PowerShell Conference Europe 2019

Hannover, Germany

June 4-7, 2019

A Palantir in your Hands!
WEF

Mateusz Czerniawski

5

Video operator, did you start the recording?

4

3

2

1

PowerShell Conference Europe 2019

Hannover, Germany

June 4-7, 2019

A Palantir in your Hands!
WEF

Mateusz Czerniawski

Platinum Sponsor

aws

This Session

After this session you'll be able to:

- Set up
  - custom Windows Event Forwarding environment
  - Azure Log Analytics workspace
- Send specific logs to Azure LA
- Query data using KQL
- Consume data using Azure Dashboards and PowerBI

Agenda

Windows Event Forwarding

- Theory
- Problem and Solution

Find-Events, WEFTools and Azure magic

Demo Time

- Prepare, Deploy, Have Fun

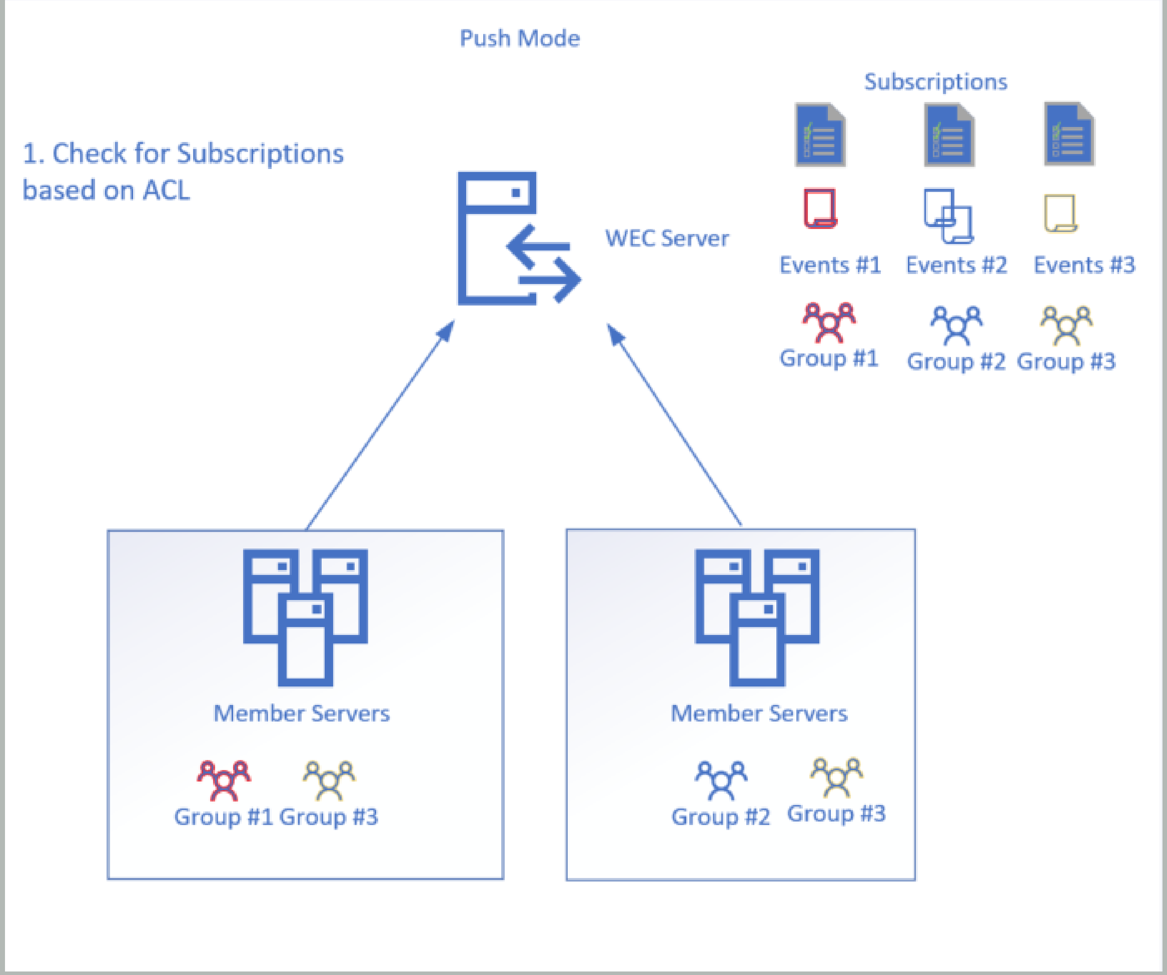
Windows Event Forwarding

Log Forwarding – built in Windows, encrypted using Kerberos

Windows Event Forwarding

Log Forwarding – built in Windows, encrypted using Kerberos

Push

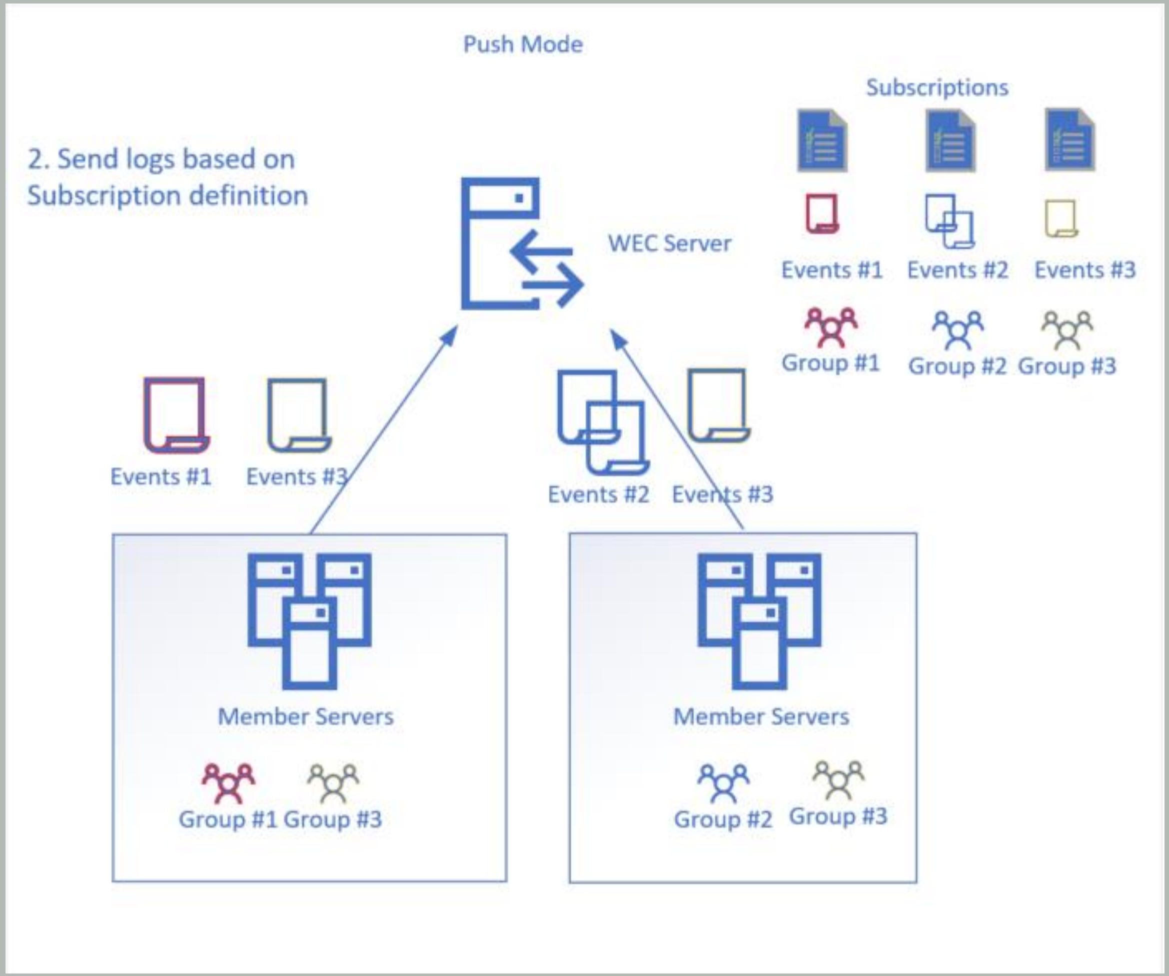


Arcontar

Windows Event Forwarding

Log Forwarding – built in Windows, encrypted using Kerberos

Push

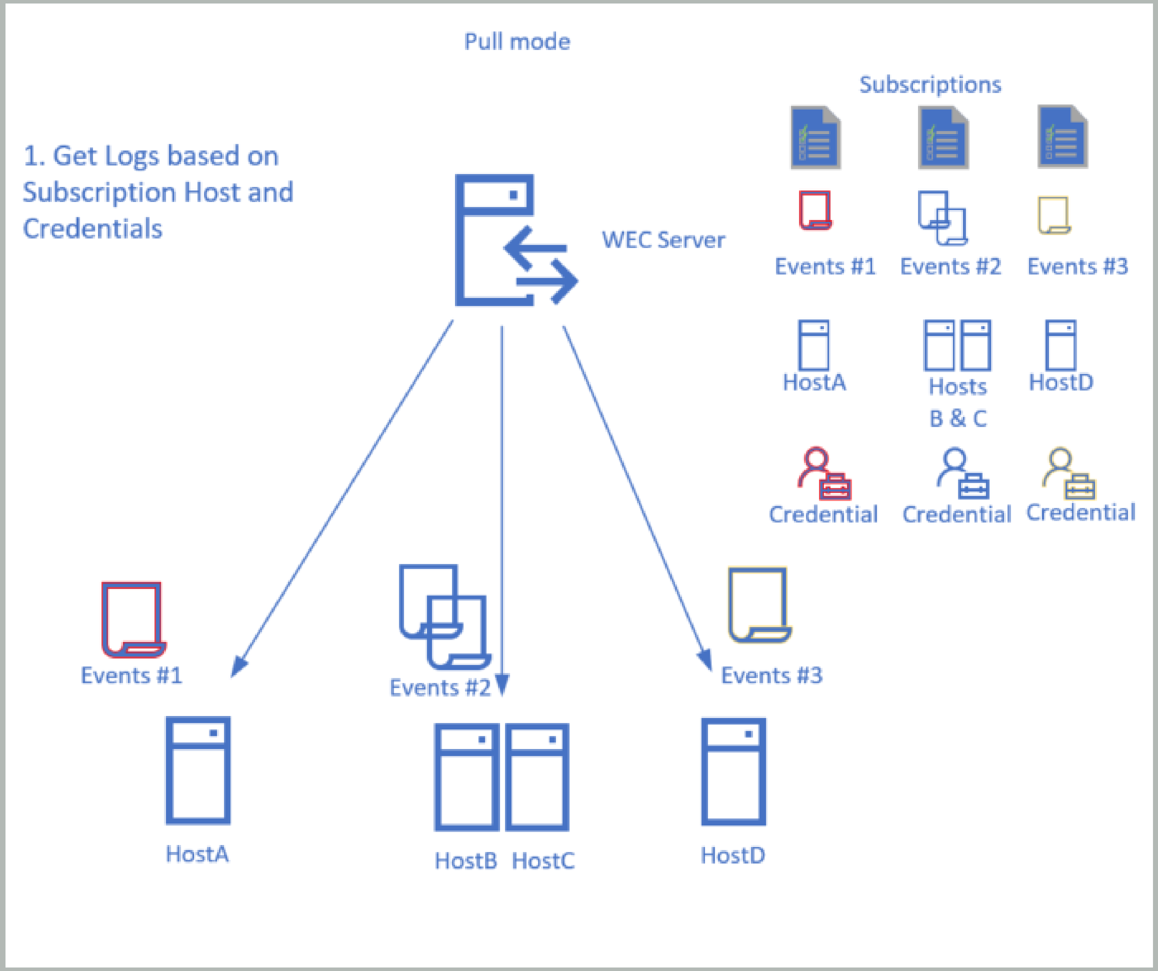


Arcontar

Windows Event Forwarding

Log Forwarding – built in Windows, encrypted using Kerberos

Pull



Arcontar

Windows Event Forwarding

Log Forwarding – built in Windows

