# Zero to Logging, In 50 Minutes

BSidesOK, April 12th 2019

# @sdanelson

- Technology enthusiast
- Security professional
- Well traveled homebody
- Football (Soccer) fan
- Entrepreneur ( www.pinpointsecurity.io )

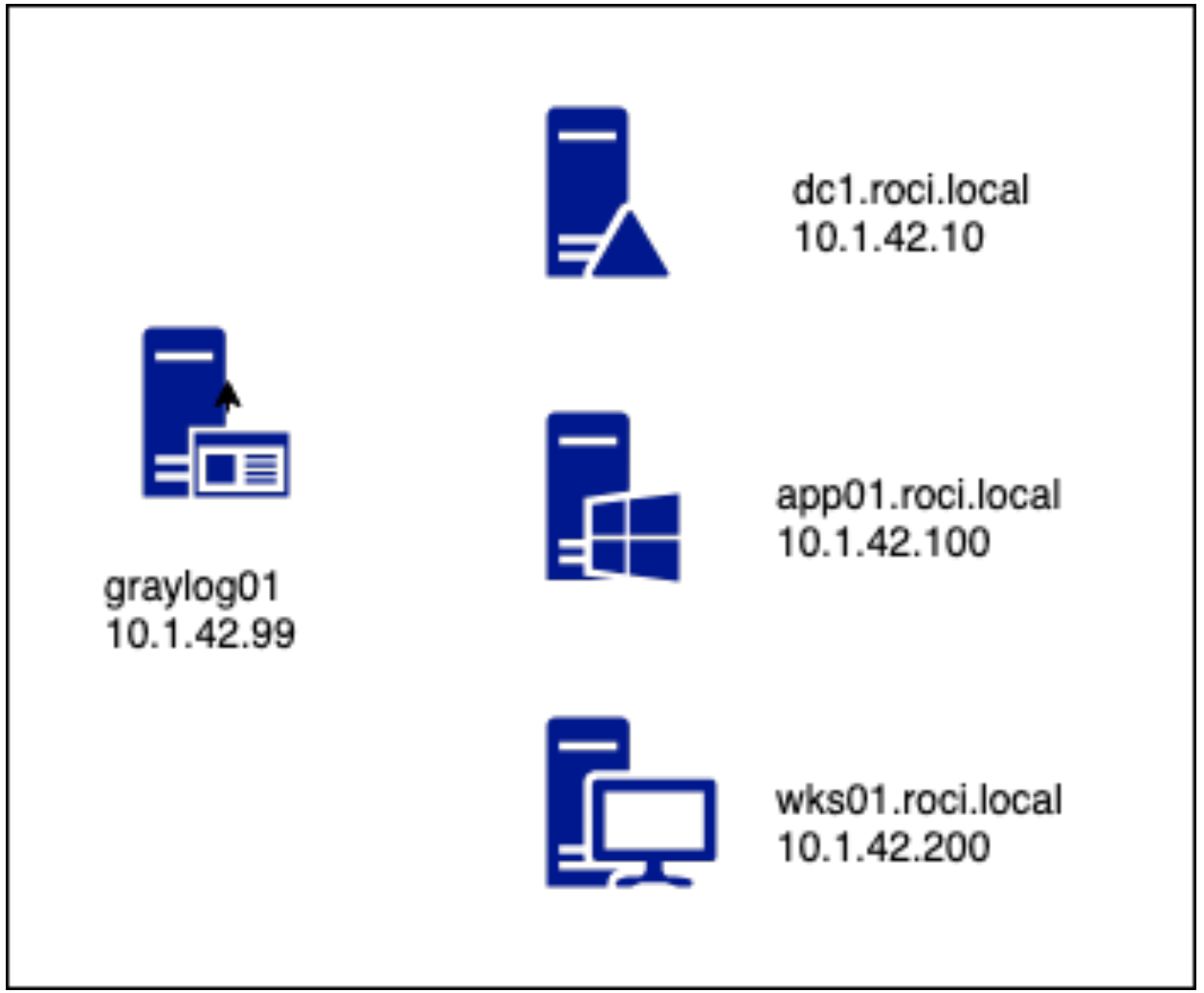
# What this talk will not be about

- Bashing SIEM providers
- Debating keeping all the logs forever
- Comparing SIEM’s
- Arguing about wasted time
- Trying to justify big $$$

