04

CLOUD SECURITY OPERATIONS / CLOUD NETWORKING (CNW) — MODULE 2, LAB 2.5

Cloud Security Operations Report: Azure Hybrid Active Directory Domain (Lab 2.5)

Multi-region Azure AD hybrid domain with load-balanced NAT pivoting and red-team lateral movement across CNW.BIZ

COURSE
Cloud Security Operations / Cloud Networking (CNW) — Module 2, Lab 2.5

DATE
April 2025

ENVIRONMENT
Azure for Students subscription (ID 4ddeee3e-9824-4cd4-ba1e-a8304c5708e7)

PAGES (REPORT)
15

STUDENT
Cody Richard · 0005288412

ORGANIZATION
Full Sail University

TECHNICAL BRIEF · EXECUTIVE SUMMARY

Cloud Security Operations Report: Azure Hybrid Active Directory Domain (Lab 2.5)

For this module I deployed and validated a hybrid Active Directory environment spanning two Azure regions (West US and Central US) under my Azure for Students subscription, engineered to mirror a segmented corporate network with a trust boundary between Azure AD and on-prem-style resources. I stood up two virtual networks (10.0.0.0/24 and 10.0.1.0/24), bridged them with bidirectional VNet peering, and fronted the VMs with two Standard-SKU load balancers using inbound NAT rules to publish RDP. I promoted cnw-websrv (Windows Server 2019) to domain controller for the CNW.BIZ domain, configured DNS across both VNets, and hybrid-joined both Windows 10 clients to the domain. From an initial NAT-published foothold on Client01 I demonstrated internal pivoting to Client02 and the web server, documenting the lateral-movement and hybrid-trust-abuse path before exposing all three systems via external RDP and performing a complete teardown of every provisioned resource.

▸ Objectives

- Deploy a hybrid Active Directory domain (CNW.BIZ) across two Azure regions with static private IP addressing
- Connect two regional virtual networks via bidirectional VNet peering to enable cross-region routing
- Publish secure RDP access through Standard-SKU load balancers and inbound NAT rules
- Promote a Windows Server 2019 VM to domain controller and configure DNS for both VNets
- Hybrid-join both Windows 10 clients to the CNW.BIZ domain and validate domain trust
- Demonstrate red-team lateral movement: initial NAT foothold pivoting internally to all hosts
- Tear down all cloud resources to comply with the lab's deletion requirements

▸ Environment

`Azure for Students subscription (ID 4ddeee3e-9824-4cd4-ba1e-a8304c5708e7)`

`Azure regions: West US and Central US`

`Resource Group: LNFI-042025`

`VNet LNFI-West-VNet — 10.0.0.0/24 (West US)`

`VNet LNFI-Central-VNet — 10.0.1.0/24 (Central US)`

`Windows Server 2019 domain controller (cnw-websrv, 10.0.0.100)`

WALKTHROUGH & EVIDENCE

This walkthrough documents a hybrid Active Directory build spanning two Azure regions (West US and Central US) under the CNW.BIZ domain, engineered to mirror a segmented corporate network with a trust boundary between Azure AD and on-prem-style resources. I stand up two peered virtual networks (10.0.0.0/24 and 10.0.1.0/24), publish RDP through Standard-SKU load-balancer NAT rules, promote cnw-websrv to domain controller, and hybrid-join both Windows 10 clients. From a NAT-published foothold on Client01 I map the lateral-movement and hybrid-trust-abuse path to Client02 and the DC, then tear the entire environment down to zero residual resources.

ENVIRONMENT

Resource Group & Network Core

Resource group LNFI-042025 anchors the build, spanning the West US and Central US regions under the Azure for Students subscription.

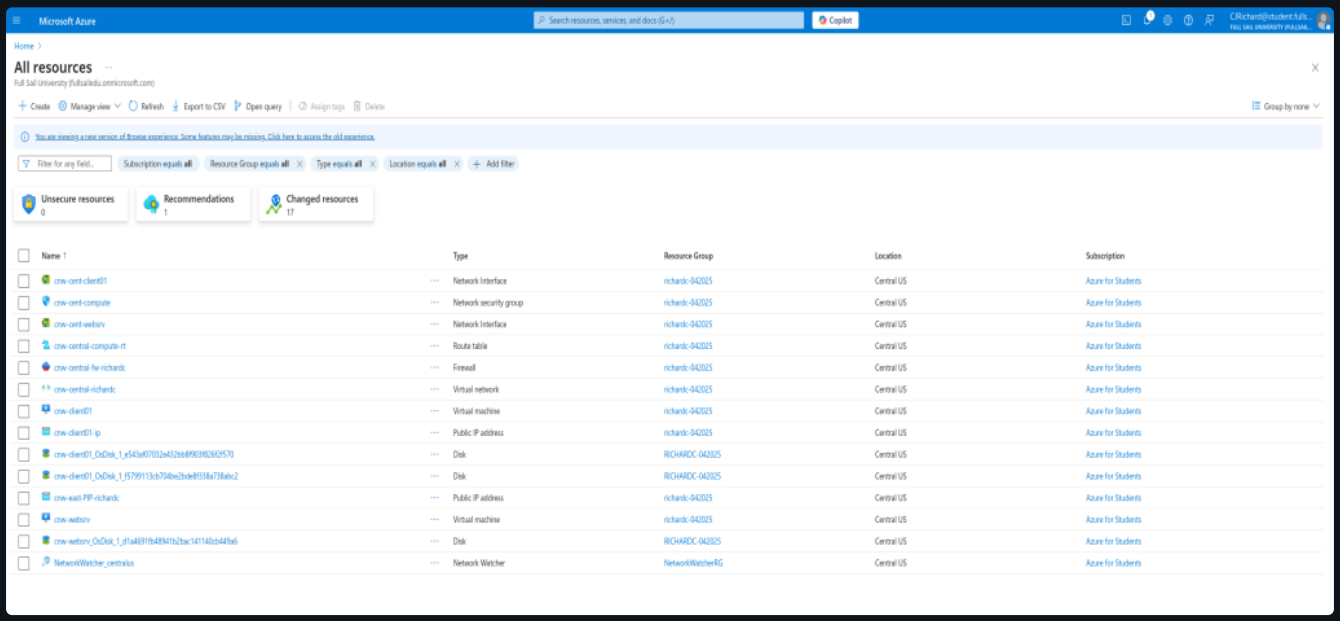

FIG 01 — Azure portal view of resource group LNFI-042025, with resources distributed across the West US and Central US regions.

