



amanox solutions

Externer DNS

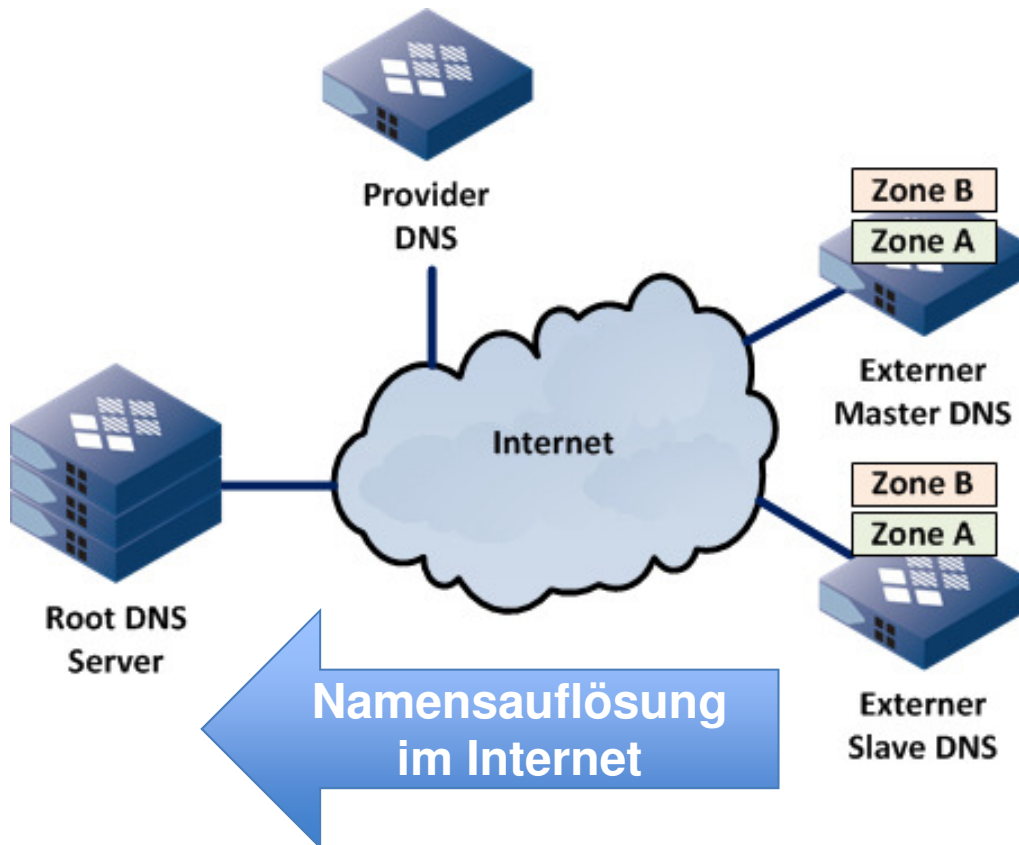
Technologien und Herausforderungen

Amanox Solutions AG
Speichergasse 39
CH-3008 Bern

Wieso brauchen wir externen DNS



amanox solutions



- **Alle Internetservices nutzen DNS**
 - E-Mail
 - Geschäftskritische Business Applikationen
 - Web (HTTP / HTTPS)
 - VoIP / Calloberation
 - Cloud Computing
- **Ohne DNS läuft das Internet nicht!**
- **Zunehmend wichtiger bei der Einführung und Migration von IPv6**

Agenda



amanox solutions

- **DNS64 und NAT64**

- Möglicher Use Case
- Funktionen und Eigenschaften
- Aktivierung und Implementierung

- **DNSSEC**

- Entwicklung und Geschichte
- Übersicht der wichtigsten Funktionen und Eigenschaften
- Aktivierung und Implementierung



