Chris Farris in…

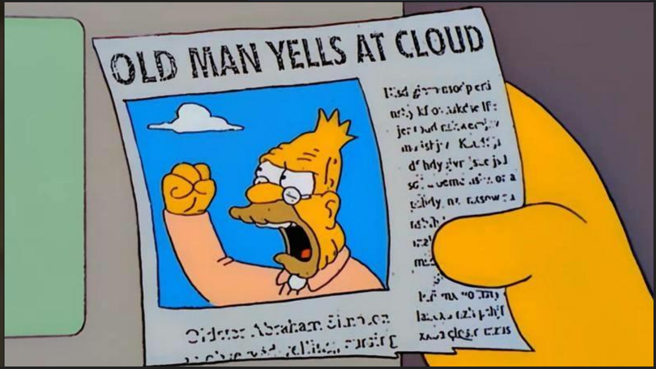
THE MULTI-CLOUD OF MADNESS

HackCon 2024

Chris Farris
PrimeHarbor Technologies

Who Am I?

- Built the cloud security programs for some media companies
- Founder: fwd:cloudsec conference
- Rants a lot on Twitter
- Somehow was named a Security Hero by AWS
- Cloud Security Consultant



Agenda

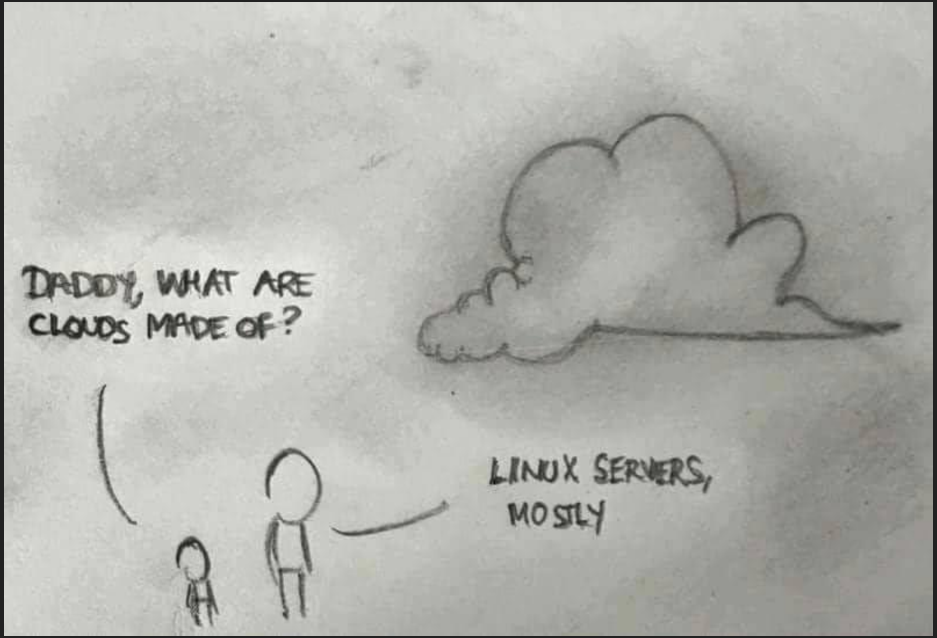
- What is Multi-Cloud
- Why it is Madness
- Cloud Governance
- Minimally Viable Multi-Cloud Governance
- Takeaways

https://pht.us/hackcon2024

What is the cloud?

NIST Definition:

1. On-demand self-service
2. Broad Network Access
3. Resource Pooling
4. Rapid Elasticity
5. Measured Service



Who is "The Cloud"?

