Security features journey

ClickHouse

Timeline

Dec 2022 (GA Launch)

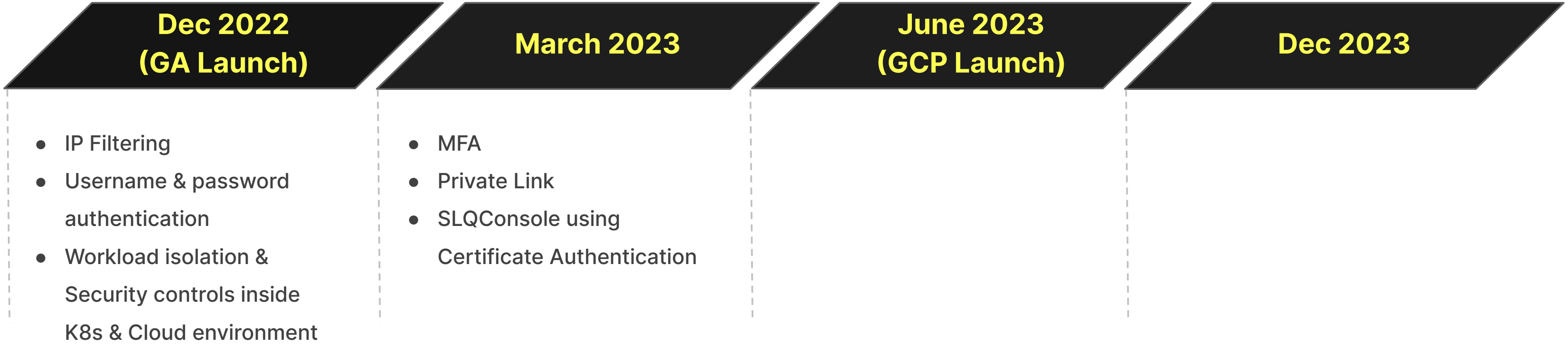
- IP Filtering
- Username & password for authentication 😅
- Workload isolation & Security controls inside K8s & Cloud environment

March 2023

June 2023 (GCP Launch)

Dec 2023

Timeline



Dec 2022 (GA Launch)

- IP Filtering
- Username & password authentication
- Workload isolation & Security controls inside K8s & Cloud environment

March 2023

- MFA
- Private Link
- SLQConsole using Certificate Authentication

June 2023 (GCP Launch)

Dec 2023

Timeline

Dec 2022 (GA Launch)

- IP Filtering
- Username & password authentication
- Workload isolation & Security controls inside K8s & Cloud environment

March 2023

- MFA
- Private Link
- SLQConsole using Certificate Authentication

June 2023 (GCP Launch)

- Customer Managed Encryption Key (CMEK)
- REST API security
- Secure S3 access

Dec 2023

Timeline

Dec 2022 (GA Launch)

- IP Filtering
- Username & password authentication
- Workload isolation & Security controls inside K8s & Cloud environment

March 2023

- MFA
- Private Link
- SLQConsole using Certificate Authentication

June 2023 (GCP Launch)

