***Attention students:***

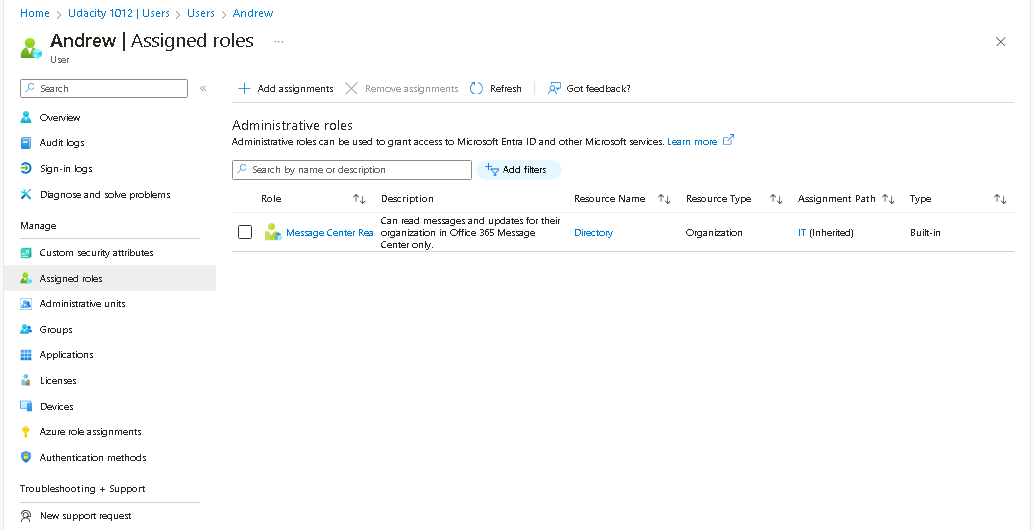
***In order to demonstrate successful completion of all components in the project, please use screenshot(s) to show each completed action step as specified on the instructions page.***

