



AZ-300T01

Module 01: Managing Azure Subscriptions and Resources

Ahmad Majeed Zahoory



1

Module Overview

- Azure Monitor
- Azure Alerts
- Log Analytics
- Network Watcher
- Subscriptions and Accounts

2

Lesson 01: Exploring Monitoring Capabilities in Azure



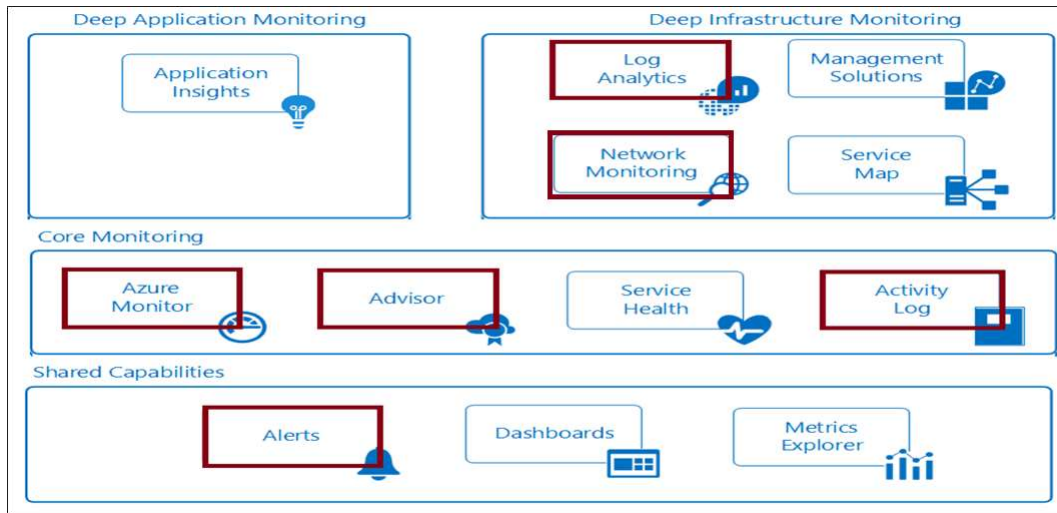
3

Azure Monitor Overview

- Azure Monitor Service
- Key Capabilities
- Monitoring Data Platform
- Log Data
- Data Types
- Azure Advisor
- Activity Log
- Query the Activity Log
- Event Categories

4

Introducing Azure Monitor Service



5

Azure Monitor: Key Capabilities



Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

[Explore Metrics](#)



Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

[Search Logs](#)



Setup Alert & Actions

Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

[Create Alert](#)

- Core monitoring for Azure services
- Collects metrics, activity logs, and diagnostic logs
- Use for time critical alerts and notifications

6

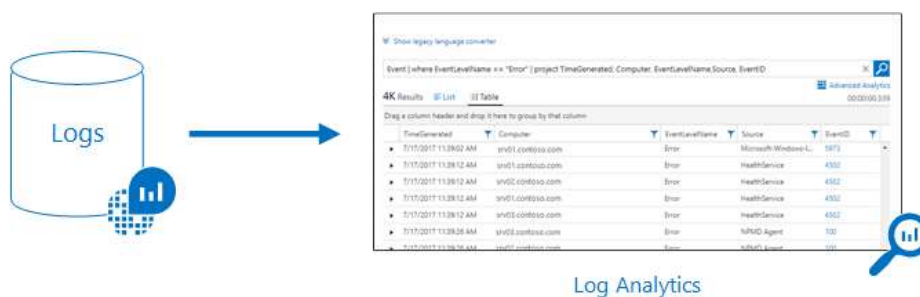
Monitoring Data Platform



- **Metrics** are numerical values that describe some aspect of a system at a point in time. They are lightweight and capable of supporting near real-time scenarios.
- **Logs** contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.