Push and Pull

Full docs: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Windows Event Forwarding

- Locked out events forwarded from DCs to a console (manual)

Windows Event Forwarding

- Locked out events forwarded from DCs to a console (manual)

- Jessica's Payne 'Host Based Firewall' to 'WEFFLES'

  https://channel9.msdn.com/Events/Ignite/New-Zealand-2016/M377

  https://channel9.msdn.com/Events/Ignite/Australia-2015/INF327

  https://blogs.technet.microsoft.com/jepayne/2017/12/08/weffles/

- 'Monitoring what matters'

  https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/

Run this within minutes and 'hack your way up'

Windows Event Forwarding

- ELK and winlogbeat – a lot of ⌛
- OMS with agents – a lot of 💰
- OMS with WEC – a lot of ℹ and 💰

Windows Event Forwarding

- Palantir
  - multiple event forwarding rules and logs
  - easily managed – subscriptions and AD groups
  - code-deployable

https://github.com/palantir/windows-event-forwarding

Windows Event Forwarding

- Palantir
  - multiple event forwarding rules and logs
  - easily managed – subscriptions and AD groups
  - code-deployable

  https://github.com/palantir/windows-event-forwarding
- WSLab
  - sample scripts to KKND

  https://github.com/Microsoft/WSLab

Windows Event Forwarding

- Palantir