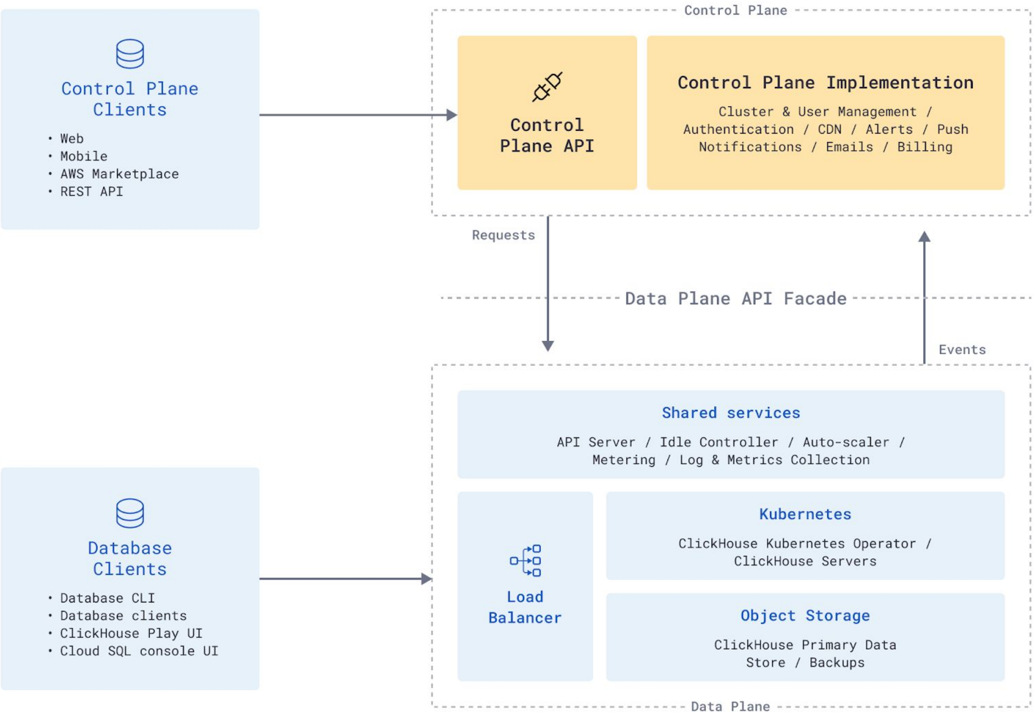
- Customer Managed Encryption Key (CMEK)
- REST API security
- Secure S3 access

Dec 2023

- ClickPipe data ingestion
- Self served Secure S3 & Private Link
- Auth0 migration in preparation for BYO SAML Identity Provider.

02 Let’s get to the details…

Workload isolation

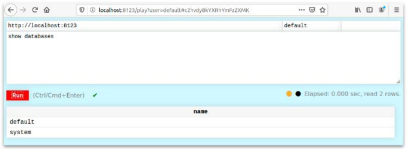

Control Plane Clients
• Web
• Mobile
• AWS Marketplace
• REST API
Control Plane
Control Plane API
Control Plane Implementation
Cluster & User Management / Authentication / CDN / Alerts / Push Notifications / Emails / Billing
Requests
Data Plane API Facade
Events
Database Clients
• Database CLI
• Database clients
• ClickHouse Play UI
• Cloud SQL console UI
Shared services
API Server / Idle Controller / Auto-scaler / Metering / Log & Metrics Collection
Load Balancer
Kubernetes
ClickHouse Kubernetes Operator / ClickHouse Servers
Object Storage
ClickHouse Primary Data Store / Backups
Data Plane

Picture taken from: https://clickhouse.com/blog/building-clickhouse-cloud-from-scratch-in-a-year

Workload Isolation - ClickPipes

ClickHouse
ClickPipe

Console Certificate Authentication

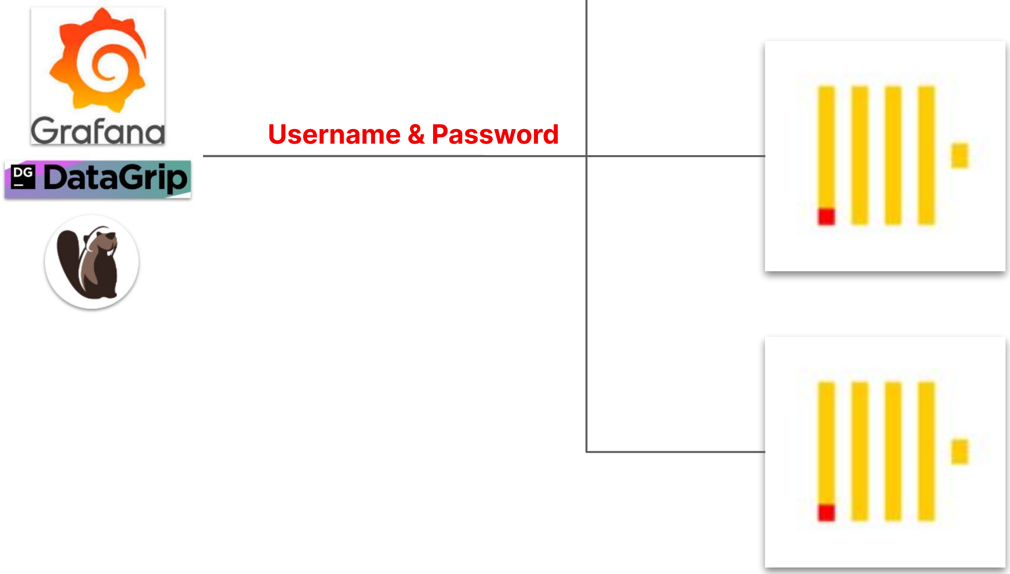


```
localhost:8123/play?user=default#c2hvdyBkYXRhYmFzZXMK
http://localhost:8123                              default
show databases
```

