Logging and Auditing in microsoft Azure

Published: March 2017

Contents

[1.0 Introduction 3](#_Toc474923253)

[1.1 Overview 3](#_Toc474923254)

[1.2 Azure Platform 3](#_Toc474923255)

[1.3 Abstract 3](#_Toc474923256)

[2.0 Activity Log 4](#_Toc474923257)

[3.0 Service Specific Logs 5](#_Toc474923258)

[3.1 Activity Logs 5](#_Toc474923259)

[3.2 Azure Diagnostic Logs 5](#_Toc474923260)

[3.2.1 What you can do with Diagnostic Logs 5](#_Toc474923261)

[3.2.2 Diagnostic Settings 6](#_Toc474923262)

[3.3 For Infrastructure 6](#_Toc474923263)

[3.3.1 AAD Log (Azure Active Directory log) 7](#_Toc474923264)

[3.3.2 Compute Service Logs 7](#_Toc474923265)

[3.3.2.1 Azure Cloud Services and Virtual Machines 8](#_Toc474923266)

[3.3.2.2 Azure App Service (Web App) 9](#_Toc474923267)

[3.3.2.2.1 Web Server Diagnostics 9](#_Toc474923268)

[3.3.2.2.2 Application Diagnostics 10](#_Toc474923269)

[3.3.2.3 Mobile Engagement Services 10](#_Toc474923270)

[3.3.2.3.1 Troubleshooting with Monitor - Events - Details 10](#_Toc474923271)

[3.3.2.3.2 Troubleshooting with Monitor - Crashes - Details 10](#_Toc474923272)

[3.3.2.4 Azure logic Apps 10](#_Toc474923273)

[3.3.2.5 Azure Batch Services 11](#_Toc474923274)

[3.3.2.6 Service Logs 11](#_Toc474923275)

[3.3.3 Networking Logs 11](#_Toc474923276)

[3.3.3.1 Azure Application Gateways 12](#_Toc474923277)

[3.3.3.2 Azure Load Balancer 12](#_Toc474923278)

[3.3.3.3 Azure Network Security Group 12](#_Toc474923279)

[3.3.4 Storage Logs 13](#_Toc474923280)

[3.3.4.1 Azure Database SQL Auditing 13](#_Toc474923281)

[3.3.4.2 Azure SQL Data Warehouse 14](#_Toc474923282)

[3.3.4.3 Azure Radis Cache 14](#_Toc474923283)

[3.3.4.4 Azure Data Lake Store 14](#_Toc474923284)

[3.3.4.5 Azure Data Factory 15](#_Toc474923285)

[3.4 Internet of Things 15](#_Toc474923286)

[3.5 Enterprise Integration 16](#_Toc474923287)

[3.5.1 BizTalk Services 16](#_Toc474923288)

[3.5.2 StorSimple 16](#_Toc474923289)

[3.6 Intelligence + Analytics 16](#_Toc474923290)

[3.6.1 Azure HDInsight Service 16](#_Toc474923291)

[3.6.2 Azure Machine Learning Service 17](#_Toc474923292)

[3.6.3 Azure Data Lake Analytics Service 17](#_Toc474923293)

[3.6.4 Azure Data Lake Store Service 17](#_Toc474923294)

[3.6.5 Azure PowerBI Embedded Service 17](#_Toc474923295)

[3.6.6 Azure Key Vault 17](#_Toc474923296)

[3.7 Monitoring & Management 18](#_Toc474923297)

[3.7.1 Azure Backup Service 18](#_Toc474923298)

[3.7.2 Developers Tools 18](#_Toc474923299)

[3.7.2.1 Azure API Management – Custom Logs 18](#_Toc474923300)

[3.7.2.2 Application Insights 18](#_Toc474923301)

[3.7.2.3 Application Diagnostic Logs 18](#_Toc474923302)

# 1.0 Introduction

## 1.1 Overview

To assist current and prospective Azure customers in understanding and using the various security-related capabilities available in and surrounding the Azure Platform, Microsoft has developed a series of white papers, security overviews, best practices and checklists. The topics range in terms of breadth and depth and will be updated periodically. This document is part of that series as summarized in the Abstract section below.

## 1.2 Azure Platform

Azure is an open and flexible cloud service platform that supports the broadest selection of operating systems, programming languages, frameworks, tools, databases and devices.

For example, you can:

* Run Linux containers with Docker integration.
* Build apps with JavaScript, Python, .NET, PHP, Java and Node.js
* Build back-ends for iOS, Android and Windows devices.

Azure public cloud services support the same technologies millions of developers and IT professionals already rely on and trust.

When you build on, or migrate IT assets to, a cloud provider, you are relying on that organization’s abilities to protect your applications and data with the services and the controls they provide to manage the security of your cloud-based assets.

Azure’s infrastructure is designed from the facility to applications for hosting millions of customers simultaneously, and it provides a trustworthy foundation upon which businesses can meet their security needs. In addition, Azure provides you with a wide array of configurable security options and the ability to control them so that you can customize security to meet the unique requirements of your deployments. This document will help you meet these requirements.

