Windows Server 2012 — 13-DNSSEC

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 aktivera DNSSEC för Active directory integrerade zoner på våra domänkontrollanter.

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 aktivera DNSSEC för vår domän eller rättare sagt för vår AD-integrerade DNS-zon. Detta kommer i första hand att säkra upp vår DNS-infrastruktur inom domänen och DNS-servrar i domänen. För att aktivera DNSSEC för klienterna så måste de konfigureras för detta.

1. Starta SERVER1 och SERVER2.
2. Logga in på SERVER1 som domänadministratör.
3. Starta **Server Manager** klicka på **Tools** och **DNS** för att starta **DNS Manager Console**
4. Expandera trädstrukturen **DNS – SERVER1 – Forward Lookup Zones – itlararen.test.com** i fönstret till vänster.
5. Högerklicka på zonen **itlararen.test.com** och välj **DNSSEC – Sign the Zone** för att starta **Zone Signing Wizard**
6. Läs igenom informationen och klicka på **Next**
7. Enklast är att välja standardinställningar. Välj **Use default settings to sign the zone** och klicka på **Next**
8. Lägg märke till krypteringsalgoritmerna som används och klicka på **Next**
9. Klicka på **Next** och **Finish** för att slutföra processen.
   SERVER1 är nu *key master* för vår zon som är skyddad av DNSSEC. En key signing key (KSK) på 2048 bitar genereras med krypteringsalgoritmen RSA/SHA-256. Den har en rollover frequency på 755 dagar och alla records som signeras med nyckeln är giltig i 168 timmar som standard.
   En zone signing key (ZSK) på 1024 bitar genereras med krypteringsalgoritmen RSA/SHA-256. Denna nyckel används för att signera vanliga resource records såsom A, SOA, NS mm. Den har en rollover frequency på 90 dagar och zon-records som signeras är giltiga i 240 timmar.

   Om zonen vi signerat är en active directory integrerad zon (vilket den är) så replikeras nu private zone-signing keys till alla domänkontrollanter som hostar zonen via AD replikeringen. Det mesta vad gäller key-management för DNSSEC är helt automatiserat i Windows Server 2012.
10. Klicka på zonen **itlararen.test.com** i **DNS Manager**
11. Lägg märke till att zonen nu innehåller en massa resource records förknippat med DNSSEC (t.ex. RRSIG, DNSKEY, DS och NSEC3). Vi kan behöva uppdatera DNS Manager genom att klicka på **F5** för att se ändringarna som skett.

Nu kommer automatiska uppdateringar, t.ex. av klienter via dynamiska uppdateringar, att uppdateras och servern kommer att generera signaturer som sedan replikeras via AD till alla andra auktoritära servrar och varje server lägger till uppdateringen till sin kopia av zonen och uppdaterar signaturerna.

Vill man använda DNSSEC för nonauthoritative (recursive eller cahching) DNS servers så måste *trust anchors* skapas och distribueras till dem. En *trust anchor* är en förkonfigurerad publik nyckel som är associerad till en specifik zon.

Vill vi säkra sista steget mellan våra DNS-klienter och lokala DNS-servrar så rekommenderas IPSec (mer om detta i annan laboration). DNS-klienterna måste också konfigureras för att kontrollera att svaret de får verkligen har validerats av DNS-servern. Detta görs genom att konfigurera Name Resolution Policy Table (NRPT) på klienterna. Detta kan göras via Powershell eller med Group Policy.

Aktivera validering för klienter

Följande exempel är hämtat från technet och aktiverar validering av DNS-informationen för alla klienter via group policy genom att ändra default domain policy som påverkar alla användare och datorer i domänen.

1. On SERVER1, on the Server Manager menu bar, click **Tools**, and then click **Group Policy Management.**
2. In the Group Policy Management console tree, **under Domains > itlararen.test.com > Group Policy Objects**, right-click **Default Domain Policy**, and then click **Edit**.
3. In the Group Policy Management Editor console tree, navigate to **Computer Configuration > Policies > Windows Settings > Name Resolution Policy**.
4. In the details pane, under **Create Rules** and **To which part of the namespace does this rule apply**, choose **Suffix** from the drop-down list and type **itlararen.test.com** next to **Suffix**.
5. On the **DNSSEC** tab, select the **Enable DNSSEC** in this rule checkbox and then under Validation select the **Require DNS clients to check that name and address data has been validated by the DNS server** checkbox.
6. In the bottom right corner, click **Create** and then verify that a rule **for itlararen.test.com** was added under **Name Resolution Policy Table**.
7. Click **Apply**, and then close the Group Policy Management Editor.
8. On DC1, type the following commands at the Windows PowerShell prompt, and then press ENTER:

   gpupdate /force

   get-dnsclientnrptpolicy (för att verifiera inställningarna)

Detta skall du kunna efter genomförd labb:

- ✓ Aktivera DNSSEC för en domän
- ✓ Aktivera validering av DNS-information hos klienterna