Azure

ORACLE CLOUD

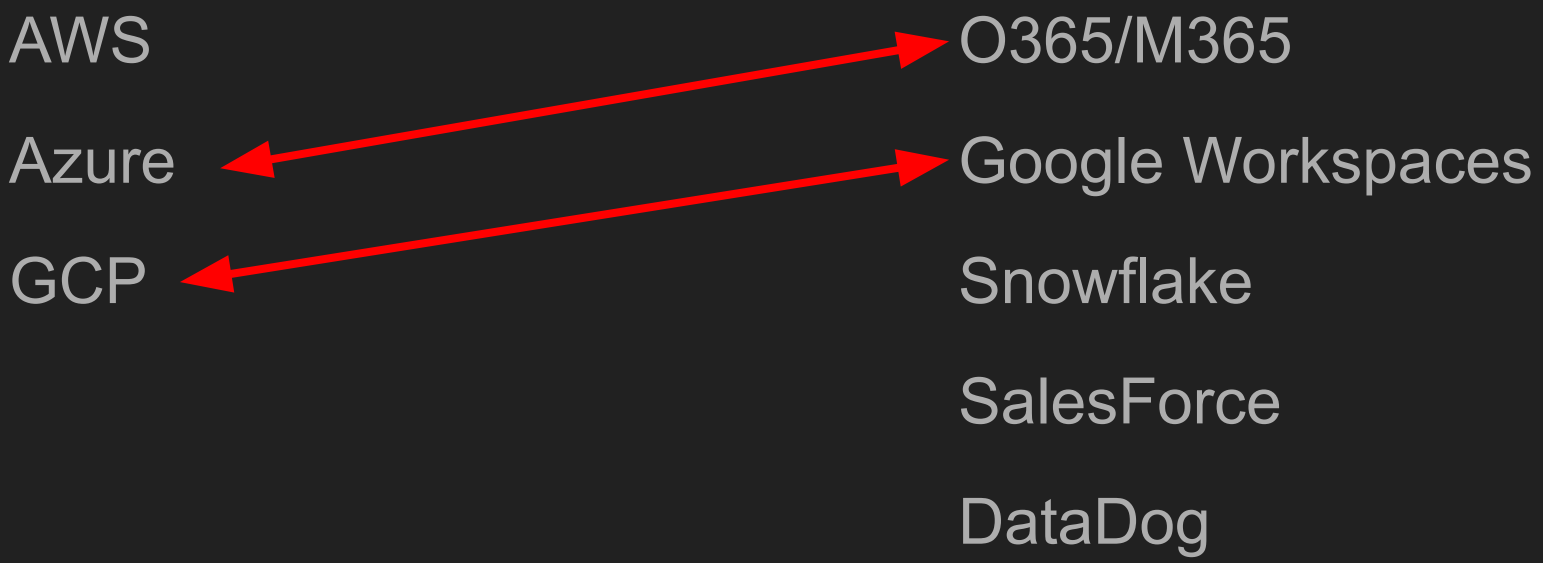
aws

Google Cloud Platform

SOFTLAYER an IBM Company

THINK THE ELECTORAL COLLEGE IS COMPLICATED?
TRY MANAGING MULTIPLE CLOUDS.

IaaS and SaaS



AWS

Azure

GCP

O365/M365

Google Workspaces

Snowflake

SalesForce

DataDog

Why is this different from on-prem?

Identity is the new perimeter

or

You need to defend three dimensionally

or

"*Cute network controls you have there if would be a shame if someone just routed around them*"

The two schools of Multi-Cloud

“Our workloads must be instantly portable to another cloud provider. We cannot depend on Amazon or Microsoft not to raise prices on us”

– An executive who has experienced an Oracle Audit

“We use AWS for our customer facing application, Azure for our back office finance systems, and Google’s Big Query for our data analytics team”

