**PRUEBAS ALWAYS ON SQL SERVER SIN DOMINIO**

**Documentación Relacionada:**

<https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/domain-independent-availability-groups?view=sql-server-ver15>

<https://www.sqlpassion.at/archive/2016/01/11/how-to-create-a-sql-server-availability-group-without-an-active-directory-domain/>

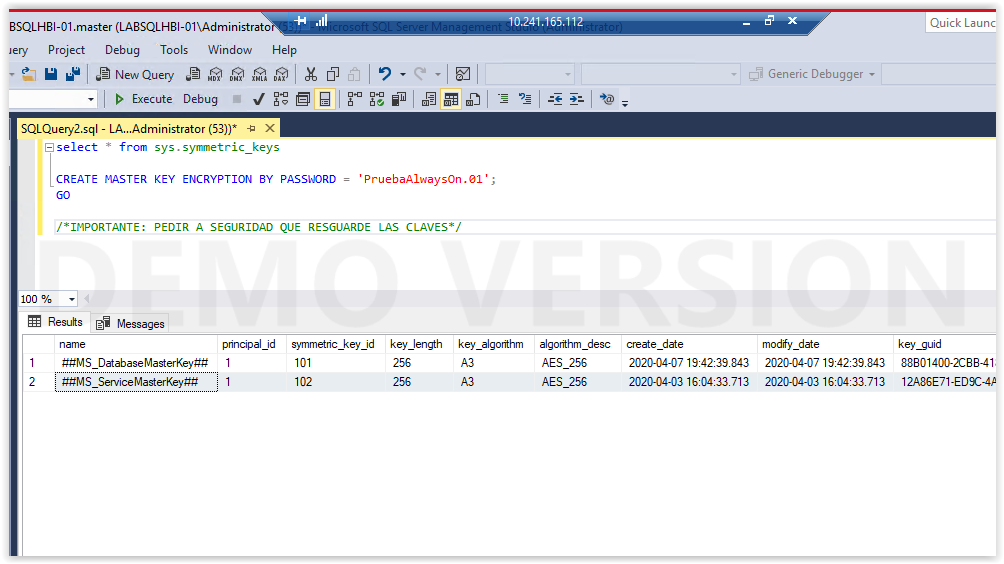
**Servidores de Prueba:**

**Servidor 1**: 10.241.165.112

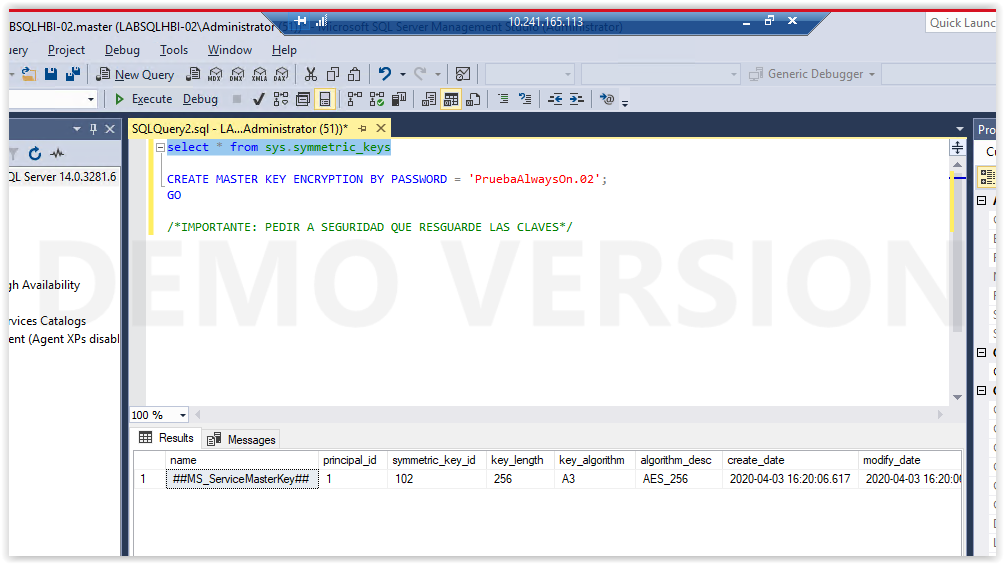
