Couchbase

Security

1 Why Security ?

Recent Security Breaches

WannaCry Ransomware
(May 2019)

Wikileaks CIA Vault 7
(March 2019)

CLOUDFLARE

Cloudbleed
(Feb 2019)

verizon

(July 2019)

U.S. SECURITIES AND EXCHANGE COMMISSION MCMXXXIV

(Sep 2019)

mongoDB

(Jan 2019)

DocuSign

(May 2019)

EQUIFAX

(Sept 2019)

Deloitte.

(Sep 2019)

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**

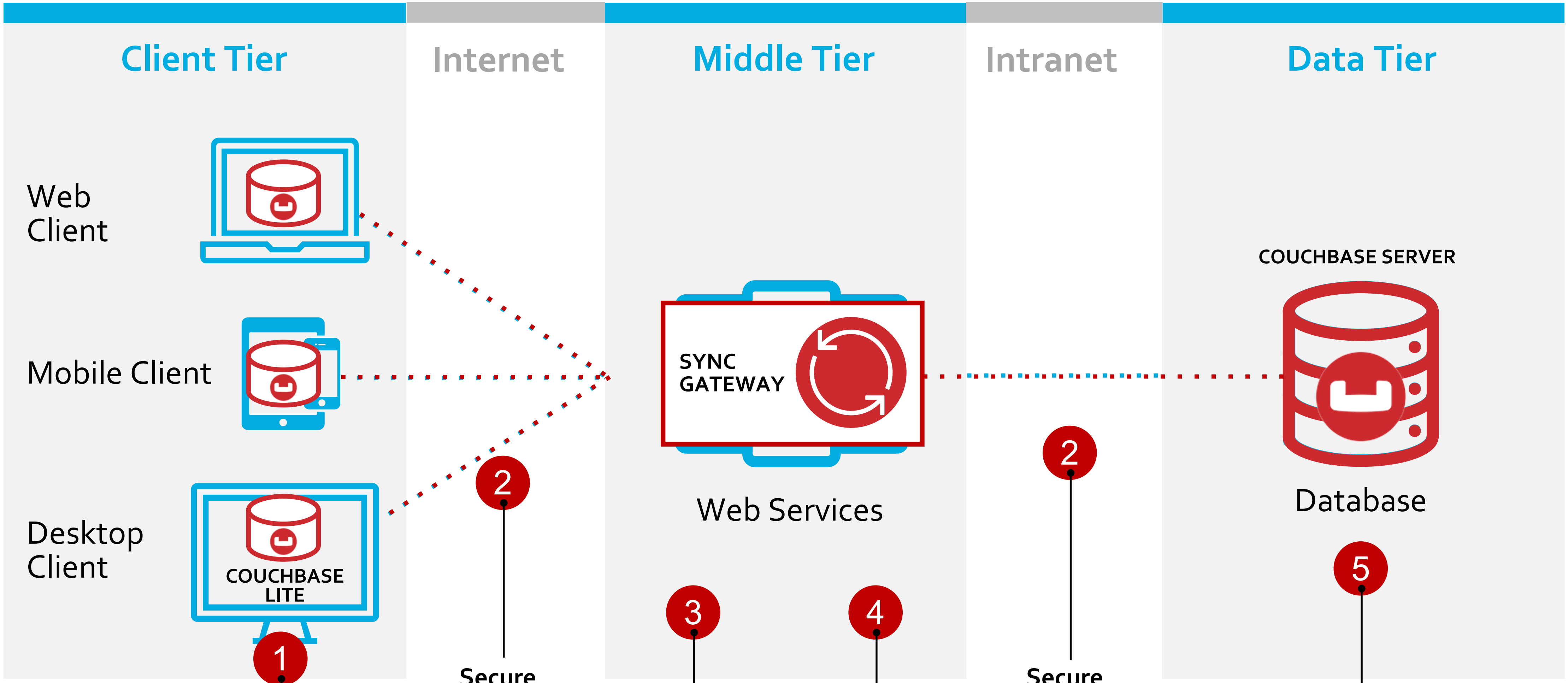
2 Security Pillars

Security Pillars in Couchbase

Authentication	Authorization	Crypto	Auditing	Operations
App/Data: SASL AuthN Admin: Local or LDAP Users or LDAP Groups PAM Authentication	Local Admin User Local Read-Only Admin RBAC for Admins RBAC for Applications (since 5.0)	TLS admin access TLS client-server access Secure XDCR X.509 certificates for TLS Data-at-rest Encryption* Field-level Encryption (since 5.5) Secret Management Support for Configurable TLS Cipher Suites	Admin auditing API request auditing (since 5.5) N1QL auditing (since 5.5)	Security management via UI/CLI/REST

* Via third-party partners

Couchbase addresses Security concerns for the full stack



Client Tier

Internet

Middle Tier

Intranet

Data Tier

Web Client

Mobile Client

Desktop Client

COUCHBASE LITE

SYNC GATEWAY

Web Services

COUCHBASE SERVER

Database

1 Local Storage Full Database AES-256 Encryption

2 Secure Transport Over Wire

3 Pluggable Authentication

4 User and Role Based Data Access Control

2 Secure Transport Over Wire

5 Secure Data Storage in the Cloud with Partner Solutions

7

Timeline of Security Features in Couchbase Server

Feature	2.x	3.x	4.0.x	4.5.x	4.6.x	5.0.x	5.5.x	6.x	7.0.0
CRAM-MD5 support for SASL authentication	■	■	■	■	■	■	■	■	■
XDCR TLS Network Encryption	■	■	■	■	■	■	■	■	■
Email Alerting Mechanism	■	■	■	■	■	■	■	■	■
Secure TLS Encrypted Admin Console		■	■	■	■	■	■	■	■
Secure TLS Encrypted REST API		■	■	■	■	■	■	■	■
Secure TLS Encrypted Client SDK Access		■	■	■	■	■	■	■	■
Saslauthd LDAP Auth Integration			■	■	■	■	■	■	■
Administrative Audit Event Logging			■	■	■	■	■	■	■
RBAC for Administrator Authorization				■	■	■	■	■	■
X.509 certificates for TLS network encryption with custom CA				■	■	■	■	■	■
Pluggable Authentication Modules (PAM) Auth					■	■	■	■	■
Secrets Management at rest encryption					■	■	■	■	■
RBAC for All Users, replacing bucket passwords.						■	■	■	■
Admin defined user password policy						■	■	■	■
X.509 certificate authentication support for all services and SDKs							■	■	■
Enhanced auditing for all admin and non-admin access, including query statements and data access							■	■	■
Field-level encryption in SDKs to protect sensitive user data							■	■	■
Log redaction to prevent leaking sensitive user data							■	■	■
OWASP certification scans							■	■	■
User Group Management								■	■
LDAP Group support								■	■
Node-Node Encryption for security compliance								■	■
Centralized Encryption Cipher Management								■	■
Non-Root Install for security controlled environments								■	■
Backup to encrypted S3 cloud storage								■	■
Collections RBAC for fine-grained control of access to data									■
Default minimum TLS protocol upgraded to version 1.2									■
Added TLS encryption protocol version 1.3 support									■
Couchbase certification for LUKS at-rest data encryption									■
Additional Admin RBAC roles for LDAP, Eventing and Backup									■
Increased Auditing Capabilities that include IP address and port.									■

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

Demo: Setting Up PAM Authentication

- Setting up PAM-based authentication, creating an external user

  https://docs.couchbase.com/server/6.0/manage/manage-security/configure-pam.html

Confidential and Proprietary. Do not distribute without Couchbase consent. © Couchbase 2018. All rights reserved.

