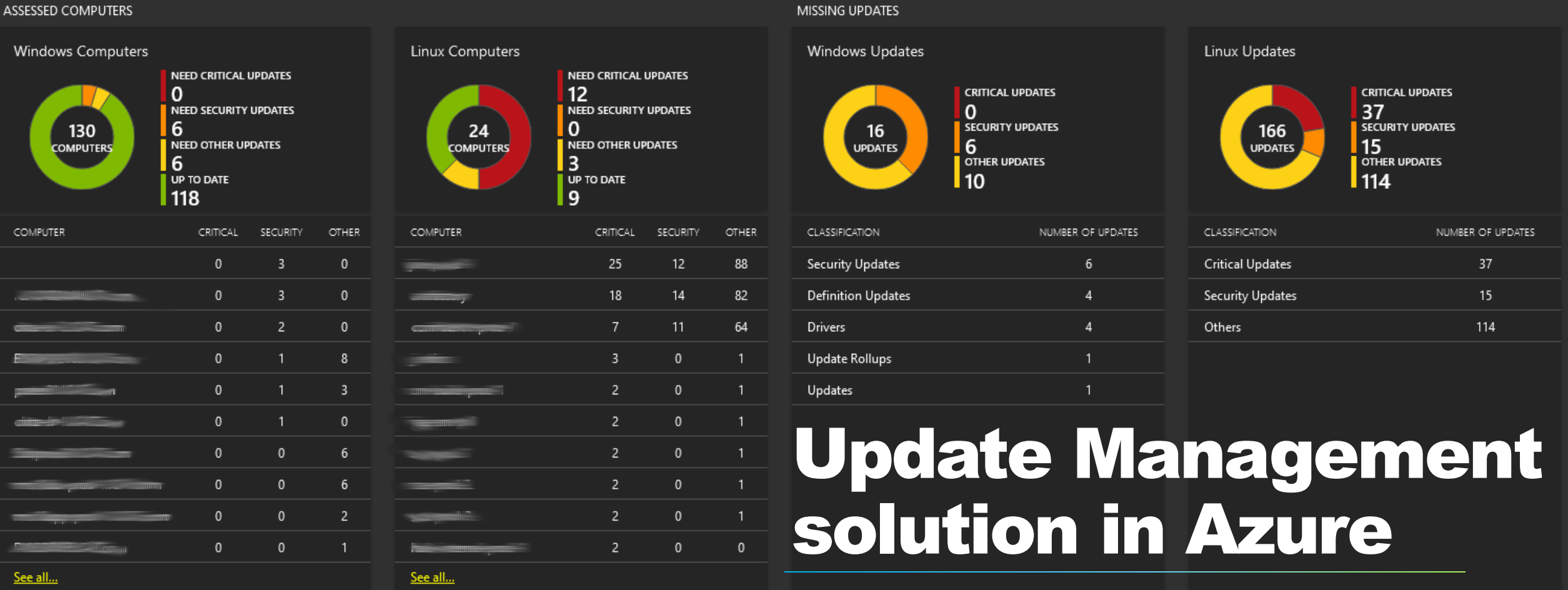




PowerShell Southampton User Group



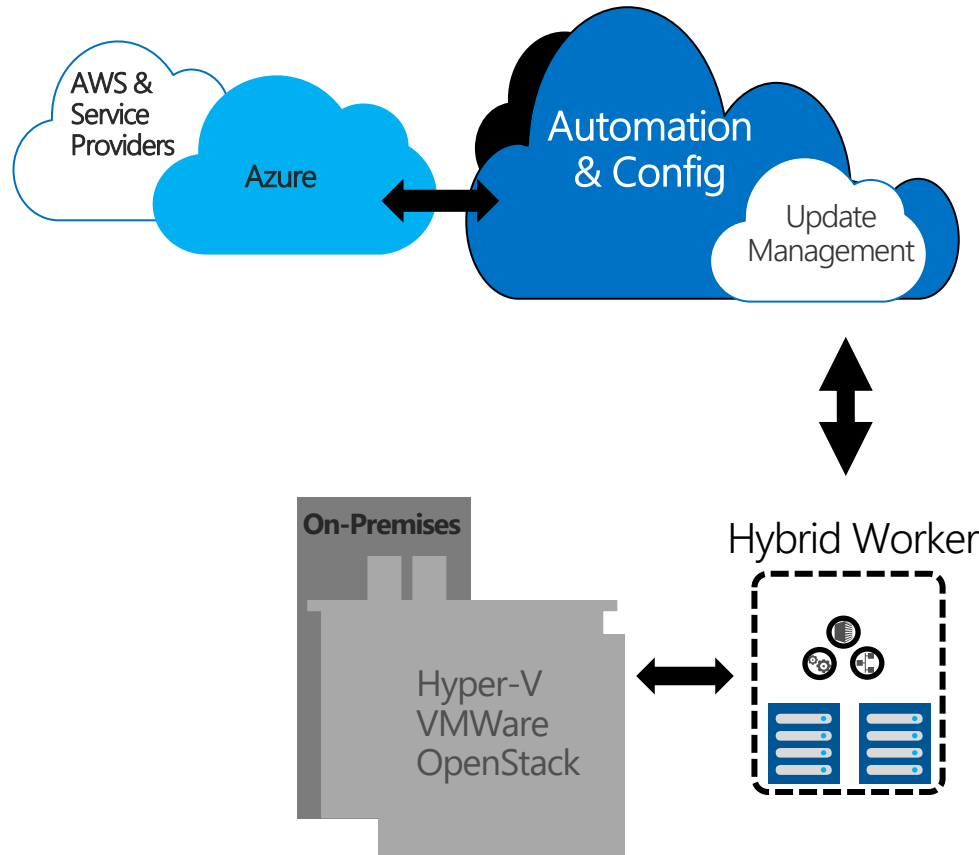
Update Management solution in Azure

Overview and getting started

About me

- Lead Architect of Catapult Systems Managed Automations Team
- Worked in IT for 15+ years
- Authored chapters for The PowerShell Conference Book
- Authoring first full book Practical Automation with PowerShell