# What this talk will be about

- A practical example of how to get
  - Active Directory Domain Logs
  - Windows Server Logs
  - Windows Client Logs
  - Application Logs
  - Cloud Logs
- Quickly into a centralized logging tool on the cheap
- And alert off of actionable events

# The demo environment



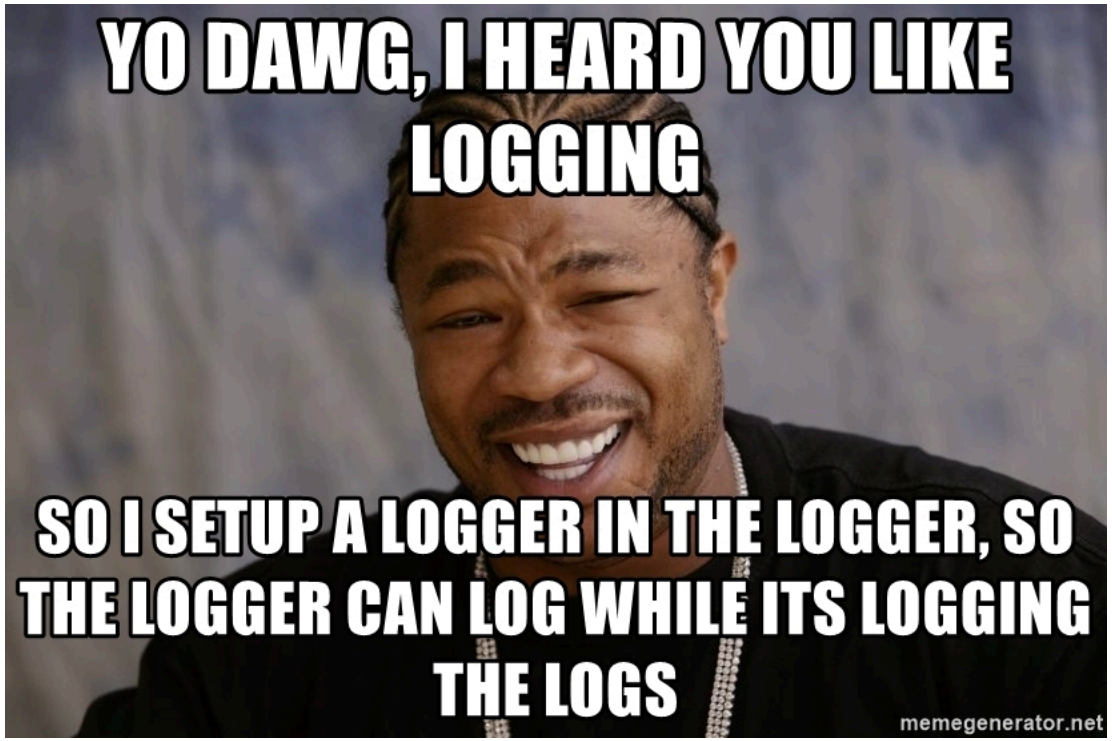
# Stand up Graylog

- Download Graylog ova
- Import into your vm host of choice
- Go through the setup

# Windows Server Logs

- Create Beats Input
- Generate Sidecar token
- Install Sidecar
- Configure Sidecar as a service
- Alert

# More logs


YO DAWG, I HEARD YOU LIKE LOGGING
SO I SETUP A LOGGER IN THE LOGGER, SO THE LOGGER CAN LOG WHILE ITS LOGGING THE LOGS
memegenerator.net

