ICT POWER.IT

Microsoft

POWERCON2020

Migrazione Active Directory a Windows Server 2019

Ermanno Goletto
Microsoft MVP Reconnect
e.goletto@outlook.it

/devadmin.it

@ermannog

Roberto Massa
Microsoft MVP Reconnect
robimassa@outlook.it

/facebook

@robi_massa

Agenda

- Prerequisiti in Windows Server 2019
- Deploy di un DC WS2019
- Demote DC WS 2008

ICT POWER.IT

Microsoft

Prerequisiti in Windows Server 2019

Migrazione Active Directory a Windows Server 2019

Prerequisiti per l'utilizzo di DC WS 2019

Per poter aggiungere un DC WS2019 il livello funzionale deve essere almeno Windows Server 2008

Non è possibile avere DC WS2003 (deprecati in WS2016)

Per poter aggiungere un DC WS2019 la replica della SYSVOL deve avvenire tramite DFS-R

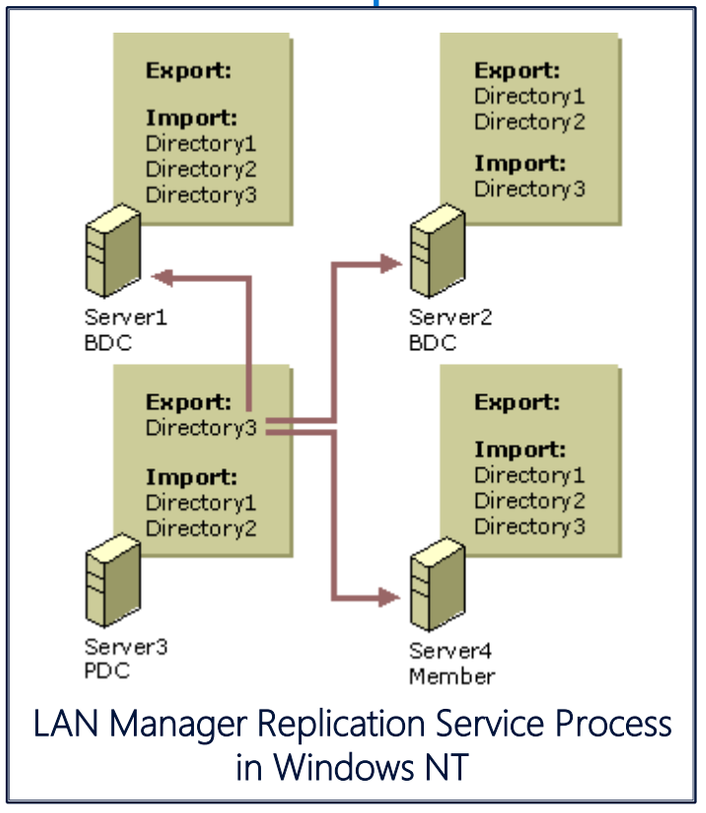
Non è possibile utilizzare FRS (deprecato in WS2012)