NETWORKING

West VNet — 10.0.0.0/24

LNFI-West-VNet hosts the domain controller and Client01 in West US on a single /24.

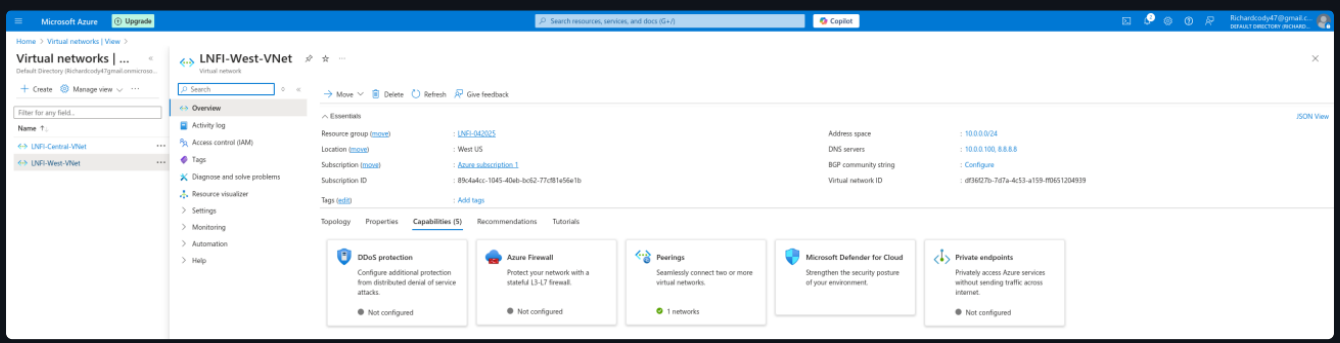

FIG 02 — LNFI-West-VNet overview: address space 10.0.0.0/24 in the West US region.

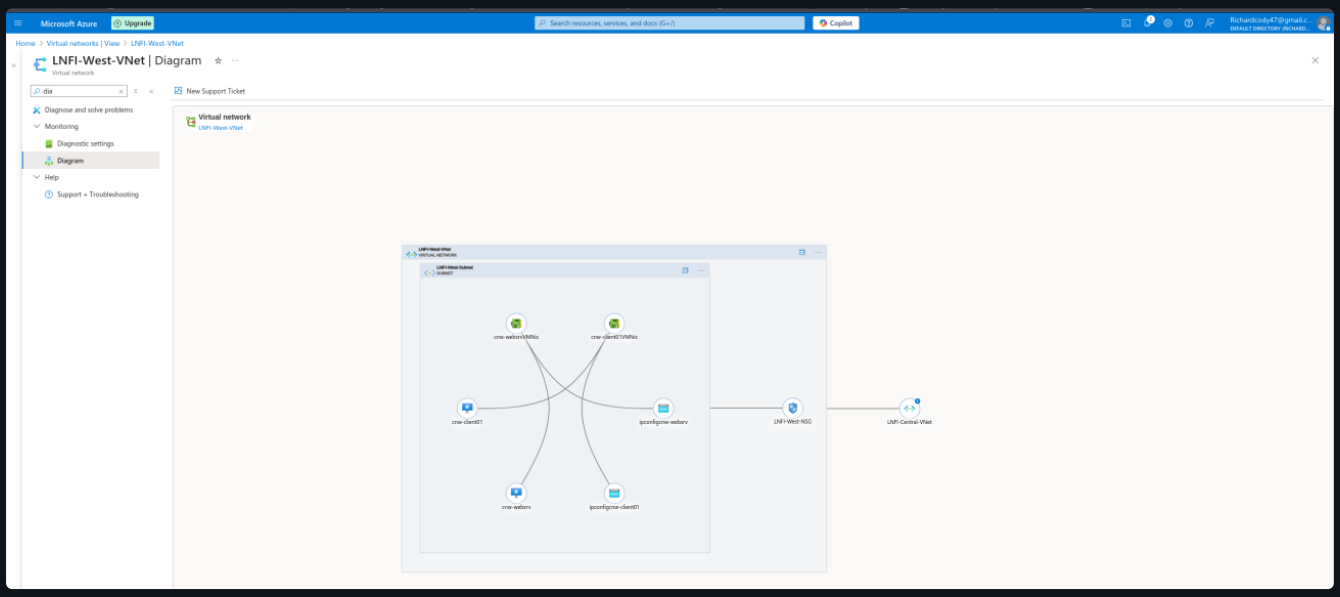

FIG 03 — West VNet subnet detail — the 10.0.0.0/24 subnet carrying cnw-websrv (10.0.0.100) and cnw-client01 (10.0.0.200).

NETWORKING

Central VNet — 10.0.1.0/24

LNFI-Central-VNet provides the second region's address space for Client02 in Central US.

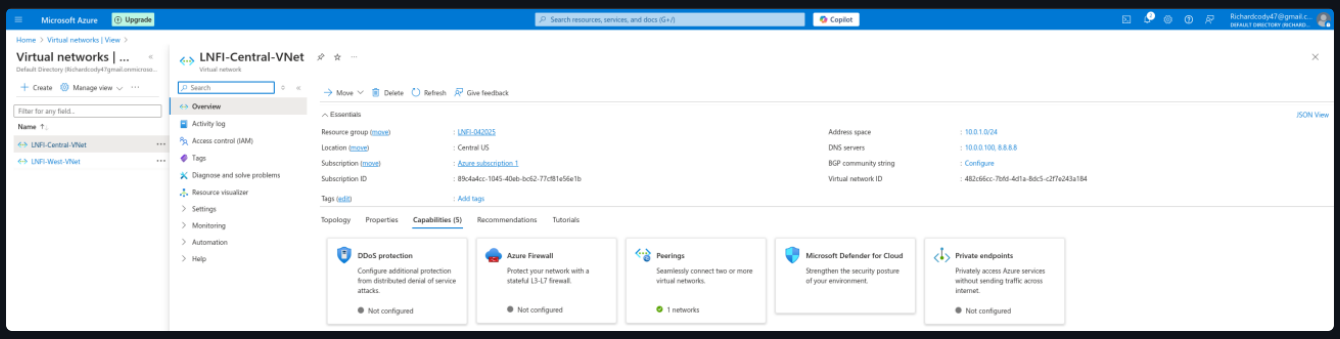

FIG 04 — LNFI-Central-VNet overview: address space 10.0.1.0/24 in the Central US region.

