

**DNS 101**  
Laborationsinstruktioner

2021-12-09 - 2021-12-10



# INNEHÅLL

<b>1 DNS</b>	<b>1</b>		
Innan ni börjar . . . . .	1		
Uppgift 1 . . . . .	1		
Auktoritativ namnserver - master . .	1		
Uppgift 2 . . . . .	1		
Auktoritativ namnserver - slav . . . .	1		
Uppgift 3 . . . . .	2		
Bakåtuppslag - publika IP-adresser .	2		
Uppgift 4 . . . . .	2		
Bakåtuppslag - privata IP-adresser .	2		
Uppgift 5 . . . . .	2		
Resolver - forwarding . . . . .	2		
<b>2 DNSSEC</b>	<b>3</b>		
		Uppgift 6 . . . . .	3
		Signera er domän . . . . .	3
		<b>3 DNS cheat sheet</b>	<b>4</b>
		BIND . . . . .	4
		Exempel på SOA . . . . .	4
		Exempel på Konfiguration (Master) .	4
		Exempel på Konfiguration (Slave) . .	5
		Exempel på Konfiguration (Resolver)	5
		TSIG exempel . . . . .	5
		Tips och trix . . . . .	5
		Tänk på att . . . . .	5
		Felsökning . . . . .	5



# KAPITEL 1: DNS

## INNAN NI BÖRJAR

---

Ni har åtkomst till samtliga maskiner från er *Jumpgate* och användaren är alltid 'ubuntu'. Se IP-planen för alla relaterade uppgifter. Sökvägar, kommandon och exempel finner ni under Kapitel 3. Ändringar i filer gör ni via valfri tillgänglig texteditor (som vim eller nano). Den publika IP-adressen på er *Jumpgate* motsvarar utsidan på en brandvägg. Det är den adressen ni ska använda i de fall en pekare kräver en publik IP.

## UPPGIFT 1

### AUKTORITATIV NAMNSERVER - MASTER

---

1. Konfigurera er namnserver att vara master för er tilldelade domän
  - Logga in på er *DNS Master*
  - Skapa en zonfil för er domän med all nödvändig information (för enkelhetens skull, sätt NS till ns1.<domän>)
  - Lägg till domänen som masterzon i konfigurationen för BIND
  - Ladda om BIND
  - Kontrollera med DIG att namnservern svarar korrekt
2. Lägg till en mailpekare för er domän
  - Lägg till en MX-pekare i zonen
  - Lägg till en A-pekare för MX-pekarens namn
  - Ladda om BIND
  - Kontrollera med DIG att namnservern svarar korrekt
3. Lägg till en pekare för en websida under er domän (med och utan www)
  - Lägg till pekare för webservern (IPv4)
  - Ladda om BIND
  - Kontrollera med DIG att namnservern svarar korrekt
  - Testa att surfa till <domän>
4. Ändra webpekaren till ett CNAME
  - Byt ut A-pekaren mot en CNAME-pekare
  - Ladda om BIND
  - Kontrollera med DIG att namnservern svarar korrekt
  - Testa att surfa till <domän>

## UPPGIFT 2

### AUKTORITATIV NAMNSERVER - SLAV

---

1. Lägg till en sekundär namnserver (slavserver) för er domän
  - På *masterservern*: Tillåt zonöverföring till er *slavserver* i konfigurationen för BIND
  - På *masterservern*: Lägg till NS och glue för slavservern i zonfilen
  - På *slavservern*: Lägg till domänen som slavzon i konfigurationen för BIND
  - Ladda om BIND på både master och slav
  - Kontrollera med DIG att båda namnservrar svarar korrekt
2. Säkra upp zonöverföringen med TSIG
  - På *masterservern*: Generera en TSIG-nyckel



- På *masterservern*: Lägg till nyckeln i konfigurationen för BIND
- På *masterservern*: Ändra så att zonöverföring bara tillåts med TSIG
- På *slavservern*: Lägg till nyckeln i konfigurationen för BIND
- Ladda om BIND på både master och slav
- Verifiera att det fungerar
  - På *masterservern*: lägg till en valfri TXT-pekare i zonen
  - På *masterservern*: Ladda om BIND
  - Kontrollera med DIG att båda namnservrar svarar korrekt

## UPPGIFT 3

### BAKÅTUPPSLAG - PUBLIKA IP-ADRESSER

---

1. Konfigurera er namnserver att vara master för er tilldelade *reversedomän* (Se tidigare uppgift)
2. Lägg till en reversepekare för IP-adressen på er masternamnserver
3. Lägg till en sekundär namnserver (slavserver) för reversedomänen (Se tidigare uppgift)
4. Kontrollera med DIG att båda namnservrar svarar korrekt

## UPPGIFT 4

### BAKÅTUPPSLAG - PRIVATA IP-ADRESSER

---

1. Konfigurera er namnserver att vara master för en av era *interna reversedomäner* (55.0.10.in-addr.arpa) (Se tidigare uppgift)
2. Lägg till reversepekare för de interna IP-adresserna för:
  - Resolvern
  - Jumpgaten
3. Lägg till en sekundär namnserver (slavserver) för reversedomänen (Se tidigare uppgift)
4. Kontrollera med DIG att masterservern svarar korrekt

**Extrauppgift:.** Konfigurera även reverse-zonen för 77.0.10.in-addr.arpa med reversepekare för mailserver och webserver

