RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CSV-W01

Logging in the Cloud: From Zero to (Incident Response) Hero

Jonathon Poling

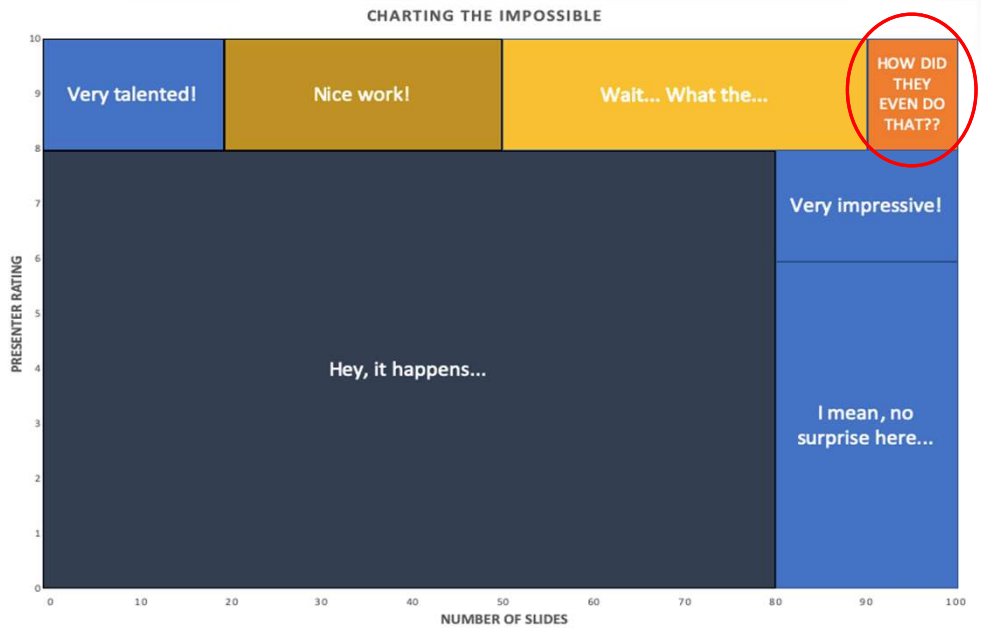
Managing Principal Consultant
Secureworks
@JPoForenso

#RSAC

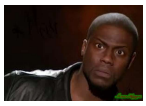
Agenda

```
for those in [ aws , Azure , Google Cloud Platform ]:
   print("What Should I Be Logging?")
   print("How *Specifically* Should I Configure it?")
   print("What Should I Be Monitoring?")
else:
   print("Questions?")
```

Today, We (Attempt to) Make History…



I plan to live here…



Why Me?

- Cloud (AWS) SME for Secureworks
- Developed Secureworks' AWS Incident Response Service Line
- Help SMB through Fortune 10 Customers…
  - Intelligently Configure/Instrument Their Environments
  - Protect Their Infrastructure
  - Effectively Respond to Incidents

Why This Presentation?

- Too many clouds, too little time
  - Many of us are still lacking foundational understanding of Cloud operations and security
  - It's extremely hard to master one cloud, let alone multiple
- Tired of presentations with no actionable takeaways
  - People need prescriptive actions to take that can help them to *immediately* start getting/operating/securing their Cloud(s) better
- Helping us to help you (to help us and help you)

How Will This Help You?

In this talk you will (hopefully) learn:

- Core log capabilities of each Cloud provider
- Which core logs should be configured (specifically how)
- Tips for Monitoring core logs
- A few tips/tricks for Incident Response along the way

Get Ready for a LOT of Material…

RSAConference2020

Amazon Web Services (AWS)

Overview of Logging

Core Logs

- CloudTrail
  - Your account's syslog on steroids
  - Enabled by Default for 90 days of retention BUT…
    - Each region's logs are kept ONLY in that region's bucket (ROYAL PAIN for response)
    - Only "Global" (IAM/STS) service events will be logged across all regions/buckets
      - But… some aren't… (DON'T @ ME "ConsoleLogin"!)

CloudTrail Events
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html

Core Logs

- CloudWatch
  - System performance metrics
    - Enabled by default (metrics sent every 15 minutes)
    - Enabling “Detailed Monitoring” will send metrics every 1 minute
  - OS/Application Logs
    - Send to CloudWatch via EC2 Systems Manager (SSM) and/or CloudWatch Logs Agent
      - Both require installation of additional agent on each Instance
  - Additional stuff you’re also sending (CloudTrail, VPC Flow Logs, etc.)

Monitoring Instances using CloudWatch
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html

Metrics Collected by CloudWatch Logs Agent
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html

Core Logs

- Config
  - Track Resource “Compliance” against a set of rules
  - Easy setup via Console or CLI
  - Deliver config logs to SNS Topic and/or S3
  - Config Rules
    - Enable various default Config Rules to monitor/alert on configuration changes as they occur or on a schedule
    - Create custom rules according to your environment and policies
    - AWS Managed Rules provided/enabled by default
  - Now with Multi-Account Multi-Region Data Aggregation

Config Walkthrough
https://cloudacademy.com/blog/aws-config-an-introduction-and-walkthrough/

About AWS Managed Config Rules
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html

AWS Managed Config Rules
https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html

Core Logs

- Config
  - (BONUS) Software Monitoring
    - Monitor/record software inventory/changes
      - Requires Instances to be configured as “Managed Instances”

Software Config Monitoring
https://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html#recording-managed-instance-inventory

Core Logs

- S3
  - Bucket-Level (aka Management Event) Logs
    - Delete/Get/Put Bucket* type actions
    - Enabled by default
  - Object-Level (aka Data Event) Logs
    - Delete/Get/Put Object* type actions
    - Must be manually configured
  - Server Access Logs
    - Apache-ish type logs (Remote IP, URI, Bytes Sent, Referer, User-Agent, etc.)
    - Must be manually configured

S3 Logging
https://docs.aws.amazon.com/AmazonS3/latest/dev/cloudtrail-logging.html

Core Logs

- VPC Flow Logs
  - Netflow(ish) type connection logs
  - Can be enabled for VPC, VPC Subnet, or Elastic Network Interface (ENI)
    - Enable for anything of which you might even remotely care about the incoming/outgoing traffic
  - Logged to CloudWatch Logs as a new Log Group with a Stream for each associated ENI
    - Create CloudWatch Metric Filters/Alarms for traffic you care about

Log and View Network Traffic Flows
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Core Logs

- Load Balancer Logs
  - Elastic Load Balancer (ELB) Logs
    - Now referred to as “Classic Load Balancer” (CLB)
    - Logs the details of each request made to the load balancer
      - Timestamp, Client/Backend IP/Port, Processing Time, Sent/Received Bytes, User Agent, etc.
    - Publishes a log file for each ELB node every 5 or 60 (default) minutes
    - Disabled by default

Classic Load Balancer Access Logs
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html

Core Logs

- Load Balancer Logs
  - Application Load Balancer (ALB) Logs
    - Logs requests (*as best effort*) sent to the load balancer, including requests that never made it to the targets (malformed requests, requests with no target response)
    - Logs the details of each request/connection made to the Load Balancer
      - Connection Type, Timestamp, Client/Target IP/Port, Status Code, Sent/Received Bytes, User Agent, etc.
    - Publishes a log file for each ALB node every 5 minutes
    - Disabled by default

Application Load Balancer Access Logs
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

Core Logs

- Load Balancer Logs
  - Network Load Balancer (NLB) Logs
    - Logs detailed information about the *TLS requests* sent to your NLB
      - **Access logs are created only if the load balancer has a TLS listener and they contain information only about TLS requests!**
    - Logs the details of each TLS single request/connection made to the Load Balancer
      - Timestamp, Client/Target IP/Port, Sent/Received Bytes, TLS Cipher, TLS Protocol Version, etc.
    - Publishes a log file for each NLB node every 5 minutes
    - Disabled by default

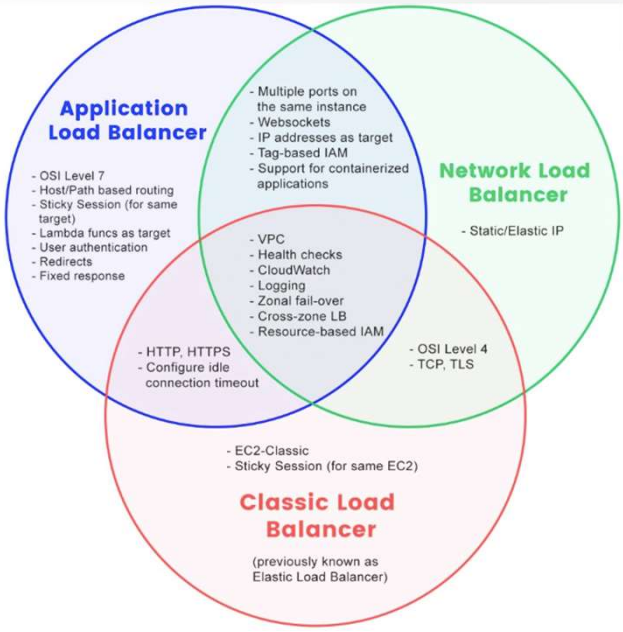
Network Load Balancer Access Logs
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-access-logs.html