7

Log Data



- Log data is stored in Log Analytics which includes a rich query language to quickly retrieve, consolidate, and analyze collected data
- The Data Explorer query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics

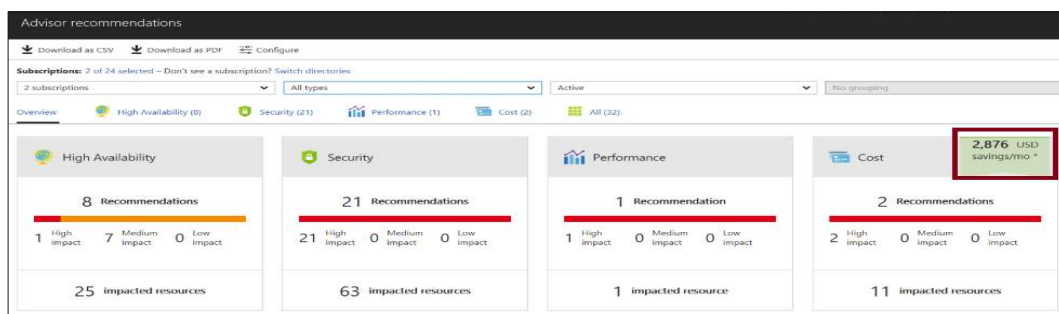
8

Data Types

- Application monitoring data - Performance and functionality of the code you have written, regardless of its platform
- Guest OS monitoring - Azure, another cloud, or on-premises
- Azure resource monitoring
- Azure subscription monitoring - Operation and management of an Azure subscription, as well as data about the health and operation of Azure itself
- Azure tenant monitoring – Operation of tenant-level Azure services, such as Azure Active Directory

9

Azure Advisor

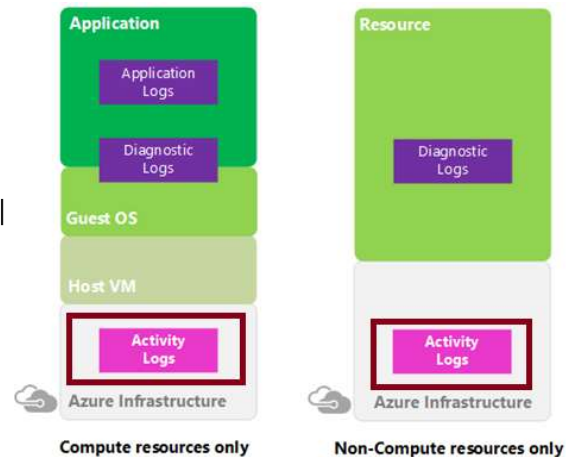


- Personalized cloud consultant
- Analyzes your configuration and recommends solutions
- Four areas: High Availability, Security, Performance, and Cost

10

Activity Log

- Send data to Log Analytics for advanced search and alerts
- Query or manage events in the Portal, PowerShell, CLI, and REST API
- Stream information to Event Hub
- Archive data to a storage account
- Analyze data with Power BI



11

Query the Activity Log

The screenshot shows the 'Activity log' interface with various filters and options. At the top, there are links for 'Columns', 'Export', and 'Log Analytics'. Below this is a 'Select query ...' dropdown and a status bar showing 'Insights (Last 24 hours): 0 failed deployments | 0 role assignments | 0 errors | 0 alerts fired | 2 outage notifications'. The main section contains several filter groups:

- * Subscription**: Visual Studio Enterprise
- Resource group**: All resource groups
- Resource**: All resources
- Resource type**: All resource types
- Operation**: 0 selected
- Timespan**: Last 24 hours
- Event category**: Service Health
- * Event severity**: 4 selected
- Event initiated by**: Email or name or service principal name
- Search**: (empty text box)

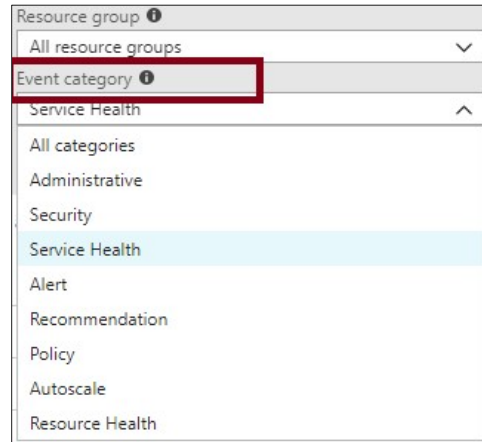
 At the bottom are 'Apply' and 'Reset' buttons.