Non sono stati aggiunti nuovi livelli funzionali di dominio e di foresta

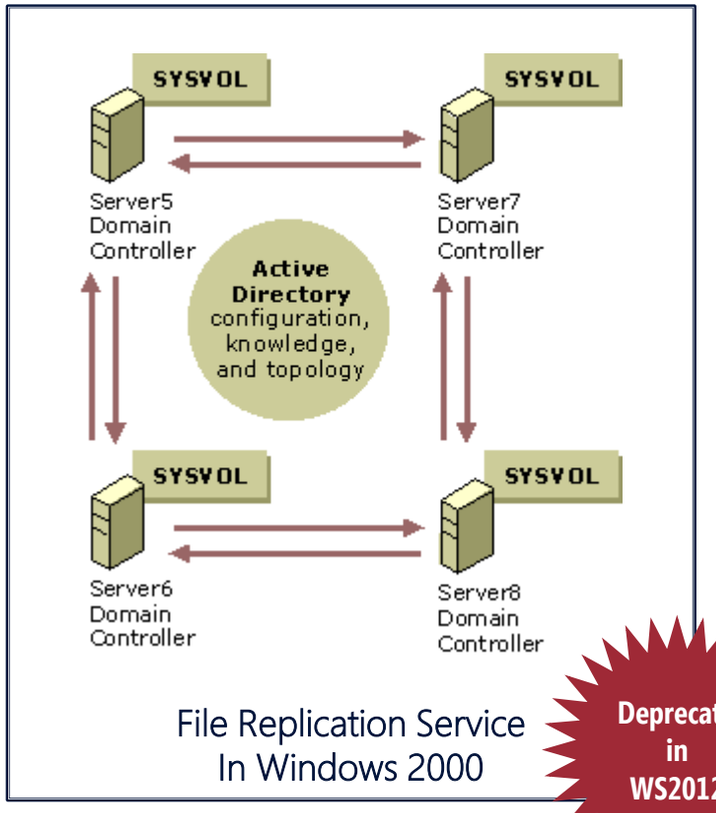
Non ci sono nuove funzionalità

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels

File Replication Service (FRS) Rimosso

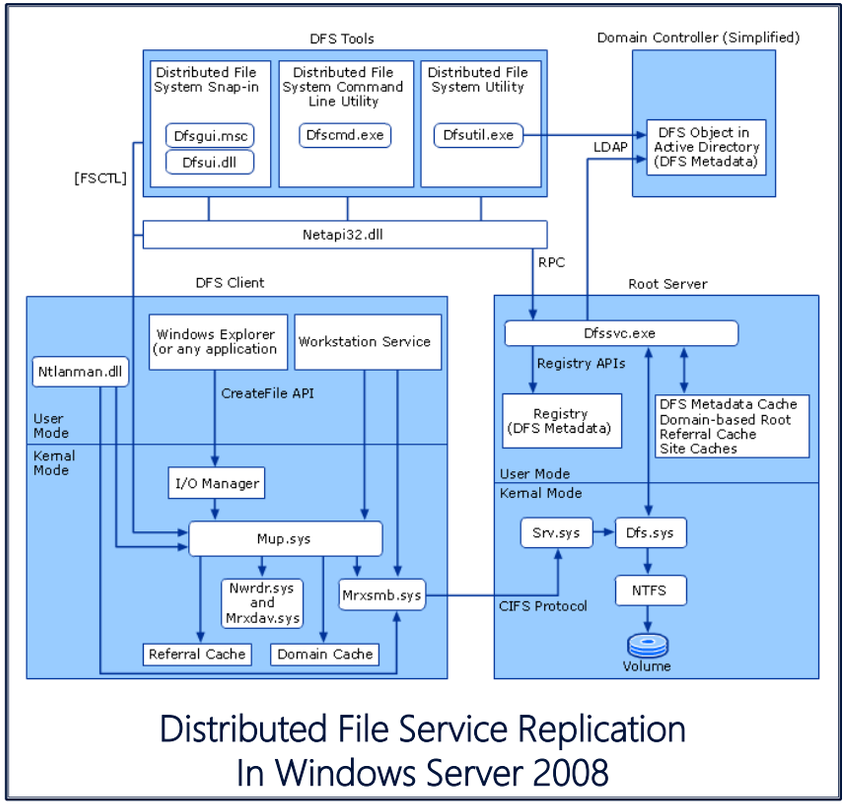


LAN Manager Replication Service Process in Windows NT



File Replication Service In Windows 2000

Deprecato in WS2012



Distributed File Service Replication In Windows Server 2008

Migrazione da FRS a DFS

I dominii con livello funzionale WS2008 o superiore possono utilizzare la DFS per la replica della SYSVOL
I dominii creati con livello funzionale inferiore a WS2008 necessitano della migrazione da FRS a DFS

KB4493934 SYSVOL DFSR Migration fails after you in-place upgrade a domain controller to Windows Server 2019
https://support.microsoft.com/en-us/help/4493934/sysvol-dfsr-migration-fails-in-place-upgrade-dc

Migrazione replica Sysvol da Frs a Dfs

Vantaggi della replica DFS

- Maggior efficienza
- Maggior scalabilità
- Banda ridotta grazie all'algoritimo Remote Differential Compression (RDC)
- Meccanismo di auto ripristino da eventuali corruzioni

Requisiti della replica DFS

- Livello funzionale di domino Windows Server 2008 o superiore
- Ultima versione di Robocopy (KB968429 per WS2008/R2 e KB2951262 per WS2012/R2)
- Spazio libero su volume su cui risiede la SYSVOL pari alla dimensione della SYSVOL più 10% su ogni DC

Per trovare l'ultima versione di Robocopy utilizzare la seguente query in http://support.microsoft.com/ selezionando l'ultimo ID:
robocopy.exe kbqfe "*<operating system version>*"

1. Verifica SYSVOL condivisa e disponibile su tutti i DC
2. Migrazione allo stato di Prepared eseguendo sul DC col ruolo FSMO di PDC Emulator il comando: *Dfsrmig /setglobalstate 1*
3. Migrazione allo stato di Redirected eseguendo sul DC col ruolo FSMO di PDC Emulator il comando: *Dfsrmig /setglobalstate 2*
4. Migrazione allo stato di Eliminated eseguendo sul DC col ruolo FSMO di PDC Emulator il comando: *Dfsrmig /setglobalstate 3*