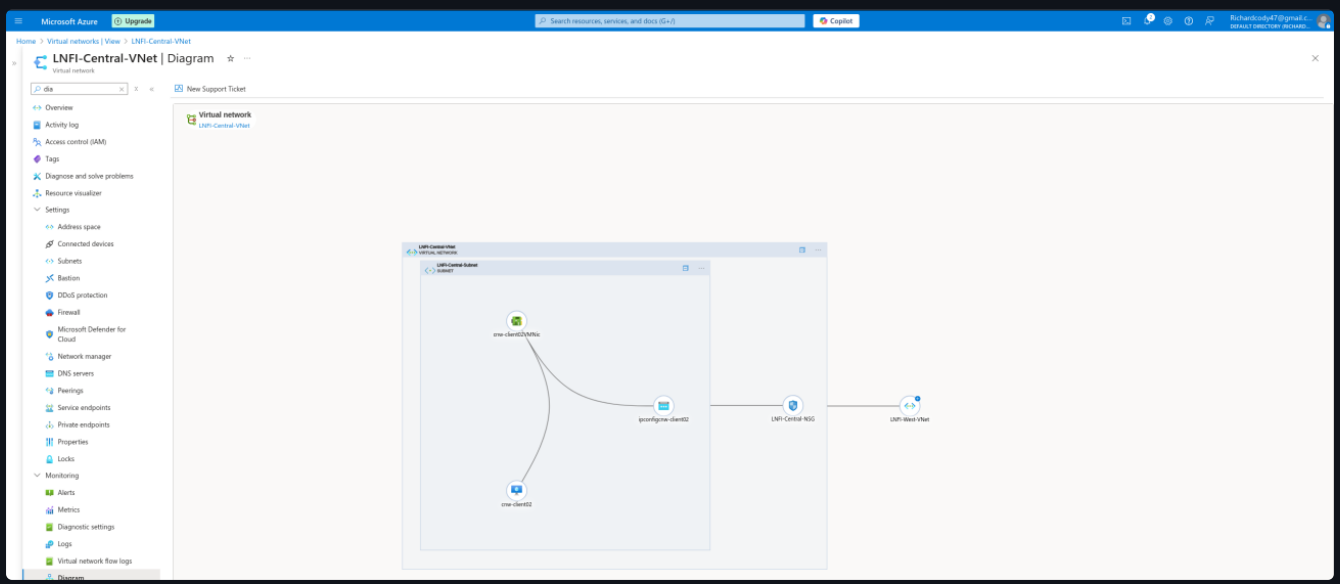

FIG 05 — Central VNet subnet detail — the 10.0.1.0/24 subnet hosting cnw-client02 (10.0.1.200).

NETWORKING

Cross-Region VNet Peering

Bidirectional peering links the West and Central VNets so the two /24s route to each other across regions.

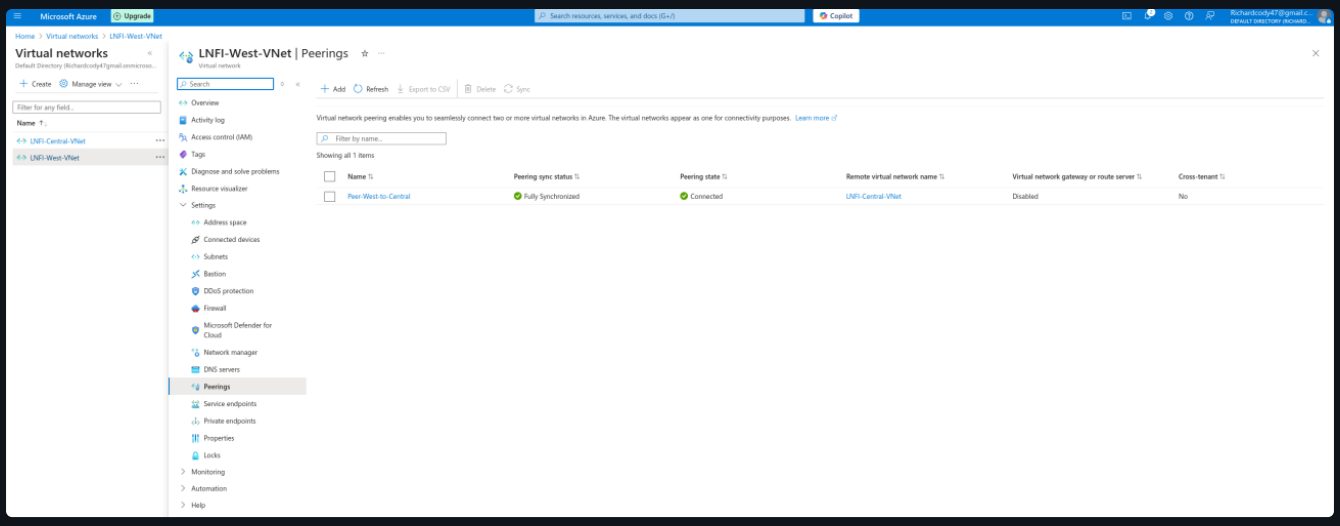

FIG 06 — VNet peering configured from LNFI-West-VNet to LNFI-Central-VNet, peering state Connected.

