Couchbase

Architecture and Administration Basics

Workshop Day 1 - Security

1 | Why Security?

Recent Security Breaches

WannaCry Ransomware
(May 2017)

Wikileaks CIA Vault 7
(March 2017)

CLOUDFLARE

Cloudbleed
(Feb 2017)

verizon

(July 2017)

(Sep 2017)

mongoDB.

(Jan 2017)

DocuSign

(May 2017)

EQUIFAX

(Sept 2017)

Deloitte.

(Sep 2017)

Agenda

- Quick review of security capabilities
- Authentication
  - PAM authentication in Couchbase
- Authorization
  - Role Based Access Control for Applications
- Cryptography
  - Secret Management for Couchbase
- Security Roadmap

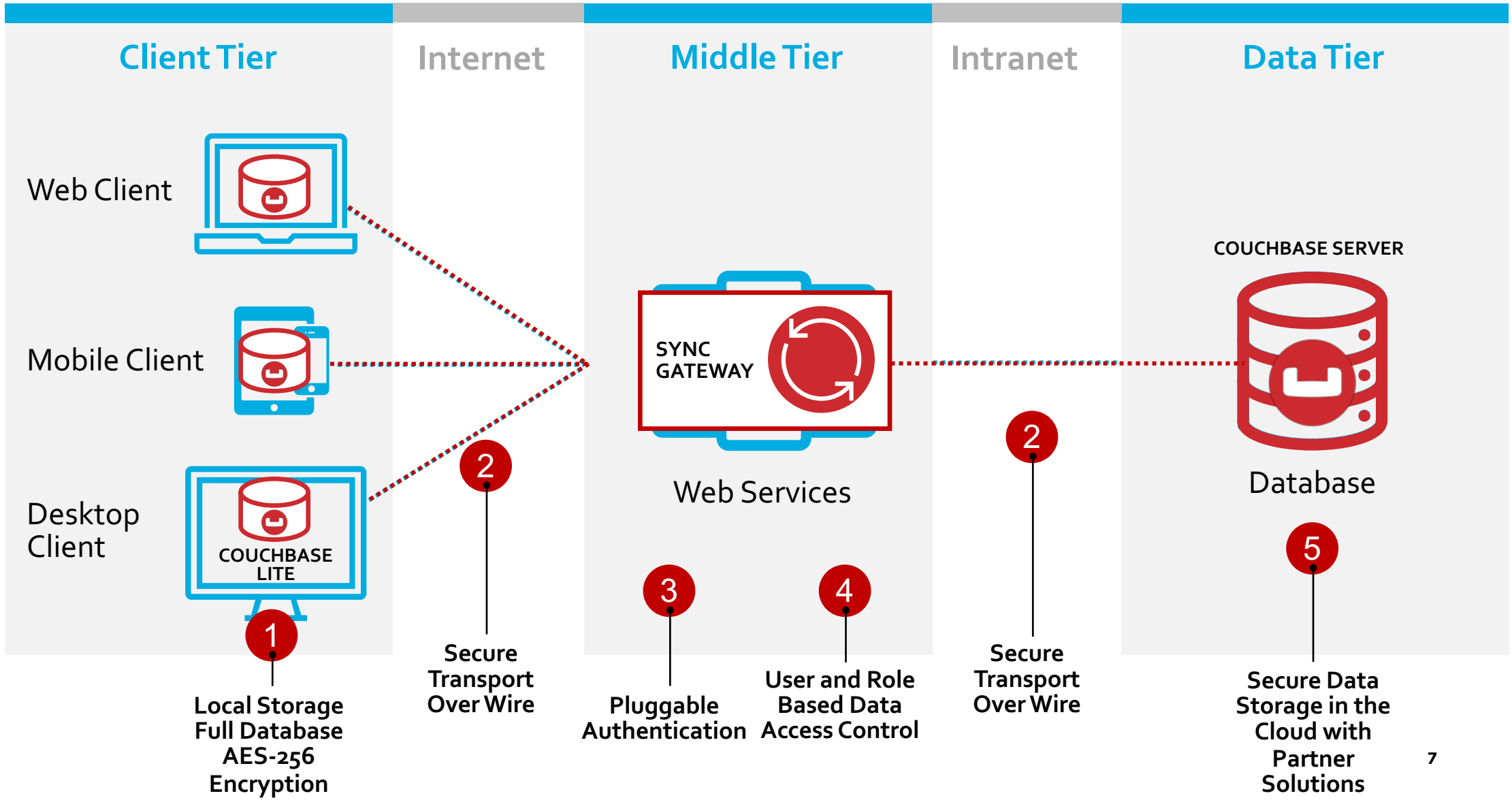
2 | Security Pillars

Security Pillars in Couchbase

Authentication	Authorization	Crypto	Auditing	Operations
App/Data: SASL AuthN Admin: Local or LDAP LDAP Groups (6.5)	Local Admin User Local Read-Only User RBAC for Admins RBAC for Applications	TLS admin access TLS client-server access Secure XDCR X.509 certificates TLS Data-at-rest Encryption* Client Field-level Encryption (5.5) Secret Management	Admin auditing KV & N1QL & Connections (5.5) Log redaction (5.5)	Security management via UI/CLI/REST

