Cloud Ctrl

Data security summary

How data is collected

Cloud Ctrl collects Billing and Usage data from vendors using the credentials provided by users when they configure a cloud account. The permissions required to access data varies based on the vendor but are controlled by the user creating the credential.

Data is transferred directly from the cloud vendor to our platform. This removes the need for data being exported and transferred via insecure methods and devices.

Types of data collected

The data collected is required to display the consumption of products and services and the associated costs. This is meta data and metrics about the services and products in use and does not include any data that is store on or by the services.

The service metadata includes information including:

- **Service Name**, for example *cloud-ctrl-production-usage (microsoft.web/serverfarms)*
- **Service Id**
- **Product Name,** for example *Premium Functions: vCPU Duration*
- **Region,** for example *Oceania (Australia Southeast)*
- **Tags**
- **Qty Consumed with Unit type**
- **Cost**
- **Resource Group**

Data storage

Cloud Ctrl is a cloud-based SaaS platform built on top of Azure PaaS offerings. All resources are hosted in the Microsoft Azure regions Australia East and Australia South East. Data is physically kept within Australia, and all data I encrypted during transfer and at rest.

Credential Storage

Credentials like API Keys and secrets are stored using Azure Key Vault and are only accessible to Cloud Ctrl Administrators and the Cloud Ctrl Platform via Azure Managed Identities.

Credentials – Azure Advanced

In addition to a usage connection Cloud Ctrl can connect directly to the Azure Resource Manager (ARM) to collection addition information about your Azure infrastructure. To do this Cloud Ctrl use an Azure AD Application credential.

Azure AD Applications are identities that you create and control within your own AD tenant and can be granted privileges on the resources that you specify. These applications have their own login credentials and are intended to be used in code, such as in Cloud Ctrl.

Cloud Ctrl uses the AD Application credential to connect to the ARM and gather metadata and metrics from your subscriptions.

Permissions

The preferred approach is to grant the application identity **READER** role on each of the Subscriptions that are in scope for the health check.

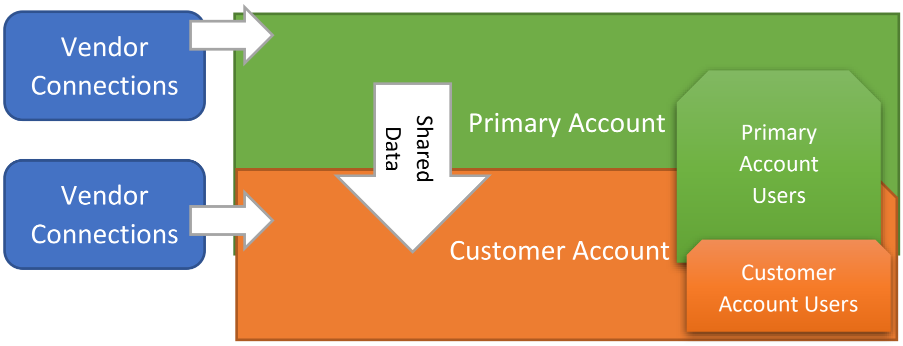
The minimum access requirements and their specific impacts are in the table below. Cloud Ctrl recommend you assign all roles for the best audit outcome. Each role must be assigned **per subscription**.

Azure Role	Description
Cost Management Reader	Can view cost data, cost configuration, and view recommendations.
Monitoring Reader	Can read all monitoring data (metrics, logs, etc.)
Security Reader	View permissions for Security Center. Can view recommendations, alerts, a security policy, and security states, but cannot make changes.

Data Sharing and control

Cloud Ctrl can be configured in several ways to allow partial or full data visibility between parties. Cloud Ctrl has a primary account, which can in turn have customers. The users of the Primary account have administrative control and visibility over the customer's account, but the users of the Customer have no visibility of the Primary Account.

Data can be selectively shared from the Primary account to a customer account, via the shared data feature. In addition to shared data customers can also add connections directly to other vendors.


Vendor Connections
Vendor Connections
Shared Data
Primary Account
Primary Account Users
Customer Account
Customer Account Users