# AD Logs

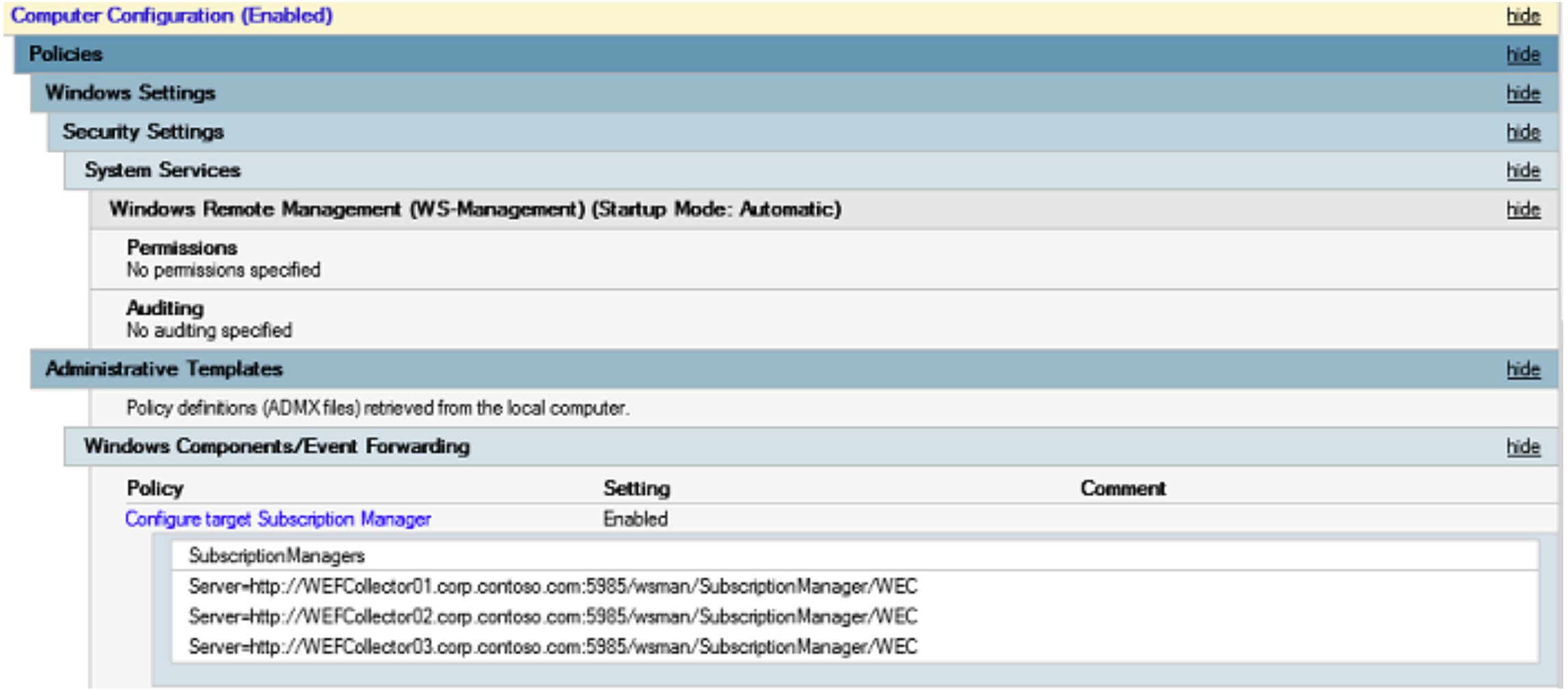
- Setup WEF on app01.roci.local
- Permissions on dc01
- Update collector config to include Forwarded Events
- Ingest