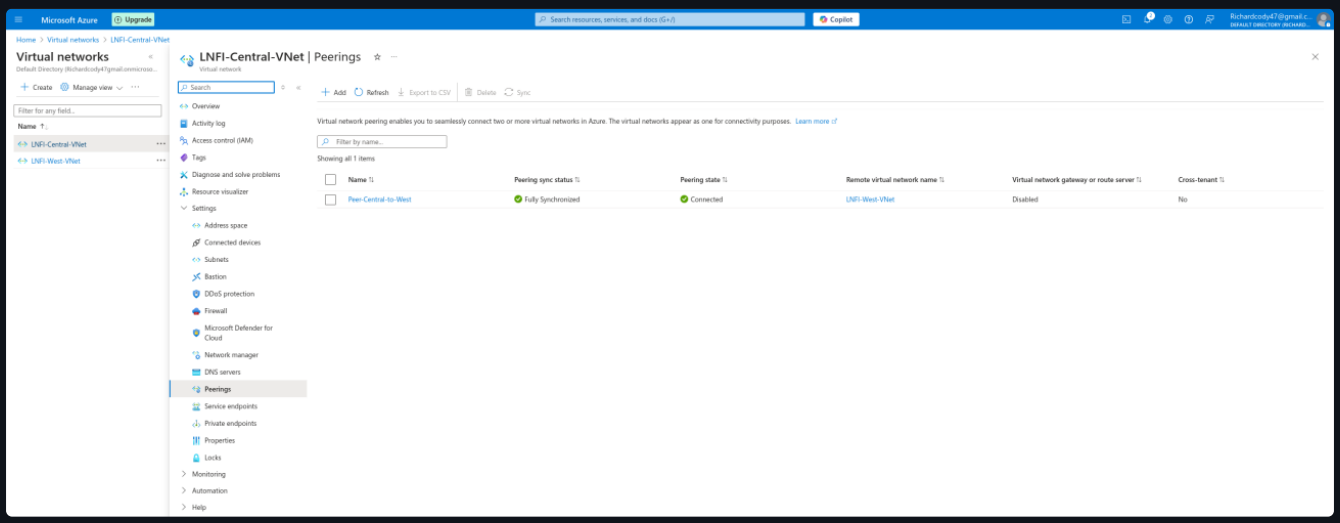

FIG 07 — Reverse peering from LNFI-Central-VNet back to LNFI-West-VNet, completing bidirectional cross-region reachability between 10.0.0.0/24 and 10.0.1.0/24.

INGRESS

West Load Balancer — NAT to DC & Client01

Standard-SKU load balancer LNFI-West-LB publishes RDP for the West-region hosts via inbound NAT rules.

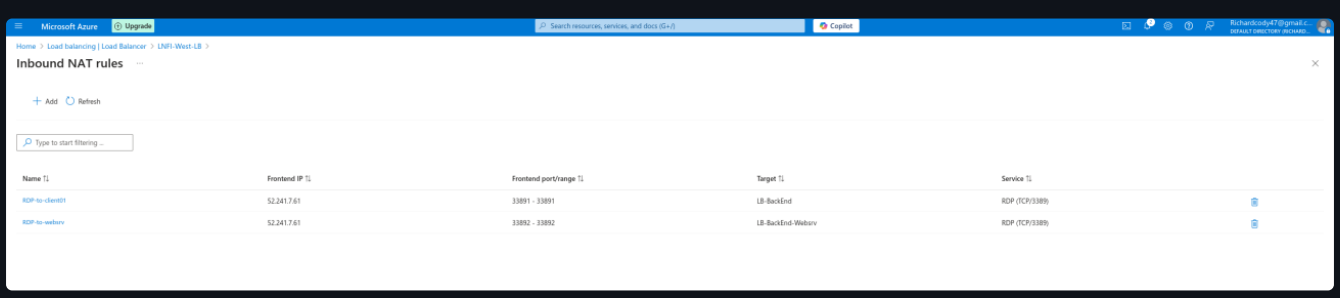

FIG 08 — LNFI-West-LB (Standard SKU) overview with its public frontend IP.

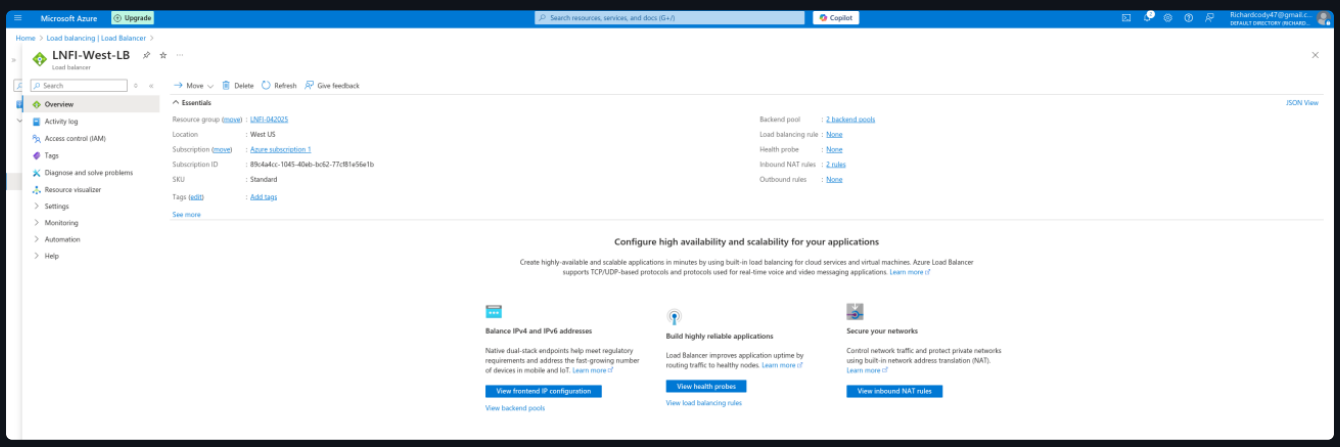

FIG 09 — West load-balancer inbound NAT rules: frontend 33891 to cnw-client01:3389 and 33892 to cnw-websrv:3389.

INGRESS

Central Load Balancer — NAT to Client02

Standard-SKU load balancer LNFI-Cent-LB fronts the Central-region client with a single NAT rule.

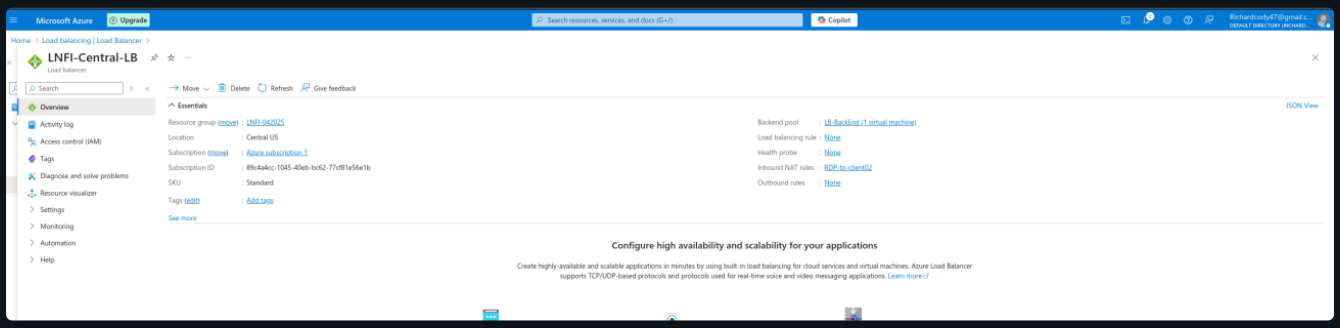

FIG 10 — LNFI-Cent-LB (Standard SKU) overview with its public frontend IP.