**Servidor 2**: 10.241.165.113

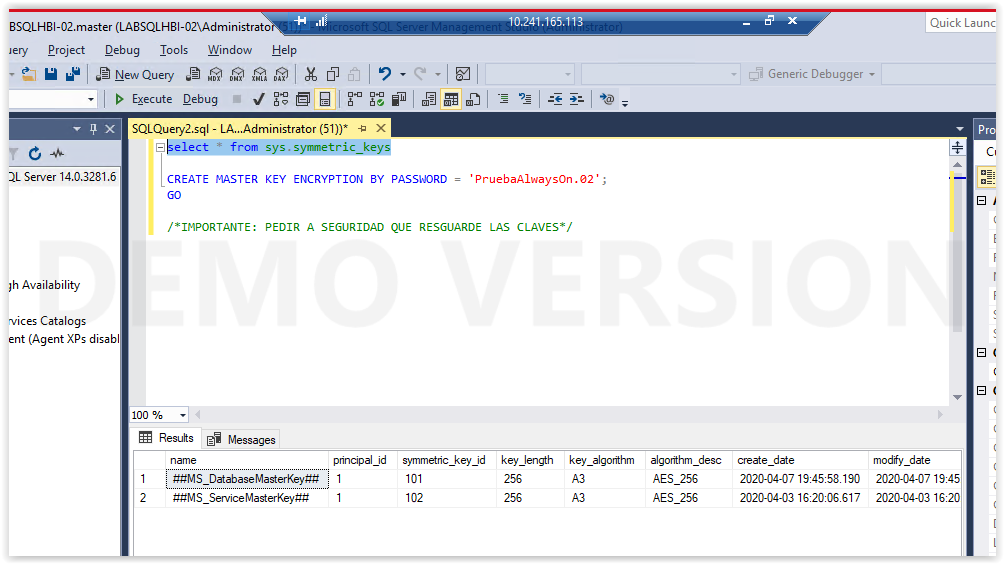
**3) Se generan las Master Keysd**

**Servidor 1:**



**Servidor 2:**

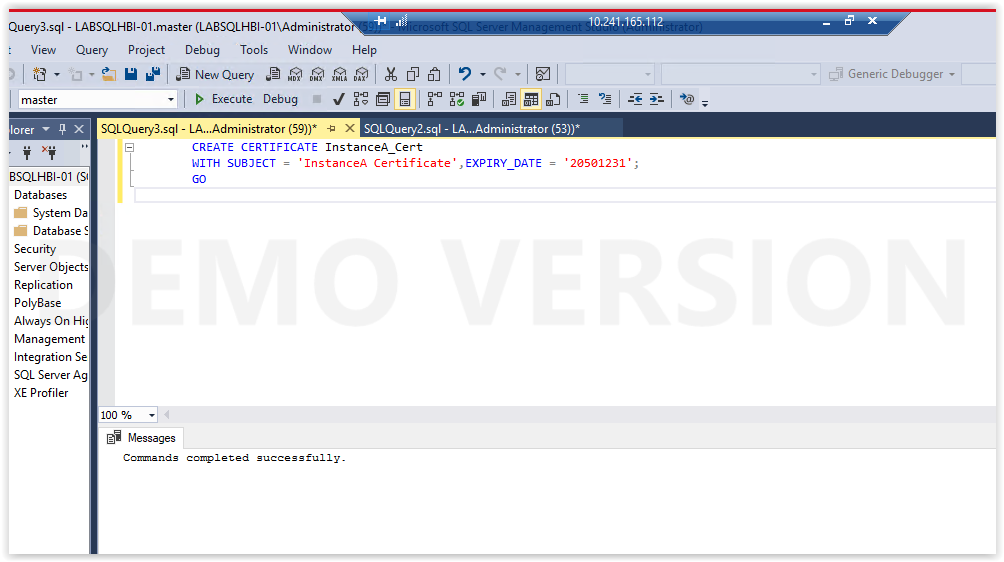




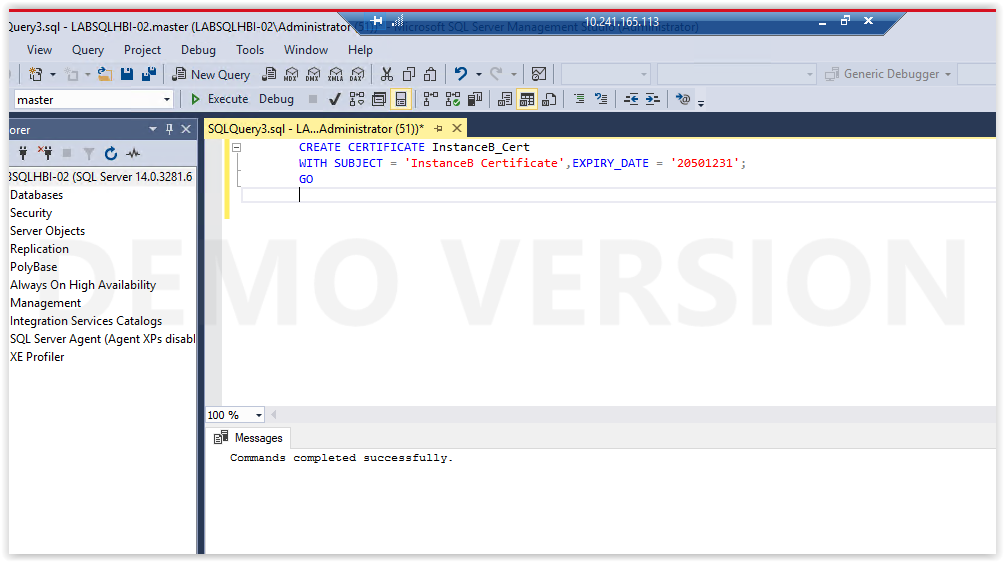
On the instance that will be the primary replica, create the certificate that will be used both for inbound connections on the secondary replicas and for securing the endpoint on the primary replica.

