|  |  |  |
| --- | --- | --- |
|  | **Generali Head Office** |  |
|  | **ADA – Piano di Disaster Recovery** |  |
| **CONTENT**  Il document raccoglie le configurazioni, le azioni, I punti di attenzione al piano di Disaster/Recovery per i sistemi ed applicazioni di Produzione di ADA. | | |
| **Marzo 2023** | | |

Table of Contents

[Table of Contents 2](#_Toc1551197005)

[1 Implementazione/Configurazione D/R su North-EU 4](#_Toc425189814)

[1.1 Generalità 4](#_Toc217183554)

[2 Configurazione Virtual Machine 4](#_Toc2009833911)

[2.1 Configurazione D/R per il DB SQL SERVER 9](#_Toc412893207)

[2.1.1 Configurazione Failover Group 9](#_Toc1898252192)

[2.1.2 Creazione delle Login su SQL Server North-EU 12](#_Toc1346435417)

[2.1.3 Configurazione NETWORK 13](#_Toc1342823734)

[2.1.4 Configurazione Informatica DEI 14](#_Toc665387676)

[2.1.5 Configurazione Custom App 14](#_Toc1355484052)

[3 Configurazione DR Synapse 14](#_Toc1570939940)

[3.1 Setup Synapse su North-EU 15](#_Toc1762227938)

[3.1.1 Setup snapshot script automation 17](#_Toc1697770191)

[4 Configurazione DR Azure Databricks 19](#_Toc1238613529)

[5 Configurazione DR per Storage Account 21](#_Toc1340553162)

[6 Configurazione DR per KEY VAULT 23](#_Toc1240429469)

[7 Configurazione DR per Gateway 23](#_Toc585077910)

[8 Configurazione dei traffic manager 27](#_Toc1370066652)

[8.1 Portale e Axon 27](#_Toc1484834380)

[8.2 VM di Informatica DEI 28](#_Toc1784187203)

[8.3 VM SFTP 28](#_Toc1567461628)

[9 Configurazione INFORMATICA DEI 29](#_Toc1803029666)

[10 Preparazione al TEST Failover 29](#_Toc564684165)

[10.1 Preparazione Test Failover Key Vault 29](#_Toc365222650)

[10.2 Preparazione Test Application Gateway 30](#_Toc524546655)

[10.3 Preparazione Test Failover SFTP 30](#_Toc2079616935)

[10.4 Predisposizione Test Failover per SQL Server 30](#_Toc1835443268)

[10.4.1 Creazione del Server SQL replicato e scrivibile 30](#_Toc609773687)

[10.4.2 Dismissione a seguito della chiusura dei test 37](#_Toc1406068335)

[10.5 Preparazione Test Failover per Informatica AXON 38](#_Toc688474961)

[10.6 Preparazione Test Failover Informatica DEI/DEQ 39](#_Toc854297250)

[10.6.1 Connessione al DB INFADBPROD 39](#_Toc2023847677)

[10.6.2 Connessione a Databricks su DR 43](#_Toc1039093977)

[10.7 Preparazione Test Failover Custom App 44](#_Toc705138656)

[10.8 Preparazione Test Failover Synapse 45](#_Toc605698601)

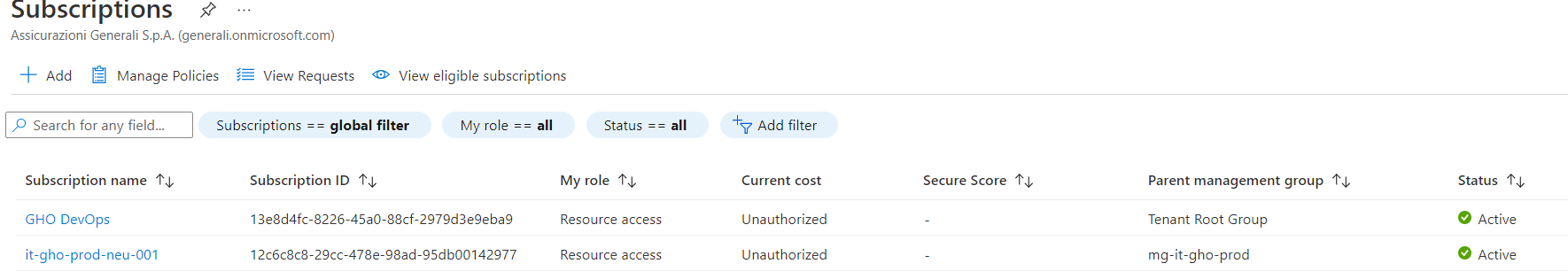
[11 Esecuzione del Test Failover 45](#_Toc836472528)

[11.1 Dismissione ambiente di Test DR 49](#_Toc575288530)

[12 Esecuzione del Failover 50](#_Toc1288652654)

# Implementazione/Configurazione D/R su North-EU

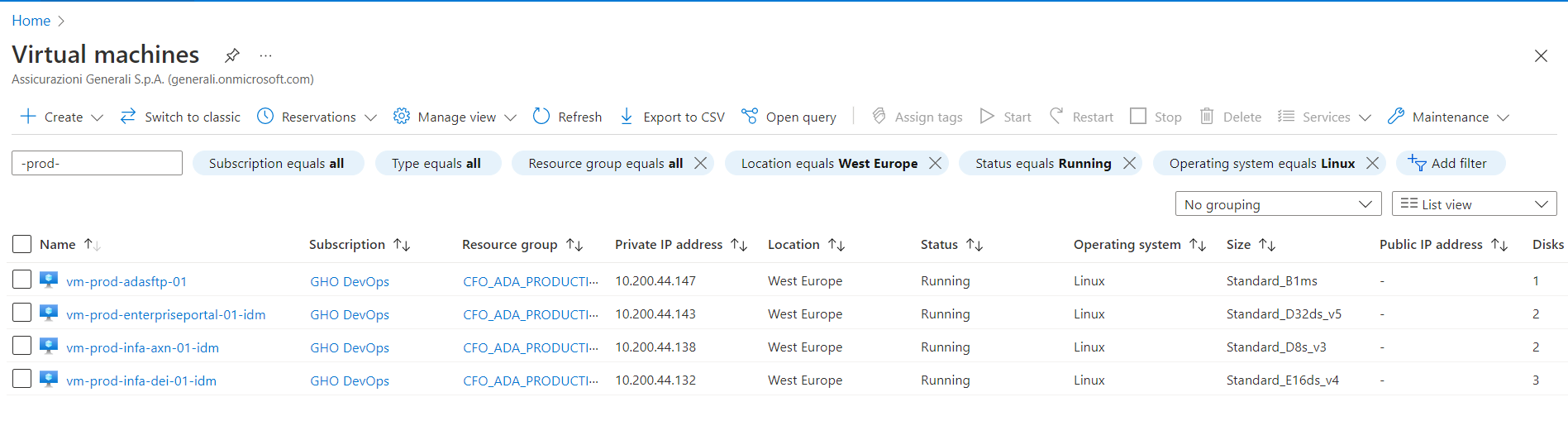
## Generalità



* GHO DevOps – sottoscrizione primaria
* It-gho-prod-neu-001 – usata per gestire le risorse DR in North EU

# Configurazione Virtual Machine

I dischi di ciascuna VM sono costantemente replicati in N-EU mediante **Azure Site Recovery** (RPO ad 1 minuto circa). Per ogni VM è presente una definizione di una risorsa non allocata realmente ma “pronta” sia per il test che per il failover che ha assegnato un IP privato ed un nome di risorsa uguale a quello di origine e suffisso “DR”.



Le risoluzioni dei nomi disponibili dall’interno della vnet in northeurope sono le seguenti:

vm-prod-enterpriseportal-01-idm-dr.azure.generali-cloud.com ==> 10.206.24.8  
vm-prod-infa-axn-01-idm-dr.azure.generali-cloud.com ==> 10.206.24.9  
vm-prod-infa-dei-01-idm-dr.azure.generali-cloud.com ==> 10.206.24.7  
vm-prod-adasftp-01-dr.azure.generali-cloud.com ==> 10.206.24.6

**Di seguito le configurazioni per la VM dedicata a SFTP – sistema operativo Centos.**

Nella sezione **Overivew** è disponibile una vista dell’infrastruttura logica.

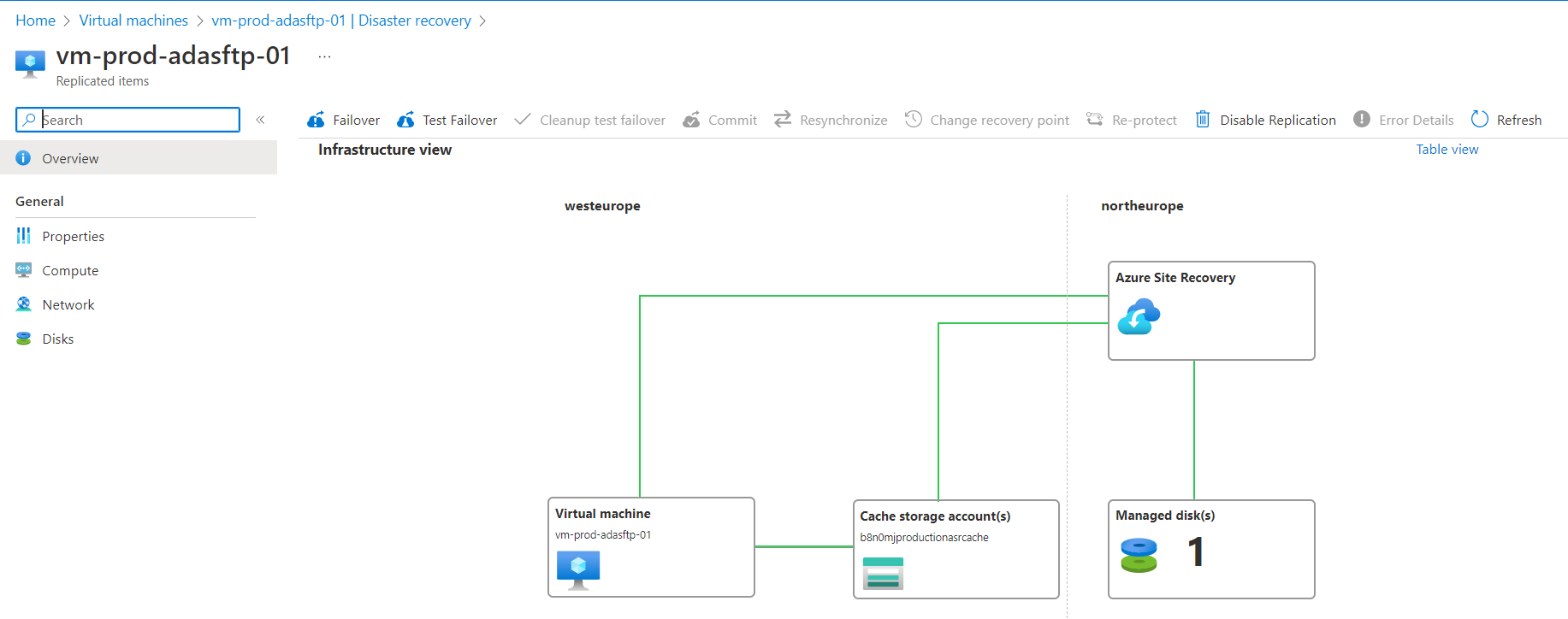
Nella sezione **Compute** è possibile definire le specifiche della VM in N-EU (bottone Edit), assegnando il nome della VM, il resource group ed il sizing.

Immagine che contiene testo

Descrizione generata automaticamenteNella sezione Network è possibile definire le specifiche relative alla rete per VM in N-EU (bottone Edit), assegnando Network Security Group, subnet, Private IP per il test failover e private IP per il failover effettivo (nel nostro contesto coincidono sempre).

Immagine che contiene testo

Descrizione generata automaticamente

Nella sezione DISKs è possibile visualizzare i dischi in replica con “site recovery”

Immagine che contiene testo

Descrizione generata automaticamente

Di seguito si riportano le configurazioni delle altre VM portate in replica su North-EU. Tutte le VM sono con sistema operativo Linux Red Hat

|  |  |
| --- | --- |
| Custom Portal | vm-prod-enterpriseportal-01-idm |
| Overview |  |
| Compute |  |
| Network |  |
| Disks |  |
|  |  |
| Informatica AXON | vm-prod-infa-axn-01-idm |
| Overview |  |
| Compute |  |
| Network |  |
| Disks |  |

|  |  |
| --- | --- |
| Informatica DEI/DEQ | vm-prod-infa-dei-01-idm |
| Overview |  |
| Compute |  |
| Network |  |
| Disks |  |

## Configurazione D/R per il DB SQL SERVER

Per il DR del DB SQL Server è stato scelto di implementare il failover group.

### Configurazione Failover Group

Prima di procedere alla creazione del gruppo di failover è stato creato su North EU il nuovo server **repos-infa-prod-dr** cui è stato assegnato lo stesso server admin (infadbprod-admin) con la stessa password che ha nella region West.

Immagine che contiene testo

Descrizione generata automaticamente

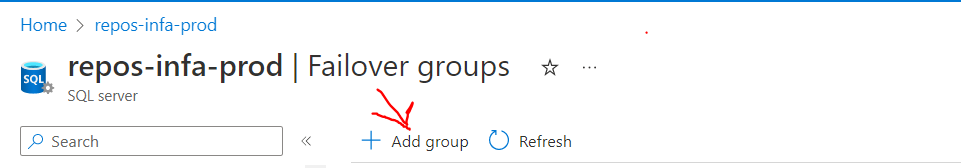
Sul server è stato definito un elastic pool con un sizing più piccolo del server primario (per tenere basso il costo) ma sufficiente a tenere i dati del primario, con lo stesso nome del primario.

Immagine che contiene testo

Descrizione generata automaticamente

Una volta creato il server si può passare alla creazione del failover group.

Riportarsi su SQL Server in West EU, selezionare “failover group” nell’elenco a sinista e quindi richiedere la creazione di un nuovo gruppo.



Indicare nome del gruppo **repo-infa-prod-fg** ed il nome del server precedentemente creato in North-EU.

Immagine che contiene testo

Descrizione generata automaticamente

Quindi assegnare i DataBase oggetto di replica sul failover group.

Al momento il D/R include i DataBase:

* ADA\_ENTERPRISEPORTAL\_PROD – database della custom App
* INFADBPROD – database di Informatica DEI/DEQ

Immagine che contiene testo

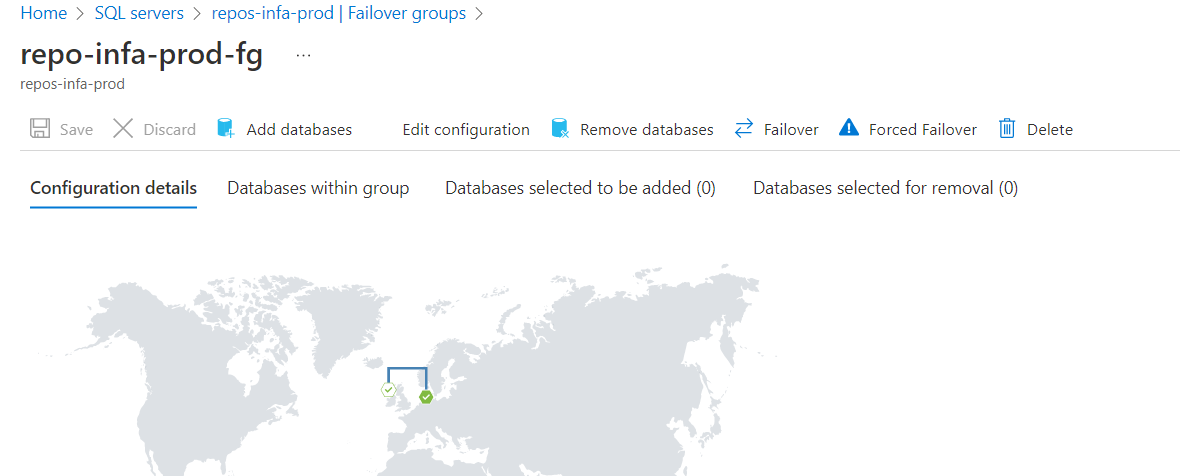
Descrizione generata automaticamente

La replica si completa dopo un certo tempo (INFADBPROD) ed è possibile visualizzare una mappa come quella che segue, che riporta le region che ospitano il DB, i rispettivi nomi dei server e i listner creati nelle rispettive region.

Da questo momento in poi è possibile referenziare il DB usando il listner nella region primaria.

In caso di failover il listner secondario diventa primario in automatico a cura di Azure e non è perciò necessario modificare le connessioni al DB da parte delle applicazioni che usano l’end-point del failover group.

La porta su cui risponde il listner è la medesima: 1433.





La configurazione dei listener rende trasparente all’applicazione il potenziale failover del DB e demanda all’infrastruttura Azure il cambio di DNS per mandare le richieste al DB sul server secondario.

### Creazione delle Login su SQL Server North-EU

La replica ricrea nel server secondario tutto quanto è nel primario eccetto le login che devono essere ricreate manualmente a completamento della configurazione del failover group.

A tale scopo , per ogni login nel sistema primario è stato recuperato il SID e con quel SID è stata ricreata la login sul secondario mantenendo anche la stessa password. Questa è attività necessaria per le utenze di tipo SQL non per le utenze di dominio AD

Con un client SQL (Management Studio), accedere a SQL Server in West-EU ed eseguire le query per ogni login sul modello di

*SELECT sid FROM sys.sql\_logins WHERE name = <login-name> --* per recuperare il SID

Con il SID e le credenziali di ogni login costruire comandi sul modello di

CREATE LOGIN <login-name> WITH PASSWORD = ..', SID = ..;

Ed eseguire i comandi da un client SQL Server su North-EU.

