Azure IaaS State of the Union

John Savill

Agenda
- Types of “as a Service”
- Azure IaaS 101
- Focus on what’s new and cool!

Types of “as a Service”

- Storage
- Servers
- Networking
- O/S
- Middleware
- Virtualization
- Data
- Applications
- Runtime

Vendor manages
Vendor manages
You manage
You manage

Infrastructure as a Service

Azure Services

- Services are deployed to a region which consist of one or more datacenters
- Subscriptions can access almost all regions except those geo-fenced

Azure Regions

- Azure VMs are created of a specific series, tier and size. Each series has different scale and capabilities
- Sizes impact CPU, memory, temporary storage size, number of data disks and network adapters, network egress and some advanced features (e.g. RDMA)
- Tier impacts IOPS, egress and some features (load balancing and auto-scale)
vCPU Changes
- Historically VM CPU was talked about in terms of cores.
- The ACU showed the relative CPU performance.
- Ensured performance consistency even if a VM of a certain SKU was deployed to a newer stamp.
- The newer SKUs Dv3, Ev3 and M expose the hyperthreaded features of the processor to the VM.
- This is why the v3 has lower ACU than v2 but is also cheaper!

Nested Virtualization
- The Dv3, Ev3 and M not only expose hyperthreading but also the hardware assisted virtualization features.
- https://github.com/charlieding/Virtualization-Documentation/tree/live/hyperv-tools/Nested has example nested configuration.
- Multi-level nesting is also supported.
  - `Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true`

Something completely Different. The B series!
- Burstable CPUs.
- Much cheaper VMs based on typically using only a fraction of the vCPU.
- Accrue credit when using less than the quota which can then be used to burst to higher utilization when needed.

Virtual Machine Storage
- Azure Storage
- Node
- OS
- Temp
- Data

VM Disks
- The VHD files exist inside a Page Blob.
- This are housed in storage accounts which have IOPS and size limits.
- Required the administrators to track the number of disks in a storage account to avoid hitting limits.
- Two types of storage account:
  - Standard – Up to 500 IOPS per disk.
  - Premium – Up to 7500 IOPS where number is based on disk size and the IOPS are guaranteed.

ALL PROBLEMS IN COMPUTER SCIENCE CAN BE SOLVED BY ANOTHER LEVEL OF INDICTION

David Wheeler
Managed Disks
- Disks become a first-class resource type with full RBAC
- Snapshot and custom image support
- Simple migration from unmanaged to managed
- Standard and Premium managed disk types
- Simple switch between Standard/Premium managed disk
- Up to 4 TB per disk

Why not always use the xS SKU
- The xS, e.g., DS, ES, GS etc., support premium storage
- Why would you not always use the xS version?
- In most cases always use the xS
- The only downside is a smaller temporary drive as a portion of the xS is used as part of the caching solution.

Availability Sets
- For the full SLA multiple instances of a service must be deployed in an availability set (99.95%)
- Single VM SLA is available when using premium storage (99.9%)
- Multiple storage accounts would be used but no guarantee they would actually be stored on separate storage clusters.

Availability Sets with Managed Disks
- Availability Set is set to a SKU of Aligned
- Each fault domain uses a separate storage cluster for the storage of the associated managed disks
- Provides protection from storage cluster failure

Availability Zones
- Provide the ability to see three AZs in a region
- When deploying resources the AZ can be selected
- Provides resiliency across datacenters within a region

Azure Files Sync
- Centralize your file services in a managed cloud service to reduce complexity associated with server sprawl while preserving on-prem compatibility and performance
Introducing the Virtual Network
- Virtual Networks allow you to define the IP space used.
- IP space used is typically from RFC 1918 but does not have to be:
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- You can divide into Virtual Subnets to separate traffic.
- Virtual Networks are bound to a region (Regional Virtual Network) instead of Affinity Group (previous).
- Up to 4096 private IPs in a Virtual Network.
- Pick IP space NOT used on-premises or in other clouds.

Providing Services to the Internet
- Public IPs are provided by Azure.
- The Public IP can be assigned directly to a VM or more typically to a load balancer as the front end.
- Avoid RDP/SSH/management via public IP. If you have to use just-in-time VM access:
  - An Azure Application Gateway can also be used to front services.
  - Web Application Firewall can be enabled on the Application Gateway.
  - Azure Traffic Manager can provide a single name to geographically distributed instances.