- Filter by: Subscription, Resource group, Resource (name), Resource type, Operation name, Timespan, Category, Severity, and Event initiated by

12

Event Categories

- Administrative events
- Service health events with status
- Alert events
- Autoscale events
- Usage recommendations
- Security events
- Policy and Resource Health (reserved)



13

Lesson 02: Azure Alerts



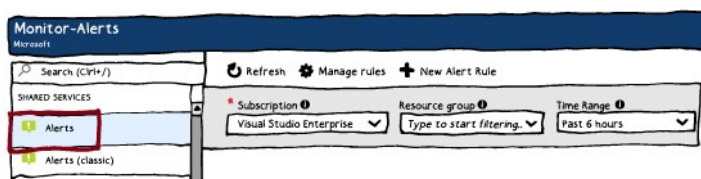
14

Azure Alerts Overview

- Azure Monitor Alerts
- Creating Alert Rules
- Action Groups
- Managing Alerts
- Alerts Experience
- Alert Detail Page
- Create an Alert

15

Azure Monitor Alerts

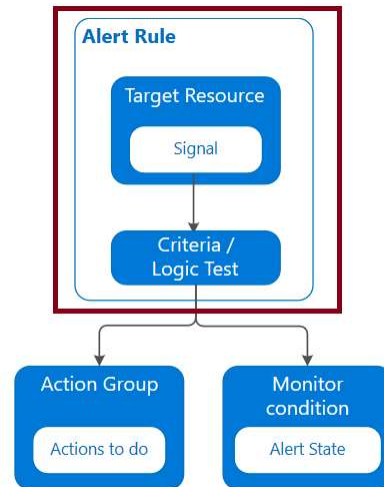


- Better notification system
- Unified authoring experience
- Log Analytics alerts display in Azure portal
- Separation of Fired Alerts and Alert Rules
- Improved workflow

16

Creating Alert Rules

1. Define alert conditions: Target selection, Alert criteria, and Alert logic
2. Define alert details: Alert rule name, description, and severity (0 to 4)
3. Define action group: notify your team via email and text messages or automate actions using webhooks and runbooks.



17

Action Groups

- Notifies a group of users that an alert has been triggered
- Is a collection of notification preferences
- Email/SMS/Voice
- Azure Function
- Logic App
- Webhook
- IT Service Management
- Automation Runbook

Add action group			
* Action group name	Sample action group ✓		
* Short name	SamleAG ✓		
* Subscription	<Subscription ID> ▼		
* Resource group	Default-ActivityLogAlerts ▼		
Actions			
ACTION NAME	ACTION TYPE	STATUS	DETAILS
	Email/SMS/Push/Voice Azure Function LogicApp Webhook ITSM Automation Runbook		

18

Managing Alerts

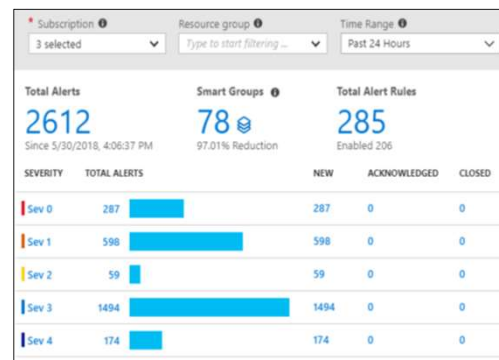
State	Description
New	The issue has just been detected and has not yet been reviewed.
Acknowledged	An administrator has reviewed the alert and started working on it.
Closed	The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.

- You can alert on metrics and logs as such as: Metric values, log search queries, activity log events, health of the underlying Azure platform, and tests for web site availability

19

Alerts Experience

- Subscription** – View up to five Azure subscriptions
- Resource Group** – One resource group at a time
- Time range** - Past hour, the past 24 hours, the past 7 days, and the past 30 days.



20

Alert Detail Page

[All Alerts](#) > Hearbeat alerts on all...