  - multiple event forwarding rules and logs
  - easily managed – subscriptions and AD groups
  - code-deployable

  https://github.com/palantir/windows-event-forwarding
- WSLab
  - sample scripts to KKND

  https://github.com/Microsoft/WSLab
- LME – Logging Made Easy

  https://github.com/ukncsc/lme
- Sauron

  https://blogs.technet.microsoft.com/russellt/2017/05/09/project-sauron-introduction/

Pros from WEF – by Jessica Payne

- Free,
- built in Windows (Servers AND Desktops)
- Configured via GPO
- Can (and should be) targeted to specific events
- Native evtx (xml) log format
- Uses WinRM (Kerberos) to prevent man in the middle
- “Push” log mode – less attack surface
- IT admins control their own logging destiny

More Pros from Palantir

- Free
- Log file per group of events - Customized Event Channel dll
- Pre-configured xml subscriptions
- Subscriptions targeted by Active Directory groups membership

Some Cons:

- Searching through Event log is slow

- Bigger team = more people with access to logs

- A lot of storage needed == slower searches

- Can be tampered with

Solution

- ~~Searching through Event log is slow –~~
  Find-Events from PSWinReportingV2 (and PSEventViewer)
- Bigger team = more people with access to logs
- A lot of storage needed == slower searches
- Can be tampered with

