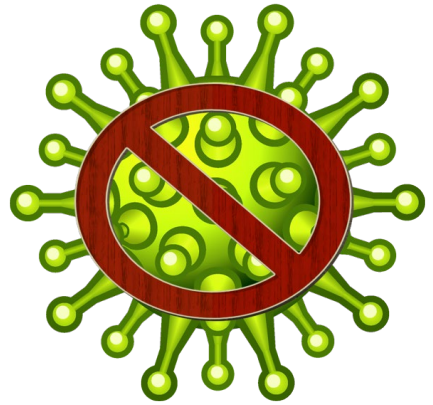
Un dominio a norma di legge e a prova di pandemia

Creazione ed evoluzione del dominio Windows per i Servizi di Amministrazione e Direzione della Sezione di Pisa negli ultimi tre anni



Gabriele Lo Re
INFN Istituto Nazionale di Fisica Nucleare

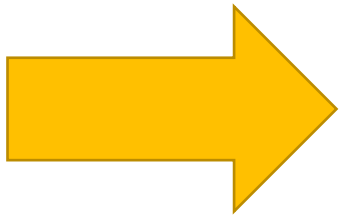
Situazione preesistente: il dominio SEGRETERIA

+ Storage condiviso a disposizione degli utenti e distribuito via rete
+ Permessi di lettura/scrittura sulle cartelle condivise attribuiti singolarmente ad ogni utente

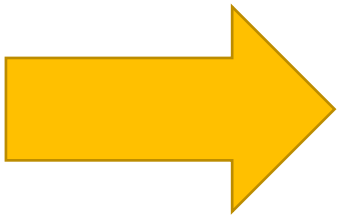
- Dominio separato virtualmente, ma collegato fisicamente alla rete standard di Sezione
- Richieste IP gestite dal DHCP server di Sezione
- Unico Domain Controller con Windows Server 2003
- Computer client con hardware variegato e spesso poco performante

Maggio 2018: entra in vigore il GDPR

- Dominio preesistente non più a norma di legge
- Necessità di modificare radicalmente un’infrastruttura vecchia



Perché non approfittarne per costruire da zero una nuova infrastruttura più moderna e appositamente studiata?



2019: creazione e implementazione del nuovo dominio

Gli obiettivi

- Seguire le linee dettate dalle misure minime del GDPR
- Standardizzare e centralizzare le operazioni di installazione e gestione dell’infrastruttura
- Rendere le postazioni di lavoro intercambiabili, legando l’ambiente di lavoro all’utente anziché alla singola macchina
- Uniformare la configurazione della scrivania per tutti gli utenti

Gli acquisti

- 2 server Dell PowerEdge R640

  + Windows Server 2016
  + Processore Intel Xenon Silver 4114 @2.20GHz 10 core
  + 64 GB RAM
  + 7 TB HDD

- 20 computer Lenovo ThinkCenter M910s

  + Windows 10 Pro
  + Processore Intel Core i3-7100 @3.90GHz 2 core
  + 8 GB RAM
  + 500 GB HDD

Il nuovo dominio

- Due Domain Controllers (primario e secondario) sistemati su una rete separata da quella standard di Sezione e su VLAN dedicata
- Domain Controller secondario configurato per fornire i servizi più essenziali in caso di necessità
- Ruoli DHCP e DNS installati sui DC per gestire la rete di dominio autonomamente
- Trust con il realm Kerberos di Sezione per poter utilizzare le credenziali AAI per l’accesso all’account Windows

Il nuovo dominio

- Condivisione di uno degli HDD del DC1 agli utenti per condividere file e cartelle; assegnazione di permessi lettura/scrittura con struttura a gruppi
- Implementazione dei roaming profiles per permettere agli utenti di trovare i propri files su ogni macchina del dominio
- Ruolo Windows Deployment Services installato per distribuire rapidamente via rete una configurazione standard ai client
- Sicurezza dell'infrastruttura aumentata tramite l'implementazione di varie policies di dominio

Marzo 2020: inizio pandemia

⚠ Urge implementare degli strumenti per il lavoro agile

- ✗ Remote Desktop di Windows non compatibile con le credenziali Kerberos degli utenti
- ✓ Si opta per UltraVNC, software con licenza libera che evita il passaggio di dati attraverso server di terze parti
- ✓ Vpn di Sezione già in funzione (OpenVPN)

2021: Progetto lavoro agile

Gli obiettivi

- Eliminare la necessità di accedere da remoto alla propria macchina
- Sostituire i pc desktop degli utenti con dei notebook
- Crittare gli hard disk delle nuove macchine per minimizzare i rischi di data breach
- Creare una VPN ad hoc gestita sui Domain Controller e utilizzata solo dagli utenti del dominio

Gli acquisti

- 20 notebook Lenovo ThinkPad X1 Carbon Gen. 7
  + Windows 10 Pro
  + Processore Intel Core i5-8265U @ 1.60GHz
  + 16 GB RAM
  + 500 GB SSD

- 20 docking station ThinkPad Pro
  + 2 porte DisplayPort
  + 3 porte USB 3.0
  + 2 porte USB 2.0

Crittazione dell'hard disk

- Crittazione dei dischi implementata con Sedutil, un pacchetto open source che sfrutta la compatibilità con OPAL 2.0 dei pc Lenovo
- Tecnologia *Self Encrypting Drives* (SED) tramite hardware: i dischi criptano i dati automaticamente senza influire sulle prestazioni
- La decrittazione avviene prima del boot del sistema operativo tramite l'inserimento di una password: se non si inserisce correttamente, il disco non si sblocca e il sistema operativo non parte
- Anche trasferendo fisicamente il disco su un'altra macchina, la crittazione non viene aggirata

Link: https://github.com/Drive-Trust-Alliance/sedutil

Il tassello finale: la VPN

- VPN ad uso esclusivo dei Servizi di Amministrazione e Direzione
- Creata sul Domain Controller primario attraverso il ruolo «Accesso remoto» di Windows Server
- Tipologia L2TP/IPSec con chiave pre-condivisa
- Configurata direttamente su Windows senza software di terze parti
- Disco remoto condiviso esplorabile direttamente dai clients
- Possibilità di assistenza all'utente da remoto senza che i dati passino per server di terze parti, usando insieme VPN e UltraVNC

Il tassello finale: la VPN

- Traffico dati indirizzato per passare attraverso la VPN solo per i servizi per cui è indispensabile
- Rotte impostate manualmente via terminale con Windows PowerShell

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "VPN ammin" -DestinationPrefix "212.189.155.192/26" ⟵ Rete del dominio

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "VPN ammin" -DestinationPrefix "212.189.156.0/22" ⟵ Rete standard di Sezione

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "VPN ammin" -DestinationPrefix "192.135.23.0/24" ⟵ Sistema Informativo INFN

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "VPN ammin" -DestinationPrefix "192.135.31.0/24" ⟵ Sistema Informativo INFN

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "VPN ammin" -DestinationPrefix "131.154.56.0/24" ⟵ Sistema Informativo INFN

Questions/answers

```
>>
>>
>> if   ( questions )
>> then
>>      answers
>> else
>>      pranzo
>>
>>
>>
>>
>>
```