CREATE CERTIFICATE InstanceA\_Cert WITH SUBJECT = 'InstanceA Certificate'; GO

Se agrega parametro para fecha de expiracion dado que por default el certificado expira al año.

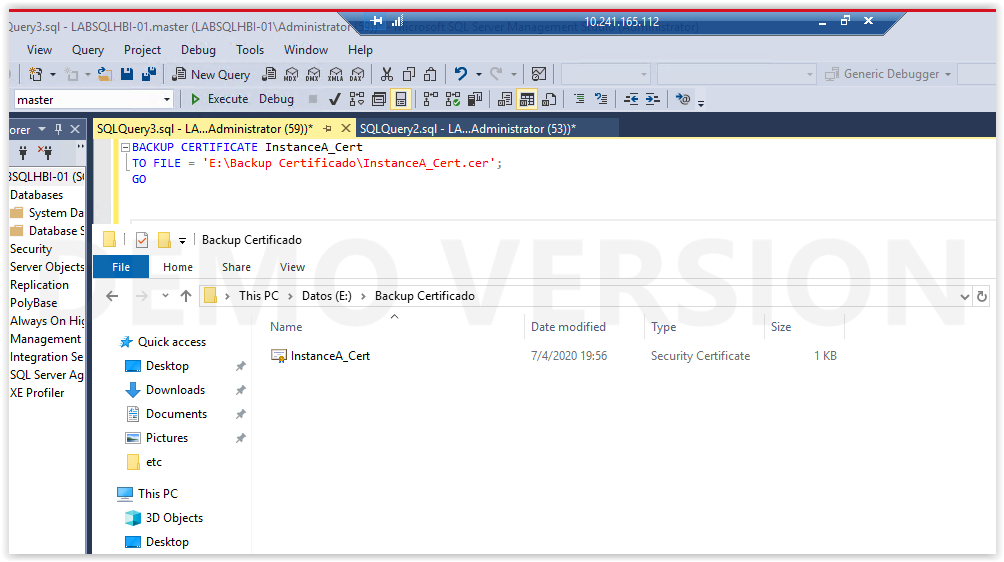


**Servidor 2**

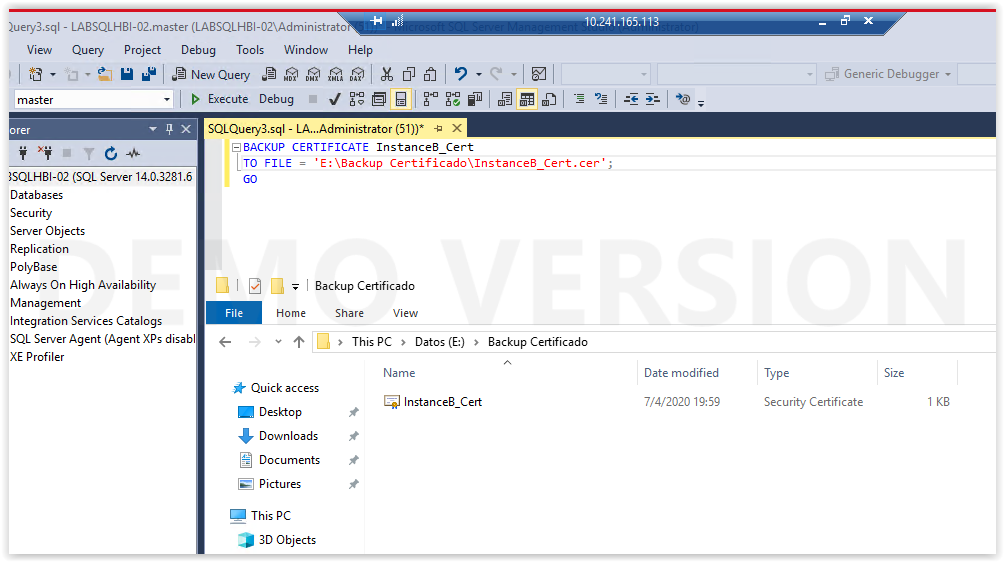


Back up the certificate. You can also secure it further with a private key if desired. This example does not use a private key.

