

Couchbase Capella™ Data Platform Shared Responsibility Model

Introduction: The advantage of the Couchbase Capella cloud platform

The Capella data platform offers outstanding performance and enables developers to streamline their application-building process. With a robust security default setting, customers can concentrate on fulfilling their business needs while reducing security concerns. Advantages include:

- Capella is a flexible JSON document Database-as-a-Service (DBaaS) that improves agility and time to market for application development
- It offers multicloud support across the top three cloud providers: AWS, Azure, and Google Cloud
- Capella natively supports a wide range of use cases, including highly scalable caching, user profiles, dynamic catalogs, full-text search, operational analytics, offline embedded mobile apps, and more

Responsibilities of security and management

Management and security in the cloud is a joint responsibility. Couchbase shoulders a large portion of the responsibility so customers can focus on developing their applications and meeting their business requirements.

Couchbase responsibilities

Capella is designed with strong security defaults to minimize the customer's security burden. These defaults include always-on authorization, authentication, encryption in transit, encryption at rest, and settings that block access from the internet. Capella's framework supports high availability using a distributed, in-memory architecture and delivers automated scaling capabilities. Automated and transparent patching for the underlying infrastructure, operating system, and Capella databases prevents downtime during maintenance.

Customer responsibilities

Customers are responsible for creating user accounts (roles, responsibilities, and access rules), choosing their cloud service provider (CSP) and region, and making minimal configuration choices for deployment. Database design, such as schema and data modeling, is the customer's responsibility. Customers can enable backup, cross data center replication (XDCR), and additional security features if desired. Additionally, customers must assess risks to their organizations and identify corresponding controls to address those risks.

The following tables highlights the responsibilities of each entity.

Deployment

Area	Couchbase responsibility	Customer responsibility
IaaS – Control Plane	<ul style="list-style-type: none"> • Provide a multicloud, multi-database UI to manage databases and services • Security of the Control Plane, with access to its services through a management API key 	<ul style="list-style-type: none"> • Create, download, and protect management API security key
IaaS – Data Plane	<ul style="list-style-type: none"> • Provide the security framework for the Data Plane and the assets within it • Control the Data Plane in the customer’s choice of CSP and region • Provide necessary compute, storage, and network for the database 	<ul style="list-style-type: none"> • Select the CSP, region, and CIDR • Select compute and storage settings at setup
Database	<ul style="list-style-type: none"> • Database is deployed within the Data Plane • Database is secured from the internet until the customer explicitly creates access 	<ul style="list-style-type: none"> • Size database appropriately for performance and cost on an ongoing basis • Choose single or multi-availability zone deployment (multi provides greater availability at a higher cost) • Enter accurate and valid data
Services	<ul style="list-style-type: none"> • Capella makes available key services, including Data, Query, Index, Search, and Eventing 	<ul style="list-style-type: none"> • Mix and match services to optimize performance and cost benefits

Management

Area	Couchbase responsibility	Customer responsibility
Users (roles)	<ul style="list-style-type: none"> • Users are managed within the Capella Control Plane • Secure user IDs and credentials when validating users • Isolate user accounts across multiple organizations with organization-level isolation 	<ul style="list-style-type: none"> • Allow UI access • Safely manage and rotate passwords • Option to enforce multi-factor authentication (MFA) • Assign and manage user roles and privileges
Single sign-on (SSO)	<ul style="list-style-type: none"> • Provide ability to add and manage users through SSO 	<ul style="list-style-type: none"> • Set up and manage SSO provider • Manage users via SSO • Option to enforce MFA via SSO provider
Access in and out	<ul style="list-style-type: none"> • Provide, by default, the database is inaccessible via the internet • Provide connections within virtual private clouds (VPCs), through VPC peering, and/or AWS private endpoints 	<ul style="list-style-type: none"> • Add appropriate client IPs for access • Create and manage database credentials for access • Secure customer’s own VPCs from unauthorized access



Management *(continued)*

Area	Couchbase responsibility	Customer responsibility
Projects	<ul style="list-style-type: none"> • Provide functionality to deploy databases within the context of projects • Enable adding users or teams to projects with the appropriate role and access privilege • Maintain the project namespace against any malicious attacks 	<ul style="list-style-type: none"> • Create projects and add users • Deploy databases within projects
Patches and upgrades	<ul style="list-style-type: none"> • Apply available security patches • Manage IaaS-related patches and upgrades • Provide Couchbase Server upgrades • Resolve potential problems during upgrades, and safely roll back in a worst-case scenario • Capella Documentation for more details 	<ul style="list-style-type: none"> • Schedule upgrade dates and times within the upgrade time window
Global secondary index (GSI) management	<ul style="list-style-type: none"> • Facilitate creation and deletion of GSIs • Maintain availability of indexes 	<ul style="list-style-type: none"> • Build and maintain appropriate indexes • Appropriately size index nodes

