

MONITORING AND AUTOMATING AZURE SOLUTIONS

MODULE OVERVIEW

- MONITORING
- BACKUP
- AUTOMATION

MONITORING

MONITORING

- AZURE NETWORK WATCHER
- AZURE SECURITY CENTER
- AZURE MONITOR & DIAGNOSTICS
- AZURE ADVISORS
- AZURE SERVICE HEALTH
- OPERATIONS MANAGEMENT SUITE – LOG ANALYTICS
- APPLICATION INSIGHTS

AZURE NETWORK WATCHER

FEATURES:

- TOPOLOGY – NOW ALSO PART OF AZURE SECURITY CENTER
- VARIABLE PACKET CAPTURE – WIRESHARK FORMAT
- IP FLOW VERIFY – CHECKING NSG'S
- NEXT HOP
- DIAGNOSTICS LOGGING
- SECURITY GROUP VIEW
- NSG FLOW LOGGING
- VPN GATEWAY TROUBLESHOOTING
- NETWORK SUBSCRIPTION LIMITS
- ROLE BASED ACCESS CONTROL
- CONNECTIVITY

AZURE MONITOR

CENTRALIZED HUB FOR DIFFERENT AZURE RESOURCES MONITORING ASPECTS:

- ALERTS
- METRICS
- LOG ANALYTICS
- SERVICE HEALTH
- APPLICATION INSIGHTS
- NETWORK WATCHER

The screenshot shows the Azure Monitor dashboard with the following details:

- Subscription:** Developer Program Benefit
- Time range:** Last 6 hours
- Metrics:**
 - Alerts fired: 0
 - Activity log errors: 0
 - Service Health:
 - Service Issues: 0
 - Planned Maintenance: 0
 - Health Advisories: 0
- Shared Services:**
 - Alerts
 - Metrics
 - Metrics (preview)
 - Log Analytics
 - Activity log
 - Service Health
- Solutions:**
 - Application Insights
 - Network watcher
 - Management solutions
- Alerts:** Alerts provide notifications for key metrics on your Azure resources. [Learn more](#)
- Configure** button
- Log Analytics:** Bring your information together into a single view with Log analytics. [Learn more](#)
- Add** button
- Application insights:** Get actionable insights for your web apps with Application insights. [Learn more](#)
- Add** button

AZURE SECURITY CENTER

CENTRALIZED DASHBOARD, FOCUSING ON SECURITY POSTURE OF AZURE AND HYBRID SYSTEMS AND APPLICATIONS.

ACTIVE IN 3 DIFFERENT AREAS:

- GENERAL SECURITY VIEW
- PREVENTION
- DETECTION

NETWORKING FEATURES:

- NETWORKING RECOMMENDATIONS
- INTERNET FACING ENDPOINTS SECURITY VIEW
- NETWORKING TOPOLOGY SECURITY VIEW

AZURE SECURITY CENTER - DEMO

AZURE MONITOR & DIAGNOSTICS

View and manage all your monitoring data easily

Set up alerts and take automated actions

Diagnose operational issues quickly

Integrate with your existing tools

Get the granular, up-to-date monitoring data you need—all in one place

AZURE ADVISORS

Improve the availability of business-critical applications

Enhance protection from potential security threats

Optimize Performance to run healthy applications

Maximize the ROI of your IT and business budget

Get the granular, up-to-date monitoring data you need—all in one place

Azure Architecture Center



Azure Application Architecture Guide

A guide to designing scalable, resilient, and highly available applications, based on proven practices that we have learned from customer engagements.



Reference Architectures

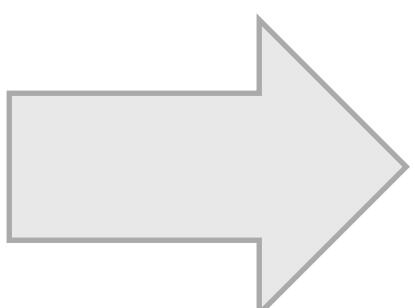
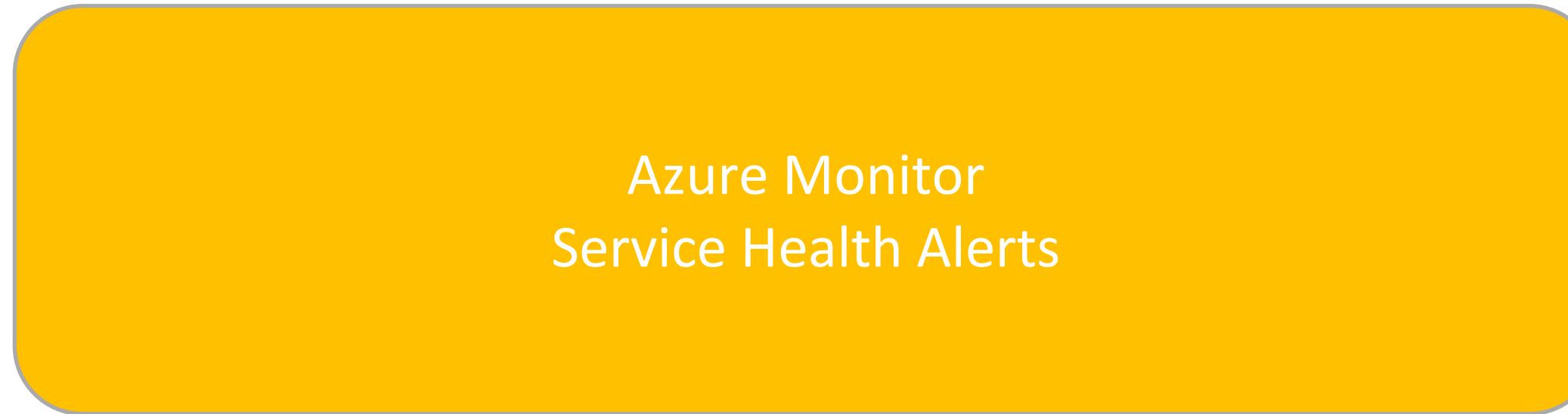
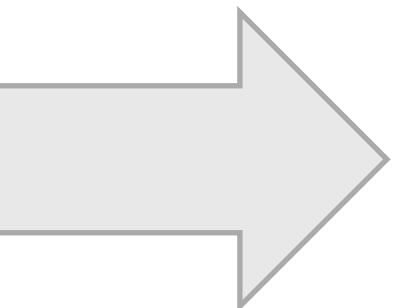
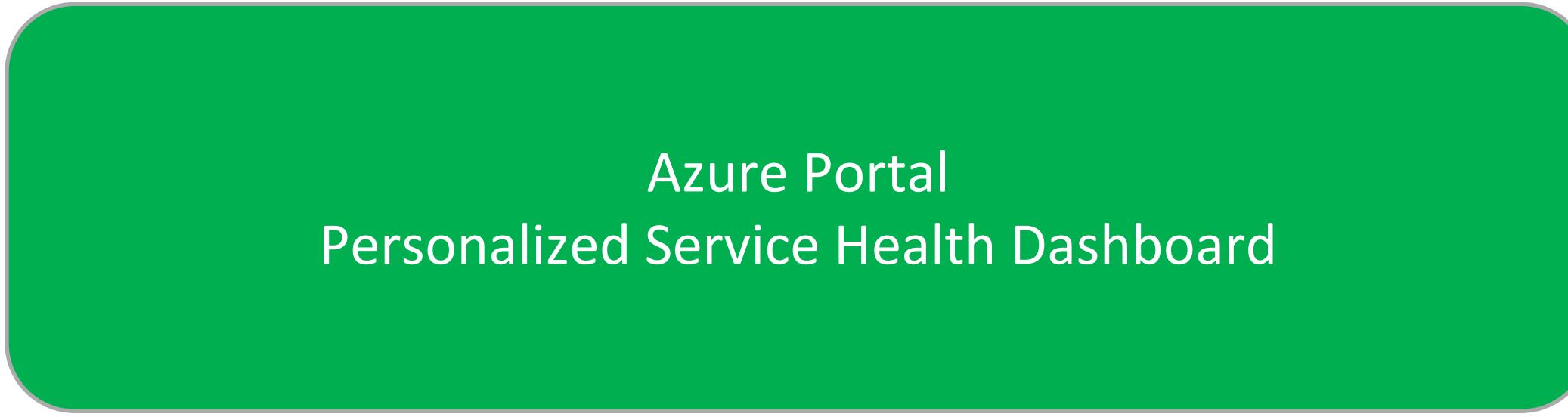
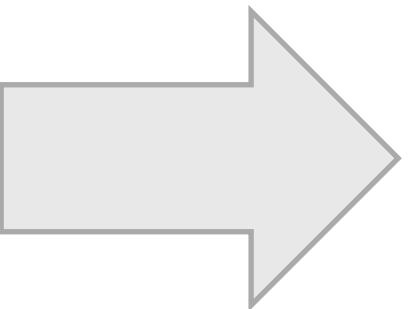
A set of recommended architectures for Azure. Each architecture includes best practices, prescriptive steps, and a deployable solution.



Cloud Design Patterns

Design patterns for developers and solution architects. Each pattern describes a problem, a pattern that addresses the problem, and an example based on Azure.

AZURE SERVICE HEALTH



AZURE SERVICE HEALTH

SERVICE ISSUES:

- SHOWS ANY ONGOING PROBLEMS IN THE AZURE PLATFORM, HAVING IMPACT ON YOU

PLANNED MAINTENANCE:

- PROVIDES INFORMATION ON SCHEDULED MAINTENANCE OF YOUR IMPACTED AZURE RESOURCES

HEALTH HISTORY:

- SHARES FEEDBACK OF PAST ISSUES WITH IMPACT ON YOUR AZURE RESOURCES

The screenshot shows the Azure Service Health - Service issues dashboard. At the top, there's a breadcrumb navigation: Dashboard > Help + support > Service Health - Service issues. Below the header, there's a search bar labeled "Search (Ctrl+ /)" and a "Select filter ..." dropdown. To the right of the search bar are three filter dropdowns: "Subscription" (2 selected), "Region" (31 selected), and "Service" (146 selected). Below these filters are buttons for "Save filter", "Delete filter", "Pin filtered world map to dashboard", and "Create service health alert". A world map on the right side shows green dots representing locations where no service issues are found. Below the map, the text "No service issues found" is displayed. At the bottom of the dashboard, there's a link "See 1 resolved service issues in the last 24 hours, or see all past issues in the health history." and a blue button labeled "Launch guided tour". On the left side of the dashboard, there's a sidebar with sections for "ACTIVE EVENTS", "HISTORY", "RESOURCE HEALTH", and "ALERTS", each with corresponding icons and links.

AZURE LOG ANALYTICS – OPERATIONS MANAGEMENT SUITE

- BASED ON **SOLUTIONS**
- SEPARATE THE **SIGNAL FROM THE NOISE**
- SEE THE FULL PICTURE IN **MEANINGFUL DETAIL**
- INTEGRATING APPLICATION **MONITORING**
- AZURE RESOURCES & HYBRID
- OMS AGENTS
- SUPPORTS “ANY” LOG FILE FORMAT

Gain immediate insights across workloads

Enable consistent control and compliance

Respond immediately to security threats

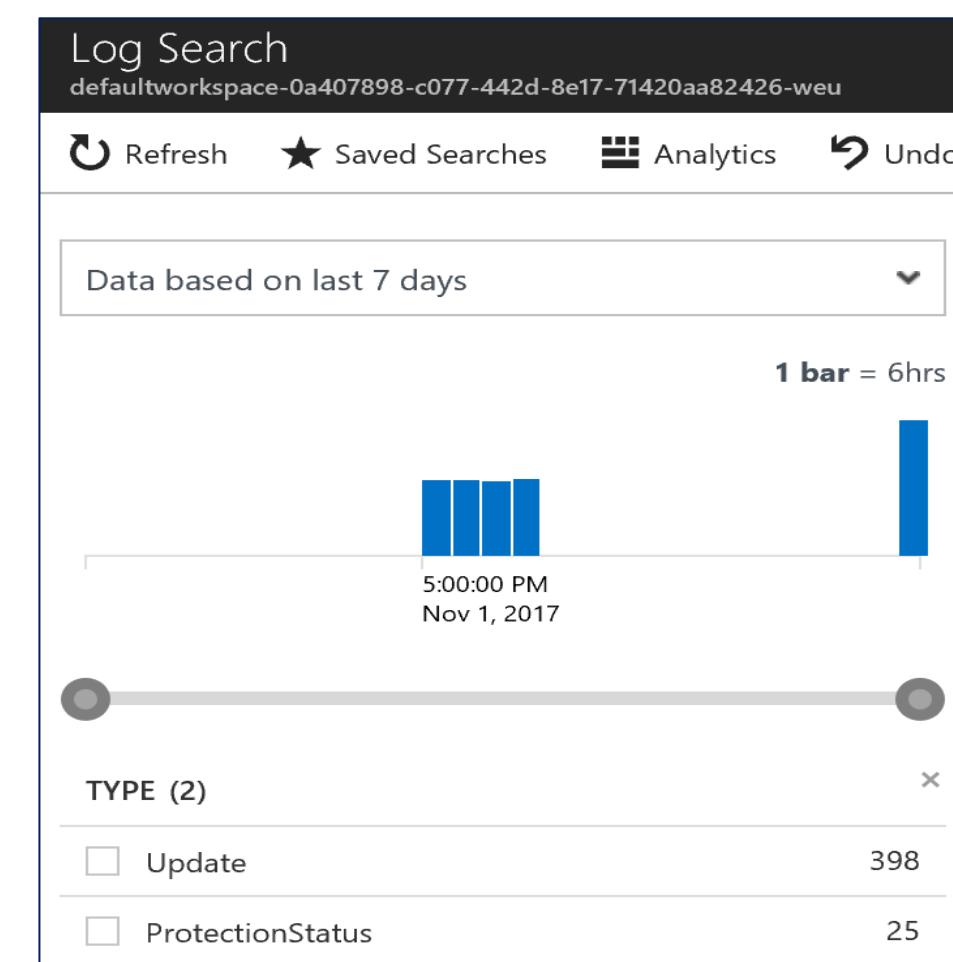
Ensure availability of apps and data

Monitoring, Management + Business Continuity & Disaster Recovery

AZURE LOG ANALYTICS – OPERATIONS MANAGEMENT SUITE

- POWERFUL QUERY LANGUAGE
- CLICK-TO-FILTER SCENARIOS
- SAVED SEARCH
- EXPORT TO CSV
- USE “AZURE LOG ANALYTICS” FOR MORE ADVANCED QUERYING

```
search * | where Type == "Heartbeat"
```



The screenshot shows the Azure Log Analytics workspace interface. On the left, a sidebar lists workspace sections: General (Quick Start, Workspace summary, View Designer), Logs (Logs (classic), Solutions, Saved searches, Pricing tier, Usage and estimated costs, Properties, Service Map), and Workspace Data Sources (Virtual machines, Storage accounts logs, Azure Activity log). The main area shows a query editor with "chmloganalytics01prd - Logs" selected. It includes a search bar ("Search (Ctrl+/)"), a "New Query 1" button, a workspace dropdown ("chmloganalytics01prd"), a "Run" button, a time range selector ("Time range: Last 24 hours"), and a "Type your query here..." input field. To the right, a "Select queries" section lists three examples: "Chart the number of reporting computers each hour" (query: Heartbeat | summarize dcoun(ComputerIP) by bin(TimeGenerated, 1h) | render timechart), "List all computer heartbeats from the last hour" (query: Heartbeat | where TimeGenerated > ago(1h)), and "Last heartbeat of each computer" (query: Heartbeat | summarize arg_max(TimeGenerated, *) by Computer). There is also a "Favorite workspaces" section.

