HP

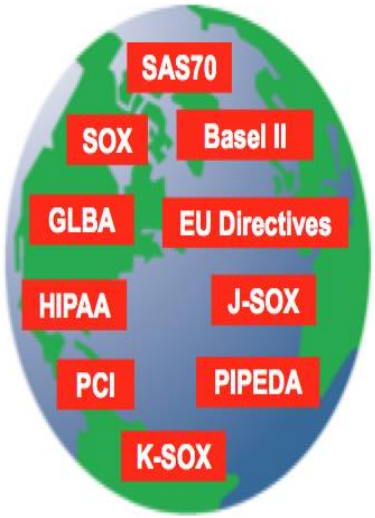
# Securing Your Couchbase Environment

HP

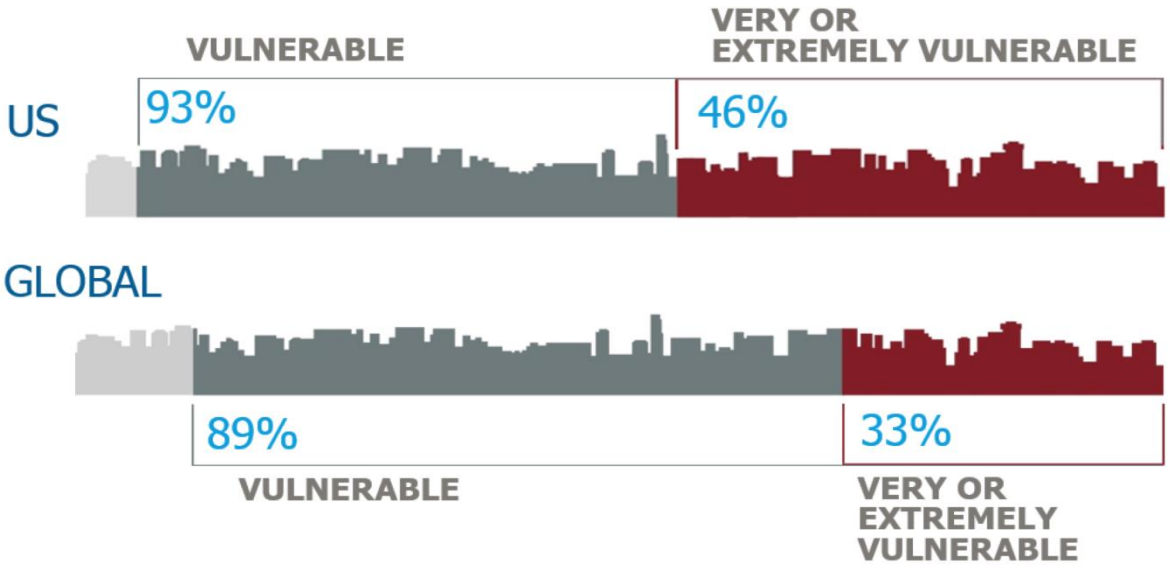
# Key drivers of NoSQL data security

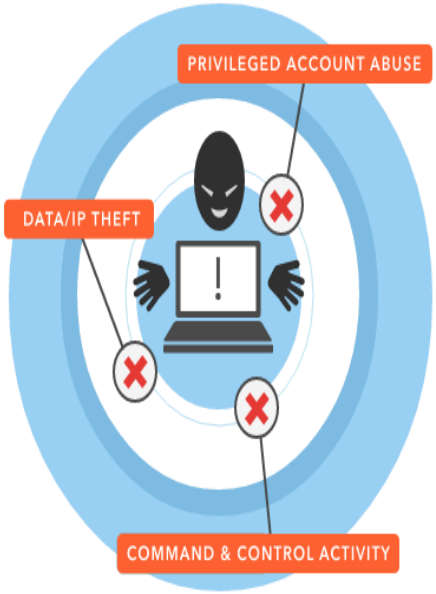
Regulatory compliance requirements

- PCI, HIPAA, EU Data Protection Directive,
- Additional corporate security policies




Growing number of insider threats




*2015 Vormetric Insider Threat Report

# Core security requirements

**AUTHENTICATION**

- Who am I/prove it
- Control access to cluster

**AUTHORIZATION**

- Admin/data access separation
- Role based access

**ENCRYPTION**

- Encrypt data at rest and in-motion

**AUDITING**

- Who did what, when, and how ?

**ADMINISTRATION**

- Security best practices

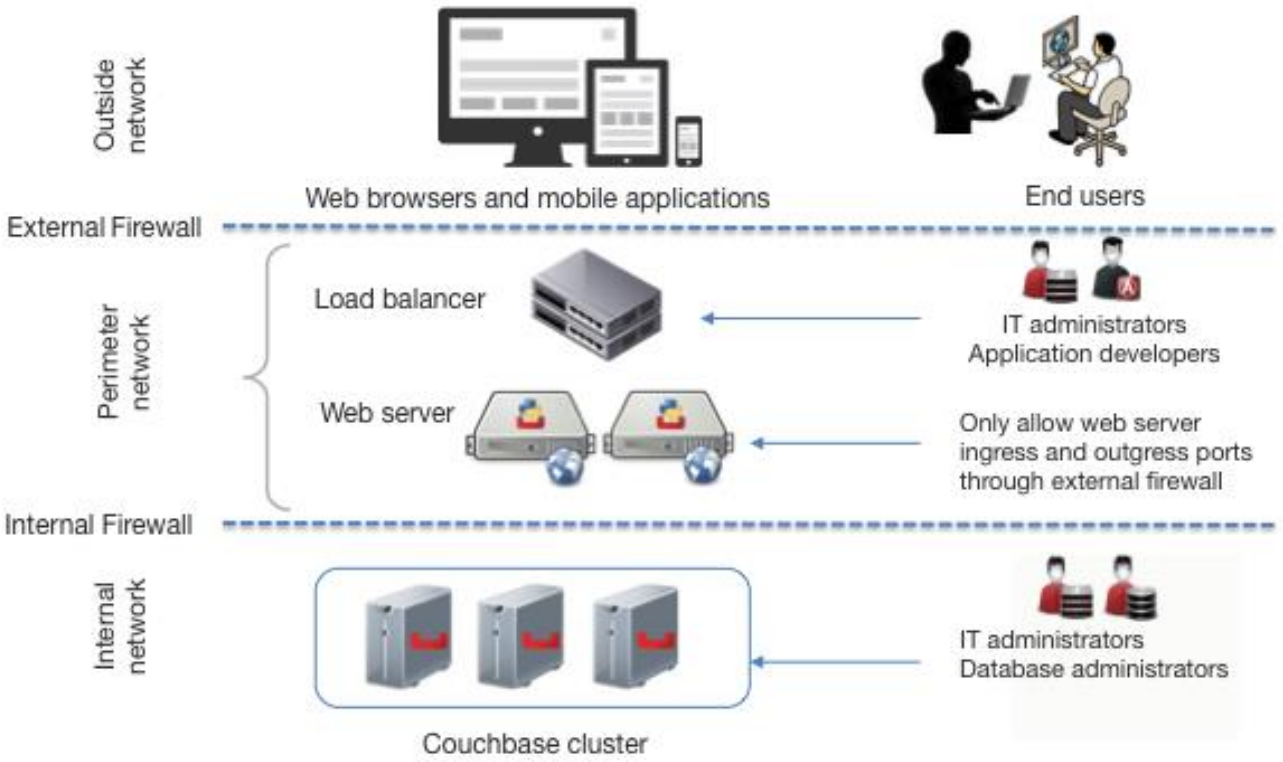
HP

# Couchbase security journey

| Previously … | In 2.2 | In 2.5 | In 3.0 | New in 4.0 |
|---|---|---|---|---|
| SASL AuthN with Bucket Passwords<br>Admin User<br>Secure Build Platform | Read-Only User<br>Easy Admin Password Reset<br>Non-Root User Deployments | Secure Communication for XDCR | Encrypted Client-Server Communication<br>Encrypted Admin Access<br>Access Log<br>Data-at-Rest Encryption | • Simplified compliance with admin auditing<br>• External identity management for admins using LDAP |