* Via third-party partners

Couchbase addresses Security concerns for the full stack



Pluggable Authentication Modules (PAM) in Couchbase 4.6

- Allows UNIX local accounts to authenticate as Couchbase administrators
- Pluggable authentication architecture that is policy driven

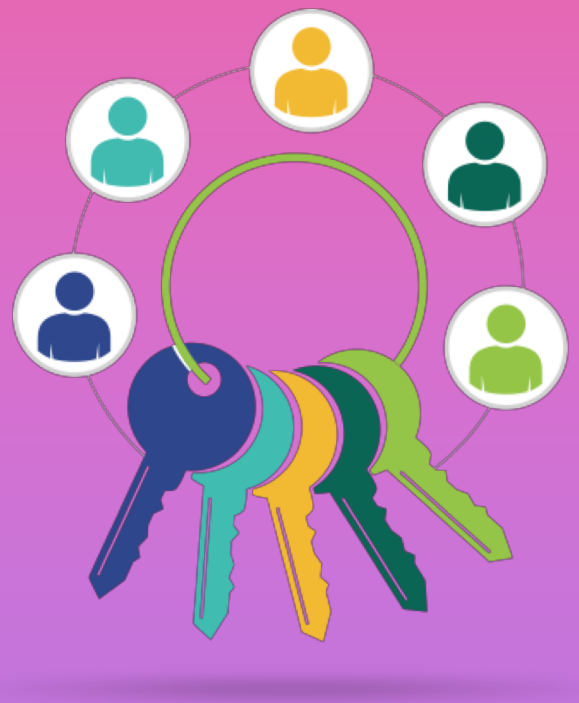
Centralized Management

Centralized and synchronize administrator account management using UNIX user management services

Security Policy Enforcement

Allows configuration of strong security policies such as strong password requirements

Authorization



Authorization for Admins

- Role based access control for Administrators

Authorization for Apps

- RBAC for applications (New)

Role-Based Access Control (RBAC) for Administrators

Role-Based Access Control (RBAC) allows you to specify what each admin can access in couchbase through role membership

Regulatory Compliance

A strong demand for applications to meet standards recommended by regulatory authorities

Segregation of Admin Duties

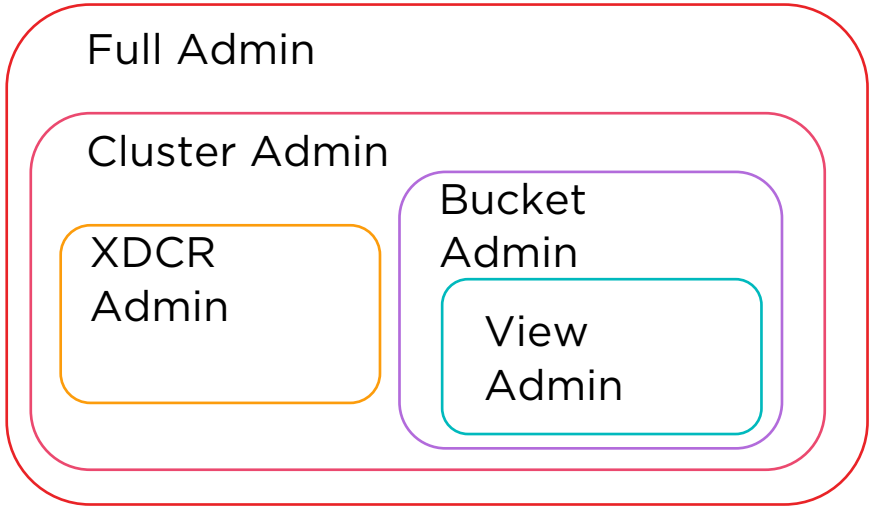
Every admin does not have all the privileges. Depending on the job duties, admins can hold only those privileges that are required.

Security Privilege Separation

Only the full-admin has the privilege to manage security, and his/her actions can be audited just like other administrators.

