

# **Azure Automation and Security Better together?!**

## Eric Berg



Lead IT-Architekt – Team Azure / Team Modern Workplace



Azure, Datacenter and Modern Workplace



Azure, System Center, Windows Server and Client



[info@ericberg.de](mailto:info@ericberg.de)



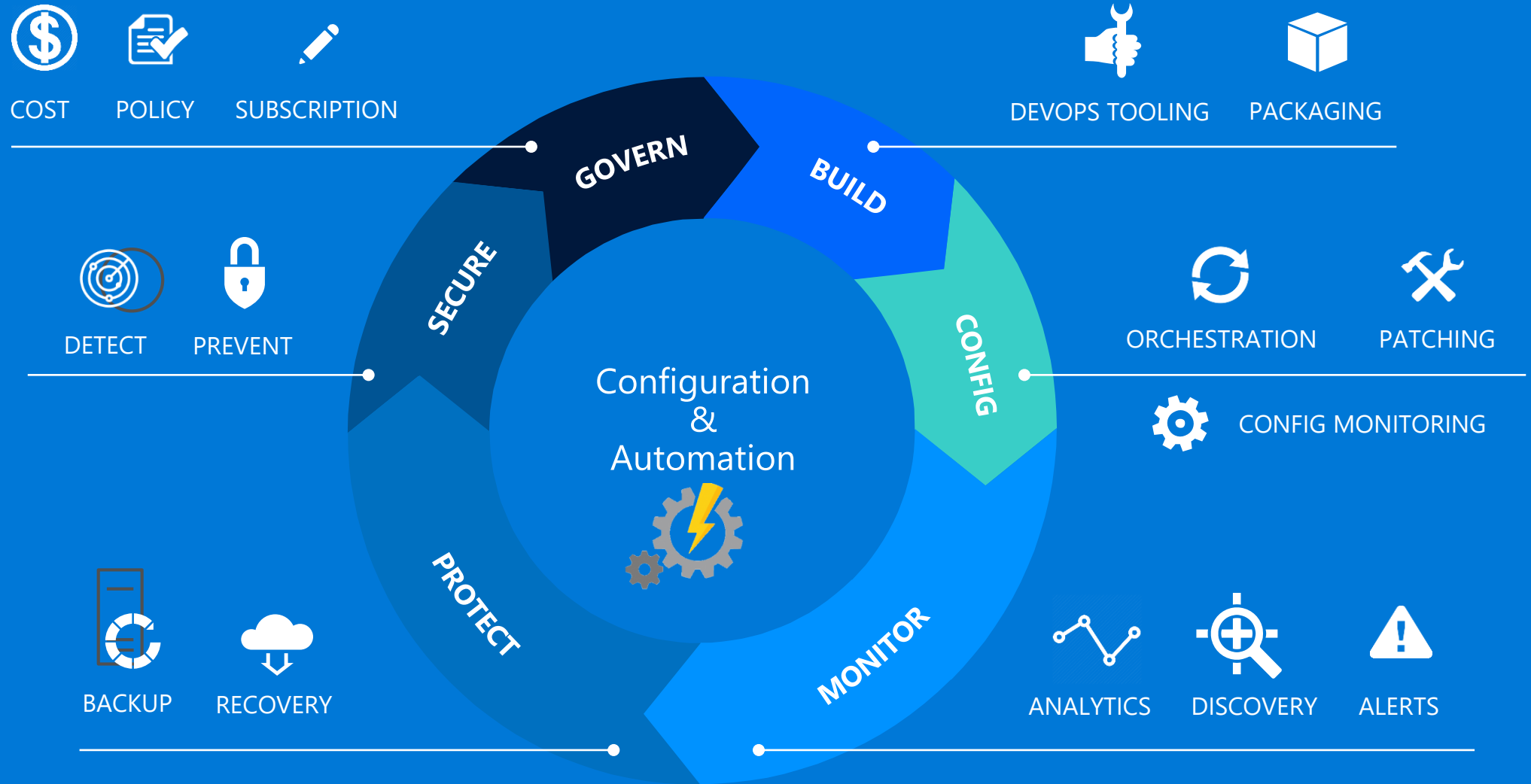
[@ericberg\\_de](https://twitter.com/ericberg_de) | [@GeekZeugs](https://twitter.com/GeekZeugs)



