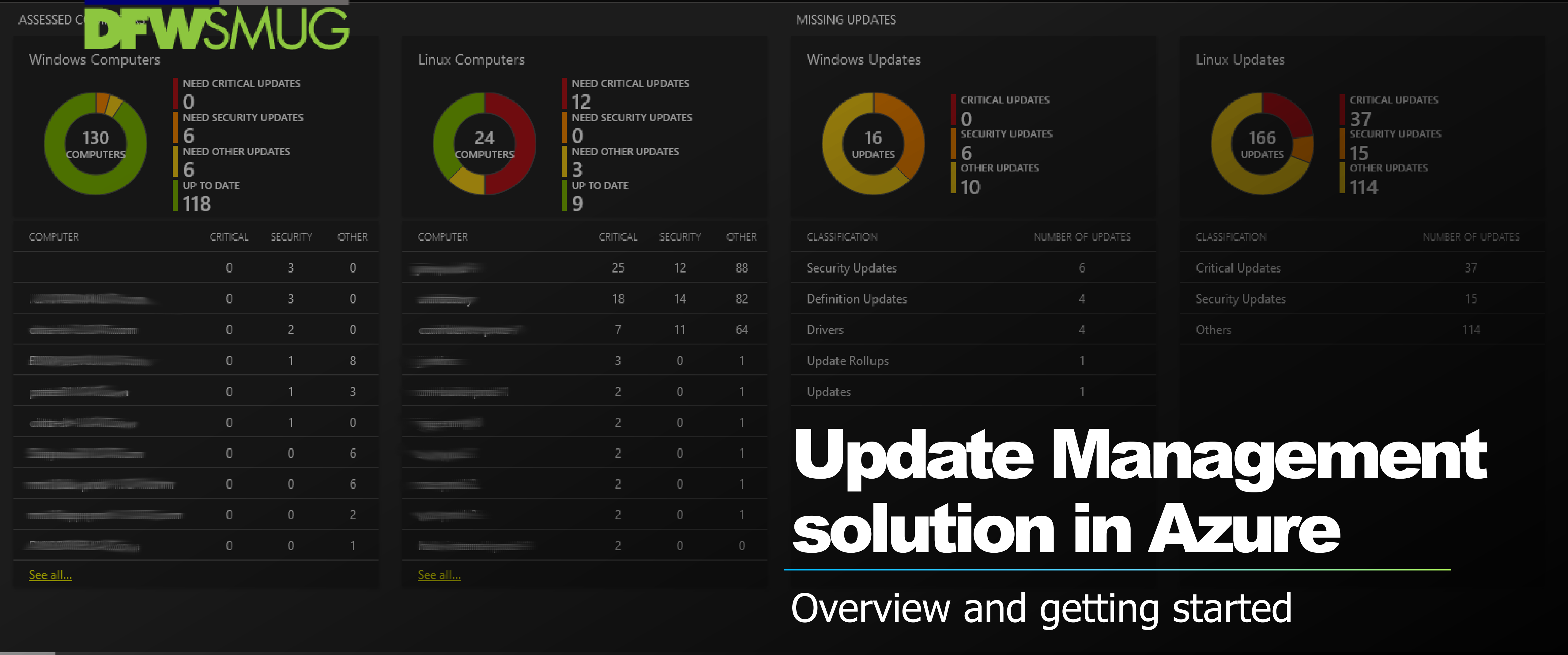


ASSESSED C

Windows Computers

130 COMPUTERS

NEED CRITICAL UPDATES 0
NEED SECURITY UPDATES 6
NEED OTHER UPDATES 6
UP TO DATE 118

COMPUTER	CRITICAL	SECURITY	OTHER
	0	3	0
[redacted]	0	3	0
[redacted]	0	2	0
[redacted]	0	1	8
[redacted]	0	1	3
[redacted]	0	1	0
[redacted]	0	0	6
[redacted]	0	0	6
[redacted]	0	0	2
[redacted]	0	0	1

See all...

Linux Computers

24 COMPUTERS

NEED CRITICAL UPDATES 12
NEED SECURITY UPDATES 0
NEED OTHER UPDATES 3
UP TO DATE 9

COMPUTER	CRITICAL	SECURITY	OTHER
[redacted]	25	12	88
[redacted]	18	14	82
[redacted]	7	11	64
[redacted]	3	0	1
[redacted]	2	0	1
[redacted]	2	0	1
[redacted]	2	0	1
[redacted]	2	0	1
[redacted]	2	0	1
[redacted]	2	0	0

See all...

MISSING UPDATES

Windows Updates

16 UPDATES

CRITICAL UPDATES 0
SECURITY UPDATES 6
OTHER UPDATES 10

CLASSIFICATION	NUMBER OF UPDATES
Security Updates	6
Definition Updates	4
Drivers	4
Update Rollups	1
Updates	1

