February 6th-7th

nic

20/20 VISION

Oslo Spektrum

Auditing Azure - Compliance, Oversight, Governance, and Protection

Aidan Finn, MVP, Innofactor Norway

Introduction

- 13 year MVP – currently Microsoft Azure (3)
  - Previously Hyper-V and SCCM
- Principal Consultant for Innofactor Norway
  - Azure infrastructure – networking & security
- Working as consultant/sys admin since 1996
- Windows Server, Hyper-V, System Center, desktop managment, and Azure

- http://aidanfinn.com
- http://innofactor.com
- http://www.cloudmechanix.com
- @joe_elway

Auditing

What is (IT) Auditing?

To our friend, Wikipedia:

*A **computer security audit** is a manual or systematic measurable technical assessment of a system or application.*

Automated assessments … include system generated audit reports or using software to monitor and report changes to files and settings on a system.

https://en.wikipedia.org/wiki/Information_technology_security_audit

OK, What Does That Mean?

- An automated recording
- What was done?
- Who did it?
- When did they do it?
- And maybe even more information

Why Do We Audit?

- Troubleshooting
  - When did something change?
  - Who did it and ask them why?
- Security investigation
  - Who made an unwanted change?
  - What was that change?
  - When was it done?
- Regulatory / Industrial Compliance
- Feel-good factor

Azure Security Logging & Auditing

Does Azure Log for Auditing?

- In a word: Yes
- And what does it audit?

Types of Azure Logs

- **Control/Management Logs**
  - ARM CREATE, UPDATE, or DELETE operations
- **Data plane logs**
  - Events from resource usage.
    - Windows guest OS logs and resource diagnostics logs
- **Processed events**
  - Information about analysed events/alerts
    - Azure Security Center alerts

What does Azure Log for Auditing?

Category	Log Type	Usage	Integration
Activity Logs *	Control plane on ARM resources	Insights into operations on resources	Azure Monitor, REST API
Azure resource logs *	Data about operation of ARM resources	Insights into operations the resource performed	Azure Monitor
Azure AD reporting *	Logs and reports	User and system sign-in activity	Graph API
VM & cloud services	Windows Event Log and Linux Syslog	System & data logging from the guest OS	Storage account
Azure Storage Analytics	Storage logging & metrics	Trace requests, usage trends, and issue diagnostics	REST API
NSG Flow Logs	Inbound & outbound flow recordings	Information on ingress & egress of protected subnets	Azure Network Watcher
Application Insight	Logs, exceptions, and custom diagnostics	Application Performance Monitoring (APM)	REST API, Power BI
Process data/security alerts	Azure Security Center and Azure Monitor alerts	Security information & alerts	REST API, JSON

Activity Log

What is Activity Log

- A recording of operations *to* your ARM resources
  - Things you do
  - Things Azure does
- Done on a per-subscription basis
- No configuration required for logging
- Found in Activity Log

Activity Log Features

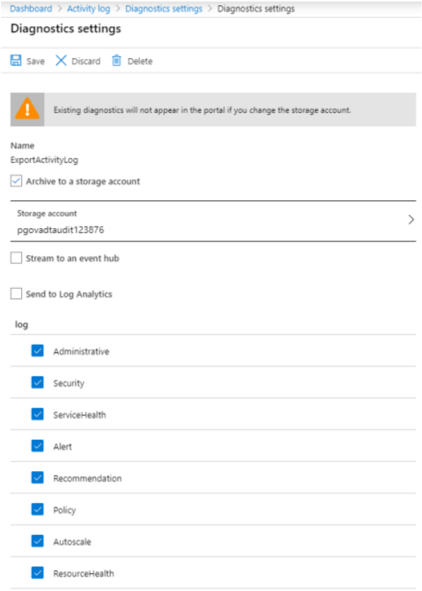
- Records data per-subscription
  - Can be viewed per-resource
- Can be filtered
  - Management Group, subscription, date/time, event severity, resource group
  - Resource, resource type, operation, event initiated by, event category
- View in the Azure Portal
- Download as CSV
- Automatic export to external sources
- Limited to 90 days of storage

True Story

- Was working with a customer
  - One of the engineers doesn’t like me
- He screwed up something that affected the business
  - He secretly fixed the problem
  - I spotted the change and subsequent fix
- He said that *I* changed something and then secretly fixed it
- I copied the *READ ONLY* audit log and proved I had modified nothing
- Blame was redirected to him

Export of Activity Log

- Activity Log data exported live as it happens
- Reasons:
  - Retain data for longer than 90 days
  - Use the features of external systems
    - Indexing & searching
    - Reporting
- Types of export:
  - Storage account
  - Azure Event Hub
  - Log Analytics Workspace (Azure Monitor Logs)


Dashboard > Activity log > Diagnostics settings > Diagnostics settings
Save
Discard
Delete

Diagnostics settings

Existing diagnostics will not appear in the portal if you change the storage account.