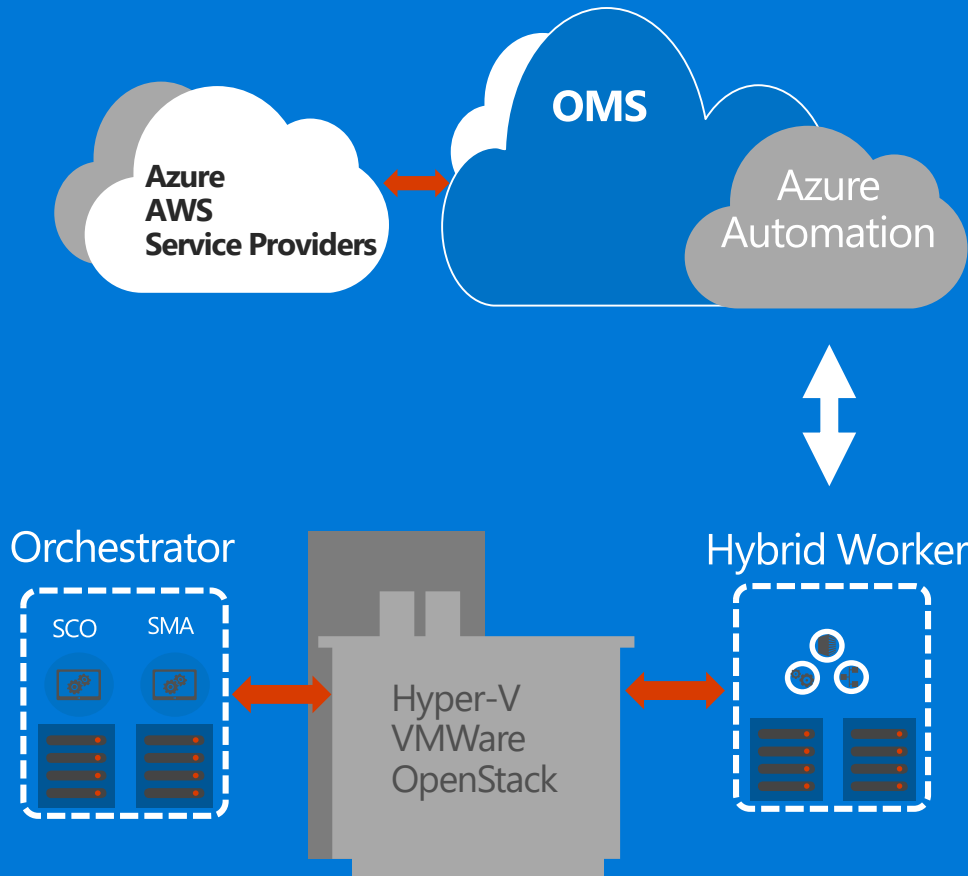
[www.ericberg.de](http://www.ericberg.de) | [www.geekzeugs.de](http://www.geekzeugs.de)



# Managing across the entire lifecycle



# Azure Automation



- ✓ Manage any cloud & on prem
- ✓ Process automation & DSC
- ✓ PowerShell & Graphical authoring
- ✓ Integrate systems
- ✓ Windows & Linux

## Key Features

### PowerShell & PS Workflow Engines

- Use your existing PS scripts
- Checkpoint/Parallel if needed

### Runbooks, Modules

- Author PS, PSWF, Graphical runbooks
- Gallery – Runbooks, modules
- Extensibility, integration