Di seguito le login necessarie per Informatica DEI e Custom App (in allegato lo script di creazione delle login con il SID del DB in West EU).

* Login per Informatica
* INFADMIN
* INFAMOD
* INFAMON
* INFAPRF
* INFAWKF
* INFADO
* INFAREF
* INFAEXCP
* Login per Custom App
  + EDCDBADMIN
  + USER\_ADA\_ENTER\_RW
  + USER\_ADA\_INFADB\_RW
  + USER\_ADA\_TEAMS\_R
  + USER\_OPT\_OPTIONS
  + DTADMIN (solo schema storico – verificare se necessario mantenere su DR)
  + DTREADER (solo schema storico – verificare se necessario mantenere su DR)

File disponibile sull’area riservata del teams al seguente link

[dr\_creatloginsql.sql](https://generali.sharepoint.com/:u:/r/sites/DataStrategy2-SecurityArea/Shared%20Documents/Security%20Area/dr_setup_withpassword/dr_creatloginsql.sql?csf=1&web=1&e=vzx5pZ)

Non sono state definite policy di BACKUP per il server secondario.

ATTENZIONE! Questo script deve essere manutenuto ogni qualvolta viene inserito o tolta una utenza SQL e revisionato ad ogni test di DR

### Configurazione NETWORK

Per il server primario sono stati creati due private endpoint: uno è nella region West (IP 10.200.44.146), l’altro è nella regione North (IP: 10.206.28.4).

Immagine che contiene testo

Descrizione generata automaticamente

I private endpoint sono:

* database-ada-privateendpoint (10.200.44.146)
* pe-database-adaprod-DR (10.206.28.4)

Allo stato, Il server secondario è “chiuso” all’esterno.

Per effettuare test di lettura (o qualunque altra attività) è necessario mettere in white list l’IP da cui si vuole accedere.

### Configurazione Informatica DEI

L’ applicazione Informatica DEI è stata modificata in modo che tutte le connessioni al DB abbiano come endpoint il failover group, invece che il server primario.

### Configurazione Custom App

L’ applicazione Custom App è stata modificata in modo che tutte le connessioni al DB abbiano come endpoint il failover group, invece che il server primario.

# Configurazione DR Synapse

Synapse, non ha automatismi di replica su una region secondaria. Per contro offre policy di Geo-Backup su una region *pair* della primaria. Per il contesto Generali la regione primaria Olanda ha il corrispettivo pair in Irlanda.

La policy di geo-backup per Synapse hanno RPO di 24 ore e non possono essere modificate.

E’ possibile anche effettuare degli snapshot estemporanei (user defined) direttamente dal portale di Azure o da PowerShell. In questo caso Azure consente di mantenere fino a 42 punti di ripristino diversi, con una retention sempre di 7 giorni.

## Setup Synapse su North-EU

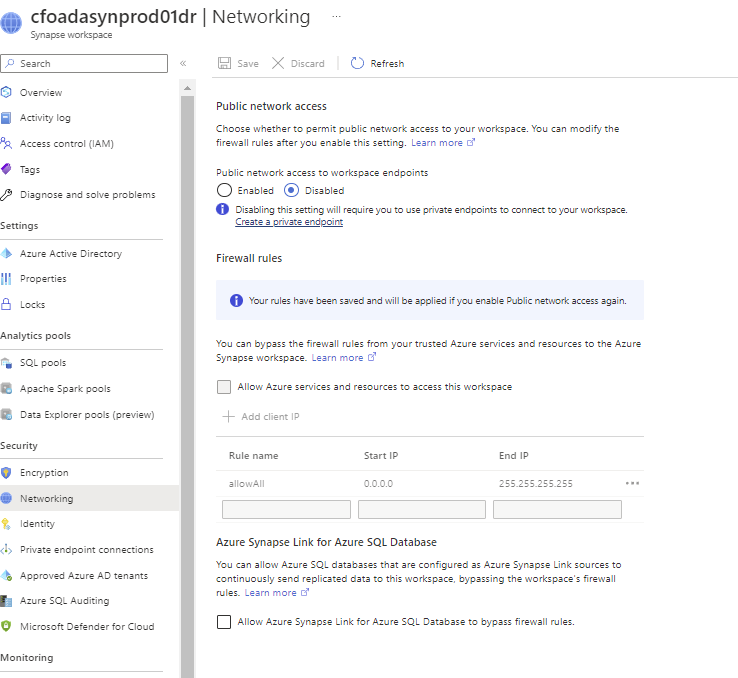
E’ stata creata una nuova istanza di synapse in modalità managed, senza accesso dall’esterno, come è gia stato fatto per i workspace in west europe. Attualmente non sono stati creati i cluster perché non necessari. Nel momento in cui verra fatto un test failover o un failover vero nella procedura verrà indicato come creare l’opportuno cluster/s. Vedi paragrafo opportuno.

L’istanza creata si chiama cfoadasynprod01dr in north europe su subscription GHO Devops e resource group CFO\_ADA\_Production\_rg.

Immagine che contiene testo

Descrizione generata automaticamente

Successivamente sono stati inseriti i private endpoint in modo da poter raggiungere l’istanza della risorsa synapse dall’interno del network di generali e bloccare l’accesso dall’esterno



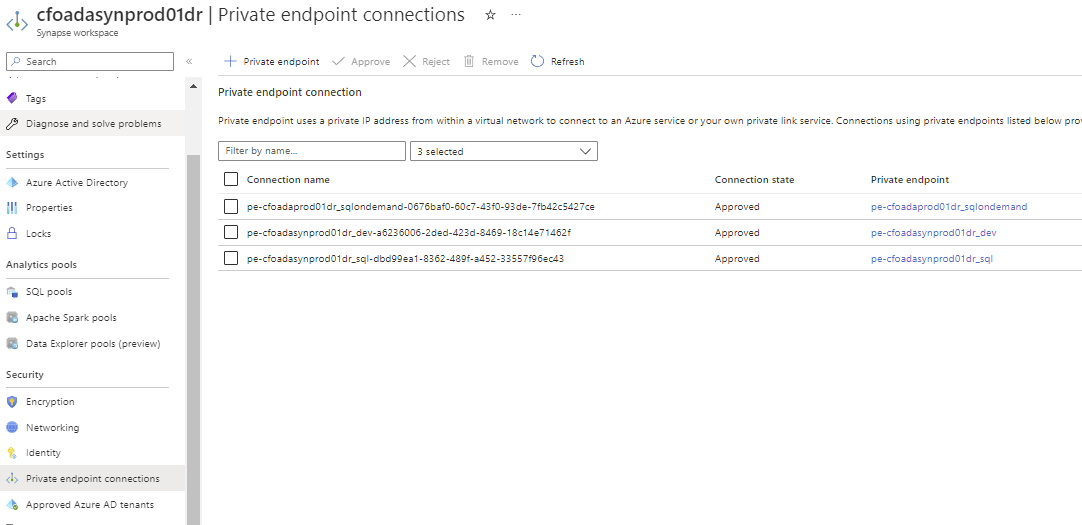
I private endpoint creati sono i seguenti

**pe-cfoadaprod01dr\_sqlondemand (10.206.28.8)**

**pe-cfoadasynprod01dr\_dev (10.206.28.10)**

**pe-cfoadasynprod01dr\_sql (10.206.28.9)**

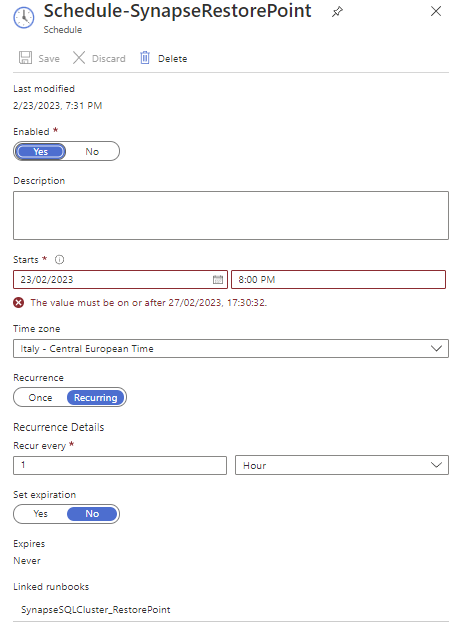
e sono raggiungibili/risolvibili solo dall’interno della vnet in north europe



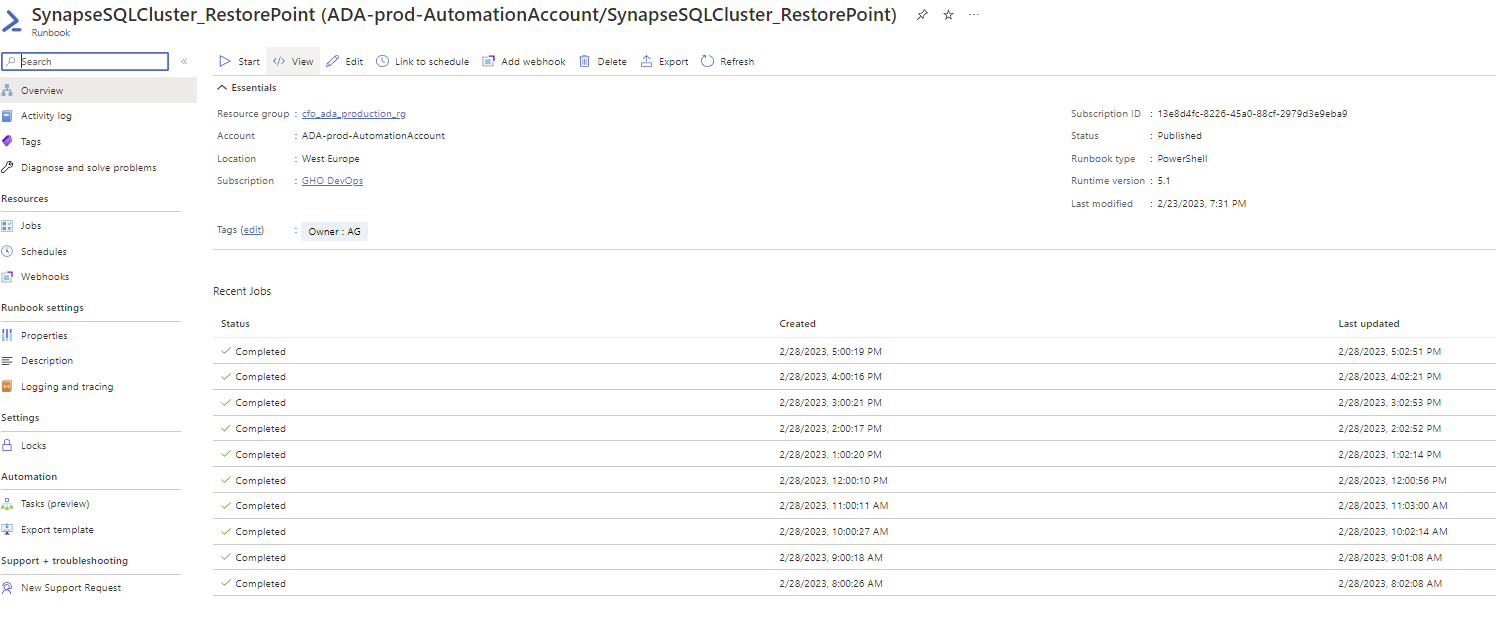
### Setup snapshot script automation

Per migliorare la frequenza di backup e quindi l’RPO, che attualmente a standard synapse è previsto ogni 24 ore, è stato creato uno script in powershell eseguito e schedulato tramite un automation account in azure.Questo script permette la generazione automatica di un nuovo restore point in base ai parametri specificati.

E’ stato impostata la schedulazione di 1 ora per l’esecuzione dello script con il nome Schedule-SynapseRestorePoint



E’ stato definito un runbook chiamato **RestorePointSynapseSQLPools** collegato alla schedulazione di cui sopra.



Lo script riceve dei parametri in input:

ParamSubscriptionName = indicazione della sottoscrizione a cui appartiene il workspace di synapse

ParamResourceGroupName = indicazione del ‘resource group’ a cui appartiene il workspace di synapse

ParamServerName = indicazione del nome del workspace

ParamDatabseName = indicazione del nome del db cluster per cui fare lo snapshot. Specificare più cluster separati da virgola senza spazi per fare lo snapshot multiplo di più cluster.



Lo script recupera la connessione Azure Run As connection (quando verrà sostituito con una managed identity forse sarà necessario rivedere lo script) e sistema il contesto della subscription. Cicla sull’array dei nomi dei cluster db per cui fare il realtivo restore point, con una label del tipo [AUTOMATIC] “nome del workspace” - “orario del restore point”

# Configurazione DR Azure Databricks

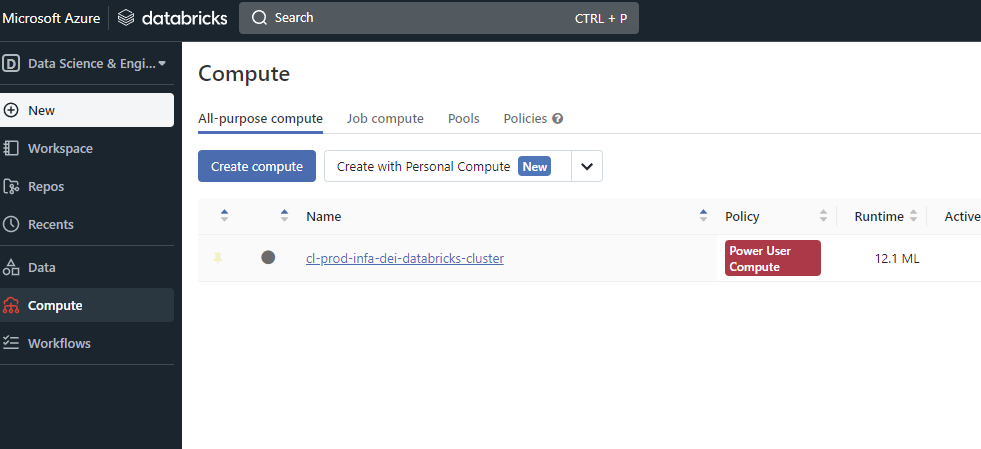
L’attività consiste nella creazione di un nuovo workspace databricks in north europe replica di quello presente in produzione in west europe con il nome **cfoadadatabricksdr**

E’ stato creato successivamente il cluster **cl-prod-infa-dei-databricks-cluster**, accedendo al workspace tramite il seguente indirizzo:

<https://adb-1133888283165035.15.azuredatabricks.net/aad/auth?has=&Workspace=/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/rg-gho-it-prod-ada-001/providers/Microsoft.Databricks/workspaces/cfoadadatabricksdr&WorkspaceResourceGroupUri=/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/databricks-rg-cfoadadatabricksdr-akgrs7gxlq7ns&l=en-us>

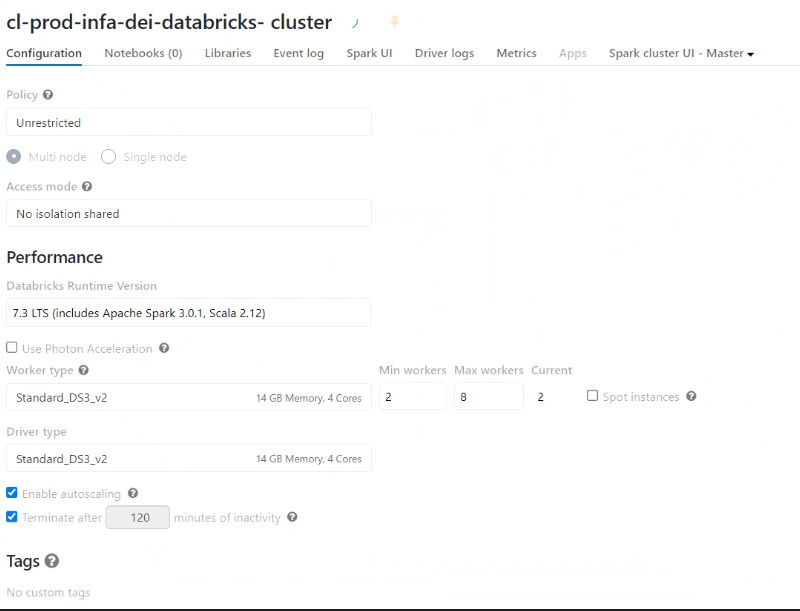
Accedere alla sezione compute options

**cl-prod-infa-dei-databricks- cluster**



E cliccare su compute.

Selezionando le seguenti configurazioni



Modificare anche gli avanced options e copiare lo spark config da ambiente di produzione.

Cliccare su create cluster.

**Successivamente spegnere il cluster (non eliminarlo) e riaccenderlo solo nel caso di test o failover.**

**ATTENZIONE! Nel caso in cui è necessario aggiornare il secret, perché in scadenza, posizionarsi su key vault di DR ADA-KV-PROD-DR e modificare il secret databricksClientSecret, come dovrebbe avvenire già per ambiente di produzione (**[**vedi documentazione relativa**](https://generali.sharepoint.com/:w:/s/DataStrategy2/EdGQaxd6Uc9EmdSUUgAYYgEBf-bq5O4otNDPhip8Hijbkg?e=i5oBbf) **paragraph 3.2)**

**E’ necessario inoltre ricordarsi di aggiornare i file contenenti tutte le caratteristiche di sicurezza nella security area su teams. File di configurazione del databricks e file di configurazione dei service principal.**

# Configurazione DR per Storage Account

Di seguito gli Storage Account di produzione

Immagine che contiene testo

Descrizione generata automaticamente

Microsoft ha una diversa gestione le failover in funzione del tipo di storage account. Per StorageV2 non è possibile una gestione da parte dell’utente ma è Microsoft che governa lo switch alla region secondaria.

