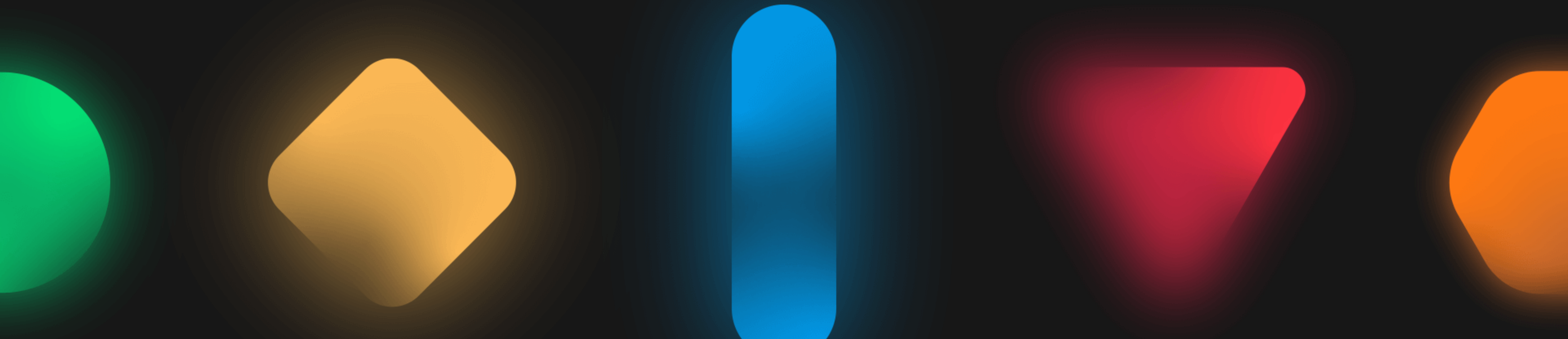
twoday



Cloud-native Server Management: Unleashing the Power of Azure Everywhere

Andreas Sobczyk

Principal Consultant @ twoday A/S

Microsoft Azure MVP

Focus Areas

- Cloud Adoption, Strategy and Architecture
- Cloud Platform engineering and governance
- DevOps & Developer Enablement
- Hybrid Cloud

✉ Andreas.Sobczyk@twoday.com

twoday

Configuration Management

Security

Backup

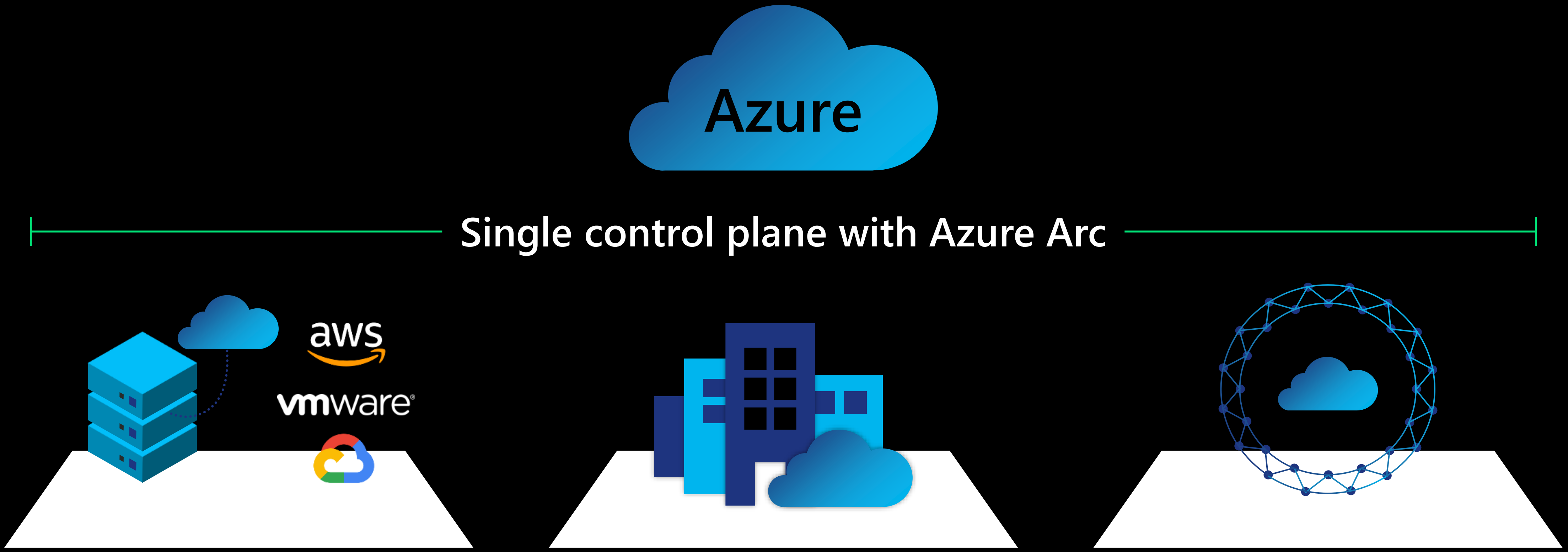
Patch Management

Monitoring

Inventory

Azure Arc

Innovation anywhere with Azure



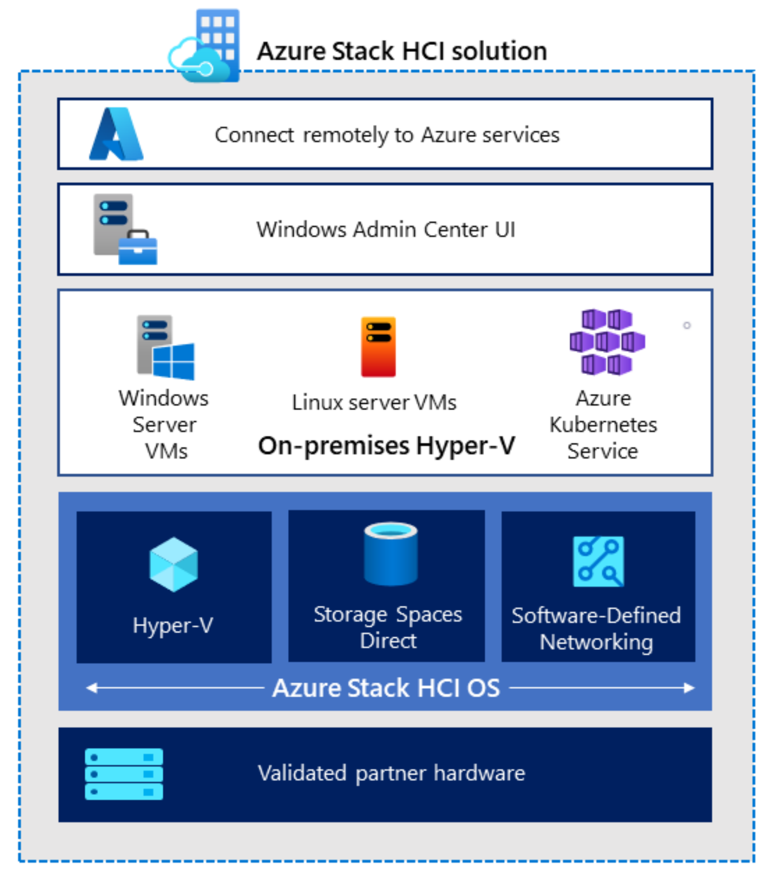
Single control plane with Azure Arc

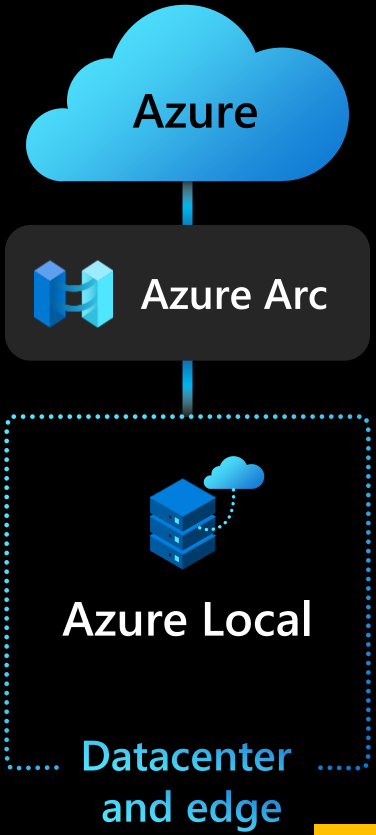
Bring Azure services to any infrastructure

Modernize datacenters with Azure Local

Extend to the edge with Azure IoT

End-to-end hybrid solution with Azure Local





Hybrid by design with Azure Arc

Enterprise scale and great price-performance

Flexible for VMs and cloud-native with AKS

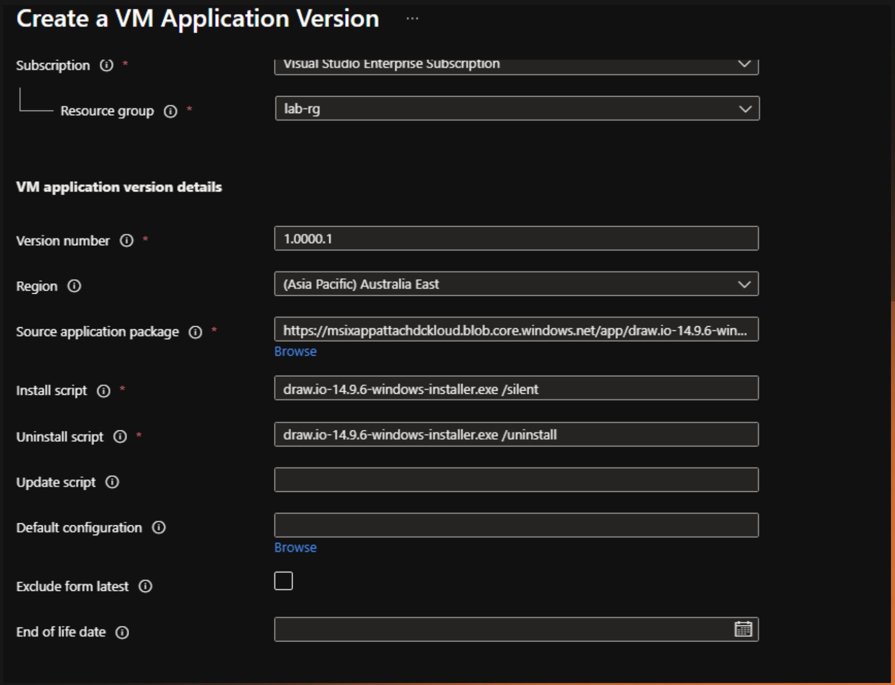
Familiar management and deployment

Cost:

Hardware starting at: ~180.000 NOK
Software: 10$ (+ 23$ for Windows) per/pCore OR WS Datacenter /w SA

Configuration Management

- Azure Policies
  - GPOs for the cloud, just better
  - **Audit**, **Deny** or **Deploy/Configure** ANY setting in the Azure control plane
    And inside Guest OS
  - Machine configurations powered by PowerShell DSC V2
- VM Applications – only for Azure VMs.. For now