HP

# Security is Enforced



HP

# Security is Enforced

From the network perspective, here are a few layers you might consider for enforcing security:

- Outside network, where web browsers and mobile applications are located.
- Perimeter network between the internal and external firewall, which typically consists of web servers and load balancing machines. This network provides physical separation between back-end and external interfaces, such as the web and mobile applications.
- Internal network within the internal firewall, where Couchbase Server is typically deployed.

HP

# Couchbase authentication

- **Application authentication**
  - Buckets are protected with challenge-response SASL protocol
  - AuthN happens over CRAM-MD5



- **Admin authentication**
  - Authentication through admin username and password
  - Authentication through LDAP (New in 4.0)

HP

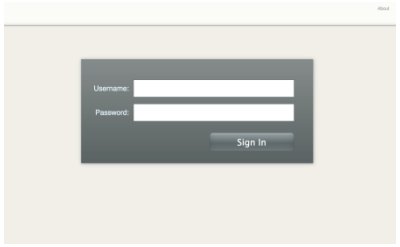
# External identity management using LDAP

- **Centralized identity management**
  - Define multiple read-only admins and full-admin
  - Centralized security policy management for admin accounts for stronger passwords, password rotation, and auto lockouts


- **Individual accountability. Simplified compliance.**
  - Define UIDs in LDAP, and map UIDs to read-only/full admin role in Couchbase
  - Comprehensive audit trails with LDAP UIDs in audit records

HP

# LDAP architecture in Couchbase


Admin UID / password

Authentication SUCCESS!

YES

YES

Authentication FAILED!

NO

CHECK IN ADMIN PASSWORD FILE

SASL protocol

UID / password

SASLAUTH D

CHECK IN LDAP ?

OpenLDAP protocol

YES / NO?

UIDs defined in LDAP

OpenLDAP

Windows Server Active Directory

saslauthd config file

# HP New UI for authorizing LDAP administrators


Couchbase

Documentation • Support • About • Sign Out

Cluster Overview | Server Nodes | Data Buckets | Views | XDCR | Log | Settings

Settings

Cluster | Update Notifications | Auto-Failover | Alerts | Auto-Compaction | LDAP Auth Setup | Account Management | Audit | Sample Buckets

LDAP Auth

Integrate with a directory server such as Active Directory or LDAP using the LDAP protocol. Users in LDAP can be mapped to Full-Admin / Read-Only Admin in Couchbase.

Setup

Enable:

Turn on/off LDAP

Read-Only Admins:

Add UIDs to read-only admins

Full Admins:

Add UIDs to full admins

Default: Read-only Full Admin None

Set default behavior if UID is not mapped

Test

Username:

Password:

Validate

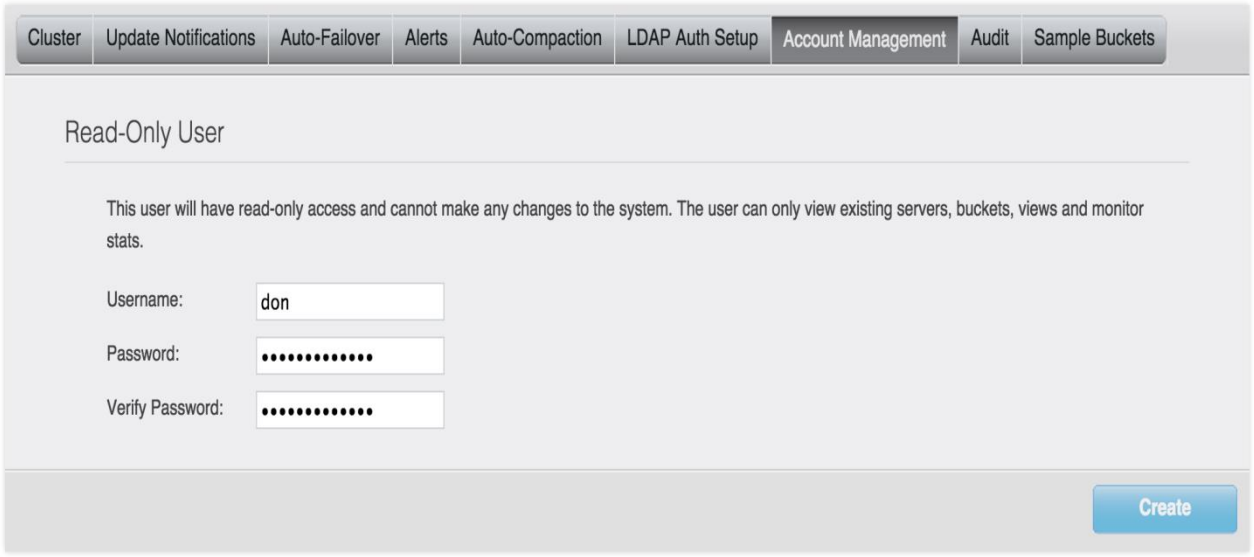
Testing credentials to verify what level of access