3 Role Based Access Control (RBAC)

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.

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

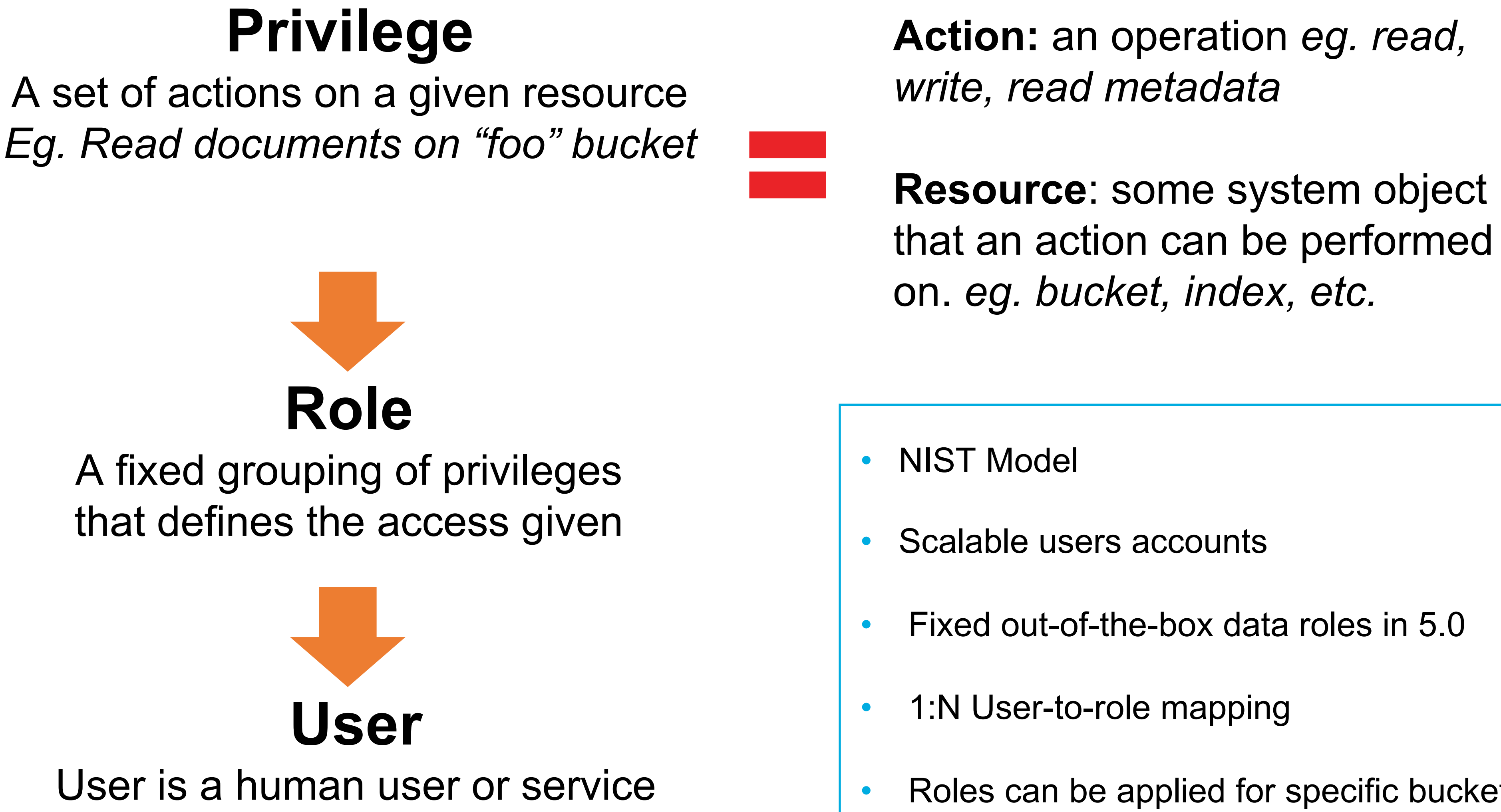
Segregation of User Duties

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

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

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

Role

A fixed grouping of privileges that defines the access given

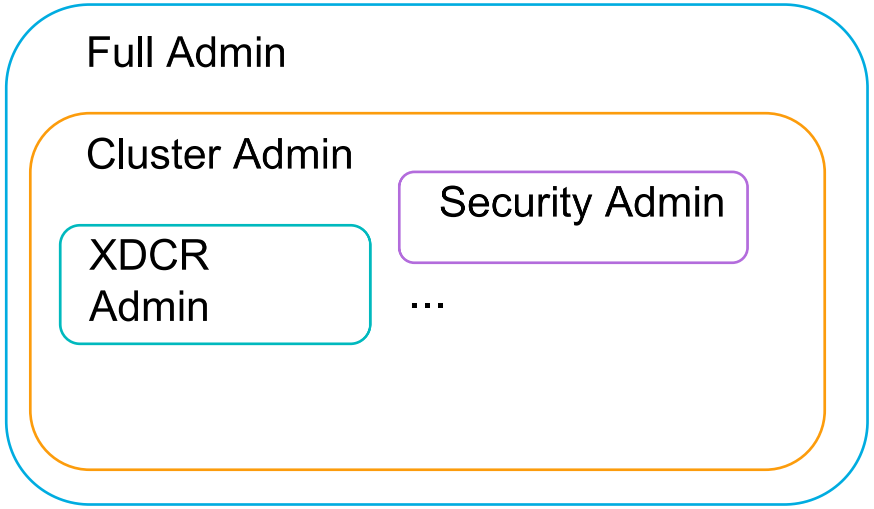
User

User is a human user or service

- 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 [*]

Global Administrator Roles

- Administrative users can be mapped to out-of-the-box roles
- Roles pre-defined with permissions for specific resources
  - Full Admin
  - Cluster Admin
  - Security Admin
  - Read-Only Admin
  - XDCR Admin
  - Query cURL Access
  - Query System Catalog
  - Analytics Reader
  - Analytics Admin

