

VNet

VNet Communication Ways	VNets
	VNet Service Points
	VNet Peering
VNet Connect On-Premises	P2S VPN
	S2S VPN
	Azure Express Route
Routing Network Traffic	UDR or BGP

Subnetting

smallest allowed	/29
largest allowed	/2
IPv6	must be /64

VNet Addressing

RFC1918	Private
224.0.0.0/4	Multicast
255.255.255.255/32	Broadcast
127.0.0.1/8	Loopback
169.254.0.0/16	Link-Local
168.63.129.16/32	Internal DNS
4 IP addresses reserved	.1 Gateway, .2 .3 Azure DNS, .255 Broadcast

On-Premises DNS with Azure VNets

VNet can connect to external DNS

Forwarding:

Forwarding	specifies another DNS server (SOA for zone)
Conditional forwarding	specify DNS server for specific zone

Child Domains

delegate subdomain to Azure DNS

same process as standard delegation

NS records must be created in parent zone rather than registrar

parent and child zones can be in different RG

Record Set	collection of records in a zone, same name 'n type
	cannot contain identical records
	empty records possible
	CNAME can contain one record at most

Delegate DNS Domains

Azure DNS name servers assigned from a pool

NS records to be updated in parent domain to point to Azure DNS name server

always use all 4 Azure name server names

SKU public ip addresses

Public IP Address	Standard	Basic
Allocation method	Static	IPv4: Sta/Dyn IPv6: Dyn
Idle Timeout	4-30 min (4 default) inbound, 4 min outbound	4-30 min (4 default) inbound, 4 min outbound
Security	Allow traffic w NSG, Secure by default	Open by default, NSG optional
Availability Zones	supp: non-zonal, zonal, zone-redundant (3 zones only)	Not supported
Routing preference	supported for granular traffic control	Not supported
Global Tier	Support via cross-region LB	Not supported

VNet Peering Types

Regional VNet-P-eering	connect in same region
Global VNet-P-eering	connect in different regions, all regions possible

VNet Default Routes

Address prefixes	Next hop type
Unique to the virtual network	Virtual network
0.0.0.0/0	Internet
10.0.0.0/8	None (dropped)
192.168.0.0/16	None (dropped)
100.64.0.0/10	None (dropped)



VNet Original Default Routes

Source	Address Prefix	Next hop type	Subnet within virtual network that route is added to
Default	unique to virtual network	VNet peering	All
Virtual network gateway	on-prem prefixes adv via BGP	Virtual network gateway	All
Default	Multiple	VirtualNetworkServiceEndpoint	only subnet service endpoint is enabled for

Regions and Subscriptions

Resource can only be in same region subscription as VNet it's created in

VNets in different regions, subscription can be connected

Subscriptions have a VNet limit

DNS - public considerations

zone name must be unique in RG, zone must not exist already

zone name can be reused in RG and different subscriptions

different name server addresses when same zone name used multiple times

root/parent domain registered at registrar, points to Azure NS

child domains in Azure DNS registered

DNS - public

use Azure DNS (uses anycast)

DNS entries created manually in zones (A/AAAA/CNAME)

no custom DNS needed, DNS zone must be created, each DNS entry created in that zone

Private DNS Services

3 methods	Azure DNS Private Zones
	Azure-provided name resolution
	Name resolution with own DNS server
Access recursive resolvers	via 169.63.129.16

Azure provided DNS

created with VNet

Azure default internal DNS zone

.internal.cloudapp.net

resource name gets registered

Limits no resolution across VNets

resource name

no manual creation

Azure Private DNS Zone

capabilities configure name for DNS zone

manual record creation

resolve across zones and VNets

provide PTR, MX, SOA, service/text records

Registration VNet link to one private Zone

Resolution VNet can link to 1000 private DNS zones

Public IP Addresses - Static/Dynamic

Available Resources	VM NICs
	VM Scale Sets
	Public LB
	Virtual Network Gateways
	NAT Gateways
	Application Gateways
	Azure Firewall
	Bastion Host
	Route Server

Each region has own pool of public ip addresses

Availability Zones - Service Categories

Zonal Services	resources pinned to specific zone
	VMs, Managed Disks, Standard IP Addresses
Zone-Redundant Services	resources replicated/distributed across zones autom.
Non-regional Services	Services always available from Azure Geos
	resilient to zone and region-wide outages

VNet Gatewaytransit and Connectivity

VPN Gateway as transit point

Remote gateway to access other resources

VNet can have only one gateway

Subnetgateway capabilities S2S VPN

VNet-to-VNet

P2S VPN

VNets can use a gateway, only one needed

Service chaining VNet connect to NVA (network virtual appliance)

VNet can be in different subscription

UDRs will be created



By **Termo**
cheatography.com/termo/

Not published yet.
Last updated 23rd June, 2023.
Page 3 of 3.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>