Save

Plus REST APIs and CLI integration for programmatic setup

# HP Couchbase authorization

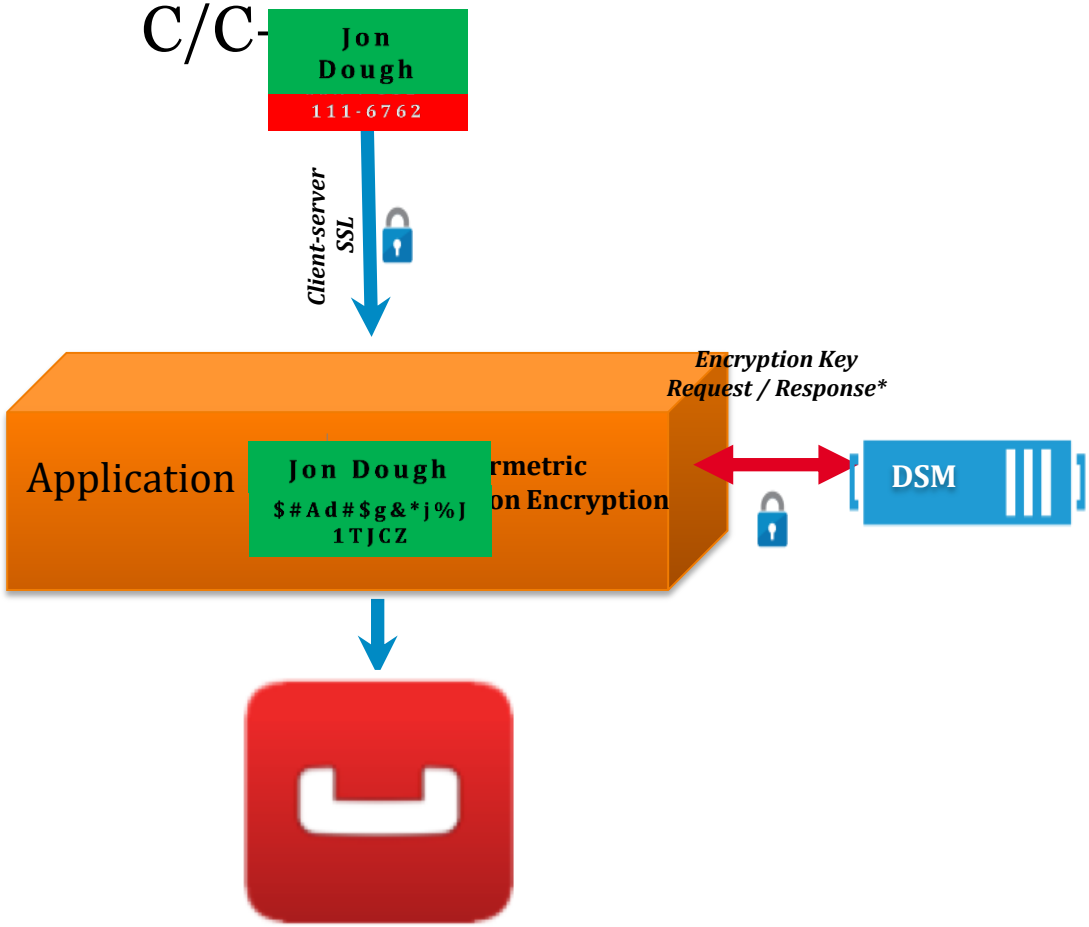

- **Application data access**
  - Full access to specific buckets
- **Admin access**
  - Full administrator has full privileges on the cluster
  - Read-only administrator cannot change cluster settings



HP

# Couchbase encryption – client


- **Encryption at the application**
  - Leverage Vormetric encryption and key manage
  - APIs, libraries, and sample code in Java, .NET, C/C-