# Did someone say 80 logs?

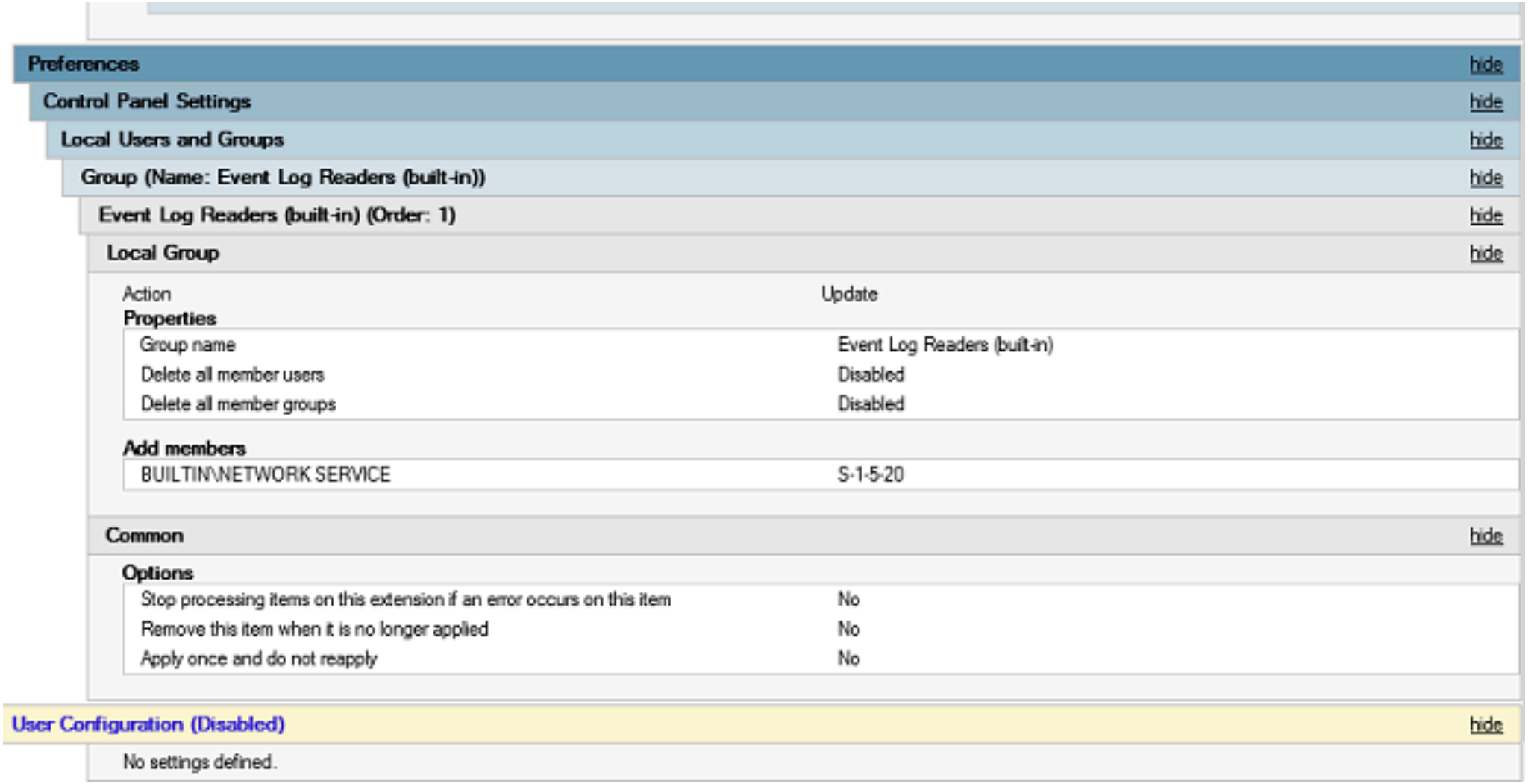
# Windows Client

- WEF?
- Lazy
- Group Policy
- Drop machine in GP to forward logs using WEF to app01
- @jepayneMSFT

# GPO


Computer Configuration (Enabled)
hide
Policies
hide
Windows Settings
hide
Security Settings
hide
System Services
hide
Windows Remote Management (WS-Management) (Startup Mode: Automatic)
hide
Permissions
No permissions specified
Auditing
No auditing specified
Administrative Templates
hide
Policy definitions (ADMX files) retrieved from the local computer.
Windows Components/Event Forwarding
hide
Policy
Setting
Comment
Configure target Subscription Manager
Enabled
SubscriptionManagers
Server=http://WEFCollector01.corp.contoso.com:5985/wsman/SubscriptionManager/WEC
Server=http://WEFCollector02.corp.contoso.com:5985/wsman/SubscriptionManager/WEC
Server=http://WEFCollector03.corp.contoso.com:5985/wsman/SubscriptionManager/WEC