Linux Updates

166 UPDATES

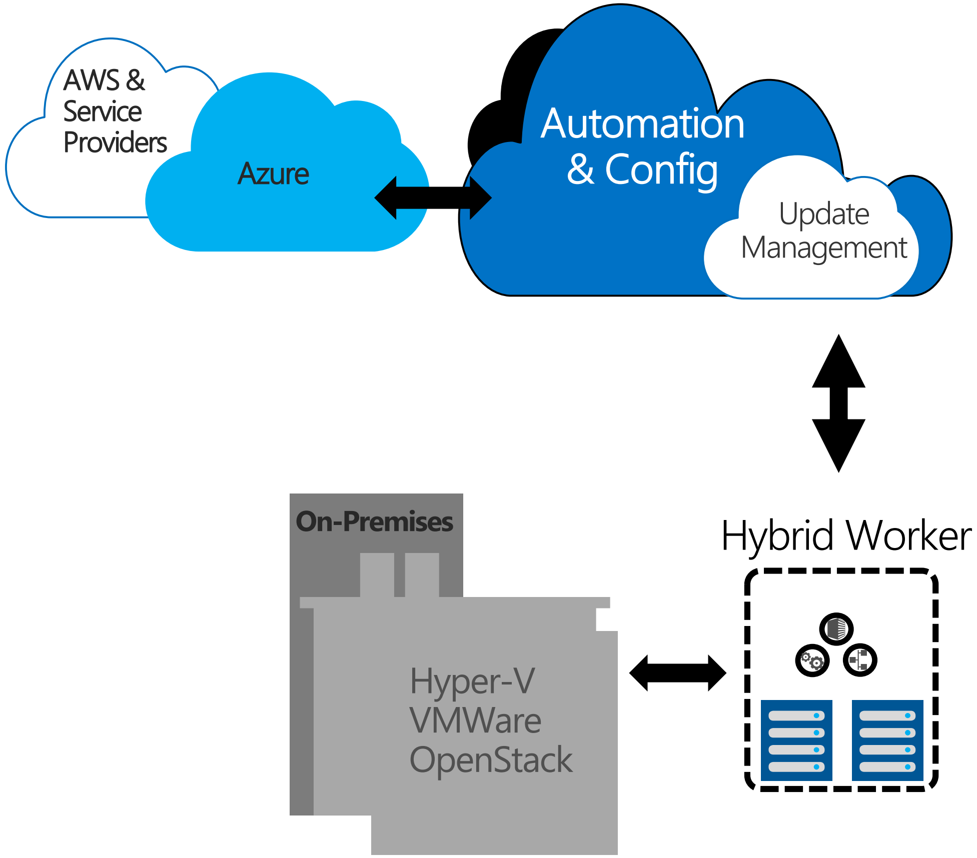
CRITICAL UPDATES 37
SECURITY UPDATES 15
OTHER UPDATES 114

CLASSIFICATION	NUMBER OF UPDATES
Critical Updates	37
Security Updates	15
Others	114

