LogLocker for Microsoft Purview eDiscovery

Prerequisites Guide

LogLocker for Microsoft Purview eDiscovery integrates with Log Analytics, Microsoft Sentinel and Defender for Cloud Apps.

This guide walks through the prerequisites required to deploy LogLocker for Microsoft Purview eDiscovery into the chosen Azure subscription.

Once the prerequisites have been met the customer should contact Byzgen to arrange the deployment date. Byzgen aim to deploy LogLocker for Sentinel within 5 working days of confirmation of the prerequisites being met.

The prerequisites required before a deployment date can be confirmed are;

1) **Microsoft Entra Tenant** with a minimum of one Azure subscription.

2) **Azure CLI**

The Azure CLI can be installed on Windows, macOS, and Linux environments. It can also be run in a Docker container and Azure Cloud Shell.

The current version of the Azure CLI is **2.57.0**. Choose your preferred operating system from the list below to install the latest version of Azure CLI:

- Install on Windows
- Install on macOS
- Install on RHEL/CentOS with dnf
- Install on SLES/OpenSUSE with zypper
- Install on Ubuntu/Debian with apt
- Install from script
- Run in Azure Cloud Shell

3) **Microsoft Entra ID** Enterprise Application with the Contributor permissions RBAC role assigned at the Resource Group level where LogLocker service will be deployed.

The values needed for deployment from the Enterprise Application:

- Log Analytics Workspace Name where Microsoft Sentinel is enabled
- Log Analytics Workspace ID
- Azure Subscription ID
- Resource Group Name where LogLocker service will be deployed
- Application (client) ID of the Enterprise Application: See how to register a new Enterprise Application in Microsoft Entra ID
- The client secret of the Enterprise Application. See how to create a client secret for the Enterprise Application
- Microsoft Entra Tenant ID

4) An Azure Billing account exists for the organization - https://learn.microsoft.com/en-us/marketplace/billing-invoicing#billing-and-invoicing-in-azure-marketplace

LogLocker application is invoiced monthly for the chosen term. Billing accounts supported are;

- Enterprise Agreement (EA)
- Microsoft Customer Agreement (MCA)
- Microsoft Online Service Program (MOSP) or pay-as-you-go
- Microsoft Partner Agreement (MPA)

5) Terraform CLI & Azure Client

Terraform uses client ID and secret to authenticate to Azure. Terraform can be installed on different operating systems. The current version of Terraform CLI is **1.7.3**. Choose your preferred OS from the list below to install the latest Terraform CLI:

- Install on Windows
- Install on Linux
- Install on macOS

Terraform Cloud account (optional)

Terraform input variables for the following four root modules:

- Infrastructure: Provisions infrastructure on Azure
- Platform: Deploys Falkor platform to Kubernetes cluster on Azure Kubernetes Engine
- Admin: Creates tenants per project
- *(Optional) Events: Deploys Event Listener and ElasticSearch credentials*

6) Microsoft Sentinel

Microsoft Sentinel deployed on top of one Log Analytics Workspace.

For more information, please refer to the deployment guide for Microsoft Sentinel.

This assumes that the customer has basic knowledge of managing Microsoft Sentinel Analytics Rules and is familiar with Kusto Query Language (KQL).

Enable Data Connector - **Microsoft Defender for Cloud Apps**

7) Microsoft Purview eDiscovery

Microsoft Purview eDiscovery deployed and licenced with either Standard or Premium. Event and audit logs will be limited to what is enabled by the licence in use.