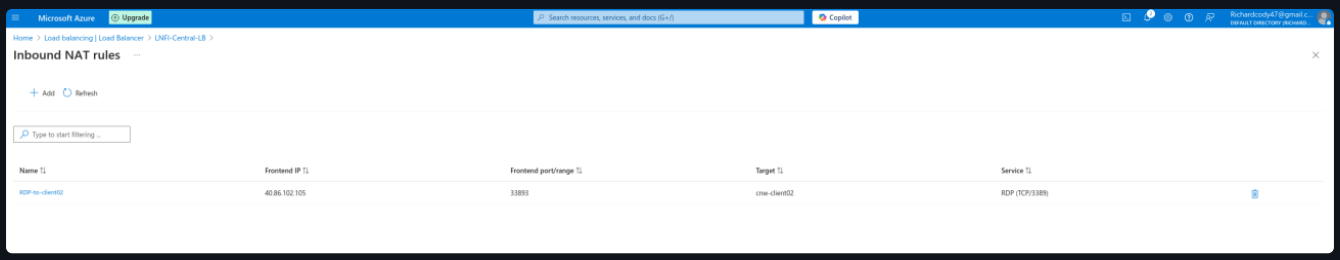

FIG 11 — Central load-balancer inbound NAT rule: frontend 33893 to cnw-client02:3389.

ATTACK PATH

Network Pivot Flow

The pivot diagram traces how the NAT-published foothold on Client01 opens full internal domain traversal.

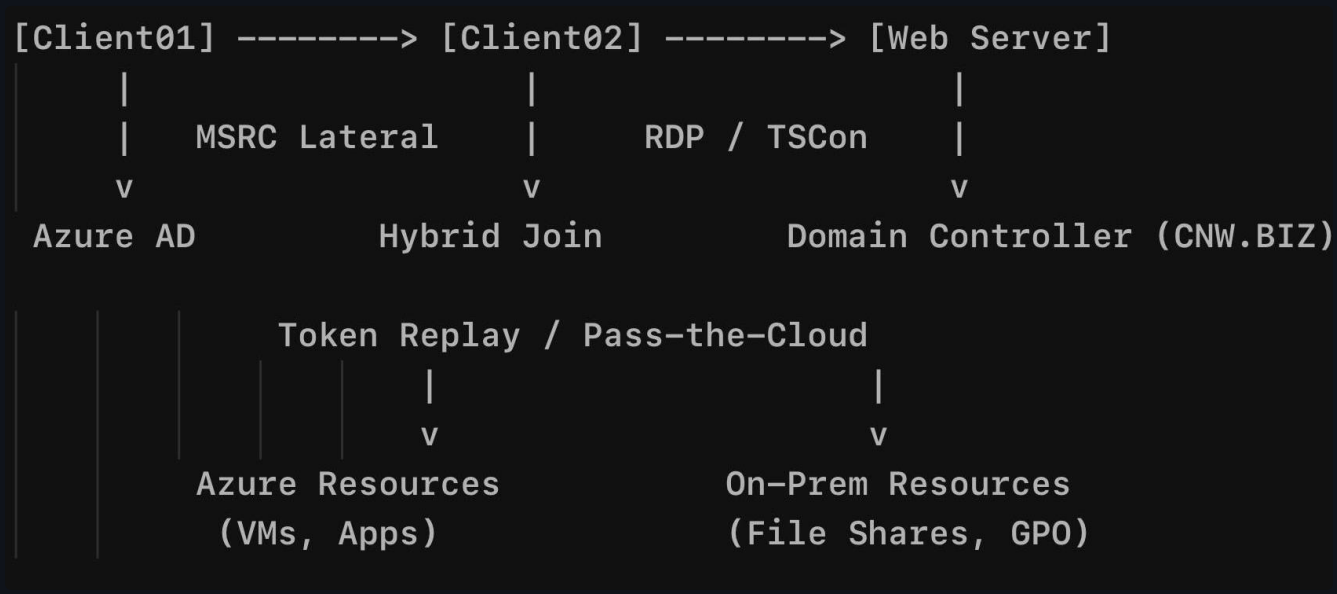

FIG 12 — Network pivot flow: initial NAT access to Client01 enables internal lateral movement to Client02 and the web server, exposing hybrid-trust abuse.

DEPLOYMENT

Virtual Machines Deployed

Three VMs make up the domain: the Server 2019 DC plus two Windows 10 clients, one per region.