Core Logs

	CLB	ALB	NLB
Protocols	TCP, SSL/TLS, HTTP, HTTPS	HTTP, HTTPS	TCP, TLS
Performance (a higher number is slower): the ability to handle more traffic	2	3	1 (fastest)
Host/Path-based routing	No	Yes	No
Sticky Session (for session-based applications)	Yes (redirect to the same machine)	Yes (redirect to the same target)	No
Static/Elastic IP	No	No	Yes
Load balancing to multiple ports on the same instance	No	Yes	Yes
Configurable idle connection timeout	Yes	Yes	No

How to Select and Migrate to the Right AWS Elastic Load Balancing (ELB) Solution
https://www.nclouds.com/blog/what-type-of-aws-elastic-load-balancing-aws-elb-is-right-for-you/

Core Logs



How to Select and Migrate to the Right AWS Elastic Load Balancing (ELB) Solution
https://www.nclouds.com/blog/what-type-of-aws-elastic-load-balancing-aws-elb-is-right-for-you/

RSAConference2020

Amazon Web Services (AWS)

Configuring Logging

CloudTrail

- Configuring Global/Central Logging to a single bucket
  - Navigate to **CloudTrail**
  - Ensure you're in the Region where you'd like your CT logs centralized
  - Select **Trails**
  - Click **Create Trail**
  - Input the **Trail Name**
  - Select **Apply trail to all regions**
- Note: IAM Events will be duplicated across all regions
  - Used to be able to disable Global Events in all Buckets except one
  - Documentation no longer references how to do this, so… YMMV

Aggregate logs from all regions to one bucket
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-log-files-from-multiple-regions.html

Preventing Duplicate Entries Across Regions
https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html#cloudtrail-integration_signin-regions

CloudWatch

- Certain Logs automatically sent to CloudWatch
  - CloudFront, Config, GuardDuty
- Enabling Detailed Monitoring (per Instance)
  - New Instances
    - In **Step 3** of your **Instance Configuration**, select **Enable Cloudwatch detailed monitoring**
  - Existing Instances
    - Navigate to **EC2**
    - Select **Instances**
    - Right-click the **Instance**
    - Select **CloudWatch Monitoring** -> **Enable Detailed Monitoring**

Using Metrics
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/working_with_metrics.html

Enabling Detailed Monitoring
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html

CloudWatch

- Configuring CloudWatch Logs Agent
  - Configure IAM Role to Allow Instance to write to CloudWatch
    - Either create a new Role or modify existing Role(s) to have the permissions specified in the **CloudWatchAgentServerPolicy** Policy
  - Configure Linux Instance to send OS/Host logs to CloudWatch
    - Download and Install the CloudWatch Logs Agent

```
$ wget <link_to_proper_package>
$ sudo rpm -U ./amazon-cloudwatch-agent.rpm
```

OR

```
$ sudo dpkg -i -E ./amazon-cloudwatch-agent.deb
```


Installing the CloudWatch Logs Agent
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/installing-cloudwatch-agent-commandline.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html

CloudWatch

- Configuring CloudWatch Logs Agent
  - Configure Linux Instance to send OS/Host logs to CloudWatch (Cont.)
    - Configure the CloudWatch Logs Agent Configuration File
      - Modify the config the collect the appropriate metrics and logs from your system(s)
    - Start the CloudWatch Logs Agent

```
$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-
agent-ctl -a fetch-config -m ec2 -c file:configuration-file-path -s
```


Installing the CloudWatch Logs Agent
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/installing-cloudwatch-agent-commandline.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html

CloudWatch

- Configuring CloudWatch Logs Agent
  - Configure Windows Instance to send OS/Host logs to CloudWatch
    - Download and Install the CloudWatch Logs Agent

      Link: `https://s3.amazonaws.com/amazoncloudwatch-agent/windows/amd64/latest/amazon-cloudwatch-agent.msi`

      ```
      > msiexec /i amazon-cloudwatch-agent.msi
      ```
    - Configure the CloudWatch Logs Agent Configuration File
      - Modify the config the collect the appropriate metrics and logs from your system(s)
    - Start the CloudWatch Logs Agent (via PowerShell)

      ```
      > & "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -c file:configuration-file-path -s
      ```


Installing the CloudWatch Logs Agent
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-iam-roles-for-cloudwatch-agent.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/installing-cloudwatch-agent-commandline.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file.html
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/install-CloudWatch-Agent-commandline-fleet.html

CloudWatch

- Configuring CloudWatch Logs Agent
  - Can also:
    - Install CloudWatch Logs Agent using SSM (if Instances are instrumented)
    - Install CloudWatch Logs Agent on on-premises systems to send to CW in AWS

Installing the CloudWatch Logs Agent Using SSM
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/installing-cloudwatch-agent-ssm.html

CloudWatch

- Configuring CloudTrail to send logs to CloudWatch
  - Navigate to **CloudTrail**
  - Select the appropriate **Trail**
  - Within the **CloudWatch Logs** section, click **Configure**
  - Specify a **New or existing log group**
  - Click **Continue**
  - Create a New or select an Existing **IAM Role** and **Policy Name**
  - Click **Allow**

Send CloudTrail to CloudWatch
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/send-cloudtrail-events-to-cloudwatch-logs.html

CloudWatch

- Configuring VPC Flow Logs to send to CloudWatch
  - Create a VPC Flow Logs IAM Role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```


Publishing VPC Flow Logs to CloudWatch
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

CloudWatch

- Configuring VPC Flow Logs to send to CloudWatch
  - Create a VPC Flow Logs IAM Role (Cont.)
    - Users will also need **PassRole** permissions for the Role

```
{
  "Version": "2012-10-17",
  "Statement": [ {
       "Effect": "Allow",
       "Action": ["iam:PassRole"],
       "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
       } ]
}
```


Publishing VPC Flow Logs to CloudWatch
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

CloudWatch

- Configuring VPC Flow Logs to send to CloudWatch
  - Configure VPC Flow Log to publish to CloudWatch
    - Navigate to **EC2**
    - Select **Network Interfaces**
    - Right-click on the appropriate network Interface and select **Create Flow Log**
    - Select the appropriate traffic **Filter** (Accept, Deny, All)
    - Select the **Maximum aggregation interval** (1 or 10 minutes)
    - Select the **Destination** to **Send to CloudWatch Logs**
    - Enter the **Destination log group**
    - Select the previously created **IAM Role**
    - Click **Create**

Publishing VPC Flow Logs to CloudWatch
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

Config

- Configuring Multi-Region Aggregation
  - Set up an Aggregator for all Regions
    - Navigate to **AWS Config**
    - Select **Aggregated View** -> **Aggregators**
    - Click **Add Aggregator**
    - Select **Allow AWS Config to replicate data from source account(s) into an aggregator account. You must select this checkbox to continue to add an aggregator.**
    - Input a unique **Aggregator Name**
    - Select either:
      - **Add individual account IDs** (input Account ID's to include)
      - **Add my organization** (create/choose the appropriate IAM Role)
    - Select all available **Region(s)**
    - Select **Allow AWS Config to aggregate data from all future AWS regions where AWS Config is enabled.**
    - Click **Save**

Multi-Account Multi-Region Data Aggregation
https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html

Config

- Configuring Multi-Region Aggregation
  - Authorize Aggregators for Regions
    - Navigate to **AWS Config**
    - Select **Authorizations**
    - Click **Add authorization**
    - Input **Aggregator Account**
    - Select **Aggregator Region**
    - Click **Add authorization**

Multi-Account Multi-Region Data Aggregation
https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html

Config

- Configuring Config Rules (that sounds weird*)
  - Adding Managed Rules
    - Navigate to **AWS Config**
    - Select **Rules**
    - Click **Add rule**
    - Search/filter based on rule name or description
    - Select the appropriate **Rule**
    - Configure the **Rule** as needed
    - Click **Save**

*But not as weird as AWS Systems Manager Session Manager…

Setting up AWS Config Rules
https://docs.aws.amazon.com/config/latest/developerguide/setting-up-aws-config-rules-with-console.html

Managing Your AWS Config Rules
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_manage-rules.html

AWS Managed Config Rules
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html
https://docs.aws.amazon.com/config/latest/developerguide/managed-rules-by-aws-config.html