– An executive who uses the right cloud for the right job

More reasons to be multi-cloud

Mergers & Acquisitions

SaaS service provider

You are multi-cloud whether you like it or not

Problems with being Multi-Cloud

1. Cost
2. Security & Identity
3. People

All Clouds are not the same

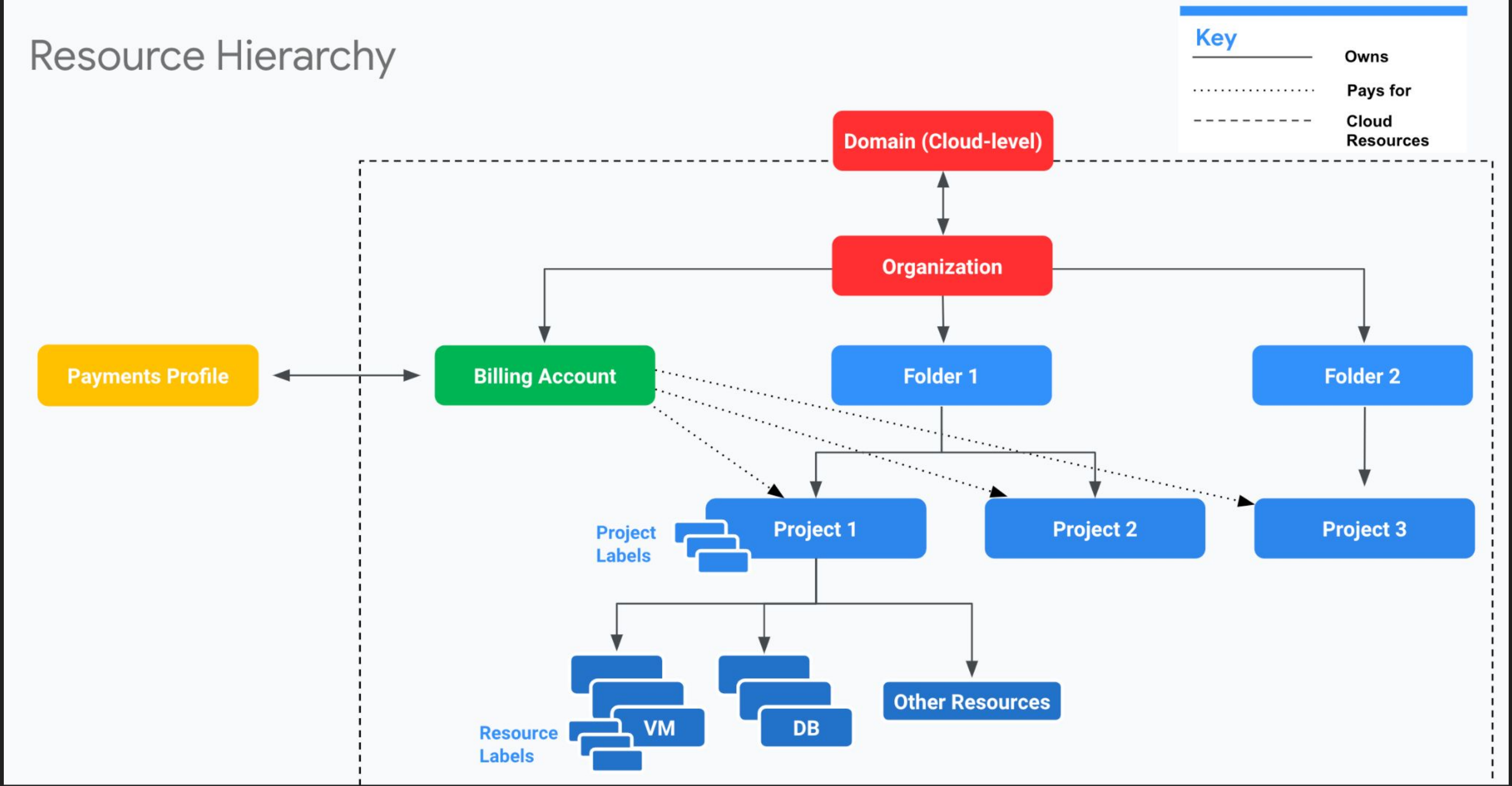
Tenancy boundaries

AWS: Account
Azure: Subscription
GCP: Project

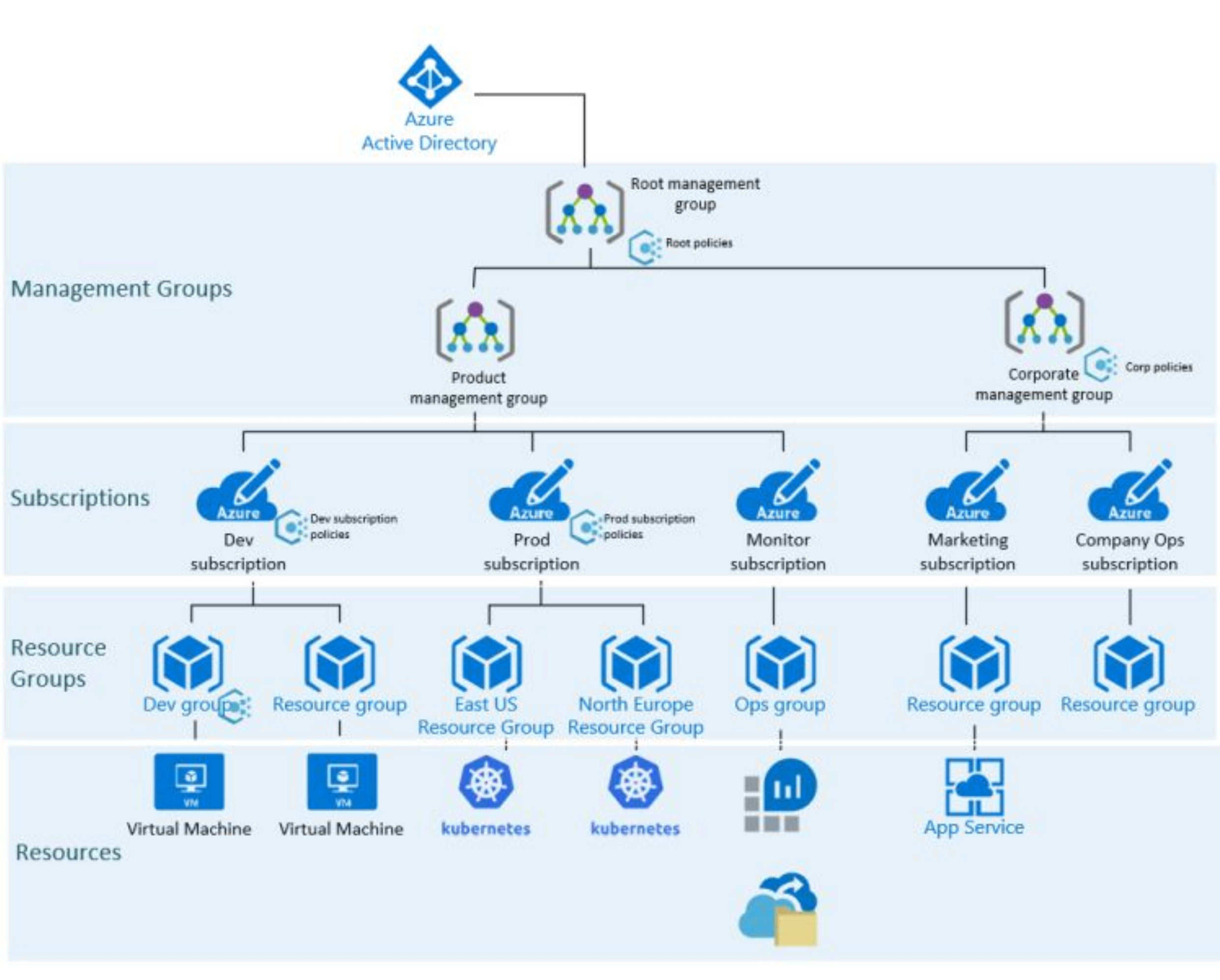
Only one of these is an actual security boundary.

