



Couchbase

Architecture and Administration Basics

Security



1

Why Security?



Recent Security Breaches



WannaCry Ransomware
(May 2017)



Cloudbleed
(Feb 2017)



(July 2017)



Wikileaks CIA Vault 7
(March 2017)



(Sep 2017)



(Jan 2017)



(May 2017)



(Sept 2017)



(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



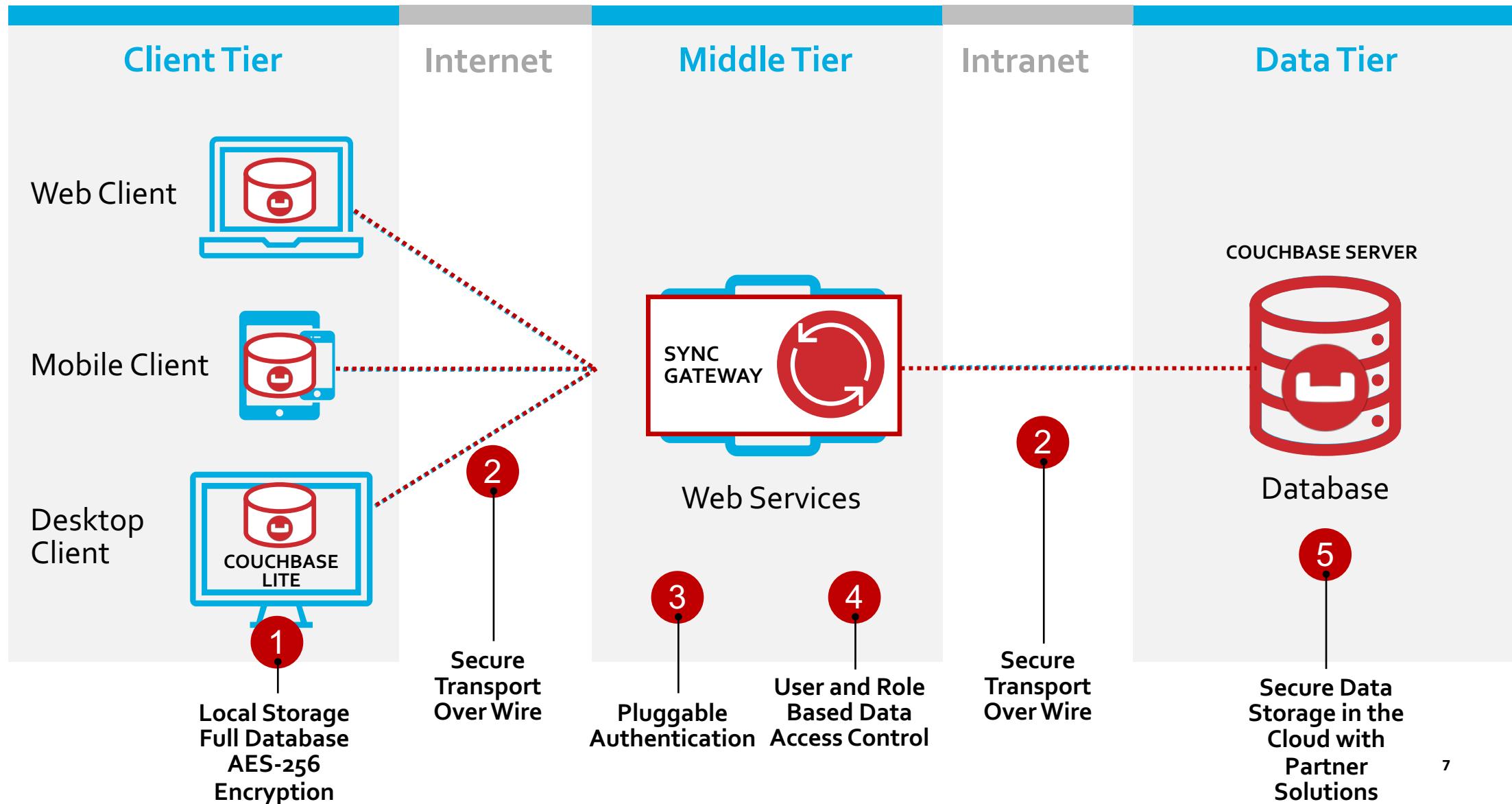
Security Pillars in Couchbase

Authentication	Authorization	Crypto	Auditing	Operations
App/Data: SASL AuthN Admin: Local or LDAP or 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	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