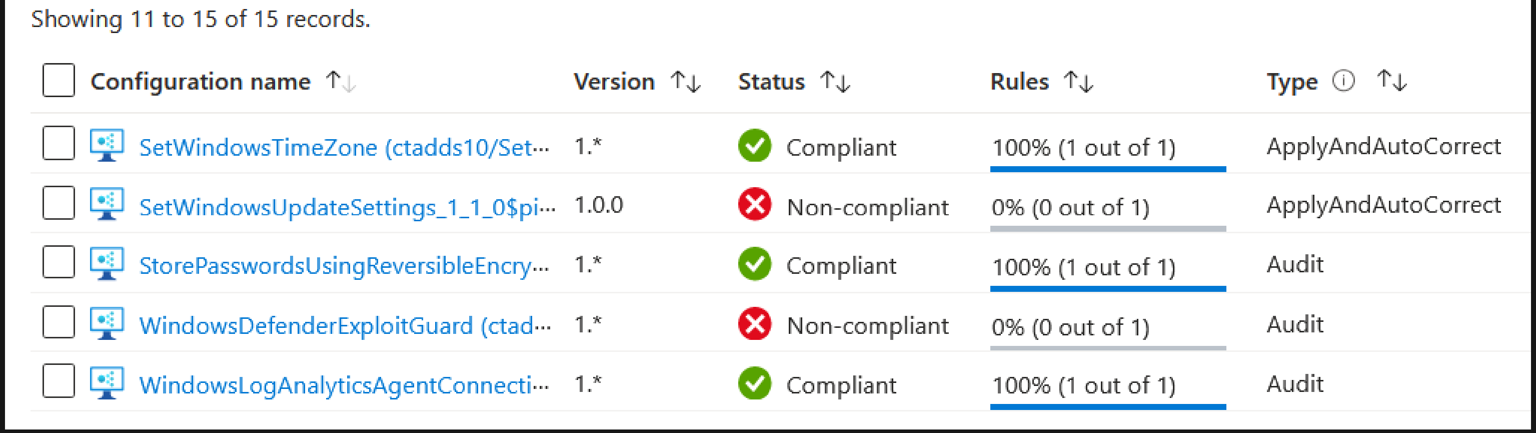


Create a VM Application Version ···

Subscription ⓘ *	Visual Studio Enterprise Subscription
Resource group ⓘ *	lab-rg

VM application version details

Version number ⓘ *	1.0000.1
Region ⓘ	(Asia Pacific) Australia East
Source application package ⓘ *	https://msixappattachdckloud.blob.core.windows.net/app/draw.io-14.9.6-win... Browse
Install script ⓘ *	draw.io-14.9.6-windows-installer.exe /silent
Uninstall script ⓘ *	draw.io-14.9.6-windows-installer.exe /uninstall
Update script ⓘ	
Default configuration ⓘ	Browse
Exclude form latest ⓘ	□
End of life date ⓘ	



Showing 11 to 15 of 15 records.

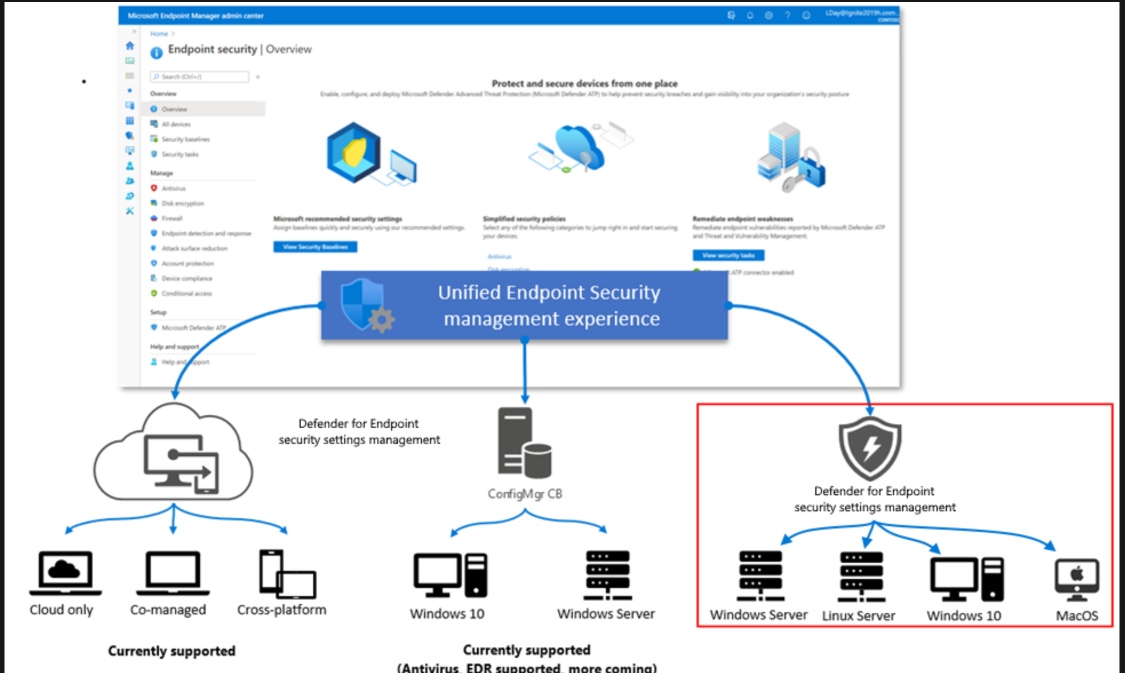
□ Configuration name ↑↓	Version ↑↓	Status ↑↓	Rules ↑↓	Type ⓘ ↑↓
□ SetWindowsTimeZone (ctadds10/Set...	1.*	✓ Compliant	100% (1 out of 1)	ApplyAndAutoCorrect
□ SetWindowsUpdateSettings_1_1_0$pi...	1.0.0	✗ Non-compliant	0% (0 out of 1)	ApplyAndAutoCorrect
□ StorePasswordsUsingReversibleEncry...	1.*	✓ Compliant	100% (1 out of 1)	Audit
□ WindowsDefenderExploitGuard (ctad...	1.*	✗ Non-compliant	0% (0 out of 1)	Audit
□ WindowsLogAnalyticsAgentConnecti...	1.*	✓ Compliant	100% (1 out of 1)	Audit

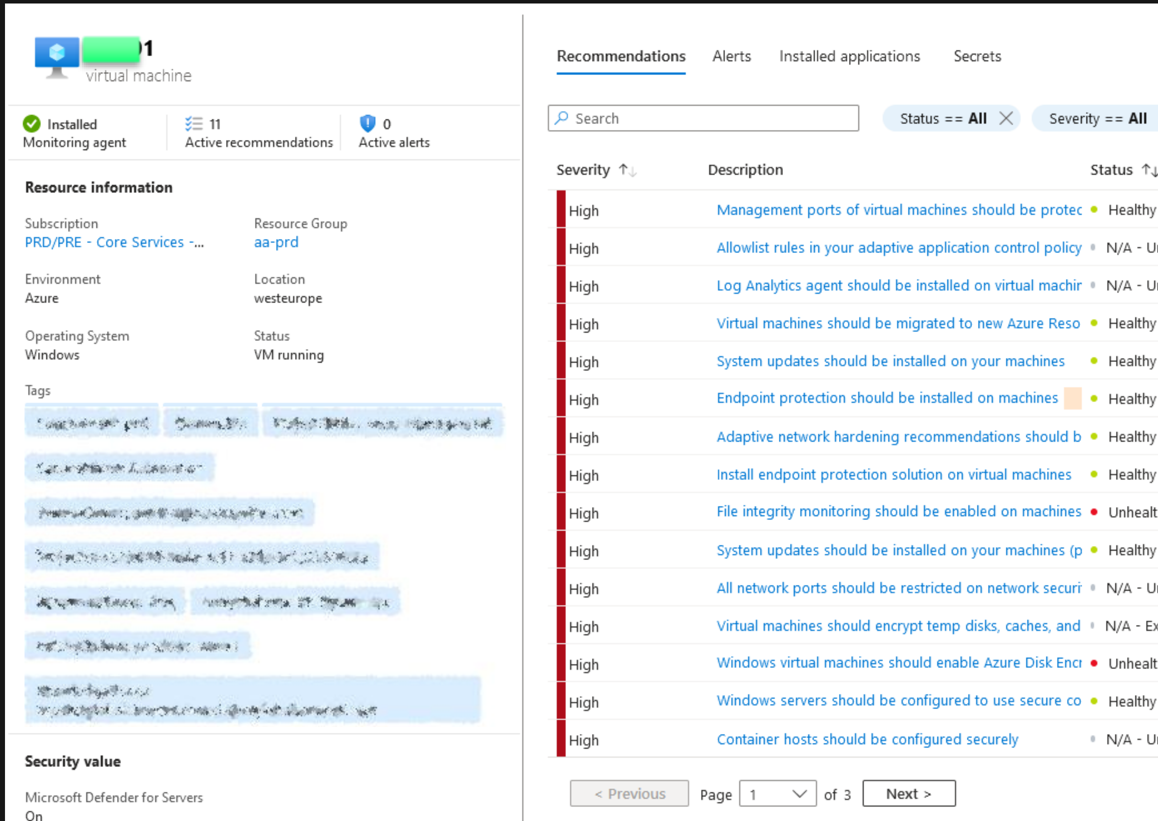
Security

Azure Policies:

- Deploy Microsoft Defender for Endpoint agent
- Audit Defender for Endpoint Onboarding (custom)

- Defender for Cloud
  - Defender for Endpoint with vulnerability assessment
    - Deploy and audit with Azure policies
    - Central control from Defender with Intune
- Azure Policy – Security baseline


Microsoft Endpoint Manager admin center
Endpoint security | Overview
Protect and secure devices from one place
Microsoft recommended security settings
Simplified security policies
Remediate endpoint weaknesses
Unified Endpoint Security management experience
Defender for Endpoint security settings management
ConfigMgr CB
Defender for Endpoint security settings management
Cloud only
Co-managed
Cross-platform
Windows 10
Windows Server
Windows Server
Linux Server
Windows 10
MacOS
Currently supported
Currently supported
(Antivirus, EDR supported, more coming)



[redacted]1
virtual machine

Installed
Monitoring agent

11
Active recommendations

0
Active alerts

Resource information

Subscription PRD/PRE - Core Services -...	Resource Group aa-prd
Environment Azure	Location westeurope
Operating System Windows	Status VM running

Tags

[redacted]