Name
ExportActivityLog

☑ Archive to a storage account

Storage account
pgovadtaudit123876

□ Stream to an event hub

□ Send to Log Analytics

log

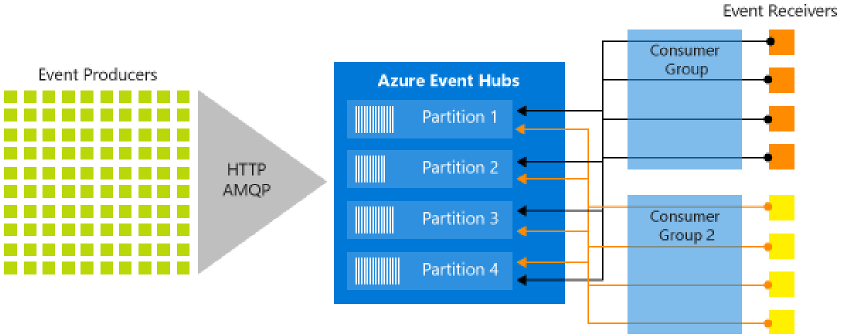
☑ Administrative
☑ Security
☑ ServiceHealth
☑ Alert
☑ Recommendation
☑ Policy
☑ Autoscale
☑ ResourceHealth

Activity Log Categories

- Administrative
  - The CREATE, UPDATE, DELETE actions *to* resources
- Service Health
  - Health incidents in Azure
- Resource Health
  - Health changes to resources
- Alert
  - Azure Monitor alerts
- Autoscale
  - Changes by the Autoscale engine
- Recommendation
  - Azure Advisor
- Security
  - Alerts generated by Azure Security Center
- Policy
  - Operations performed by Azure Policy

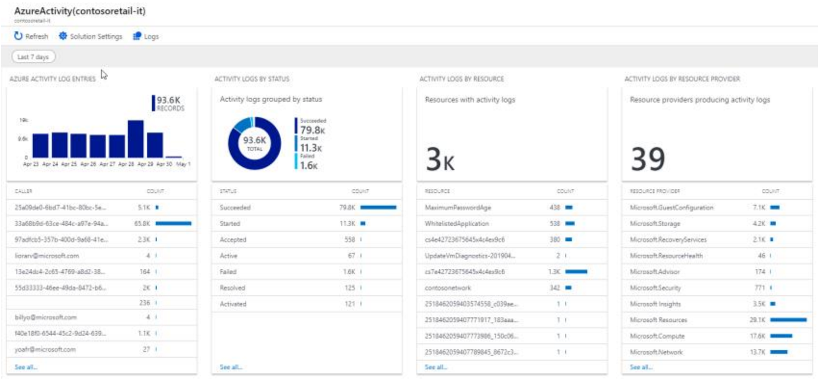
Activity Log | Event Hubs

- AKA Azure Monitor Logs
- Export of data to 3rd party systems
- Pros:
  - Unify data from many sources
  - 3rd party functionality
- Cons:
  - Complexity
  - Cost



Activity Log | Log Analytics Workspace

- AKA Azure Monitor Logs
- Maximum retention of 720 days
- Pros:
  - Easy to search
- Cons:
  - Relatively expensive storage


AzureActivity(contosoretail-it)
contosoretail-it
Refresh
Solution Settings
Logs
Last 7 days
AZURE ACTIVITY LOG ENTRIES
93.6K
RECORDS
19k
9.6k
0
Apr 23
Apr 24
Apr 25
Apr 26
Apr 27
Apr 28
Apr 29
Apr 30
May 1
ACTIVITY LOGS BY STATUS
Activity logs grouped by status
93.6K
TOTAL
Succeeded
79.8K
Started
11.3K
Failed
1.6K
ACTIVITY LOGS BY RESOURCE
Resources with activity logs
3K
ACTIVITY LOGS BY RESOURCE PROVIDER
Resource providers producing activity logs
39
See all...

