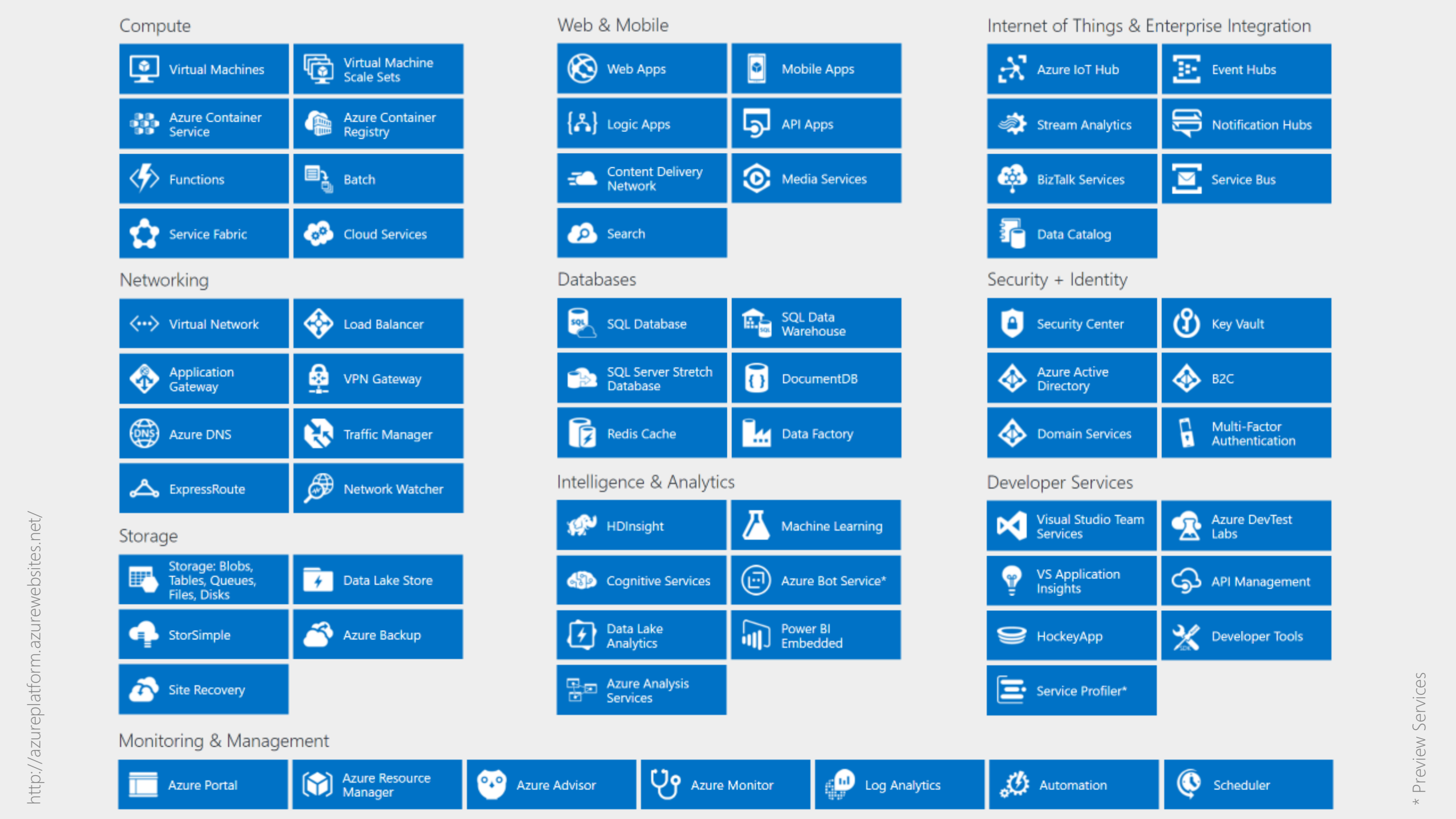
Microsoft

Azure Monitoring and Management

Microsoft Services

Design for Operations (10-15%)

- Design an application monitoring and alerting strategy
  - Determine the appropriate Microsoft products and services for monitoring applications on Azure; define solutions for analyzing logs and enabling alerts using Azure Log Analytics; define solutions for analyzing performance metrics and enabling alerts using Azure Monitor; define a solution for monitoring applications and enabling alerts using Application Insights
- Design a platform monitoring and alerting strategy
  - Determine the appropriate Microsoft products and services for monitoring Azure platform solutions; define a monitoring solution using Azure Health, Azure Advisor, and Activity Log; define a monitoring solution for Azure Networks using Log Analytics and Network Watcher service; monitor security with Azure Security Center
- Design an operations automation strategy
  - Determine when to use Azure Automation, Chef, Puppet, PowerShell, Desired State Configuration (DSC), Event Grid, and Azure Logic Apps; define a strategy for auto-scaling; define a strategy for enabling periodic processes and tasks


Compute
Virtual Machines
Virtual Machine Scale Sets
Azure Container Service
Azure Container Registry
Functions
Batch
Service Fabric
Cloud Services
Networking
Virtual Network
Load Balancer
Application Gateway
VPN Gateway
Azure DNS
Traffic Manager
ExpressRoute
Network Watcher
Storage
Storage: Blobs, Tables, Queues, Files, Disks
Data Lake Store
StorSimple
Azure Backup
Site Recovery
Web & Mobile
Web Apps
Mobile Apps
Logic Apps
API Apps
Content Delivery Network
Media Services
Search
Databases
SQL Database
SQL Data Warehouse
SQL Server Stretch Database
DocumentDB
Redis Cache
Data Factory
Intelligence & Analytics
HDInsight
Machine Learning
Cognitive Services
Azure Bot Service*
Data Lake Analytics
Power BI Embedded
Azure Analysis Services
Internet of Things & Enterprise Integration
Azure IoT Hub
Event Hubs
Stream Analytics
Notification Hubs
BizTalk Services
Service Bus
Data Catalog
Security + Identity
Security Center
Key Vault
Azure Active Directory
B2C
Domain Services
Multi-Factor Authentication
Developer Services
Visual Studio Team Services
Azure DevTest Labs
VS Application Insights
API Management
HockeyApp
Developer Tools
Service Profiler*
Monitoring & Management
Azure Portal
Azure Resource Manager
Azure Advisor
Azure Monitor
Log Analytics
Automation
Scheduler
http://azureplatform.azurewebsites.net/
* Preview Services

Azure Monitoring and Management

- Azure Monitor
- Azure Advisor
- Azure Service Health
- Azure Network Watcher
- Azure Log Analytics
  - Service Map
  - Traffic Analytics
  - Network Performance Monitor
  - Other Solutions ….
- Azure Security Center
- Azure Application Insights
- Azure Automation
- Event Grid
- Azure Backup
- Azure Site Recovery
- Azure Cost Management (ACM)

Microsoft

Azure Monitor

Microsoft Services

Azure Monitor Overview

Provides a single source for the monitoring of Azure resources

Gives insight into

Metrics

Activity and Diagnostic Logs

Alerts from different sources including Azure Monitor, Log Analytics and Application Insights

Fast metric pipeline enabling time critical alerts and notifications

Activity Log

Provides insight into all operations performed on resources within the subscription

Information includes

- Operation performed
- Time
- User or service performing the operation

Who, what, when!

JSON can be viewed of exactly what change occurred

Queries can be created and saved/pinned

Logs are stored for 90 days

Diagnostic Logs

Azure has a vast number of services and resources

While Azure Monitor collects large amounts of data not everything is available

Diagnostic logs are a resource-level logs providing insight into operations within the specific resource

Resource-level diagnostic logs can be exported to

- Azure Storage
- Log Analytics Workspace
- Event Hubs

Configured via the Diagnostics settings centrally in Azure Monitor (or directly on each resource via its Diagnostics logs setting)

Metrics

Enable visibility into the performance and health of workloads via the metrics (performance counters) emitted by most resources

Default of one-minute frequency and are automatically available

Azure Monitor provides a central location to view metrics for all resources within the subscription

Guest Metrics

For VMs host metrics are available (including VM Scale Sets)

Through the IaaS Diagnostics extension guest level metrics in addition to various logs can also be collected

Log data is sent to a storage account which can also be ingested by Application Insights and Event Hub

Dashboards

status.azure.com provides a high level overview of service health

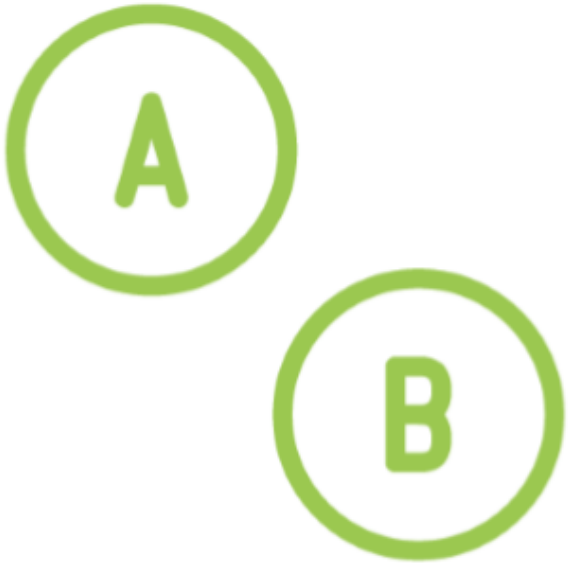
The Azure portal supports multiple dashboards

Charts can be added along with other Azure resources

Dashboards can be downloaded and uploaded in JSON format

Dashboards can be shared with access control to restrict who can utilize

Action Groups



Enable a series of actions to be defined

Action Groups can then be used by multiple Alerts

An Action Group is made up of one or more actions which is:

- Name for the action (which must be a unique identifier)
- An Action Type
- Details of the action

Action Types can trigger automated actions, contact groups and integrate with ITSM systems

Alerts

Provides a unified alert experience across multiple subscriptions and from multiple sources including metrics, certain logs and Log Analytics

Log Analytics uses Azure Monitor Alerts for its alerting but automatically selects the current workspace

Alerts are available in the Azure portal

Alerts can be created using multiple metrics

Trigger Action Groups

Microsoft

Azure Advisor

Microsoft Services

Advisor recommendations

Download as CSV | Download as PDF | Configure

Subscriptions: 1 of 5 selected – Don't see a subscription? Open Directory + Subscription settings

Microsoft Azure Internal Consumption | All types | Active | No grouping

Overview | High Availability (4) | Security (11) | Performance (0) | Cost (0) | All (15)

High Availability

4 **Recommendations**

0 High impact | 3 Medium impact | 1 Low impact

10 **Impacted resources**

Security

11 **Recommendations**

11 High impact | 0 Medium impact | 0 Low impact

15 **Impacted resources**

Performance

0 **Recommendation**

0 High impact | 0 Medium impact | 0 Low impact

You are following all of our performance recommendations

See all performance recommendations

Cost

0 **Recommendation**

0 High impact | 0 Medium impact | 0 Low impact

You are following all of our cost recommendations

See all cost recommendations

Microsoft

Azure Service Health

Microsoft Services

Home > Service Health - Service issues

Service Health - Service issues

Search (Ctrl+/)

ACTIVE EVENTS

- Service issues
- Planned maintenance
- Health advisories

HISTORY

- Health history

RESOURCE HEALTH

- Resource health

ALERTS

- Health alerts

Select filter ...