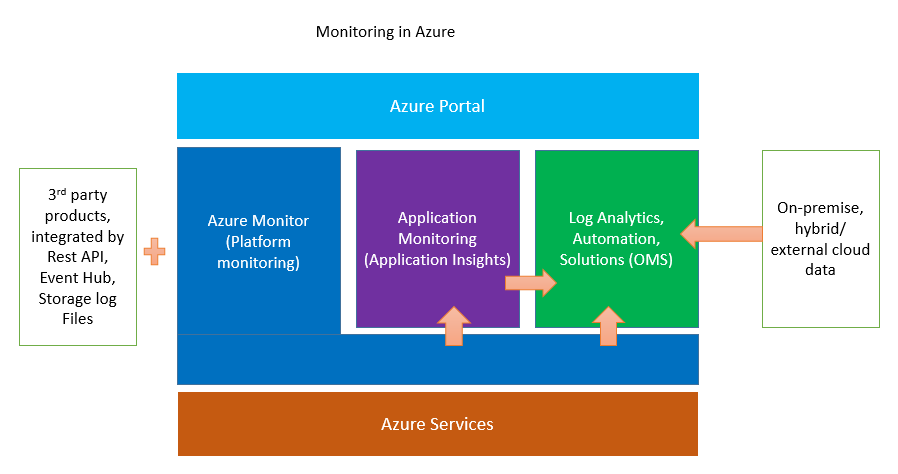
## 1.3 Abstract

The security logs in Microsoft Azure Cloud Services (which provides Platform as a Service or PaaS) and Virtual Machines (which provides Infrastructure as a Service or IaaS) contain vital information that can provide intelligence and powerful insights into the following security issues:

* Policy violations
* Internal and external threats
* Regulatory compliance
* Network, host, and user activity anomalies

This whitepaper provides an introduction for generating, collecting, and analyzing security logs from services hosted on Azure, and it can help you gain security insights into your Azure deployments. The scope of this white paper is limited to applications and services built and deployed in Azure and that are using the Windows Server operating system.

Figure 1 Monitoring in Azure



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Activity Log | [Activity Log](https://docs.microsoft.com/en-in/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) |  |  |  |  |  |
| Service Specific Logs | [Activity Logs](https://docs.microsoft.com/en-in/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) | [Azure Diagnostic Logs](https://docs.microsoft.com/en-in/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs) | [For Infrastructure](https://docs.microsoft.com/en-in/azure/active-directory/active-directory-reporting-audit-events) | [Internet of Things](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-stream-activity-logs-event-hubs) | [Enterprise Integration](https://azure.microsoft.com/en-us/resources/videos/enterprise-integration-with-azure-logic-apps/) | [Intelligence + Analytics](https://docs.microsoft.com/en-in/azure/hdinsight/hdinsight-debug-jobs) |
| Logging as a Service | [For Applications](https://docs.microsoft.com/en-in/azure/application-insights/app-insights-search-diagnostic-logs) |  |  |  |  |  |

# 2.0 Activity Log

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Activity Log | [Activity Log](https://docs.microsoft.com/en-in/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) |  |  |  |  |  |

The [Azure Activity Log](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs), provides insight into the operations that were performed on resources in your subscription. The Activity Log was previously known as “Audit Logs” or “Operational Logs,” since it reports [control-plane events](https://driftboatdave.com/2016/10/13/azure-auditing-options-for-your-custom-reporting-needs/) for your subscriptions. Using the Activity Log, you can determine the “what, who, and when” for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties. The Activity Log does not include read (GET) operations.

Here PUT, POST, DELETE refers to all the write operations activity log contains on the resources. For example, you can use the audit logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.

# 3.0 Service Specific Logs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Service Specific Logs | [Activity Logs](https://docs.microsoft.com/en-in/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) | [Azure Diagnostic Logs](https://docs.microsoft.com/en-in/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs) | [For Infrastructure](https://docs.microsoft.com/en-in/azure/active-directory/active-directory-reporting-audit-events) | [Internet of Things](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-stream-activity-logs-event-hubs) | [Enterprise Integration](https://azure.microsoft.com/en-us/resources/videos/enterprise-integration-with-azure-logic-apps/) | [Intelligence & Analytics](https://docs.microsoft.com/en-in/azure/hdinsight/hdinsight-debug-jobs) |

## 3.1 Activity Logs

The activity log contains all write operations (PUT, POST, and DELETE) performed on your resources. It does not include read operations (GET). You can use the audit logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.

**Export the Activity Log with Log Profiles**

A Log Profile controls how your Activity Log is exported. Using a Log Profile, you can configure:

* Where the Activity Log should be sent (Storage Account or [Event Hubs](https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-what-is-event-hubs))
* Which event categories (Write, Delete, Action) should be sent
* Which [regions (locations)](https://azure.microsoft.com/en-in/regions/) should be exported
* How long the Activity Log should be retained in a Storage Account – a retention of zero days means logs are kept forever. Otherwise, the value can be any number of days between 1 and 2147483647. If retention policies are set, but storing logs in a Storage Account is disabled (for example, if only Event Hubs or [OMS](https://docs.microsoft.com/en-us/azure/operations-management-suite/operations-management-suite-overview) options are selected), the retention policies have no effect.

## 3.2 Azure Diagnostic Logs

Azure Diagnostic Logs are emitted by a resource that provide rich, frequent data about the operation of that resource. The content of these logs varies by resource type (for example, [Windows event system logs](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-sources-windows-events) are one category of Diagnostic Log for VMs and [blob, table, and queue logs](https://docs.microsoft.com/en-us/azure/storage/storage-monitor-storage-account) are categories of Diagnostic Logs for storage accounts) and differ from the Activity Log, which provides insight into the operations that were performed on resources in your subscription.