Security value

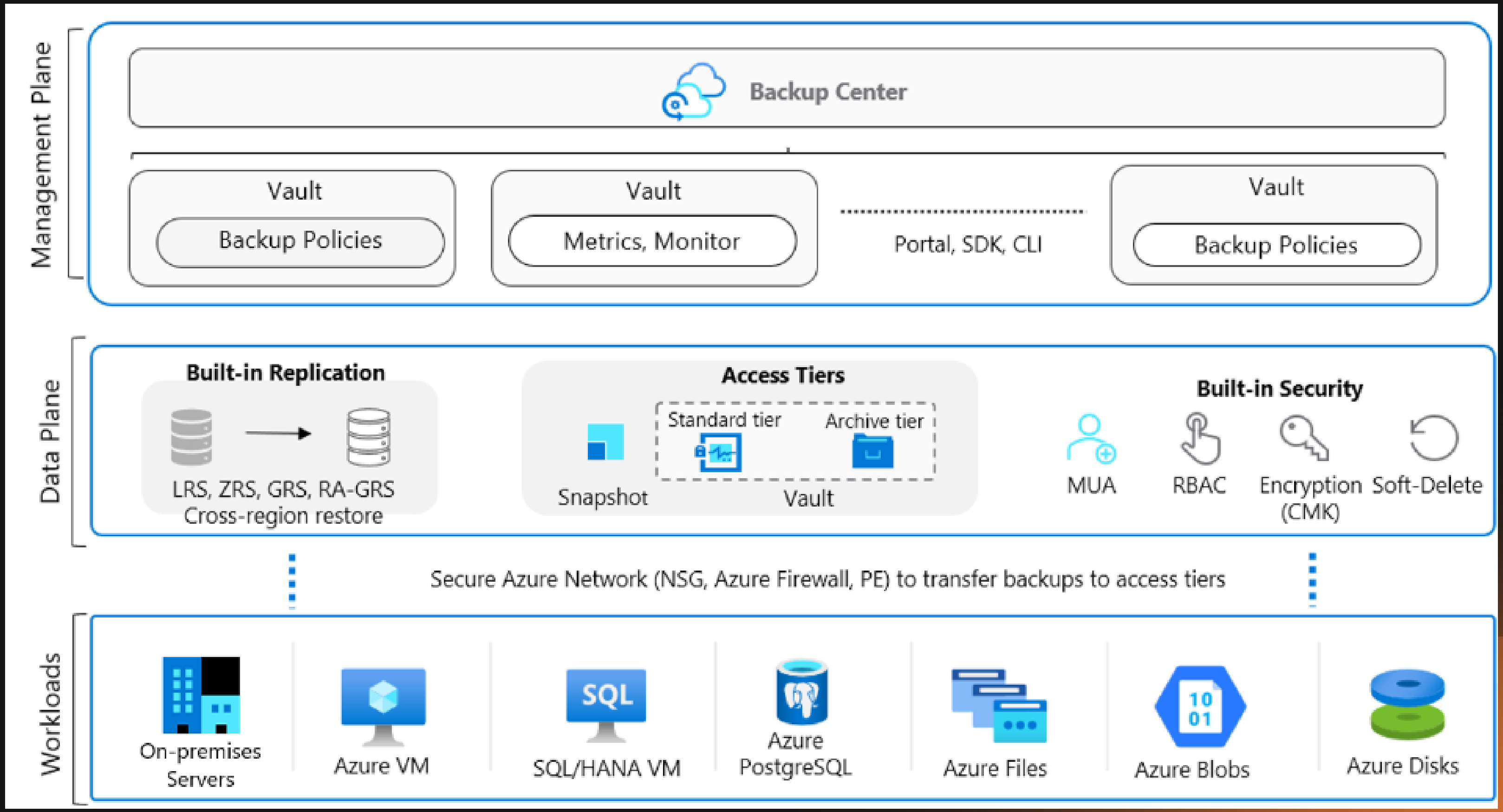
Microsoft Defender for Servers
On

Severity	Description	Status
High	Management ports of virtual machines should be protec	● Healthy
High	Allowlist rules in your adaptive application control policy	● N/A - U
High	Log Analytics agent should be installed on virtual machir	● N/A - U
High	Virtual machines should be migrated to new Azure Reso	● Healthy
High	System updates should be installed on your machines	● Healthy
High	Endpoint protection should be installed on machines	● Healthy
High	Adaptive network hardening recommendations should b	● Healthy
High	Install endpoint protection solution on virtual machines	● Healthy
High	File integrity monitoring should be enabled on machines	● Unhealt
High	System updates should be installed on your machines (p	● Healthy
High	All network ports should be restricted on network securi	● N/A - U
High	Virtual machines should encrypt temp disks, caches, and	● N/A - Ex
High	Windows virtual machines should enable Azure Disk Encı	● Unhealt
High	Windows servers should be configured to use secure co	● Healthy
High	Container hosts should be configured securely	● N/A - U

< Previous Page 1 of 3 Next >

Backup – Azure Backup Services

- Zero Maintenance
- Highly Secure
- Policy-driven
- Central Management



Management Plane

Backup Center

Vault

Backup Policies

Vault

Metrics, Monitor

Portal, SDK, CLI

Vault

Backup Policies

Data Plane

Built-in Replication

LRS, ZRS, GRS, RA-GRS
Cross-region restore

Access Tiers

Snapshot

Standard tier

Archive tier

Vault

Built-in Security

MUA

RBAC

Encryption (CMK)

Soft-Delete

Secure Azure Network (NSG, Azure Firewall, PE) to transfer backups to access tiers

Workloads

On-premises Servers

Azure VM

SQL/HANA VM

Azure PostgreSQL

Azure Files

Azure Blobs

Azure Disks

Backup – Recovery Vaults

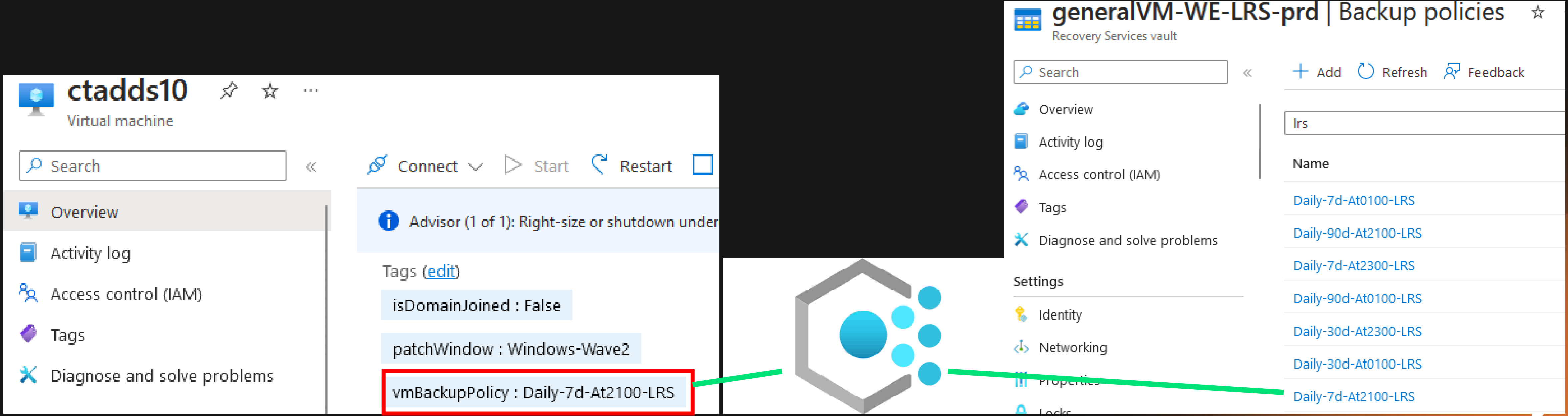
- Vaults
  - Subscriptions x Regions x Redundancy Type
  - Tiering to Archive
- Backup Policies
  - VMs - Instant recovery
  - SQL Backup for Azure VMs
- Security
  - Soft delete - Always-on
  - Resource Guard – protect critical operations
  - Disable Cross Subscription Restore
  - Immutable
    - Lock

Onboarding and Auditing

- Use tags to define backup policy for a VM
- Azure policies to apply backup policy job
  - Deploy & Audit

Azure Policies:

- Azure Backup should be enabled for Virtual Machines
- Configure backup on virtual machines with a given tag to……
- Audit Backup Policy tag (custom)
- Enable Azure Backup on VMs based on tag value (custom)



ctadds10

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect   Start   Restart

Advisor (1 of 1): Right-size or shutdown under

Tags (edit)

isDomainJoined : False

patchWindow : Windows-Wave2

vmBackupPolicy : Daily-7d-At2100-LRS

generalVM-WE-LRS-prd | Backup policies

Recovery Services vault

Search

Add   Refresh   Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Identity

Networking

Properties

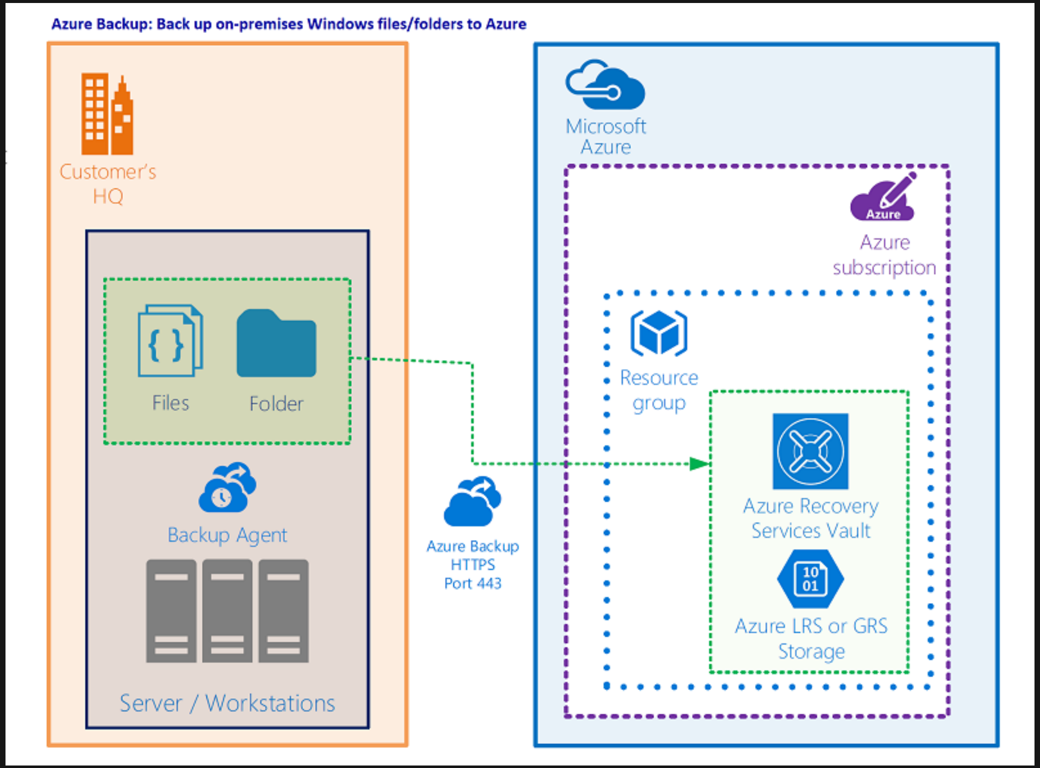
Locks

lrs

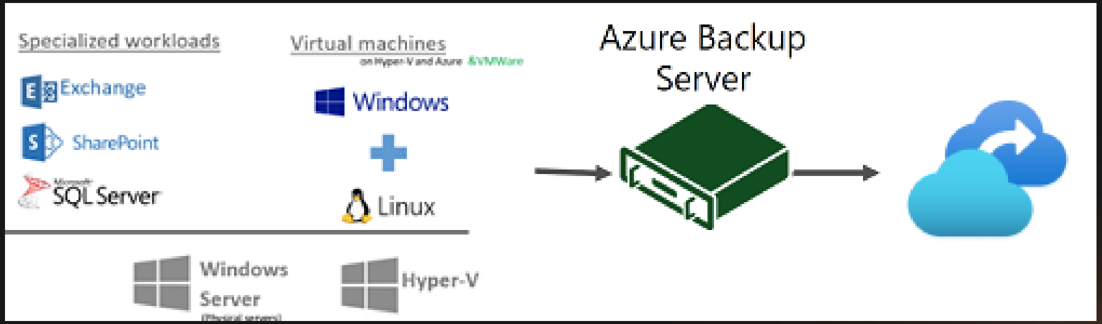
Name
Daily-7d-At0100-LRS
Daily-90d-At2100-LRS
Daily-7d-At2300-LRS
Daily-90d-At0100-LRS
Daily-30d-At2300-LRS
Daily-30d-At0100-LRS
Daily-7d-At2100-LRS