Alert Name	Created Time	Severity	State
Hearbeat alerts on all Windows computers in a workspace [Log to Metric]	10/30/2018, 11:06:16 AM	Sev3	New

[Change alert state](#)

- Essentials
- History
- Smart group
- More details

21

Create an Alert

- Resource
- Condition
- Action Group
- Alert rule name
- Description
- Enable rule upon creation

Create rule
Rules management

RESOURCE
Select the target(s) that you wish to monitor

[Select](#)

CONDITION
No condition defined, click on 'Add condition' to select a signal and define its logic

[Add condition](#)

ACTION GROUPS
Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. [Learn more here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
No action group selected	

[Select existing](#) [Create New](#)

22

Lesson 03: Azure Activity Logs and Log Analytics



23

Log Analytics Overview

- Log Analytics Scenarios
- Create a Workspace
- Connected Sources
- Data Sources
- Log Analytics Querying
- Query Language Syntax

24

Log Analytics Scenarios

Example 1 - Assessing updates

- IT Administrators assess systems update requirements
- Must be able to accurately schedule updates
- OMS/Log Analytics collects data from all customers performing updates
- Uses "Crowd-sourced" data to provide an average time to help meet strict SLAs

Example 2 - Change tracking

- Troubleshooting operational incidents is a complex process
- OMS/Log Analytics let you perform analysis from multiple angles, using a variety of sources
- Everything correlated through a single interface
- Track issues such as unexpected system reboots or shutdowns

25

Create a Workspace

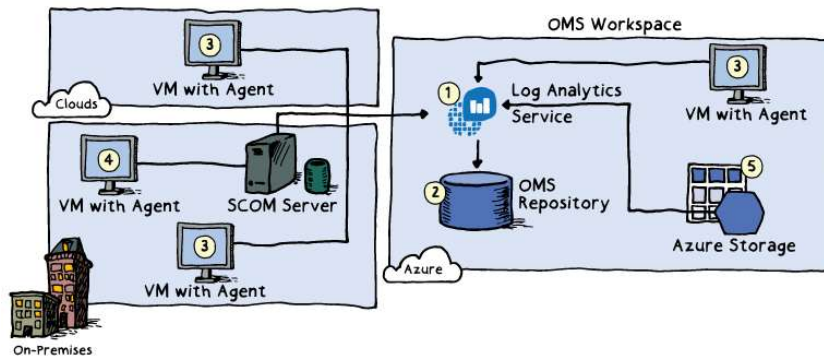
- A workspace is an Azure resource and is a container where data is collected, aggregated, analyzed, and presented
- You can have multiple workspaces per Azure subscription, and you can have access to more than one workspace
- A workspace provides a geographic location, data isolation, and scope

The screenshot shows the 'Log Analytics workspace' creation window. At the top, it says 'Create new or link existing one created in OMS...'. There are two radio buttons: 'Create New' (selected) and 'Link Existing'. Below are four fields with asterisks indicating they are required:

- OMS Workspace**: A text input field containing 'TestAnalyticsWorkspace' with a green checkmark on the right.
- Subscription**: A dropdown menu showing 'Visual Studio Enterprise'.
- Resource group**: Radio buttons for 'Create New' and 'Use Existing' (selected). Below is a dropdown menu showing 'ash-rg'.
- Location**: A dropdown menu showing 'West Europe'.

26

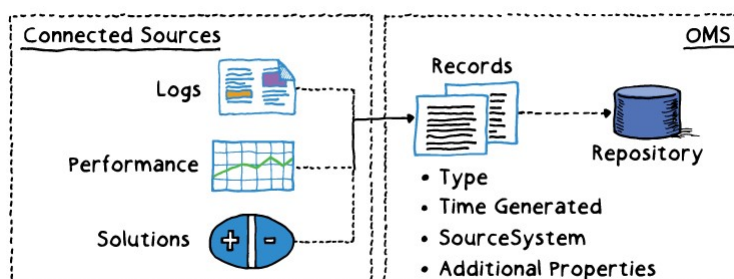
Connected Sources



- Connected Sources generate data
- Data can be collected from Windows, Linux, SCOM and Azure Storage

27

Data Sources



- Data sources include: Windows Event Logs, Windows Performance Counters, Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog.
- Each data source has additional configuration options.

