**Handout: Design and Implement Network Monitoring in Azure (AZ-700 - Module 8)**

**Module Overview**

In this module, we explore the comprehensive network monitoring capabilities of Microsoft Azure. We cover how to utilize **Azure Monitor** for observing the performance and health of network resources, and **Azure Network Watcher** for real-time troubleshooting and diagnostics. This handout includes deep-dive explanations, practical use cases, and detailed examples to help you implement monitoring strategies effectively.

**Section 1: Monitor Your Networks Using Azure Monitor**

**1.1 Introduction to Azure Monitor**

Azure Monitor is a unified monitoring service that collects and analyzes telemetry data from Azure resources, applications, and on-premises environments. It supports proactive identification of issues and automation based on insights gathered.

**1.2 Types of Monitoring Data**

Azure Monitor collects two primary types of data:

* **Metrics**:
  + Lightweight and real-time numerical data.
  + Examples: CPU usage, network throughput, disk IOPS.
  + Useful for dashboards, alerts, and autoscaling.
* **Logs**:
  + Structured records collected over time.
  + Includes telemetry data, performance logs, diagnostics, and application traces.
  + Enables querying using Kusto Query Language (KQL).

**1.3 Azure Monitor Tools and Interfaces**

* **Metrics Explorer**:
  + Provides interactive charting of metric data.
  + Enables time-based filtering, aggregation, and visualization.
* **Alerts**:
  + Triggered based on thresholds for metrics/logs.
  + Integrates with email, Azure Logic Apps, and ITSM tools.
* **Workbooks**:
  + Interactive dashboards for combining metrics and logs.
  + Useful for customized network health visualization.

**1.4 Azure Monitor Network Insights**

A specialized solution within Azure Monitor focused on networking:

* **Network Health**: Status of load balancers, VPNs, gateways, etc.
* **Traffic View**: Monitors traffic between VMs, subnets, and services.
* **Connectivity**: Analyzes reachability of endpoints.
* **Diagnostics Toolkit**: Integrates with NSG flow logs and traffic analytics.

**1.5 Exercise: Monitor a Load Balancer Using Azure Monitor**

* Enable diagnostics on Azure Load Balancer.
* Use Metrics Explorer to analyze data (e.g., SNAT port exhaustion).
* Set up alerts for packet drop or probe failure metrics.

**Section 2: Monitor Your Networks Using Azure Network Watcher**

**2.1 Introduction to Network Watcher**

Azure Network Watcher is a region-based service offering diagnostic and visualization tools for Azure networks. It enables detailed investigation of packet flow, connectivity status, and network topologies.

**2.2 Functional Components**

**2.2.1 Topology Viewer**

* Visualizes all resources within a virtual network.
* Displays relationships between interfaces, NSGs, route tables, and gateways.

**2.2.2 Connection Monitor**

* Continuously tests connectivity between VMs or from on-prem to Azure.
* Reports metrics such as packet loss, latency, jitter, and hop count.

**2.2.3 IP Flow Verify**

* Determines whether traffic is allowed based on NSG rules.
* Inputs: Source/Destination IP, Port, Protocol, NIC.
* Returns: Allow/Deny result and matched NSG rule.

**2.2.4 NSG Diagnostics**

* Evaluates network traffic against NSG rules.
* Identifies whether traffic is blocked or permitted.
* Aids in debugging connectivity issues.

**2.2.5 Next Hop**

* Shows the route a packet takes from a VM.
* Identifies route table paths and potential misconfigurations.

**2.2.6 Effective Security Rules**

* Displays the actual NSG rules applied to a NIC.
* Considers all inherited and explicit NSG associations.

**2.2.7 VPN Troubleshoot**

* Diagnoses issues with VPN gateways and connections.
* Returns error messages, latency, and connection status.

**2.2.8 Packet Capture**

* Captures traffic at VM NIC level.
* Saves to a storage account or local file for offline analysis.
* Filters available by protocol, IP, and port.

**2.2.9 Connection Troubleshoot**

* On-demand connectivity test between source and destination.
* Identifies DNS resolution, NSG, UDR, and routing issues.
* Graphical view of network path with latency metrics.

**2.2.10 NSG Flow Logs**

* Provides logs of all allowed and denied flows via NSGs.
* Stored in JSON format, consumable by Power BI, Kibana, etc.
* Useful for analyzing anomalous traffic and threats.

**2.2.11 Traffic Analytics**

* Visual analytics over NSG Flow Logs.
* Identifies top talkers, protocol usage, flows per port/IP.
* Built on Log Analytics workspace.

**2.3 Exercise: Monitor Load Balancer with Network Watcher**

* Enable packet capture and NSG flow logs.
* Review flow logs for dropped packets.
* Use Connection Troubleshoot to verify traffic routing.

**Summary and Best Practices**

**Azure Monitor**

* Use Metrics for real-time thresholds and dashboards.
* Use Logs for deep insights and historical analysis.
* Workbooks provide consolidated dashboards.
* Set alerts for anomalies and thresholds.

**Azure Network Watcher**

* Enables fine-grained diagnostics and traffic flow analysis.
* Use Connection Monitor for SLA monitoring.
* Use Packet Capture and NSG Flow Logs for forensic analysis.
* Next Hop and IP Flow Verify assist with routing and NSG issues.

**Recommended Learning Resources**

* **Microsoft Learn**:
  + [Monitor your networks using Azure Monitor](https://learn.microsoft.com/en-us/training/modules/monitor-networks-azure-monitor/)
  + [Monitor your networks using Azure Network Watcher](https://learn.microsoft.com/en-us/training/modules/monitor-networks-azure-network-watcher/)
* **Documentation**:
  + [Azure Monitor Documentation](https://learn.microsoft.com/en-us/azure/azure-monitor/)
  + [Azure Network Watcher Documentation](https://learn.microsoft.com/en-us/azure/network-watcher/)