amanox solutions

DNS64 und NAT64

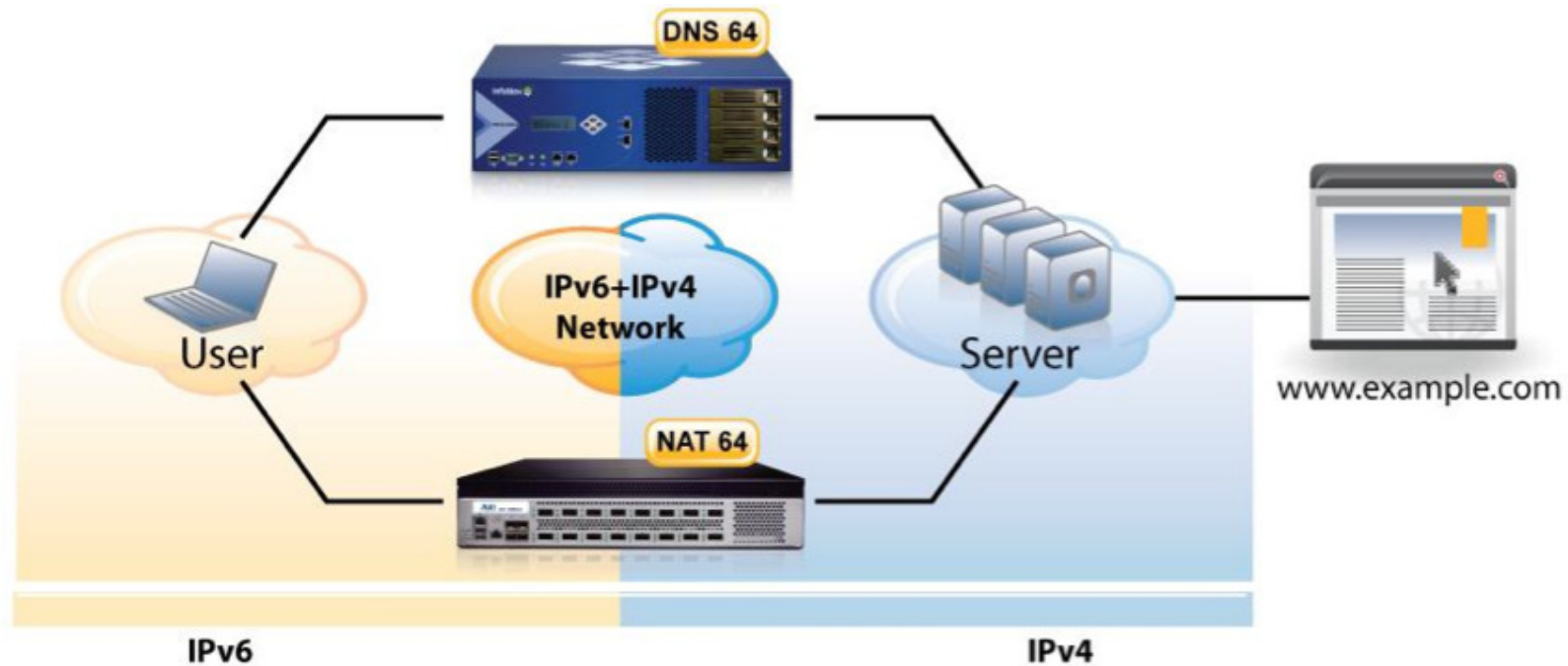
Funktionen und Eigenschaften

Amanox Solutions AG
Speichergasse 39
CH-3008 Bern

DNS64 / NAT64 Szenario



amanox solutions

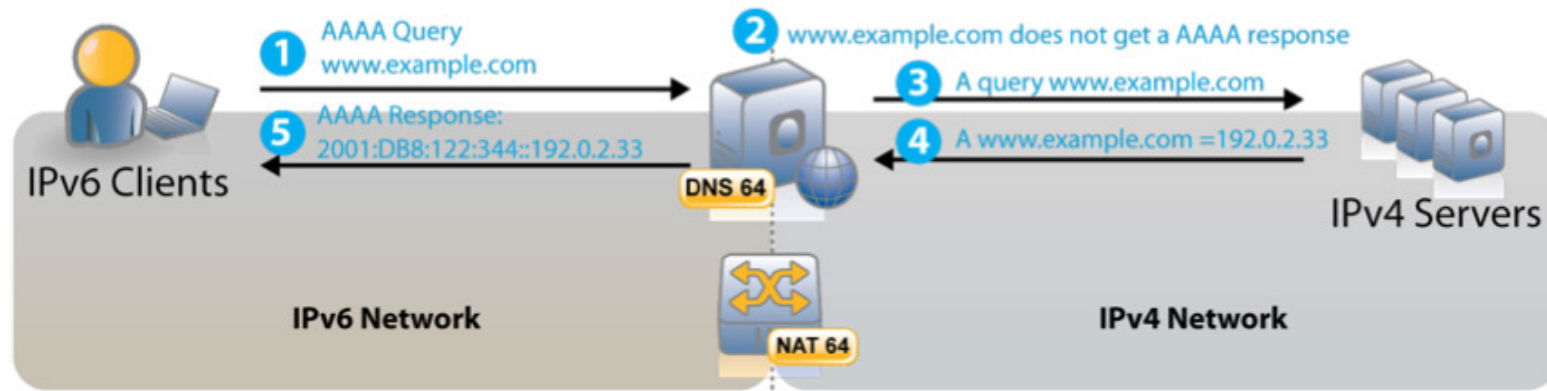


- Clients sind nur über das im interne Netzwerk (LAN) sind nur über das IPv6 Protokoll erreichbar.
- Clients nutzen aber Dienste im Internet, die nur über eine IPv4 Verbindung aufgerufen werden können.