Update Management solution in Azure

Overview and getting started

What is Update Management



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

Key Features

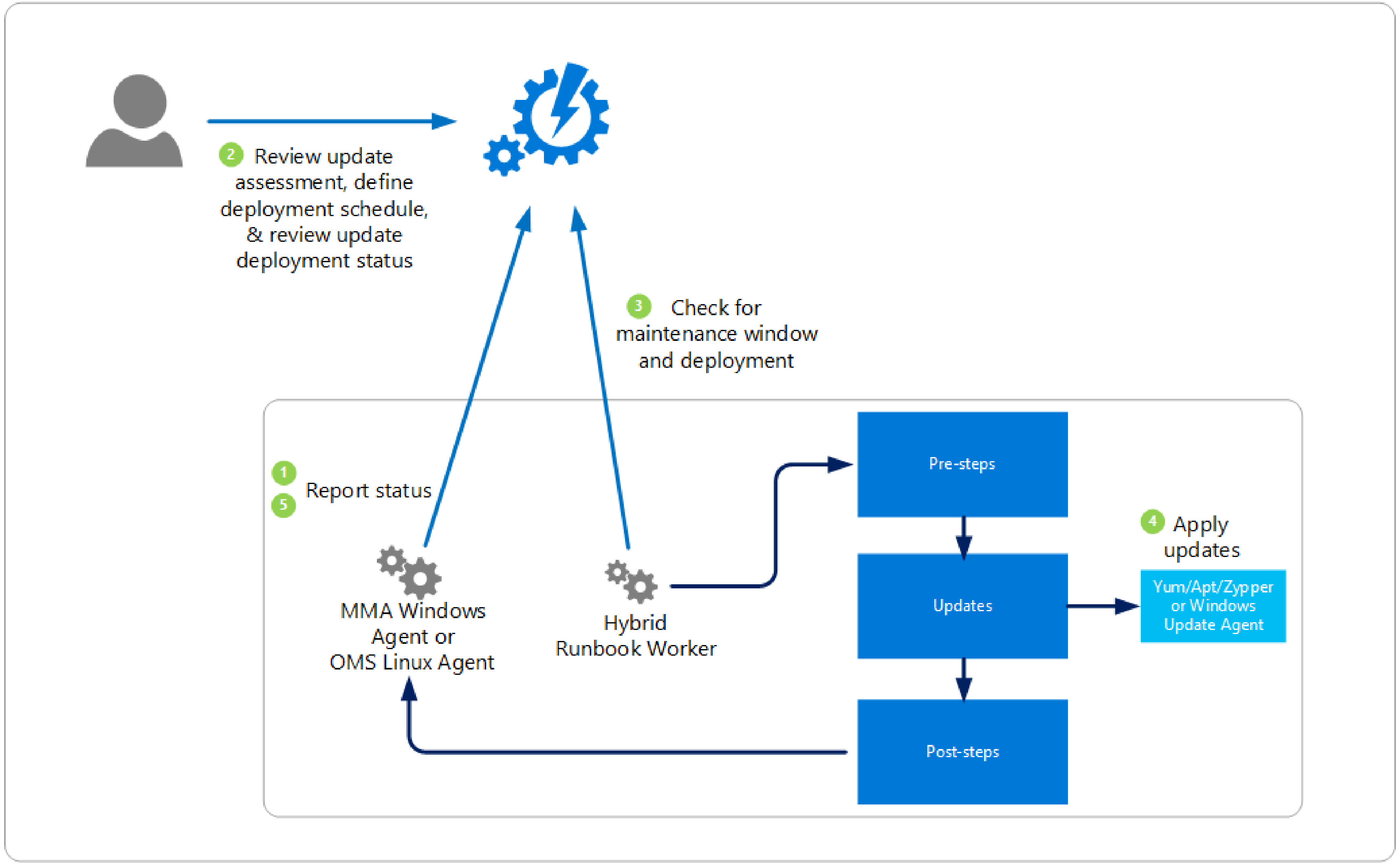
Update Deployments

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

Update Insights

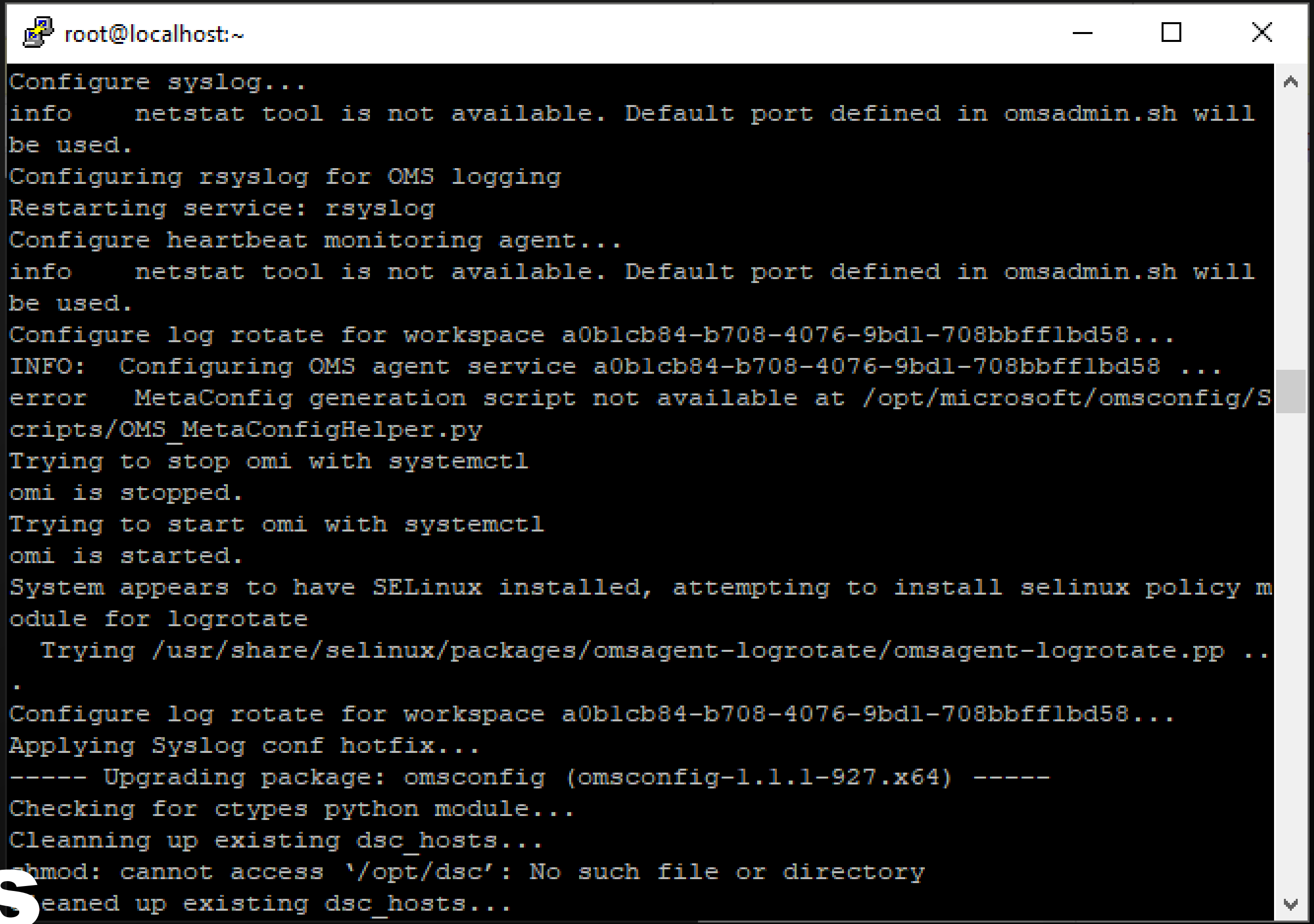
- Detailed reporting / compliance across Windows and Linux distros
- Domain or non joined servers
- Leverages native Windows and Linux tools
- Rich search capabilities cross updates
- WS 2008 R2 & above.
- Redhat, CentOS, Ubuntu, SuSE, AMI

How it works



2 Review update assessment, define deployment schedule, & review update deployment status
3 Check for maintenance window and deployment
1
5
Report status
MMA Windows Agent or OMS Linux Agent
Hybrid Runbook Worker
Pre-steps
Updates
Post-steps
4 Apply updates
Yum/Apt/Zypper or Windows Update Agent