AZURE APPLICATION INSIGHTS

APPLICATION MAP

- DIAGRAM OF APP COMPONENTS AND INTERACTIONS BETWEEN ALL SERVICES

LIVE METRICS

- REAL-TIME REQUESTS INFORMATION

SERVERS

- DETAILED PERFORMANCE PER INSTANCE VIEW

AVAILABILITY

- RUN SCHEDULED TESTS FOR UPTIME

Web App Performance Management

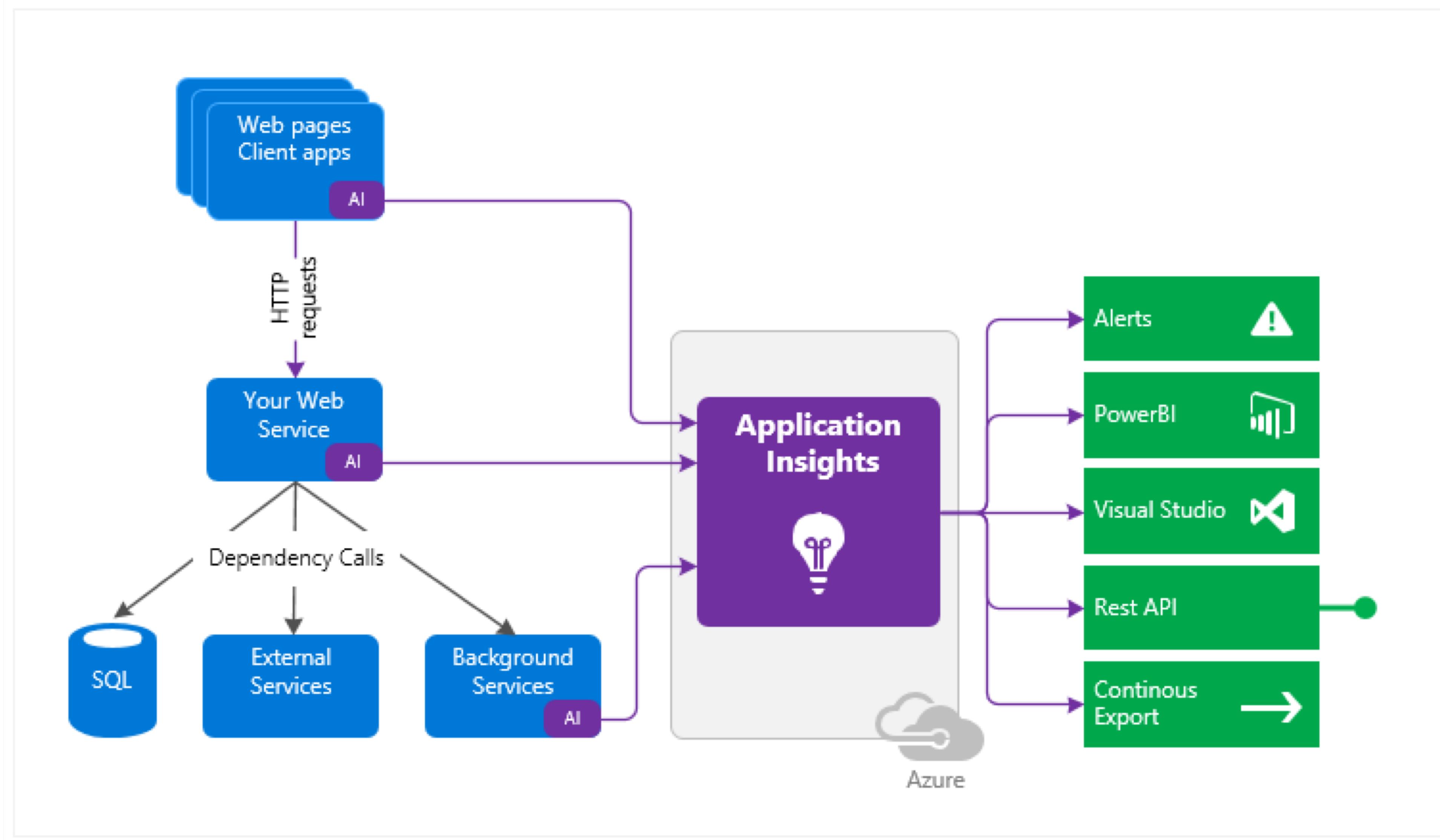
Integrated in the Web App code, running in Azure or on-premises

Diagnostics, proactively detecting lifecycle issues

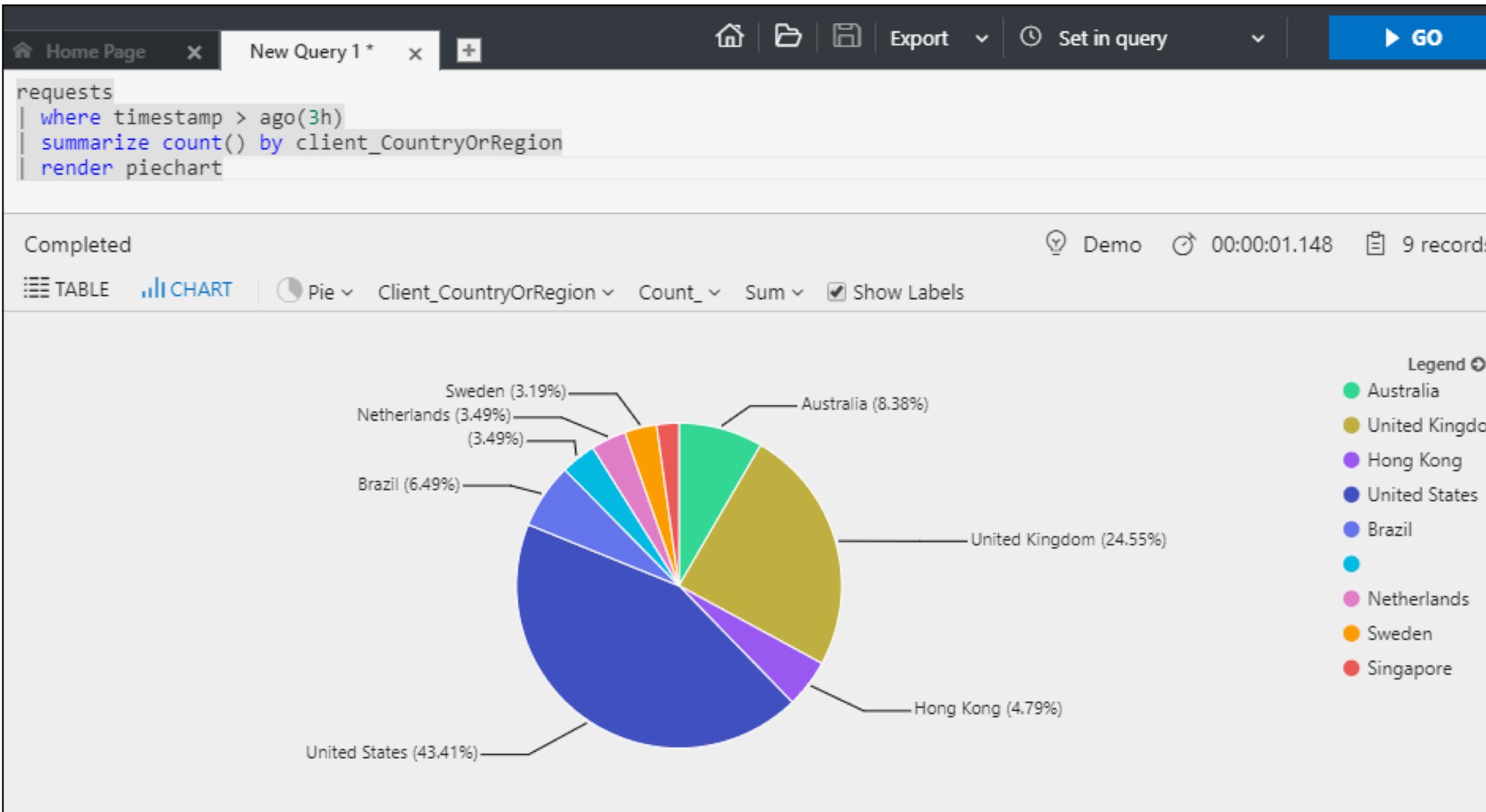
DevOps integration from within VS2017, GitHub,...

Monitoring, Management + Business Continuity & Disaster Recovery

AZURE APPLICATION INSIGHTS



AZURE APPLICATION INSIGHTS



```
C# CustomAIFunction.cs C# SecondCustomAF.cs •
```

```
47 // StartOperation is a helper method that initializes the telemetry item
48 // and allows correlation of this operation with its parent and children.
49 var operation = telemetryClient.StartOperation<DependencyTelemetry>("enqueue " + queueName);
50 operation.Telemetry.Type = "Queue";
51 operation.Telemetry.Data = "Enqueue " + queueName;
52
53 var message = new BrokeredMessage(payload);
54 // Service Bus queue allows the property bag to pass along with the message.
55 // We will use them to pass our correlation identifiers (and other context)
56 // to the consumer.
57 message.Properties.Add("ParentId", operation.Telemetry.Id);
58 message.Properties.Add("RootId", operation.Telemetry.Context.Operation.Id);
59
60 try
61 {
62     await queue.SendAsync(message);
63
64     // Set operation.Telemetry Success and ResponseCode here.
65     operation.Telemetry.Success = true;
66 }
67 catch (Exception e)
68 {
69     telemetryClient.TrackException(e);
70 }
71 }
```

```
1 reference
private static string key =
TelemetryConfiguration.Active.InstrumentationKey = "1125a051-8b19-4649-b097-0e2cb8243282";
5 references
private static TelemetryClient telemetryClient =
    new TelemetryClient() { InstrumentationKey = key };

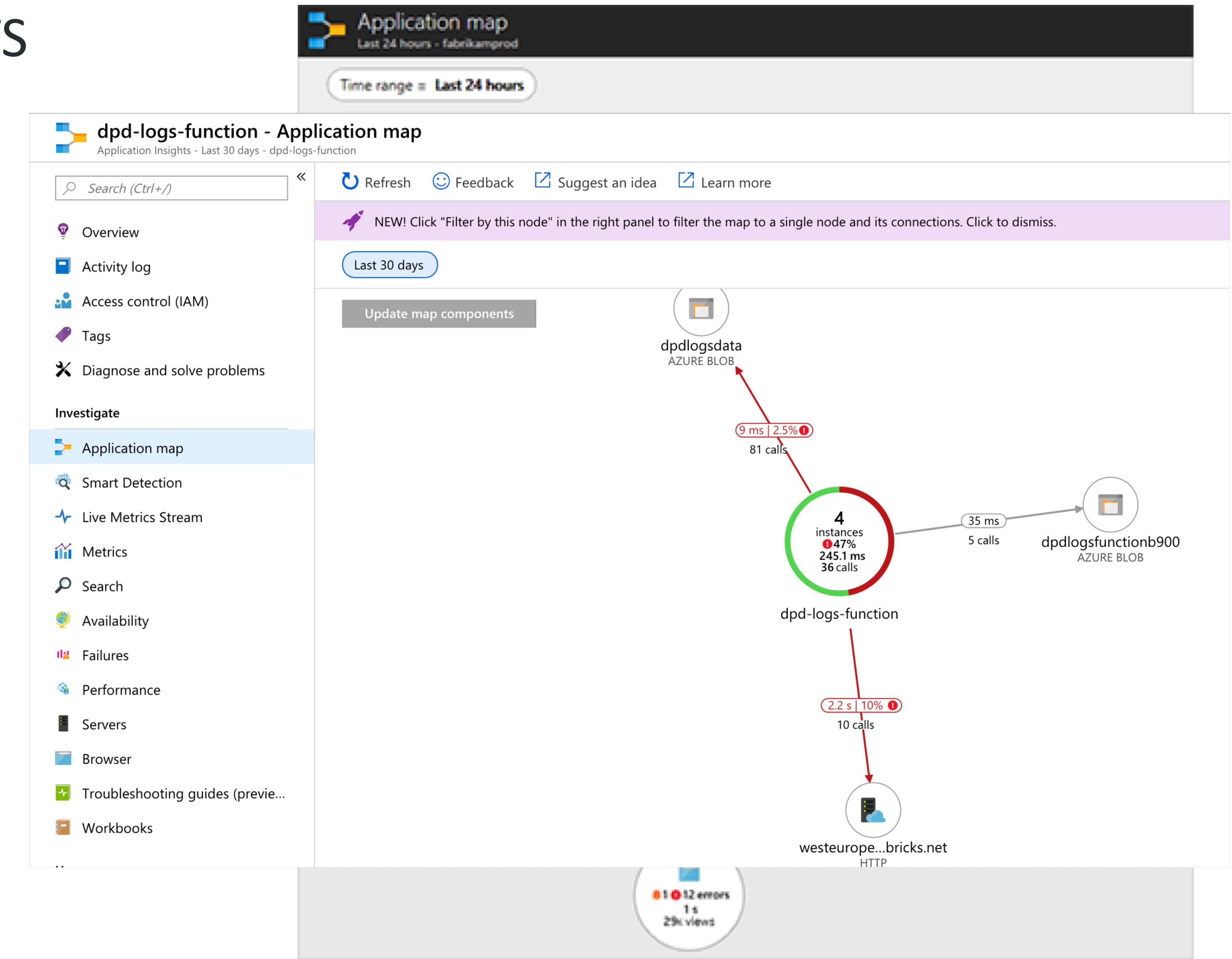
[FunctionName("CustomAIFunction")]
0 references
public static IActionResult Run([HttpTrigger(AuthorizationLevel.Function, "post", Route = null)]HttpRequest
{
    log.Info("C# HTTP trigger function processed a request.");

    var name = GetName(req);

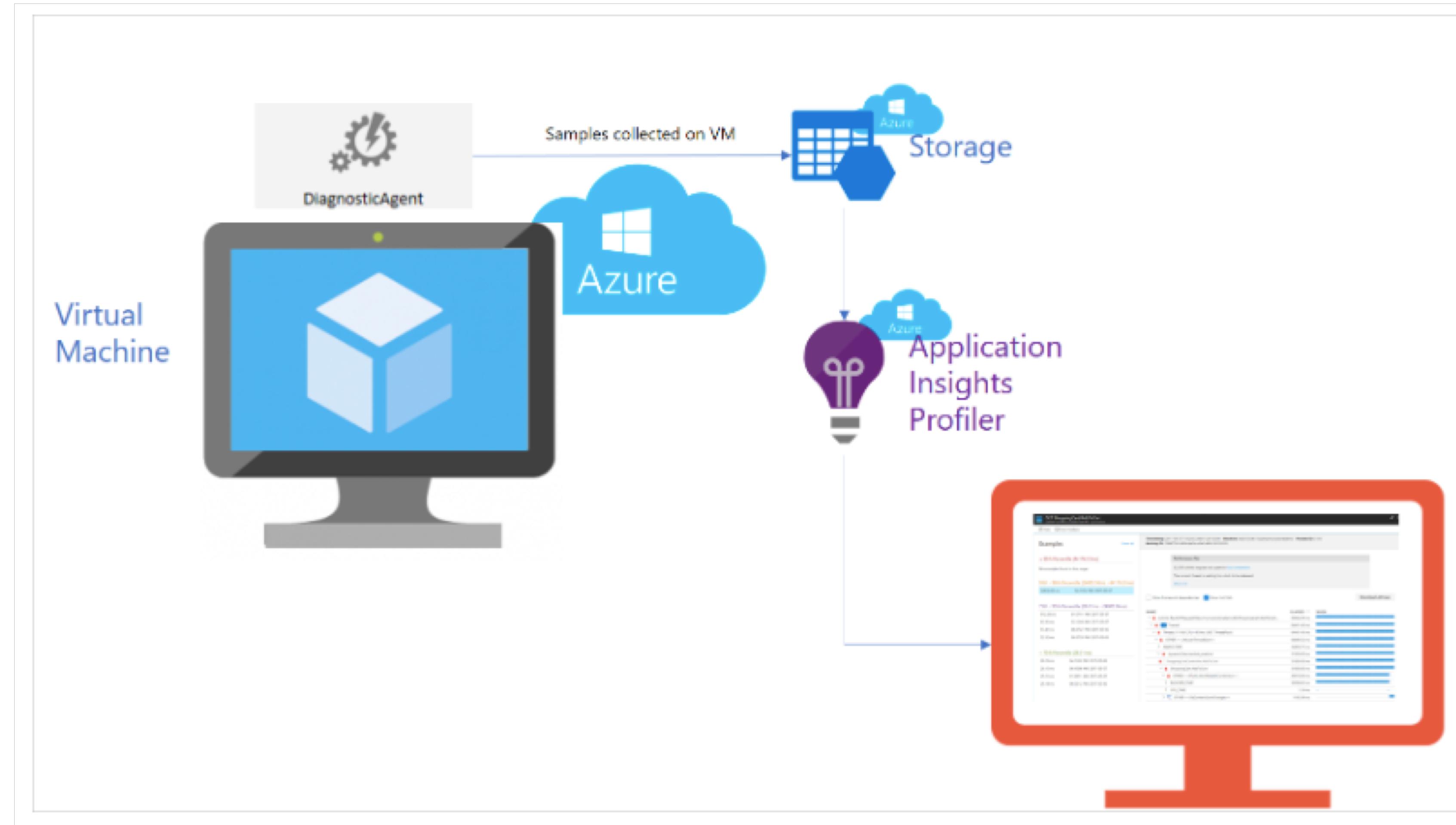
    telemetryClient.Context.Operation.Id = "myId";
    telemetryClient.Context.Operation.ParentId = "myParentId";
    telemetryClient.TrackEvent("myCustomEvent");
    telemetryClient.TrackTrace("myCustomTrace");
    telemetryClient.Context.Cloud.RoleName = "MyAppSet";
```