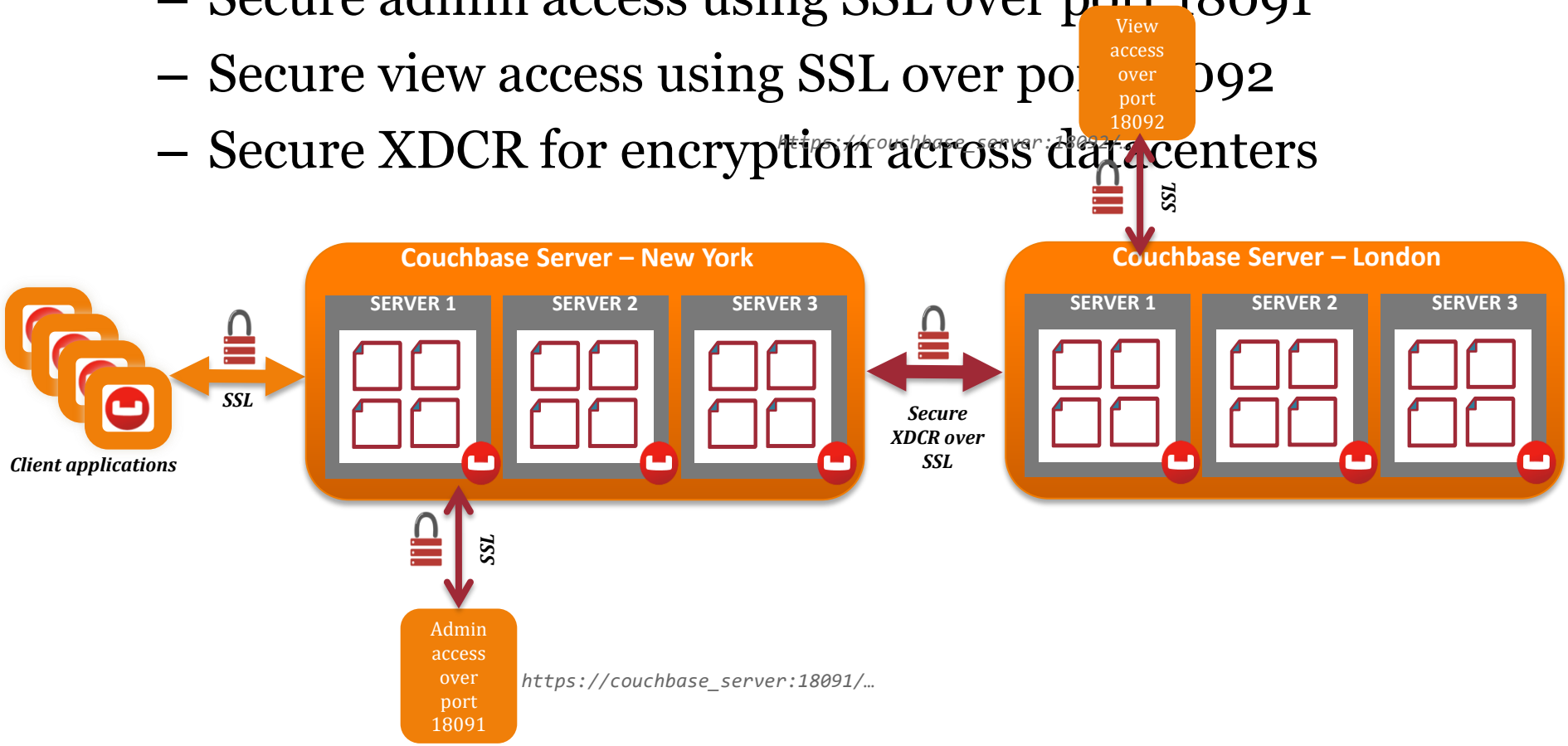


HP

# Couchbase encryption – in motion

ENCRYPTION

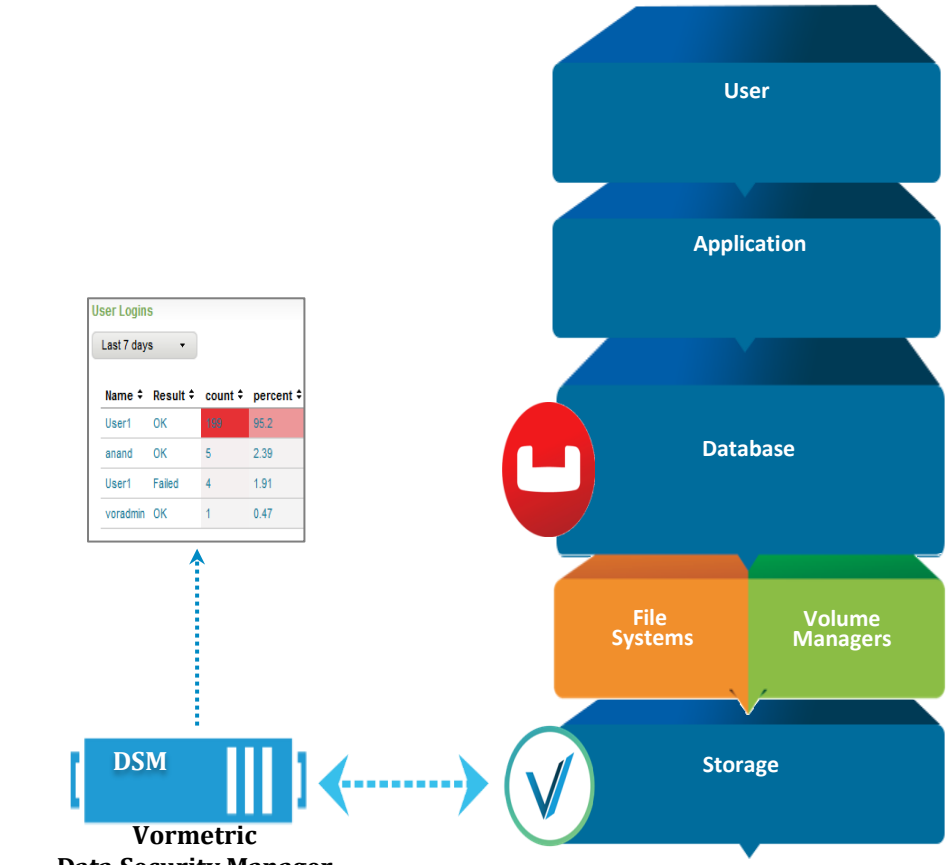
- **Data-in-motion encryption**
  - Client-server communication should be encrypted using SSL
  - Secure admin access using SSL over port 18091
  - Secure view access using SSL over po 092
  - Secure XDCR for encryption across datacenters



# Couchbase encryption – at rest



- **Transparent data-at-rest encryption solution**




**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

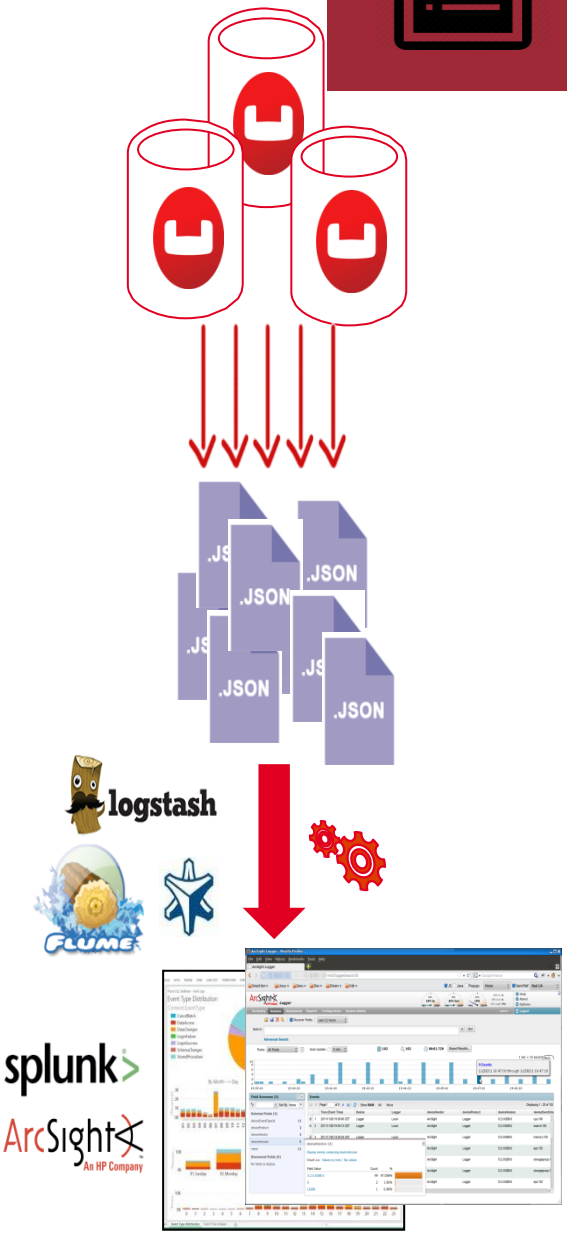
HP

# Admin auditing in Couchbase

AUDITING

- **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
- **Target**
  - The *target* of a Couchbase Server audit is

a JSON file; which is rotated after a configured time interval, and whose location path is configurable.