Per verificare se si sta utilizzando FRS e/o lo stato dei passi di migrazione Prepared, Redirected e Eliminated utilizzare il comando:
Dfsrmig /getmigrationstate

Dettagli della migrazione

Gli utenti possono continuare ad operare

Stato Prepared

FRS e DFSR hnno le proprie copie della SYSVOL, le shares **SYSVOL e Netlogon si referenziano alla copia FRS** (è possibile eseguire il rollback)

Stato Redirect

FRS e DFSR hanno le proprie copie della SYSVOL, le shares SYSVOL e Netlogon si referenziano alla copia DFS (è possibile eseguire il rollback)

Stato Eliminated

DFS replica la SYSVOL e FRS viene rimossa (non è possibile eseguire il rollback)

Durata della migrazione

La migrazione è **correlata alla replica di AD** in quanto la SYSVOL DFSR avviene durante una schedulazione della replica AD, quindi la DFRS legge/scrive gli stati ogni 5 min su ogni DC

Può impiegare pochi minuti in piccoli domini, ma alcune ore o giorni in domini estesi

Force della push replication di tutte le partizioni AD:
Repadmin /syncall /force /APed

Force della push replication di tutte le partizioni AD:
Repadmin /syncall /force /APed

Force poll delle modifiche di config a DFSR in AD:
Update-DfsrConfigurationFromAD

*Per eseguire la migrazione il **built-in Administrators group deve avere i privilegi di "Manage Auditing and Security Log" su tutti i DC**, come da impostazione di default (KB 2567421). Per verificare l'impostazione utilizzare il comando:*
Gpresult /s *dominio.ext* /h *path/gpreport.htm*

Migrate SYSVOL replication to DFS Replication https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/migrate-sysvol-to-dfsr

ICT POWER.IT

Microsoft

Deploy di un DC WS2019

Migrazione Active Directory a Windows Server 2019

Prerequisti per il deploy di un DC WS2019

Prerequisti Active Directory

- Livello Funzionale di Dominio Windows Server 2008
- Livello Funzionale di Foresta Windows Server 2008

Prerequisti Hardware

- 2 GB MB di RAM
- 32 GB di spazio libero su disco
- Risoluzione video 1024 x 768 o superiore

Verifica livello funzionale Foresta e Dominio tramite il tool Active Directory Domains and Trusts oppure tramite i comandi:

```
dsquery * CN=Partitions,CN=Configuration,DC=devadmin,DC=local -scope base -attr msDS-Behavior-Version
dsquery * DC=devadmin,DC=local -scope base -attr msDS-Behavior-Version ntMixedDomain
```


```
(Get-ADForest).ForestMode
(Get-ADDomain).DomainMode
```

Verifica versione schema Active Dyrectory tramite i comandi:

```
dsquery * cn=schema,cn=configuration,dc=devadmin,dc=local -scope base -attr objectVersion
```


```
Get-ADObject (Get-ADRootDSE).schemaNamingContext -Property objectVersion
```

msDS-Behavior-Version

0 = Windows 2000
1 = Windows 2003 interim
2 = Windows 2003
3 = Windows 2008
4 = Windows 2008 R2
5 = Windows 2012
6 = Windows 2012 R2
7 = Windows Server 2016

ntMixedDomain

0 = Native level
1 = Mixed level

Versioni schema Active Directory

13 = Windows 2000
30 = Windows 2003
31 = Windows 2003 R2
44 = Windows 2008
47 = Windows 2008 R2
56 = Windows 2012
69 = Windows 2012 R2
87 = Windows Server 2016
88 = Windows Server 2019