[How Diagnostic Logs differ from Audit logs:](https://azure.microsoft.com/en-in/blog/diagnostic-logs-streaming-to-event-hubs/)

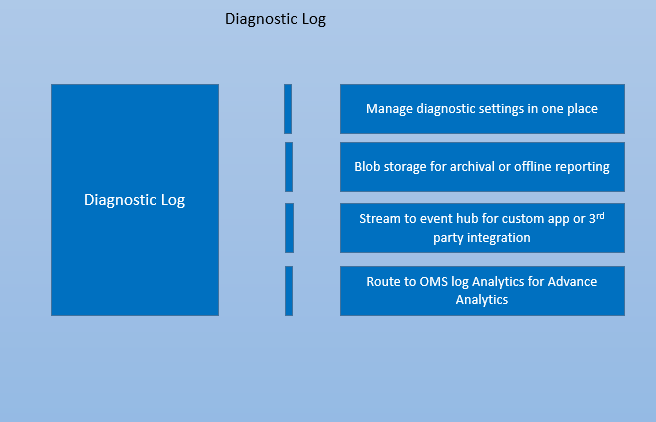
[Diagnostic Logs](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs), are all logs emitted by a resource, whereas [Audit Logs](https://azure.microsoft.com/en-us/documentation/articles/resource-group-audit/), provide insight into the operations that were performed on resources in your subscription.

### 3.2.1 What you can do with Diagnostic Logs

Here are some of the things you can do with Diagnostic Logs:

* Save them to a Storage Account for auditing or manual inspection. You can specify the retention time (in days) using the Diagnostic Settings.
* Stream them to Event Hubs for ingestion by a third-party service or custom analytics solution such as [PowerBI](https://powerbi.microsoft.com/en-us/documentation/powerbi-azure-and-power-bi/).
* Analyze them with [OMS Log Analytics](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-overview).

Figure 2 Diagnostic Log



### 3.2.2 Diagnostic Settings

Diagnostic Logs for [non-compute resources](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-enable-diagnostic-logs-using-template) are configured using [Diagnostic Settings for a resource control](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs):

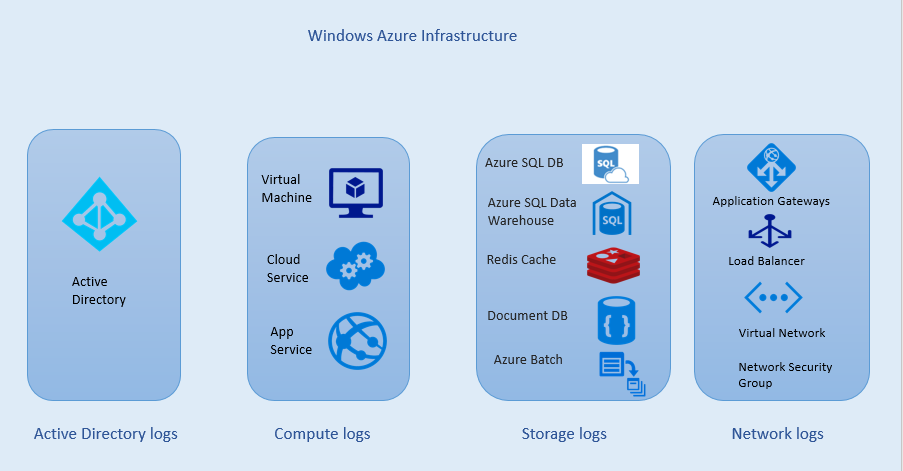
* Where Diagnostic Logs are sent.
* Which Log Categories are sent.
* How long each log category should be retained in a Storage Account – a retention of zero days means that logs are kept forever. Otherwise, this value can range from 1 to 2147483647.
* If retention policies are set but storing logs in a Storage Account is disabled (for example if only Event Hubs or OMS options are selected), the retention policies have no effect.

## 3.3 For Infrastructure

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service Specific Logs | [AAD Log (Azure Active Directory log)](https://docs.microsoft.com/en-in/azure/active-directory/active-directory-reporting-audit-events) | [Compute Service Logs](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs) | [Networking Logs](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-networking-analytics) | [Storage Logs](https://docs.microsoft.com/en-us/rest/api/storageservices/fileservices/enabling-storage-logging-and-accessing-log-data) |

The Infrastructure Service layer contains [Azure Active directory log](https://blogs.msdn.microsoft.com/azuresecurity/2015/06/11/azure-active-directory-audit-logs/), [compute log](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs), [storage log](https://docs.microsoft.com/en-us/rest/api/storageservices/fileservices/enabling-storage-logging-and-accessing-log-data) and [network log](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-networking-analytics).

Figure 3 Microsoft Azure Infrastructure



### 3.3.1 AAD Log

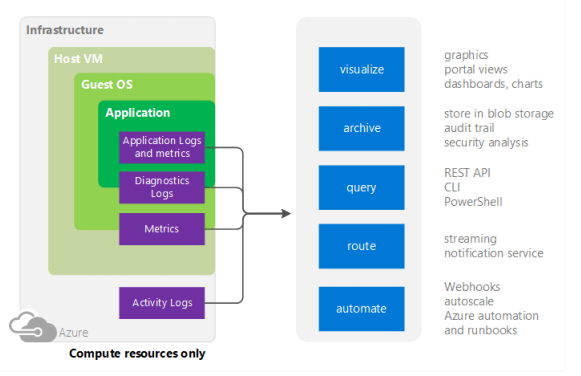
* The identities of administrative users are authenticated through Active Directory on Windows Server 2016 or Azure Active Directory in the cloud.
* The [Azure Active Directory Audit Report](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-audit-events) helps customers to identify privileged actions that occurred in their Azure Active Directory. Privileged actions include elevation changes (for example, role creation or password resets), changing policy configurations (for example password policies), or changes to directory configuration (for example, changes to domain federation settings).
* The reports provide the audit record for the event name, the actor who performed the action, the target resource affected by the change, and the date and time (in UTC). Customers are able to retrieve the list of audit events for their Azure Active Directory via the [Azure Portal](https://portal.azure.com/), as described in [View your Audit Logs](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-azure-portal).