# GPO Continued



# Baseline WEF subscription

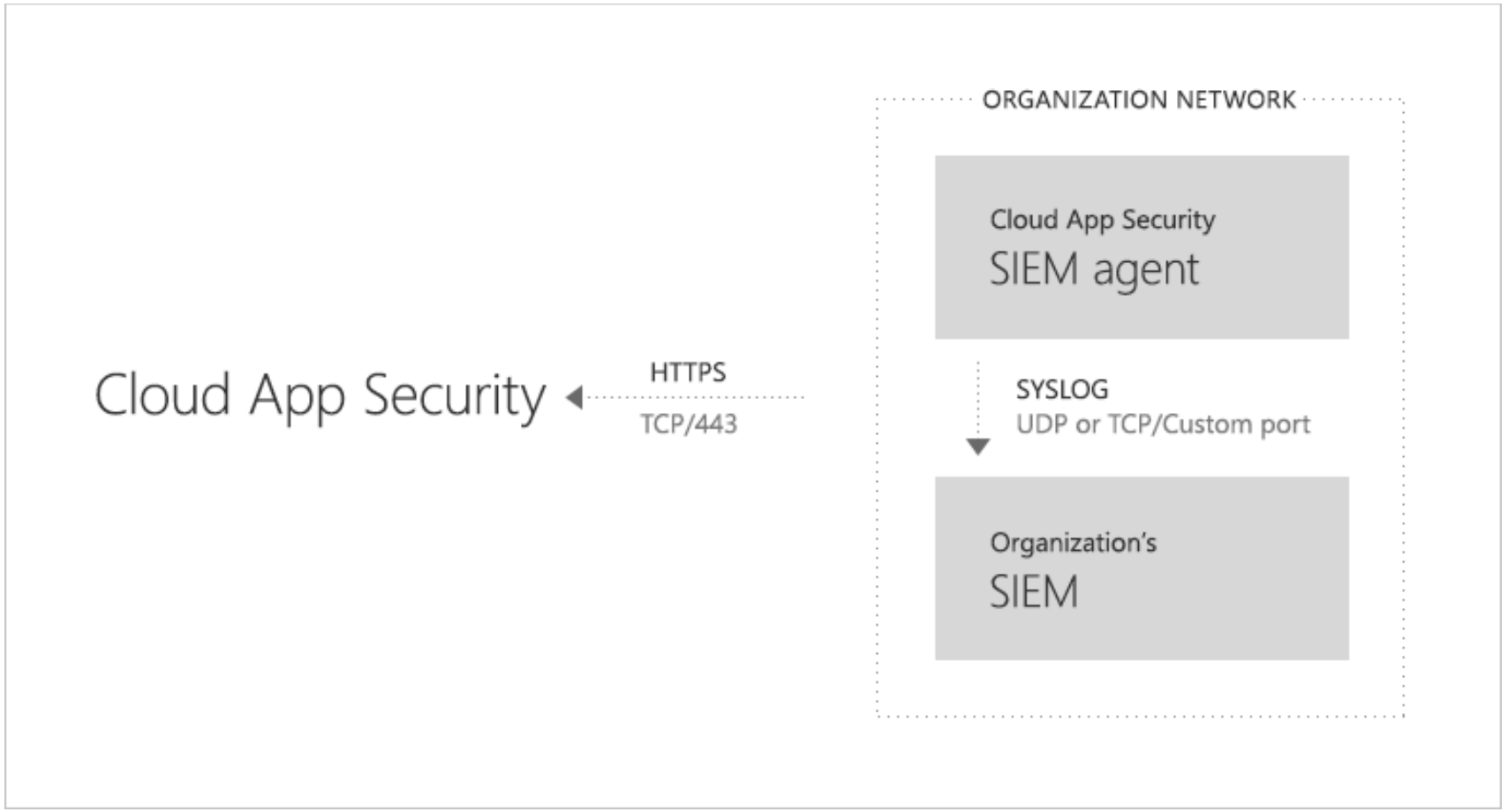
```
</Query>
<Query Id="26" Path="Security">
  <!-- Special Privileges (Admin-equivalent Access) assigned to new logon, excluding
  <Select Path="Security">*[System[(EventID=4672)]]</Select>
  <Suppress Path="Security">*[EventData[Data[1]="S-1-5-18"]]</Suppress>
</Query>
<Query Id="27" Path="Security">
  <!-- New user added to local security group-->
  <Select Path="Security">*[System[(EventID=4732)]]</Select>
</Query>
<Query Id="28" Path="Security">
  <!-- New user added to global security group-->
  <Select Path="Security">*[System[(EventID=4728)]]</Select>
</Query>
<Query Id="29" Path="Security">
  <!-- New user added to universal security group-->
  <Select Path="Security">*[System[(EventID=4756)]]</Select>
</Query>
<Query Id="30" Path="Security">
  <!-- User removed from local Administrators group-->
  <Select Path="Security">*[System[(EventID=4733)]] and (*[EventData[Data[@Name="Targ
</Query>
<Query Id="31" Path="Microsoft-Windows-TerminalServices-RDPClient/Operational">
  <!-- Log attempted TS connect to remote server -->
  <Select Path="Microsoft-Windows-TerminalServices-RDPClient/Operational">*[System[(E
</Query>
```

# Someone said windows client

# Cloud Logs

- O365
- Azure
- AWS

# O365 CAS Logs



# O365 Logs

## Running the script:

- Retrieve all logs and send to a network socket / Graylog server: `python3 AuditLogCollector.py 'tenant_id' 'client_key' 'secret_key' --exchange --dlp --azure_ad --general --sharepoint -p 'random_publisher_id' -g -gA 10.10.10.1 -gP 6000`