Elapsed: 0.000 sec, read 2 rows.

name
default
system

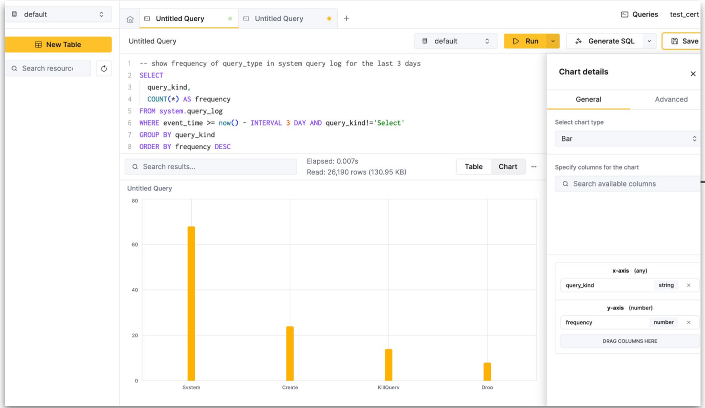
PlayUI



Username & Password

Console Certificate Authentication

SQLConsole/Arctype



```
-- show frequency of query_type in system query log for the last 3 days
SELECT
  query_kind,
  COUNT(*) AS frequency
FROM system.query_log
WHERE event_time >= now() - INTERVAL 3 DAY AND query_kind!='Select'
GROUP BY query_kind
ORDER BY frequency DESC
```

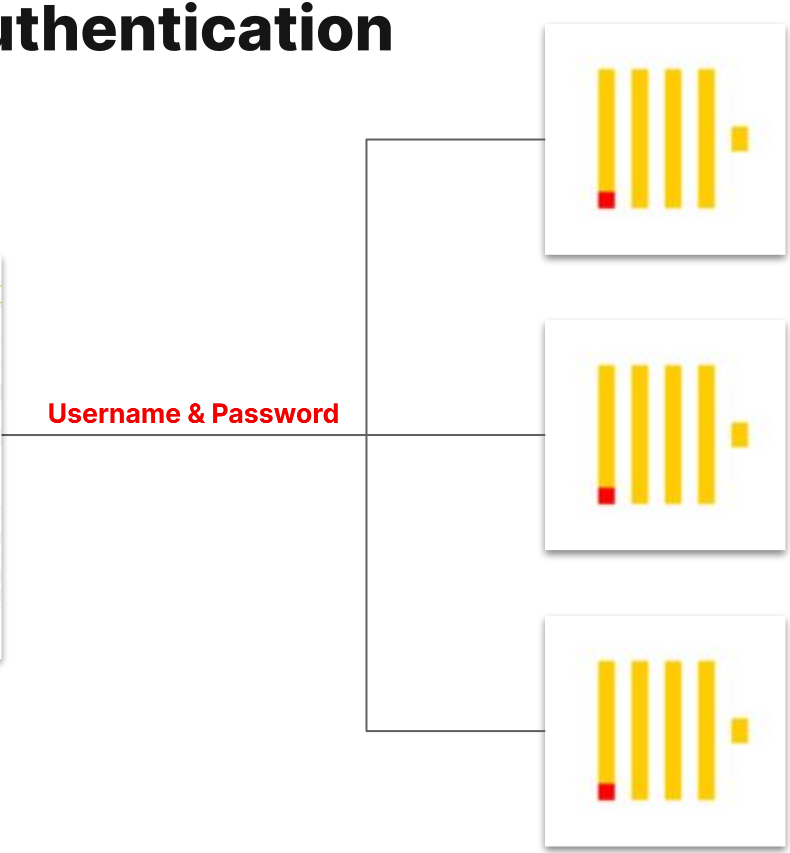
Elapsed: 0.007s
Read: 26,190 rows (130.95 KB)