Solution

- ~~Searching through Event log is slow –~~

    Find-Events from PSWindReportingV2 (and PSEventViewer)

- ~~Bigger team = more people with access to logs~~

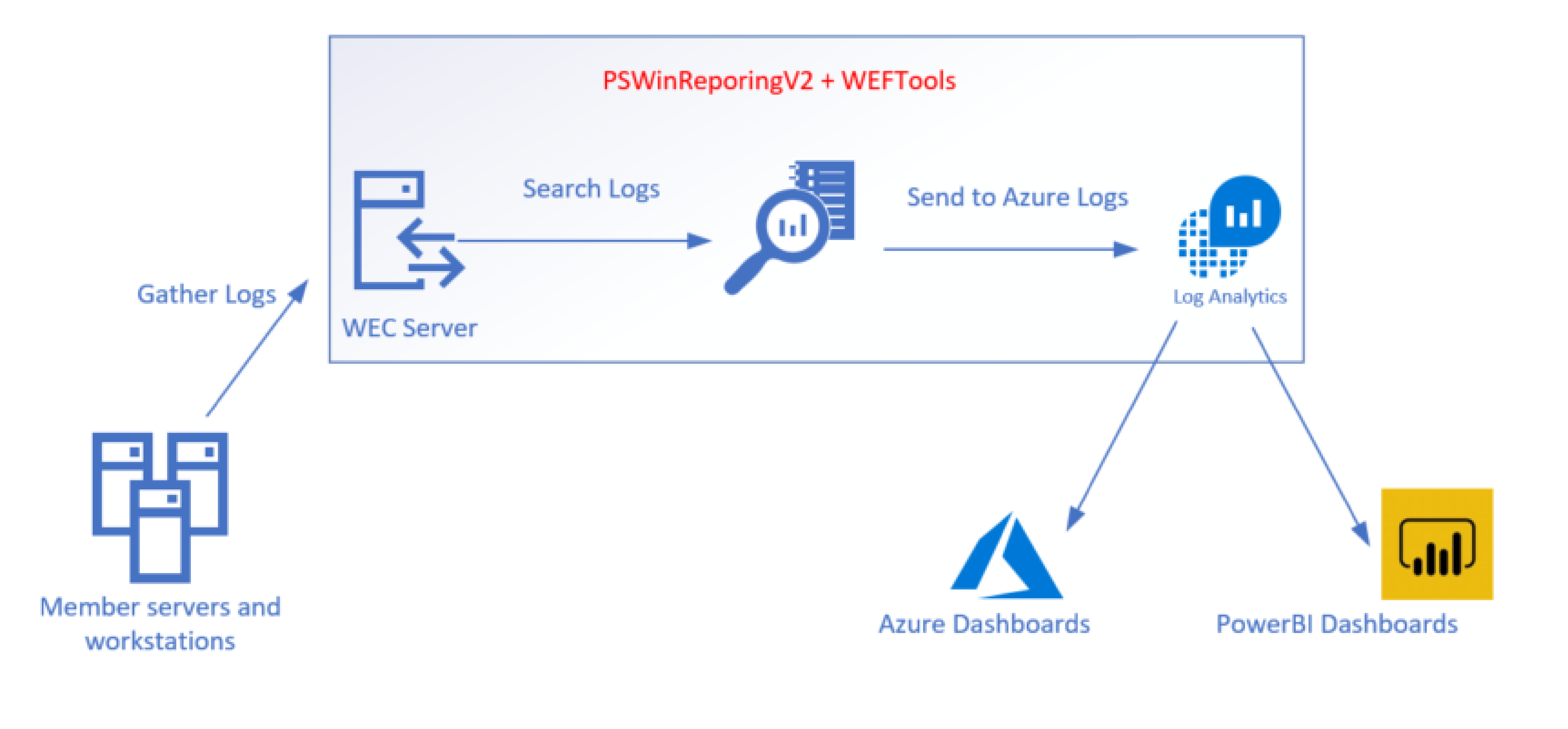
- ~~A lot of storage needed == slower searches~~