**Identity and Access Management**

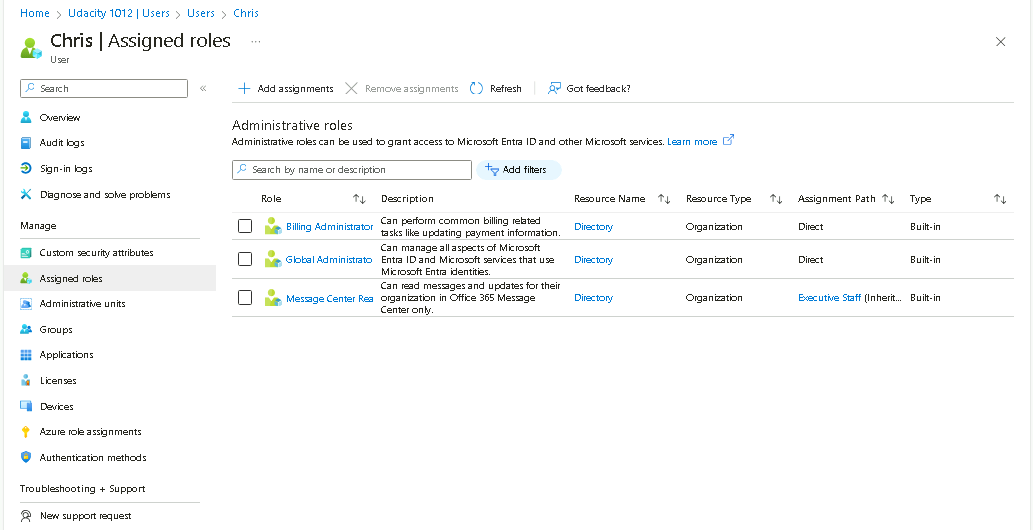


Proof of Assigned roles and AD assignments

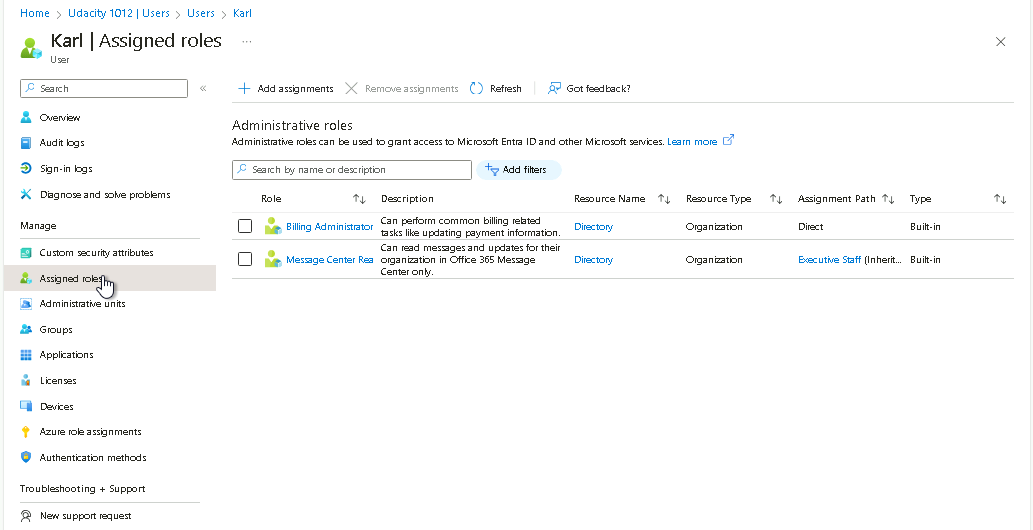
* 1. Andrew



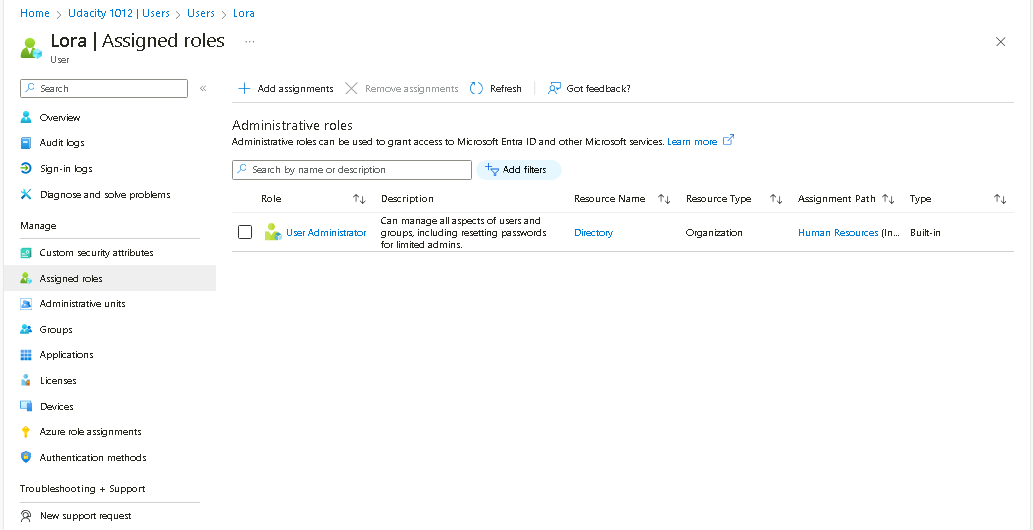
* 1. Chris



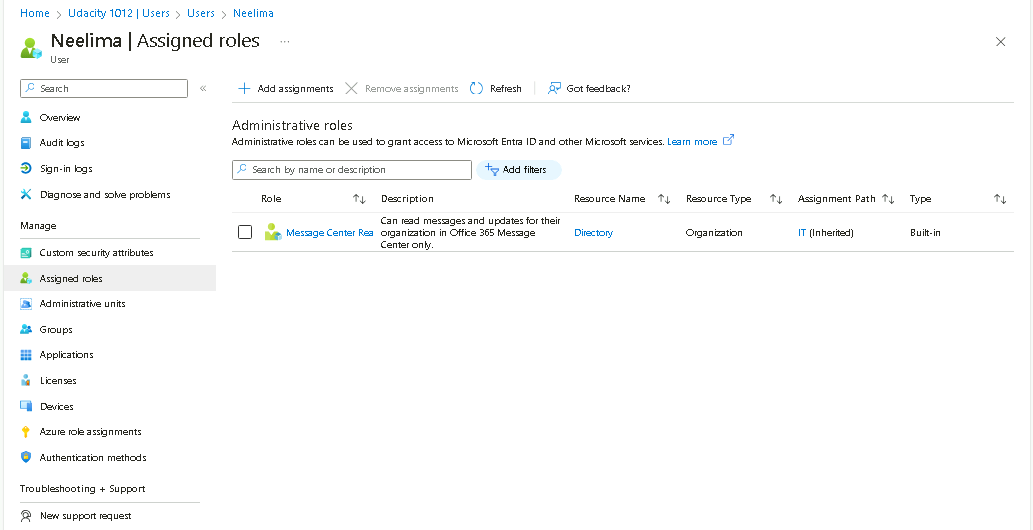
* 1. Karl



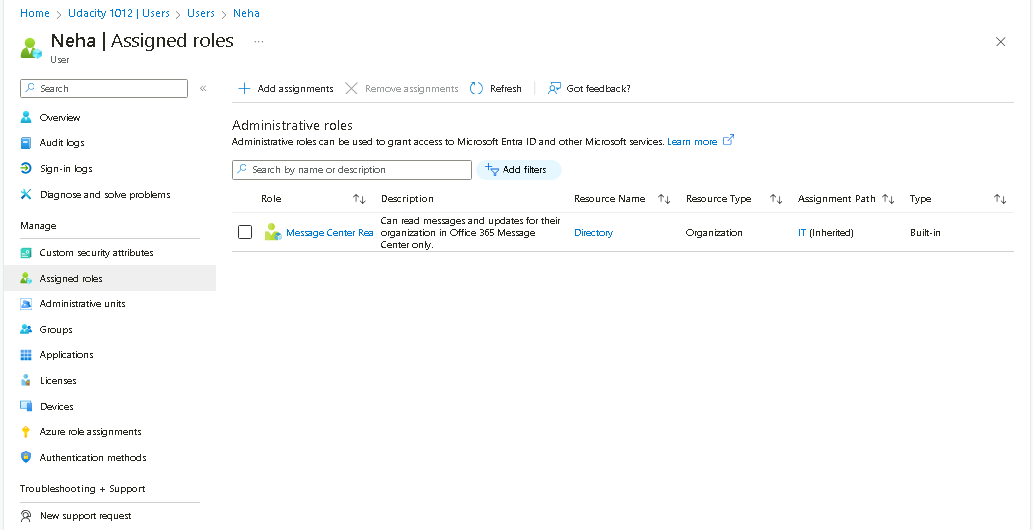
* 1. Lora



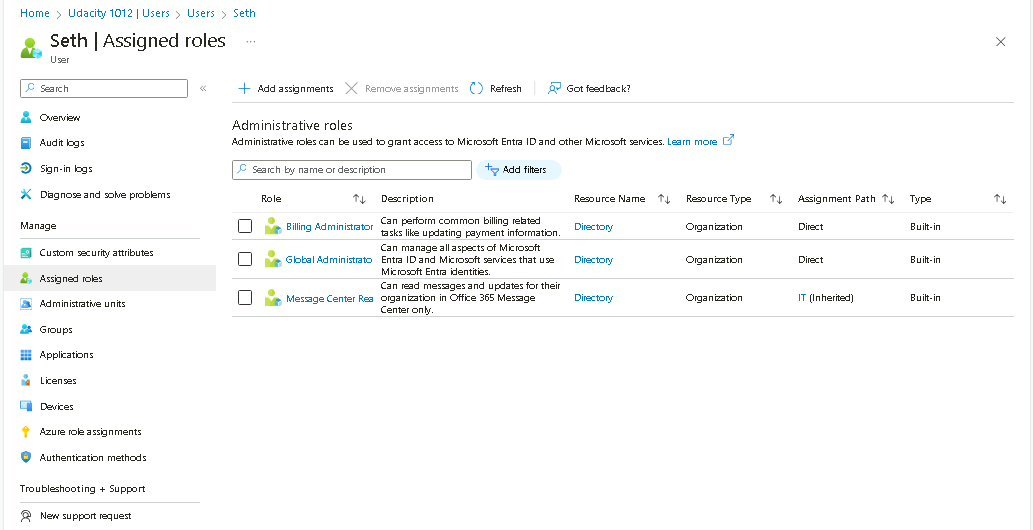
* 1. Neelima



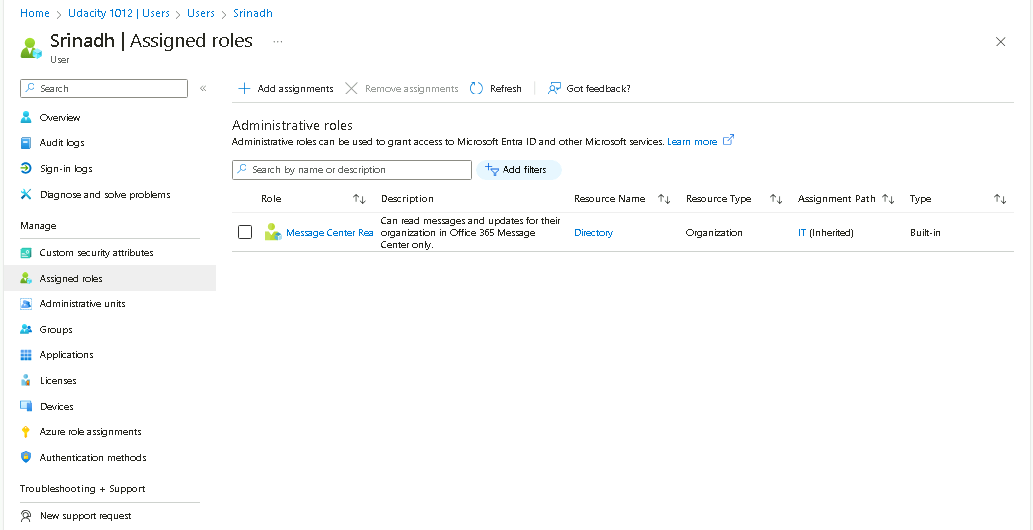
* 1. Neha



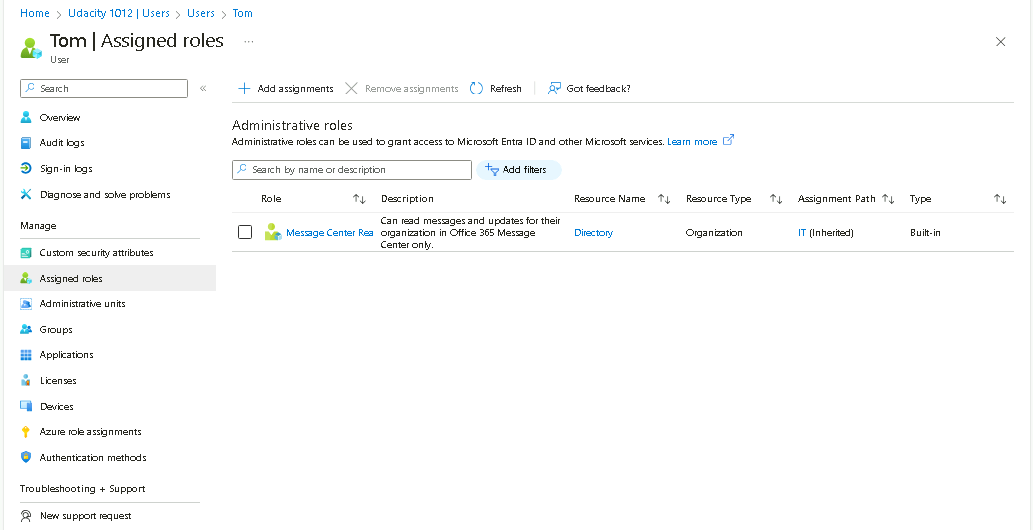
* 1. Seth



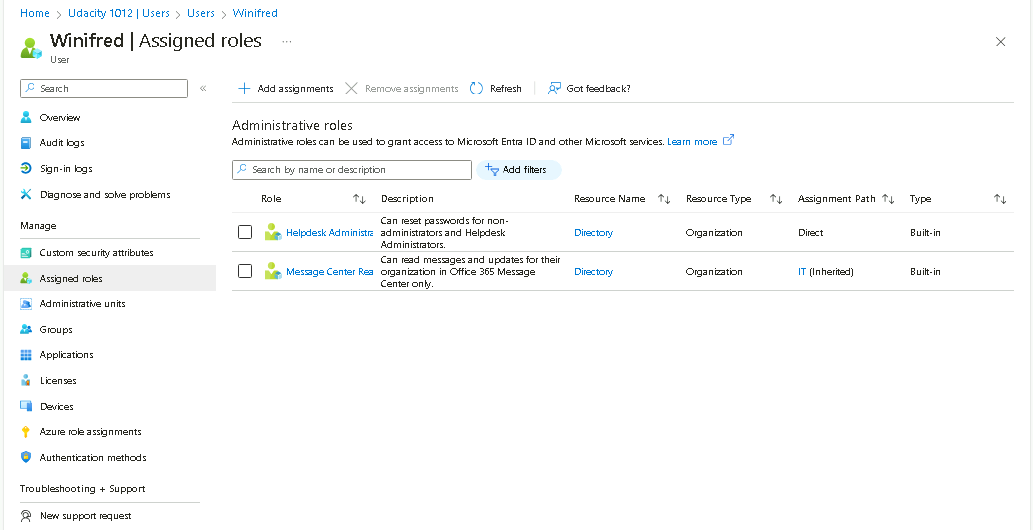