Working With AWS Managed Rules
https://docs.aws.amazon.com/config/latest/developerguide/managing-aws-managed-rules.html

Config

- Configuring Config Rules (that sounds weird*)
  - Adding Custom Rules
    - Navigate to **AWS Config**
    - Select **Rules**
    - Click **Add rule**
    - Click **Add custom rule**
    - Configure the **Custom Rule** as needed
      - Name, Description, Lambda, Trigger, Rule Parameters, and Remediation Action
    - Click **Save**

Creating Custom AWS Config Rules
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules.html

S3

- Enabling MFA Delete
  - Can only be configured via the AWS CLI (unless I am missing something)
  - Configuring MFA Delete for a Bucket via the AWS CLI

```
$ aws s3api put-bucket-versioning --bucket my_bucket
--versioning-configuration '{"MFADelete":"Enabled"}'
```

  - Consider using **S3 Object Lock** as an alternative and/or added measure for preventing unintended/malicious data deletion

S3 MFA Delete
https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html#MultiFactorAuthenticationDelete
https://www.cloudmantra.net/blog/how-to-enable-mfa-delete-for-s3-bucket/

AWS CLI S3API
https://docs.aws.amazon.com/cli/latest/reference/s3api/put-bucket-versioning.html

S3 Object Lock
https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock-overview.html

S3

- Enabling Object-Level Logging
  - Via S3 (for Specific Bucket)

    *Can also configure upon Bucket Creation in **Configure options**

    - Navigate to **S3**
    - Select the appropriate **Bucket**
    - Navigate to the **Properties** tab
    - Click **Obect-level logging**
    - Select the **Bucket** for recording the activity
    - Select **Read** and **Write** for Events
    - Click **Create**

Enabling Object-Level (Data Event) Logging
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html

S3

- Enabling Object-Level Logging
  - Via CloudTrail (For All Buckets)
    - Navigate to **CloudTrail**
    - Select **Trails**
    - Click the appropriate **Trail**
    - Under **Data events**, click **Configure** under the **S3** tab
    - Click **Select all S3 buckets in your account**
    - Click **Save**

Enabling Object-Level (Data Event) Logging
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-data-events-with-cloudtrail.html

S3

- Enabling Server Access Logs
  - Navigate to **S3**
  - Create Target Bucket for collecting the Server Access Logs
    - Click **Create bucket**
      - Within the **Set permissions** tab, under **Manage system permissions**, ensure **Grant Amazon S3 Log Delivery Group write access to this bucket** is selected from the drop-down list

Enabling Server Access Logs + Format
https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html

S3

- Enabling Server Access Logs
  - Configure Server Access Logging (per Bucket)
    - Click the **Bucket** for which you'd like to enable Server Access Logs
    - Navigate to the **Properties** tab
    - Select **Server access logging**
    - Click **Enable logging**
    - Input the previously created **Target Bucket**
    - (Optional) Enter a **Target prefix** (e.g., "ServerAccessLogs")
    - Click **Save**

Enabling Server Access Logs + Format
https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html

VPC Flow Logs

- Configuring per ENI
  - Navigate to **EC2**
  - Right-click the appropriate **ENI**, select **Create flow log**
- Configuring per Subnet
  - Navigate to **VPC** -> **Subnets**
  - Right-click the appropriate **Subnet**, select **Create flow log**
- Configuring per VPC
  - Navigate to **VPC** -> **Your VPCs**
  - Right-click the appropriate **VPC**, select **Create flow log**

VPC Flow Logs – Log and View Network Traffic Flows
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

Publishing Flow Logs to CloudWatch Logs
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html

Load Balancer Logs

- Configuring ALB/NLB Access Logs
  - Navigate to **EC2** -> **Load Balancers**
  - Select the appropriate **Load Balancer**
  - Scroll to the bottom of the **Description** tab
  - Click **Edit Attributes**
  - Check the **Access logs** box
  - Input the appropriate **S3 location**
    - Select **Create this location for me** if it does not yet exist
  - Click **Save**

Enable Application Load Balancer Access Logs
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html#enable-access-logging

Enable Network Load Balancer Access Logs
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-access-logs.html#enable-disable-access-logging

Load Balancer Logs

- Configuring ELB (Classic) Access Logs
  - Navigate to **EC2** -> **Load Balancers**
  - Select the appropriate **Load Balancer**
  - Scroll to the bottom of the **Description** tab
  - Click **Configure Access Logs**
  - Check the Enable **Access logs** box
  - Select the appropriate **Interval**
  - Input the appropriate **S3 location**
    - Select **Create this location for me** if it does not yet exist
  - Click **Save**

Enable Classic Load Balancer Access Logs
https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-access-logs.html

CloudFront Logs

- Configuring CloudFront Access Logs (per Distribution)
  - Navigate to **CloudFront -> Distributions**
  - Select the appropriate **Distribution**
  - Under the **General** tab, click **Edit**
  - Within the **Distribution Settings** tab, scroll down to the **Logging** section
  - Select **On** for **Logging**
  - Input the appropriate target **Bucket for Logs**
  - (Optional) Input a **Log Prefix**
  - Click **Yes, Edit**

CloudFront Access Logs
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

Enabling CloudFront Access Logs
https://www.cloudconformity.com/knowledge-base/aws/CloudFront/cloudfront-logging-enabled.html
https://cloudsploit.com/remediations/aws/cloudfront/cloudfront-logging-enabled

RSAConference2020

Amazon Web Services (AWS)

Tips for Monitoring

CloudWatch Alarms

- Create CloudWatch Alarms for various Metrics:
  - CloudFront
    - Inordinate number of 4xx/5xx errors, anomalous bytes downloaded/uploaded, …
  - EC2 Instances
    - High CPU/Memory utilization, high CPU Credit Usage, StatusCheckFailed's, …
  - Load Balancers
    - High number of active or rejected connections, auth errors, high response times, …
  - VPC Flow Logs
    - Anomalous traffic increases/spikes or inbound/outbound data transfer, …
  - …

Monitoring CloudFront with CloudWatch
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/monitoring-using-cloudwatch.html

EC2 Metrics
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html

CloudWatch Events

- Create CloudWatch Events for:
  - Config Rules
    - Disable accounts when/where MFA is disabled
  - CloudTrail Actions/API Calls
    - Alert and re-enable CloudTrail Logging if ever stopped/deleted
  - GuardDuty Alerts
    - Shut down Instances found to be compromised with CryptoMiners
  - TrustedAdvisor Findings
    - Alert/respond (lambda) to MFA disable for root account, public EBS Snapshots, service limits hit, …
  - VPC Flow Logs
    - Alert on known malicious IP's, SSH Brute Force attacks, RDP traffic, …
  - …

Monitor AWS Config with CloudWatch Events
https://docs.aws.amazon.com/config/latest/developerguide/monitor-config-with-cloudwatchevents.html

Monitoring GuardDuty with CloudWatch
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html

Monitoring TrustedAdvisor with CloudWatch
https://docs.aws.amazon.com/awssupport/latest/user/cloudwatch-ta.html

Log Analysis in Athena

- Athena provides a super easy and scalable option for log analysis
- Query any data (directly) that resides in S3
- Create tables/queries on the fly
- Perform highly parallelized and efficient searches across massive amounts of data*

  * With the proper data partitioning!

Analyze Security, Compliance, and Operational Activity Using AWS CloudTrail and Amazon Athena
https://aws.amazon.com/blogs/big-data/aws-cloudtrail-and-amazon-athena-dive-deep-to-analyze-security-compliance-and-operational-activity/

Analyzing VPC Flow Logs in Athena
https://aws.amazon.com/blogs/mt/analyzing-vpc-flow-logs-got-easier-with-support-for-s3-as-a-destination/

Tons More Tips for AWS Alerting/Monitoring…

If you're interested in learning more about AWS Alerting and Monitoring, check out my other talks on the subjects (links on my website)…

RSAConference2020

Microsoft Azure

Overview of Logging

Core Logs

- Activity Logs
  - Management Plane events (Operations performed against your subscription)
    - All Create, Update, List, or Delete actions performed
      - Create Virtual Machine, Delete Network Security Group (NSG), …
- Resource (Diagnostics) Logs
  - Data Plane events (Operations your Resource itself performed)
    - Getting a Secret from a Key Vault, Querying a DB, VM Metrics/Operations, …
- Azure Active Directory Logs
  - Active Directory activities/events (with built-in reports)

Azure Security Logging and Auditing
https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit

Activity + Resource Logs
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/platform-logs-overview

Activity Log Schema
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema

List of All Resource Operations
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

Resource Log Schemas (by Service)

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-schema

Azure Active Directory Logs
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/