- Curate PowerShell Weekly newsletter (dowst.dev)

What is Update Management



- ✓ Update Azure & non-Azure
- ✓ Windows & Linux
- ✓ Update Insights
- ✓ Update Deployments

Key Features



Update Deployments

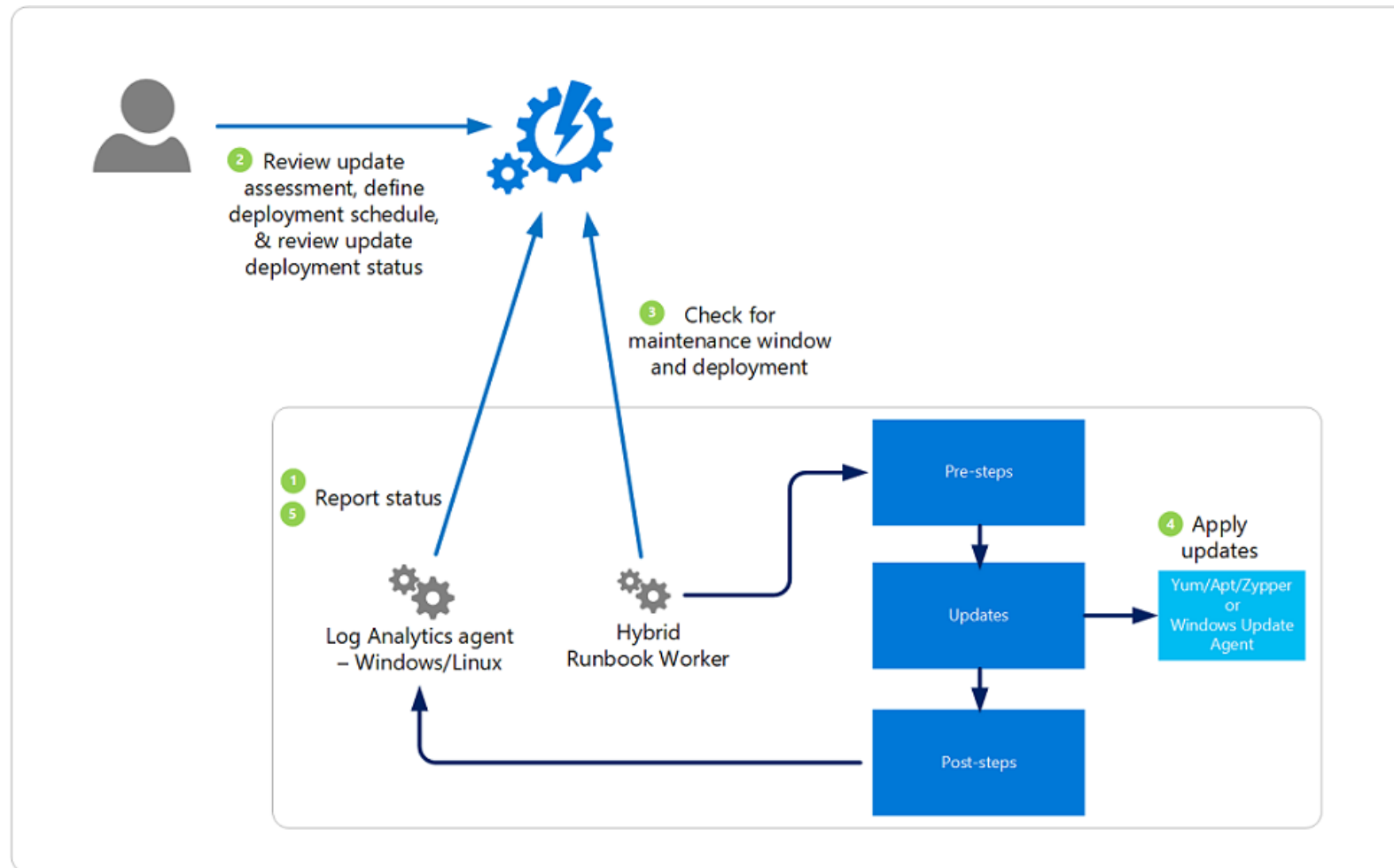
- Approval via Update Classifications
- Targeting: Leverage existing groups (Log Analytics, WSUS, AD, SCCM)
- Flexible scheduling options
- ConfigMgr integration
- Pre and Post patching automation