Onboarding Devices



```
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 a0b1cb84-b708-4076-9bd1-708bbff1bd58...
INFO:  Configuring OMS agent service a0b1cb84-b708-4076-9bd1-708bbff1bd58 ...
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 a0b1cb84-b708-4076-9bd1-708bbff1bd58...
Applying Syslog conf hotfix...
----- Upgrading package: omsconfig (omsconfig-1.1.1-927.x64) -----
Checking for ctypes python module...
Cleanning 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

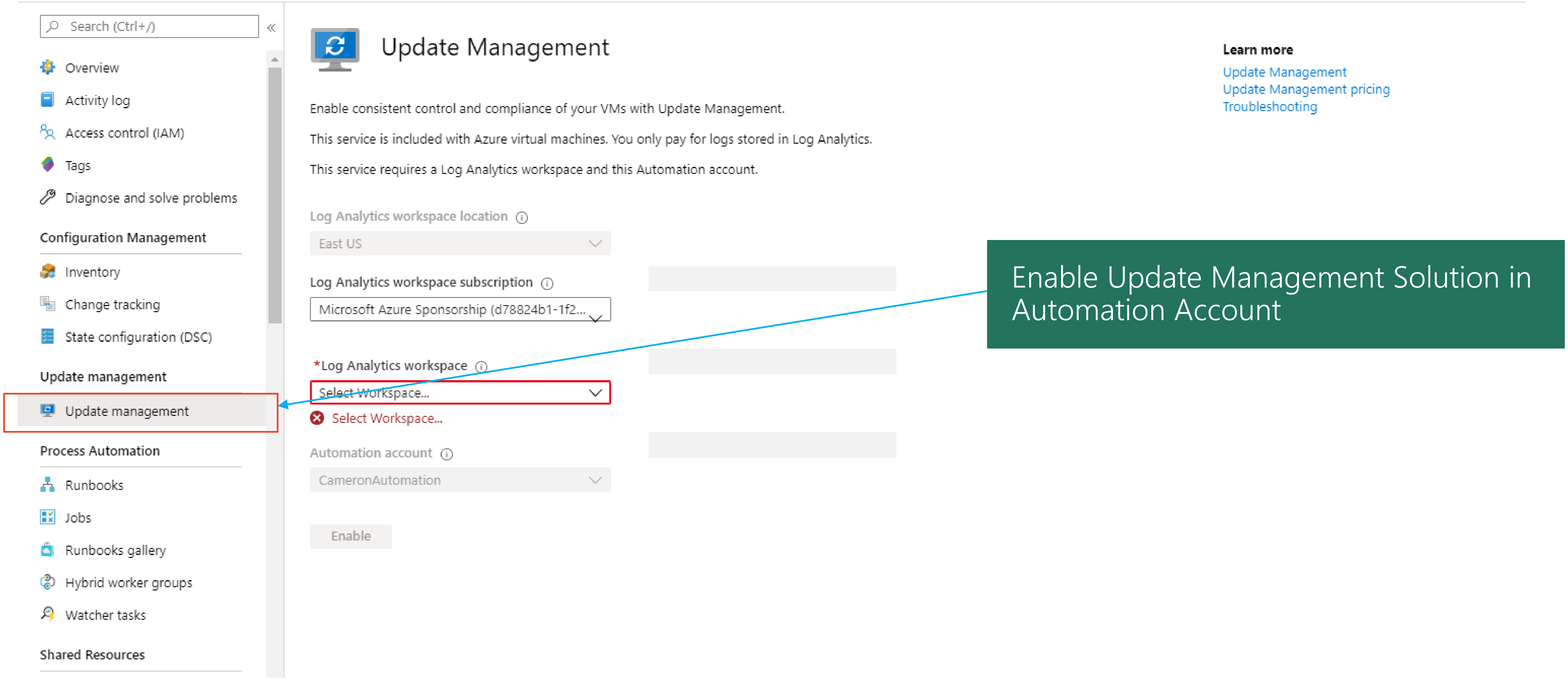
Microsoft Update

Windows Server Update Services (WSUS)

Configuration Manager

Apt-Get/Yum/Zypper

Enable Update Management



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...

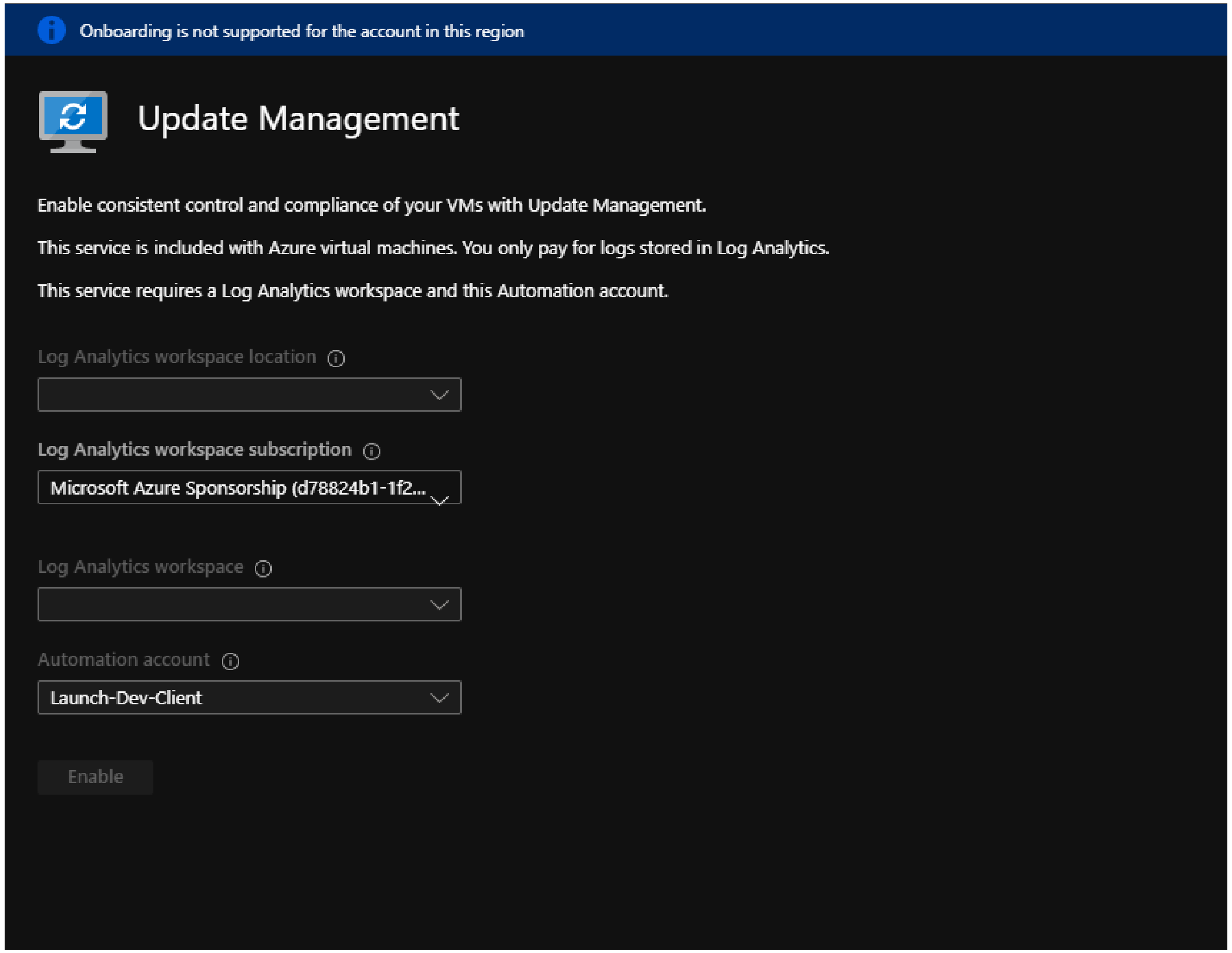
Select Workspace...

Automation account: CameronAutomation

Enable Update Management Solution in Automation Account

Enable Update Management

Log Analytics Workspace Region	Azure Automation Region
US	
East US 1	East US 2
West US 2	West US 2
West Central US 2	West Central US2
Canada	
Canada Central	Canada Central
Asia Pacific	