Core Logs

- Windows Azure Diagnostics (WAD)
  - Collects host/system logs
- Application Logs/Insights
  - Monitor Application Health and Performance
  - Collect and Monitor Application/Server Logs
- Storage Analytics Logs
  - Detailed information about requests to Storage service

Windows Azure Diagnostics
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostics-extension-overview

Application Insights
https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

Application (Diagnostics) Logs
https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs

Storage Analytics Logs
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging

https://docs.microsoft.com/en-us/rest/api/storageservices/storage-analytics-logged-operations-and-status-messages
https://docs.microsoft.com/en-us/rest/api/storageservices/storage-analytics-log-format

Core Logs

- Network Security Group (NSG) Flow Logs
  - Netflow(ish) Logs
    - Source/Dest IP, Source/Dest Port, Protocol, Allowed/Denied, Bytes/Packets Sent
  - Diagnostic Logs
    - See which (and how) firewall rules were triggered/applied to traffic
- Security Center
  - Provides a variety of endpoint and account-based monitoring and threat detections
  - Endpoint log analytics agent (Microsoft Monitoring Agent) must be specifically configured

Network Security Group (NSG) Flow Logs
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log

Security Center
https://docs.microsoft.com/en-us/azure/security-center/security-center-intro
https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started

RSAConference2020

Microsoft Azure

Configuring Logging

Activity Logs

- Activity Logs
  - Enabled by default
  - Configure via:
    - Navigate to **Azure Monitor**
    - Select **Activity Log**
    - Select **Diagnostic Settings**
    - Configure + send to:
      - Storage
      - Log Analytics Workspace (for Azure Monitor)
      - Event Hub

Activity Logs
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/platform-logs-overview
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings

Resource Logs

- Resource (Diagnostic) Logs
  - Each Resource requires its own configuration
  - Configuration for a single resource:
    - Select **Monitoring** -> **Diagnostic Settings**
    - Select **Add diagnostic setting**
    - Configure + send to:
      - Storage
      - Log Analytics Workspace (for Azure Monitor)
      - Event Hub
  - Configuration for multiple resources:
    - Navigate to **Azure Monitor**
    - Select **Settings** -> **Diagnostic Settings**

Resource Logs

- Configure Diagnostics per Resource: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings
- Collect to Storage: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/resource-logs-collect-storage
- Send to Log Analytics Workspace (Azure Monitor): https://docs.microsoft.com/en-us/azure/azure-monitor/platform/resource-logs-collect-workspace
- Send to Event Hub: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/resource-logs-stream-event-hubs

Active Directory Logs

- Active Directory Logs
  - Enabled by default with the following logs/reports:
    - Audit Logs
    - Sign-in Logs
    - Risky Sign-in Logs
    - Users Flagged for Risk Logs
    - Provisioning Logs
  - Configure via:
    - Navigate to **Azure Active Directory** -> **Diagnostic Settings**
    - Select **Add diagnostic setting**
    - Configure **AuditLogs** and/or **SignInLogs** to send to:
      - Storage
      - Log Analytics Workspace (for Azure Monitor)
      - Event Hub

Active Directory Logs

- Collect to Storage: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-azure-monitor-route-logs-to-storage-account
- Send to Log Analytics Workspace (for Azure Monitor): https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
- Send to Event Hub: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub

Windows Azure Diagnostics (WAD) Logs

- Windows Azure Diagnostics
  - Configuration via:
    - Windows Azure Diagnostics (send to Storage, Log Analytics, Azure Monitor)
    - Windows Event Forwarding (send to your SIEM)
  - Configuration for VM's:
    - Configure diagnostics at run/build time manually or using templates

Windows Azure Diagnostics

- Configure for VM's to collect diagnostics and host logs: https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-windows
- Enable Application Logging: https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs
- VM Diagnostics Template: https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/diagnostics-template

Application (Diagnostic) Logs

- Configure Application Logging (Windows) – per App:
  - Navigate to **App Service Logs**
  - Select **On** for:
    - **Application Logging (Filesystem) – Temporary (12-hour) storage for debugging purposes**
    - **Application Logging (Blob) – Long term storage**
  - Select the (Log) **Level**
- Configure Application Logging (Linux/Container) – per App:
  - Navigate to **App Service Logs**
  - Select **Application Logging** -> **File System**
  - Configure:
    - **Quota (MB)**
    - **Retention Period (Days)**

Application Logs

- Enable Diagnostics Logs: https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs

Application (Diagnostic) Logs

- Configure Web Server Logging – per App:
  - Navigate to **App Service Logs**
  - Select **Web Server Logging**
  - Select to send to:
    - **Storage**
    - **File System**
  - Configure **Retention Period (Days)**
- Configure Detailed Error Messages – per App:
  - Navigate to **App Service Logs**
  - Set **Detailed Error Logging** to **On**

Application Logs

- Enable Diagnostics Logs: https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs

Application (Diagnostic) Logs

- Configure Failed Request Tracing – per App:
  - Navigate to **App Service Logs**
  - Set **Failed Request Tracing** to **On**
- Configure Deployment Logging – per App:
  - Enabled by default
    - "Happens automatically and there are no configurable settings for deployment logging. It helps you determine why a deployment failed."

Application Logs

- Enable Diagnostics Logs: https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs

Storage Analytics Logs

- Storage Analytics
  - Configure via Azure Portal – per Storage Account:
    - Navigate to **Storage Accounts**
    - Select the appropriate **Storage Account**
    - Select **Monitoring (Classic)** -> **Diagnostics Settings (Classic)**
    - Select the appropriate **Metrics**:
      - **API Metrics, Delete Data**
    - Select the appropriate **Logging**:
      - **Read, Write, Delete, Delete Data**
    - Set the **Retention (Days)**

Storage Analytics

- Enable Logging
  - https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging#enable-storage-logging
  - https://docs.microsoft.com/en-us/azure/storage/common/storage-monitor-storage-account?#configure-monitoring-for-a-storage-account

Network Security Group (NSG) Logs

- NSG Flow Logs
  - Pre-Requisites:
    - Register Microsoft.Insights Provider – per Subscription:
      - Navigate to **Subscriptions**
      - Select the appropriate **Subscription**
      - Select **Settings** -> **Resource Provider**
      - Select **Register**
    - Enable Network Watcher – per Region:
      - Navigate to **Network Watcher**
      - Click the "**>**" next to the Regions to expand them
      - Select the "**…**" next to each appropriate Region
      - Select **Enable Network Watcher**

Network Security Group (NSG) Flow Logs

- Enable NSG Traffic Analytics: https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

Network Security Group (NSG) Logs

- NSG Flow Logs
  - Configure NSG Flow Logs – per NSG:
    - Navigate to Network Watcher
    - Select **Logs** -> **NSG Flow Logs**
    - Select the appropriate **NSG**
    - Under **Flow Logs**, select **On**
    - Select **Version 2** for Flow Logs version (includes bytes/packets count + flow state)
    - Select the appropriate **Storage Account**
    - Select the appropriate **Retention Period (Days)** – for Storage v2 Accounts

Network Security Group (NSG) Flow Logs

- Enable NSG Flow Logs: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal
- Enable Diagnostic Logs: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log
- Ensure Storage is a “v2” account to allow for NSG Retention Policy: https://azure.microsoft.com/en-us/updates/nsg-flow-logs-retention-restored/

Network Security Group (NSG) Logs

- NSG Flow Logs
  - Configure NSG Flow Logs – per NSG:
    - Optional
      - Under **Traffic Analytics Status**, select **On**
      - Select **Processing Interval** (1 Hour, 10 Minutes)
      - Select existing (or new) **Log Analytics Workspace** as a log destination (for later analysis)

Network Security Group (NSG) Flow Logs

- Enable NSG Flow Logs: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal
- Enable Diagnostic Logs: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log
- Ensure Storage is a “v2” account to allow for NSG Retention Policy: https://azure.microsoft.com/en-us/updates/nsg-flow-logs-retention-restored/

Security Center

- Security Center
  - Configure endpoint log analytics agent via:
    - Automatic Provisioning (for all Azure VM's)
      - Select **Pricing & Settings**
      - Select the appropriate **Subscription**
      - Select **Data Collection**
      - Set **Auto Provisioning** to **On**
      - Select the appropriate **Workspace** for log destination

Security Center

- Configure Automatic Provisioning: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection#enable-automatic-provisioning-of-the-log-analytics-agent-

Security Center

- Security Center
  - Configure endpoint log analytics agent via:
    - Automatic Provisioning (for all Azure VM's)
      - Optional – **Store Additional Raw Data**
        - **None** (not recommended)
        - **Minimal** ("This set covers only events that might indicate a successful breach and important events that have a very low volume.") – 4624 / 4625 / 4688 / …
        - **Common** ("Provide a full user audit trail in this set.") – 4634 / ...
        - **All Events** (All Windows Security and AppLocker events)