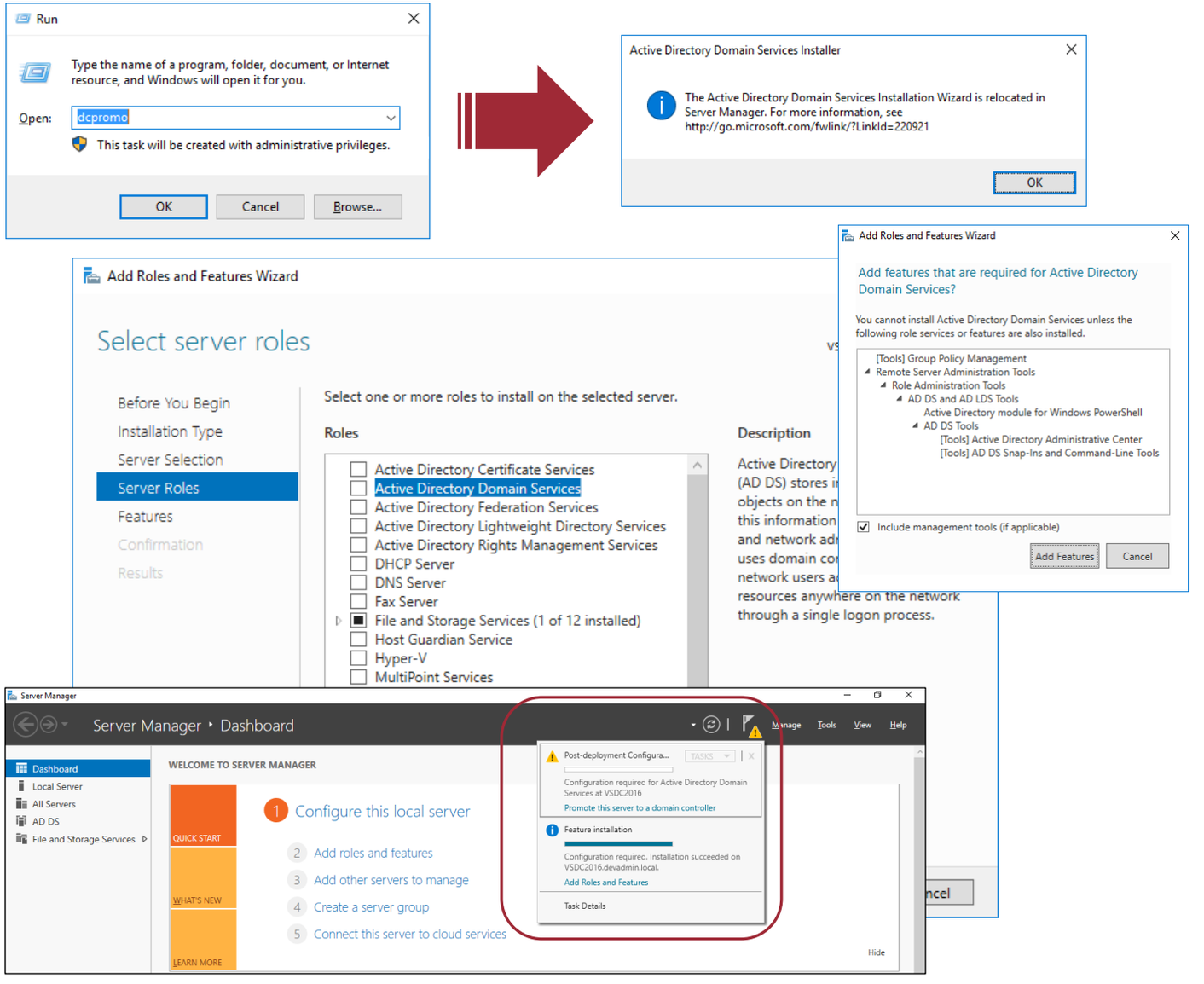
Deploy DC WS2019 tramite GUI

Deploy nuovo DC

- Tutti gli step eseguiti nella GUI del Server Manager
- Dcpromo deprecato da WS2012
- Processo di installazione basato su PowerShell
  - Esecuzione su server multipli
  - Deploy remoto di DC
  - Wizard di esportazione script per installazione con le opzioni specificate nella GUI

Upgrade di AD

- Integrazione di Adprep.exe nel processo di installazione
  - Può ancora essere eseguito da command line
  - Reperibile in media\support\adprep
  - Non esiste una versione a 32 bit di Adprep
- Validazione dei prerequisiti



Deploy DC WS2019 tramite PowerShell

```
# Join a dominio del nuovo server WS2019
Add-Computer -DomainName "ICTPOWER.LOCAL" -Restart

# Installazione del servizio DNS
Install-WindowsFeature -Name DNS -IncludeManagementTools

# Installazione del ruolo AD Domain Services
Install-WindowsFeature -Name AD-Domain-Services  -IncludeManagementTools

# Promozione del nuovo server a Domain Controller
Install-ADDSDomainController  -Credential (Get-Credential ICTPOWER\Administrator)
  -DomainName ictpower.local –SafeModeAdministratorPassword
  (ConvertTo-SecureString -AsPlainText "SafeM0deAdminPwd!" -Force)
  -ReplicationSourceDC "dc01.ictpower.local"
  -DatabasePath "C:\Windows\NTDS"
  -LogPath "C:\Logs"
  -SysvolPath "C:\Windows\SYSVOL"
  -Force:$True
```

https://www.ictpower.it/sistemi-operativi/migrare-active-directory-da-windows-server-2008-2008-r2-a-windows-server-2019.htm