Update Insights

- Detailed reporting / compliance across Windows and Linux distros
- Domain or non joined servers
- Leverages native Windows and Linux tools
- Rich search capabilities cross updates
- WS 2008 R2 & above.
- Redhat, CentOS, Ubuntu, SuSE, AMI

How it works



Onboarding Devices

```
root@localhost:~  
Configure syslog...  
info    netstat tool is not available. Default port defined in omsadmin.sh will  
be used.  
Configuring rsyslog for OMS logging  
Restarting service: rsyslog  
Configure heartbeat monitoring agent...  
info    netstat tool is not available. Default port defined in omsadmin.sh will  
be used.  
Configure log rotate for workspace a0blcb84-b708-4076-9bd1-708bbfflbd58...  
INFO:   Configuring OMS agent service a0blcb84-b708-4076-9bd1-708bbfflbd58 ...  
error   MetaConfig generation script not available at /opt/microsoft/omsconfig/S  
cripts/OMS_MetaConfigHelper.py  
Trying to stop omi with systemctl  
omi is stopped.  
Trying to start omi with systemctl  
omi is started.  
System appears to have SELinux installed, attempting to install selinux policy m  
odule for logrotate  
    Trying /usr/share/selinux/packages/omsagent-logrotate/omsagent-logrotate.pp ..  
.  
Configure log rotate for workspace a0blcb84-b708-4076-9bd1-708bbfflbd58...  
Applying Syslog conf hotfix...  
----- Upgrading package: omsconfig (omsconfig-1.1.1-927.x64) -----  
Checking for ctypes python module...  
Cleaning up existing dsc_hosts...  
chmod: cannot access '/opt/dsc': No such file or directory  
Cleaned up existing dsc_hosts...
```

Requirements



Log Analytics Workspace

Microsoft Monitoring Agent (MMA) for Windows or Linux



Automation Account

Automation Hybrid Runbook Worker



Update Repository

Microsoft Update
Windows Server Update Services (WSUS)
Configuration Manager
Apt-Get/Yum/Zypper

Requirements

The screenshot shows the Azure portal interface for the 'Update Management' service. On the left is a navigation pane with a search bar and categories: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration Management (Inventory, Change tracking, State configuration (DSC)), Update management (highlighted with a red box), Process Automation (Runbooks, Jobs, Runbooks gallery, Hybrid worker groups, Watcher tasks), and Shared Resources. The main content area is titled 'Update Management' and includes instructions: 'Enable consistent control and compliance of your VMs with Update Management.', 'This service is included with Azure virtual machines. You only pay for logs stored in Log Analytics.', and 'This service requires a Log Analytics workspace and this Automation account.' Below this are configuration fields: 'Log Analytics workspace location' (East US), 'Log Analytics workspace subscription' (Microsoft Azure Sponsorship), '*Log Analytics workspace' (a dropdown menu with 'Select Workspace...' highlighted by a red box and a blue arrow pointing to a green callout box), and 'Automation account' (CameronAutomation). An 'Enable' button is at the bottom. On the right, there are links for 'Learn more', 'Update Management', 'Update Management pricing', and 'Troubleshooting'.