CALLER	COUNT
25a09de0-6bd7-41bc-80bc-5e...	5.1K
33a68b9d-63ce-484c-a97e-94a...	65.8K
97adfcb5-357b-400d-9a68-41e...	2.3K
liorarv@microsoft.com	4
13e24dc4-2c65-4769-a8d2-38...	164
55d33333-46ee-49da-8472-b6...	2K
	236
billyo@microsoft.com	4
f40e18f0-6544-45c2-9d24-639...	1.1K
yoafr@microsoft.com	27

STATUS	COUNT
Succeeded	79.8K
Started	11.3K
Accepted	558
Active	67
Failed	1.6K
Resolved	125
Activated	121

RESOURCE	COUNT
MaximumPasswordAge	438
WhitelistedApplication	538
cs4e42723675645x4c4ex9c6	380
UpdateVmDiagnostics-201904...	2
cs7e42723675645x4c4ex9c6	1.3K
contosonetwork	342
2518462059403574558_c039ae...	1
2518462059407771917_183aaa...	1
2518462059407773986_150c06...	1
2518462059407789845_8672c3...	1

RESOURCE PROVIDER	COUNT
Microsoft.GuestConfiguration	7.1K
Microsoft.Storage	4.2K
Microsoft.RecoveryServices	2.1K
Microsoft.ResourceHealth	46
Microsoft.Advisor	174
Microsoft.Security	771
Microsoft Insights	3.5K
Microsoft Resources	29.1K
Microsoft.Compute	17.6K
Microsoft.Network	13.7K

Log Analytics Workspace | Tips

- Subscription
  - Dedicated
  - Limited number of *Readers* only
- Workspace
  - Default retention = 720 days
  - Add the Azure Activity Logs solution
- Put a lock (delete) on the Workspace resource

Activity Log | Storage Account

- Data exported as JSON records
  - Blob storage
  - 1 blob per hour
  - Organized with folders: subscription | year | month | day
- Pros:
  - Very cheap storage
  - “Infinite” retention
- Cons:
  - Not easy to use

Storage Account | Tips

- Subscription
  - Dedicated
  - Limited number of *Readers* only
- Storage Account
  - General Purpose V2 / GPv2
  - Enable blob tiering (hot | cool | archive)
  - Auto delete = max retention plus 1 day
- Blob policy
  - Read Only = max retention
  - Admin Lock enabled
- Put a lock (delete) on the Storage Account resource

Azure Resource Logs

What Are Azure Resource Logs?

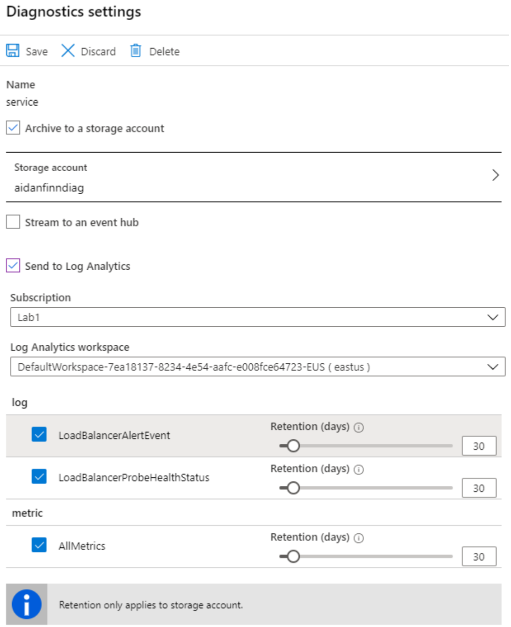
- Things that your resource do
- Examples:
  - Guest OS logs from virtual machines
  - Diagnostics logs from resources

Where is this Configured?

- Well … that depends on the resource type
- Typically:
  - Resource > Diagnostics Settings
  - Historically:
    - A few had this in the resource settings
    - Others had it in Azure Monitor
    - It’s been getting better – both locations
- Virtual Machines:
  - VM > Monitoring > Diagnostics Settings

Typical Diagnostics Settings

- Export data *just after* it happens
  - Storage account (with maximum retention)
  - Event Hub
  - Log Analytics
- Choose what to export:
  - Resource-specific logs
  - Performance metrics



Diagnostics settings

Name
service

☑ Archive to a storage account

Storage account
aidanfinndiag

☐ Stream to an event hub

☑ Send to Log Analytics

Subscription
Lab1

Log Analytics workspace
DefaultWorkspace-7ea18137-8234-4e54-aafc-e008fce64723-EUS (eastus)

log

☑	LoadBalancerAlertEvent	Retention (days) 30
☑	LoadBalancerProbeHealthStatus	Retention (days) 30

