Зонов трансфер. Динамично обновяване.

Зонов трансфер

Зоновия трансфер е механизъм за репликация на бази данни.

- Зонов трансфер – репликиране на вторичната зона

- Master Server – сървър, от който се тегли зоната. Може да бъде основен и вторичен, като вторичния трябва да знае IP адреса на Master сървъра.

- Slave Server – сървър, който тегли зоната.

Зоновият трансфер може да бъде:

Пълен зонов трансфер – вторичният сървър през определено време извършва трансфер на целия зонов файл.

Трансфер на промените в зоната – вторичният сървър изтегля само промените

Пропагандиране на промените – Master сървъра изпраща съобщение за промяна в зоната. Съобщението е DNS Notify и предизвиква зонов трансфер.

Итеративно запитване – DNS сървъра връща най-добрия отговор от своята зона или от

кеш паметта или предава указател за отговорен сървър за подходящо по-долно ниво в йерархията на домейните.

Рекурсивно запитване – При получаване на такова запитване сървърът изпълнява цялата работа за осигуряване на отговора. Ако няма отговор от своята база или кеш, той праща итеративни запитвания към други сървъри за да осигури отговор.

Кеширане – запомняне на получаваните отговори в кеш памет. Кешът се поддържа от сървърите и клиентите. Могат да се кешират положителните и отрицателните заявки.

Ресурсни записи

Формат за съхранения на информация за зоната.

Owner – име на хост, домейн за който се отнася записът

TTL – време за живот на записа в кеш паметта

Class – определя фамилията протоколи за които се отнася

Type – тип на ресурсния запис

RDATA – данни за ресурсния запис

Типове записи:

SOA – началния запис в зоновия файл

NS – Name Server

A – Адресен запис

PTR - указател

CNAME – псевдоним

MX – mail server

SRV – сървър за определени услуги

Формат за запис на SOA:

Име на зона IN SOA (

……..; отговорен сървър за зоната

.....; email на администратор на зоната

.....; Serial Number – номер на зоновия файл

.....; Refresh (1 Hour) – време за опресняване на зоната

.....; Retry (10 min) – време за повторен опит за опресняване

.....; Expire (1 day) – време за получаване на зонов файл

.....); min TTL – минимално време за живот

Запис на NS: Име на зона IN NS име на сървър

Адресен запис: Име на хост IN A IP адрес на хоста

Запис за указател: 1.48.16.172.in-addr.arpa IN PTR myhost.noamreskit.com

SRV запис: Service.proto.name TTL Class SRV Priority Weight Port Target

Преимущества на зоновия трансфер:

1) Можем да организираме DNS в Active Directory (услуга, която осигурява по-добра сигурност).

2) Използва се протокола IXFR

3) Имаме динамично обновяване, което може да бъде защитено с помощта на възможностите на Активната Директория

4) Лесно администриране с помощта на програми

5) Възможност за работа с КЕШ

6) Интегриране с DHCP и WINS

7) Нови ресурсни записи

Принцип на работа на протокола IXFR (Инкрементиран зонов трансфер)

Функцията на IXFR е намаляване на трафика при зоновия трансфер.

Динамично обновяване

Използва се при наличие на DHCP, тъй като при промяна на IP адреса на дадено PC зоновия файл трябва да се обнови. Обновяването става със съобщението UPDATE.

Чрез UPDATE могат да се добавят нови и да се унищожават стари записи. Тези съобщения се буферират, тъй като по време на зонов трансфер не е възможна промяна на зоновия файл.

1. DHCP клиентът за IP адрес. В DHCP Request съобщението се включва името на

клиента.

2. DHCP сървъра връща на клиентът IP адрес.
3. Клиентът изпраща заявка към DNS сървъра за обновяване на своя адресен запис (A запис) в зоната.
4. DHCP сървъра изпраща съобщение към DNS сървъра за обновяване на указателния запис (PRT запис) клиента в обратната зона. Използва името на клиента от първата стъпка.