### Assets

- Secure, global store for variables, credentials, ...
- Schedules

### Jobs

- Troubleshoot/audit via job history

### PowerShell DSC

- Configurations, Pull service
- Node Management & Reporting

### Hybrid Runbook Workers

- Install on any machine
- Secure, only outbound ports

### Webhooks

- URL to start runbook remotely
- Integration



Reliable, highly available, scalable



Hybrid management

## Build

- Create VMs and Cloud infrastructure
- Integrate into Dev tools

## Configure

- Update management
- Configure cloud and VMs per application

## Monitor

- Identify changes causing issues
- Integrate into ITSM solutions on Alerts

## Protect

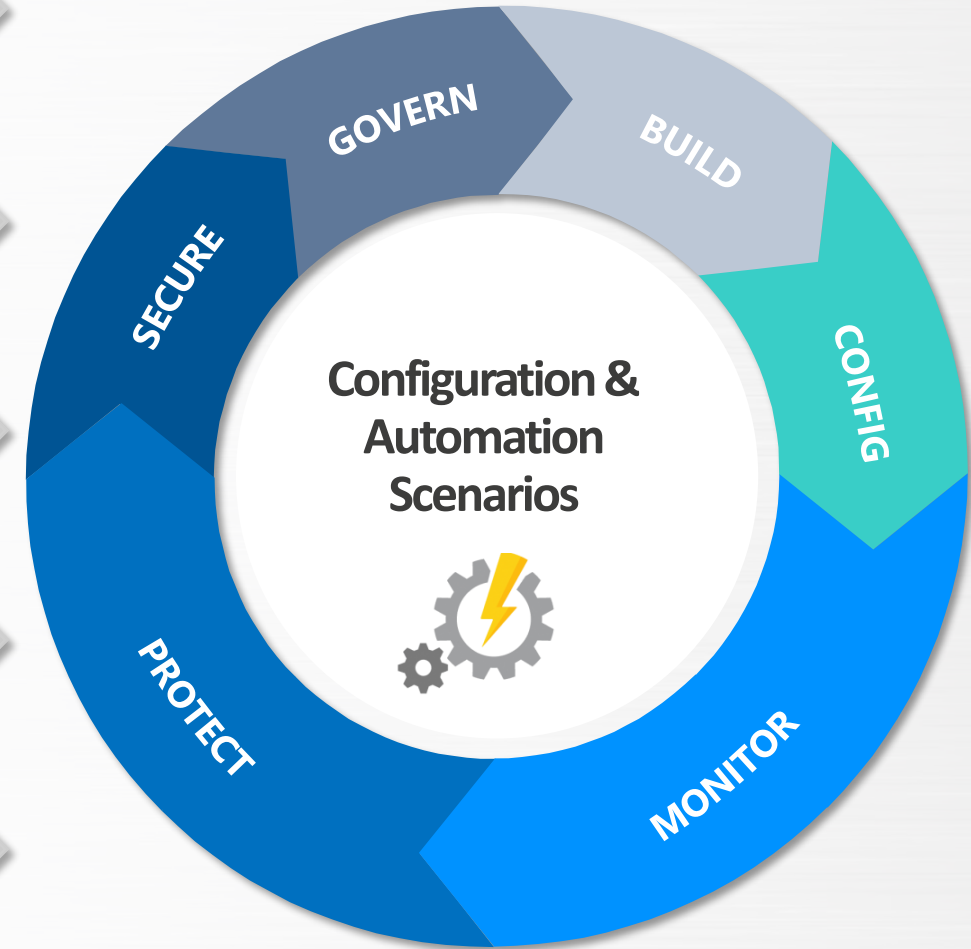
- Recover application / VM from backup
- Integrate into Site Recovery for fail over

## Secure

- Quarantine VM if exploited
- Set policy for infrastructure and app

## Govern

- Set up RBAC per user / group
- Recover unused resources



# One Automation Solution for Azure, 3<sup>rd</sup> party clouds and On Premises

## User Interface

- Web portal
- Access Permissions (RBAC)
- Source control & versioning

## Authoring

- Graphical Authoring to visualize end-to-end orchestration
- PowerShell Authoring
- Gallery
- PowerShell Desired State Configuration support

## Runbook Engine

- Highly available
- PowerShell-based engine
- Hybrid runbook worker to enable management across public and private clouds.
- REST web service and PowerShell modules to enable integration from 3<sup>rd</sup> party systems / web portals

## Integration

- Based on PowerShell modules with a rich ecosystem
- Use existing PowerShell modules for Microsoft and 3<sup>rd</sup> party systems
- Create PowerShell modules for additional resources/systems

## Tools

- Tools to convert SCO Integration Packs and runbooks and import into Azure Automation