metric

☑	AllMetrics	Retention (days) 30

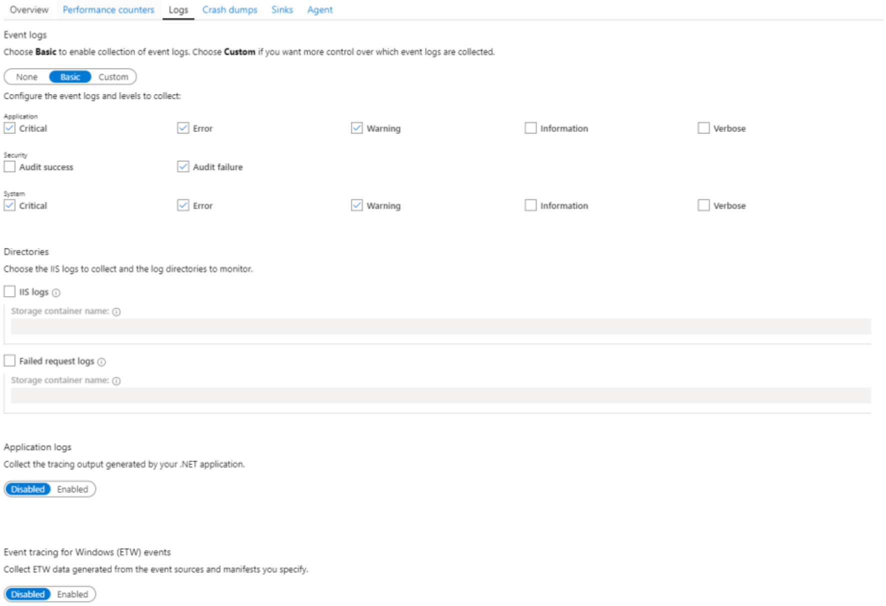
Retention only applies to storage account.

Examples

- Azure Application Gateway / Web Application Firewall
  - Log of web client requests
  - Log of allowed/denied requests (OWASP)
- Azure Firewall
  - Log of allowed/denied flows

Virtual Machine Diagnostics Settings

- Export to storage account
  - Guest OS performance counters
  - Windows event logs
  - IIS logs
  - .NET logs
  - ETW events
  - Crash dumps
- In preview
  - Sending data to Azure Monitor
  - VM requires managed service identity



Event logs

Choose **Basic** to enable collection of event logs. Choose **Custom** if you want more control over which event logs are collected.

None [✓ Basic] Custom

Configure the event logs and levels to collect:

Application

☑ Critical ☑ Error ☑ Warning □ Information □ Verbose

Security

□ Audit success ☑ Audit failure

System

☑ Critical ☑ Error ☑ Warning □ Information □ Verbose

Directories

Choose the IIS logs to collect and the log directories to monitor.

□ IIS logs ⓘ

Storage container name: ⓘ

□ Failed request logs ⓘ

Storage container name: ⓘ

Application logs

Collect the tracing output generated by your .NET application.

[✓ Disabled] Enabled

Event tracing for Windows (ETW) events

Collect ETW data generated from the event sources and manifests you specify.

[✓ Disabled] Enabled

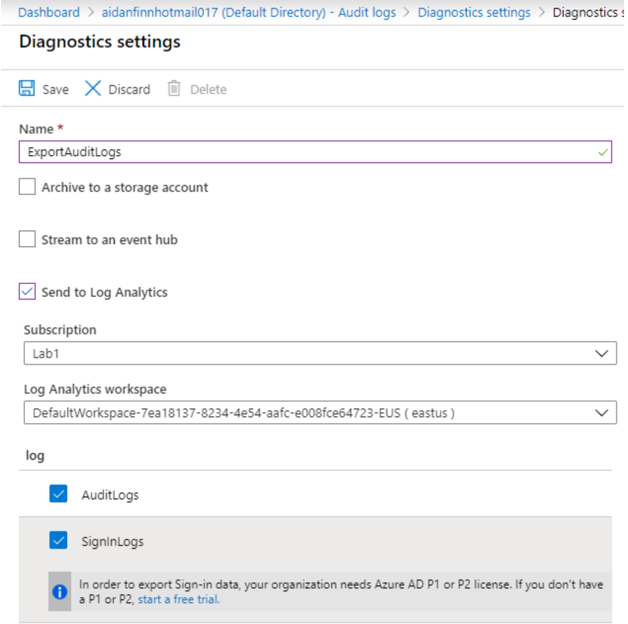
Azure AD Audit Logs

Azure AD

- The authentication/authorization engine of your tenant
  - All sign-ins to Azure via Azure AD
- Logs: Diagnostic Settings
  - Sign-ins (requires Azure AD P1/P2)
  - Audit Logs
- Reports: Security
  - Risky Sign-Ins
  - Risky Users (to be replaced soon by Azure AD -> Users)

Azure AD | Audit Logs

- Azure AD > Audit Log > Diagnostic Settings
- Export to the usual suspects:
  - Storage account
  - Event Hub
  - Log Analytics Workspace