* 1. Srinadh

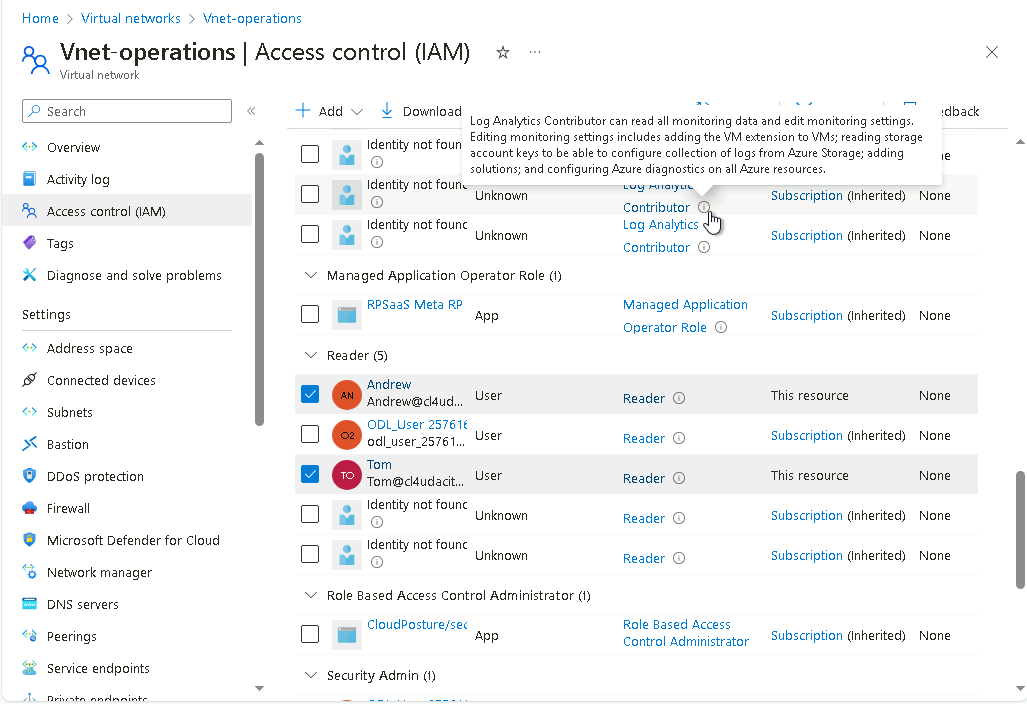


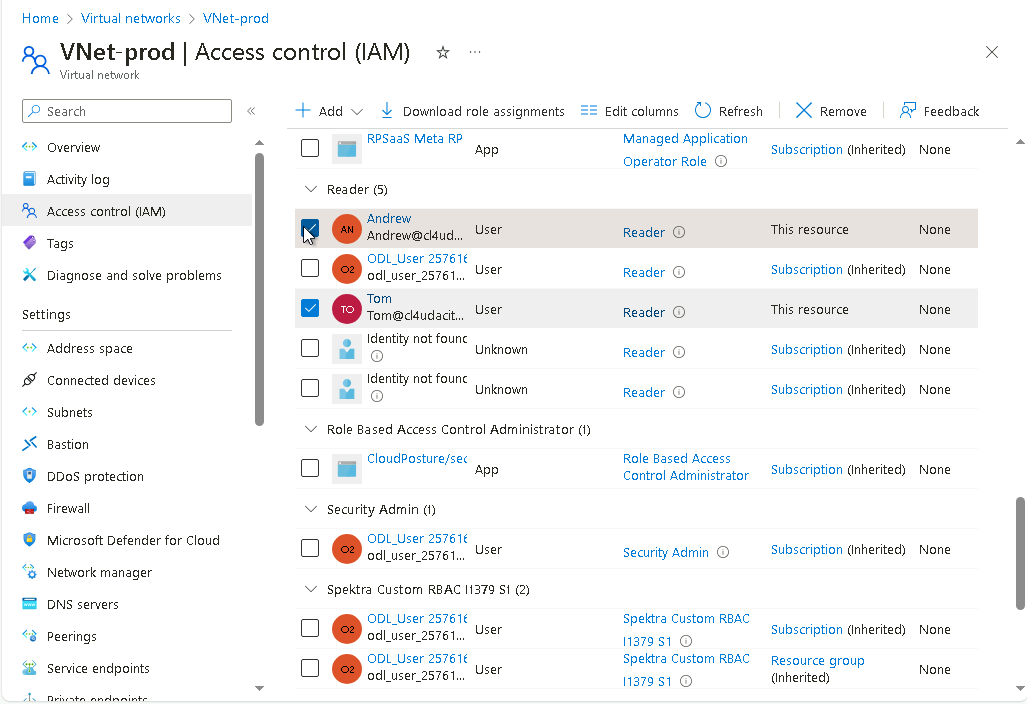
* 1. Tom

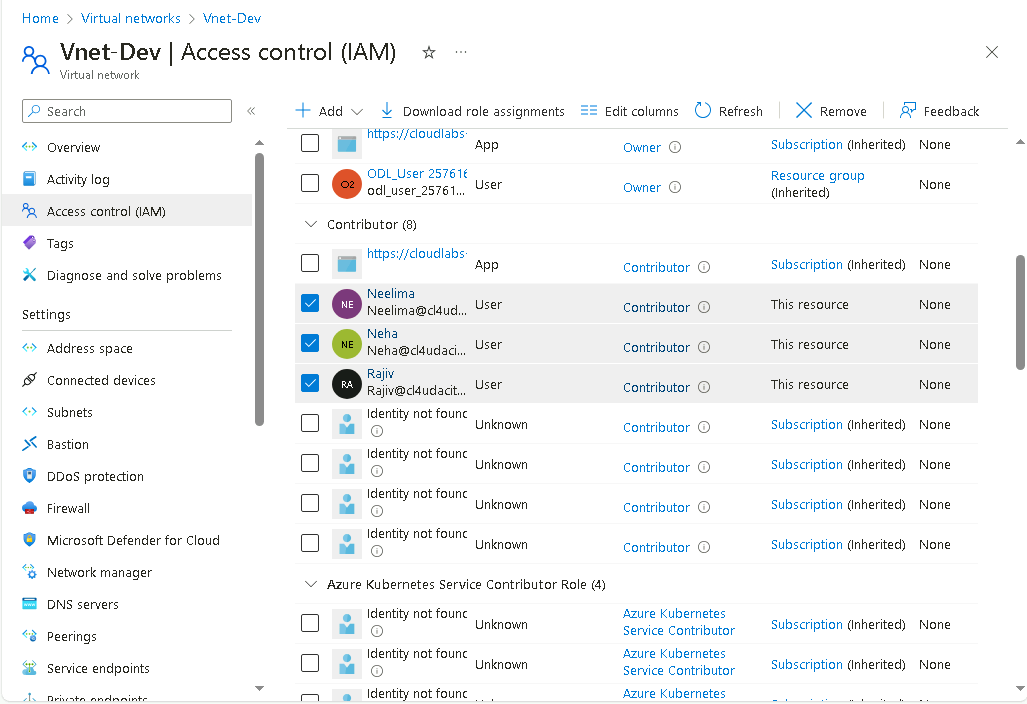


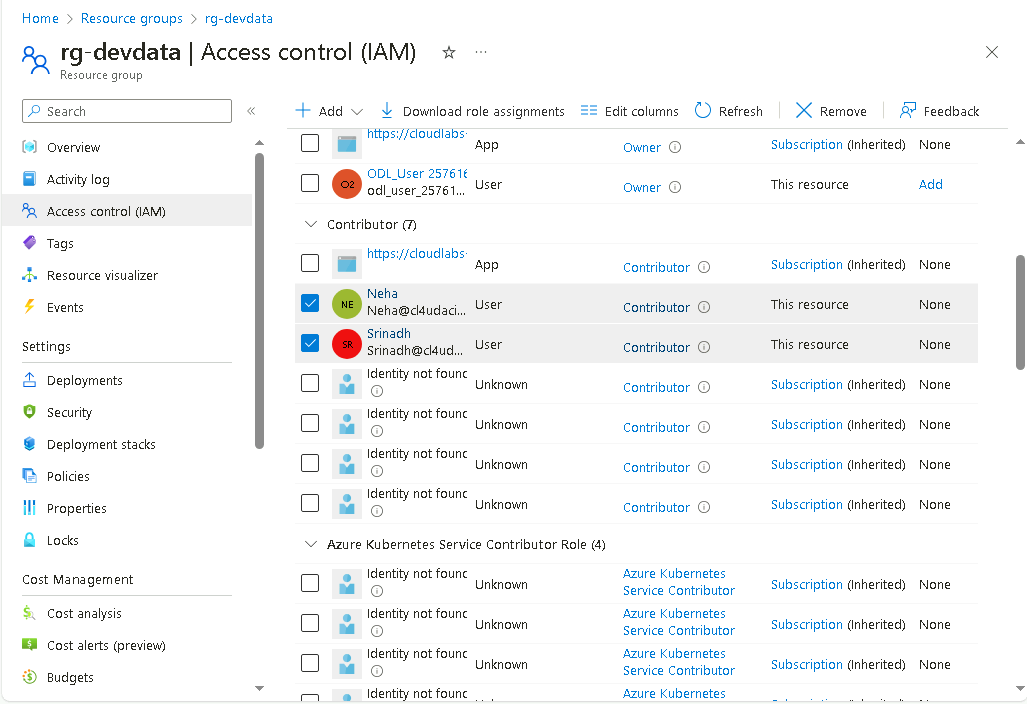
* 1. Winifred

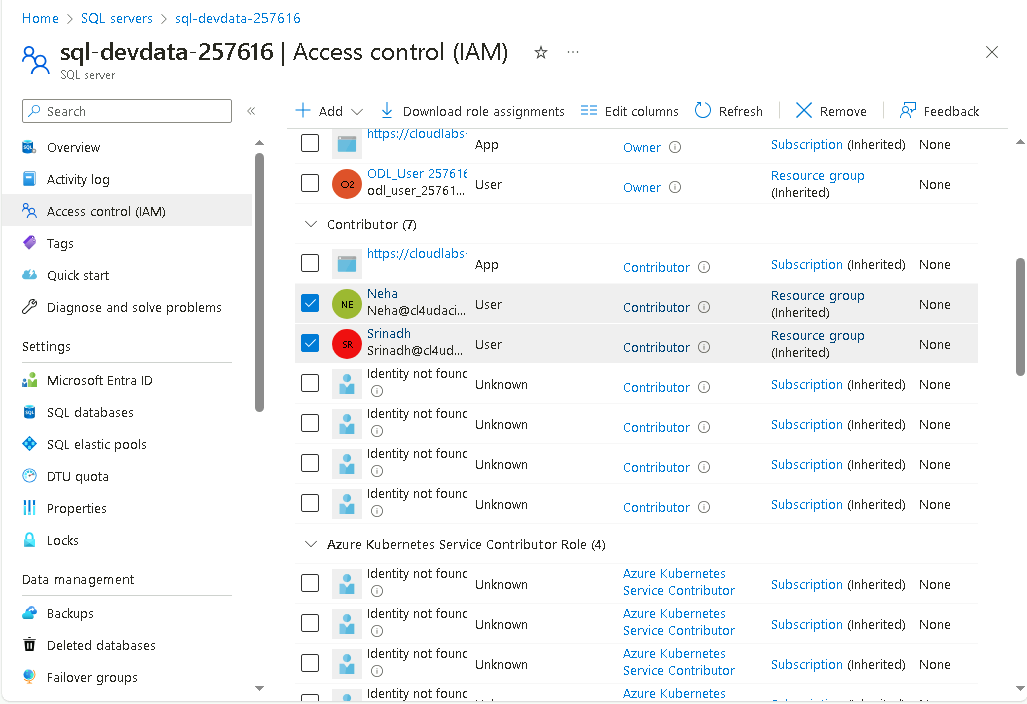


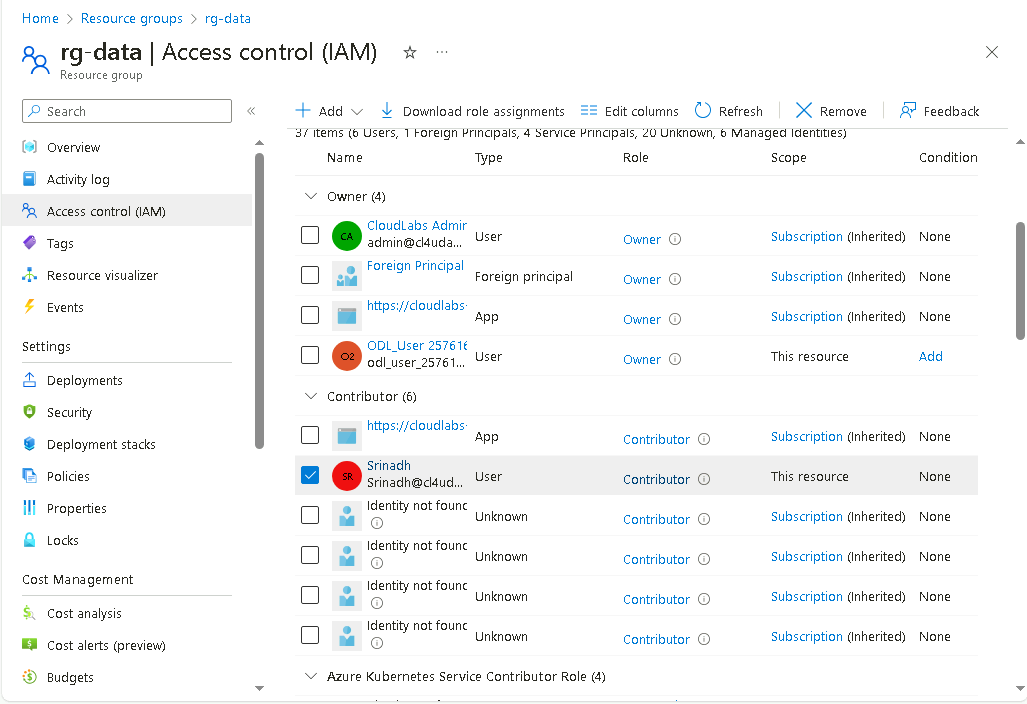


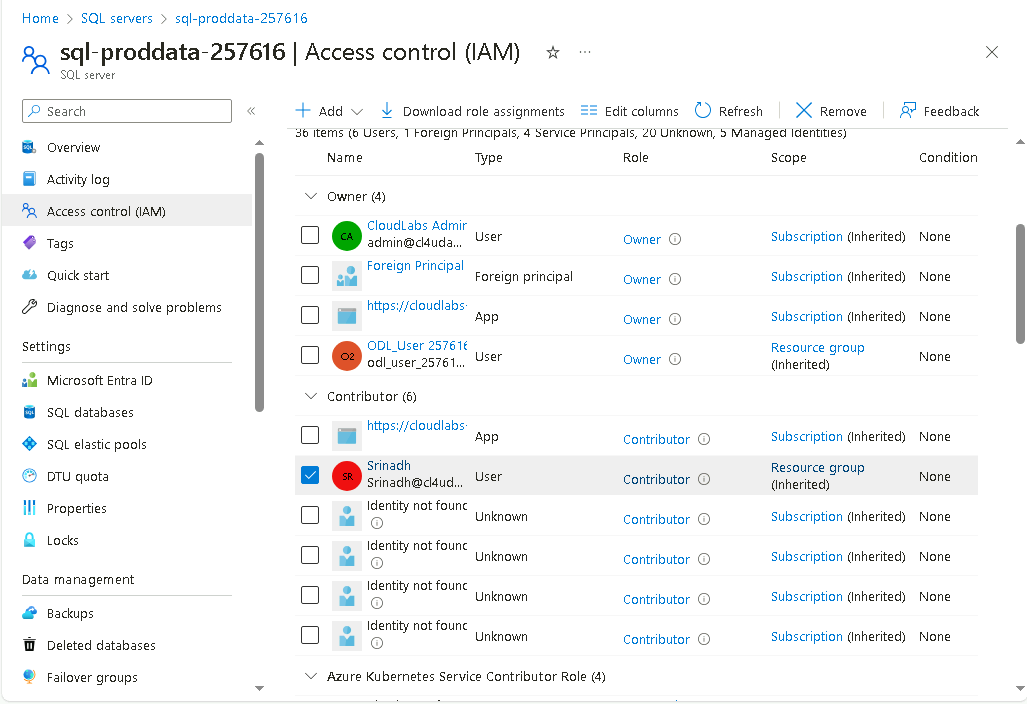




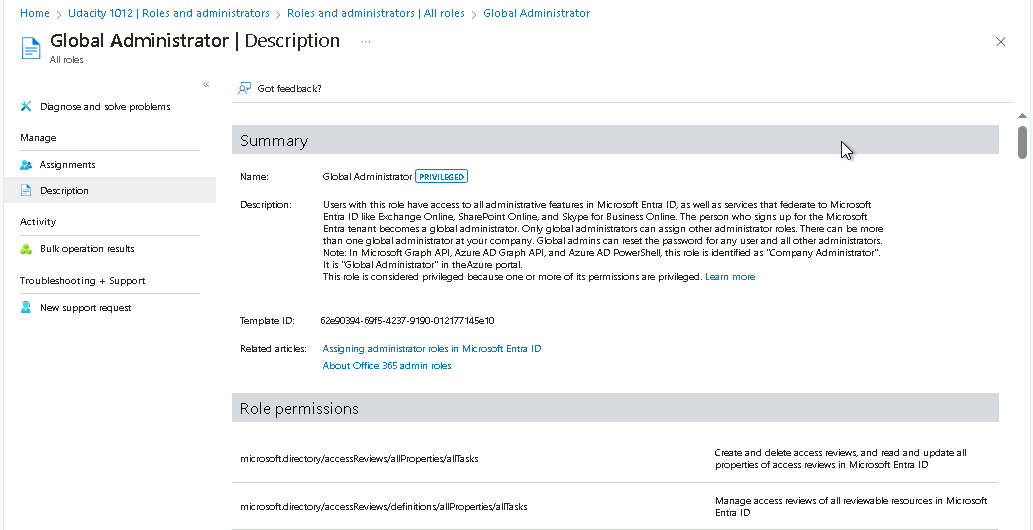




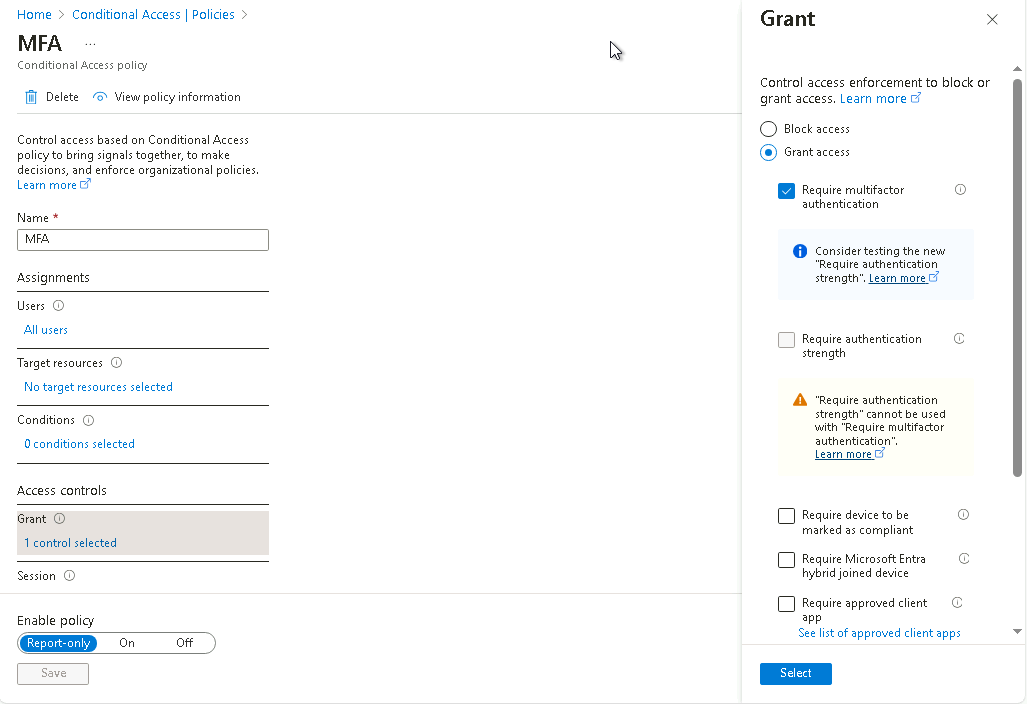




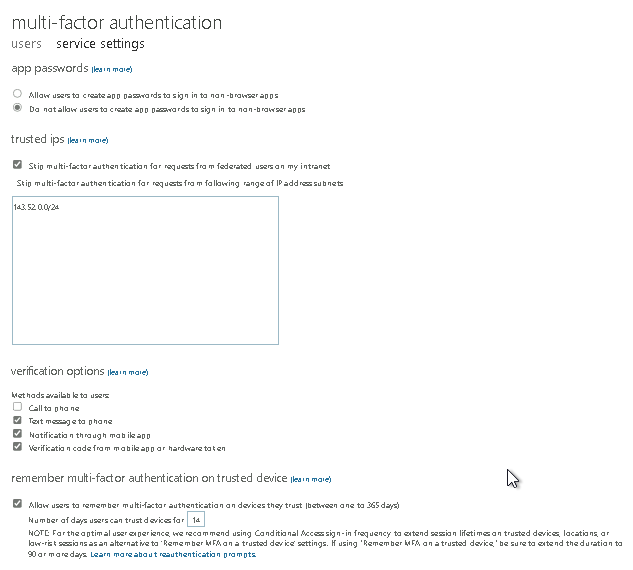
1. Proof of Global Administrator setting with duration, eligibility, expiration



