YouTestMe

Logging

Table of Contents

1 Introduction

This document provides answers to the most frequently asked questions about logging.

Answers are all related to the mechanism provided by YouTestMe's hosting provider - Microsoft Azure.

2 FAQ

2.1 What activities are logged by the provider?

Azure provides various logging and monitoring capabilities to help you track and analyze activities within your virtual machine (VM) infrastructure. Here are some activities that are typically logged:

1. Network Traffic, File, and Server Access:
    - Azure Network Security Group (NSG) logs: These logs capture inbound and outbound network traffic, including IP addresses, ports, protocols, and traffic patterns.
    - Azure Storage logs: If you use Azure Storage, it can generate logs related to file access, including read and write operations on storage accounts and containers.
2. Security Systems:
    - Azure Security Center logs: This service provides security recommendations and can log security-related events, such as vulnerability assessments, threat intelligence, and security alerts.
    - Azure Active Directory (AD) logs: Azure AD logs record authentication and authorization events, including user sign-ins, role assignments, and registrations.
3. Databases and Servers:
    - Azure Database logs: Azure offers various database services like Azure SQL Database, Azure Cosmos DB, and Azure Database for PostgreSQL. These services typically provide auditing and diagnostic logs for database activities.
    - Azure Monitor: This service allows you to collect and analyze logs from virtual machines, including performance metrics, diagnostic logs, and custom application logs.
4. Active Directory:
    - Azure Active Directory logs: Azure AD logs capture activities related to user management, authentication, and authorization within the Azure AD environment.
5. Web and Mail Servers:
    - Web server logs: If you are using Apache or other web servers on your virtual machines, they can generate access logs that record details about incoming requests, URLs accessed, user agents, and more.
    - Mail server logs: If you have configured mail servers, they may generate logs related to incoming and outgoing emails, SMTP transactions, and mail delivery status.
6. VPN Systems:
    - Azure VPN Gateway logs: If you are using Azure VPN Gateway to establish virtual private network connections, it can generate logs related to connection establishment, authentication, and disconnection events.
7. VM Systems:
    - Azure Monitor for VMs: This service provides insights into the performance and health of virtual machines, including metrics like CPU usage, disk I/O, memory utilization, and network traffic.

2.2 Does the provider's logging framework allow isolation of an incident to specific tenants?

Azure provides several mechanisms to ensure that logging and monitoring data remains isolated and accessible only to the respective tenant:

1. Azure Active Directory (Azure AD): Azure AD is a cloud-based identity and access management service. It provides authentication and authorization services, allowing each tenant to have its own isolated directory with separate user accounts and access controls.

2. Azure Resource Groups and Role-Based Access Control (RBAC): Azure Resource Groups are logical containers for organizing and managing resources. RBAC allows you to grant specific permissions to users or groups at the resource group level or even down to individual resources. This means you can restrict access to the logging and monitoring resources for a particular tenant or set of users.

3. Azure Log Analytics Workspaces: Azure Log Analytics is a central logging and monitoring service that collects and analyzes data from various Azure resources and external sources. Log Analytics Workspaces can be created at the subscription level, allowing you to isolate logs and monitoring data for specific tenants or applications within separate workspaces. Access to each workspace can be controlled through RBAC, ensuring that only authorized users can view the data.

4. Azure Monitor Access Control: Azure Monitor, which provides monitoring and alerting capabilities, allows you to define alerts and actions based on specific conditions or metrics. Access to Azure Monitor and its associated features, such as alerts and action groups, can be controlled using RBAC, enabling you to restrict access to specific tenants or users.

By leveraging these features, Azure allows you to isolate logging and monitoring data, control access to these resources, and ensure that incidents and data related to a specific tenant or customer remain separate and secure.