### 3.3.2 Compute Service Logs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Compute Service Logs | [Azure Cloud Services and Virtual Machines](https://docs.microsoft.com/en-in/azure/cloud-services/cloud-services-diagnostics-powershell) | [Azure App Service (Web App)](https://docs.microsoft.com/en-in/azure/app-service-web/web-sites-enable-diagnostic-log) | [Mobile Engagement Services](https://docs.microsoft.com/en-in/azure/mobile-engagement/mobile-engagement-user-interface-monitor) | [Azure Logic Apps](https://docs.microsoft.com/en-us/azure/app-service-logic/app-service-logic-scenario-error-and-exception-handling) | [Azure Batch Services](https://docs.microsoft.com/en-us/azure/batch/batch-diagnostics) |

Compute logs Discovers logs for [Azure VM](https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-overview?toc=%2fazure%2fvirtual-machines%2fwindows%2ftoc.json), [Azure Cloud Service](https://azure.microsoft.com/en-in/services/cloud-services/), [Azure App service](https://docs.microsoft.com/en-us/azure/app-service/app-service-value-prop-what-is) (Web App).

Figure 4 Compute Log



#### 3.3.2.1 Azure Cloud Services and Virtual Machines

Diagnostic log- These are logs emitted by a resource that provide rich, frequent data about the operation of that resource. The content of these logs varies by resource type.

You can collect diagnostic data like application logs, performance counter, Windows Event logs, .NET Event Source, IIS Logs, Manifest based ETW, Crash dumps, Custom error logs, Azure Diagnostic infrastructure logs etc. from a [Cloud Service](https://azure.microsoft.com/en-in/services/cloud-services/) using the [Azure Diagnostics extension](https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-extensions-diagnostics-template). The sources of diagnostic data for Microsoft Azure Cloud Services (web and worker roles) is in many ways the same as on-premises solutions. We can continue to use Windows event logs, IIS logs, performance counters, and custom logs. We can even use RDP to connect to a machine instance and view the data. [Diagnostics logs](https://azure.microsoft.com/en-us/documentation/articles/cloud-services-dotnet-diagnostics/) can be used for Virtual Machines and Cloud Services. These logs include:

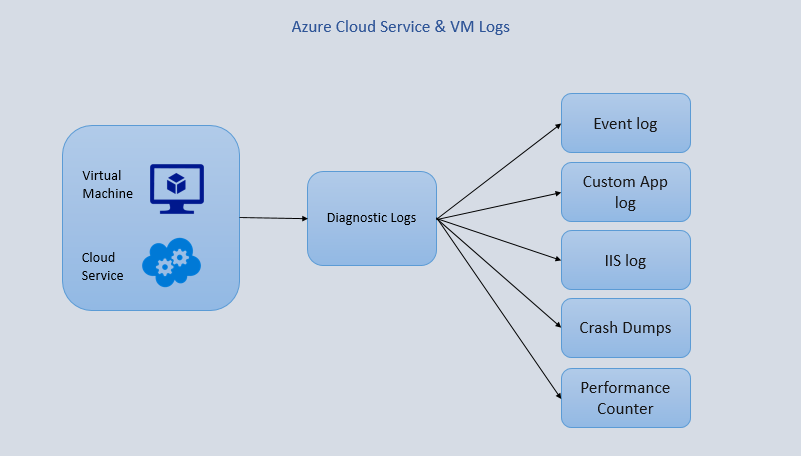
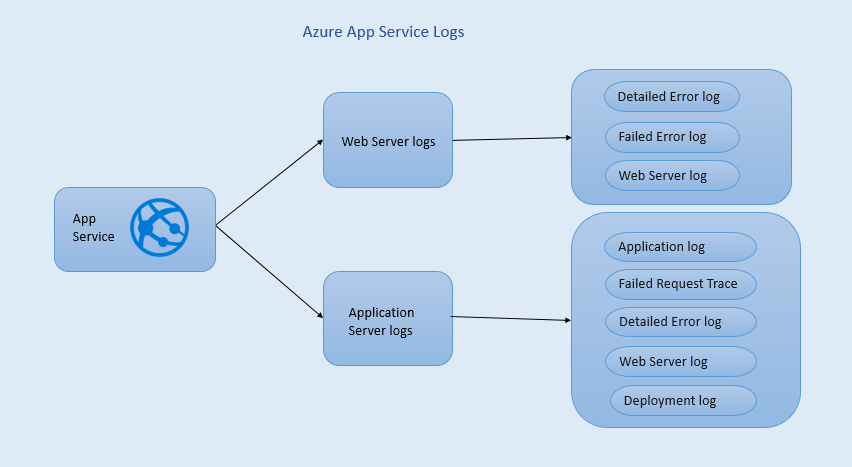


Figure 5 Azure Cloud Service & VM Logs

#### 3.3.2.2 Azure App Service (Web App)

|  |  |  |
| --- | --- | --- |
| Azure App Service (Web App) | Web Server Diagnostics | Application Diagnostics |

Figure 6 Azure App Service Log



##### 3.3.2.2.1 Web Server Diagnostics

You can enable or disable the following kinds of logs:

* **Detailed Error Logging** - Detailed error information for HTTP status codes that indicate a failure (status code 400 or greater).
* **Failed Request Tracing** - Detailed information on failed requests, including a trace of the IIS components used to process the request and the time taken in each component.
* **Web Server Logging** - Information about HTTP transactions using the [W3C extended log file format](http://msdn.microsoft.com/library/windows/desktop/aa814385.aspx).