1. Proof of Conditional Access policy all users

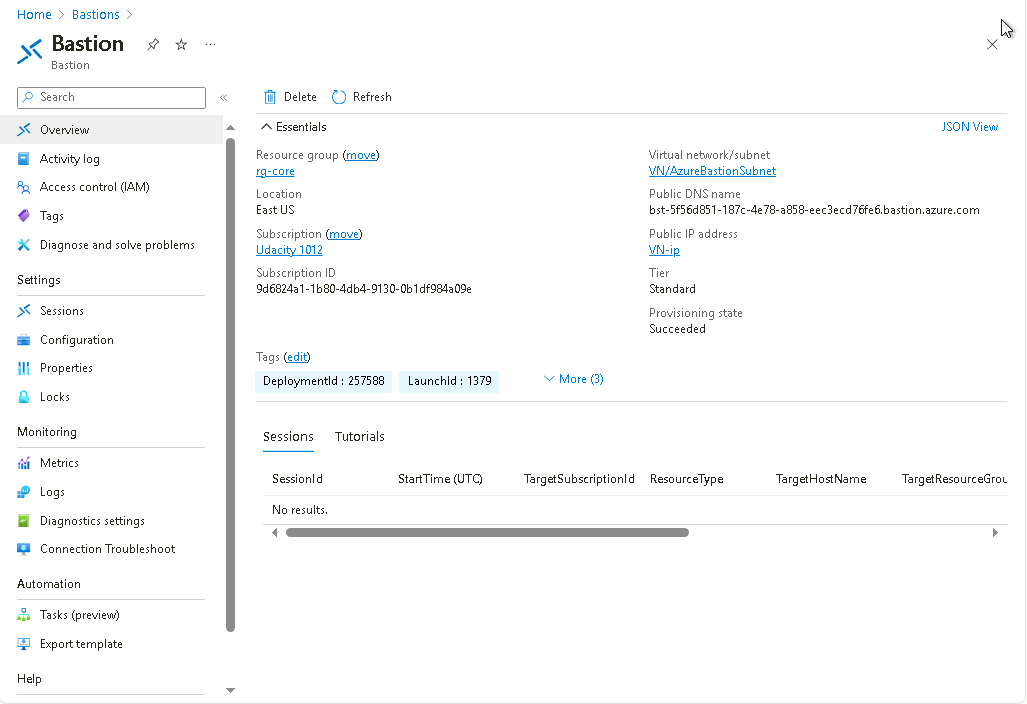


1. Proof of Multi-factor authentication(14 days, Charlotte office info)

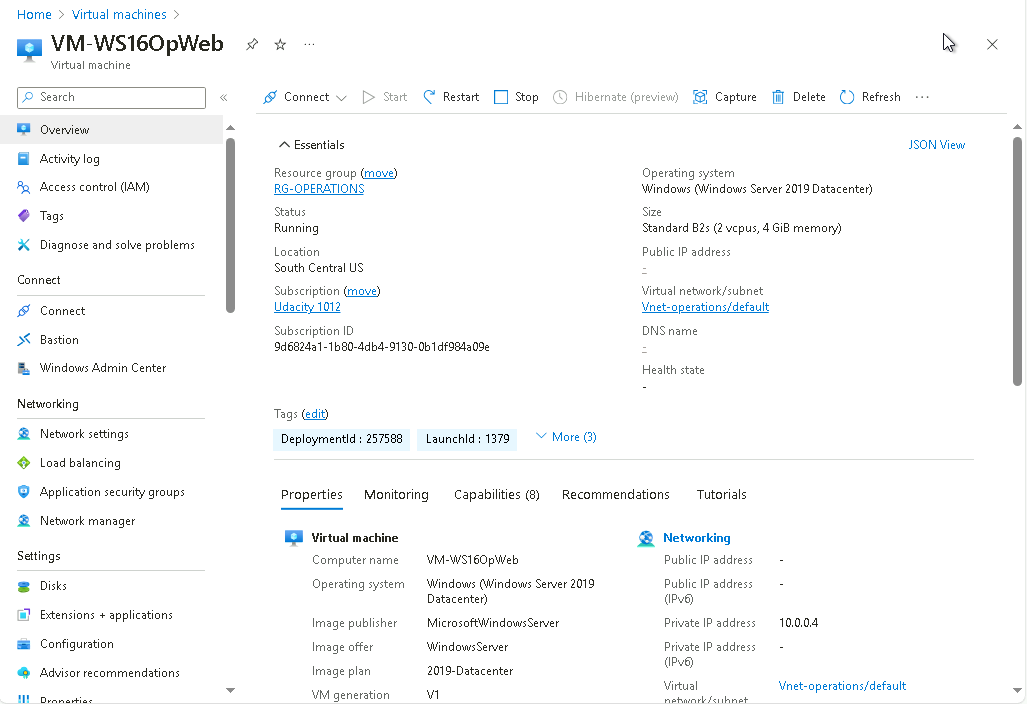


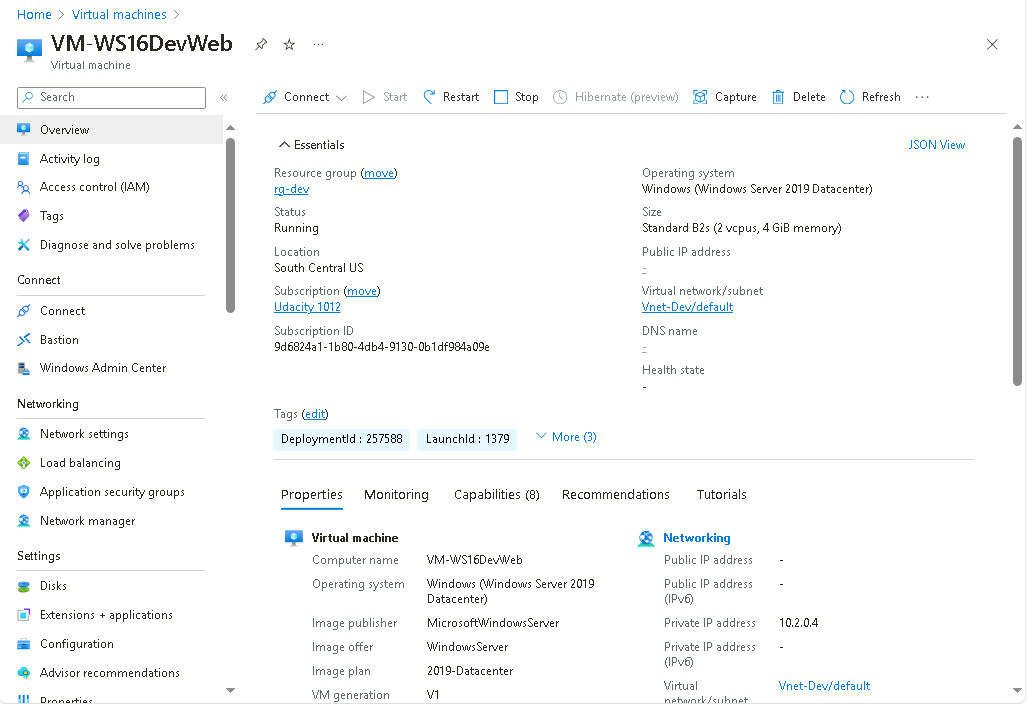
**Network Security**

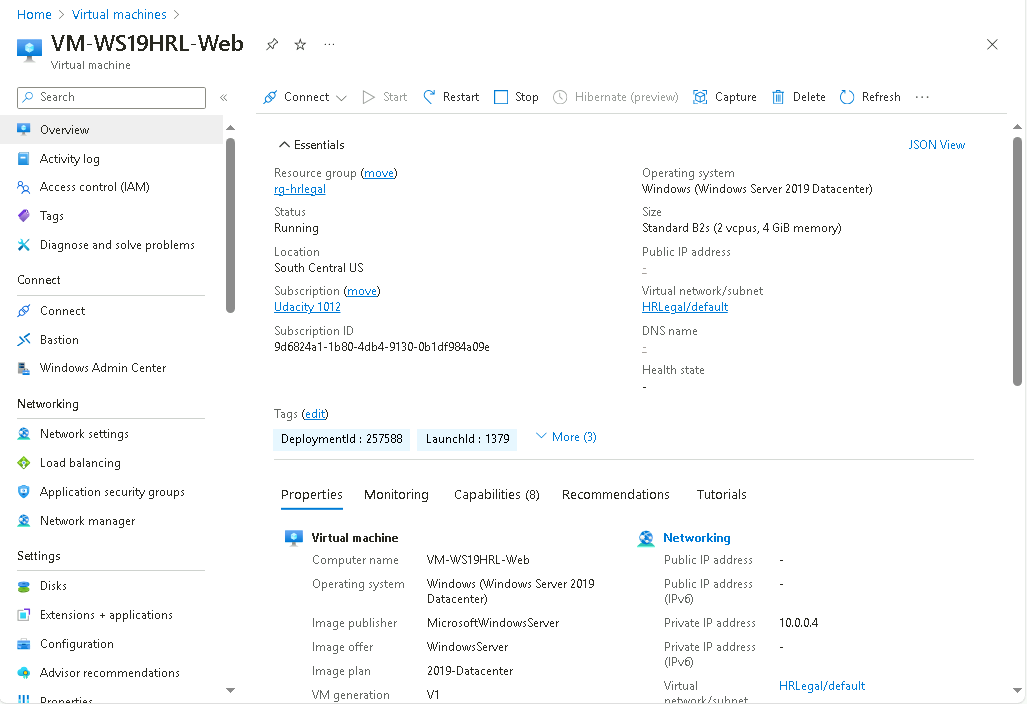
1. Bastion overview



1. Proof of public IP addresses removed

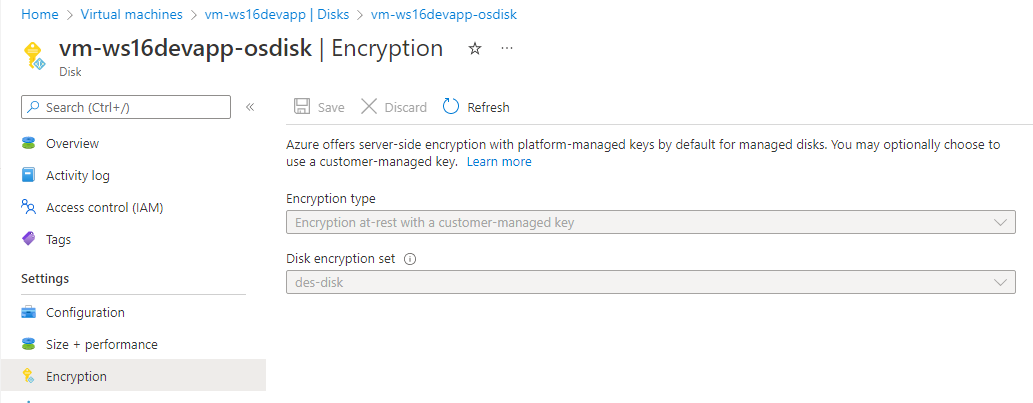


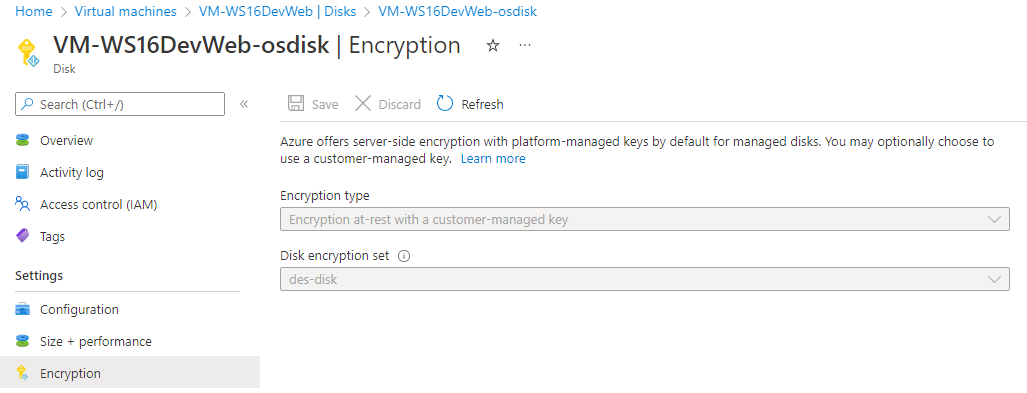


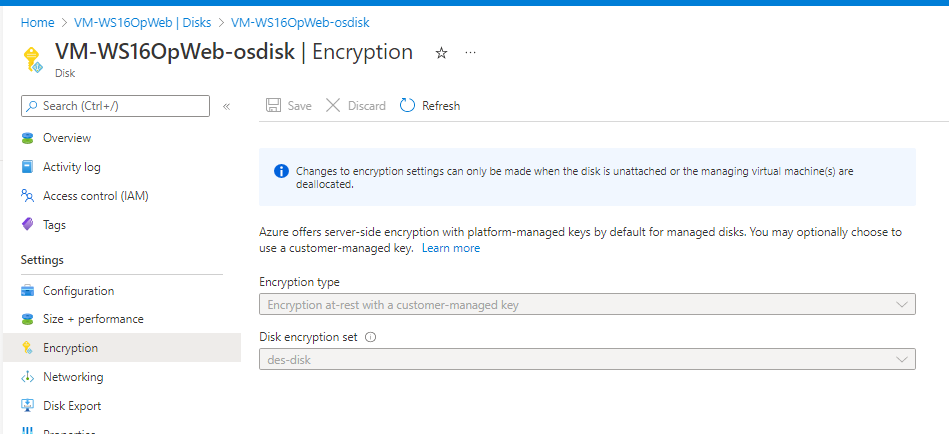


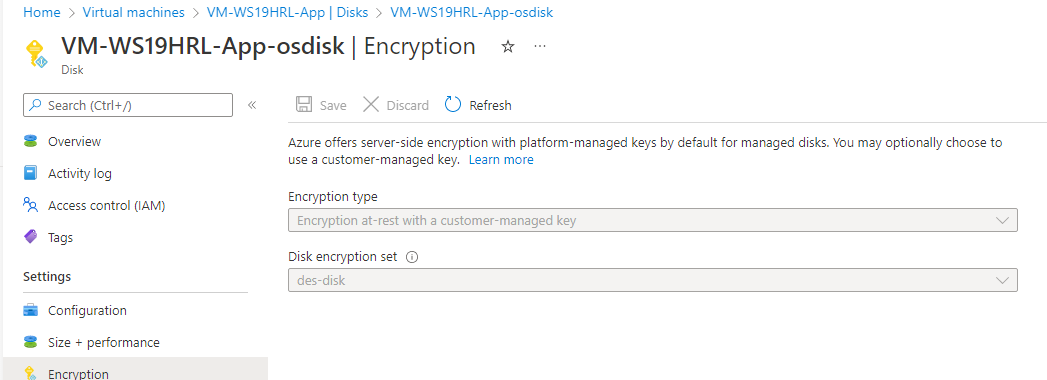
**Data and Encryption**

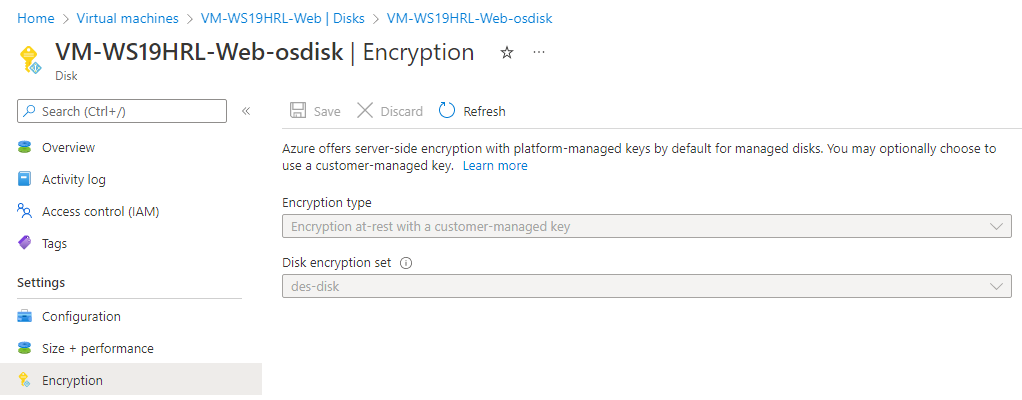
1. Proof of Encryption types for VM ( devapp,OpWeb,HRL-App,OPApp, HRL-Web)

