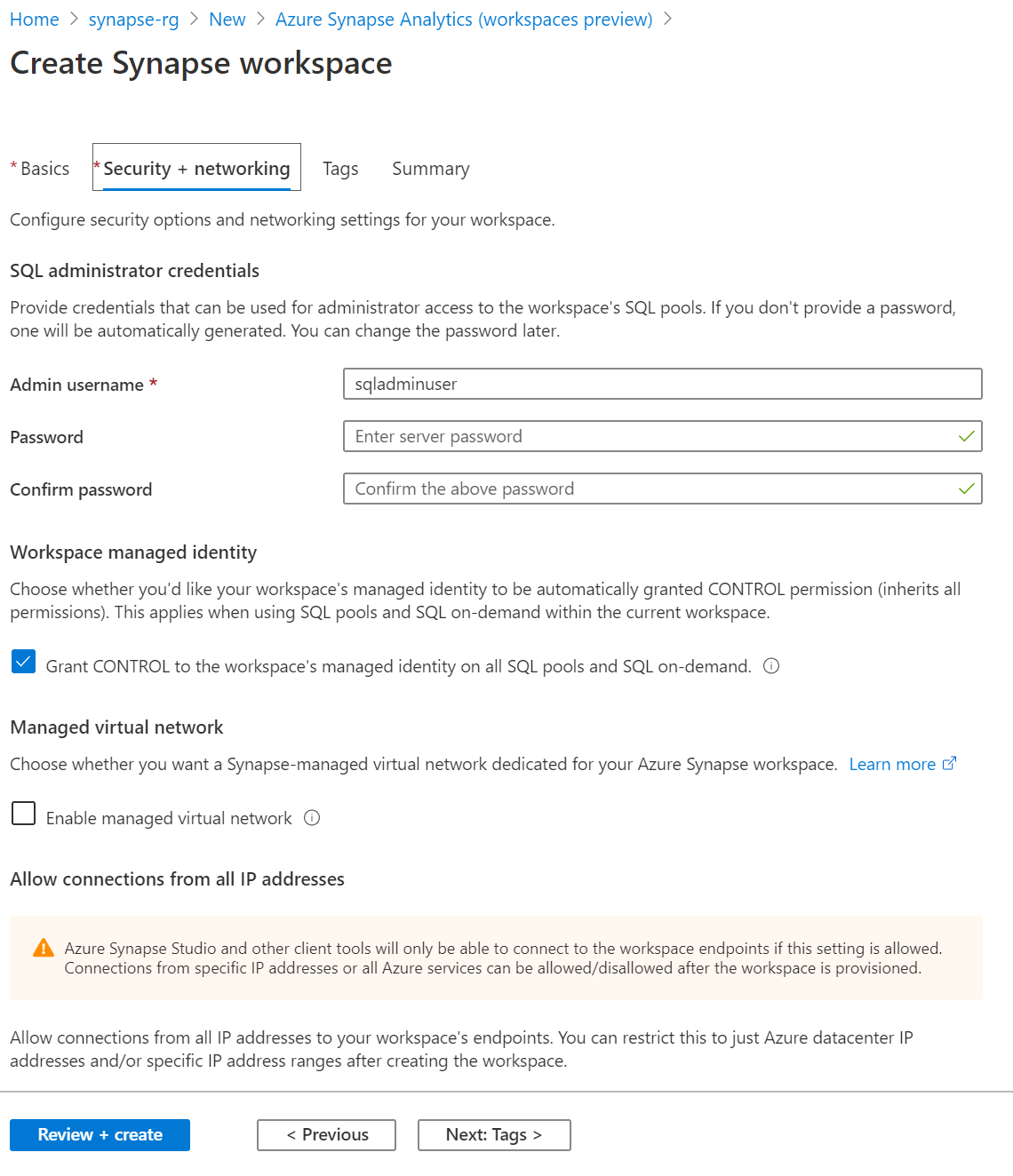
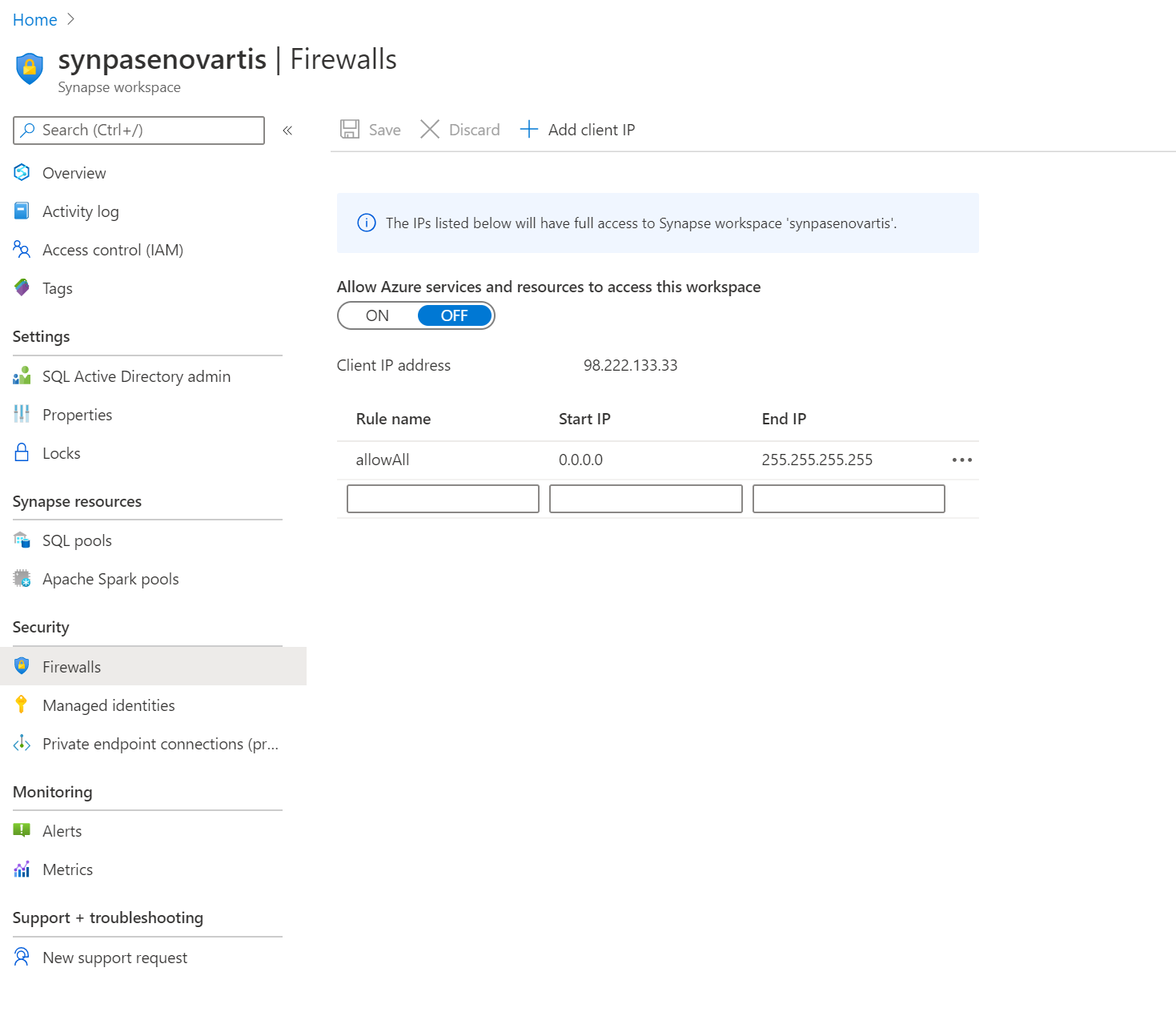
Managed VNets: (while creating the Synapse workspace :



