# Sjunet robust DNS

Teknisk Beskrivning

inera

| Revisionshistorik | | |
|---|---|---|
| Version | Författare | Kommentar |
| 0-0.9 | Björn Gustavsson | |
| 0.91 | Christoffers Johansson | |

# 1. Inledning

Detta dokument syftar till att ge berörda intressenter en teknisk överblick hur Sjunets robusta DNS fungerar och hur det driftas och förvaltas.

# 2. Syfte

Detta dokument är till för att beskriva hur Sjunets DNS-system är designat samt till att öka förståelsen för lösningen

# 3. Bakgrund

DNS-systemets syfte är att översätta DNS namn/värden till IP-adresser oberoende av Internet. Systemet är verksamhetskritiskt för tjänster inom e-Hälsa och är därför robust designat och förvaltat för att ha en hög tillgänglighet.

De flesta anrop som sker över ett nätverk till fjärrsystem görs genom att källmaskinen skickar förfrågan om ett DNS värde till en eller flera DNS servrar. Dessa svarar i sin tur med aktuell IP adress. Detta underlättar konfiguration av system genom att man bara behöver ändra IP adress centralt i DNS istället för på varje källmaskin. Om kontakten med Internet går ner och man försöker ställa DNS förfrågningar dit istället för via Sjunet medför det nästintill lika stora konsekvenser som om Sjunet i sig låg nere för berörda parter.

Inera AB har därför identifierat ett behov av att införa en robust DNS- funktion på Sjunet för att homogenisera verksamheternas DNS-arkitektur samt eliminera alla beroenden till Internet för en fungerande DNS-funktion på Sjunet.

# 4. Kontaktvägar

Frågor/incidenter skall ställas/anmälas till Inera AB.

Kontaktvägarna hittas på www.inera.se

# 5. IP-adresser

De IP-adresser som finns i miljön:

| DNS-namn | IP-adress | Funktion |
|---|---|---|
| dnsadmin.sjunet.org | 81.89.151.36 | Administratörsgränssnittet |
| login.dnsadmin.sjunet.org | 81.89.151.42 | Administratörsgränssnitt för inloggning med SITHS- |

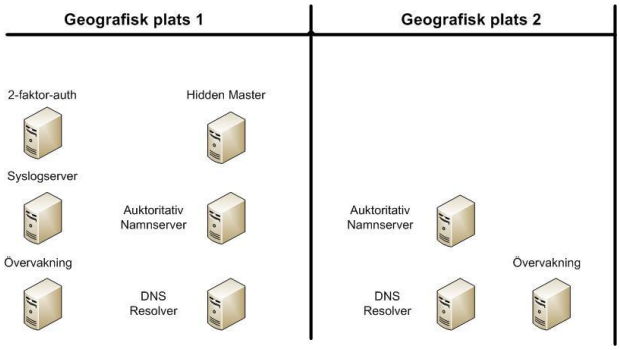
| | | kort |
|---|---|---|
| dns1.sjunet.org | 81.89.151.38 | DNS1,auth |
| dns2.sjunet.org | 81.89.151.10 | DNS2,auth |
| dns3.sjunet.org | 81.89.151.40 | DNS3,resolver |
| dns4.sjunet.org | 81.89.151.12 | DNS4,resolver |
| dns1.sjunet.inera.se | 193.44.76.181 | DNS1,auth (internet) |
| dns2.sjunet.inera.se | 82.196.191.243 | DNS2,auth (internet) |

# 6. Lösningen

Fysiskt skilda drifthallar, funktionerna i lösningen är sedan fördelade enligt följande

Geografisk plats 1:

- Hidden Master
- Auktoritativ namnserver1
- DNS-resolver1
- Övervakning
- Syslogserver
- Front-end för 2-faktor-autentisering (login)




Geografisk plats 2:

- Auktoritativ namnserver2
- DNS-resolver2
- Övervakning

# 7. Administration

Administrationsgränssnittet är en webbaserad lösning. Behörighet för administration till utvalda resurser och subzoner delegeras av Inera efter beställning till Kundservice av den som är Sjunet-ansvarig eller motsvarande inom respektive organisation.