##### 3.3.2.2.2 Application Diagnostics

It allows you to capture the information produced by a Web Application. ASP.NET Applications can use the System.Diagnostics. It traces class to log the information to the [Application diagnostics](http://www.c-sharpcorner.com/article/discuss-diagnostics-logging-in-webapps-of-azure-app-service/) log.

* **Application Logs** - This contains one or more text files containing information produced by application logging.
* **Failed Request Traces** - This folder contains an XSL file and one or more XML files
* **Detailed Error Logs** - This contains one or more .htm files that provide extensive information for any HTTP errors that have occurred.
* **Web Server Logs** - This contains one or more text files formatted using the [W3C extended log file format](http://msdn.microsoft.com/library/windows/desktop/aa814385.aspx).
* **Deployment** **Logs** - This contains logs generated by the internal deployment processes used by Azure web apps, as well as logs for Git deployments.

#### 3.3.2.3 Mobile Engagement Services

|  |  |  |
| --- | --- | --- |
| [Mobile Engagement Services](https://azure.microsoft.com/en-in/services/mobile-engagement/) | Troubleshooting with Monitor - Events - Details | Troubleshooting with Monitor - Crashes - Details |

You can see how many users are currently in session and on specific screens or doing specific actions. You can view user activity divided by Sessions, Jobs, Events, Errors, and Crashes. You can see the current information and show the information from the last hour, day, or week. You can see all of the information in each category or sort by the specific Session, Job, Event, Error, and Crash.

**Monitoring** - [Azure Monitor](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-get-started) is the platform service that provides a single source for monitoring Azure resources. With Azure Monitor, you can visualize, query, route, archive, and take action on the metrics and logs coming from resources in Azure.

##### 3.3.2.3.1 Troubleshooting with Monitor - Events - Details

Generating an event in your application from your test device and finding it in Monitoring section is one of the easiest ways to find your Device ID for your test device and to confirm that Azure Mobile Engagement integration of Analytics, Monitoring, and Segments is working from your application.

##### 3.3.2.3.2 Troubleshooting with Monitor - Crashes - Details

You can review crash information about your app from Monitoring section to help determine why your app is crashing. You should also look up known issues with each version of the SDK in the release notes for each version of the SDK for Android/iOS/Web/Windows/Windows Phone.

#### 3.3.2.4 Azure logic Apps

Choose [Azure DocumentDb](https://azure.microsoft.com/services/documentdb/) as a repository for the log and error records ([DocumentDb](https://azure.microsoft.com/en-in/services/documentdb/) refers to records as documents). Because [Logic Apps](https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-what-are-logic-apps) has a standard template for all responses, we would not have to create a custom schema.

#### 3.3.2.5 Azure Batch Services

|  |  |
| --- | --- |
| Azure Batch Services | Service Logs |

As with many Azure services, the [Batch service](https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview) emits log events for certain resources during the lifetime of the resource. You can enable Azure Batch diagnostic logs to record events for resources like pools and tasks, and then use the logs for [diagnostic evaluation and monitoring](https://docs.microsoft.com/en-us/azure/best-practices-monitoring). Events like pool create, pool delete, task start, task complete, and others are included in [Batch diagnostic logs](https://docs.microsoft.com/en-us/azure/batch/batch-diagnostics).

[**Getting Batch diagnostic log**](https://docs.microsoft.com/en-us/azure/batch/batch-diagnostics)

To persist Batch diagnostic logs, you must create an Azure Storage account where Azure will store the logs. You specify this Storage account when you [enable diagnostic logging](https://docs.microsoft.com/en-us/azure/batch/batch-diagnostics#enable-diagnostic-logging) for your Batch account

#### 3.3.2.6 Service Logs

Azure Batch Service Logs contain events emitted by the Azure Batch service during the lifetime of a Batch resource like a pool or task. Each event emitted by Batch is stored in the specified Storage account in JSON format. The Batch service currently emits the following Service Log events:

* Pool Create, [Pool delete start](https://msdn.microsoft.com/library/azure/mt743610.aspx), [Pool delete complete](https://msdn.microsoft.com/library/azure/mt743618.aspx), [Pool resize start](https://msdn.microsoft.com/library/azure/mt743609.aspx), [Pool resize complete](https://msdn.microsoft.com/library/azure/mt743608.aspx), [Task start](https://msdn.microsoft.com/library/azure/mt743616.aspx), [Task complete](https://msdn.microsoft.com/library/azure/mt743612.aspx), [Task fail](https://msdn.microsoft.com/library/azure/mt743607.aspx)

### 3.3.3 Networking Logs

|  |  |  |  |
| --- | --- | --- | --- |
| Networking Logs | [Azure Application Gateways](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-diagnostics) | [Azure Load Balancer](https://azure.microsoft.com/en-in/documentation/articles/load-balancer-monitor-log/) | Azure Network Security Group |

The networking layer contains log sabout various services like Application Gateways, Load balancer and network security group.