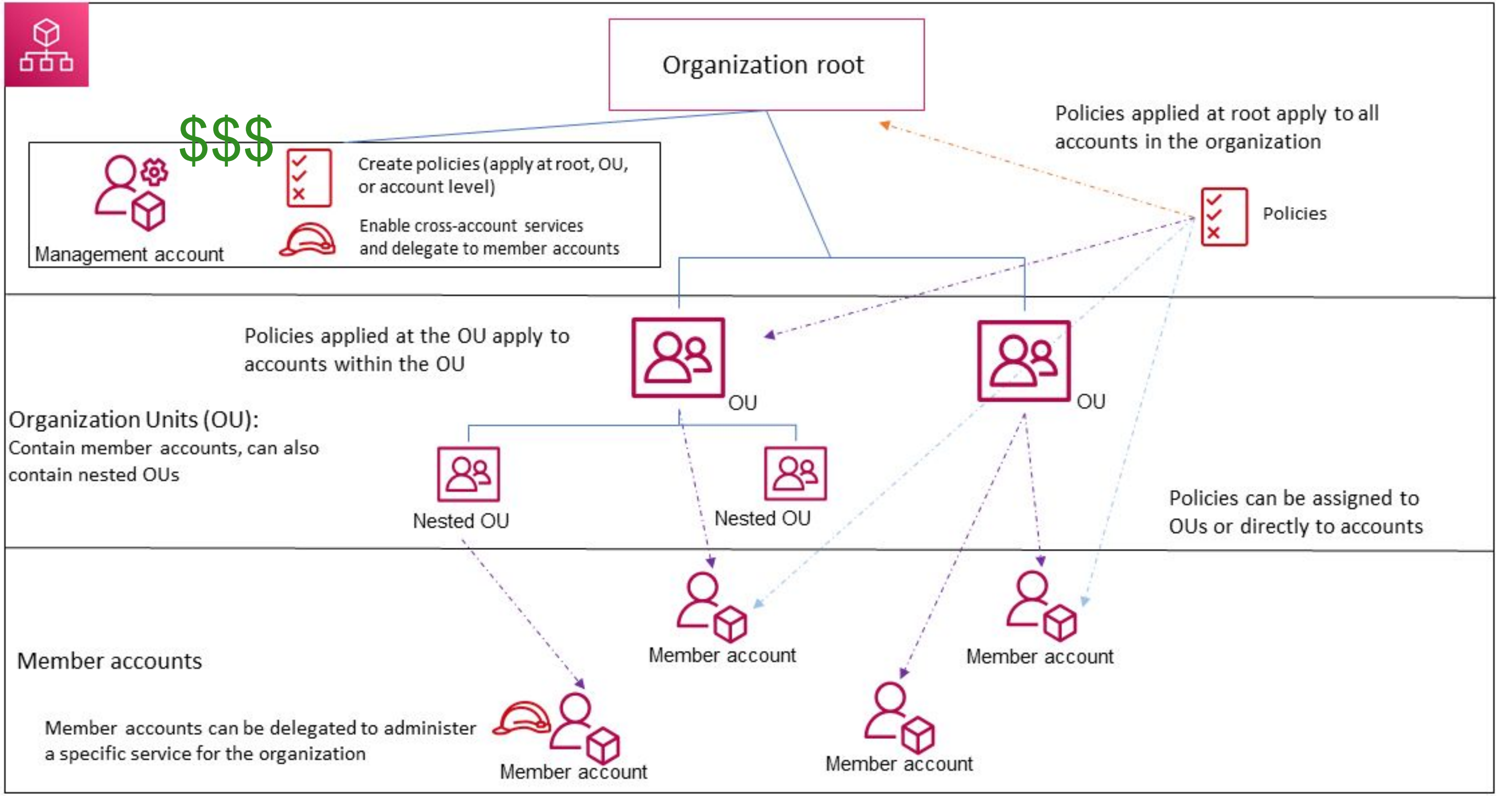
All of these have the concept of “an Organization”.