- ~~Can be tampered with~~

    WEFTools and Azure Log Analytics + PowerBI

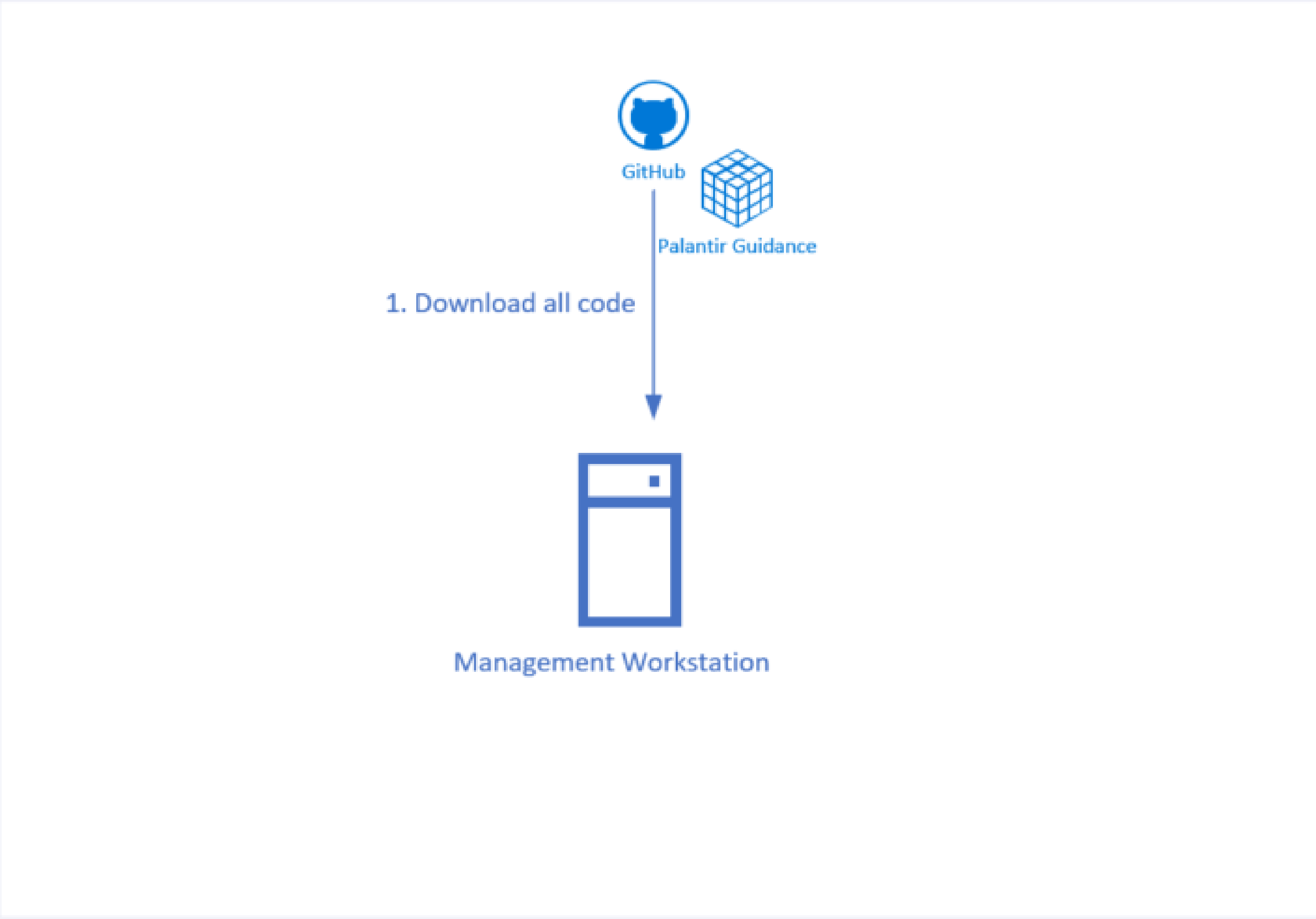
Arcontar

Solution



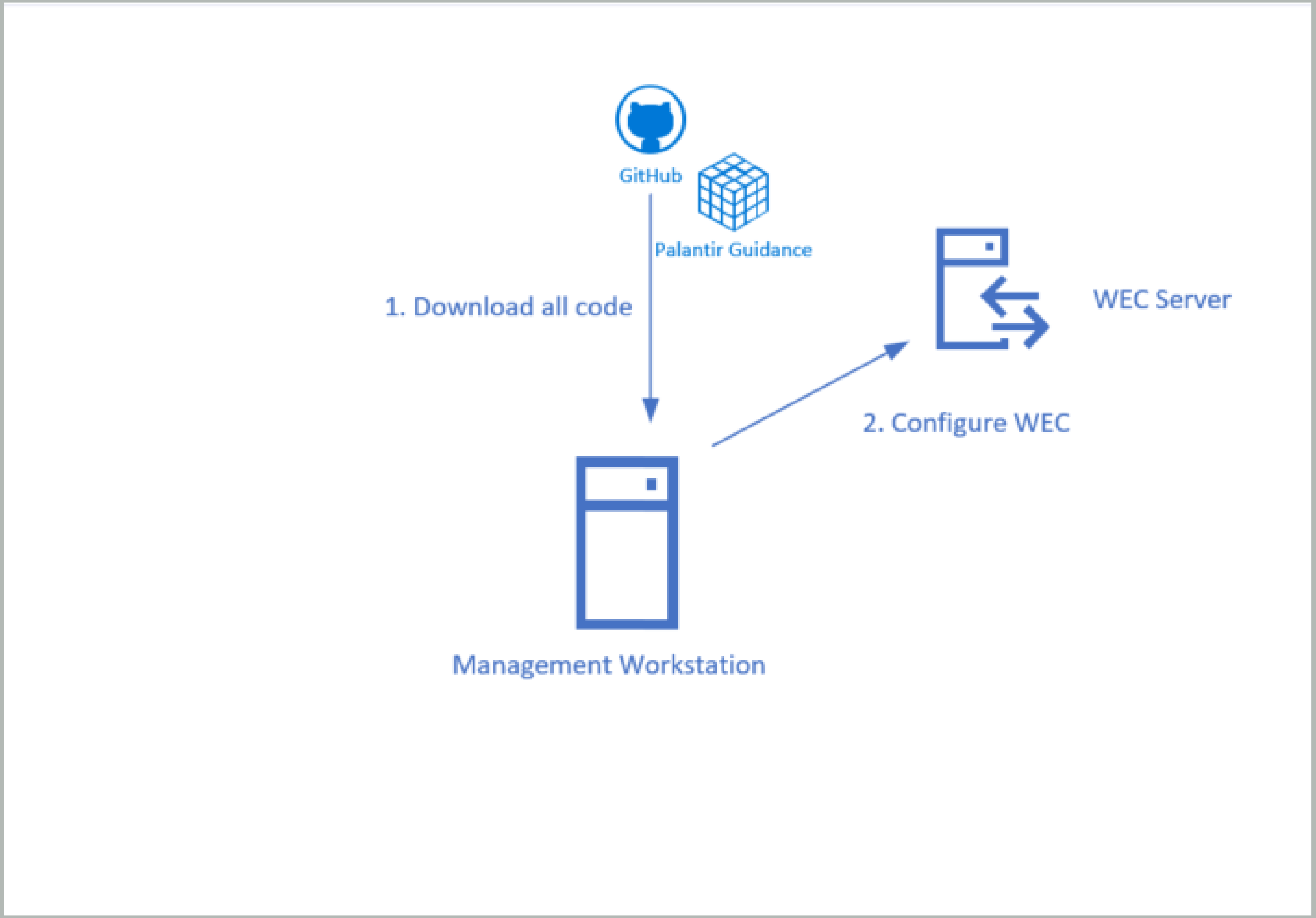
Arcontar

Solution



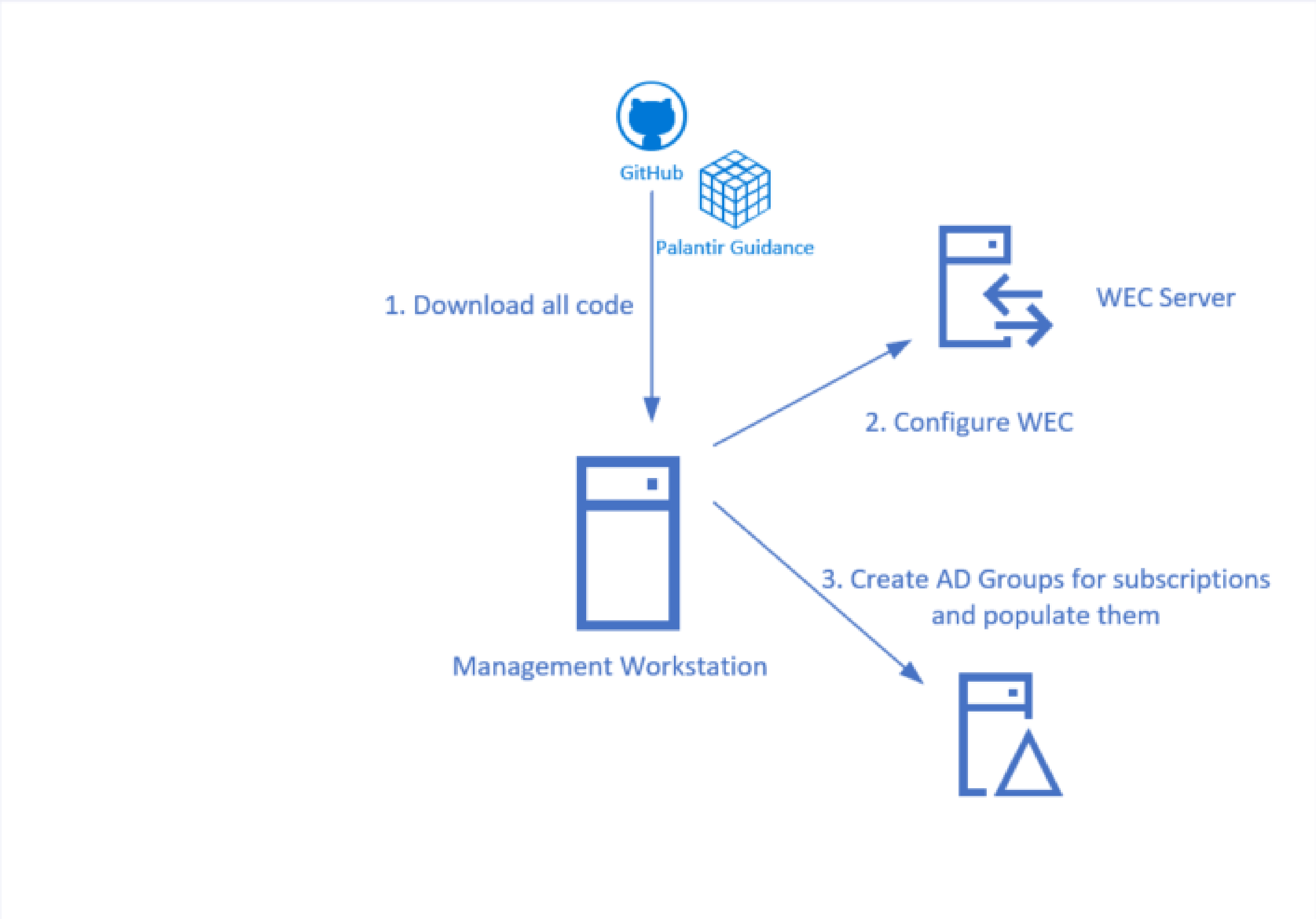
Arcontar

Solution



Arcontar

Solution



GitHub

Palantir Guidance

1. Download all code

WEC Server

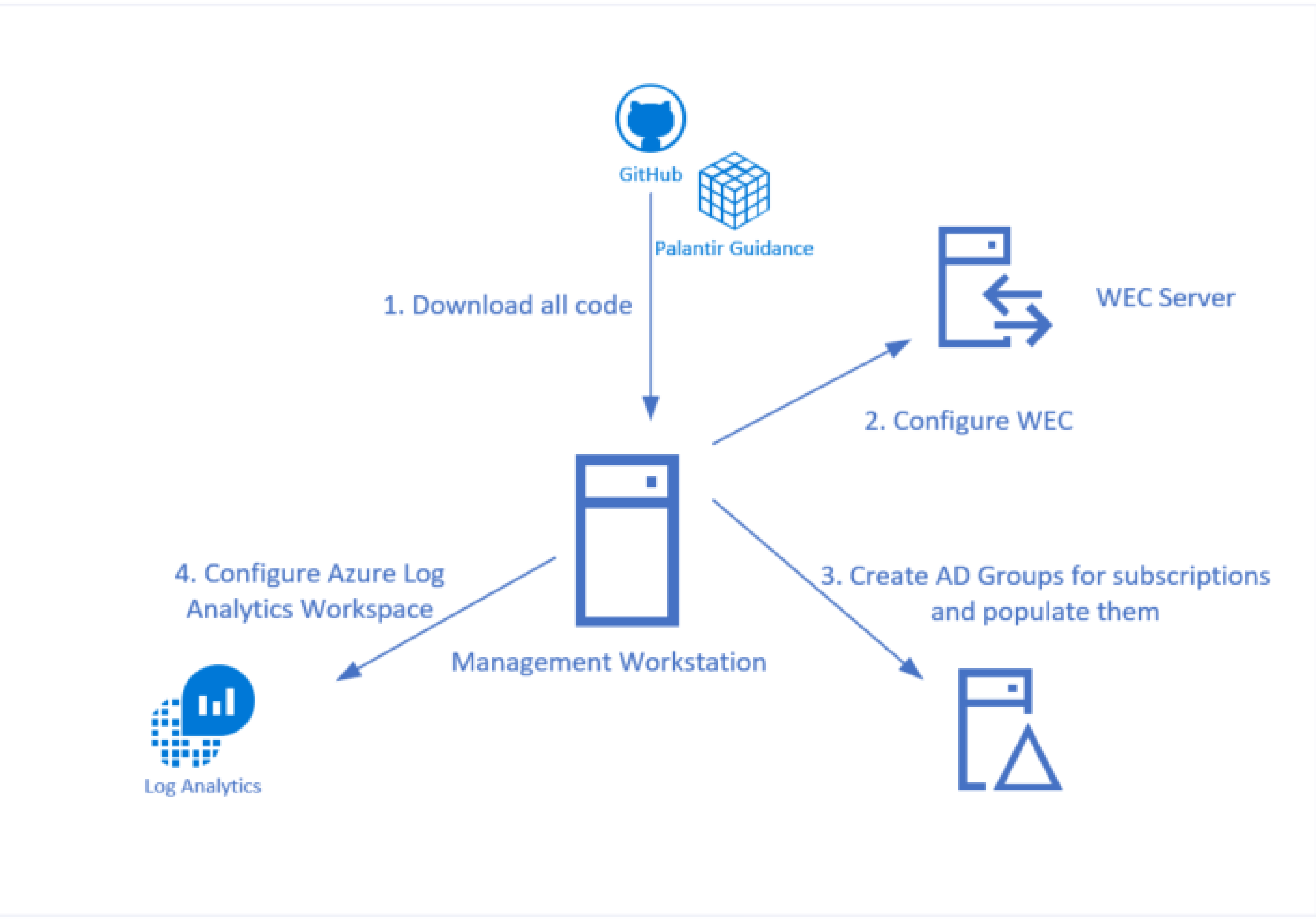
2. Configure WEC

