

Build It Yourself

An Azure landing zone a DBA can read: everything from Part 2 in build order, with the exact values. Prefer code? Skip to the end for the Bicep route.

1 Resource groups

Resource groups > Create. Use region **West US 3** and tag project = hybrid-ag-lab on both.

Name	Holds
rg-hyb-core	Network and storage
rg-hyb-compute	VMs (later parts)

2 Network security groups

Network security groups > Create (in rg-hyb-core), then **Settings > Inbound security rules > Add.**

On every allow rule:

- Source: IP addresses 192.168.100.0/24, 10.20.0.0/16
- Source port: *
- Destination: Any

nsg-hyb-sql

Priority	Name	Protocol	Destination ports	Action
100	allow-sql-tcp	TCP	1433, 5022, 3343, 135, 445, 3389, 5985, 49152-65535	Allow
110	allow-sql-udp	UDP	3343	Allow
120	allow-icmp	ICMPv4	Any	Allow
4000	deny-vnet-other	Any (source: service tag VirtualNetwork)	Any	Deny

5985 was added in Part 6.

nsg-hyb-identity

Priority	Name	Protocol	Destination ports	Action
100	allow-ad-tcp	TCP	53, 88, 135, 389, 445, 464, 636, 3268-3269, 3389, 9389, 49152-65535	Allow
110	allow-ad-udp	UDP	53, 88, 123, 389, 464	Allow
120	allow-icmp	ICMPv4	Any	Allow
4000	deny-vnet-other	Any (source: service tag VirtualNetwork)	Any	Deny

nsg-hyb-edge

Priority	Name	Source	Protocol	Port	Action
100	allow-wireguard	Service tag Internet	UDP	51820	Allow

Two forwarded-traffic rules join this NSG in Part 5.

3 Route table

Route tables > Create: rt-hyb-to-lab, Propagate gateway routes **No**. Then **Settings > Routes > Add:**

Route name	Destination	Next hop type	Next hop address
to-lab	192.168.100.0/24	Virtual appliance	10.20.0.4

4 Virtual network

Virtual networks > Create: vnet-hyb-westus3, address space 10.20.0.0/16, with these subnets:

Subnet	Range	NSG	Route table	Extra
snet-edge	10.20.0.0/24	nsg-hyb-edge	None	
snet-identity	10.20.1.0/24	nsg-hyb-identity	rt-hyb-to-lab	
snet-sql	10.20.2.0/24	nsg-hyb-sql	rt-hyb-to-lab	Service endpoint: Microsoft.Storage

Leave "private subnet" unchecked on snet-identity and snet-sql. Part 5 explains why.

5 DNS

The VNet's **Settings > DNS servers > Change > Custom**. Use your lab DC: 192.168.100.10. In Part 5, AZ-DC02 (10.20.1.10) gets added in front of it.

6 Storage account for the witness

Storage accounts > Create (in rg-hyb-core):

Setting	Value
Name	Your choice (globally unique)
Performance	Standard
Redundancy	Locally redundant storage (LRS)
Minimum TLS	1.2
Anonymous blob access	Disabled

Rather use code?

The full **core.bicep** is in my GitHub repo (github.com/Jordan-A-Boich). Point it at your storage account name and run `what-if` first to see what it would change:

```
$sa = '<your storage account name>'
az deployment group what-if -g rg-hyb-core -f .\core.bicep -p witnessStorageName=$sa
az deployment group create -g rg-hyb-core -f .\core.bicep -p witnessStorageName=$sa
```

Beyond Port 1433 is a home lab series, not a production design. Part 11 covers what changes in a real environment. · dbaunfiltered.com