Australia Southeast	Australia Southeast
Southeast Asia	Southeast Asia
Central India	Central India
Japan East	Japan East
Europe	
UK South	UK South
West Europe	West Europe
US Gov	
US Gov Virginia	US Gov Virginia



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.

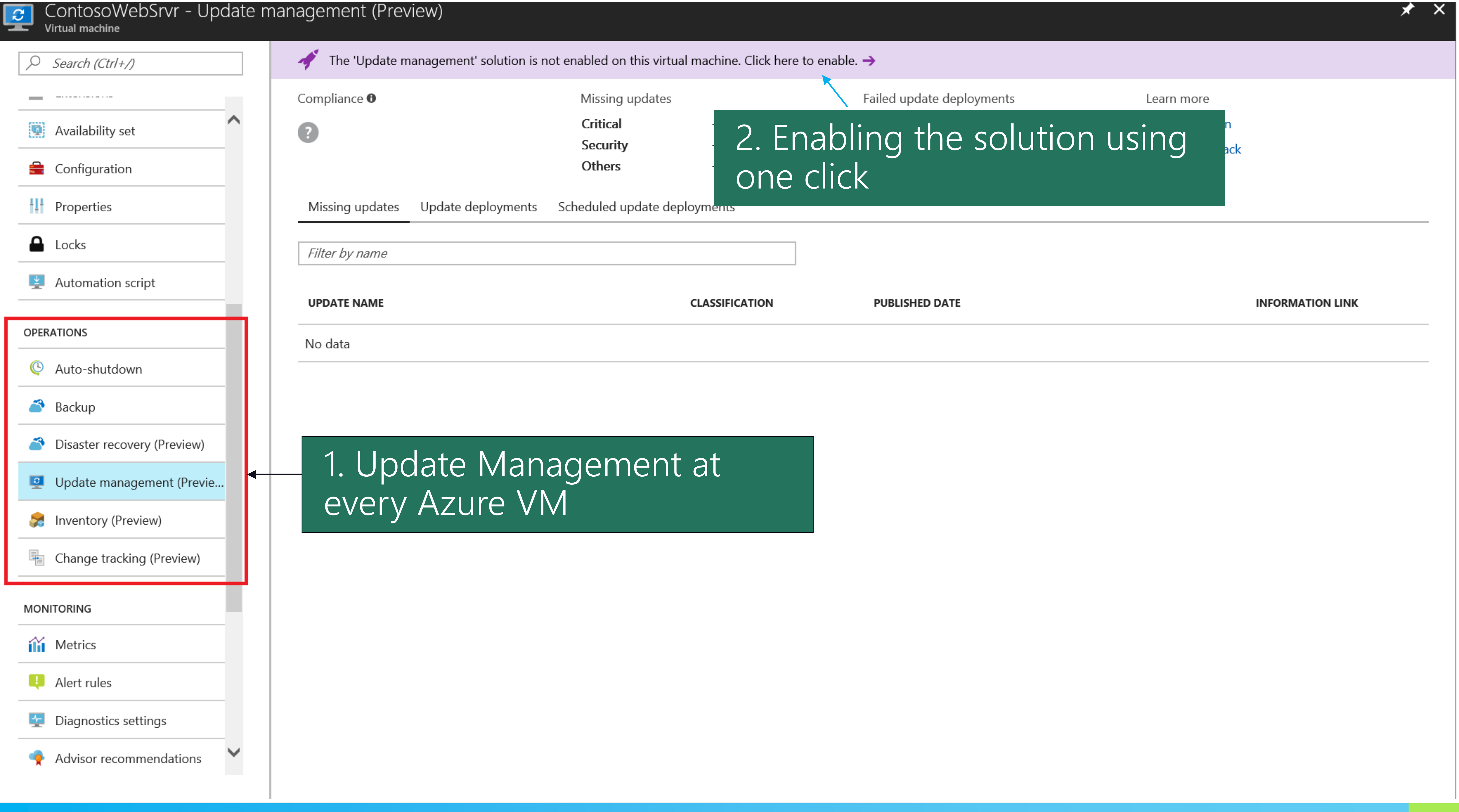
This service requires a Log Analytics workspace and this Automation account.

Log Analytics workspace location

Log Analytics workspace subscription: Microsoft Azure Sponsorship (d78824b1-1f2...

Log Analytics workspace

Automation account: Launch-Dev-Client

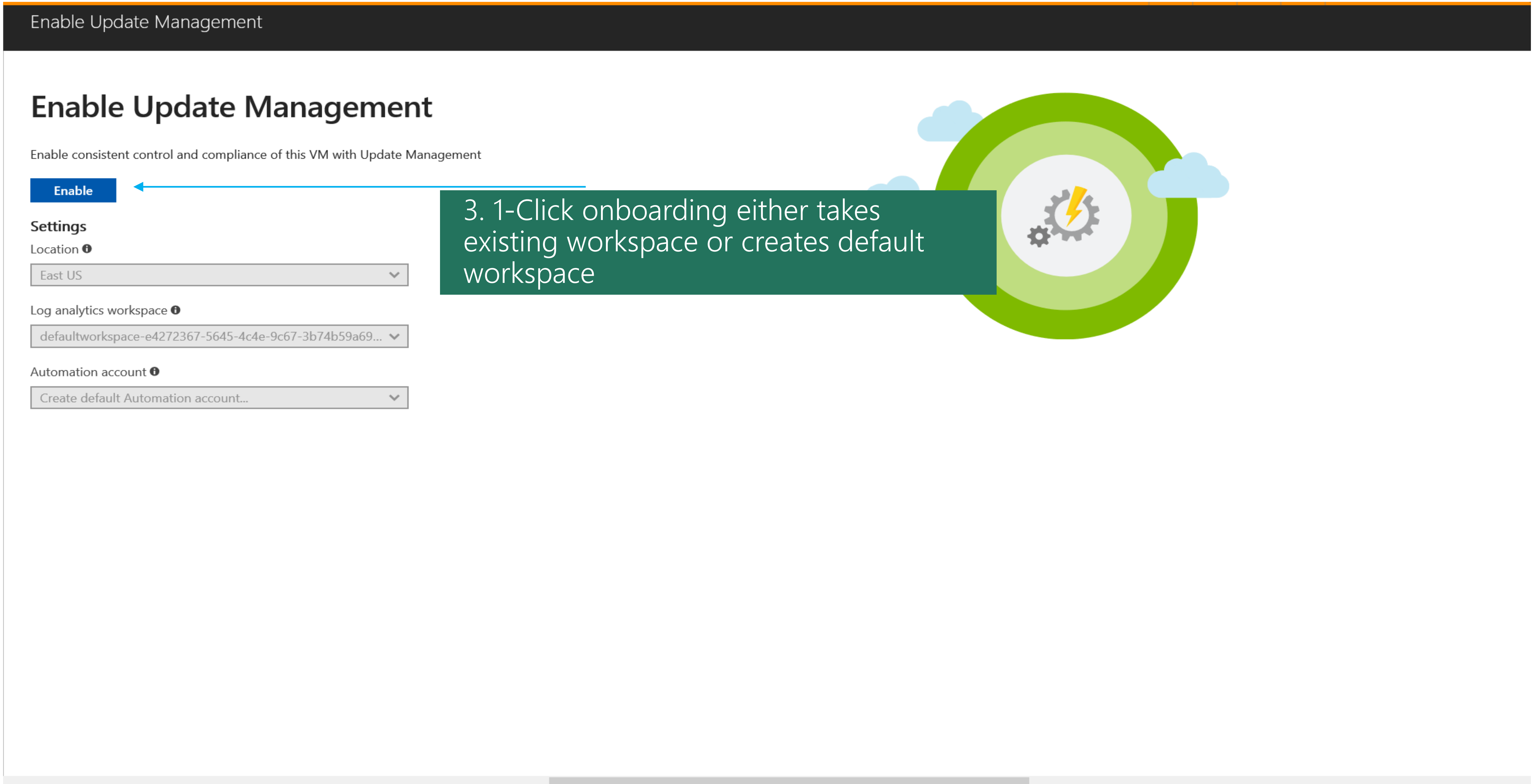


The 'Update management' solution is not enabled on this virtual machine. Click here to enable. →

UPDATE NAME	CLASSIFICATION	PUBLISHED DATE	INFORMATION LINK
No data			

2. Enabling the solution using one click

1. Update Management at every Azure VM



Enable Update Management

Enable consistent control and compliance of this VM with Update Management

Settings

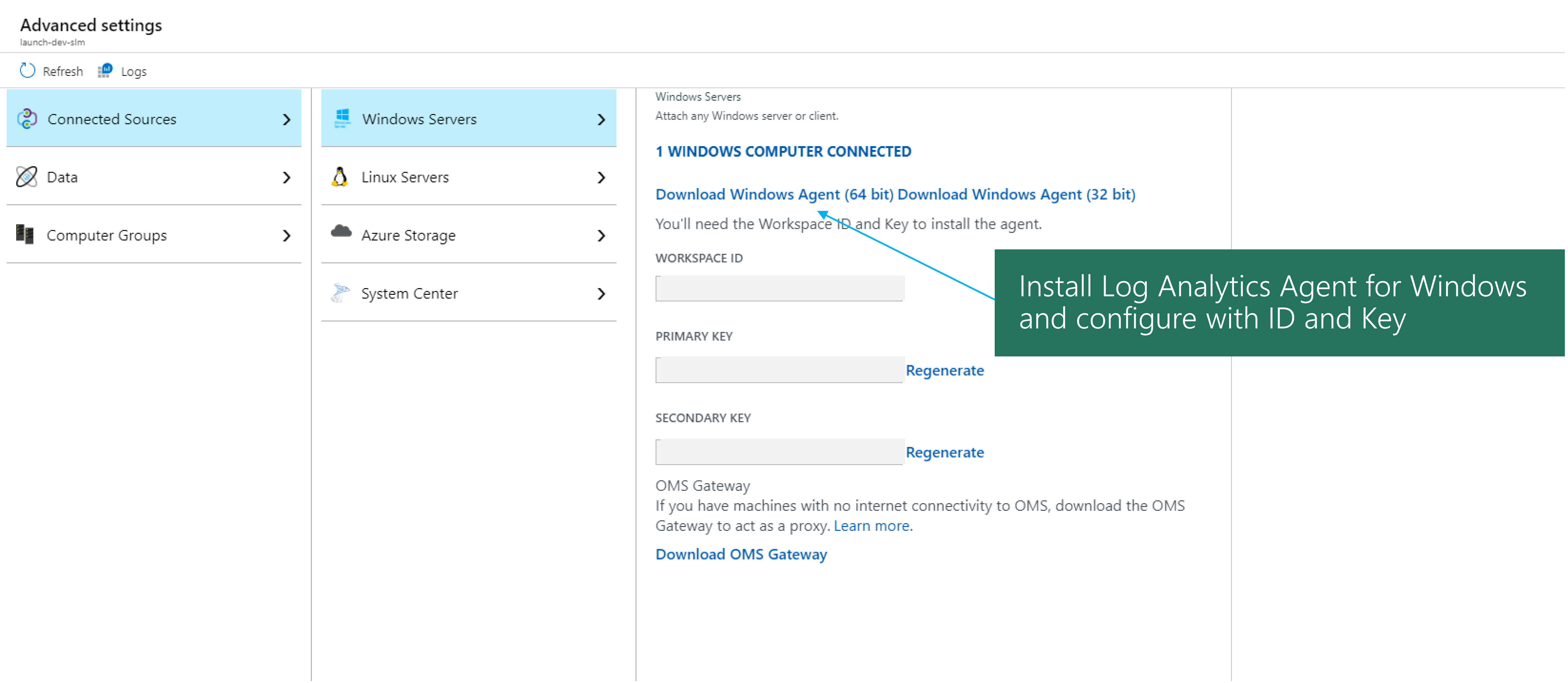
Location: East US

Log analytics workspace: defaultworkspace-e4272367-5645-4c4e-9c67-3b74b59a69...