Allo stato solo per **cfoadaadslgen2dlprod** è stata definita la ridondanza geografica (RA\_GRS).

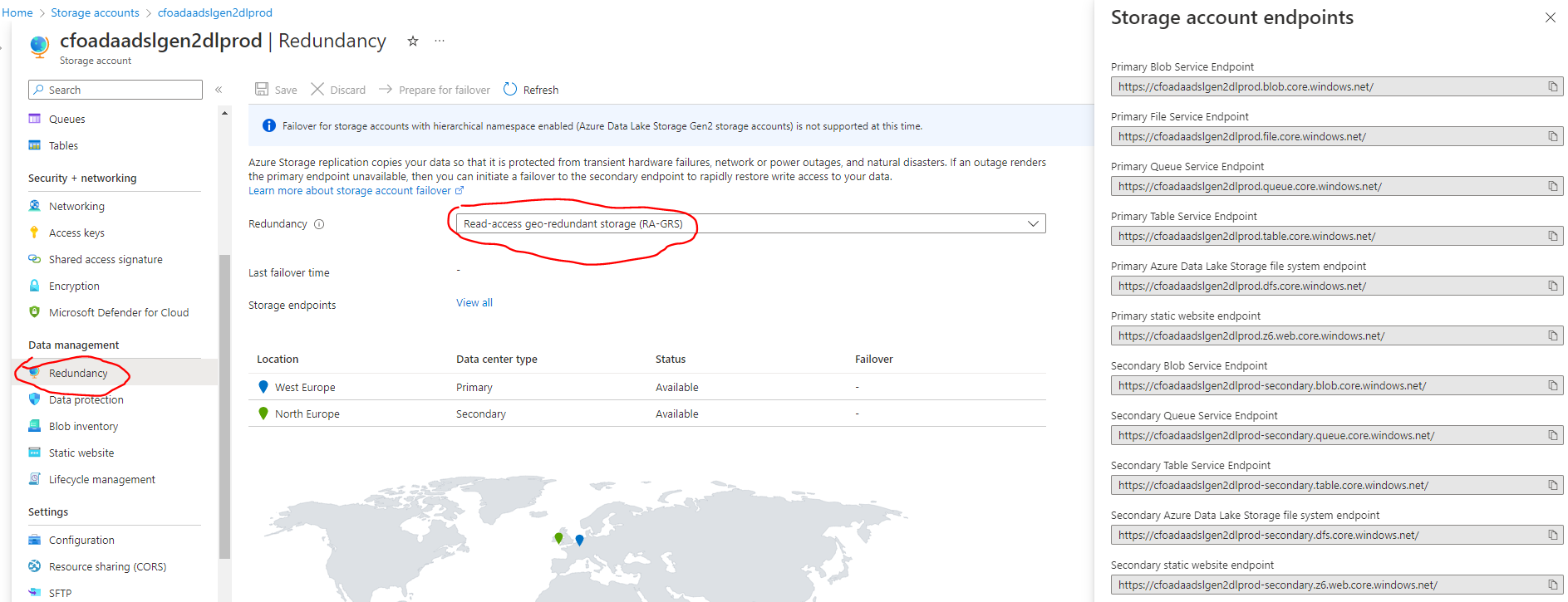


Immagine che contiene testo

Descrizione generata automaticamente

**ATTENZIONE! Nel caso specifico della connsessione di Informatica come da immagine qui sopra bisogna fare attenzione anche all’aggiornamento del secret. Come per databricks qual’ora sia necessario rinnovare il secret perché in scadenza è necessario aggiornare come gia dovrebbe avvenire per l’ambiente di produzione (**[**vedi documentazione ad-hoc**](https://generali.sharepoint.com/:w:/s/DataStrategy2/EdGQaxd6Uc9EmdSUUgAYYgEBf-bq5O4otNDPhip8Hijbkg?e=i5oBbf) **paragraph 3.3) il relativo secret per consentire la corretta connessione di informatica dei dr verso il datalake.**

**E’ necessario inoltre ricordarsi di aggiornare i file contenenti tutte le caratteristiche di sicurezza nella security area su teams. File di configurazione del databricks e file di configurazione dei service principal.**

# Configurazione DR per KEY VAULT

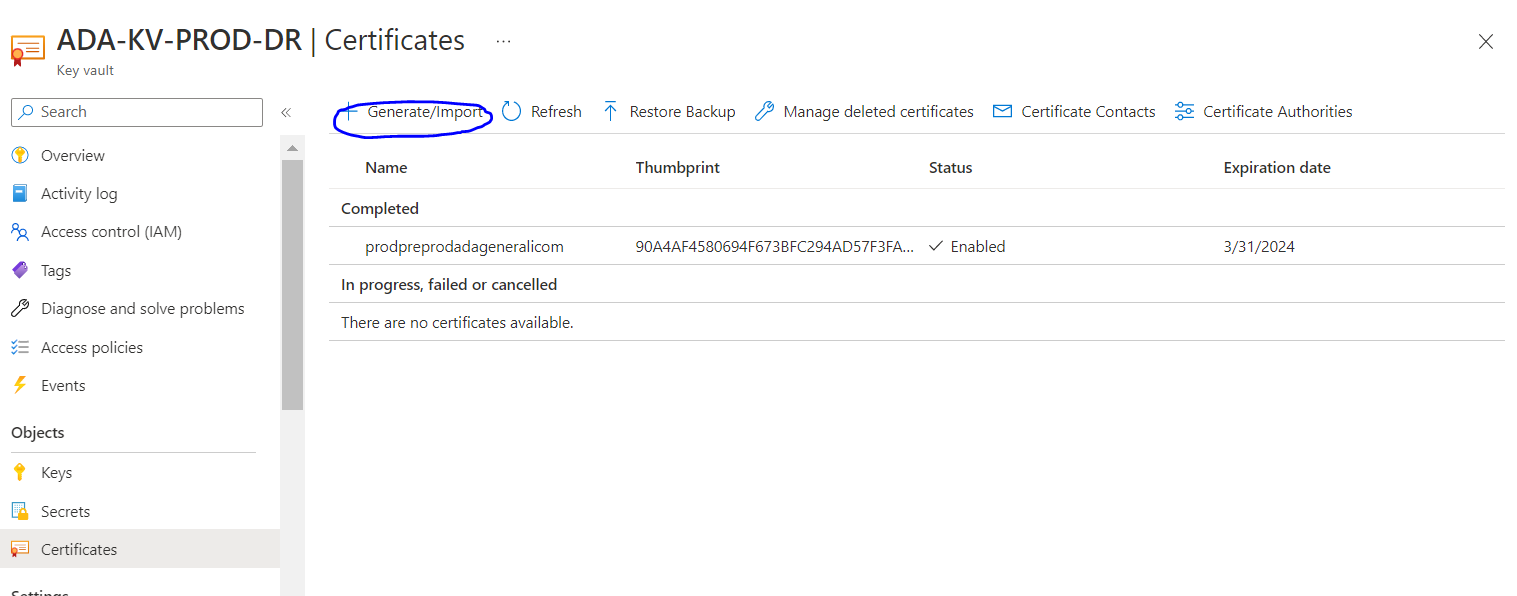
Le risorse key vault sono replicate direttamente cross su tutte le region, e sono garantite da microsoft.

Per questo motivo verrà riutilizzato sempre lo stesso key vault per tutte le configurazioni e password applicative.

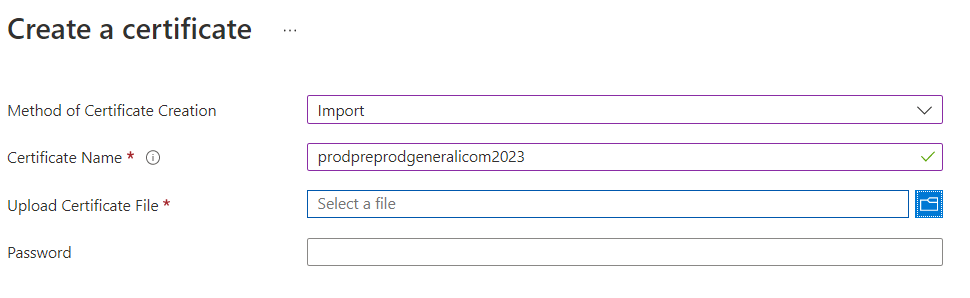
E’ stato creato un key vault anche per il DR **ADA-KV-PROD-DR** per il salvataggio dei certificati pubblici utilizzato dall’application gateway in north europe **ADA-Gateway-DR**

L’accesso ai certificati avviene sempre attraverso la manged instance **cfoadaidentityDR**

Per l’installazione del certificato è necessario entrare nelle sezione Certificates e cliccare su Generate/Import



Inserire tutte le informazioni necessarie per importare il certificato esistente disponibile al seguente folder in teams



# Configurazione DR per Gateway

Non esistono funzionalità native a supporto del DR per application gateway. E’ necessario pertanto procedere manualmente con la replilca di tutte le configurazioni necessarie o passare attraverso il template che Azure predispone sulla risorsa e che contiene tutte le configurazioni al momento in cui il template si crea.

E’ necessario però riportare tutte le modifiche effettuate sul gateway primario dopo la creazione (a mano o con il template) in modo da riportare tutte le configurazioni, in particolare le custom rule per il WAF.

Immagine che contiene testo

Descrizione generata automaticamente

Cui è stata assegnata la configurazuine WAF V2 come quella del gateway primario in modo da consentire la specifica di regole firewall (WAF).

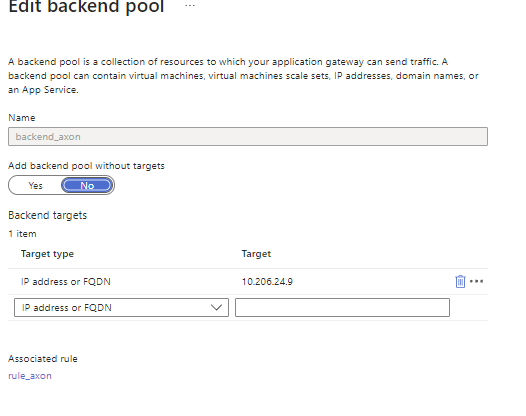
Immagine che contiene testo

Descrizione generata automaticamente

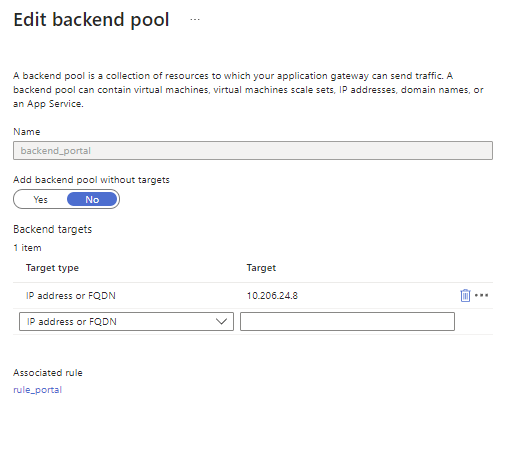
Sono stati definiti dei backend pools

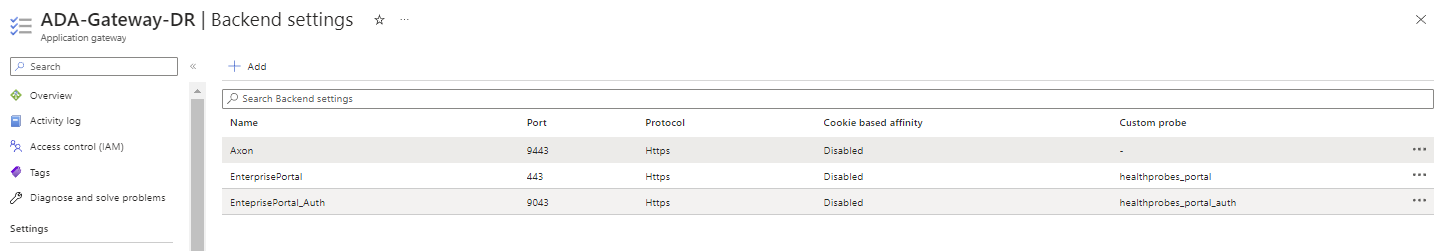


Configurando il backend pool di axon “backend\_axon” che punta all’ip 10.206.24.9



Mentre il backend del portale punta all’indirizzo ip della macchina del portale in north europe.

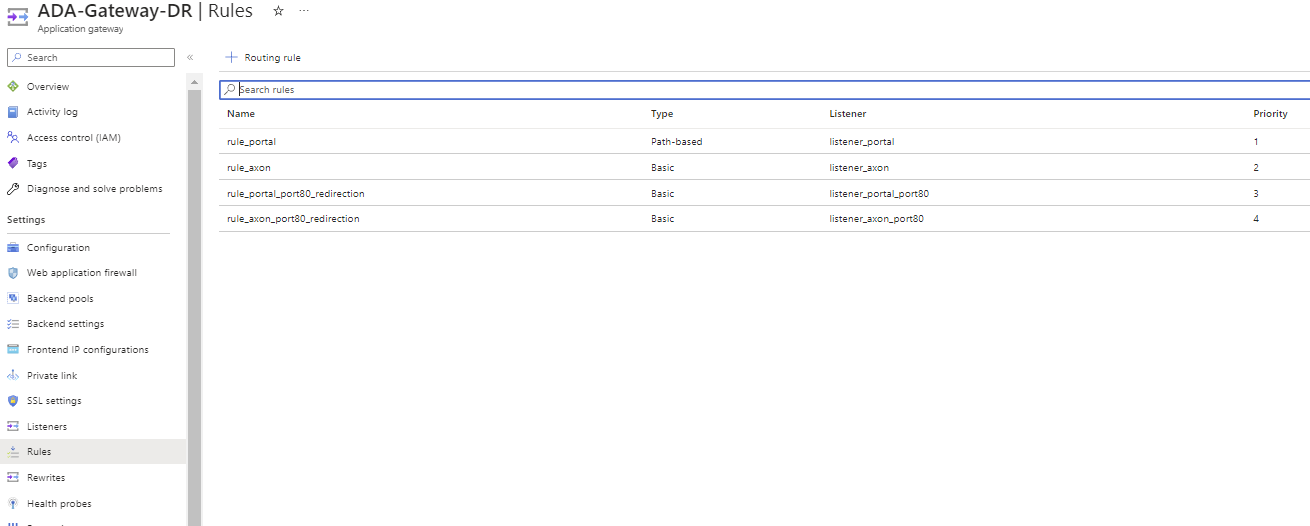




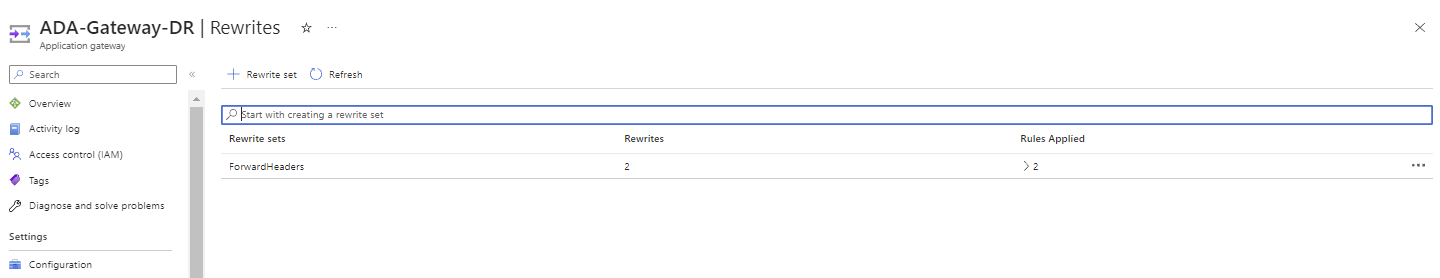
Sono stati configurati 3 backend settings per consentire l’accesso ad:

* Axon con la porta 9443
* Enterprise portal sulla porta 443
* Enterprise portal sulla porta 9043

Sono state definite le regole



Per consentire l’accesso ad axon e portale non che il redirect in caso di errato inserimento http o mancanza del path sull’url per il portale.



Sono stati inoltre definiti i forwards reader per gestire la parte di autenticazione su axon e portale con il server ADFS.

# Configurazione dei traffic manager

I traffic manager sono stati introdotti per gestire lo switch di alcune risoluzione di nomi tra west e north europe.