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>



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*



Role

A fixed grouping of privileges that defines the access given



User

User is a human user or service

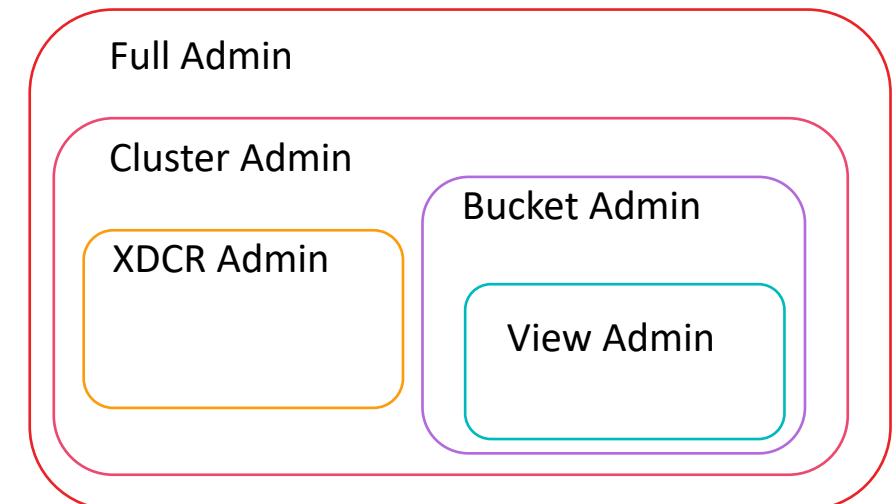
Resource: some system object that an action can be performed on. *eg. bucket, index, etc.*

- 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 [*]



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
 - Bucket Admin
 - View Admin
 - XDCR Admin
- Can work with internal and external users





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

The screenshot shows a user management interface with the following elements:

- Header:** Security, with tabs for Users, Root Certificate, and Audit.
- Status Bar:** authentication Not enabled, with an enable button.
- Action Buttons:** + Add User.
- Table Headers:** Username, Full Name, Roles, Auth.
- Table Content:** Users list is empty.
- Pagination:** 10, 1.



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

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



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

- ▼ Query Roles
- Query External Access
 - Query System Catalog
 - ▶ Query Manage Index
 - ▶ Query Delete
 - ▶ Query Insert
 - ▶ Query Update
 - ▶ Query Select



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

▼ FTS Roles

- ▶ FTS Searcher
- ▶ FTS Admin



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

▼ Bucket Roles

- ▶ Bucket Full Access
- ▶ Bucket Admin



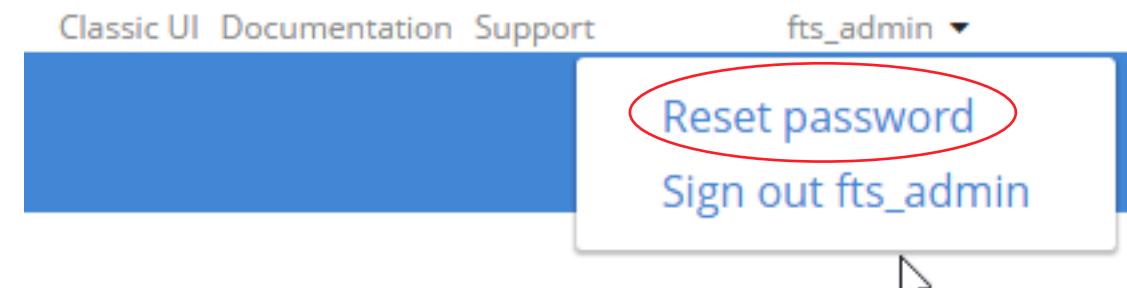
Password Policy and Rotation

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)

The screenshot displays two main panels of the DemoCluster web console.

Dashboard Panel: This panel shows cluster status and performance metrics. It includes sections for Data Service, GSI Service, FTS Service, Query Service, and XDCR. Below these are memory and disk usage charts. A graph titled "Operations Per Second" shows activity over time, and another titled "Disk Fetches Per Second" also shows activity over time.

