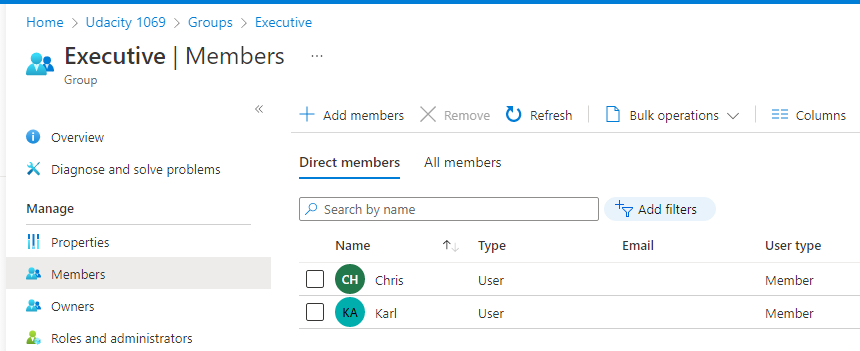
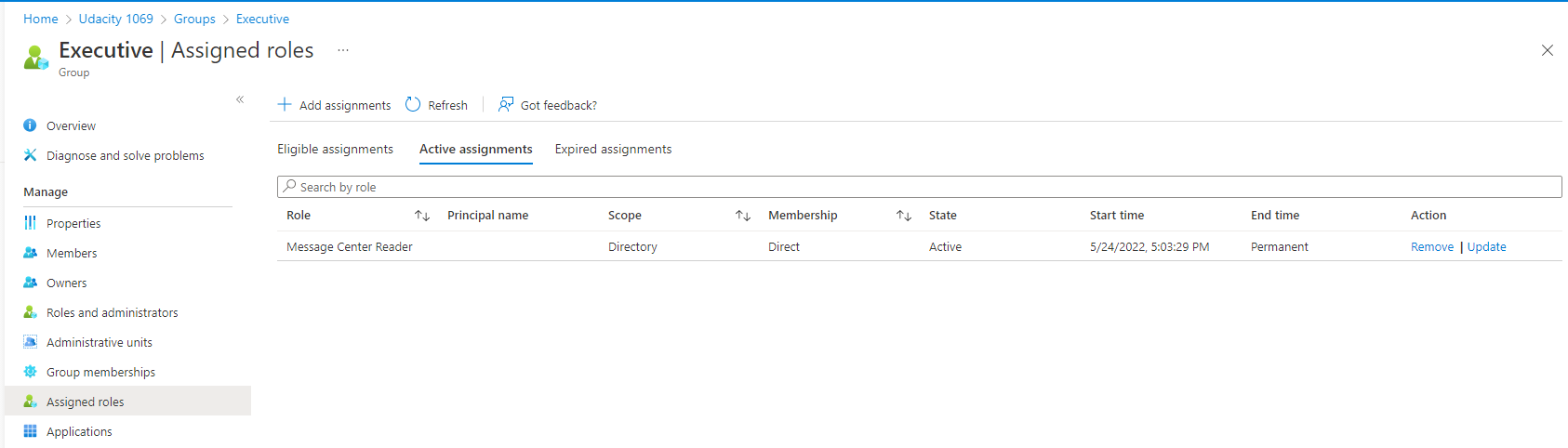
***Attention students:***

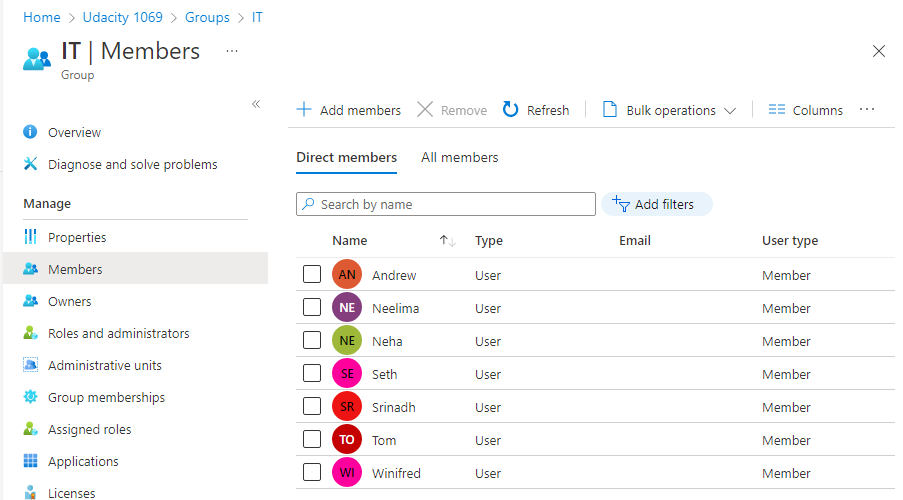
***In order to demonstrate successful completion of all components in the project, please use screenshot(s) to show each completed action step as specified on the instructions page.***

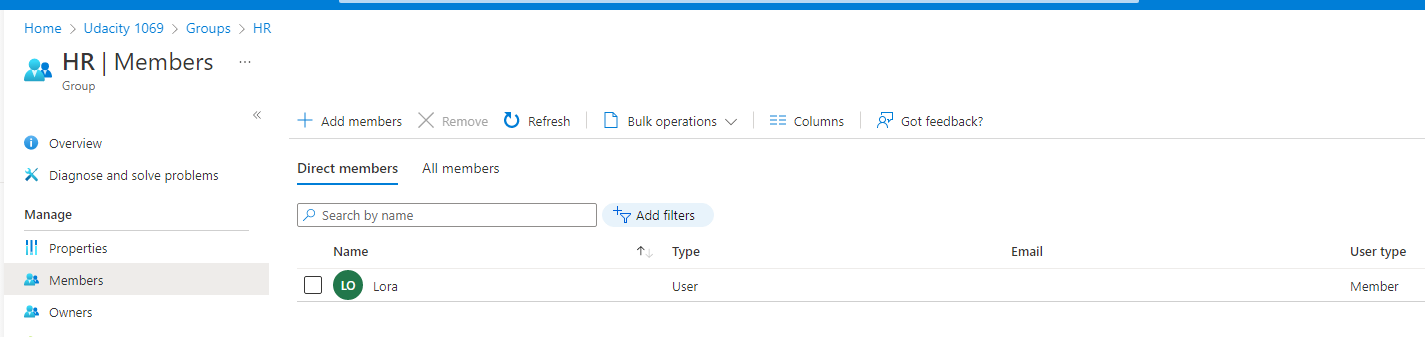
**Identity and Access Management**

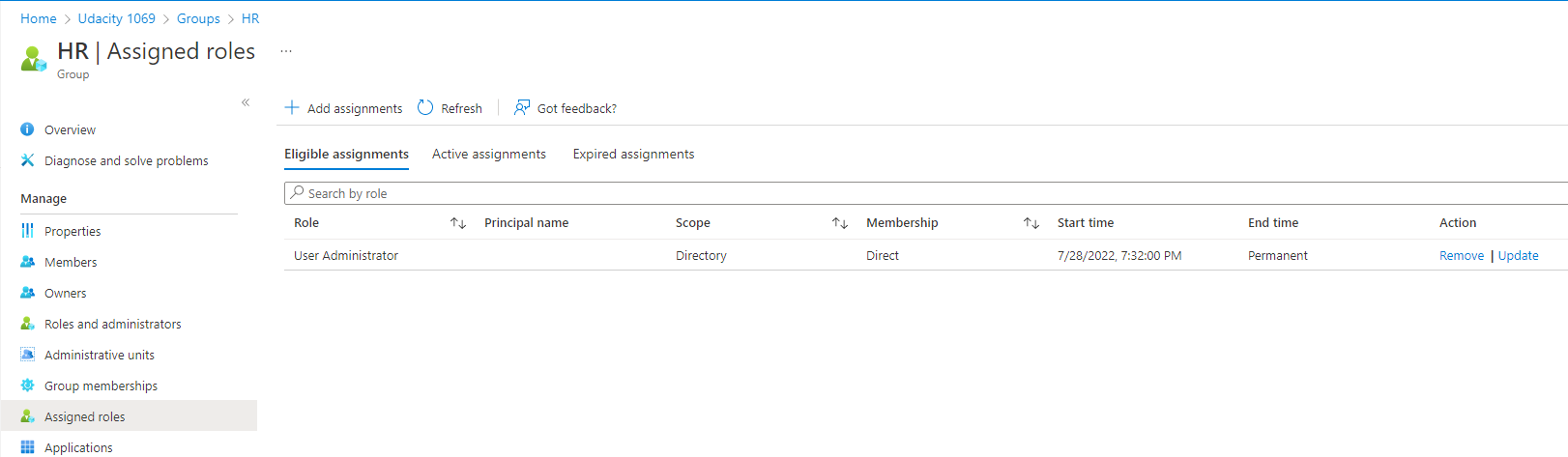
1. Proof of Assigned roles and AD assignments
   1. Andrew
   2. Chris
   3. Karl
   4. Lora
   5. Neelima
   6. Neha
   7. Seth
   8. Srinadh
   9. Tom
   10. Winifred