Funktionsweise DNS64 / NAT64



amanox solutions



- DNS64 stellt sicher, dass **AAAA Queries** in **A Queries** konvertiert werden.
- aufgelöste IPv4 Adresse wird durch die IPv6 Adresse des NAT64 Gateways ersetzt.
- Datenverkehr der IPv6 Client wird anschliessend über den NAT64 Gateway weitergeleitet.

DNS64 / NAT64 Use Case



amanox solutions



Carrier/ISP/Mobile

- **Zu wenig IPv4 Adressen verhindern den Rollout von neuen Services**
 - WiFi / 3G / 4G Networks
 - Smart Phones
 - Consumer Broadband
- **Notwendig um IPv6 only Customers mit “legacy” IPv4 Kunden zu verbinden, die noch kein IPv6 besitzen**



Enterprise IT

- **Wird in den meisten Enterprise IT Umgebungen nicht benötigt**
- **Wird wichtiger, wenn der IPv6 Rollout fortgeschritten ist.**
 - Kunden möchten IPv4 auf den ihrer Infrastruktur deaktivieren
 - Einige “legacy” Systeme unterstützen nicht IPv6
 - Kunden können DNS64 / NAT64 nutzen um diese IPv4 Inseln miteinander zu verbinden



amanox solutions

DNSSEC

Funktionen und Eigenschaften

Amanox Solutions AG
Speichergasse 39
CH-3008 Bern

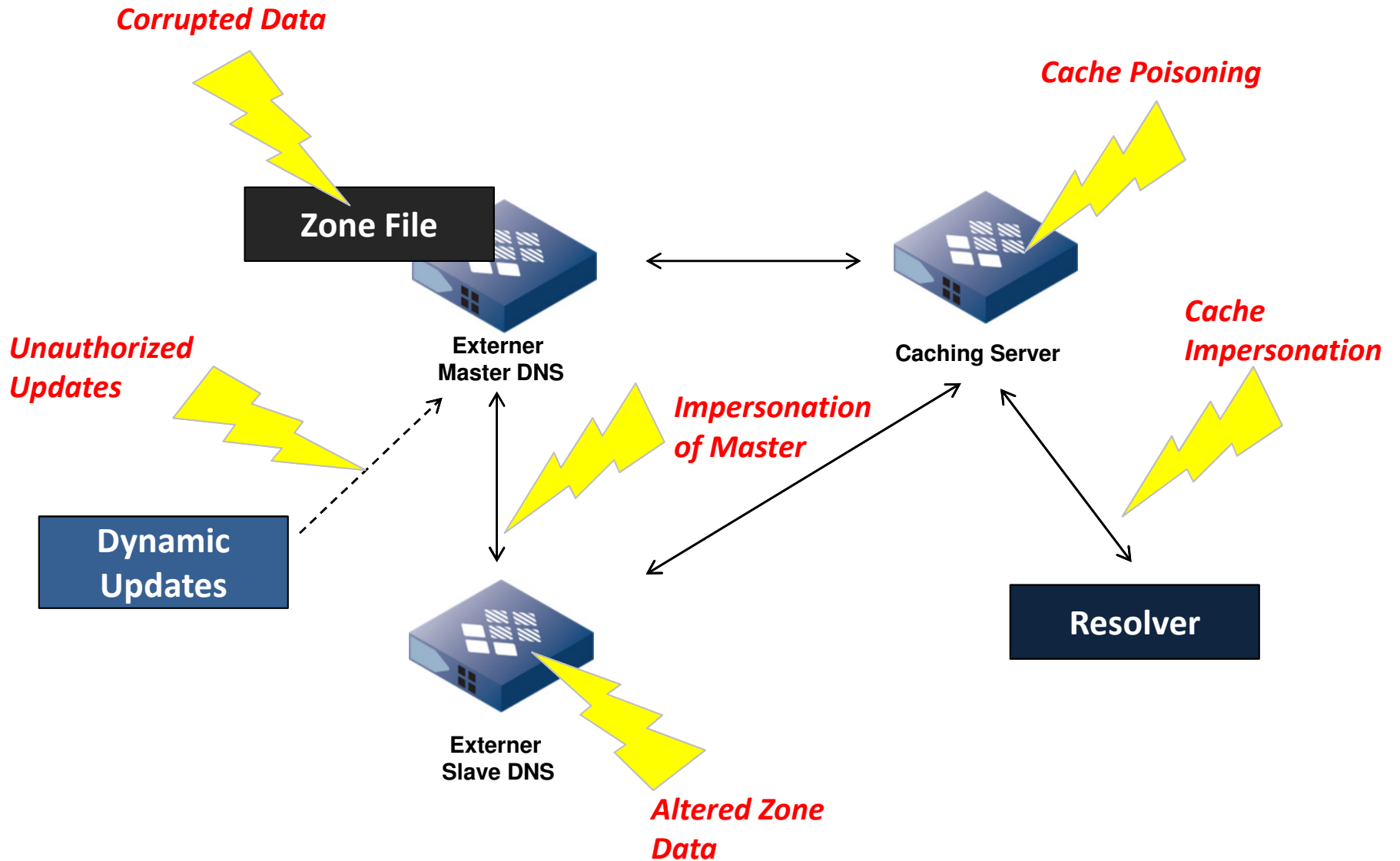
Entwicklung von DNSSEC



amanox solutions

- **1983:** Erfindung von DNS
- **2005:** Überarbeitete Version von RFC 2535 veröffentlicht
RFC 4033, RFC 4034, RFC 4035
- 2005:** Schweden (.se) aktiviert DNSSEC
- 2010:** .ch aktiviert DNSSEC (1. Februar)
- 2010:** Publikation von root zone trust anchors (15. Juli)

Wieso brauche ich DNSSEC?



Wieso brauche ich DNSSEC?



amanox solutions

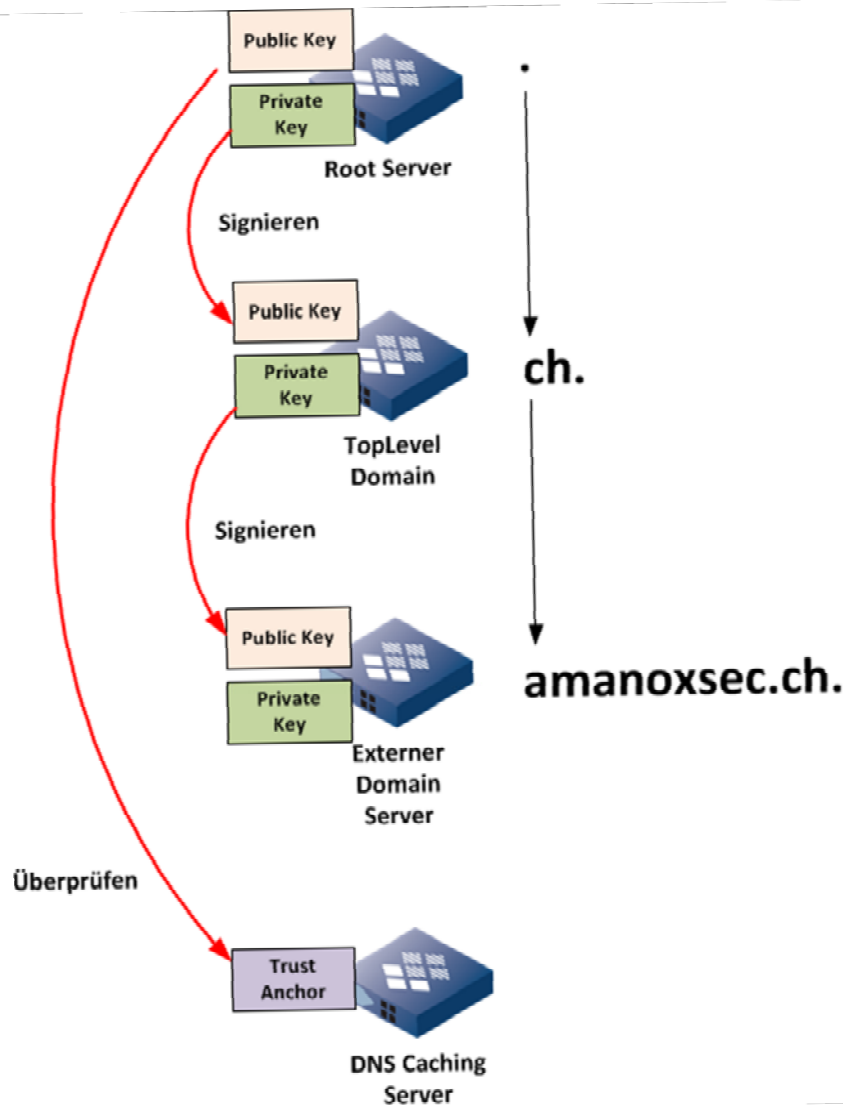
Gewährleistung von Authentizität und Datenintegrität!

