DotAlign Cloud – Azure deployment details

This is a document that details Azure deployment related aspects of DotAlign Cloud. If you are looking for a broader technical or security overview, please see the architecture and security document.

Table of contents

# Summary

DotAlign Cloud is a solution that analyzes mailbox data (messages, calendar entries and contact cards) and provides up-to-date contact information and relationship intelligence based on that data. The solution is single tenant and is deployed and hosted on your, i.e. the customer's Azure tenant. All data storage and processing happen there. No user data leaves your Azure tenant.

A primer on Azure resource organization

If you're not already familiar with how resources are organized within Azure, the following, simplified diagram may be helpful.
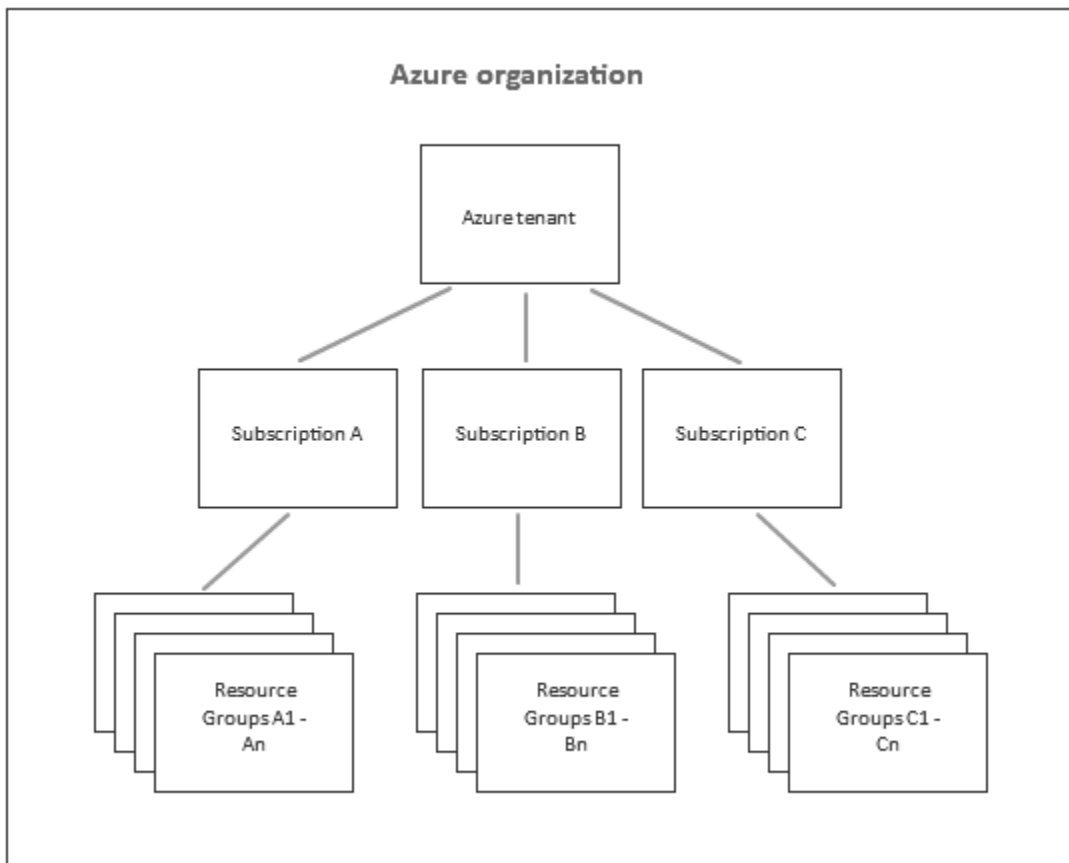
At the highest level is the tenant. Usually, an enterprise will have one tenant, and often the phrase "Azure Active Directory tenant" is used in its place, because a tenant is almost always one to one with an Azure Active Directory instance.

A tenant can have multiple subscriptions under it. Subscriptions are a way to organize the billing of Azure resources. For example, there may be a subscription for all production resources and one for all development and testing resources. Another example is a subscription for every department within the company. So, there may be a subscription each for the recruitment team, the marketing team and the investment team.

Under subscriptions are resource groups. Each subscription can have many resource groups under it. Resource groups act as a container for actual resources – i.e. services like Azure SQL, web apps, function apps etc., and infrastructure like virtual machines etc. They are a convenient way to group, manage, permission and budget resources.

This Microsoft article provides many relevant details about resource organization and deployment.

During the DotAlign Cloud deployment process, you will get an opportunity to choose which subscription you want to deploy under. One resource group will be created, and all resources will be deployed under that resource group.