Backup On-premises

Microsoft Azure Recovery Services (MARS) – Agent per machine



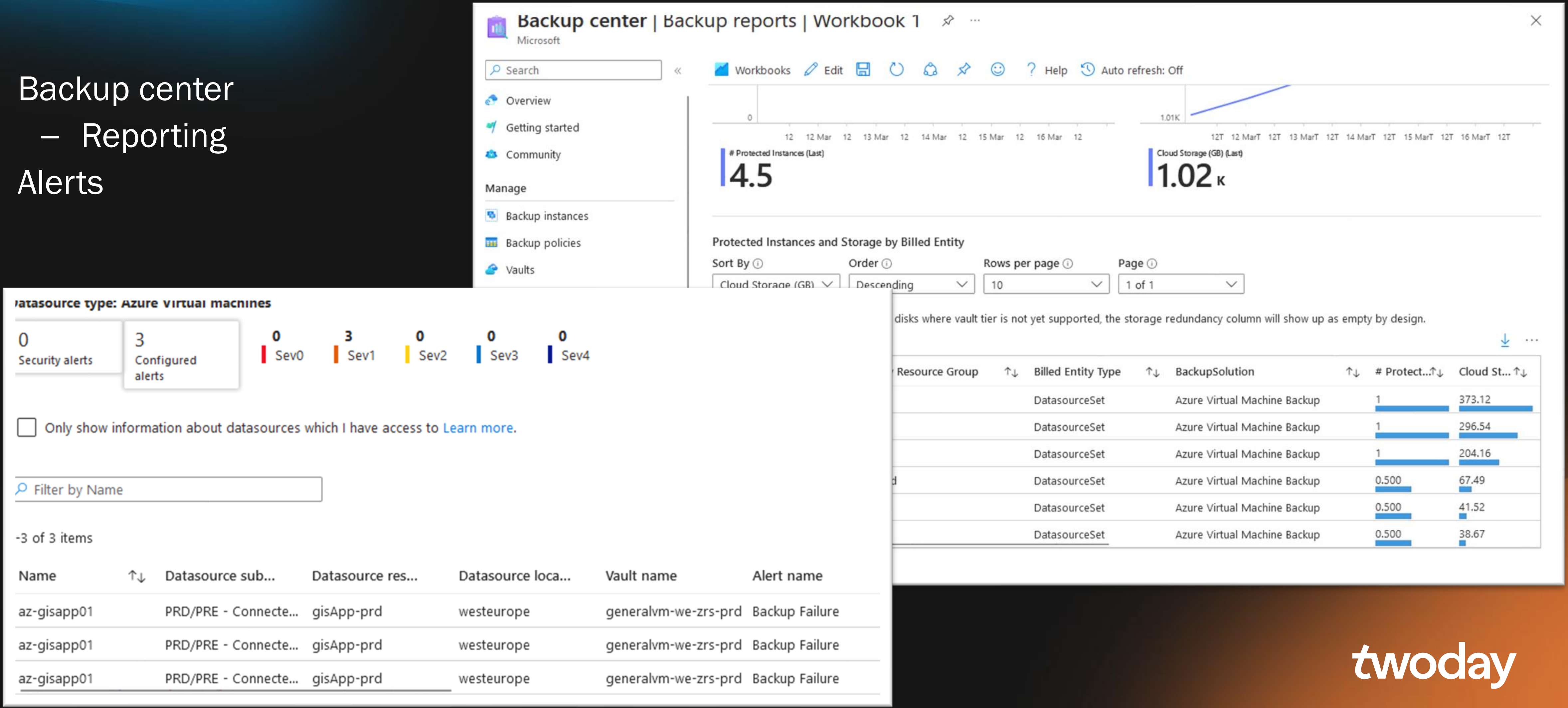
Microsoft Azure Backup Server (MABS) – Central server, local storage, tier to cloud



twoday

Backup – Monitoring and reporting

- Backup center
  - Reporting
- Alerts



Backup center | Backup reports | Workbook 1

Microsoft

Protected Instances (Last) 4.5

Cloud Storage (GB) (Last) 1.02 K

Protected Instances and Storage by Billed Entity

Sort By: Cloud Storage (GB)

Order: Descending

Rows per page: 10

Page: 1 of 1

disks where vault tier is not yet supported, the storage redundancy column will show up as empty by design.

Resource Group	Billed Entity Type	BackupSolution	# Protect...	Cloud St...
	DatasourceSet	Azure Virtual Machine Backup	1	373.12
	DatasourceSet	Azure Virtual Machine Backup	1	296.54
	DatasourceSet	Azure Virtual Machine Backup	1	204.16
d	DatasourceSet	Azure Virtual Machine Backup	0.500	67.49
	DatasourceSet	Azure Virtual Machine Backup	0.500	41.52
	DatasourceSet	Azure Virtual Machine Backup	0.500	38.67

atasource type: Azure Virtual machines

0 Security alerts

3 Configured alerts

0	3	0	0	0
Sev0	Sev1	Sev2	Sev3	Sev4

□ Only show information about datasources which I have access to Learn more.

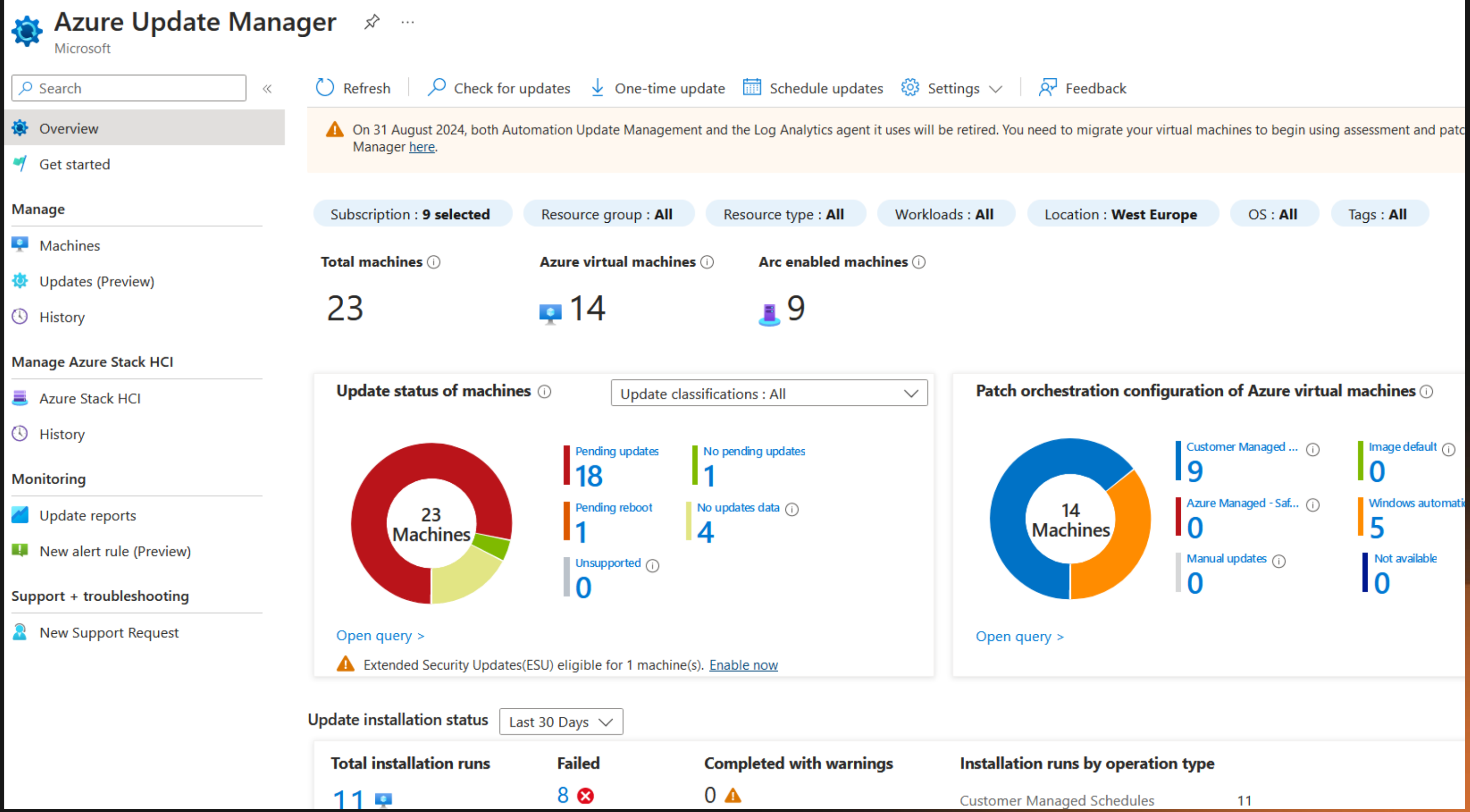
Filter by Name

-3 of 3 items

Name	Datasource sub...	Datasource res...	Datasource loca...	Vault name	Alert name
az-gisapp01	PRD/PRE - Connecte...	gisApp-prd	westeurope	generalvm-we-zrs-prd	Backup Failure
az-gisapp01	PRD/PRE - Connecte...	gisApp-prd	westeurope	generalvm-we-zrs-prd	Backup Failure
az-gisapp01	PRD/PRE - Connecte...	gisApp-prd	westeurope	generalvm-we-zrs-prd	Backup Failure

Patch Management

- No special agents
- Cross Platform
- Schedule Update
- On-demand Update



Azure Update Manager

Microsoft

On 31 August 2024, both Automation Update Management and the Log Analytics agent it uses will be retired. You need to migrate your virtual machines to begin using assessment and patc
Manager here.