28

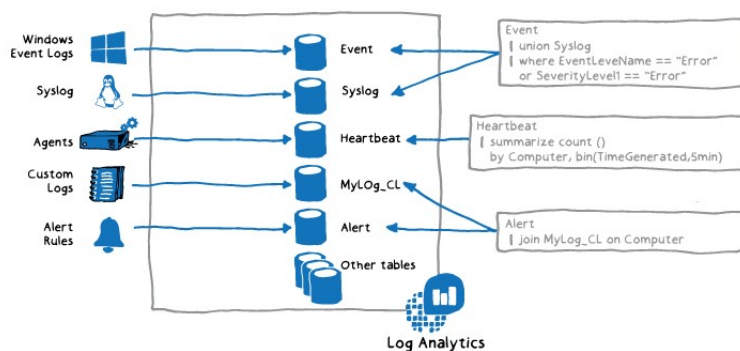
Log Analytics Querying



- Log Analytics provides a query syntax
- Quickly retrieve and consolidate data in the repository
- Save or have log searches run automatically to create an alert
- Export the data to Power BI or Excel

29

Query Language Syntax



```
Event
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCount = count() by Computer
| top 10 by ErrorCount desc
```

30

Lesson 04: Network Watcher



31

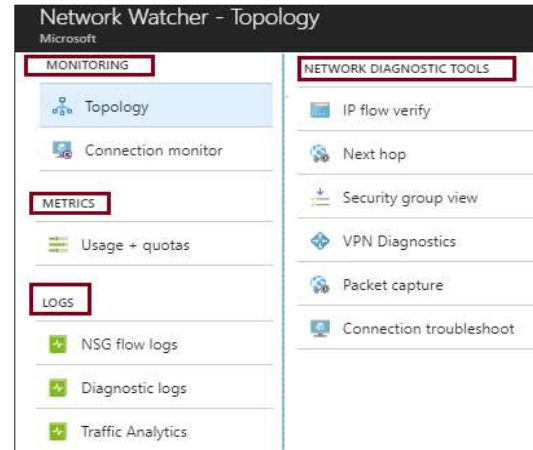
Network Watcher Overview

- Network Watcher
- Monitoring and Visualization
- Diagnostics – IP Flow Verify
- Diagnostics – Next Hop
- Diagnostics – VPN Diagnostics
- NSG Flow Logs
- Connection Troubleshoot

32

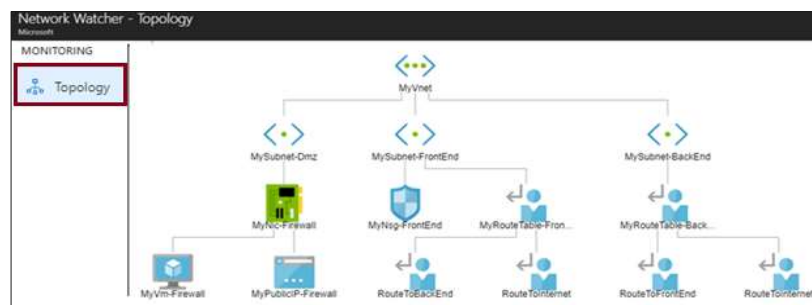
Network Watcher

- Is a regional service
- Provides tools to monitor, diagnose, view metrics, and enable or disable logs
- Provides scenario level monitoring so you can diagnose problems at an end to end network level view



33

Monitoring and Visualization



- Provides a visual representation of your networking elements
- View all the resources in a virtual network, resource to resource associations, and relationships between the resources

34

Diagnostics - IP Flow Verify

Diagnose connectivity issues from or to the internet and from or to the on-premises environment. Ideal for ensuring security rules are being correctly applied.

Network Watcher - IP flow verify
Microsoft

Network diagnostic tools

- IP flow verify
- Next hop
- Effective security rules

Packet details

Protocol: ☒ TCP ☐ UDP

Direction: ☒ Inbound ☐ Outbound

Local IP address*: 10.0.1.4 Local port*: 3389

Remote IP address*: 13.4.6.21 Remote port*: *

Check

Result

Access denied
Security rule: Deny_All_Internet

35

Diagnostics - Next Hop

Helps with determining whether traffic is being directed to the intended destination by showing the next hop

Network Watcher - Next hop
Microsoft

Network diagnostic tools

- IP flow verify
- Next hop
- Effective security rules

Specify a target virtual machine and destination IP address to view the next hop.