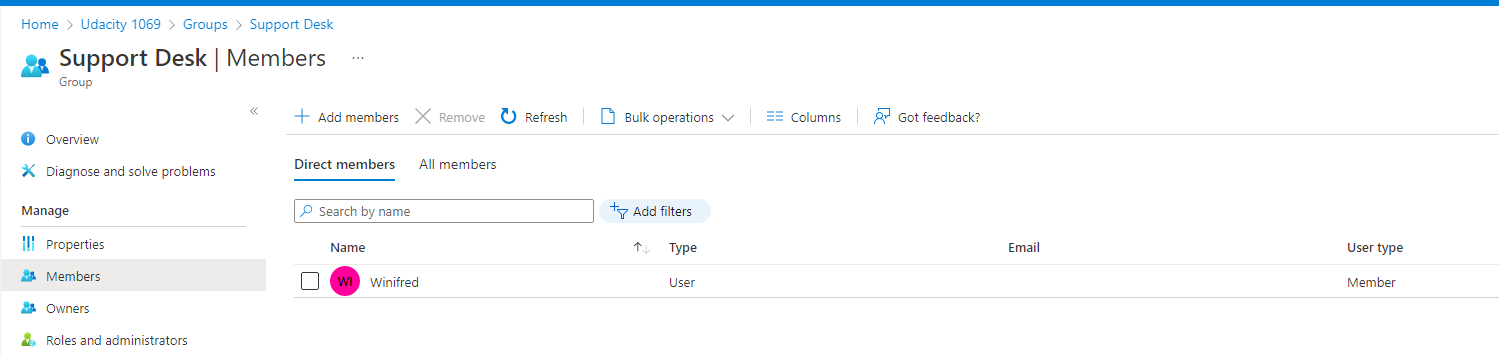


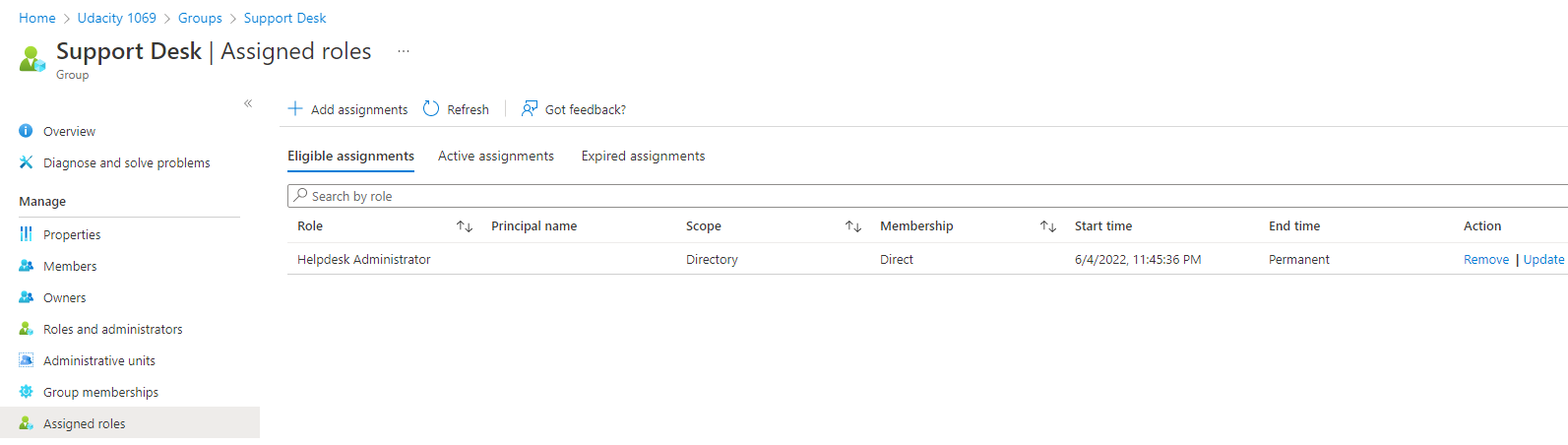


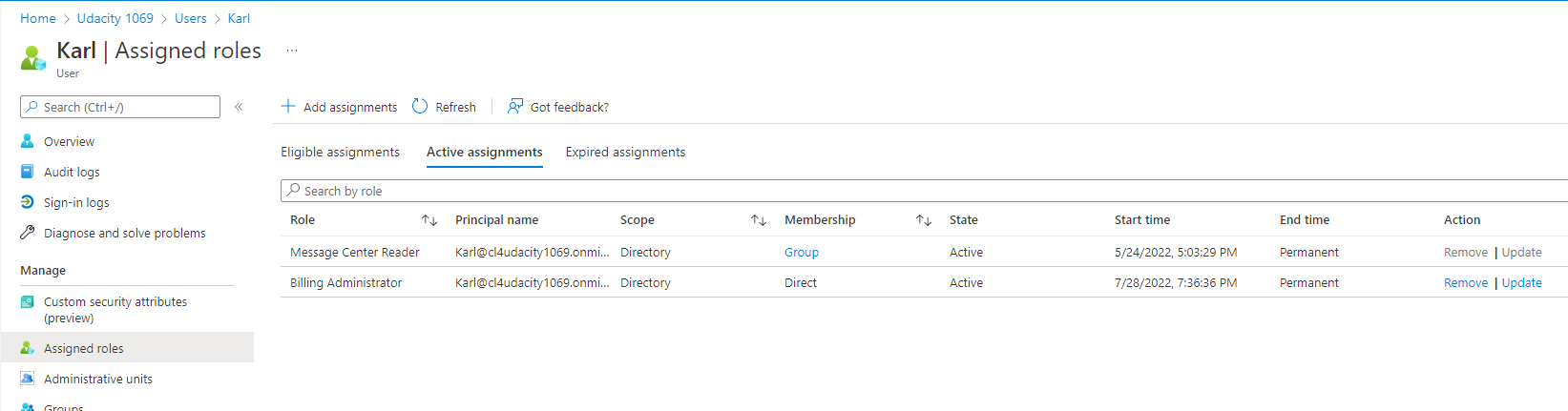


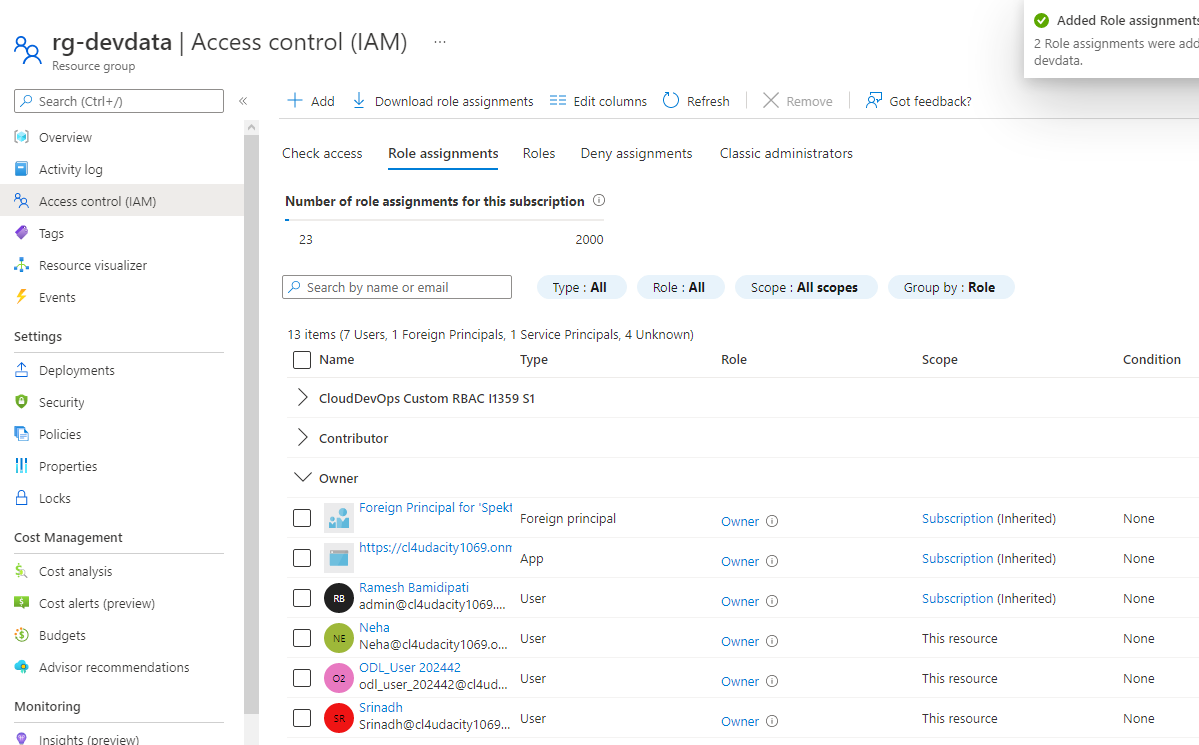


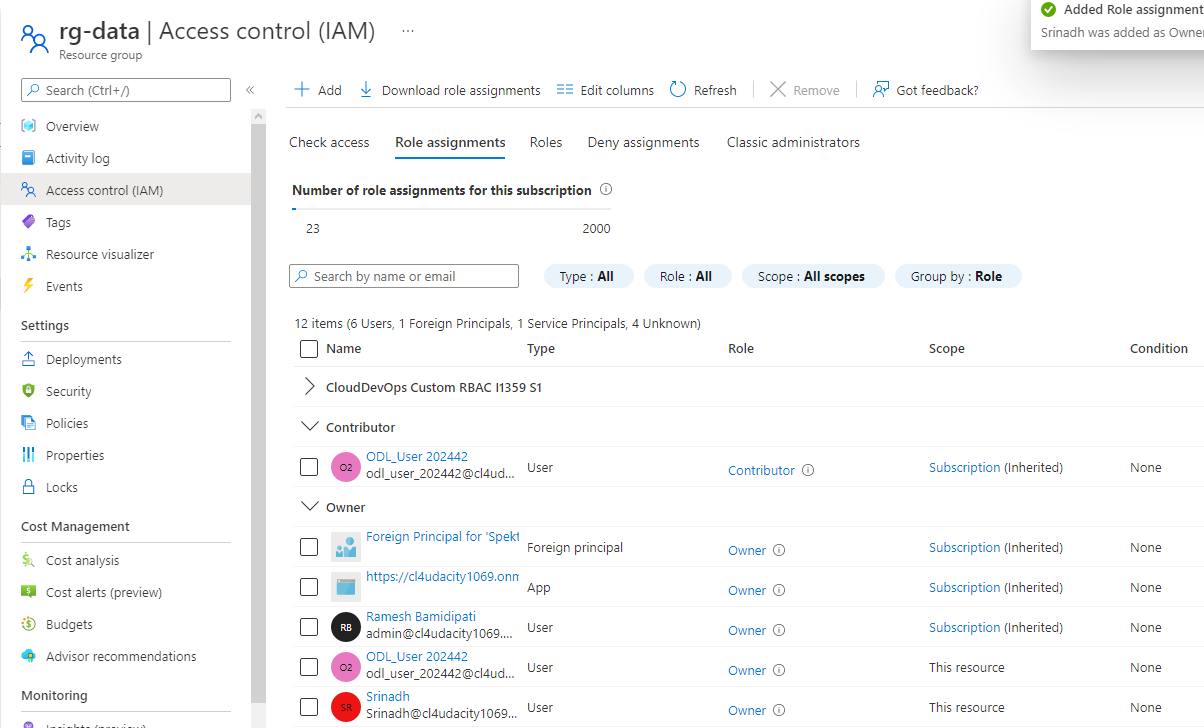






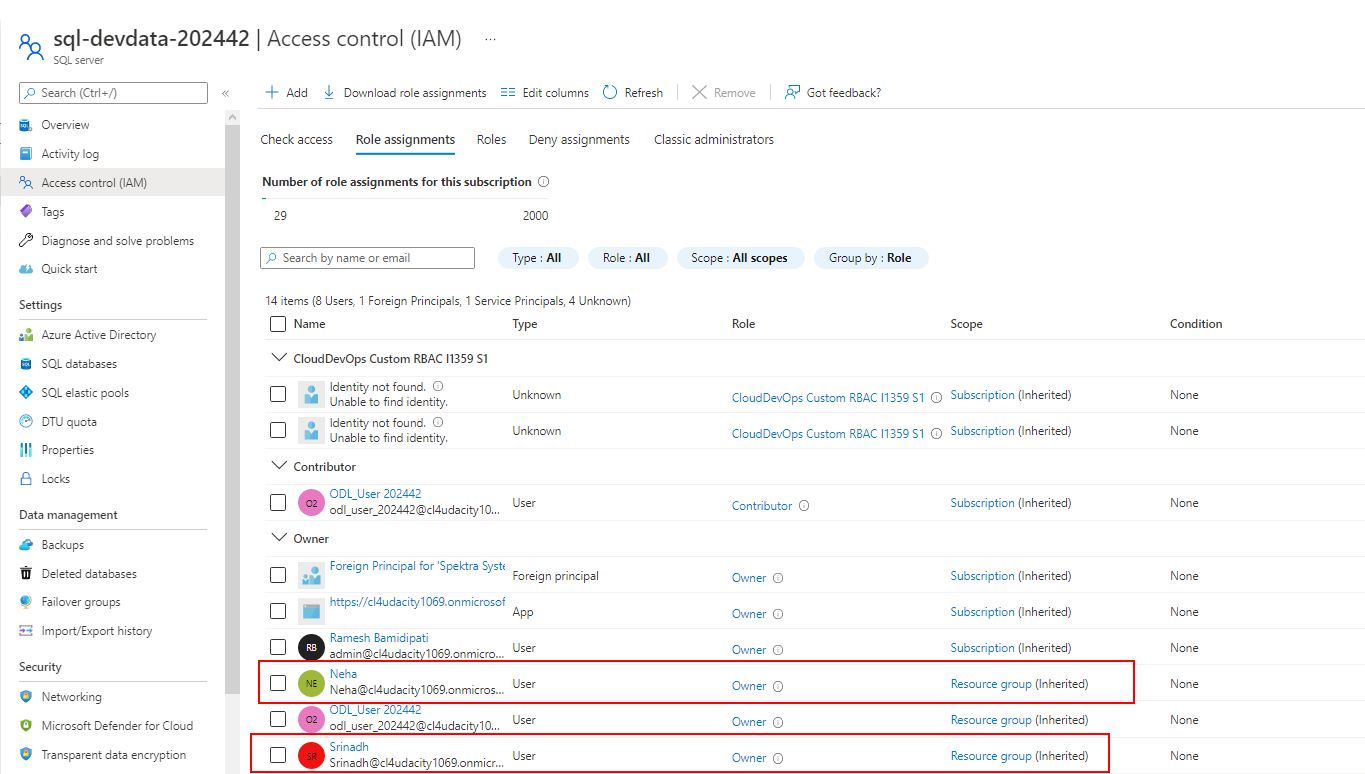


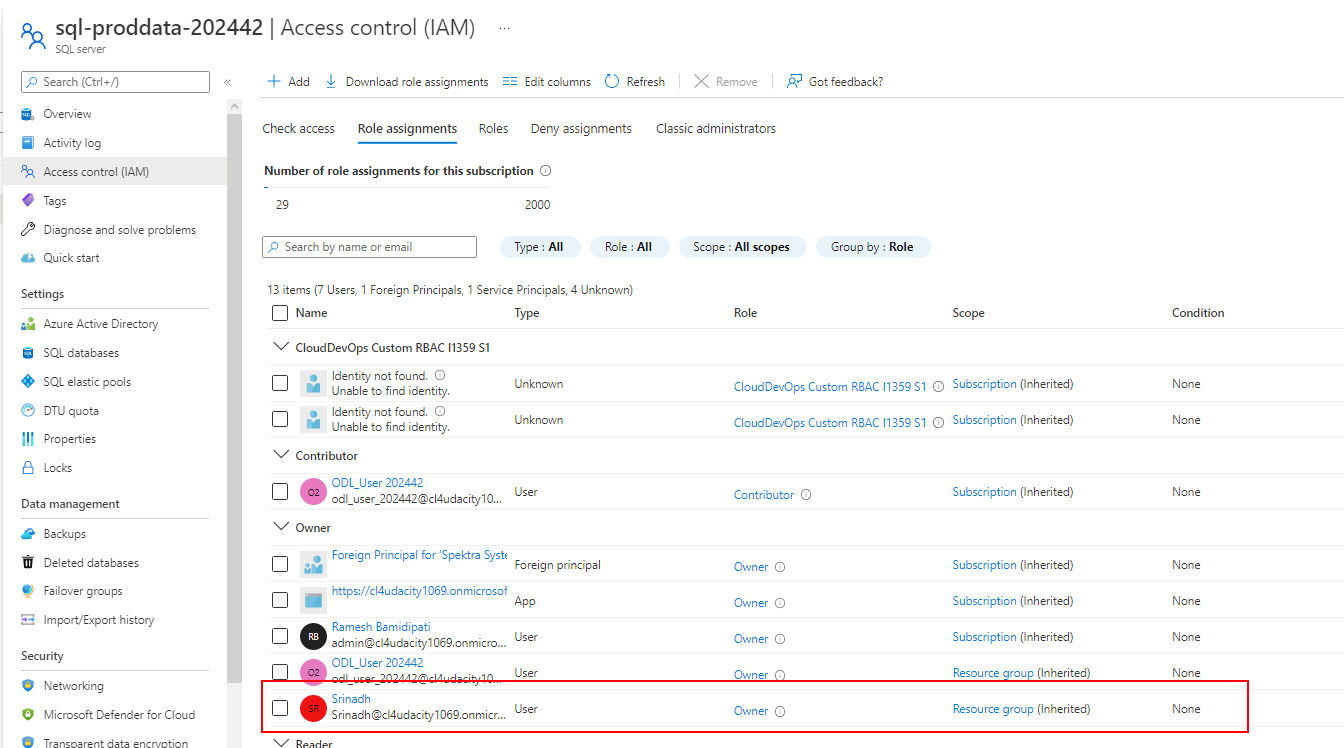


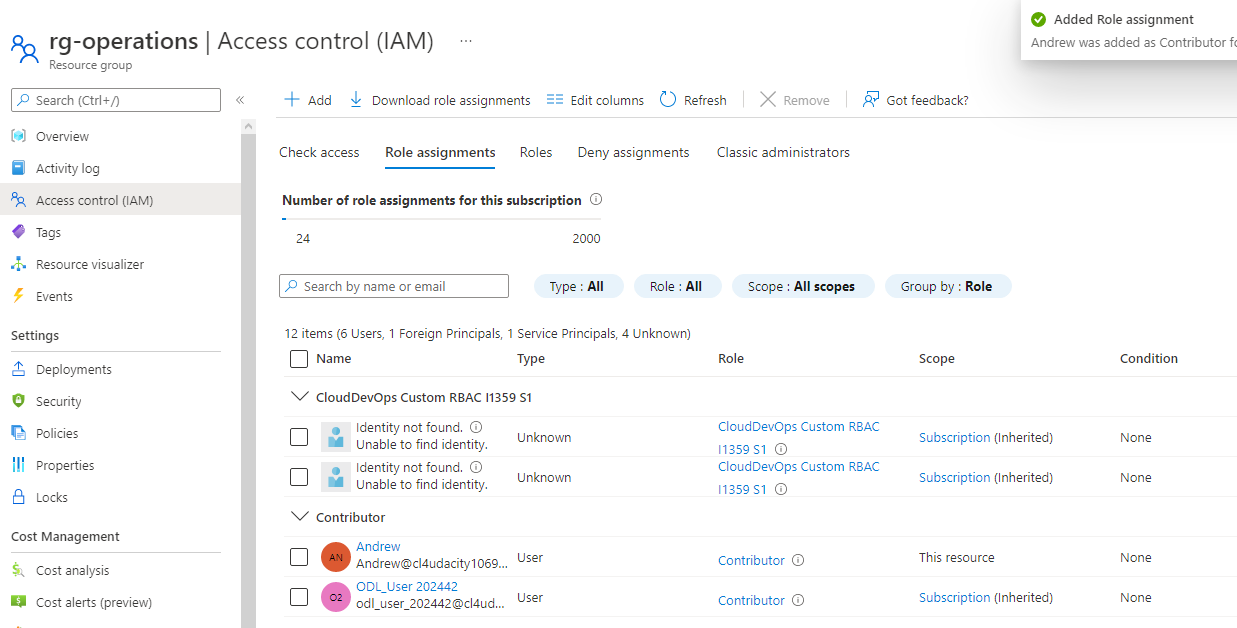


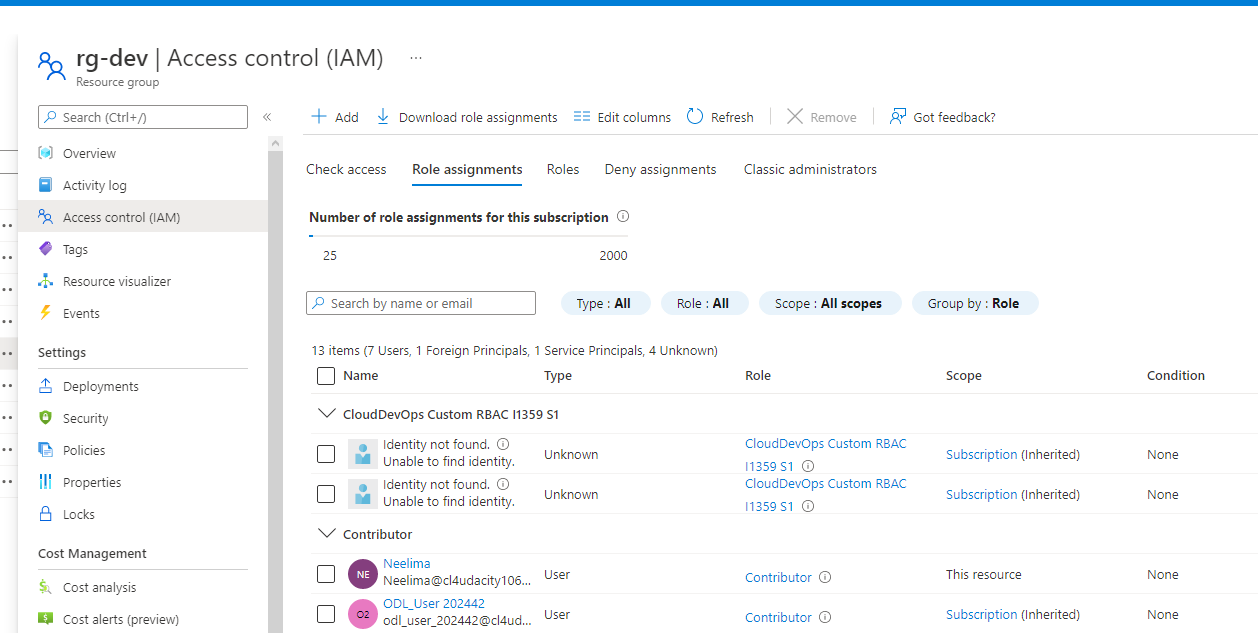
V2:

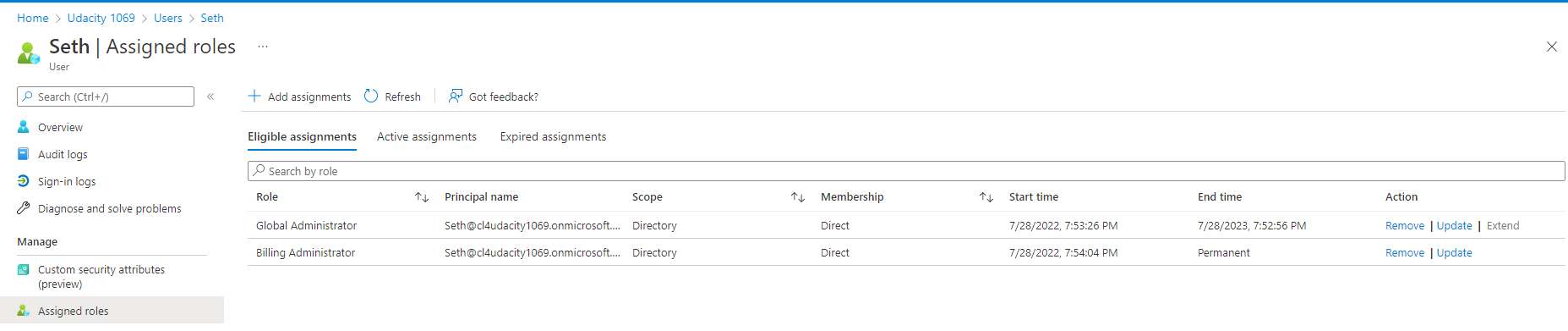
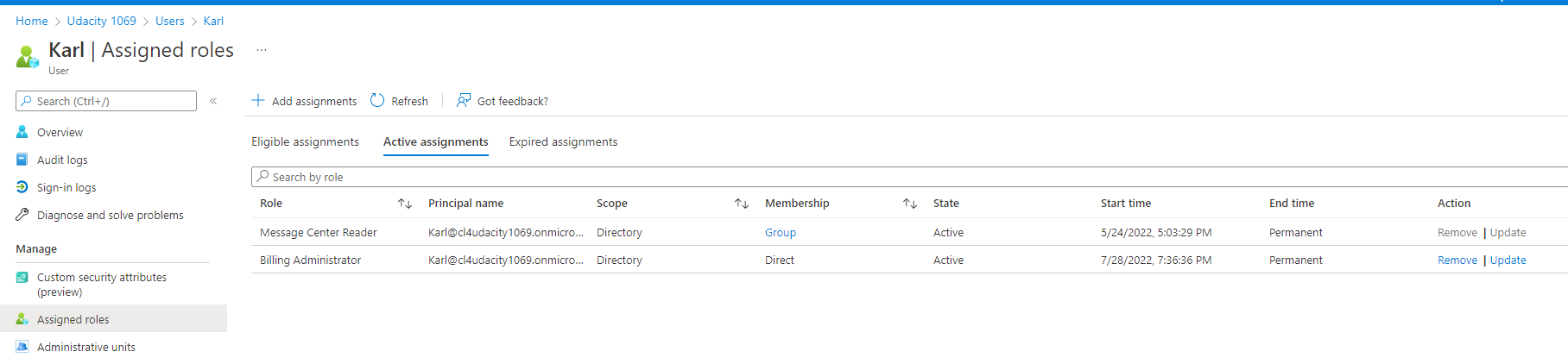
Owner Access to Dev and Prod SQL Servers:



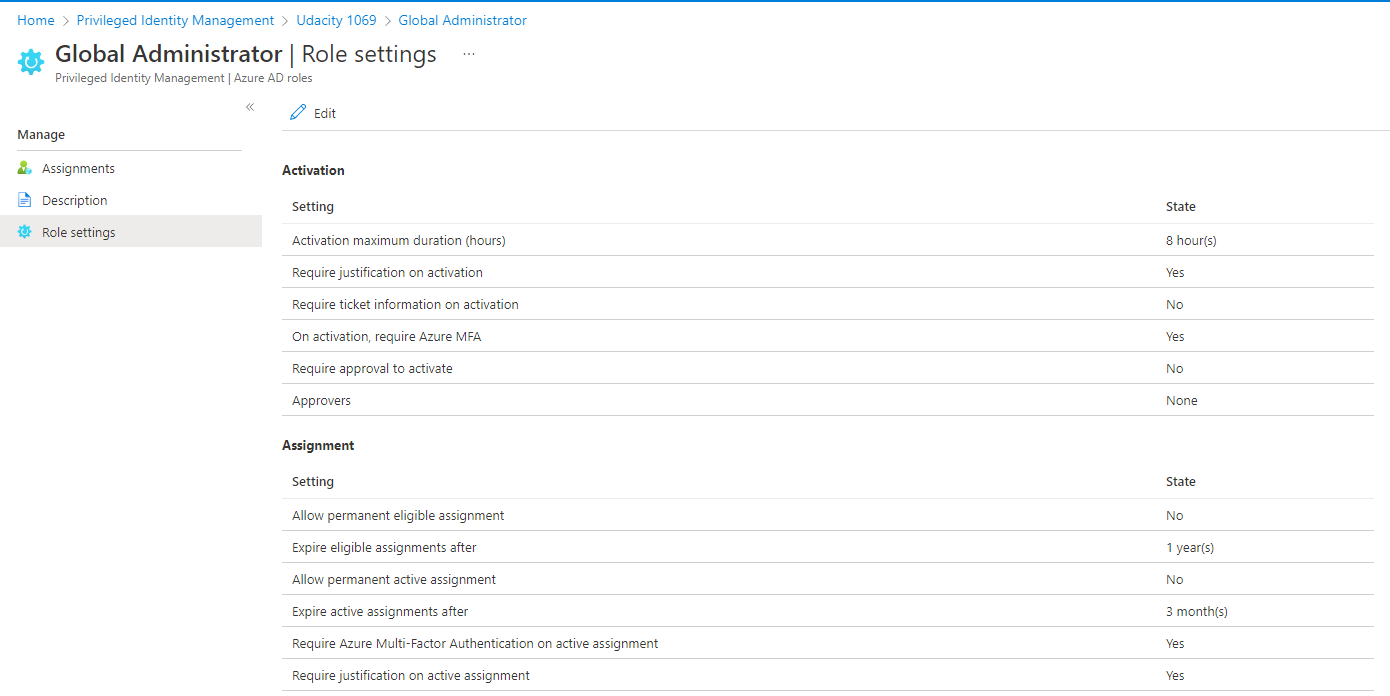




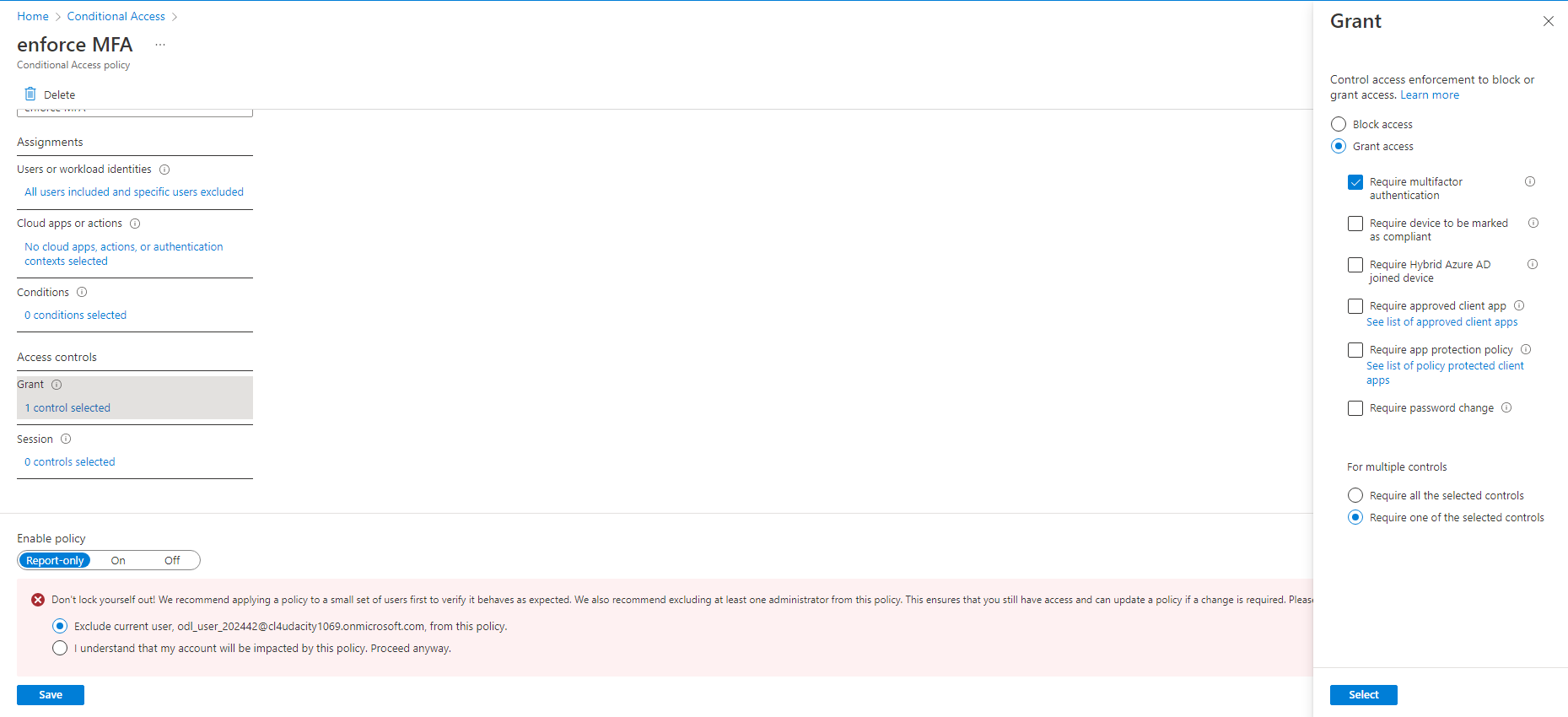




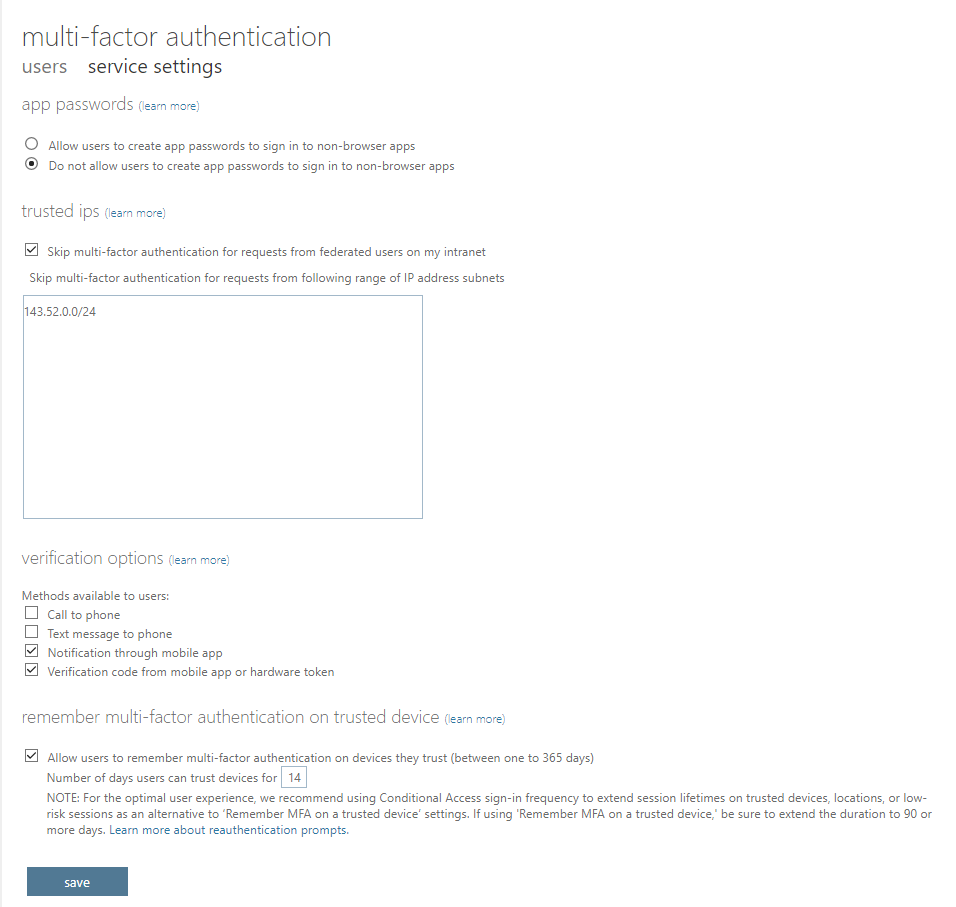
1. Proof of Global Administrator setting with duration, eligibility, expiration