* Subscription: 5 selected
* Region: 28 selected
* Service: 140 selected

Save filter | Delete filter | Pin filtered world map to dashboard | Create service health alert

No service issues found

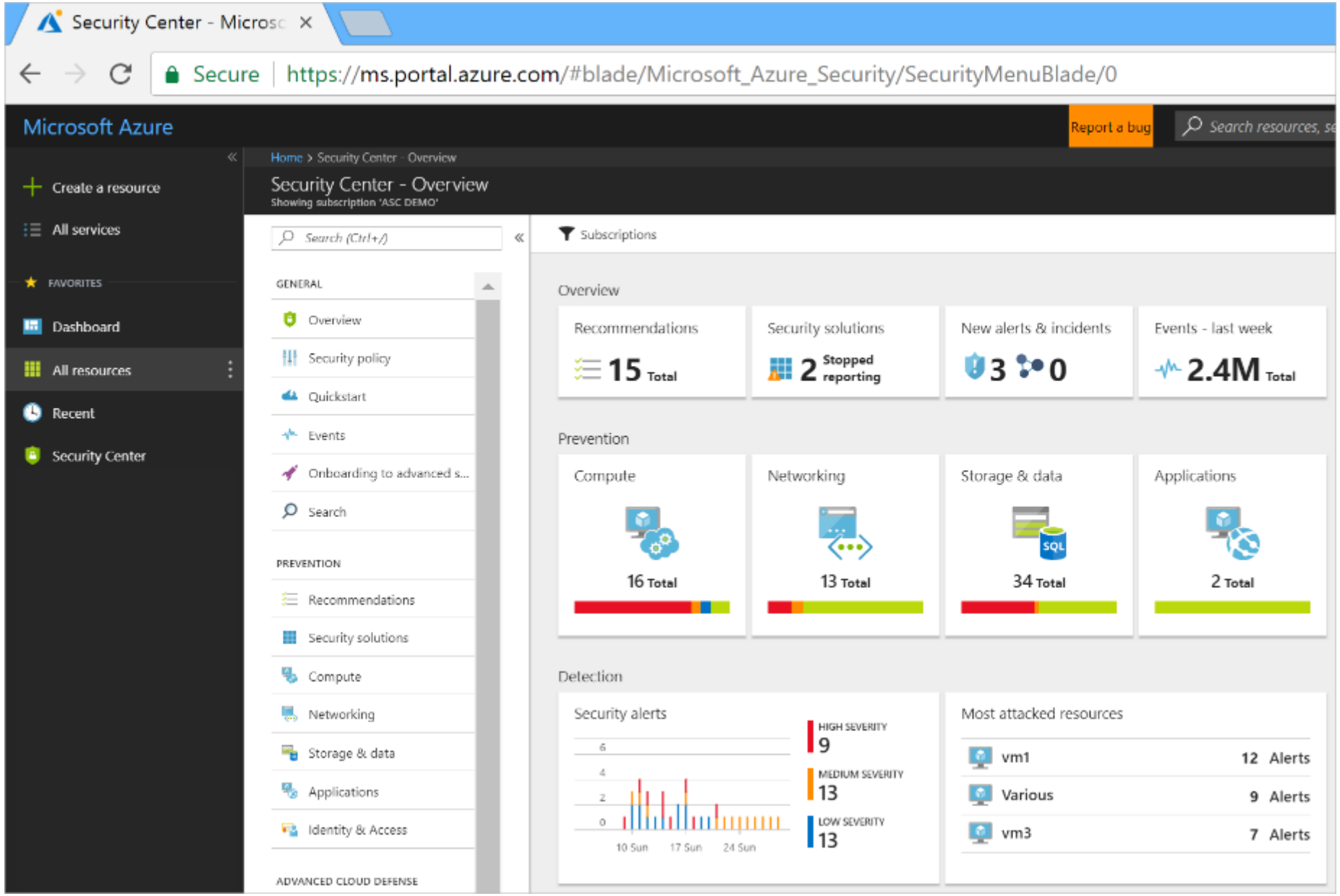
See all past issues in the health history.

Launch guided tour

Microsoft

Azure Security Center

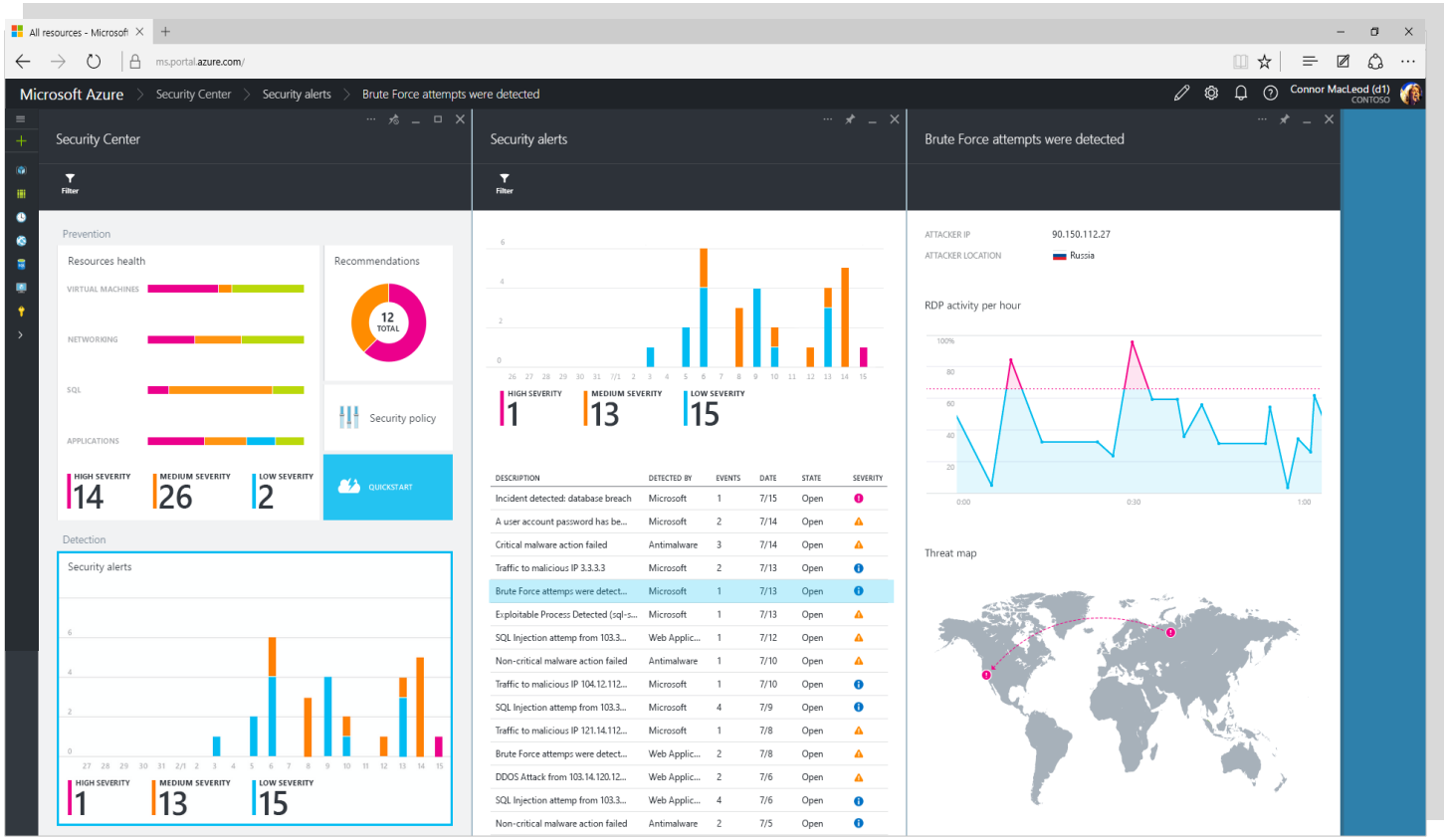
Microsoft Services



https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

Azure Security Center

- Monitor the security state of resources
- Prioritized recommendations
- Easily deploy partner security solutions
- Security policies for subscriptions and resource groups
- Central view of your security posture
- Prioritized security alerts



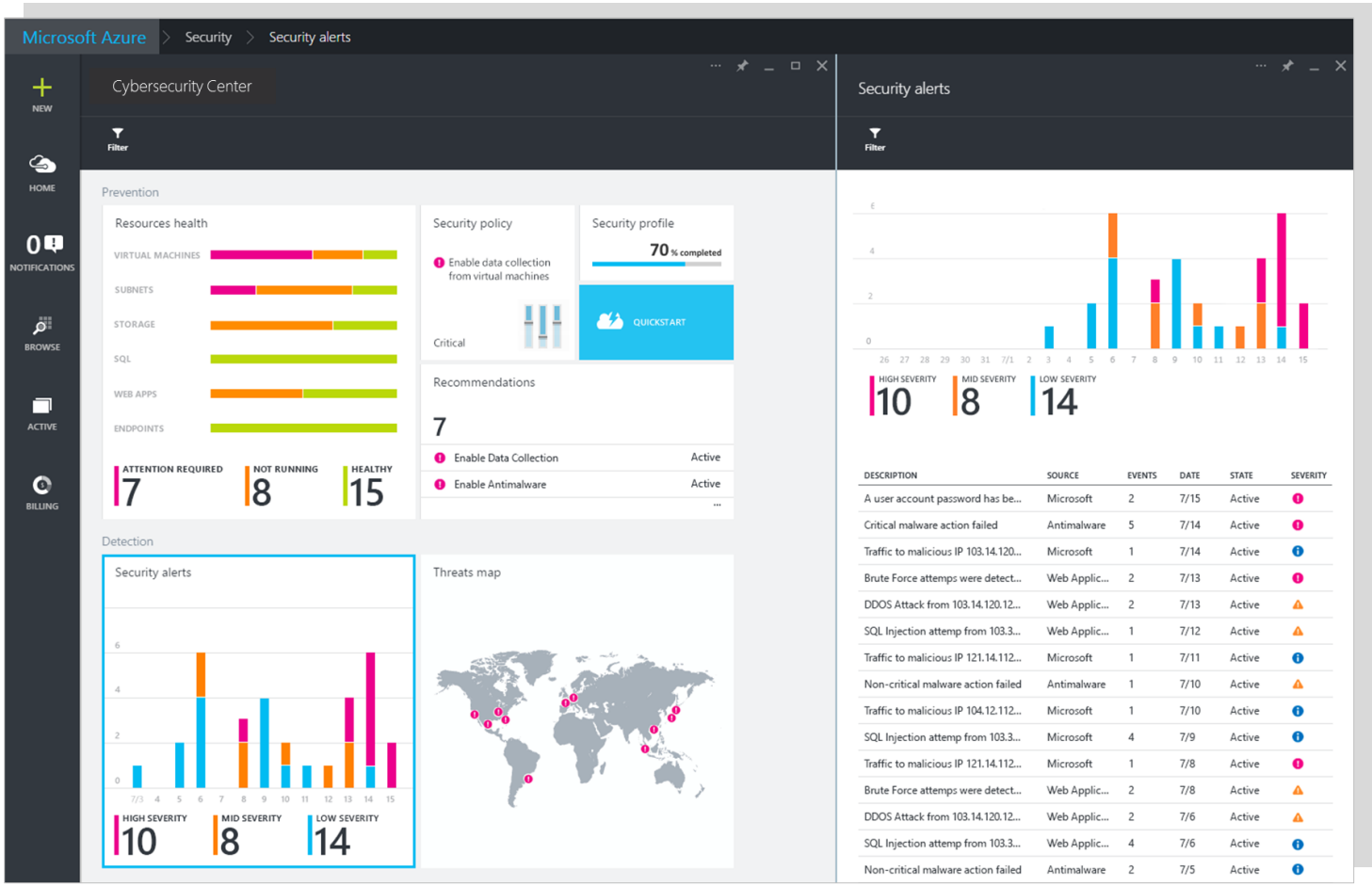
Azure Security Center

Advanced Prevention

- Application whitelisting
- Just-in-time network access to VMs

Advanced Threat Detection

- Brute force detections
- Outboard DDoS Botnet Detection
- New behavioral analytics servers and VMs to identify suspicious activity
- Azure SQL database threat detection



https://azure.microsoft.com/en-us/blog/preview-the-new-enhancements-to-azure-security-center/

Microsoft

Azure Network Watcher

Microsoft Services

Azure Network Watcher

Large number of capabilities:

- Topology Viewer
- Packet Capture (via an agent installed into VM)
- IP Flow Verify and Next Hop Determination
- Connection Monitor and Troubleshoot

Full RBAC support

Azure Network Watcher

Large number of capabilities:

Security Group View

NSG Flow Logging

Virtual Network Gateway and Gateway Connection Troubleshooting

Network Use Against Subscription Limits

Full RBAC support

Network Watcher

New

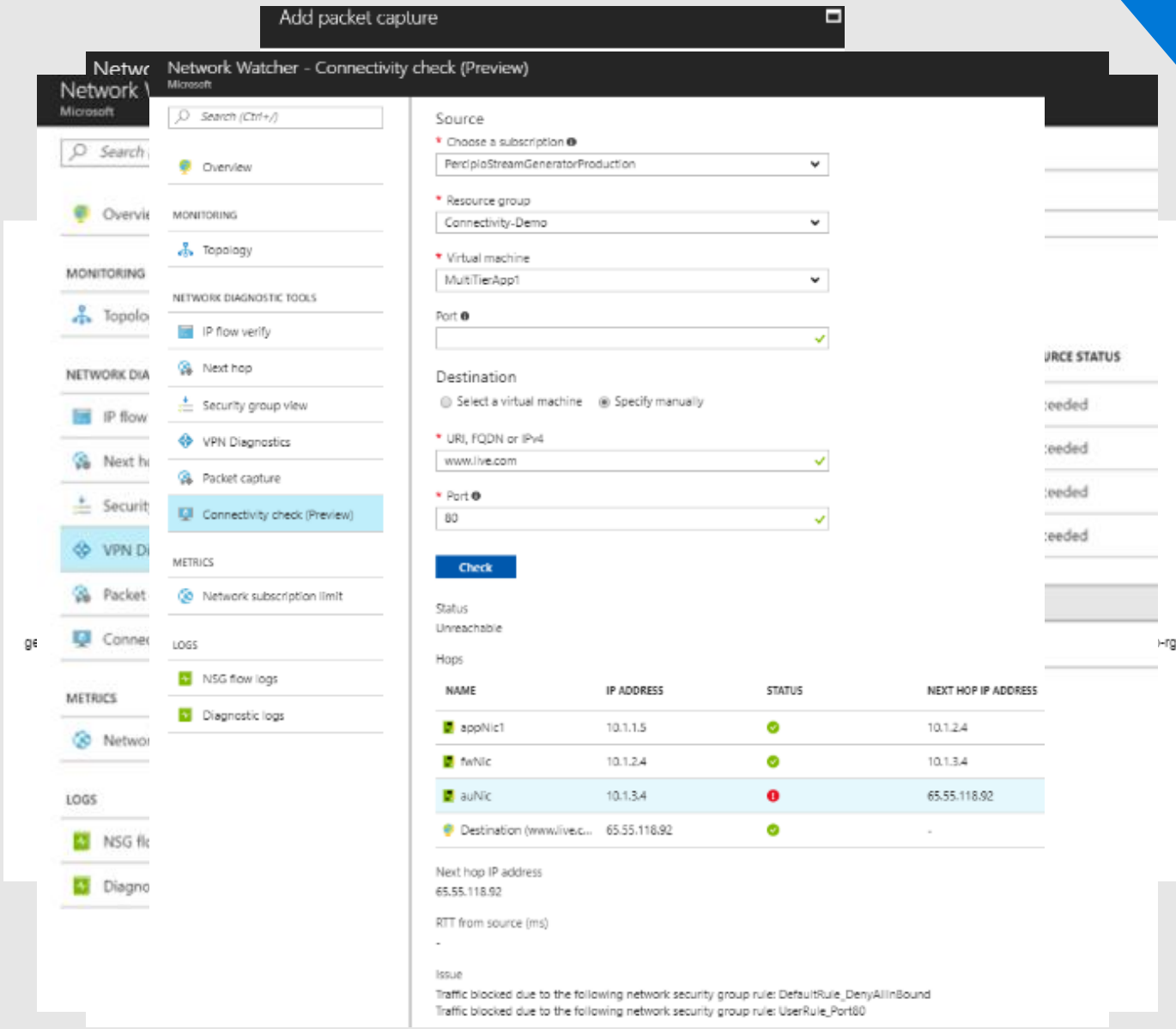
Topology
- Visualize your network

Packet Capture
- Initiate packet capture from portal or programmatically
- Captures stored in .cap format

IP Flow Verify
- Identify configured NSG rules blocking traffic

VPN Diagnostics
- Troubleshoot VPN Gateway and Connections and identify issues like
  - Preshared Key mismatch
  - Unsupported IKE policies
  - Gateway Unreachable
  - Gateway instance under maintenance

Connectivity
- Diagnose connectivity and latency issues between VM and an Endpoint (VM, FQDN, URI, IPv4 Address)
- Identify configuration issues impacting connectivity



Microsoft

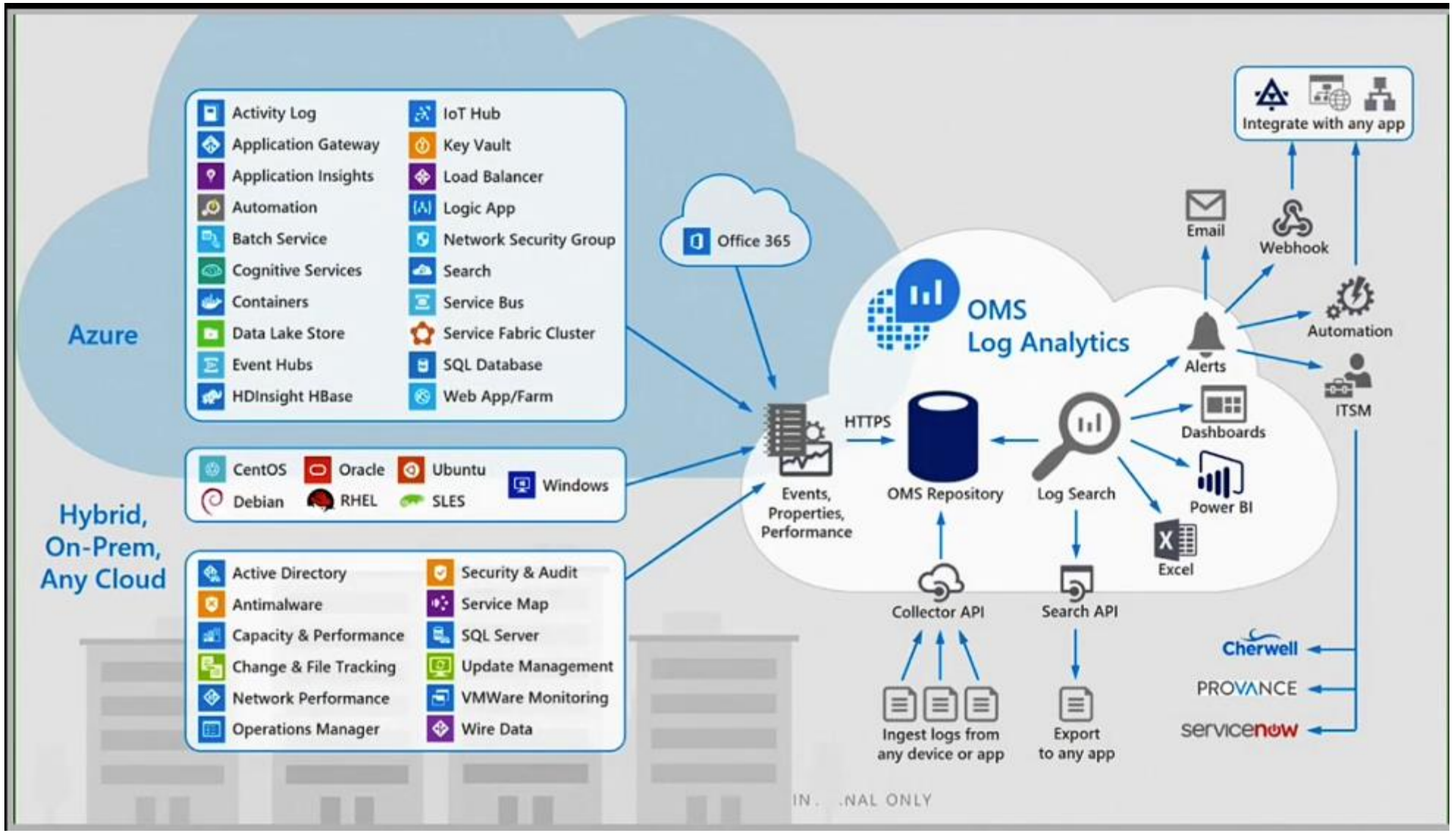
Azure Log Analytics

Microsoft Services

Log Analytics Overview

- Log Analytics ingests logs from a large number of sources and in different formats including metrics typically in Azure Monitor
- A workspace is an instance of Log Analytics and multiple workspaces can exist within a subscription
- Queries are executed against the logs to produce insight into the state of systems
- Management solutions build on the logs and queries to offer service based insight, for example AD health, patch status and SQL best practices
- Data can be retained for a configurable period

Log Analytics



Compute Resources

For Azure IaaS VMs connect to Log Analytics using the Microsoft Monitoring Agent extension which can be configured as part of JSON template

For Azure PaaS services utilize the Azure Diagnostics Logs & Metrics

For non-Azure VMs install the Microsoft Monitoring Agent and configure the workspace

MMA for Windows can be multi-homed enabling it to communicate with multiple workspaces (and System Center Operations Manager environments)

Data Sources

- Each workspace can be configured to receive data from storage logs, Azure activity logs, storage accounts and specific resources
- Data collected can be customized via the Advanced Settings which can include
  - Windows Event Logs/Syslogs
  - Windows and Linux Performance Counters
  - IIS Logs
  - Custom Fields and Custom Logs
- Deployed Management Solutions may also add additional collected data

```
Perf
| where CounterName == '% Processor Time'
```

Performing Queries

Kusto is the query language used to query Log Analytics

A typeful query language with intellisense

Very logical structure similar to SQL

Performing Queries

Large number of built in queries to help get started

Advanced Analytics interface which includes schema pane with different data sources available and their tables/attributes

Results can be pinned to custom dashboards

Visualizing Data with PowerBI

Data sets can be used as data inputs for PowerBI

The visualization capabilities of PowerBI can then be leveraged on the data in addition to its own insight capabilities

Triggering Alerts from Log Analytics

This uses the Azure Monitor alert capabilities

Alerts created in a Log Analytics workspace are actually just Azure Monitor alerts focused on the Log Analytics workspace as the target

Management Solutions

- Management Solutions provide a collection of:
  - Rules to acquire data
  - Logic to interpret the data
  - How to visualize the data
- Management Solutions are added to the workspace
- Exposed via Azure Marketplace and within the workspace via Workspace summary – Add
- The queries used by the solution can be viewed!

Log Analytics

Microsoft

Update Management

Microsoft

OMS Network Performance Monitor

Utilizes synthetic transactions to detect and locate network performance bottlenecks

Provides overviews of network health and detailed drill downs

Utilizes agents on OS instances to provide deep insight including ExpressRoute topology and health

Can view trend data over configurable time ranges

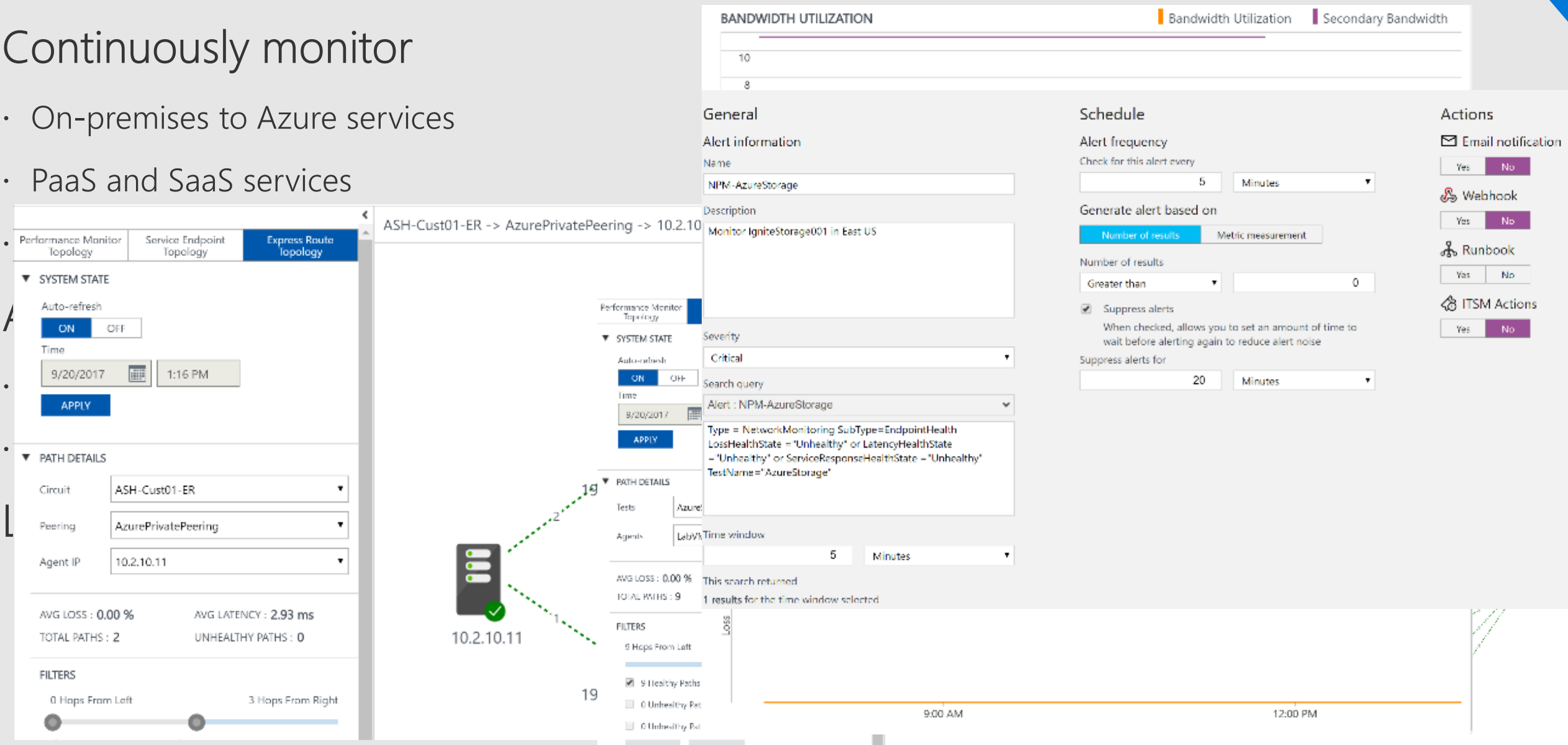
Built on Log Analytics enabling custom reporting

Network Performance Monitor for ExpressRoute

New

Continuously monitor

- On-premises to Azure services
- PaaS and SaaS services



Azure Traffic Analytics

Built on top of Network Watcher

Provides analytics of traffic passing through the cloud network as an integrated service

Provides customers knowledge about their environment to assist with: Security, Capacity, Performance

Microsoft

Azure Application Insights

Microsoft Services

Why do we need Application Insights?

