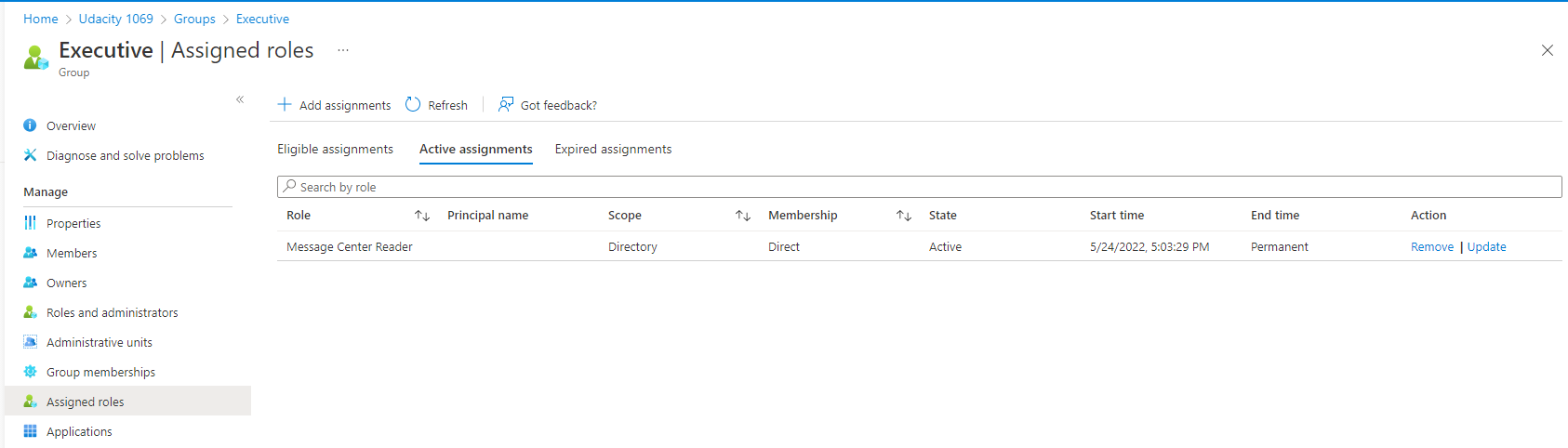
**Secure the Juice**

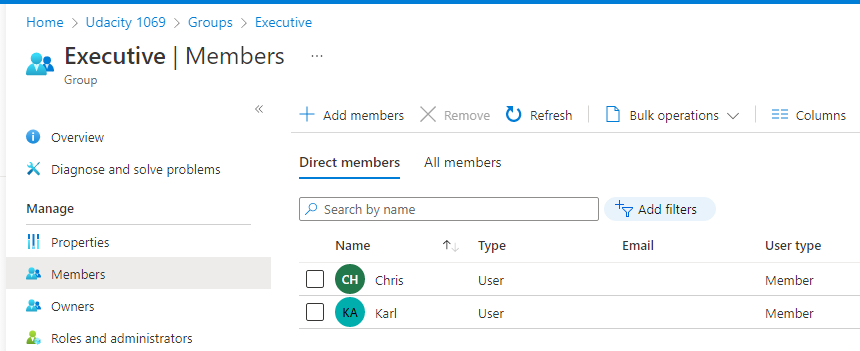
**Identity and Access Management**

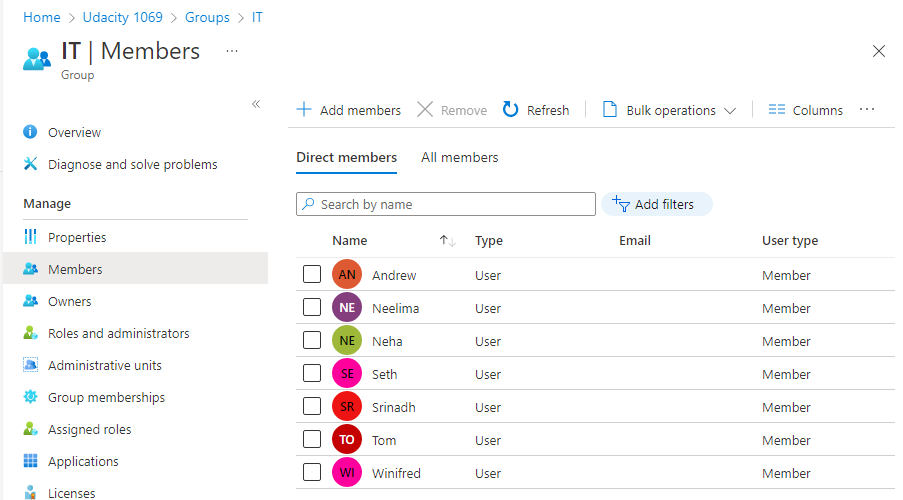
1. **Design authentication and authorization controls that manage access, role assignments, and identity**

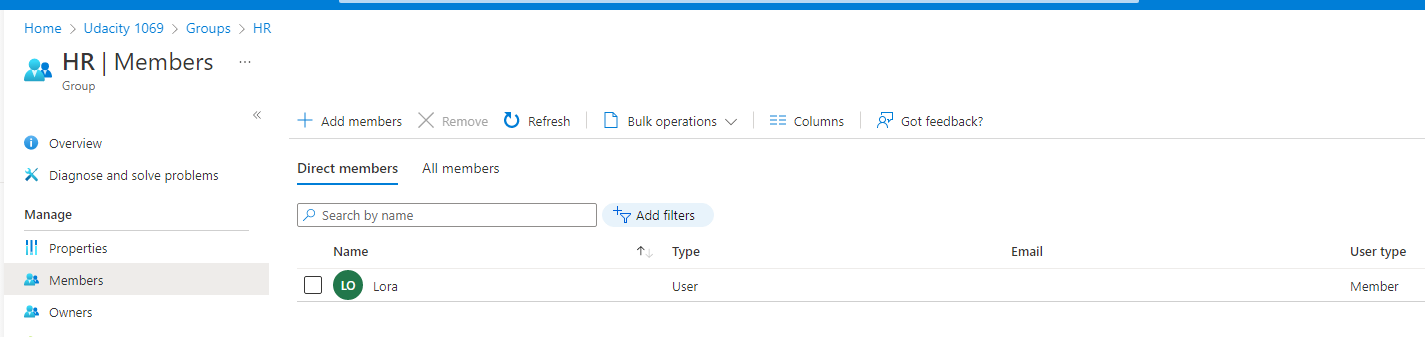
Proof of Assigned roles and AD assignments

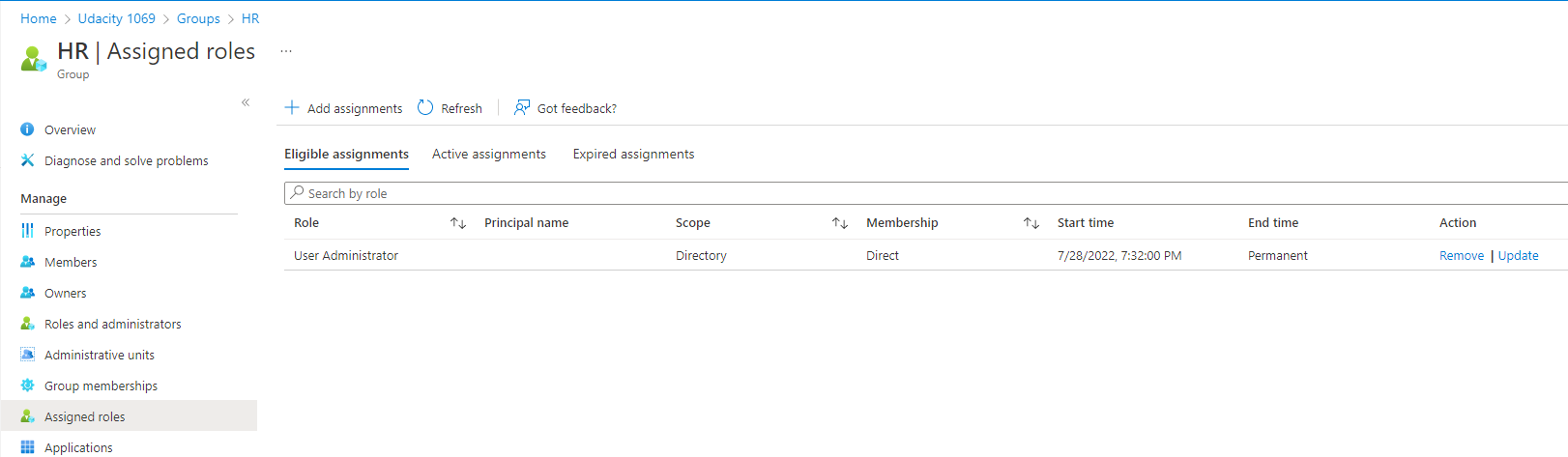
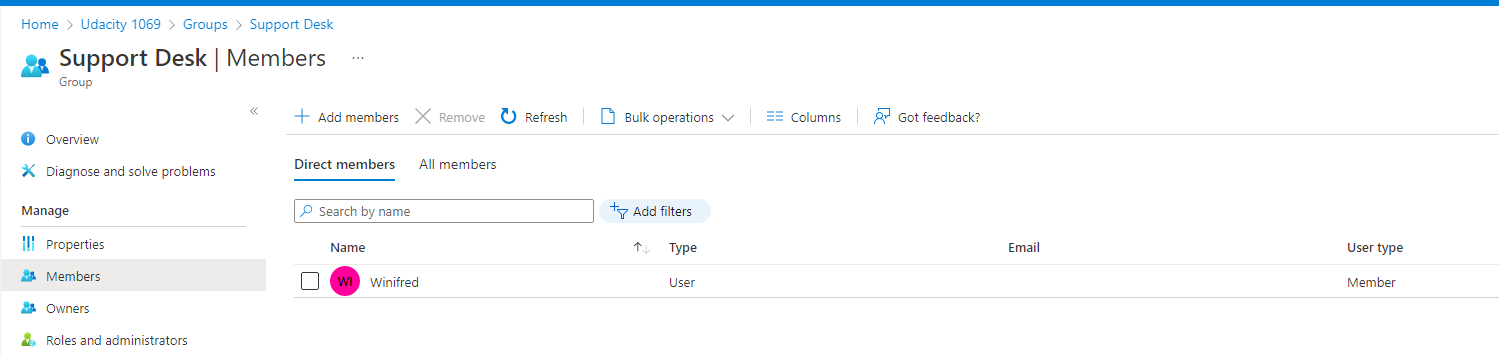
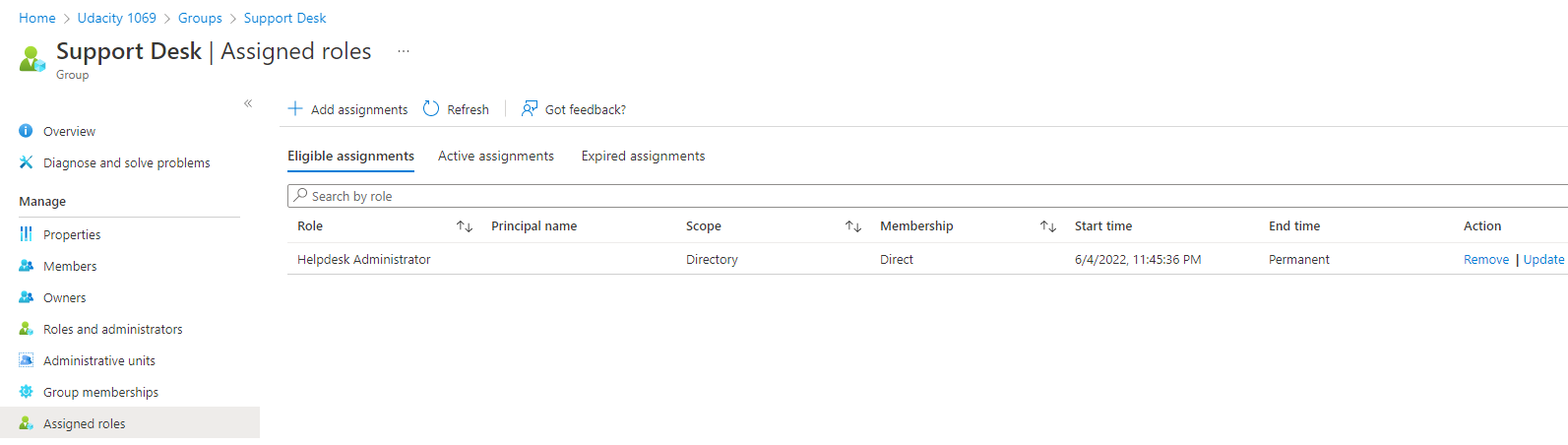
* 1. Andrew
  2. Chris
  3. Karl
  4. Lora
  5. Neelima
  6. Neha
  7. Seth
  8. Srinadh
  9. Tom
  10. Winifred
* Screenshot(s) that clearly display all Azure AD roles and Azure AD Assignments for all required users.