RBAC for Administrators – How it works

- Administrative users can be mapped to out-of-the-box roles
- Roles pre-defined with permissions for specific resources
  - Full Admin
  - Cluster Admin
  - Bucket Admin
  - View Admin
  - XDCR Admin
- Can work with internal and external users



3 | RBAC for Applications

Role-Based Access Control (RBAC) for Applications

- Meet regulatory compliance requirements for data users and applications
- Simplified access control management for data and admin users across the cluster

Regulatory Compliance

A strong demand for applications to meet standards recommended by regulatory authorities

Segregation of User Duties

Depending on the job duties, users can hold only those privileges that are required

Locking Down Services

Depending on what the service is needed for, only those roles can be assigned

RBAC Security Model

Privilege

A set of actions on a given resource

Eg. Read documents on "foo" bucket

Role

A fixed grouping of privileges that defines the access given

User

User is a human user or service

Action: an operation *eg. read, write, read metadata*

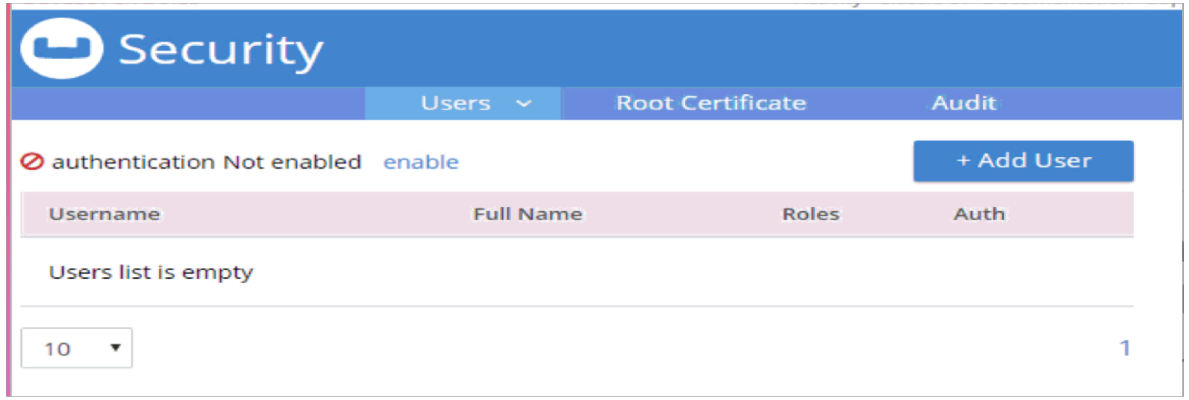
Resource: some system object that an action can be performed on. *eg. bucket, index, etc.*

- NIST Model
- Scalable users accounts
- Fixed out-of-the-box data roles in 5.0
- 1:N User-to-role mapping
- Roles can be applied for specific buckets / across all buckets [*]

User Management

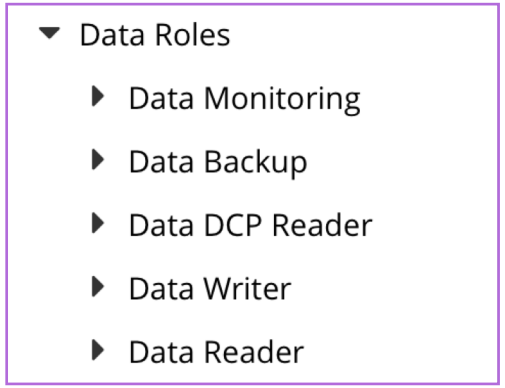
Flexible User Management

- Internal and External authorization support
- Unique identities for data users and services
- REST and CLI configurable
- Seamless upgrades without application changes
- Scalable



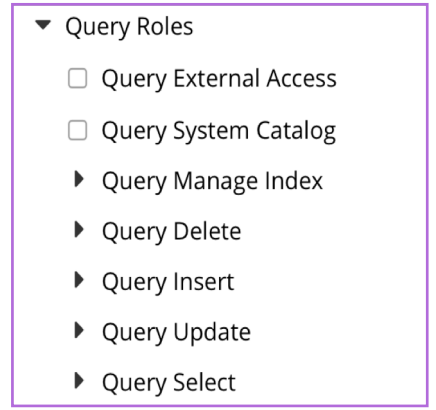
New Roles for Data Service – RBAC in 5.0

Data Reader	• Read data from bucket
Data Writer	• Write data to bucket
Data DCP Reader	• Can read the DCP stream from bucket
Data Backup	• Can backup/restore the bucket
Data Monitoring	• Can monitor statistics for bucket



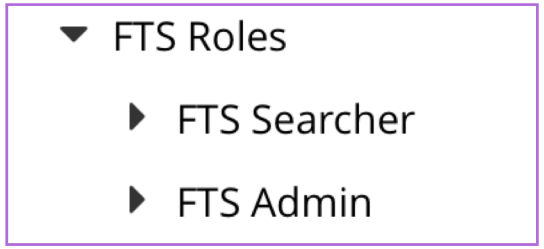
New Roles for Query Service – RBAC in 5.0

Query Select	• Can execute SELECT N1QL statement for bucket
Query Update	• Can execute UPDATE N1QL statement for bucket
Query Insert	• Can execute INSERT N1QL statement for bucket
Query Delete	• Can execute DELETE N1QL statement for bucket
Query Manage Index	• Can execute index management statements for bucket
Query System Catalog	• Can query system tables for bucket
Query External Access	• Can execute N1QL CURL statement



New Roles for Full Text Search Service – RBAC in 5.0

FTS Admin	• Can administer FTS service
FTS Searcher	• Can execute search queries for a bucket



Bucket Roles – RBAC in 5.0

So, can I get a role that gives me the application behavior similar to pre-5.0?