Verifica promozione DC WS2019

Aggiornamento dello schema di Active Directory a Windows Server 2019 (88)

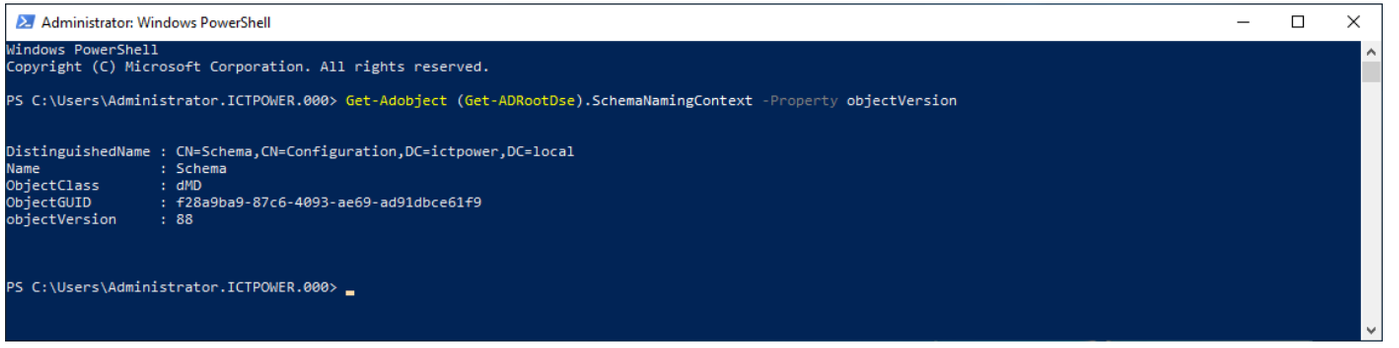
Verifica della corretta registrazione del Domain Controller WS 2019 in Active Directory

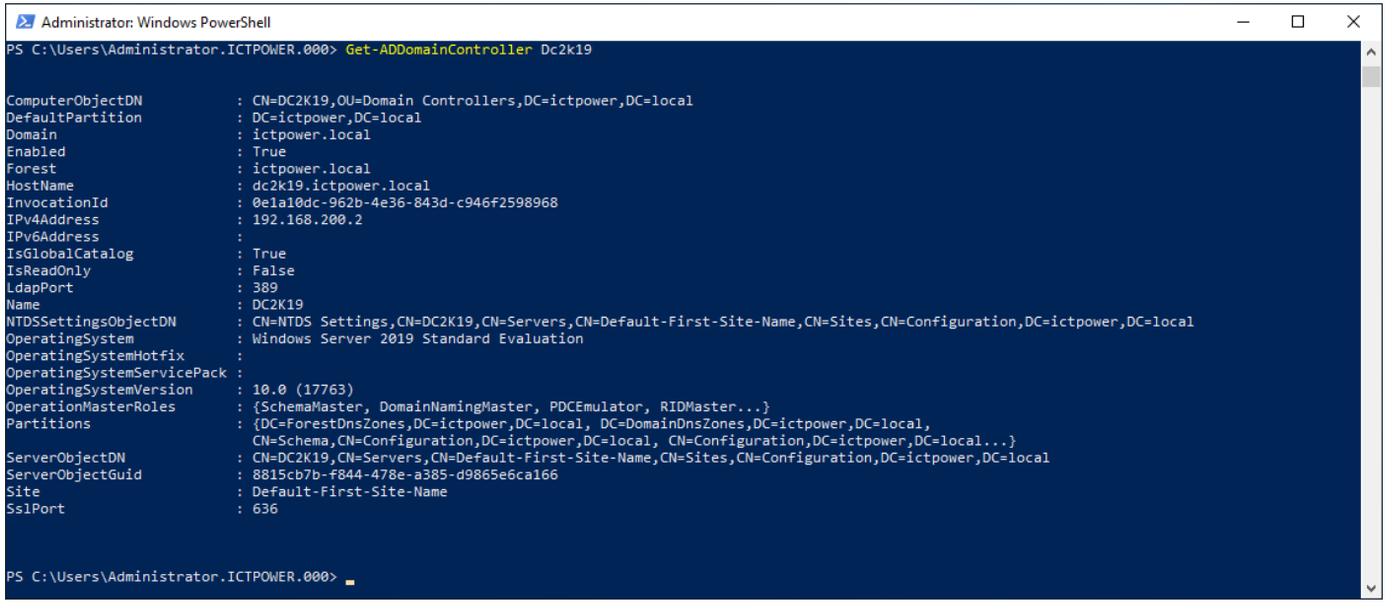
Verifica eventi registro Directory Services:
- ID 1000 Info - ActiveDirectory_DomainService
- ID 1394 Info - ActiveDirectory_DomainService