As infrastructure people we can gather logs but that requires the application to write interesting information to the file, e.g. IIS logs

APM solutions enable the developers to leverage provided SDKs (or not) without having to instrument their own monitoring solutions

How does it talk to the application?

The Application Insights SDKs must be attached to the codebase

This enablement can be done in a number of ways

- **Runtime Monitoring (similar to an agent)**
  - The Azure extension can be used for App Services
  - The Status Monitor can be installed into a VM running the application for IIS and J2EE servers
- **Development Time**
  - The developer includes Application Insights as part of the project

Not Restricted to Visual Studio

For example adding into a Node.js application

Install App Insights SDK's using npm

- npm install --save applicationinsights

Add 2 lines of code to enable monitoring

- let appInsights = require('applicationinsights');
- appInsights.setup("fe1dfe20-fc17-425a-9e77-2f30d68dba7f").start();

Application Monitoring

Application Insights constantly monitors the application for performance and problems

Can perform analytics (using Kusto) with machine learning to understand anomalies and then alert on those

Baselines are established and if the baseline is stepped outside above or below then notified

Monitoring for the application can be done from within Visual Studio or from the portal

Alerts can be created to proactively notify to enable resolution before customers impacted with granular detail of the cause

Application Insights Availability Monitoring

- Can perform end-point monitoring of services using Azure's global foot print
- This can monitor ANY service, not just those that are .NET/J2E
- Can ping your site and report on availability and time taken
- More advanced test allowing synthetic transactions if the developer has enabled within their application

Application Insights Application Map

Creates application dependency map

Works via the codebase monitoring

Understands when a function call in .NET via HTTP/HTTPS to a service means its dependent on that