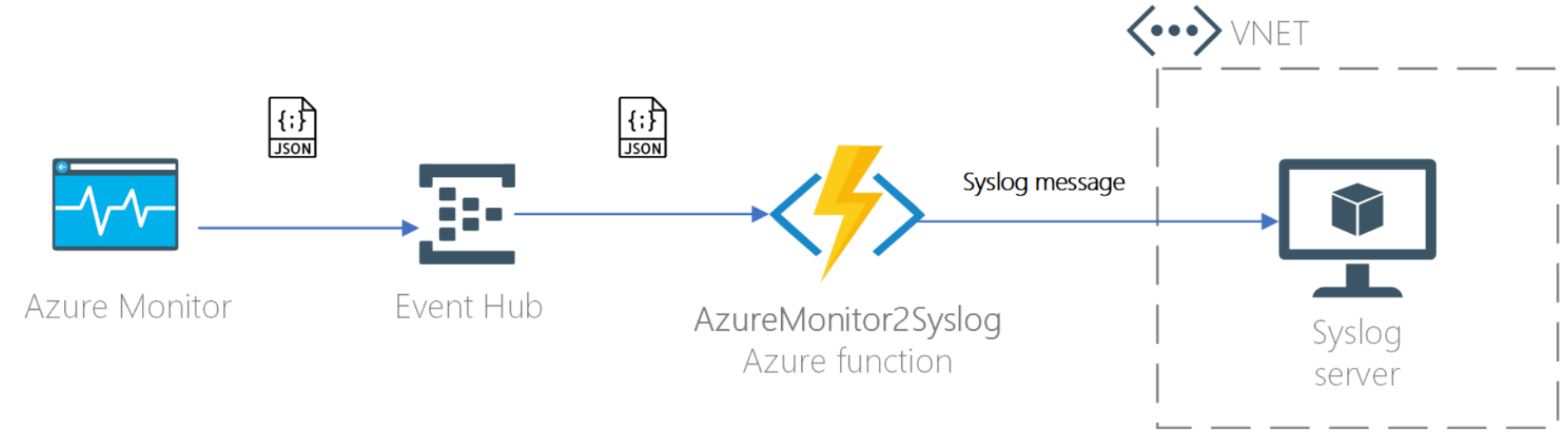
## Script options:

```
usage: AuditLogCollector.py [-h] [--general] [--exchange] [--azure_ad]
                            [--sharepoint] [--dlp] [-p publisher_id]
                            [-l log_path] [-f] [-fP file_output_path] [-g]
                            [-gA graylog_address] [-gP graylog_port]
                            tenant_id client_key secret_key`

positional arguments:
  tenant_id             Tenant ID of Azure AD
  client_key            Client key of Azure application
  secret_key            Secret key generated by Azure application`

optional arguments:
  -h, --help            show this help message and exit
  --general             Retrieve General content
  --exchange            Retrieve Exchange content
  --azure_ad            Retrieve Azure AD content
  --sharepoint          Retrieve SharePoint content
  --dlp                 Retrieve DLP content
  -p publisher_id       Publisher GUID to avoid API throttling
  -l log_path           Path of log file
  -f                    Output to file.
```