Bucket Full Access	• Full Read/Write access over the bucket
Bucket Admin	• Full Read/Write access over the bucket, and ability to change bucket settings

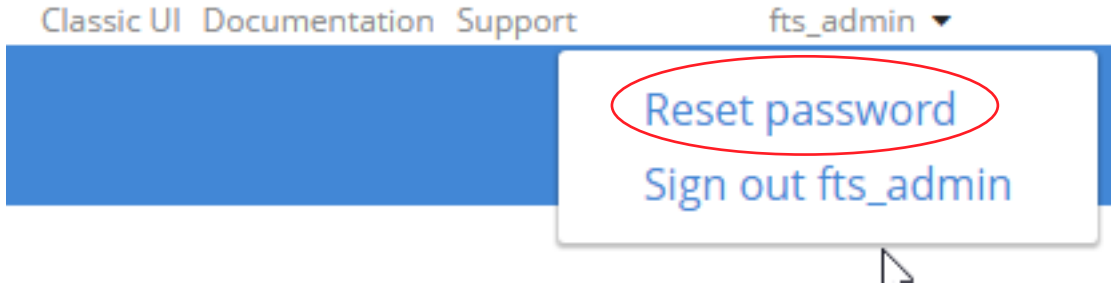
Password Policy and Rotation

Default Policy

```
{
  "enforceDigits": false,
  "enforceLowercase": false,
  "enforceSpecialChars": false,
  "enforceUppercase": false,
  "minLength": 6
}
```

Policy and Rotation

- Simple password policy rules enforced when initially set or rotated
- Policy can be set using REST or CLI
- Password can be reset using UI, REST or CLI



Role Assignment – Using REST and CLI

Using REST

```
curl -X PUT
http://localhost:8091/settings/rbac/users/local/don-data-user
 -u Administrator:password -d "roles=data_reader[travel-sample]" -d "password=donpassword”
```

Using CLI

```
./couchbase-cli user-manage --set --rbac-username don-n1ql-user --rbac-password donpassword --auth-domain local --roles "data_reader[*], query_select[*]" -c http://localhost:8091 -u Administrator -p password
```

GRANT /REVOKE statements in N1QL for RBAC

GRANT ROLE

```
GRANT ROLE data_reader(`*`) to don
```

REVOKE ROLE

```
REVOKE ROLE data_reader(`*`) from don
```

New system tables for RBAC

system:applicable_roles (provides user-role mappings)

```
SELECT * FROM system:applicable_roles
WHERE bucket_name="travel-sample"
```

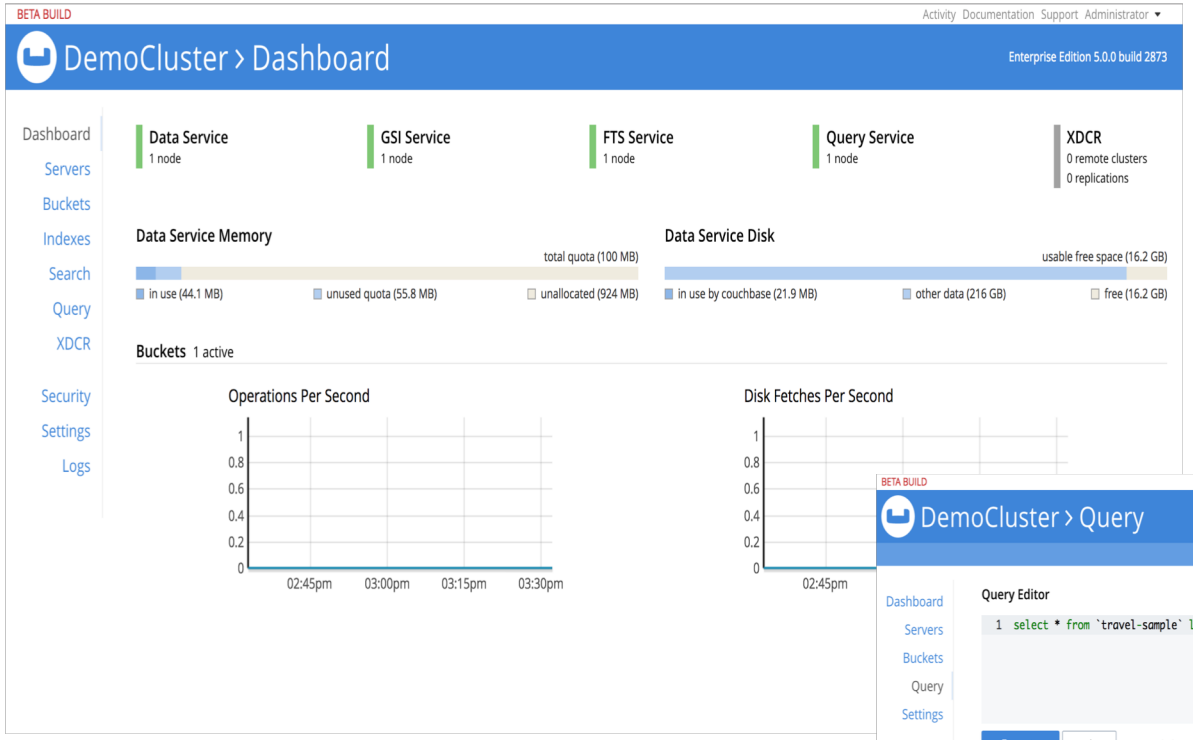
system:user_info (provides full user information)