- DNS Teilnehmer kann Zonendaten auf Echtheit überprüfen und sicherstellen, dass die Daten unterwegs nicht verändert wurden
- Schützt DNS vor Man-in-the-middle oder Cache Poisoning Attacken
- Zukünftige Einsatzgebiete:
 - DNS als Vertrauensquelle für Zertifikate (Kombination mit SSL)

DNSSEC Chain of Trust



amanox solutions



- DNS nutzt eine verteilte hierarchische Datenbank
- DNSSEC Chain of Trust stellt das Signieren und die Überprüfung der DNSSEC Keys sicher.
- Root Server und Top Level Domains müssen DNSSEC unterstützen und entsprechend signiert sein.

Vorgehensweise für die Einführung von DNSSEC



amanox solutions

- **Asymmetrisches Kryptosystem**
 1. Generierung von Schlüsselpaar
 2. Veröffentlichung von Public Key (z.B. bei Switch)
 3. Beglaubigung von Public Key (Chain of Trust)
 4. Signieren von Zonendaten mit Private Key
 5. Überprüfen der Zonendaten mit beglaubigtem Public Key (andere DNS Server)

- **Schlüsselmanagement**
 - **Key signing key (KSK)**
 - Lange Gültigkeit / Grosser Key
 - Rollover durch doppeltes signieren von ZSK

 - **Zone signing key (ZSK)**
 - Kurze Gültigkeit / Kleiner Key
 - Rollover durch vorgängige Veröffentlichung

DNSSEC Ressource Records



amanox solutions

- **DS**
 - Delegation Signer (Signierter public Key bei Parent Domain)
- **DNSKEY**
 - Public Key der Domain
- **RRSIG**
 - Pro Ressource Record wird ein neuer RRSIG erstellt (=> doppelt so grosse Zone)
- **NSEC**
 - Kennzeichnet einen nicht existierenden Ressource Record. (NX Record)
 - Pro Ressource Record im Zonenfile wird ein NSEC Record erstellt (=> doppelt so grosse Zone)
- **NSEC3 / SNEC3PARAM**
 - Sichere Variante von NSEC. Verhindert Brute Force Zonentransfers

DNSSEC Ressource Records



amanox solutions

•
↓
ch.

```
dig ch. @a.root-servers.net. DS  
ch. 86400 IN DS 14268 7 2  
5A1B2BCBD3D5E1D451F247537254E149E1C64CE208699E8FE9380E0D C2FF6632
```

```
dig ch. dnskey +multi  
ch. 86184 IN DNSKEY 257 3 7  
AwEAAAdAqpy19+3Mw9xSroJnYLhTugUBluCVZ0fDdpz/hPYv9QXebXICUzaKB3Z/63Q  
CNn8YorPlprYv2YwOYCT7R4f5IM1qLntQeuS3xu24+caDN5F0pUxl77FQMWUPY7zLz  
LyZcunp6Z+XJk+DgdJ84LmD69iy2TYvf192dt5GJ5/X ; key id = 14268
```

```
dig amanoxsec.ch. @a.nic.ch. DS  
amanoxsec.ch. 3600 IN DS 53166 7 2  
2E5BA5F00A2466D1FF03BBF7EE75415CC8A8152EBE5D7659B629E5B5 70893516
```

```
dig amanoxsec.ch. dnskey +multi  
amanoxsec.ch. 84282 IN DNSKEY 257 3 7  
AwEAAZxjYyOX3AlsG3sGyQZOBDZlbn67A7jv8Lk8FWjdzWsciz8RzLigyM5IUyYG5kdR  
E977zUcpPFbjWLN28T9jbtweqlWvnhFweTzmbdVDvWgXvUzCbYgSVbdbEudwIAbH  
MoGZOewo3WBzdzyOZb9JCUS7jUoK1zyITZ3zTzt5GbmtddTFG5VZ2LQPNj/i4oPhww  
Rob3ssVYT/OP95PFjevCnSjfNvY59tsbjgSjtwb0VRghmztIRr2kpjJfT1CdF4soTJd4NK/  
1WtkKZqJ0O8Gs0jl0rH0UUBccNimLnXe0ndqN5U8urUYaCzr6jmkxgBF5M/+AvLPpZM  
QtdpRUF1bEc= ; key id = 53166
```

↓
amanoxsec.ch.