Алгоритъм за динамично обновяване (няма го в сниманите лекции)

Клиентът даващ заявка за обновяване трябва да открие главен name server, към който да я изпрати.

- Клиентът използва заявка за SOA запис, в резултат на която открива сървъра и зоната, към която се отнася обновяването.

- Към открития сървър клиентът изпраща условно съобщение за обновяване, за да провери дали исканата регистрация вече съществува. Ако тя не съществува, клиентът изпраща подходящо съобщение за динамично обновяване, за да се регистрира нужния запис.

- Ако обновяването не се осъществи по някаква причина, клиентът прави опит за регистрация на записа при друг главен сървър.

В случай на неуспех опитът се повтаря след 5 минути, после след 10 минути, след което опитите продължават периодично на всеки 50 минути.

Всеки хост, изпълняващ Windows 2000 прави опит да регистрира своите адресни и указателни записи (A и PTR записи). Това се прави основно от услугата DHCP клиент. Тя се изпълнява на всяка машина, независимо дали тя е конфигурирана като DHCP клиент или не. По подразбиране A записът се взима от DHCP клиента, а PTR записът от DHCP сървъра.

DHCP сървъра може да бъде конфигуриран да „Update DSN server according to client request” (by default) или „Always update forward and reverse look-ups”. При втората конфигурация DHCP сървъра обновява A и PTR записите.

Ако на DHCP сървъра е забранено да изпълнява динамично обновяване DHCP клиента ще се опита да обновява A и PTR записите. След изтичането на определено време записите трябва да бъдат изтрити от съответната зона. Може да възникне проблем ако машината бъде изключена преди това, тъй като там ще останат недействителни записи.

Динамичното обновяване изисква - Записите да бъдат изтривани от компютъра, който ги е регистрирал – DHCP сървър, клиент или и от двата. Тъй като DHCP сървърът е собственик на IP адресите той трябва да се стимулира да извършва PTR регистрацията, когато това е възможно.

Конфликт на имена:

Клиент може да открие, че неговото име вече е регистрирано в DNS сървъра с IP адрес, принадлежащ на друга машина. По подразбиране клиентът изтрива стария запис и регистрира собствен нов запис. Само собственикът на съществуващият запис може да го променя.

Secure Dynamic Update

Може да се построи ACL (Access Control List), който задава списък от групи или потребители, които могат да променят записи в зоните. Secure Dynamic Update създава защитена среда чрез предаване на защитени маркери. Използва се средата за ограничено време за създаване и проверка на записите на базата на маркирани съобщения.

Процес на промяна на име от страна на клиент:

1. Клиентът прави заявка към локалния Name Server за да определи кой Name Server е отговорен за името, което клиента иска да промени.
2. Клиентът пита отговорния Name Server дали е отговорен за името, което иска да промени.
3. Клиентът се опитва да извърши незащитена промяна и сървърът отказва.
4. Клиентът и сървърът се договарят за защитена среда на общуване. Те обменят един или повече защитени маркери. За пренасяне на маркерите се използват TKEY ресурсни записи. Първо се договарят за използвания защитен механизъм, решават механизма да е Kerberos, използвайки Kerberos проверява своята идентичност.

TSIG – Transaction Signature for DNS. Това е ресурсен запис за изпращане и проверка на защитени съобщения. Осигурява защитено предаване на зонов файл, Notify съобщенията при рекурсивна резолюция и при динамично обновяване.

ACL – Access Control List

TKEY – Ресурсен запис, механизъм за автоматично генериране на общ секретен ключ между двата хоста. Механизъм за прехвърляне на секретни маркери между клиент и сървър. Има няколко механизма за генериране и присвояване на ключове: Diffie-Hellman Key и Kerberos (При Windows 2000). TKEY процеса трябва да използва подписани съобщения чрез TSIG или SIG(0).