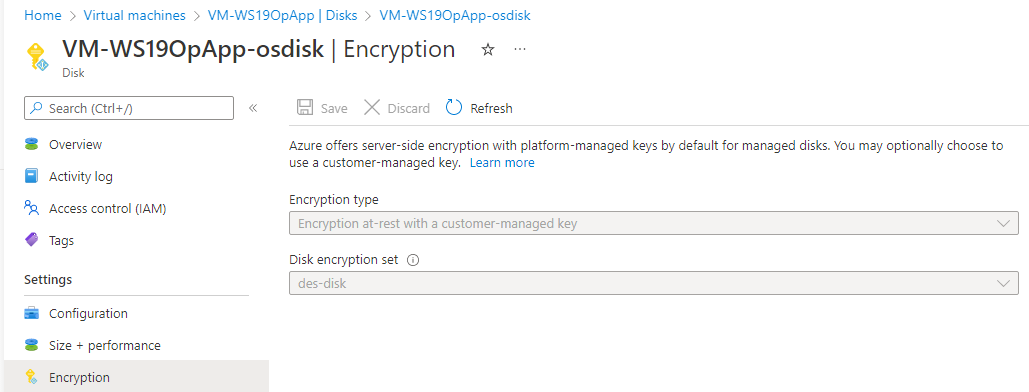




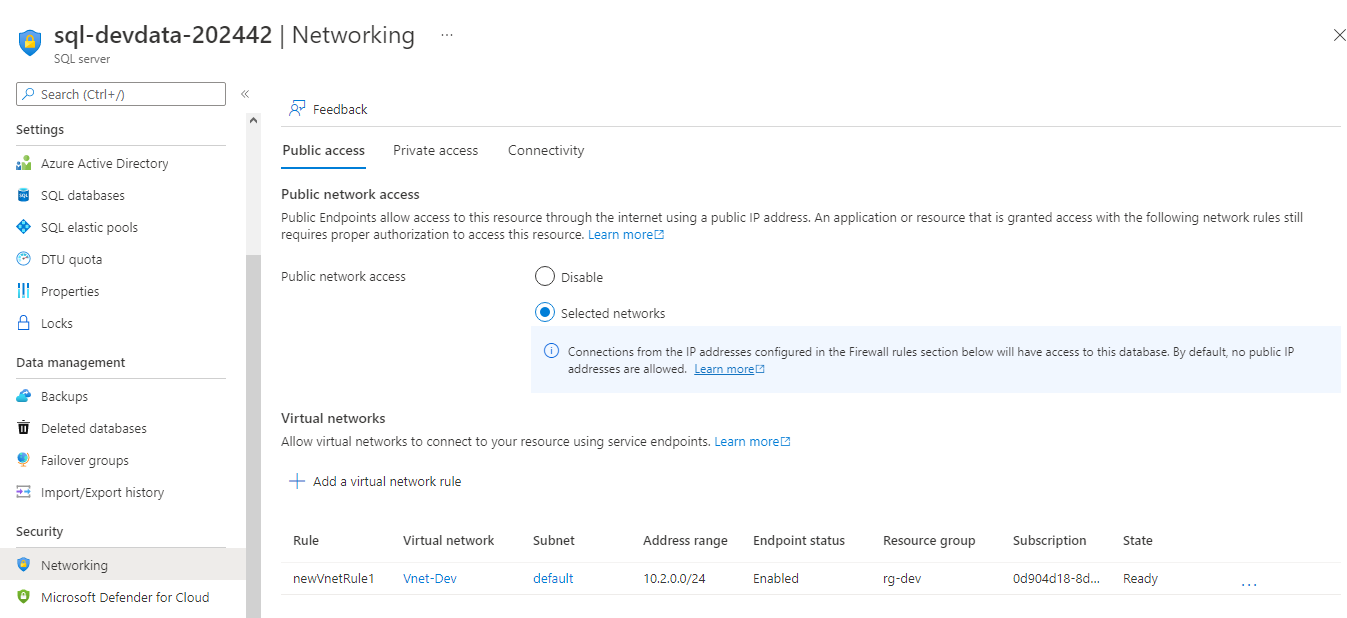


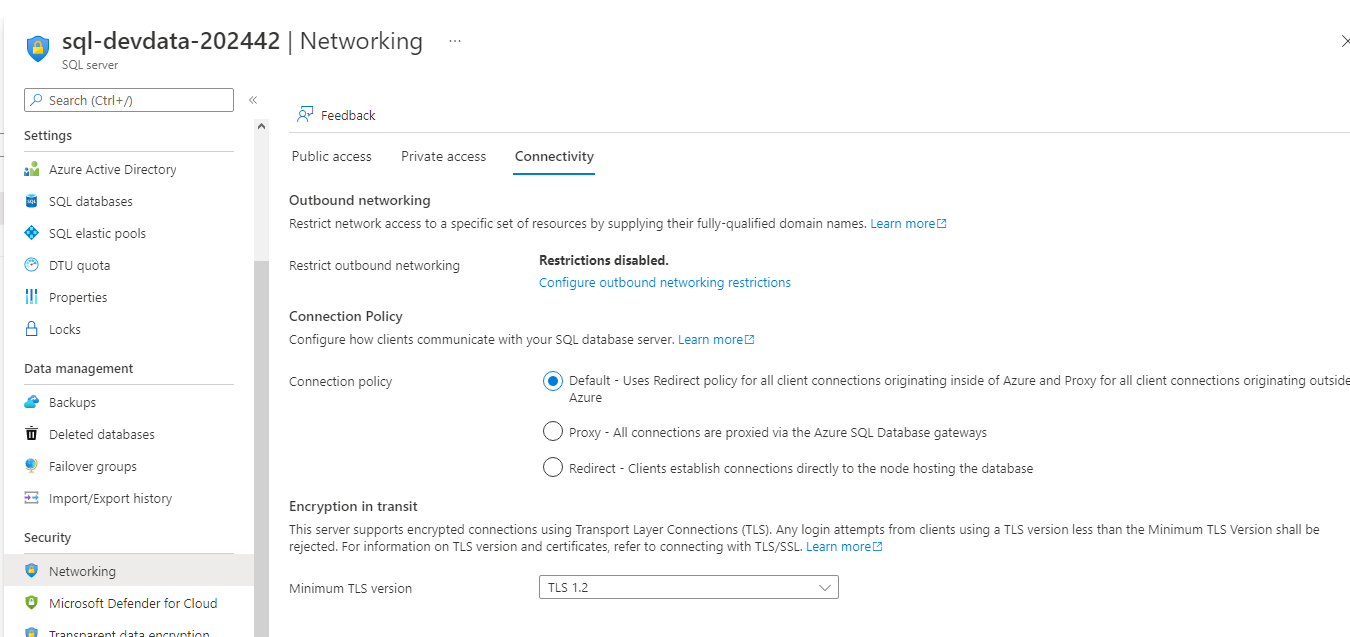


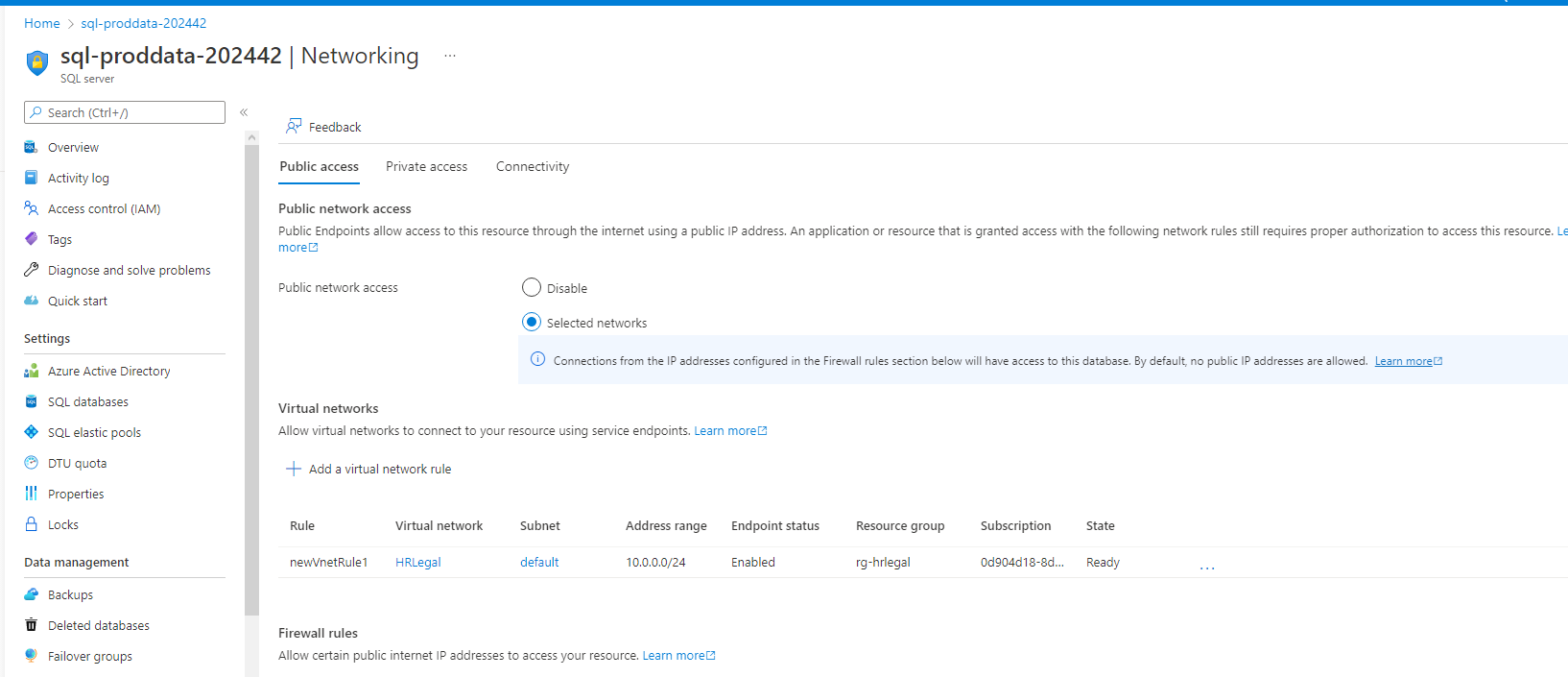


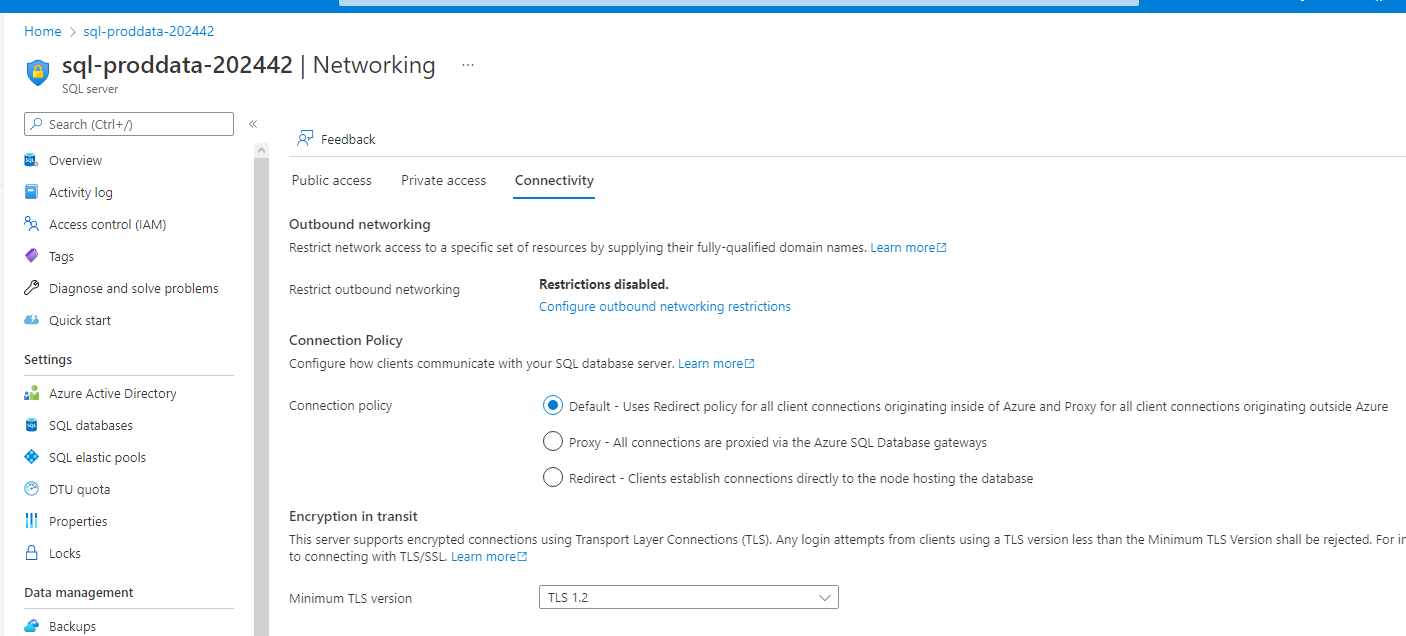


1. Firewalls and virtual networks page
   1. Proof of no public access and TLS for SQL servers(prod, dev)