Calls are all prebuilt in .NET which means it understands what it means

Microsoft

Azure Backup

Microsoft Services

Azure Backup enables and solves…

Azure

100 Encrypted VMs

100 SQL in IaaS VMs

200 Linux App VMs

10 Azure File Shares

On-Premises

1 vCenter with 500+ VMs

Active Directory RODC

File Server

Remote Offices

Active Directory RODC

File Server

Customer Challenges

Cost

Security

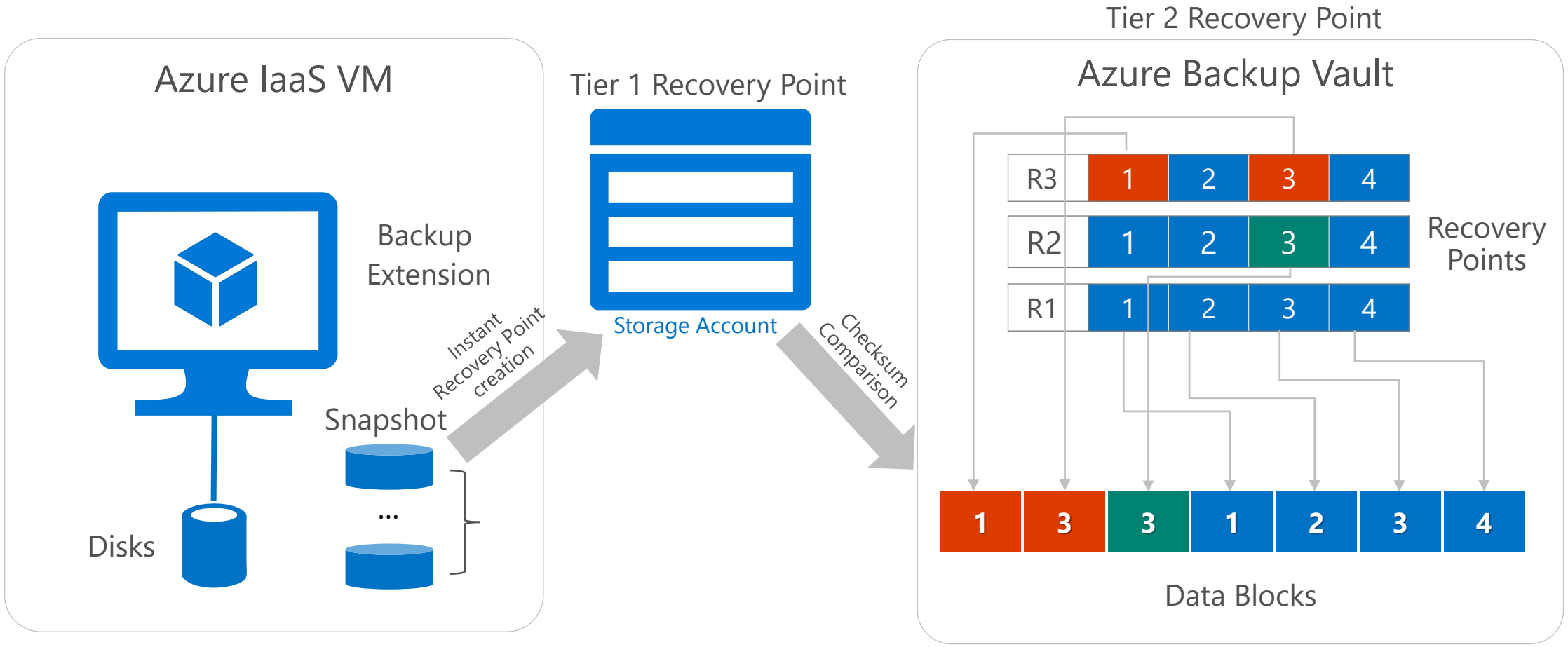
Compliance

Send Quickly

Recover Quickly

Management at Scale

Azure Backup

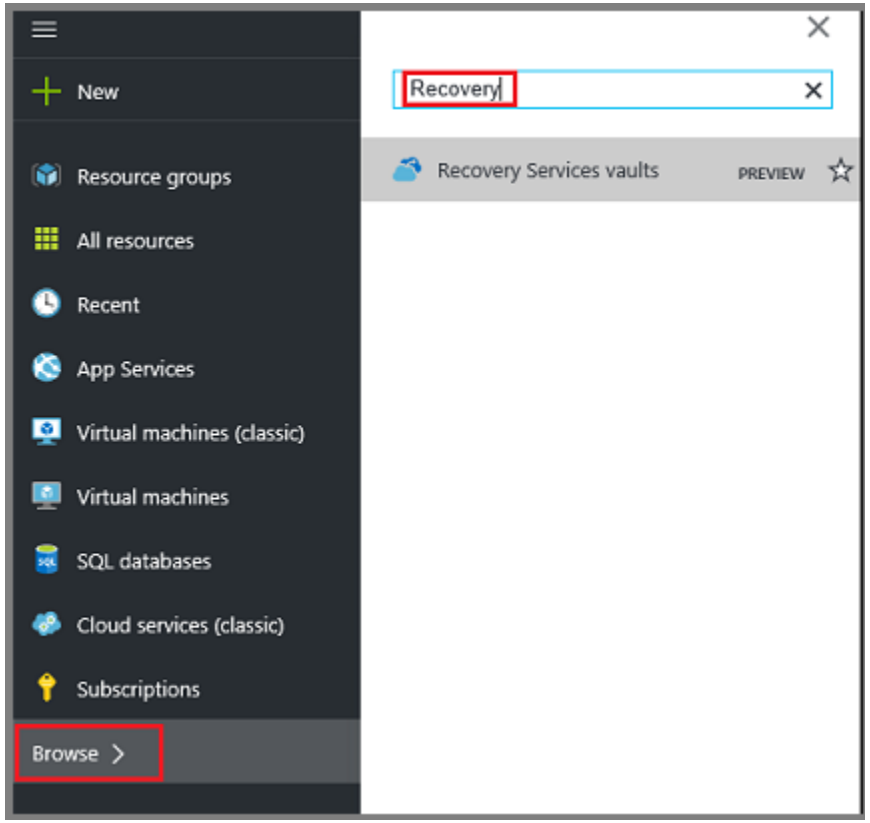


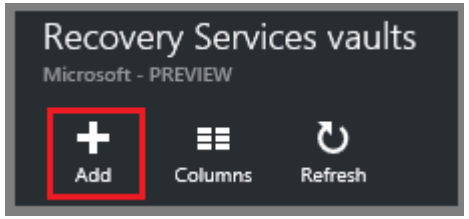
Lightning Fast Backups

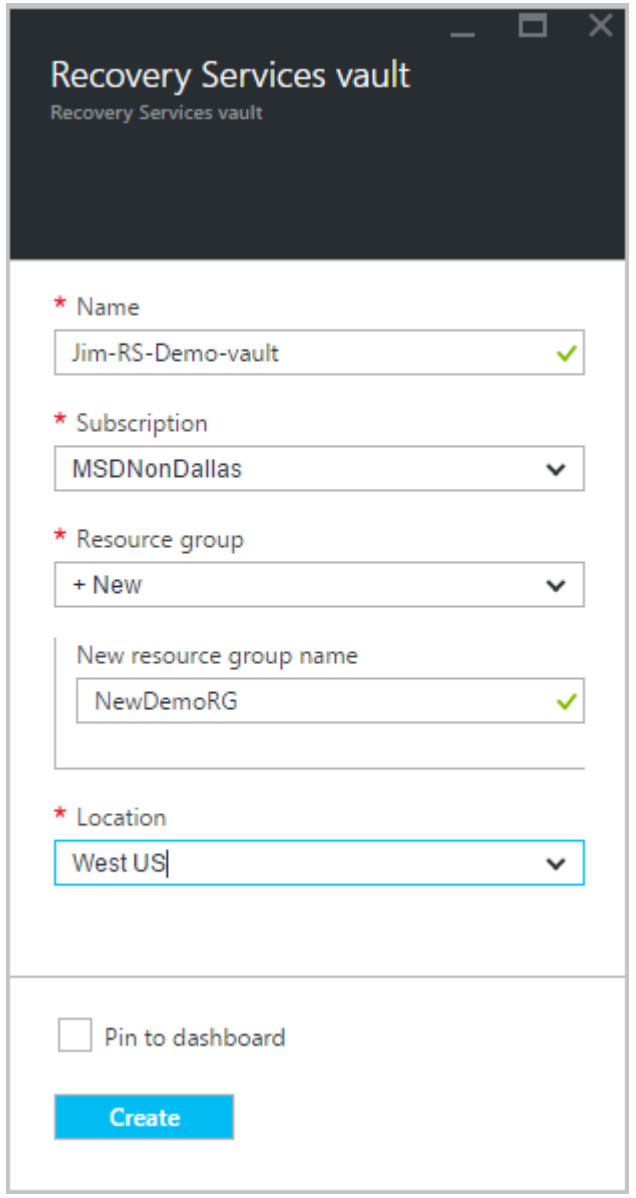
Ideal for Patch Scenarios

Full Restore Fidelity

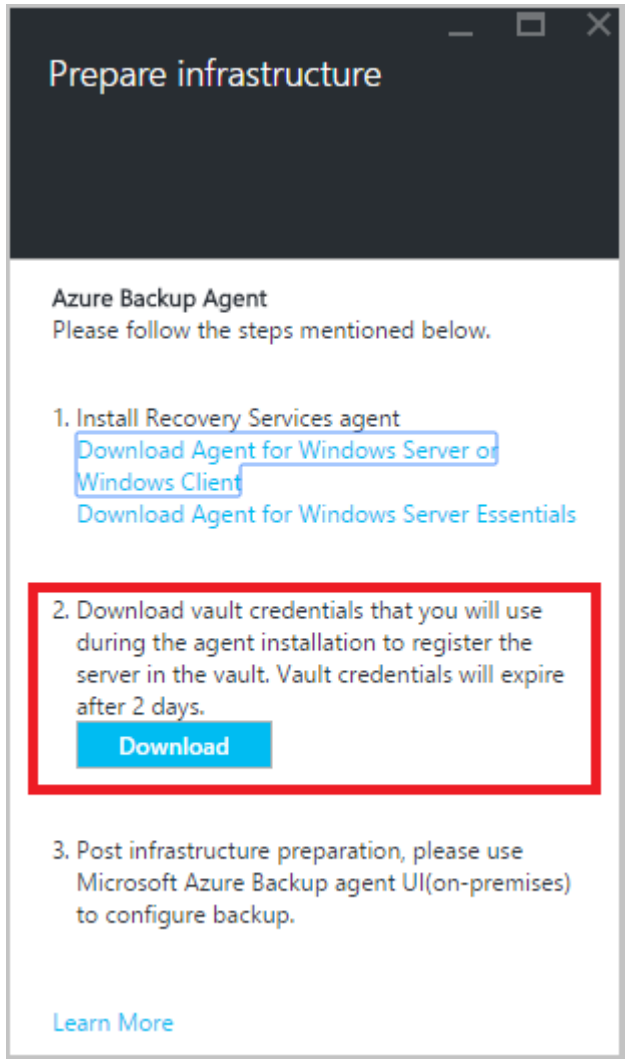
Create a Recovery Services Vault



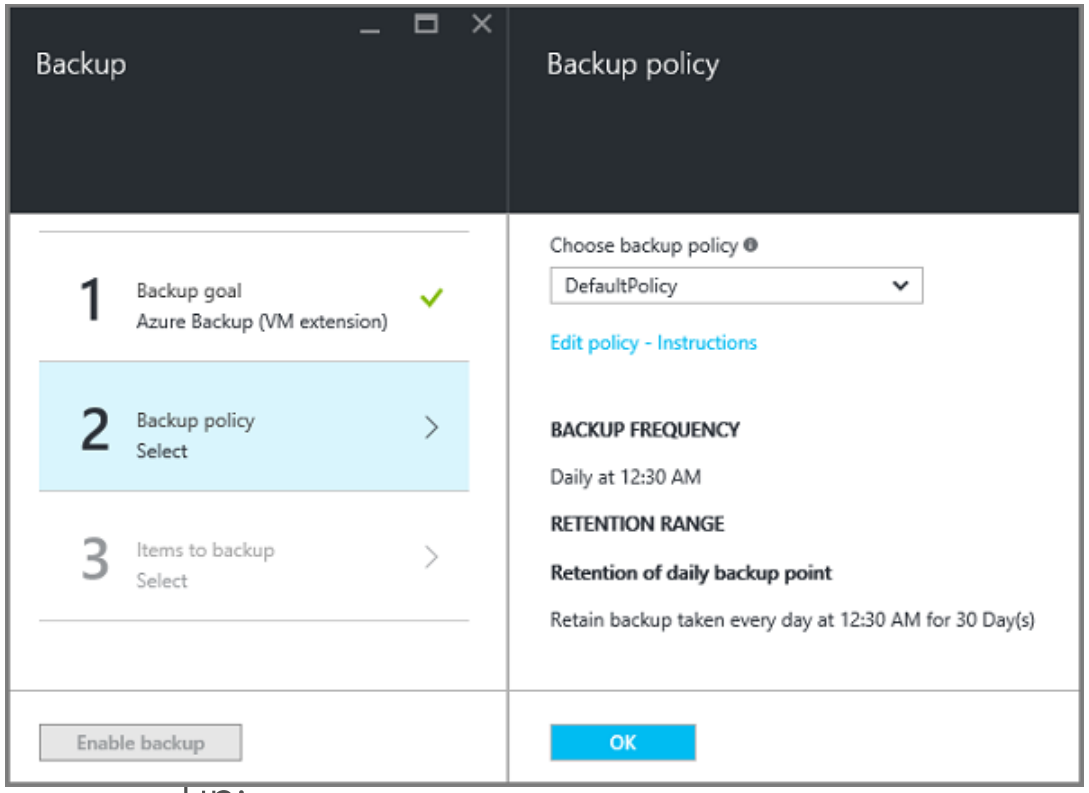


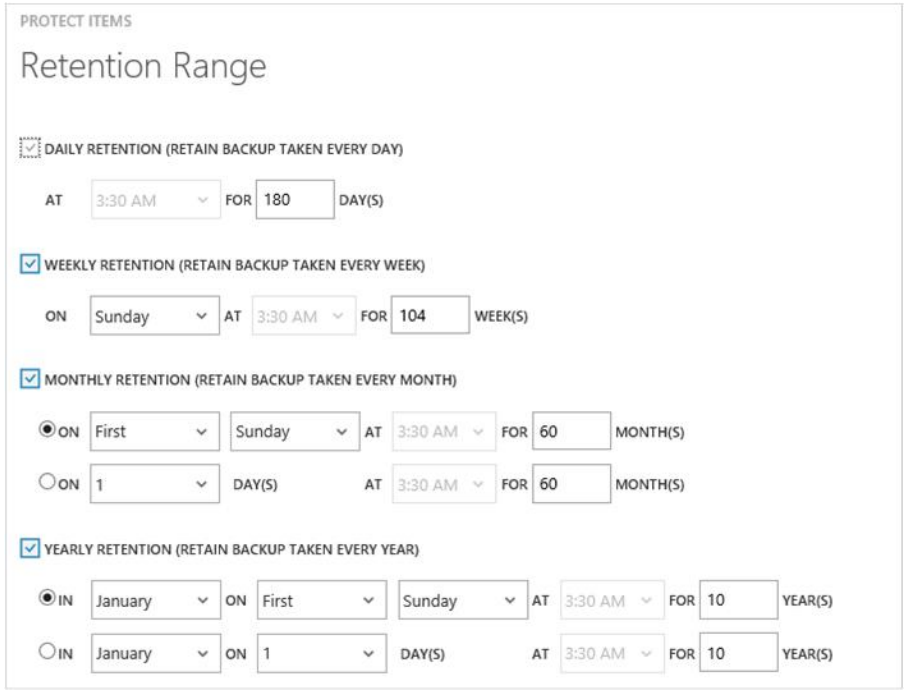


Vault Credentials



Define a backup policy





Tip:

- A backup policy includes a retention scheme for the scheduled backups. If you select an existing backup policy, you cannot modify the retention options in the next step.
- Virtual machine backups can be retained for up to 99 years.