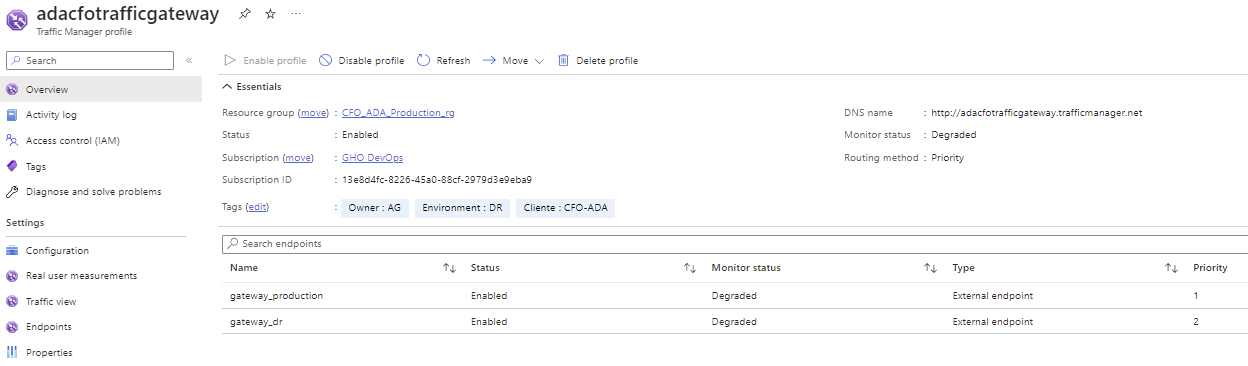
ATTENZIONE! Per testare il traffic manager sicuramente crea impatto in ambiente di produzione per cui il test su queste risorse deve essere preventivamente concordato

In particolare i traffic manager sono stati impiegati per gestire le seguenti risoluzioni:

* Portale e axon
* VM di Informatica DEI
* VM SFTP

## Portale e Axon

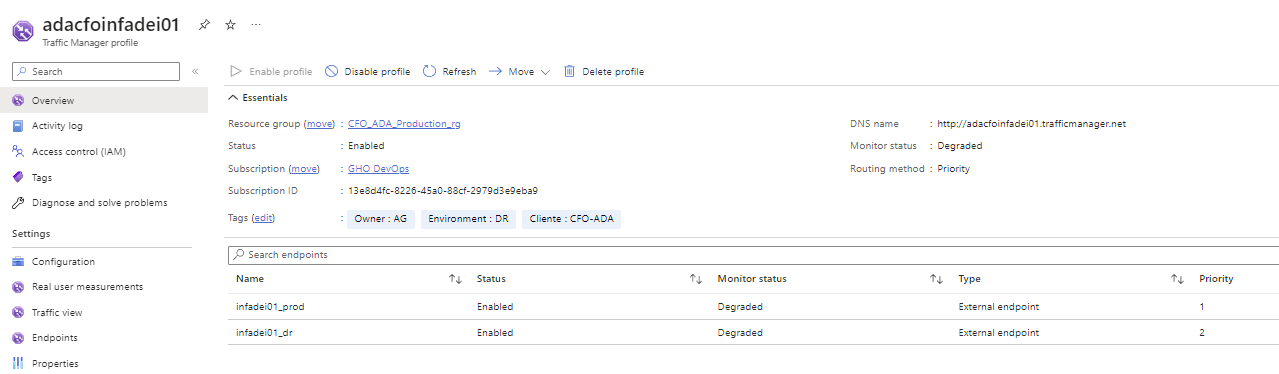
Viene naturale utilizzare questa risorse per permettere lo switch della risoluzione dei nomi sul portale da west europe a north europe. Attività da effettuare in fase di failover o di test dr. E’ stata anche cambiato il DNS publico associando due alias ada.generali.com e ada-axon.generali.com all’indirizzo del traffic manager <https://adacfotrafficgateway.trafficmanager.net>. In questo modo quando decidiamo di effettuare il failover in north europe tutto il traffico verrà dirottato all’indirizzo ip del gateway in north europe pur mantenendo i nomi originali ada.generali.come ada-axon.generali.com.



Vedere punti di attenzione in fase di test failover.

## VM di Informatica DEI

Nel seguente caso l’uso del traffic manager è stato un forzato per l’impossibilità di gestire diversamente i dns interni di generali, per la risoluzione dei private IP delle due macchine in west e north europe. Per cui la risoluzione del nome della macchina permette di girare il traffico in north europe quando viene effettuato il failover o il relativo test dr. L’indirizzo del traffic manager da utilizzare è <https://adacfoinfadei01.trafficmanager.net>

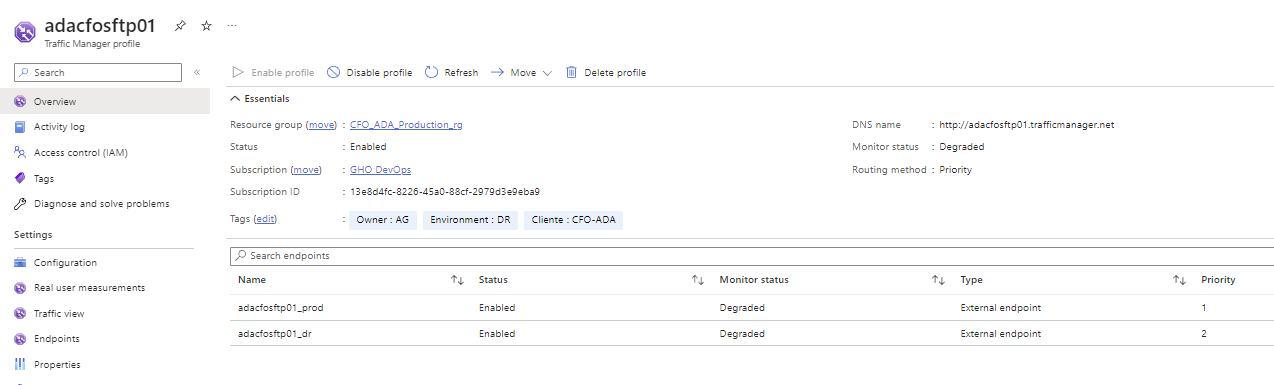


CONSIGLIO! L’impiego dell’indirizzo del traffic manager sui client degli sviluppatori per accedere all’ambiente di produzione permette di rendere il passaggio da north a west europe in maniera più trasparente

Vedere punti di attenzione in fase di test failover

## VM SFTP

Anche nel seguente caso l’uso del traffic manager è stato un forzato per l’impossibilità di gestire diversamente i dns interni di generali, per la risoluzione dei private IP delle due macchine in west e north europe. Per cui la risoluzione del nome della macchina permette di girare il traffico in north europe quando viene effettuato il failover o il relativo test dr. L’indirizzo del traffic manager da utilizzare è <https://adacfosftp01.trafficmanager.net>



CONSIGLIO! L’impiego dell’indirizzo del traffic manager sui client o sugli applicativi che accedono all’ambiente di produzione permette di rendere il passaggio da north a west europe in maniera più trasparente

Vedere punti di attenzione in fase di test failover

# Configurazione INFORMATICA DEI

Nessuna rilevante attività di preparazione se non soltanto il setup della macchina IaaS sul site recovery.

In aggiunta sono stati creati dei workflow di test in modalità read-only sul datalake, in modo da utilizzare sia la componente del server di informatica e la componente del databricks.

La lista dei nomi dei workflow è la seguente:

* wf\_test\_databricks
* wf\_test\_datalake

Questi workflow saranno individuabili nel progetto Test\_DR sulla macchina dei in north europe.

# Preparazione al TEST Failover

Tutti i test di failover previsti nel runbook test verranno effettuati dalla macchina di test vm-dev-infa-win-01-dr (10.206.24.4).

## Preparazione Test Failover Key Vault

Nel Key vault di west europe in fase di preparazione è necessario cambiare il puntamento alla replica dell’elastic pool, con le dovute precauzioni. Vedi paragarafo Preparazione Test per il portale custom.

## Preparazione Test Application Gateway

Nessuna attività preliminare è richiesta. Verificare che le attività di modifica in west europe siano correttamente replicate sul gateway di north europe.

## Preparazione Test Failover SFTP

Dopo avere avviato il “test failover” dal portale di Azure, non sono necessarie ulteriori attività di configurazione: il server è disponibile per l’utilizzo in una sessione sFTP. Il test dovrà essere effettuato partendo dalla macchina vm-dev-infa-win-01-dr

## Predisposizione Test Failover per SQL Server

Il failover group, sebbene sia una replica completa ed allineata per i Database, è in sola lettura. Diventa scrivibile solo a seguito di un failover e non si può tornare indietro.

Per questa ragione, per effettuare il test del DR è necessario definire una nuova “replica” scrivibile che a completamento del test potrà essere distrutta, altrimenti gli strumenti di informatica dei e il portale non potranno funzionare.

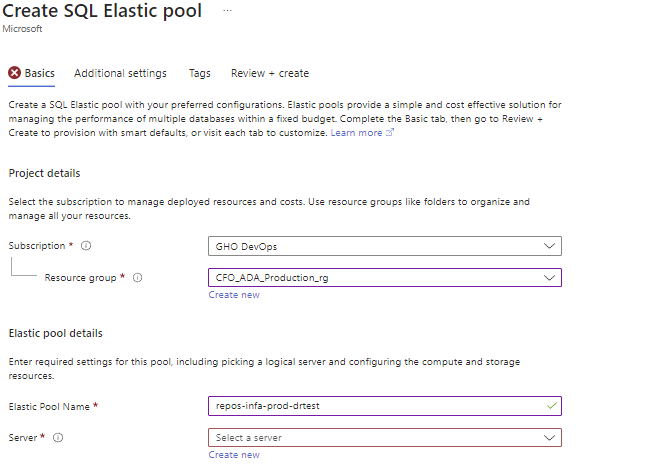
La strada da seguire per il test failover è di creare, al momento del test, un nuovo SQL Server e replicare su di esso i Database delle applicazioni/sistemi oggetto del test.

### Creazione del Server SQL replicato e scrivibile

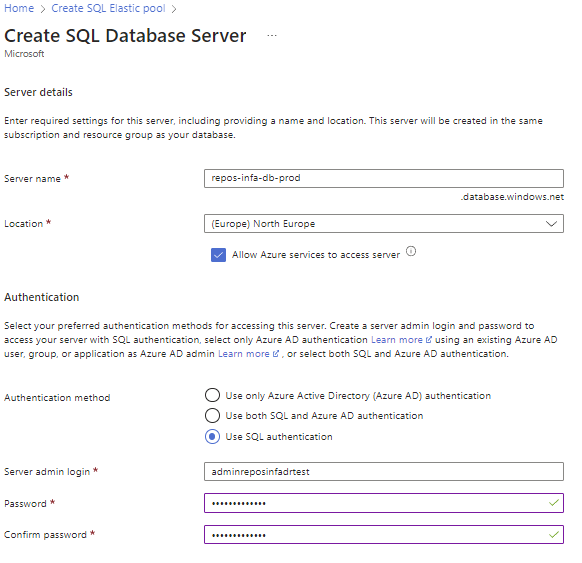
NJOTA: Il nome del database server è repos-infa-db-prod-dr da sistemare gli screenshot

Per la creazione di una copia di SQL server è necessario seguire i seguenti passi:

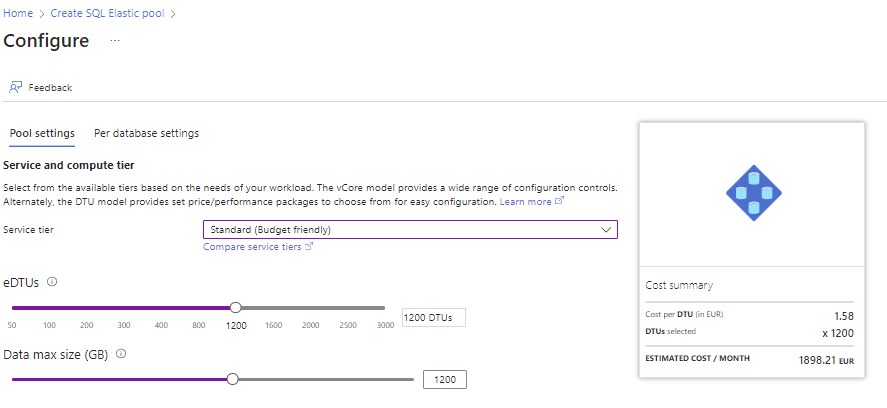
1. Creare un nuovo elastic pool in north europe chiamato repos-infa-prod-drtest. Vedi le configurazioni qui sotto e i vari step a livello di interfaccia



1. Creare un nuovo sql server con lo stesso nome (repos-infa-db-prod) e dimensionato almeno in termini di spazio quanto quello presente in west europe. Impostando l’utente admin come adminreposinfadrtest

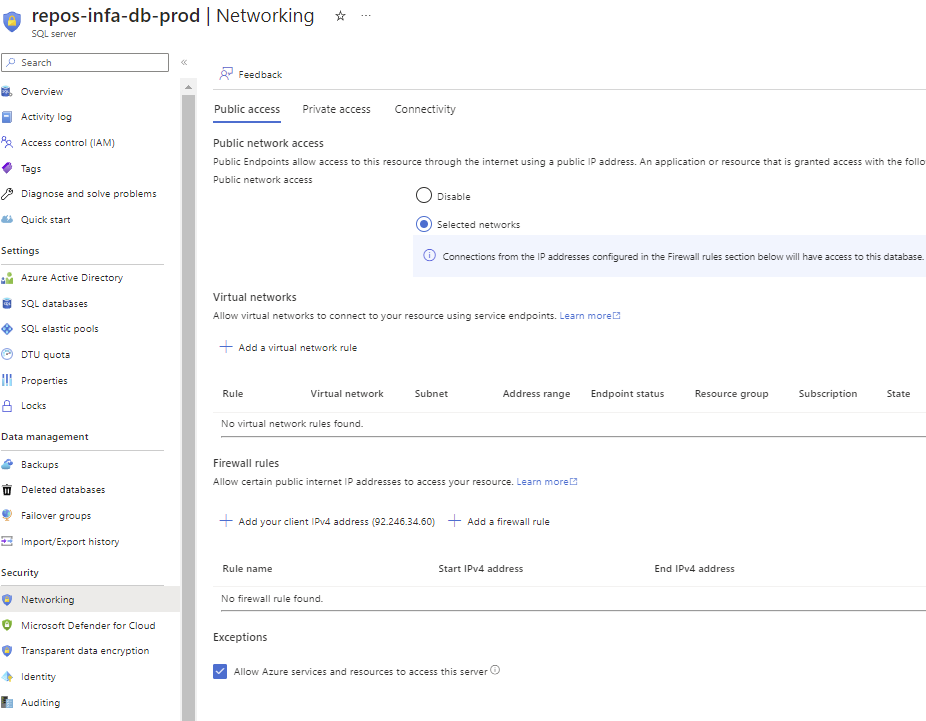


1. Una volta creato l’istanza sql procedere con il dimensionamento dell’elastic pool cliccando su “configure elastic pool” e impostando i seguenti valori sempre proporzionati rispetto alle dimensioni attualmente di produzione in west europe



1. Procediamo con i next step senza modifiche particolari alla creazione della risorsa elastic pool.

Completata l’attività di creazione dell’elastic pool repos-infa-prod-drtest accedere al setup della sezione networking sul server in north europe, flaggando le Exceptions “Allow Azure Services and resources to access this server”. Questo servirà per consentire l’accesso al database server con il client SSMS in vm-dev-infa-win-01-dr.



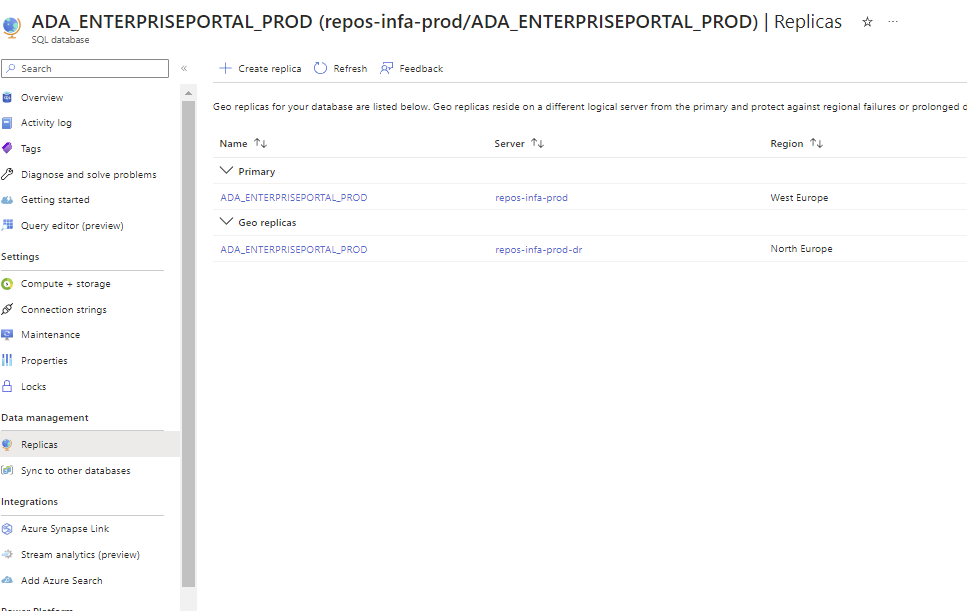
Si procede a questo punto con la creazione per ogni database da replicare con la geo-replica dall’ambiente di produzione west-europe verso l’ambiente di testdr nort-europe appena creato.

La stessa procedura deve essere fatta per ogni db da replicare.