AZURE APPLICATION INSIGHTS

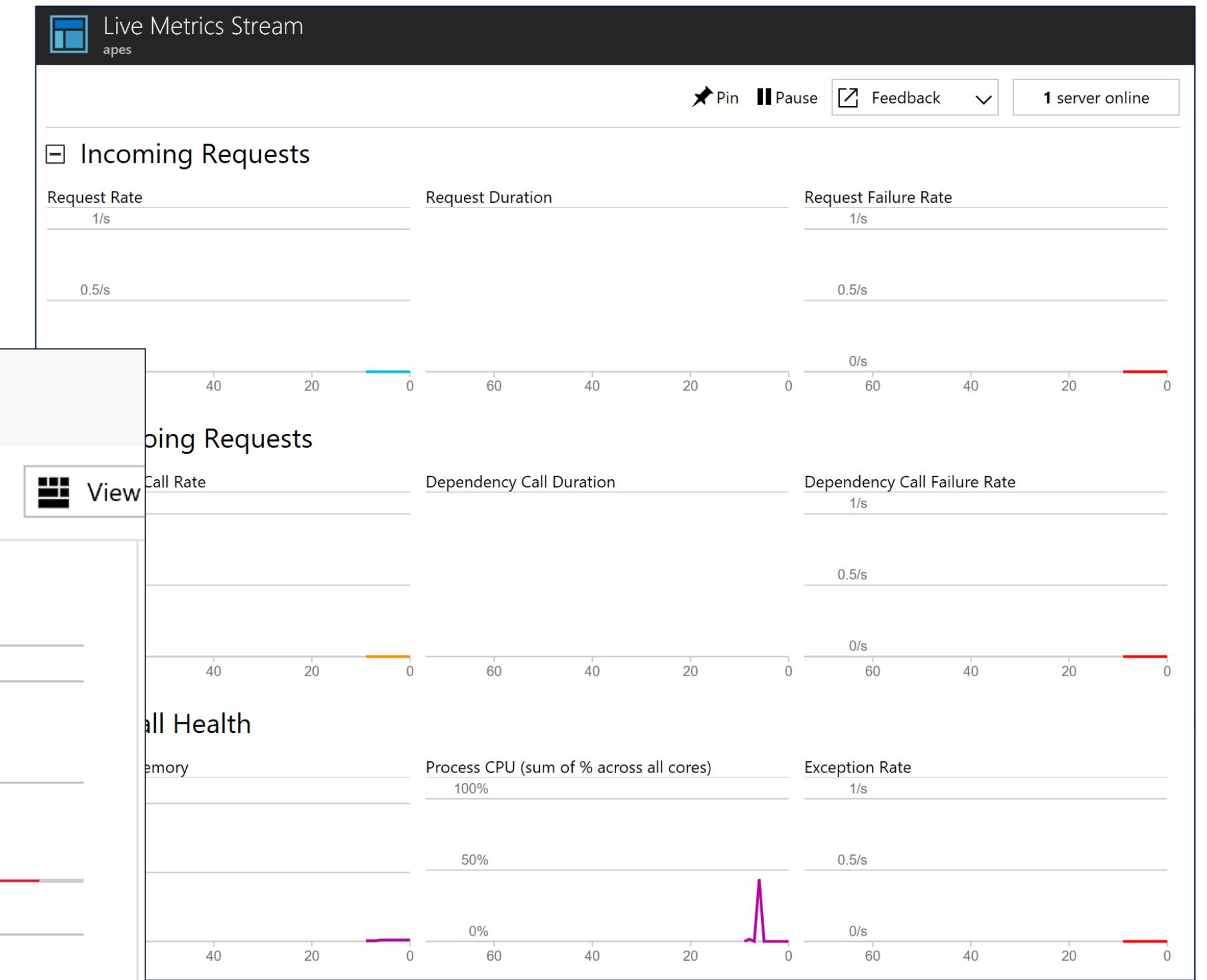
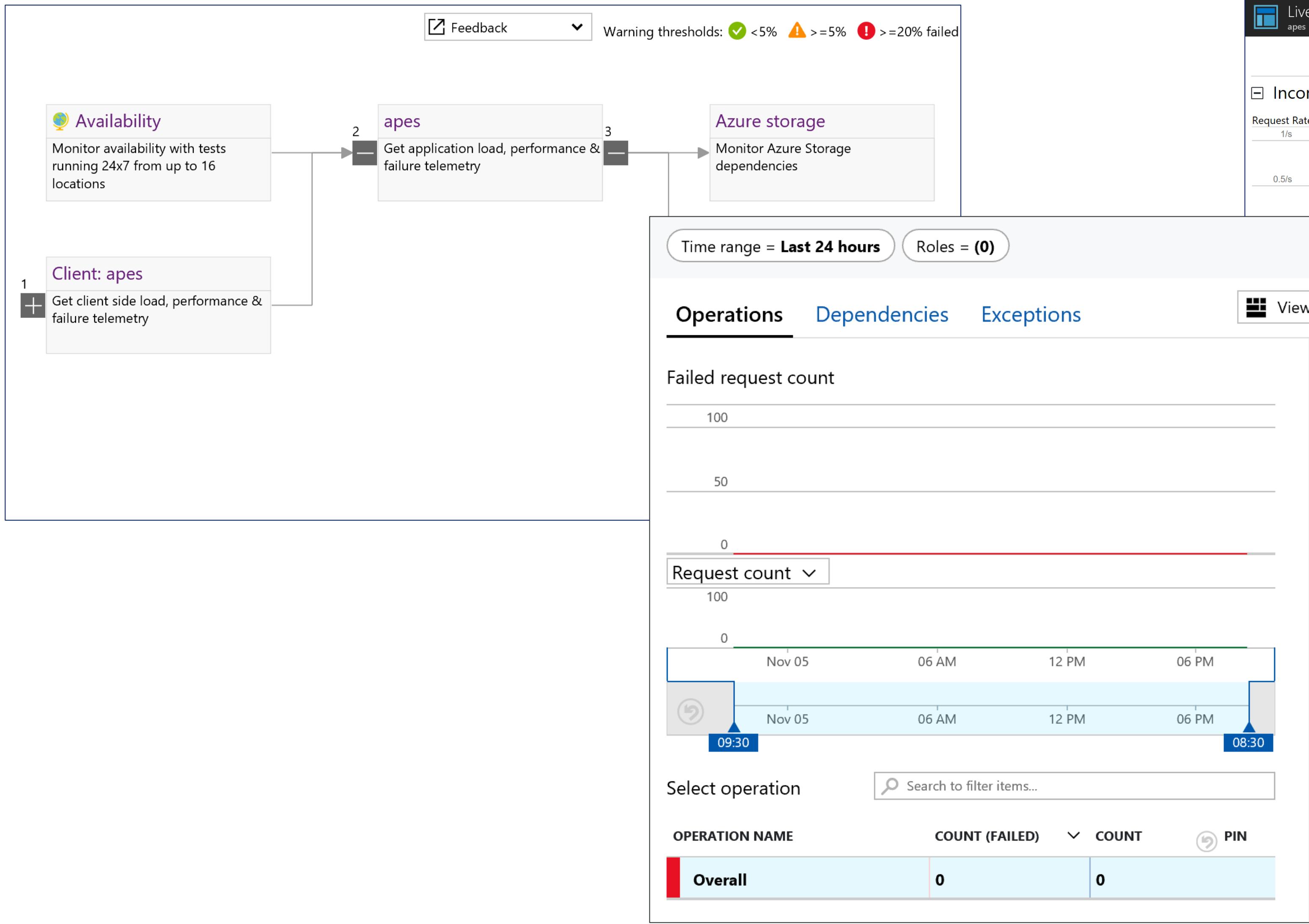
- **APPLICATION MAP HELPS YOU SPOT PERFORMANCE BOTTLENECKS OR FAILURE HOTSPOTS ACROSS ALL COMPONENTS OF YOUR DISTRIBUTED APPLICATION**
- **YOU CAN SEE THE FULL APPLICATION TOPOLOGY ACROSS MULTIPLE LEVELS OF RELATED APPLICATION COMPONENTS. COMPONENTS COULD BE DIFFERENT APPLICATION INSIGHTS RESOURCES, OR DIFFERENT ROLES IN A SINGLE RESOURCE**



AZURE APPLICATION INSIGHTS



AZURE APPLICATION INSIGHTS



POWER BI INTEGRATIONS

Connect to different data sources, create reports and data charts

Get access to powerful dashboards, alerts and drill down for info

Simplify Mgmt, expose IT data to non-IT teams, achieve compliance

Embed interactive data visuals and reporting features into your apps

Monitoring, Management + Business Continuity & Disaster Recovery

| | | | |
|--|--|---|---|
|  Azure Active Directory Activity Logs By Microsoft Power BI Gain insights into Azure Active Directory Activity logs using our Power BI Content Pack |  Azure Audit Logs By Microsoft Power BI Analyze your events, notifications and usage logs |  Azure Backup By Microsoft Power BI Gain insights and create custom reports for protected data assets to drive key business decisions |  Azure Mobile Engagement By Microsoft Power BI Measure the success of your app and important information at a glance |
|  Azure Search By Microsoft Power BI Visualize your search service performance and usage for the last 30 days |  Azure Security Center Policy Management By Microsoft Power BI Gain visibility and insights on security policy adherence across your organization |  Azure Security Center Security Insights By Microsoft Power BI Get insights into the security of your Azure workload such as protection status and detected alerts |  Microsoft Azure Consumption Insights By Microsoft Power BI Analyze and gain insights into your Azure consumption. |

MONITORING - SUMMARY

- AZURE NETWORK WATCHER
- AZURE SECURITY CENTER
- AZURE MONITOR & DIAGNOSTICS
- AZURE ADVISORS
- AZURE SERVICE HEALTH
- OPERATIONS MANAGEMENT SUITE – LOG ANALYTICS
- APPLICATION INSIGHTS

AZURE BACKUP

AZURE BACKUP

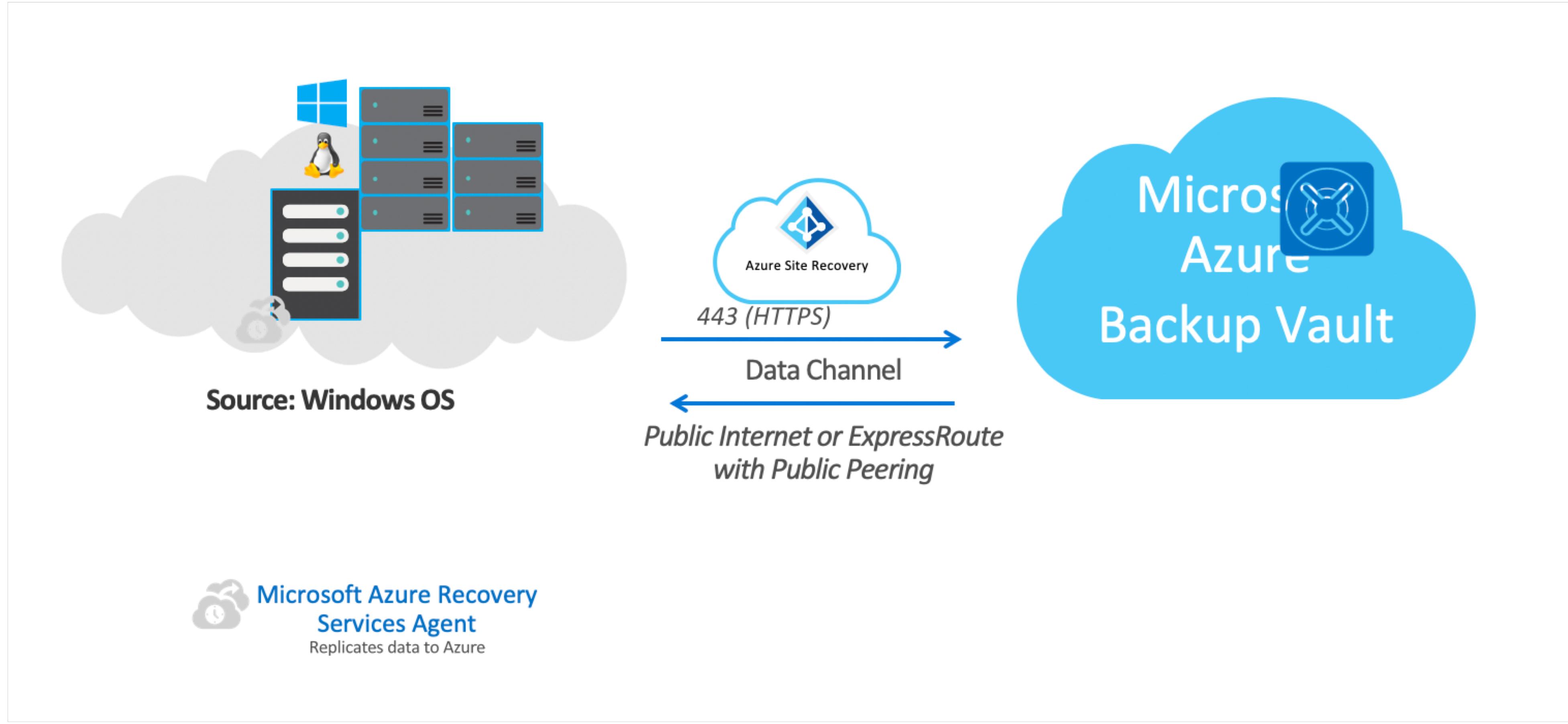
- AZURE BACKUP
- BACKUP OPTIONS
- SPECIALIZED BACKUP