Search (Ctrl+/) <<

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Configuration Management

Inventory

Change tracking

State configuration (DSC)

Update management

Update management

Process Automation

Runbooks

Jobs

Runbooks gallery

Hybrid worker groups

Watcher tasks

Shared Resources

Update Management

Enable consistent control and compliance of your VMs with Update Management.

This service is included with Azure virtual machines. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and this Automation account.

Log Analytics workspace location ⓘ

East US

Log Analytics workspace subscription ⓘ

Microsoft Azure Sponsorship (d78824b1-1f2...

*Log Analytics workspace ⓘ

Select Workspace...

Select Workspace...

Automation account ⓘ

CameronAutomation

Enable

Learn more


[Update Management](#)


[Update Management pricing](#)


[Troubleshooting](#)


Enable Update Management Solution in Automation Account


Onboarding Azure VM


 **PSUG-Win02** | Guest + host updates ...
Virtual machine


 Advisor recommendations


 Extensions


 Continuous delivery

 Availability + scaling


 Configuration


 Identity


 Properties


 Locks


Operations


 Bastion


 Auto-shutdown


 Backup


 Disaster recovery


 **Guest + host updates**

 Inventory


 Change tracking


 Configuration management (Preview)


 Policies

 Run command

Monitoring

 Insights

 Alerts


 Metrics

Guest + host updates
Customize how and when you receive guest and host updates for your virtual machine.

Guest OS updates
Update management
Update management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines. You can quickly assess the status of available updates and manage the process of installing required updates for your servers. [Learn more](#)

[Go to Update management](#)

Host updates
Maintenance timeline
Choose when you want to take a host update within a set, Azure predefined time window. [Learn more](#)

 You have no pending updates for maintenance. [Learn more](#)

Update Management (PSUG-Win02 - VM) ⚙ ...

Update Management

Enable consistent control and compliance of this VM with Update Management.

This service is included with Azure virtual machines and Azure Arc machines. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and an Automation account. You can use your existing workspace and account or let us configure the nearest workspace and account for use.

Log Analytics workspace location ⓘ

UK South

Log Analytics workspace ⓘ

PSUG-2108240901

Automation account subscription ⓘ

Visual Studio Enterprise Subscription – MPN

Automation account ⓘ

PSUG-2108240901

[Enable](#)

Onboarding non-Azure Devices

PSUG-2108240901 | Agents management

Log Analytics workspace

Search (Ctrl+ /)

Windows serversLinux servers

OverviewActivity logAccess control (IAM)TagsDiagnose and solve problems

SettingsLocksAgents managementAgents configurationCustom logsComputer GroupsLinked storage accountsNetwork IsolationGeneralWorkspace summaryWorkbooksLogsSolutionsUsage and estimated costs

2 Windows computers connected

Go to logs

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

Download Windows Agent (64 bit)Download Windows Agent (32 bit)

Workspace ID5548dc24-d8b5-4a2e-a7f5-e2902cf24c84

Primary keynlouxBgRgAuMhEugSuqHlo5+jU8olFwTrR6f6lNqQ/0oT7uWSeh81k7k

Secondary keyZYPajcpOge/9MZ8+SV/atyHOJrNWnoHS/XOQu2eIQ0XX0/4vuBQoCC

Log Analytics Gateway

If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway.