* Subscription: MSDN Platforms

Resource group*: NetworkWatcherRG

Virtual machine*: LinuxVM

Network interface*: linuxvm493

Source IP address*: 10.0.1.4

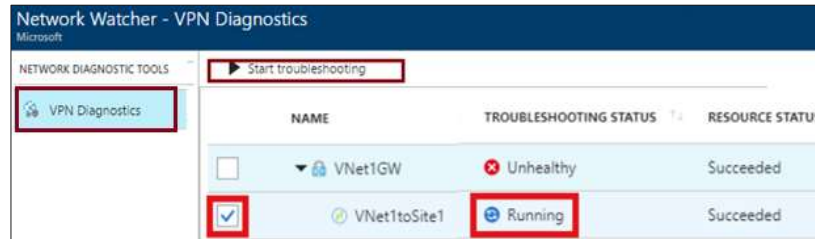
Destination IP address*: 10.1.1.4

Next hop

Next hop type: **Virtual Appliance**
IP address: **10.1.2.4**
Route table ID: /subscriptions/6515xxxxx

36

Diagnostics - VPN Diagnostics



- Helps you troubleshoot gateways and connections
- Provides summary information and detailed information
- Can troubleshoot multiple gateways or connections simultaneously

37

NSG Flow Logs

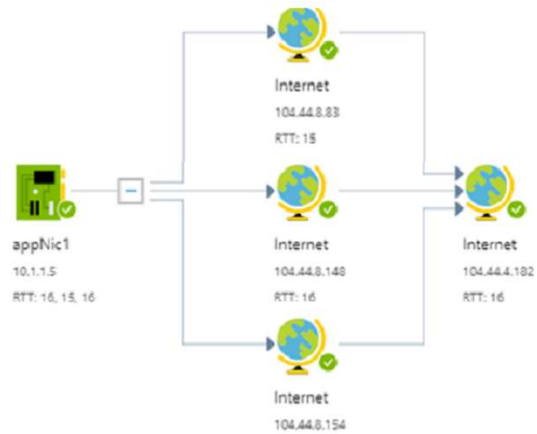
LOGS	NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS	LOCATION
NSG flow logs	Backend-NSG	Network security group	ContosoApplication	Disabled	West US
Diagnostic logs	DefaultNSG	Network security group	contosoapplication	Enabled	West US
Traffic Analytics	Frontend-NSG	Network security group	ContosoApplication	Enabled	West US

- View information about ingress and egress IP traffic through an NSG
- Flow logs are written in JSON format and show outbound and inbound flows on a per rule basis
- The JSON format can be visually displayed in Power BI or third-party tools like Kibana

38

Connection Troubleshoot

- Check connectivity between source VM and destination
- Identify configuration issues that are impacting reachability
- Provide all possible hop by hop paths from the source to destination
- Review hop by hop latency - min, max, and average between source and destination
- View a graphical topology from your source to destination



39

Lesson 05: Subscriptions and Accounts



40

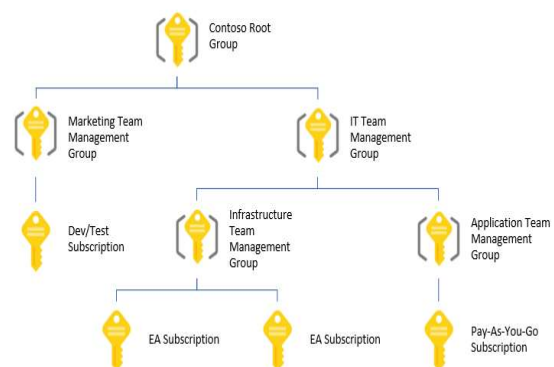
Subscriptions and Accounts Overview

- Management Group
- Creating Management Groups
- Azure Subscriptions
- Getting a Subscription
- Subscription Usage
- Subscription User Types
- Check Resource Limits
- Resource Tags
- Billing

41

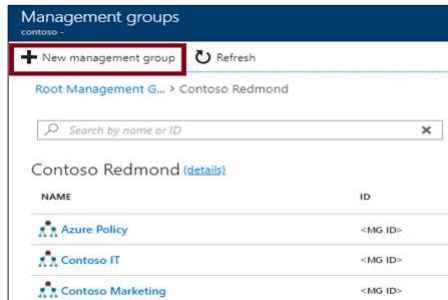
Management Groups

- Provides a level of scope above subscriptions
- Organizational alignment for your Azure subscriptions through custom hierarchies and grouping
- Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies
- Compliance and cost reporting by organization (business/teams)