Microsoft

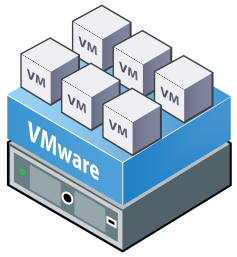
Azure Site Recovery

Microsoft Services

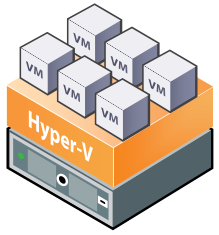
Azure Site Recovery

Private cloud to Azure

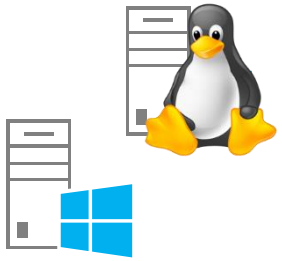
Azure



VMware

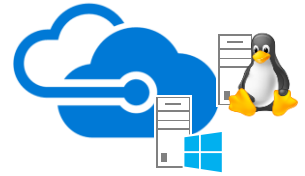


Hyper-V

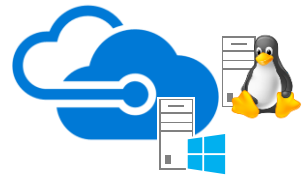


Physical

Any Cloud

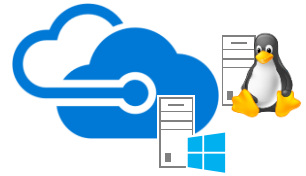


Azure to Azure



AWS

AWS to Azure



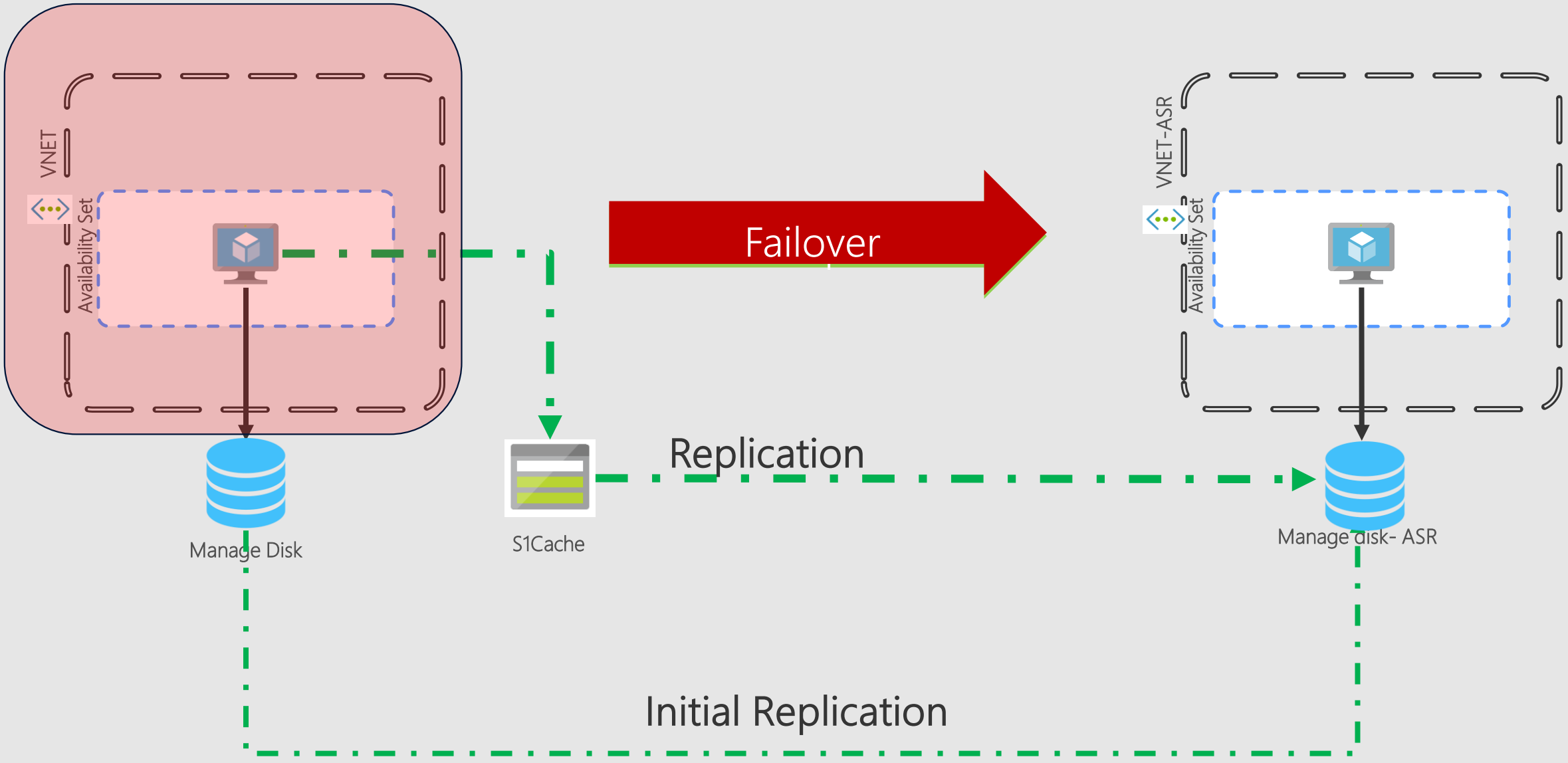
Public cloud to Azure

Windows

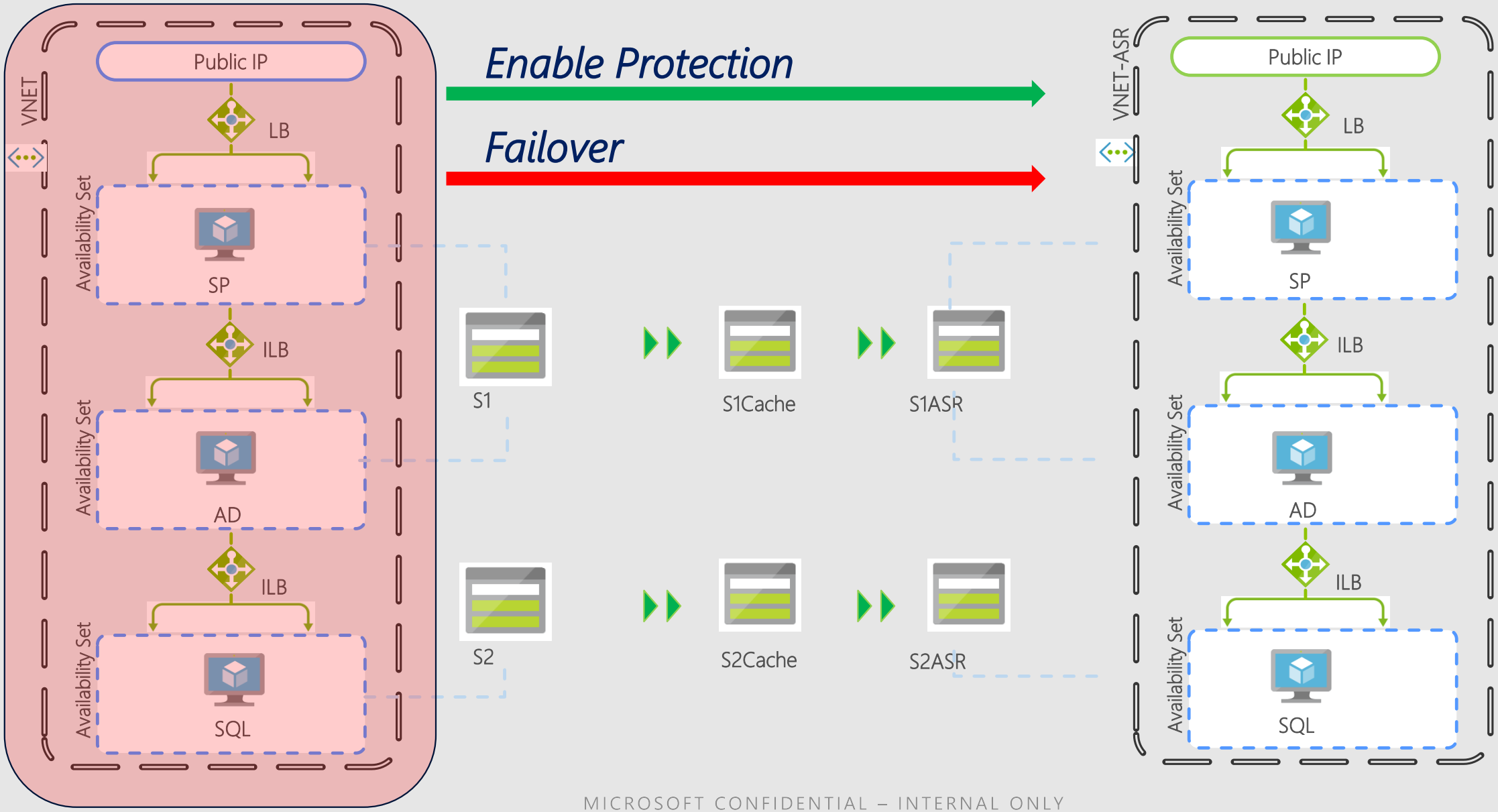
Any OS

Linux

Azure to Azure : Architecture



Application-aware Recovery



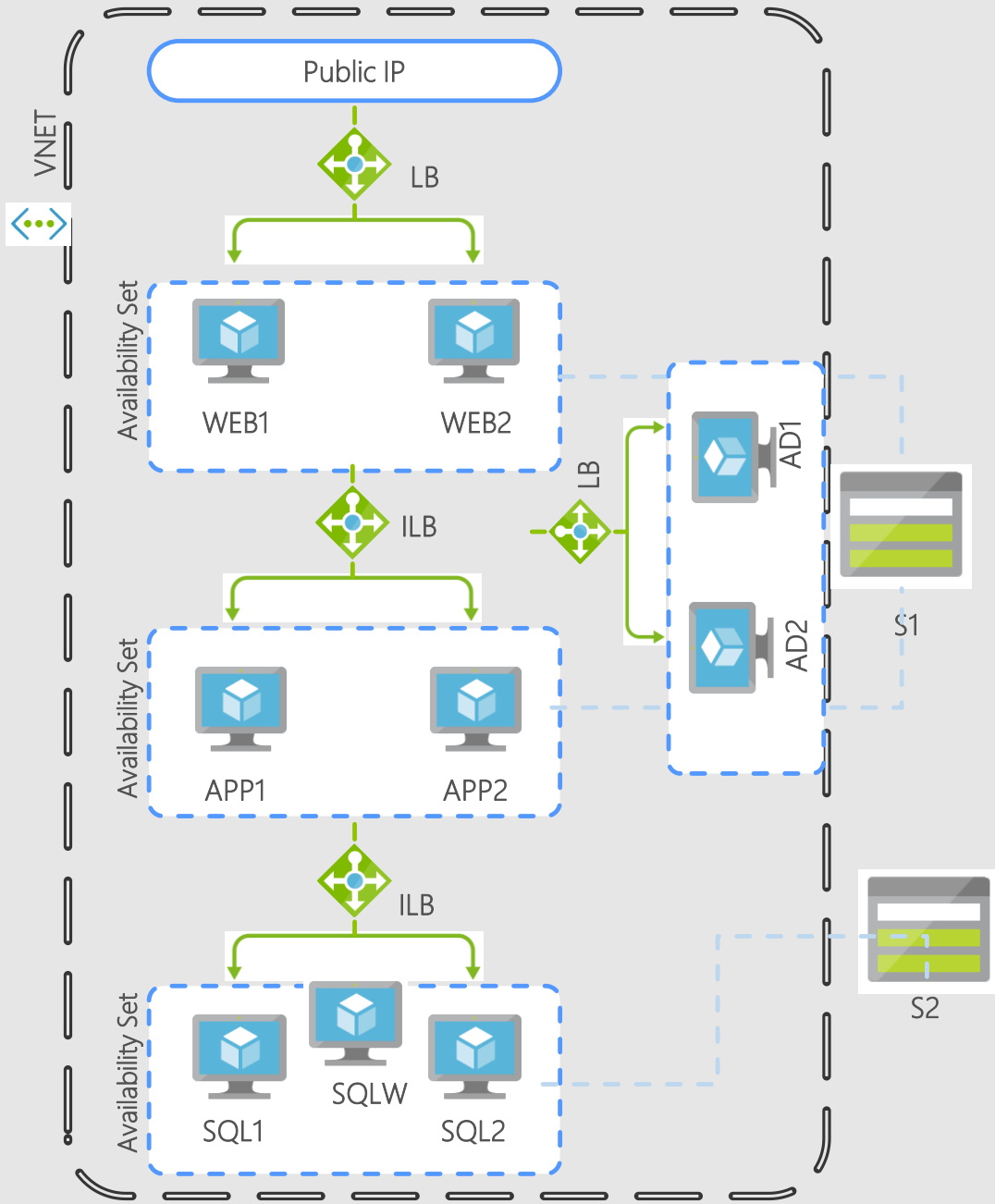
SharePoint –HA Farm

Multi-tiered with Availability Set

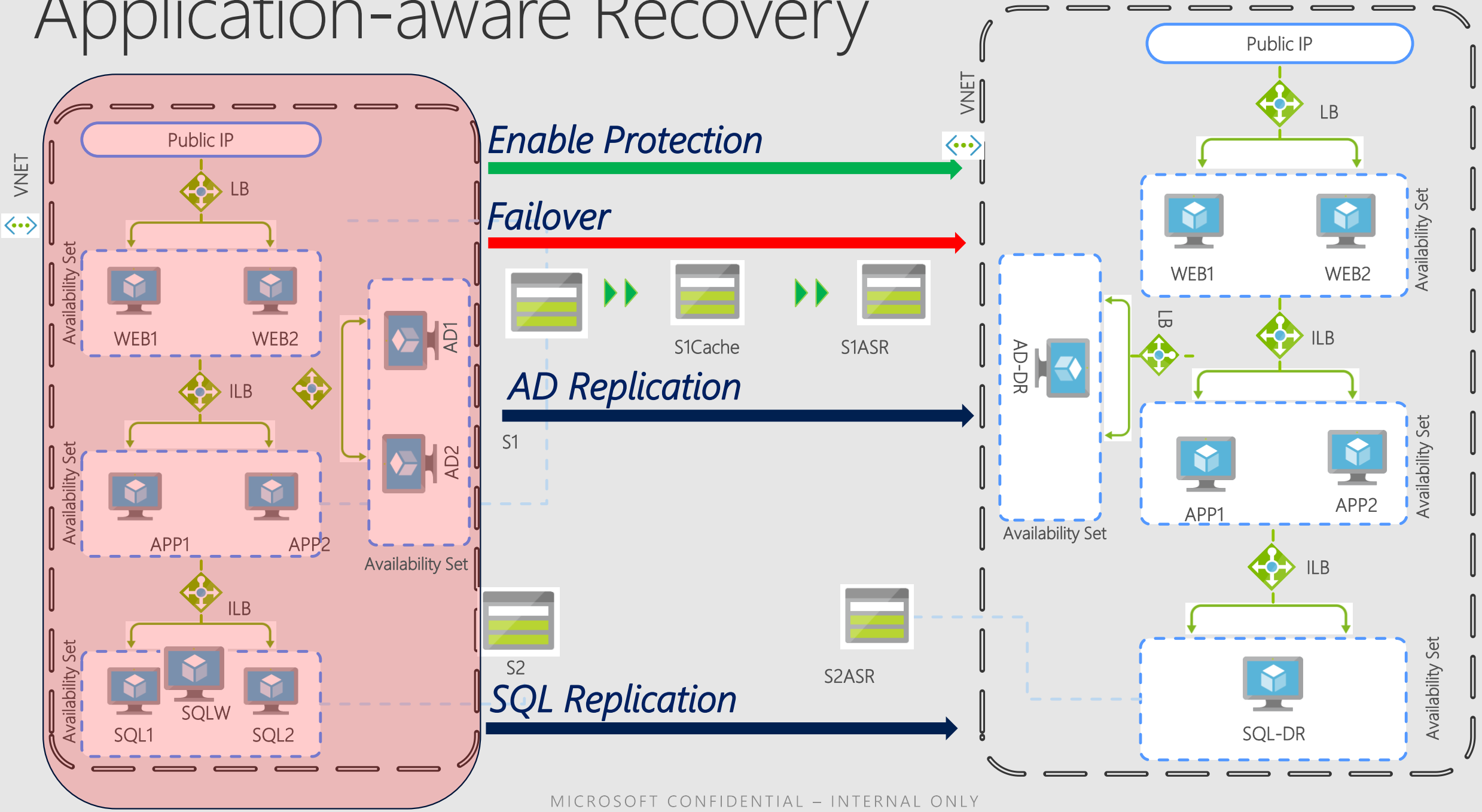
Load balancers

Public IP connectivity

SQL Always ON



Application-aware Recovery



Microsoft

Azure Automation

Microsoft Services

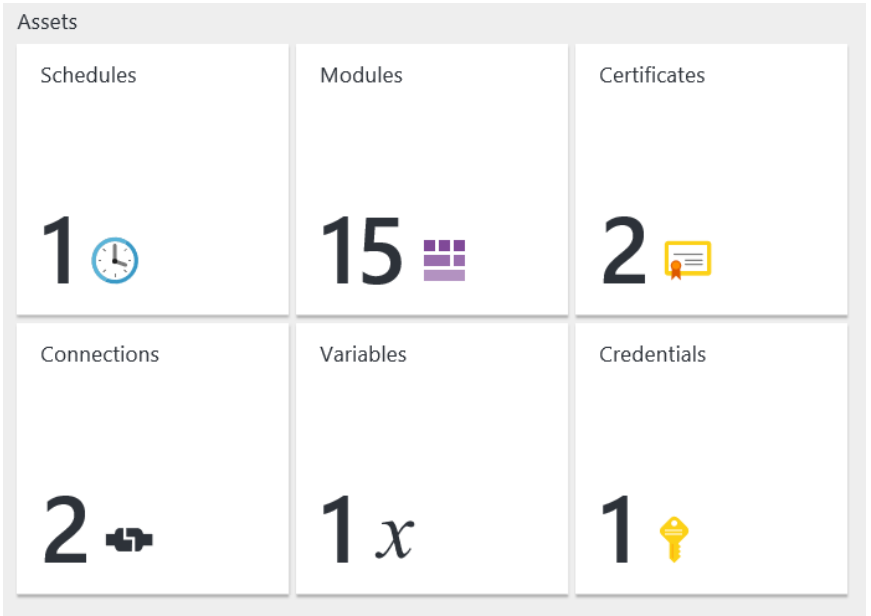
Azure Automaton

- Automation Account
- Assets
- Runbooks
- Author Runbooks
- Desired State Configuration
- Monitoring & Troubleshooting

Automation Assets

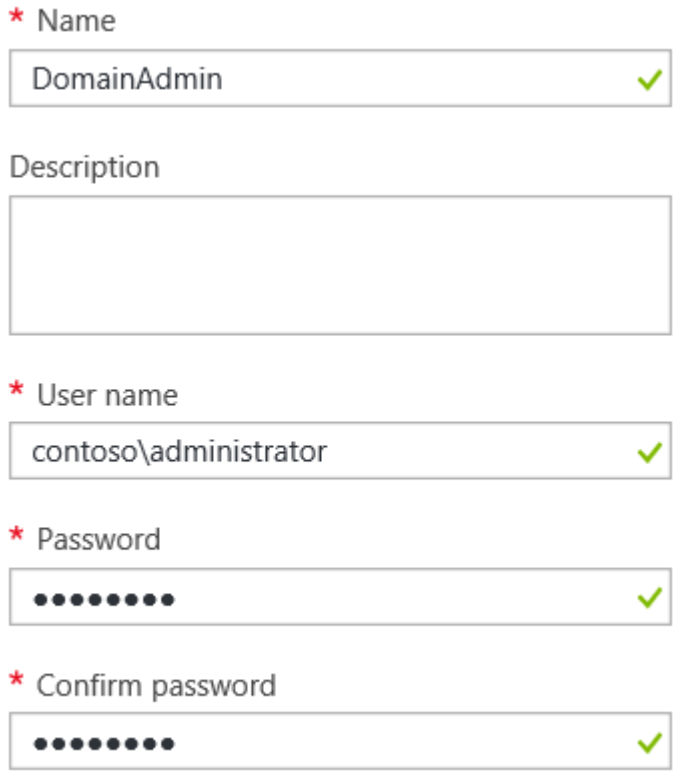
- Azure Automation Assets are settings that are saved and made globally available to be used in or associated with a Runbook.
- Assets are encrypted and stored in Azure Automation using a unique key that is generated for each Automation account.
- The unique key is encrypted by a master certificate and stored in Azure Automation.
- There are six different types of Automation Assets:

- Certificates
- Connections
- Credentials
- Integration Modules
- Schedules
- Variables



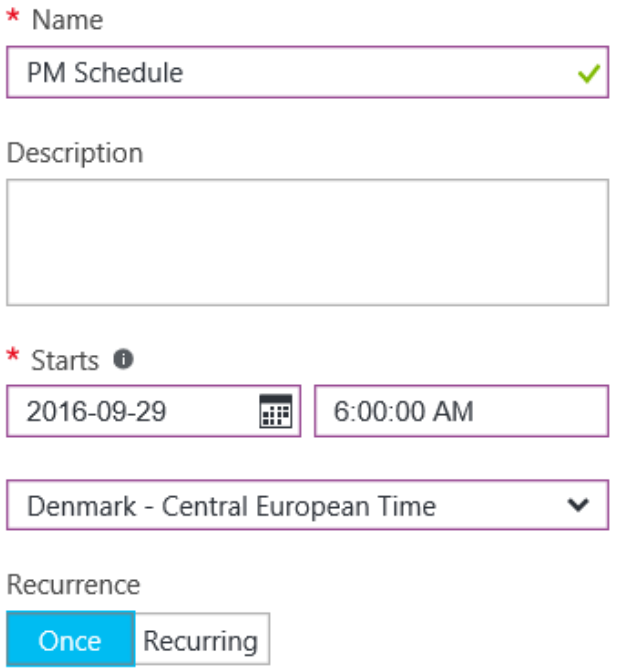
Credentials

- An Automation credential asset holds a PSCredential object which contains security credentials such as a username and password.
- Simplifies Runbook and DSC configurations that may use cmdlets that accept a PSCredential object for authentication.
- Credentials can be created using PowerShell or the Azure portal.