Automation account: Create default Automation account...

3. 1-Click onboarding either takes existing workspace or creates default workspace

Enable Update Management



Advanced settings

launch-dev-slm

Refresh Logs

- Connected Sources >
- Data >
- Computer Groups >

- Windows Servers >
- Linux Servers >
- Azure Storage >
- System Center >

Windows Servers

Attach any Windows server or client.

1 WINDOWS COMPUTER CONNECTED

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

You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID

PRIMARY KEY

Regenerate

SECONDARY KEY

Regenerate

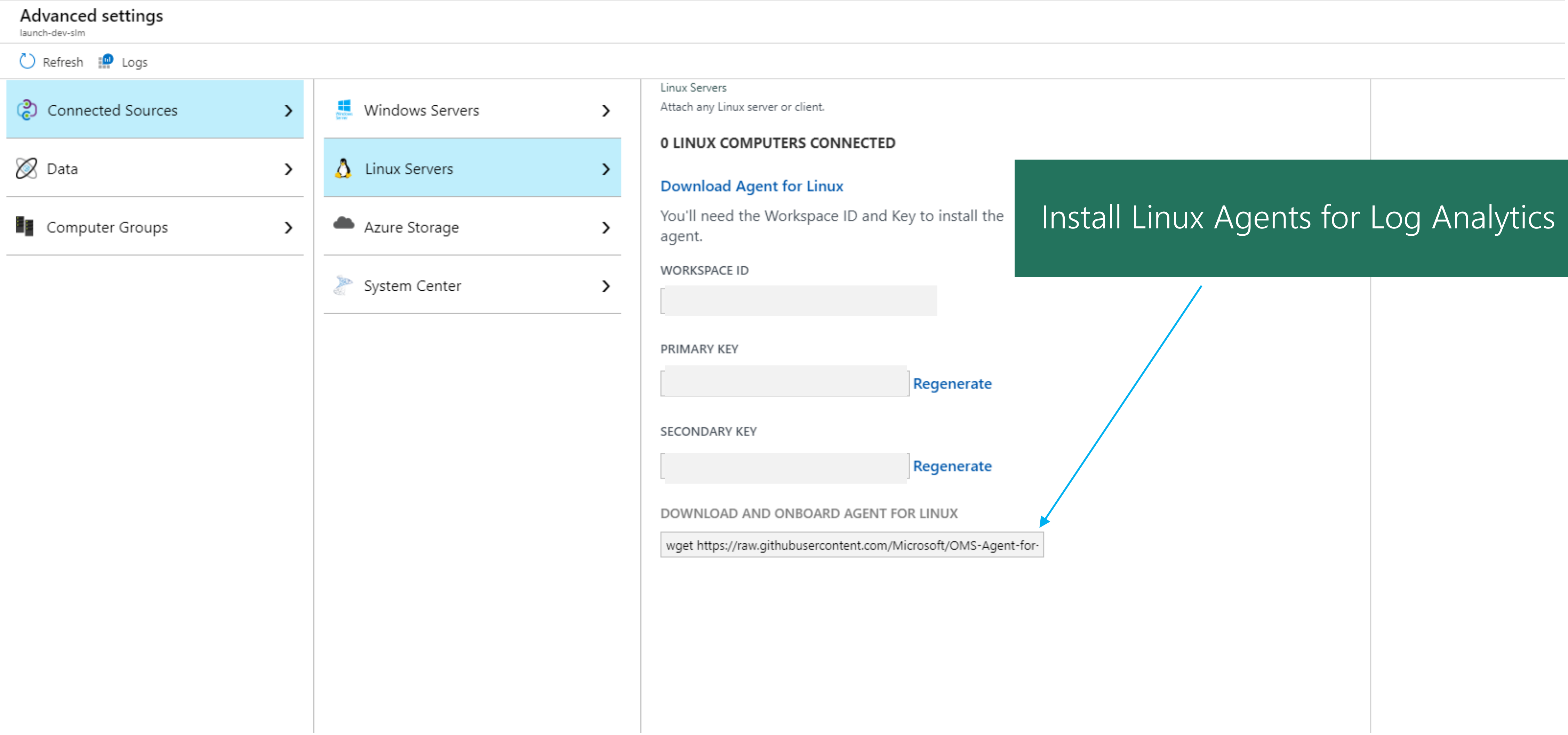
OMS Gateway

If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. Learn more.

Download OMS Gateway

Install Log Analytics Agent for Windows and configure with ID and Key

Enable Update Management



Linux Servers

Attach any Linux server or client.

0 LINUX COMPUTERS CONNECTED

Download Agent for Linux

You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID

PRIMARY KEY

Regenerate

SECONDARY KEY

Regenerate

DOWNLOAD AND ONBOARD AGENT FOR LINUX