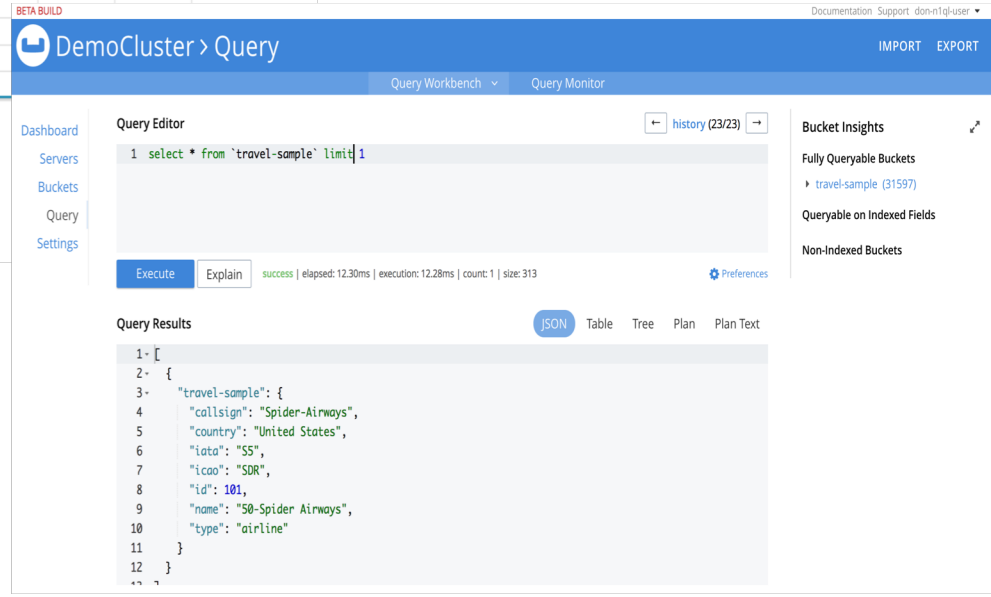
```
SELECT * FROM system:user_info
```

Web Console For Administrators and Developers

Who gets to log into web console ?

1. Administrators (Any administrator role)
2. Developers (Users who have one ore more query role)





3 | Encryption

Encryption

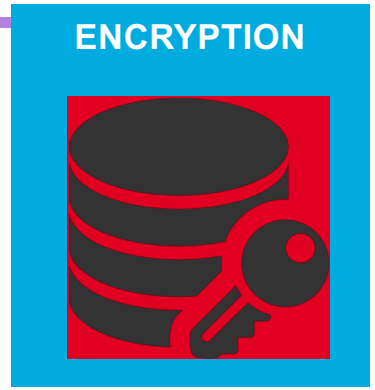
On-the-wire Encryption

- TLS between client and server
- TLS between datacenters using secure XDCR
- X.509 CA Certificates for trusted encryption between client and server