**Servidor 1**



**Servidor 2**

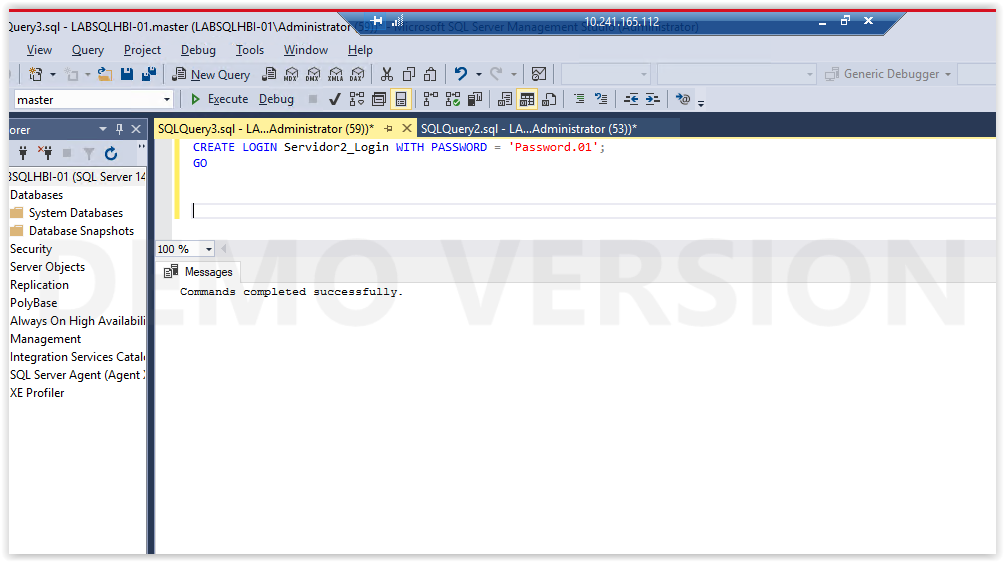


Repeat Steps 4 and 5 to create and back up certificates for each secondary replica, using appropriate names for the certificates, such as InstanceB\_Cert.

On the primary replica, you must create a login for each secondary replica of the availability group. This login will be granted permissions to connect to the endpoint used by the Domain Independent Availability Group. For example, for a replica named InstanceB:

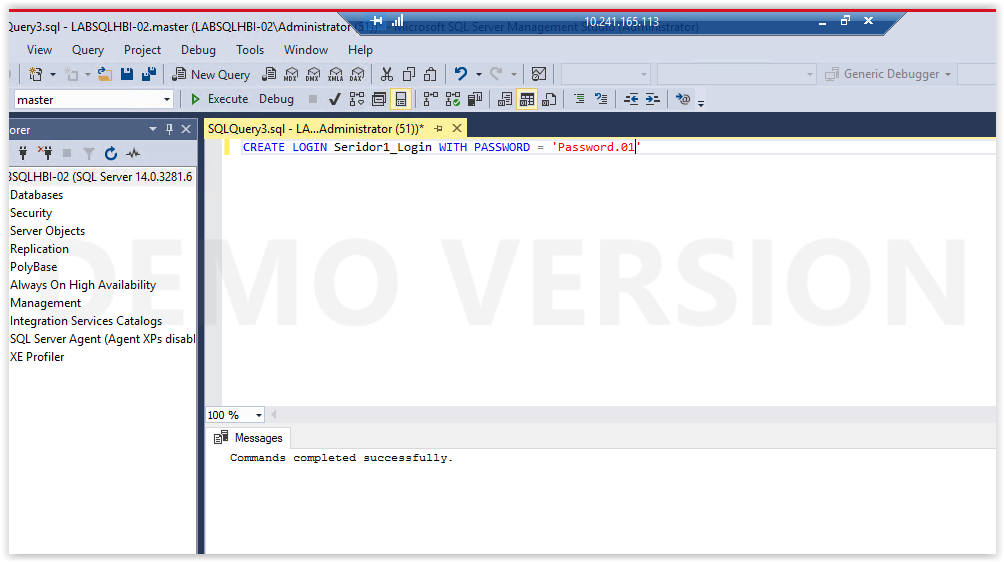
**Servidor 1:**

CREATE LOGIN InstanceB\_Login WITH PASSWORD = 'Strong Password'; GO



**Servidor 2:**

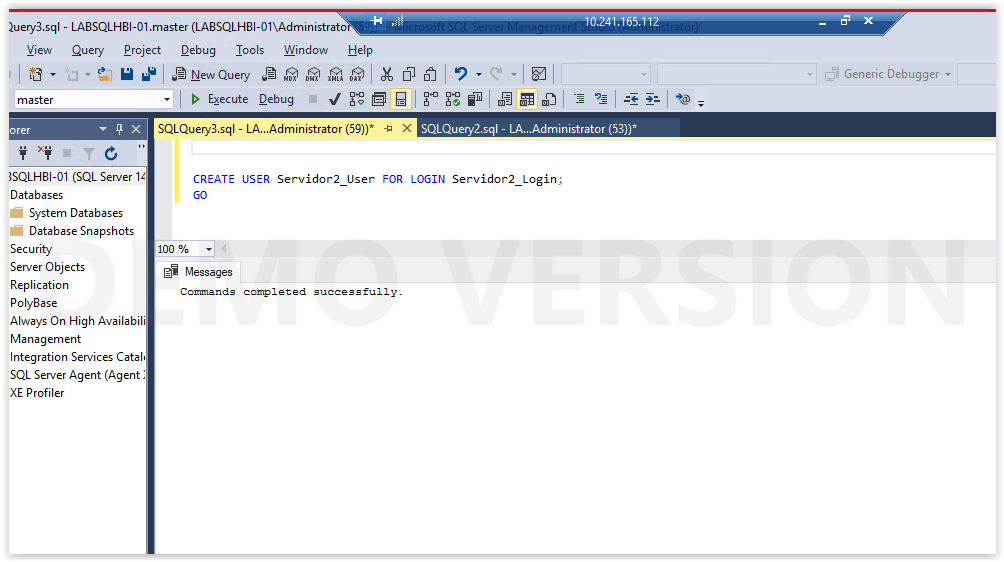
CREATE LOGIN InstanceA\_Login WITH PASSWORD = 'Strong Password'; GO



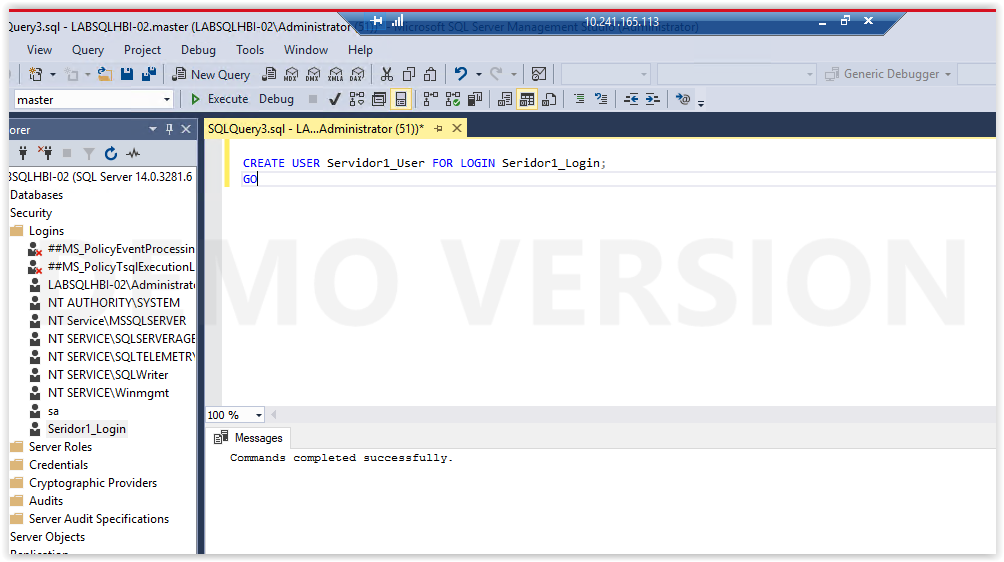
On all instances, create a user for each login that was created. This will be used when restoring the certificates. For example, to create a user for the primary replica:

CREATE USER InstanceA\_User FOR LOGIN InstanceA\_Login; GO

**Servidor 1**



**Servidor 2**

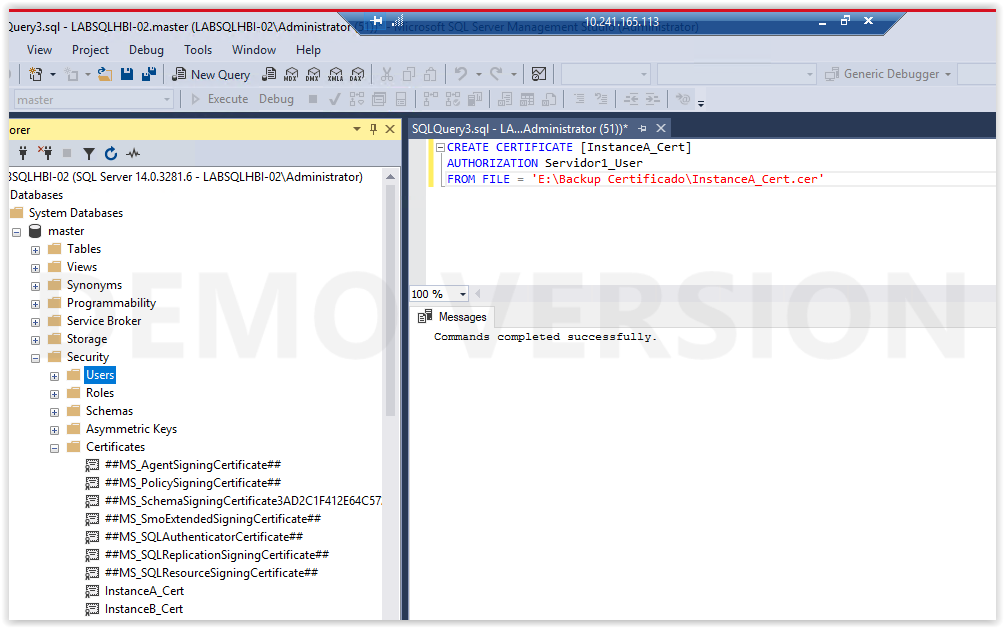


On each instance, restore the certificates for the other instances that had a login and user created. On the primary replica, restore all secondary replica certificates. On each secondary, restore the certificate of the primary replica, and also on any other replica that could be a primary. For example:

SQLCopy

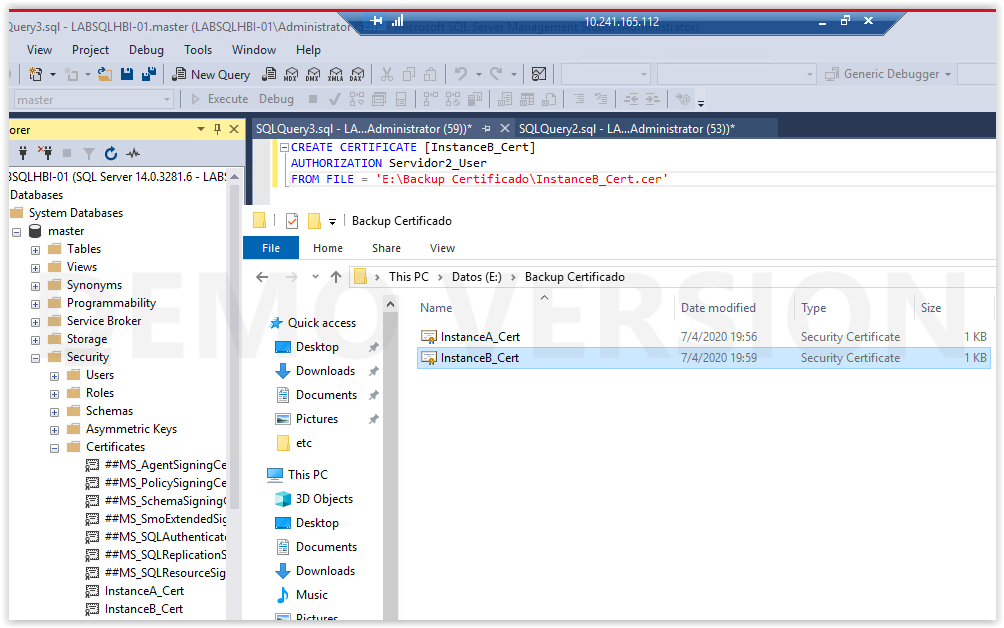
CREATE CERTIFICATE [InstanceB\_Cert]AUTHORIZATION InstanceB\_UserFROM FILE = 'Restore\_path\InstanceB\_Cert.cer'