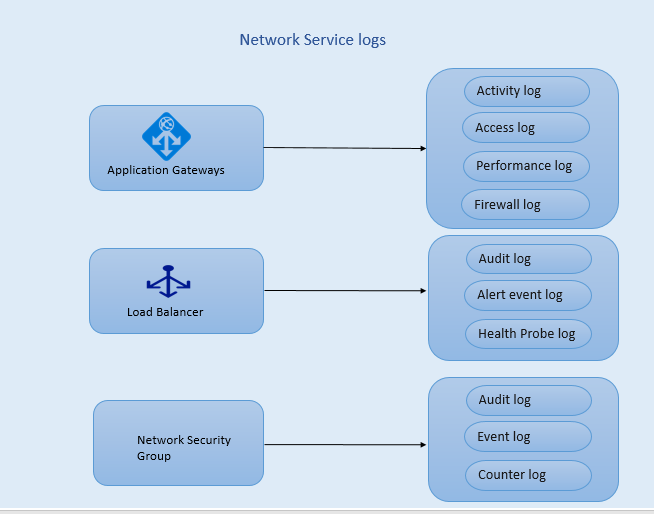


Figure 7 Network Service Logs

#### 3.3.3.1 [Azure Application Gateways](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-introduction)

It provides Application Delivery Controller (ADC) as a service, offering various layer 7 load balancing capabilities for your application. It allows customers to optimize web farm productivity by offloading CPU intensive SSL termination to the Application Gateway.

* **Activity Log** - The [Azure Activity Log](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) is a log that provides insight into the operations that were performed on resources in your subscription. The Activity Log was previously known as “Audit Logs” or “Operational Logs”.

You can use [Azure Activity Log](https://azure.microsoft.com/en-us/documentation/articles/insights-debugging-with-events/) (formerly known as Operational Logs and Audit Logs) to view all operations being submitted to your Azure subscription, and their status.

* **Access Logs** - You can use this log to view application gateway access pattern and analyse important information including caller's IP, URL requested, response latency, return code, bytes in and out. Access log is collected every 300 seconds.
* **Performance Logs** - You can use this log to view how application gateway instances are performing. This log captures performance information on per instance basis including total request served, throughput in bytes, total requests served, failed request count, healthy and unhealthy back-end instance count.
* **Firewall Logs** - You can use this log to view the requests that are logged through either detection or prevention mode of an application gateway that is configured with web application firewall.

#### 3.3.3.2 [Azure Load Balancer](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview)

It delivers high availability and network performance to your applications. It is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy instances of services defined in a load-balanced set.

You can use different types of logs in Azure to manage and troubleshoot load balancers. Some of these logs can be accessed through the portal. All logs can be extracted from an Azure blob storage, and viewed in different tools, such as Excel and PowerBI. You can learn more about the different types of logs from the list below.

* **Audit Logs** - You can use [Azure Audit Logs](https://azure.microsoft.com/en-in/documentation/articles/insights-debugging-with-events/) (formerly known as Operational Logs) to view all operations being submitted to your Azure subscription(s), and their status. Audit logs are enabled by default, and can be viewed in the Azure portal.
* **Alert Event Logs** - You can use this log to view what alerts for load balancer are raised. The status for the load balancer is collected every five minutes. This log is only written if a load balancer alert event is raised.
* **Health Probe Logs** -You can use this log to check for probe health check status, how many instances are online in the load balancer back-end and percentage of virtual machines receiving network traffic from the load balancer. This log is written on probe status event change.

#### 3.3.3.3 Azure Network Security Group

You can use different types of logs in Azure to manage and troubleshoot NSGs. Some of these logs can be accessed through the portal, and all logs can be extracted from an Azure blob storage, and viewed in different tools, such as [Log Analytics](https://azure.microsoft.com/en-in/documentation/articles/log-analytics-azure-networking-analytics/), Excel and PowerBI. You can learn more about the different types of logs from the list below.

* **Audit Logs**- You can use [Azure Audit Logs](https://azure.microsoft.com/en-in/documentation/articles/insights-debugging-with-events/) to view all operations being submitted to your Azure subscription(s), and their status.
* **Event Logs**- You can use this log to view what NSG rules are applied to VMs and instance roles based on MAC address. The status for these rules is collected every 60 seconds.
* **Counter Logs**- You can use this log to view how many times each NSG rule was applied to deny or allow traffic.

### 3.3.4 Storage Logs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Storage Logs | [Azure Database SQL Auditing](https://azure.microsoft.com/en-us/documentation/articles/sql-database-auditing-get-started/) | [Azure SQL Data Warehouse](https://docs.microsoft.com/en-us/azure/sql-data-warehouse/sql-data-warehouse-auditing-overview) | Azure Radis Cache | Azure Data Lake Store | [Azure Data Factory](https://docs.microsoft.com/en-in/azure/data-factory/data-factory-monitor-manage-pipelines) |

#### 3.3.4.1 Azure Database SQL Auditing

Azure SQL Database Auditing tracks database events and writes them to an audit log in your Azure Storage account. Auditing can help you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations. SQL Database Auditing allows you to retain an audit trail of selected events. You can define categories of database actions to be audited and also allows to report on database activity. There are two Auditing methods:

* **Blob Auditing** - logs are written to Azure Blob Storage. This is a newer auditing method, which provides higher performance, supports higher granularity object-level auditing, and is more cost effective.
* **Table Auditing** - logs are written to Azure Table Storage. Table Auditing logs are saved as a collection of Azure Storage Tables with a “SQLDBAuditLogs” prefix.

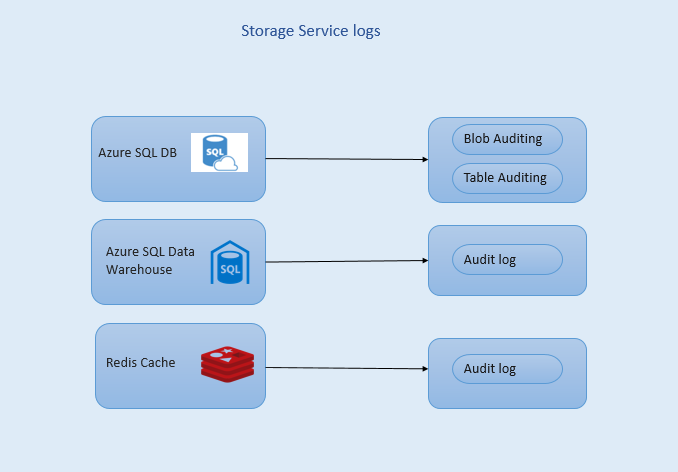


Figure 8 Storage Service Logs

#### 3.3.4.2 Azure SQL Data Warehouse

SQL Data Warehouse auditing allows you to record events in your database to an audit log in your Azure Storage account. Auditing can help you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.