Query Panel: This panel shows the "Query Editor" where a query is being typed: `1 select * from `travel-sample` limit 1`. Below it, the "Query Results" section displays the JSON output of the query:

```
1- [
2-   {
3-     "travel-sample": {
4-       "callsign": "Spider-Airways",
5-       "country": "United States",
6-       "iota": "SS",
7-       "icao": "SDR",
8-       "id": 101,
9-       "name": "S0-Spider Airways",
10-      "type": "airline"
11-    }
12-  }
```



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
- Field-level Encryption

On-Disk Encryption

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

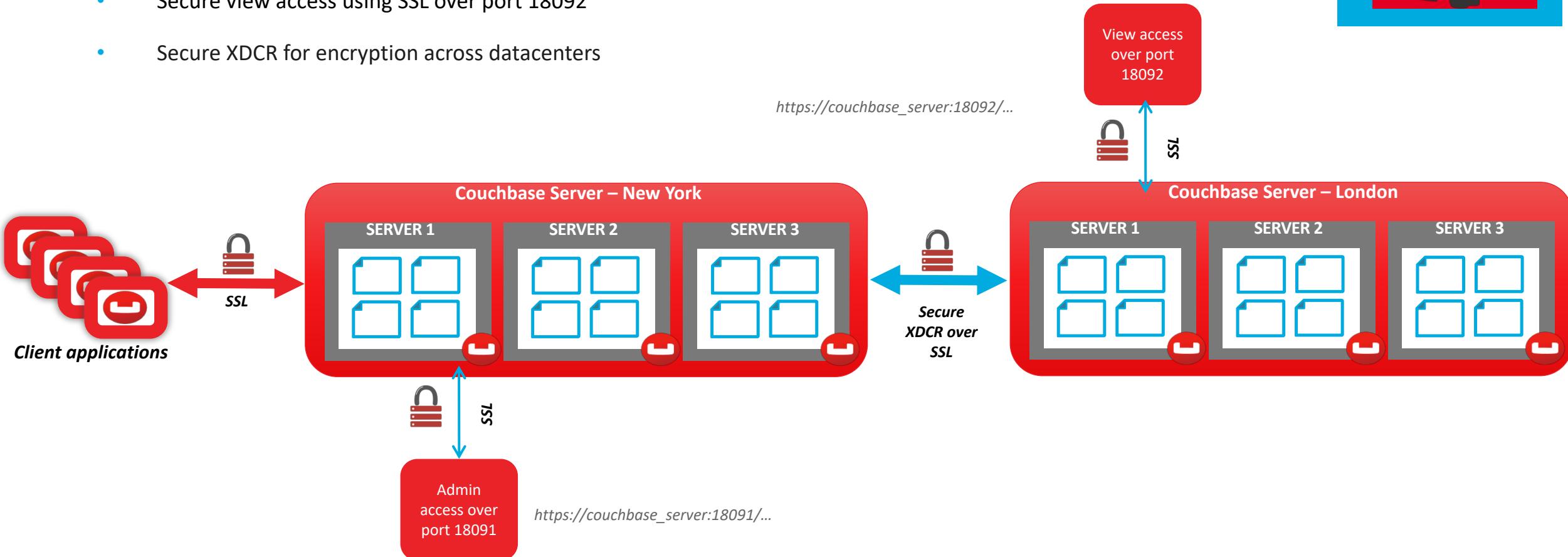


Couchbase encryption overview (In Motion)