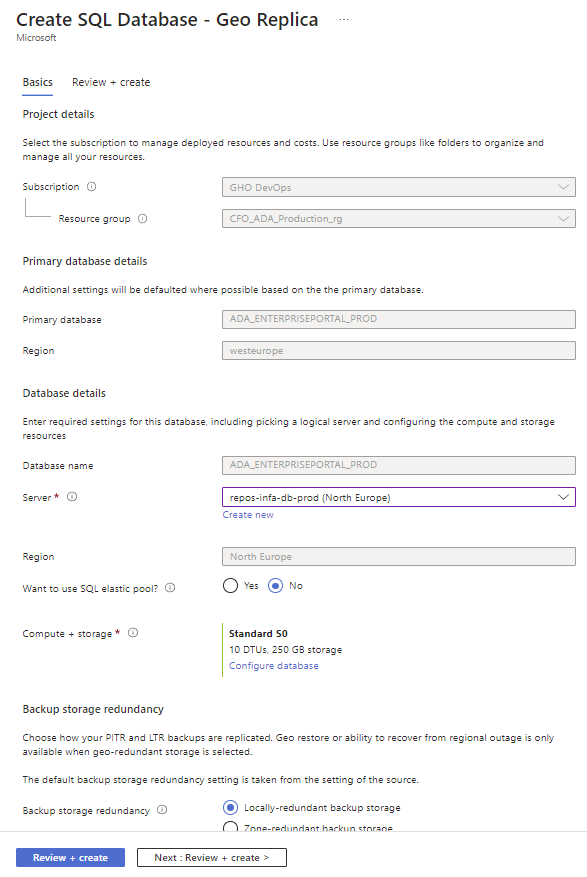
I db da replicare sono:

* ADA\_ENTERPRISE\_PORTAL\_PROD
* INFADBPROD

1. Entrare nella sezione del DB in west europe produzione cliccando su Replicas.



1. Cliccare su “create replica”, facendo attenzione ad inserire il database server corretto in north-europe



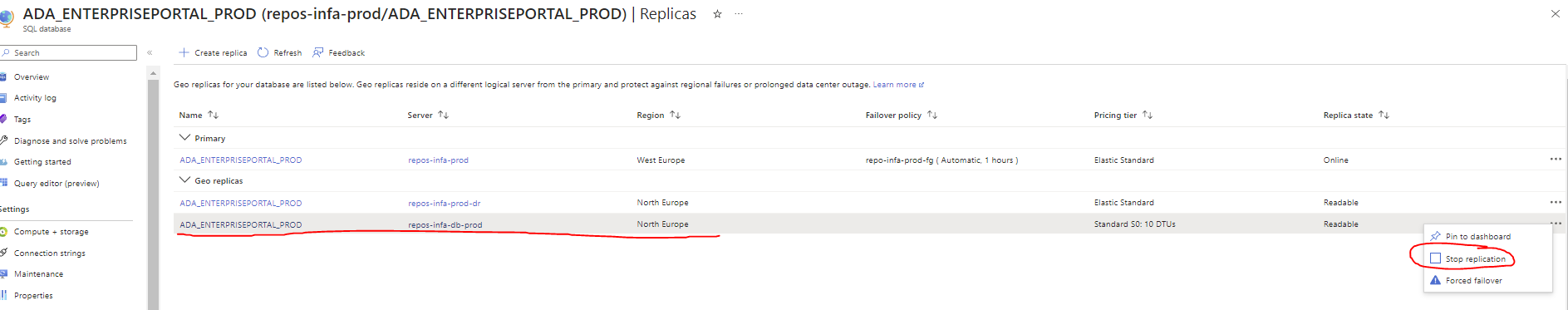
1. Proseguire con i next step fino alla creazione della georeplica.

Completata la geo-replica bisogna sganciare il db dalla georeplica in modo che non sia più readable ma scrivibile.

Per procedere con lo sgancio della georeplica:

1. posizionarsi sul db di west europe nella sezione replicas.

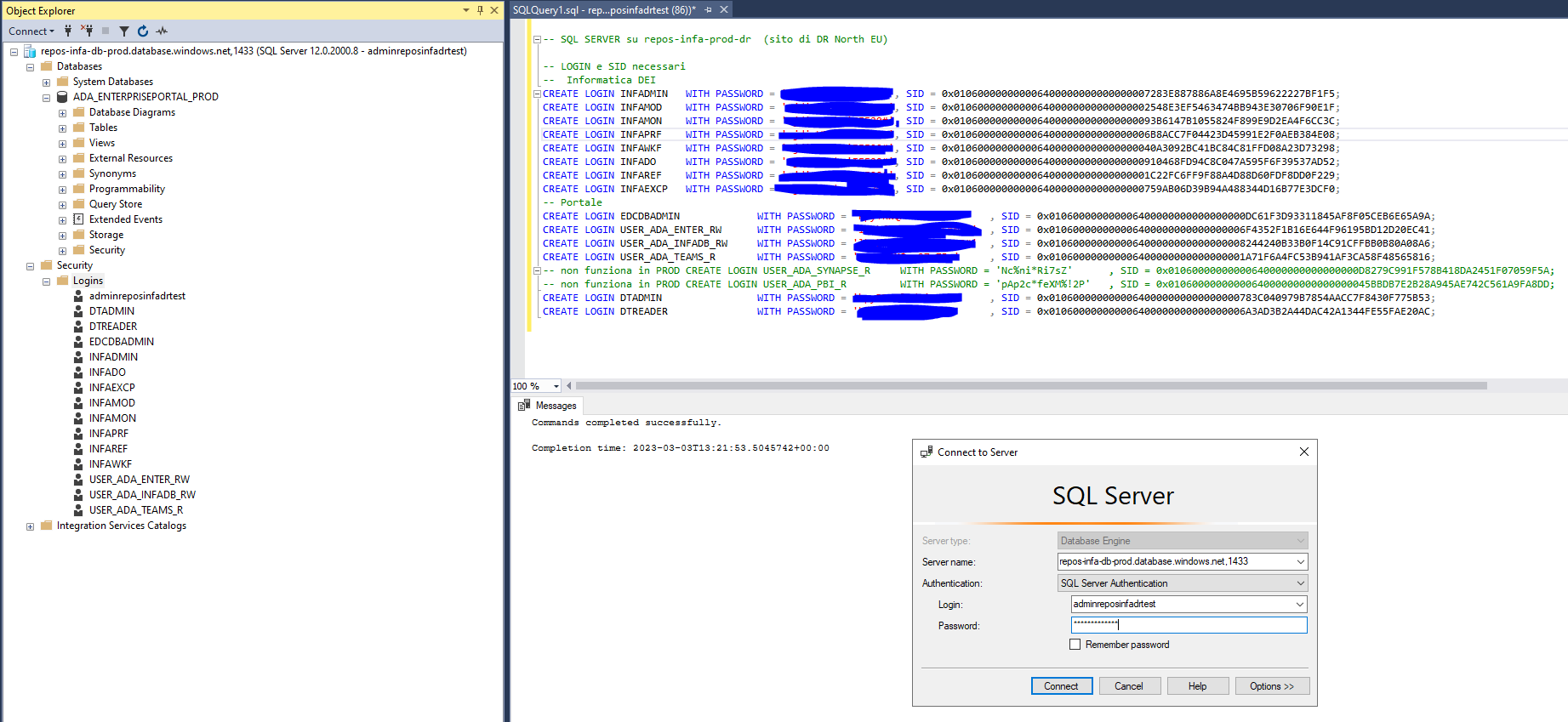
2. ci sarà il db georeplicato appena creato che è possibile sganciare cliccando su stop replication.

ATTENZIONE NON SGANCIARE LA GEOREPLICA DEL FAILOVER GROUP.

Attendere 10 minuti perché lo sgancio sia completato. Una volta sganciato il db sarà scrivibile in north europe

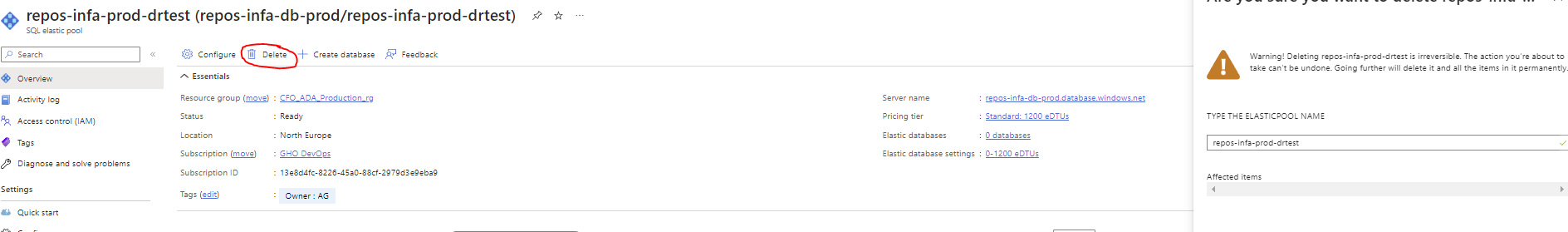
La stessa attività deve essere fatta per tutti db da replicare.

Per finalizzare la configurazione di queste repliche accedere al database server in north-europe dalla vm vm-dev-infa-win-01-dr, ed eseguire gli stessi script per replicare i login dei due database sql server disponibili nel capitolo “2.1.2 Creazione delle Login su SQL Server North-EU”.

x\

### Dismissione a seguito della chiusura dei test

Per dismettere le risorse create in north-europe al solo scopo del test andare sulla risorsa elastic pool e cancellare tutti i db ad esso associati, poi il server ed infine l’elastic pool rispettando questo ordine.



ATTENZIONE! Fare attenzione a non cancellare west europe o il failover group in north europe

## Preparazione Test Failover per Informatica AXON

Le attività dovranno essere eseguite successissevamente all’esecuzione del test failover.

Informatica AXON è un sistema le cui componenti sono tutte presenti all’interno dello stesso server che ha come Sistema Operativo Linux RedHat 7.9.

Accedere al server con una connessione SSH. L’installazione di Axon è stata eseguita dallo user infaaxn.

Dopo avere acceduto al server con lo user infaaxn, spegnere i servizi Axon (dovrebbero essere stati attivati in automatico) con il comando:

sh /informatica/axon7.2/bin/shutdown.sh

E’ necessario modificare l’hostname nei file di configurazione e nella VM

# modifica dell’hostname nel file /etc/hostaname

sudo hostnamectl set-hostname vm-prod-infa-axn-01-idm-dr

#modifica dell’hostname nei file di configurazione

cd /informatica/axon7.2/bin

sh changehostname.sh vm-prod-infa-axn-01-idm-dr.azure.generali-cloud.com

#riavviare I servizi di Axon

sh startup.sh

# attendere qualche minuto e poi verificare che tutti i servizi siano attivati

cd /informatica/axon7.2/axonhome/third-party-app/scripts

./axonStatus

Far riferimento alla KB:

*https://knowledge.informatica.com/s/article/000097678?language=en\_US*

Le interconnessioni con sistemi esterni sono relative a:

* configurazione del SSO che richiama la url per l’autenticazione in CPAS
* estrazione delle misure di qualità dalle scorecord in Informatica DEI/DEQ.

La configurazione SSO viene rimandata alla configurazione del gateway in DR.

In alternativa si può fare il test senza SSO disabilitando la configurazione derivata dal server primario ed eseguendo sul server Axon DR i seguenti comandi:

cd /informatica/axon7.2/scripts/

source exportEnv.sh

cd /informatica/axon7.2/axonhome/third-party-app/php/bin

./php /informatica/axon7.2/axonhome/axon/bin/console informatica:sso-disable

cd /informatica/axon7.2/axonhome/third-party-app/scripts/

./paramsync

Per riabilitare il SSO

cd /informatica/axon7.2/scripts/

source exportEnv.sh

cd /informatica/axon7.2/axonhome/third-party-app/php/bin

./php /informatica/axon7.2/axonhome/axon/bin/console informatica:sso-enable

cd /informatica/axon7.2/axonhome/third-party-app/scripts/

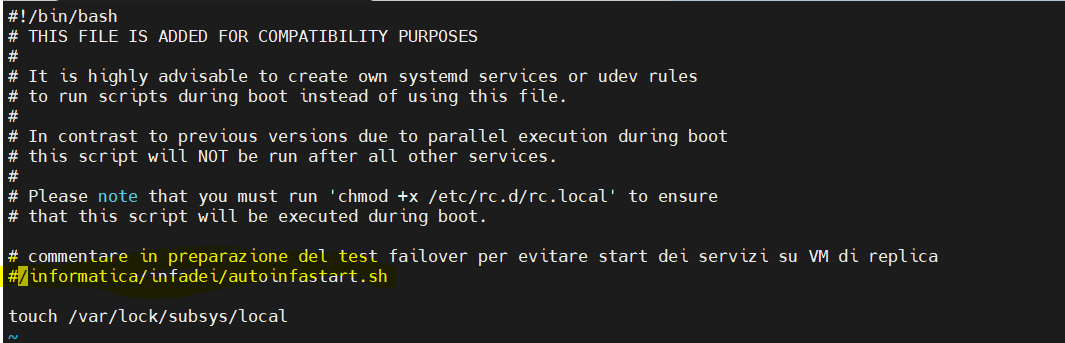
./paramsync

## Preparazione Test Failover Informatica DEI/DEQ

Le azioni descritte di seguito richiedono che:

* sia stata attivata la (seconda) replica di DB Sql Server e siano state create le login relativa ad Informatica DEI
* sia stato predisposto Databricks su North-EU.

Nota: sul server primario vm-prod-infa-dei-01-idm è necessario “spegnere” l’avvio automatico dei servizi di Informatica in modo che quanto si avvia la VM di DR questi non partino in automatico. E’ necessario intervenire su /etc/rc.local e commentare il comando di avvio dei servizi di Informatica:



Attendere qualche minuto in modo che la modifica sia recepita anche sulla replica.

Avviare “test failover” per la VM di replica.

Immagine che contiene testo

Descrizione generata automaticamente

Quindi avviare la VM e connettersi in SSH con le stesse modalità della VM primaria (user AzureUser – passphrase), quindi collegarsi con l’utente **infadei**.

### Connessione al DB INFADBPROD

Se non stati definiti endpoint privati per il DB SQL Server di replica è necessario inserire nella sua white list l’IP del server di Informatica in DR (10.206.24.7), mentre sul server Informatica DEI DR inserire in /etc/hosts la risoluzione dell’endpoint al DB.

Deve essere modificato l’hostname della VM (essendo i discgi delle repliche portano con loro tutta la configurazione del server primario:

Entrare come root per fare questa attività:

sudo hostnamectl set-hostname vm-prod-infa-dei-01-idm-dr

Prima della seguente attività entrare come infadei sudo su - infadei

Deve essere modificata la stringa di connessione al “dominio” di Informatica e l’hostname del nodo su cui è eseguito Informatica con i comand:

*cd $INFA\_HOME/isp/bin*

*./infasetup.sh updategatewaynode -cs "jdbc:informatica:sqlserver://****repos-infa-prod-dr****.database.windows.net:1433;database=INFADBPROD;encrypt=true;trustServerCertificate=false;hostNameInCertificate=\*.database.windows.net;loginTimeout=30;EncryptionMethod=SSL;ValidateServerCertificate=false" -dn DMN\_DEI\_PRD*

*./infasetup.sh updategatewaynode -na vm-prod-infa-dei-01-idm-dr.azure.generali-cloud.com:6005 -rst*

Prima di riavviare la macchina eseguire questi comandi di pulizia ambiente:

*cd /informatica/infadei/services/DataIntegrationService/*  
*rm -R sqldataviewer*  
*rm -R DataIntegrationService*  
  
*cd /informatica/infadei/services/SchedulerService*  
*rm -R Scheduler*  
  
*cd /informatica/infadei/tomcat/bin/target/repository/1595859022617/MRS\_DEI\_PROD/index*  
*rm -R searchdata*  
  
*cd /informatica/infadei/tomcat/bin/target/repository/1595858796637/mMRS\_DEI\_PROD/index*  
*rm -R searchdata*  
  
*cd /informatica/infadei/services/work\_dir*  
*rm -R MassIngestion*  
*rm -R ContentManagementService*  
*rm -R DataIntegrationService*  
*rm -R ModelRepositoryService*  
*rm -R AnalystService*  
  
*cd /informatica/infadei/tomcat/work*  
*rm -R Catalina*  
  
*cd /informatica/infadei/tomcat/temp*  
*rm -rf \**  
  
*cd /informatica/infadei/tomcat/webapps*  
*rm -R adminconsole*  
*rm -R ROOT*  
*rm -R csm*  
*rm -R coreservices*

Questi comandi andranno rifatti anche dopo la modifica di tutte le connessioni.