HP

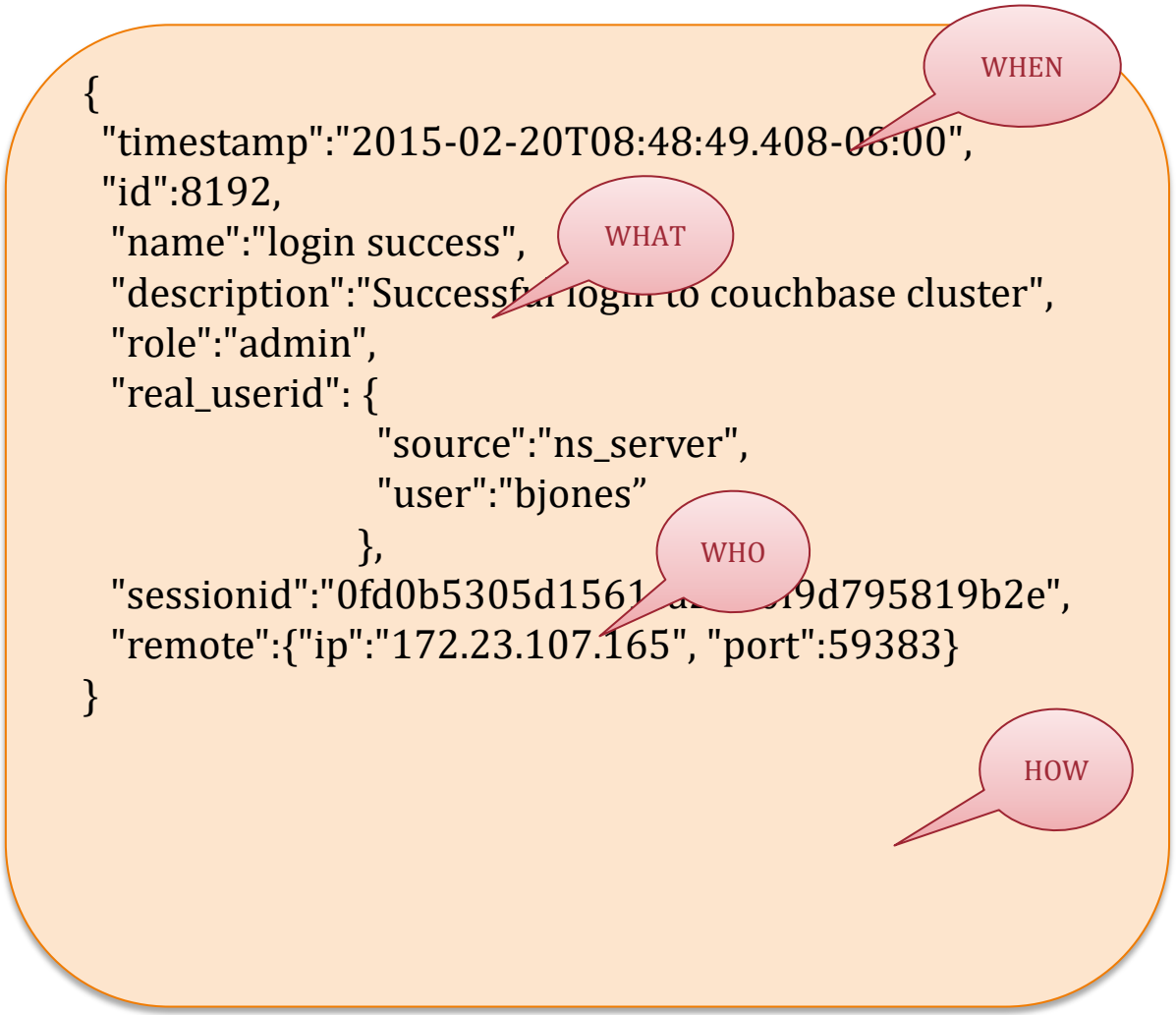
# Auditing events

AUDITING

| LIST OF ADMIN AUDIT EVENTS |
| --- |
| Success/failure login for administrator |
| Audit configuration changes |
| Enable/disable audit |
| Add a node to the cluster |
| Remove a node from the cluster |
| Failover a node |
| Rebalance the cluster |
| Shutdown/startup of the system by the administrator |
| Create a bucket |
| Delete a bucket |
| Flush a bucket |
| Modify bucket settings |
| Change configured disk and index path |
| Add read-only administrator user |
| Backup |

| |
| --- |
| Remove read-only administrator user |
| Add admin user |
| Remove admin user |
| Setup remote cluster reference |
| Delete remote cluster reference |
| Changes to XDCR |
| Creating/deleting XDCR profile |
| Pause resume XDCR stream |
| Changing XDCR filter rules |
| Add/remove query node |
| Add/remove index node |
| Create server group |
| Add node to server group |
| Remove node from server group |
| Delete server group |
| Admin password changes/resets |

# Auditing a successful login

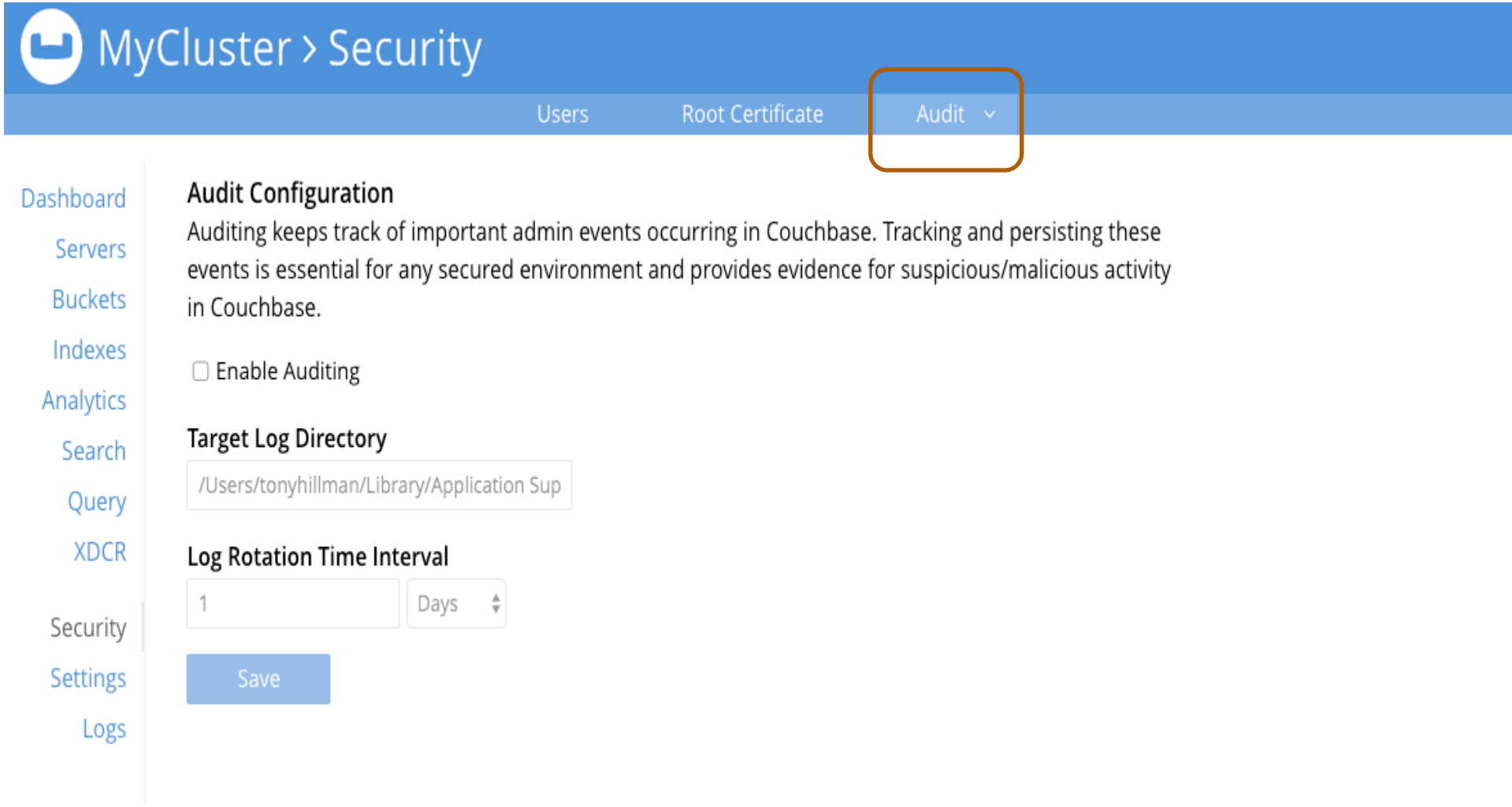
HP

# Bucket Creation


```
{
    "props": {
       "storage_mode": "couchstore",
       "conflict_resolution_type": "seqno",
       "eviction_policy": "value_only",
       "num_threads": 3,
       "flush_enabled": false,
       "purge_interval": "undefined",
       "auth_type": "sasl",
       "ram_quota": 1156579328,
       "replica_index": false,
       "num_replicas": 1
    },
    "type": "membase",
    "bucket_name": "auditBucket",
    "real_userid": {
    "source": "ns_server",
    "user": "Administrator"
    },
    "sessionid": "dca284b5efe1937a1a4085ef88c2fbcb",
    "remote": {
    "ip": "127.0.0.1",
    "port": 64477
    },
    "timestamp": "2017-03-16T15:43:35.187Z",
    "id": 8201,
    "name": "create bucket",
    "description": "Bucket was created"
}
```