Subscription : **9 selected** | Resource group : **All** | Resource type : **All** | Workloads : **All** | Location : **West Europe** | OS : **All** | Tags : **All**

Total machines	Azure virtual machines	Arc enabled machines
23	14	9

Update status of machines

Update classifications : All

Pending updates 18	No pending updates 1
Pending reboot 1	No updates data 4
Unsupported 0	

Open query >

Extended Security Updates(ESU) eligible for 1 machine(s). Enable now

Patch orchestration configuration of Azure virtual machines

Customer Managed ... 9	Image default 0
Azure Managed - Saf... 0	Windows automati 5
Manual updates 0	Not available 0

Open query >

Update installation status

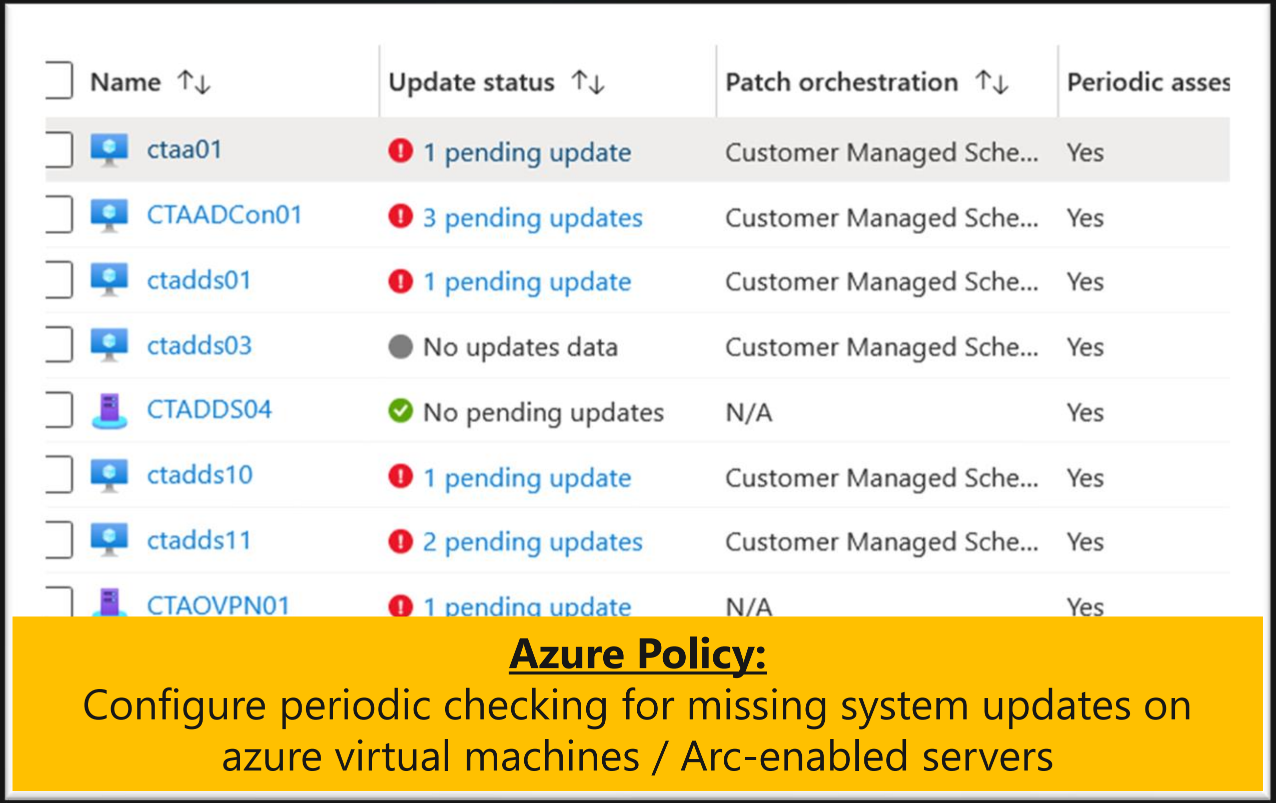
Last 30 Days

Total installation runs	Failed	Completed with warnings	Installation runs by operation type
11	8	0	Customer Managed Schedules 11

twoday

Assessment & Schedules

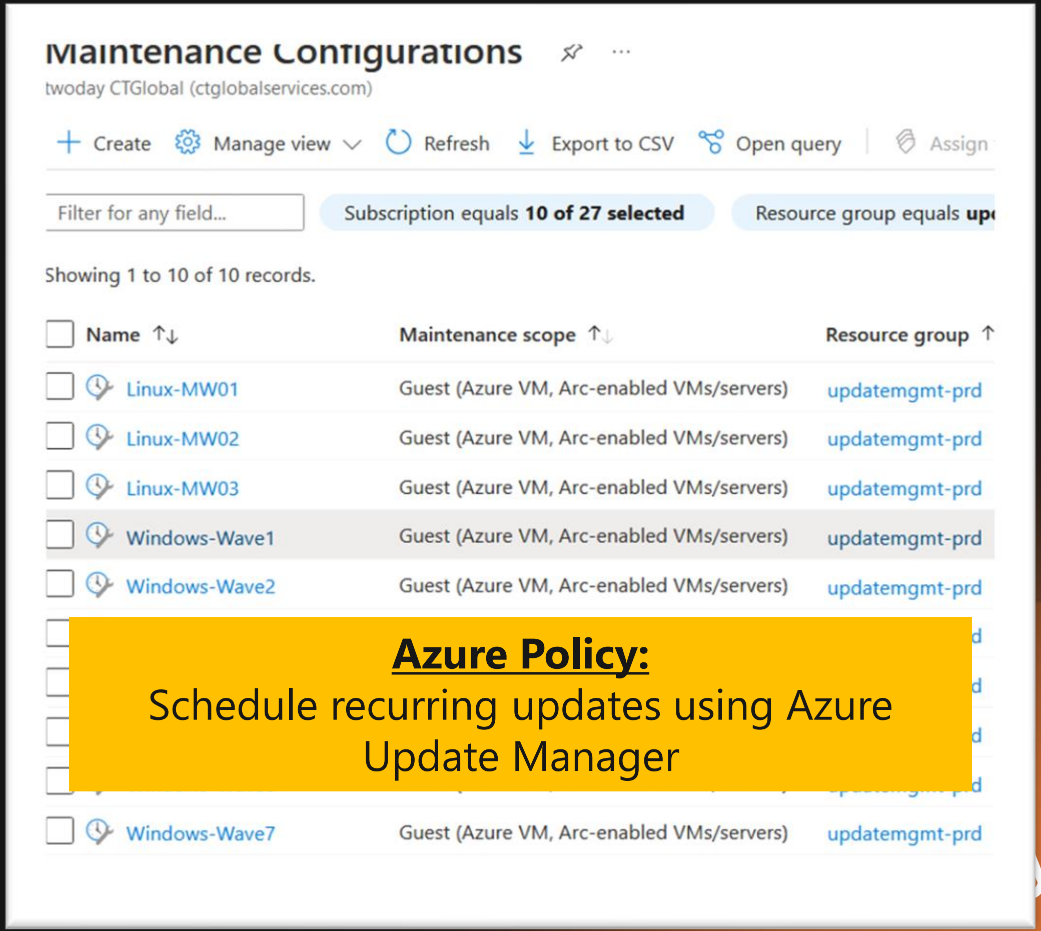
Periodic Assessment



□ Name ↑↓	Update status ↑↓	Patch orchestration ↑↓	Periodic asses
□ ctaa01	! 1 pending update	Customer Managed Sche...	Yes
□ CTAADCon01	! 3 pending updates	Customer Managed Sche...	Yes
□ ctadds01	! 1 pending update	Customer Managed Sche...	Yes
□ ctadds03	● No updates data	Customer Managed Sche...	Yes
□ CTADDS04	✓ No pending updates	N/A	Yes
□ ctadds10	! 1 pending update	Customer Managed Sche...	Yes
□ ctadds11	! 2 pending updates	Customer Managed Sche...	Yes
□ CTAOVPN01	! 1 pending update	N/A	Yes

Azure Policy:
Configure periodic checking for missing system updates on azure virtual machines / Arc-enabled servers

Maintenance Schedule



Maintenance Configurations

twoday CTGlobal (ctglobalservices.com)

Filter for any field...

Subscription equals **10 of 27 selected**

Resource group equals **upd**

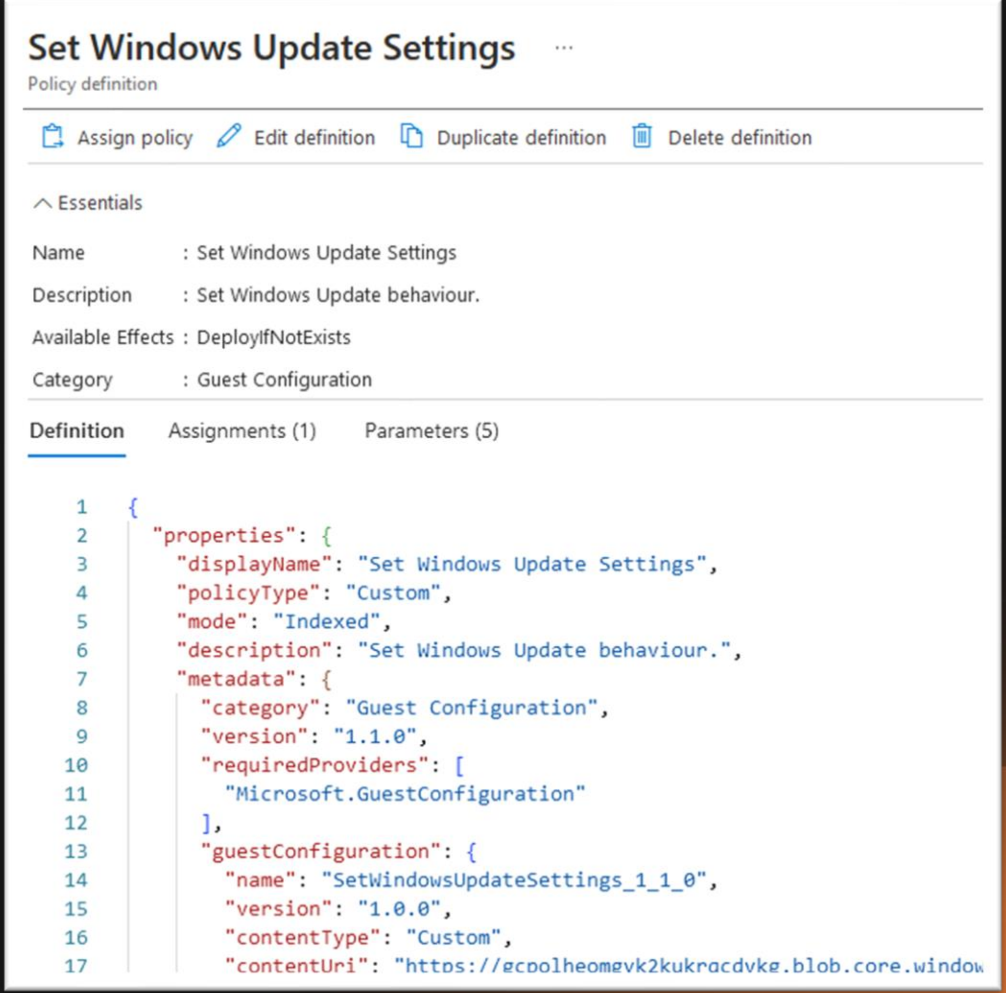
Showing 1 to 10 of 10 records.