Data Operations

Area	Couchbase responsibility	Customer responsibility
Buckets, scopes, and collections	<ul style="list-style-type: none"> • Ability to create buckets, scopes, and collections 	<ul style="list-style-type: none"> • Size buckets and choose options like bucket storage engine, durability, document expiry time, and number of replicas
Backup/Restore	<ul style="list-style-type: none"> • Security and integrity of backups maintained by Couchbase • Backups in Capella are at a bucket-level - they are not automatic and must be scheduled 	<ul style="list-style-type: none"> • Choose backup schedule for individual buckets • Manage the cost of storage by retaining backups on cloud storage as needed
Data movement - Replication*	<ul style="list-style-type: none"> • Ability to replicate data across databases (using XDCR) to improve availability across regions • Security of data moving across databases 	<ul style="list-style-type: none"> • Configure database for high availability • Optimize applications to fetch the right amount of data to manage network costs



Data Operations *(continued)*

Area	Couchbase responsibility	Customer responsibility
Data movement – Mobile synchronization*	<ul style="list-style-type: none"> Security of data synchronized between the cloud DBaaS and mobile/IoT apps 	<ul style="list-style-type: none"> Configure Capella App Services to optimize fetching the right amount of data to manage network costs Configure app endpoints with the right access control policies to ensure correct user access Size App Services for specific load and throughput needs
Alerts and scaling	<ul style="list-style-type: none"> Provide alerts for key metrics like CPU, disk usage, etc. 	<ul style="list-style-type: none"> Enable email notification in profile to receive alerts Take action on alerts in a timely fashion
Metrics	<ul style="list-style-type: none"> Provide a curated set of metrics in the form of graphs Provide a metrics endpoint to connect Prometheus/Grafana infrastructure 	<ul style="list-style-type: none"> Customize metrics dashboards If using Prometheus/Grafana, set up the infrastructure and build the dashboard

*Note: Cloud providers charge for data egress from an availability zone. These costs are passed on to the customer.

Security

Area	Couchbase responsibility	Customer responsibility
Certificates	<ul style="list-style-type: none"> Create, manage, and rotate the certificates used for encryption in transit Protect the underlying Public Key Infrastructure (PKI) from unauthorized access 	<ul style="list-style-type: none"> Ensure that applications and API access use only validated certificates from the trusted Capella Certificate Authority (CA)
MFA (optional)	<ul style="list-style-type: none"> Ability to use MFA for UI users 	<ul style="list-style-type: none"> Enforce MFA usage within your organization (MFA is optional, but recommended) In the case of SSO, Capella will disable MFA; customers must enforce MFA with the SSO provider
Incident management	<ul style="list-style-type: none"> Manage any incidents that affect Capella infrastructure or customer data 	<ul style="list-style-type: none"> Inform Couchbase of any actual or suspected information security breaches or unauthorized use of Capella services For systems and processes not under Couchbase management: manage the systems of records and logging specifically to support monitoring and incident response processes with Couchbase Support the Capella team with timely responses to any incidents



Security *(continued)*

Area	Couchbase responsibility	Customer responsibility
Database audit logging	<ul style="list-style-type: none">• Provide audit logging via REST API for Enterprise plans• Store audit logs in an encrypted S3 bucket for 30 days• Provide download links for audit logs (user-defined time window)	<ul style="list-style-type: none">• Enable audit logging• Regularly download audit logs• Securely store downloaded audit logs

Additional security information and whitepapers can be found in the Couchbase Capella [Trust Center](#).

Development

Area	Couchbase responsibility	Customer responsibility
Applications and SDKs	<ul style="list-style-type: none">• Ensure the latest SDKs are compatible	<ul style="list-style-type: none">• Use the latest SDKs (as documented)
Application connectivity	<ul style="list-style-type: none">• Provide multiple options of application connectivity: public internet, VPC peering, and private endpoints (for select CSPs)	<ul style="list-style-type: none">• Choose appropriate application connectivity to meet customer security requirements

Support

Area	Couchbase responsibility	Customer responsibility
Incident management	<ul style="list-style-type: none">• Provide the ability to open support tickets from the UI• Collect and analyze Capella logs• Provide timely root cause analysis per documented support policy	<ul style="list-style-type: none">• Open tickets with the appropriate priority and as much detail as possible

For any questions related to shared responsibility or security, please reach out to us at: www.couchbase.com/contact/



Modern customer experiences need a flexible database platform that can power applications spanning from cloud to edge and everything in between. Couchbase's mission is to simplify how developers and architects develop, deploy and consume modern applications wherever they are. We have reimagined the database with our fast, flexible and affordable cloud database platform Capella, allowing organizations to quickly build applications that deliver premium experiences to their customers—all with best-in-class price performance. More than 30% of the Fortune 100 trust Couchbase to power their modern applications. For more information, visit www.couchbase.com and follow us on Twitter.