DotAlign Cloud deployment

Block diagram of deployed resources

The following is a high-level diagram of the various resources that get deployed into the DotAlign Cloud resource group.
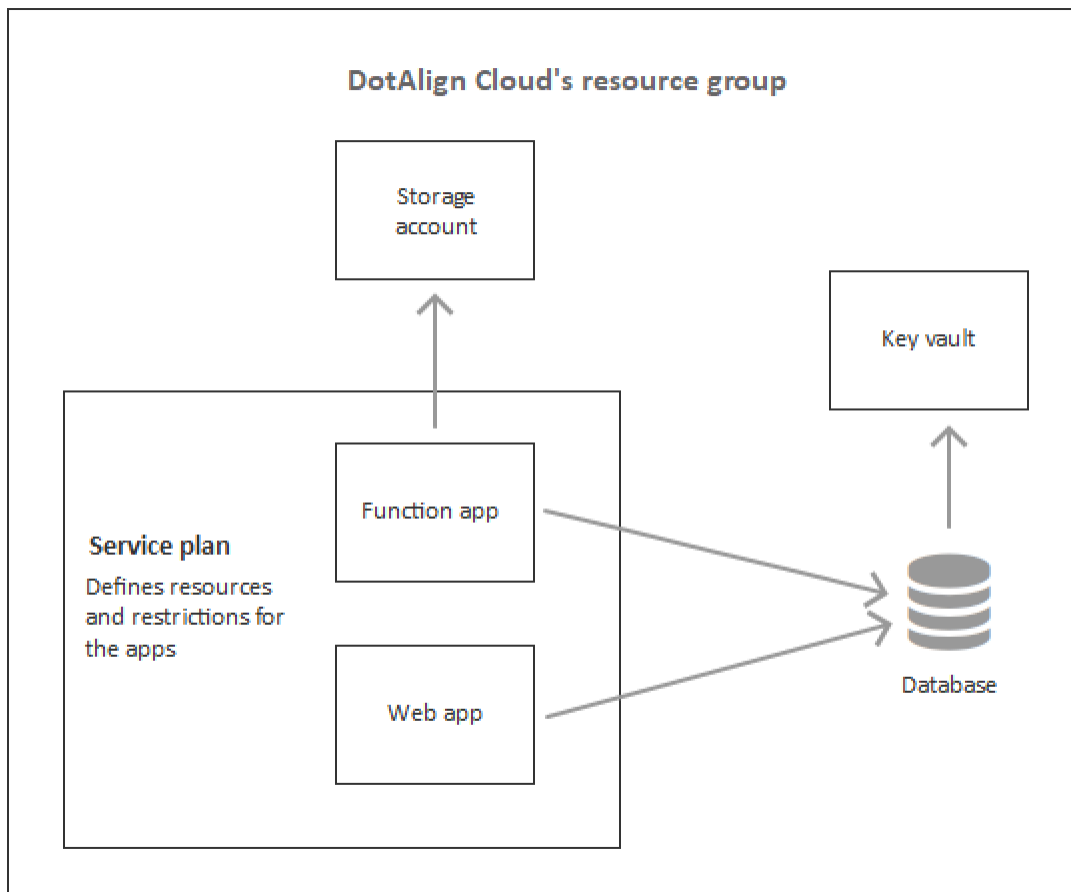
Following is a brief description of each resource:

a. **Service plan** – The service plan is an Azure construct that defines the resources that participating apps will be able to leverage, for example, the CPU power, memory size etc.,

whether the apps will run on dedicated infrastructure or not, and lastly, any network restrictions to be placed on the apps. DotAlign Cloud, by default used a premium plan called P1V2. You can read more about the available plans [here](#).

b. **Function app** – This is DotAlign Cloud's data pipeline, which runs a series of "functions" to fetch and run transformations of data into the desired insights. There are separate functions for fetching and processing data, and for running analytics. Together they run in the context of a "function app". The resources used by, and the restrictions placed on the function app are derived from the service plan.

c. **Web app** – This is the component that powers all user experiences, admin and end-user, and all the API endpoints. It is a standard Azure web app and like the function app, the resources used by, and the restrictions placed on the web app are derived from the service plan.

d. **Storage account** – The storage account is a way to create diskspace that can then be used for various operations. DotAlign Cloud primarily uses the storage account for queue data, which is used to trigger functions inside the function app.

e. **Key Vault** – The key vault is a service which allows data like security keys to be securely stored. DotAlign Cloud uses it to store database encryption keys used in conjunction with TDE (Transparent Data Encryption).

f. **Database** – The database used is an Azure SQL database, which Azure provides as a service (i.e. no machines to manage). It comes with many inbuilt security features and can be scaled up or down as need be. The deployment script will configure it to use the recommended level of horsepower and security and will enable a firewall on it to restrict access only from other Azure services. As with all other resources, the database can be further configured to align with your company data management policies.