□ Name ↑↓	Maintenance scope ↑↓	Resource group ↑
□ Linux-MW01	Guest (Azure VM, Arc-enabled VMs/servers)	updatemgmt-prd
□ Linux-MW02	Guest (Azure VM, Arc-enabled VMs/servers)	updatemgmt-prd
□ Linux-MW03	Guest (Azure VM, Arc-enabled VMs/servers)	updatemgmt-prd
□ Windows-Wave1	Guest (Azure VM, Arc-enabled VMs/servers)	updatemgmt-prd
□ Windows-Wave2	Guest (Azure VM, Arc-enabled VMs/servers)	updatemgmt-prd
□ Windows-Wave7	Guest (Azure VM, Arc-enabled VMs/servers)	updatemgmt-prd

Azure Policy:
Schedule recurring updates using Azure Update Manager

Windows Update settings

- Control Windows update behavior with Azure Policies
  - AUOptions – Update/Download setting
  - NoAutoUpdate – OS Installation
  - WUServer – WSUS Server
  - EnableMicrosoftUpdate – Other Microsoft Updates, SQL etc…



Name : Set Windows Update Settings

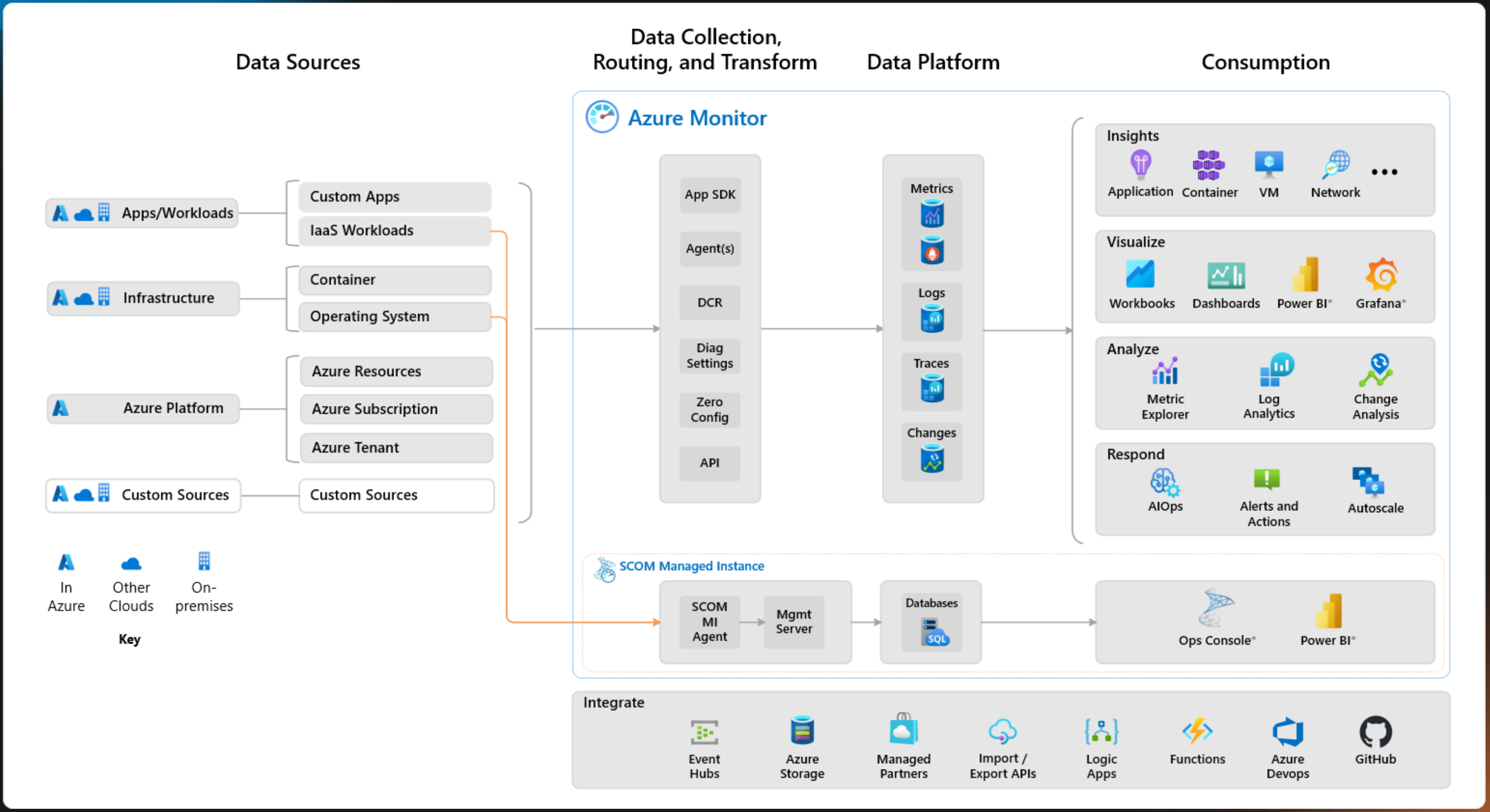
Description : Set Windows Update behaviour.

Available Effects : DeployIfNotExists

Category : Guest Configuration

```
{
  "properties": {
    "displayName": "Set Windows Update Settings",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "Set Windows Update behaviour.",
    "metadata": {
      "category": "Guest Configuration",
      "version": "1.1.0",
      "requiredProviders": [
        "Microsoft.GuestConfiguration"
      ],
      "guestConfiguration": {
        "name": "SetWindowsUpdateSettings_1_1_0",
        "version": "1.0.0",
        "contentType": "Custom",
        "contentUri": "https://gcpolheomgvk2kukracdvkg.blob.core.window
```

Monitoring



Data Sources

Data Collection, Routing, and Transform

Data Platform

Consumption

Apps/Workloads

- Custom Apps
- IaaS Workloads

Infrastructure

- Container
- Operating System

Azure Platform

- Azure Resources
- Azure Subscription
- Azure Tenant

Custom Sources

- Custom Sources

Key: In Azure, Other Clouds, On-premises

Azure Monitor

App SDK, Agent(s), DCR, Diag Settings, Zero Config, API

Metrics, Logs, Traces, Changes

Insights: Application, Container, VM, Network, ...

Visualize: Workbooks, Dashboards, Power BI*, Grafana*

Analyze: Metric Explorer, Log Analytics, Change Analysis

Respond: AIOps, Alerts and Actions, Autoscale

SCOM Managed Instance

SCOM MI Agent → Mgmt Server → Databases (SQL) → Ops Console*, Power BI*

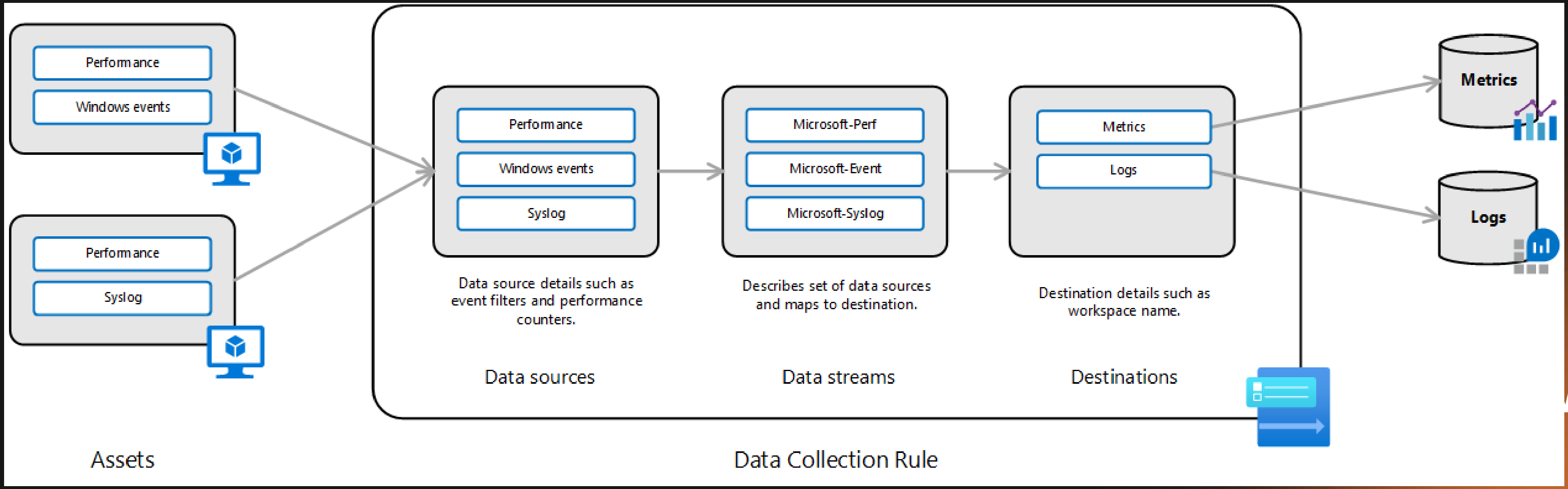
Integrate: Event Hubs, Azure Storage, Managed Partners, Import / Export APIs, Logic Apps, Functions, Azure Devops, GitHub

Monitoring – Data Collection

Azure Policy:

- Configure xxOS machines to run Azure Monitor Agent and associate them to a Data Collection Rule
- Configure xxOS Machines to be associated with a Data Collection Rule

- Azure Monitor Agent
  - Replacement for MMA
- Data collection rules
  - Granular control event and performance data
  - Events logs and Syslogs for Sentinel and Defender for Cloud



Performance
Windows events
Performance
Syslog
Assets

Performance
Windows events
Syslog
Data source details such as event filters and performance counters.
Data sources

Microsoft-Perf
Microsoft-Event
Microsoft-Syslog
Describes set of data sources and maps to destination.
Data streams

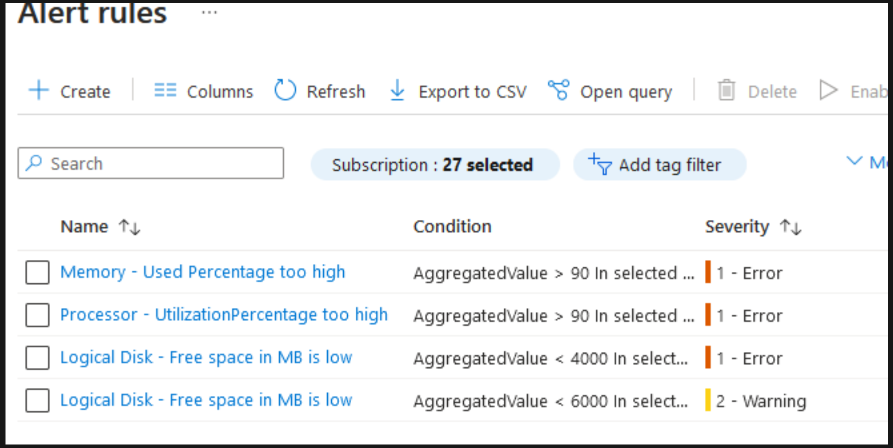
Metrics
Logs
Destination details such as workspace name.
Destinations