Select chart type: Bar

Specify columns for the chart

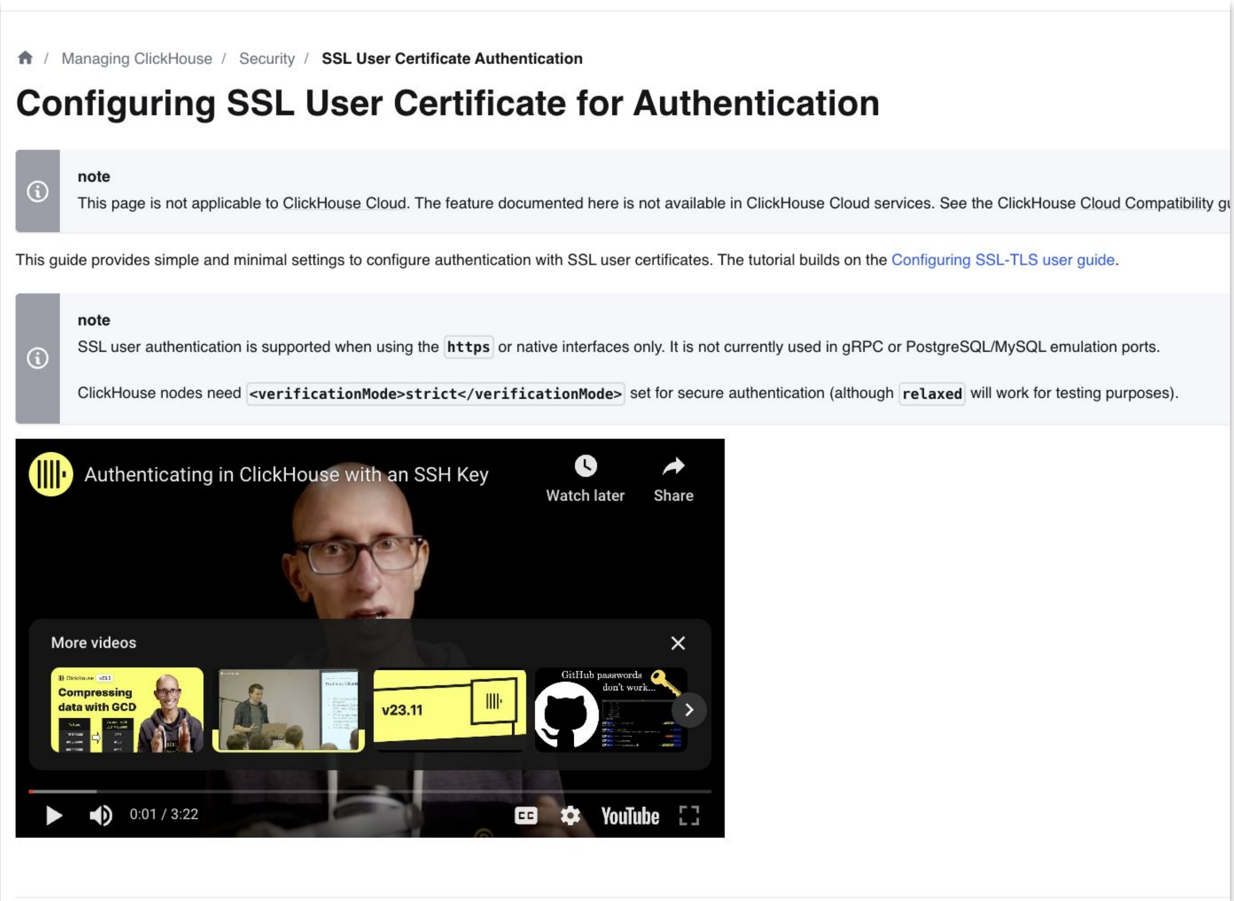
x-axis (any): query_kind string

y-axis (number): frequency number



Username & Password

Say NO to passing client credentials where we can!