IP Firewalls

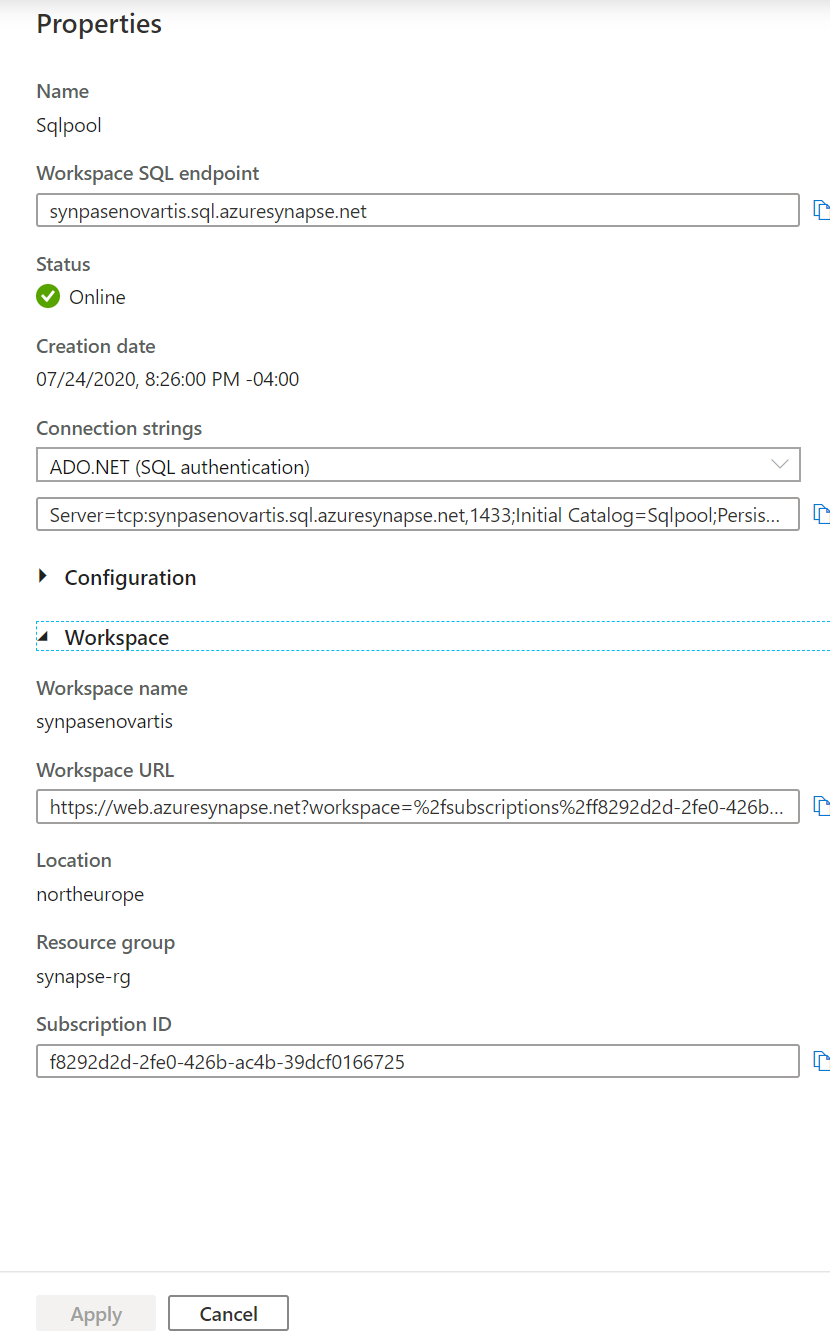
Method 1 :



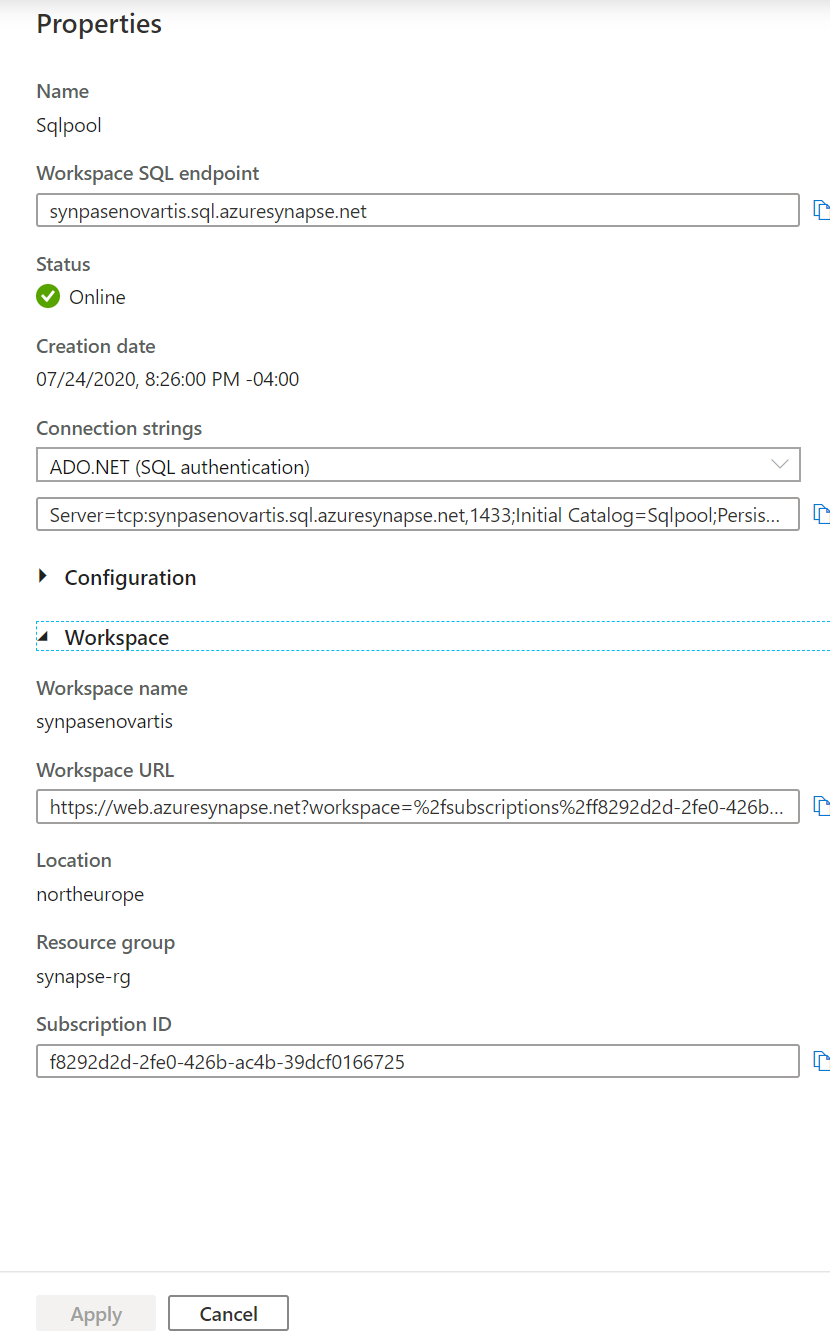
Method 2 : sp\_set\_firewall\_rule in the powershell