- **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

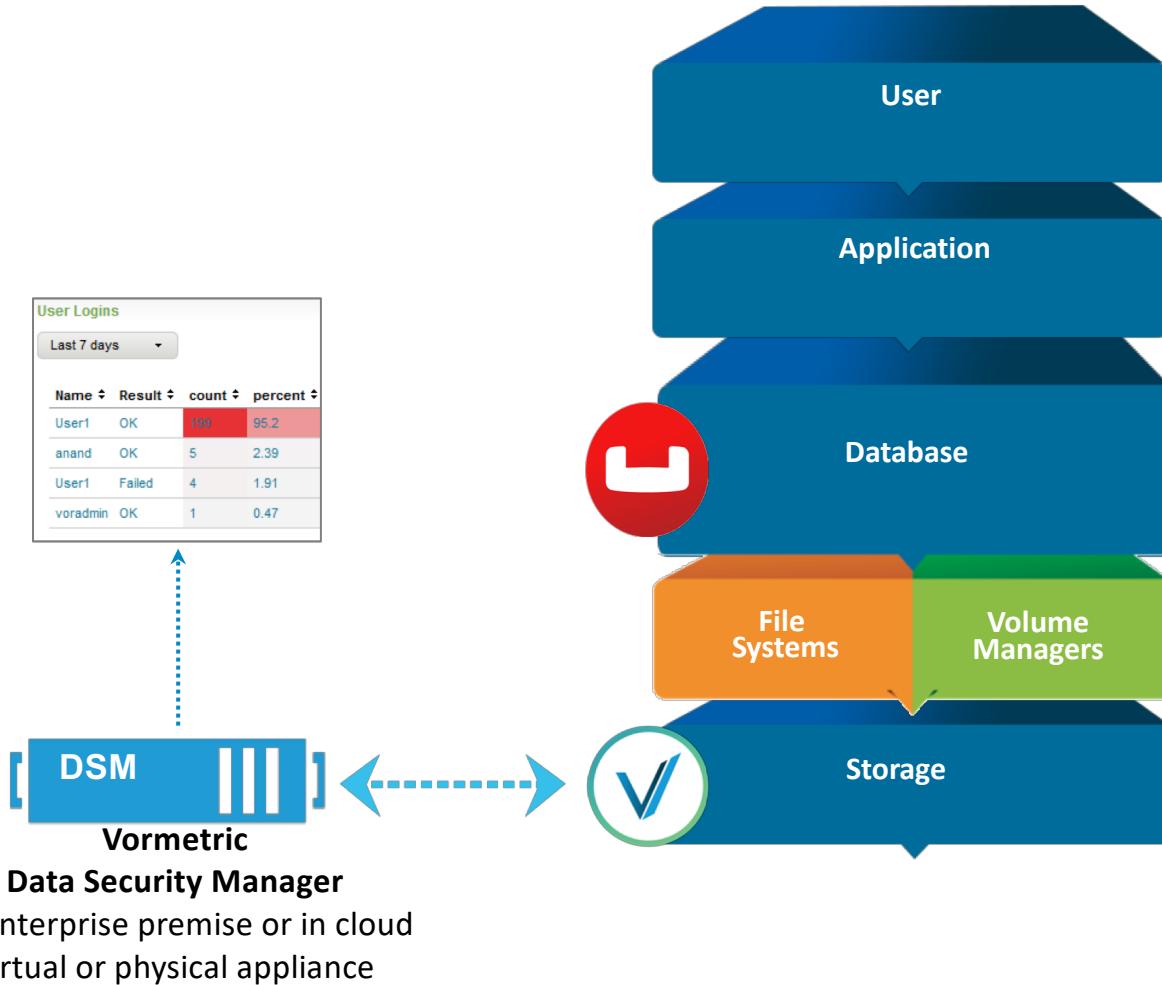
ENCRYPTION





Couchbase encryption overview

- Transparent data-at-rest encryption solution



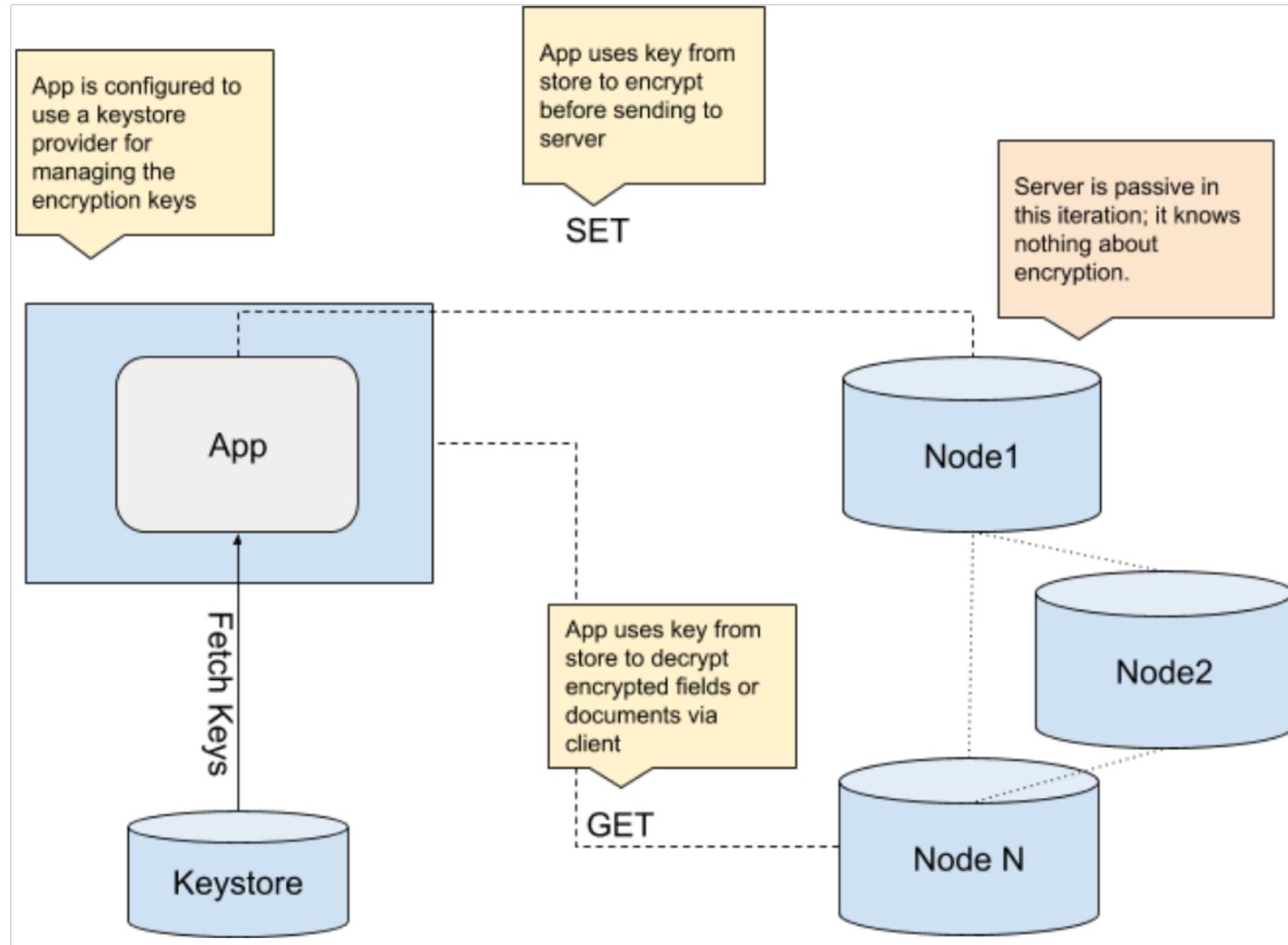
Secure Personally Identifiable Information