Dashboard > aidanfinnhotmail017 (Default Directory) - Audit logs > Diagnostics settings > Diagnostics s

Diagnostics settings

Name *

ExportAuditLogs

□ Archive to a storage account

□ Stream to an event hub

☑ Send to Log Analytics

Subscription

Lab1

Log Analytics workspace

DefaultWorkspace-7ea18137-8234-4e54-aafc-e008fce64723-EUS (eastus)

log

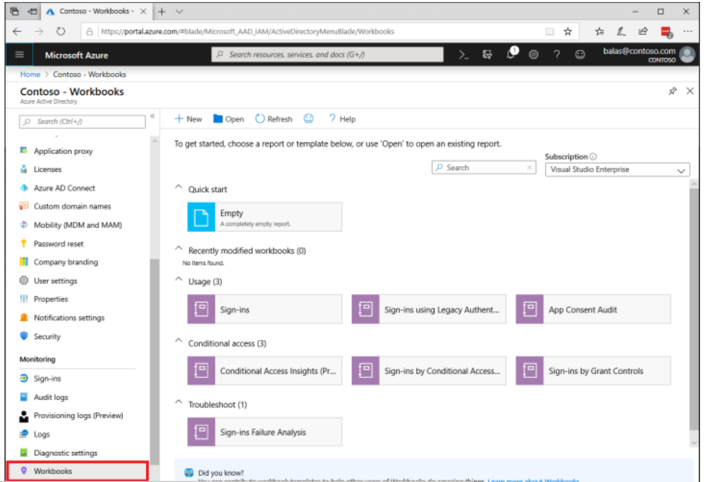
☑ AuditLogs

☑ SignInLogs

In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

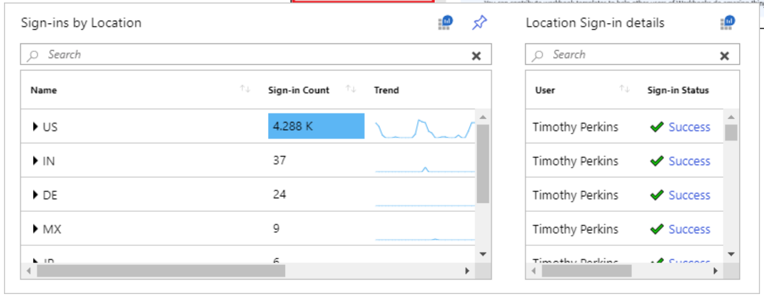
Azure AD | Reports

- There *was* an Azure AD Power BI content pack
  - Deprecated October 1st 2019
- Replaced by Workbooks
  - Requires Azure AD P1/P2 licensing
  - Log Analytics Workspace (with access)
  - Role membership in Azure AD:
    - Security administrator
    - Security reader
    - Report reader
    - Global administrator



Contoso - Workbooks
Azure Active Directory

To get started, choose a report or template below, or use 'Open' to open an existing report.



Sign-ins by Location

Name	Sign-in Count	Trend
▸ US	4.288 K	
▸ IN	37	
▸ DE	24	
▸ MX	9	
▸ JP	6	

Location Sign-in details

User	Sign-in Status
Timothy Perkins	✓ Success
Timothy Perkins	✓ Success
Timothy Perkins	✓ Success
Timothy Perkins	✓ Success
Timothy Perkins	✓ Success

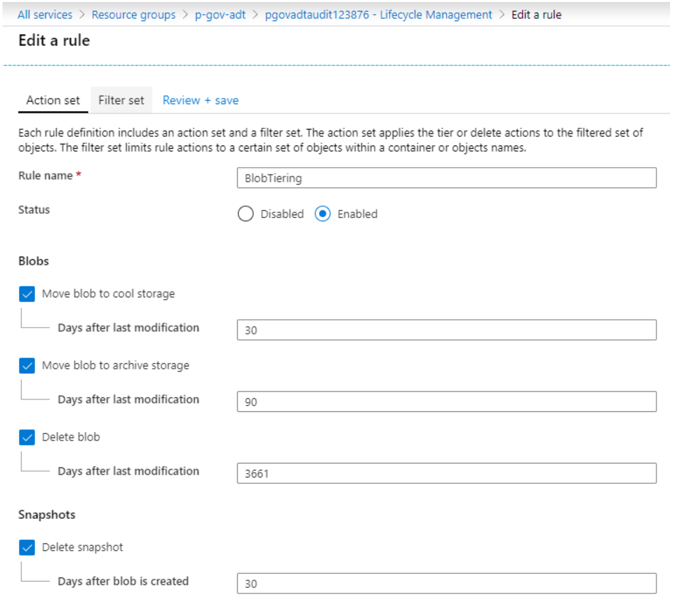
Enough With The Theory

Activity Log | Storage

- GPv2 Storage Account:
  - Long-term retention (many years)
  - Containers called insights-activity-logs & insights-activity-logs-suffix
- Log Analytics Workspace:
  - Mid-term retention (1 year)
  - Query/reporting
  - Table called MicrosoftInsightsAzureActivityLog