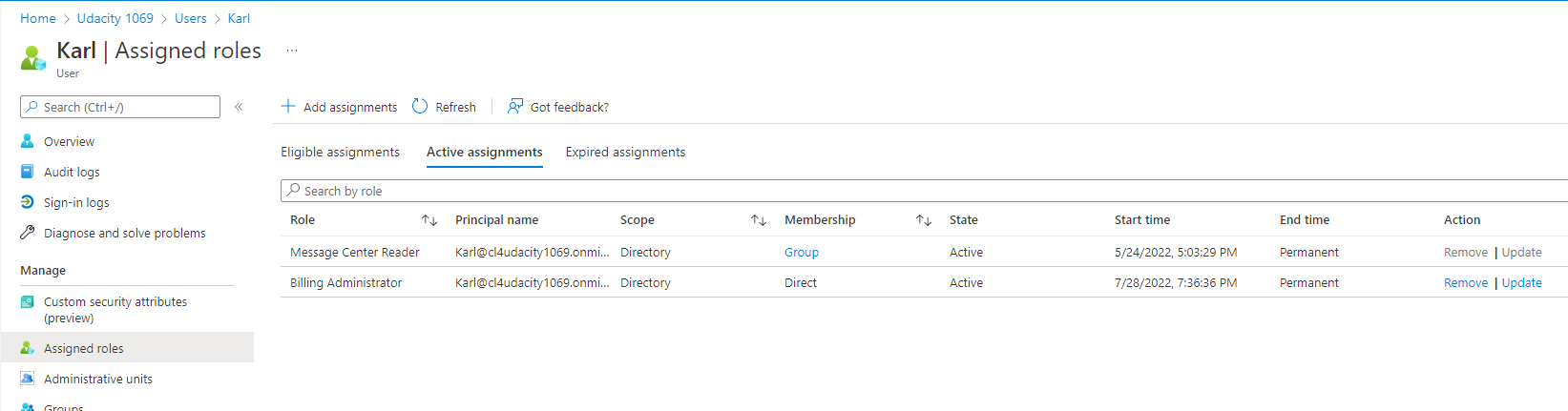


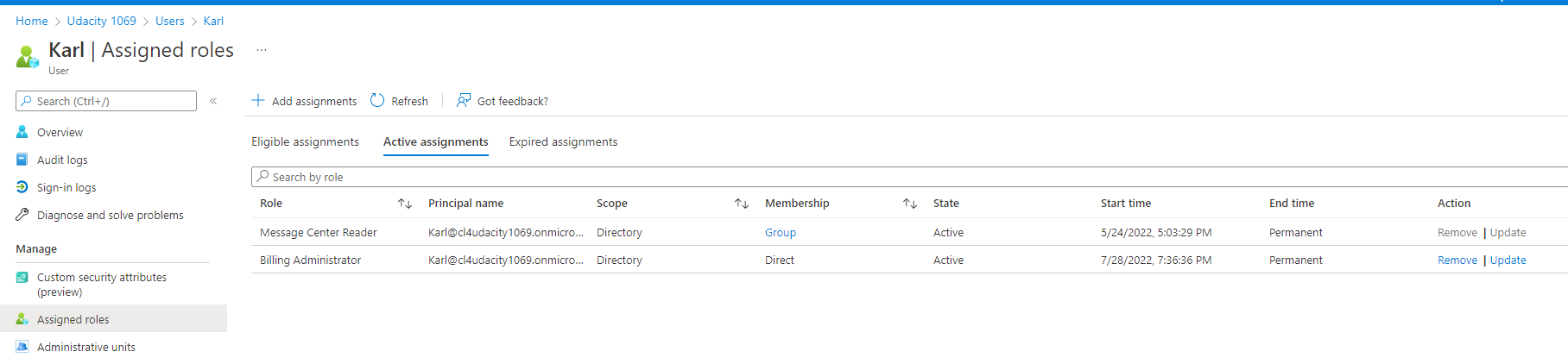


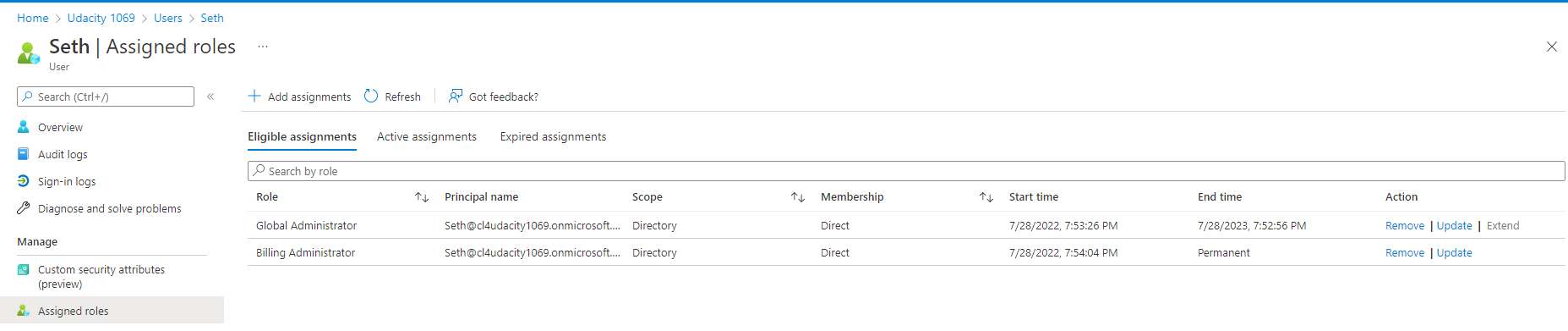


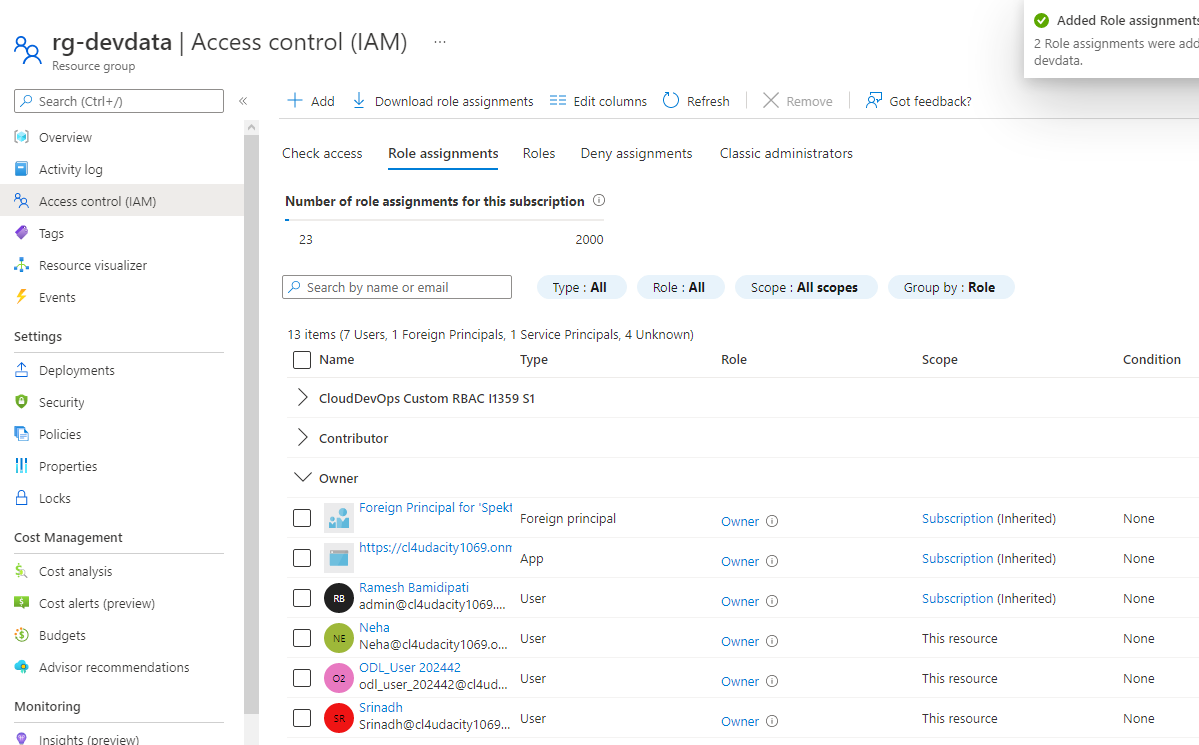


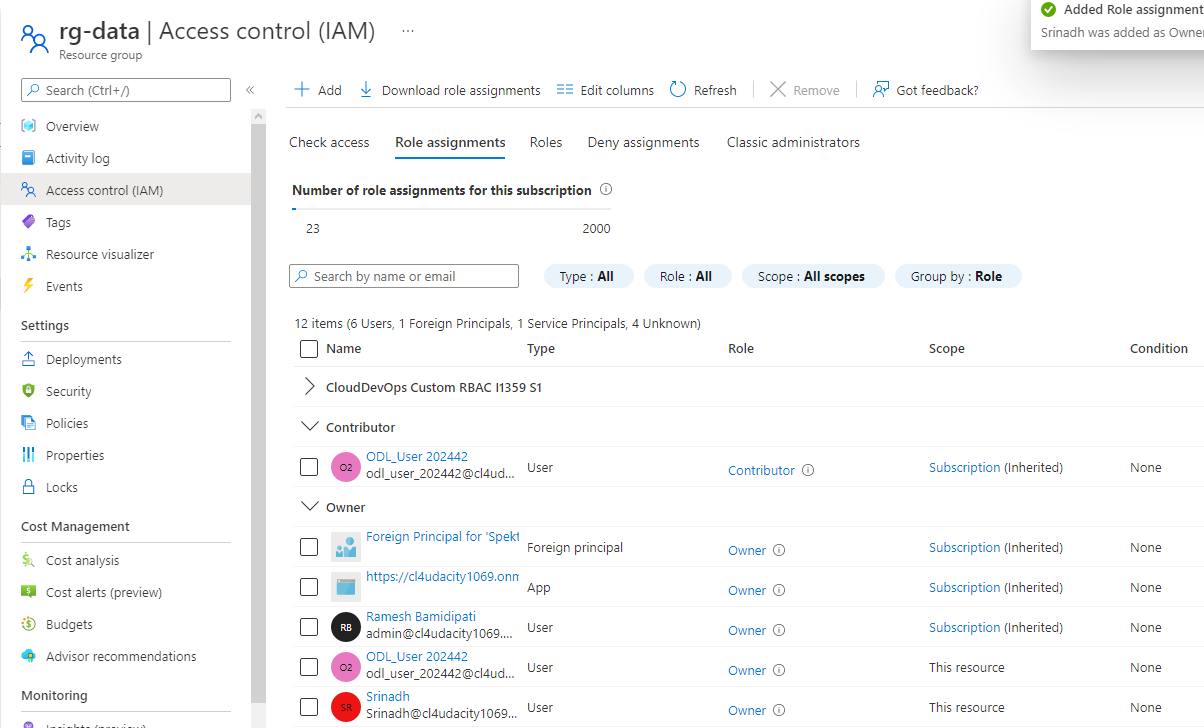


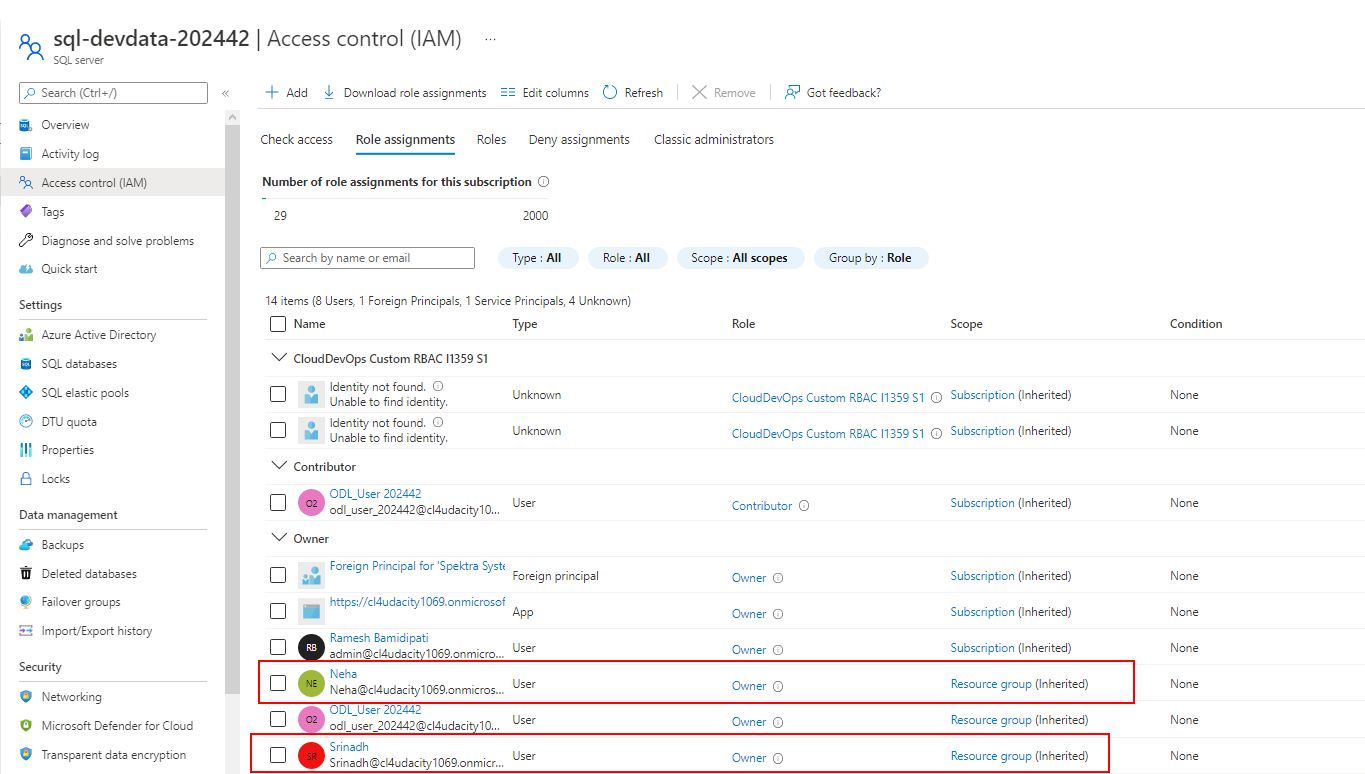


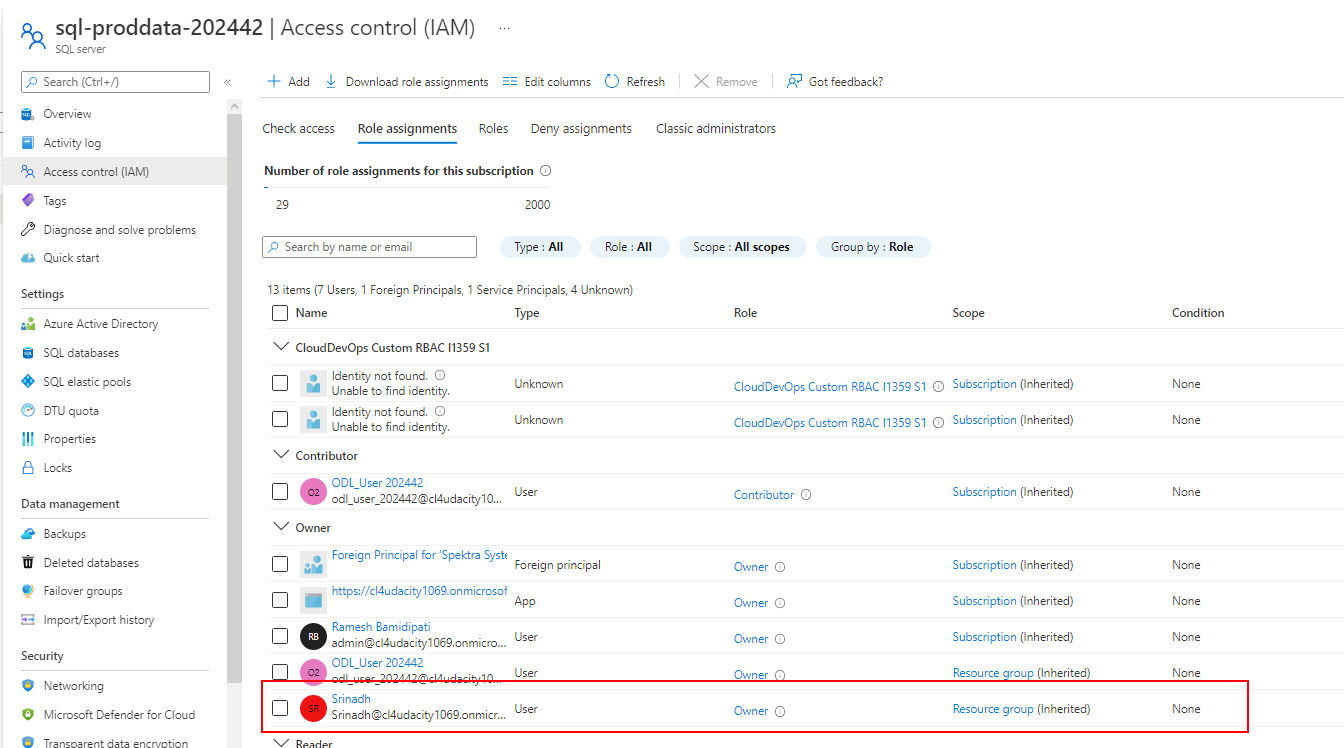


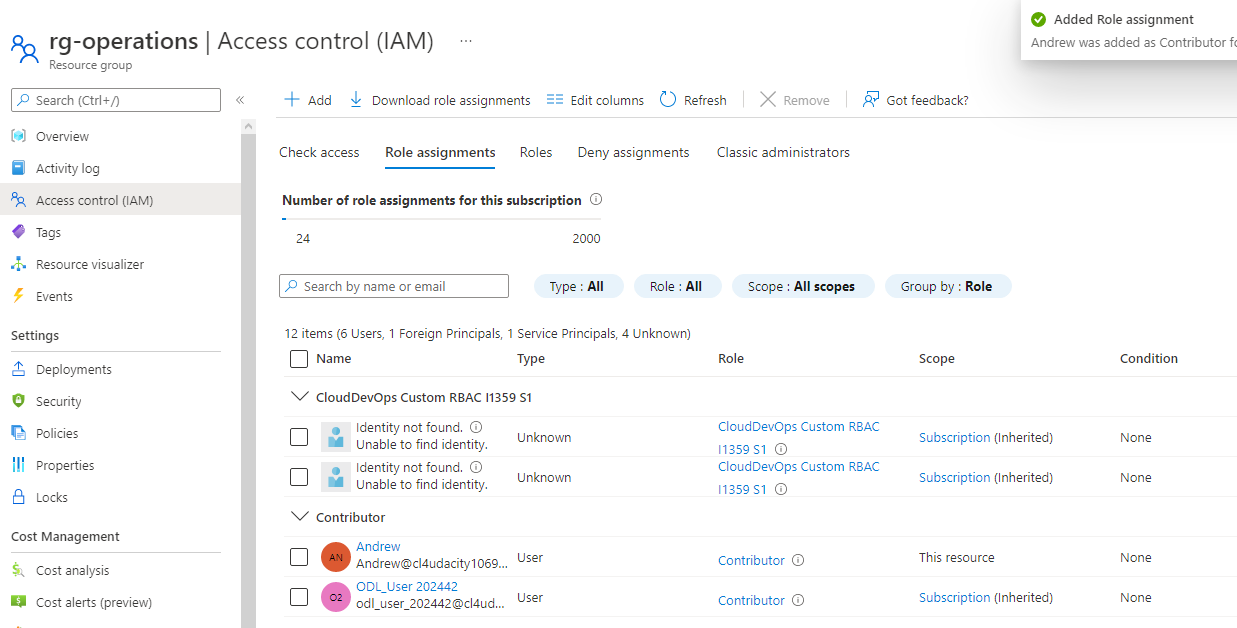


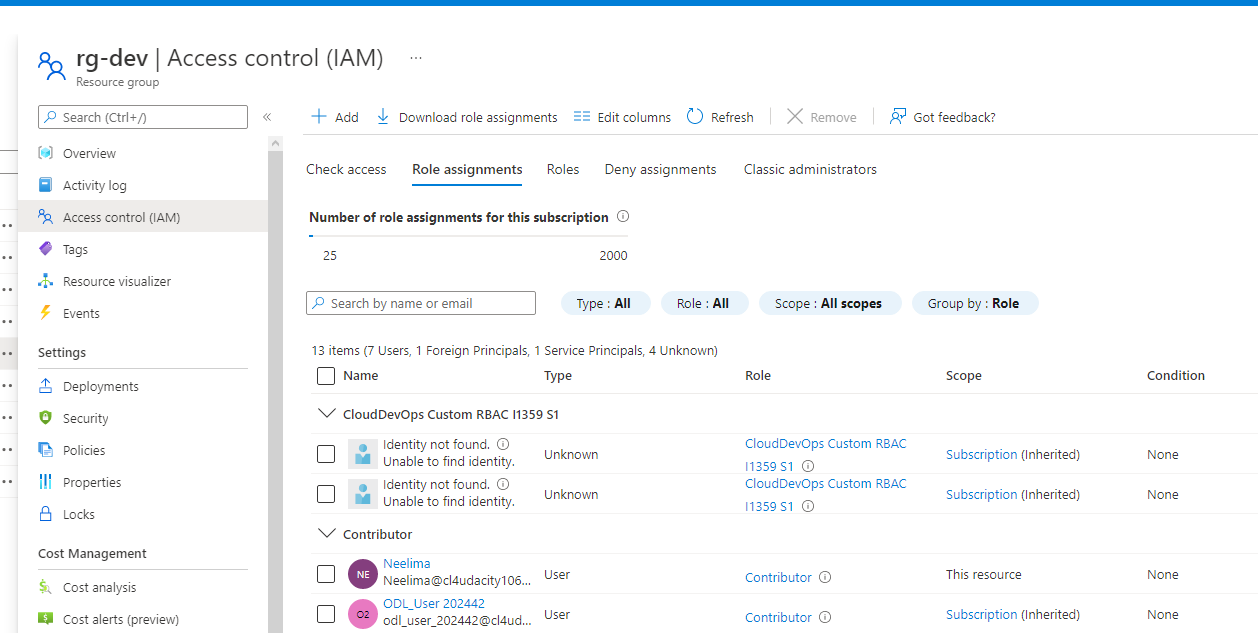
* Screenshot(s) that clearly displays Global Admin PIM screen showing duration, eligibility, and expiration.