## UPPGIFT 5

### RESOLVER - FORWARDING

---

1. Konfigurera er resolver att skicka frågor för er interna reversedomän till er auktoritativa namnserver
  - logga in på resolvern
  - Lägg till reversedomänen som en *forward-zon* i konfigurationen för BIND
  - Ladda om BIND
2. Kontrollera med DIG att du får korrekt svar från er *jumpgate*

**Extrauppgift:.** Lägg även upp en forward för reverse-zonen 77.0.10.in-addr.arpa enligt ovan.



# KAPITEL 2: DNSSEC

## UPPGIFT 6

### SIGNERA ER DOMÄN

---

1. **Alternativ 1:** Manuell nyckelgenerering
2. Generera nycklar
  - Skapa en katalog att lägga nycklarna i (lämpligen under /var/cache/bind)
  - Se till att BIND kan läsa från katalogen och alla filer i den
  - Generera nyckelpar för ZSK
  - Generera nyckelpar för KSK
  - Lägg till nödvändiga uppgifter i zon-konfigurationen för BIND
  - Ladda om BIND
3. Kontrollera med DIG att zonen blivit signerad
4. Generera ett DS-record att skicka upp till föräldrazonen
5. Skicka DS-record till kursinstruktör
6. Vänta på ett OK från kursinstruktör att DS ligger i föräldrazonen
7. Kontrollera med DIG *mot en extern resolver* att zonen validerar

**Automatisk nyckelgenerering:** Som alternativ till manuell nyckelgenerering kan man låta BIND generera nycklar och signera automatiskt. Skapa i så fall som vanligt en katalog för nycklar och ge BIND rättigheter att både läsa och skriva till den. Se alternativ zon-konfiguration för detta nedan



# KAPITEL 3: DNS CHEAT SHEET

## BIND

### BIND KONFIGURATION

/etc/bind/named.conf.local

Konfigurationsfil för zoner

/var/cache/bind/

Katalog för zonfiler med tillhörande metadata

**Notera.** Tecken för att kommentera text skiljer sig mellan konfigurationsfiler och zonfiler

- konfigurationsfil: // kommenterar all följande text på raden. Det går också att använda /\* \*/ för att kommentera hela block.
- zonfil: ; för att kommentera bort rad

### EXEMPEL PÅ SOA

```
group1.examples.nu. 3600 IN SOA ns1.group1.examples.nu. hostmaster.examples.nu. (  
    1606898653 ; serial  
    4400      ; refresh (4 hours)  
    3600      ; retry (1 hour)  
    604800    ; expire (1 week)  
    600       ; minimum (1 hour)  
    )
```

**Alternativ:.** Kan även skrivas som en rad

```
group1.examples.nu. 3600 IN SOA ns1.group1.examples.nu. hostmaster.examples.nu. 1606898653 4400 3600 604800 3600
```

### EXEMPEL PÅ KONFIGURATION (MASTER)

```
zone "group1.examples.nu" {  
    type master;  
    file "/var/cache/bind/group1.examples.nu";  
    allow-transfer {  
        key "group1-tsig";  
    };  
};
```

```
key "group1-tsig" {  
    algorithm hmac-sha256;  
    secret "KSL8qbZ6KYVz8GCefi4qKOMgg+oQ3rUM++0VJv657y0=";  
};
```



## EXEMPEL PÅ KONFIGURATION (SLAVE)

```
zone "group1.examples.nu" {
    type slave;
    masters {45.155.99.160;};
};
```

```
key "group1-tsig" {
    algorithm hmac-sha256;
    secret "KSL8qbZ6KYVz8GCefi4qK0mgg+oQ3rUM++0VJv657y0=";
};

server 45.155.99.160 {
    keys { group1-tsig; };
};
```

## EXEMPEL PÅ KONFIGURATION (RESOLVER)

```
zone "55.0.10.in-addr.arpa" {
    type forward;
    forward only;
    forwarders {10.0.77.53;};
};
```

## TSIG EXEMPEL

```
tsig-keygen -a hmac-sha256 <zona>
```

**Not:** Kommandot ovan skriver bara ut i terminalen, inte till någon fil.

## TIPS OCH TRICK

### TÄNK PÅ ATT

- Uppdatera zonens serienummer vid varje ändring
- Kontrollera zon och konfiguration med BINDS verktyg
- Felorsaken kan ofta hittas i /var/log/syslog

## FELSÖKNING

### BIND VERKTYG

named-checkconf	Kontrollerar konfiguration i BIND (ingen output = syntax ok)
named-checkzone <zonnamn> <zonfil>	Kontrollerar att BIND kan läsa och ladda zonen
rndc status	Visar status för BIND (i.e. om BIND är igång eller inte)
rndc reload	Laddar om BIND efter ändringar i zoner och/eller konfiguration

### EXTERNA VERKTYG

<a href="https://zonemaster.iis.se">https://zonemaster.iis.se</a>	kontrollerar uppsättningen av en zon. OBS. Cachar resultatet från ett test i ca 10 minuter.
<a href="https://zonemaster.net">https://zonemaster.net</a>	Alternativ till zonemaster.iis.se.
<a href="https://dnsviz.net">https://dnsviz.net</a>	Visar delegeringsträd grafiskt. Speciellt bra vid felsökning av DNSSEC. Man måste aktivt be verktyget göra om ett test, annars visas resultat från det senaste testet