Storage Account | Archive Policy

- Centrally placed storage account
  - GPv2
  - Add a delete lock to the resource/resource group
  - Dedicated subscription with restricted access
- Policy calculation example:
  - Retain data for 10 years
  - Move from hot to cool: 30 days
  - Move from cool to archive: 90 days
  - Automatically delete blobs:
    - (10 * 366) ***+ 1*** = 3661



All services > Resource groups > p-gov-adt > pgovadtaudit123876 - Lifecycle Management > Edit a rule

Edit a rule

Action set | Filter set | Review + save

Each rule definition includes an action set and a filter set. The action set applies the tier or delete actions to the filtered set of objects. The filter set limits rule actions to a certain set of objects within a container or objects names.

Rule name * BlobTiering

Status ○ Disabled ● Enabled

Blobs

☑ Move blob to cool storage

Days after last modification 30

☑ Move blob to archive storage

Days after last modification 90

☑ Delete blob

Days after last modification 3661

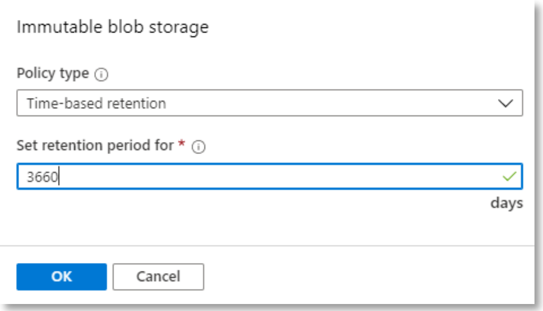
Snapshots

☑ Delete snapshot

Days after blob is created 30

Storage Account | Immutable Policy

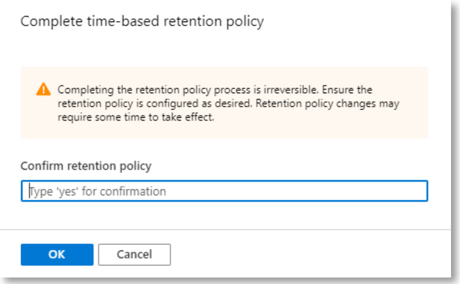
- WORM (Write-Once, Read Many)
  - Prevent record deletion/modification
- Set per container
  - We will have several containers
- Configuration:
  - Example: 10 years retention
  - Policy Type: Time-Based Retention
  - Retention Period: 10 * 366 = 3660
  - Enable Lock Policy (cannot be removed!)



Immutable blob storage

Policy type: Time-based retention

Set retention period for *: 3660 days



Complete time-based retention policy

Completing the retention policy process is irreversible. Ensure the retention policy is configured as desired. Retention policy changes may require some time to take effect.

Confirm retention policy: Type 'yes' for confirmation

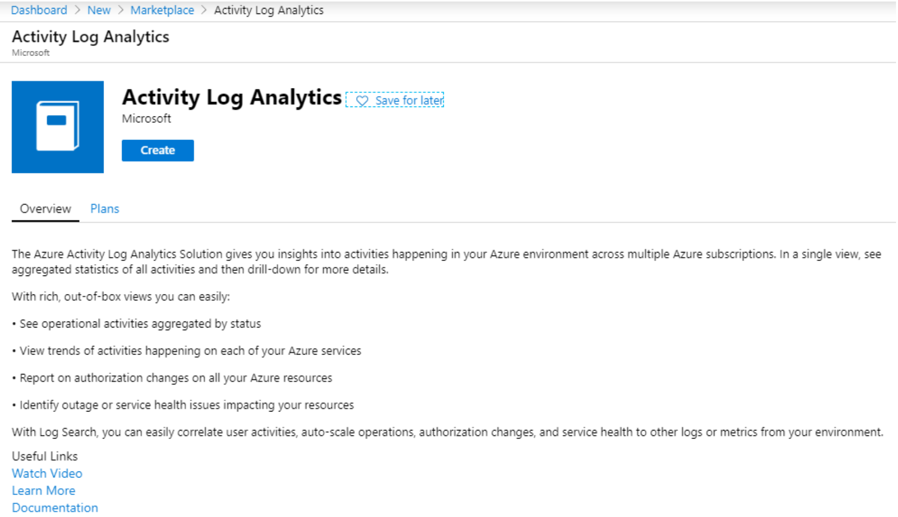
Using Activity Log Data | Workspace Search