Virtual Network Security
- Virtual Networks are completely isolated from each other.
- A virtual network can be thought of as a trust boundary.
- Network Security Groups enable ACLs to be defined to control traffic between virtual subnets/Internet.
- Rules added to a NSG based on 5 tuple.

Network Security Groups
- vmNIC speeds are published for most VM SKUs and sizes.
- VMs can have multiple NICs based on SKU/size.
- All NICs must be on the same virtual network but can be connected to different subnets.
- This speed is across all the NICs, not PER NIC.
- Each NIC can have one or more IP configurations assigned to it.
- Each IP configuration can have:
  - A static or dynamic private IP (up to 50).
  - A public IP address (optional).
Site-to-site VPN

- Once a Virtual Network exists a site-to-site VPN can be configured to enable on-premises to Azure connectivity
- Supports multiple tunnels across on-premises locations and other virtual networks
- New SKUs support up to 1.25 Gbps

Virtual Network Peering

- Enables virtual networks in the same region to be connected via the Azure backbone without S2S VPN gateway
- Can connect networks in different subscriptions
- Must not have overlapping IP space
- NOT transitive
- Data transfer fee for inbound and outbound

ExpressRoute

- Provides direct layer 3 connectivity between your network and your services in Azure giving a predictable path and therefore performance
- Does not leverage public Internet but instead dedicated connectivity giving high security and isolation
- High throughput, low and consistent latency
- Enables services such as storage, big data, backup/recovery, media and hybrid apps with improved connectivity
- Two types of ExpressRoute connectivity
  - Network Service Provider
  - Exchange Provider

ExpressRoute Detail

- Peering partner has dedicated connectivity to Azure region using redundant configuration/path
- Up to 10 Gbps via different tiers
- Control over the routing and high flexibility
- Monthly fee with included unlimited or metered outbound data transfer (option) and unlimited inbound data transfer
- Supports Private and Public peering
Backup and Disaster Recovery
- IaaS VMs are not automatically backed up or replicated as part of the base service
- You are responsible!
- Azure Backup integration provides schedule backup with retention policies at daily, weekly, monthly, and yearly granularity
- Azure Site Recovery integration enables simple replication of the VM to another region of choice

Azure Cloud Shell and Cloud Drive
- The Azure portal provides easy access to PowerShell and CLI management
- A cloud drive is also provided for storage of profiles and other data which is hosted in Azure Files
- In addition an Azure PSProvider is provided to enable file system like navigation

Constant New Features!
- Follow me on twitter
- @NTFAQGuy
- I’ll try to keep you updated 😊

Take the Survey!
Your feedback is important! Please rate the session for a chance to win!
Survey is below session description at http://elus18.expertslive.us

Related Sessions - Azure

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Room</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/8: 10:30</td>
<td>Wren</td>
<td>Waterway 6</td>
<td>Advanced Analytics in Azure</td>
</tr>
<tr>
<td>2/8: 10:30</td>
<td>Joyner</td>
<td>College Park</td>
<td>Azure Site Recovery – Tips from the Trenches</td>
</tr>
<tr>
<td>2/8: 11:45</td>
<td>Savill</td>
<td>Waterway 6</td>
<td>Azure IaaS: State of the Union</td>
</tr>
<tr>
<td>2/8: 2:15</td>
<td>Nikolic</td>
<td>Alden Bridge</td>
<td>Cloud Shell: Your Admin Machine for Azure</td>
</tr>
<tr>
<td>2/8: 3:30</td>
<td>Savill</td>
<td>Alden Bridge</td>
<td>Understanding Identity with Azure AD</td>
</tr>
<tr>
<td>2/8: 3:30</td>
<td>Rangama</td>
<td>Sterling Ridge</td>
<td>Infrastructure-as-Code with ARM</td>
</tr>
<tr>
<td>2/9: 9:00</td>
<td>Rangama</td>
<td>College Park</td>
<td>Building Process Automation w/ Azure Logic Apps</td>
</tr>
<tr>
<td>2/9: 3:30</td>
<td>Wren</td>
<td>Waterway 6</td>
<td>Management in Azure, the Big Picture</td>
</tr>
<tr>
<td>2/9: 3:30</td>
<td>Joyner</td>
<td>Sterling Ridge</td>
<td>Business Continuity in the Microsoft Cloud</td>
</tr>
</tbody>
</table>