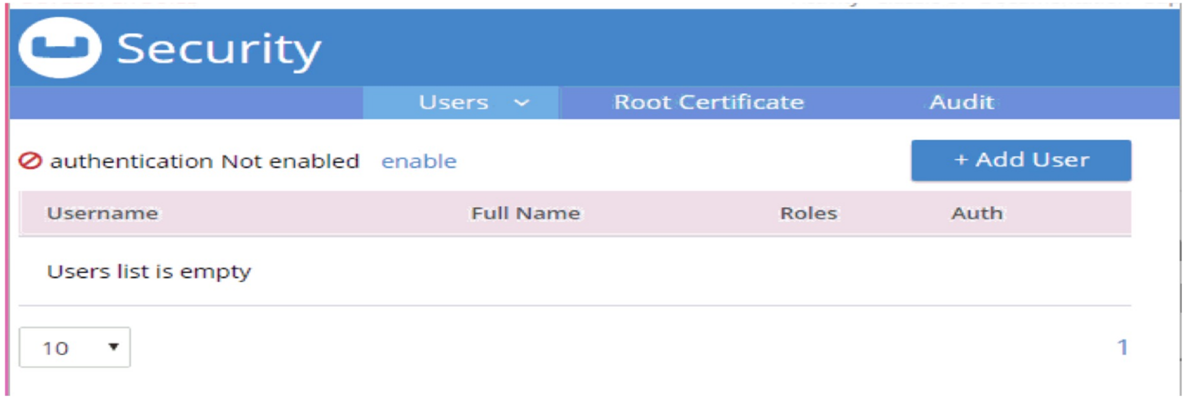


- Can work with internal and external users

Bucket Level RBAC

- All Buckets
  - Bucket Admin - Full Read/Write access over the bucket, and ability to change bucket settings
  - Application Access
  - XDCR Inbound
  - Sync Gateway
  - Data Service (Data Reader, Data Writer, DCP Reader, Data Backup & Restore, Data Monitor)
  - Views (Admin, Reader)
  - Query and Index Service (Select, Update, Insert, Delete, Manage Index)
  - Search Service (Admin, Reader)
  - Analytics Service (Manager, Select)

Flexible User Management



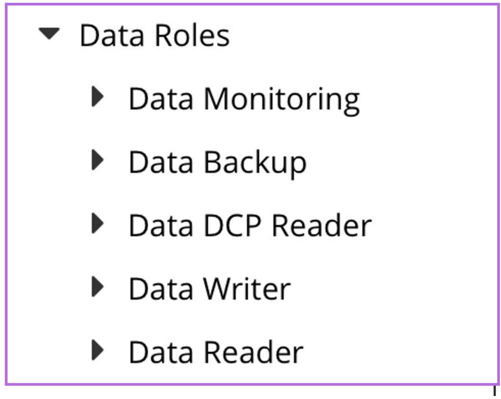
⊘ authentication Not enabled enable

Username	Full Name	Roles	Auth
Users list is empty			

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

Data Service – RBAC

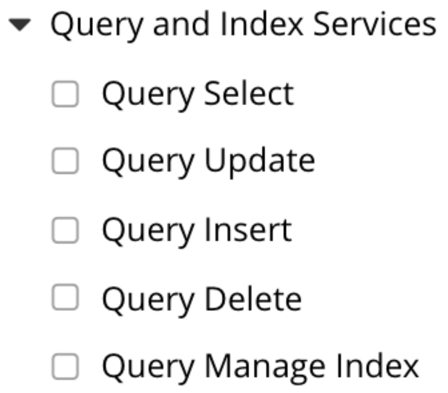
Data Reader	• Read data from bucket
Data Writer	• Write data to bucket
Data DCP Reader	• Can read the DCP stream from bucket
Data Backup	• Can backup/restore the bucket
Data Monitoring	• Can monitor statistics for bucket



- Data Roles
  - Data Monitoring
  - Data Backup
  - Data DCP Reader
  - Data Writer
  - Data Reader

Query Service – RBAC

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

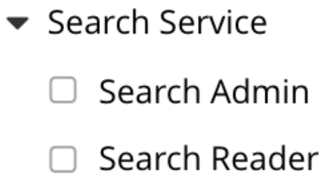


▾ Query and Index Services

- □ Query Select
- □ Query Update
- □ Query Insert
- □ Query Delete
- □ Query Manage Index