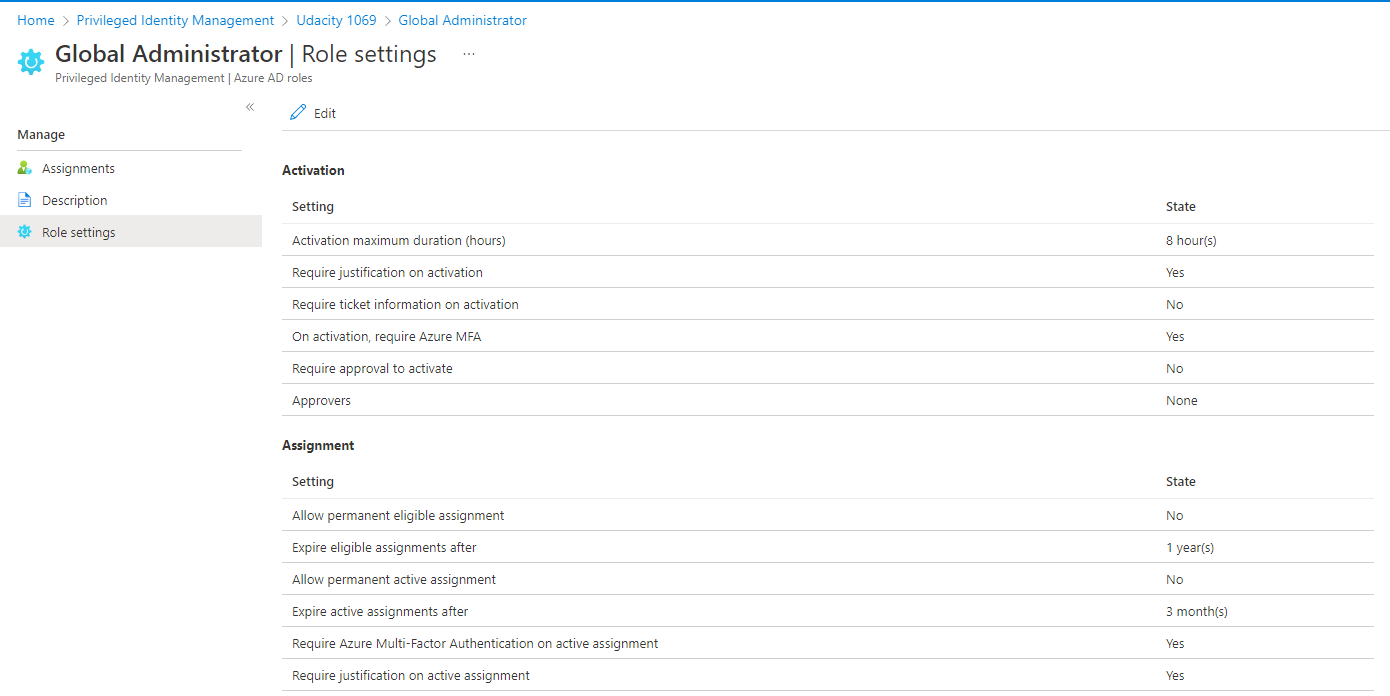






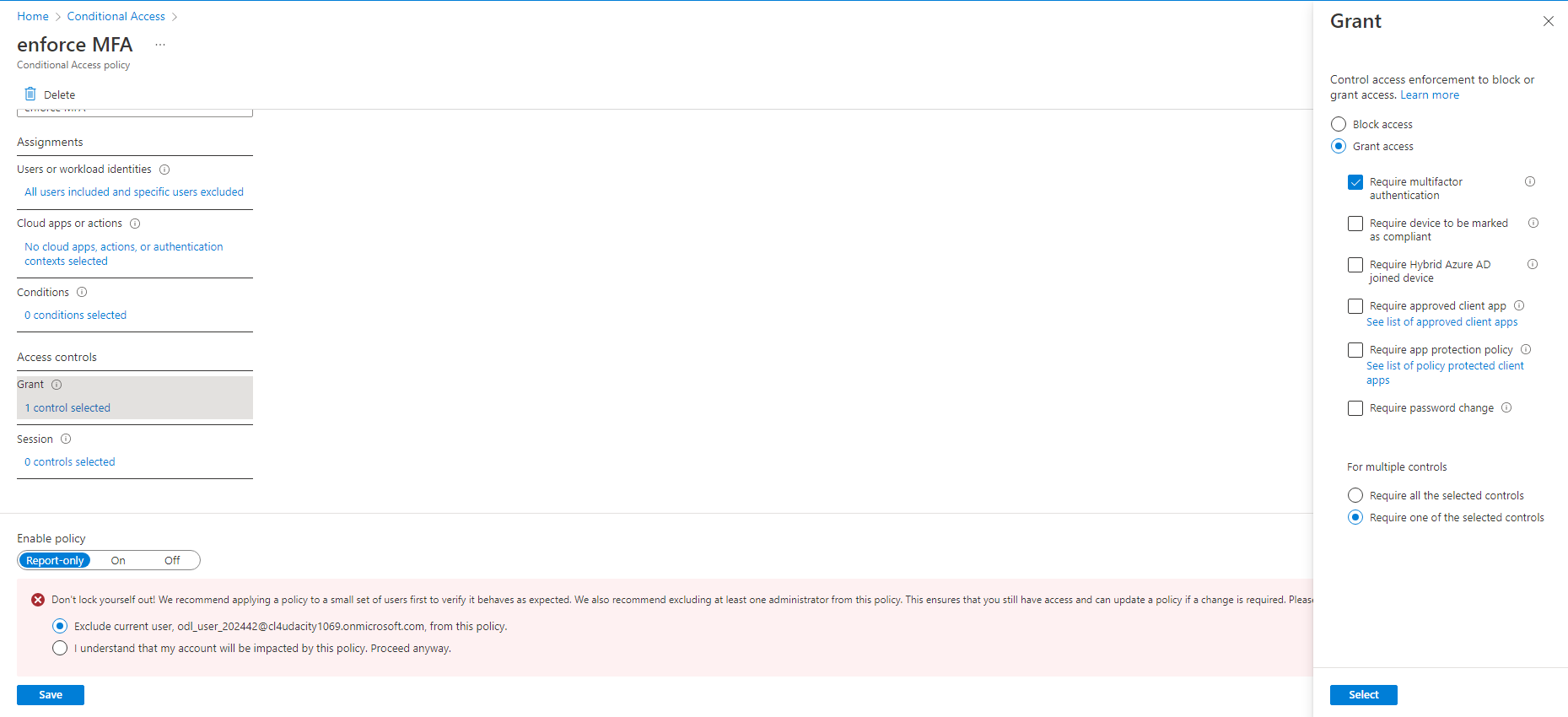


Proof of Global Administrator setting with duration, eligibility, expiration



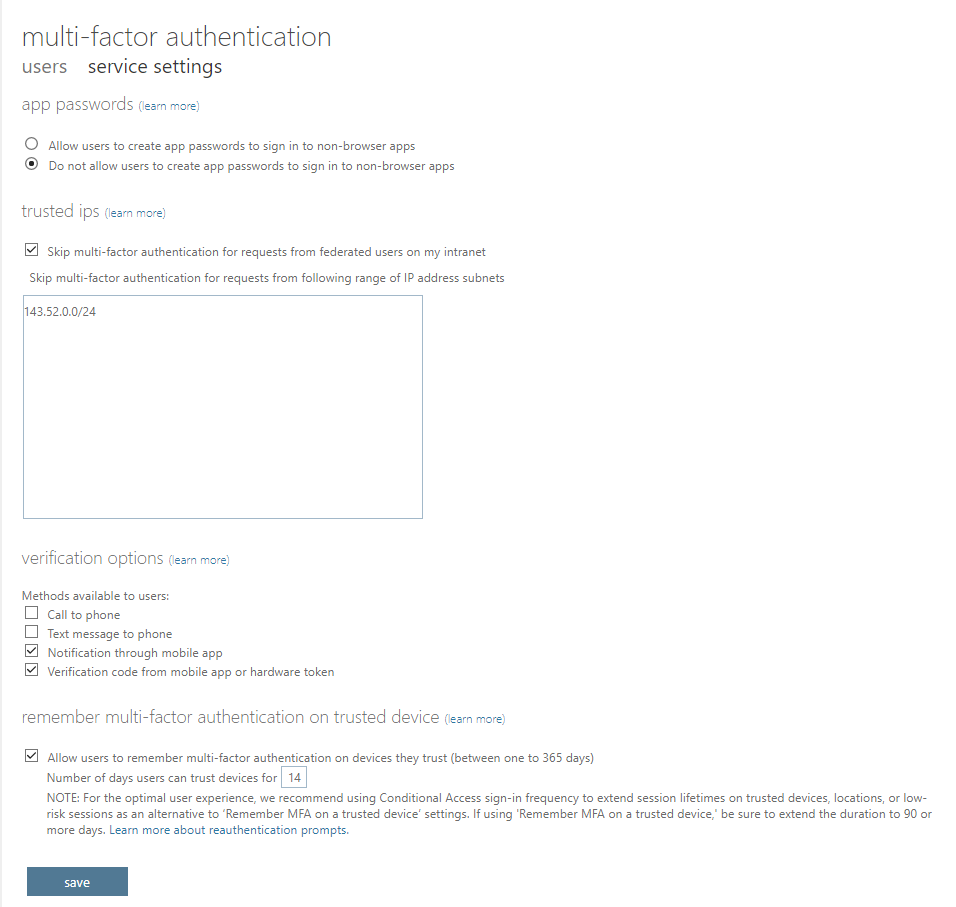
1. **Configure MFA and Conditional Access policies to require MFA for all users.**

* Screenshots of Conditional Access policy that clearly demonstrates that MFA has been configured for all users.