Data Collection Rule

Metrics
Logs

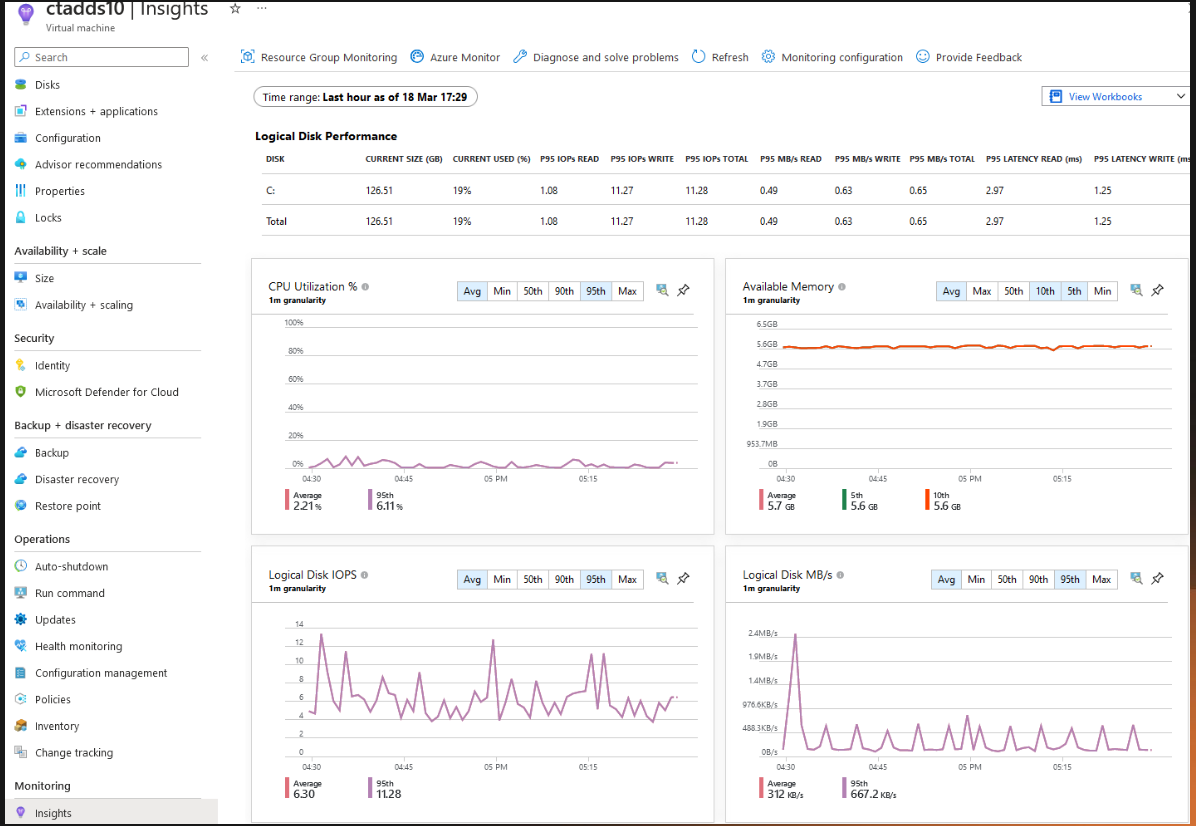
Monitoring – VM Insights

- Basic Guest OS monitoring, CPU, Disk, Memory, Network
  - Configure with DCRs
- Alert in data collected
- SCOM MI for Advanced



Alert rules

	Name ↑↓	Condition	Severity ↑↓
□	Memory - Used Percentage too high	AggregatedValue > 90 In selected ...	1 - Error
□	Processor - UtilizationPercentage too high	AggregatedValue > 90 In selected ...	1 - Error
□	Logical Disk - Free space in MB is low	AggregatedValue < 4000 In select...	1 - Error
□	Logical Disk - Free space in MB is low	AggregatedValue < 6000 In select...	2 - Warning



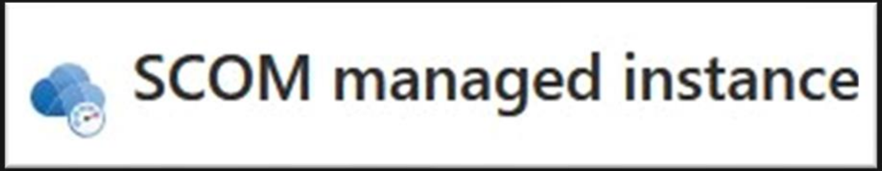
ctadds10 | Insights

Virtual machine

Time range: **Last hour as of 18 Mar 17:29**

Logical Disk Performance

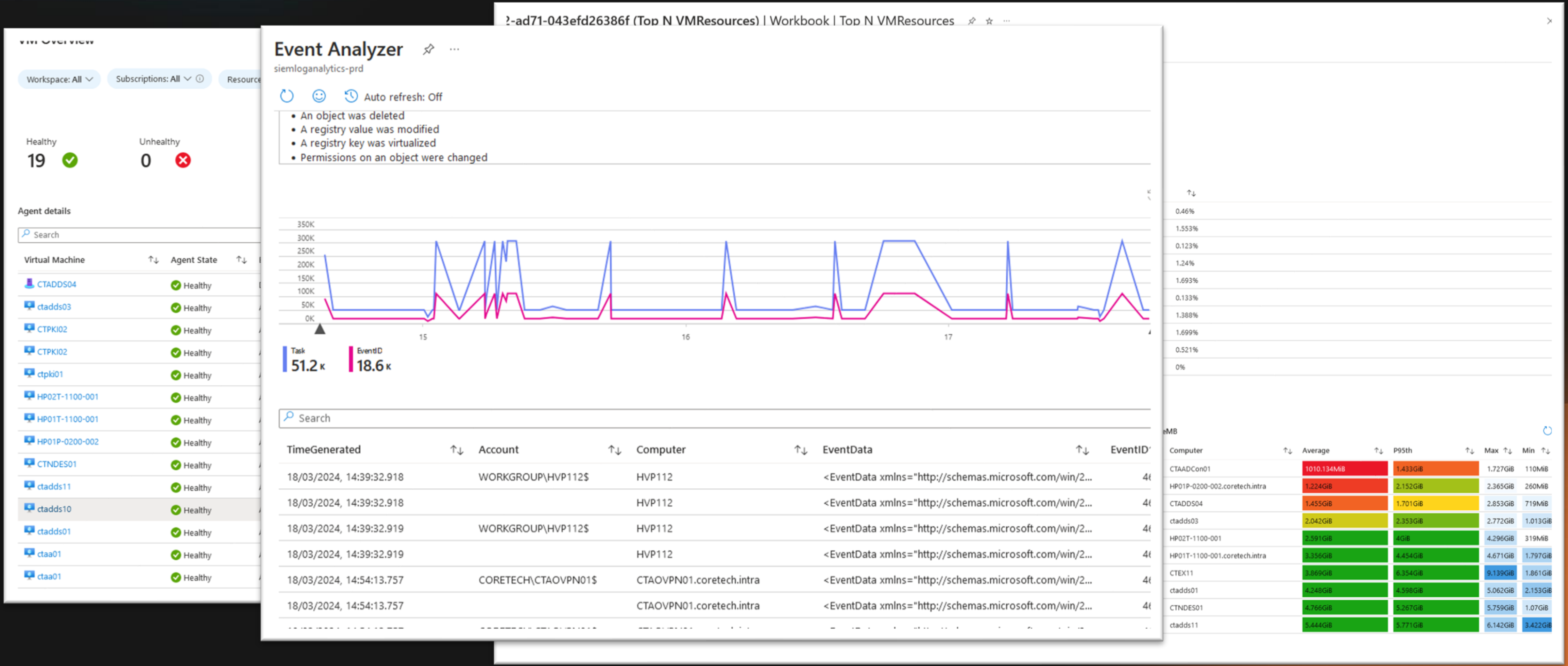
DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPs READ	P95 IOPs WRITE	P95 IOPs TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL	P95 LATENCY READ (ms)	P95 LATENCY WRITE (ms
C:	126.51	19%	1.08	11.27	11.28	0.49	0.63	0.65	2.97	1.25
Total	126.51	19%	1.08	11.27	11.28	0.49	0.63	0.65	2.97	1.25



SCOM managed instance

Monitoring –Visualization

– Workbooks - Dashboards for everything in Azure



VM Overview

Workspace: All ⌄ Subscriptions: All ⌄ Resource

Healthy 19 ✓ Unhealthy 0 ✕

Agent details

Search

Virtual Machine	Agent State
CTADDS04	Healthy
ctadds03	Healthy
CTPKI02	Healthy
CTPKI02	Healthy
ctpki01	Healthy
HP02T-1100-001	Healthy
HP01T-1100-001	Healthy
HP01P-0200-002	Healthy
CTNDES01	Healthy
ctadds11	Healthy
ctadds10	Healthy
ctadds01	Healthy
ctaa01	Healthy
ctaa01	Healthy

Event Analyzer

siemloganalytics-prd

Auto refresh: Off

- An object was deleted
- A registry value was modified
- A registry key was virtualized
- Permissions on an object were changed

Search

TimeGenerated	Account	Computer	EventData	EventID
18/03/2024, 14:39:32.918	WORKGROUP\HVP112$	HVP112	<EventData xmlns="http://schemas.microsoft.com/win/2...	4(
18/03/2024, 14:39:32.918		HVP112	<EventData xmlns="http://schemas.microsoft.com/win/2...	4(
18/03/2024, 14:39:32.919	WORKGROUP\HVP112$	HVP112	<EventData xmlns="http://schemas.microsoft.com/win/2...	4(
18/03/2024, 14:39:32.919		HVP112	<EventData xmlns="http://schemas.microsoft.com/win/2...	4(
18/03/2024, 14:54:13.757	CORETECH\CTAOVPN01$	CTAOVPN01.coretech.intra	<EventData xmlns="http://schemas.microsoft.com/win/2...	4(
18/03/2024, 14:54:13.757		CTAOVPN01.coretech.intra	<EventData xmlns="http://schemas.microsoft.com/win/2...	4(