Managing ClickHouse / Security / **SSL User Certificate Authentication**

Configuring SSL User Certificate for Authentication

note

This page is not applicable to ClickHouse Cloud. The feature documented here is not available in ClickHouse Cloud services. See the ClickHouse Cloud Compatibility gu

This guide provides simple and minimal settings to configure authentication with SSL user certificates. The tutorial builds on the Configuring SSL-TLS user guide.

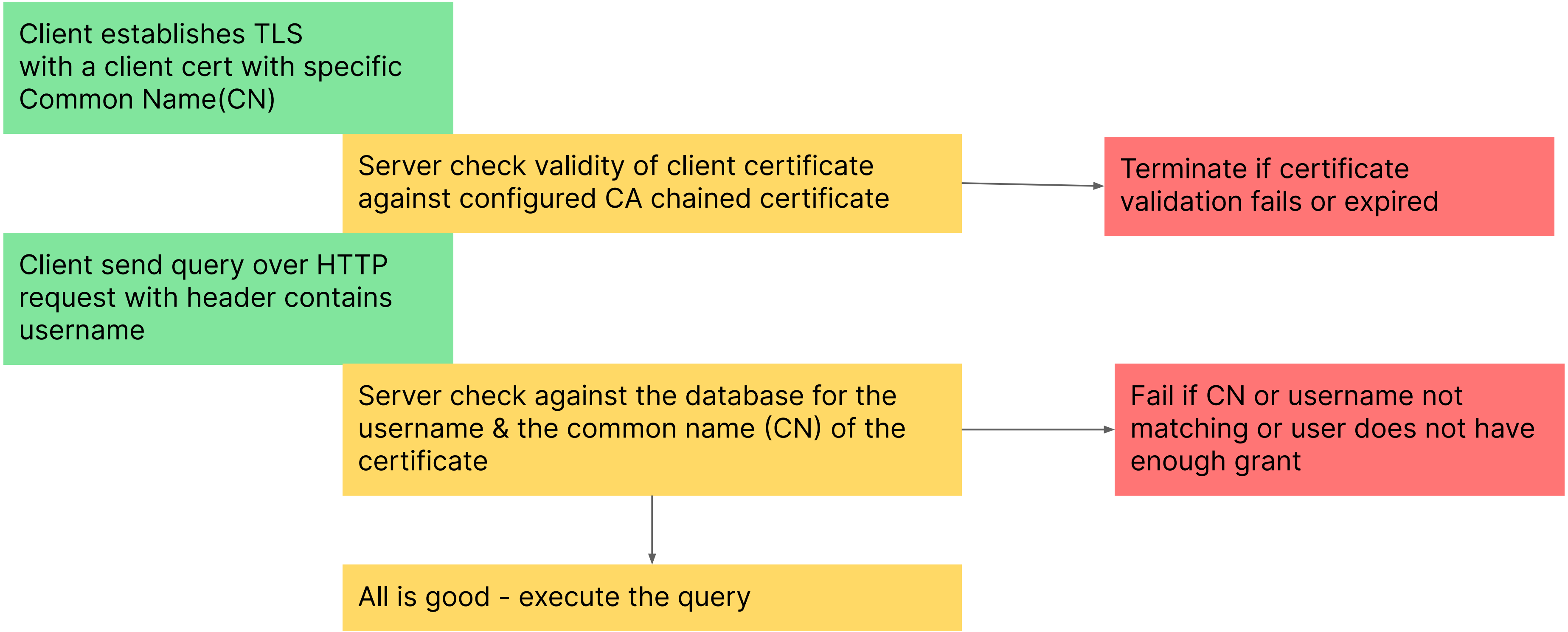
note

SSL user authentication is supported when using the `https` or native interfaces only. It is not currently used in gRPC or PostgreSQL/MySQL emulation ports.

ClickHouse nodes need `<verificationMode>strict</verificationMode>` set for secure authentication (although `relaxed` will work for testing purposes).