2.3 Who can set up activities to be logged?

1. Cloud Provider (Microsoft):
   Microsoft Azure provides built-in logging and monitoring capabilities for various services and resources. As the cloud provider, Microsoft configures and manages the logging infrastructure at the platform level, ensuring that essential logs are captured. Microsoft sets up logging activities for core Azure services, such as Azure Network Security Group (NSG) logs, Azure Storage logs, Azure Active Directory (AD) logs, and Azure Database logs. These logs are generated by default or can be enabled through specific configuration options.
2. Tenant (Application Owner):
   As the tenant or application owner, you have the responsibility to configure and enable logging for the resources and services that you deploy within your Azure environment. This includes activities such as:
   - Configuring Virtual Machines (VMs): For VMs, you can enable diagnostic settings to collect performance metrics, diagnostic logs, and custom application logs using Azure Monitor.
   - Setting up Web and Mail Servers: If you have Apache web servers or other web servers running on your VMs, you need to configure the web server software to generate access logs. Similarly, if you have mail servers, you will configure the mail server software to generate relevant logs.
   - Enabling Azure Security Center: Azure Security Center provides security recommendations and can log security-related events. You would need to enable and configure Azure Security Center to capture and analyze security logs for your resources.
   - Defining Azure Monitor Workspaces: For centralized logging and monitoring with Azure Log Analytics, you would create Log Analytics Workspaces at the subscription level and configure the necessary data sources and agents to collect logs from your resources.

Setting up Azure Monitor Alerts: Azure Monitor allows you to define alerts and actions based on specific conditions or metrics. You can configure alerts to notify you when specific events or thresholds are triggered.

2.4 Who has access to these logs?

1. Tenant (Application Owner):
   As the tenant or application owner, you have access to the logs generated by the resources and services deployed within your Azure environment. Your level of access depends on the roles and permissions assigned to your Azure account. You can view and analyze the logs through Azure's logging and monitoring services, such as Azure Monitor and Azure Log Analytics, based on the access controls configured for your account.
2. Azure Subscription Administrators:
   Azure subscription administrators, including the global administrator and other administrative roles within the Azure Active Directory, have access to logs at the subscription level. These administrators can view and manage logs across the resources within the subscription. It's important to carefully manage and restrict access to subscription-level logs to maintain security and privacy.
3. Azure Role-Based Access Control (RBAC):
   RBAC allows you to grant granular access control to specific resources and services within Azure. By assigning appropriate roles and permissions, you can control who has access to the logs of particular resources. RBAC enables you to assign access to specific individuals or groups within your organization, limiting access to only those who need it.
4. Azure Monitor and Log Analytics Users:
   Users specifically granted access to Azure Monitor and Azure Log Analytics workspaces can access and analyze logs within those workspaces. Access to these services can be controlled using RBAC, allowing you to grant access to relevant individuals or teams responsible for monitoring and analyzing logs.

Additionally, it's worth noting that Microsoft Azure has implemented security measures and compliance standards to protect customer data and maintain the confidentiality of logs. These measures include encryption of data in transit and at rest, data isolation, and compliance with industry standards and regulations.

2.5 How long are logs maintained by the provider?

Azure offers various logging and monitoring services, and the retention periods for logs can differ based on these services. Here are some factors to consider:

1. Azure Activity Logs:
   Azure Activity Logs provide insights into operations performed on resources within your Azure subscription. By default, Azure retains these logs for 90 days. However, you have the option to extend the retention period up to 365 days by configuring diagnostic settings on the Azure Monitor service.
2. Azure Monitor Logs:
   Azure Monitor allows you to collect and analyze logs from various Azure resources and external sources through Log Analytics workspaces. The retention period for logs stored in Azure Monitor Logs can be configured based on your requirements. You can choose to retain logs for as short as one day or extend the retention period to several years, depending on the pricing tier and storage capacity you select for the Log Analytics workspace.
3. Azure Storage Logs:
   If you enable logging for Azure Storage accounts, you have control over the retention period for the storage logs. You can configure the retention period as per your needs, ranging from a minimum of one day to a maximum of indefinitely.

Azure Security Center Logs:
Azure Security Center provides security recommendations and logs security-related events. The retention period for these logs can vary depending on the type of event. For example, security recommendations are retained for 90 days, while security alerts and other security-related logs are retained for 90 days by default but can be extended up to 365 days.