```
wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-
```

Install Linux Agents for Log Analytics

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 execption

Troubleshooting Agents

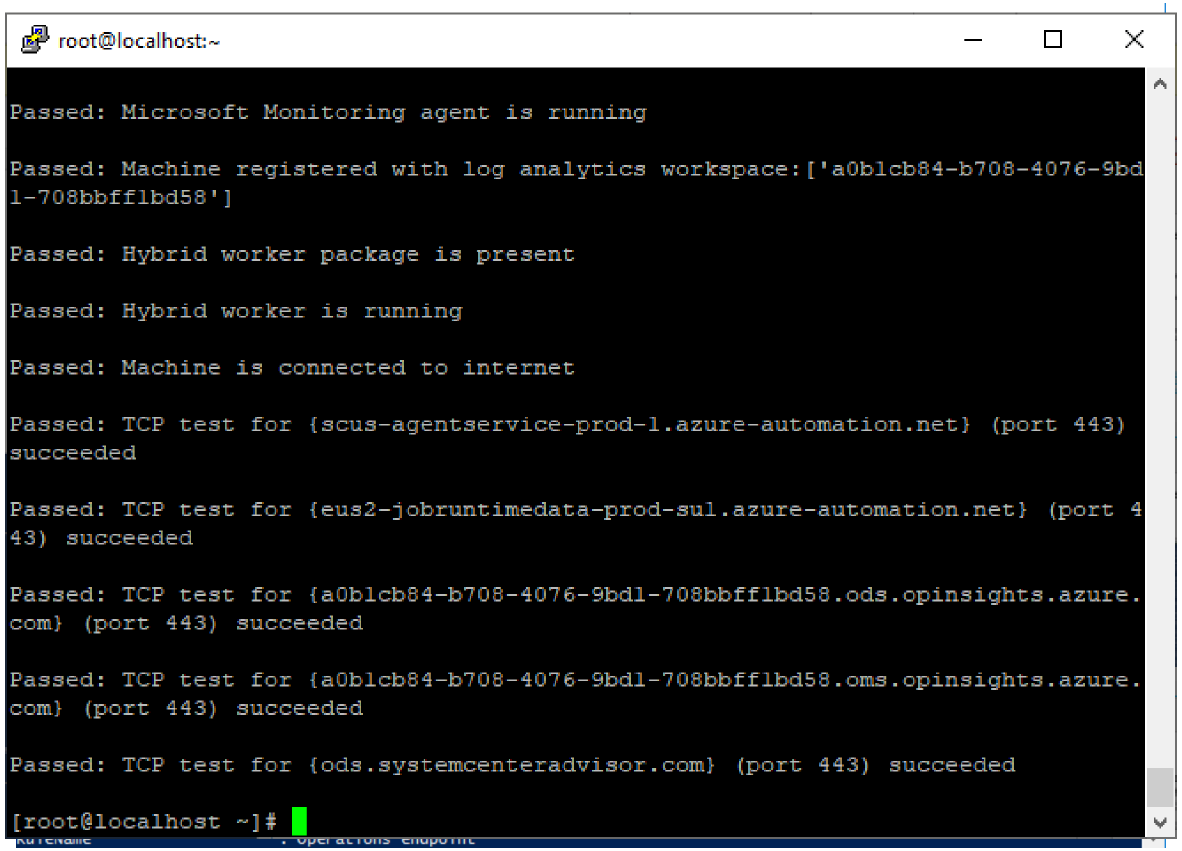
- Confirm Microsoft Monitoring Agent is running and reporting
- Confirm Hybrid Runbook Worker configuration and connection

○ 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