Learn more about Log Analytics GatewayDownload Log Analytics Gateway

PSUG-2108240901 | Agents management

Log Analytics workspace

Search (Ctrl+ /)

Windows serversLinux servers

OverviewActivity logAccess control (IAM)TagsDiagnose and solve problems

SettingsLocksAgents managementAgents configurationCustom logsComputer GroupsLinked storage accountsNetwork IsolationGeneralWorkspace summaryWorkbooksLogsSolutionsUsage and estimated costs

1 Linux computers connected

Go to logs

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

Download Linux Agent

Download and onboard agent for Linux

wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/scripts/onboard_agent.sh

Workspace ID

Primary key

Secondary key

United Kingdom

UKSouth

Norway

NorwayEast

Europe

NorthEurope

WestEurope

Switzerland

SwitzerlandNorth

US

EastUS - EastUS2 *

EastUS2 - EastUS *

WestUS

WestUS2

NorthCentralUS

CentralUS

SouthCentralUS

WestCentralUS

US Gov

USGovVirginia

USGovArizona³

Brazil

BrazilSouth

Canada

CanadaCentral

China

ChinaEast2³

Asia Pacific

EastAsia

SoutheastAsia

India

CentralIndia

Japan

JapanEast

Australia

AustraliaEast

AustraliaSoutheast

Korea

KoreaCentral

United Arab Emirates

UAENorth

France

FranceCentral

 Onboarding is not supported for the account in this region



Update Management

Enable consistent control and compliance of your VMs with Update Management.

This service is included with Azure virtual machines. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and this Automation account.

Log Analytics workspace location ⓘ

Log Analytics workspace subscription ⓘ

Microsoft Azure Sponsorship (d78824b1-1f2...)