# Authoring

- Graphical runbooks
  - New type of graphical runbook based on native PowerShell
  - Improvements to graphical authoring and runbook capabilities
- PowerShell ISE add-on
  - Author textual runbooks (PowerShell, PowerShell Workflow)
  - Continued improvements in response to feedback
- Start-AzureRmAutomationRunbook cmdlet
  - Added –Wait and –MaxWaitSeconds parameters
  - Parent runbook can now wait for child runbook to finish and send back output
  - Enables any runbook type to call any runbook type and get back results
- More Gallery runbooks
  - We continue to add useful runbooks to the gallery



# Remediate VM alert with Automation runbook

- Integrate Automation in Azure
  - Seamlessly use Automation to manage Azure resources
- Trigger runbook from VM alert
  - Configure VM alert to start a runbook when alert triggers
  - Microsoft runbook or user runbook
  - Alert context passed to runbook
- Account creation as needed
  - Create Automation account and Run As credentials as needed for user
  - Make it seamless to get going with alert remediation

The screenshot displays two side-by-side windows from the Azure portal. The left window, titled 'Add an alert rule', shows a line graph of a metric over time. Below the graph, the 'Condition' is set to 'greater than', the 'Threshold' is '95', and the 'Period' is 'Over the last 10 minutes'. At the bottom, a 'Take Action' button is labeled 'Run a runbook from this alert'. The right window, titled 'Configure Runboo..', shows the 'Run runbook' settings. The 'Run runbook' toggle is 'Enabled', and the 'Runbook source' is 'Standard'. The 'Runbook' dropdown menu is open, showing options: 'Choose a runbook', 'Restart VM' (highlighted), 'Stop VM', 'Scale Up VM', 'Scale Down VM', and 'Remove VM'. Both windows have an 'OK' button at the bottom.

**Add an alert rule**

40%  
20%  
0%

6 PM Jul 24 6 AM 12 PM

\* Condition  
greater than

\* Threshold ①  
95 %

\* Period ①  
Over the last 10 minutes

Email owners, contributors, and readers  
☐

Additional administrator email(s)  
Add email addresses separated by semicolons

Webhook ①  
HTTP or HTTPS endpoint to route alerts to  
[Learn more about configuring webhooks](#)

Take Action ①  
Run a runbook from this alert

**OK**

**Configure Runboo..**  
Alert rule

\* Run runbook  
Enabled Disabled

\* Runbook source ①  
Standard User

\* Runbook  
Choose a runbook  
Choose a runbook  
Restart VM  
Stop VM  
Scale Up VM  
Scale Down VM  
Remove VM


**OK**




# Alert remediation in OMS

- IT Management
  - Logs ingested by OMS from managed systems
  - Log analytics for system state information
  - Monitor and alert
  - Integrated automation for actions on machines or across systems
- Alert Remediation
  - Alert triggered from log search
  - Start runbook from alert and pass search results
  - Runbook performs remediation, troubleshooting, reporting