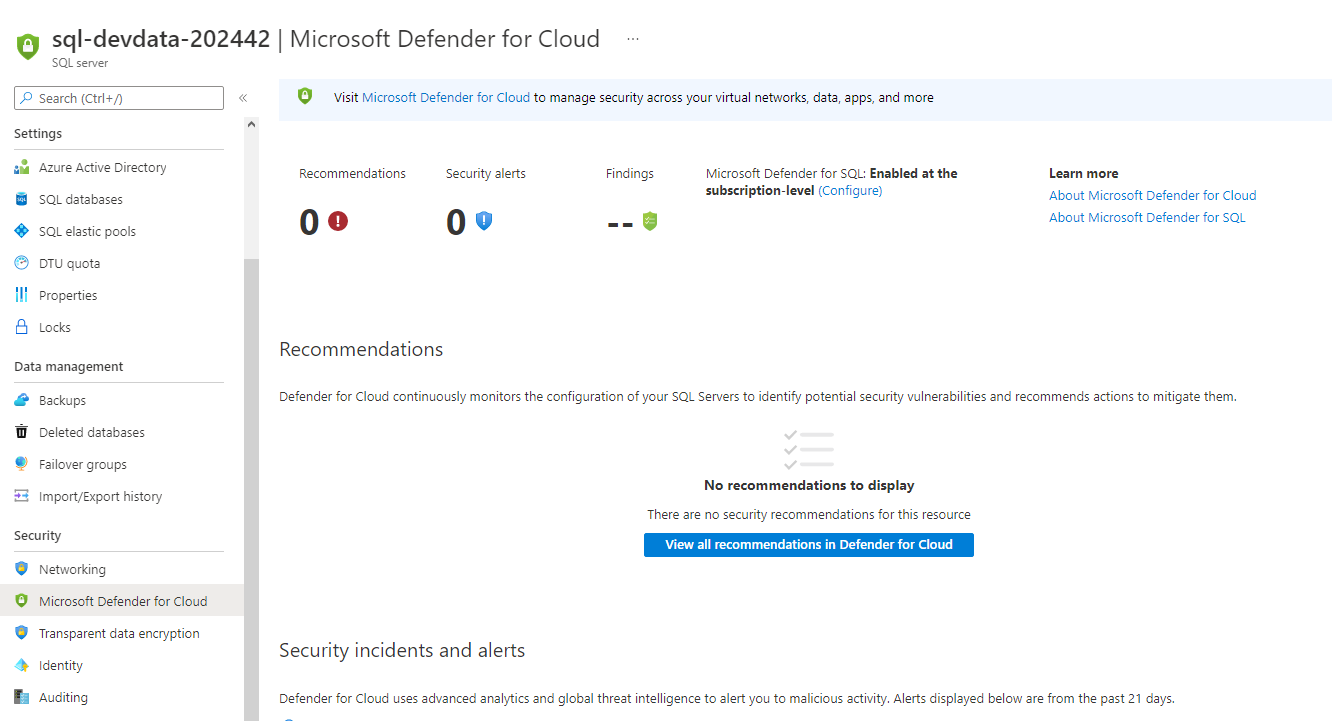


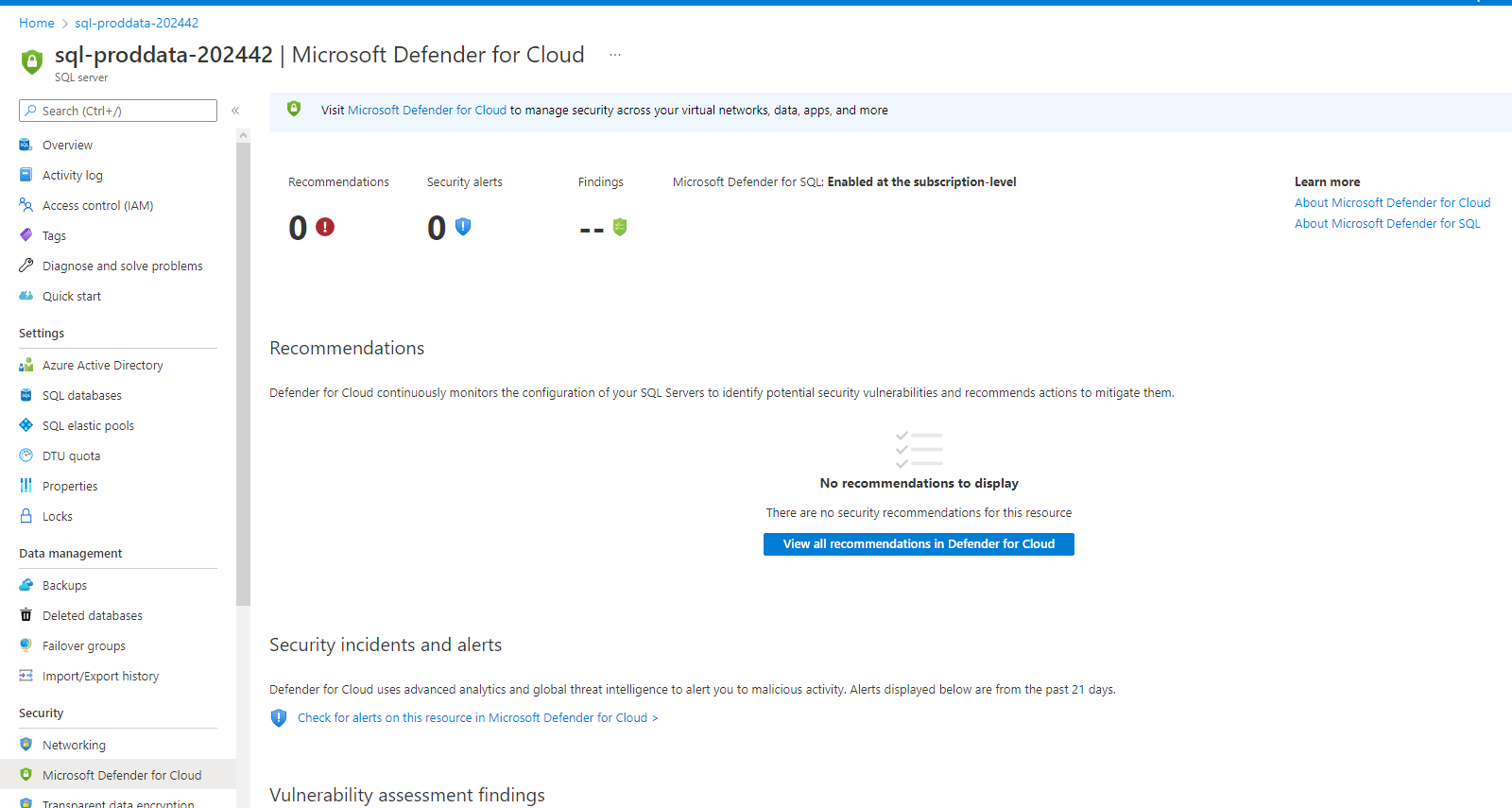




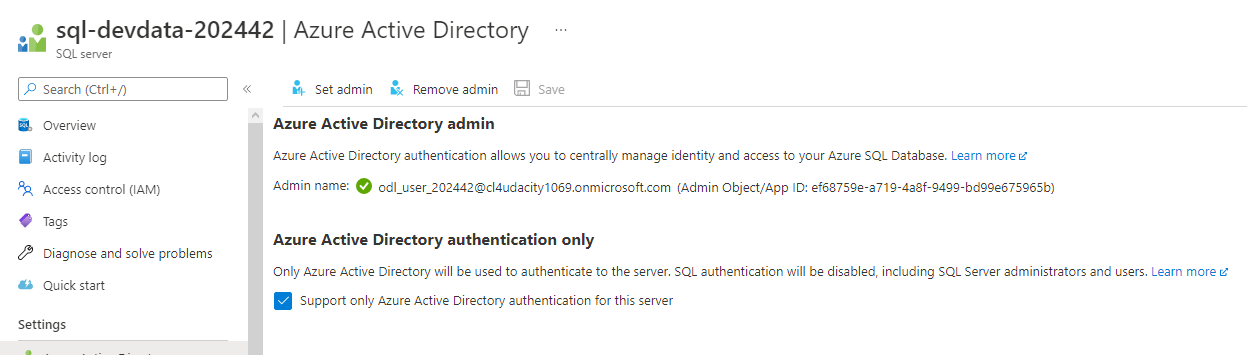


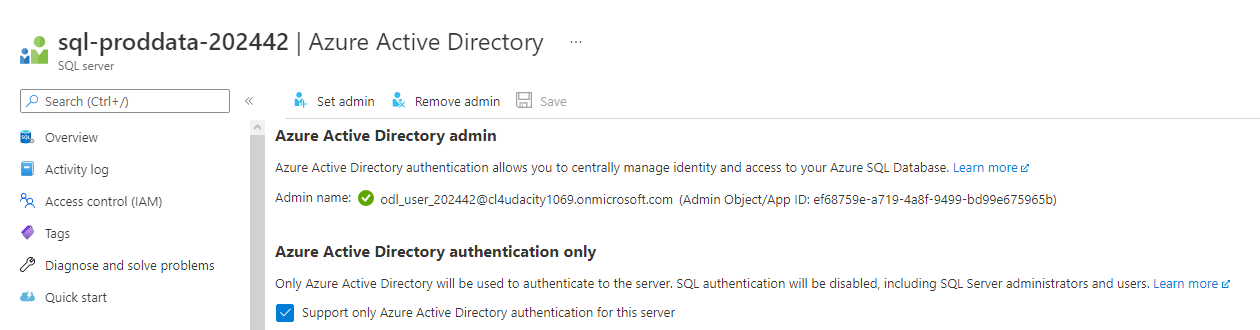
1. Proof of Azure Defender SQL server enabled(prod, dev)





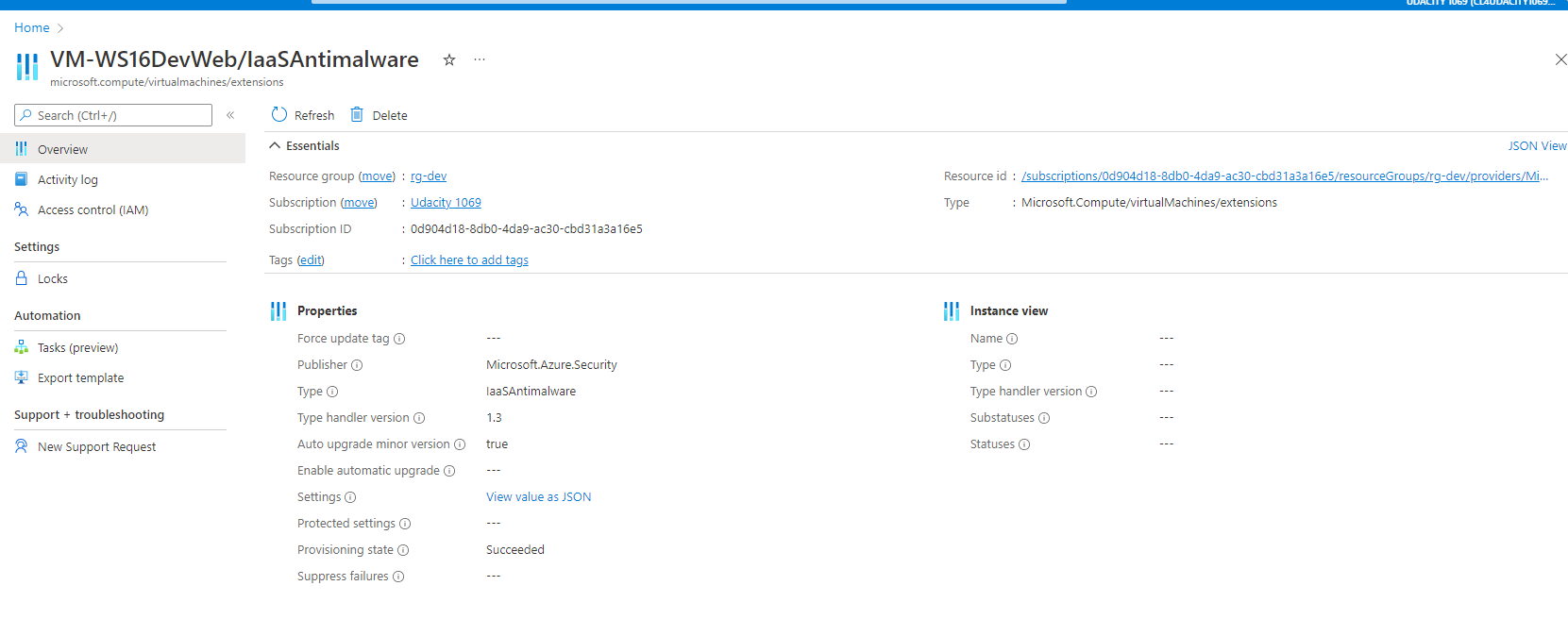
1. Proof of Azure AD authentication for SQL enabled(prod, dev)