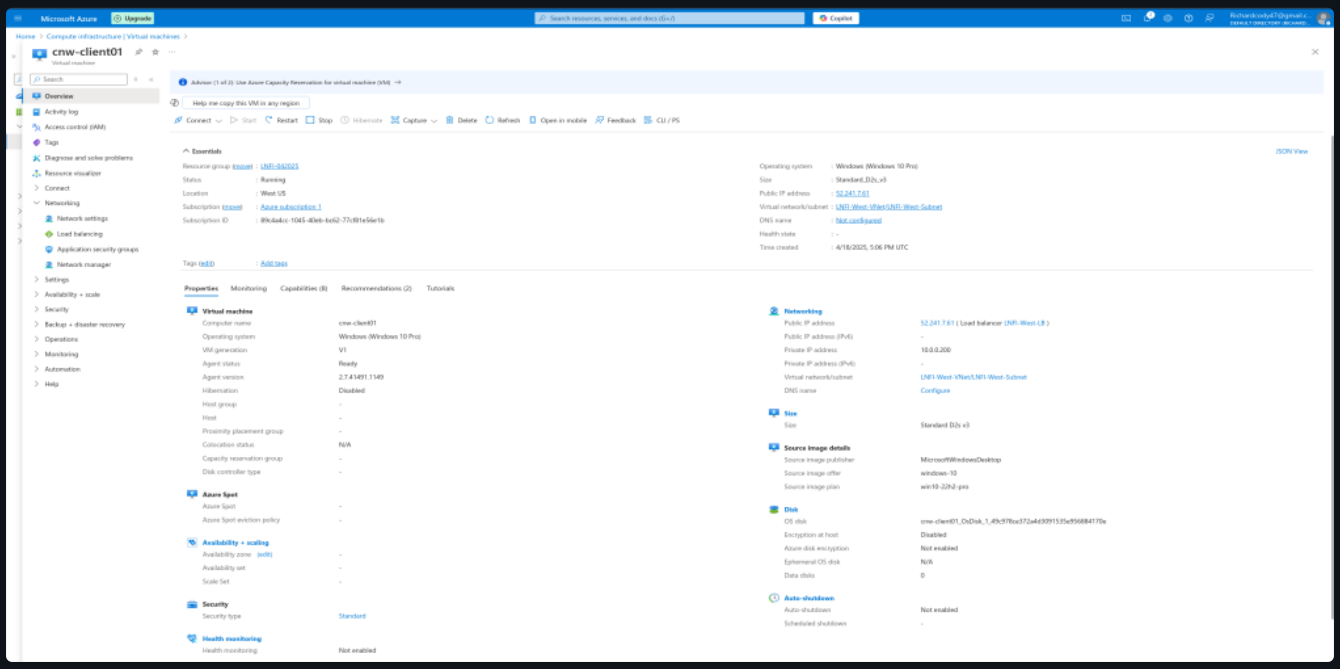

FIG 13 — Deployed VM inventory in the Azure portal across both regions.

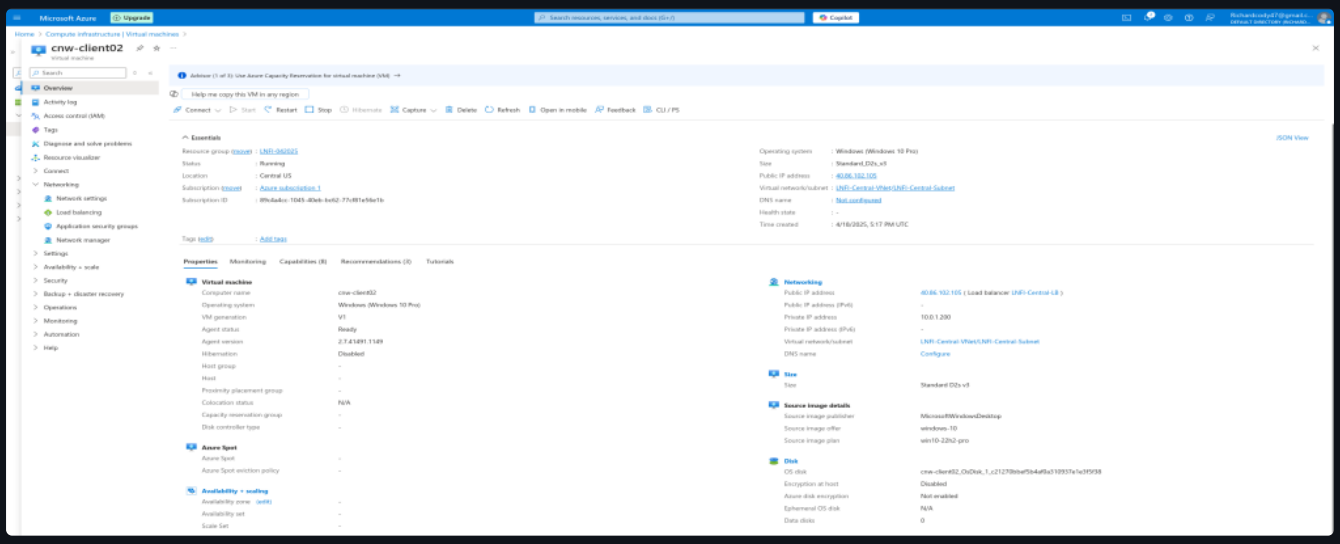

FIG 14 — VM detail — cnw-websrv (Windows Server 2019, 10.0.0.100, West US) and cnw-client01 (Windows 10, 10.0.0.200, West US).

DEPLOYMENT

Central-Region Client

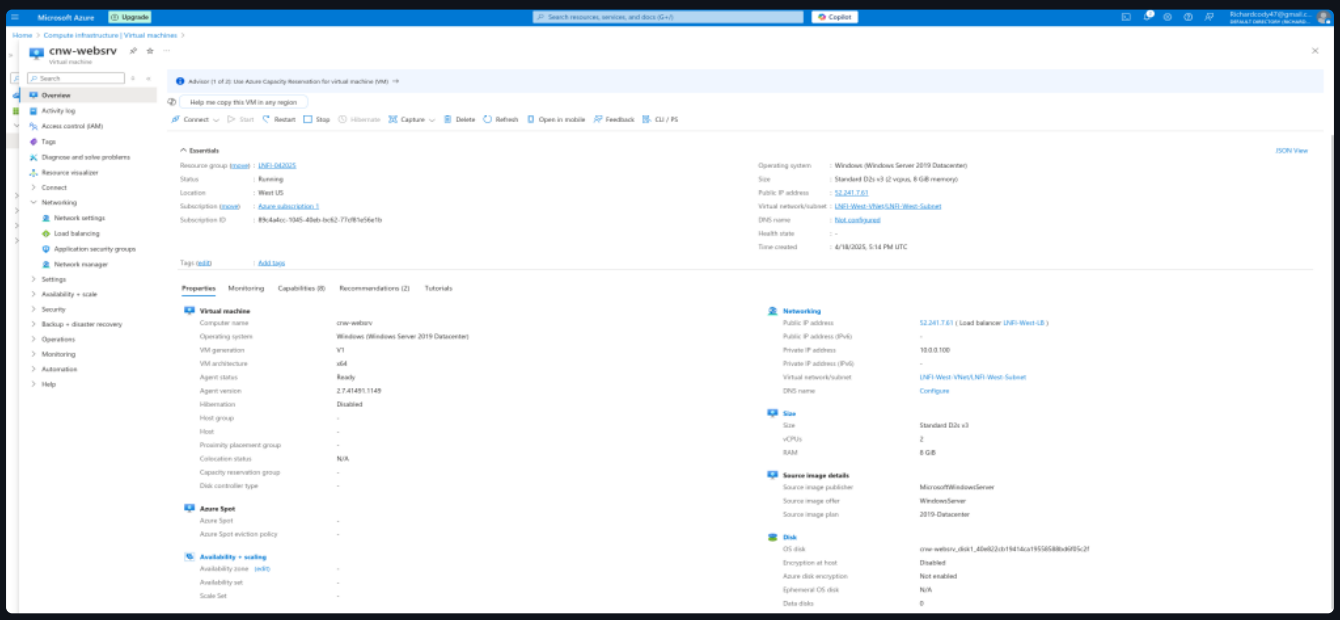

FIG 15 — VM detail — cnw-client02 (Windows 10, 10.0.1.200, Central US).

