Windows Server 2012 — 05-Lägg till en extra DC

Denna laboration är en del av en serie labbar om Windows Server 2012R2 som till stor del bygger vidare på varandra. I denna laboration kommer vi att lägga till SERVER2 till domänen och sedan via SERVER1 installera AD DS på SERVER2 och göra SERVER2 till en extra domänkontrollant. På detta sätt kommer vi att få redundans och automatisk lastbalansering för ökad säkerhet och tillgänglighet.

Antal: Enskilt eller i grupp om 2.

Material: Tillgång till SERVER1 och SERVER2 från tidigare laborationer.

Tips: Titta på relevanta genomgångar på webbplatsen http://itlararen.se/videos.html#video3

Utförande: Vi kommer i denna laboration att visa hur man lägger till SERVER2 till domänen och installerar AD DS samt gör SERVER2 till DC via SERVER1 med Powershell. Det går givetvis lika bra att göra samma sak via det grafiska gränssnittet direkt på SERVER2 likt det vi gjorde i förra laborationen. Observera att SERVER2 skulle lika gärna kunna vara en Server Core installation för denna laboration.

1. Starta SERVER2 och logga in som lokal administratör. Obs! SERVER1 måste också vara igång.
2. Starta Powershell som administratör genom att högerklicka på Powershell-ikonen i snabbstartsfältet och välj **Run as Administrator**.
3. När Powershellprompten startat. Kör kommandot **sconfig** och tryck enter för att starta Server Configuration Tool.
4. Skriv **8** och tryck på enter för att komma åt Network Adapter Settings sidan. Nu visas en lista över tillgängliga nätverkskort.
5. Ange indexnummer för aktuellt nätverkskort som är anslutet till labbnätverket (det bör vara det som är konfigurerat med IP-adressen 192.168.0.2 från tidigare laboration) och tryck på **Enter**.
6. Skriv **2** och tryck på enter för att konfigurera DNS-inställningar för valt nätverkskort.
7. Ange IP-adress till SERVER1 som är vår DNS-server (och domänkontrollant). Tryck på enter. Klicka sedan på **Ok** när nästa dialogfönster dyker upp.
8. Tryck på enter igen för att inte ange någon sekundär DNS-server.
9. Kontrollera så att allt är konfigurerat korrekt innan ni skriver **4** och trycker på enter för att komma tillbaka till huvudmenyn.
10. Skriv **1** och tryck på enter. Skriv sedan **D** och tryck på enter för att ange att du vill ansluta SERVER2 till en domän.
11. Ange **itlararen.test.com** som den domän du vill ansluta till. Tryck på enter.
12. Ange användarnamnet **ITLARAREN\Administrator** som är NetBIOS-namnet för domänen följt av användarnamnet för domänadministratören. Tryck på enter.
13. Nu dyker det upp ett nytt kommandoprompts-fönster där man ombeds att mata in lösenordet för vald användare. Observera att när man skriver lösenordet nu så kommer det ej att visas i fönstret. Detta för att ingen ska kunna se lösenordet i klartext när du skriver in det. Ange lösenordet. Det bör vara 1qaz!QAZ eller 1qaz!QAZ2 beroende på ifall det ändrades eller ej i en tidigare laboration. Tryck på enter.
14. Klicka **No** i Change Computer Name dialog box som dyker upp.
15. Klicka på **Yes** i Restart dialog box för att starta om SERVER2.