AZURE BACKUP

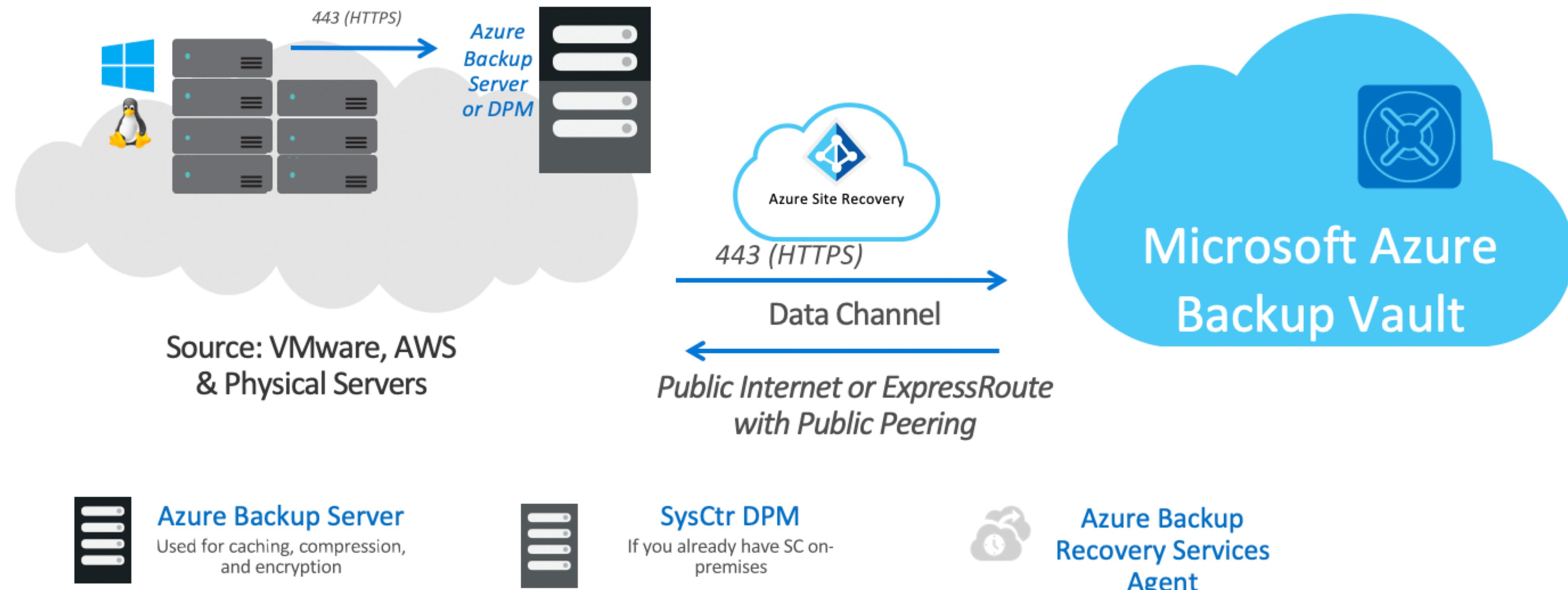
THERE ARE THREE POPULAR SCENARIOS WHERE AZURE IS SELECTED AS THE IDEAL BACKUP TARGET:

1. ON-PREMISES BACKUPS OF FILES & FOLDERS INTO AZURE BACKUP VAULT
2. ON-PREMISES BACKUPS OF FULL WINDOWS & LINUX VMS INTO AZURE BACKUP VAULT
3. AZURE VM BACKUP TO AZURE BACKUP VAULT – THE MOST COMMONLY USED AS IT IS VERY NATIVE, THEN NOT VERY FEATURE RICH SOLUTION

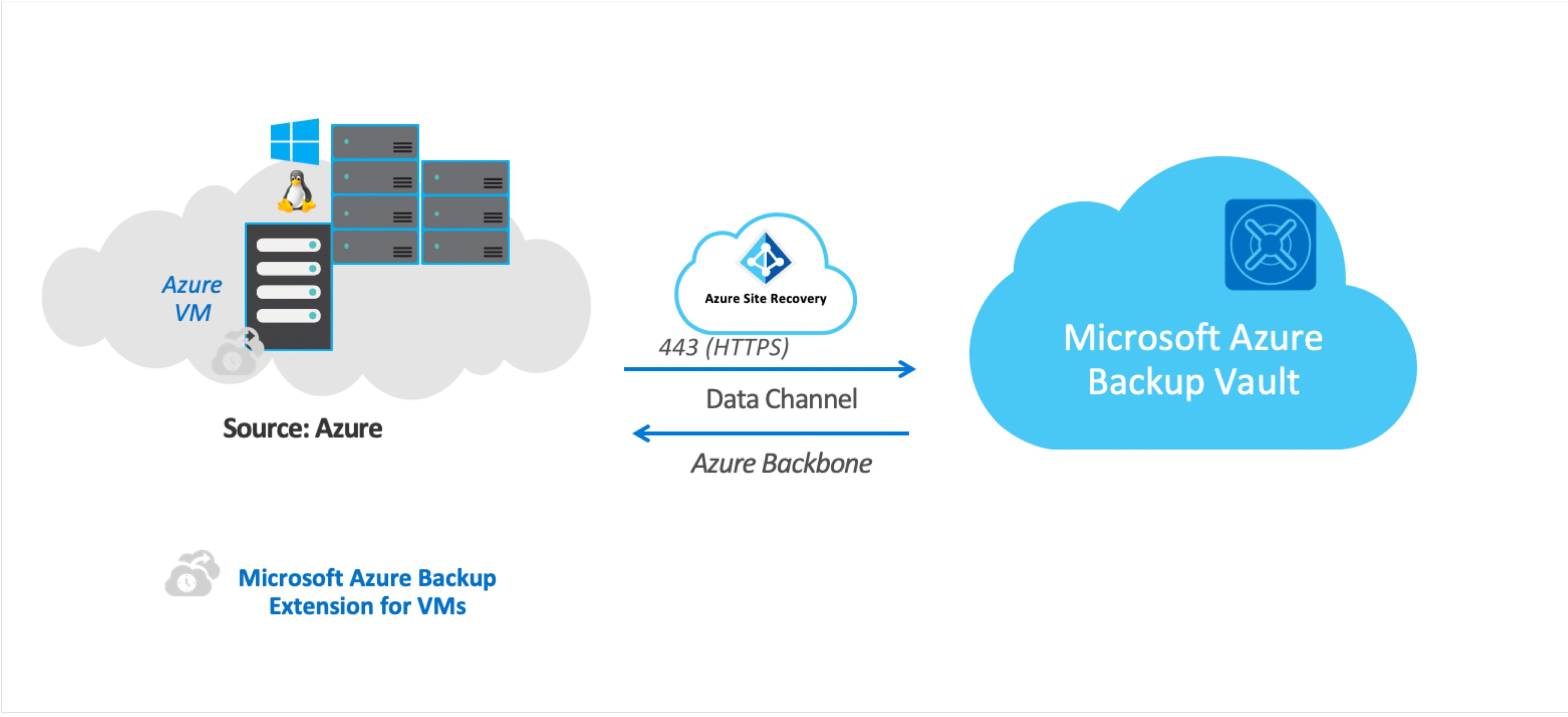
AZURE BACKUP / RESTORE OF ON-PREMISES FILES & FOLDERS



AZURE BACKUP / RESTORE OF ON-PREMISES RUNNING FULL WORKLOADS (OS, SYSVOL, AND APPLICATIONS)



AZURE VM BACKUP / RESTORE TO AZURE BACKUP VAULT

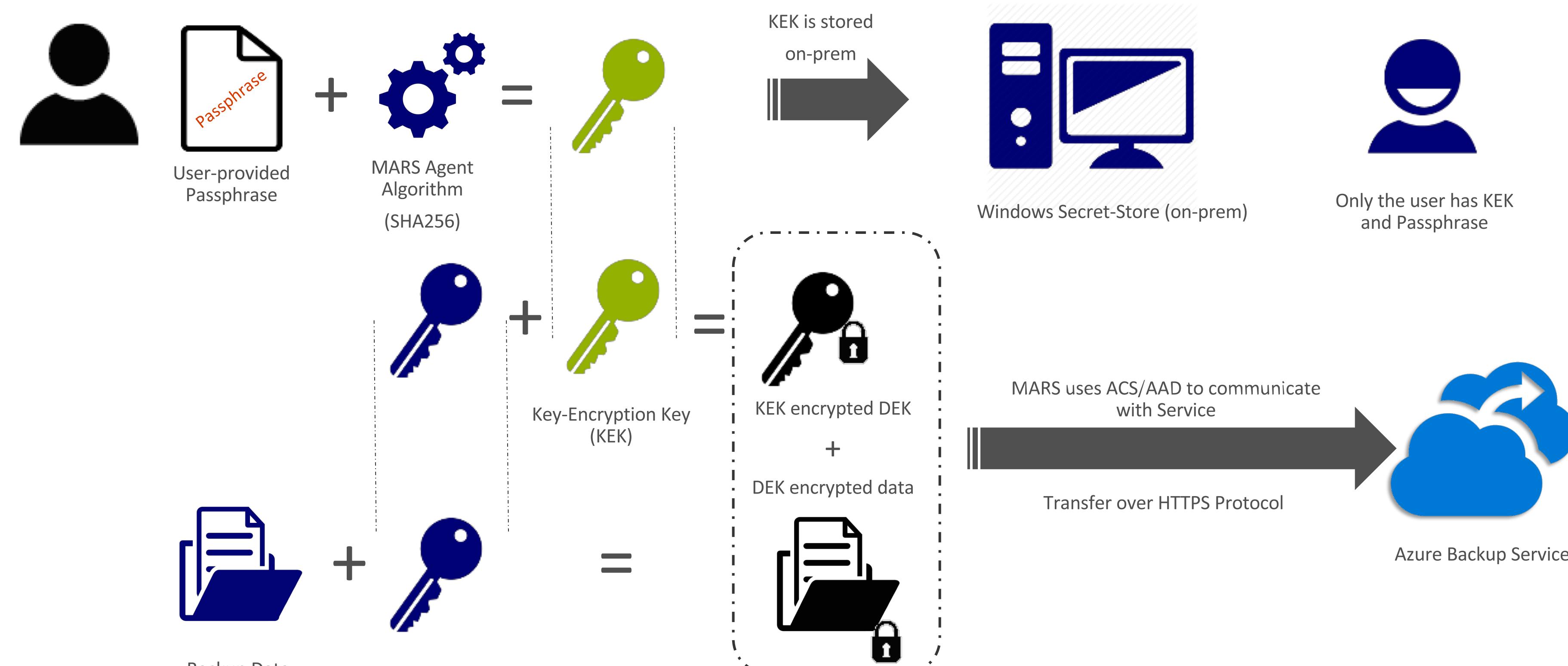


AZURE BACKUP

OTHER POSSIBILITIES

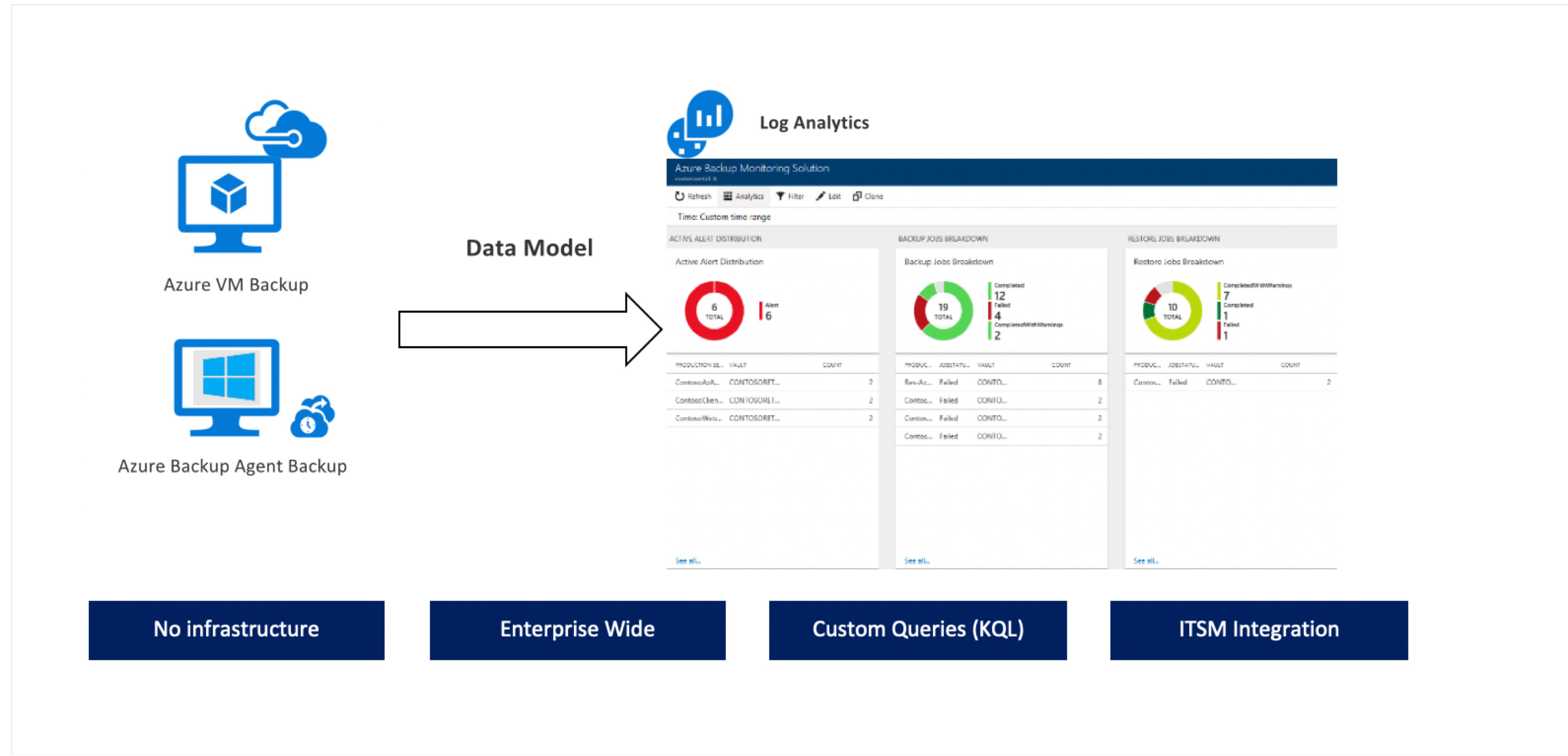
- HYBRID BACKUP ENCRYPTION
- AZURE BACKUP MONITORING WITH LOG ANALYTICS
- AZURE BACKUP REPORTS WITH POWER BI
- LINUX APPLICATION CONSISTENT AZURE BACKUP