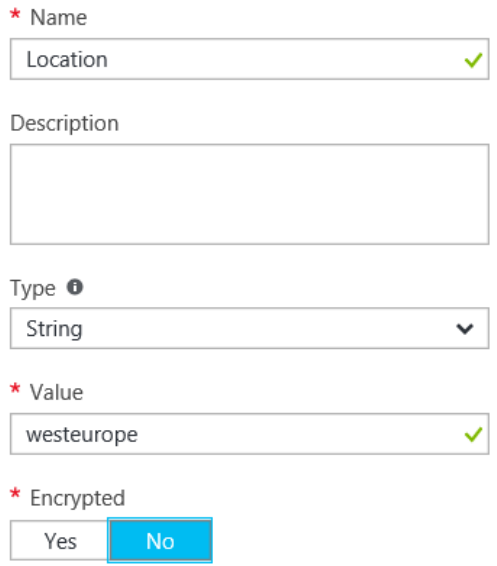
Schedules

- Azure Automation Schedules are used to schedule Runbooks to run automatically.
- Could be either a single date and time or it could be a recurring hourly, daily, weekly, or monthly schedule to start the Runbook multiple times.
- Schedules can be created using PowerShell or the Azure portal.
- Schedules do not currently support Azure Automation DSC configurations.



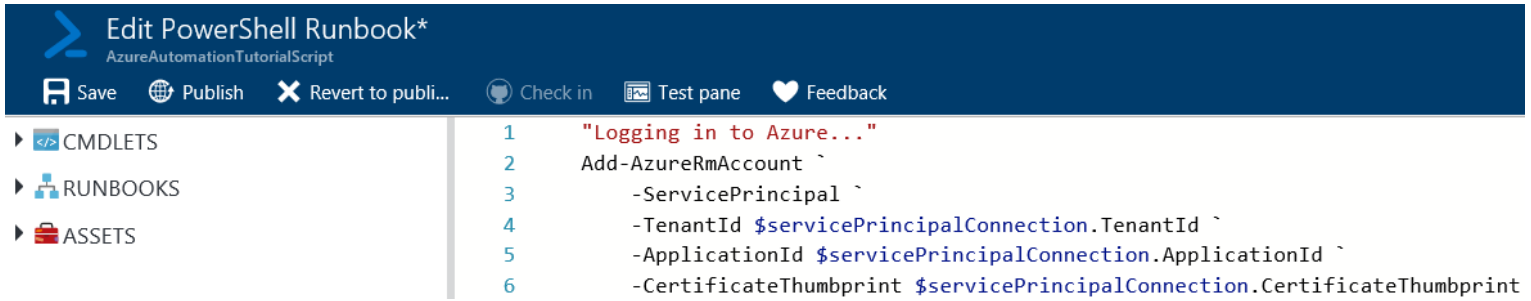
Variables

- Variable assets are values that are available to all Runbooks and DSC configurations in your automation account.
- Can be created, modified, and retrieved from the Azure portal, PowerShell, and from within a Runbook or DSC configuration.
- Automation variables are useful for:
  - Sharing a value between multiple Runbooks or DSC configurations.
  - Sharing a value between multiple jobs from the same Runbook or DSC configuration.
  - Managing a value from the portal or from a PowerShell command line that is used by Runbooks or DSC configurations.
- Variables can be stored encrypted.



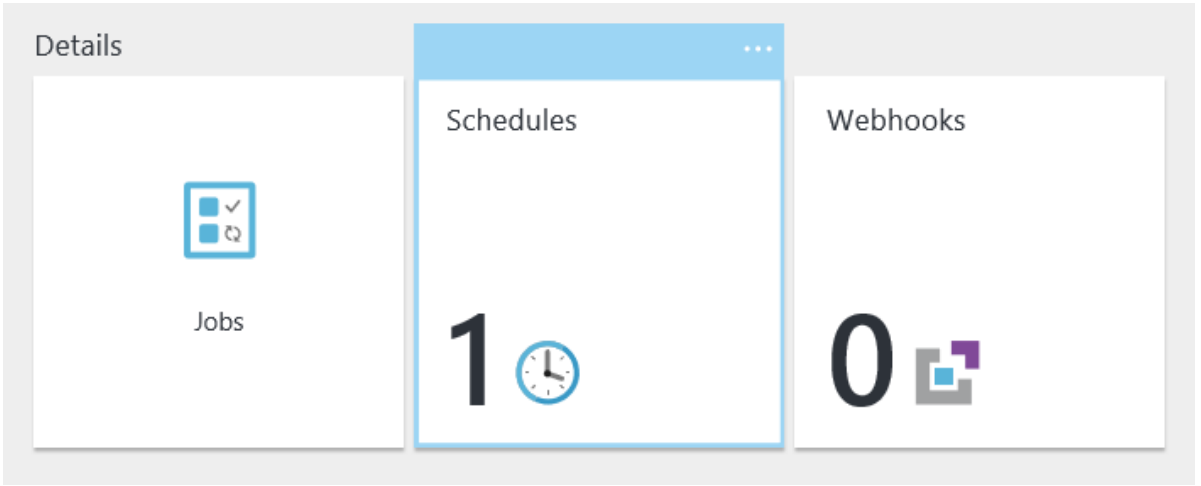
What is a Runbook

- In Azure Automation, a Runbook is a file that contains a set of procedures and operations.
- Runbooks are used as input for the Azure Automation service to process.
- The contents of a Runbook file is written using PowerShell or PowerShell Workflow commands.
- PowerShell Workflow is a PowerShell extension that allows you to run a PowerShell script on multiple devices in parallel with added functionality such as checkpoints, suspend & restart.



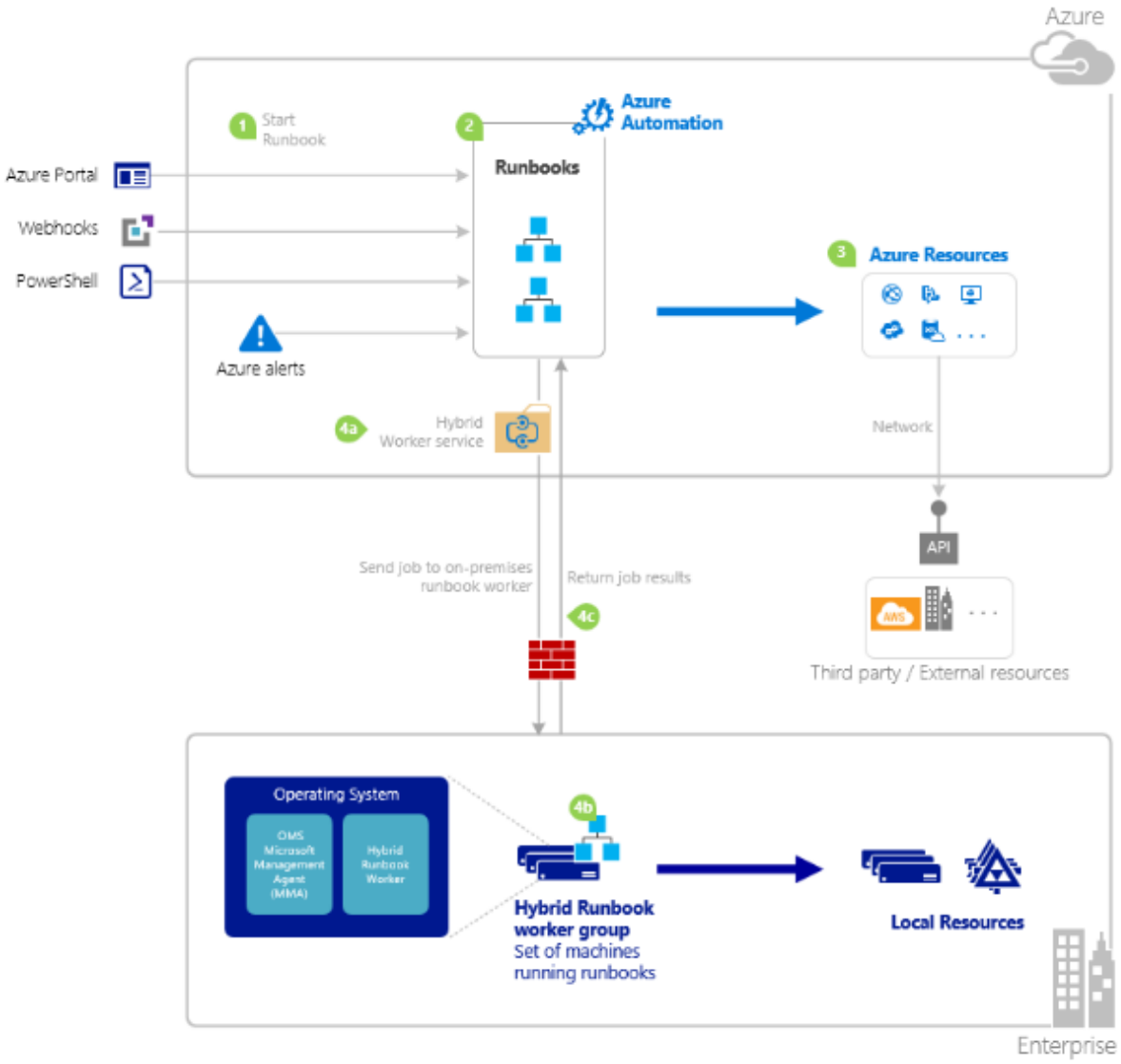
Start a Runbook

- There are 7 different ways in which you can start a Runbook.
  - Azure Portal
  - PowerShell
  - Azure Automation API
  - Webhooks
  - Respond to Azure Alert
  - Schedule
  - From Another Runbook



- The most common methods in use today are Schedule, PowerShell, the Azure Portal and Webhooks.

Runbook Processing



1. An Actor starts a runbook
2. Azure Automation notes that the runbook should be started
3. Cloud resources – Runbook acts on local Azure resources or other external resources reachable via the network

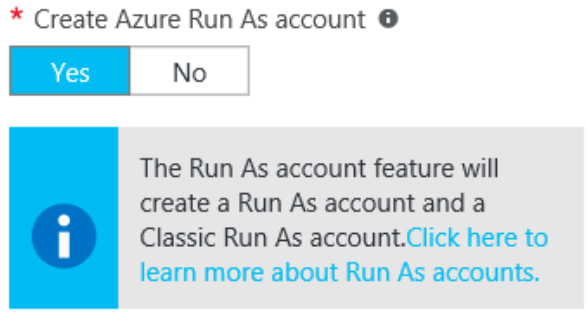
4a. On-Premises – Hybrid runbook group sends the runbook to an on-premises machine to run

4b. Runbook acts on its local networked resources

4c. Job results are returned from on-premises

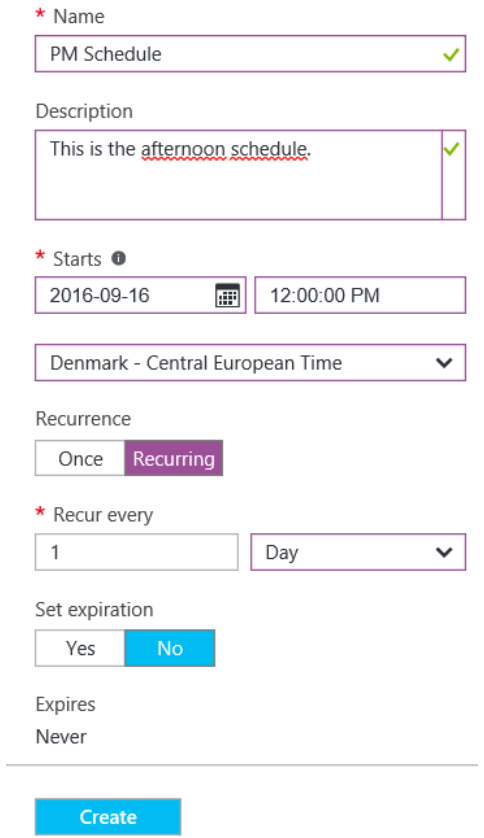
Runbook Authentication

- Runbooks are authenticated using a Run As account, this allows the Runbook to execute it's tasks under this accounts security context.
- A Run As account can be created during the creation of an Azure Automation account or an existing account can be added later using PowerShell.
- The Run As account that is created during the creation of an Azure Automation account is granted the Contributor Role for the Azure subscription.
- Existing accounts that are used must be granted the appropriate permissions in order for the Runbook to complete its tasks.