Search Service – RBAC

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



▾ Search Service

□ Search Admin

□ Search Reader

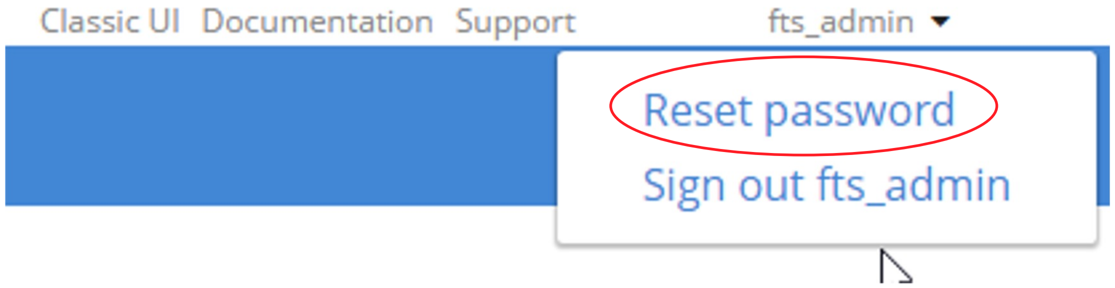
Password Policy and Rotation

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

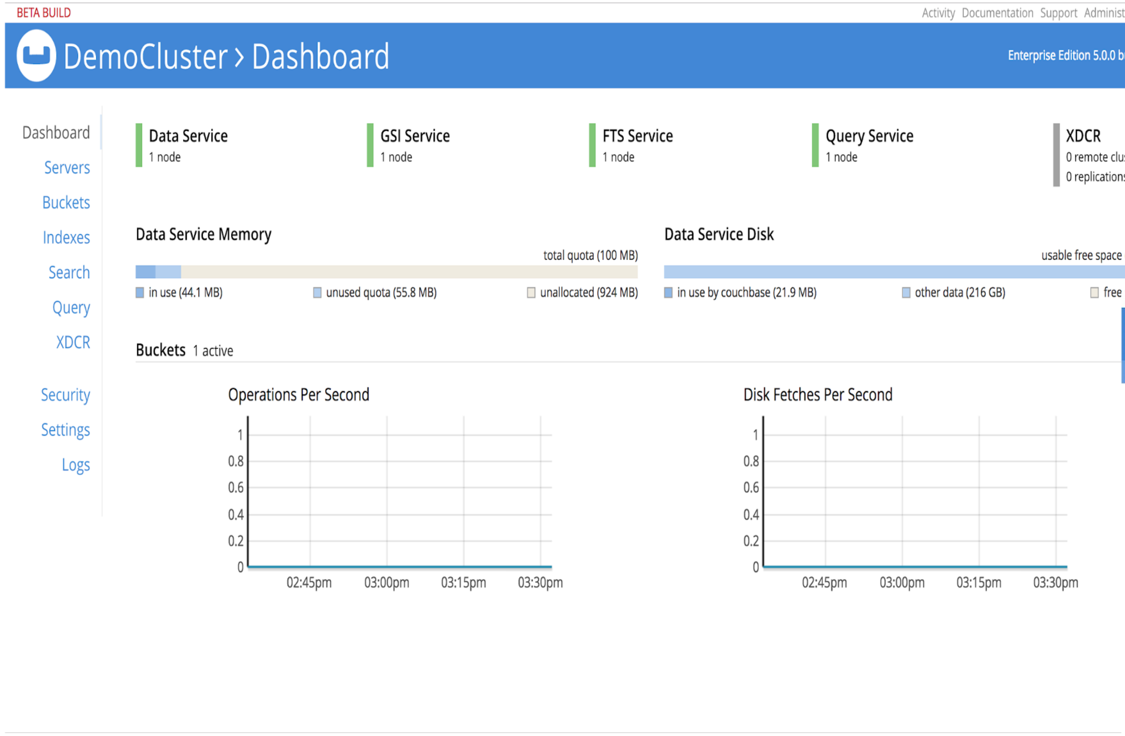
GRANT ROLE data_reader(`*`) to don

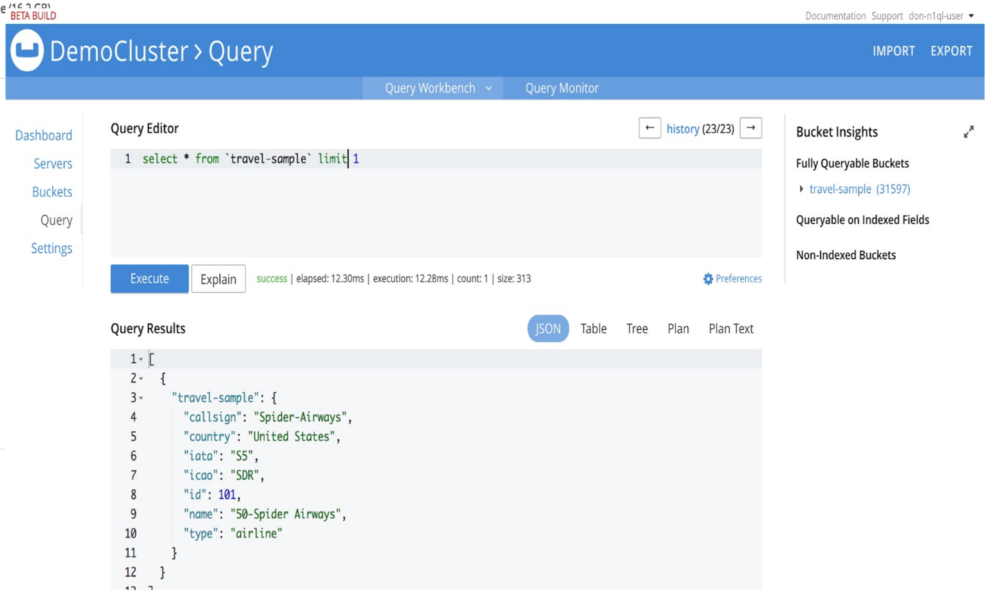
REVOKE ROLE

REVOKE ROLE data_reader(`*`) from don

Who gets to log into web console ?

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





```
select * from `travel-sample` limit 1
```

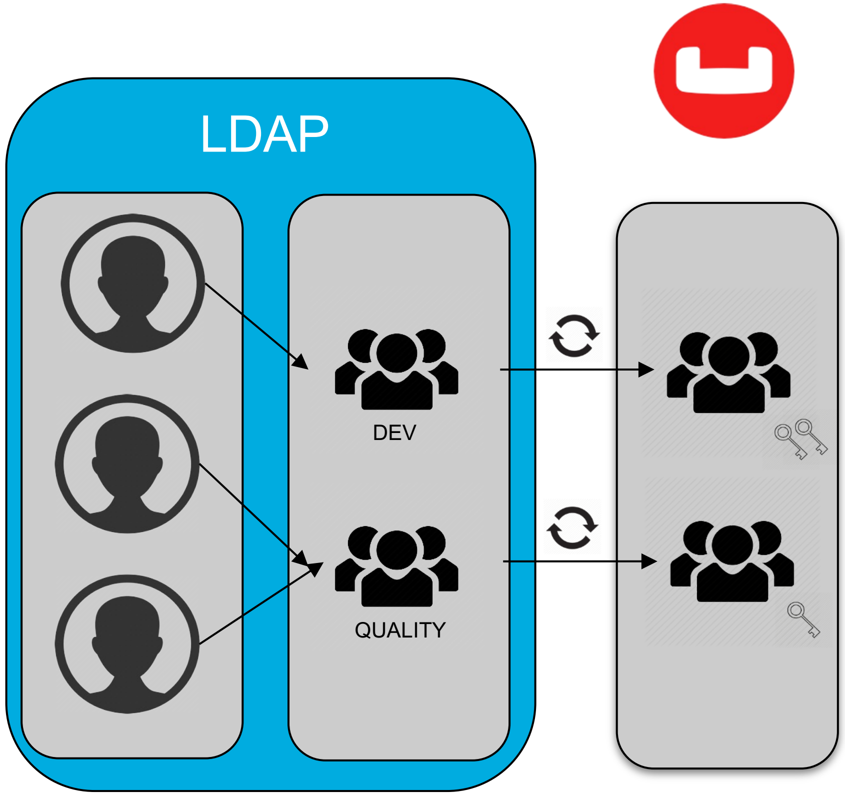
success | elapsed: 12.30ms | execution: 12.28ms | count: 1 | size: 313

```
[
  {
    "travel-sample": {
      "callsign": "Spider-Airways",
      "country": "United States",
      "iata": "S5",
      "icao": "SDR",
      "id": 101,
      "name": "50-Spider Airways",
      "type": "airline"
    }
  }
```

Security - Native LDAP Group Support

LDAP Group support simplifies LDAP integration and includes local group support

- LDAP Group Support enables easy integration with existing LDAP servers, and RBAC user management
- Native LDAP works without SASLauthd support, lighting up LDAP for Couchbase on Windows
- LDAP users and groups reside externally in LDAP
- Couchbase Groups map and sync to LDAP groups
- RBAC privileges assigned to Couchbase groups



