Tessell

Tessellate Data Transform Enterprise

The Tessell platform provides unparalleled security for your data and users

We understand that data is the most important asset to any business. Hence, at Tessell, our platform has a security first design. From strong identity and access management engine to SSO integration with popular Identity Providers like MS AD, Okta and Google, to encryption of data at rest and in transit, industry leading security policies and practices have been built in to ensure data teams can securely access relevant data while enforcing your data governance policies.

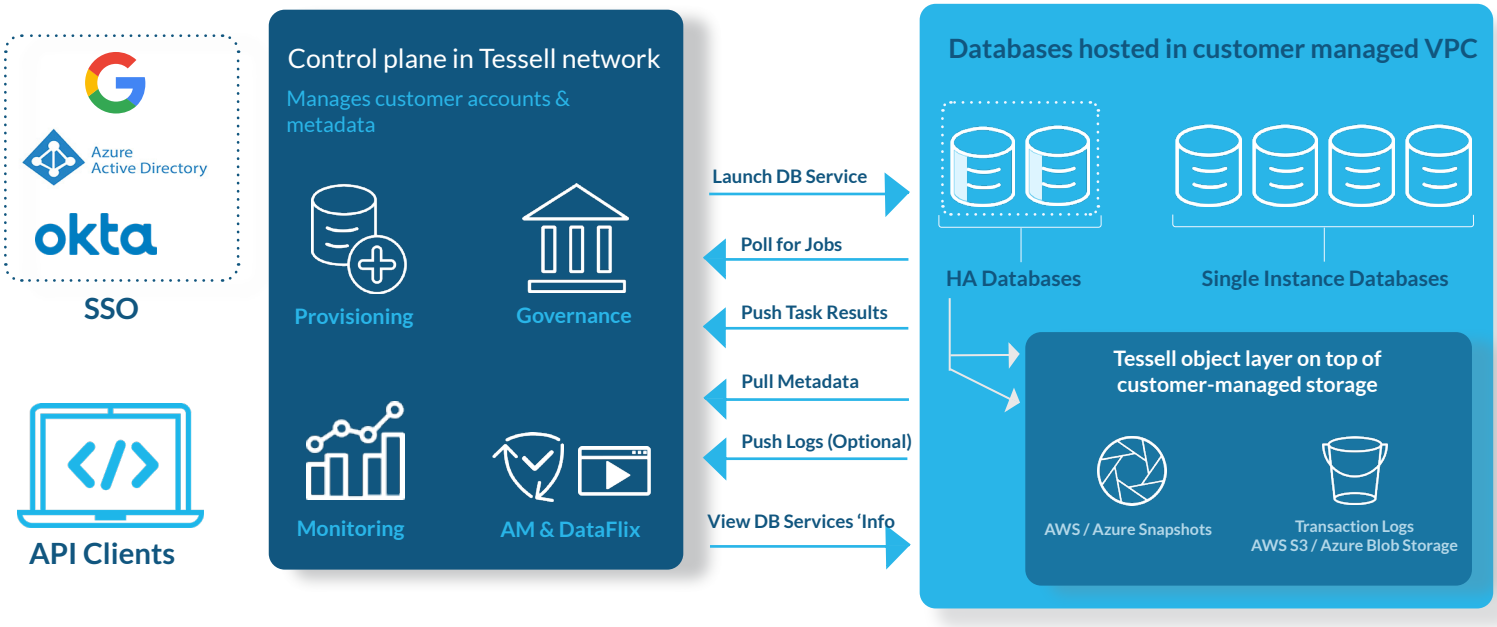
NOTE:

Tessell is already available on AWS, and Azure and will be coming soon to be on other cloud service providers like GCP, VMC etc.

Architecture

The Tessell architecture is split into two planes, in order to decouple the Tessell management logic from the customer data. This empowers the customers with the option of keeping their data in their own cloud account.

CONTROL PLANE	DATA PLANE
This is hosted entirely in the Tessell cloud service provider account. This manages all the deployments and is responsible for the management of the Data Plane.	This resides in the customer cloud service provider account, or optionally, in the Tessell account. This is where all the Databases are hosted along with their corresponding Backups, Snapshots, S3 objects and Networking.