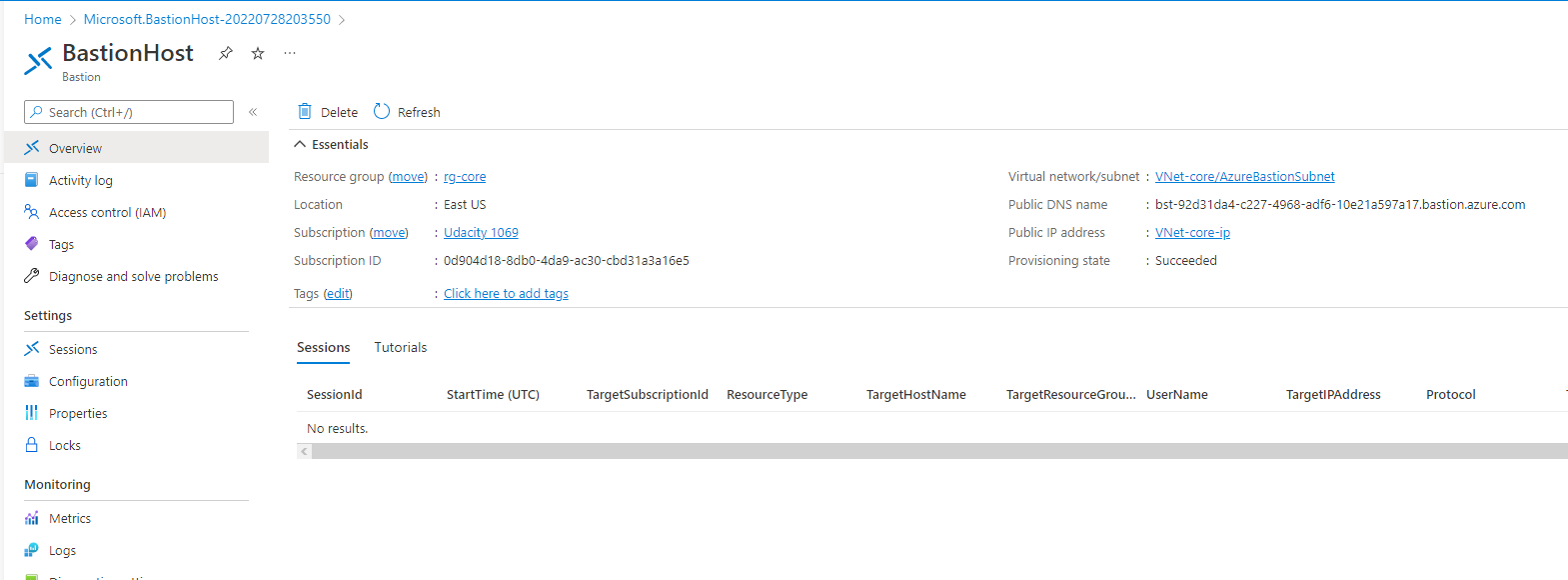
Screenshots of Multi-Factor authentication configuration pages that clearly demonstrate the stated requirements here:

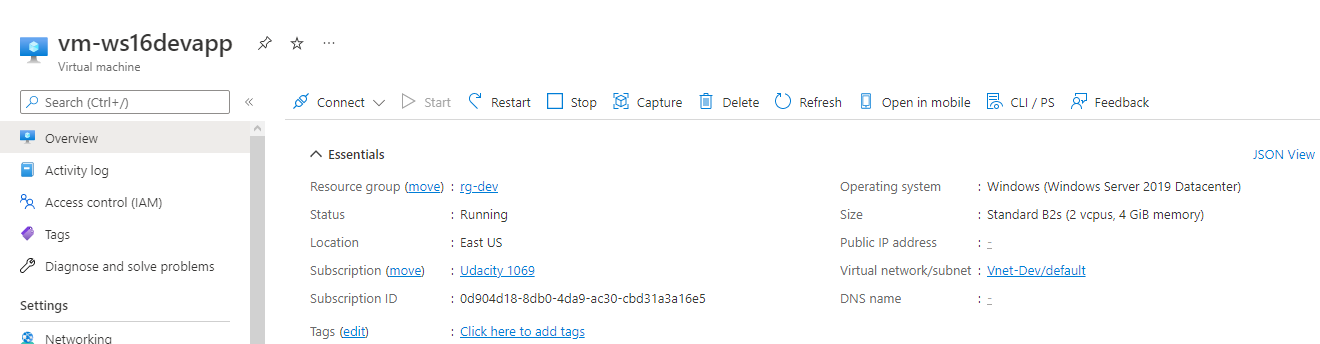
* MFA tokens should expire every 14 days.
* The Charlotte office is considered a trusted site
* MFA should not be required in the Charlotte Office.
* The Charlotte office has an IP address range of 143.52.0.0/24

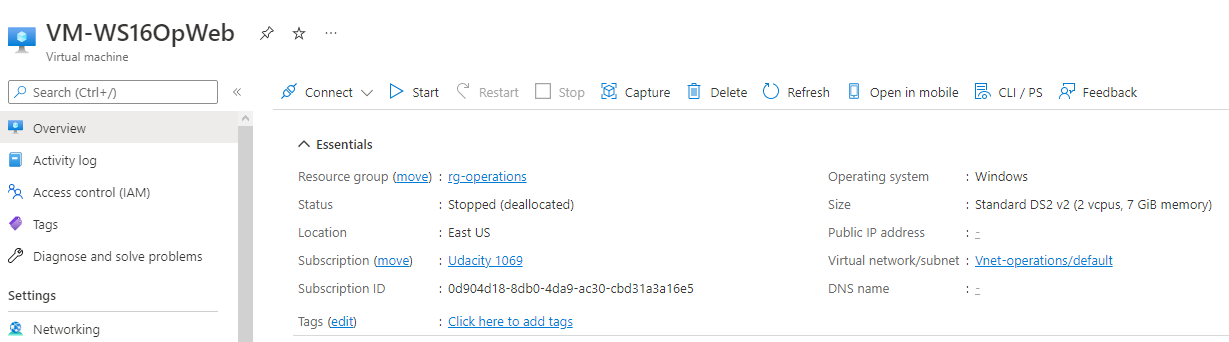


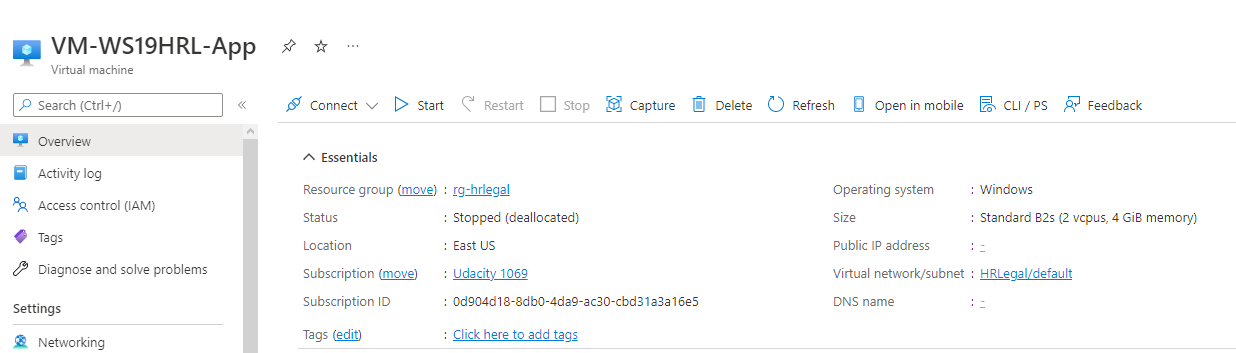
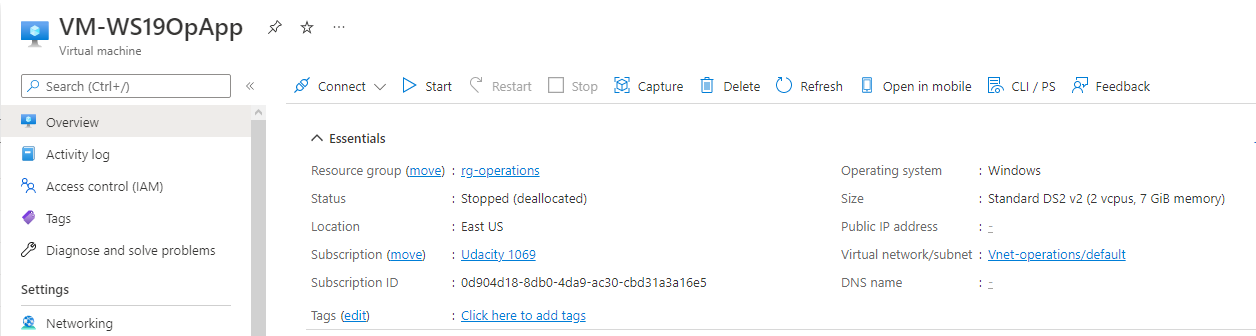
**Network Security**

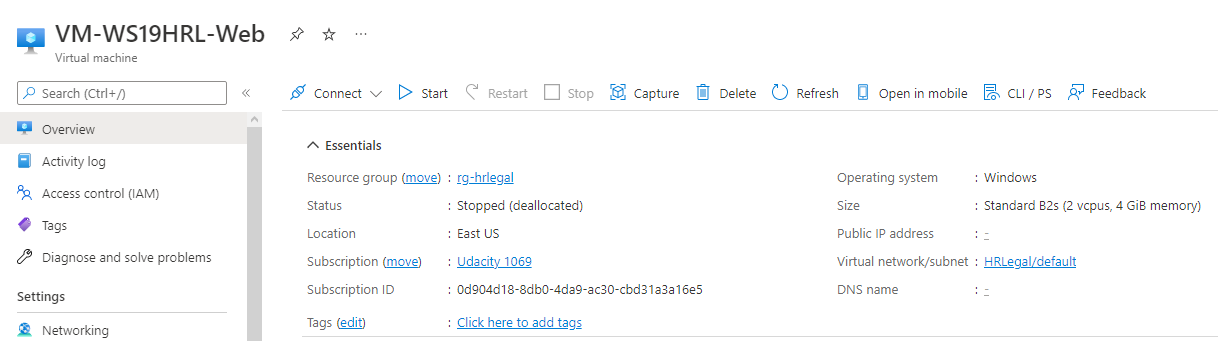
1. **Configure Azure Bastion to allow secure connectivity from the Azure Portal to the Azure Virtual machines.**

Screenshot of the Bastion Overview page should indicate the virtual network/subnet. Placed correctly, only one Bastion will be needed.



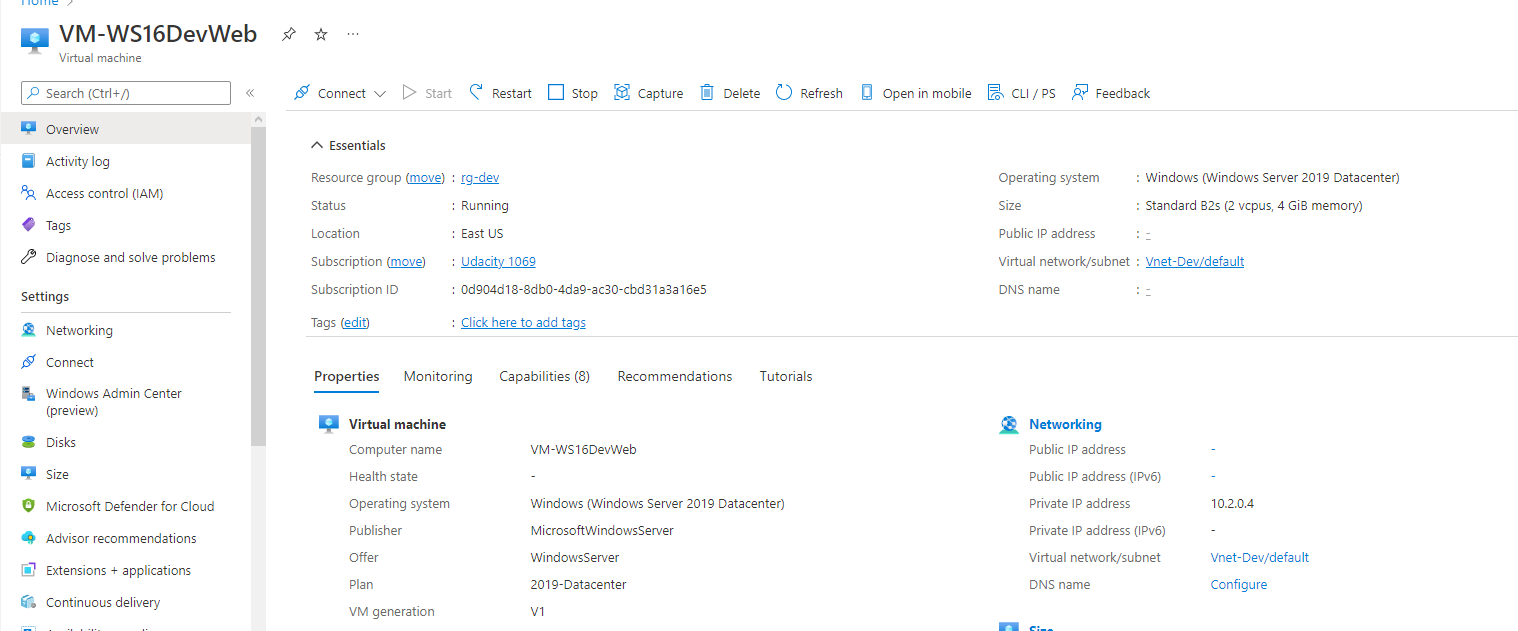






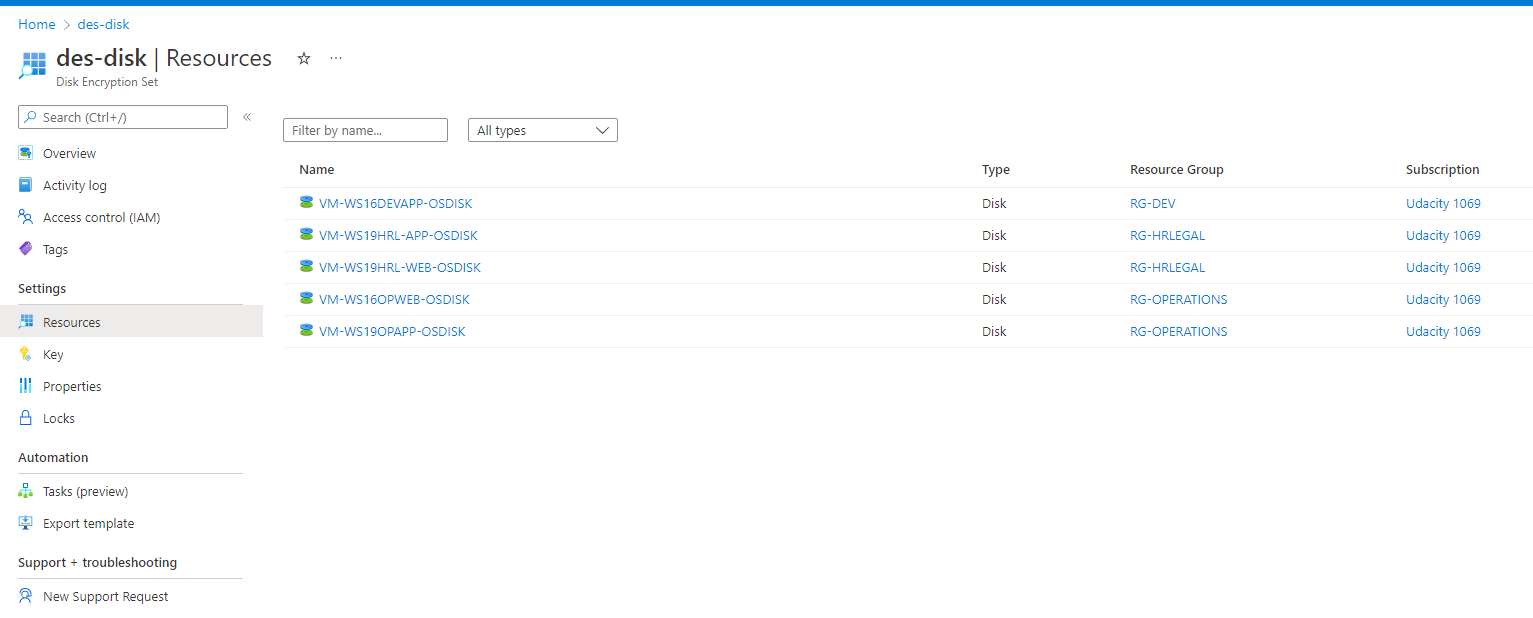
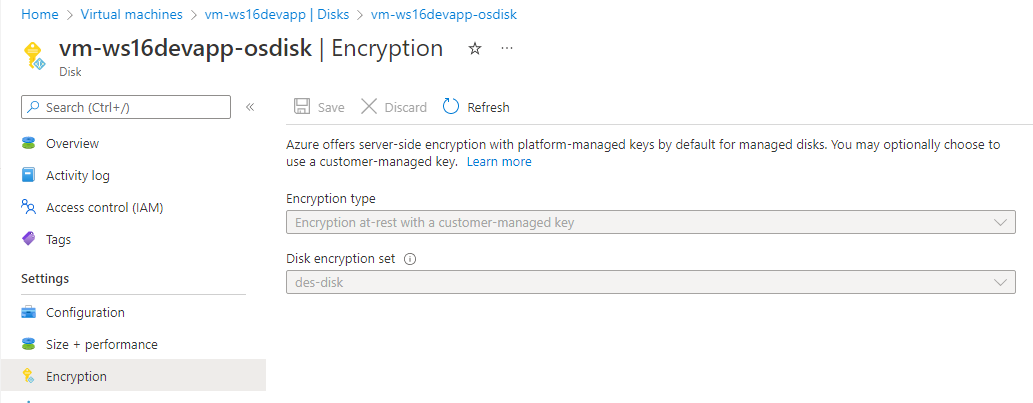
1. **Reduce attack footprint by removing public IP addresses.**