Da putty o altro adnda seul server sulla path cd /informatica/infadei/ODBC7.1

Aprire l’odbc.ini

E modificare tutti i puntamenti :

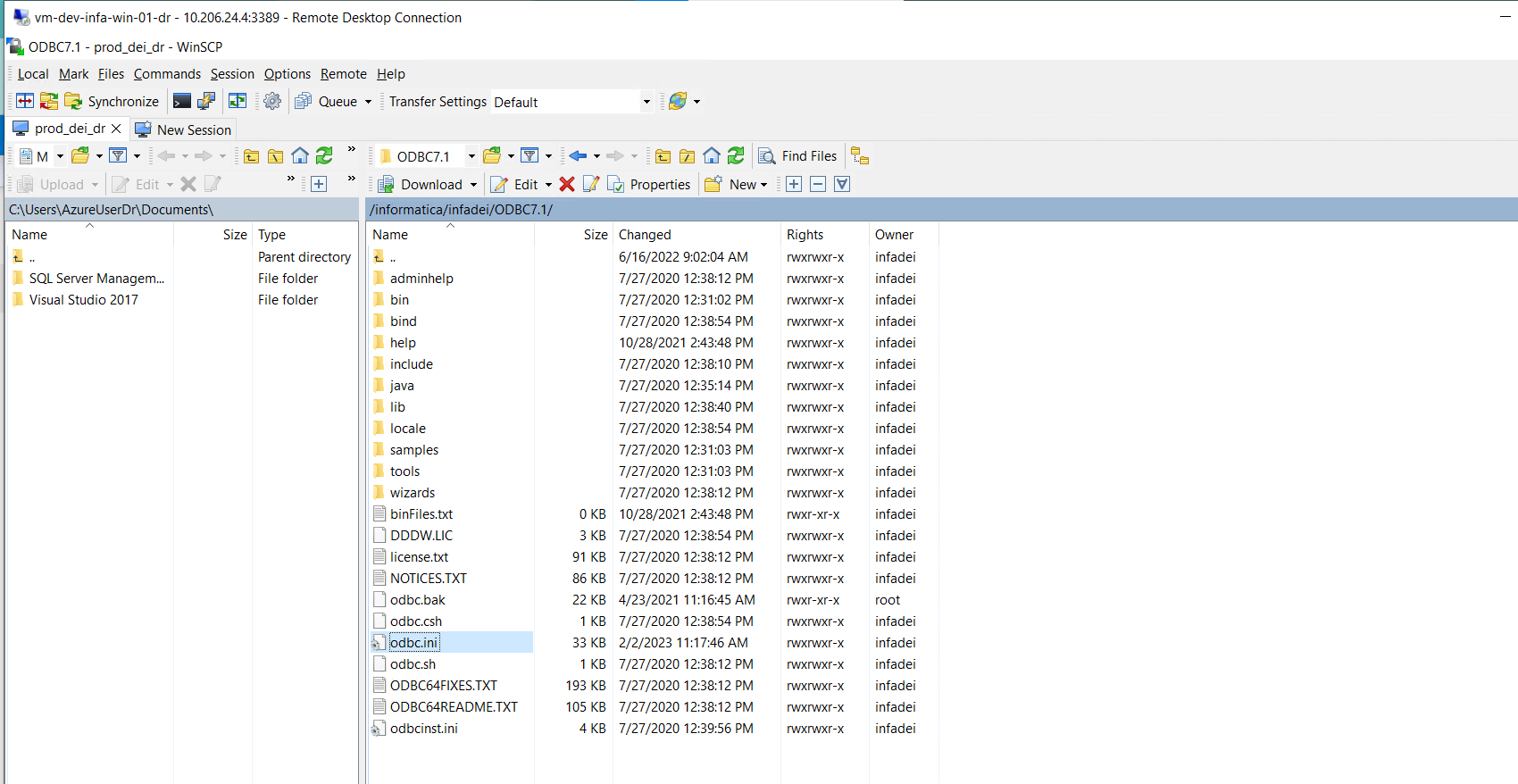
Esempio :

[repos-infa-prod.dsn]

HostName=repos-infa-prod.database.windows.net a --> HostName=repos-infa-prod-testdr.database.windows.net

[CON\_SQL\_EDCDB]

HostName=repos-infa-prod.database.windows.net a --> HostName=repos-infa-prod-testdr.database.windows.net



Avviare quindi i servizi di Informatica:

cd $INFA\_HOME/tomcat/bin

./infaservice startup

Attendere qualche minuto e aprire su browser la console di amministrazione alla url:

<https://vm-prod-infa-dei-01-idm-dr.azure.generali-cloud.com:8443/administrator>

Inserire le credenziali dell’utenza Administrator.

Modificare la stringa :

Dalla console di amministrazione devono essere modificate le stringhe di connessioni al DB SQL Server per i servizi: Model Repository Service – MRS\_DEI\_PROD. La url di connessione repo-infa-prod-fg deve essere sostituita con repos-infa-prod-testdr.

Immagine che contiene testo

Descrizione generata automaticamente

Con modalità simili è necessario agire sulla configurazione di mMRS\_DEI\_PROD e delle connessioni:

* CACHE
* CON\_SQL\_EDCDB
* CON\_SQL\_EDCPORTAL
* CON\_WHTREP
* EXCP
* PRF
* REF
* WKF

Stoppare i servizi ed eseguire questi comandi di pulizia ambiente:

*cd /informatica/infadei/services/DataIntegrationService/*  
*rm -R sqldataviewer*  
*rm -R DataIntegrationService*  
  
*cd /informatica/infadei/services/SchedulerService*  
*rm -R Scheduler*  
  
*cd /informatica/infadei/tomcat/bin/target/repository/1595859022617/MRS\_DEI\_PROD/index*  
*rm -R searchdata*  
  
*cd /informatica/infadei/tomcat/bin/target/repository/1595858796637/mMRS\_DEI\_PROD/index*  
*rm -R searchdata*  
  
*cd /informatica/infadei/services/work\_dir*  
*rm -R MassIngestion*  
*rm -R ContentManagementService*  
*rm -R DataIntegrationService*  
*rm -R ModelRepositoryService*  
*rm -R AnalystService*  
  
*cd /informatica/infadei/tomcat/work*  
*rm -R Catalina*  
  
*cd /informatica/infadei/tomcat/temp*  
*rm -rf \**  
  
*cd /informatica/infadei/tomcat/webapps*  
*rm -R adminconsole*  
*rm -R ROOT*  
*rm -R csm*  
*rm -R coreservices*

Riattivare i servizi.

### Connessione a Databricks su DR

Sulla VM di Informatica DEI in DR è necessario modificare la configurazione della connessione usata per Databricks:

Immagine che contiene testo

Descrizione generata automaticamente

Con l’opzione di refresh si fa in modo di puntare al nuovo Databricks di cui è necessario conoscere:

* **Databricks Domain**: è l’end-point del cluster
* **Databricks Token ID**: è una stringa che restituisce Azure al momento della creazione del cluster
* **Cluster ID**: E’ l’identificativo del cluster

Immagine che contiene testo

Descrizione generata automaticamente

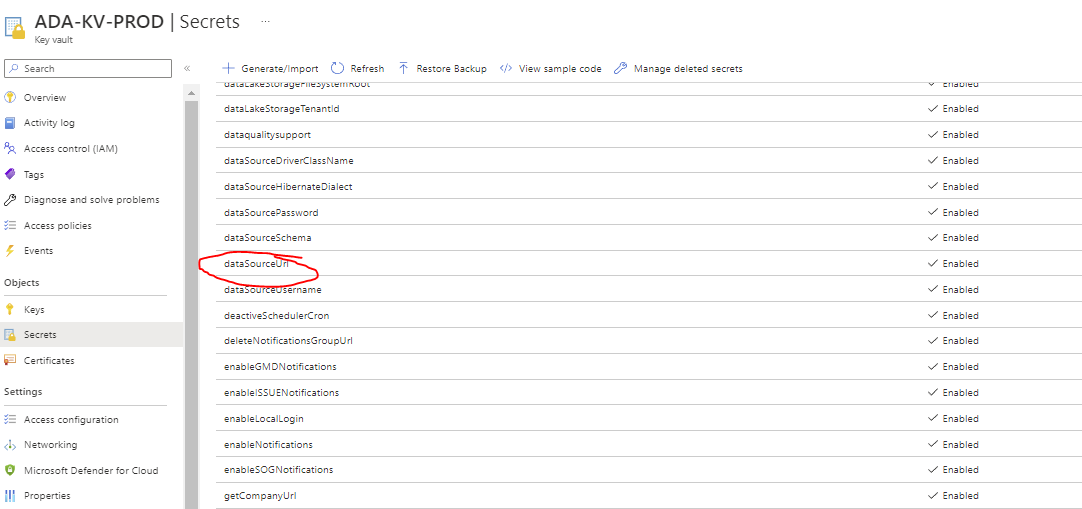
Salvare la nuova configurazione.

Al momento del primo test Informatica installa le librerie necessarie sul cluster. Dopo lo spegnimento del cluster Databricks le librerie non vengono rimosse, pertanto nei successivi test non è necessario aggiornarle, e sono ancora valide in caso di failover effettivo.

**NOTA: in caso di aggiornamento del run time di Databricks primario (es. LTS 9.x) è necessario procedere all’aggiornamento di Databricks in DR.**

## Preparazione Test Failover Custom App

La preparazione al test failover per la custom app consiste nel cambiare preventivamente (prima dell’avvio del test failover del server IaaS) il puntamento della connection string al database utilizzato per il test failover. La connection string si trova sul key vault di produzione



L’informazione si trova nel secret dataScourceUrl il cui valore è

jdbc:sqlserver://repo-infa-prod-fg.database.windows.net:1433;database=ADA\_ENTERPRISEPORTAL\_PROD;encrypt=true;trustServerCertificate=false;hostNameInCertificate=\*.database.windows.net;loginTimeout=30

e deve essere cambiato in

jdbc:sqlserver://repo-infa-prod-dr.database.windows.net:1433;database=ADA\_ENTERPRISEPORTAL\_PROD;encrypt=true;trustServerCertificate=false;hostNameInCertificate=\*.database.windows.net;loginTimeout=30

ATTENZIONE! Una volta cambiata questa impostazione bisogna fare attenzione a non riavviare il server di produzione in westeurope altrimenti il server recepirà la connessione al database sbagliato **con impatti in produzione.**

Una volta sistemata questa configurazione si potrà avviare il server in modalità test failover in north europe.

ATTENZIONE! Una volta acceso il server in north europe, ricordarsi di ripristinare la connessione al db di produzione sul key vault di produzione per evitare gli impatti in produzione.

## Preparazione Test Failover Synapse

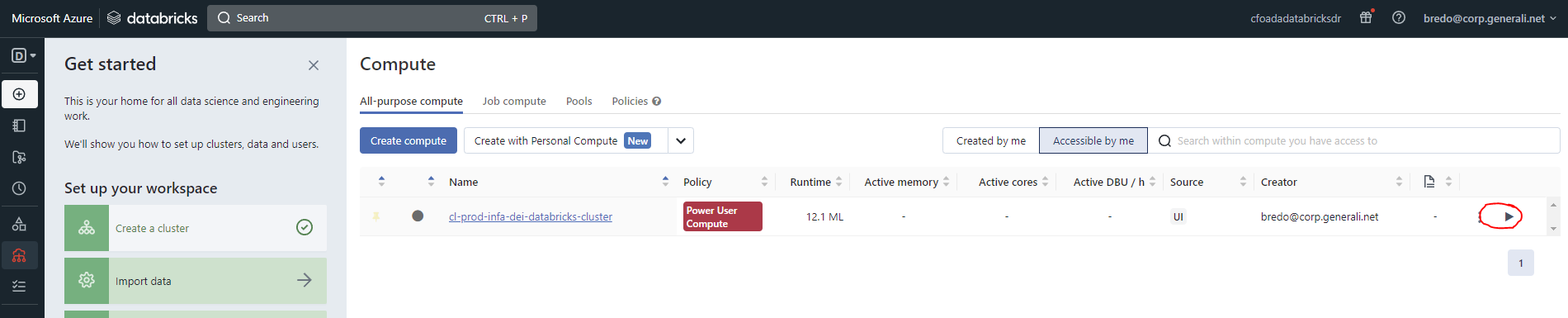
Nessuna attività deve essere svolta in particolare per effettuare una preparazione al test se non la stessa attività prevista in fase di failover vero.

# Esecuzione del Test Failover

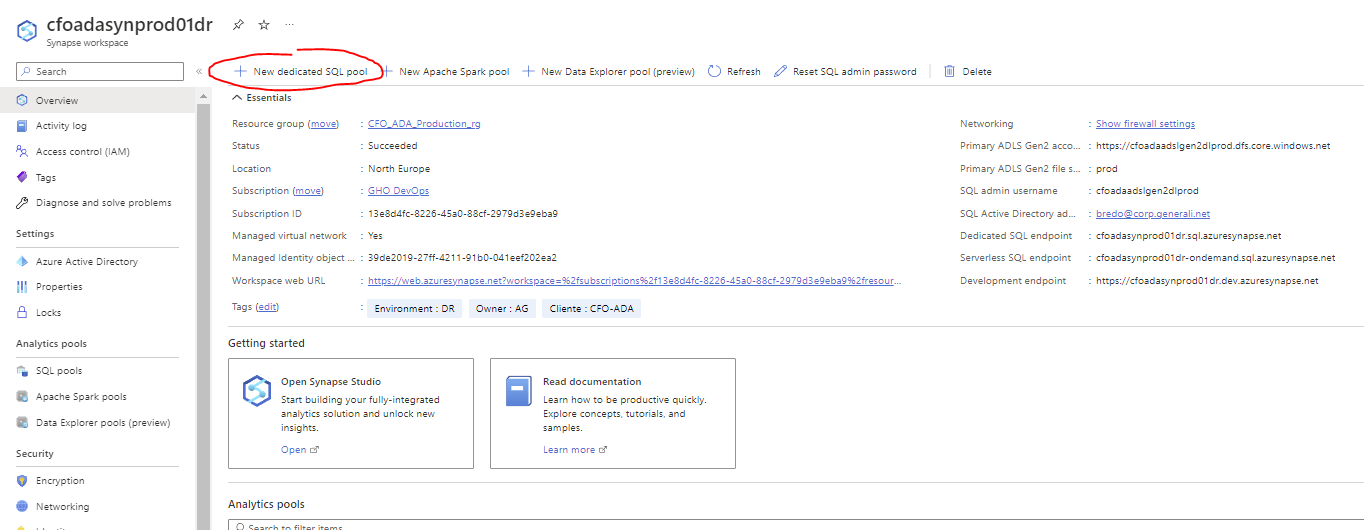
Il seguente paragrafo indica la procedura sequenziale per il test failover:

1. Avviare i cluster del databricks in north europe accedendo al portale databricks <https://adb-1133888283165035.15.azuredatabricks.net/aad/auth?has=&Workspace=/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/rg-gho-it-prod-ada-001/providers/Microsoft.Databricks/workspaces/cfoadadatabricksdr&WorkspaceResourceGroupUri=/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/databricks-rg-cfoadadatabricksdr-akgrs7gxlq7ns&l=en-us>

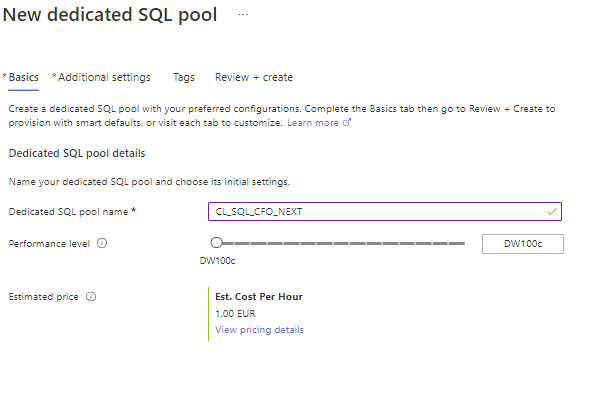
Nella sezione compute avviare il cluster



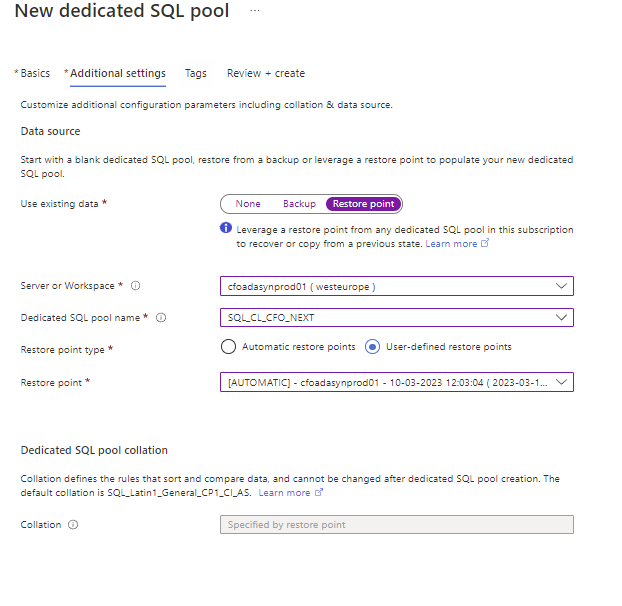
1. Creare sia il cluster NEXT che Data MAnagemente su Synapse cfoadasynprod01dr in north europe. Dal portale creare un nuovo cluster SQL



Inserire le informazioni del cluster e relativo sizing (il minimo)



Selezionare il restore point

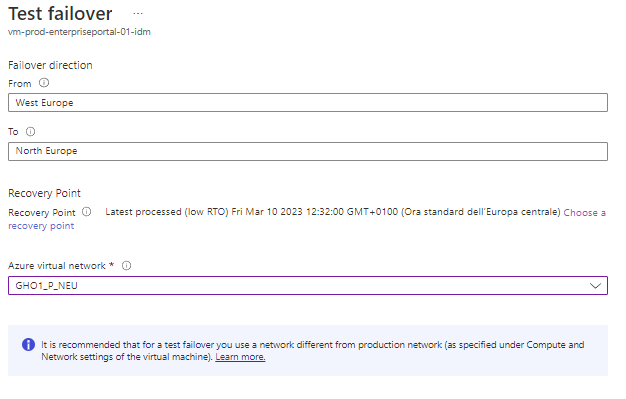


Completare l’attività fino alla creazione del cluster. LA stessa attività deve essere fatta per entrambi i cluster.

Una volta creati i cluster sul cluster del CL\_SQL\_CFO\_NEXT eseguire lo script SQL per allineare il sid del login.