- Data stored in AzureActivity Table
- Example query:

```
AzureActivity
| parse Authorization with * '/resourcegroups/' auditResourceGroup '/providers/' stuff '/' auditResourceType '/' auditResource '",' stuff3
| project TimeGenerated, EventSubmissionTimestamp, Caller, auditResourceGroup, auditResource, auditResourceType, OperationNameValue
```

Using Activity Log Data | Workspace Solution

- Activity Log Analytics
  - Solution in the Azure Marketplace
- Built-in:
  - Queries
  - Visualisations



The Azure Activity Log Analytics Solution gives you insights into activities happening in your Azure environment across multiple Azure subscriptions. In a single view, see aggregated statistics of all activities and then drill-down for more details.

With rich, out-of-box views you can easily:

- See operational activities aggregated by status
- View trends of activities happening on each of your Azure services
- Report on authorization changes on all your Azure resources
- Identify outage or service health issues impacting your resources

With Log Search, you can easily correlate user activities, auto-scale operations, authorization changes, and service health to other logs or metrics from your environment.

Useful Links
Watch Video
Learn More
Documentation

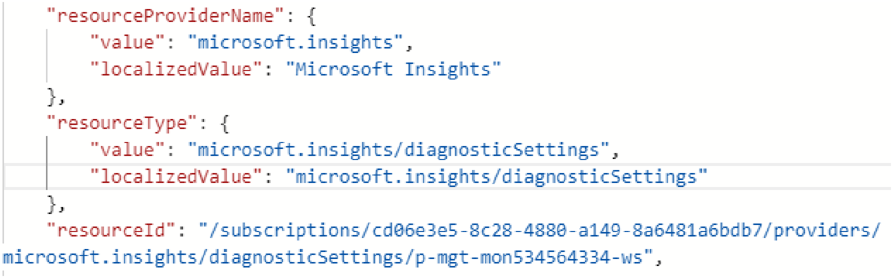
Using Activity Log Data | Visualisations

- Workbooks
  - Azure Monitor
  - Visualisations based on Workspace KQL queries
  - Can be pinned to Azure Portal dashboards
- Power BI
  - There *was* an Activity Log content pack – deprecated
  - You can still connect to Workspace or Storage Account blob storage
    - Data will require parsing

Demo: Storage Account & Workspace

Activity Log | Scale Problem

- Enabled via “Activity Log” diagnostics settings
- That’s per-subscription
- What if you have lots of subscriptions?
- The answer is in Activity Log!



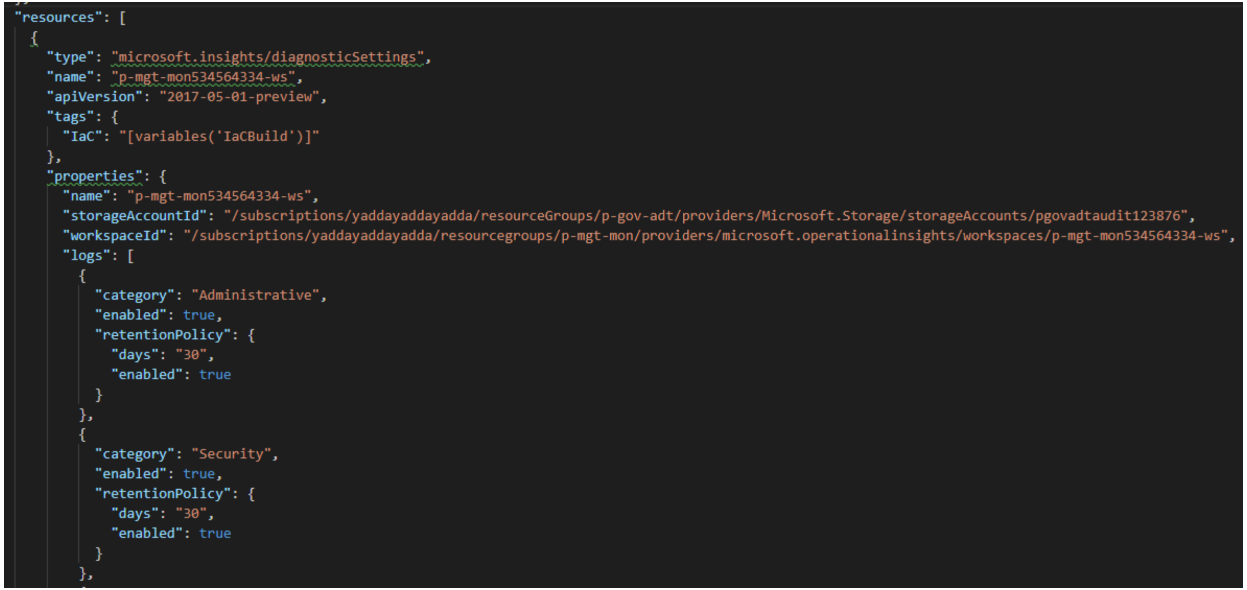
```
    "resourceProviderName": {
        "value": "microsoft.insights",
        "localizedValue": "Microsoft Insights"
    },
    "resourceType": {
        "value": "microsoft.insights/diagnosticSettings",
        "localizedValue": "microsoft.insights/diagnosticSettings"
    },
    "resourceId": "/subscriptions/cd06e3e5-8c28-4880-a149-8a6481a6bdb7/providers/
microsoft.insights/diagnosticSettings/p-mgt-mon534564334-ws",
```