1. Proof of Conditional Access policy all users

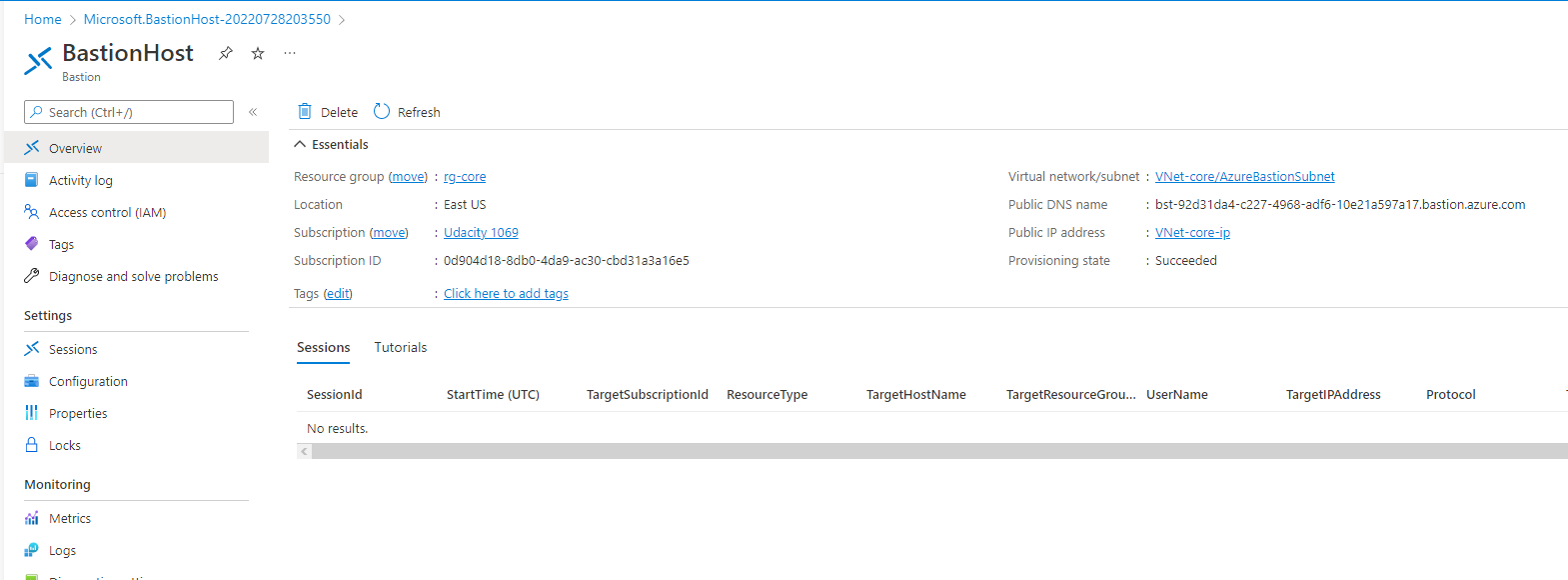


1. Proof of Multi-factor authentication(14 days, Charlotte office info)

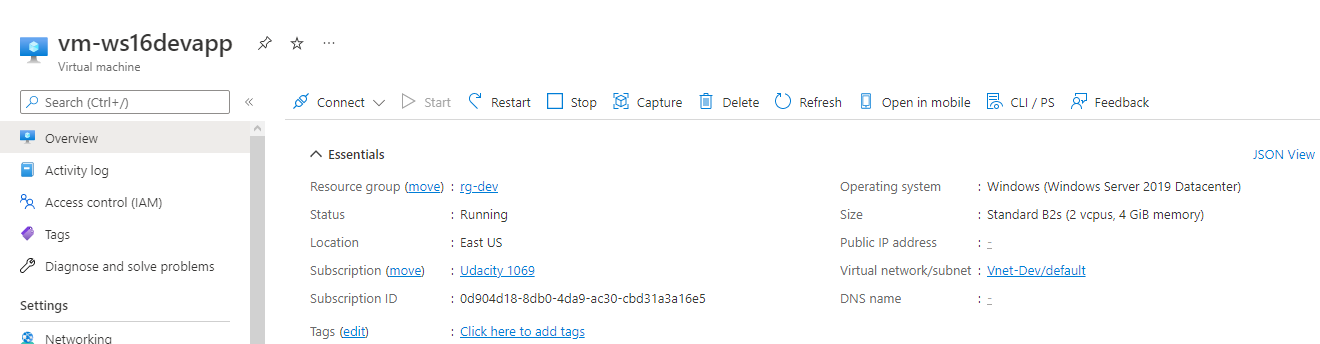
****

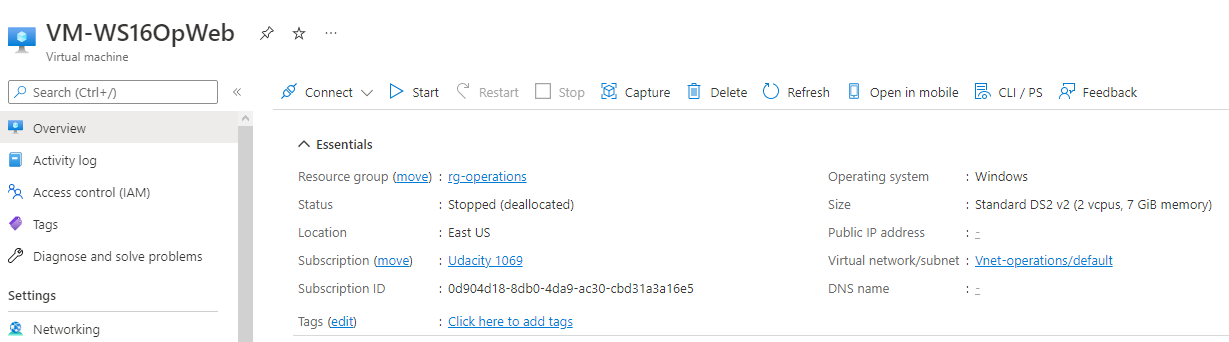
**Network Security**

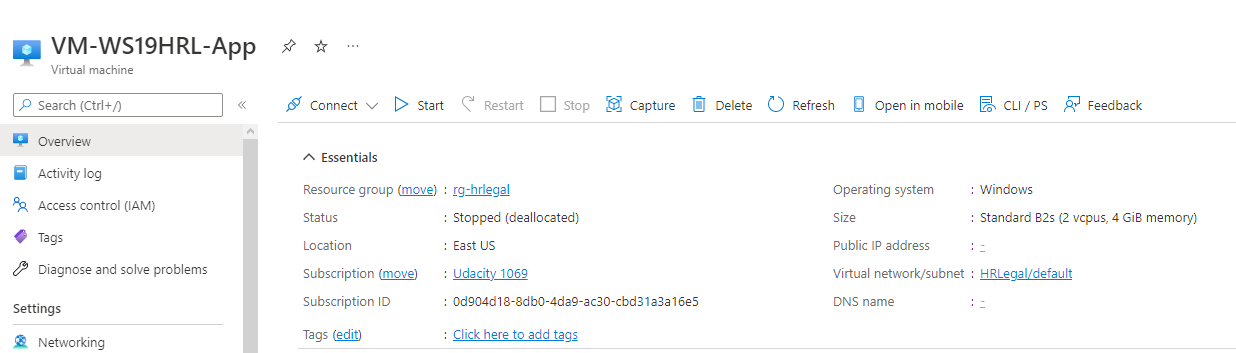
1. Bastion overview

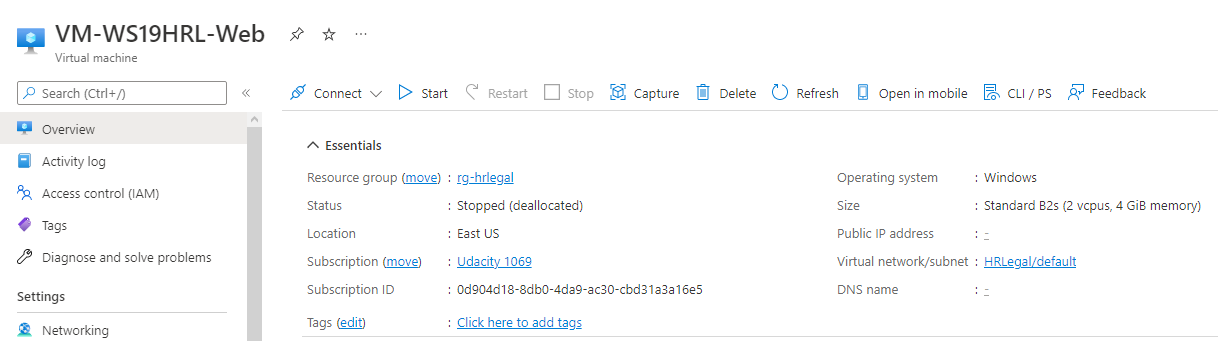


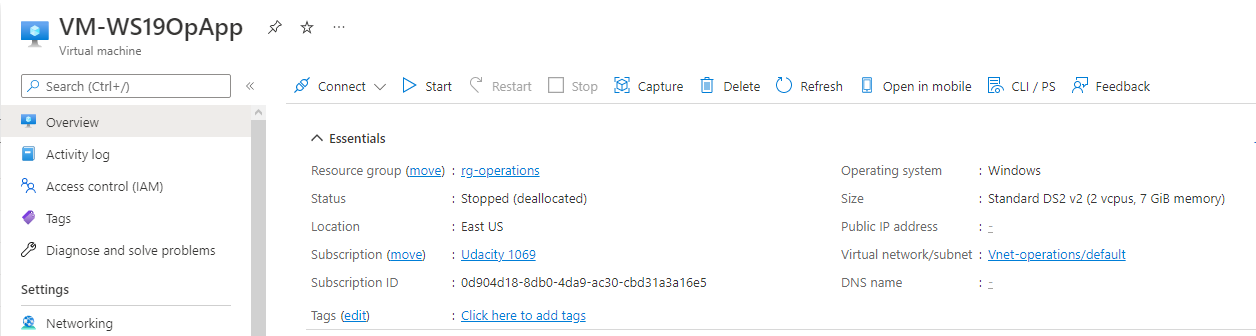
1. Proof of public IP addresses removed





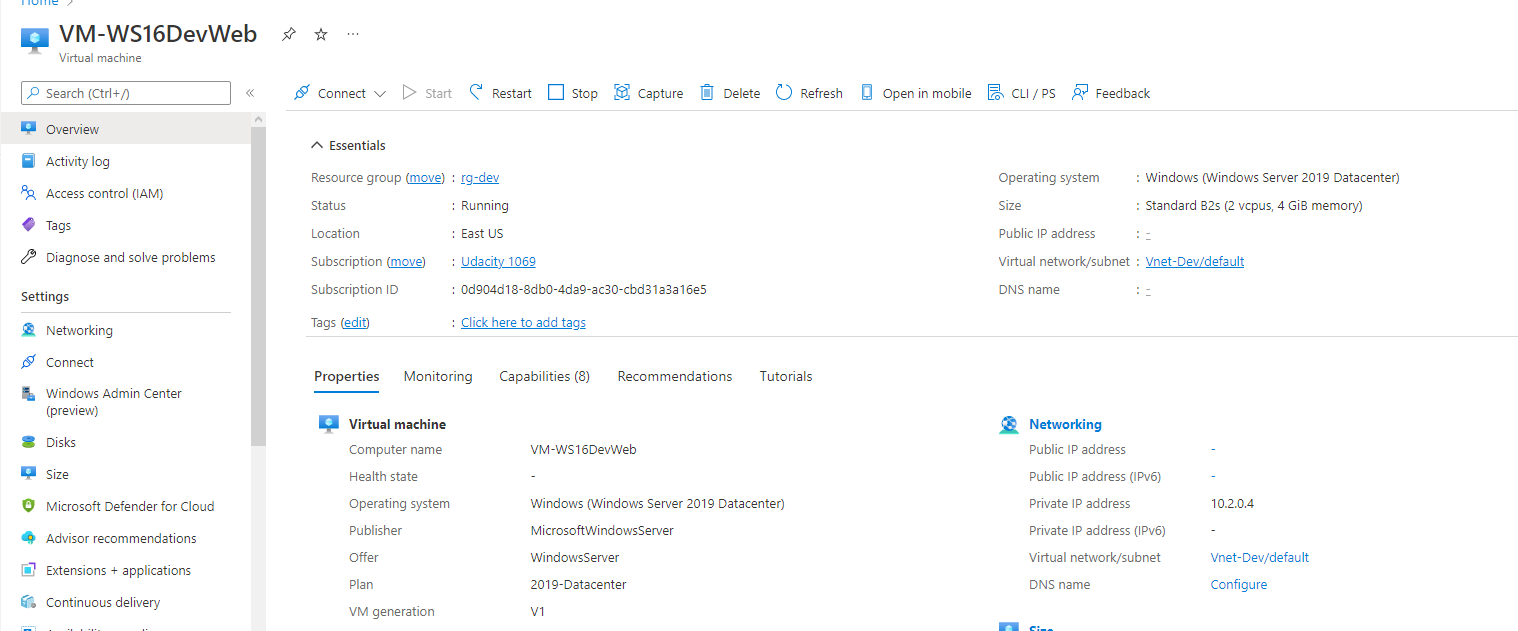






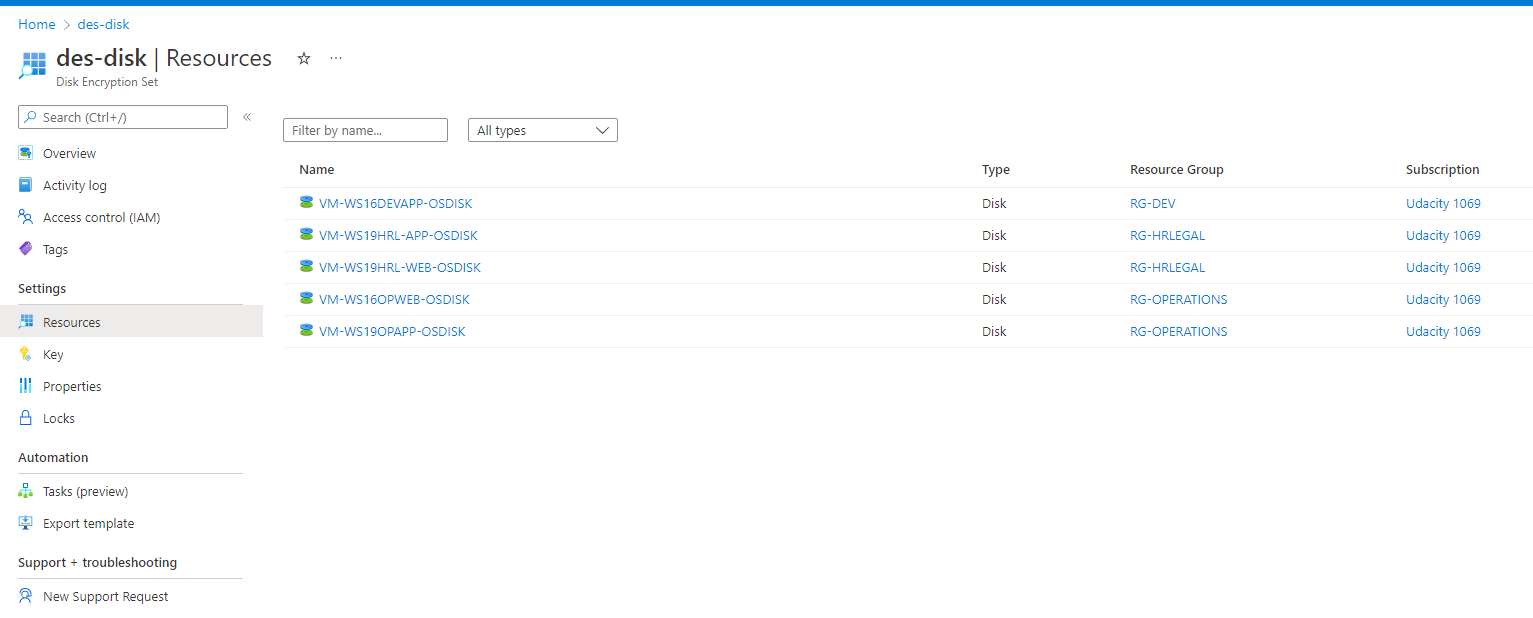
V2:

Removed public ip address from VM-WS16DevWeb



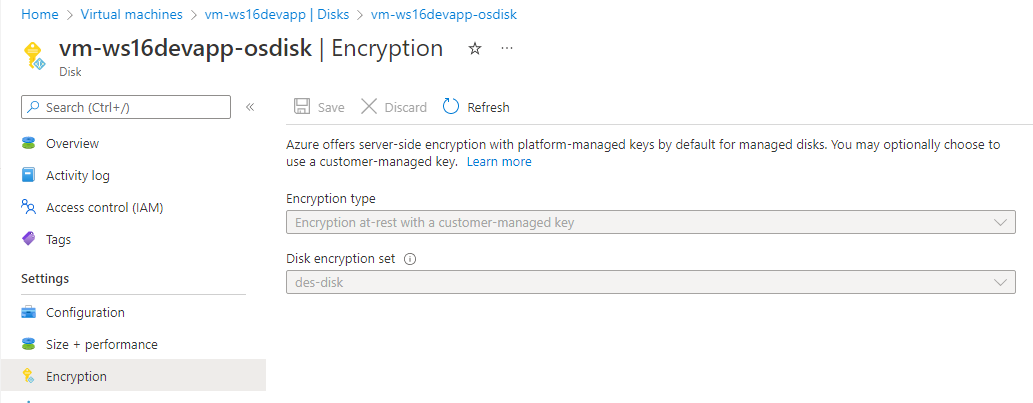
**Data and Encryption**

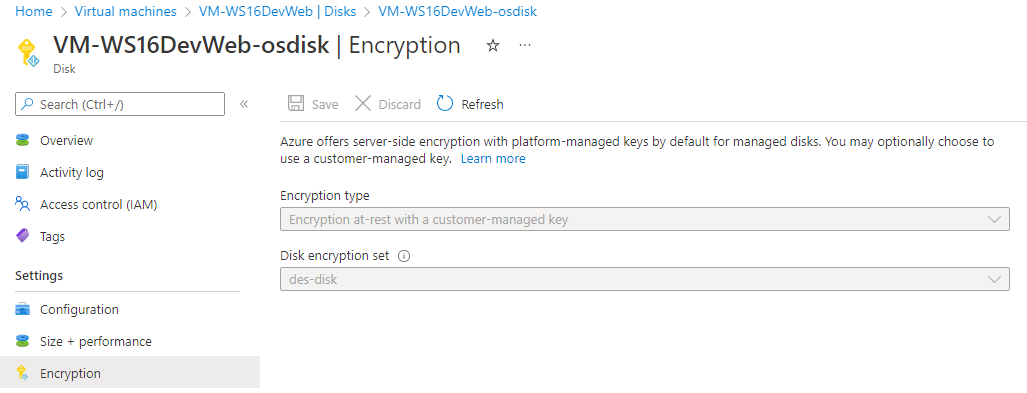
1. Proof of Encryption types for VM ( devapp,DevWeb,OpWeb,HRL-App,OPApp, HRL-Web)

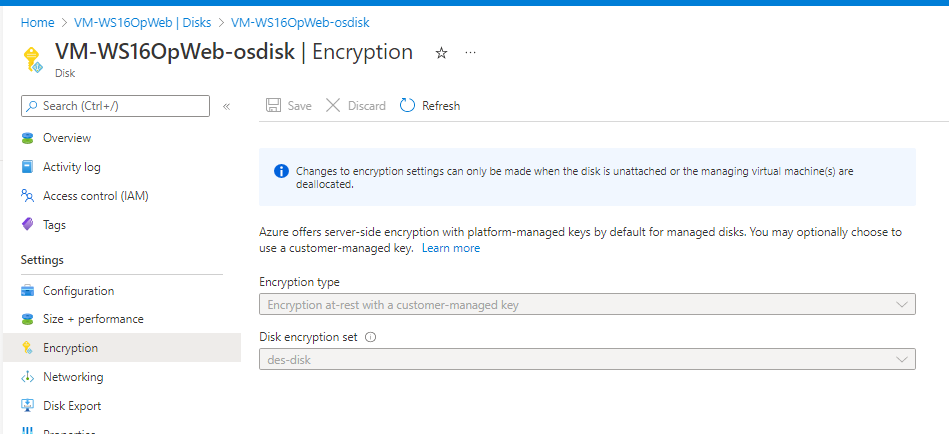


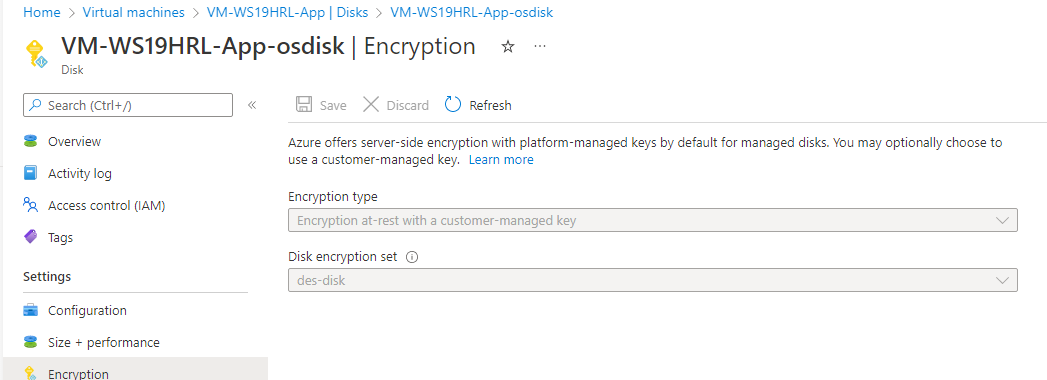
V3:

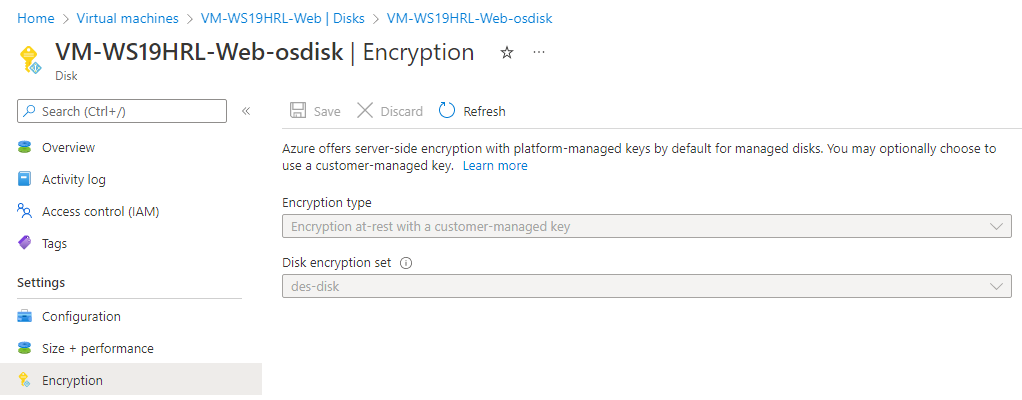
Proof that OS disks are encrypted:

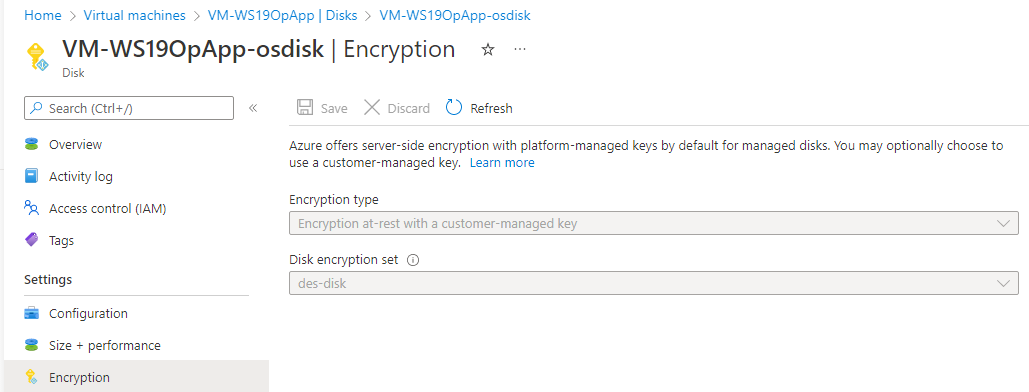




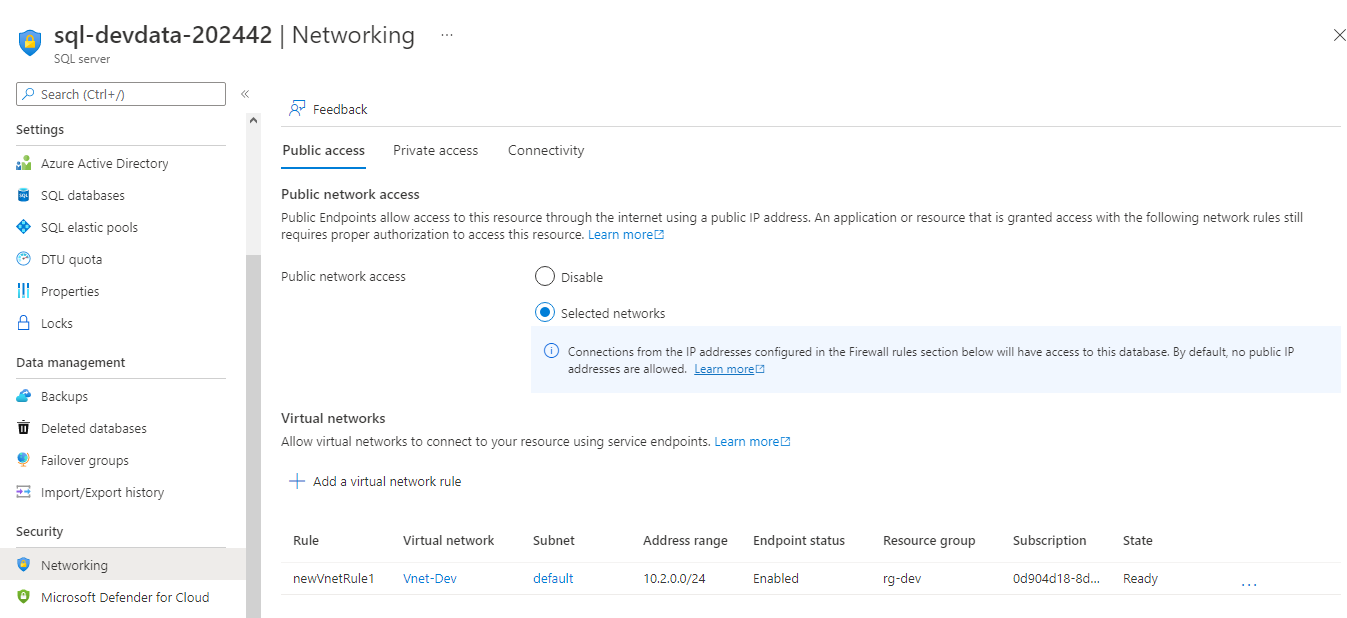


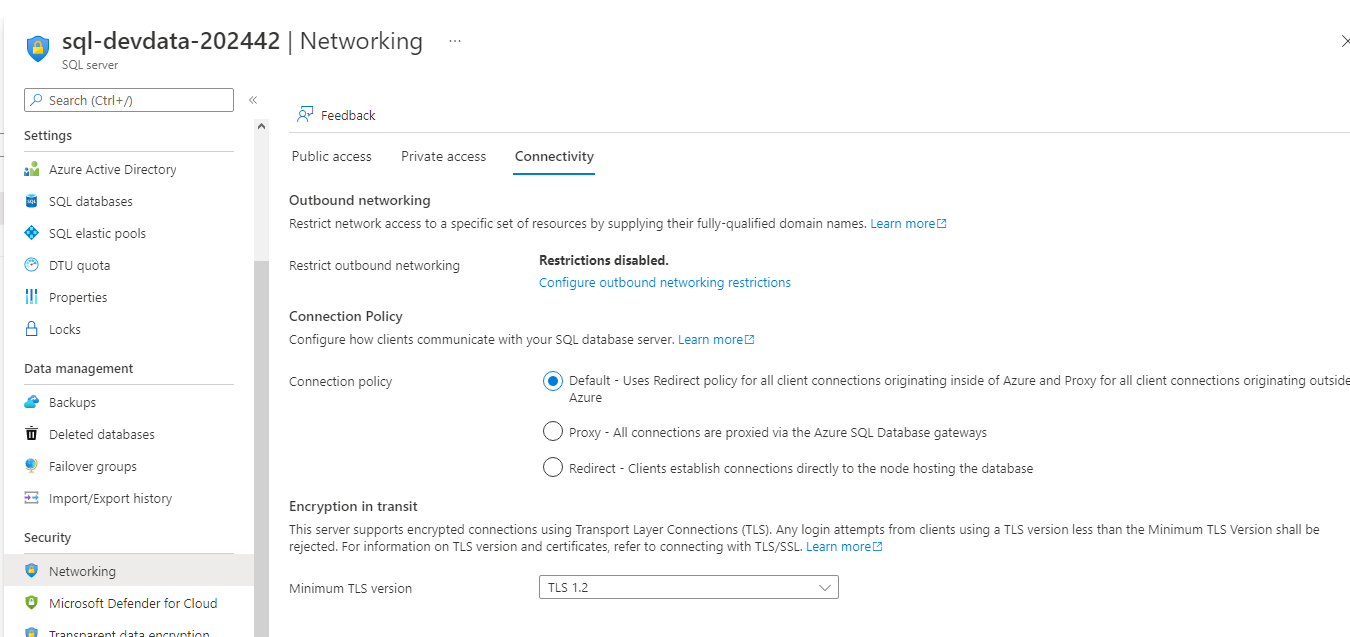


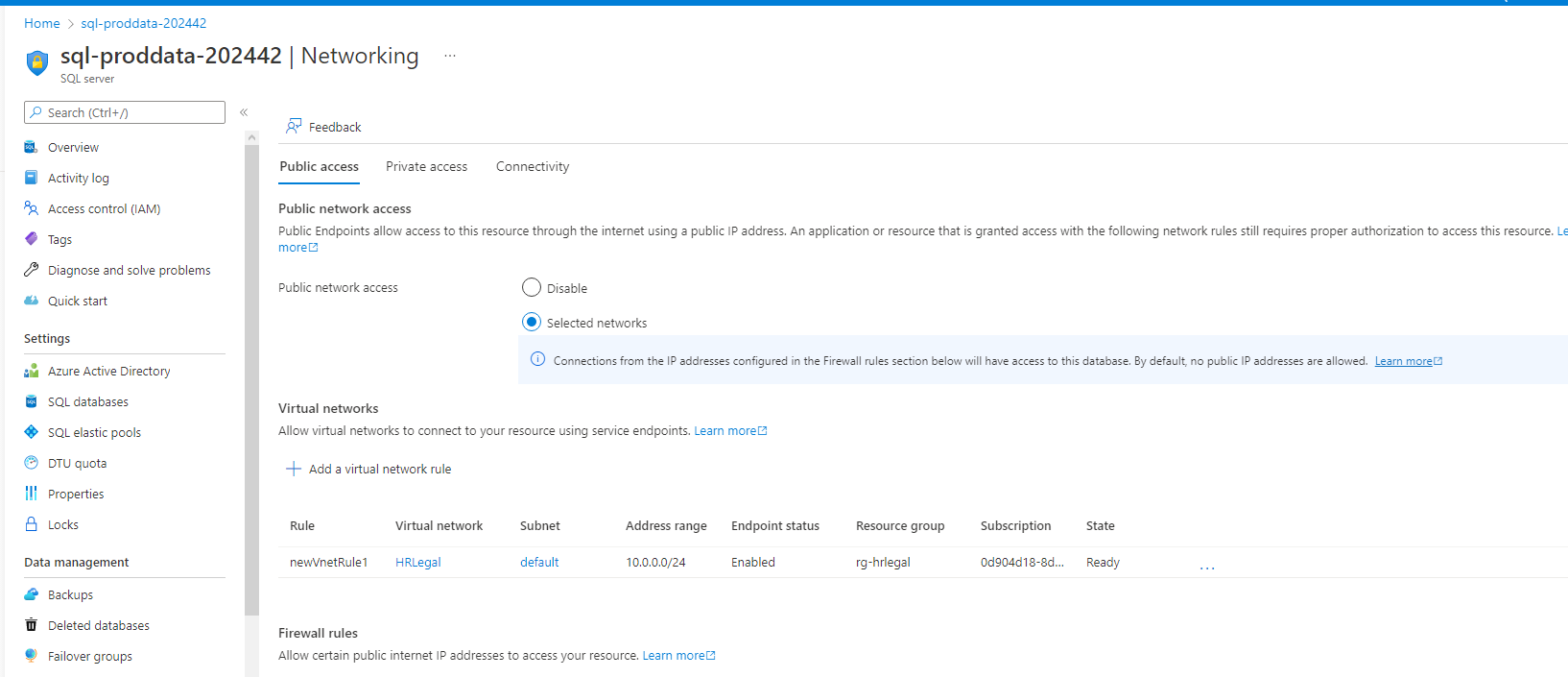


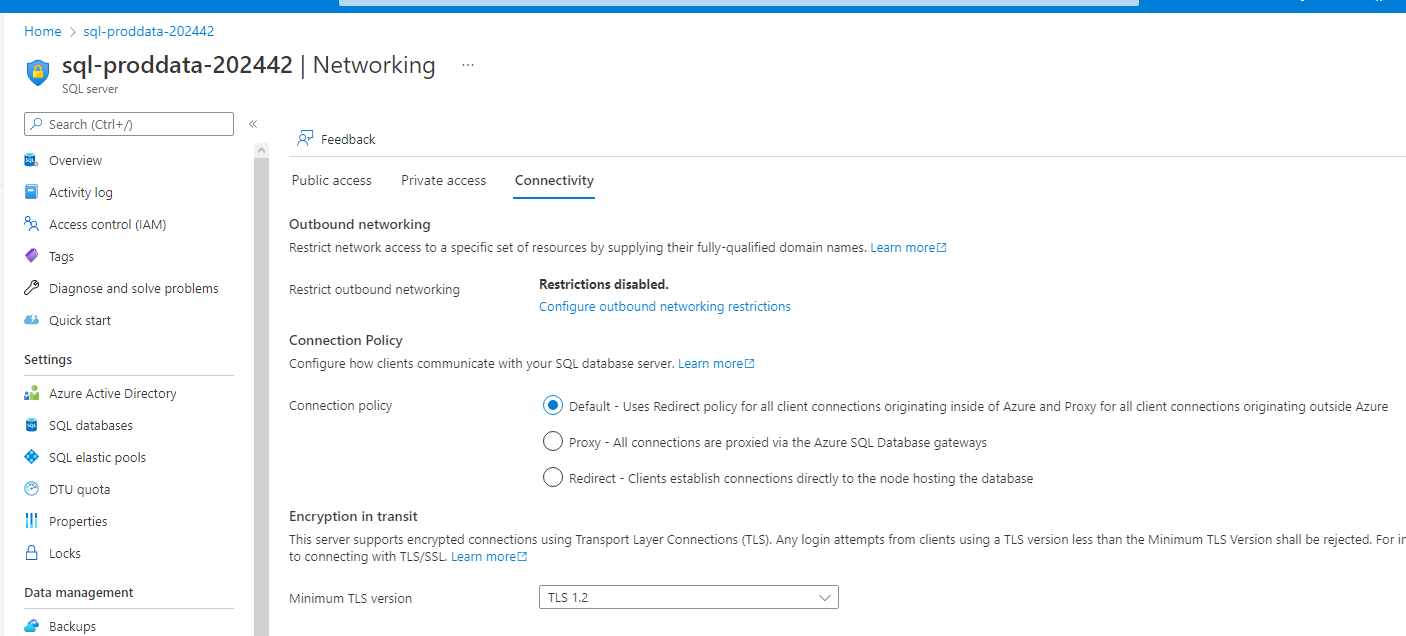


1. Firewalls and virtual networks page
   1. Proof of no public access and TLS for SQL servers(prod, dev)

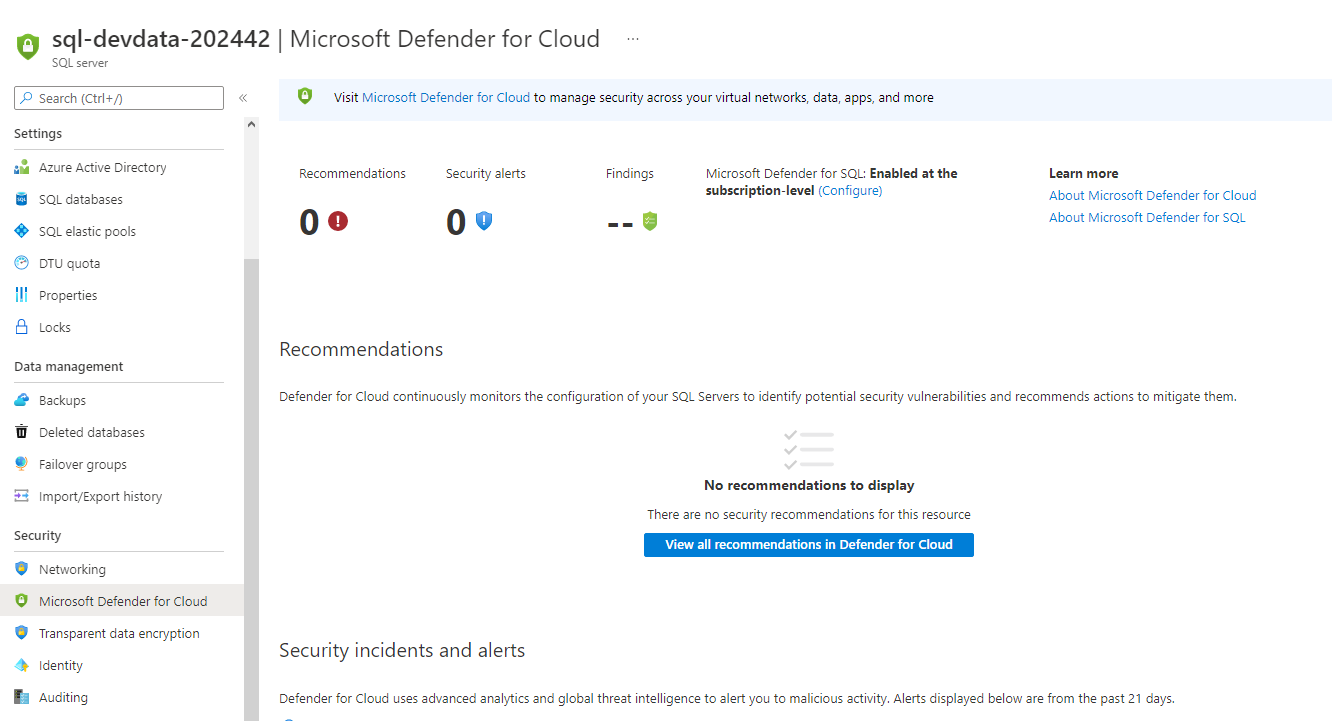


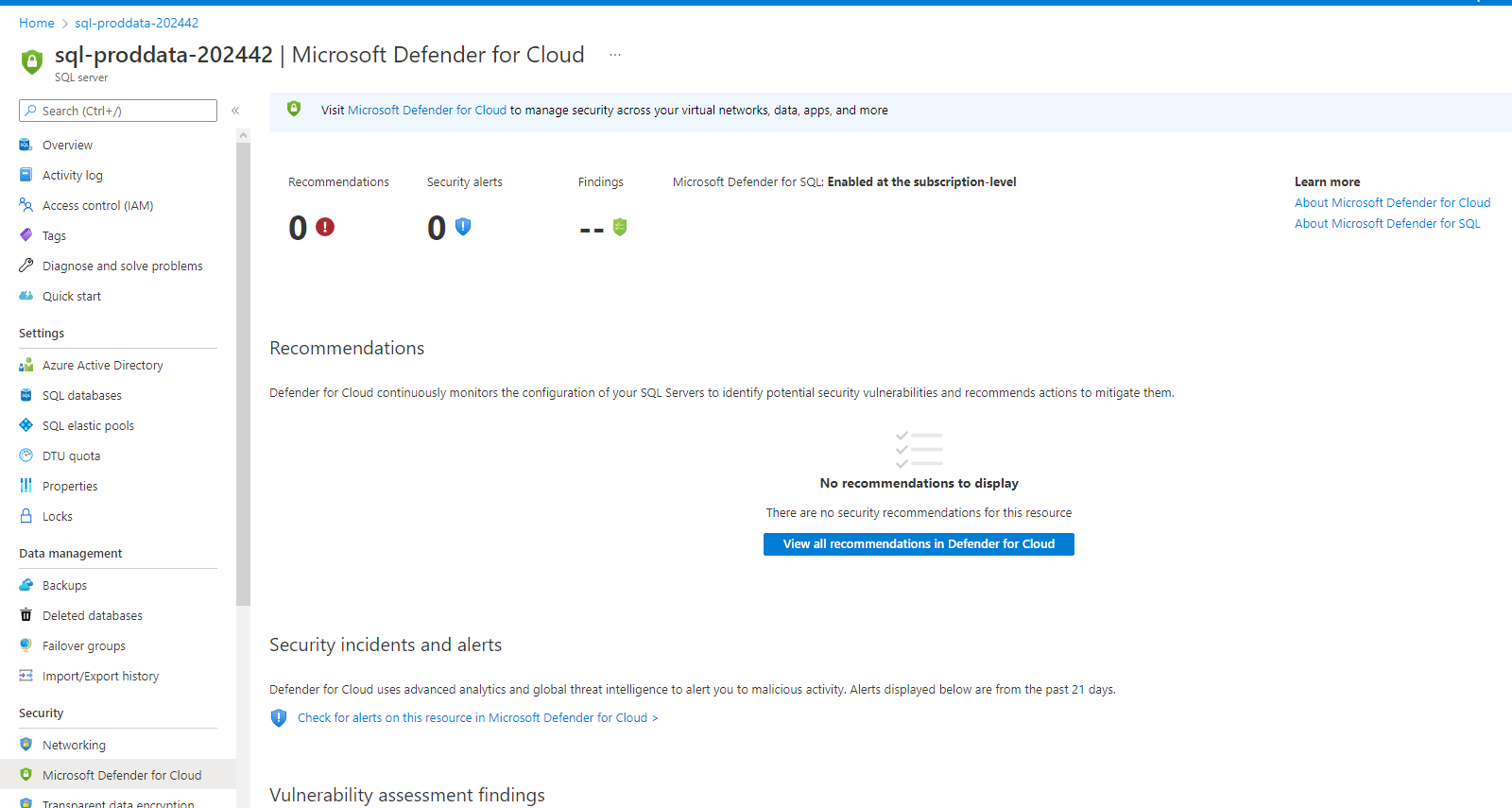




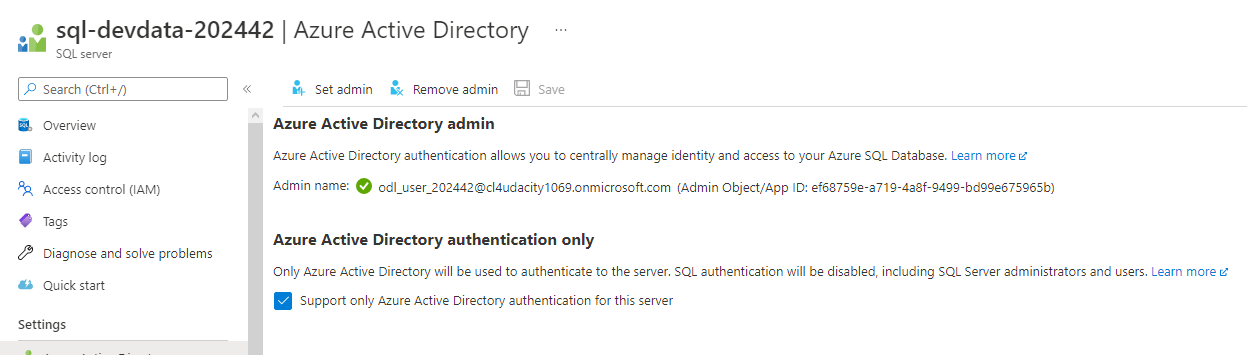


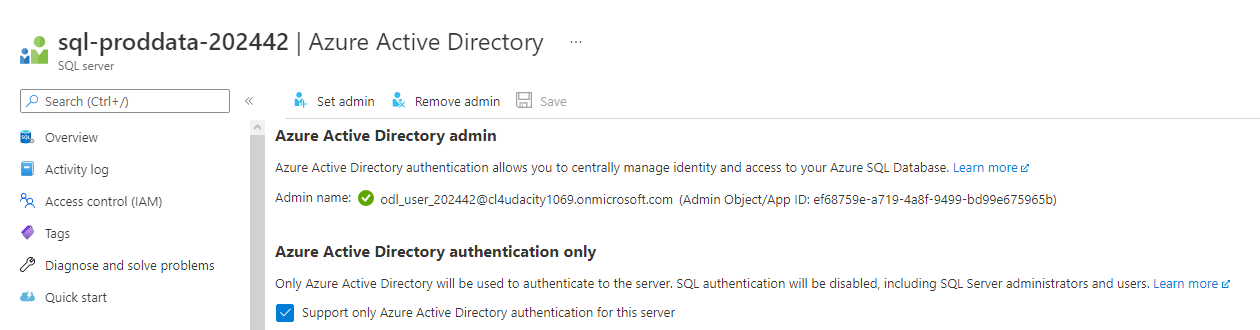
1. Proof of Azure Defender SQL server enabled(prod, dev)





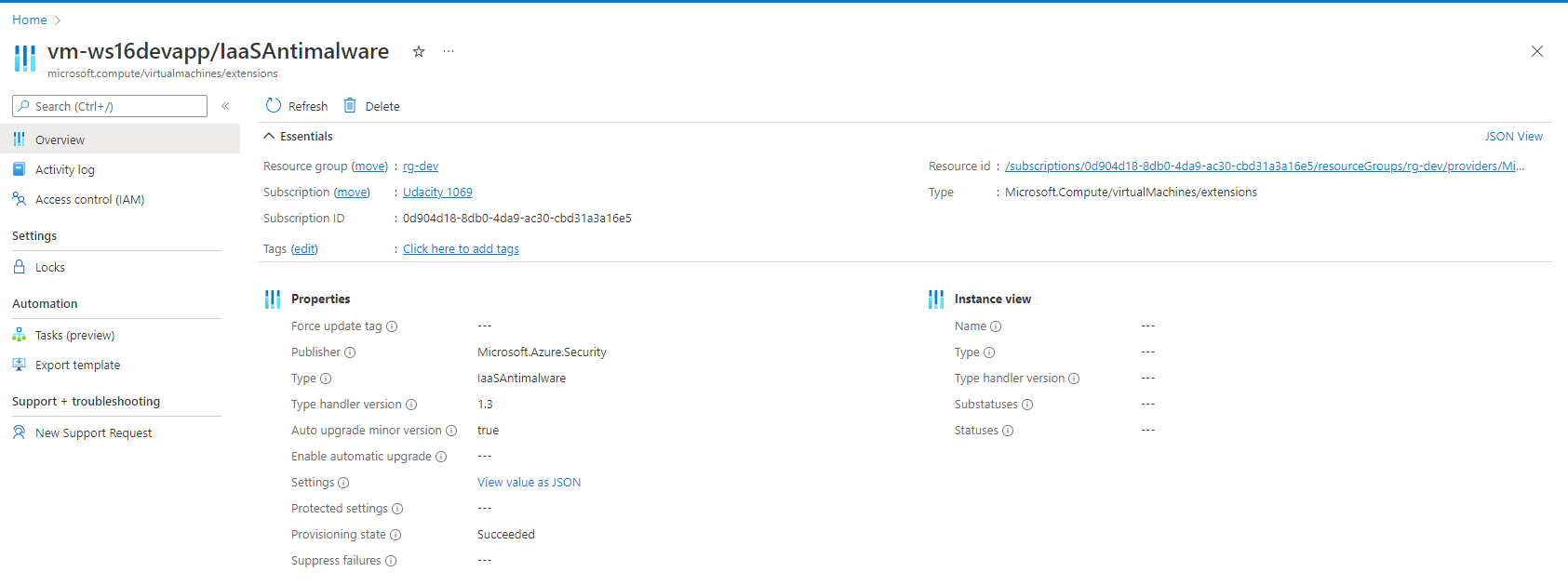
1. Proof of Azure AD authentication for SQL enabled(prod, dev)