4 Encryption

On-the-wire Encryption

- TLS between client and server
- TLS between nodes within a cluster
- TLS between datacenters using secure XDCR
- X.509 CA Certificates for trusted encryption between client and server
- Field-level Encryption

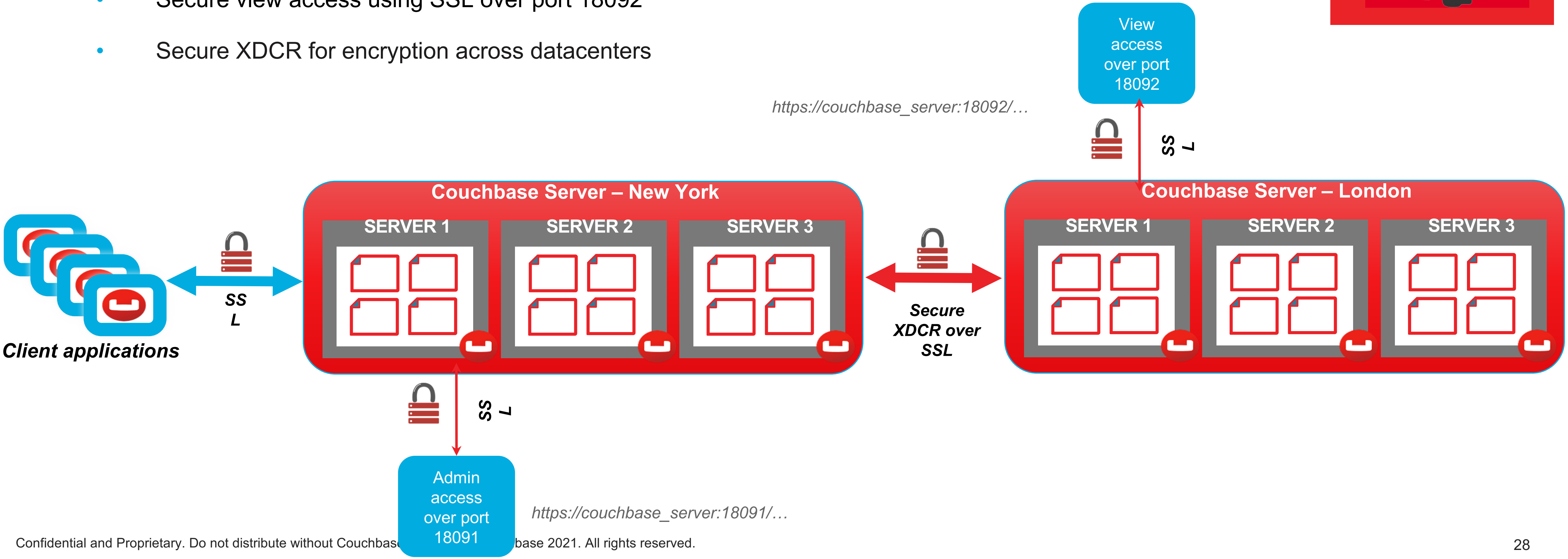
On-Disk Encryption

- Volume and application level encryption through trusted partners (Vormetric, Protegrity, SafeNet)
- LUKS
- FIPS 140-2 compliant
- Field-level Encryption

Couchbase encryption overview (In Motion)

ENCRYPTION

- **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


View access over port 18092
https://couchbase_server:18092/…
SS
L
Couchbase Server – New York
SERVER 1
SERVER 2
SERVER 3
Couchbase Server – London
SERVER 1
SERVER 2
SERVER 3
SS
L
Client applications
Secure XDCR over SSL
SS
L
Admin access over port 18091
https://couchbase_server:18091/…

Security - TLS Cipher Settings

TLS Cipher settings with centralized management and persistent settings to manage TLS security easily

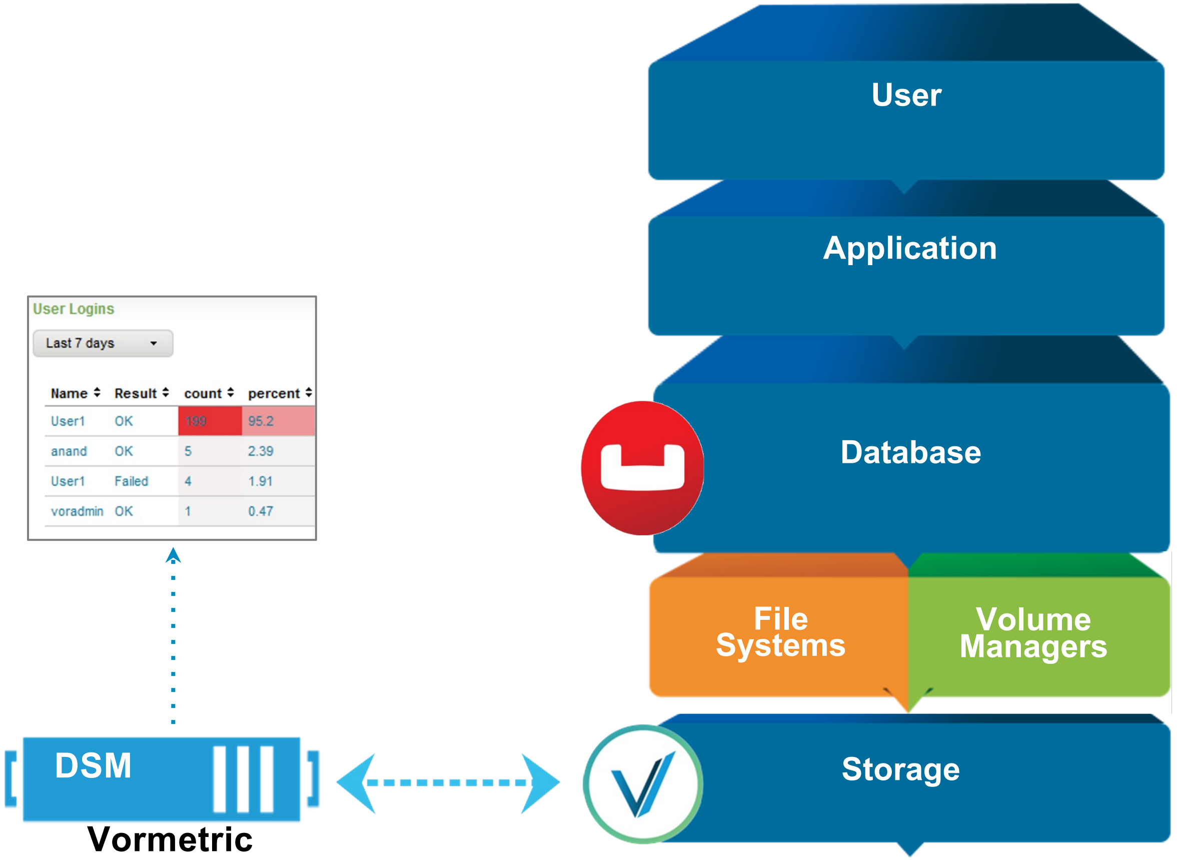
- Centralized management of TLS cipher settings:
  - Get the set of supported ciphers supported across the different Couchbase services
  - Set the list of ciphers to be used consistently across services or per service
  - Persistent TLS cipher settings across cluster, node restarts and upgrades

```
curl localhost:8091/settings/security \
        -u Administrator:password \
            -d 'cipherSuites="[TLS_RSA_WITH_AES_128_CBC_SHA, \
                           TLS_RSA_WITH_AES_256_CBC_SHA, ...]"'
```