## Actions

 Email notification

Yes No

 Webhook

Yes No

 Runbook

Yes No

Automation account


ChrisOMSEastUS

Select a runbook

HandleFailedJob ▼

Run on

Azure Hybrid worker

 Incident

Yes No

# Automation Webhooks

- Webhook

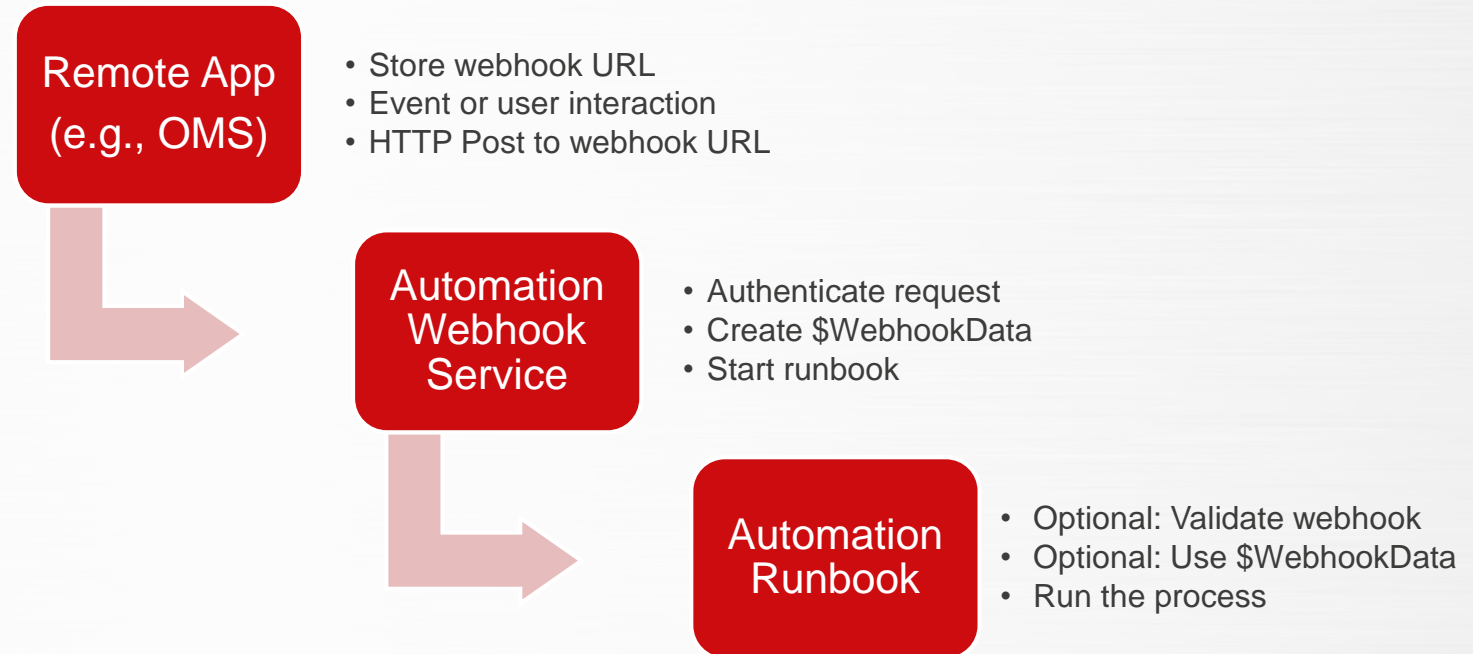
- URL to start runbook from remote app
- HTTP Post
- Works with Visual Studio Online, GitHub, custom web sites, OMS alerts, Azure alerts, etc.

- Runbook Parameters

- At webhook creation, you configure parameter values to pass to runbook.
- Additional \$WebhookData parameter with HTTP headers and body (with data)

- Example

[https://s4events.azure-automation.net/webhooks?token=1CH%Ha8\\$H3U7E%G38Ur7s7aG](https://s4events.azure-automation.net/webhooks?token=1CH%Ha8$H3U7E%G38Ur7s7aG)



# Security considerations

- How many automation accounts?
- Run as Accounts?
- Webhooks?
- RBAC?
- Script repository?
- Code changes?
- Access Keys?
- Hybrid Runbook Worker?