AWS Organization is mostly a collection of accounts with some bolted on management



GCP Resource Hierarchy


Azure
Active Directory
Root management group
Root policies
Management Groups
Product management group
Corporate management group
Corp policies
Subscriptions
Azure
Dev subscription
Dev subscription policies
Prod subscription
Prod subscription policies
Monitor subscription
Marketing subscription
Company Ops subscription
Resource Groups
Dev group
Resource group
East US Resource Group
North Europe Resource Group
Ops group
Resource group
Resource group
Resources
VM
Virtual Machine
Virtual Machine
kubernetes
kubernetes
App Service



Organization root
$$$
Create policies (apply at root, OU, or account level)
Enable cross-account services and delegate to member accounts
Management account
Policies applied at root apply to all accounts in the organization
Policies
Policies applied at the OU apply to accounts within the OU
OU
OU
Organization Units (OU):
Contain member accounts, can also contain nested OUs
Nested OU
Nested OU
Policies can be assigned to OUs or directly to accounts
Member account
Member account
Member accounts
Member accounts can be delegated to administer a specific service for the organization
Member account
Member account

Identity - For Humans

GCP: Google Workspace Users or Cloud Identity

AWS: Users, Roles - external identity sources

Azure: ~~Azure AD~~ Entra ID Users

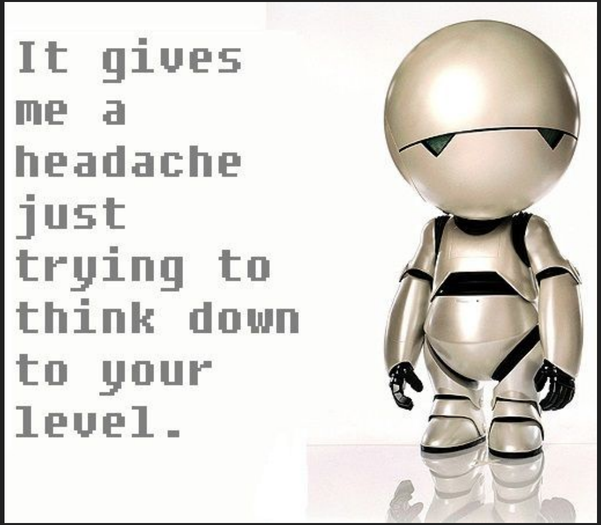
“two cozy bears in a midnight blizzard” (DALL-E 2)

Identity - For non-Humans

AWS: Users, Roles, Service Principals

Azure: Service Principals

GCP: Service Accounts


It gives me a headache just trying to think down to your level.

Consumer Identities

Google -> GMail

Microsoft -> MCA - Microsoft Consumer Accounts

Xbox, Minecraft, etc.

AWS Underpants accounts

Telemetry - AWS CloudTrail

```
{
  "awsRegion": "us-east-1",
  "eventName": "CreateBucket",
  "eventSource": "s3.amazonaws.com",
  "eventType": "AwsApiCall",
  "requestParameters": { ... },
  "sourceIPAddress": "192.168.357.420",
  "userIdentity": {
    "accessKeyId": "ASIATFNORDFNORDAZQ",
    "accountId": "123456789012",
    "arn": "arn:aws:sts::123456789012:assumed-role/rolename/email@company.com",
    "type": "AssumedRole"
}
```

Telemetry - AWS CloudTrail

```
{
  "awsRegion": "us-east-1",
  "eventName": "CreateBucket",
  "eventSource": "s3.amazonaws.com",
  "eventType": "AwsApiCall",
  "requestParameters": { ... },
  "sourceIPAddress": "192.168.357.420",
  "userIdentity": {
    "accessKeyId": "ASIATFNORDFNORDAZQ",
    "accountId": "123456789012",
    "arn": "arn:aws:sts::123456789012:assumed-role/rolename/email@company.com",
    "type": "AssumedRole"
}
```

CreateBucket is the action

S3 is the Service

Where the call came from

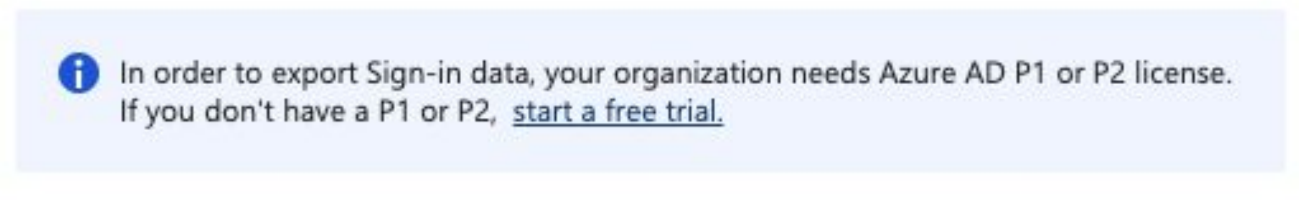
Who Did it?