SQL Data Warehouse database auditing allows you to:

* Retain an audit trail of selected events. You can define categories of database actions to be audited.
* Report on database activity. You can use preconfigured reports and a dashboard to get started quickly with activity and event reporting.
* Analyze reports, you can find suspicious events, unusual activity, and trends.

Plain SQL and Parameterized SQL for which the collected audit logs are classified as

* Access to data
* Schema changes (DDL)
* Data changes (DML)
* Accounts, roles, and permissions (DCL)
* Stored Procedure, Login and, TransactionManagement**.**

For each Event Category, Auditing of Success and Failure operations are configured separately. Audit logs are stored in your Azure storage account. You can define an audit log retention period.

#### 3.3.4.3 Azure Radis Cache

Azure Redis Cache provides several options for monitoring your cache instances. You can view metrics, pin metrics charts to the Starboard, customize the date and time range of monitoring charts, add and remove metrics from the charts, and set alerts when certain conditions are met. When cache diagnostics are enabled, metrics for Azure Redis Cache instances are collected approximately every 30 seconds and stored so they can be displayed in the metrics charts and evaluated by alert rules. Azure Redis Cache provides you the ability to have diagnostics data stored in a storage account so you can use any tools you want to access and process the data directly. In order for cache diagnostics to be collected, stored, and displayed in the Azure portal, a storage account must be configured.

#### 3.3.4.4 Azure Data Lake Store

Organizations can enable diagnostic logging for their Azure Data Lake Store account to collect data access audit trails that provides information such as list of users accessing the data, how frequently the data is accessed, how much data is stored in the account, etc.

There are two ways to view the log data for your Data Lake Store account.

* From the Data Lake Store account settings view
* From the Azure Storage account where the data is stored

In the Diagnostic Logs blade, you should see the logs categorized by Audit Logs and Request Logs.

* Request logs capture every API request made on the Data Lake Store account.
* Audit Logs are similar to request Logs but provide a much more detailed breakdown of the operations being performed on the Data Lake Store account. For example, a single upload API call in request logs might result in multiple "Append" operations in the audit logs.

#### 3.3.4.5 Azure Data Factory

The Data Factory service provides reliable and complete view of your storage, processing, and data movement services. The service provides you a monitoring dashboard helps that you can use to perform the following tasks:

* Quickly assess end-to-end data pipeline health.
* Identify issues, and take corrective action if needed.
* Track data lineage.
* Track relationships between your data across any of your sources.
* View full historical accounting of job execution, system health, and dependencies.

Data Factory allows you to capture various metrics and create alerts on metrics. You can monitor and create alerts on the following metrics for the slices in your data factory.

* Failed Runs
* Successful Runs

## 3.4 Internet of Things

The Azure Activity Log can be streamed in near real time to any application using the built-in “Export” option in the portal, or by enabling the Service Bus Rule Id in a Log Profile via the Azure PowerShell Cmdlets or Azure CLI.

Here are just a few ways you might use the streaming capability for the Activity Log:

* Stream to third-party logging and telemetry systems – Over time, Event Hubs streaming will become the mechanism to pipe your Activity Log into third-party SIEMs and log analytics solutions.
* Build a custom telemetry and logging platform – If you already have a custom-built telemetry platform or are just thinking about building one, the highly scalable publish-subscribe nature of Event Hubs allows you to flexibly ingest the activity log.

## 3.5 Enterprise Integration

|  |  |  |
| --- | --- | --- |
| Enterprise Integration | BizTalk Services | StorSimple |

### 3.5.1 BizTalk Services

**Operation Logs**- Operation log is a Management Services feature available in the Azure classic portal that allows you to view historical logs of operations performed on your Azure services, including BizTalk Services. This feature only captures logs for management operations on BizTalk Services, such as when the service was started, backed up, and so on.

### 3.5.2 StorSimple

StorSimple includes several tools that you can use to troubleshoot StorSimple solution. These include:

* Cmdlets specifically designed for troubleshooting
* Support packages and device logs

A support package contains all the relevant logs that can assist the Microsoft Support team with troubleshooting device issues. You can use Windows PowerShell for StorSimple to generate an encrypted support package that you can then share with support personnel.

## 3.6 Intelligence + Analytics

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Intelligence + Analytics | [Azure HDInsight Service](https://docs.microsoft.com/en-in/azure/hdinsight/hdinsight-debug-jobs) | [Azure Machine Learning Service](https://docs.microsoft.com/en-in/azure/machine-learning/machine-learning-web-services-logging) | [Azure Data Lake Analytics Service](https://docs.microsoft.com/en-in/azure/data-lake-analytics/data-lake-analytics-get-started-powershell) | [Azure PowerBI Embedded service](https://azure.microsoft.com/en-in/blog/analyze-azure-audit-logs-in-powerbi-more/) | [Azure Data Lake Store Service](https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-diagnostic-logs) |