Verifica eventi registro DNS Server:
- ID 4 Info - DNS-Server-Service
- ID 2 Info - DNS-Server-Service

Verifica eventi registro Servizi Web Active Directory:
- ID 1004 Info - ADWS

Verifica funzionalità replica tramite Active Directory Replication Status Tool



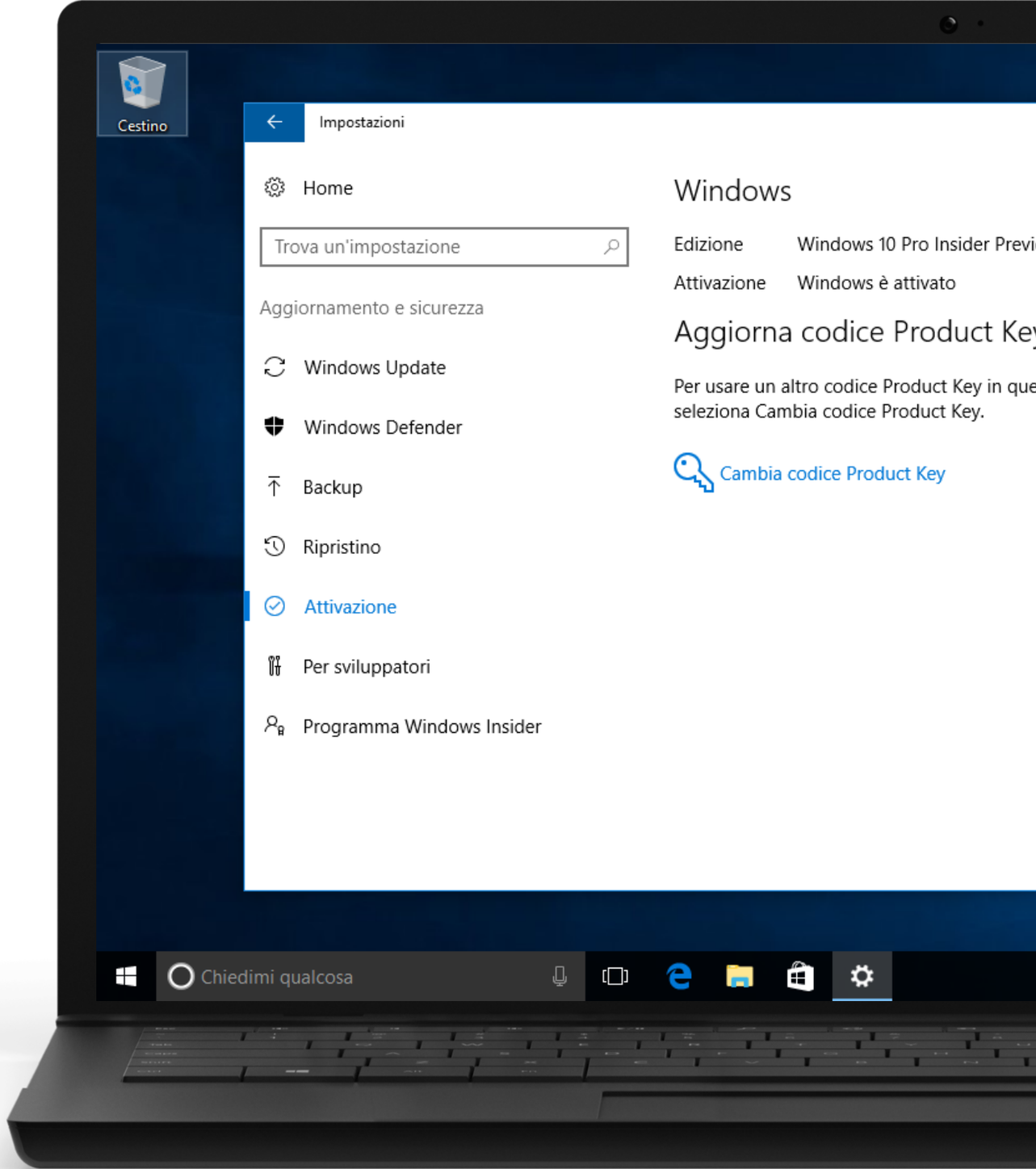


Verifica promozione DC WS2019 tramite PowerShell

```
# Verifica dell'installazione dei servizi AD
Get-Service adws,kdc,netlogon,dns

# Verifica della presenza dei ruoli FSMO di dominio
Get-ADDomain | Format-Table PDCEmulator,RIDMaster,InfrastructureMaster

# Verifica della presenza dei ruoli FSMO di foresta
Get-Forest | Format-Table SchemaMaster, DomainNamingMaster

# Verifica errori di replica a livello di dominio
Get-ADReplicationFailure -Target ICTPOWER.LOCAL -Scope Domain

# Verifica errori di replica a livello di foresta
Get-ADReplicationFailure -Target ICTPOWER.LOCAL -Scope Forest
```

DEMO

Deploy DC WS2019



ICT POWER.IT

Microsoft

Demote DC WS 2008

Migrazione Active Directory a Windows Server 2019

Spostamento ruoli FSMO

```
# Ricerca ruoli FSMO di foresta
Get-ADForest | Select DomainNamingMaster, SchemaMaster

# Ricerca ruoli FSMO di dominio
Get-ADDomain | Select InfrastructureMaster, RIDMaster, PDCEmulator
```

Ruolo	Scope	Diritti necessari al move
SchemaMaster	Foresta	Schema Admins
Domain Naming Master	Foresta	Enterprise Admins
RID Master	Domino	Domain Admins
PDC Emulator	Domino	Domain Admins
Infrastructure Master	Domino	Domain Admins

```
# Move di tutti i ruoli FSMO
Move-ADDirectoryServerOperationMasterRole -Identity "DCName" -OperationMasterRole SchemaMaster,
DomainNamingMaster, RIDMaster,InfrastructureMaster,PDCEmulator