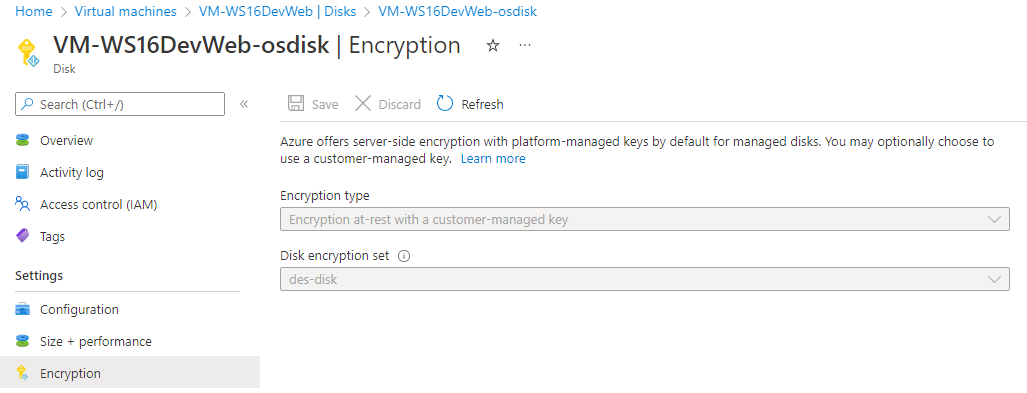
The screenshot clearly shows public IP address is blank for each VM

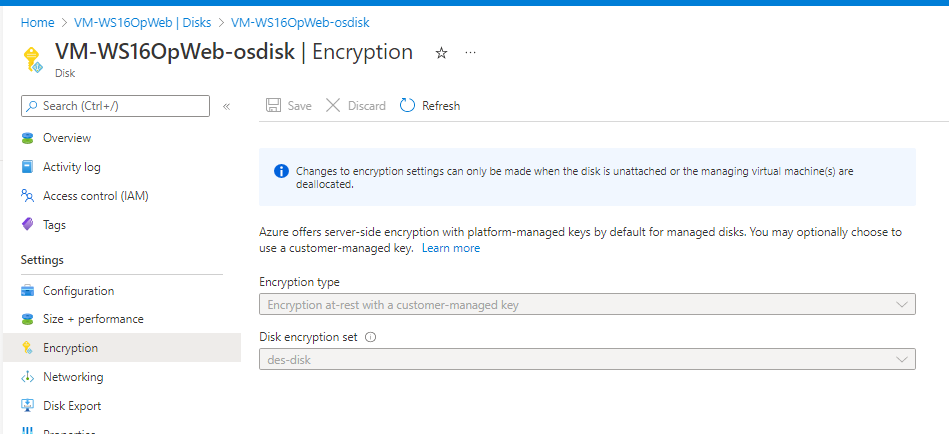
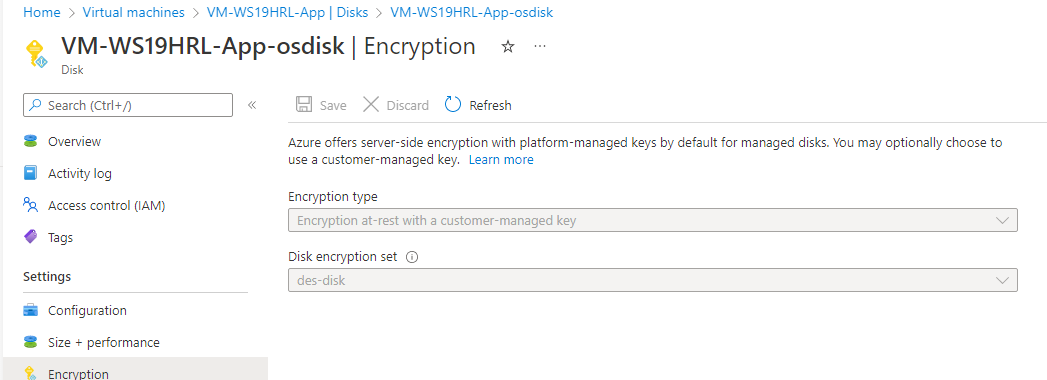


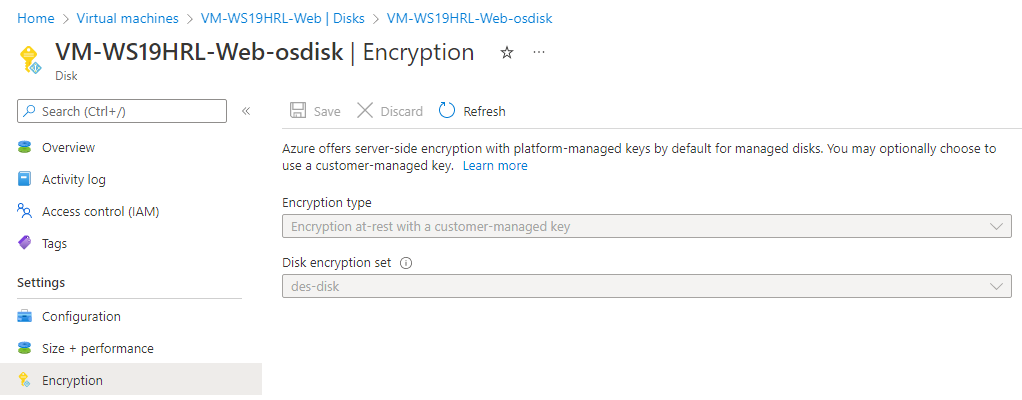
**Data and Encryption**

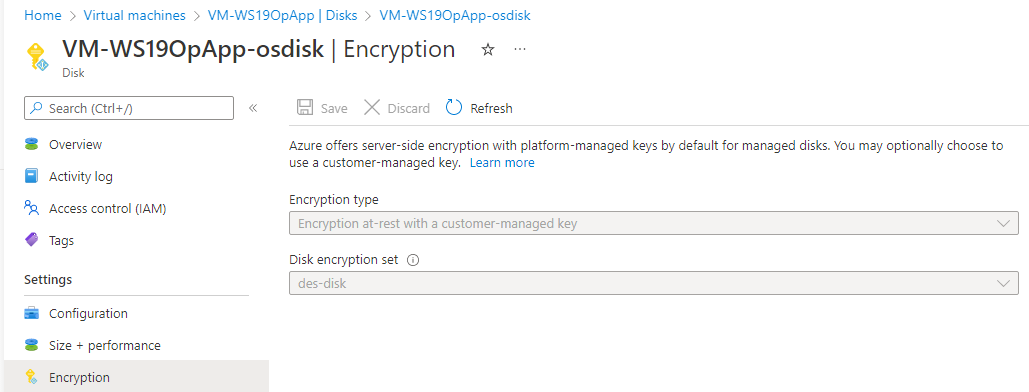
1. **Protect data at rest by encrypting data disks using a customer-managed key**

Screenshots should show the disk encryption type for each VM.



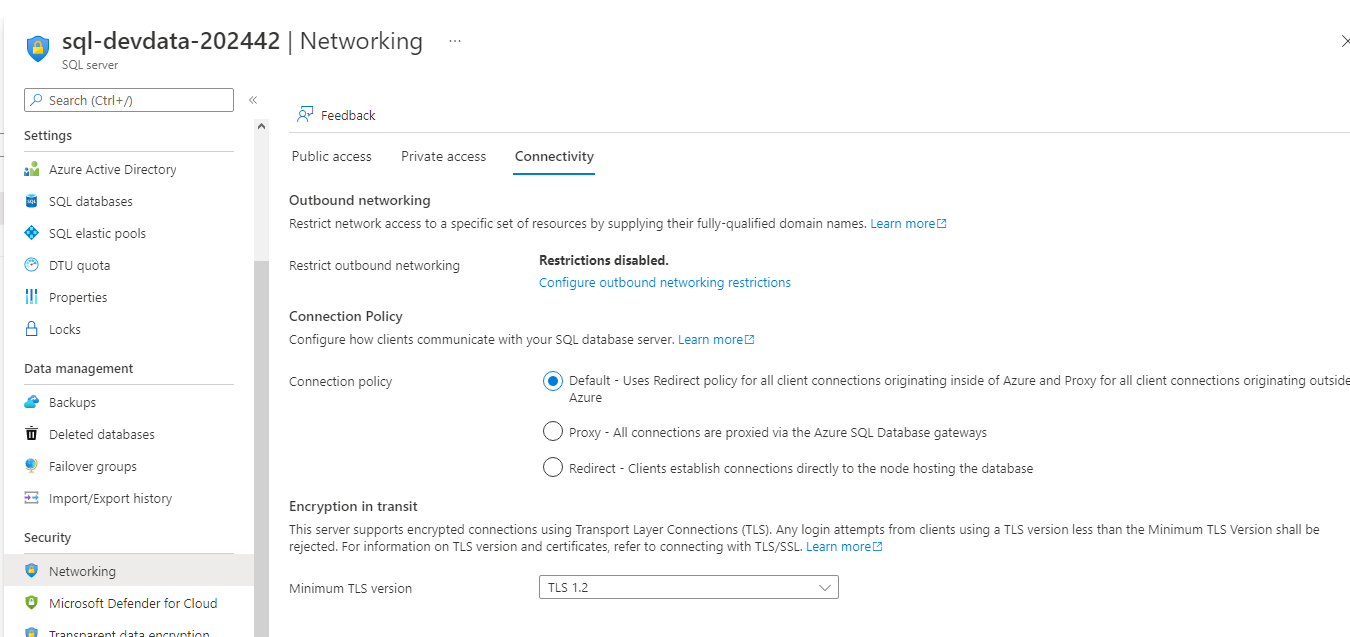


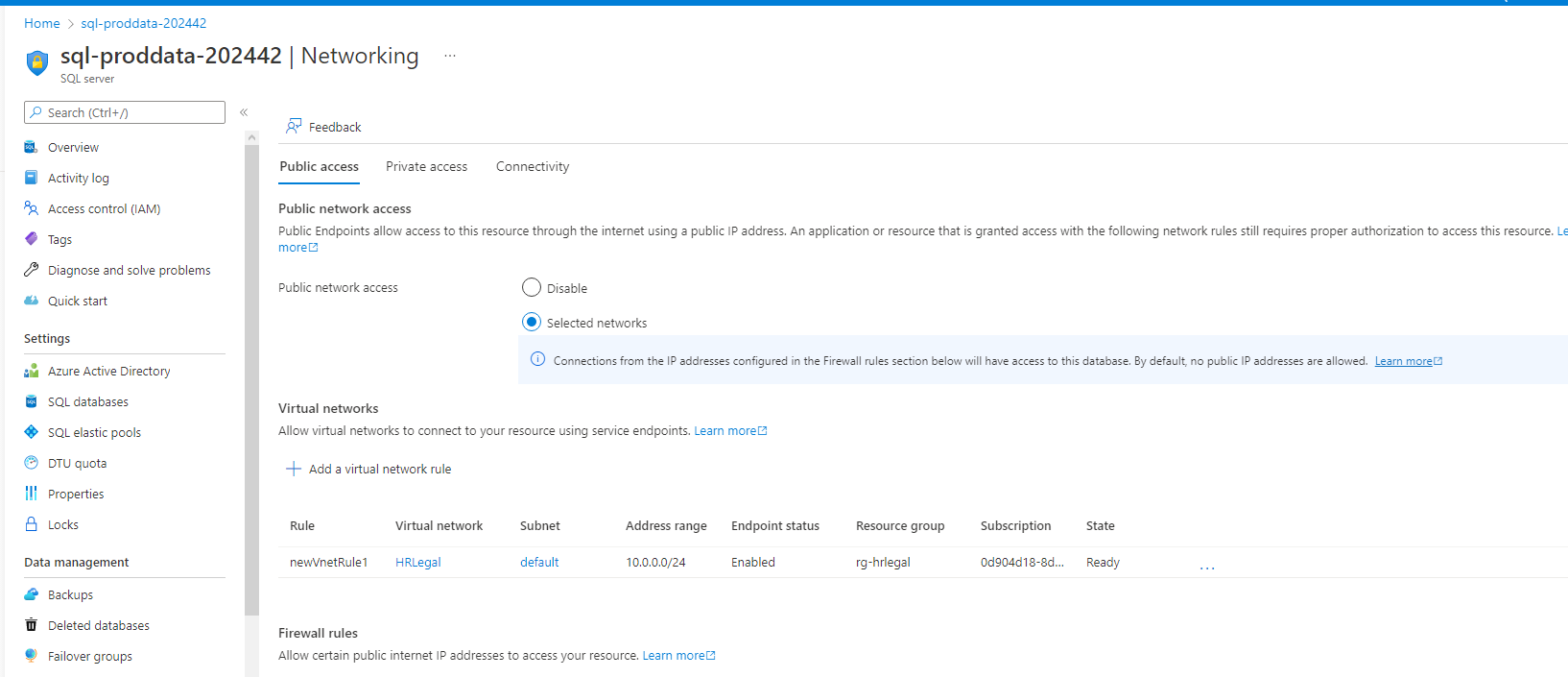
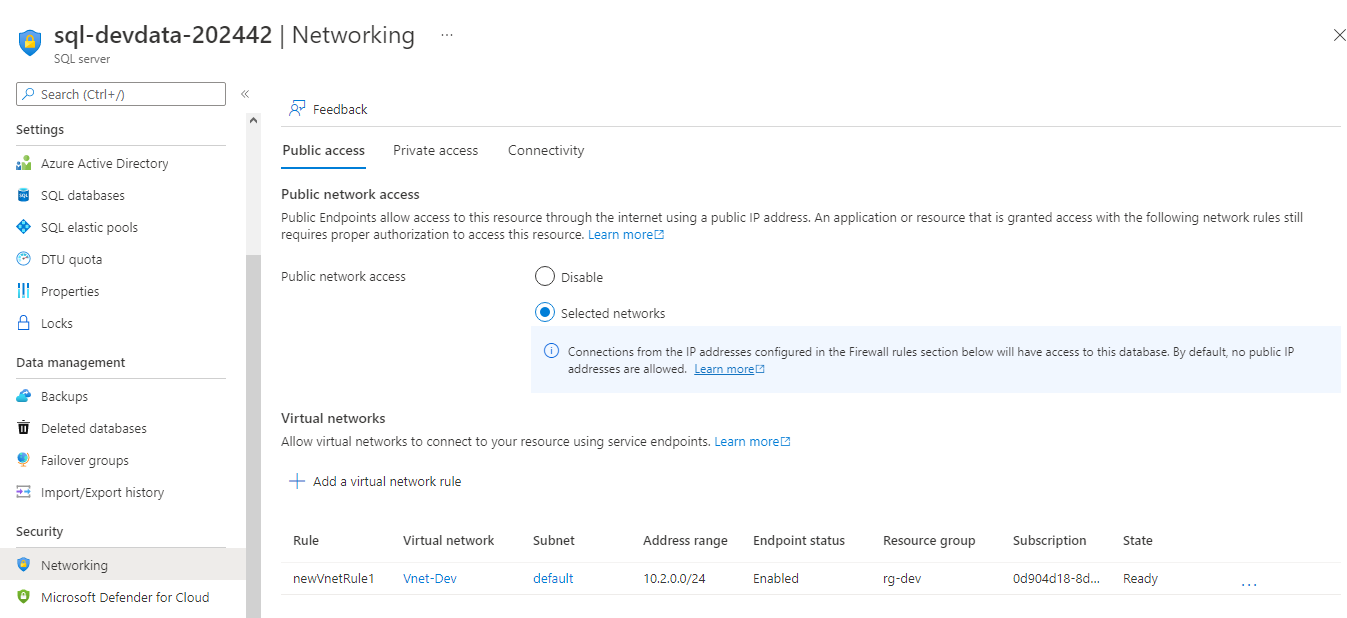