### 3.6.1 Azure HDInsight Service

Each Hadoop cluster in Azure HDInsight has an Azure storage account used as the default file system. Cluster uses the Azure Table storage and the Blob storage on the default Storage account to store its logs. The logs retain in the Storage account even after the cluster is deleted. The logs written to Azure Tables provide one level of insight into what is happening with an HDInsight cluster. When you create an HDInsight cluster, 6 tables are automatically created for Linux-based clusters in the default Table storage:

* hdinsightagentlog,
* syslog,
* daemonlog,
* hadoopservicelog,
* ambariserverlog,
* ambariagentlog

Three tables are created for Windows-based clusters:

* setuplog: Log of events/exceptions encountered in provisioning/setting up of HDInsight clusters.
* hadoopinstalllog: Log of events/exceptions encountered when installing Hadoop on the cluster. This table may be useful in debugging issues related to clusters created with custom parameters.
* hadoopservicelog: Log of events/exceptions recorded by all Hadoop services. This table may be useful in debugging issues related to job failures on HDInsight clusters.

### 3.6.2 Azure Machine Learning Service

Enabling logging in Web services provides additional information, beyond just an error number and a message, that can help you troubleshoot your calls to the Machine Learning APIs. When logging is enabled, all the diagnostics and errors from the selected endpoint are logged to the Azure Storage Account linked with the user’s workspace.

Each blob in the container holds the diagnostics info for exactly one of the following:

* An execution of the Batch-Execution method
* An execution of the Request-Response method
* Initialization of a Request-Response container

### 3.6.3 Azure Data Lake Analytics Service

Search log- The search log can be stored in either Data Lake store or Azure Blob storage.

### 3.6.4 Azure Data Lake Store Service

In the Diagnostic Logs blade, you should see the logs categorized by Audit Logs and Request Logs.

* **Request Logs** – Request logs capture every API request made on the Data Lake Store account.
* **Audit Logs**- Audit logs are similar to request Logs but provide a much more detailed breakdown of the operations being performed on the Data Lake Store account.

### 3.6.5 Azure PowerBI Embedded Service

Azure Audit Logs (Operational Logs) include all the provisioning actions performed in the Azure Resource Manager in addition to other actions related to managing Azure resources (ex. Alerts, Auto Scaling, deployments etc.).

These data points usually require accessing the logs via data analysis and visualization tools. The Azure Insights and Power BI team collaborated to bring you exactly this - a free and easy-to-use extension in Power BI, the Content Pack for Azure Audit Logs.

### 3.6.6 Azure Key Vault

You can do this by enabling logging for Key Vault, which saves information in an Azure storage account that you provide. A new container named insights-logs-auditevent is automatically created for your specified storage account, and you can use this same storage account for collecting logs for multiple key vaults.

You can access your logging information at most, 10 minutes after the key vault operation. In most cases, it will be quicker than this. It's up to you to manage your logs in your storage account:

* Use standard Azure access control methods to secure your logs by restricting who can access them.
* Delete logs that you no longer want to keep in your storage account.

## 3.7 Monitoring & Management

|  |  |  |
| --- | --- | --- |
| Monitoring & Management | [Azure Backup Service](https://azure.microsoft.com/en-us/blog/alerting-and-monitoring-for-azure-backup/) | [Developers Tools](https://docs.microsoft.com/en-in/azure/log-analytics/log-analytics-data-sources-custom-logs) |

### 3.7.1 Azure Backup Service

Preview release of alerting and monitoring for Azure backup, which is currently the top-voted idea on Azure Backup User Voice. In a continuation of the simplified experience using the new Recovery Services vault, customers can now monitor cloud backups for their on-premises servers and Azure IaaS virtual machines in a single dashboard.

## 3.7.2 Developers Tools

#### 3.7.2.1 Azure API Management – Custom Logs

The Custom Logs data source in Log Analytics allows you to collect events from text files on both Windows and Linux computers. Many applications log information to text files instead of standard logging services such as Windows Event log or Syslog.

#### 3.7.2.2 Application Insights

Application Insights includes a powerful Diagnostic Search tool that enables you to explore and drill in to telemetry sent by the Application Insights SDK from your application. Many events such as user page views are automatically sent by the SDK.

You can also write code to send custom events, exception reports, and traces. And if you already use a logging framework such as log4J, log4net, NLog, or System.Diagnostics.Trace, you can capture those logs and include them in the search. This makes it easy to correlate log traces with user actions, exceptions and other events.

#### 3.7.2.3 Application Diagnostic Logs

When you set up a Cloud Services project or a Virtual Machine in Microsoft Azure, [Azure can generate a diagnostic log](https://docs.microsoft.com/en-us/azure/vs-azure-tools-diagnostics-for-cloud-services-and-virtual-machines). You can have this sent on to Application Insights so that you can analyze it along with diagnostic and usage telemetry sent from within the app by the Application Insights SDK. The Azure log includes events in the management of the app such as start, stop, crashes, as well as performance counters. The log also includes calls in the app to System.Diagnostics.Trace.

(<https://docs.microsoft.com/en-us/azure/app-service-web/web-sites-enable-diagnostic-log>)

Application diagnostics stores information in a specific format for .NET applications, depending on whether you store logs to the file system, table storage, or blob storage. The base set of data stored is the same across all three storage types - the date and time the event occurred, the process ID that produced the event, the event type (information, warning, error,) and the event message.

Four Types of Storage is there to store log: -

* **File System** - Each line logged to the file system or received using streaming.
* **Table Storage** - When logging to table storage, additional properties are used to facilitate searching the data stored in the table as well as more granular information on the event.
* **Blob Storage** - When logging to blob storage, data is stored in comma-separated values (CSV) format.
* **Failed Request Traces** - Failed request traces are stored in XML files.