Security Center

- What's Collected in Each Data Collection Tier: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection#data-collection-tier

Security Center

- Security Center
  - Configure endpoint log analytics agent via:
    - Manual Provisioning
      - Ensure Auto Provision is set to Off
      - Select **Pricing & Settings**
      - Select the appropriate **Subscription**
      - Ensure the **Pricing Tier** is set to **Standard**
      - Deploy Monitoring Agents to:
        - New VM's via a Resource Manager Template
        - Existing VM's via

Security Center

- Manual Log Analytics Agent Provisioning: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection#manual-agent-provisioning-

Security Center

- Security Center
  - Configure endpoint log analytics agent via:
    - Manual Provisioning
      - Deploy Monitoring Agents to:
        - New VM's via a Resource Manager Template
        - Existing VM's via **Log Analytics Workspace** -> **Virtual Machines** -> Select **VM** -> Click **Connect**
        - Existing VM's via PowerShell

Security Center

- Manual Log Analytics Agent Provisioning: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection#manual-agent-provisioning-
- Deploying to existing VM's: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

RSAConference2020

Microsoft Azure

Tips for Monitoring

Azure Monitor

- Activity Logs
  - Review for anomalous CREATE / DELETE / UPDATE actions
    - New Accounts
    - New resources created in unapproved methods / regions
- Network Activity
  - Review for anomalous traffic
    - After-hours traffic spikes
    - Heartbeat (C2)
    - Possible DDoS

Azure Monitor
https://docs.microsoft.com/en-us/azure/azure-monitor/overview

- Analyze Activity Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal
- Create Activity Log Alerts: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
- Analyze Active Directory activities
  - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics
  - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
- Analyze Storage activity:
  - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/storage-insights-overview
  - https://docs.microsoft.com/en-

    - us/azure/storage/common/storage-monitor-storage-account
- Analyze NSG Flow Logs
    - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-networking-analytics

Azure Diagnostics
- Configure: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-how-to-monitor

Azure Graph API
- Analyze Active Directory Activities: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api-quickstart

Application Insights
- Dashboard: https://docs.microsoft.com/en-us/azure/azure-monitor/app/overview-dashboard

Azure Monitor

- Resource Diagnostics (OS-level Logs)
  - Run queries for:
    - Host-level authentications
    - Process executions
    - Command-line/PowerShell activity
    - ..
- Use “Insights” Features for Anomaly Discovery

Azure Monitor
https://docs.microsoft.com/en-us/azure/azure-monitor/overview

- Analyze Activity Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal
- Create Activity Log Alerts: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
- Analyze Active Directory activities
  - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics
  - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
- Analyze Storage activity:
  - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/storage-insights-overview
  - https://docs.microsoft.com/en-

    - us/azure/storage/common/storage-monitor-storage-account
- Analyze NSG Flow Logs
    - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-networking-analytics

Azure Diagnostics
- Configure: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-how-to-monitor

Azure Graph API
- Analyze Active Directory Activities: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api-quickstart

Application Insights
- Dashboard: https://docs.microsoft.com/en-us/azure/azure-monitor/app/overview-dashboard

Network Watcher

- Analyze NSG Flow Logs in Network Watcher
  - Identify “Top Talkers”
  - Visualize Activity by Geographic Map
  - Statistics of Allowed vs. Blocked traffic
  - Identify “badness”:
    - Connection initiated inbound w/ large outbound data (web shell or just web server?)
    - Connection initiated outbound w/ large outbound data (reverse shell?)
    - Regular X byte connection started every Y minutes (C2?)
  - Query for known malicious IP’s

Network Watcher
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

Active Directory

- Utilize Built-In Auditing and Reports to Review Authentications
  - Security Reports
    - "Users At Risk" Report
      - A "risky" user is an indicator for a user account that might have been compromised
    - "Risky Sign-In" Report
      - A "risky sign-in" is an indicator for a sign-in attempt that might have been performed by someone who is not the legitimate owner of a user account

Active Directory Monitoring

- Security Reports
  - "Users At Risk" Report: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-user-at-risk
  - "Risky Sign-In" Report: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins
- Activity Reports
  - Audit Logs: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs
  - Sign-In Report: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Azure Monitor

https://docs.microsoft.com/en-us/azure/azure-monitor/overview

- Analyze Activity Logs: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics
- Create Activity Log Alerts: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
- Analyze Active Directory activities
    - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics
    - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
- Analyze Storage activity:
    - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/storage-insights-overview
    - https://docs.microsoft.com/en-us/azure/storage/common/storage-monitor-storage-account
- Analyze NSG Flow Logs
    - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-networking-analytics

Azure Diagnostics

- Configure: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-how-to-monitor

Azure Graph API

- Analyze Active Directory Activities: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api-quickstart

Application Insights

- Dashboard: https://docs.microsoft.com/en-us/azure/azure-monitor/app/overview-dashboard

Active Directory

- Utilize Built-In Auditing and Reports to Review Authentications
  - Activity Reports
    - Audit Logs
      - Audit all AD activities (New Users/Groups, Password Changes, New/Modified Admin Groups New/Modified Service Accounts)
    - Sign-In Report
      - Identify sign-in patterns of specific users (signing in from new location out of nowhere?)

Active Directory Monitoring

- Security Reports
  - "Users At Risk" Report: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-user-at-risk
  - "Risky Sign-In" Report: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risky-sign-ins
- Activity Reports
  - Audit Logs: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs
  - Sign-In Report: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Azure Monitor

https://docs.microsoft.com/en-us/azure/azure-monitor/overview

- Analyze Activity Logs: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics
- Create Activity Log Alerts: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log
- Analyze Active Directory activities
    - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics
    - https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics
- Analyze Storage activity:
    - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/storage-insights-overview
    - https://docs.microsoft.com/en-us/azure/storage/common/storage-monitor-storage-account
- Analyze NSG Flow Logs
    - https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-networking-analytics

Azure Diagnostics

- Configure: https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-how-to-monitor

Azure Graph API

- Analyze Active Directory Activities: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api-quickstart

Application Insights

- Dashboard: https://docs.microsoft.com/en-us/azure/azure-monitor/app/overview-dashboard

Security Center

- Security Center
  - Use this as a force multiplier for your monitoring/security efforts
  - Secure Score
    - Review, investigate, and remediate findings
    - Start with highest impact Recommendations
  - Security Alerts
    - Monitor for, and investigate, these alerts
    - Can be early (or only) indicators of compromise

Security Center

- Secure Score: https://docs.microsoft.com/en-us/azure/security-center/security-center-secure-score
- Security Alerts: https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview

Azure Sentinel

- Azure-based native SIEM
- Connect/send all your logs to Sentinel to:
  - Use built-in (and custom) analytics for searching/alerting
  - Use built-in (or custom) workbooks to search/investigate
  - Use built-in Investigations capability (and graphs) to investigate possible incidents
  - Use Playbooks to build and automate responses to incidents

Azure Sentinel
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-built-in
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

RSAConference2020

Google Cloud Platform (GCP)

Overview of Logging

Core Logs

- Activity Logs
  - API calls or other administrative actions that modify the configuration or metadata of resources
  - Enabled by default (at no charge)
  - Always written – you cannot configure/disable them
  - Automatically retained for 400 days

Admin Activity Logs
https://cloud.google.com/logging/docs/audit#admin-activity

Data Access Logs
https://cloud.google.com/logging/docs/audit#data-access

System Event Audit Logs
https://cloud.google.com/logging/docs/audit#system-event

Audit Log Retention
https://cloud.google.com/logging/docs/audit#audit_log_retention

Best Practices for Working with Google Cloud Audit Logging
https://cloud.google.com/blog/products/gcp/best-practices-for-working-with-google-cloud-audit-logging

Google Services with Audit Logs

https://cloud.google.com/logging/docs/audit/services

Monitored Resources List
https://cloud.google.com/logging/docs/api/v2/resource-list

Core Logs

- Data Access Logs
  - API calls that create, modify, or read user-provided data
  - Disabled by default
  - Automatically retained for 30 days

Core Logs

- System Event Audit Logs
  - Log entries for Google Cloud administrative actions that modify the configuration of resources
  - Generated by Google systems (not driven by direct user action)
  - Always written – you cannot configure/disable them
  - Automatically retained for 400 days

Core Logs

- Application/Host/OS Logs
  - Collect Application and Host/OS-level logs via the Stackdriver Logging Agent
    - GCP's customized version of Fluentd
  - Monitors/collects the following logs by default:
    - Linux
      - Syslog, nginx, apache2, apache-error
    - Windows
      - Windows Event Logs