Start a Runbook using a Schedule

- Automatically start a Runbook on an hourly, daily, or weekly schedule.
- Manipulate the schedule through the Azure portal, PowerShell cmdlets, or Azure API.
- Provide parameter values to be used with the schedule.



Start a Runbook using PowerShell

- Runbooks can be called from a command line with Windows PowerShell cmdlets.
- The call can be included in an automated solution with multiple steps.
- The request is authenticated with a certificate or OAuth user principal / service principal.
- Provide simple and complex parameter values to start the Runbook.
- Track job state.
- Client required to support PowerShell cmdlets.

```
PS C:\> Start-AzureRmAutomationRunbook -Name AzureAutomationTutorialScript -ResourceGroupName cbauto -AutomationAccountName cbauto
```

Start a Runbook using the Azure Portal

- Is the simplest method with an interactive user interface.
- Forms based to provide simple parameter values.
- Easily track job state.
- Access authenticated with Azure logon.

Start a Runbook using Webhooks

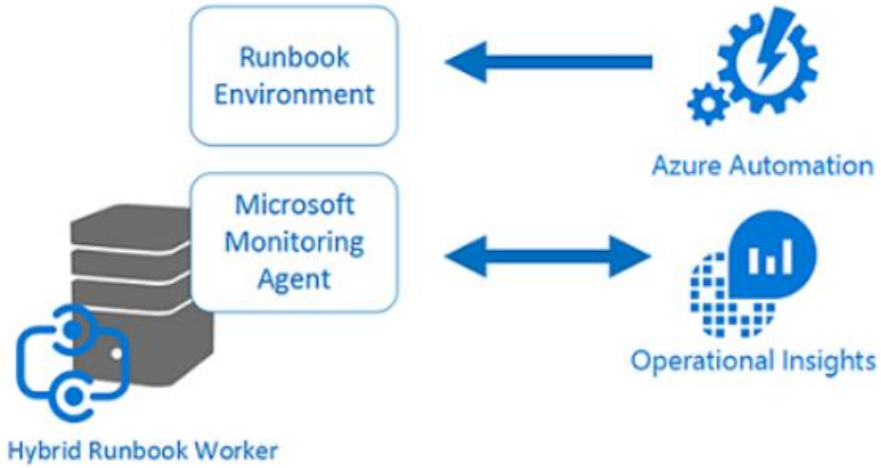
- A Webhook is a HTTP POST request that is sent to a specific URL, on receiving the POST request, some action is taken i.e. start a Runbook.
- The URL is generated during the creation of a Webhook and includes a built in security token that is used to authenticate the request when it is received by the Azure Automation service.
- The Webhook URL must be specified in the application that will be making the request.
- You cannot specify a custom URL and the URL expiration date cannot be changed after the Webhook as been created.
- No ability to track job state through a Webhook URL.

A Webhook URL

```
https://s2events.azure-automation.net/webhooks?token=HiQsFa4HqNbrmAhbD4jxwvGbcWVkOwI5E%2bsIQ3rKmdk%3d
```

Hybrid Runbook Workers

- Hybrid Runbook Workers allow you to run Runbooks on machines located in your local data center in order to manage local resources.
- Runbooks are stored and managed in Azure Automation and downloaded by one or more designated on-premises machines via an agent.
- Outbound TCP 443 is required since the agent on the local computer initiates all communication with Azure Automation.
- Whitelist URL: *.azure-automation.net
- Use the RunOn option in the Azure portal to select the name of the Hybrid Runbook Worker to start a Runbook.



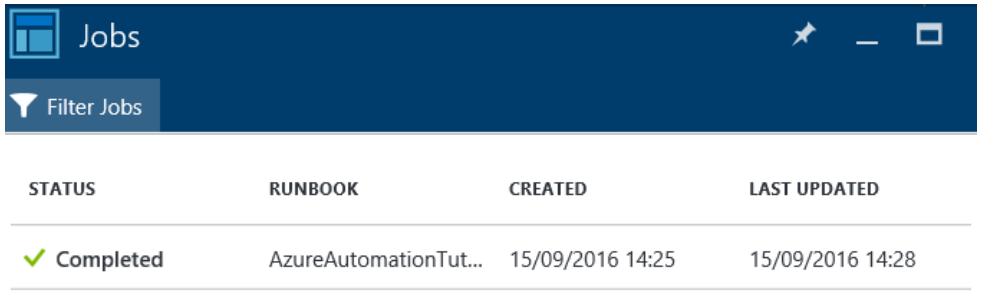
Runbook Job Status

- Runbook job status can be monitored using the Jobs tile in the Azure Portal or using Get-AzureRmAutomationJob in PowerShell.

- Runbook jobs running for more than 3 hours will be temporarily unloaded and resumed from their last checkpoint, this is known as the Fair Share Limit.

- PowerShell Runbooks will be started from the beginning since they don't support checkpoints.

- Runbooks are terminated with a status of 'Failed, waiting for resources' if they are restarted 3 consecutive times.



Microsoft

Azure Event Grid

Microsoft Services

Azure Event Grid

Fully-managed event routing

Near real-time event delivery at scale

Broad coverage within Azure and beyond

Backbone of event-driven computing

Manage all events in one place

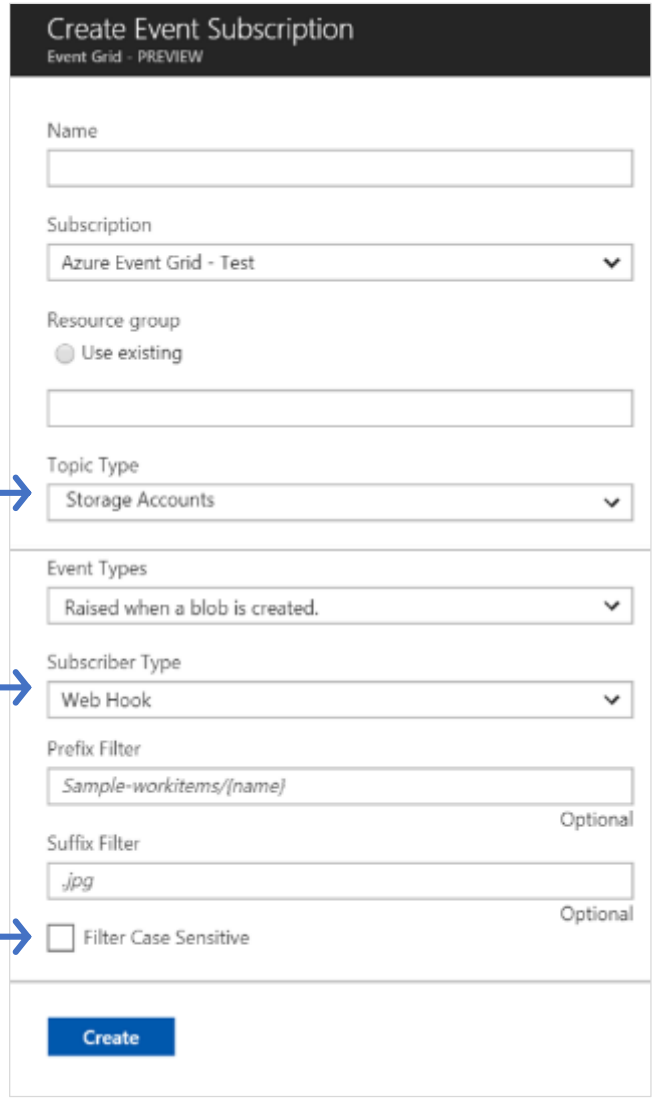
Event publishers

- Blob Storage
- Resource Groups
- Azure Subscriptions
- Event Hubs
- Custom Events

Subscribe to pre-defined system events in Azure or create your own custom topics

Route events to any end-points, Azure or even beyond

Enable filtering and efficient routing of events



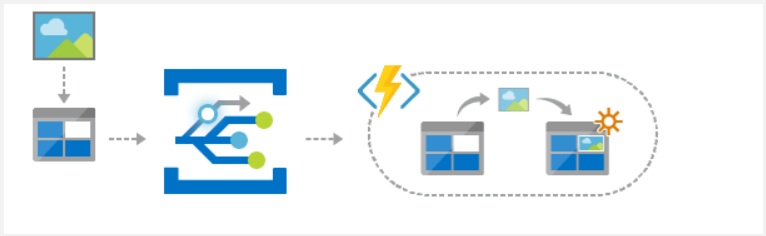
Event handlers

- Azure Functions
- Logic Apps
- Azure Automation
- WebHooks

Scenarios

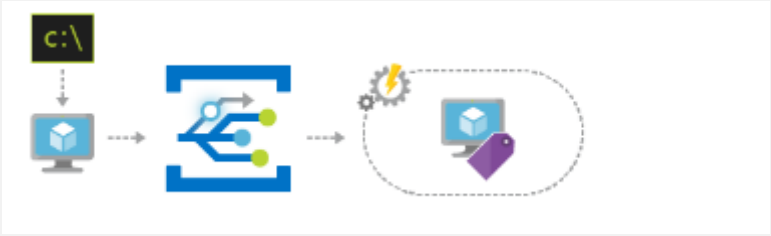
Serverless apps

Instantly trigger a serverless function to run analysis when a new file is added to a blob storage container.



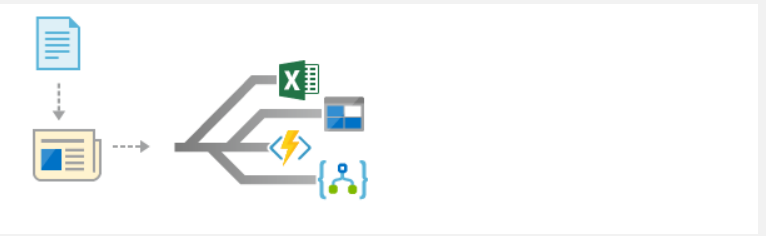
Ops automation

Speed up automation and simplify policy enforcement by notifying Azure Automation when underlying infrastructure is provisioned



Application integration

Connects your app with other services. Create an application topic to route your app's event data to any desired destination



Microsoft

Azure Infra Provisioning and Configuration Management

Microsoft Services

Azure Infra Provisioning and Configuration Management

Infrastructure Provisioning

- Azure PowerShell
- Azure CLI
- Azure ARM Templates
- Teraform

Configuration Management

- PowerShell DSC (Desired State Configuration)
- Chef
- Puppet
- Ansible

Microsoft

Azure Cost Management

Microsoft Services

CIO Dashboard | Overview | Spot Overview | **Manageme... Dashboard** | Cost Controller | Asset Controller | Optimizer | S3 Tracker

Add New +
Dashboard Settings

Management Dashboard

Default

Cost Entity Summary

3 Cost Entities
51 Accounts

Cost Over Time
Cost for last day

$2,507

Cost trend for last 30 days

Asset Controller
Number of Running Instances

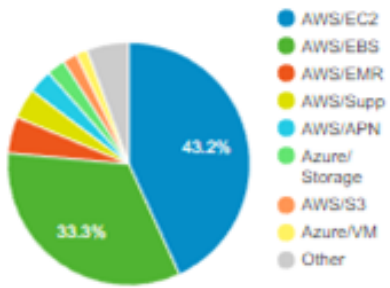
188 instances

Usage trend for last 30 days

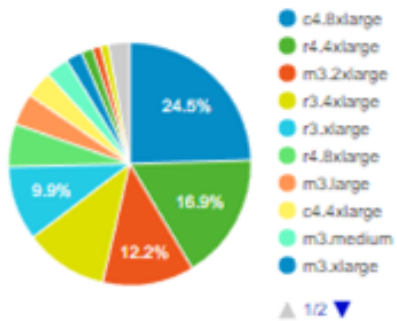
Unused RI Detector
Number of unused Reserved Instances

4 unused RIs

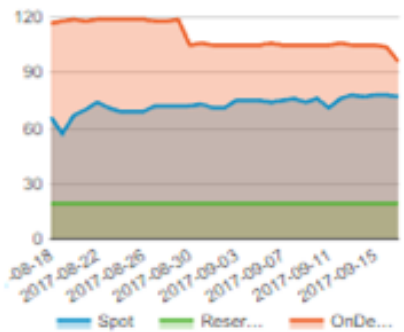
Cost By Service
Last 30 days



Potential Savings
Instance Type Pricing Recommendations



Compute Instances - Daily Trend
Last 30 days



Storage by Department