Type of Identity

Telemetry - Azure

Azure Monitor

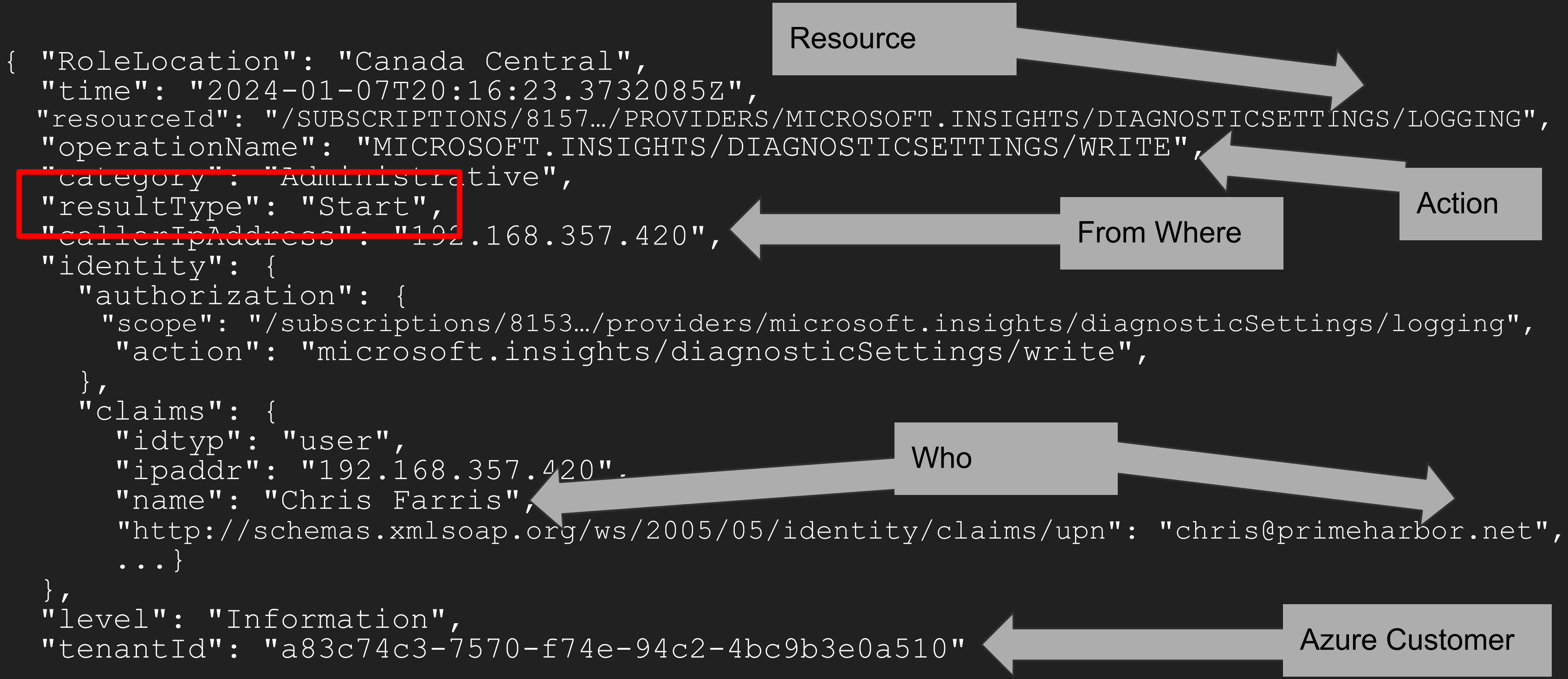
- Per Subscription (automate with blueprints)
- Must setup Azure AD separate, but….



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.

In what I can only assume is a request from Cozy Bear, Azure doesn’t actually log read only events

Telemetry - Azure



```
{ "RoleLocation": "Canada Central",
  "time": "2024-01-07T20:16:23.3732085Z",
  "resourceId": "/SUBSCRIPTIONS/8157…/PROVIDERS/MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/LOGGING",
  "operationName": "MICROSOFT.INSIGHTS/DIAGNOSTICSETTINGS/WRITE",
  "category": "Administrative",
  "resultType": "Start",
  "callerIpAddress": "192.168.357.420",
  "identity": {
    "authorization": {
      "scope": "/subscriptions/8153…/providers/microsoft.insights/diagnosticSettings/logging",
       "action": "microsoft.insights/diagnosticSettings/write",
    },
    "claims": {
       "idtyp": "user",
       "ipaddr": "192.168.357.420",
       "name": "Chris Farris",
       "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "chris@primeharbor.net",
       ...}
  },
  "level": "Information",
  "tenantId": "a83c74c3-7570-f74e-94c2-4bc9b3e0a510"
```