16. Kontrollera att SERVER2 har anslutits till domänen genom att logga in på SERVER2 som lokal administratör och kör sconfig igen när servern startat om (eller titta i Server Manager). Stäng ner System Configuration Tool när detta är klart.
17. Byt till SERVER1 och logga in som domänadministratör.
18. Stäng ner Server Manager.
19. Öppna en Powershell prompt på SERVER1.
20. Vi ska nu via Powershell kontrollera att Rollen AD DS ej är installerad på SERVER2. Kör kommandot **Get-WindowsFeature -ComputerName SERVER2** och tryck på enter. Kontrollera resultatet. Observera att nu körs WinRM via Powershell men till skillnad från tidigare så ansluter vi nu till en dator som är medlem i en domän som vi administrerar och därför är det betydligt enklare än i tidigare laboration med RSAT. Vi skulle lika gärna kunna lagt till SERVER2 som en server att administrera via SERVER1s Server Manager och sedan göra allt via det grafiska gränssnittet men för träningens skull så gör vi allt via Powershell.
21. För att installera serverrollen AD DS på SERVER2 via SERVER1 skriv: **Install-WindowsFeature -ComputerName SERVER2 -Name AD-Domain-Services –IncludeManagementTools** och tryck på enter. När detta är klart kör kommandot **Invoke-Command -ComputerName SERVER2 {Install-ADDSDomainController -InstallDns -Credential (Get-Credential ITLARAREN\Administrator) -DomainName itlararen.test.com}** för att göra SERVER2 till domänkontrollant för domänen itlararen.test.com. Ange domänadministratörslösenordet (1qaz!QAZ2) följt av återställningslösenordet för domänen två gånger (1qaz!QAZ) klicka sedan på **Yes to all**. Invoke-kommandot används för att köra skript på fjärrdatorer då kommandot Install-ADDSDomainController ej kan köras remote direkt med –ComputerName parametern. Bra att veta: för att göra detta på äldre servrar, t.ex. Windows Server 2008 så måste remote signing av skript aktiveras på fjärrdatorn. Detta är aktiverat som standard i Windows Server 2012.
22. Skulle något gå snett så kan vi kontrollera att SERVER2 uppfyller alla krav för att bli domänkontrollant genom att köra kommandot Invoke-Command -ComputerName SERVER2 -ScriptBlock {Test-ADDSDomainControllerInstallation -DomainName itlararen.test.com -Credential (Get-Credential ITLARAREN\Administrator)}
23. När SERVER2 blivit domänkontrollant och startat om så är det dags att kontrollera så att allt fungerar som det ska. Starta **Server Manager** på SERVER1. Klicka på **Add other Servers to Manage** för att lägga till SERVER2 till vår server pool. Välj fliken **Active Directory** och sök på SERVER2. SERVER2 bör dyka upp meddetsamma i listan. Markera SERVER2 och klicka på pilen för att lägga till SERVER2. Klicka på **Ok** för att slutföra. Observera att hade vi gjort detta meddetsamma så hade vi enkelt kunnat installera AD DS och göra SERVER2 till DC via det grafiska gränssnittet.
24. Klicka på **Tools** och starta **Active Directory Users and Computers** konsolen. Välj behållaren (ser ut som mappar) **Domain Controllers** under itlararen.test.com. Verifiera att SERVER2 nu också är en domänkontrollant för domänen. SERVER1 och SERVER2 replikerar nu data mellan varandra automatiskt. Skulle en av servrarna gå ner så ska det inte märkas så länge en av servrarna fungerar.
25. Byt till SERVER2 och logga in som domänadministratör. Observera att som domänkontrollant så används inte längre de lokala kontona så använd domänadministratörskontot (ITLARAREN\Administrator).
26. Kontrollera IP-inställningarna för aktuellt nätverkskort på SERVER2. Observera att SERVER2 fortfarande använder SERVER1 som primär DNS-server och att sekundära DNS-servern nu är 127.0.0.1 (localhost). Som DC kör även SERVER2 DNS-server. Lastbalansering och replikering för DNS-tjänsten görs också automatiskt då DNS-databasen är en del av AD (för normala AD-

integrerade zoner). Best practice är att SERVER1 och SERVER2 använder varandras DNS-server tjänst tillsammans med sina egna så därför borde man ändra konfigurationen på SERVER1 och lägga till SERVER2 som sekundär DNS-server.

27. Vill man göra ett BPA (Best Practice Analyzer) test på SERVER2 via SERVER1 med Powershell så går det bra. Först får man köra kommandot **Invoke-Command –ComputerName SERVER2 {Invoke-BpaModel –ModelId Microsoft/Windows/DirectoryServices}** följt av kommandot **Invoke-Command –ComputerName SERVER2 {Get-BpaResult Microsoft/Windows/DirectoryServices}**