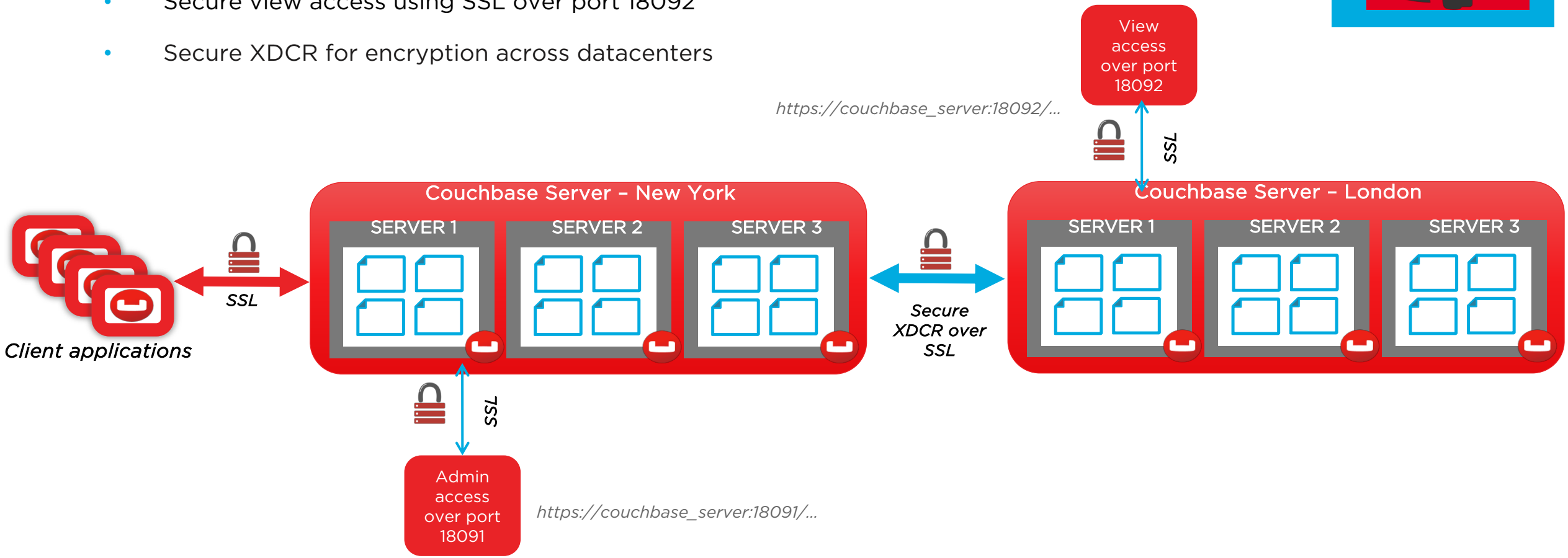
On-Disk Encryption

- Volume and application level encryption through our trusted 3rd partners (Vormetric, Protegrity, SafeNet)
- FIPS 140-2 compliant

Couchbase encryption overview (In Motion)