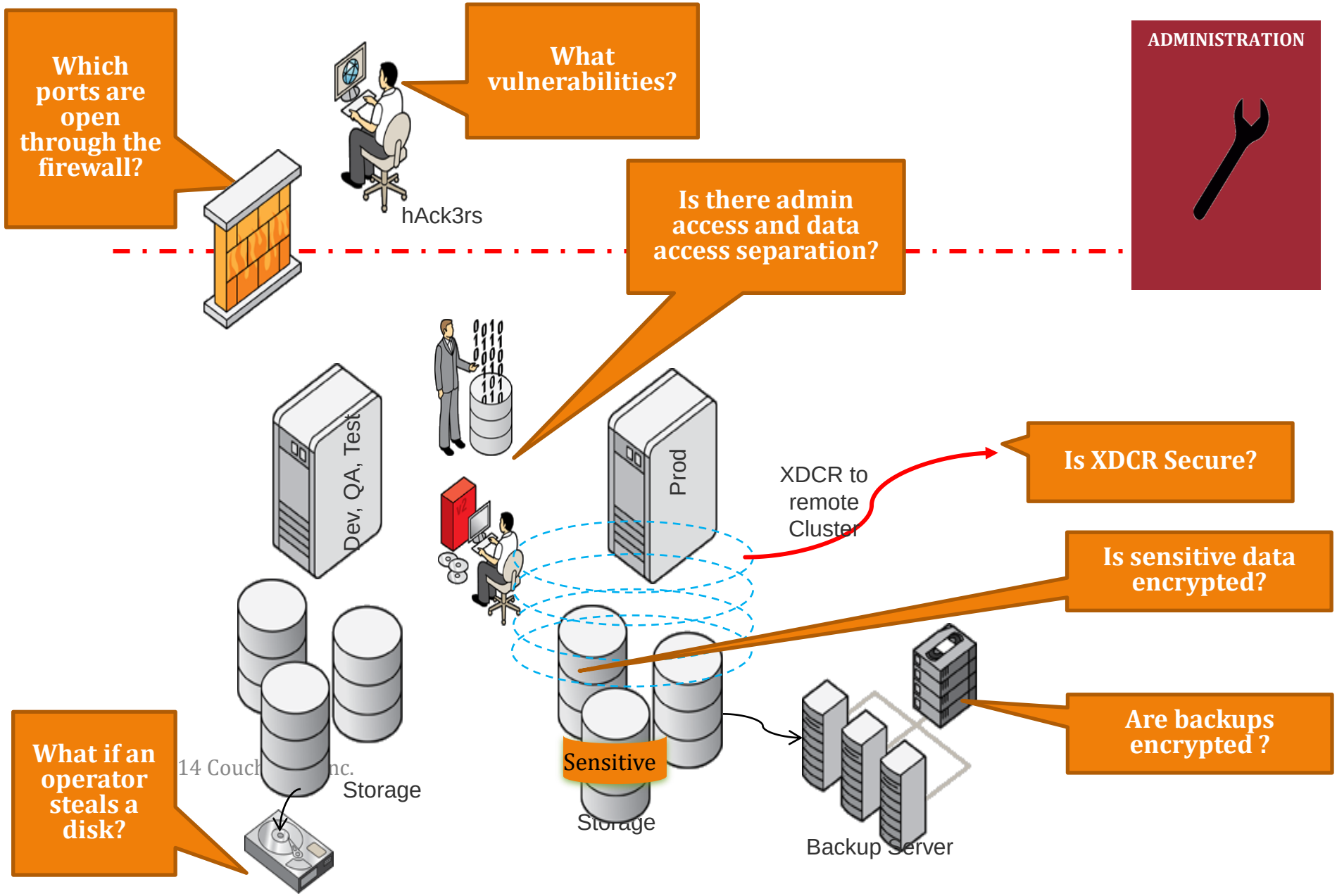
# HP Audit Configuration

- Only a *Full Administrator* can configure auditing.



HP

# Questions to ask



HP

# New security-features

- Role-Based Access Control
  - Access privileges are assigned to fixed roles; which are in turn assigned to administrators and applications.

- Authentication Domains
  - Couchbase Server assigns users to different authentication domains, based on whether their definition is local (that is, on Couchbase Server itself) or external (that is, by means of LDAP or PAM)

HP

# LDAP Authentication

- Steps:
  - Setting up LDAP administrators on the LDAP server
  - Mapping user IDs using the Couchbase Web Console
  - Configure the ***saslauthd*** agent.

HP

# Configuration

- Perform these tasks on the LDAP server:
  - Create users.
  - Set up user passwords.
- These tasks are performed using the Couchbase Web Console:
  - Mapping users in LDAP to full administrators or read-only administrators in Couchbase.
  - Validating LDAP credentials.

HP

# Configuration

- ***saslauthd***
  - The ***saslauthd*** process handles authentication requests on behalf of Couchbase Server.
  - daemon process that handles plaintext authentication requests on behalf of the SASL library.
- Install saslauthd 2.1.26
- Enable LDAP Authentication:
  - MECH=ldap → ( /etc/sysconfig/saslauthd)
- /etc/saslauthd.conf

```
ldap_servers: ldap://192.168.188.165
ldap_search_base:dc=tos,dc=com
ldap_filter: (uid=%u)
ldap_bind_dn: CN=henry,DC=tos,DC=com
ldap_password:  password
```

HP

# Role-Based Access Control

- Access privileges are assigned to fixed roles; which are in turn assigned to administrators and applications.
- RBAC Concepts
  - *Resource*
  - *Privilege*
  - *Role*
  - *User*