AZURE BACKUP - ENCRYPTION

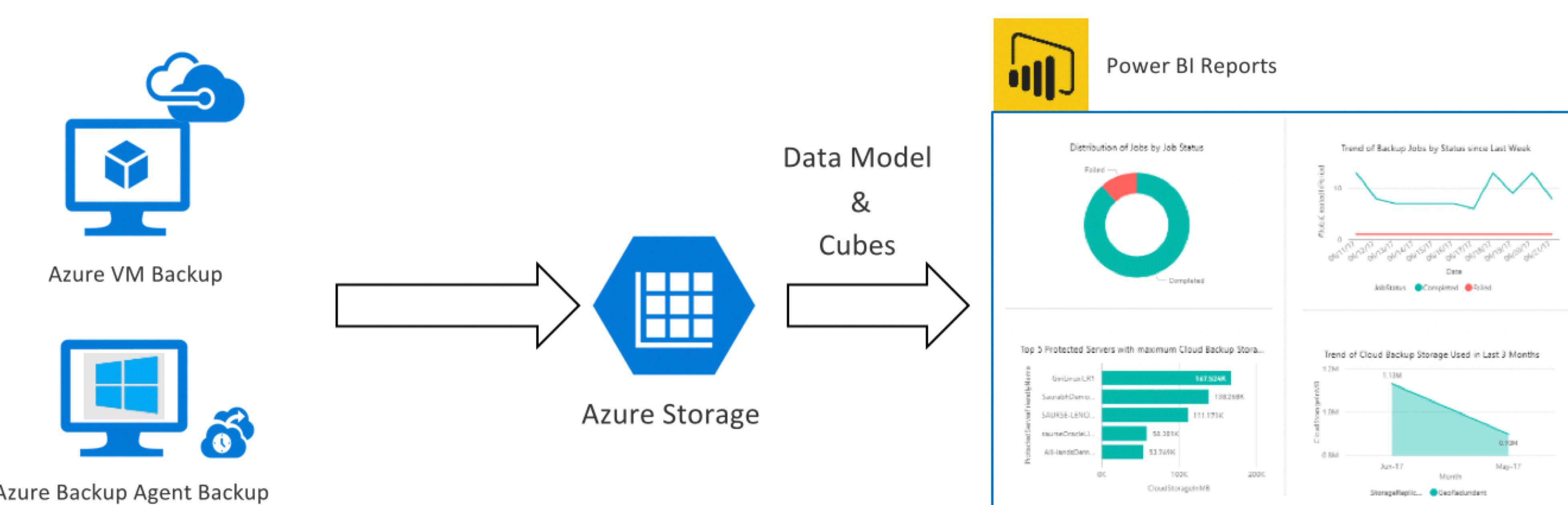


*All assets are AES256 Encrypted

AZURE BACKUP – MONITORING WITH LOG ANALYTICS



AZURE BACKUP – MONITORING WITH POWER BI



No infrastructure

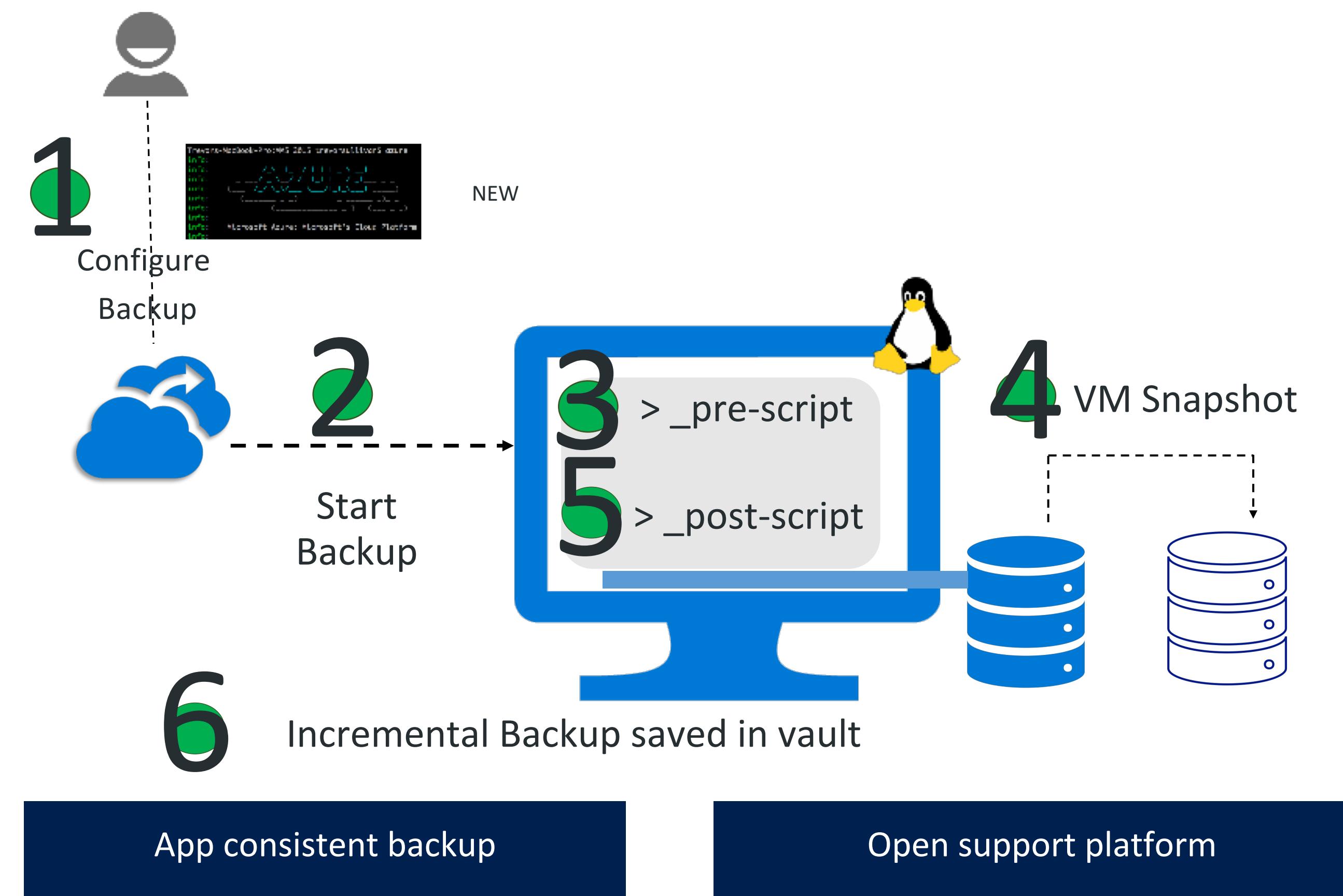
Enterprise Wide

Custom Reports

Access Control

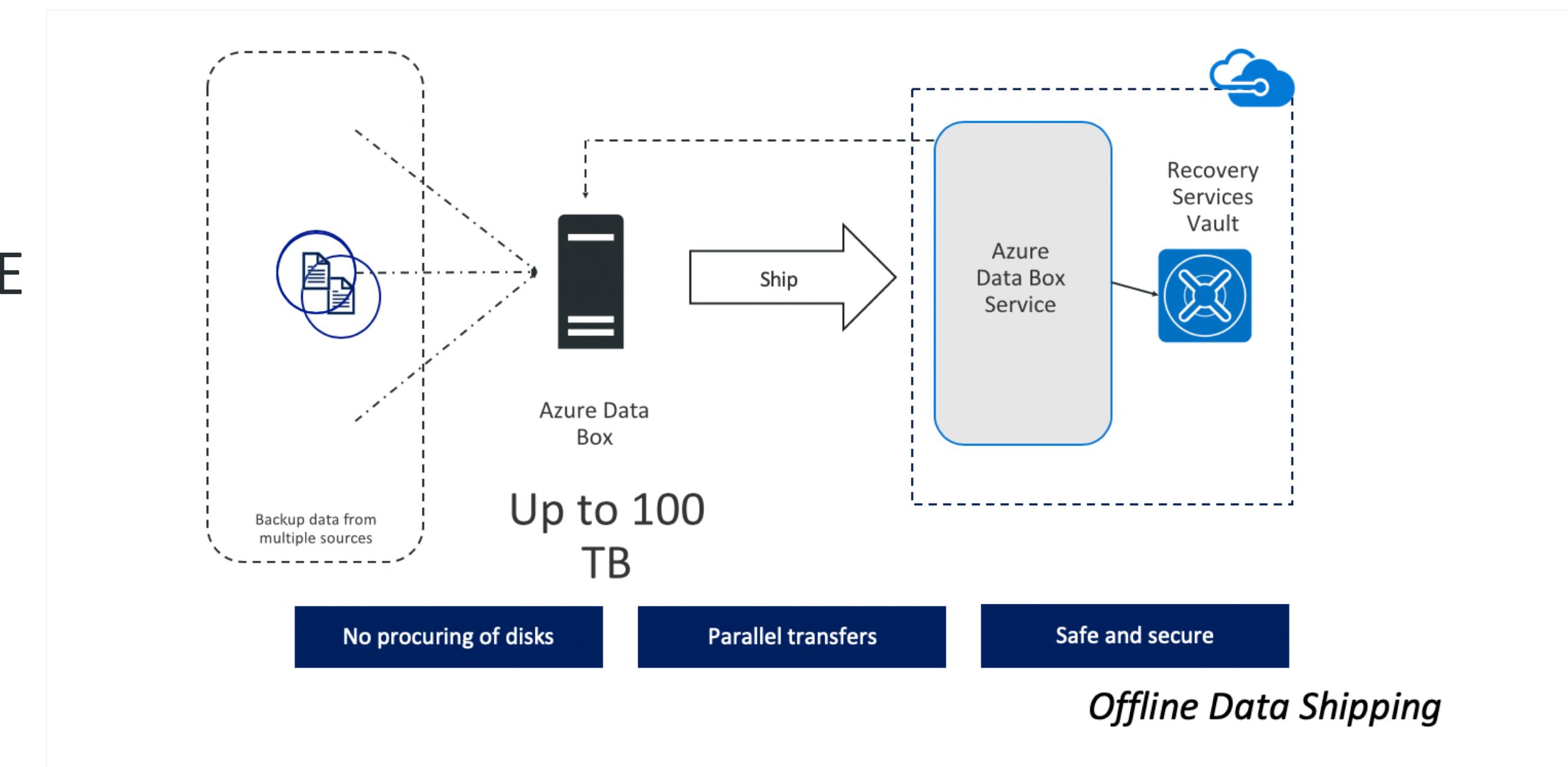
AZURE BACKUP – APPLICATION CONSISTENT BACKUP

- TAKING BACKUPS OF AZURE VMS RUNNING LINUX OS IS FULLY SUPPORTED, FOR AZURE SUPPORTED LINUX OPERATING SYSTEMS.
- TO ALLOW FOR APPLICATION CONSISTENT BACKUPS, YOU NEED TO RUN A PRE- & POST- BACKUP SCRIPT. THE VM SNAPSHOT WILL BE YOUR VM BACKUP, WHICH GETS STORED IN THE BACKUP VAULT USING AN INCREMENTAL UPDATE PROCESS.



AZURE DATA BOX

- USE THE AZURE DATA BOX SERVICE WHEN YOU WANT TO TRANSFER LARGE AMOUNTS OF DATA TO AZURE BUT ARE LIMITED BY TIME, NETWORK AVAILABILITY OR COSTS.
- THE AZURE DATA BOX PROVIDES A SECURE, TAMPER-RESISTANT METHOD FOR QUICK AND SIMPLE TRANSFER OF YOUR DATA TO AZURE.
- YOU CAN ORDER THE DATA BOX THROUGH THE AZURE PORTAL
- THE DATA BOX IS RETURNED TO THE AZURE DATA CENTER TO BE UPLOADED TO AZURE, THEN THE DEVICE IS SECURELY ERASED.