Authenticating in ClickHouse with an SSH Key
Watch later
Share
More videos
Compressing data with GCD
v23.11
GitHub passwords don't work...
0:01 / 3:22
YouTube

How cert-auth works end to end with ClickHouse for HTTP Protocol?



Client establishes TLS with a client cert with specific Common Name(CN)

Server check validity of client certificate against configured CA chained certificate

Terminate if certificate validation fails or expired

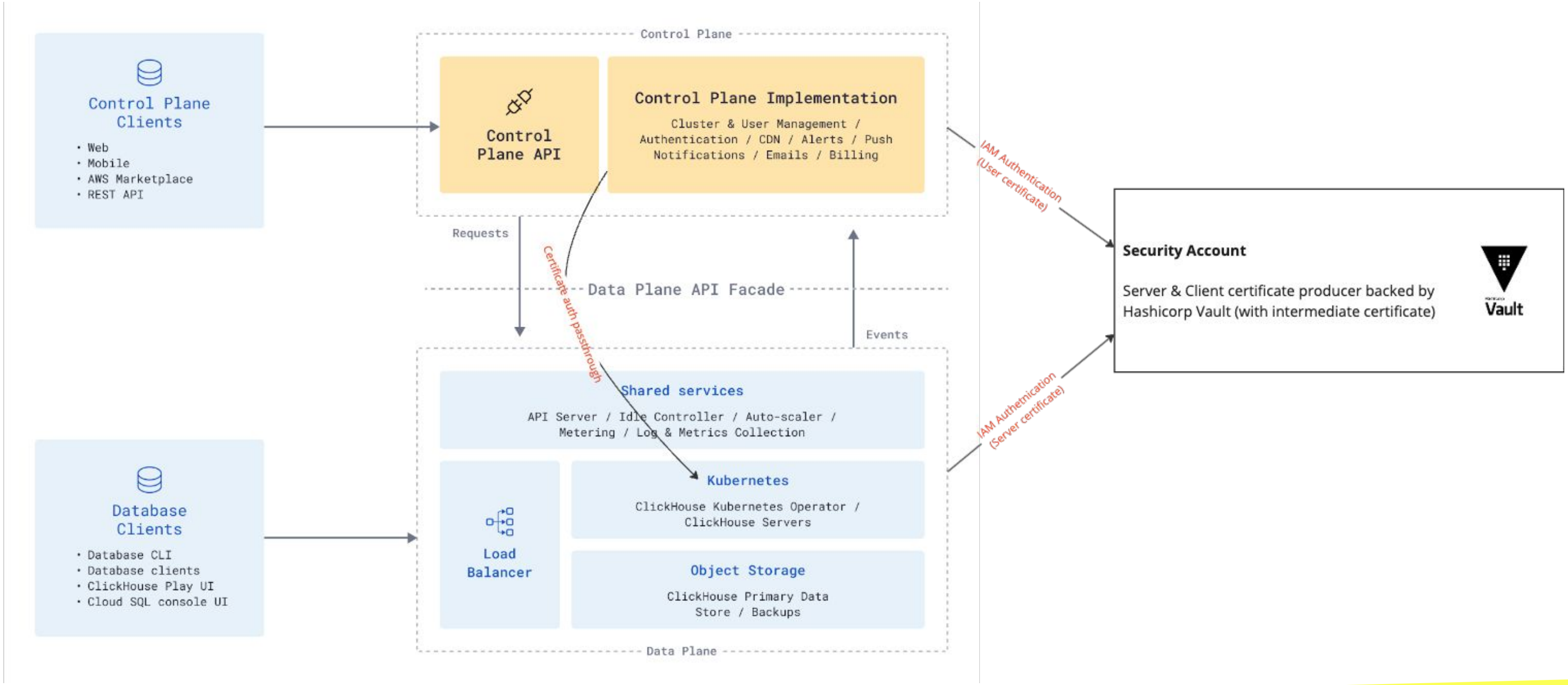
Client send query over HTTP request with header contains username

Server check against the database for the username & the common name (CN) of the certificate