Management Workstation

3. Create AD Groups for subscriptions and populate them

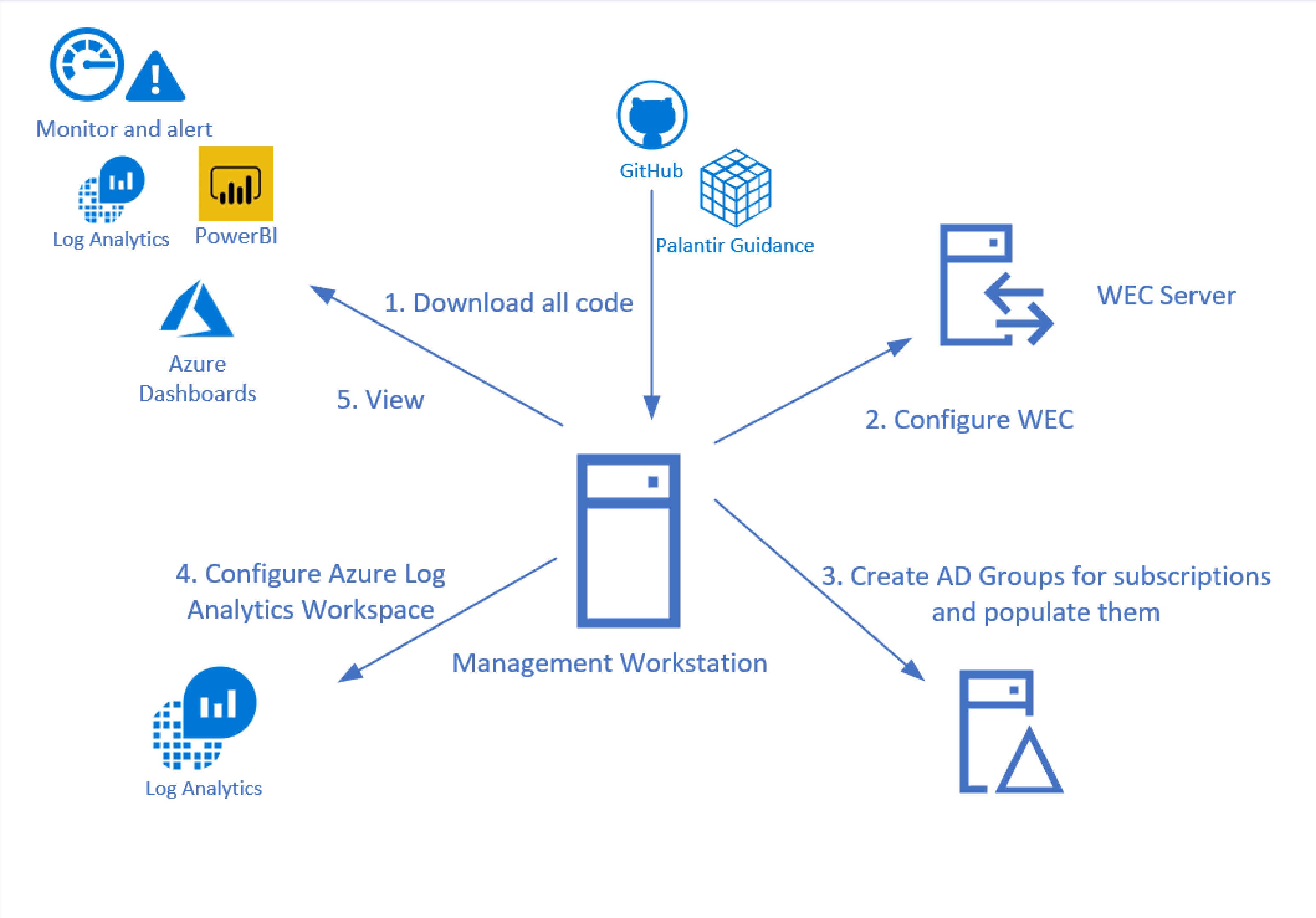
Arcontar

Solution



Arcontar

Solution



Arcontar

DEMO

Let’s have some fun

Fun fact

Demo Lab – built 3 times same error:

- Group Policy set up correctly
- Replication working as expected
- GPUpdate and GPResult showing OK
- auditpol /get /category:* returns 'No Auditing'

Fix?

-Remove audit.csv from:

\\domainname\SYSVOL\domain\Policies\{GPOGUID}\Machine\microsoft\windows nt\Audit

- Configure GPO again!

https://blogs.msdn.microsoft.com/spatdsg/2011/06/06/audit-policy-not-registering-audits/

Summary

- Collect your Events (FREE)

  WEF + Palantir's Guidance

- Deploy and run with PowerShell (FREE)

  WEFTools + Find-Events (PSWinReporting + PSEventViewer)

- Store and Analyze (FREE or dirt cheap)

  Azure Log Analytics, KQL, Azure Dashboards, PowerBI

Slides and demo code

```
Start-Process -FilePath https://github.com/psconfeu/2019
```

Arcontar

Questions?

Use the conference app to vote for this session:
https://my.eventraft.com/psconfeu

Arcontar

about_Speaker

Mateusz Czerniawski

Arcontar

mczerniawski@arcon.net.pl

@Arcontar

www.mczerniawski.pl

mczerniawski