Couchbase encryption overview

ENCRYPTION

- Transparent data-at-rest encryption solution



User Logins

Last 7 days

Name	Result	count	percent
User1	OK	199	95.2
anand	OK	5	2.39
User1	Failed	4	1.91
voradmin	OK	1	0.47

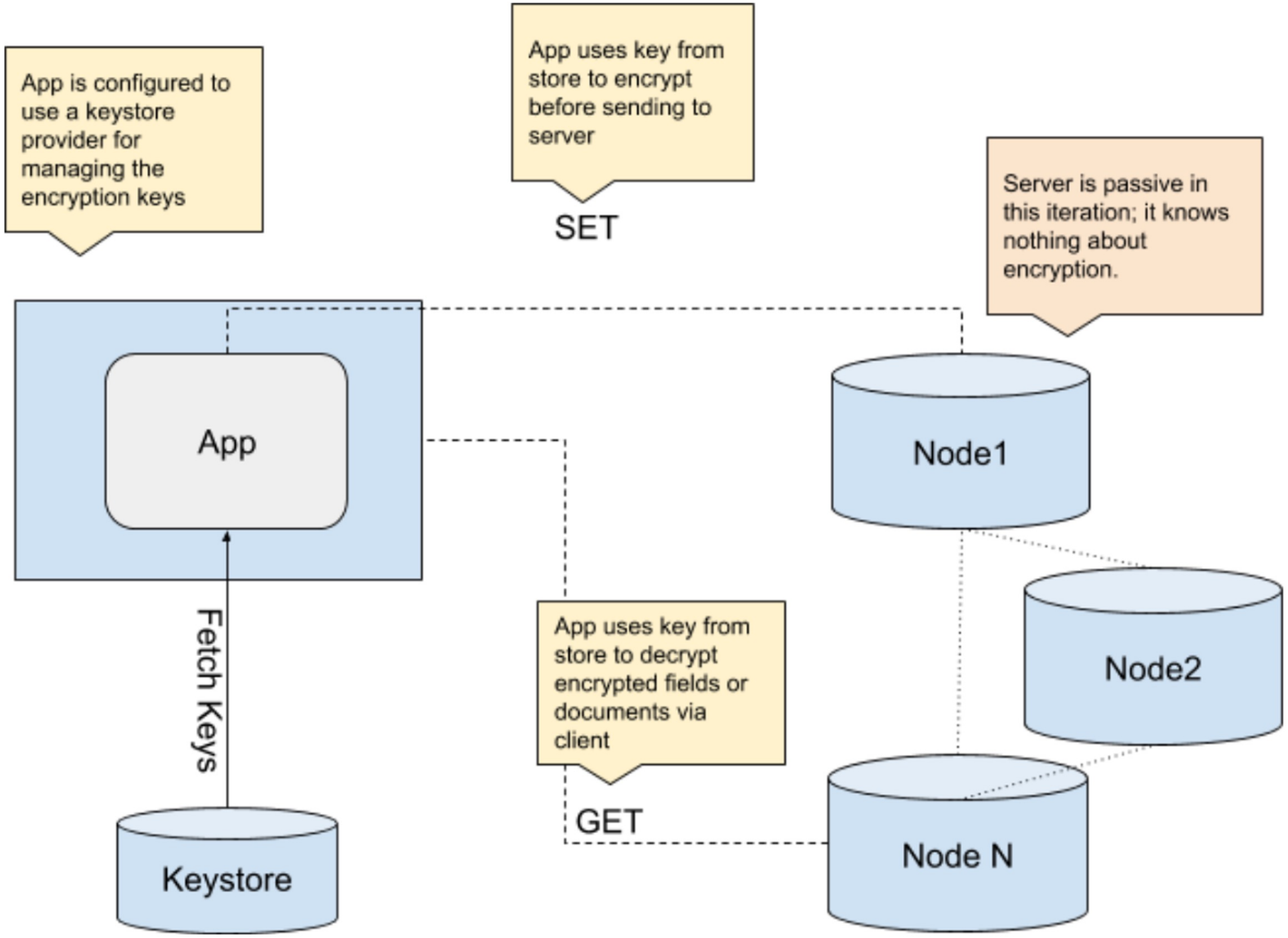
Vormetric
Data Security Manager
on Enterprise premise or in cloud
virtual or physical appliance

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

Field Level Encryption (since CB5.5)



App is configured to use a keystore provider for managing the encryption keys

App uses key from store to encrypt before sending to server

Server is passive in this iteration; it knows nothing about encryption.