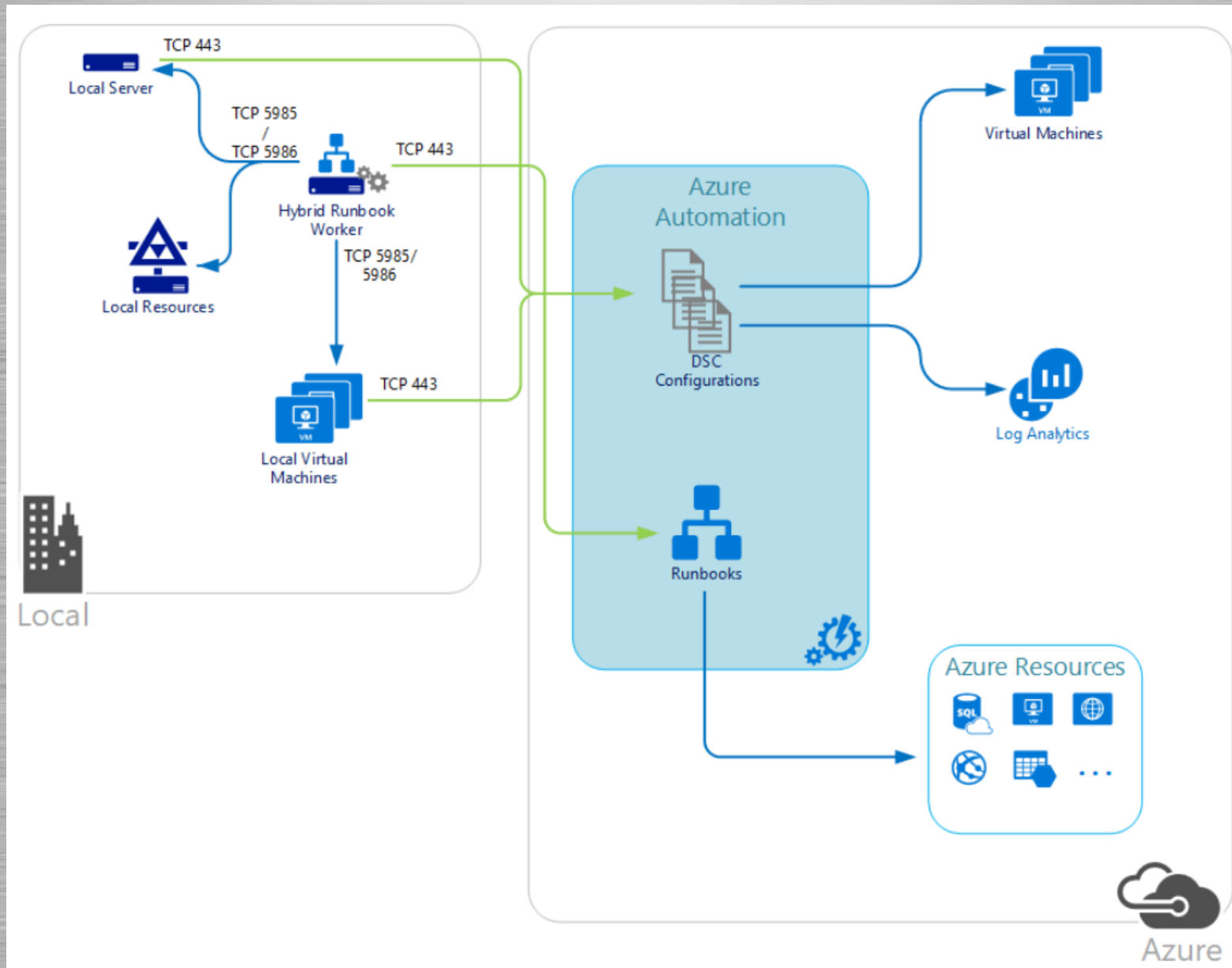
# Roles

Role	Description
Owner	access to all resources and actions within an Automation account
Contributor	manage everything except modifying other user's access permissions
Reader	view all the resources but cannot make any changes.
Automation Operator	view runbook name and properties and create and manage jobs for all runbooks
Automation Job Operator	create and manage jobs for all runbooks
Automation Runbook Operator	view a runbook's name and properties
Log Analytics Contributor	read all monitoring data and edit monitoring settings
Log Analytics Reader	view and search all monitoring data as well as view monitoring settings
Monitoring Contributor	read all monitoring data and update monitoring settings
Monitoring Reader	read all monitoring data
User Access Administrator	manage user access to Azure Automation accounts