Aktivierung DNSSEC



amanox solutions

Manuelles Deployment und Management

- Generierendes KSK (Option -f KSK)

```
$dnssec-keygen -f KSK -n ZONE -a DSA -b 1024 sec.example.net Ksec.example.net.+003+16004
```

- Generiere ZSK

```
$dnssec-keygen -n ZONE -a RSASHA1 -b 512 sec.example.net  
Ksec.example.net.+005+57764
```

- Einfügen der Keys in die Zone

- Erhöhen der Seriennummer!

- Signieren + Neuladen

```
$dnssec-signzone -o sec.example.net zone.db zone.db.signed  
$rndc reload sec.example.net
```

- KSK in der trusted-key Section des Resolver eintragen!

- Einfügen eines Verweises auf den KSK in der Parentzone

```
dnssec-signzone
```

- Signieren der Parent Zone

```
$dnssec-signzone -g -o example.net zone.db zone.db.signed
```

- Periodisches Rollover! Und so weiter und sofort...

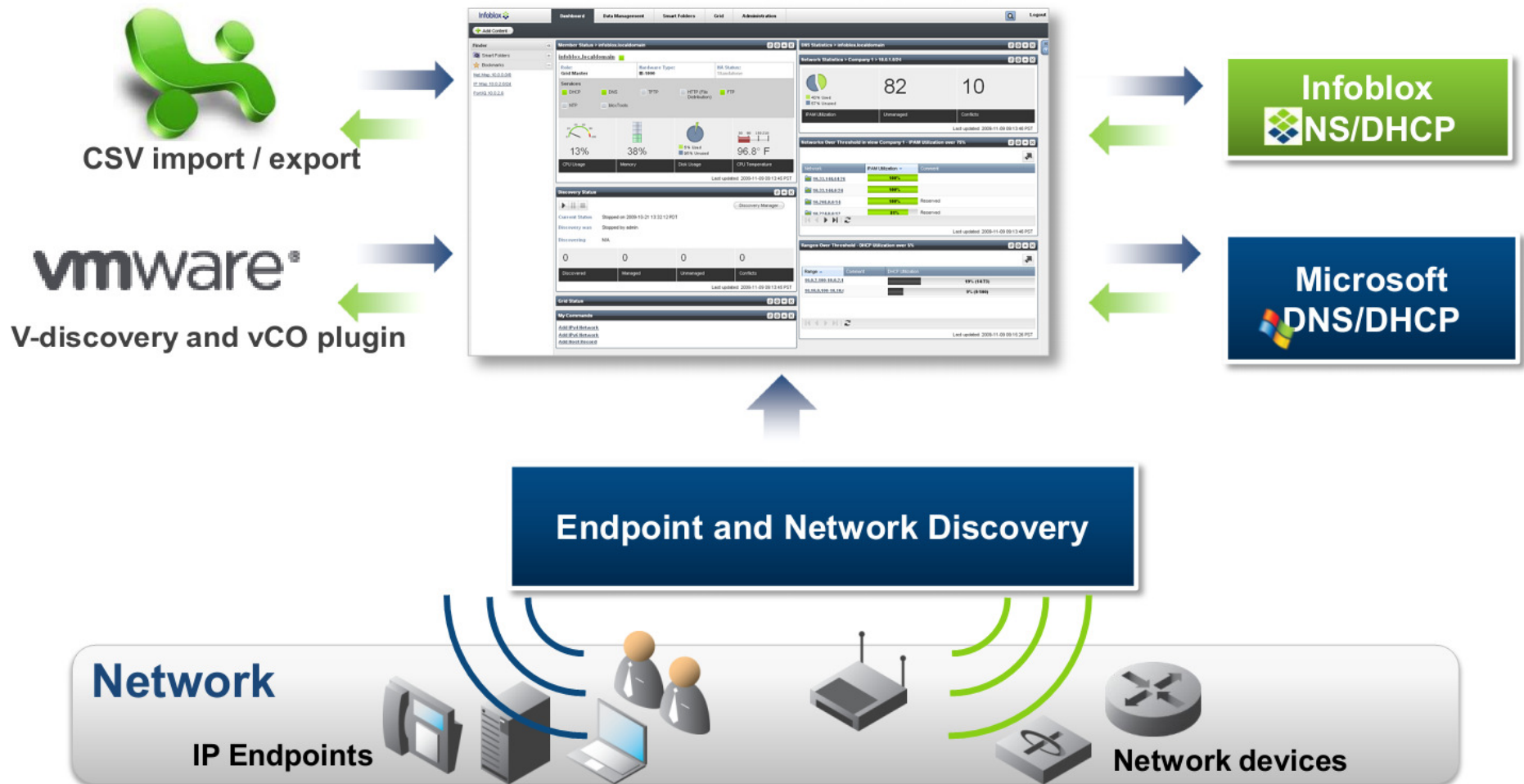


Übersicht DDI Lösungen