Endpoint:

Sql Pool: ( Manage Hub -> Analytics pools -> Select the Sql Pools )



Spark End point: ( Manage Hub -> Analytics pools -> Select the Apache Spark Pools )



Object Level security

GRANT SELECT ON OBJECT::Person.Address TO RosaQdM;

GO

Row Level security ( Security policy with filter predicate)

CREATE SECURITY POLICY [FederatedSecurityPolicy]

ADD FILTER PREDICATE [rls].[fn\_securitypredicate]([CustomerId])

ON [dbo].[Customer];

Column level security

GRANT SELECT ON Patients (

PatientID, FirstName, LastName, Phone, Email

) TO MKSMITH;

Dynamic data masking

ALTER TABLE [Employee]

ALTER COLUMN [SocialSecurityNumber]

ADD MASKED WITH (FUNCTION = 'DEFAULT()')

ALTER TABLE [Employee]

ALTER COLUMN [Email]

ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee]

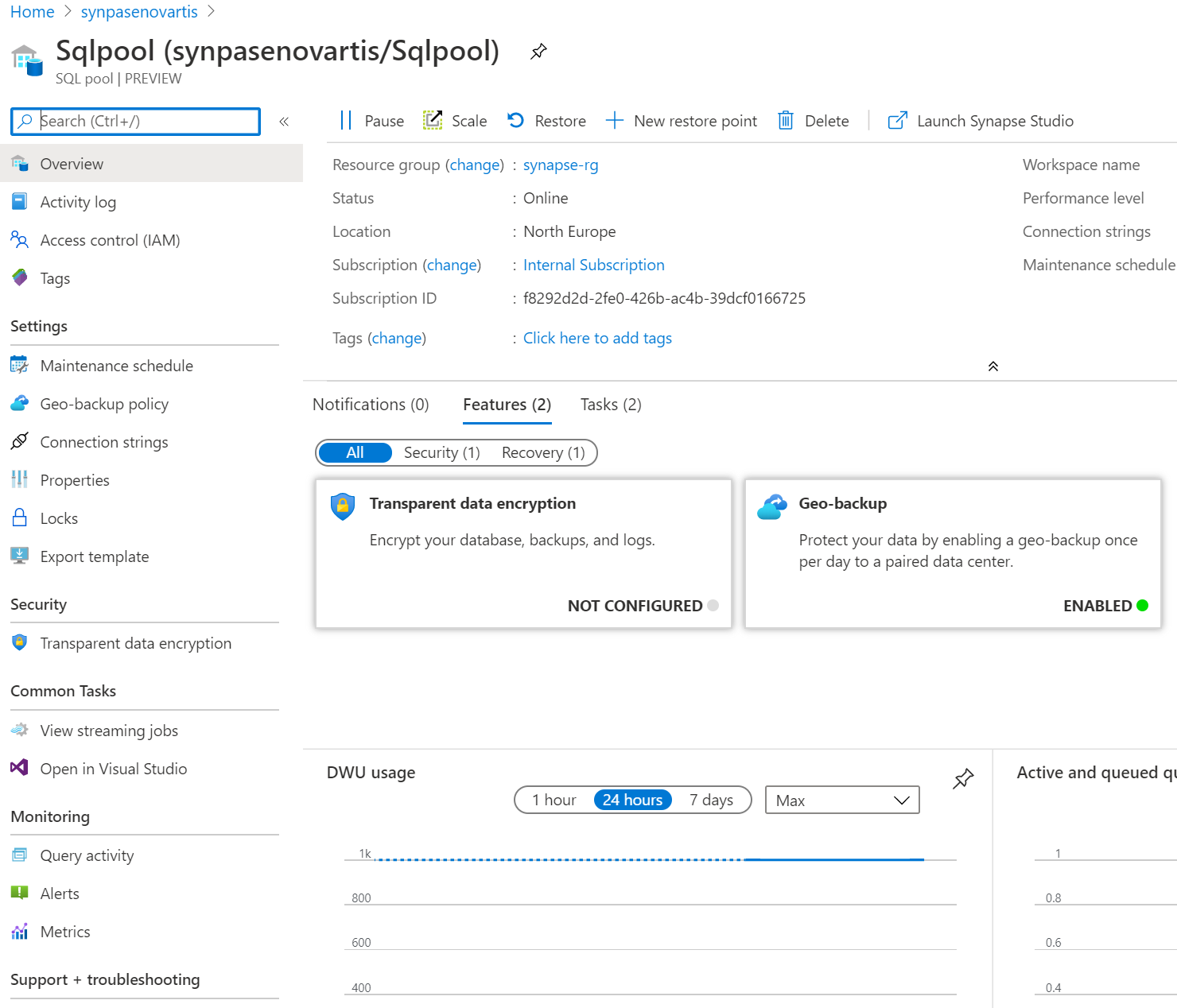
ALTER COLUMN [Salary]