DOMAIN SERVICES

DNS & Domain Join

cnw-websrv (10.0.0.100) is promoted to domain controller for CNW.BIZ; DNS is applied to both VNets with 8.8.8.8 as secondary.

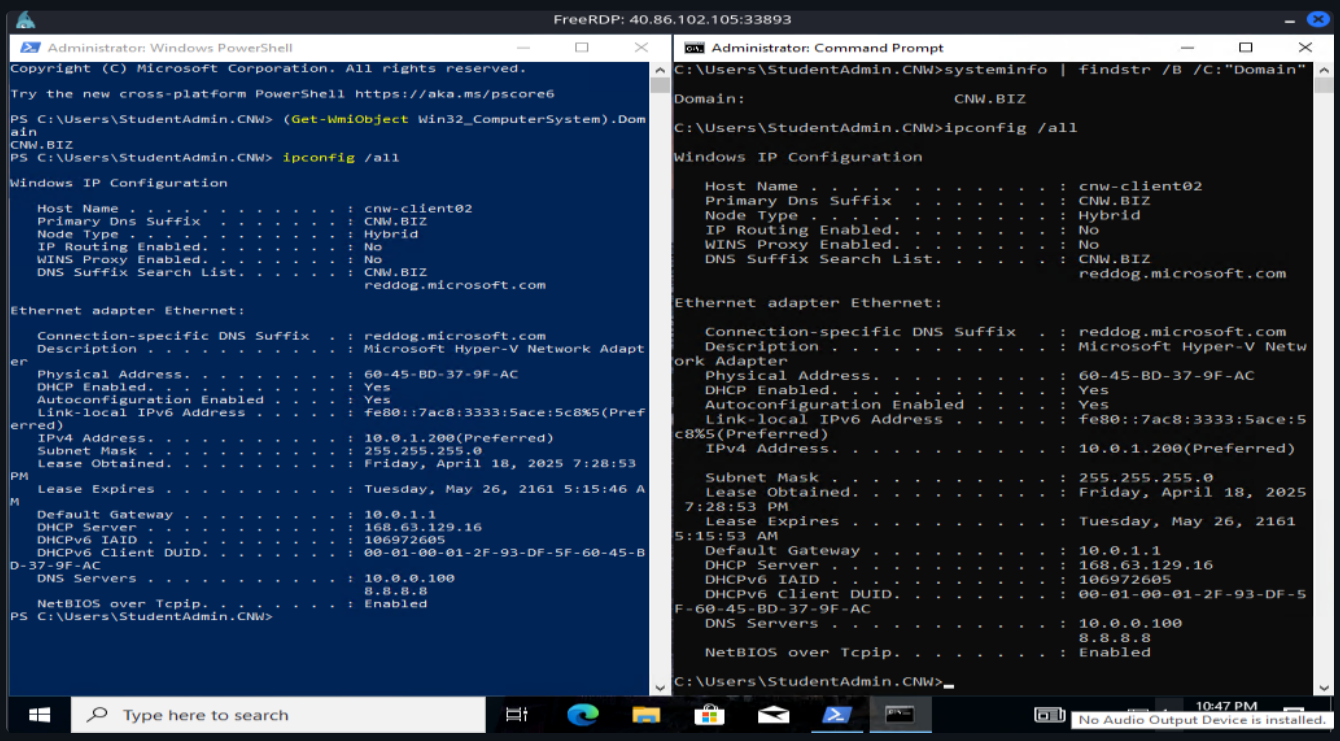

FIG 16 — Domain controller promotion / Active Directory configuration on cnw-websrv for the CNW.BIZ domain.