```
Passed: Microsoft Monitoring agent is running

Passed: Machine registered with log analytics workspace:['a0b1cb84-b708-4076-9bd
1-708bbff1bd58']

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-jobruntimedata-prod-su1.azure-automation.net} (port 4
43) 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 ~]#
```

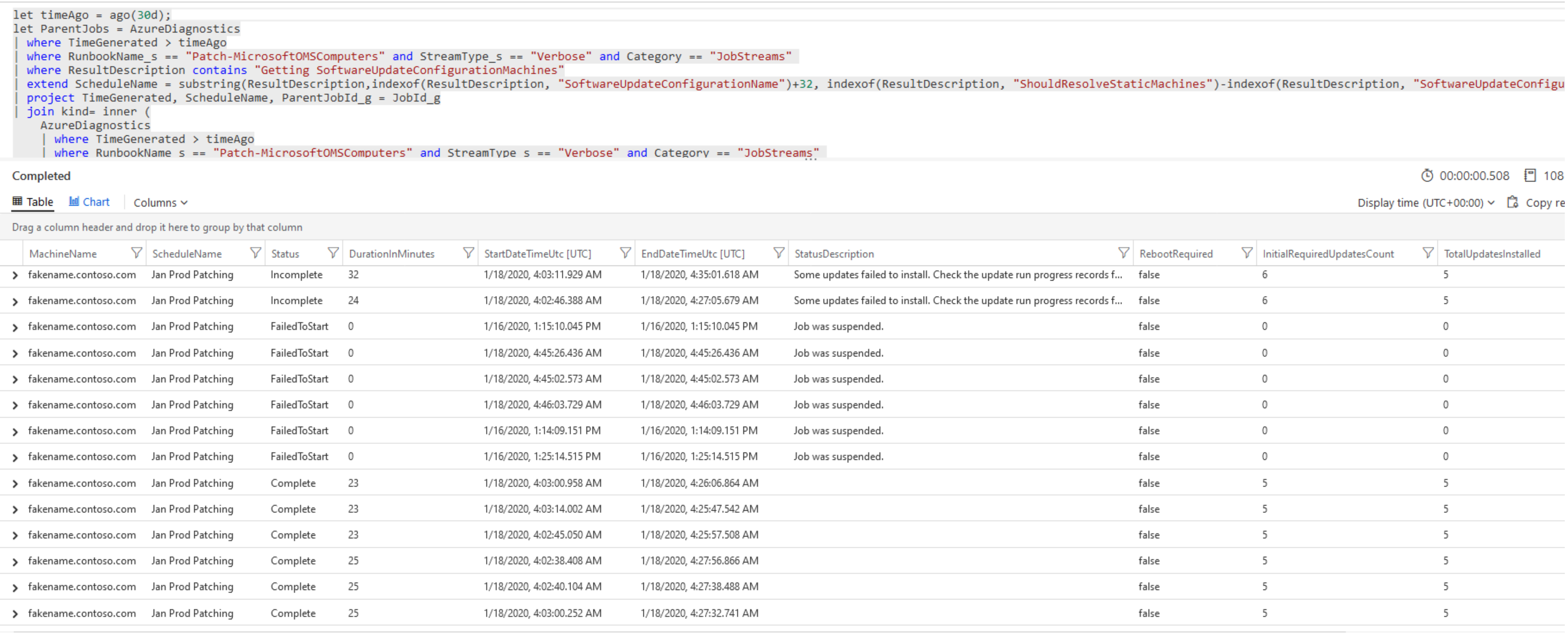
Demo

Monitoring Deployments

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

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.

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

Twitter @mdowst