8) Microsoft Defender XDR

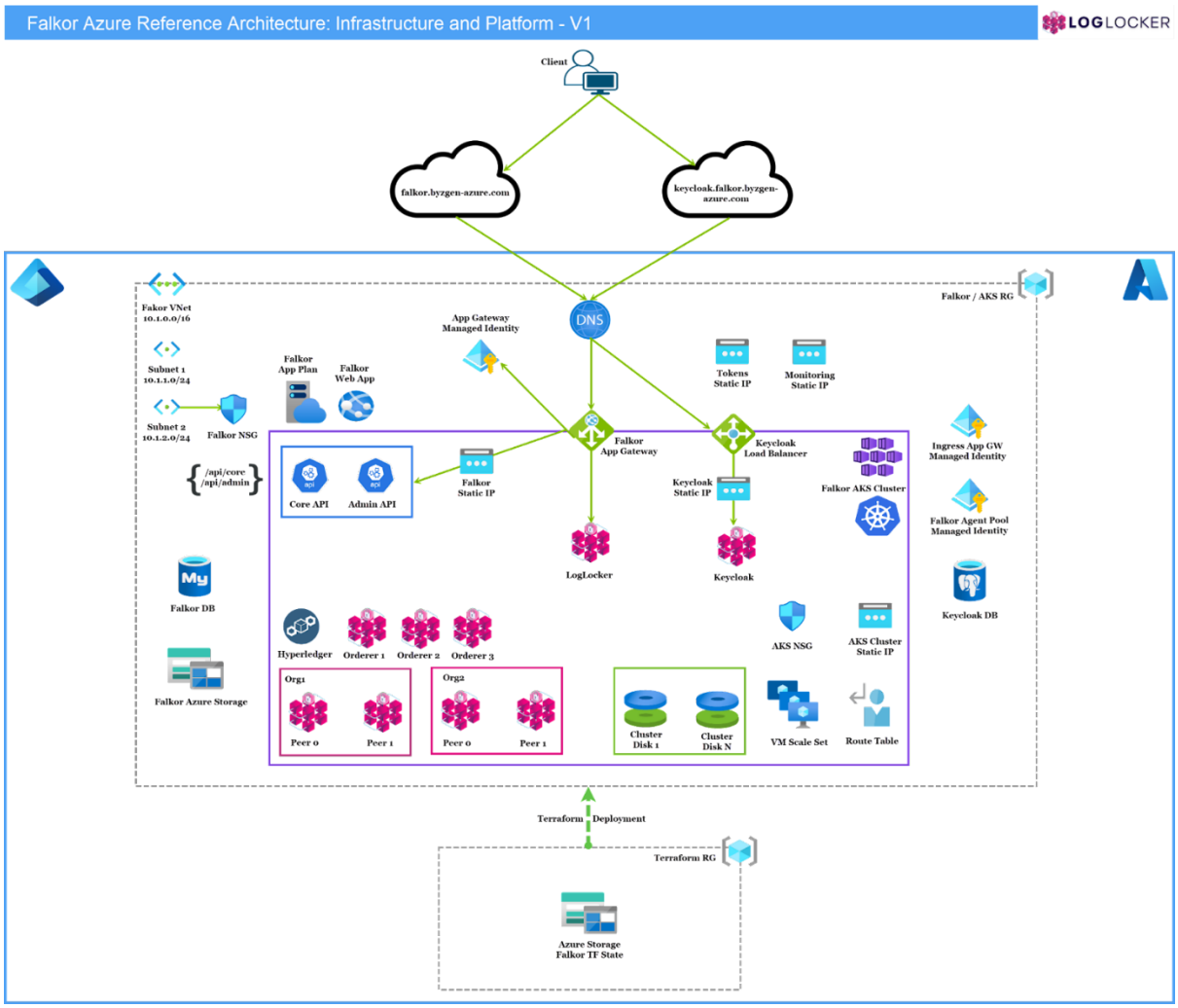
Microsoft Defender XDR is licenced and enabled and connected to the Microsoft Sentinel / Log Analytics Workspace.

9) Power BI

A valid Power BI subscription is required if the customer wants to use the Power BI Templates provided as part of the LogLocker for Purview eDiscovery v1.

Other search and discovery platforms will be supported in the upcoming releases.

Reference Architecture



Troubleshooting

For support with troubleshooting email support@log-locker.com.