Stackdriver Logging Agent
https://cloud.google.com/logging/docs/agent

How to log your application on Google Compute Engine
https://medium.com/google-cloud/how-to-log-your-application-on-google-compute-engine-6600d81e70e3

Writing Developer logs with Google Cloud Logging
https://medium.com/google-cloud/writing-developer-logs-with-google-cloud-logging-484016c05e16

Core Logs

- VPC Flow Logs
  - Per-VM or Per-VPC network flow logs
  - Allow you to:
    - Monitor the VPC network
    - Perform network diagnosis
    - Filter the flow logs by VMs and by applications to understand traffic changes
    - Understand traffic growth for capacity forecasting
  - Built into the networking stack of the VPC network infrastructure
    - No extra delay or performance penalty in enabling

VPC Flow Logs
https://cloud.google.com/vpc/docs/using-flow-logs

Core Logs

- Cloud Storage Logs
  - Access Logs
    - Provides info for all of the requests made on a specified bucket
      - Access to public objects
      - Changes made by the Object Lifecycle Management feature
    - Server access style logs (client/dest IP, port, method, uri, bytes, etc.)
    - Created Hourly, when there is activity (typically created 15 minutes after the end of the hour)
  - Storage Logs
    - Provide info about the storage size (in “byte_hours”) of buckets per 24 hour period
    - Created Daily with previous day’s info (typically created before 10:00 am PST)
    - Not generally recommended to use - suggested to use **Monitoring** -> **Metrics Explorer** instead

Cloud Storage Logs (Access and Storage Logs)
https://cloud.google.com/storage/docs/access-logs

Cloud Storage Logs Collection Info
https://cloud.google.com/storage/docs/access-logs#downloading

RSAConference2020

Google Cloud Platform (GCP)

Configuring Logging

Data Access Logs

- Configure Data Access Logs (logging per Service)
  - Navigate to **IAM & Admin** -> **Audit Logs**
  - Select the appropriate Project/Folder/Organization
  - Select a **Service**
  - Turn on/off the following logging for the selected **Service**:
    - **Admin Read**
    - **Data Read**
    - **Data Write**
  - Click **Save**

Configuring Data Access Logs – Per Service
https://cloud.google.com/logging/docs/audit/configure-data-access

Data Access Logs

- Configure Data Access Logs (default logging for All New/Existing Services)
  - Navigate to **IAM & Admin** -> **Audit Logs**
  - Select the appropriate Project/Folder/Organization
  - Click **Default Audit Config**
  - Turn on/off the following logging for the **All Services**:
    - **Admin Read**
    - **Data Read**
    - **Data Write**
  - Click **Save**

Configuring Data Access Logs – Default for All Services
https://cloud.google.com/logging/docs/audit/configure-data-access#config-console-default

Application Logs

- Stackdriver Logging Agent

  *Note: Installed by default on VM's running in **Google Kubernetes Engine** or **App Engine**

  - Installing the Agent
    - Linux (via Command-Line)

```
$ curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
$ sudo bash install-logging-agent.sh
```

      - (Optional) - Edit Proxy config in `/etc/default/google-fluentd` to export `http_proxy`, `https_proxy`, and `no_proxy` environment variables

```
$ sudo service google-fluentd restart
```


Collecting Logs Using the Stackdriver Logging Agent
https://cloud.google.com/logging/docs/agent/installation

Application Logs

- Stackdriver Logging Agent
  - Installing the Agent
    - Windows (via Command Line)
      - (Optional) – Export proxy variables via Admin Command Prompt

```
> setx http_proxy http://<PROXY_IP>:<PROXY_PORT> /m
> setx https_proxy http://<PROXY_IP>:<PROXY_PORT> /m
> setx no_proxy 169.254.169.254 /m
```

      - Open PowerShell terminal (No Admin Needed)

```
> cd $env:UserProfile;
> (New-Object
Net.WebClient).DownloadFile("https://dl.google.com/cloudagents/windows/S
tackdriverLogging-v1-10.exe", ".\StackdriverLogging-v1-10.exe")
> .\StackdriverLogging-v1-10.exe /S /D="C:\Preferred\Install\Dir\"
```

URL may change over time

Specify Silent Install

Set Install Dir

Collecting Logs Using the Stackdriver Logging Agent
https://cloud.google.com/logging/docs/agent/installation

Application Logs

- Stackdriver Logging Agent
  - Installing the Agent
    - Windows (via GUI)
      - Simply download + install the Stackdriver Logging Agent executable

Collecting Logs Using the Stackdriver Logging Agent
https://cloud.google.com/logging/docs/agent/installation

Application Logs

- Stackdriver Logging Agent
  - Configuring the Agent
    - "The Logging agent comes with a default configuration; in most common cases, no additional configuration is required." (YMMV)
      - Due to GCP's implementation/inclusion of a `fluentd-catch-all-config`
    - Agent configuration files locations:
      - Linux

        `/etc/google-fluentd/google-fluentd.conf`
      - Windows

        `C:\Program Files (x86)\Stackdriver\LoggingAgent\fluent.conf`

Collect Logs with Fluentd
https://medium.com/google-cloud/how-to-log-your-application-on-google-compute-engine-6600d81e70e3
https://medium.com/google-cloud/writing-developer-logs-with-google-cloud-logging-484016c05e16
https://cloud.google.com/solutions/real-time/fluentd-bigquery

Stackdriver Logging Agent Configuration
https://cloud.google.com/logging/docs/agent/configuration
https://cloud.google.com/logging/docs/agent/configuration#configure

GCP Fluentd "Catch-All" Config
https://github.com/GoogleCloudPlatform/fluentd-catch-all-config

Fluentd Parsers
https://docs.fluentd.org/parser#list-of-built-in-parsers

Application Logs

- Stackdriver Logging Agent
  - Customizing the Agent to collect additional (non-standard) logs
    - Create a new config file (e.g. `new-log.conf`) within the following directory:
      - Linux

        `/etc/google-fluentd/config.d/`
      - Windows

        `C:\Program Files (x86)\Stackdriver\LoggingAgent\`
    - Set the appropriate `path`, `format`, `tag`, … in the config file
    - Restart the service

Streaming Logs from Additional Inputs
https://cloud.google.com/logging/docs/agent/configuration#streaming_logs_from_additional_inputs

Container (GKE) Logs

- Stackdriver Logging for Kubernetes (GKE)
  - Metrics (CPU/Mem Utilization, Incidents, etc.) for GKE Clusters/Nodes
  - Configuring Stackdriver (New Cluster)
    - Navigate to **Kubernetes Engine** -> **Clusters**
    - Click Create Cluster
    - Click **Availability, networking, security, and additional features**
    - Select Enable Stackdriver Kubernetes Engine Monitoring
    - Click **Create**
  - Configuring Stackdriver (Existing Cluster)

Stackdriver Support for GKE
https://cloud.google.com/monitoring/kubernetes-engine/

Container (GKE) Logs

- Stackdriver Logging for Kubernetes (GKE)
  - Configuring Stackdriver (Existing Cluster)

    *Requires cluster to version 1.12.7 or higher (will need to manually upgrade if not)
    - Navigate to **Kubernetes Engine** -> **Clusters**
    - Click the **Edit (pencil)** icon on the appropriate Cluster
    - In the **Stackdriver Kubernetes Engine Monitoring** drop down, select **Enabled**
    - Click **Save**
  - (Optional) Configuring Prometheus Monitoring Support
    - Stackdriver configured as sidecar, exports metrics as “External Metrics”

Stackdriver Support for GKE
https://cloud.google.com/monitoring/kubernetes-engine/

Manually Upgrading a Cluster
https://cloud.google.com/kubernetes-engine/docs/how-to/upgrading-a-cluster

Configuring Prometheus for GKE
https://cloud.google.com/monitoring/kubernetes-engine/prometheus

Container (GKE) Logs

- Enabling Auditd Logs on GKE Nodes
  - Provides OS/Host-level auditing logs (errors, logins, binary execution, etc.) to provide info on the state of your cluster/workloads
  - Requires use of a Kubernetes DaemonSet**

    **Works only on nodes running Container-Optimized OS
    - Manages groups of replicated Pods
    - Runs one Pod on each cluster node with 2 Containers to configure auditd:
      - First is an `init-container` that starts the cloud-audit-setup systemd service
      - Second is `fluentd-gcp-cos-auditd` Container that configures auditd

Enabling Linux Auditd Logs on GKE Node
https://cloud.google.com/kubernetes-engine/docs/how-to/linux-auditd-logging

DaemonSet
https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset

Container (GKE) Logs

- Enabling Auditd Logs on GKE Nodes
  - Configuring Auditd Logging (per Cluster)**