Fail if CN or username not matching or user does not have enough grant

All is good - execute the query

Console Certificate Authentication - high level design



Control Plane Clients

- Web
- Mobile
- AWS Marketplace
- REST API

Control Plane

Control Plane API

Control Plane Implementation

Cluster & User Management / Authentication / CDN / Alerts / Push Notifications / Emails / Billing

Requests

Events

Certificate auth passthrough

Data Plane API Facade

IAM Authentication (User certificate)

IAM Authetnication (Server certificate)

Security Account

Server & Client certificate producer backed by Hashicorp Vault (with intermediate certificate)

Vault

Database Clients

- Database CLI
- Database clients
- ClickHouse Play UI
- Cloud SQL console UI

Shared services

API Server / Idle Controller / Auto-scaler / Metering / Log & Metrics Collection

Load Balancer

Kubernetes

ClickHouse Kubernetes Operator / ClickHouse Servers

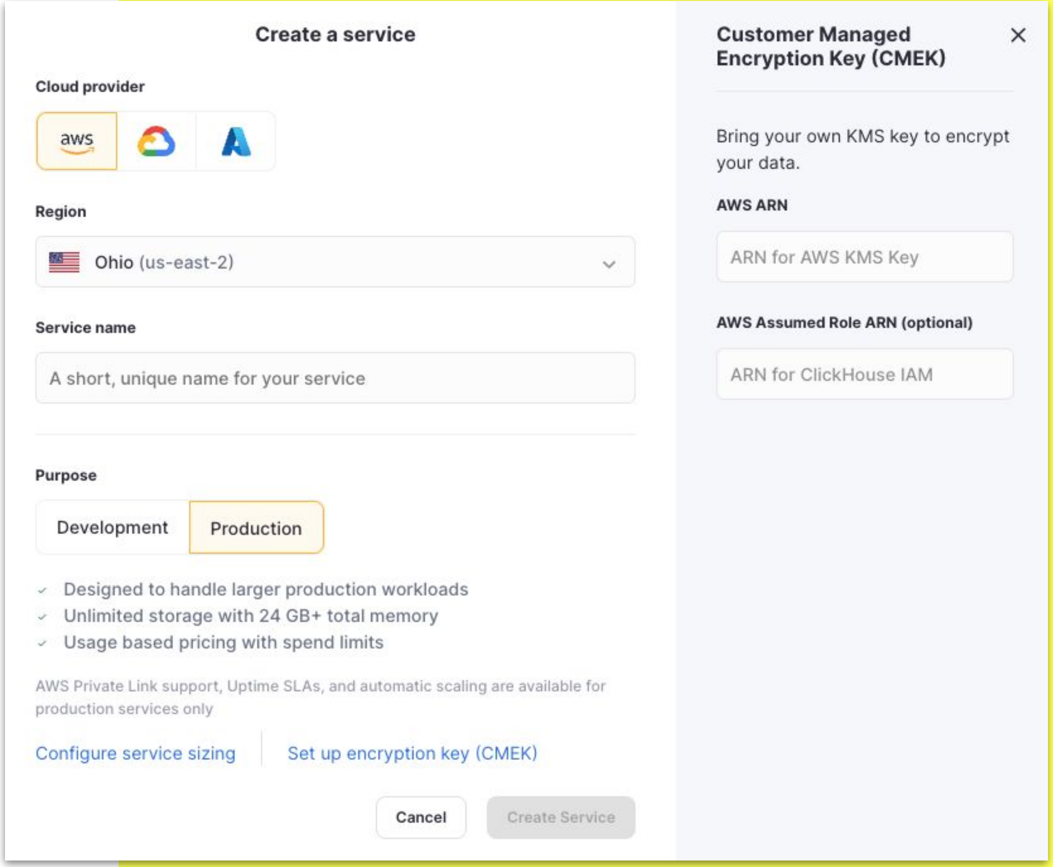
Object Storage

ClickHouse Primary Data Store / Backups

Data Plane

Customer Managed Encryption Key aka BYOK(Bring Your Own Key)

- Support for AWS KMS(Key Management System) with GKS and AKS support coming soon.
- Advanced protection over data at rest by allowing users to manage keys that control encryption/decryption of data
- Making use of envelope encryption technique to enable multi-cloud support & reduce operational overhead