# Move dei singoli ruoli FSMO
Move-ADDirectoryServerOperationMasterRole -Identity "DCName" -OperationMasterRole SchemaMaster
Move-ADDirectoryServerOperationMasterRole -Identity "DCName" -OperationMasterRole DomainNamingMaster
Move-ADDirectoryServerOperationMasterRole -Identity "DCName" -OperationMasterRole RIDMaster
Move-ADDirectoryServerOperationMasterRole -Identity "DCName" -OperationMasterRole InfrastructureMaster
Move-ADDirectoryServerOperationMasterRole -Identity "DCName" -OperationMasterRole PDCEmulator
```

*Controllare che nel **registro Directory Services** siano registrati **5 eventi d'informazioni ActiveDirectory_DomainService 1458***

Rimozione del ruolo Global Catalog

```
# Ricerca Global Catalog della foresta
Get-ADDomainController -Filter * | Select Name, IsGlobalCatalog

# Rimozione del ruolo Global Catalog dal DC WS2008
Set-ADObject -Identity (Get-ADDomainController -Identity "DCName").NTDSSettingsObjectDN -Replace @{options='0'}

# Verifica record DNS relative al Global Catalog
Get-DnsServerResourceRecord -ZoneName domain.ext -RRType "SRV" -Name "_gc._tcp"
```

Richiede l'appartenenza al gruppo **Enterprise Admins nella foresta** o al gruppo **Domain Admins nel dominio root della foresta**

*Controllare che nel **registro Directory Services** del **DC WS2008 su cui è stato rimosso il GC** sia registrato l'**evento d'informazioni NTDS General 1120***

*Controllare che nel **registro Directory Services** del **DC WS2019** sia registrato l'**evento d'informazioni ActiveDirectory_DomainService 1869***

Verificare che sia stato **rimosso il record DNS SRV _gc relativo al DC WS2008 su cui è stato rimosso il GC** e che sia presente solamente il record DNS SRV _gc relativo al DC WS2019