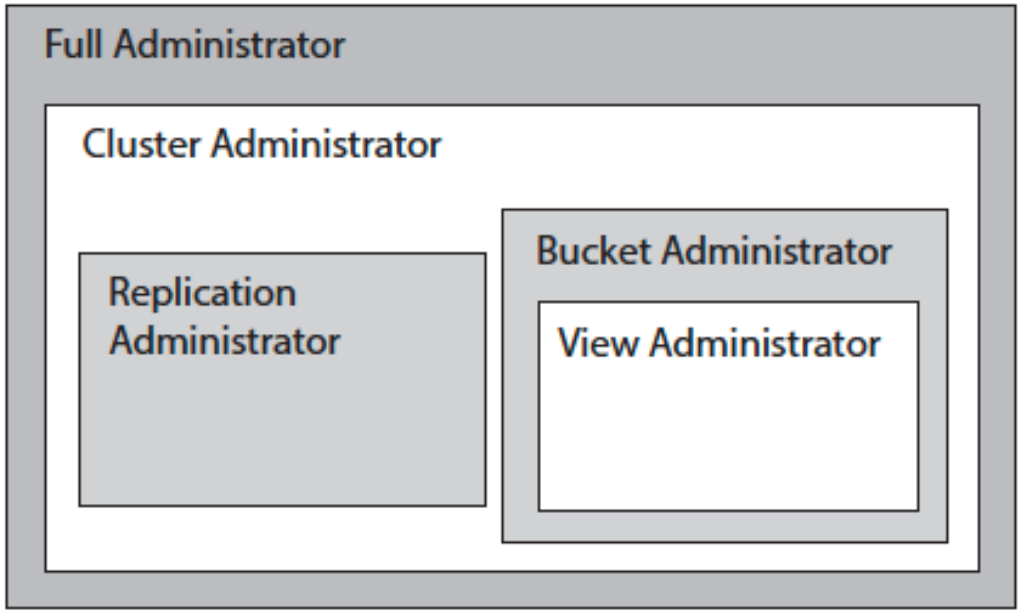
HP

# RBAC Concepts

- *Resource*: An entity the access to which must be controlled. A resource can be specified either individually, by name; or as a group (for example, all buckets), by means of a wildcard character.
- *Privilege*: The right, assigned by Couchbase Server, to apply an action to a resource. Possible actions include *read*, *write*, and *execute*.
- *Role*: An entity associated with a fixed set of privileges.
- *User*: An identity, recognized by Couchbase Server, based on the passing of a *username* and *password*. A user can be assigned one or more *roles*: the privileges associated with each assigned role determine the resource-access granted the user. Users can be *local* (defined on Couchbase Server) or *external* (defined on a remote, network-accessible system). Each user might be an administrator or an application.

HP

# Administrative roles



HP

# RBAC for Applications

- Couchbase Server 5.0 adds RBAC for applications.
- Privileges are actions such as **Read**, **Write**, **Execute**, **Manage**, **Flush**, or **List**; or a combination of some or all of these.

HP

# Roles

- The **Bucket Full Access** role provides full access to bucket data.
- The **Data Reader** role allows data to be read from a specified bucket. Note that the role does *not* permit the running of N1QL queries (such as SELECT) against data.
- The **Data Writer** role allows information to be written to and read from a specified bucket.
- The **Data Backup** role allows data to be backed up and restored.
- The **Query Select** role allows the SELECT statement to be executed on a specified bucket.
- The **Query Insert** role allows the INSERT statement to be executed on a specified bucket.
- The **Query Delete** role allows the DELETE statement to be executed on a specified bucket.