# Azure Monitoring Logs



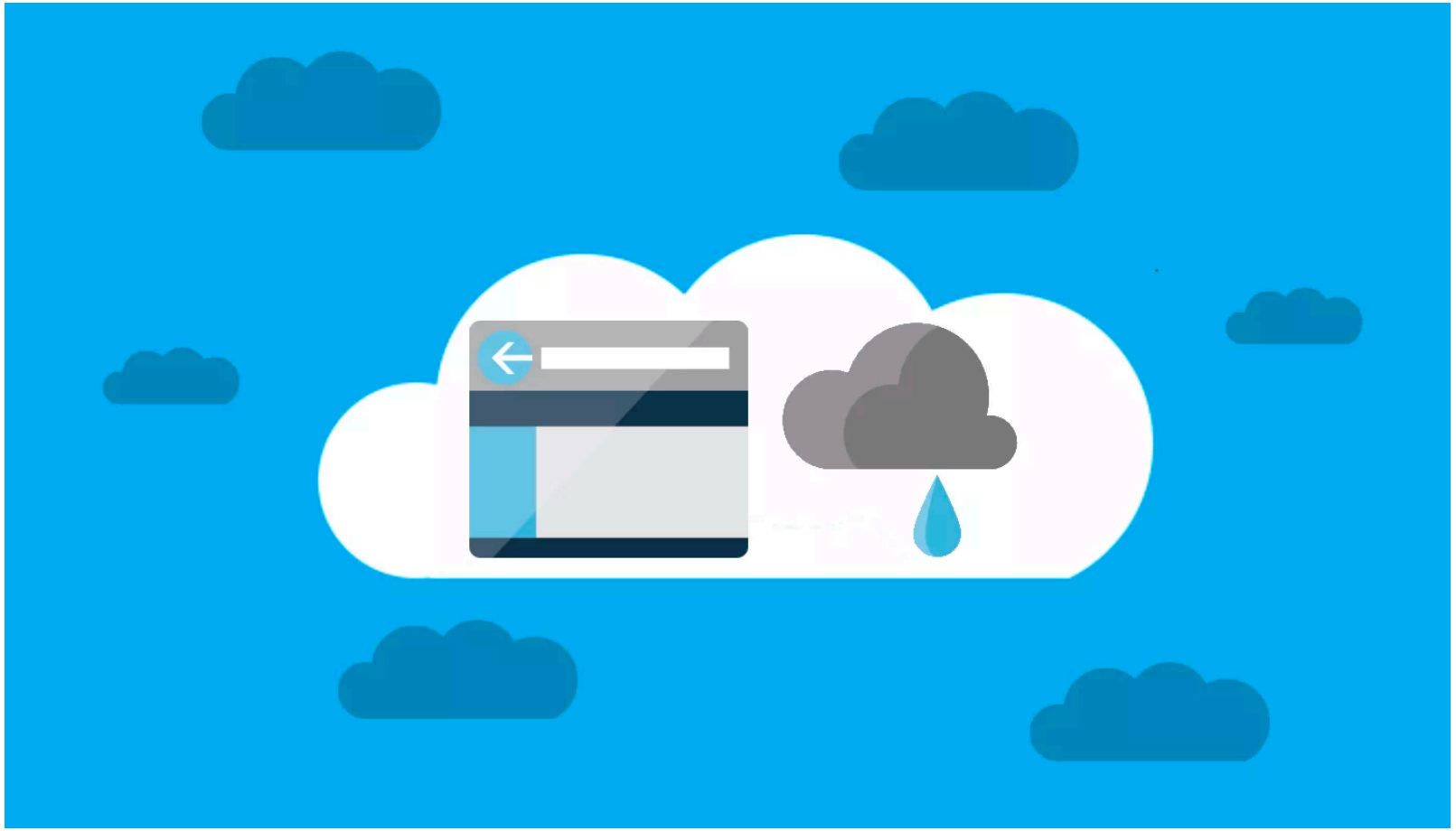

The Azure monitor will send metrics to Event Hub. The Event Hub messages will trigger this Javascript Azure Function that will convert the message to syslog format and send to the correct server.

Note: To send the syslog messages to an internal server in a VNET, configure the Function App with VNET integration.

# AWS

- CloudWatch support is baked into Graylog

# Make it rain



# Questions ? / Resources

- Graylog - https://www.graylog.org/
- Graylog Docs - https://docs.graylog.org/en/3.0/
- Graylog Sidecar - http://docs.graylog.org/en/3.0/pages/sidecar.html
- Windows Event Forwarding for Intrusion Detection - https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
- WEF on a DC - https://www.petri.com/configure-event-log-forwarding-windows-server-2012-r2
- WEF for domain logging - https://www.syspanda.com/index.php/2017/03/01/setting-up-windows-event-forwarder-server-wef-domain-part-13/
- O365 CAS Logging - https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas
- O365 Logging Script for Graylog - https://github.com/ddbnl/office365-audit-log-collector
- Stream Azure monitoring data - https://docs.microsoft.com/en-us/azure/azure-monitor/platform/stream-monitoring-data-event-hubs
- Azure Logging to Syslog - https://github.com/miguelangelopereira/azuremonitor2syslog/

# Next Steps

- Firewall/Flow/DNS/Proxy
- Look at other options
- Go forth and log
- Email me stephen at pinpointsecurity.io
- DM me at @sdanelson
- Slides will be at https://github.com/sdanelson/bsidesok2019