1. Modificare la connessione al key vault di produzione come indicato nella procedura di preparazione al test
2. Creare il DB scrivibile come indicato nelle procedure di preparazione al test
3. Dalla risorsa del site recovery ProductionSiteRecoveryVault nella sezione “Replicated Items” accendere tutte le macchine selezionando per ciascuna il bottone “Test Failover”

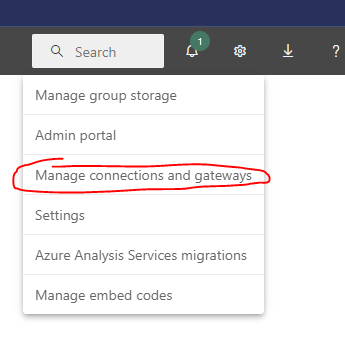
Inserire le informazioni come da screenshot

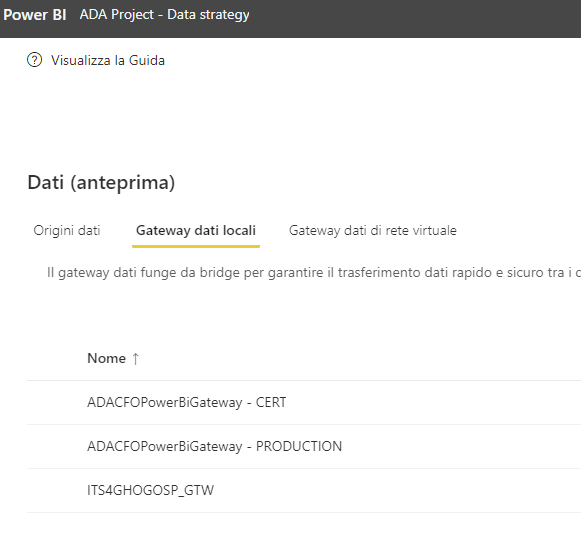


Completare la procedura per ciascun server

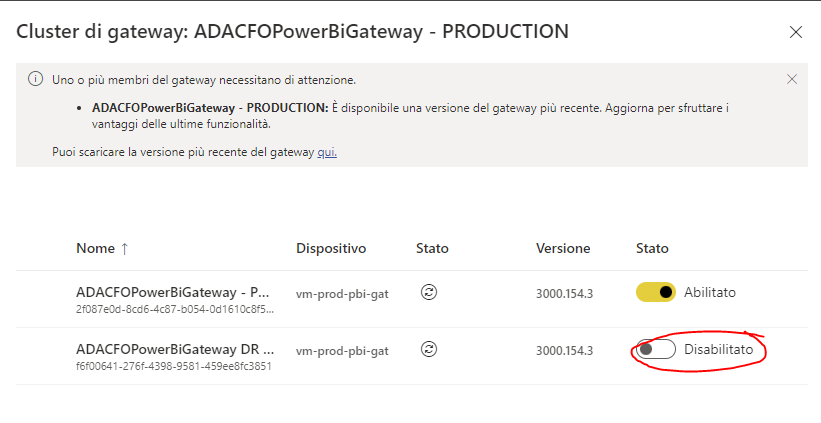
1. Modificare la macchina DEI come indicato nelle procedure di preparazione al test
2. Andando sul portale di power bi app.powerbi.com cambiare il puntamento del cluster del gateway

Per sistemare il puntamento del cluster andare sulla sezione “Manage Connections and gateways”





Aprire i dettagli del gateway di produzione



Abilitare il cluster disabilitato di north europe e disabilitare quello di west europe

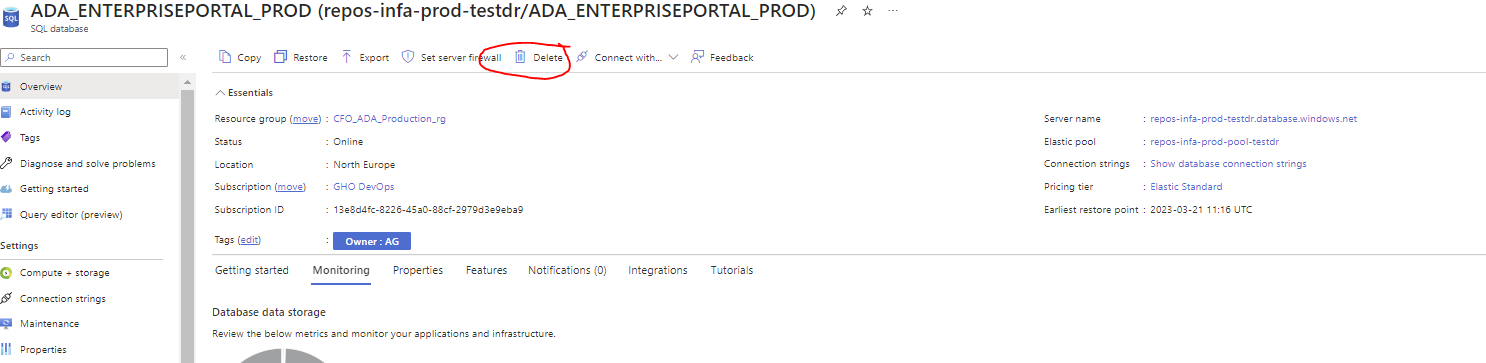
1. Procedere con i test del runbook

## Dismissione ambiente di Test DR

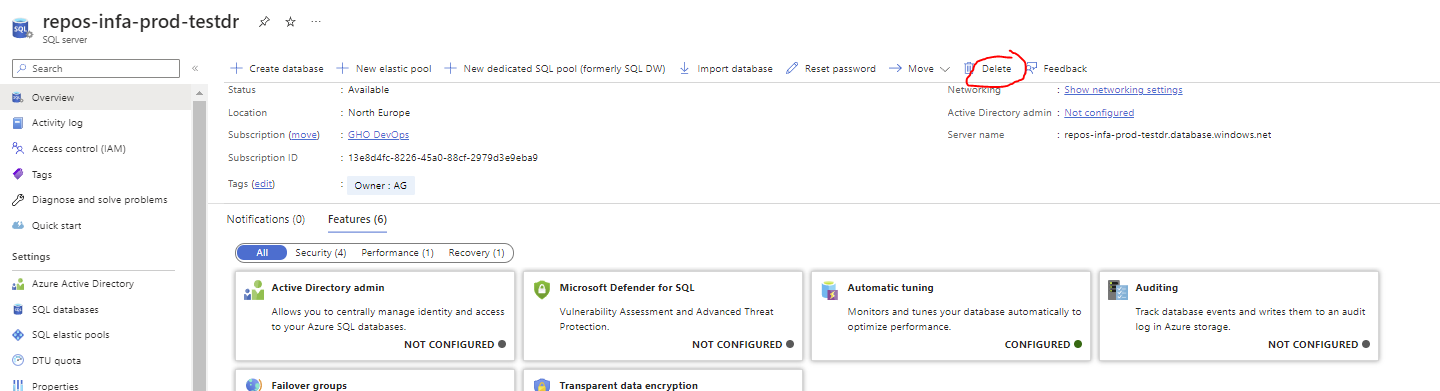
Completati i test di DR procedere con la dismissione delle risorse.

1. Per dismettere la parte IaaS cliccare su ogni istanza delle VM nel Site Recovery il comando Cleanup Test Discovery
2. Per dismettere la parte PaaS SQL Elastic pool:

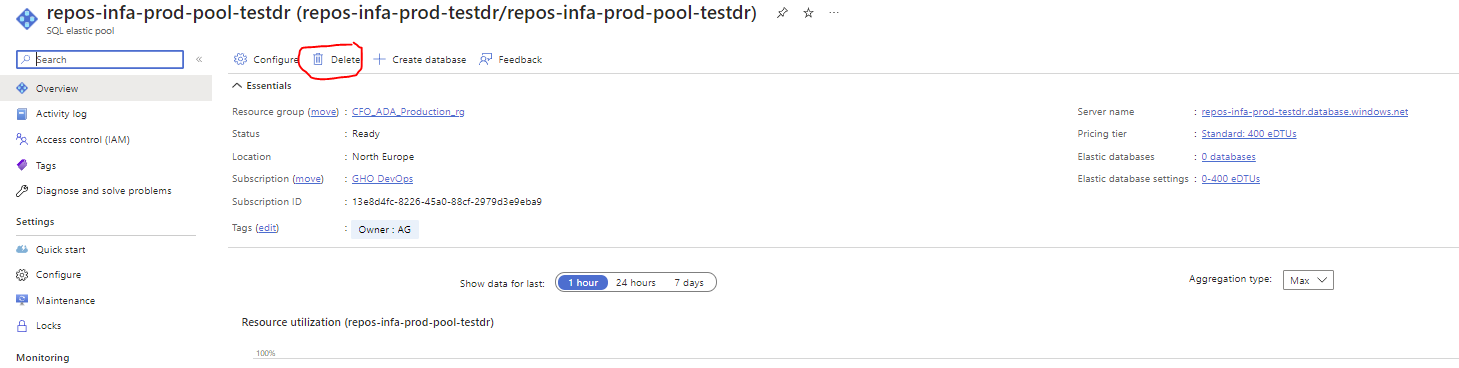
Cancellare tutti i database dal sql server repos-infa-prod-testdr. Entrare nella risorsa SQL Database e per ogni database cliccare Delete



Cancellare il database server repos-infa-prod-testdr entrando sulla risorsa e premere delete



Infine cancellare la risorsa SQL Elastic Pool:



1. Per dismettere il databrikcs spegnere tutti i cluster attivi (NON eliminarli)
2. Per dismettere la risorsa Synapse eliminare tutti i cluster esistenti (non eliminare il workspace ma solo i cluster)
3. Per sicurezza verificare che la stringa di connessione sul key vault sia stata precedentemente riallineata e che punti al database di failover group.

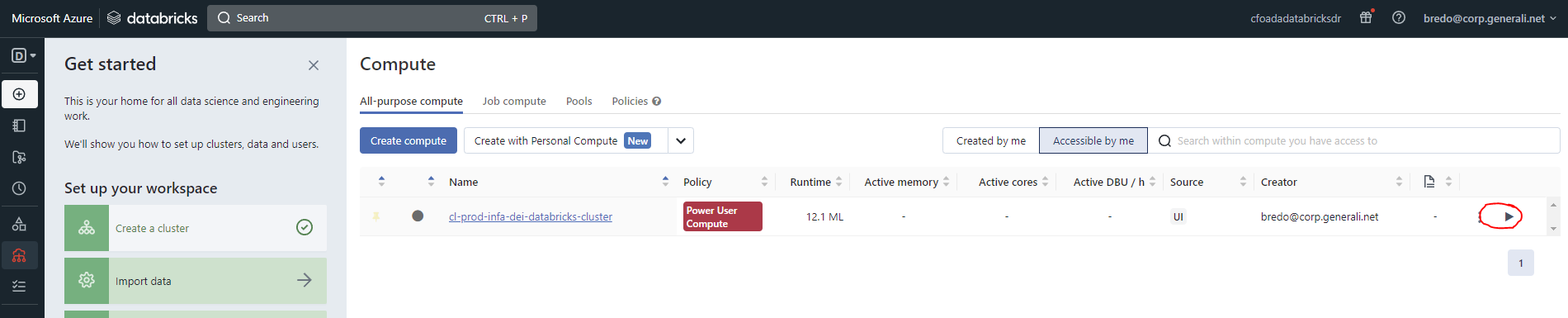
# Esecuzione del Failover

In caso di disastro procedere come da descrizioni qui sotto, rispettando la sequenza dei passaggi:

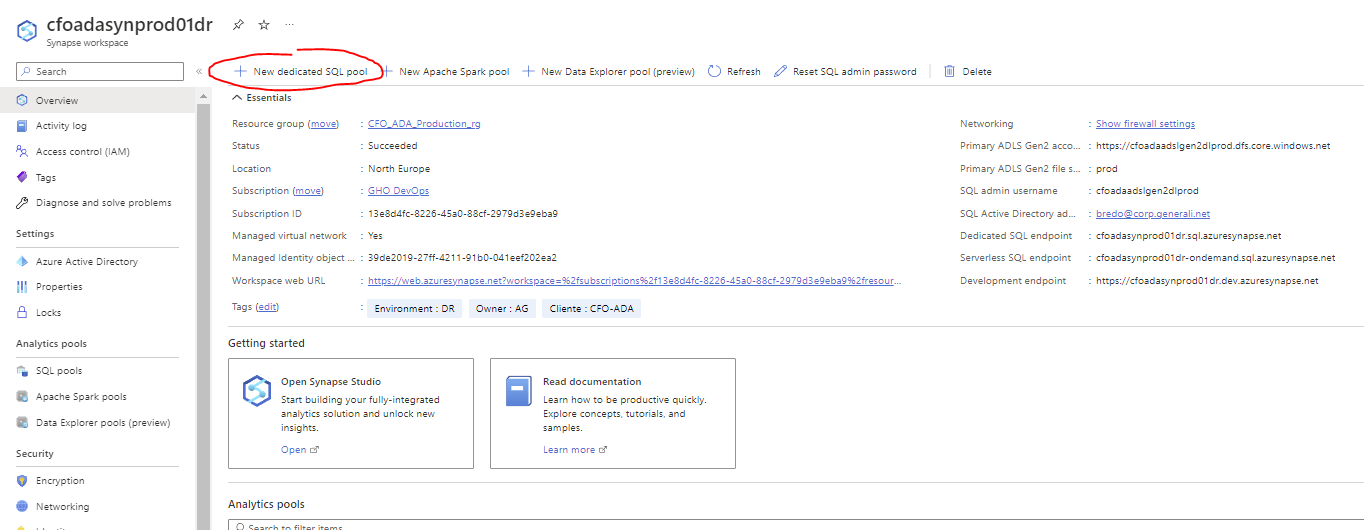
Il seguente paragrafo indica la procedura sequenziale per il test failover:

1. Avviare i cluster del databricks in north europe accedendo al portale databricks <https://adb-1133888283165035.15.azuredatabricks.net/aad/auth?has=&Workspace=/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/rg-gho-it-prod-ada-001/providers/Microsoft.Databricks/workspaces/cfoadadatabricksdr&WorkspaceResourceGroupUri=/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/databricks-rg-cfoadadatabricksdr-akgrs7gxlq7ns&l=en-us>

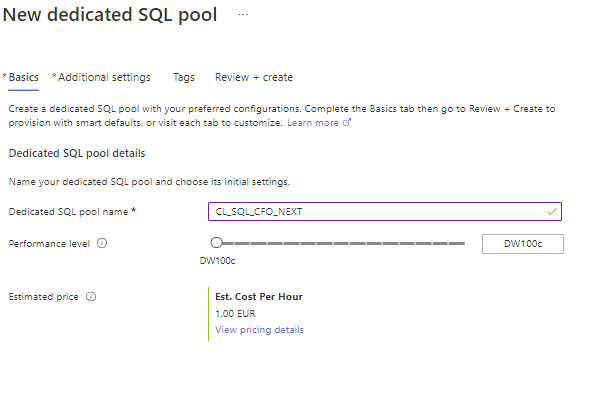
Nella sezione compute avviare il cluster



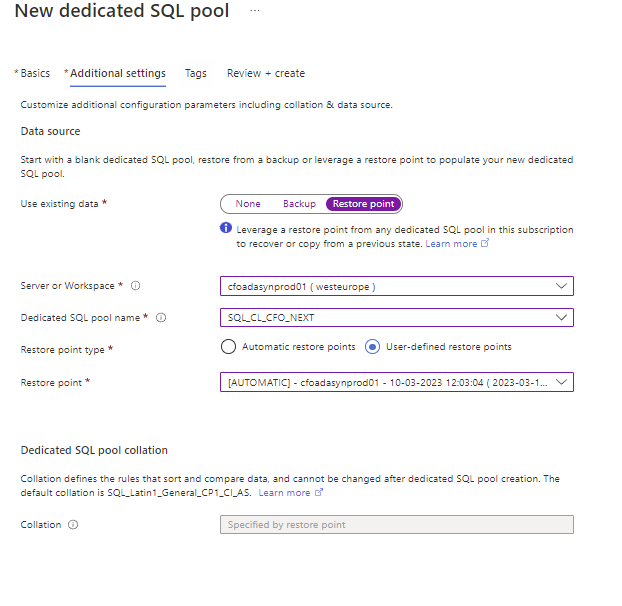
1. Creare sia il cluster NEXT che Data MAnagemente su Synapse cfoadasynprod01dr in north europe. Dal portale creare un nuovo cluster SQL



Inserire le informazioni del cluster e relativo sizing (il minimo)



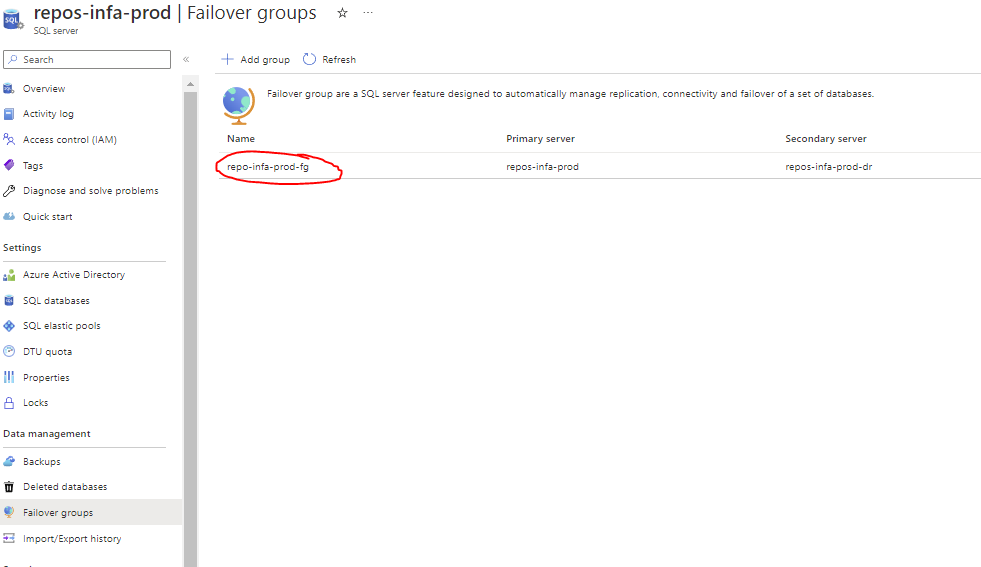
Selezionare il restore point



Completare l’attività fino alla creazione del cluster. LA stessa attività deve essere fatta per entrambi i cluster.