App uses key from store to decrypt encrypted fields or documents via client

Field Level Encryption: Example

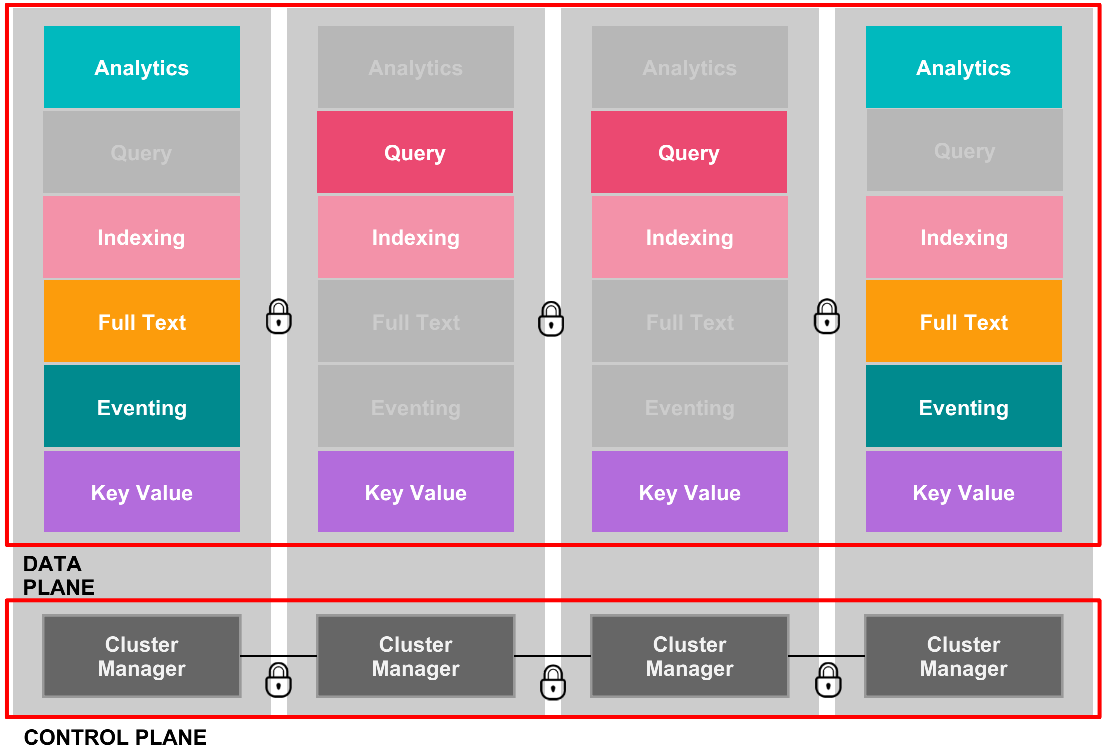
```
{
"message":"The old grey goose jumped over the wrickety gate.",
“recipient”: “jeffry.morris@couchbase.com”
}
```

```
{
  "__crypt_message": {
    "alg": "RSA-2048-OAEP-SHA1",
    "kid": "MyPublicKeyName",
    "ciphertext":
"iX2MXbUlief8Xxk4DYysivEsUXeoiFBLkm4/EC7E9vRnGikDOiuaWIILTJU/
oNKeVNIWPzfN6r/uLEpttp+BLC0DswdxLkA3ONeO85TDdHaHmrJ3dJQ7q
gDFe35K6MbTEPXE98f1wL2vOL70xJxW+3KsgdcYYYqg8VNw2U9eKVC2
Iv4DS19I/r+6I+O8EGvBaa0FidezgF7CzgdXpGmG20cA0D8yCmmGoW8oq
7KWoq0PNaKsb9JOYfOYi13bxpPOIbyI003qLb5b7y1qVms8KDZ0+nk7Xnn
5OYFmBHQDyJ39nuibEMKNMIA2ZNICvfFqE1dU3iqqZYyS7OTukFBO2g=
="
  },
“recipient”: “jeffry.morris@couchbase.com”
}
```

Security - Node-to-Node Encryption

Node-to-node certificate-based encryption greatly and easily improves security within a cluster.

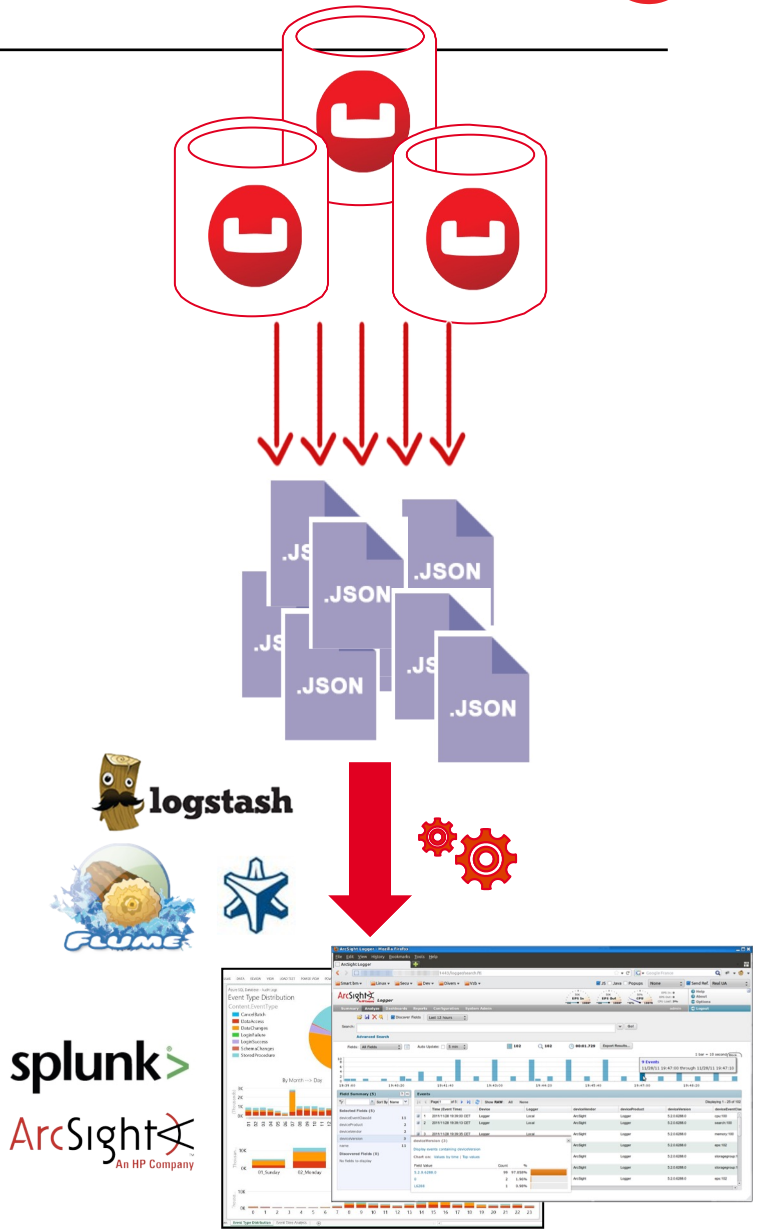
- On-the-wire encryption for data and control plane, across multiple nodes
- Certificate-based encryption management using existing node and cluster certificates
- Encryption can be controlled and enabled just for the control plane separately
- Using IPSec is not required
- Simple to setup and manage