Log Analytics workspace ⓘ

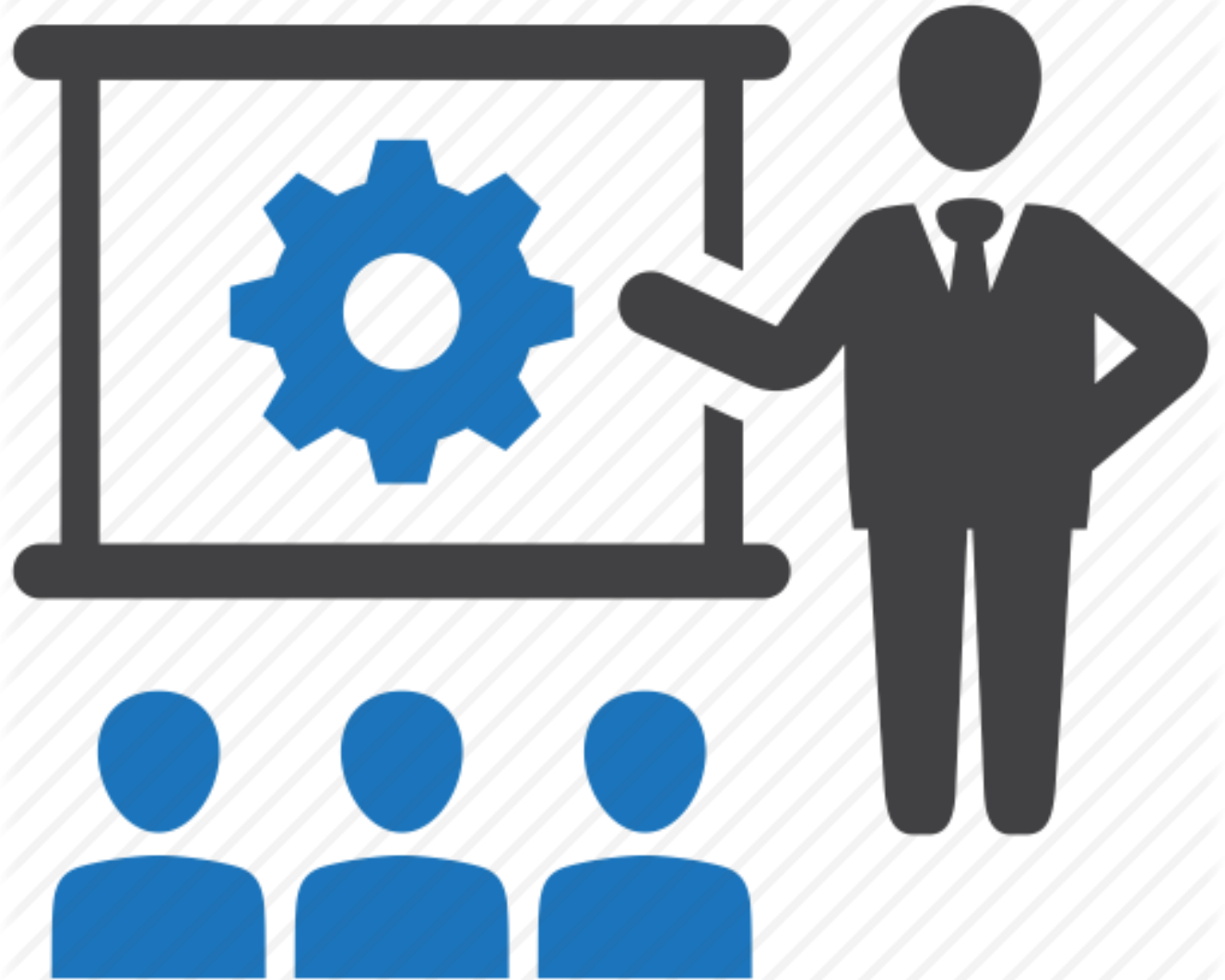
Automation account ⓘ

Launch-Dev-Client

Enable

Demo

Creating Deployments



Pre and Post Scripts

- Let's you run a script before (pre-task) and after (post-task)
- Script must be PowerShell and imported in the Automation Account
- Parameters can be defined in Update Deployment
- Script can only run in Azure
- SoftwareUpdateConfigurationRunContext
- Deployment stops if pre-script throws an exception

Troubleshooting Agents

- Confirm Microsoft Monitoring Agent is running and reporting
- Confirm Hybrid Runbook Worker configuration and connection
- Windows
 - Install-Script -Name Troubleshoot-WindowsUpdateAgentRegistration
- Linux
 - wget https://gallery.technet.microsoft.com/scriptcenter/Troubleshooting-utility-3bcbefe6/file/216573/1/update_mgmt_health_check.py
 - sudo python update_mgmt_health_check.py

```
root@localhost:~  
  
Passed: Microsoft Monitoring agent is running  
  
Passed: Machine registered with log analytics workspace:['a0b1cb84-b708-4076-9bd1-708bbff1bd58']  
  
Passed: Hybrid worker package is present  
  
Passed: Hybrid worker is running  
  
Passed: Machine is connected to internet  
  
Passed: TCP test for {scus-agentservice-prod-1.azure-automation.net} (port 443) succeeded  
  
Passed: TCP test for {eus2-jobruntimeprod-sul.azure-automation.net} (port 443) succeeded  
  
Passed: TCP test for {a0b1cb84-b708-4076-9bd1-708bbff1bd58.ods.opinsights.azure.com} (port 443) succeeded  
  
Passed: TCP test for {a0b1cb84-b708-4076-9bd1-708bbff1bd58.oms.opinsights.azure.com} (port 443) succeeded  
  
Passed: TCP test for {ods.systemcenteradvisor.com} (port 443) succeeded  
  
[root@localhost ~]#  
  
RuleId : AutomationAgentServiceConnectivityCheck1  
RuleGroupId : connectivity  
RuleName : Registration endpoint  
RuleGroupName : connectivity  
RuleDescription : Proxy and firewall configuration must allow Automation Hybrid Worker agent to communicate with a0b1cb84-b708-4076-9bd1-708bbff1bd58.agentsvc.azure-automation.net  
CheckResult : Passed  
CheckResultMessage : TCP Test for a0b1cb84-b708-4076-9bd1-708bbff1bd58.agentsvc.azure-automation.net (port 443) succeeded  
CheckResultMessageId : AutomationAgentServiceConnectivityCheck1.Passed  
CheckResultMessageArguments : {a0b1cb84-b708-4076-9bd1-708bbff1bd58.agentsvc.azure-automation.net}  
  
RuleId : AutomationJobRuntimeDataServiceConnectivityCheck  
RuleGroupId : connectivity  
RuleName : Operations endpoint
```

Reporting on Deployments

- Report data is stored in Log Analytics Workspace
- Update only shows as required if approved
- Be careful of false positives

Reporting on Deployments

```
let timeAgo = ago(30d);
let ParentJobs = AzureDiagnostics
| where TimeGenerated > timeAgo
| where RunbookName_s == "Patch-MicrosoftOMSComputers" and StreamType_s == "Verbose" and Category == "JobStreams"
| where ResultDescription contains "Getting SoftwareUpdateConfigurationMachines"
| extend ScheduleName = substring(ResultDescription,indexOf(ResultDescription, "SoftwareUpdateConfigurationName")+32, indexOf(ResultDescription, "ShouldResolveStaticMachines")-indexOf(ResultDescription, "SoftwareUpdateConfigu
| project TimeGenerated, ScheduleName, ParentJobId_g = JobId_g
| join kind= inner (
    AzureDiagnostics
    | where TimeGenerated > timeAgo
    | where RunbookName_s == "Patch-MicrosoftOMSComputers" and StreamType_s == "Verbose" and Category == "JobStreams"
```