Create a service

Cloud provider: aws

Region: Ohio (us-east-2)

Service name: A short, unique name for your service

Purpose: Development | Production

- ✓ Designed to handle larger production workloads
- ✓ Unlimited storage with 24 GB+ total memory
- ✓ Usage based pricing with spend limits

AWS Private Link support, Uptime SLAs, and automatic scaling are available for production services only

Configure service sizing | Set up encryption key (CMEK)

Cancel | Create Service

Customer Managed Encryption Key (CMEK)

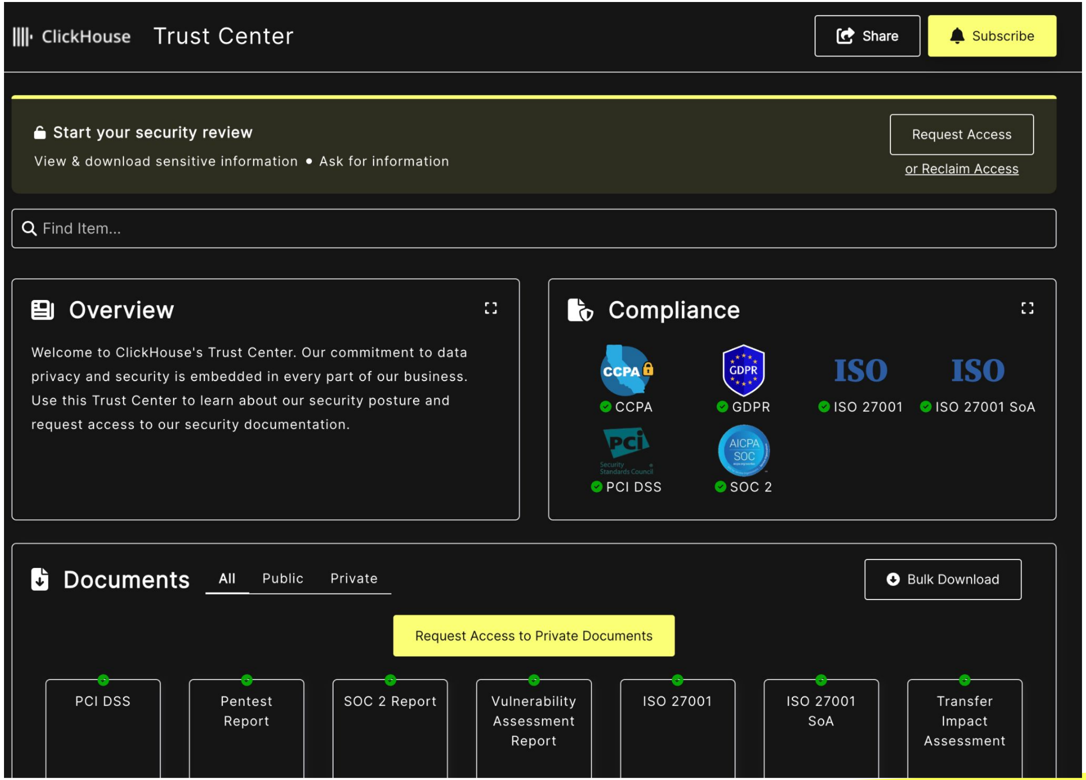
Bring your own KMS key to encrypt your data.

AWS ARN: ARN for AWS KMS Key

AWS Assumed Role ARN (optional): ARN for ClickHouse IAM

Question?

https://trust.clickhouse.com/



Start your security review

View & download sensitive information • Ask for information

Overview

Welcome to ClickHouse's Trust Center. Our commitment to data privacy and security is embedded in every part of our business. Use this Trust Center to learn about our security posture and request access to our security documentation.

Compliance

- ✓ CCPA
- ✓ GDPR
- ✓ ISO 27001
- ✓ ISO 27001 SoA
- ✓ PCI DSS
- ✓ SOC 2

Documents

- PCI DSS
- Pentest Report
- SOC 2 Report
- Vulnerability Assessment Report
- ISO 27001
- ISO 27001 SoA
- Transfer Impact Assessment