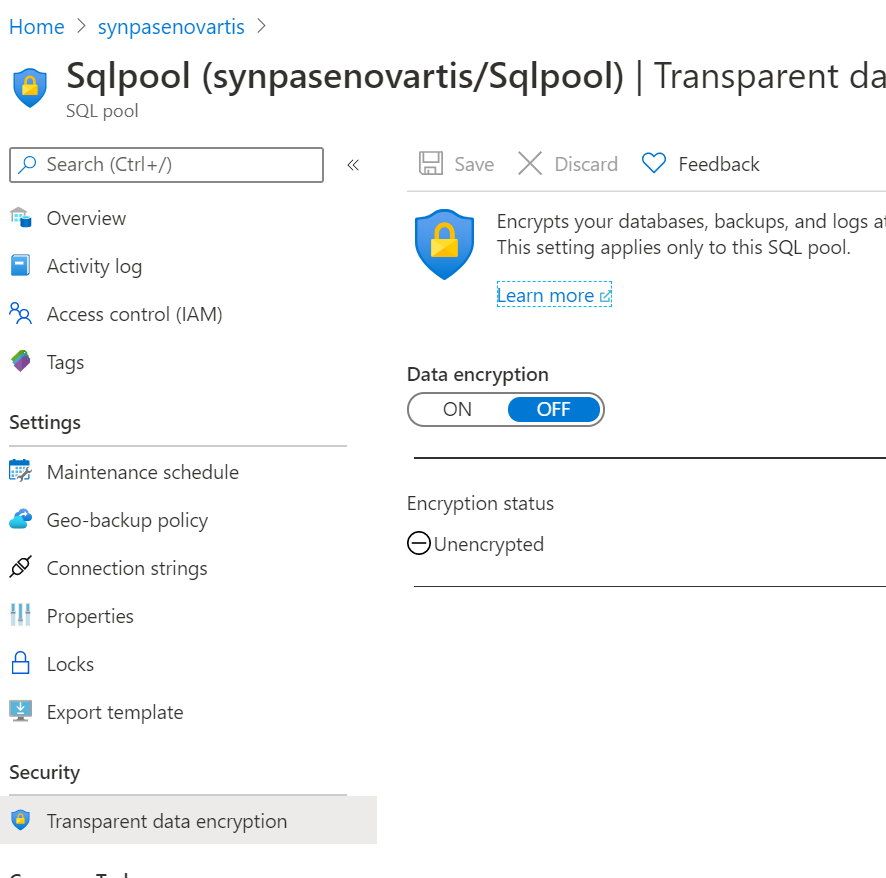
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to admin1

Transparent Data Encryption :

Create Master key , enable TDE





Synapse Roles – Workspace admin , sql admin , spark admin