Completed 🕒 00:00:00.508 📄 108

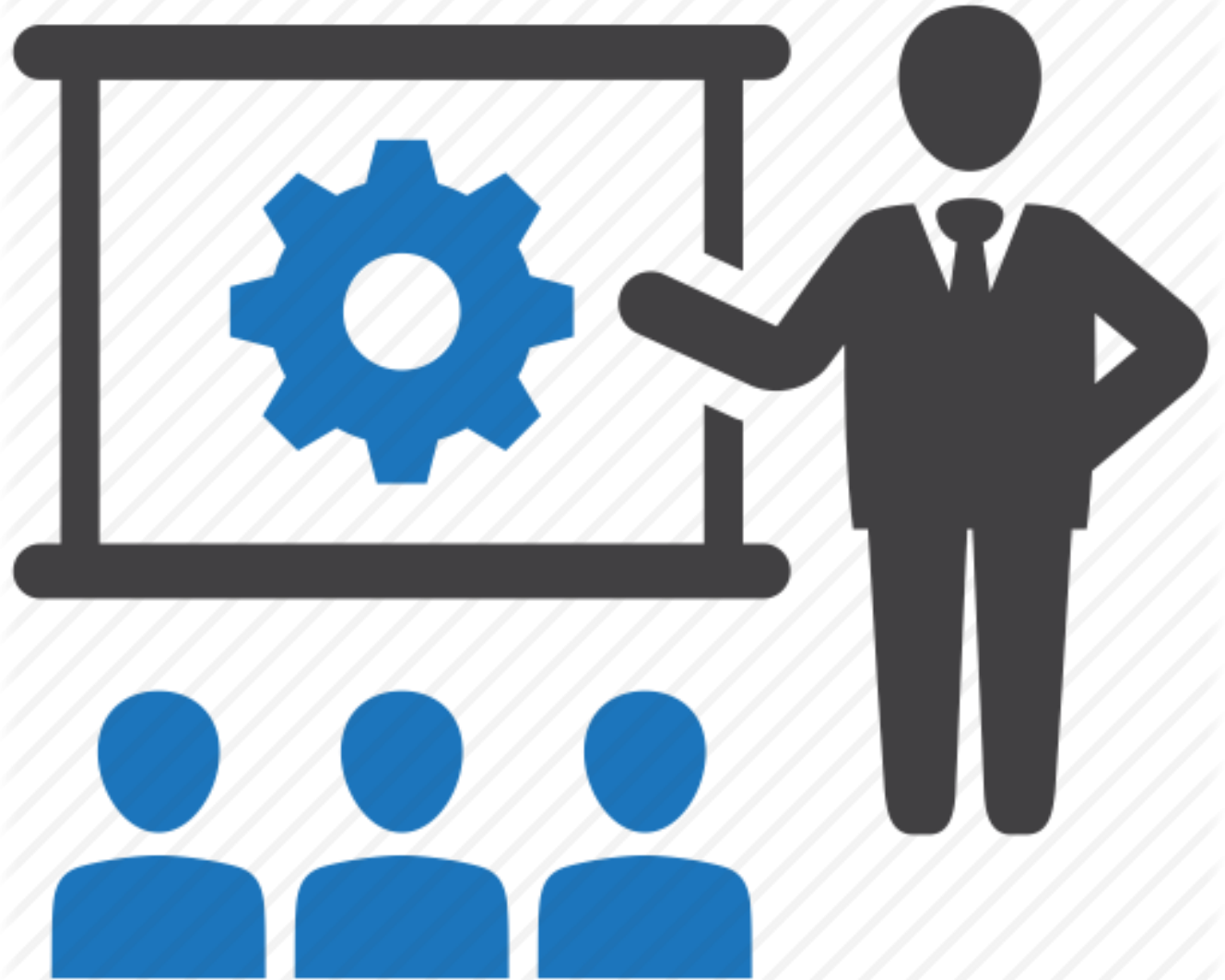
Table Chart Columns ▾ Display time (UTC+00:00) ▾ 📄 Copy re