Azure portal view of the resources

The following is a view of the deployed resources in [Azure portal](#), which is the management interface for Azure services.

	Name ↑↓	Type ↑↓	Location ↑↓	
☐	dotalign (mpntsdahxungl-db/dotalign)	SQL database	East US	⋯
☐	dotalign-mpntsdahxungl-webapp	App Service	East US	⋯
☐	mpntsdahxungl-db	SQL server	East US	⋯
☐	mpntsdahxungl-func	App Service	East US	⋯
☐	mpntsdahxungl-kv	Key vault	East US	⋯
☐	mpntsdahxungl-sp	App Service plan	East US	⋯
☐	mpntsdahxunglstorage	Storage account	East US	⋯

How is DotAlign Cloud deployed?

Deployment of DotAlign Cloud happens via a PowerShell script. This script will set up all required resource and create the required "app-registration" with Azure Active Directory.

The script uses authorizes via the Office 365 OAuth flow, and so the person running the script will be first redirected to your company's Office 365 auth flow. If your organization has an IDaaS layer like Okta, you may be redirected to your Okta auth flow.

The person running the script must be authorized to create a resource group, and the required resources under it. In some organizations, the person creating the resources may be different than the one with the authorization to register the application with Active Directory. The DotAlign Cloud deployment process does support that scenario.

Azure portal view of app registration

For any application to be accessing the Microsoft Graph API, it needs to be "registered" with your tenant's Azure AD. This includes single tenant applications like DotAlign Cloud which are deployed entirely on your company tenant.

The following is a view of the app registration screen inside Azure portal, which lists exactly the permissions required by DotAlign Cloud.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission   Grant admin consent for DotAlign, Inc.

API / Permissions name	Type	Description	Admin Consent Requir...	Status	
˅ Microsoft Graph (12)					...
Calendars.Read	Application	Read calendars in all mailboxes	Yes	✅ Granted for DotAlign, Inc.	...
Contacts.Read	Application	Read contacts in all mailboxes	Yes	✅ Granted for DotAlign, Inc.	...
Directory.Read.All	Delegated	Read directory data	Yes	✅ Granted for DotAlign, Inc.	...
Directory.Read.All	Application	Read directory data	Yes	✅ Granted for DotAlign, Inc.	...
Group.Read.All	Delegated	Read all groups	Yes	✅ Granted for DotAlign, Inc.	...
Group.Read.All	Application	Read all groups	Yes	✅ Granted for DotAlign, Inc.	...
Mail.Read	Application	Read mail in all mailboxes	Yes	✅ Granted for DotAlign, Inc.	...
openid	Delegated	Sign users in	-	✅ Granted for DotAlign, Inc.	...
profile	Delegated	View users' basic profile	-	✅ Granted for DotAlign, Inc.	...
User.Read	Delegated	Sign in and read user profile	-	✅ Granted for DotAlign, Inc.	...
User.Read.All	Delegated	Read all users' full profiles	Yes	✅ Granted for DotAlign, Inc.	...
User.Read.All	Application	Read all users' full profiles	Yes	✅ Granted for DotAlign, Inc.	...

Contact us

If you have any questions about Azure, deployment or any aspect of DotAlign Cloud, please feel free to reach out to us at team@dotalign.com or call our office at 212 706 8630.

Related links

1. **Azure Active Directory**
   https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

2. **Resource management in Azure**
   https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/resource-consistency/resource-access-management

3. **App service plans overview**
   https://docs.microsoft.com/en-us/azure/app-service/overview-hosting-plans

4. **Transparent Data Encryption (TDE) – aka, encryption at rest**
   https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql

5. **Azure SQL Database service, an overview**
   https://docs.microsoft.com/en-us/azure/sql-database/sql-database-technical-overview

6. **Azure Functions, an overview**

https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview

7. **Azure Web Apps, an overview**
   https://docs.microsoft.com/en-us/azure/app-service

8. **Azure Storage Service Encryption, an overview**
   https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

9. **Microsoft Graph API, an overview**
   https://docs.microsoft.com/en-us/graph/overview

10. **Dynamic Data Masking (DDM)**
    https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-2017

11. **Azure SQL firewall rules**
    https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure

12. **Azure SQL security, an overview**
    https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview

13. **Microsoft Graph API permissions**
    https://docs.microsoft.com/en-us/graph/permissions-reference