Resource

Action

From Where

Who

Azure Customer

Telemetry - GCP

```
{
  "protoPayload": {
    "logName": "projects/logging-xx[illegible]ogs/cloudaudit.googleapis.com%2Factivity",
    "authenticationInfo": {
      "principalEmail": "chris@room17.com"
    },
    "methodName": "google.iam.admin.v1.CreateServiceAccount",
    "request": {...},
    "requestMetadata": {
      "callerIp": "192.168.357.420",
      "callerSuppliedUserAgent": "Mozilla/5.0 ..."
    },
    "resourceName": "projects/workspace-svc-accounts",
    "response": {...},
    "serviceName": "iam.googleapis.com"
  },
  "resource": {
    "labels": {
      "email_id": "deleteme@workspace-svc-accounts.iam.gserviceaccount.com",
      "project_id": "workspace-svc-accounts"
    },
    "type": "service_account"
  },
  "severity": "NOTICE",
  "timestamp": "2023-12-26T12:17:48.197431961Z"
}
```

Activity is a change event

chris@room17 is the actor

CreateServiceAccount is the action

Connection Details

Service Account Created

Project Name

APIs

Google

- You have to opt-in to every API
- Constantly changing versions

Azure

- Graph API vs Resource API
- Lots more Powershell
- Lots of SDKs

IaC - Infrastructure as Code

AWS

- CloudFormation
- Terraform

GCP

- Terraform

Azure

- ARM Templates
- Terraform (five of them)
- Blueprints

CSPM is not a silver bullet

Cloud Security Posture Monitoring (or Management)

Finds (and maybe fixes) the misconfigurations

Doesn’t solve the “are you using this cloud right?” problem.

AWS Service Control Policies

- Part of AWS Organizations
- Intended to deny the “security invariants”
- IAM Policies that apply to an entire AWS account
- Applied at the OU or Account level

```
{
 "Statement": [
   {
     "Sid": "DenyRootUsage",
     "Effect": "Deny",
     "Action": "*",
     "Resource": "*",
     "Condition": {
       "StringLike": {
         "aws:PrincipalArn": [
           "arn:aws:iam::*:root"
         ]
       }
     }
   }
```

GCP Organization Policies

Used to constrain behavior

Applied at the organization root or folder

```
name:
organizations/ORGID/policies/iam.disableServiceAccountCreation
spec:
  rules:
  - enforce: true
```

Azure Blueprints & Policy

Blueprints -

- define the environment in the subscription
- Can be attached and enforced on management groups

Policy

- Like the other clouds
- Supports an Audit in addition to a Deny action

Multi-Cloud Governance

What is “Cloud Governance” anyway?

1. Cost management
2. Security Baseline
3. Identity Baseline
4. Resource Consistency
5. Operational Excellence
    a. Change Management
    b. Deployment Acceleration

Minimal Viable Cloud Governance Strategy

- Right to Use
- Manage Tenancy
- Manage Identity
- Manage Connectivity
- Audit & CSPM

Right To Use

Who needs to approve the use of the non-primary cloud provider?

- Security
- Finance
- Enterprise Architecture?
- Procurement/Legal/Risk Management?

Managing Tenancy & Identity

- Reduces shadow IT
- Ensure that access follows standard processes
  - Access requests & reviews
  - Joiners/Movers/Leavers are handled properly
- The cloud and security teams know where resources are
- Audit Logging for the cloud API is captured and monitored

Managing Connectivity

***Objective*:**

Provide a secure path for accessing private resources in non-preferred cloud

***Alternative*:**

Lots of things with public IP addresses so your builders can get to them

Audit & CSPM

1. Do something with your audit logs - SIEM, lake, etc
2. Get some CSPM
    a. They probably know the most common misconfigurations

Warning: they may not know the the misconfigurations for the new services that drove your builders to the alternate cloud.

Minimal Viable Cloud Governance Strategy - AWS

- AWS Organizations
- AWS SSO tied to standard identity store
  - Avoid AWS IAM Users
- CloudTrail to SIEM
- 1 account per product/application
- Sandbox account
  - Leverage Budgets & AWS Nuke
- Set the alternate contacts for all accounts

Minimal Viable Cloud Governance Strategy - Azure

- Setup an AzureAD Tenant
- Enable and use Management Groups
- Monitor Service Principals
- Leverage ea.azure.com to ensure all subscriptions are monitored.

Minimal Viable Cloud Governance Strategy - GCP

- Setup a Google Domain
  - Secure your Google Domain & SuperAdmins
- Enable Cloud Identity tied to corp identity provider
  - Or Google Workspace if you have Google Docs usage
- Create a GCP Organization
- Create Project folder structure
- Avoid use of *IAM Basic Roles* for services.
- Set the Essential Contacts for all projects

Google - Managing the unmanaged

Google offers the Transfer tool for unmanaged users

1. List the users that already have consumer accounts
2. Reach out to them directly and let them know they will get an email from google
3. Send them the transfer request
4. Wait/rinse/repeat
5. Finally - rename the accounts that didn’t accept or are no longer with your org

Takeaways

Create your Cloud Governance Strategies

1. Define a full strategy for your primary cloud
    a. Security Baseline
    b. FinOps Team & Enterprise discounting
    c. Centralized Deployment & “Paved Roads”
    d. Invest here
2. Define exception process for alternate clouds
    a. Who has authority to decide?
    b. How will cost allocation work?
    c. How will owners be held accountable?