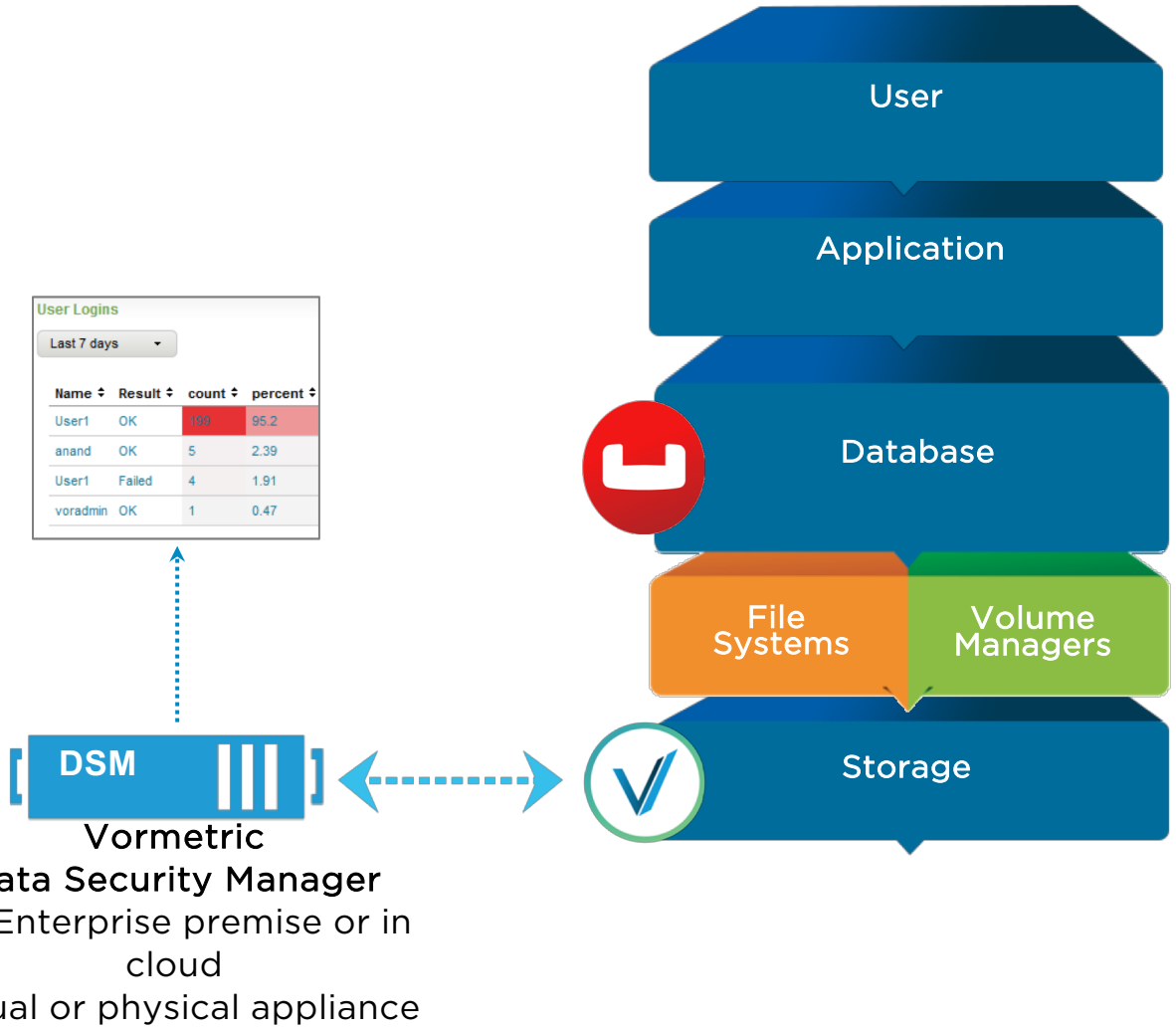


- Data-in-motion encryption
  - Client-server communication can be encrypted using SSL
  - Secure admin access using SSL over port 18091
  - Secure view access using SSL over port 18092
  - Secure XDCR for encryption across datacenters



Couchbase encryption overview

- Transparent data-at-rest encryption solution



Vormetric
Data Security Manager
on Enterprise premise or in cloud
virtual or physical appliance

ENCRYPTION

Secure Personally Identifiable Information

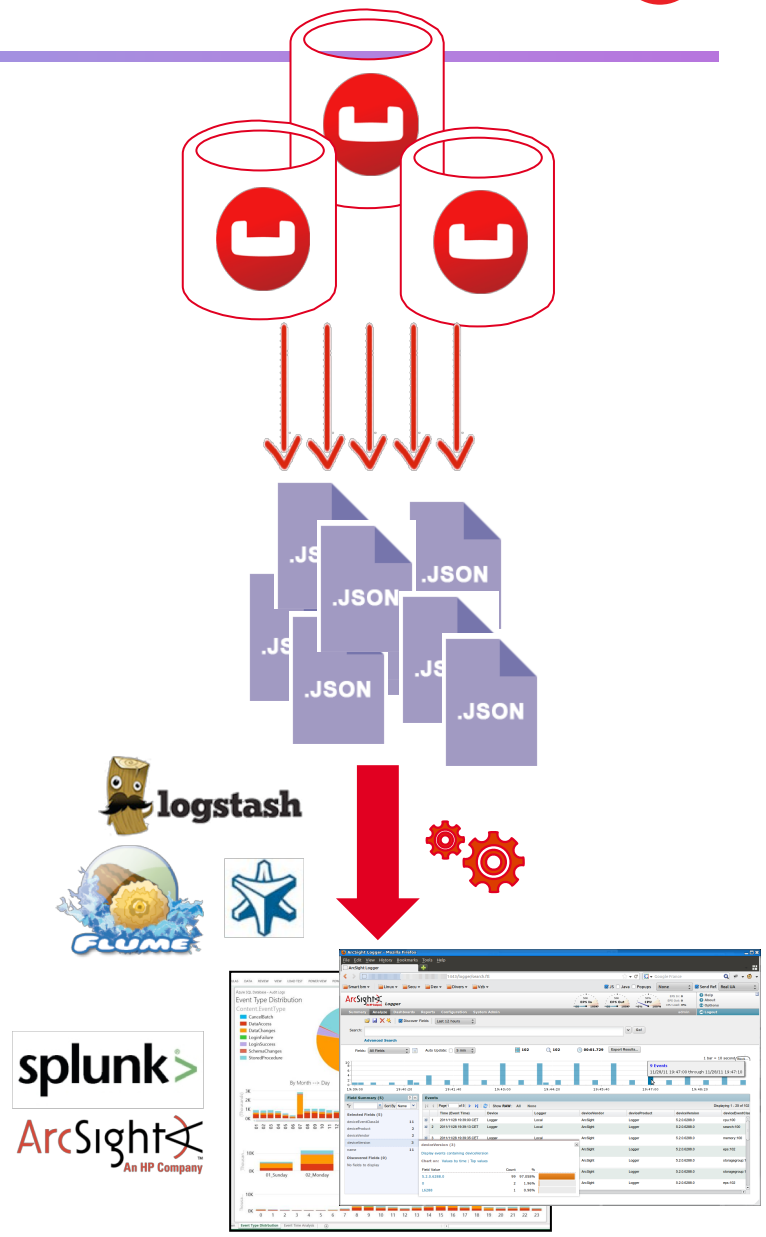
- User profile information
- Login Credentials
- IP Addresses

- Centrally manage keys and policy
- Virtual and physical appliance
- High-availability with cluster
- Multi-tenant and strong separation of duties
- Proven 10,000+ device and key management scale
- Web, CLI, API Interfaces
- FIPS 140-2 certified