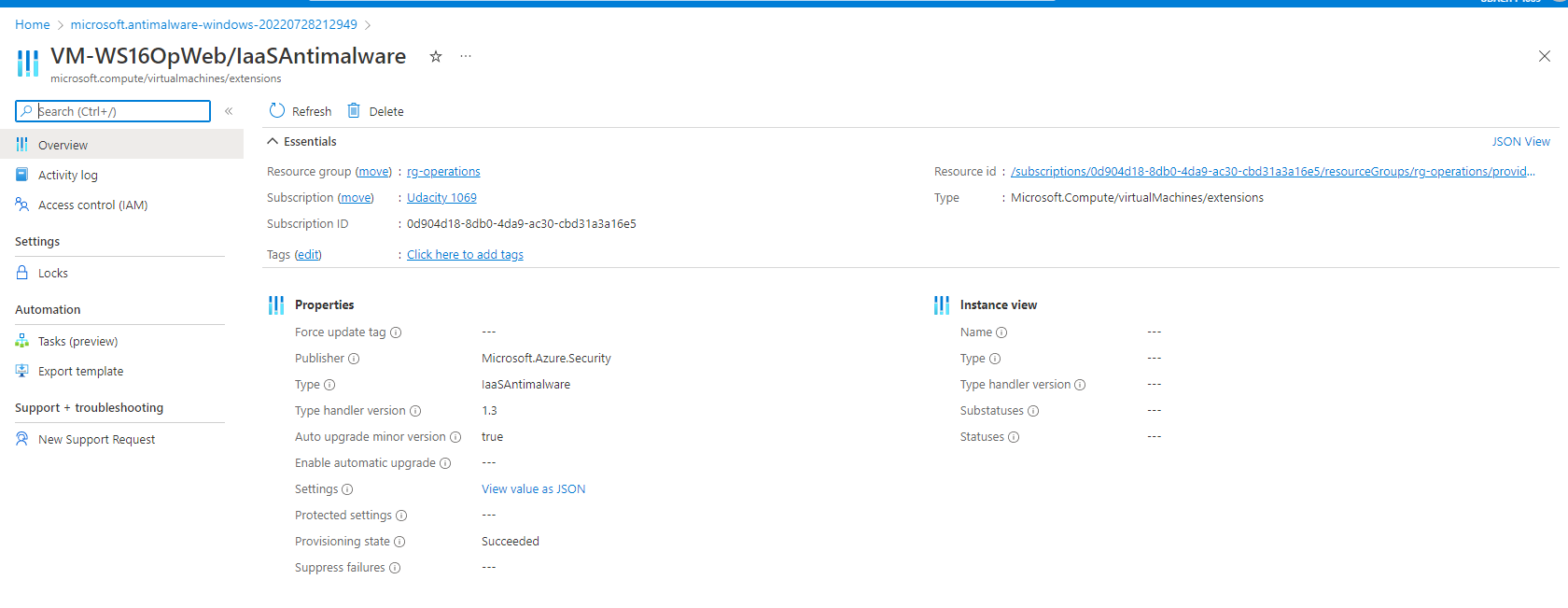


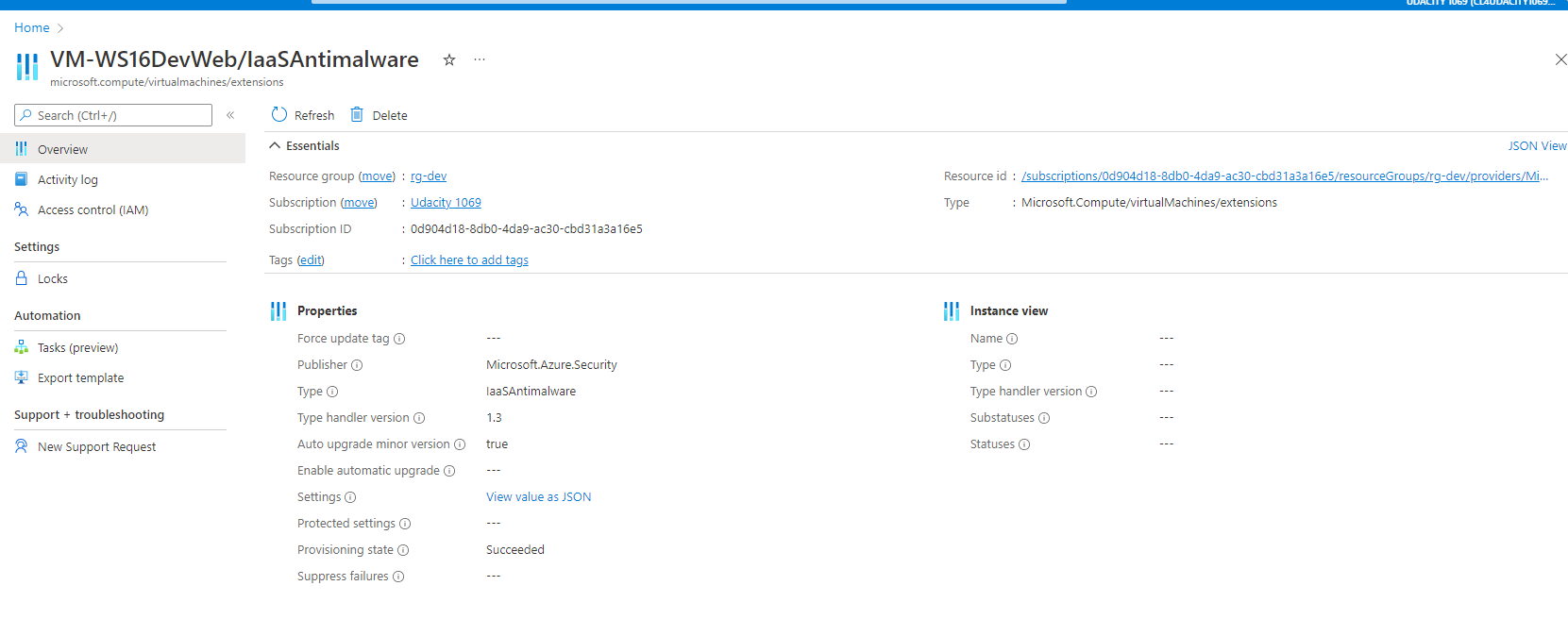


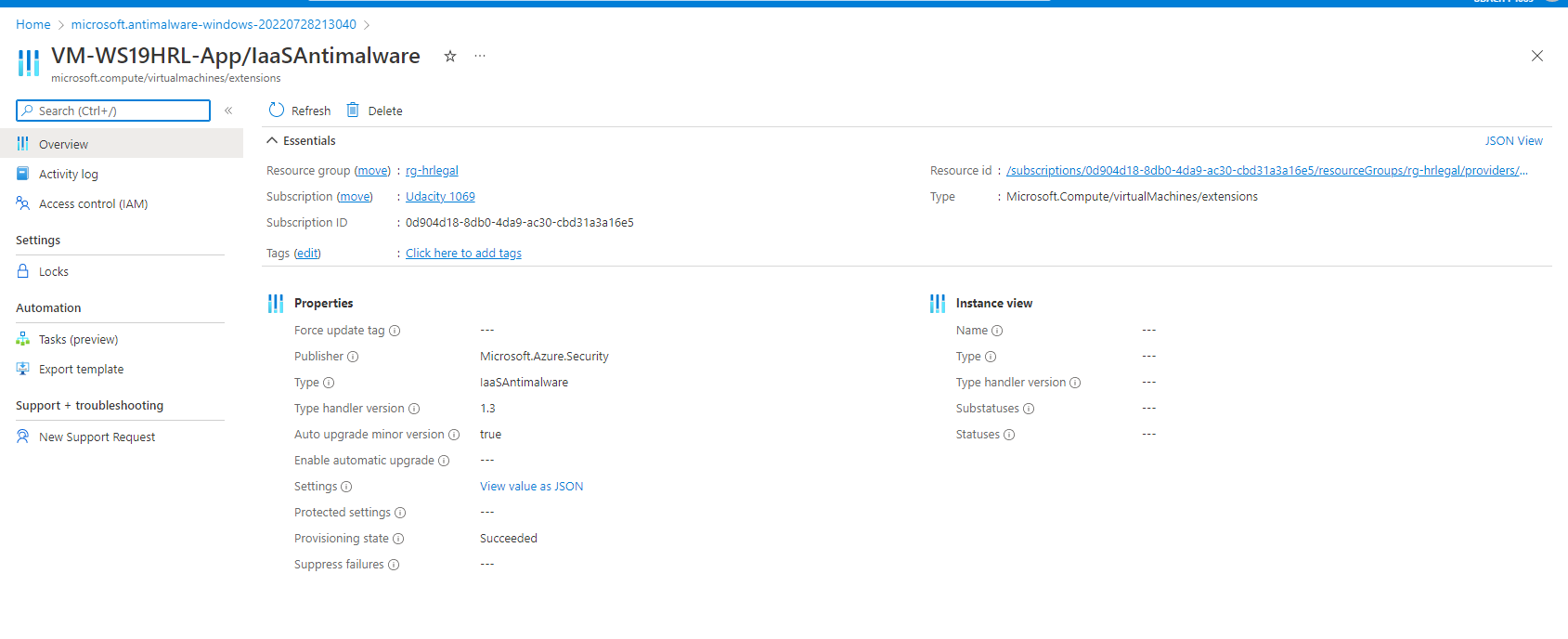
**Cloud Protection**

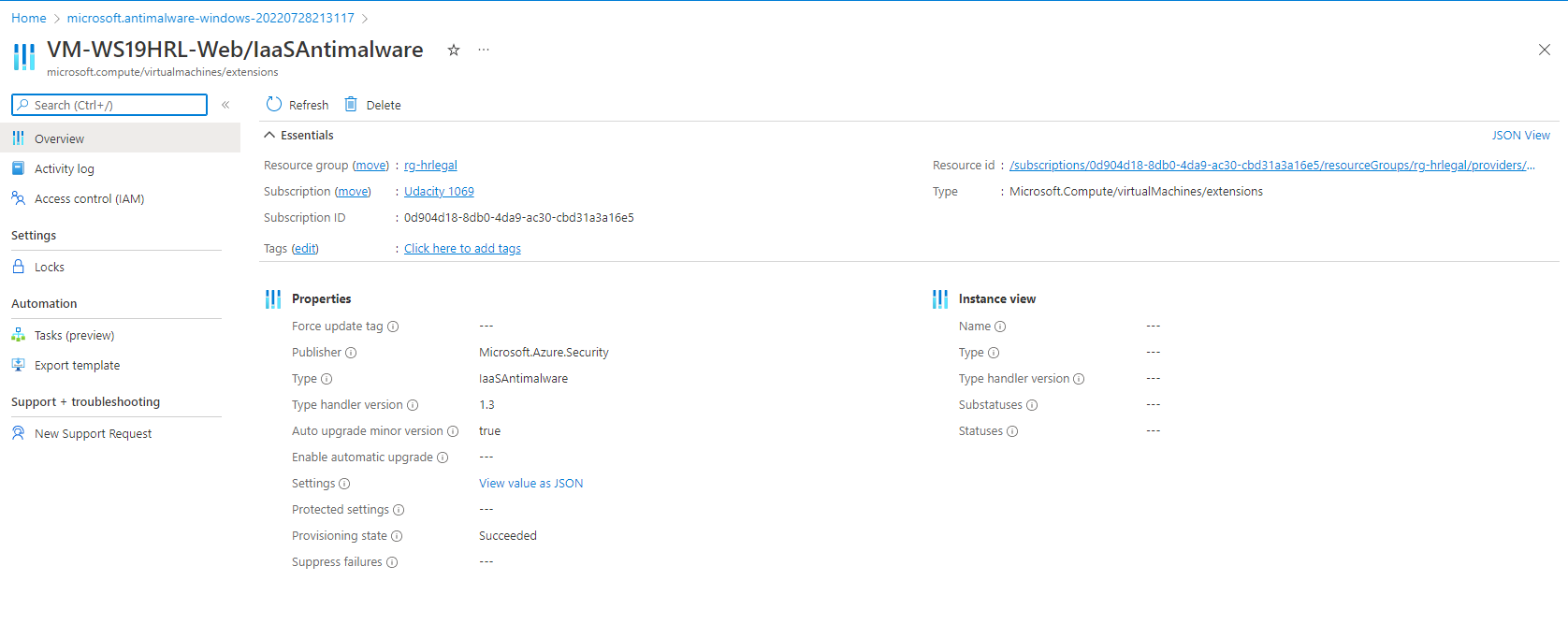
1. Proof of IaaSAntimalware enabled ( devapp,OpApp,HRL-Web, HRL-App,OpWeb)