**Servidor 2**



**Tener en cuenta el cruce de Certificados!!!!!!**

**Servidor 1**

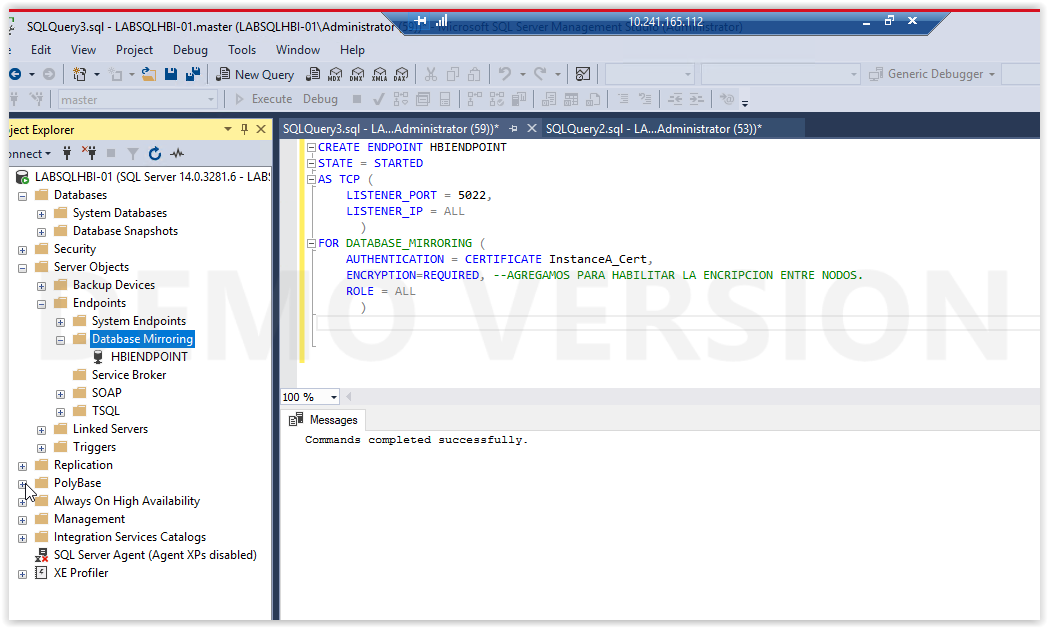


**Tener en cuenta el cruce de Certificados!!!!!!**

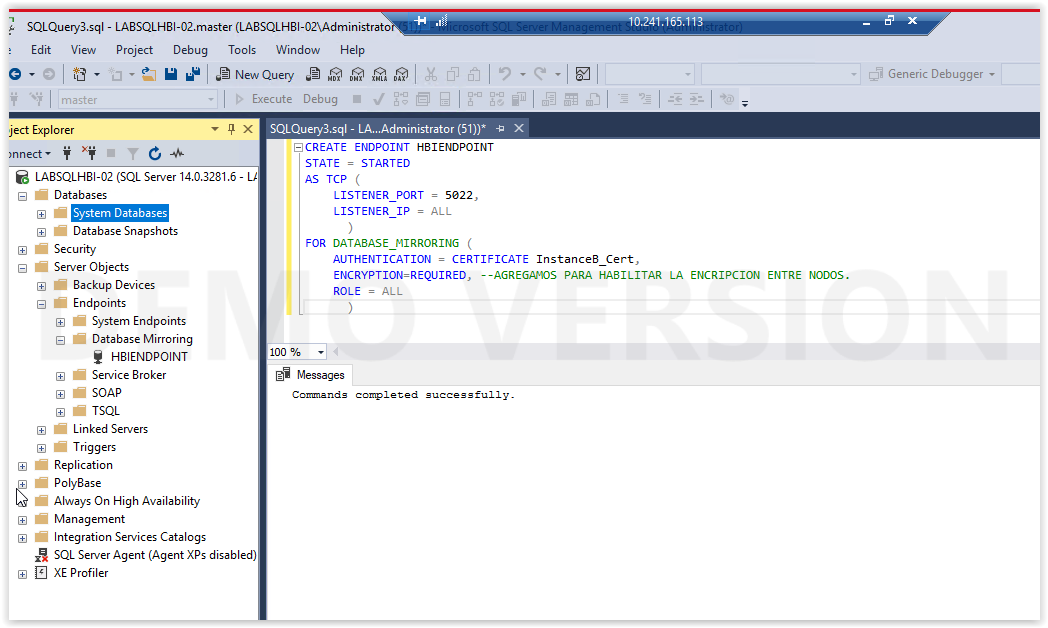
Create the endpoint that will be used by the availability group on each instance that will be a replica. For availability groups, the endpoint must have a type of DATABASE\_MIRRORING. The endpoint uses the certificate created in Step 4 for that instance for authentication. Example syntax is shown below to create an endpoint using a certificate. Use the appropriate encryption method and other options relevant to your environment. For more information on the options available see [CREATE ENDPOINT (Transact-SQL)](https://docs.microsoft.com/en-us/sql/t-sql/statements/create-endpoint-transact-sql?view=sql-server-ver15).