Dopo la verifica riavviare il DC WS2008

Demote DC WS2008

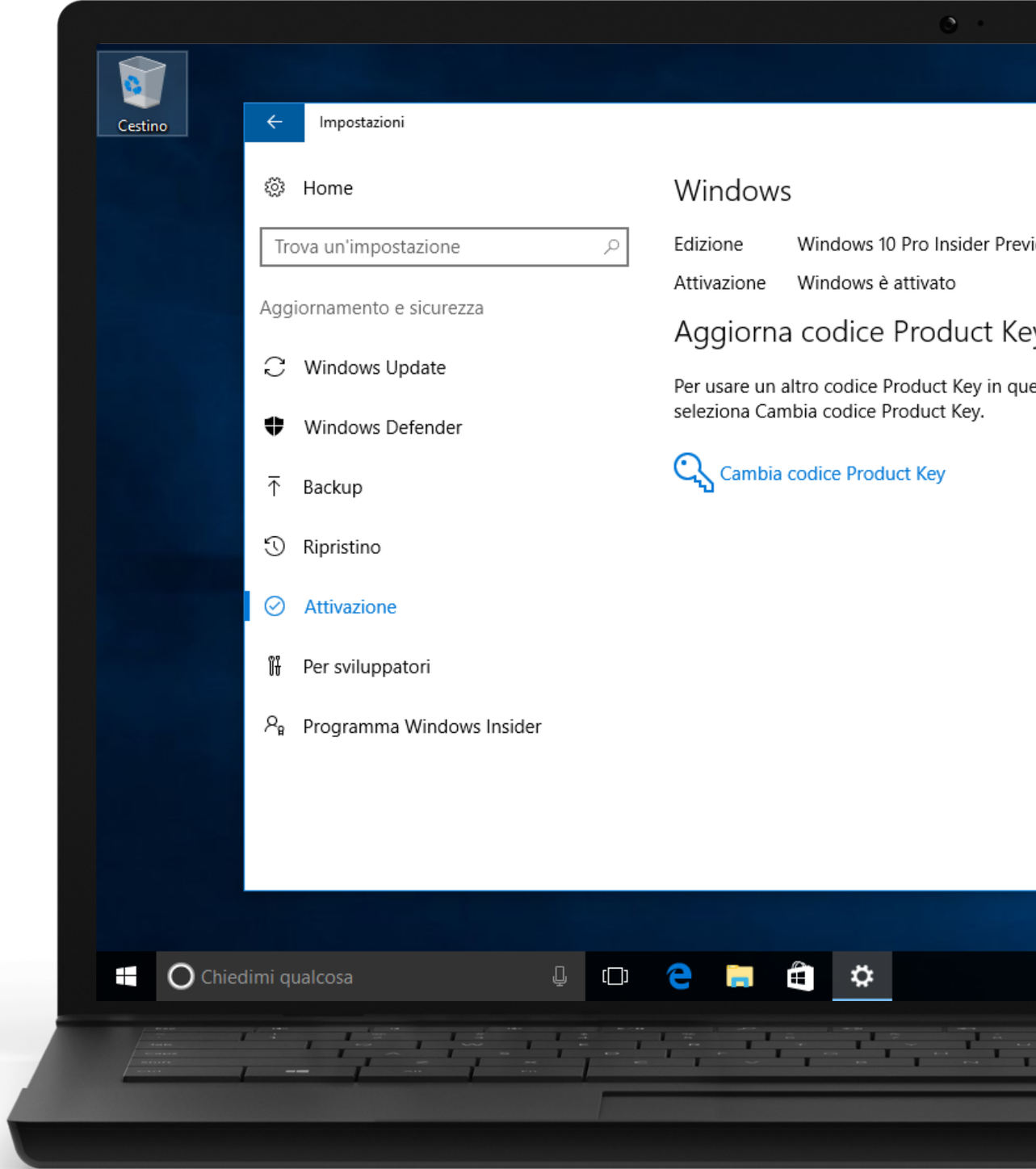
1. Controllare che il DC non sia utilizzato nell'infrastruttura (xes. come NTP/DNS server da host non a domino)
2. Impostare il DC WS2019 come primo DNS per evitare problemi di risoluzione DNS durante il demote
3. Rimozione del server DNS dal Domain Controller Windows Server 2008 tramite DCPROMO (richiede privilegi Enterprise Admin)
4. Rimozione manuale dei riferimenti al DC WS2008 in Active Directory

```powershell
# Verifica livello funzionale di Dominio
(Get-ADDomain).DomainMode

# Innalzamento del livello funzionale di Dominio alla versione 2019
Set-ADDomainMode -Identity ICTPOWER.LOCAL
  -DomainMode Windows2019Domain -Confirm:$False

# Verifica livello funzionale di Foresta
(Get-ADForest).ForestMode

# Innalzamento del livello funzionale di Foresta alla versione 2019
Set-ADForestMode -Identity ICTPOWER.LOCAL
  -ForestMode Windows2019Forest -Confirm:$False
```

Dalla versione 2008 R2 è possibile innalzare ed abbassare il livello funzionale di Dominio e Foresta, l'operazione possibile esclusivamente tramite PowerShell e non tramite GUI

DEMO

Demote DC WS2008



Grazie

Ermanno Goletto
Microsoft MVP Reconnect
e.goletto@outlook.it


/devadmin.it


@ermannog

Roberto Massa
Microsoft MVP Reconnect
robimassa@outlook.it


/facebook


@robi_massa