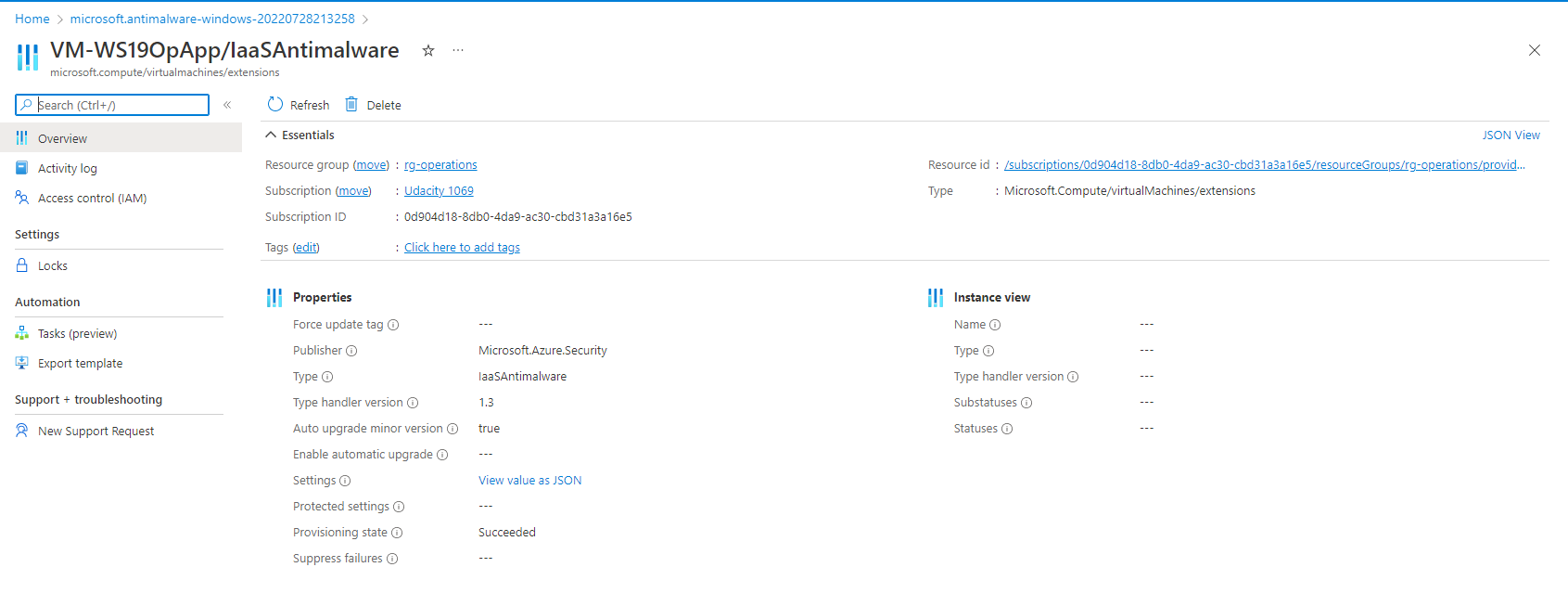




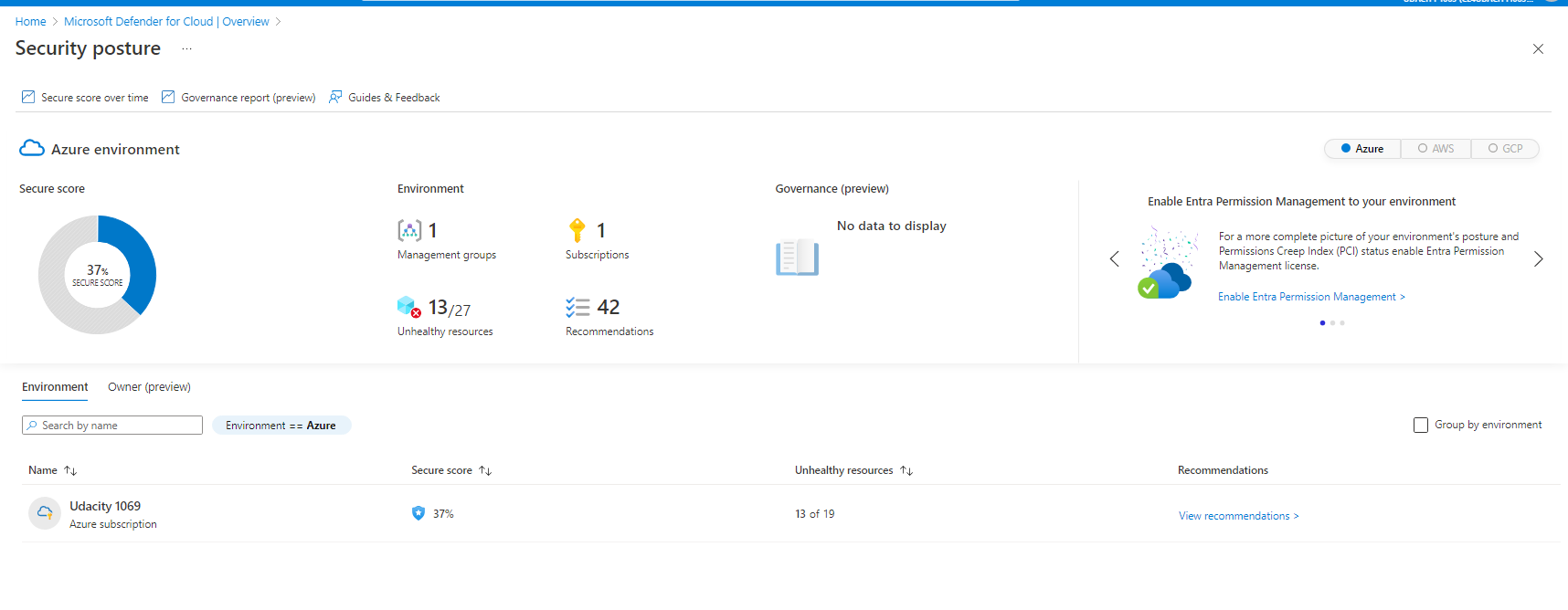


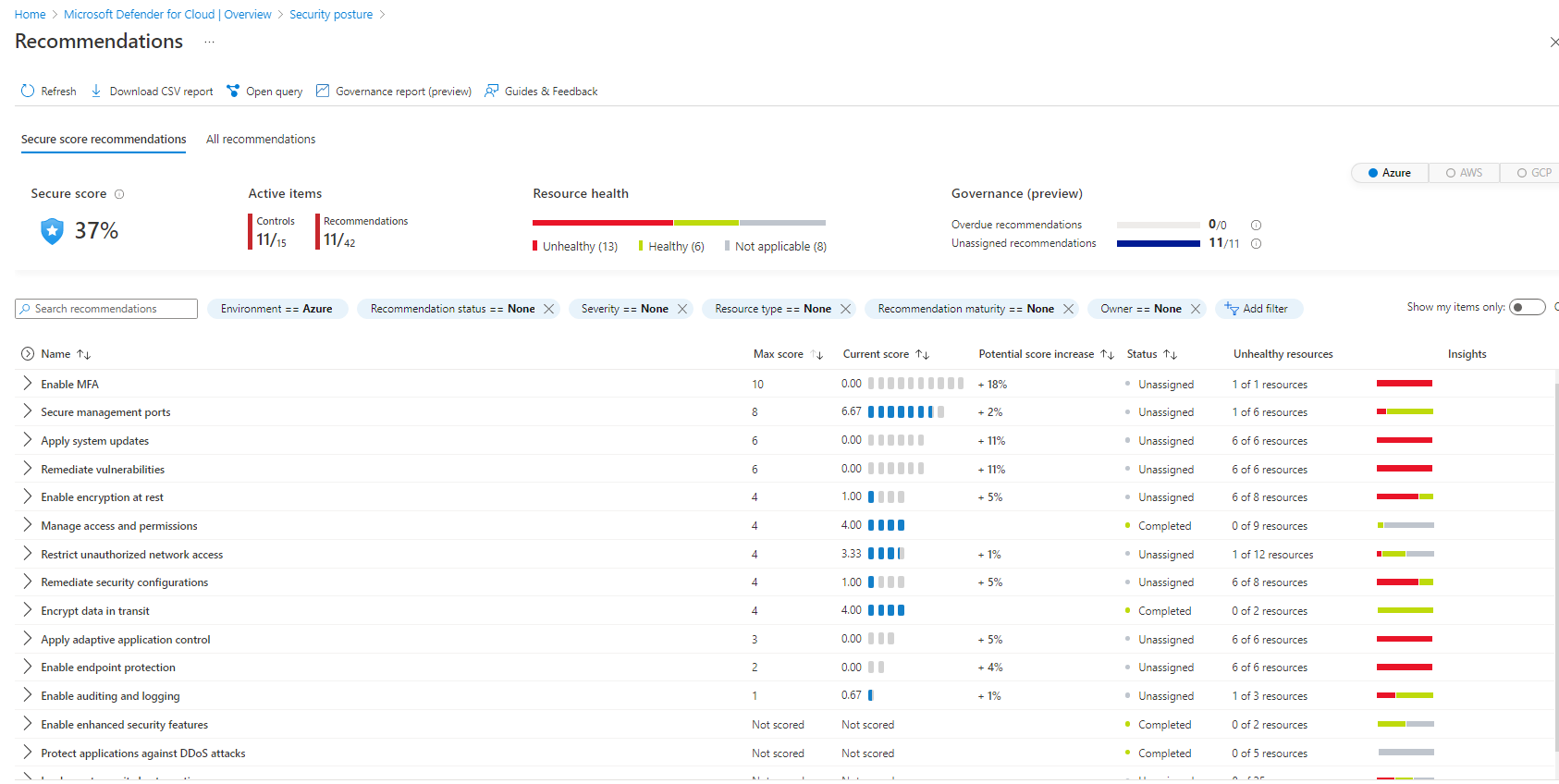


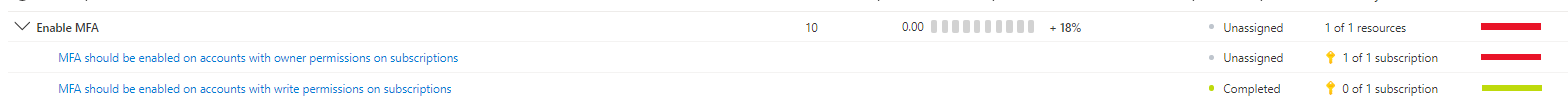


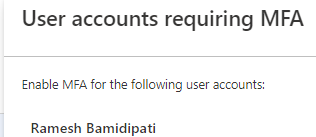


1. Recommendations

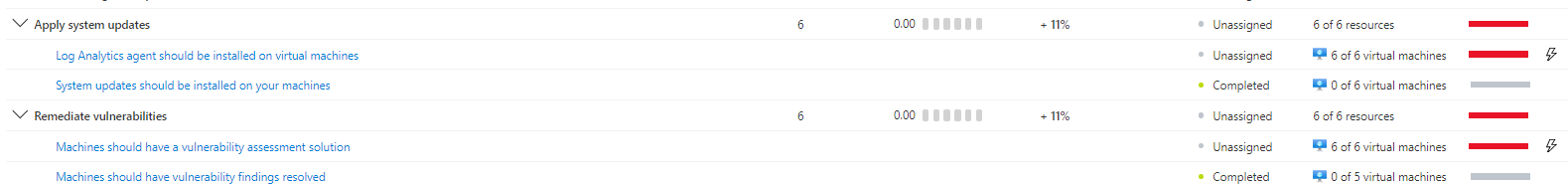




“Enable MFA” currently has a score of 0/10. So it has the biggest impact on security if we fix it.MFA is not set up for user account Ramesh Bamidipati.

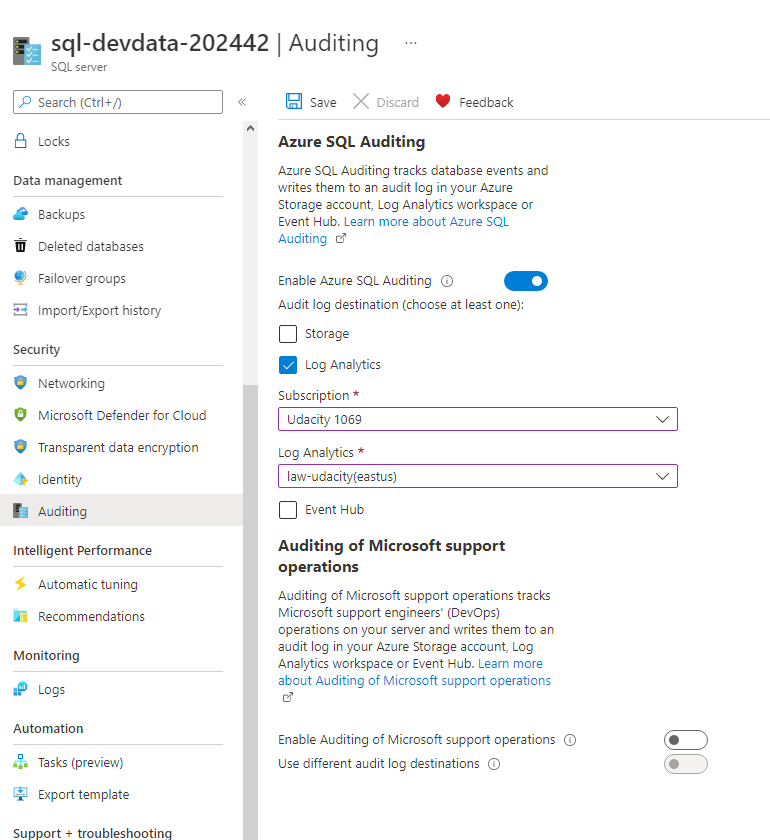


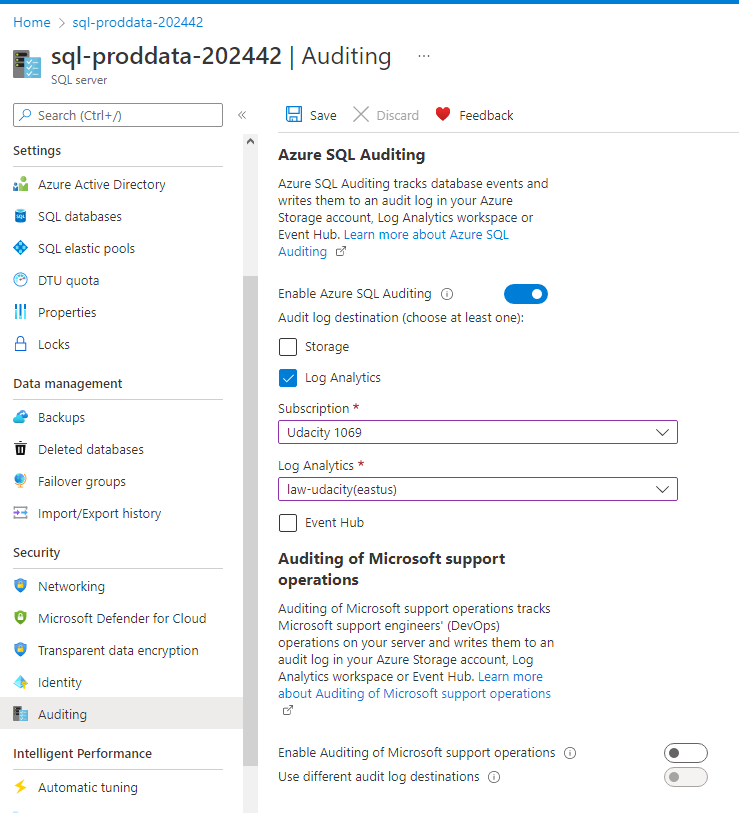
The other 2 top remidations are “Apply system updates” and “Remidate vulnerabilities”. Both of them have a score of 0/6.

We should install the log analytics agent on all of our Vms. And we should install vulnerability assessment tools on our VMs.

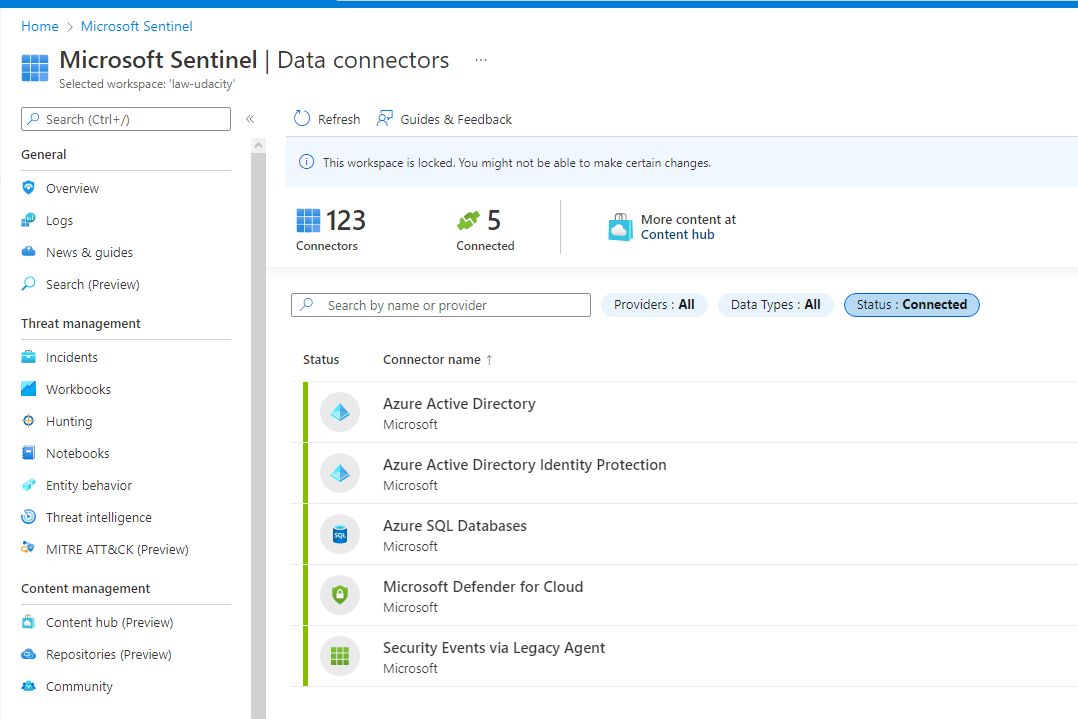
**Monitoring**

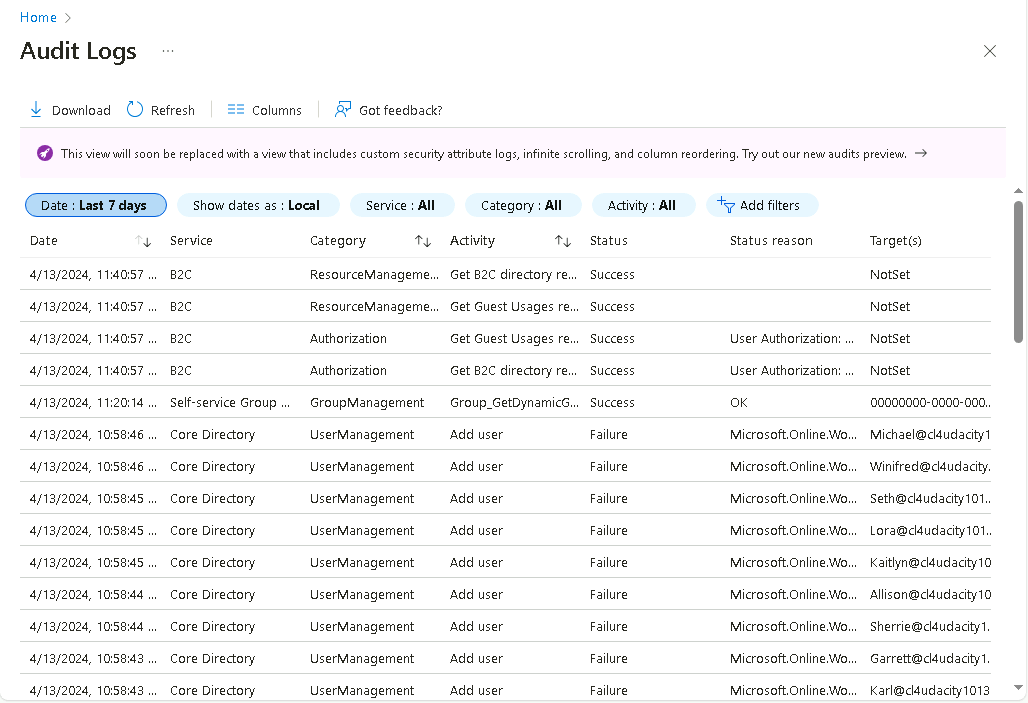
1. Proof of Azure SQL auditing with Log analytics (devdata,proddata)





1. Proof of Sentinel connectors (2+)





1. Login Log: The login log records information when a user logs into a system or application. It includes details such as the username, login timestamp, IP address, and whether the login attempt was successful or not. The login log helps in detecting unauthorized access attempts and troubleshooting authentication issues.

2. Access Log: The access log records information when a user accesses files, directories, or resources. It includes details like the username, access timestamp, and the location of the accessed file or resource. The access log helps in identifying unauthorized access attempts and permission-related issues.

3. Change Log: The change log records information about changes made to the system or application settings and configurations. It includes details such as the modified settings, the username of the user who made the change, and the timestamp of the change. The change log helps in identifying potential security issues and troubleshooting system-related issues.

**Compliance**

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