42

Creating Management Groups



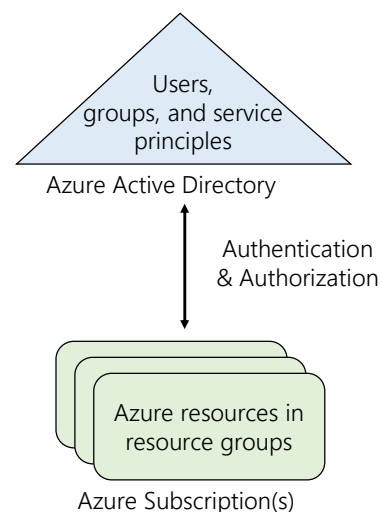
The 'Add management group' dialog box shows options to 'Create new' or 'Use existing'. It includes fields for 'Management group ID' (with a note that it cannot be updated after creation) and 'Management group display name' (with an example 'e.g. Group1').

- The **Management Group ID** is the directory unique identifier that is used to submit commands on this management group
- The **Display Name** field is the name that is displayed within the Azure portal

43

Azure Subscriptions

- A subscription is a logical unit of Azure services that is linked to an Azure account
- Subscriptions help you organize access to cloud service resources
- Subscriptions have accounts
- An Azure account is simply an identity in Azure Active Directory (Azure AD) or in a directory that is trusted by Azure AD, such as a work or school organization



44

Getting a Subscription

- **Enterprise Agreement** customers make an upfront monetary commitment and consume services throughout the year
- **Resellers** provide a simple, flexible way to purchase cloud services
- **Partners** can design and implement your Azure cloud solution
- **Personal free account** -start right away



45

Subscription Usage

Subscription	Usage
Free	Includes a \$200 credit for the first 30 days, free limited access for 12 months
Pay-As-You-Go	Charges you monthly
Enterprise	One agreement, with discounts for new licenses and Software Assurance - targeted at enterprise-scale organizations.
Student	Includes \$100 for 12 months – must verify student access

46

Subscription User Types

Administrative Role	Limit	Summary
Account Administrator	1 per Azure account	Authorized to access the Account Center
Service Administrator	1 per Azure subscription	Authorized to access the Azure Management Portal for all subscriptions in the account
Co-administrator	200 per subscription	Same as the Service Administrator but can't change the association of subscriptions to Azure directories


47

Check Resource Limits


Visual Studio Enterprise - Usage + quotas

Subscription


SETTINGS




Resource groups



Resources



Usage + quotas



Policies

QUOTA	PROVIDER	LOCATION	USAGE	Request Increase
Network Watchers	Microsoft.Network	West US 2	<div><div></div></div> 100 %	1 of 1
Public IP Addresses	Microsoft.Network	South Central US	<div><div></div></div> 3 %	2 of 60
Route Tables	Microsoft.Network	West US	<div><div></div></div> 2 %	2 of 100
Virtual Networks	Microsoft.Network	South Central US	<div><div></div></div> 2 %	1 of 50

- All resources have a maximum limit listed in Azure limits
- Helpful to track current usage, and plan for future use
- You can request an increase

48

Resource Tags

Daily Usage						
Usage Date	Meter Category	Unit	Consume	Resource Gr	Instance Id	Tags
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"computeRG"	"virtualMachines/catalogVM"	"{"costCenter":"finance", "env":"prod"}"
5/14/2015	"Virtual Machines"	"Hours"	3.999984	"businessRG"	"virtualMachines/dataVM"	"{"costCenter":"hr", "env":"test"}"

- Tags logically organize your resources
- Tags consist of a name and value
- Useful especially in billing

49

Billing

- Pricing Calculator – estimate expenditures in all areas of Azure
- Billing Alert Service - monitor and manage billing activity
- Create and Manage a Budget - plan for and drive organizational accountability
- Azure Reservations - helps you save money by pre-paying for services

50

Module Review Questions