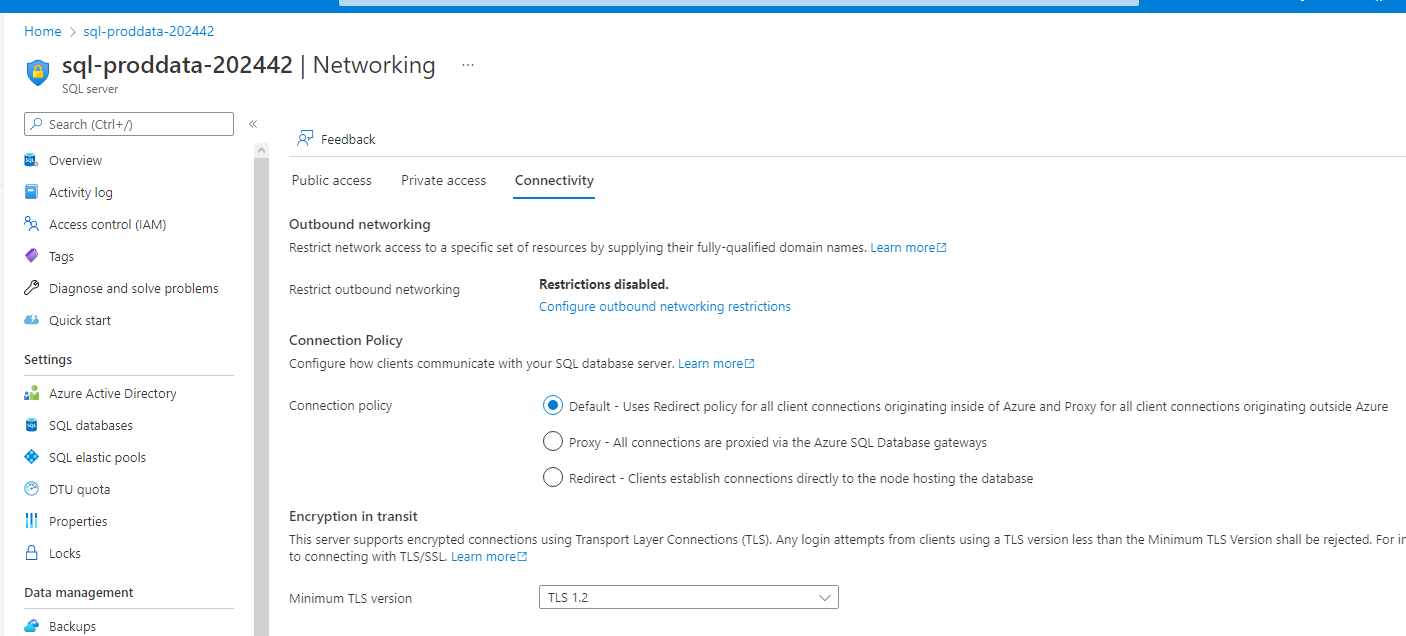


1. **Secure traffic to SQL servers and databases by limiting public network access, enforcing TLS minimum requirements, and setting allowed IPs or network requirements**

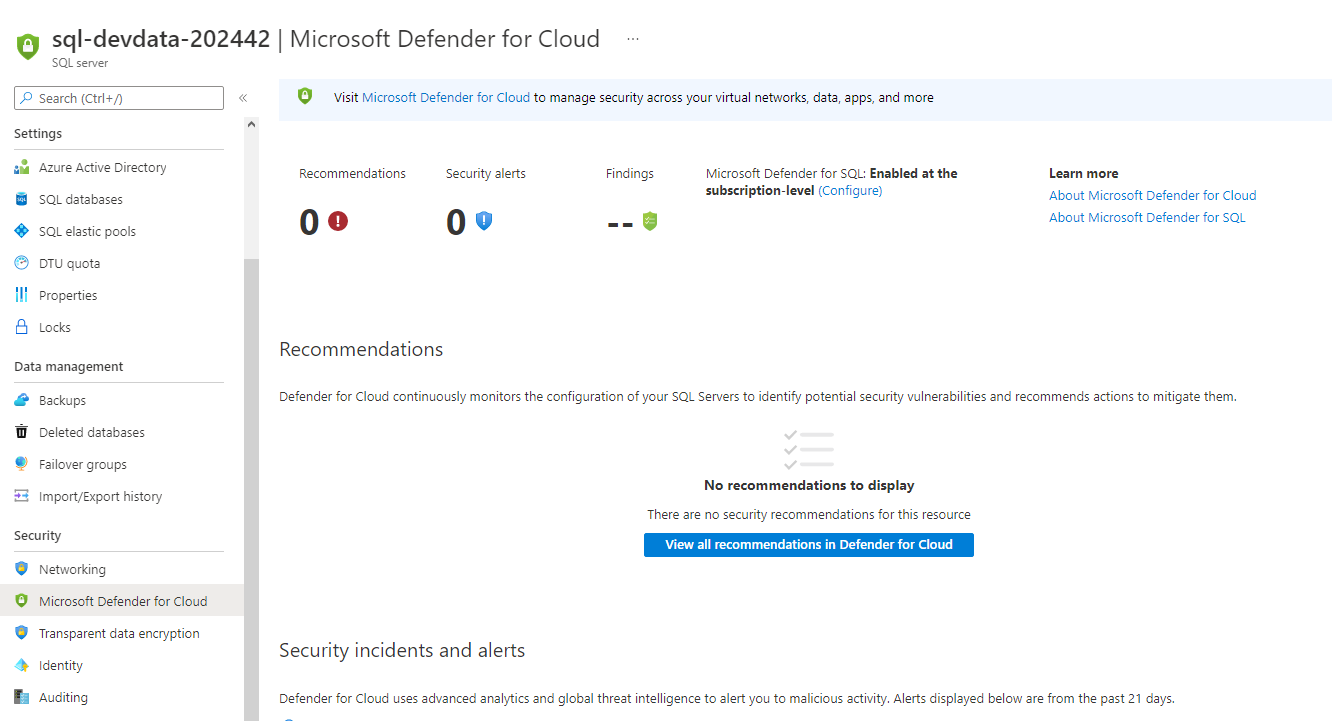
A screenshot of the Firewalls and Virtual networks page for SQL servers that clearly shows the required configuration for no public access and TLS

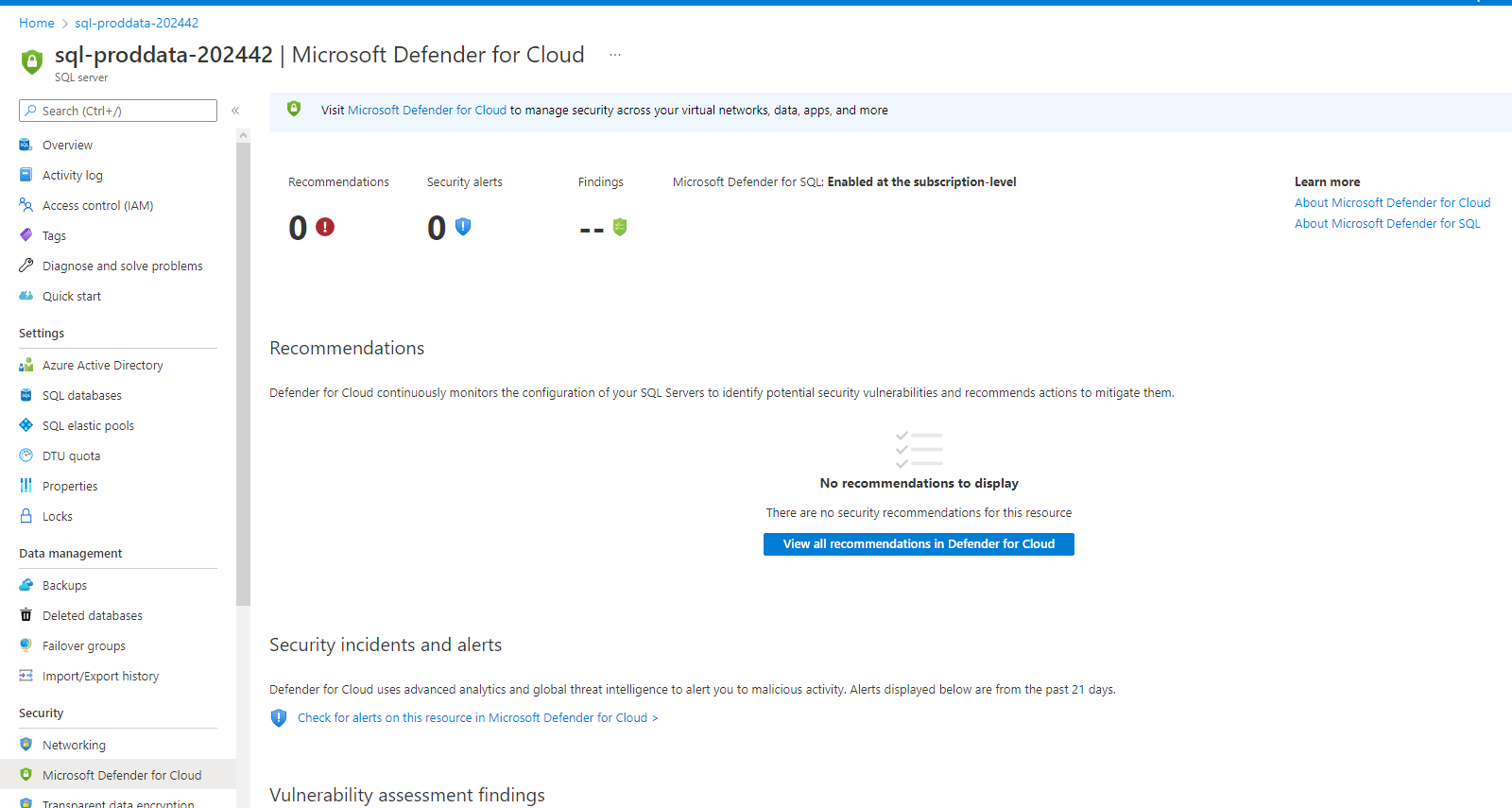






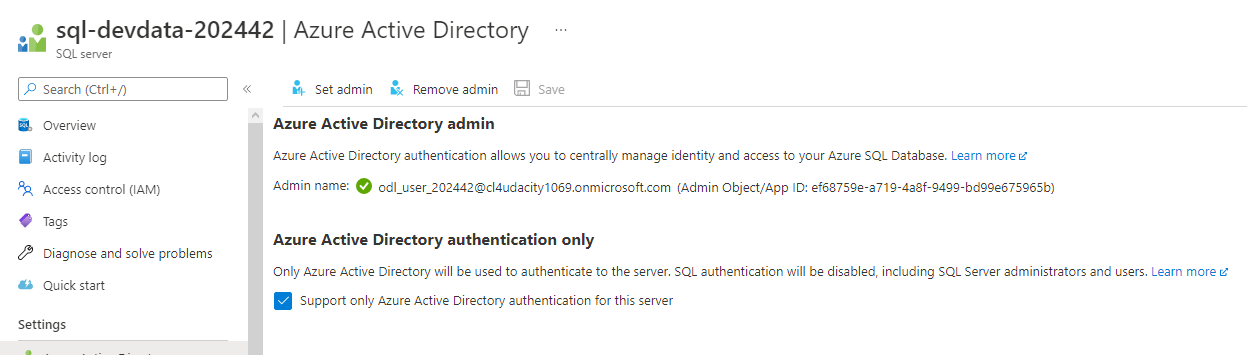
1. **Protect SQL data by enabling Azure Defender for SQL.**

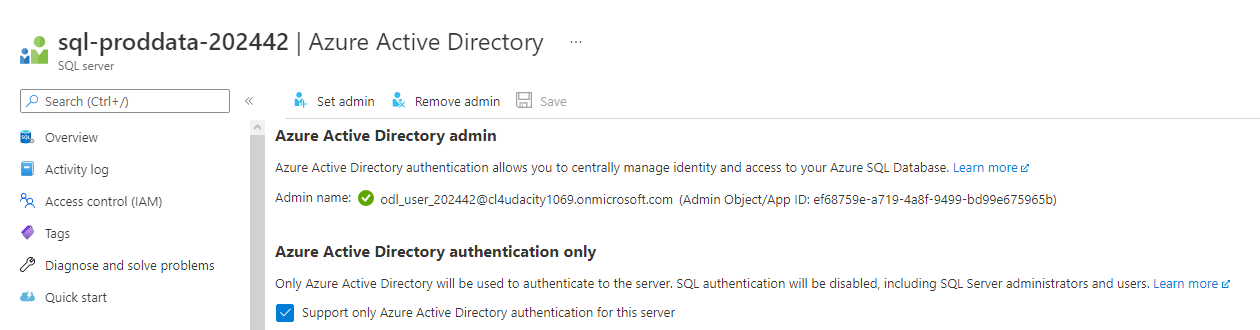
Screenshot that shows Azure Defender for SQL is enabled.



1. **Secure Azure SQL by enforcing Azure AD authentication over the weaker SQL authentication methods.**

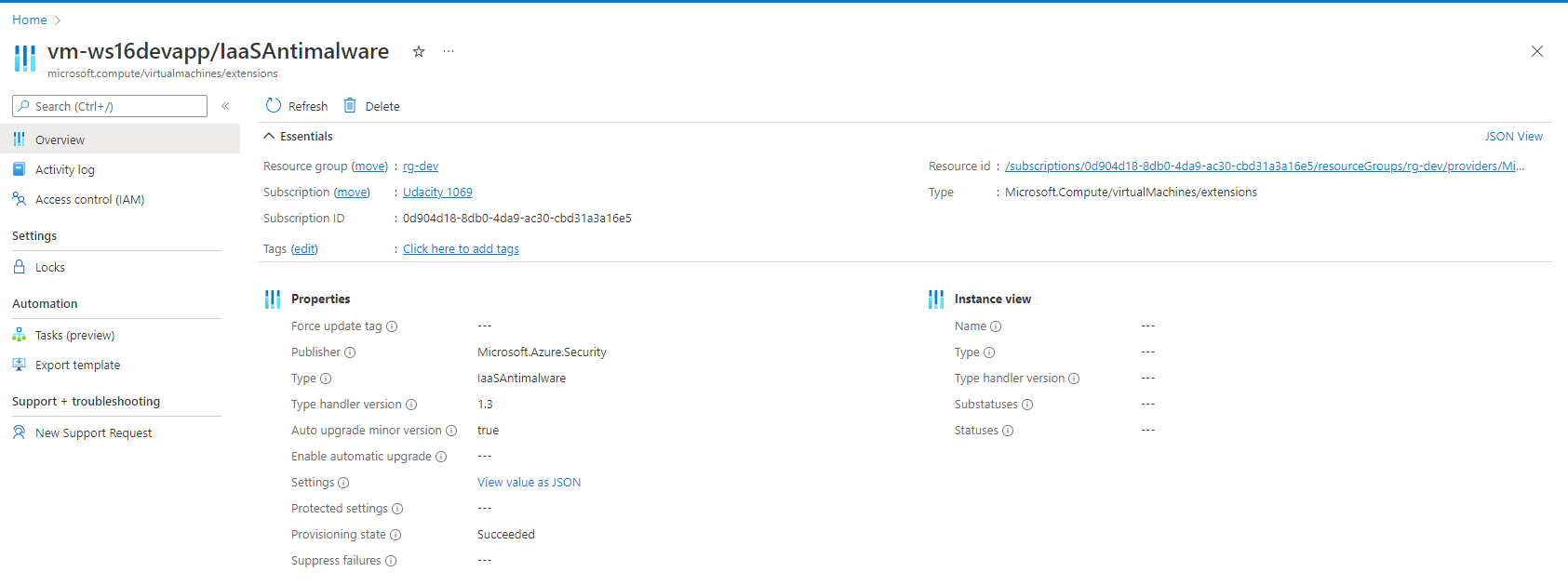
Show screenshot of Azure AD authentication for SQL enabled