Activity Log | Subscription Deployment

- You can deploy some ARM resources to a subscription
  - Normally we deploy to a resource group
- One such resource:
  - Type: microsoft.insights/diagnosticSettings
  - Name: Your chosen name for the diagnostic settings configuration
- The following example:
  - Sends data to a central Log Analytics Workspace
  - Stores data in a central storage account for “infinite” days
    - We’ll deal with that later

Activity Log | JSON

```
{
  "type": "microsoft.insights/diagnosticSettings",
  "name": "p-mgt-mon534564334-ws",
  "apiVersion": "2017-05-01-preview",
  "tags": {
    "IaC": "[variables('IaCBuild')]"
  },
  "properties": {
    "name": "p-mgt-mon534564334-ws",
    "storageAccountId": "/subscriptions/yaddayaddayadda/resourceGroups/p-gov-adt/providers/Microsoft.Storage/storageAccounts/pgovadtaudit123876",
    "workspaceId": "/subscriptions/yaddayaddayadda/resourcegroups/p-mgt-mon/providers/microsoft.operationalinsights/workspaces/p-mgt-mon534564334-ws",
    "logs": [
      {
        "category": "Administrative",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "Security",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "ServiceHealth",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "Alert",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "Recommendation",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "Policy",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "Autoscale",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      },
      {
        "category": "ResourceHealth",
        "enabled": true,
        "retentionPolicy": {
          "days": "0",
          "enabled": true
        }
      }
    ]
  }
}
```



```
"resources": [
  {
    "type": "microsoft.insights/diagnosticSettings",
    "name": "p-mgt-mon534564334-ws",
    "apiVersion": "2017-05-01-preview",
    "tags": {
      "IaC": "[variables('IaCBuild')]"
    },
    "properties": {
      "name": "p-mgt-mon534564334-ws",
      "storageAccountId": "/subscriptions/yaddayaddayadda/resourceGroups/p-gov-adt/providers/Microsoft.Storage/storageAccounts/pgovadtaudit123876",
      "workspaceId": "/subscriptions/yaddayaddayadda/resourcegroups/p-mgt-mon/providers/microsoft.operationalinsights/workspaces/p-mgt-mon534564334-ws",
      "logs": [
        {
          "category": "Administrative",
          "enabled": true,
          "retentionPolicy": {
            "days": "30",
            "enabled": true
          }
        },
        {
          "category": "Security",
          "enabled": true,
          "retentionPolicy": {
            "days": "30",
            "enabled": true
          }
        },
```

Activity Log | Blueprints

1. Use a Management Group hierarchy
   - Place subscriptions based on RBAC/policy design (not an org chart!)
2. Create a system managed identity
   - Assign it necessary rights at the top of the Management Group hierarchy
3. Create a Blueprint
   - Add the diagnosticsSettings JSON as an artefact
   - Save the Blueprint to the top Management Group
4. Assign the Blueprint to subscriptions in the Management Group hierarchy

Demo: Blueprint

Azure AD | Export

- Fairly simple
  - One set of configurations per tenant
- Diagnostics Settings Export:
  - Storage account
    - Container called insights-logs-auditlogs
  - Log Analytics Workspace
    - Table called AuditLogs

Demo: Azure AD Auditing

Wrapping Up

Summary

- Governance requires auditing
- Configure:
  - Per-subscription Activity Log
  - Azure Active Directory
  - Resource Logs
- Enable export:
  - Workspace
  - Storage account
- Enable visualisations & search
  - Workspace
  - Workbooks
  - Power BI

Thank You!

- http://aidanfinn.com
- http://www.innofactor.com
- http://www.cloudmechanix.com
- @joe_elway