AZURE BACKUP - SUMMARY

- AZURE BACKUP
- BACKUP OPTIONS
- SPECIALIZED BACKUP

AZURE SITE RECOVERY

AZURE SITE RECOVERY

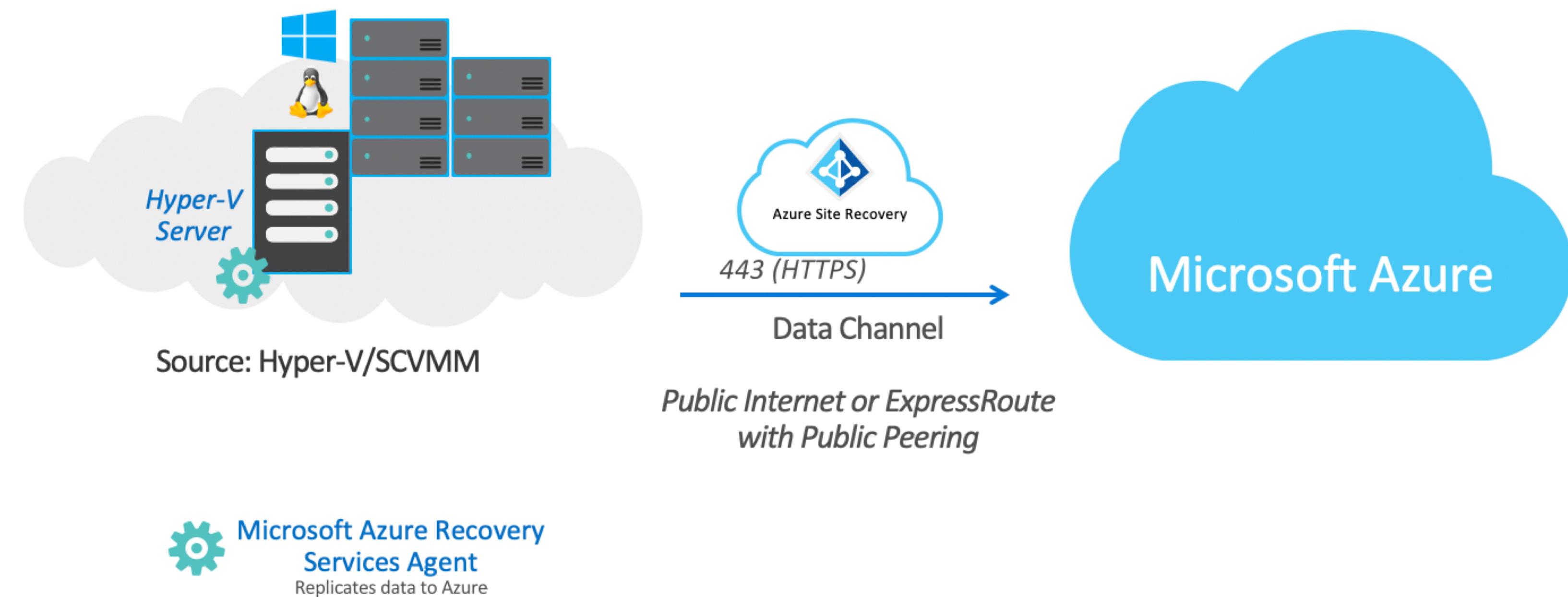
- HYPER-V TO AZURE
- VMWARE TO AZURE
- AZURE TO AZURE

AZURE SITE RECOVERY

- DESIGNED FOR ZERO-DATA LOSS DURING MIGRATION
- NEAR-ZERO DOWNTIME FOR THEIR USERS
- COMPREHENSIVE COVERAGE FOR ALL APPLICATIONS
- ABILITY TO TEST APPLICATION IN THE NEW CLOUD BEFORE MIGRATION
- ZERO APPLICATION DATA LOSS DURING MIGRATION
- NEAR-ZERO APPLICATION DOWNTIME DURING MIGRATION
- BROAD COVERAGE FOR HYPERVISORS, APPLICATIONS, OPERATING SYSTEMS, AND AZURE FEATURES
- NO-IMPACT APPLICATION TESTING IN AZURE

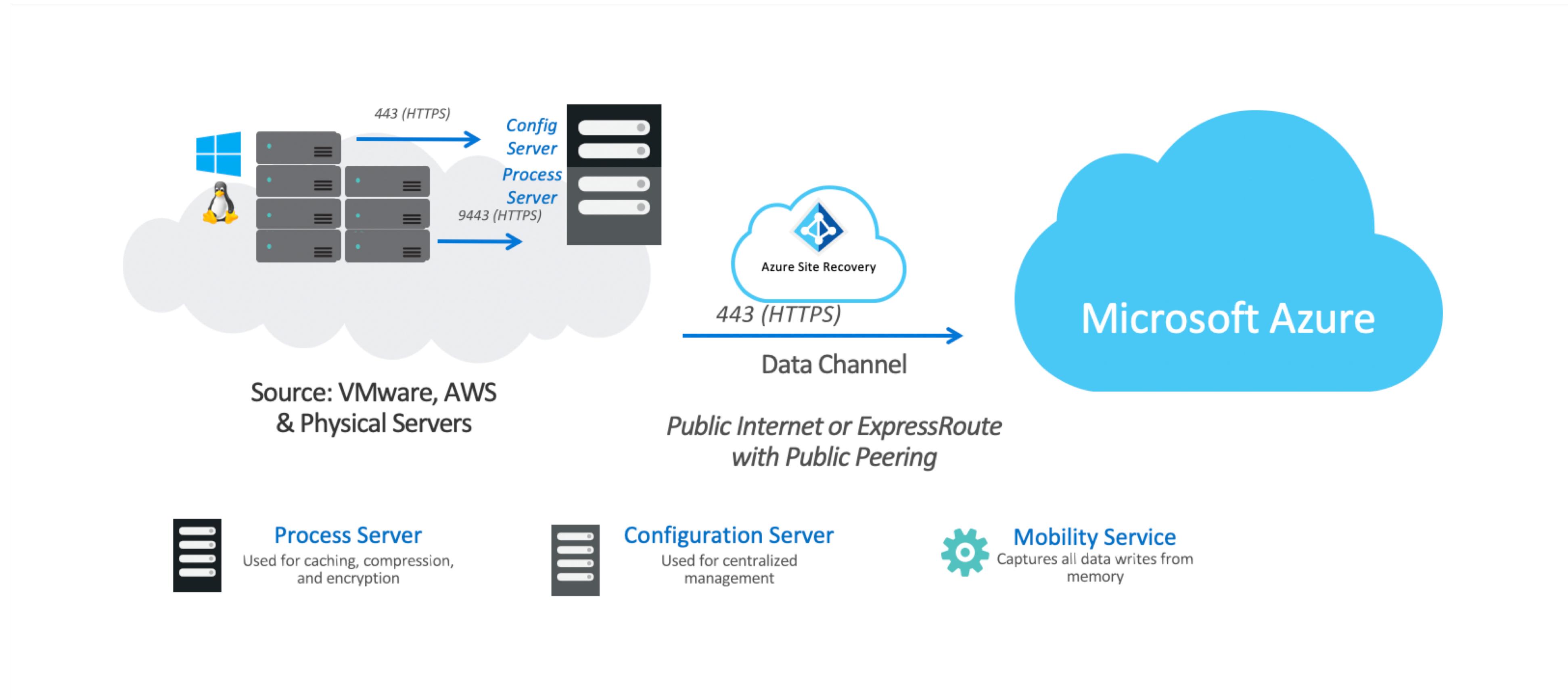
AZURE SITE RECOVERY - DISASTER RECOVERY OR WORKLOAD

Migration from Hyper-V/SCVMM

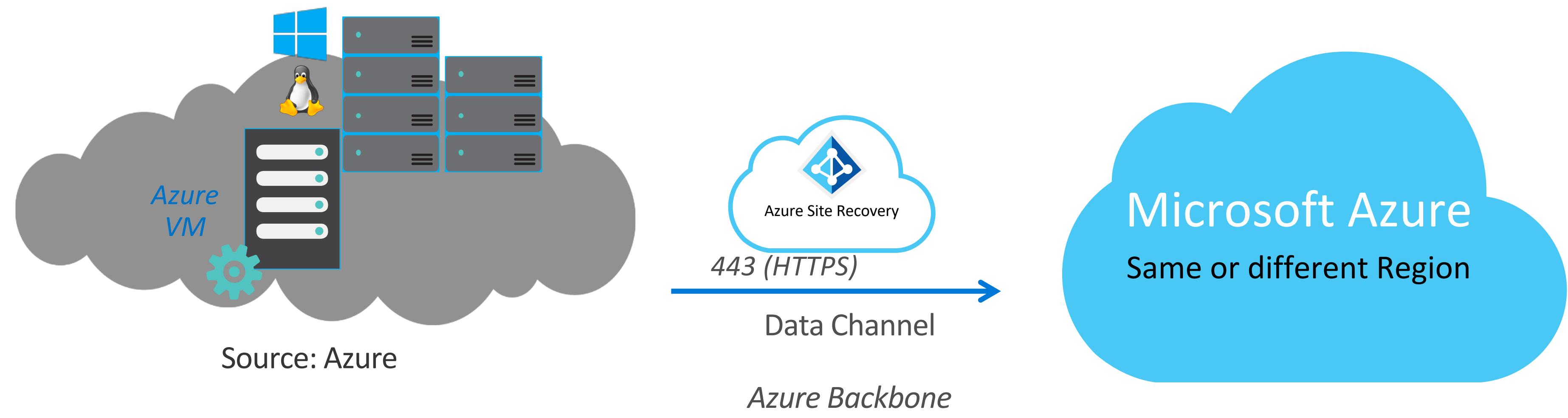


AZURE SITE RECOVERY - DISASTER RECOVERY OR WORKLOAD

Migration from VMware/AWS/Physical



AZURE SITE RECOVERY – AZURE 2 AZURE



 **Microsoft Azure Recovery Services Agent**
Replicates data to Azure

AZURE SITE RECOVERY - SUMMARY

- HYPER-V TO AZURE
- VMWARE TO AZURE
- AZURE TO AZURE

AZURE AUTOMATION

AZURE AUTOMATION

- AZURE AUTOMATION
- AZURE AUTOMATION – DESIRED STATE CONFIGURATION
- OTHER OPTIONS

AZURE AUTOMATION

CONFIGURATION AND CONTROL PLANE FOR AZURE, ON-PREMISE AND OTHER CLOUD PROVIDERS:

- ROBUST CONFIGURATION MANAGEMENT TOOLKIT BUILT-IN
- ACCESS GOVERNANCE AND CONTROL
- SERVERLESS EXECUTION OF MANAGEMENT SCRIPTS
- INTEGRATION WITH EXISTING PLATFORMS, SYSTEMS AND OS FEATURES

AZURE AUTOMATION - FEATURES

PROCESS AUTOMATION

- AUTHOR RUNBOOKS - **POWERSHELL, SCRIPTS POWERSHELL WORKFLOW, GRAPHICAL, PYTHON2**
- HYBRID RUNBOOK WORKERS WITH PROXY SUPPORT

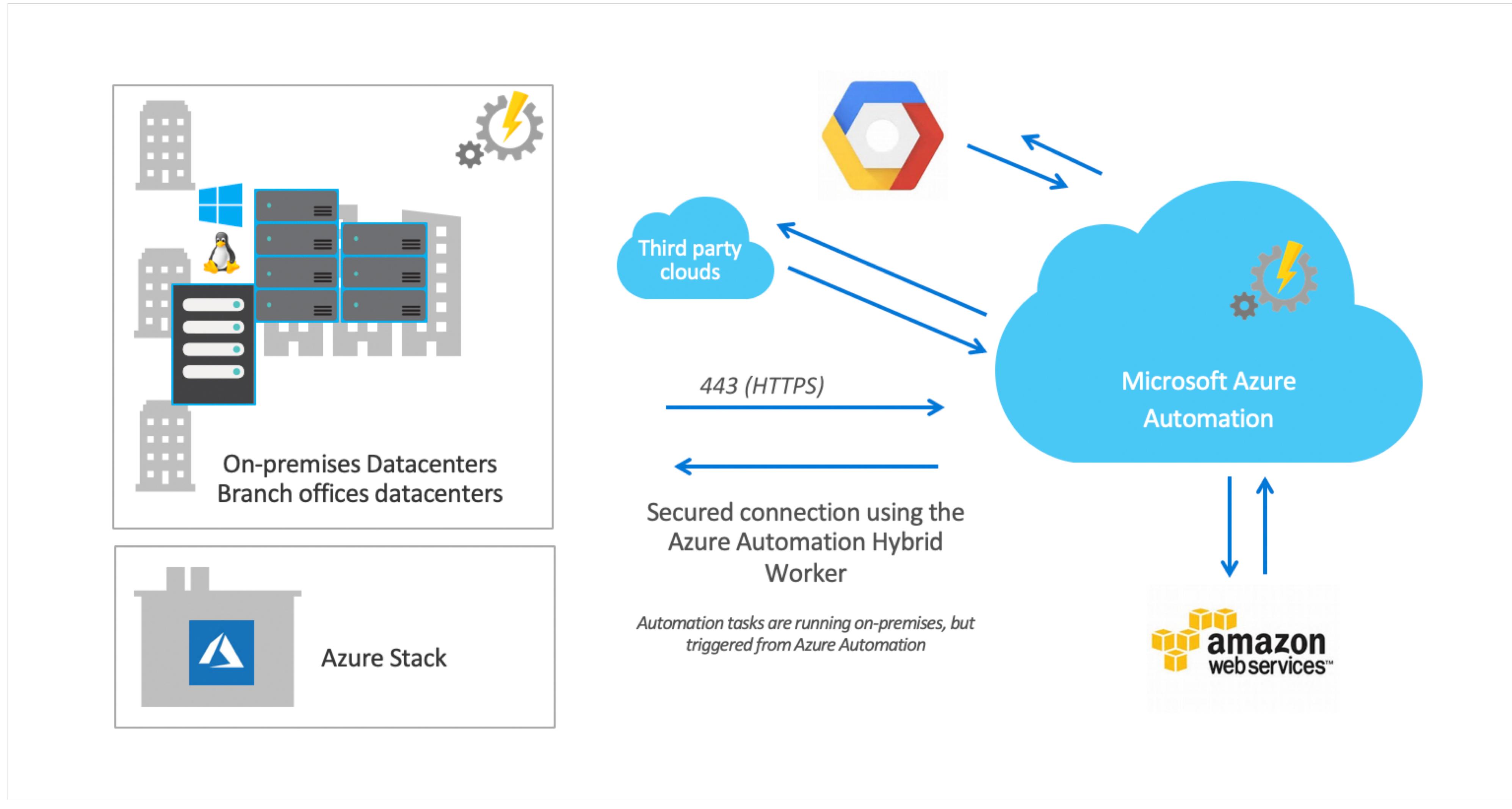
CONFIGURATION MANAGEMENT

- DSC CONFIGURATIONS, PULL SERVICE
- NODE MANAGEMENT & REPORTING

CHANGE TRACKING & INVENTORY

- UPDATE MANAGEMENT:
- INSIGHTS ACROSS A HYBRID ENVIRONMENT
- ORCHESTRATED UPDATES AND TROUBLESHOOTING

AZURE AUTOMATION - FEATURES



AZURE AUTOMATION - DSC

- HOST DSC SCRIPTS AND CLIENTS PULL THEIR CONFIGURATIONS AUTOMATICALLY
- SUPPORT FOR CLOUD OR ON-PREMISES VMS AND HOSTS
- SIMPLE ONBOARD PROCESS FOR AZURE VIRTUAL MACHINES

CHARACTERISTICS & USE CASES:

- IMPORT, AUTHORING, COMPILING
- INTEGRATED SOURCE CONTROL,
- CONTROLLED DISTRIBUTION TO NODES
- REPORTING

AZURE AUTOMATION - DSC

- BUILT-IN INTEGRATION WITH ON-PREMISES SYSTEMS AND POWERSHELL DSC NODES
- RUN AZURE AUTOMATION RUNBOOKS ON-PREMISES
- AUTOMATION ACCESSIBLE VIA NEW REST API (INCLUDING GITHUB, VSO AND ARM)
- GRAPHICAL WORKFLOW-AUTHORING TOOL
- RUNBOOK MANAGEMENT FROM THE NEW MICROSOFT AZURE PORTAL

AZURE AUTOMATION - DSC

AUTOMATION DSC CAN BE USED TO MANAGE VARIOUS MACHINES:

- AZURE VIRTUAL MACHINES RUNNING WINDOWS OR LINUX
- AMAZON WEB SERVICES (AWS) VIRTUAL MACHINES RUNNING WINDOWS OR LINUX
- PHYSICAL/VIRTUAL WINDOWS COMPUTERS ON-PREMISES, OR IN A CLOUD OTHER THAN AZURE OR AWS
- PHYSICAL/VIRTUAL LINUX COMPUTERS ON-PREMISES, OR IN A CLOUD OTHER THAN AZURE OR AWS

```
PowerShell

configuration LAMPServer {
    Import-DSCResource -module "nx"

    Node localhost {

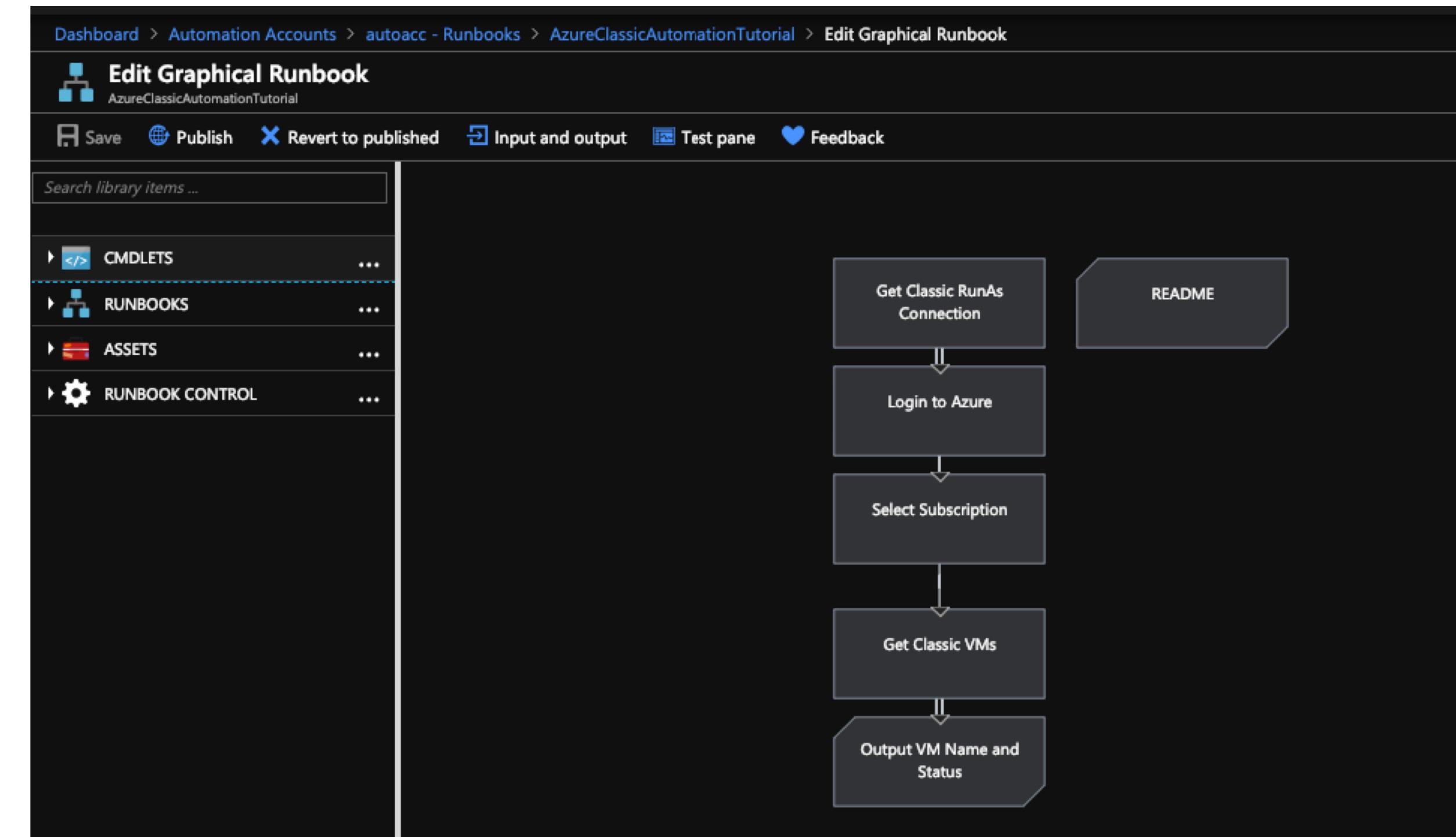
        $requiredPackages = @("httpd","mod_ssl","php","php-mysql","mariadb","mariadb-
$enabledServices = @("httpd","mariadb")

        #Ensure packages are installed
        ForEach ($package in $requiredPackages){
            nxPackage $Package{
                Ensure = "Present"
                Name = $Package
                PackageManager = "yum"
            }
        }

        #Ensure daemons are enabled
        ForEach ($service in $enabledServices){
            nxService $service{
                Enabled = $true
                Name = $service
                Controller = "SystemD"
                State = "running"
            }
        }
    }
}
```

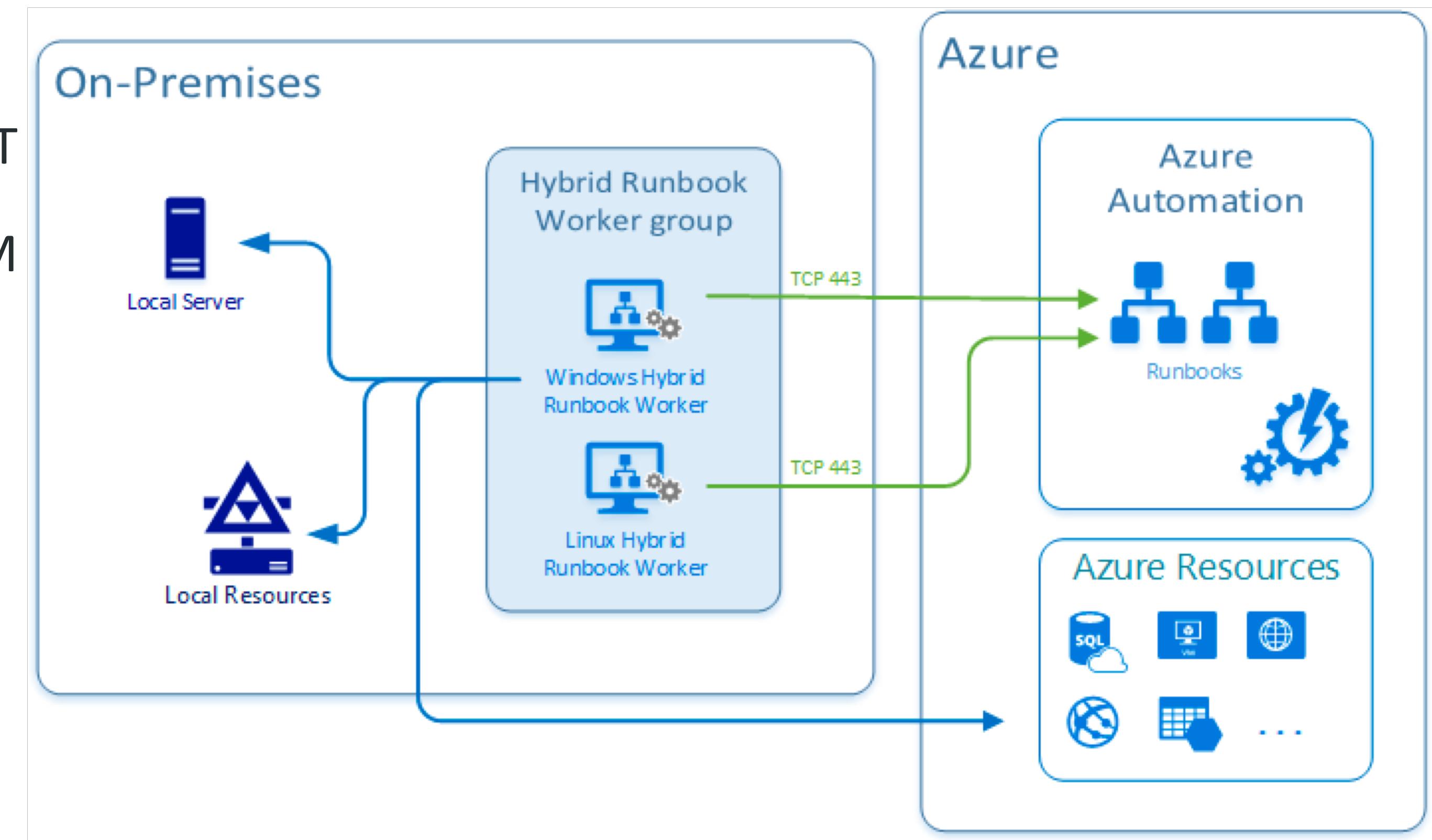
AZURE AUTOMATION - DSC

- BUILT-IN INTEGRATION WITH ON-PREMISES SYSTEMS AND POWERSHELL DSC NODES
- RUN AZURE AUTOMATION RUNBOOKS ON-PREMISES WITH HYBRID NODES – EASY TO INSTALL FUNCTION ON WINDOWS
- AUTOMATION ACCESSIBLE VIA REST API (INCLUDING GITHUB, DEVOPS AND ARM)
- GRAPHICAL WORKFLOW-AUTHORING TOOL – YOU CAN CONVERT GRAPHICAL RUNBOOK INTO CODE ONE
- RUNBOOK MANAGEMENT FROM AZURE PORTAL

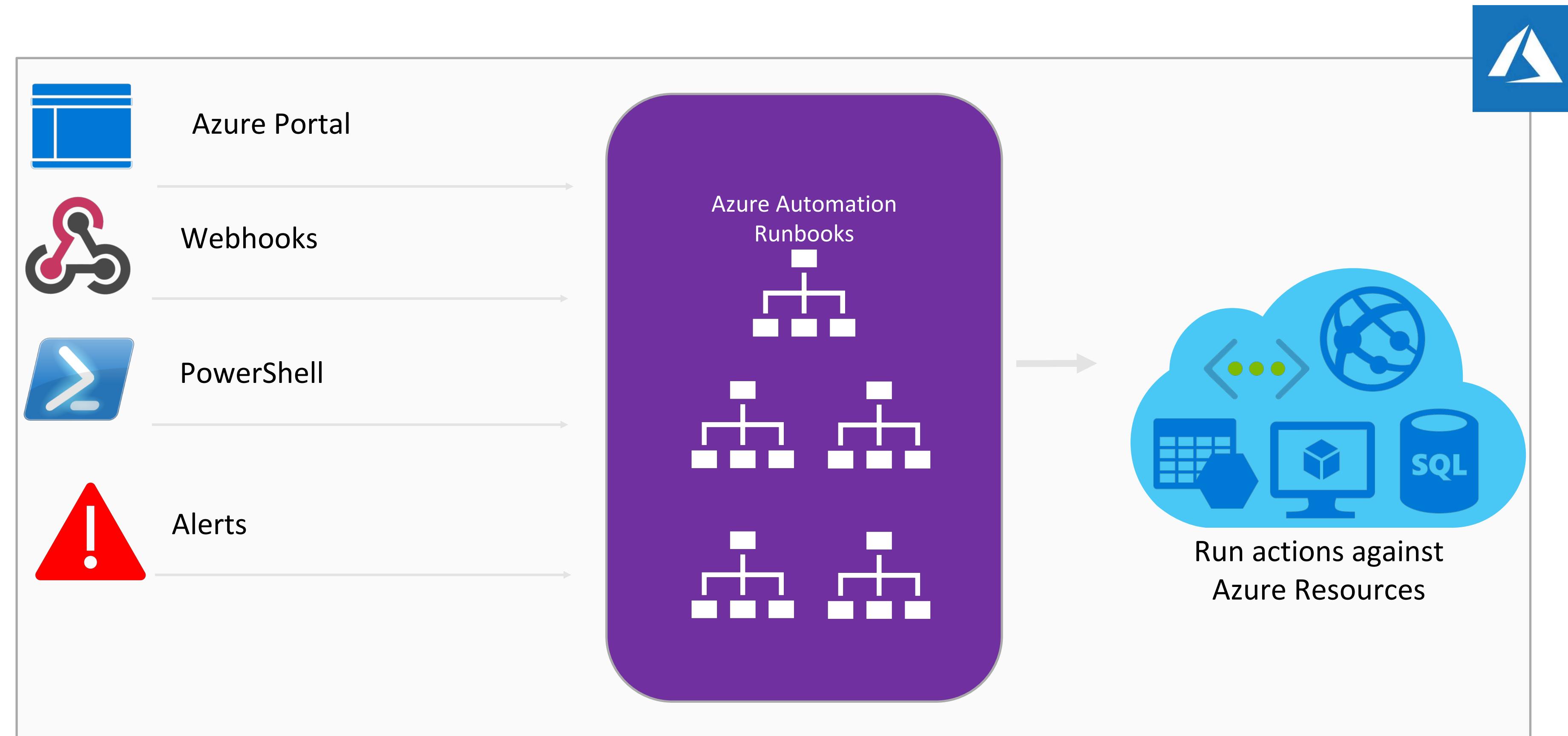


AZURE AUTOMATION - DSC

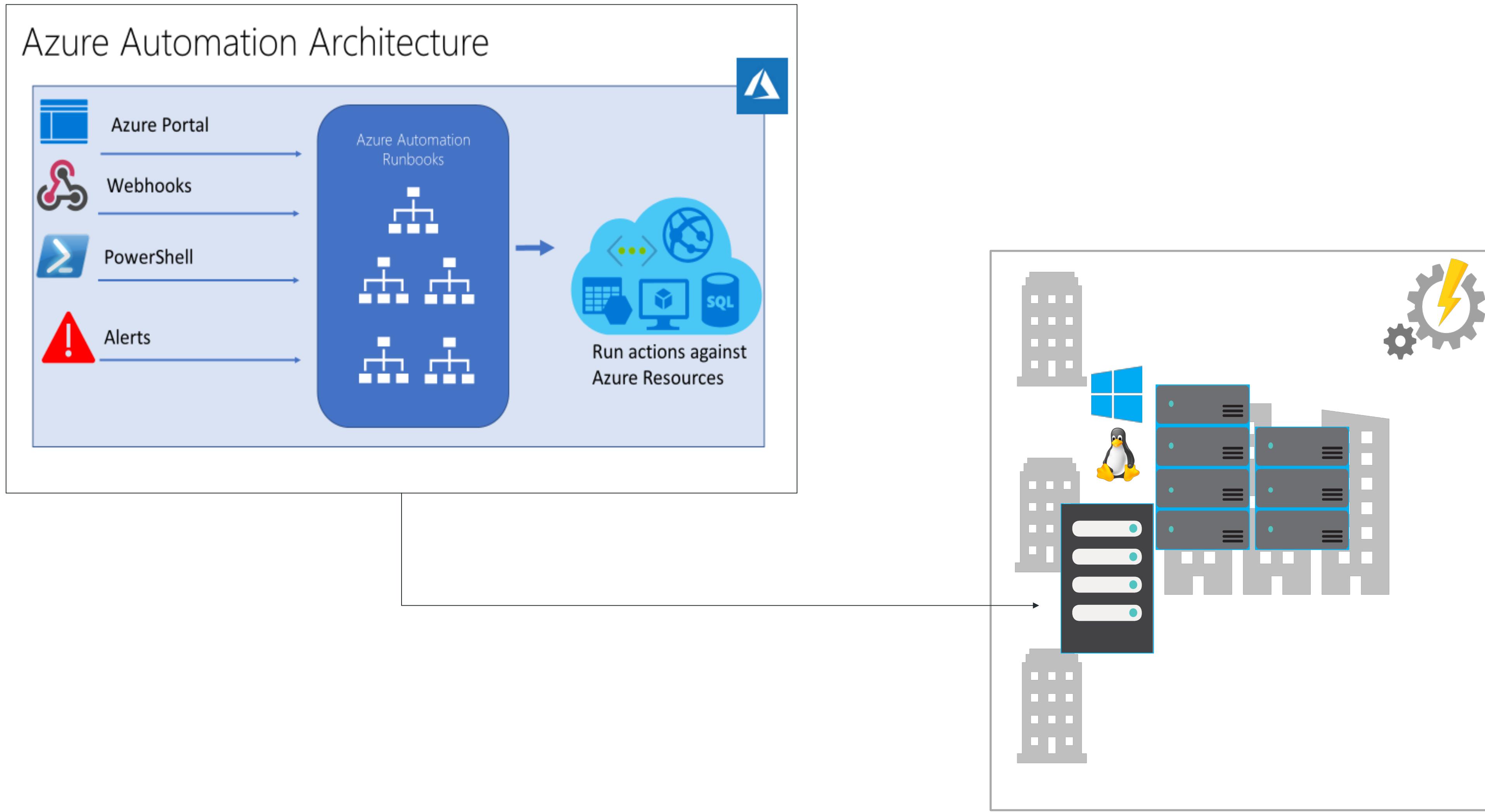
- AN ON-PREM SERVER RUNNING MICROSOFT AGENT
- EXECUTES RUNBOOKS DOWNLOADED FROM AZURE AUTOMATION
- REPORTS RESULTS BACK TO AZURE AUTOMATION AND OMS / LOG ANALYTICS
- CAN BE DEPLOYED IN GROUPS FOR HIGH AVAILABILITY
- REQUIRES NO PORTS (OUTSIDE-IN)