Loggning av åtkomst, förändringar och versioner sparas för uppföljningssyfte.

Autentiseringsmodulen för inloggning i administrationsgränssnittet baseras på 2-faktor-autentisering med SITHS-certifikat. Policy för hanteringen av ex. TTL-värden, SOA-poster baseras på RFC 1912.

# 8. Lokala DNS-Inställningar

Beroende på hur man i dagsläget har satt upp sin interna DNS-struktur så kan man behöva implementera DNS zonen *.sjunet.org på olika sätt.

Metod 1:

- Villkorlig forward till autentiseringsservrar för just zonen *.sjunet.org.

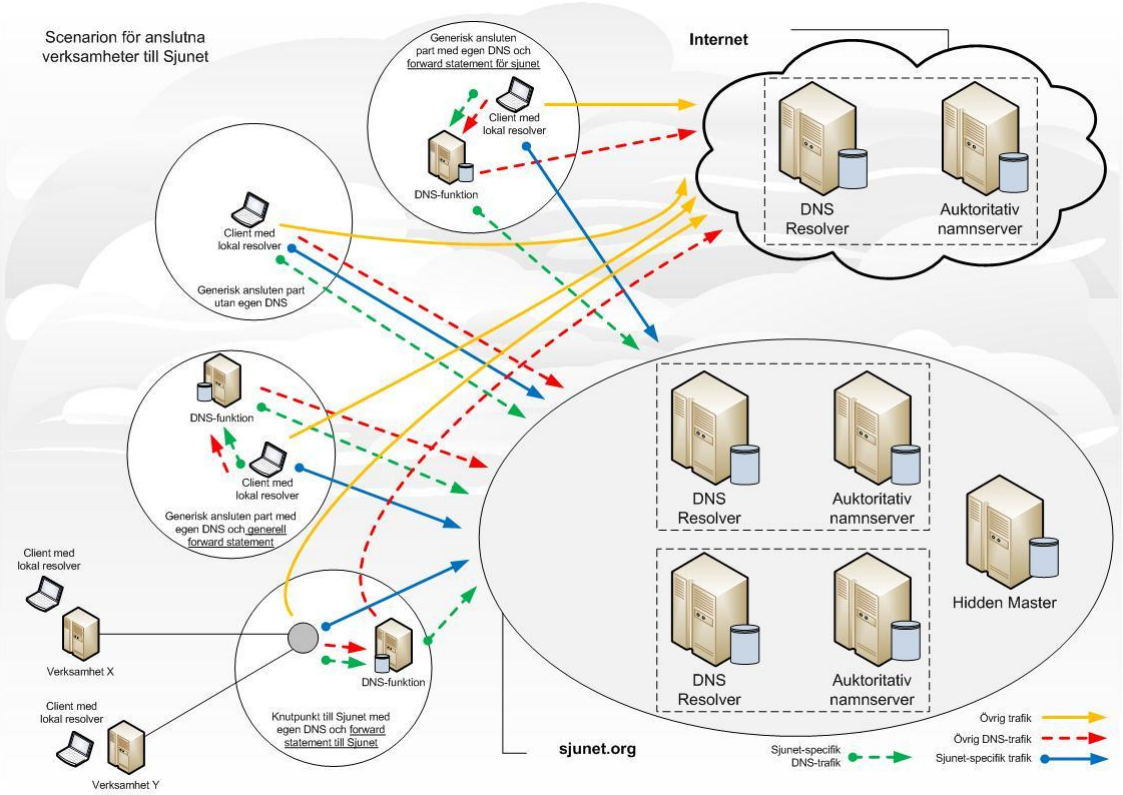
Metod 2:

- DNS forwardlookup till resolverservrar, så att alla DNS uppslag skickas vidare till Sjunets DNS servrar.

Metod 3:

- At man använder resolverservrarna på Sjunet direkt.

Scenarion som vi identifierat:



# 9. Vyer

I den nya lösningen så har vi implementerat två olika vyer.