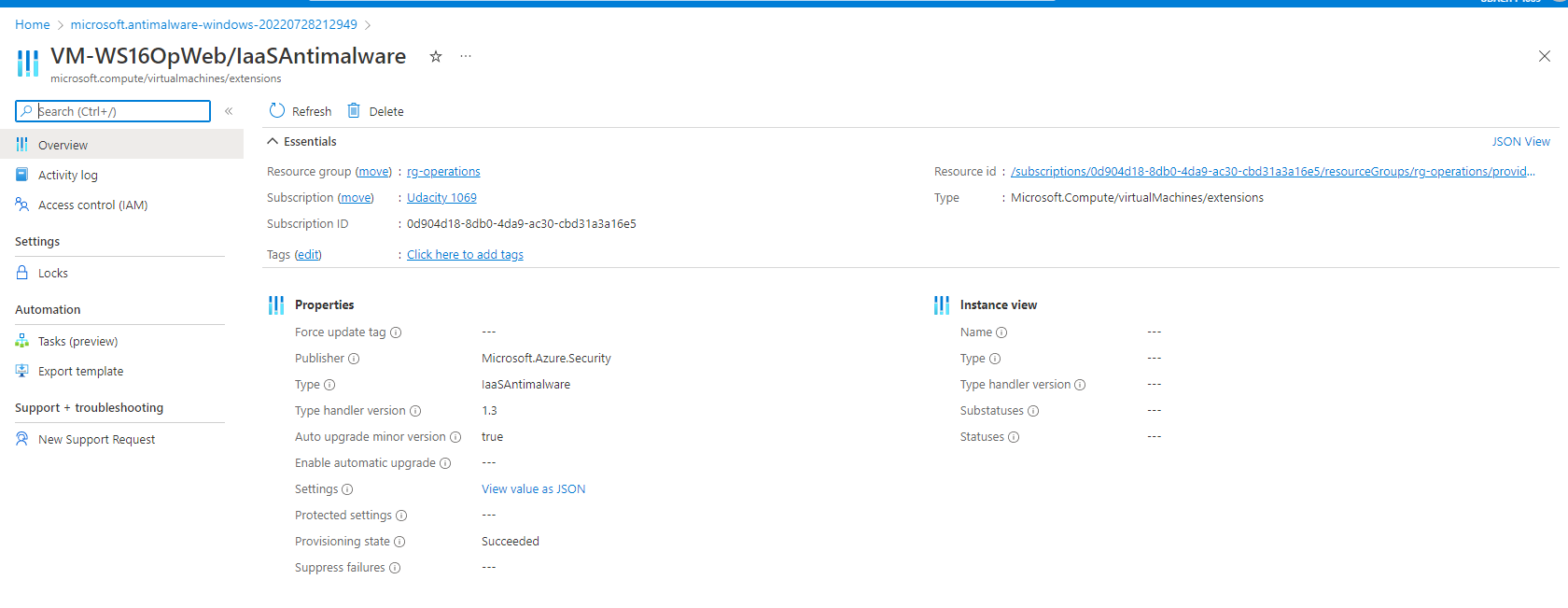


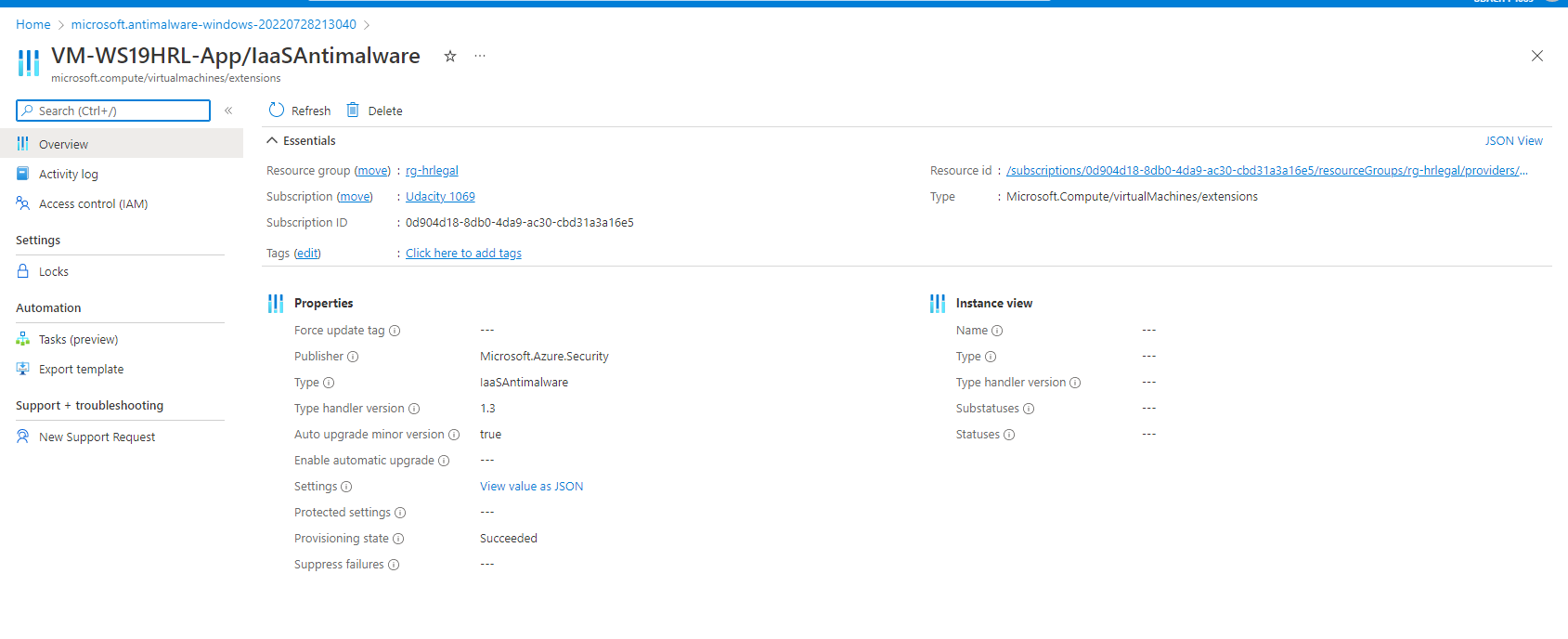


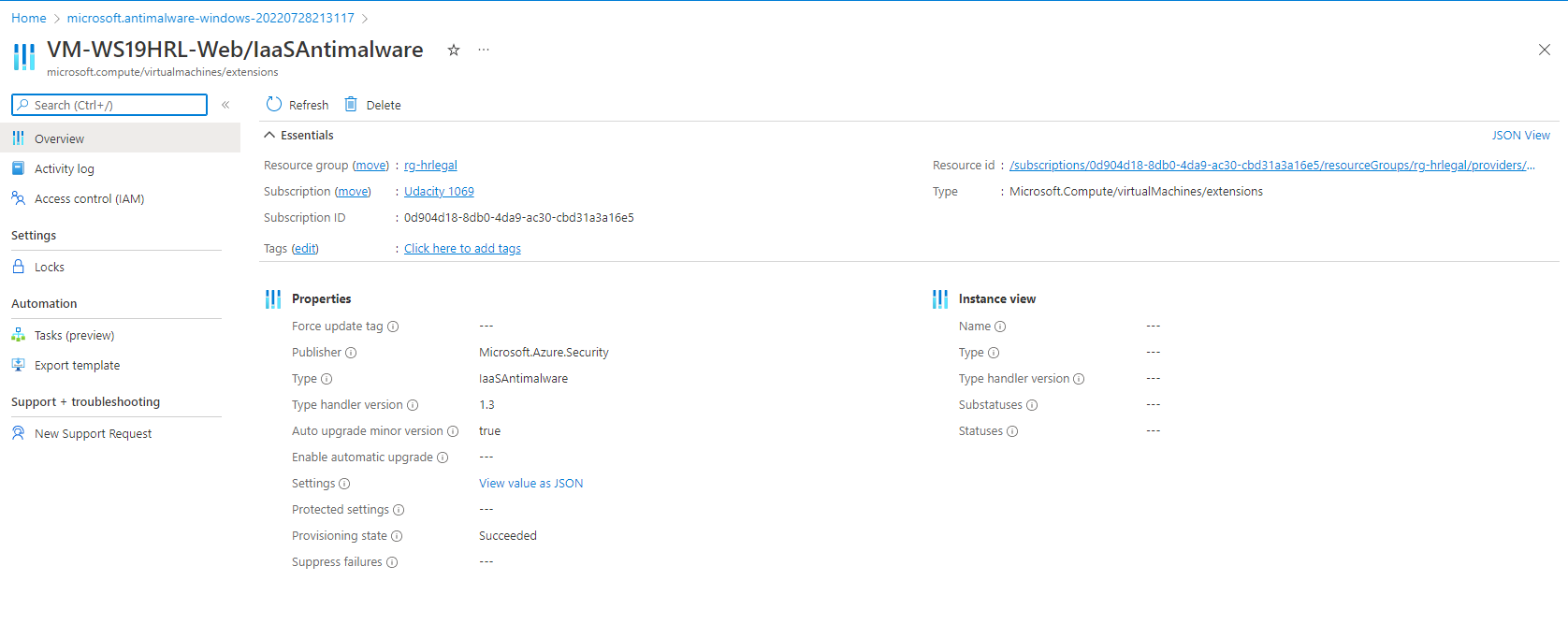
**Cloud Protection**

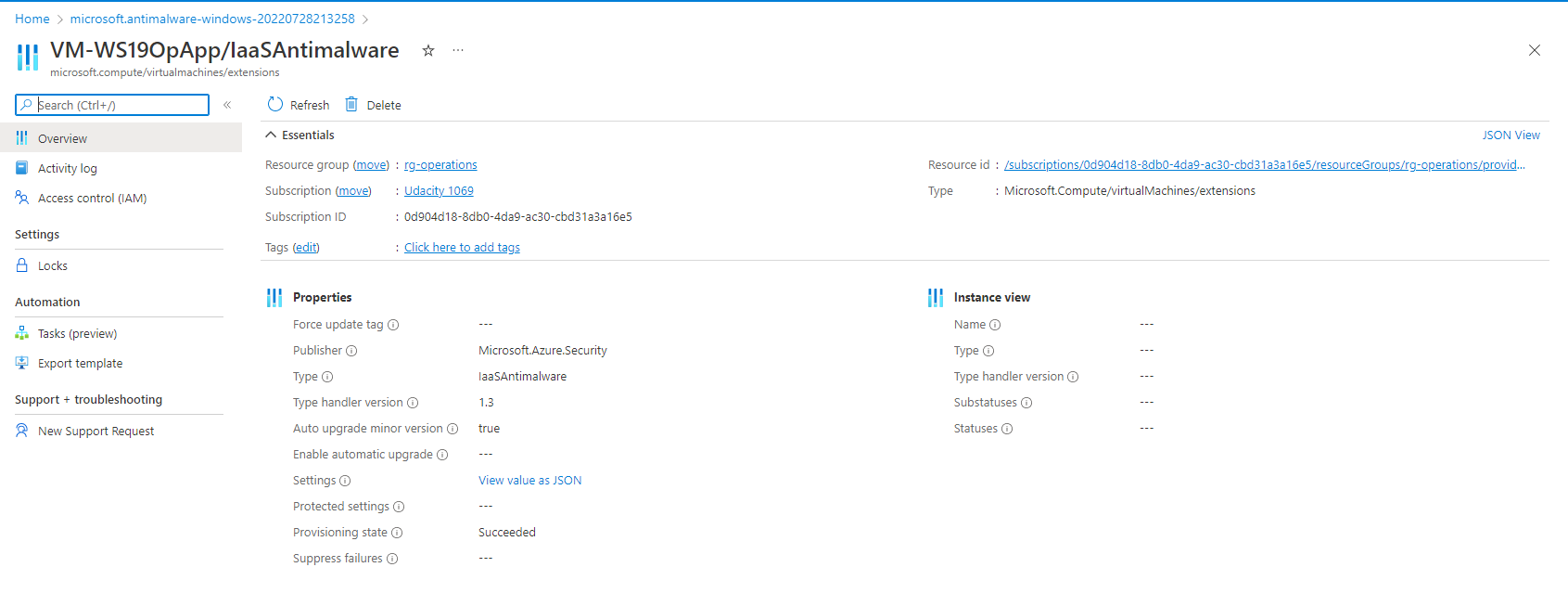
1. Proof of IaaSAntimalware enabled ( devapp,DevWeb,OpApp,HRL-Web, HRL-App,OpWeb)