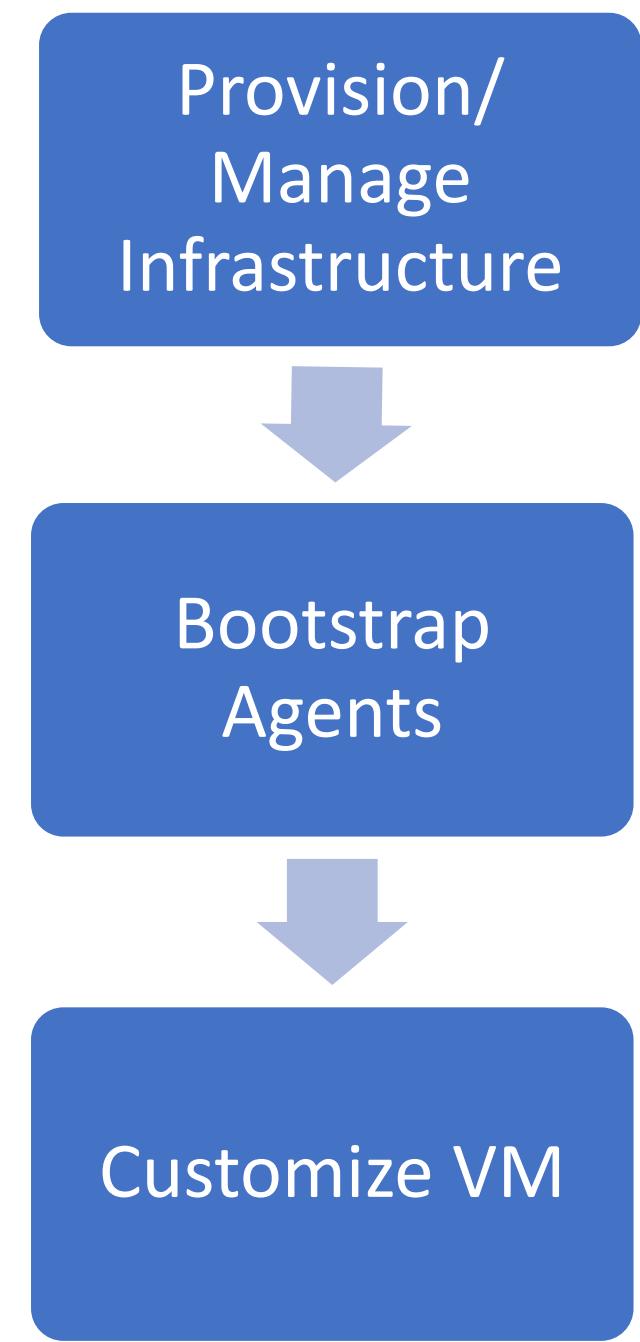
AZURE AUTOMATION - INTEGRATION



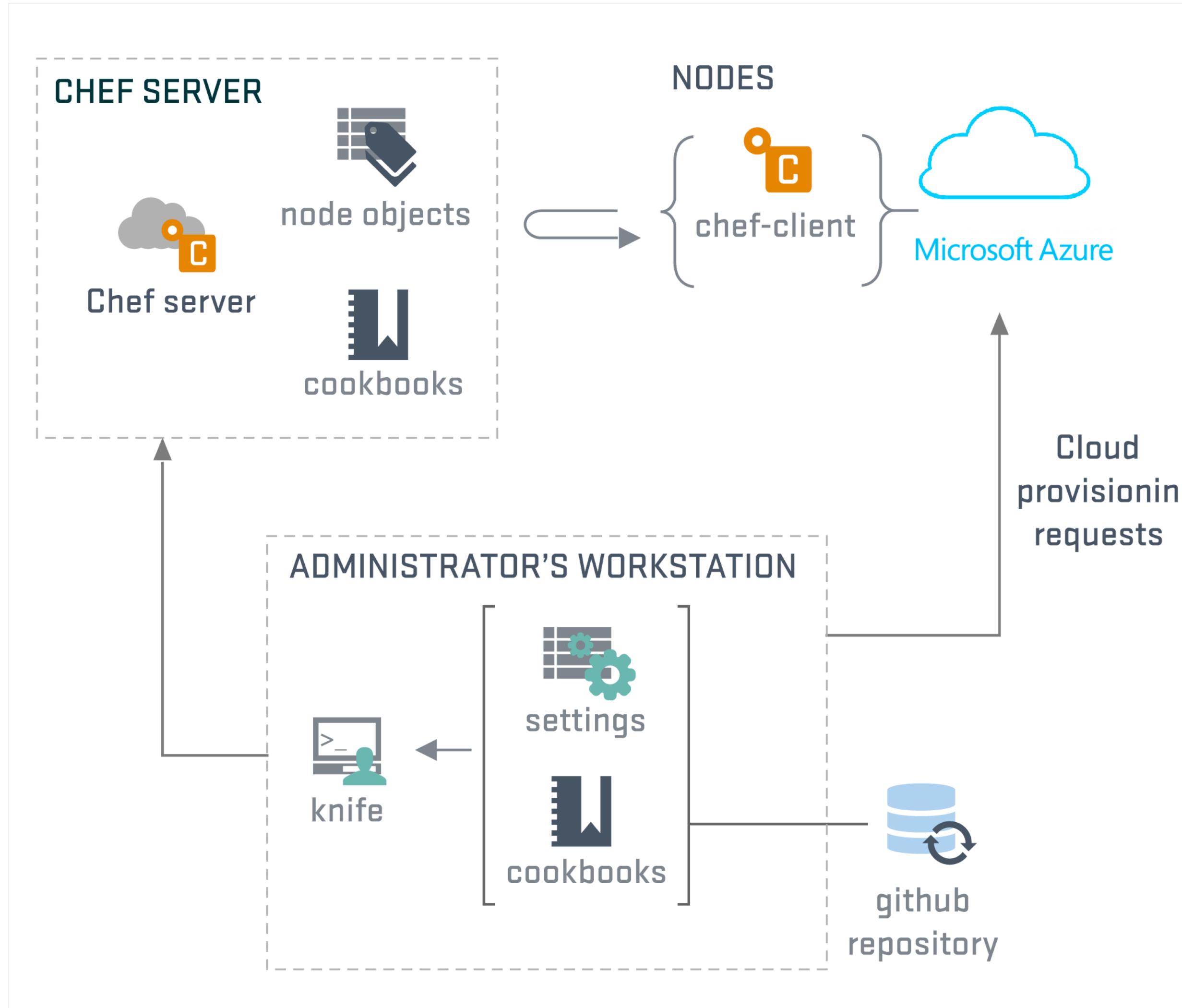
AZURE AUTOMATION - INTEGRATION



OTHER OPTIONS



CHEF ARCHITECTURE

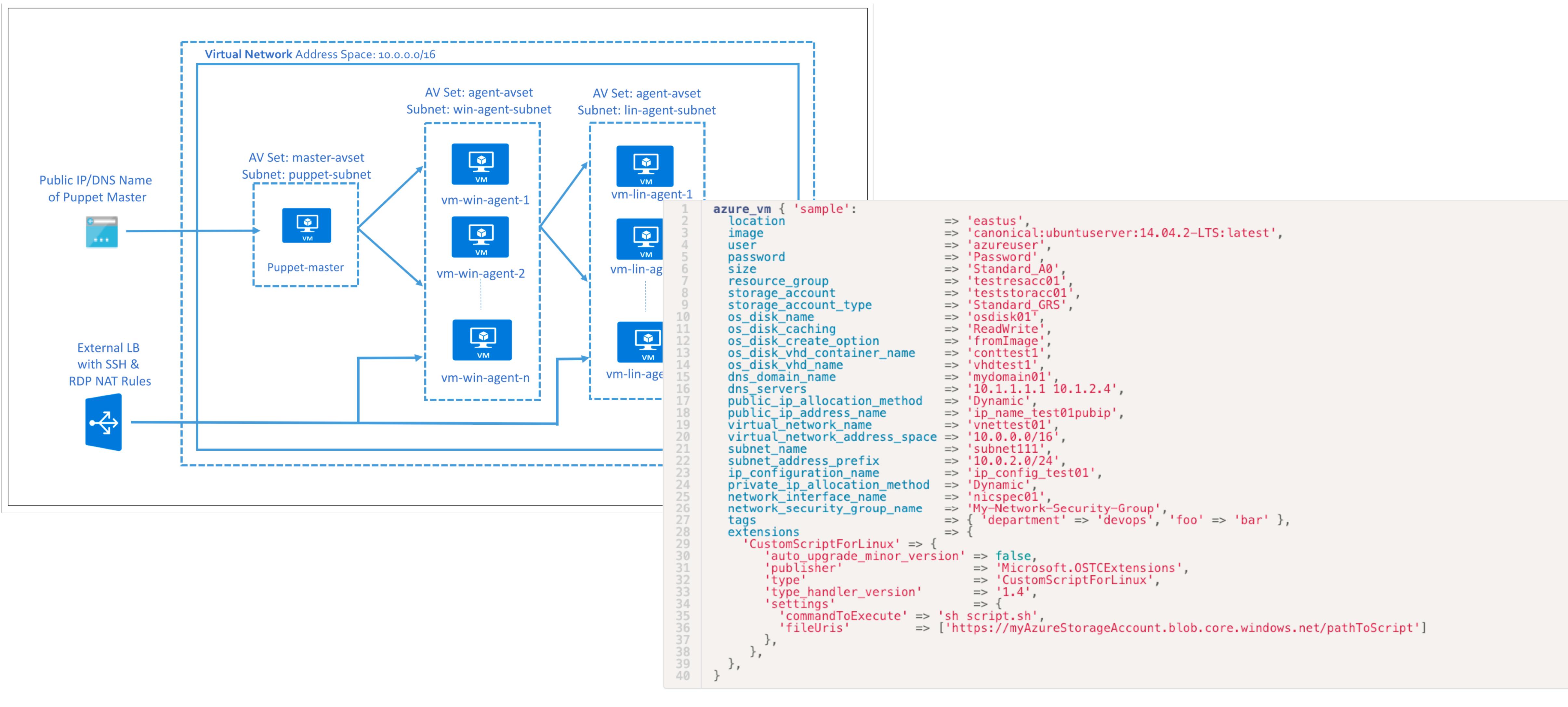


```
powershell_script 'Install IIS' do
  action :run
  code 'add-windowsfeature Web-Server'
end

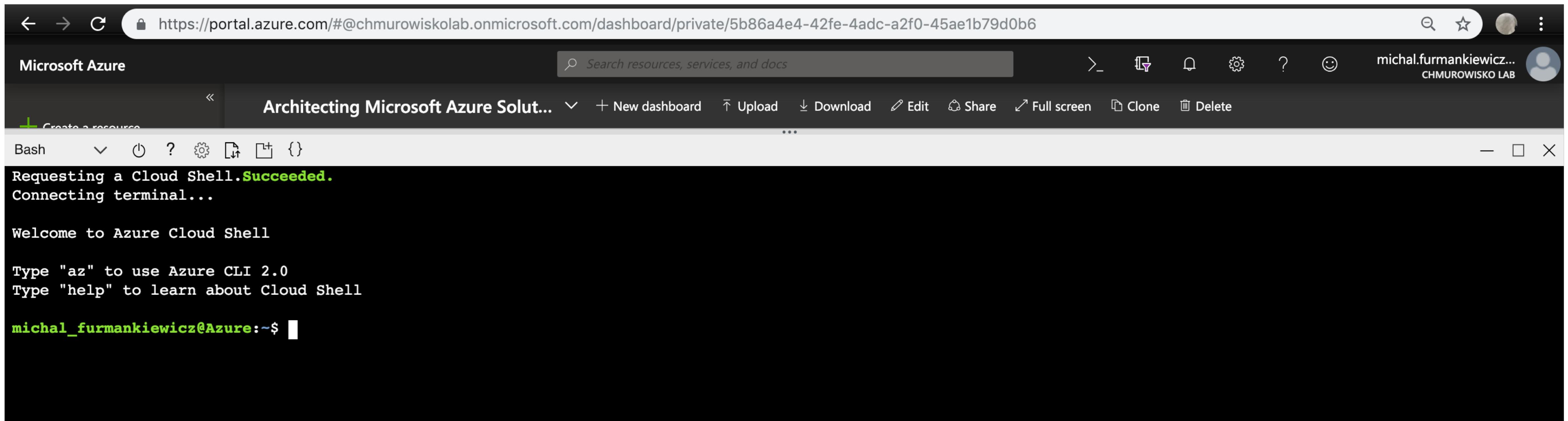
service 'w3svc' do
  action [ :enable, :start ]
end

template 'c:\inetpub\wwwroot\Default.htm' do
  source 'Default.htm.erb'
  rights :read, 'Everyone'
end
```

PUPPET SAMPLE



AZURE CLOUD SHELL



The screenshot shows the Microsoft Azure Cloud Shell interface. At the top, there is a browser header with the URL <https://portal.azure.com/#@chmurowiskolab.onmicrosoft.com/dashboard/private/5b86a4e4-42fe-4adc-a2f0-45ae1b79d0b6>. Below the header, the Microsoft Azure navigation bar includes a search bar, a user profile for michal.furmarkiewicz, and various dashboard actions like '+ New dashboard', 'Upload', 'Download', 'Edit', 'Share', 'Full screen', 'Clone', and 'Delete'. A 'Create a resource' button is also present. The main area is a terminal window titled 'Architecting Microsoft Azure Solut...'. The terminal output shows:

```
Bash
Requesting a Cloud Shell. Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI 2.0
Type "help" to learn about Cloud Shell

michal_furmarkiewicz@Azure:~$
```

AZURE AUTOMATION - SUMMARY

- AZURE AUTOMATION
- AZURE AUTOMATION – DESIRED STATE CONFIGURATION
- OTHER OPTIONS