VIEW-SJUNET och VIEW-INTERNET. DNS systemet känner av källadressen och presenterar olika vy för *.sjunet.org beroende på om klienten gör sina uppslag via Internet eller Sjunet

Detta har vi gjort då vi vill censurera vad för DNS svar en Internetanvändare får på zonen sjunet.org.

# 10. Subzone

Subzoner hanteras idag enligt två olika metoder.

Metod 1:

- Det centrala systemet har hand om subzoner och dessa administreras via gränssnittet.

Metod 2:

- Det centrala systemet delegerar zonen till en annan DNS server

Detta får konsekvenser att det inte bara räcker att öppna brandväggen emot det centrala DNS systemet utan man måste även öppna emot alla subzons DNS servrar. Då dessa kan bytas och ändra IP adresser utan att vi hinner förvarna alla slutanvändare så är det sanktionerat att ha en generell udp/tcp öppning för port 53 mot alla Sjunets IP spann. (TCP krävs för DNSsec)

# 11. Drift och förvaltning

Inera upphandlade DNS systemet som en funktion. Ansvaret för driften ligger hos leverantören Evry (Före detta SYSteam Drift Uppsala). Förvaltningen hanteras av Inera AB med stöd av Sjunets förvaltningsgrupp.

# 12. SLA

| Tillgänglighet | |
|---|---|
| Definition: | Med Tillgänglighet avses procentuell del av den totala tiden per månad som DNS-funktionen kan utnyttjas på avtalat sätt. |
| SLA: | 99,95% per månad. |
| Vite: | Etthundra (100) procent av den totala månadskostnad för drift och förvaltning för varje påbörjad procent som tillgängligheten understiger avtalad servicenivå per månad. |

| Maximalt antal fel | |
|---|---|
| Definition: | Med maximalt antal Fel avses summan av de incidenter som klassificerats som Fel under en tidsperiod |
| SLA: | Antalet Fel i DNS-funktionen skall vara maximalt ett (1) st per månad,<br>samt maximalt sex (6) st per kalenderår. |
| Vite: | Tjugofem (25) procent av månadskostnad för varje antal Fel som felet/bristen överstiger avtalad servicenivå. |

| Åtgärdstid | |
|---|---|
| Definition: | Med Åtgärdstid avses maximal tid inom Servicetid som det får ta att helt åtgärda Fel räknat från att det upptäckts. |
| SLA: | < 1 timmar |
| Vite: | Tjugofem (25) procent av månadskostnad för varje påbörjad timme som felet/bristen överstiger avtalad servicenivå.<br>timme som felet/bristen överstiger avtalad servicenivå. |

| Fel | |
|---|---|
| Definition: | Fel räknas från den tidpunkt som först inträffar av följande:<br>• Fel detekteras av övervakningssystem eller på annat sätt.<br>• Beställaren felanmäler via nationell kundtjänst<br>• Om Leverantörens funktion för felanmälan ej är nåbar skall tidpunkten räknas från den tidpunkt då anmälningsförsöket görs.<br>Fel varar till dess Leverantören funnit att DNS-funktionen fungerar |

| | |
|---|---|
| | korrekt och Beställaren meddelats och accepterat. |

| **Planerat underhåll** | |
|---|---|
| Definition: | Planerat underhåll klassas som Fel om den anslutna Nyttjarens möjlighet att bruka DNS-funktionen begränsas så att det motsvarar ett Fel och att Beställaren inte godkänt det planerade underhållet.<br><br>Leverantören informerar Beställaren om önskad tidpunkt för planerat underhåll senast 10 Arbetsdagar i förväg.<br><br>Planerat underhåll, om godkänts av Beställaren, utförs av Leverantören på lördag morgnar mellan kl. 00:00-06:00 och på måndag morgnar mellan kl. 02:00-06:00 CET (Central European Time).<br><br>Beställaren skall ha rätt att få tidpunkt för planerat underhåll ändrat, för det fall tillgängligheten på DNS-funktionen är mycket väsentlig för Nyttjarens verksamhet. |