CREATE ENDPOINT DIAG\_EP STATE = STARTED AS TCP ( LISTENER\_PORT = 5022, LISTENER\_IP = ALL ) FOR DATABASE\_MIRRORING ( AUTHENTICATION = CERTIFICATE InstanceX\_Cert, ROLE = ALL )

**Servidor 1**



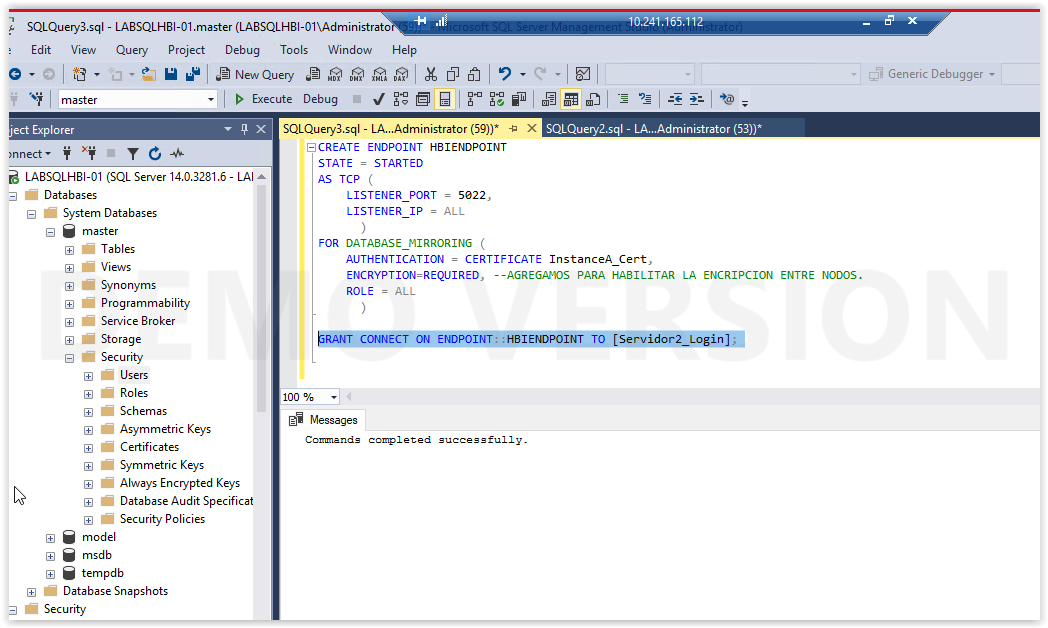
**Servidor 2**



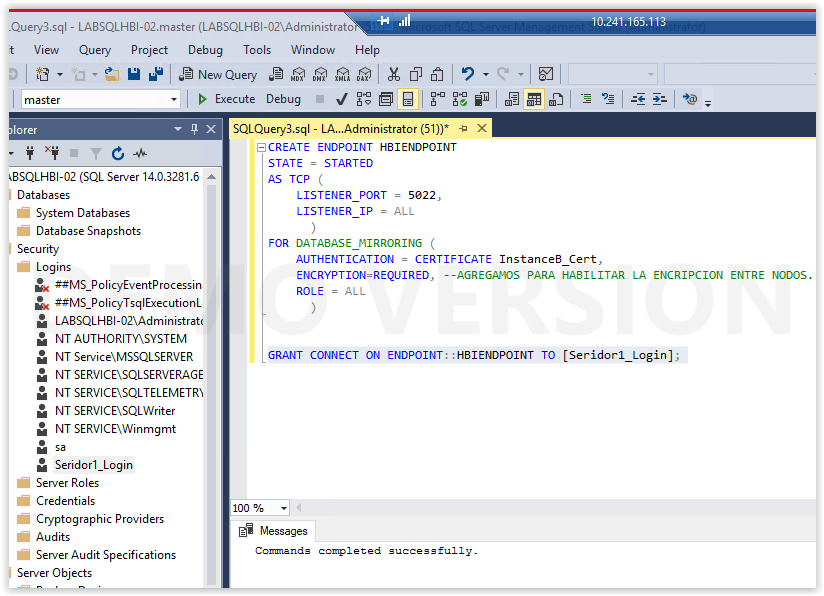
Assign rights to each user created on that instance in Step 9 to be able to connect to the endpoint.

GRANT CONNECT ON ENDPOINT::DIAG\_EP TO [InstanceX\_User];GO

**Servidor 1**



**Servidor 2**



**Realizar el backup master KEY del servidor IMPORTANTE!!!**

BACKUP MASTER KEY TO FILE = 'path\_to\_file' ENCRYPTION BY PASSWORD = 'password'

La password es de cada server para realizar la master.key y resguardar la password. La password compleja es para encriptar en archivo de backup. Es importante tener resguardo en caso de necesitar rearmar el servidor.