    **As always with configuring auditd – *be aware of performance implications!*

    - Download the example manifests

      ```
      $ curl
      https://raw.githubusercontent.com/GoogleCloudPlatform/k8s-
      node-tools/master/os-audit/cos-auditd-logging.yaml > cos-
      auditd-logging.yaml
      ```

    - Deploy the logging DaemonSet and ConfigMap

      ```
      $ kubectl apply -f cos-auditd-logging.yaml
      ```

    - Verify logging pods have started

      ```
      $ kubectl get pods --namespace=cos-auditd
      ```


Enabling Linux Auditd Logs on GKE Node
https://cloud.google.com/kubernetes-engine/docs/how-to/linux-auditd-logging

DaemonSet
https://cloud.google.com/kubernetes-engine/docs/concepts/daemonset

VPC Flow Logs

- Configuring VPC Flow Logs (per Subnet*)

  *Note: VPC Flow logs may only be enabled per-Subnet

  – New Subnet
    - Navigate to **Networking** -> **VPC Networks**
    - Select the appropriate **Network**
    - Click **Add Subnet**
    - Under **Flow Logs**, select **On**
    - Click **Configure Logs** to set **Aggregation Interval**, **Include Metadata**, and **Sample rate**
    - Click **Add**

Enabling VPC Flow Logging
https://cloud.google.com/vpc/docs/using-flow-logs#enabling_vpc_flow_logging

VPC Flow Logs

- Configuring VPC Flow Logs (per Subnet*)

  *Note: VPC Flow logs may only be enabled per-Subnet

  - Existing Subnet
    - Navigate to **Networking** -> **VPC Networks**
    - Select the appropriate **Subnet**
    - Under **Flow Logs**, select **On**
    - Click **Configure Logs** to set **Aggregation Interval**, **Include Metadata**, and **Sample rate**
    - Click **Add**

Enabling VPC Flow Logging
https://cloud.google.com/vpc/docs/using-flow-logs#enabling_vpc_flow_logging

Cloud Storage Logs

- Configure Log Delivery for Access and Storage Logs

  *Requires use of `gsutil` tool (or XML/JSON API's)

  – Create a Bucket to store the logs (if not already created)

  ```
  $ gsutil mb gs://example-logs-bucket
  ```

  – Configure Bucket to allow Cloud Storage `WRITE` permissions

  ```
  $ gsutil acl ch -g cloud-storage-analytics@google.com:W
  gs://example-logs-bucket
  ```

  – (Optional) Configure default object ACL

  ```
  $ gsutil defacl set project-private gs://example-logs-bucket
  ```


Configuring Cloud Storage Access and Storage Log Delivery
https://cloud.google.com/storage/docs/access-logs#delivery

Gsutil Tool
https://cloud.google.com/storage/docs/gsutil

Cloud Storage Logs

- Configure Log Delivery for Access and Storage Logs
  - Enable Logging for each Bucket in scope

```
$ gsutil logging set on -b gs://example-logs-bucket [-o
log_object_prefix ] gs://example-bucket
```

    - Optionally can specify `log_object_prefix`
    - By default, the object prefix is the name of the bucket for which the logs are enabled

Configuring Cloud Storage Access and Storage Log Delivery
https://cloud.google.com/storage/docs/access-logs#delivery

Gsutil Tool
https://cloud.google.com/storage/docs/gsutil

Exporting Logs

- Can export logs to 3 destination types:
  - Cloud Storage Bucket (for simple retention)
  - BigQuery Datasets (to stage for queries/investigations)
    - Ideal for native investigation and response capabilities
  - Pub/Sub Topics (to send to another application/SIEM)
    - Useful if you're using a separate/dedicated SIEM for log retention, monitoring, and querying

Best Practices for Cloud Audit Logs
https://cloud.google.com/logging/docs/audit/best-practices

Overview of Logs Exports
https://cloud.google.com/logging/docs/export

Best Practices for Common Logging Export Scenarios
https://cloud.google.com/solutions/design-patterns-for-exporting-stackdriver-logging

Exporting Logs

- Exporting Logs to BigQuery with Log Viewer

  *You can also use the `gloud` tool or Stackdriver Logging API

  - Per-Project Sink (All Logs, No Filtering)
    - Navigate to **Stackdriver** -> **Logging** -> **Logs Router**
    - Click **Create Sink**
      - Enter **Sink Name**
      - Select **BigQuery** as the **Sink Service**
      - Select **Use Partitioned Tables**
      - For **Sink Destination**, select **Create New BigQuery Dataset**
      - Enter the **BigQuery Dataset Name** and click **Create**
      - Click **Create Sink**

Exporting Logs with Log Viewer
https://cloud.google.com/logging/docs/export/configure_export_v2

Exporting Logs

- Exporting Logs to BigQuery with Log Viewer
  - Organization-Level Sink (Aggregate Sink of all Admin Activity)

```
$ gcloud logging sinks create my-bq-sink
bigquery.googleapis.com/projects/my-project/datasets/my_dataset
--log-filter='logName: "logs/cloudaudit.googleapis.com%2Factivity"'
--organization=<org_ID> --include-children
```


Aggregated Exports
https://cloud.google.com/logging/docs/export/aggregated_exports

Creating Sinks with Gcloud Tool
https://cloud.google.com/logging/docs/reference/tools/gcloud-logging#creating_sinks

Manually Creating Sinks
https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/gcp/manually-create-sink.htm

Exporting Logs

- Exporting Logs to BigQuery with Log Viewer
  - Folder-Level Sink (Aggregate Sink of all Data Access Activity)

```
$ gcloud logging sinks create my-bq-sink
bigquery.googleapis.com/projects/my-project/datasets/my_dataset
--log-filter='logName: "logs/cloudaudit.googleapis.com%2Fdata_access"'
--folder=<folder_ID> --include-children
```


Aggregated Exports
https://cloud.google.com/logging/docs/export/aggregated_exports

Creating Sinks with Gcloud Tool
https://cloud.google.com/logging/docs/reference/tools/gcloud-logging#creating_sinks

Manually Creating Sinks
https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/gcp/manually-create-sink.htm

Log Sink Cheat Sheet

Log Types Supported by the GCP Sensor

Log Type	Filter to Capture This Log	Notes
Audit Logs at the Organization Level	organizations/<organization-id>/logs/cloudaudit.googleapis.com	To filter these logs further, append: • **%2Factivity**: For activity logs • **%2Fdata_access**: For data access logs • **%2Fsystem_event**: For system events
Audit Logs at the Project Level	projects/<project-id>/logs/cloudaudit.googleapis.com	To filter these logs futher, append: • **%2Factivity**: For activity logs • **%2Fdata_access**: For data access logs • **%2Fsystem_event**: For system events
VPC Flow Logs	projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows	
Firewall Logs	projects/<project-id>/logs/compute.googleapis.com%2Ffirewall	
Syslog	projects/<project-id>/logs/syslog	These logs are delivered via the Stackdriver logging agent
Apache Logs	projects/<project-id>/logs/apache	• **-access**: For access logs • **-error**: For error logs
Nginx Logs	projects/<project-id>/logs/nginx	• **-access**: For access logs • **-error**: For error logs

Source Link

RSAConference2020

Manually Creating Sinks
https://cybersecurity.att.com/documentation/usm-anywhere/deployment-guide/gcp/manually-create-sink.htm

RSAConference2020

Google Cloud Platform (GCP)

Tips for Monitoring

Stackdriver Monitoring/Alerting

- Utilize Stackdriver Monitoring to create alerts
  - Metrics-Based Alerts
    - Create Alerts based on:
      - High CPU Usage (bitcoin miner? ransomware encryption?)
      - High Memory Usage (resource exhaustion?)
      - Uptime (something recently rebooted? why?)
  - Application Log-Based Alerts
    - Gratuitous 404 errors

Stackdriver Monitoring and Alerting
https://cloud.google.com/monitoring/alerts/using-alerting-ui

Creating an Alerting Policy on a Counter-Based Metric
https://cloud.google.com/logging/docs/logs-based-metrics/charts-and-alerts#alert-on-lbm

Using Stackdriver Logs Viewer for Investigations

- Utilize Stackdriver Logs query service to perform regular queries for anomalies
- Define log(s) to search:

```
log_name:"/logs/cloudaudit.googleapis.com%2Factivity" AND...
log_name:"/logs/cloudaudit.googleapis.com%2Fdata_access" AND...
log_name:"/logs/cloudaudit.googleapis.com%2Fsystem_event" AND...
```

- Search a specific resource:

```
logName:"projects/[PROJECT_ID]/logs" AND
resource.type=[RESOURCE_TYPE] AND
resource.labels.instance_id=[INSTANCE_ID]
```