End to end example

Suppose you have a developer or DB admin that signs in to Tessell portal and creates a database (DB) service on his/her choice of cloud (AWS or Azure).

User Experience and behind the scenes

- Log into Tessell using SSO (Single Sign-On, like Google OAuth, Okta, LDAP), or basic user-password. After a successful login, the UI lands you on the My Services page.
- Navigate to the Provisioning page.
- Select a Database Engine of your choice. Currently, Tessell supports only Oracle, PostgreSQL, MySQL and MS SQL Server. Support for more engines will be coming soon.
- Click on One-Click Provision to start the provisioning. Optionally, you can follow through the Next pages to customize the configuration for the Database to be provisioned and Submit the provisioning request. The provisioning status can be tracked under the My Services page.
- Once the provisioning is complete, click on the Database to go to its info page, where from the Connectivity tab, you can get the connection string to connect to your newly provisioned Tessell Database.

Behind the scenes

- When a provisioning request is submitted from the UI, the UI communicates the request to the Tessell Control Plane.
- Depending on the choice of cloud, the control plane, using cloud service provider APIs, creates the Database hosting VM along with any other required components in the Data Plane.
- Once the VM boots up, the Database Engine is configured by a job embedded in the Tessell OS images.
- As soon as the DB Engine is ready for use, the above-mentioned job, upon its completion, notifies the control plane about the status.
- This completion is then reflected in the UI as Ready in the Status column of the My Services page.

Networking

Tessell supports 2 models of networking: Tessell Managed and Customer Managed. As the names suggest, in the Tessell Managed model, Tessell manages all the networking configuration of VPCs, whereas, whenever Customers like to have control over the networking configurations (due tocompany security policies), they can choose to register their self-managed VPCs with Tessell. This feature is called Tessell BYOA (Bring Your Own Account).

In the case of BYOA, Tessell only creates the Databases and the corresponding resources (VMs, NICs etc.) in the provided/registered VPC, without any changes to the VPC configurations. Customers can choose to configure such VPCs however they like, except a few egress whitelist that Tessell needs for connecting each such Data Plane to the Tessell Control Plane.

For connectivity to the Tessell Databases, customers can either choose to have completely private VPCs, where they can reach their Databases over VPC Peering, or they can also opt for connectivity over the public internet. In either cases, the source IPs/CIDRs of ingress to each Database service can be whitelisted via Network ACLs configured for each Database.

Regardless of whether the connectivity is over public or private internet, Database connections to the clients are always secured by establishing mutual TLS, the client certificates for which can be fetched from Tessell UI/API, only after proper authentication and authorization. connect to your newly provisioned Tessell Database.

Servers

Tessell Databases, in the TDP (Tessell Data Plane), are hosted on VMs that run the latest versions of OS images. For security patches and OS level updates, Tessell Databases in Tessell Managed VPCs fetch the updates from the appropriate package repositories.

In case of Customer Managed VPCs, if egress to the public internet is blocked, it is expected that the customers have a private repository mirror, and such mirrors are reachable from the Database VMs. The endpoints to the private mirrors can be provided when registering a Customer Managed VPC.
In order to ensure that automatic updates do not have any backward compatibility or security vulnerabilities, Tessell first simulates such updates to the latest image in use and scans for vulnerabilities, and only when all the checks are met, the TCP (Tessell Control Plane) publishes a signal for fetching the current updates.

In each Database VM runs a Tessell agent which listens for signals dispatched from the TCP (Tessell Control Plane).
Any communication for the VMs from the TCP is done over such channels. This design ensures that no ingress is required from the TCP to the TDP for management of the Tessell databases and their host VMs.

Networking

Apart from the vanilla username-password method, Tessell supports Single Sign-On (SSO) leveraging either of SAML or OIDC, which helps in integrating with various IdPs (Identity Providers like Okta, Azure AD).

Once on the Tessell platform, Tessell provides multiple access control functionalities.

Tessell Personas determine whichTessell applications users have access.