Drag a column header and drop it here to group by that column

	MachineName ▾	ScheduleName ▾	Status ▾	DurationInMinutes ▾	StartDateTimeUtc [UTC] ▾	EndDateTimeUtc [UTC] ▾	StatusDescription ▾	RebootRequired ▾	InitialRequiredUpdatesCount ▾	TotalUpdatesInstalled
➤	fakename.contoso.com	Jan Prod Patching	Incomplete	32	1/18/2020, 4:03:11.929 AM	1/18/2020, 4:35:01.618 AM	Some updates failed to install. Check the update run progress records f...	false	6	5
➤	fakename.contoso.com	Jan Prod Patching	Incomplete	24	1/18/2020, 4:02:46.388 AM	1/18/2020, 4:27:05.679 AM	Some updates failed to install. Check the update run progress records f...	false	6	5
➤	fakename.contoso.com	Jan Prod Patching	FailedToStart	0	1/16/2020, 1:15:10.045 PM	1/16/2020, 1:15:10.045 PM	Job was suspended.	false	0	0
➤	fakename.contoso.com	Jan Prod Patching	FailedToStart	0	1/18/2020, 4:45:26.436 AM	1/18/2020, 4:45:26.436 AM	Job was suspended.	false	0	0
➤	fakename.contoso.com	Jan Prod Patching	FailedToStart	0	1/18/2020, 4:45:02.573 AM	1/18/2020, 4:45:02.573 AM	Job was suspended.	false	0	0
➤	fakename.contoso.com	Jan Prod Patching	FailedToStart	0	1/18/2020, 4:46:03.729 AM	1/18/2020, 4:46:03.729 AM	Job was suspended.	false	0	0
➤	fakename.contoso.com	Jan Prod Patching	FailedToStart	0	1/16/2020, 1:14:09.151 PM	1/16/2020, 1:14:09.151 PM	Job was suspended.	false	0	0
➤	fakename.contoso.com	Jan Prod Patching	FailedToStart	0	1/16/2020, 1:25:14.515 PM	1/16/2020, 1:25:14.515 PM	Job was suspended.	false	0	0
➤	fakename.contoso.com	Jan Prod Patching	Complete	23	1/18/2020, 4:03:00.958 AM	1/18/2020, 4:26:06.864 AM		false	5	5
➤	fakename.contoso.com	Jan Prod Patching	Complete	23	1/18/2020, 4:03:14.002 AM	1/18/2020, 4:25:47.542 AM		false	5	5
➤	fakename.contoso.com	Jan Prod Patching	Complete	23	1/18/2020, 4:02:45.050 AM	1/18/2020, 4:25:57.508 AM		false	5	5
➤	fakename.contoso.com	Jan Prod Patching	Complete	25	1/18/2020, 4:02:38.408 AM	1/18/2020, 4:27:56.866 AM		false	5	5
➤	fakename.contoso.com	Jan Prod Patching	Complete	25	1/18/2020, 4:02:40.104 AM	1/18/2020, 4:27:38.488 AM		false	5	5
➤	fakename.contoso.com	Jan Prod Patching	Complete	25	1/18/2020, 4:03:00.252 AM	1/18/2020, 4:27:32.741 AM		false	5	5

Demo

Monitoring Deployments



Update Management Future

- Already available to onboard through Arc
 - Still requires Log Analytics agent (for now)
- Hybrid Worker Extension for Arc (Q3 2021)
- PowerShell 7 Runbooks (Q4 2021)
- User Assigned Managed Identities (In Public Preview)

All scripts are available at: <https://github.com/mdowst/Presentation-Materials>

Twitter [@mdowst](#)

Update Management Key Takeaways

- Pre and Post scripts do not run on Hybrid Workers.
- Using a WSUS backend is highly recommended to give control over which patches get installed.
- Exclude works great for things like java. The include does not exclude all others.
- You can get false positives if things like Monthly Quality and Security Only both try to install.
- If a job fails to start it will not show in the Log Analytics jobs as failed.

Questions?

35% Discount on Practical Automation with PowerShell with offer code: au35dow

<https://www.manning.com/books/practical-automation-with-powershell>

All scripts are available at: <https://github.com/mdowst/Presentation-Materials>

Web dowst.dev

Twitter [@mdowst](https://twitter.com/mdowst)