Create your Cloud Governance Strategies

3. Establish basic governance for alternate clouds
    a. Create the official tenancy container
    b. Establish centralized human identities
    c. Capture cloud-plane audit logs
    d. Deploy CSPM
4. Go out and find the shadow-clouds that already exist
    a. Email Subject search
    b. P-Card & Procurement search
    c. Outreach to the builders in your organization

DEVELOPERS
FIND A WAY
imgflip.com

QUESTIONS?

@jcfarris

https://github.com/jchrisfarris

https://www.linkedin.com/in/jcfarris

http://www.chrisfarris.com

https://pht.us/hackcon2024

https://pht.us/multicloudgov

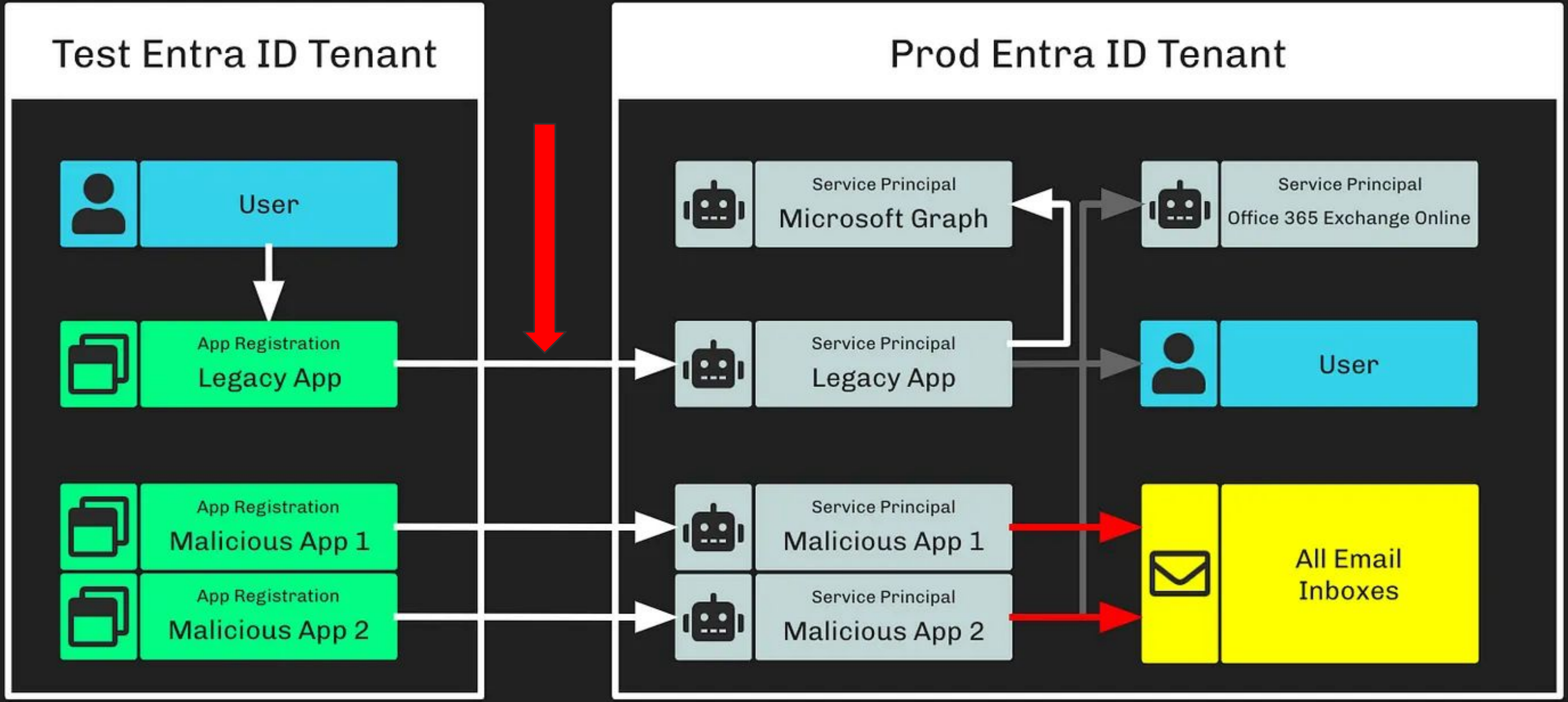


Diagram courtesy SpectorOps