Under each Tessell application, the application specific roles determine their privileges.

Access to different Tessell resources like Databases can be controlled and configured using Tessell ACLs.

Controlling who can see what data can be done via Data Access Policies (DAP)

Tessell Access

The Tessell Control Plane or the Tessell team have no access to the Tessell Databases or their hosts.
Communication between the TCP (Tessell Control Plane) and the TDP (Tessell Data Plane) is achieved via a pub-sub mechanism, where a Tessell Agent daemon running on each VM pulls instructions from the TCP to perform automated tasks like scheduled backups and snapshots.

On the BYOA front, Tessell needs a few roles in the customer account, which Tessell uses for STS to invoke cloud service provider APIs for Database provisioning and related workflows.
The VMs hosting the Tessell Databases always have their SSH servers disabled. Regardless of the type of account in use, the VMs are never accessed unless a Tessell Support ticket is opened. In case, Tessell Support is engaged for debugging some system level issues, the requesting user has to authorize the Tessell Support executive for accessing the VM over SSH.

This access feature is called Tessell Genie, where, upon authorization, the Tessell Agent daemon running in the VM will enable the SSH server for a short period of time. Although the SSH server is enabled, no ingress whitelisting is required. In order to provide a pathway for Tessell Genie to reach the VM, the Tessell Agent within the VM reaches out to a Tessell Bastion host and creates a tunnel for the Tessell Genie to land on the VM.

Tessell Supports SLAs

Priority	Priority Defination	Target Response time
Sev 1	A critical failure in the operational activity of services or an error that causes the services to be severely impacted or completely shut down or customer is unable to use the services and no workaround is available.	2 hours
Sev 2	High impact issues in which services are inoperative or seriously degraded where a short-term workaround is available.	4 hours
Sev 3	An error limits the functionality of services. A workaround readily available and can be applied little or no operational impact.	6 hours
Sev 4	Minimal problems in the services arising from a unsatisfactory component or feature, no data integrity as well as operational impact.	8 hours

Data Security

Encryption at Rest:

- All Tessell Databases use encrypted data disks, that is, the file system on which a Tessell Database runs and writes data to, is always encrypted.
- Tessell Database Snapshots and Backups are created using the above-mentioned encrypted disks. Hence, all Tessell Snapshots and Backups are always encrypted as well, while residing in cloud storage (S3/Blob).

Encryption in Transit:

- Tessell Databases does not support client connections without TLS. All communication between a Tessell database and its clients has to be over TLS.
- All communication between the Tessell Control Plane and Tessell Data Plane is always encrypted. Once the VM boots up, the Database Engine is configured by a job embedded in the Tessell OS images.

Data Security (Conti.)

Encryption at Rest:

- The Availability Machine feature of Tessell lets Data Owners share data with other Data Owners in the form of Snapshots and Backups. The sharing can be both inter- and intra- cloud, as well as inter- and intra- region. The data made available using Tessell Availability Machine is always encrypted at the destination as well.

- Customers can always choose to provide their own encryption key. By default though, Tessell generates and manages the encryption keys for each Tessell Database and its snapshots.

Encryption in Transit:

- In case of HA enabled Tessell Databases, all intra-cluster communications between servers is over TLS as well.

Learn More

Tessell provides industry first app driven data management platform that is built on a strong platform security posture for organizations small and large, and across all industries. We're happy to discuss your specific needs in more detail — please reach out to your account representative at Tessell via email **sales@Tessell.com** or schedule a **Demo** here to understand our product and services.

About Tessell

Tessell is a Next gen Cloud Data Management company revolutionizing industry with the vision to "Tessallate data to transform Enterprises". Tessell provides secure, dynamic, and affordable Multi-cloud DBaaS platform to customers which built on the infrastructure of hyper-scalers like AWS, Azure, GCP, OCI and others. Tessell is headquartered in San Ramon, and our development center located in the heart of Bangalore. Tessell is on a mission to help data teams solve the world's toughest problems. Learn more about HYPERLINK "https://tessell.com/" \t "_blank" **Tessell** here.