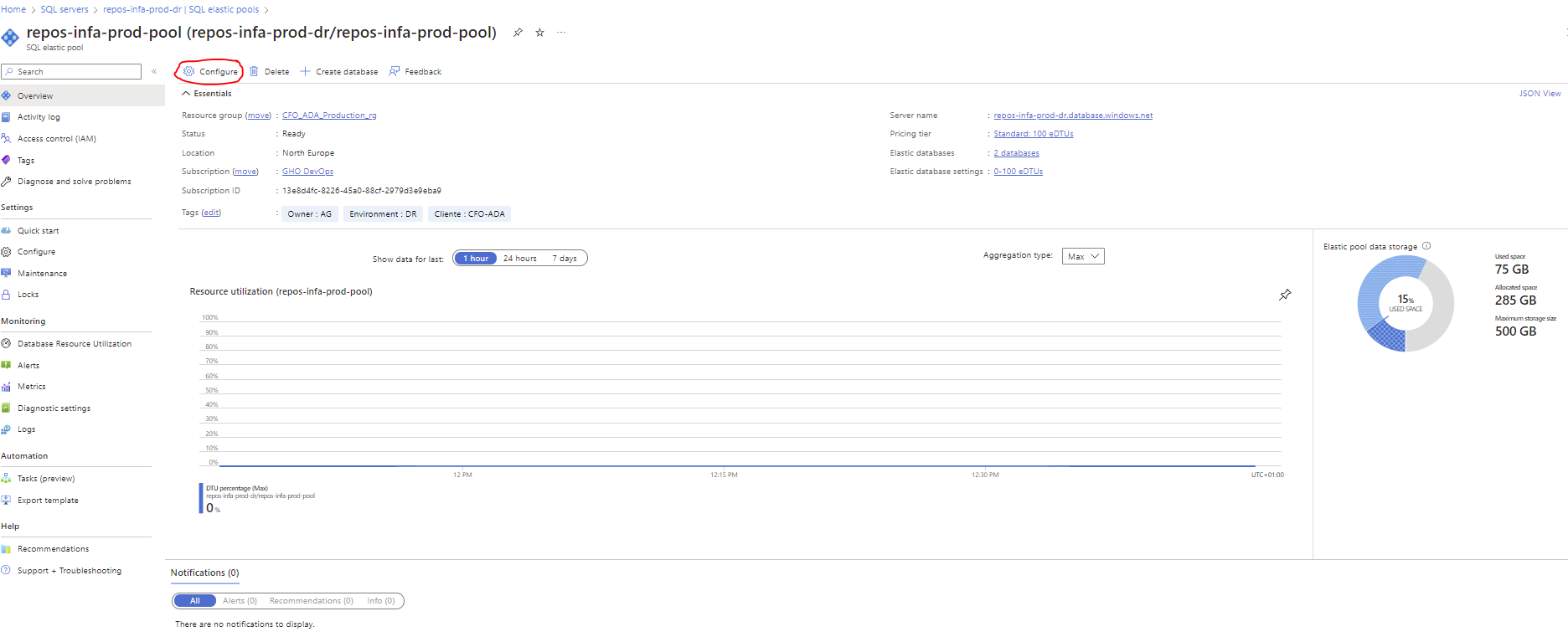
Una volta creati i cluster sul cluster del CL\_SQL\_CFO\_NEXT eseguire lo script SQL per allineare il sid del login.

1. Procedere ad effettuare il failover della georeplica. Andando sulla risorsa SQL server di produzione cliccare nella sezione failover groups e poi cliccando

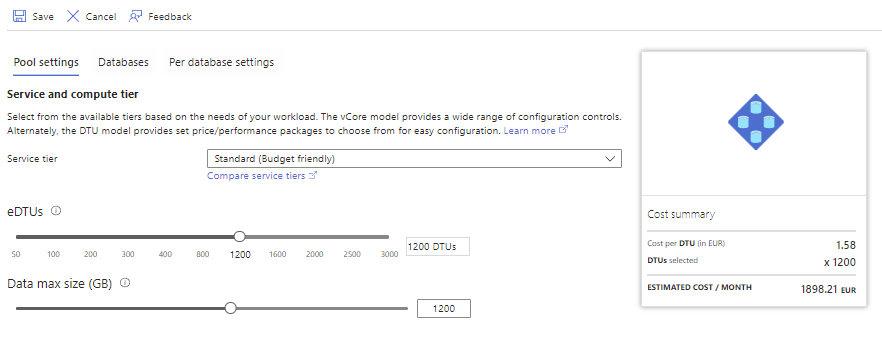


Procedere successivamente cliccando sul bottone di Failover. Solo se l’attività non dovrebbe sbloccarsi provare con Forced Failover.

Quando il servizio è stato ripristinato ricordarsi di scalare le prestazioni della macchina accedendo alla risorsa elastic pool in **north europe** con il nome **repos-infa-prod-pool**



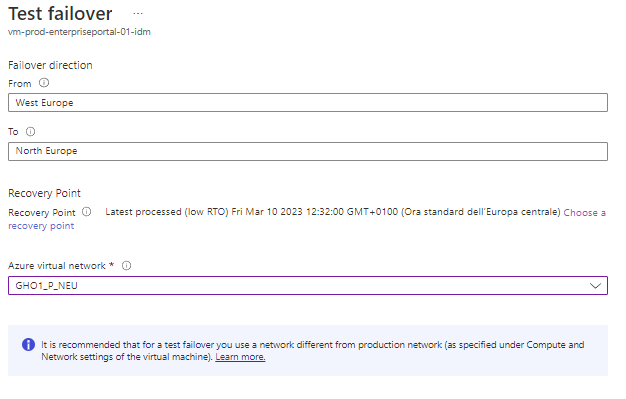
Una volta entrato nella configurazione dell’elastic pool in north europe ripristinare il sizing della macchina come in produzione



ATTENZIONE! Nel caso in cui l’ambiente di produzione ricordarsi di aggiornare questa documentazione indicando il corretto sizing.

1. Dalla risorsa del site recovery ProductionSiteRecoveryVault nella sezione “Replicated Items” accendere tutte le macchine selezionando per ciascuna il bottone “Failover”

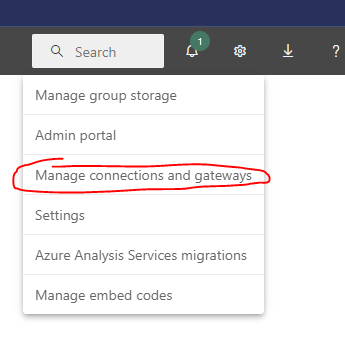
Inserire le informazioni come da screenshot

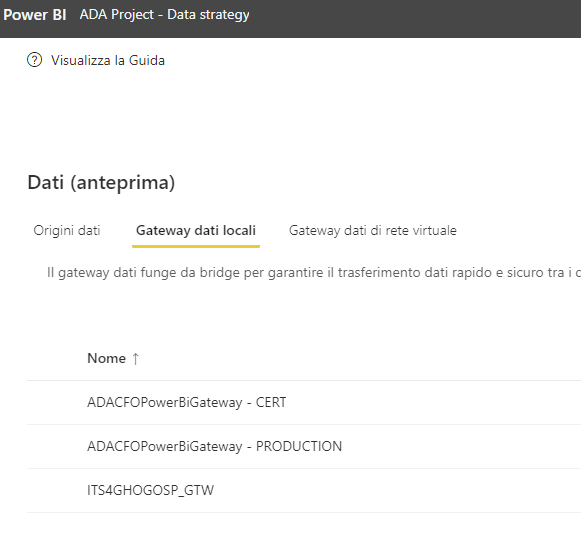


Completare la procedura per ciascun server

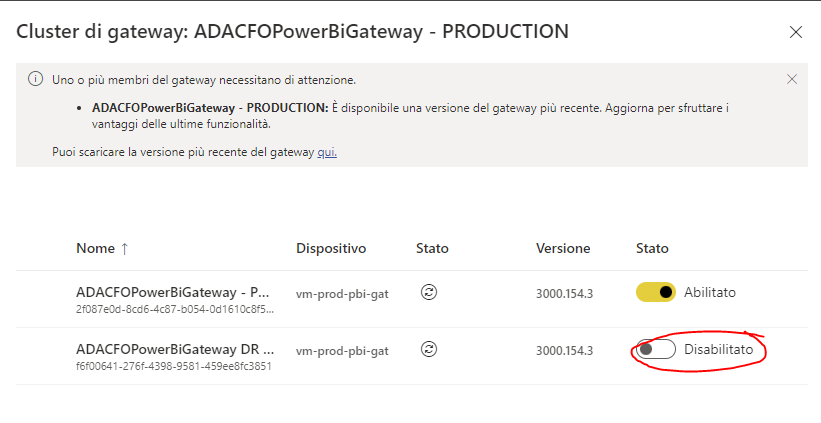
1. Andando sul portale di power bi app.powerbi.com cambiare il puntamento del cluster del gateway

Per sistemare il puntamento del cluster andare sulla sezione “Manage Connections and gateways”





Aprire i dettagli del gateway di produzione

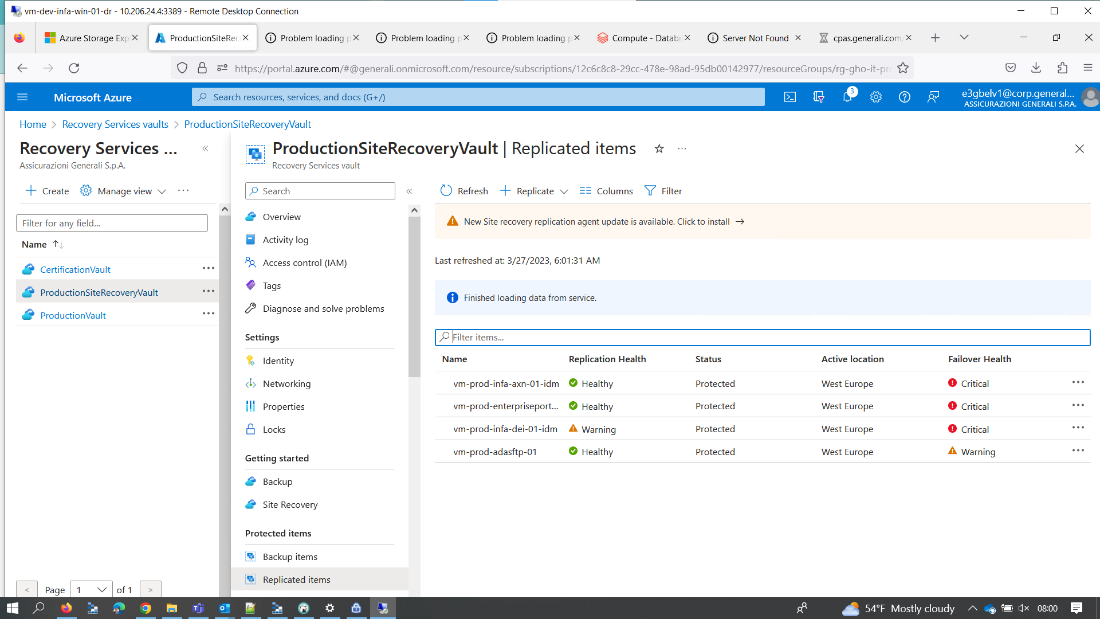


Abilitare il cluster disabilitato di north europe e disabilitare quello di west europe

1. Procedere con i test del runbook

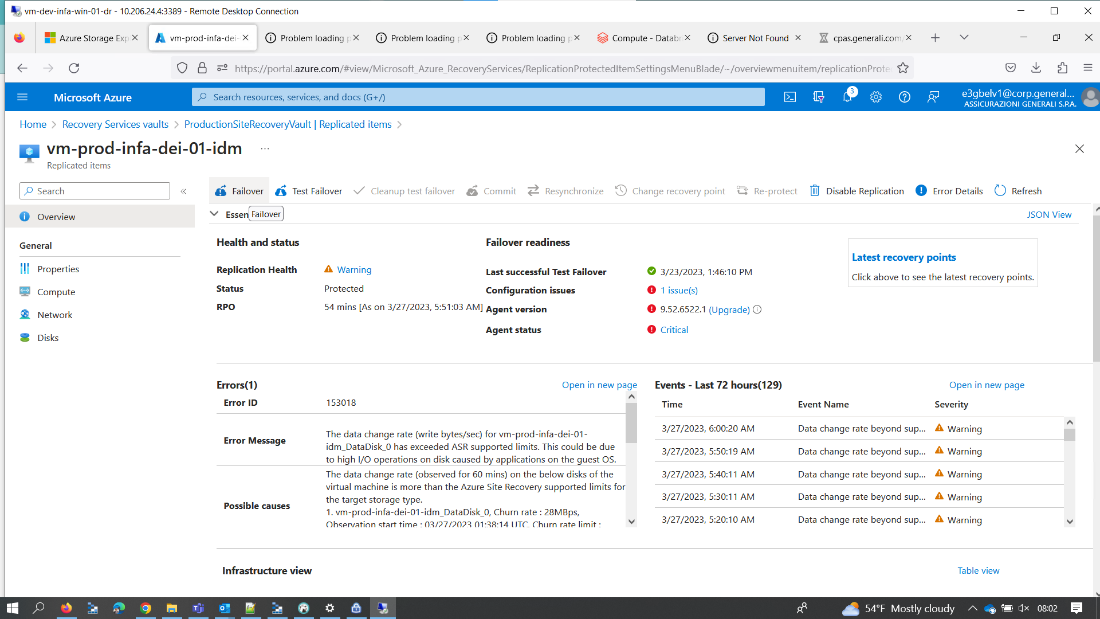
In caso di distastro andare su questo link :

<https://portal.azure.com/#@generali.onmicrosoft.com/resource/subscriptions/12c6c8c8-29cc-478e-98ad-95db00142977/resourceGroups/rg-gho-it-prod-ada-001/providers/Microsoft.RecoveryServices/vaults/ProductionSiteRecoveryVault/replicationProtectedItems>



Selezionare onguna delle macchine :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Replication Health** | **Status** | **Active location** | **Failover Health** |  |
| vm-prod-infa-axn-01-idm | Healthy | Protected | West Europe | Critical |  |
| vm-prod-enterpriseportal-01-idm | Healthy | Protected | West Europe | Critical |  |
| vm-prod-infa-dei-01-idm | Warning | Protected | West Europe | Critical |  |
| vm-prod-adasftp-01 | Healthy | Protected | West Europe | Warning |  |

E attivare il failover come segue :  
  


Replicare l’attività per tutte le macchine.

Per la sola macchina della dei vm-prod-infa-dei-01-idm

Dovranno essere eseguite delle attività manuali:

Pulizia dell’ambiente prima di startare i servizi:

loggarsi sulla macchina tramite sudo su – infadei

cd /informatica/infadei/services/DataIntegrationService/

rm -R sqldataviewer

rm -R DataIntegrationService

cd /informatica/infadei/services/SchedulerService

rm -R Scheduler

cd /informatica/infadei/tomcat/bin/target/repository/1595859022617/MRS\_DEI\_PROD/index

rm -R searchdata

cd /informatica/infadei/tomcat/bin/target/repository/1595858796637/mMRS\_DEI\_PROD/index

rm -R searchdata

cd /informatica/infadei/services/work\_dir

rm -R MassIngestion

rm -R ContentManagementService

rm -R DataIntegrationService

rm -R ModelRepositoryService

rm -R AnalystService

cd /informatica/infadei/tomcat/work

rm -R Catalina

cd /informatica/infadei/tomcat/temp

rm -rf \*

cd /informatica/infadei/tomcat/webapps

rm -R adminconsole

rm -R ROOT

rm -R csm

rm -R coreservices

Succissivamente restartare i servizi :

/informatica/infadei/tomcat/bin/infaservice.sh startup

Sulla VM di Informatica DEI in DR è necessario modificare la configurazione della connessione usata per Databricks:

Immagine che contiene testo

Descrizione generata automaticamente

Con l’opzione di refresh si fa in modo di puntare al nuovo Databricks di cui è necessario conoscere:

* **Databricks Domain**: è l’end-point del cluster
* **Databricks Token ID**: è una stringa che restituisce Azure al momento della creazione del cluster
* **Cluster ID**: E’ l’identificativo del cluster

Informazioni che sono disponibile nell’area di sicurezza al seguente link: <https://generali.sharepoint.com/:t:/s/DataStrategy2-SecurityArea/EcOfdDKSKW1Mh8-_TWxaHrQBfPO0atCjmOe7QtQjRQ12YQ?e=ei0nnN>

Immagine che contiene testo

Descrizione generata automaticamente

Salvare la nuova configurazione.