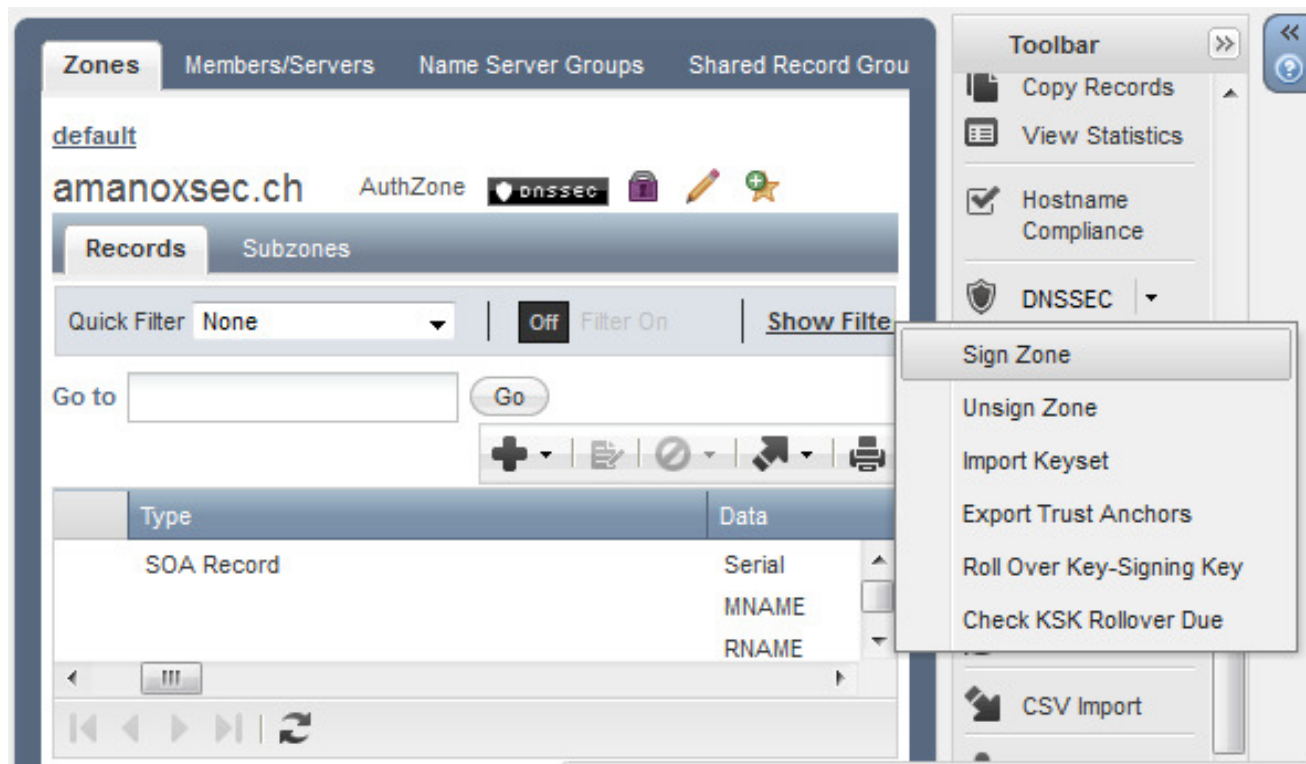
amanox solutions

Integrated Database, Single Point of Management



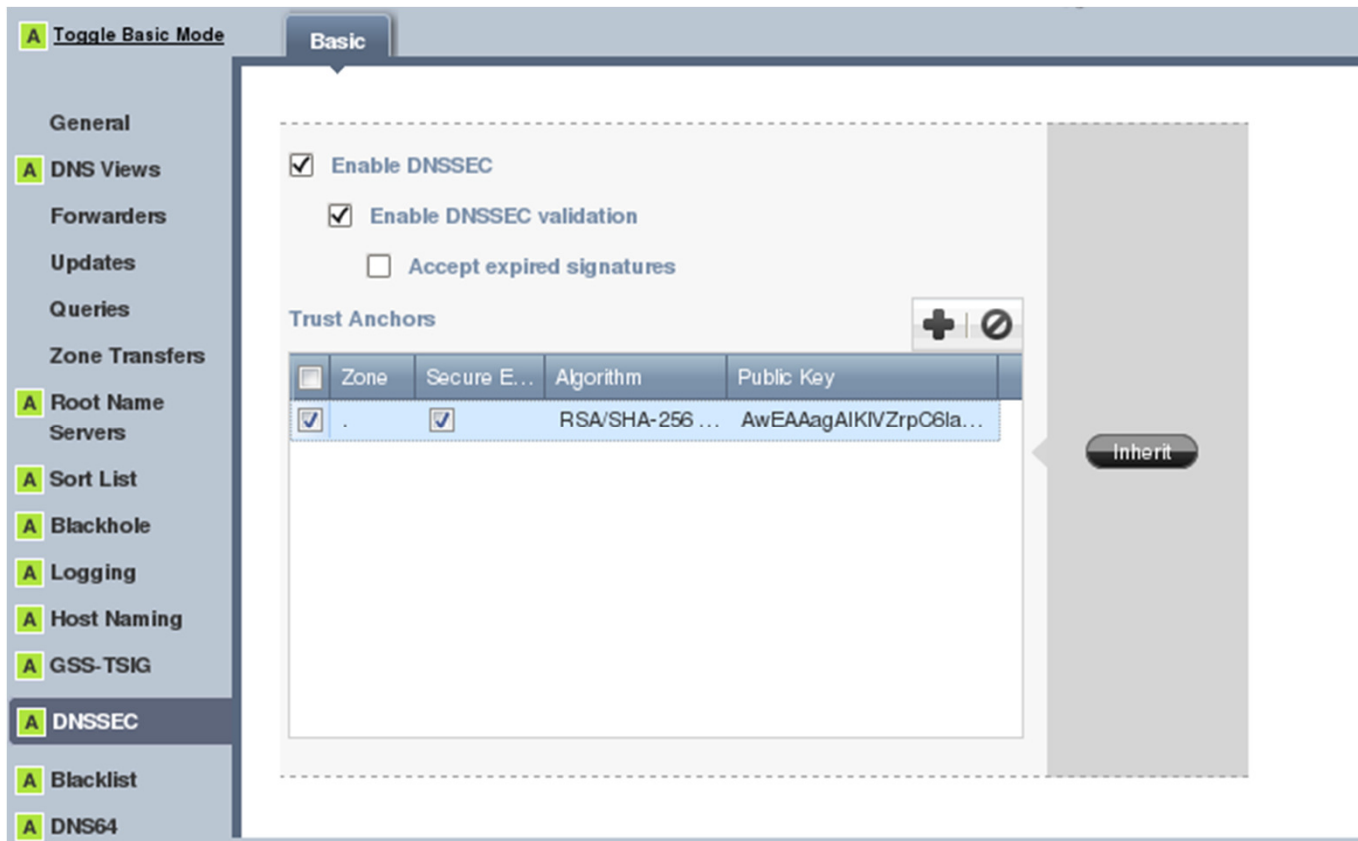
Aktivierung DNSSEC mit Infoblox

- Signieren einer DNS Zone



Aktivierung DNSSEC mit Infoblox

- Aktivieren von DNSSEC Validierung



The screenshot shows the 'Basic' configuration tab for DNSSEC. The 'Enable DNSSEC' checkbox is checked, and 'Enable DNSSEC validation' is also checked. The 'Accept expired signatures' checkbox is unchecked. Below these options is a 'Trust Anchors' table with a '+' and a '-' icon to its right. The table has four columns: 'Zone', 'Secure E...', 'Algorithm', and 'Public Key'. One row is visible, representing the root zone, with a checked checkbox in the 'Zone' column, a checked checkbox in the 'Secure E...' column, 'RSA/SHA-256 ...' in the 'Algorithm' column, and 'AwEAAgAIKIVZrpC6la...' in the 'Public Key' column. To the right of the table is a grey vertical bar with an 'Inherit' button.

<input type="checkbox"/>	Zone	Secure E...	Algorithm	Public Key
<input checked="" type="checkbox"/>	.	<input checked="" type="checkbox"/>	RSA/SHA-256 ...	AwEAAgAIKIVZrpC6la...

Tools, Tipps & Tricks



amanox solutions

- **Dig mit +dnssec Option**
Setzt das DNSSEC OK bit (DO)
- **Drill**
Vergleichbar mit dig, jedoch speziell für DNSSEC konzipiert. Sehr hilfreich für Nachvollziehbarkeit der Chain of Trust und Debugging
- <http://dnsviz.net/d/amanoxsec.ch/dnssec/>
Grafische Aufbereitung der DNSSEC Authentication Chain
- <http://dnssec-debugger.verisignlabs.com/amanoxsec.ch>
Analyse von DNSSEC Problemen
- <https://addons.mozilla.org/en-US/firefox/addon/dnssec-validator/>
DNSSEC Validator: Plugin für Firefox, welches URL verifiziert