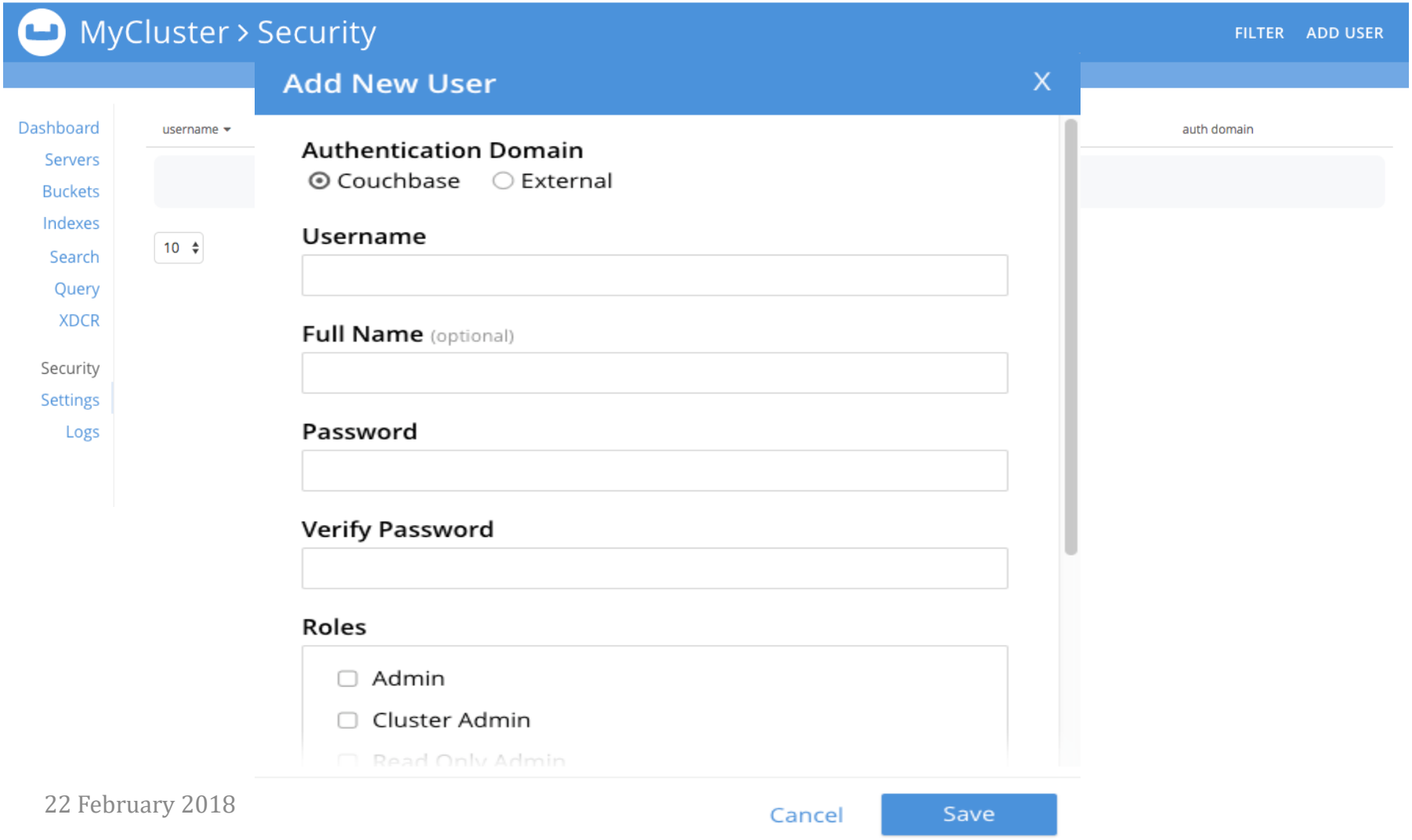
HP

# Upgrading to RBAC

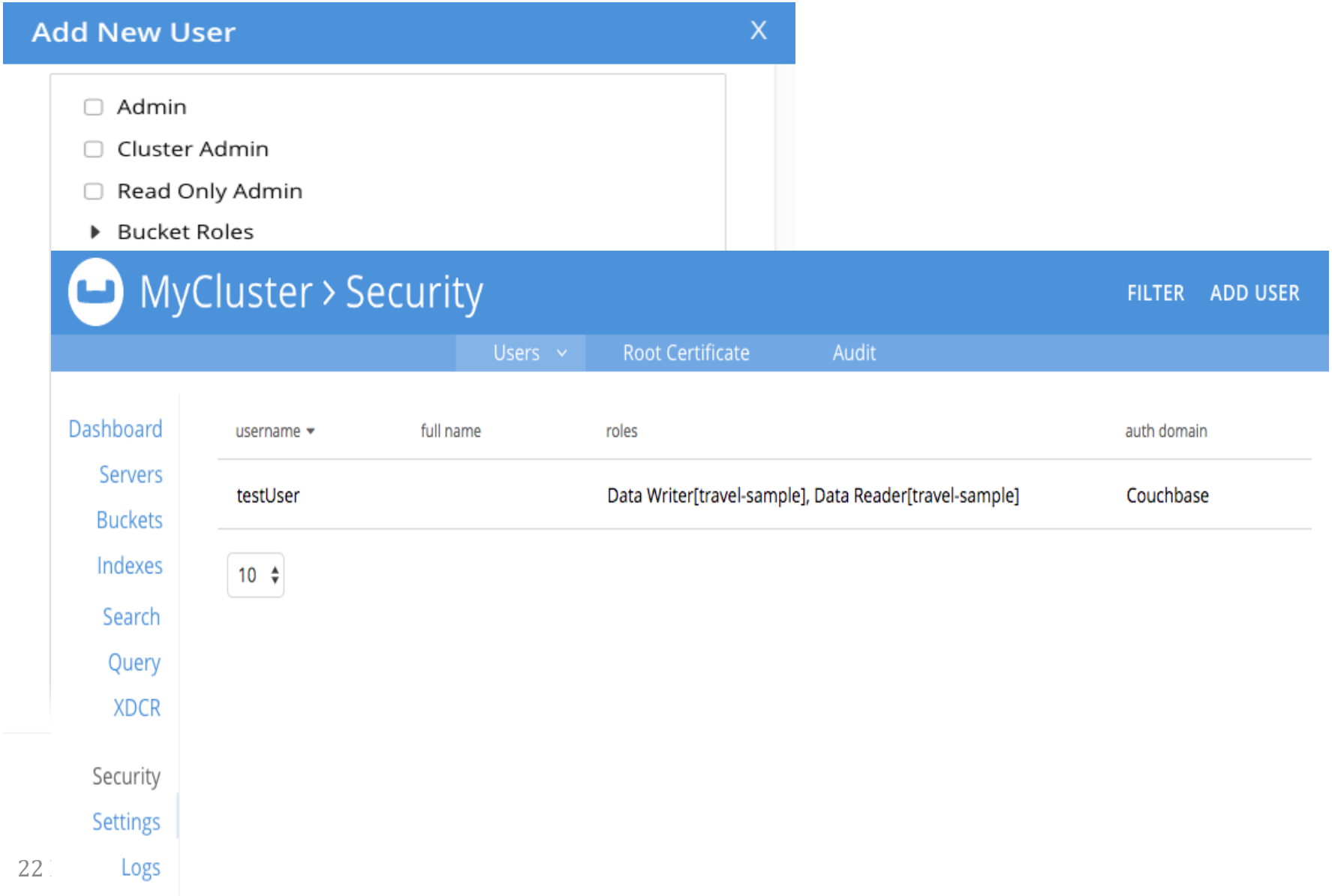
- Legacy Buckets on the Standard Port
  - A new *user* is created, whose username is identical to the name of the bucket.
  - bucket-password of the legacy bucket

# HP Creating and Managing Users with the UI

- Adding Users

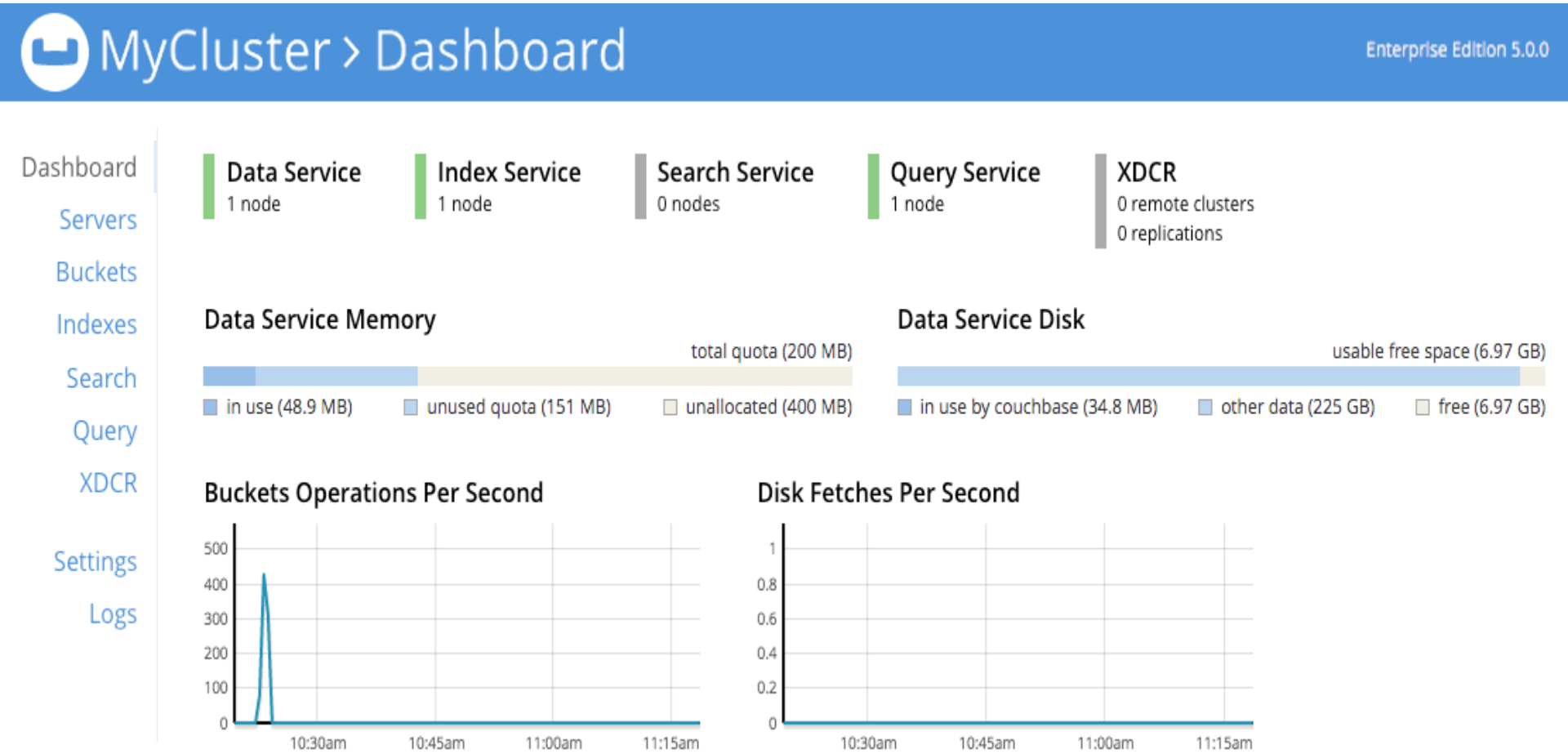


# Adding Roles



HP

# Role-Based Console Appearance




**Security** option has been removed from the vertical navigation-bar, at the left; since the *Cluster Admin* role is not privileged to read or write security-related data.

# Lab : LDAP Authentication and Auditing