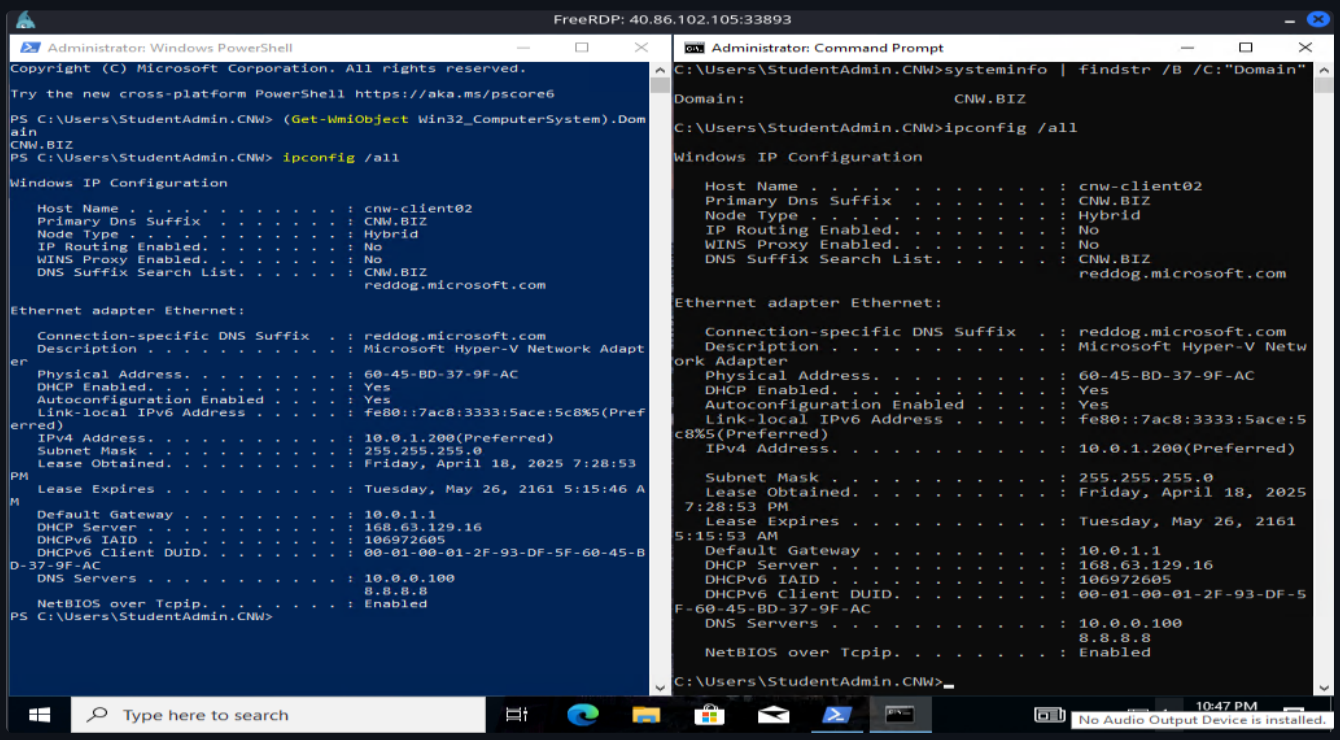

FIG 17 — DNS configuration applied to both VNets — primary 10.0.0.100 (DC), secondary 8.8.8.8 (Google Public DNS).

VERIFICATION

Domain Join Confirmed

Both Windows 10 clients hybrid-join CNW.BIZ, validating domain trust across the two regions.

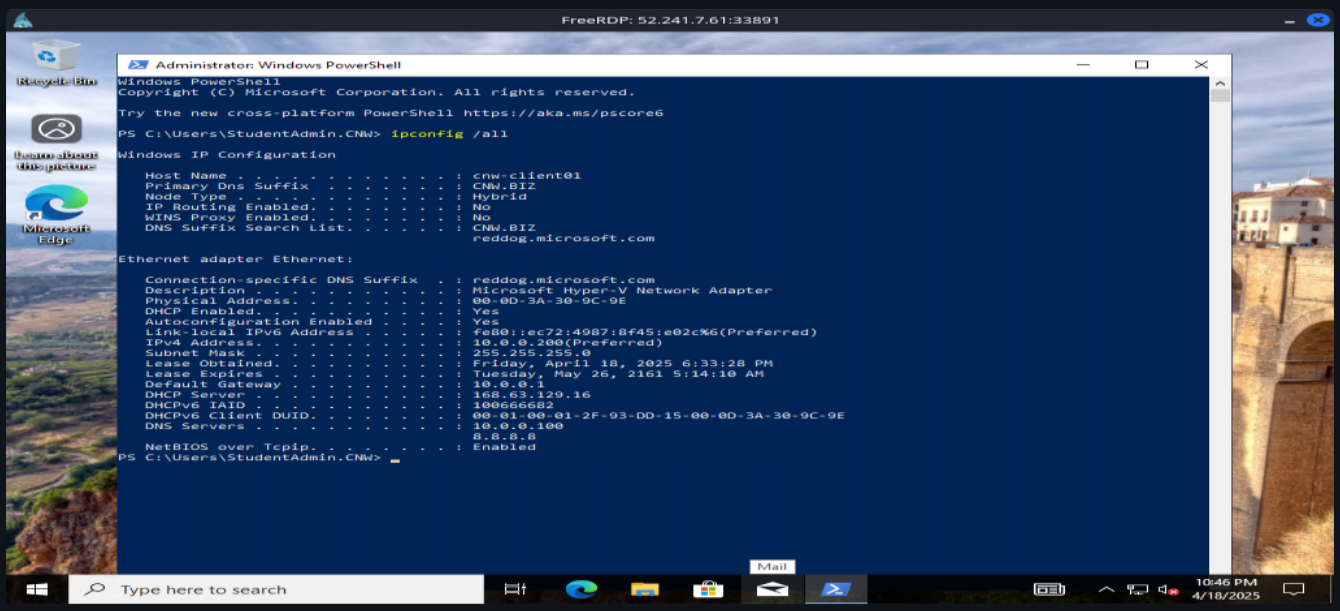

FIG 18 — Domain membership verified — cnw-client01 and cnw-client02 successfully joined to CNW.BIZ.

TEARDOWN

Full Resource Cleanup

Per the lab's deletion requirement, every provisioned resource is removed — both load balancers, all public IPs, NSGs, peerings, all three VMs, both VNets, and the resource group itself.

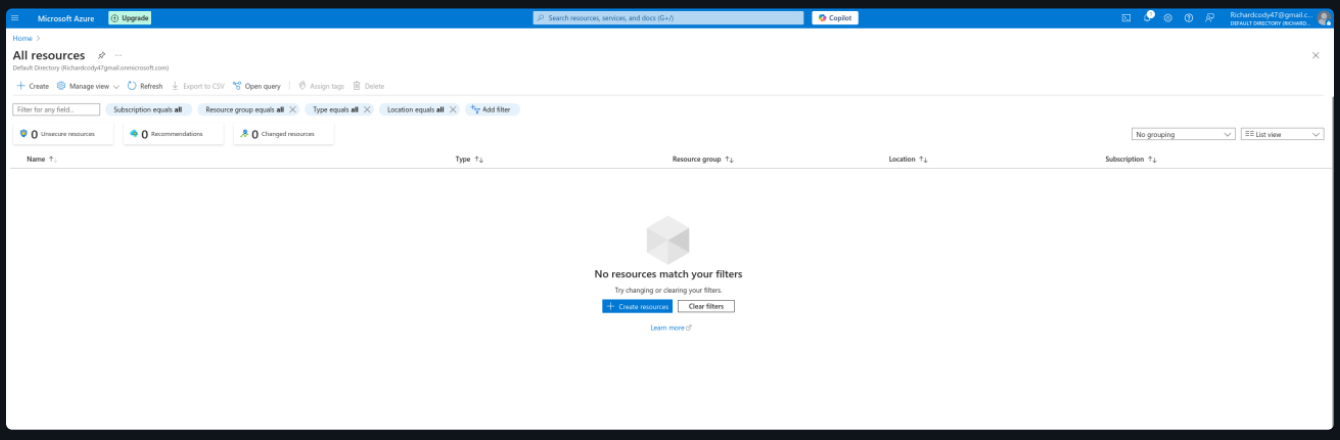

FIG 19 — Teardown confirmation — deletion of the LNFI-042025 resource group and all child resources, leaving no residual infrastructure in the subscription.