- 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)





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":  
      "iX2MXbUlief8Xxk4DYysivEsUXeoFBLkm4/EC7E9vRnGikD0iuawl  
      lLTJU/oNKeVNlWPzfN6r/uLEpttp+BLCOswdxLkA30Ne085TDdHaHm  
      rJ3dJQ7qgDFe35K6MbTEPXE98f1wL2v0L70xJxW+3KsgdcYYYqg8VNm  
      2U9eKVC2lv4DS19l/r+6l+08EGvBaa0FidezgF7CzgdXpGmG20cA0D8  
      yCmmGoW8oq7KWoq0PNaKsb9J0Yf0Yi13bxpP0IbyI003qLb5b7y1qVm  
      s8KDZ0+nk7Xnn50YFmBHQDyJ39nuibEMKNM1A2ZN1CvfFqE1dU3iqqZ  
      YyS70TukFB02g=="  
  },  
  "recipient": "jeffry.morris@couchbase.com"  
}
```



4

Auditing



Admin Auditing in Couchbase

- Rich audit events

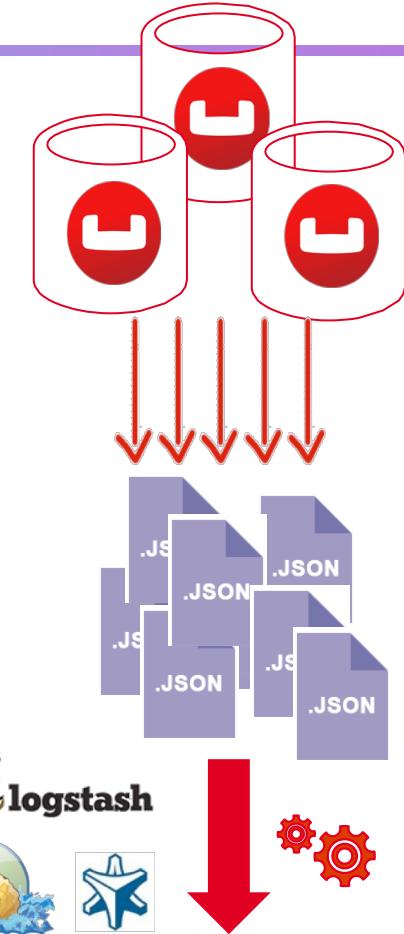
- Over 25+ different, detailed admin audit events
- Auditing for tools including backup

- 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 syslog



splunk>
ArcSight
An HP Company



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}  
}
```

WHAT

WHEN

WHO

HOW

Thank you



Couchbase