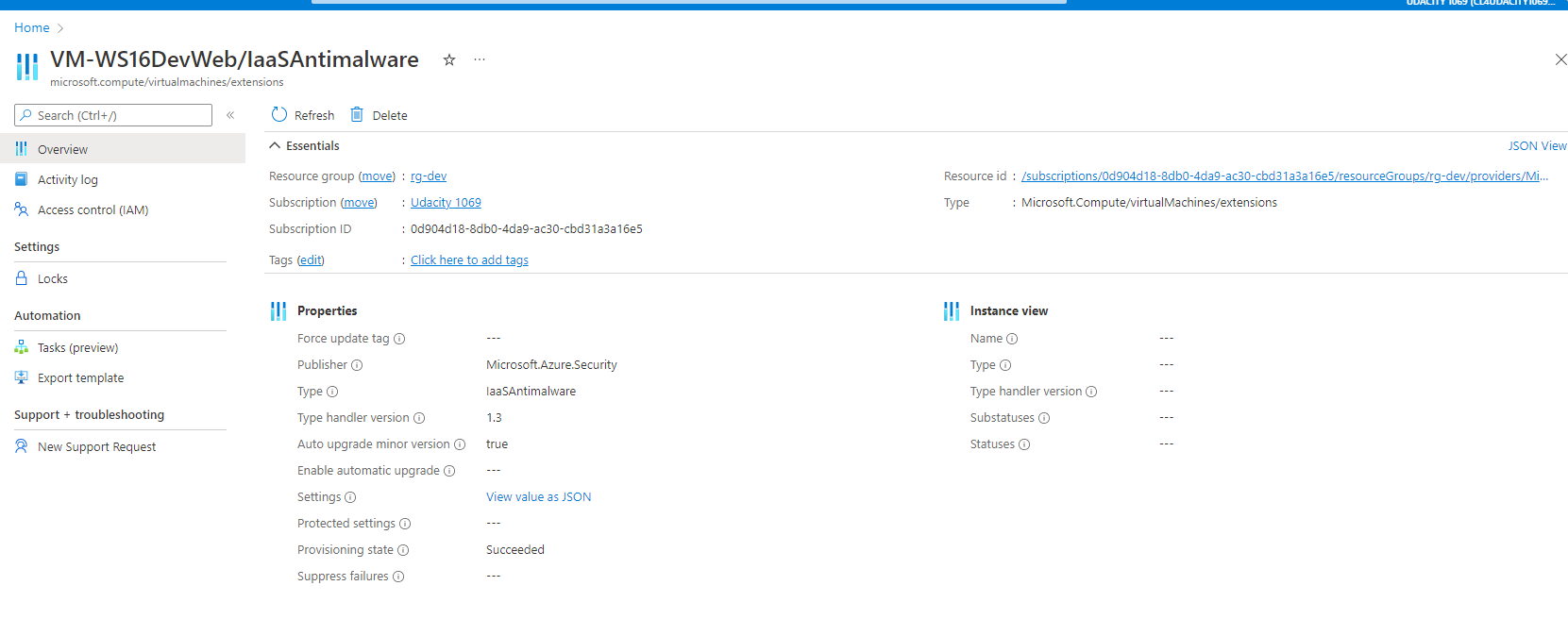




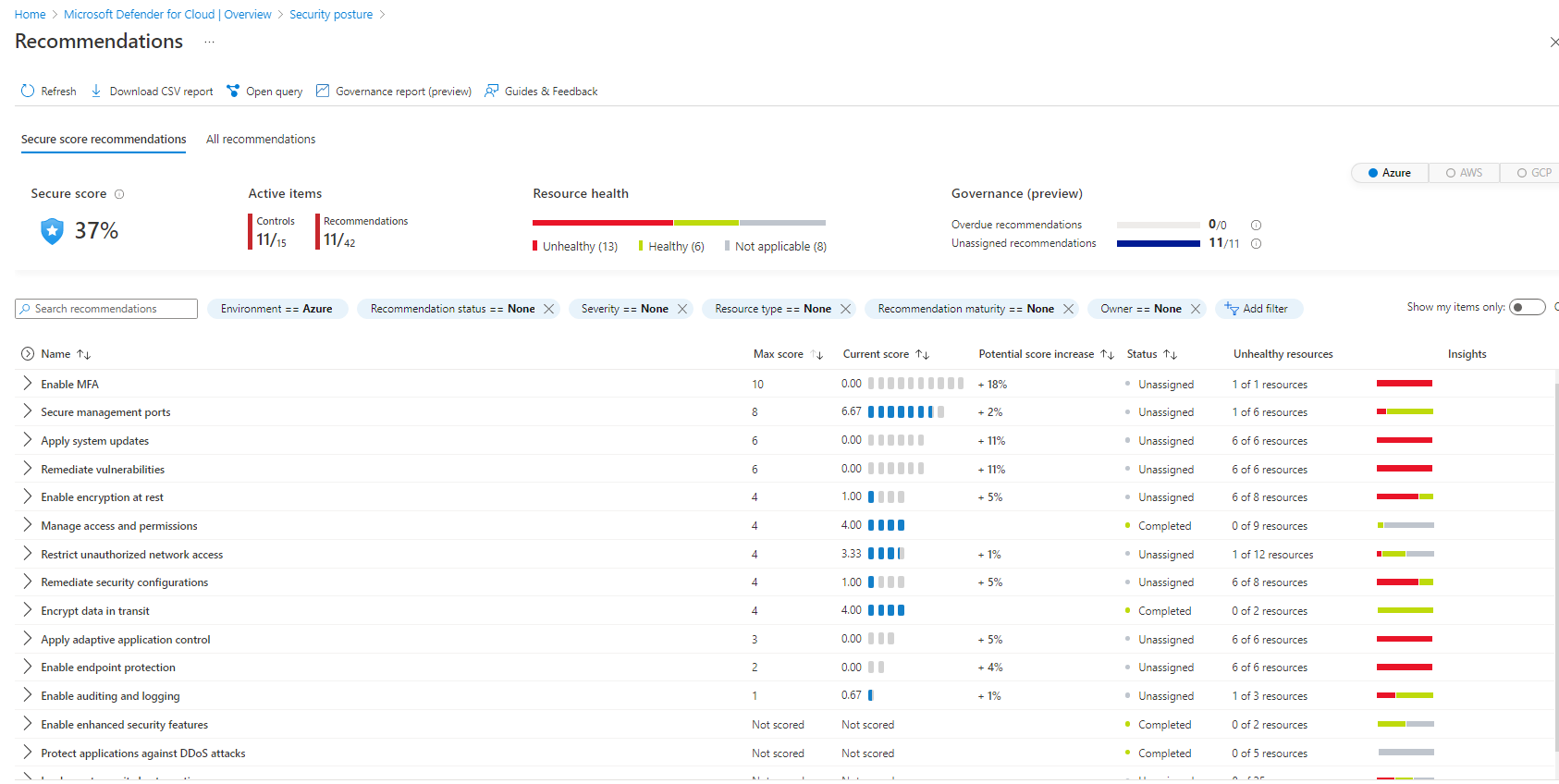
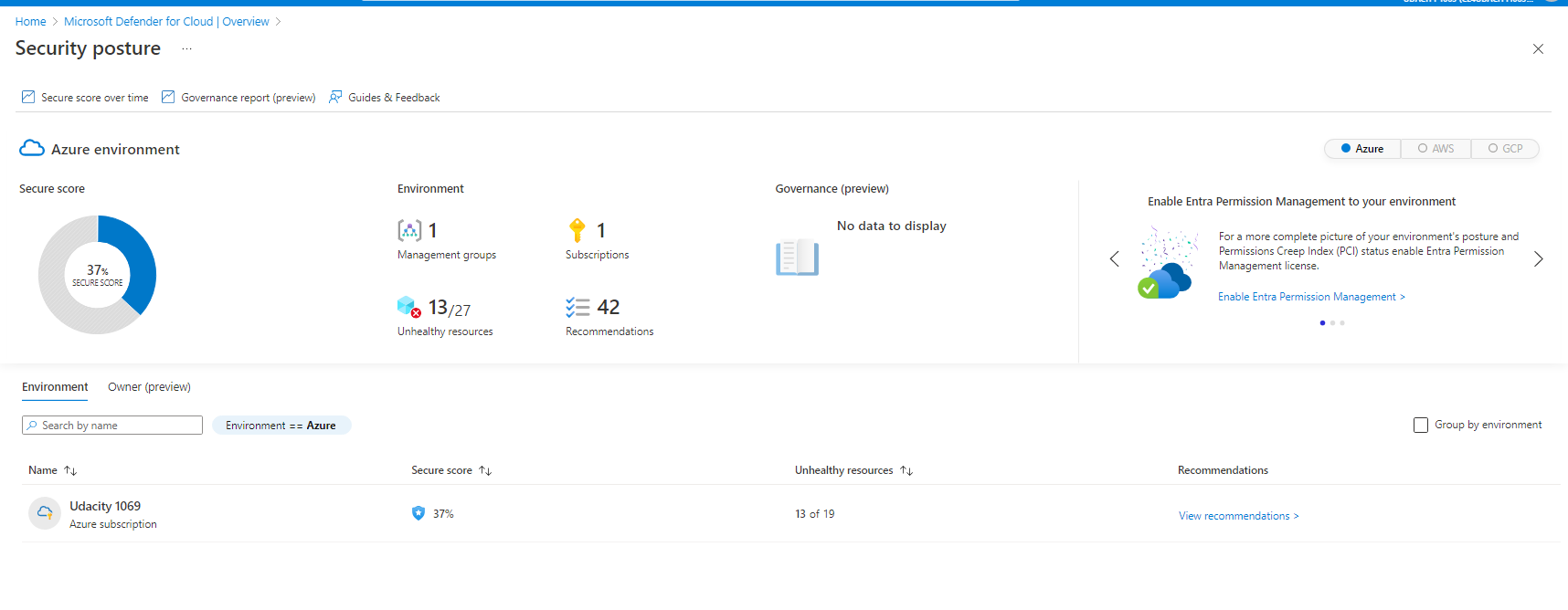


V2:

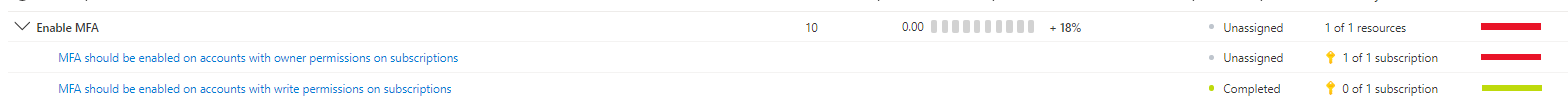
Antimalware on VM-WS16DevWeb:

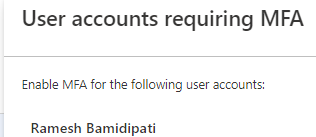


1. Recommendations

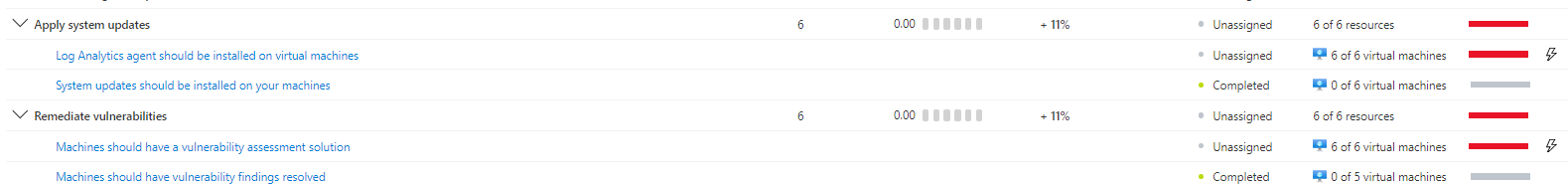


“Enable MFA” currently has a score of 0/10. So it has the biggest impact on security if we fix it.

MFA is not set up for user account Ramesh Bamidipati.



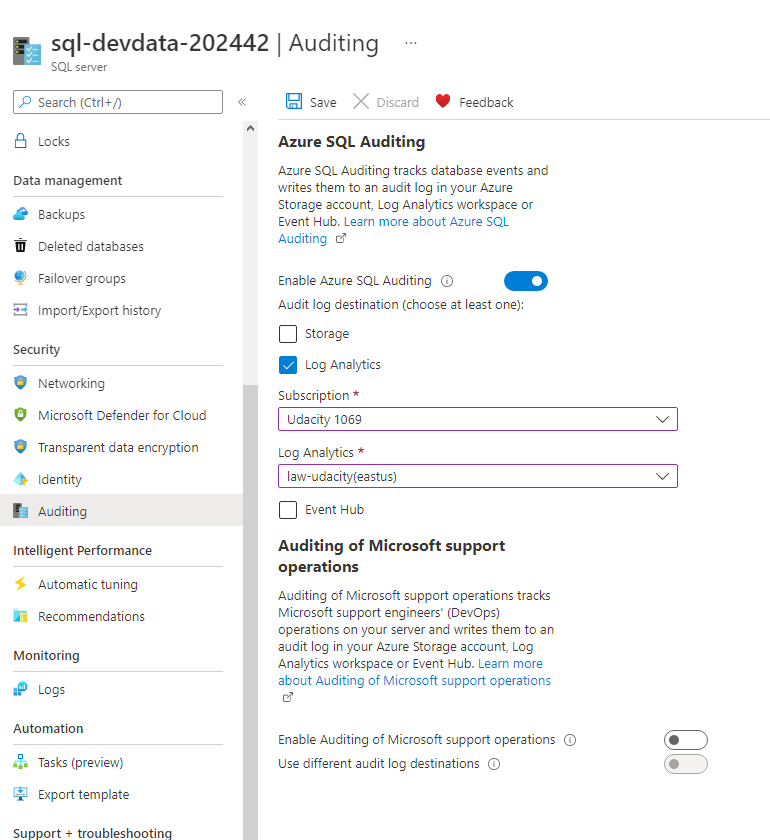
The other 2 top remidations are “Apply system updates” and “Remidate vulnerabilities”. Both of them have a score of 0/6.

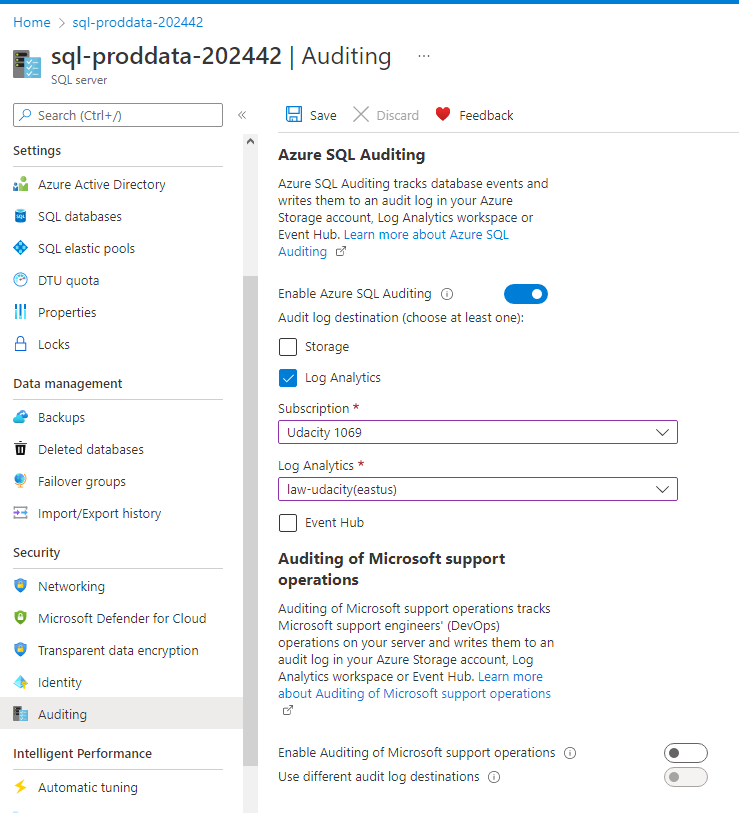
We should install the log analytics agent on all of our VMs.

And we should install vulnerability assessment tools on our VMs.

**Monitoring**

1. Proof of Azure SQL auditing with Log analytics (devdata,proddata)

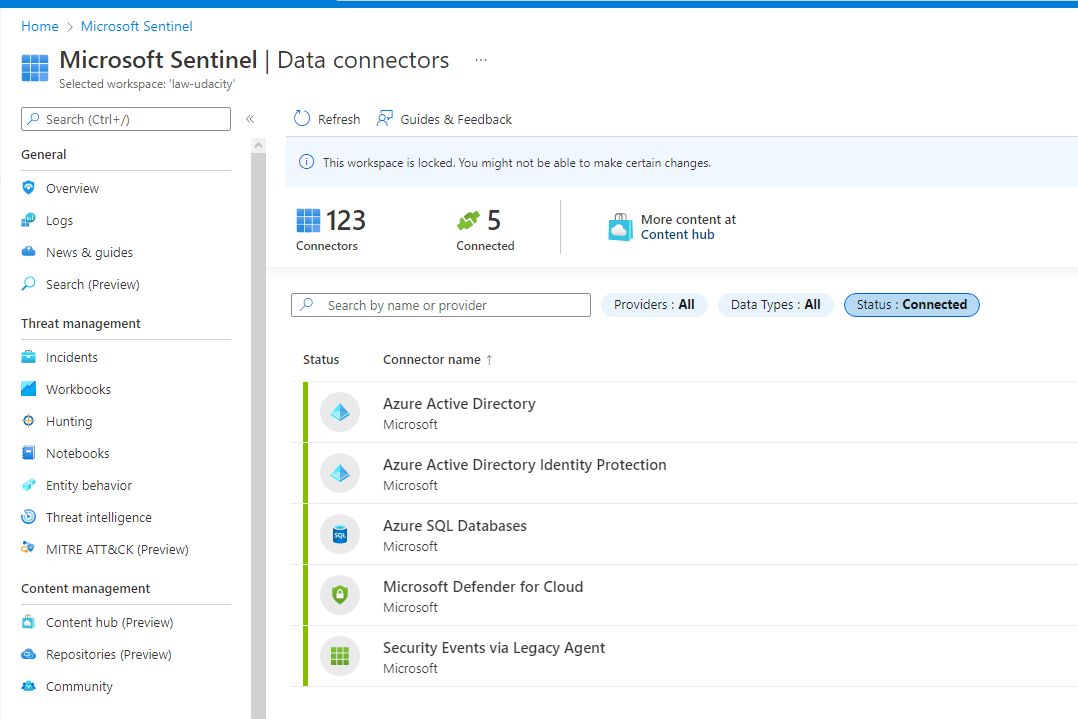




1. Proof of Sentinel connectors (2+)

V2:

Add Azure Active Directory Connector to Sentinal

**Compliance**

1. Proof of NIST SP 800-53 rev4 policy added