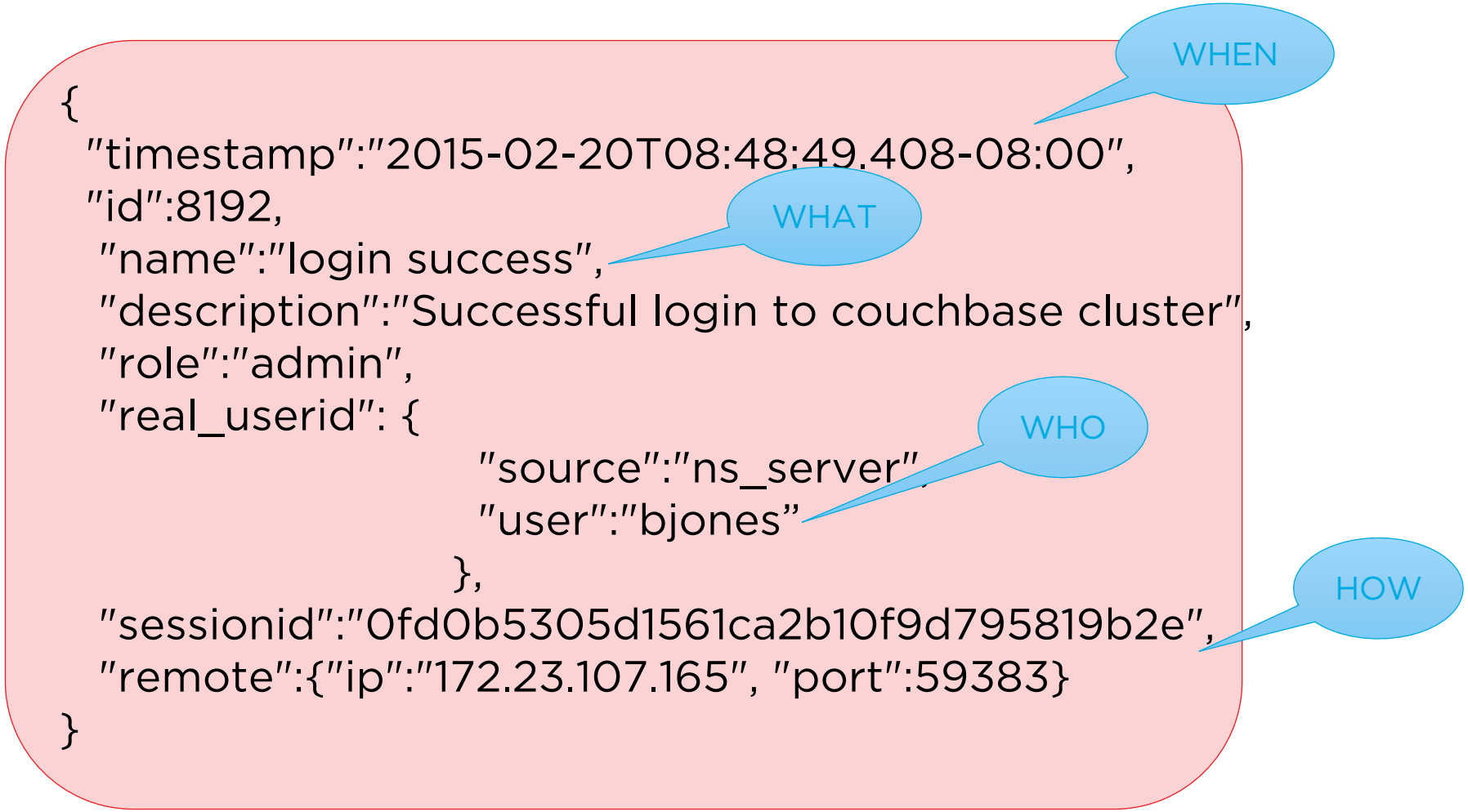
4 | Auditing

Admin Auditing in Couchbase

- Rich audit events
  - Over 25+ different, detailed admin audit events
  - Auditing for tools including backup
- Configurable auditing
  - Configurable file target
  - Support for time based log rotation and audit filtering
- Easy integration
  - JSON format allows for easy integration with downstream systems using flume, logstash, and syslogd



Auditing a successful login



5 | Roadmap

Couchbase Security Feature Roadmap – At-a-glance

CB 5.0

- **X.509** certificate authentication support for data service
- **Role-based access controls** (RBAC) for users and applications
- **Auditing** for administrative operations
- **SSL/TLS** support for admin access, client-server access, and XDCR
- **Encryption** (third-party): data at rest, field level

CB 5.5

- **X.509** certificate authentication support for all services and SDKs
- Compatibility with **OpenSSL 1.1** series
- **Enhanced auditing** for all admin and non-admin access, including auditing of query statements
- **Field-level encryption** in SDKs to protect sensitive user data
- **Log redaction** to prevent leaking sensitive user data
- **OWASP** certification scans

CB 6.5+

- **X.509** certificate authentication support for analytics service
- **LDAP Group** support
- **Auditing** for KV data access
- Ability to disable **unencrypted access** for security compliance
- **Node-Node Encryption** for security compliance

Thank you

Couchbase