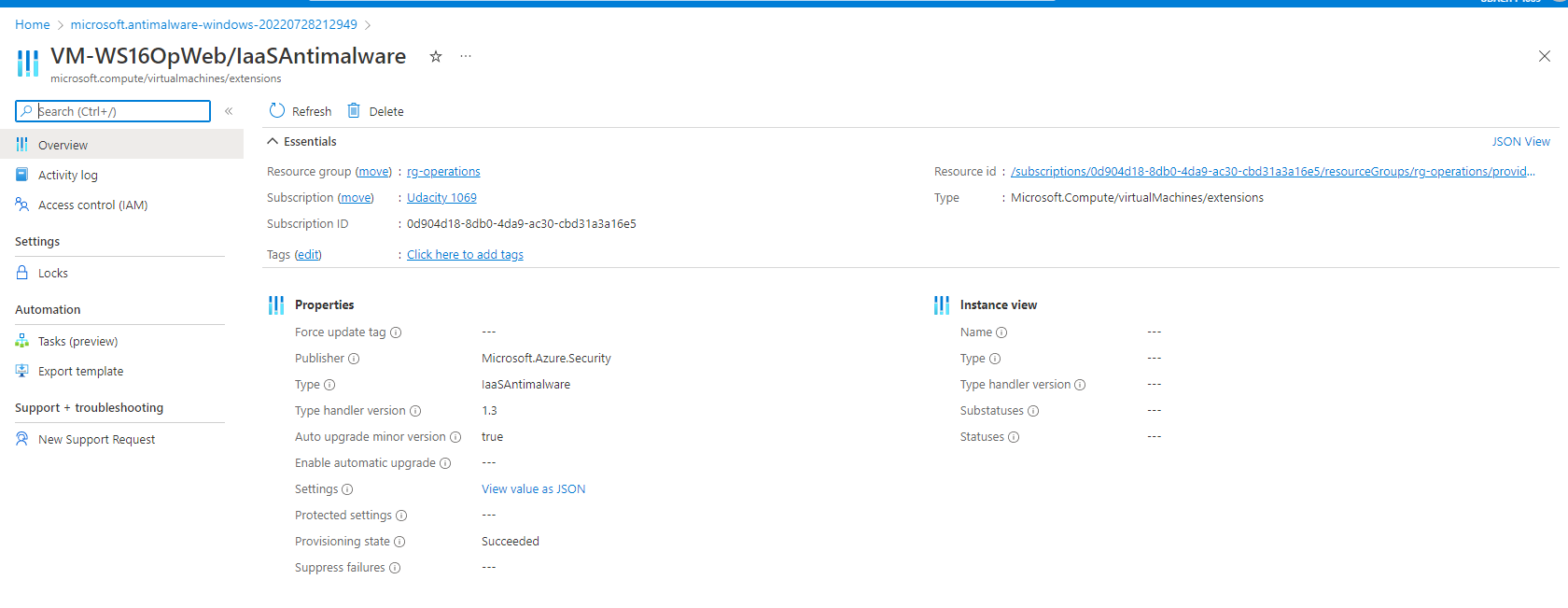
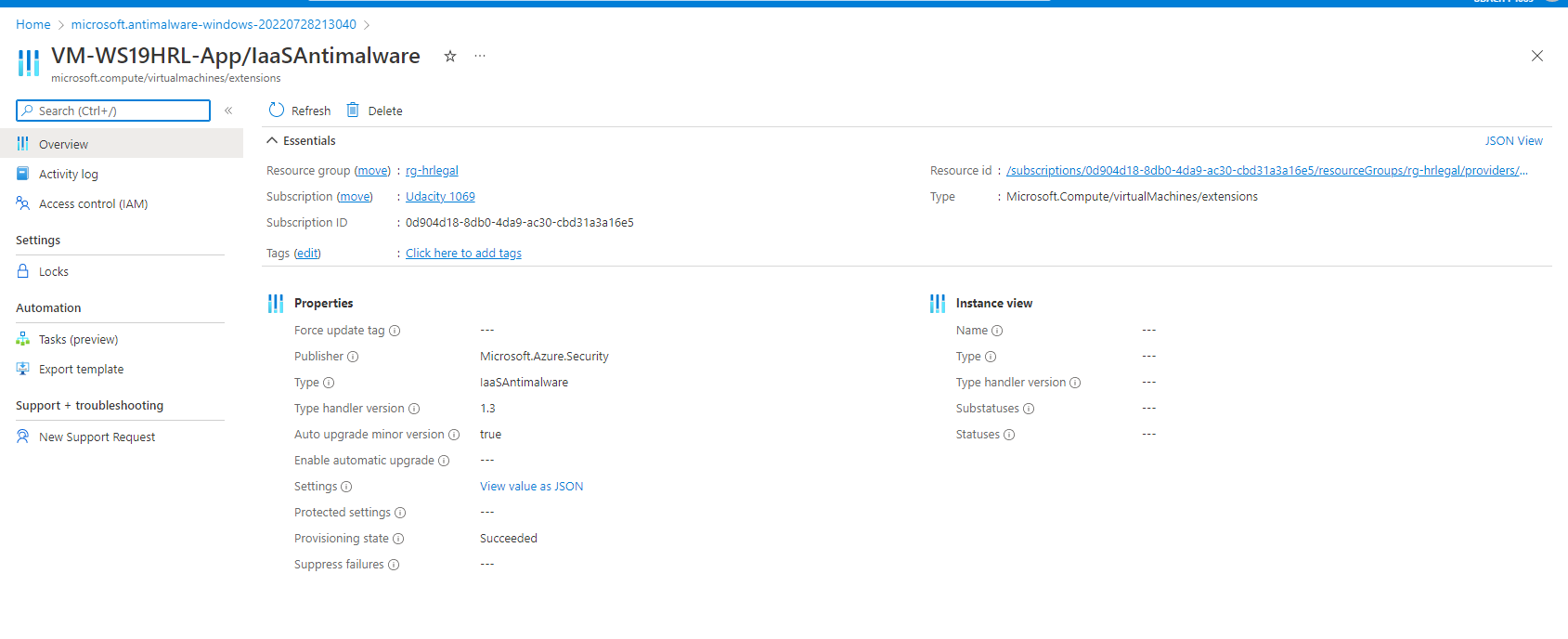


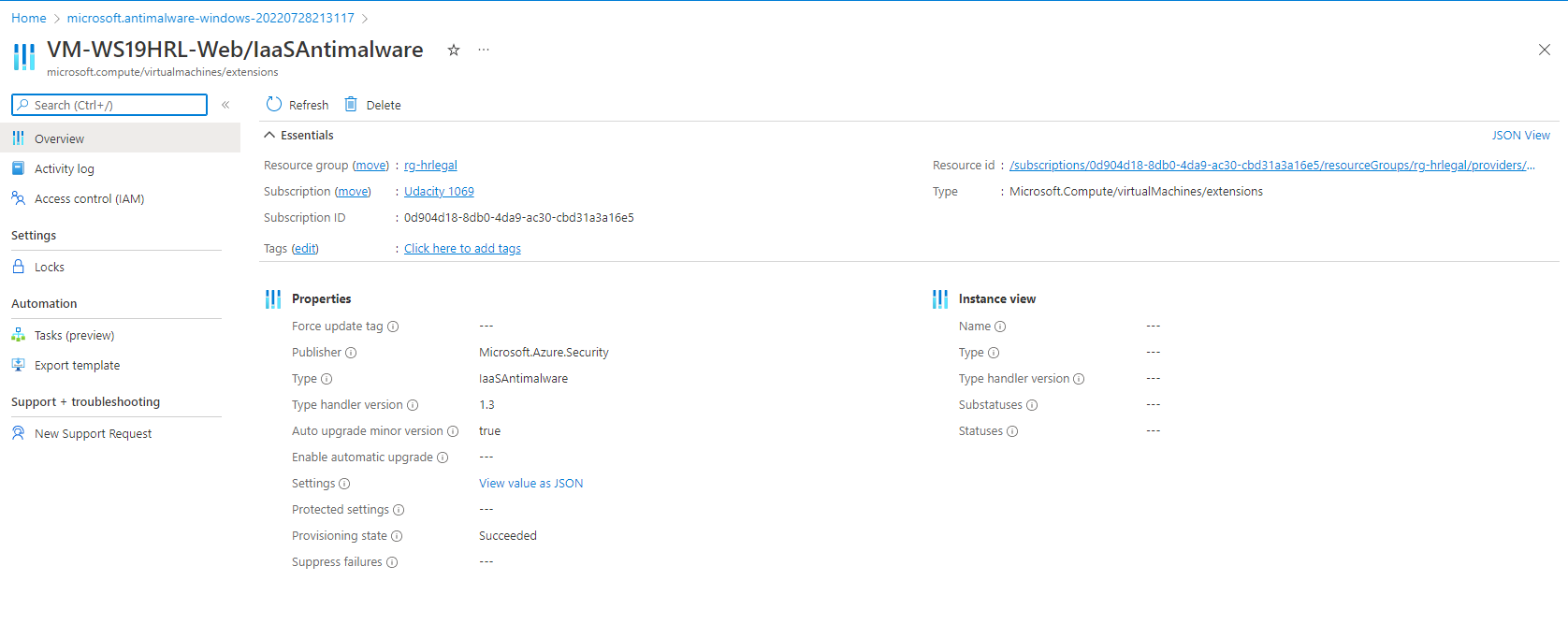
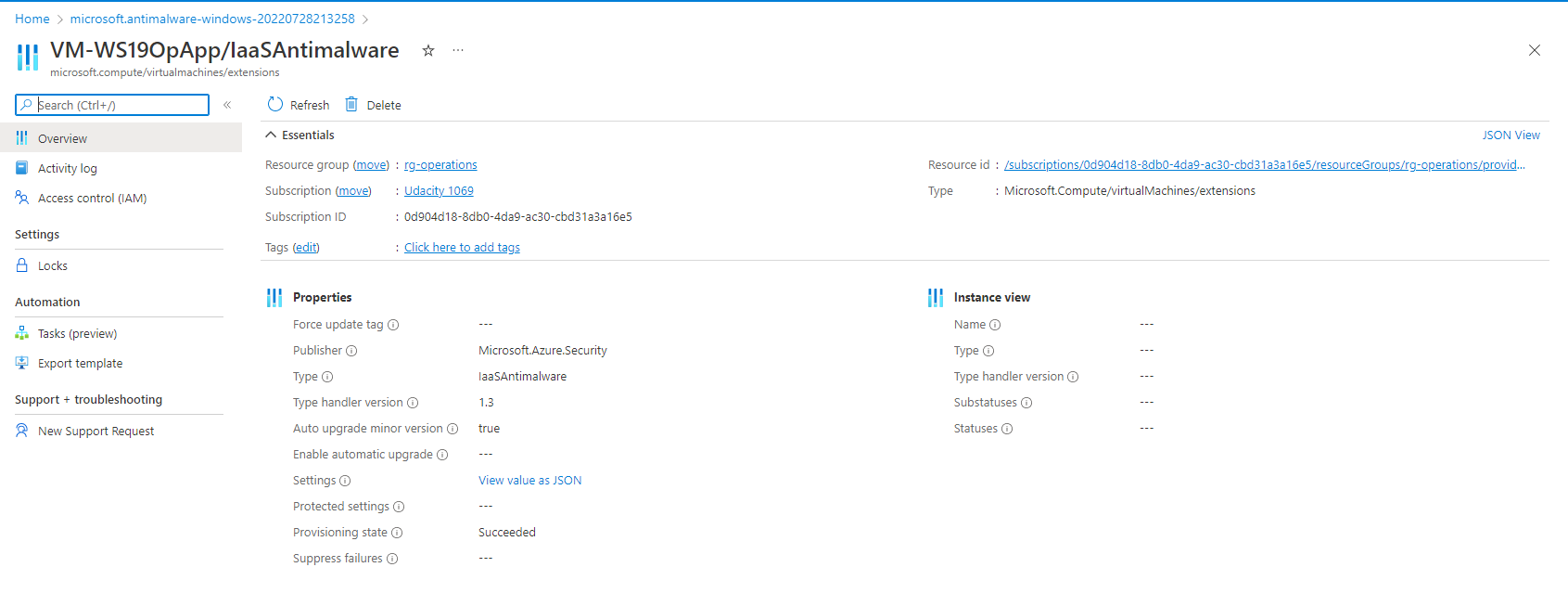
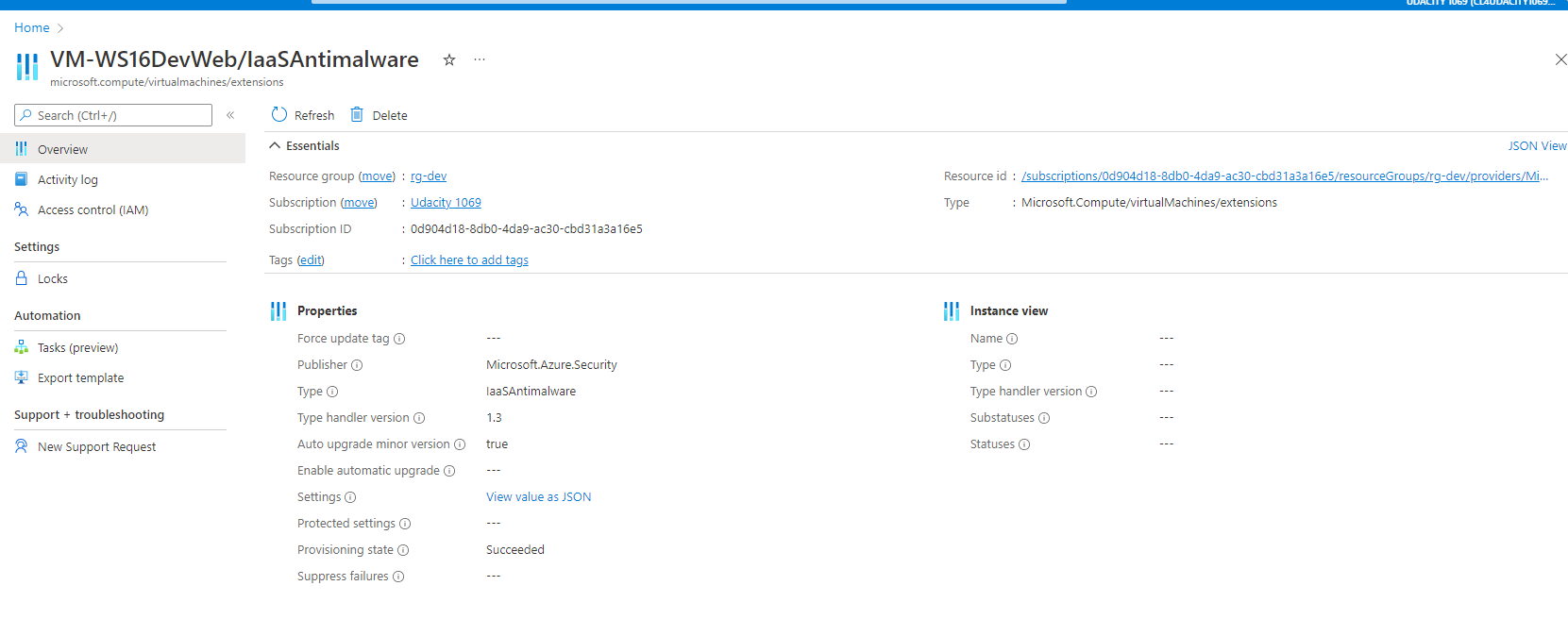