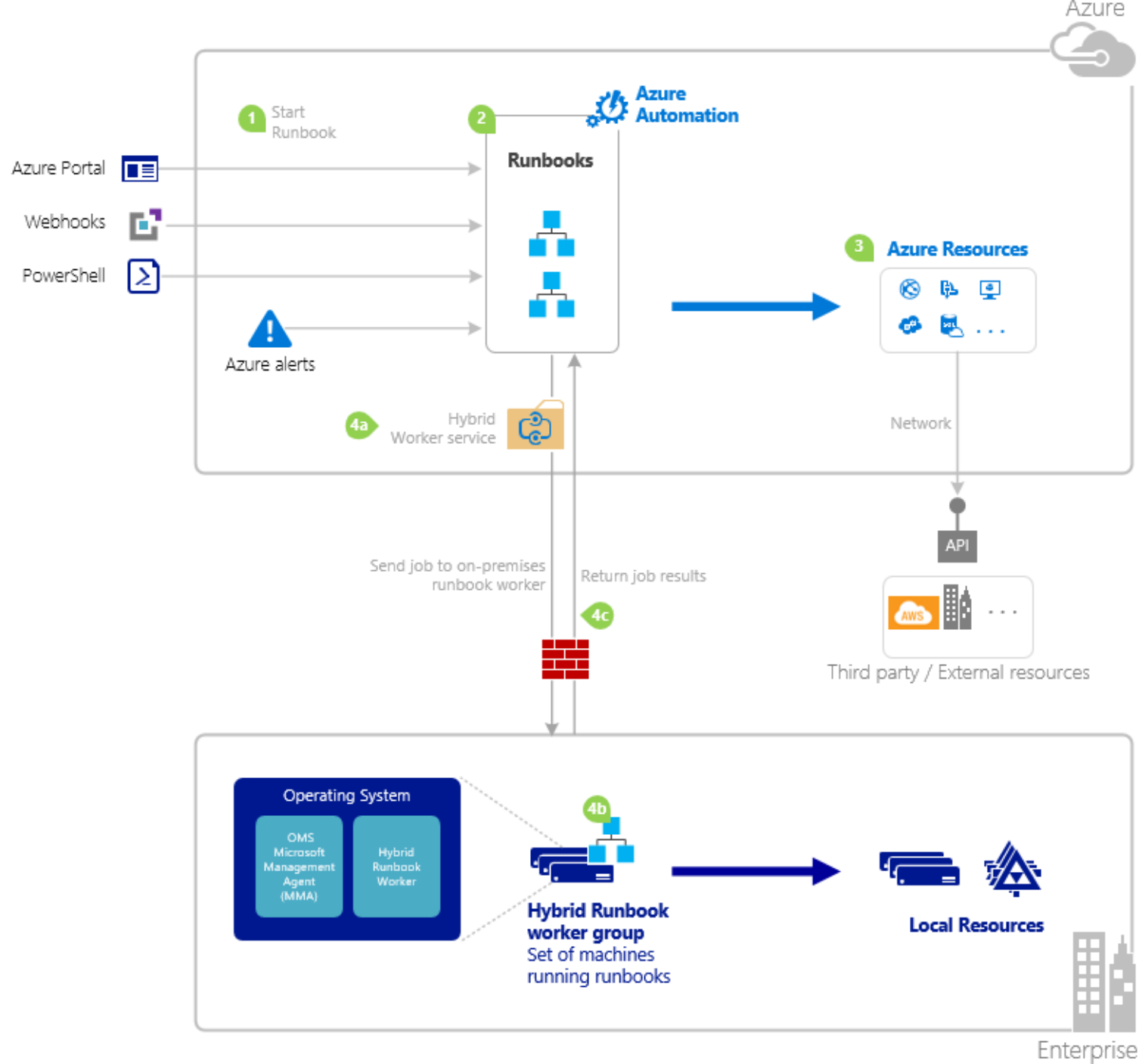
# Run As accounts

- Easily authenticate to manage Azure resources
  - Get started quickly.
  - When you create a new Automation account you can have Run As accounts created too.
- Azure Run As
  - Service principal with certificate
  - Contributor role
  - Manage ARM resources from runbooks
  - Assets: AzureRunAsCertificate, AzureRunAsConnection
- Azure Classic Run As
  - Certificate
  - Manage ASC resources from runbooks
  - Assets: AzureClassicRunAsCertificate, AzureClassicRunAsConnection

# Hybrid Worker







- 1 An actor starts a runbook
- 2 Azure automation notes that a runbook should be started
- 3 Cloud resources - Runbook acts on local Azure resources or other external resources reachable via the network
- 4a On-premises - Hybrid runbook group sends the runbook to an on-premises machine to run
- 4b Runbook acts on its local networked resources
- 4c Job results are returned



# Azure Epic Shit 😊

- Azure Functions
  - 5 minutes runtime (max 10 minutes)
  - Split code
  - Parallel processing with auto scale
- Azure Logic Apps
  - Business integration
  - Workflow processing
  - Integratin with Functions
- Many more....whatever you need

# QUIZ

- Wie oft steht das Wort „Fisch“ in dieser Präsentation?!
  - 4 ;-)
- Wer kann Jobs ausführen und sonst nichts?
  - Automation Job Operator
- Wie lang ist das Self-Signed Cert des Run-As Accounts gültig?
  - 1 Jahr
- BONUS: Wer hält auf der Ignite 2019 den besten Vortrag?
  - t.b.d.

**Time for your questions...**