?-ad71-043efd26386f (Top N VMResources) | Workbook | Top N VMResources

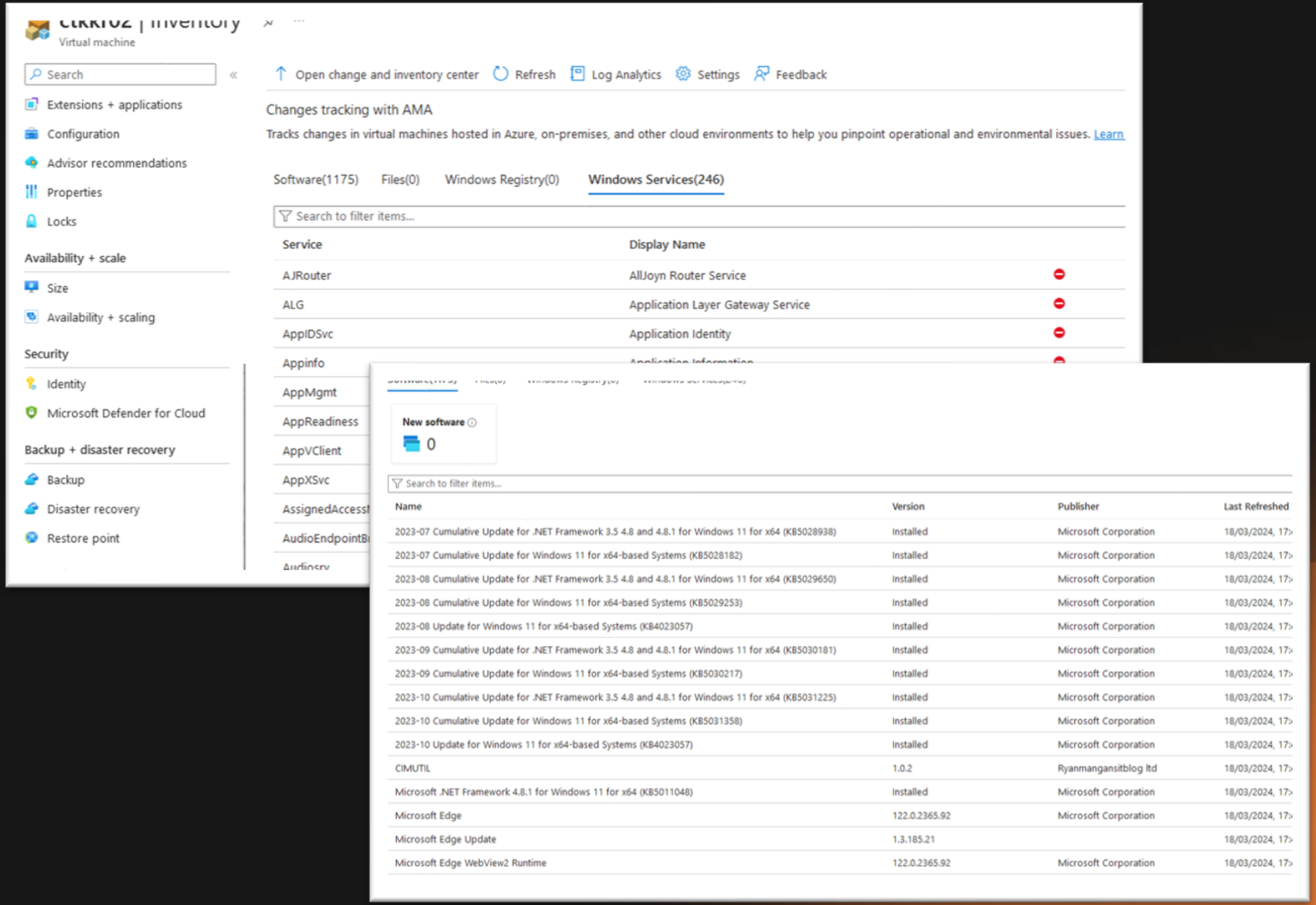
0.46%
1.553%
0.123%
1.24%
1.693%
0.133%
1.388%
1.699%
0.521%
0%

eMB

Computer	Average	P95th	Max	Min
CTAADCon01	1010.134MiB	1.433GiB	1.727GiB	110MiB
HP01P-0200-002.coretech.intra	1.224GiB	2.152GiB	2.365GiB	260MiB
CTADDS04	1.455GiB	1.701GiB	2.853GiB	719MiB
ctadds03	2.042GiB	2.353GiB	2.772GiB	1.013GiB
HP02T-1100-001	2.591GiB	4GiB	4.296GiB	319MiB
HP01T-1100-001.coretech.intra	3.356GiB	4.454GiB	4.671GiB	1.797GiB
CTEX11	3.869GiB	6.354GiB	9.139GiB	1.861GiB
ctadds01	4.248GiB	4.598GiB	5.062GiB	2.153GiB
CTNDES01	4.766GiB	5.267GiB	5.759GiB	1.07GiB
ctadds11	5.444GiB	5.771GiB	6.142GiB	3.422GiB

Inventory and Change Tracking

- Based on AMA & Data Collection Rules
- Track
  - Windows registry
  - Windows file
  - Linux file
  - Windows services
  - Windows software
  - Linux software
  - Linux Daemons



ctkkr02 | Inventory

Virtual machine

Changes tracking with AMA

Tracks changes in virtual machines hosted in Azure, on-premises, and other cloud environments to help you pinpoint operational and environmental issues. Learn

Service	Display Name	
AJRouter	AllJoyn Router Service	⊖
ALG	Application Layer Gateway Service	⊖
AppIDSvc	Application Identity	⊖
Appinfo	Application Information	⊖
AppMgmt		
AppReadiness		
AppVClient		
AppXSvc		
AssignedAccessM		
AudioEndpointB		
Audiosrv		

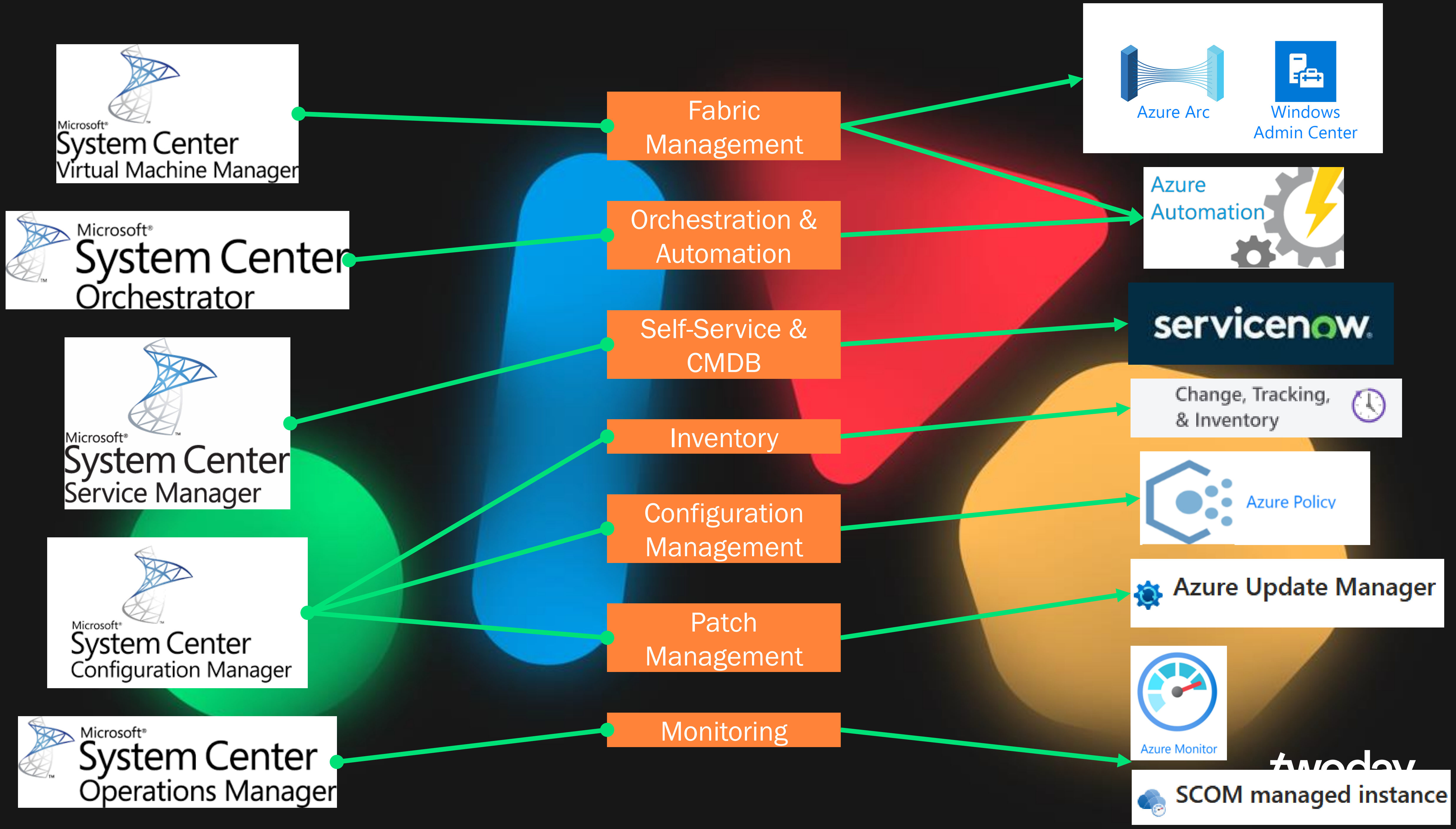
New software ⓘ

0

Name	Version	Publisher	Last Refreshed
2023-07 Cumulative Update for .NET Framework 3.5 4.8 and 4.8.1 for Windows 11 for x64 (KB5028938)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-07 Cumulative Update for Windows 11 for x64-based Systems (KB5028182)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-08 Cumulative Update for .NET Framework 3.5 4.8 and 4.8.1 for Windows 11 for x64 (KB5029650)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-08 Cumulative Update for Windows 11 for x64-based Systems (KB5029253)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-08 Update for Windows 11 for x64-based Systems (KB4023057)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-09 Cumulative Update for .NET Framework 3.5 4.8 and 4.8.1 for Windows 11 for x64 (KB5030181)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-09 Cumulative Update for Windows 11 for x64-based Systems (KB5030217)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-10 Cumulative Update for .NET Framework 3.5 4.8 and 4.8.1 for Windows 11 for x64 (KB5031225)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-10 Cumulative Update for Windows 11 for x64-based Systems (KB5031358)	Installed	Microsoft Corporation	18/03/2024, 17:
2023-10 Update for Windows 11 for x64-based Systems (KB4023057)	Installed	Microsoft Corporation	18/03/2024, 17:
CIMUTIL	1.0.2	Ryanmangansitblog ltd	18/03/2024, 17:
Microsoft .NET Framework 4.8.1 for Windows 11 for x64 (KB5011048)	Installed	Microsoft Corporation	18/03/2024, 17:
Microsoft Edge	122.0.2365.92	Microsoft Corporation	18/03/2024, 17:
Microsoft Edge Update	1.3.185.21		18/03/2024, 17:
Microsoft Edge WebView2 Runtime	122.0.2365.92	Microsoft Corporation	18/03/2024, 17:

Bringing everything together
Demo demo demo

twoday



Microsoft® System Center Virtual Machine Manager

Microsoft® System Center Orchestrator

Microsoft® System Center Service Manager

Microsoft® System Center Configuration Manager

Microsoft® System Center Operations Manager

Fabric Management

Orchestration & Automation

Self-Service & CMDB

Inventory

Configuration Management

Patch Management

Monitoring

Azure Arc

Windows Admin Center

Azure Automation

servicenow.

Change, Tracking, & Inventory

Azure Policy

Azure Update Manager

Azure Monitor

SCOM managed instance

But… what’s the price?

	Azure / Azure HCI VMs / With SA	Other
Guest Policies	Free	5$
Security, Defender P2 Including 500 mb/day logs	15$	15$
Backup	~8$	~8$
Update Manager	Free	Free with P2 or 5$
Inventory	~0$	~0$
Monitoring - Perf	~0,6$	~0,6$
Total	~23$ / 160DKK per/VM	~28-33$ / 225DKK per/VM

twoday

No guarantees, do your own calculations ;)