Sample Queries
https://cloud.google.com/logging/docs/view/query-library

Monitored Resources
https://cloud.google.com/logging/docs/api/v2/resource-list

Using Stackdriver Logs Viewer for Investigations

- Perform targeted searches
  - HTTP Error Logs

```
resource.type="gae_app" AND proto_payload.status >= 400 AND
sample(insertId, 0.1)
```

  - Service Account Creation

```
resource.type="service_account" AND
log_name="projects/[PROJECT_ID]/logs/cloudaudit.googleapi
s.com%2Factivity" AND
proto_payload.method_name="google.iam.admin.v1.CreateServ
iceAccount”
```


Sample Queries
https://cloud.google.com/logging/docs/view/query-library

Monitored Resources
https://cloud.google.com/logging/docs/api/v2/resource-list

Using Stackdriver Logs Viewer for Investigations

- Perform targeted searches
  - Firewall Rule Deletion

```
resource.type="gce_firewall_rule" AND
log_name="projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fact
ivity" AND proto_payload.method_name:"firewalls.delete"
```

  - Bucket Creation

```
resource.type="gcs_bucket" AND
log_name="projects/[PROJECT_ID]/logs/cloudaudit.googleapis.com%2Fact
ivity" AND proto_payload.method_name="storage.buckets.create"
```


Sample Queries
https://cloud.google.com/logging/docs/view/query-library

Monitored Resources
https://cloud.google.com/logging/docs/api/v2/resource-list

Accessing VPC Flow Logs
https://cloud.google.com/vpc/docs/using-flow-logs#accessing_logs_via

Using Stackdriver Logs Viewer for Investigations

- Perform targeted searches
  - All Inbound SSH Activity (VPC Flow Logs)

```
resource.type="gce_subnetwork" AND
log_name="projects/[PROJECT_ID]/logs/compute.googleapis.com%2Fvpc_flows" AND json_payload.connection.dst_port=”22"
```


Sample Queries
https://cloud.google.com/logging/docs/view/query-library

Monitored Resources
https://cloud.google.com/logging/docs/api/v2/resource-list

Accessing VPC Flow Logs
https://cloud.google.com/vpc/docs/using-flow-logs#accessing_logs_via

GKE Monitoring

- Native Tooling
  - Stackdriver Kubernetes Engine Monitoring
    - Dashboard interface to your Kubernetes Clusters
    - View alerts, metrics, logs, and details surrounding them
    - Can view by Aggregation categories:
      - Infrastructure (Aggregate by Cluster -> Node -> Pod -> Container)
      - Workloads (Aggregate by Cluster -> Namespace -> Workload -> Pod -> Container)
      - Service (Aggregate by Cluster -> Namespace -> Service -> Pod -> Container)

Observing your GKE Clusters
https://cloud.google.com/monitoring/kubernetes-engine/observing

GKE Monitoring

- Native(ish*) Tooling
  - Prometheus
    - *Technically third-party, but GCP has built a Stackdriver Prometheus sidecar
    - Utilize standard Monitoring console's Metrics Explorer
    - Select Kubernetes Container as Resource Type
    - Specify external Metric fields with "external/prometheus/" prefix

Using Prometheus to monitor Kubernetes
https://cloud.google.com/monitoring/kubernetes-engine/prometheus

Viewing Prometheus Metrics
https://cloud.google.com/monitoring/kubernetes-engine/prometheus#viewing_metrics

Stackdriver Prometheus Sidecar
https://github.com/Stackdriver/stackdriver-prometheus-sidecar/blob/master/README.md

GKE Monitoring

- Third-Party Tooling
  - Falco
    - Dedicated security auditing/monitoring solution for Kubernetes
    - "Falco lets you continuously monitor and detect container, application, host, and network activity, all in one place, from one source of data, with one set of rules."
    - Behavior monitoring/analytics (via SysCall monitoring) to help identify/alert when:
      - A shell is run inside a container
      - A server process spawns a child process of an unexpected type
      - A sensitive file, like /etc/shadow, is unexpectedly read
      - A non-device file is written to /dev
      - A standard system binary (like ls) makes an outbound network connection

Using Falco for Security Auditing/Monitoring
https://kubernetes.io/docs/tasks/debug-application-cluster/falco/
https://falco.org/docs/event-sources/kubernetes-audit/
https://github.com/falcosecurity/falco/blob/master/rules/k8s_audit_rules.yaml
https://github.com/falcosecurity/falco

Using BigQuery for Investigations

- Query BigQuery DataSets established previously
  - Utilize Log Sinks to aggregate/segregate certain types of data into certain DataSets (i.e. Tables) as the source(s) for queries
- Can run Active and Scheduled Queries
  - Manually run queries if/when needed
  - Run Scheduled Queries and regularly review results

Big Query QuickStart
https://cloud.google.com/bigquery/docs/quickstarts/quickstart-web-ui

Scheduling BigQuery Queries
https://cloud.google.com/bigquery/docs/scheduling-queries

Using BigQuery for Investigations

- Identify Virtual Machine Deletions in Activity Logs

```
SELECT timestamp, resource.labels.instance_id,
protopayload_auditlog.authenticationInfo.principalEmail,
protopayload_auditlog.resourceName, protopayload_auditlog.methodName

FROM (TABLE_DATE_RANGE(
[PROJECT].[DATASET].cloudaudit_googleapis_com_activity,
DATE_ADD(CURRENT_TIMESTAMP(),-7,'DAY'), CURRENT_TIMESTAMP()) )

WHERE resource.type = "gce_instance" AND operation.first IS TRUE AND
protopayload_auditlog.methodName = "v1.compute.instances.delete"

ORDER BY timestamp, resource.labels.instance_id

LIMIT 1000
```


BigQuery Sample Queries
https://cloud.google.com/solutions/exporting-stackdriver-logging-for-security-and-access-analytics#sample_questions_and_queries

BigQuery Audit Logs Overview
https://cloud.google.com/bigquery/docs/reference/auditlogs/

Querying Exported Logs
https://cloud.google.com/bigquery/docs/reference/auditlogs/#querying_exported_logs

GCP API Explorer
https://developers.google.com/apis-explorer/

Compute API
https://cloud.google.com/compute/docs/reference/rest/v1/

Using BigQuery for Investigations

- Identify Most Common Actions in Data Access Logs

```
SELECT protopayload_auditlog.methodName, resource.type, COUNT(*) AS
counter

FROM (TABLE_DATE_RANGE(
[PROJECT].[DATASET].cloudaudit_googleapis_com_data_access,
DATE_ADD(CURRENT_TIMESTAMP(),-30,'DAY'), CURRENT_TIMESTAMP()) )

GROUP BY protopayload_auditlog.methodName, resource.type

ORDER BY COUNTER DESC

LIMIT 1000
```


BigQuery Sample Queries
https://cloud.google.com/solutions/exporting-stackdriver-logging-for-security-and-access-analytics#sample_questions_and_queries

BigQuery Audit Logs Overview
https://cloud.google.com/bigquery/docs/reference/auditlogs/

Querying Exported Logs
https://cloud.google.com/bigquery/docs/reference/auditlogs/#querying_exported_logs

GCP API Explorer
https://developers.google.com/apis-explorer/

RSAConference2020

In Conclusion…

(TL;DR)

TL;DR

There is no TL;DR…

Too. Much. Material.

How Can You Apply This Starting Right Now?

- Next week you should:
  - Begin getting familiar with the core logs in each provider
    - I'd suggest assigning one (or more) SME's to each Cloud
    - Or accept that one person is about to be extremely busy form here on out…
  - Start poking around the Consoles and playing with configurations
  - Start identifying and testing multiple access and logging configuration methods
    - Console
    - CLI
    - Custom (and/or Open Source) Scripts

How Can You Apply This Starting Right Now?

- In the first three months following this presentation you should:
  - Have the core logs enabled and centralized
  - Begin testing and verifying the log configurations and contents:
    - How easy is it to access the logs?
    - Do the logs contain all the information needed to perform comprehensive investigations?
    - If not… (in this order)
      - How can those gaps be addressed with native tooling?
      - How can those gaps be address with third-party tooling?
    - Do we have an effective and efficient way to aggregate and analyze the logs?

How Can You Apply This Starting Right Now?

- Within six months you should:
  - Identify any gaps in log collection methodologies and/or content
  - Have a roadmap for fixing the identified gaps
  - Be planning several tabletop exercises to test your logging configuration, content, and access with real-world scenarios
    - Compromised Access Key
    - Compromised Instance(s) involving SSRF
    - Unauthorized S3 Data Access/Transfer
    - DDoS
    - …
  - Get creative – you know what needs testing

The End

Please feel free to reach out!

Email: jpoling@secureworks.com
Twitter: @JPoForenso
Blog: https://www.ponderthebits.com