**Protection**

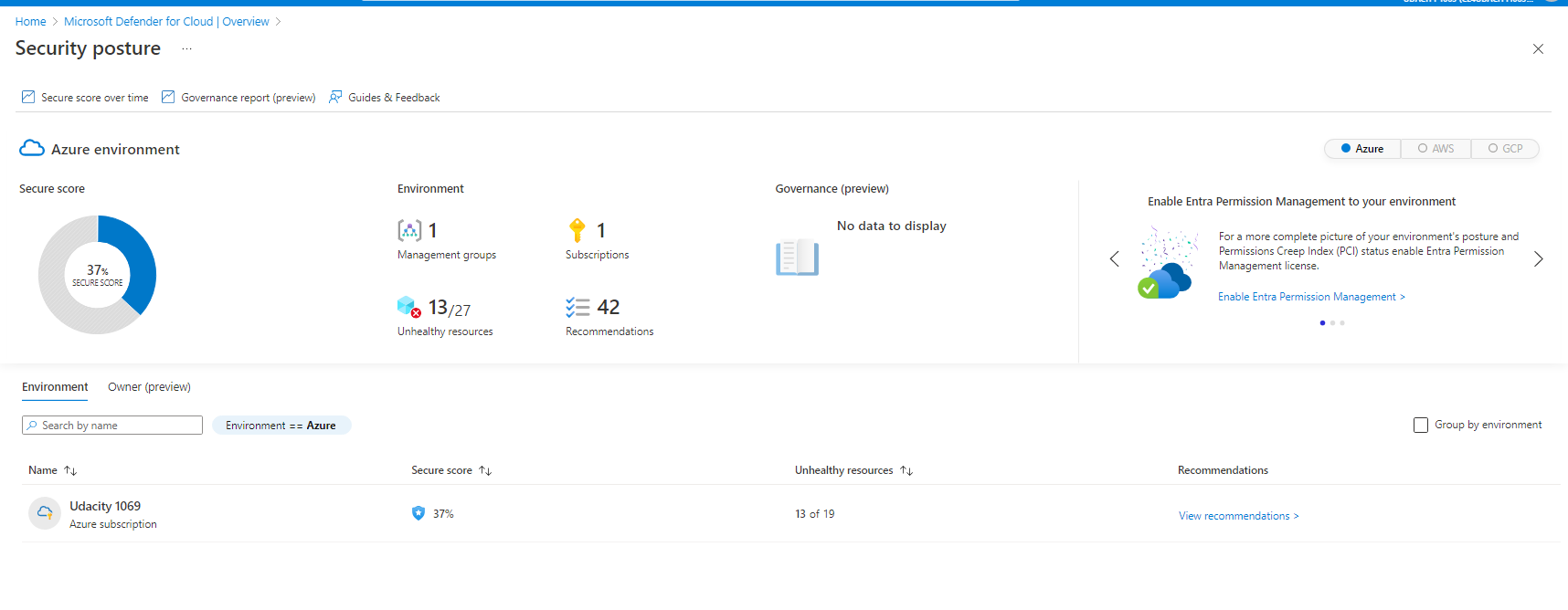
1. **Protect virtual machines from malware by using available extensions.**

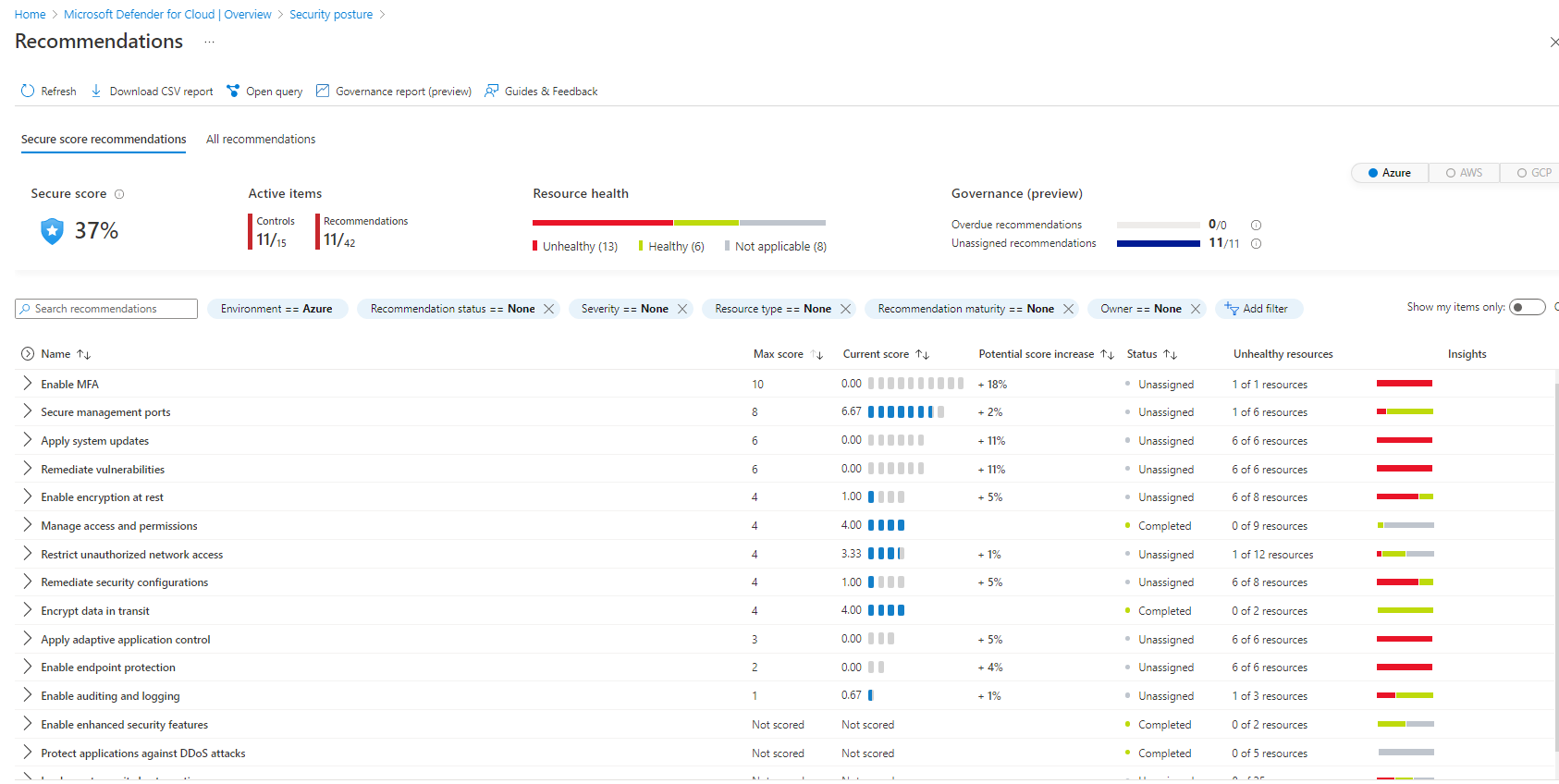
Screenshot of the extensions tab for all VM shows anti-malware is enabled

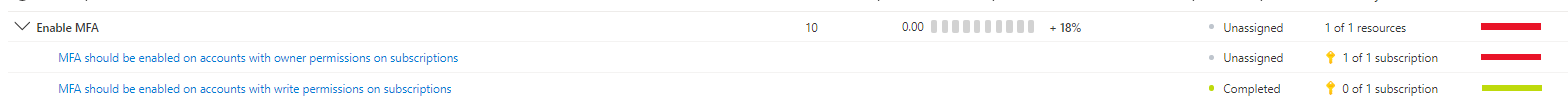


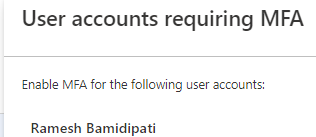


1. **Track and remediate vulnerabilities against Azure Security Center (ASC) Default policy**

A list of at least 3 recommendations with the justification to remediate vulnerabilities (text file)

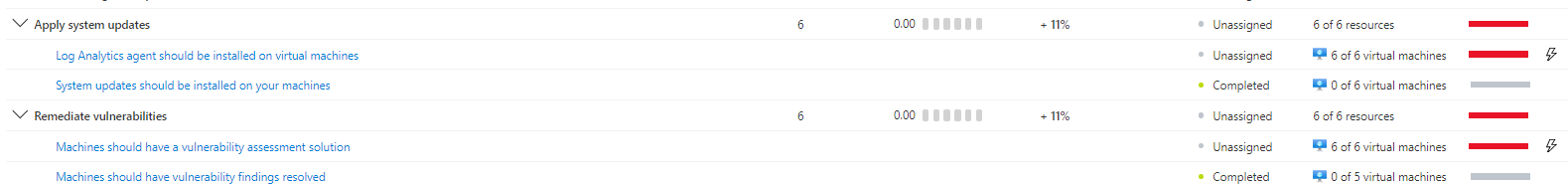






1. “Enable MFA” currently has a score of 0/10. So it has the biggest impact on security if we fix it.

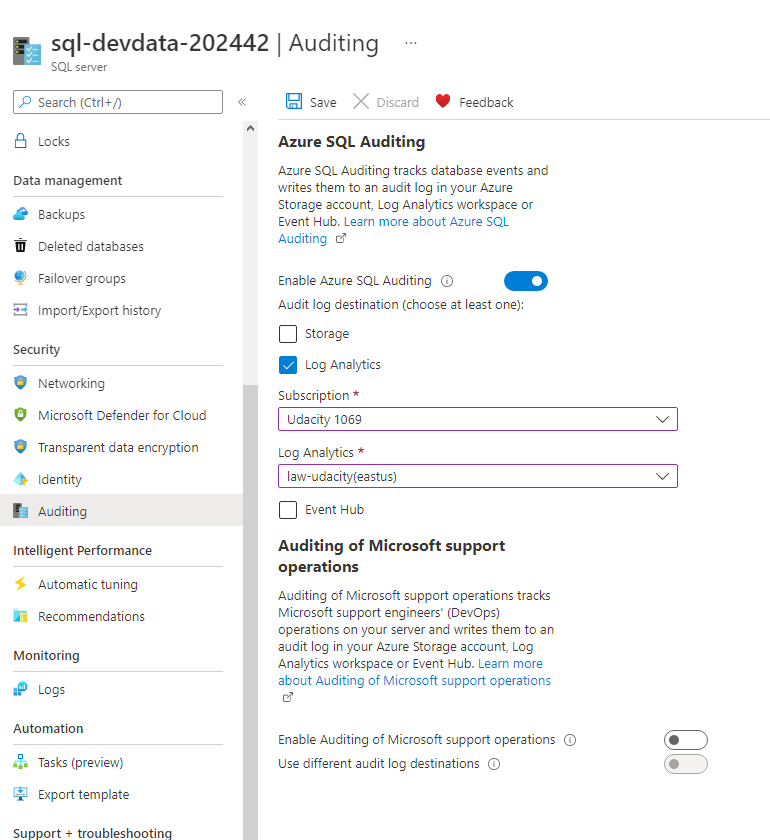
MFA is not set up for user account Ramesh Bamidipati.



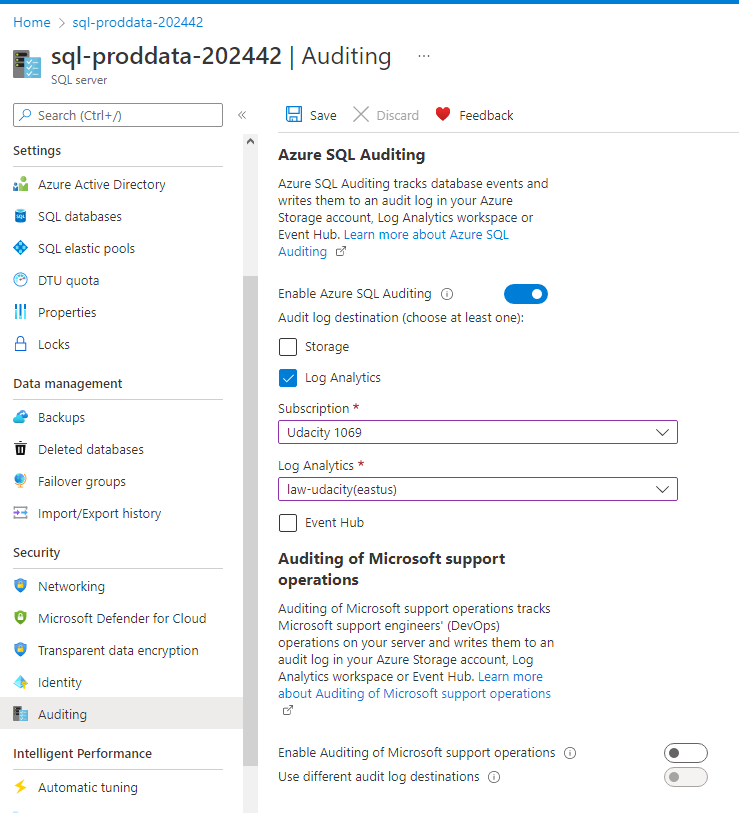
1. The other 2 top remediations are “Apply system updates” and “Remediate vulnerabilities”. Both of them have a score of 0/6.
2. We should install the log analytics agent on all of our VMs.
3. And we should install vulnerability assessment tools on our VMs.

**Monitoring**

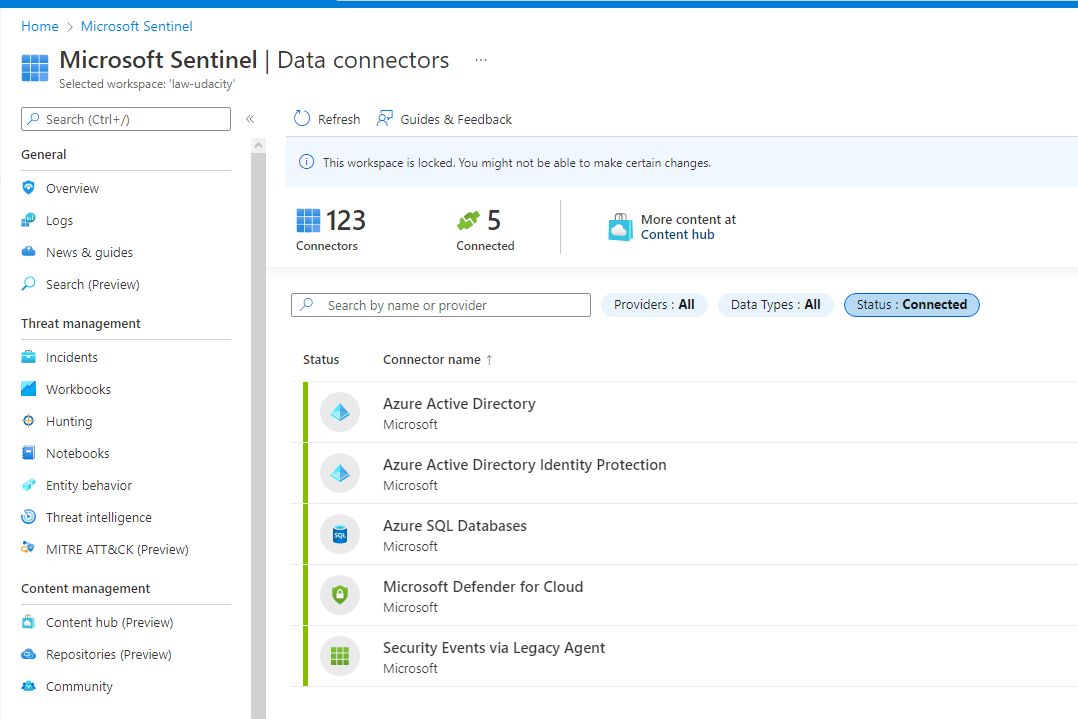
1. **Configure Azure Sentinel Connectors.**

Provide screenshot of Azure Sentinel Data Connectors Page.

At least Azure Active Directory and Azure Active Directory Identity Protection connectors should be selected



1. **Monitor and Protect SQL databases by configuring auditing.**

Provide screenshot showing SQL Auditing is enabled with Log Analytics Workspace

**Compliance**

1. **Enable monitoring of established industry and regulatory standards**

Screenshot proof of added NIST SP 800-53 rev4 policy