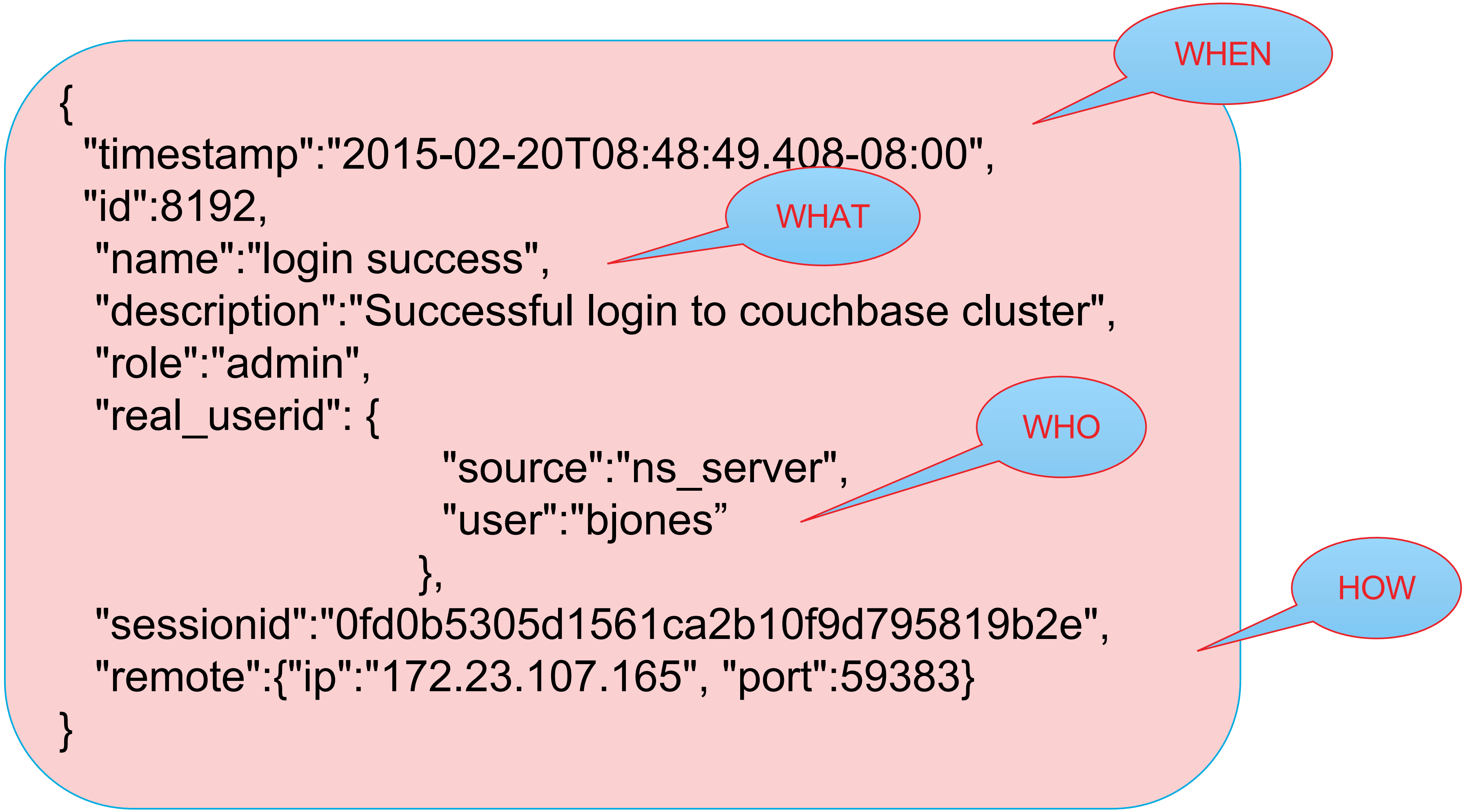
5 Auditing

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



```
{
  "timestamp":"2015-02-20T08:48:49.408-08:00",
  "id":8192,
   "name":"login success",
   "description":"Successful login to couchbase cluster",
   "role":"admin",
   "real_userid": {
                              "source":"ns_server",
                              "user":"bjones”
                            },
   "sessionid":"0fd0b5305d1561ca2b10f9d795819b2e",
   "remote":{"ip":"172.23.107.165", "port":59383}
}
```

Security Checklist - Administration

Minimum Recommendation

The internal full administrator account uses a strong and unique password.

External users are configured with roles according to the principle of least privilege.

Monitoring systems are configured to use the Read-Only Admin account.

Admin auditing is configured and externally monitored.

XDCR replications that traverse untrusted networks are secured with SSL/TLS.

Administrative access is secured with SSL/TLS.

Administrative UI access over HTTP is disabled.

CLI access uses environment variables to pass admin usernames and passwords.

The installed Couchbase Server version is up-to-date and the same on all nodes.

Security Checklist - Administration

Situational Controls

Cluster and per-node X.509 certificates have been configured.

Configure the correct level of Ciphers.

Email alerts are configured with TLS enabled.

The LDAP repository for external users has a defined security policy for strong password requirements, password rotation, and auto lockouts.

6 Security Checklist

Security Checklist- Data & Applications

Minimum Recommendations

The "default" bucket and all sample buckets are not present.

All buckets are configured using Role-based access controls

Role-based access control passwords are stored using the language's secrets management facility

The Couchbase client SDK versions are up-to-date

Situational Controls

Application-to-Couchbase connections are secured with SSL/TLS.

Sensitive data are stored hashed, tokenized, or encrypted (field-level encryption Couchbase 5.5+).

Confidential and Proprietary. Do not distribute without Couchbase consent. © Couchbase 2019. All rights reserved.

Security Checklist - Network

Minimum Recommendations

All Couchbase Server nodes are deployed behind a firewall and access to Couchbase ports are

restricted to only necessary internal networks.

Access to node-to-client ports is restricted to internal application servers.

External access to cluster administration ports requires a VPN connection and/or jump box.

Consider using specific ACLs as a part of your Network Configuration to secure access via policies.

External access to only XDCR HTTPS ports is permitted to specific networks to support cluster-to-cluster replication.

Situational Controls

Node-to-node connections are secured with IPSEC.

The Couchbase cluster is isolated to its own VLAN.

Security Checklist- Server & Operating Systems

Minimum Recommendation

Proper physical security for Couchbase servers and backup storage is maintained.

The operating system is up to date with the latest patches. Review your security updates specific to your OS.

The operating system is hardened per the OS vendor's best practices.

Privileged access for managing Couchbase services is controlled via sudo and the sudoers log is externally monitored. Sudo access is only required for installing the Couchbase package, starting/stopping/status the Couchbase service, and running cbcollect_info is required.

Access to backup repositories is restricted.

Situational Controls

Encryption at rest is configured through one of the supported options.

Essentials Checklist

- ❑ Transport Layer Encrypted?(Web, Client, XDCR)
- ❑ Disk volumes encrypted?
- ❑ Disable non-https ports outside Couchbase cluster ?
- ❑ X.509 Certificates for TLS, Data,N1QL ?
- ❑ Optional Client-side field-level encryption setup ?
- ❑ Log redactions enabled?
- ❑ Password Policy & Rotation in place?
- ❑ Auditing (Admin, Data & Other Services) enabled ?
- ❑ Session Timeouts configured?
- ❑ Secret Management configured?

Confidential and Proprietary. Do not distribute without Couchbase consent. © Couchbase 2019. All rights reserved.

Couchbase

Thank You