

Active Directory Domain Services 2012 R2 -Grundkonfiguration - Teil 1

Active Directory Domain Services 2012 R2 -Grundkonfiguration - Teil 1

Inhalt

| Windows Server Vorbereitung | 2 |
|--|----|
| Netzwerkarte(n) konfigurieren für eine saubere Namensauflösung | 3 |
| Reverse-Lookupzone im DNS-Server einrichten | 4 |
| DNSSEC einrichten (Optional zu Testzwecken) | 7 |
| Vertrauensanker (Trustanchors) im Netzwerk verteilen | 14 |
| Mehr Sicherheit mit SocketPoolSize und CacheLockingPercent | 17 |
| Gruppenrichtlinie für DNSSEC aktivieren | 18 |
| Alterung der DNS Serverzonen einstellen | 20 |
| Active Directory Objekte vor versehentlichen löschen schützen | 23 |
| Zeitserver für den PDC Emulator konfigurieren | 24 |
| Active Directory – Standort und Dienste | 25 |

1



Windows Server Vorbereitung

Um dieses HowTo schreiben zu können, wurde das Ganze in einer Virtuellen Umgebung mit Oracle VM VirtualBox nachgestellt.

- → Microsoft Windows Server 2012 R2 (Deutsch)
- └→ Active Directory Domänendienste Server Rolle
- └→ DNS-Server Rolle



Netzwerkarte(n) konfigurieren für eine saubere Namensauflösung

Nach dem der erste Domänencontroller im Netzwerk installiert wurde, beginnen wir den Server sauber zu konfigurieren.



Wenn man nun zum ersten Mal eine CMD Konsole öffnet und den Befehl **nslookup** absetzt, seht ihr folgendes Ergebnis, das hat den Grund weil die Installation der Active Directory Server Rolle, die Loopback Adresse als Bevorzugten DNS-Server setzt, diese müssen wir anpassen.

| Eigenschaften von Internetprot | okoll Version 4 (TCP/IP 🗙 |
|--|--|
| Allgemein | |
| IP-Einstellungen können automatisch z Netzwerk diese Funktion unterstützt. V Netzwerkadministrator, um die geeigne | ugewiesen werden, wenn das Venden Sie sich andernfalls an den tten IP-Einstellungen zu beziehen. |
| O IP-Adresse automatisch beziehen | |
| Folgende IP-Adresse verwenden: | · |
| IP-Adresse: | 192 . 168 . 178 . 100 |
| Subnetzmaske: | 255 . 255 . 255 . 0 |
| Standardgateway: | 192 . 168 . 178 . 1 |
| O DNS-Serveradresse automatisch l | beziehen |
| Folgende DNS-Serveradressen ve | erwenden: |
| Bevorzugter DNS-Server: | 192 . 168 . 178 . 100 |

Hier setzen wir die Original Server IP-Adresse ein.

| Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6) | x |
|--|---|
| Allgemein | |
| IPv6-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IPv6-Einstellungen zu beziehen. | |
| IPv6-Adresse automatisch beziehen | |
| O Folgende IPv6-Adresse verwenden: | _ |
| IPv6-Adresse: | |
| Subnetzpräfixlänge: | |
| Standardgateway: | |
| DNS-Serveradresse automatisch beziehen O Folgende DNS-Serveradressen verwenden: | |
| Bevorzugter DNS-Server: | |

Im den Einstellungen der IPv6, setzen wir die Einstellung auf automatisch beziehen.



Reverse-Lookupzone im DNS-Server einrichten



Im nächsten Schritt richten wir auf den DNS-Server eine Reverse-Lookupzone ein, diese benötigen wir um IP-Adressen in Namen aufzulösen.

| Assistent zum Erstellen neuer Zonen |
|---|
| Active Directory-Zonenreplikationsbereich Sie können festlegen, wie DNS-Daten im Netzwerk repliziert werden. |
| Wie sollen Zonendaten repliziert werden? |
| Auf allen DNS-Servern, die auf Dom |
| Auf allen DNS-Servern, die auf Domänencontrollern in dieser Domäne ausgeführt werden: htdom.local |
| Auf allen Domänencontrollern in dieser Domäne (Windows 2000-Kompatibilität): htdom.local |
| Auf allen Domänencontroller, die im Bereich dieser Verzeichnispartition angegeben werden: |
| × |
| |
| |
| < Zurück Weiter > Abbrechen |

Diese Zone veröffentlichen wir für die komplette Domain.





Wir richten eine IPv4 Reverse-Lookupzone ein.

| Assistent zum Erstelle | n neuer Zonen 🛛 🗙 |
|---|---|
| Name der Reverse-Lookupzone Eine Reverse-Lookupzone übersetzt IP-Adresse | n in DNS-Namen. |
| Geben Sie die Netzwerk-ID oder den Namen der Netzwerk-ID: 192 .168 .178 . Die Netzwerk-ID ist der Teil der IP-Adresse, Netzwerk-ID in ihrer normalen Reihenfolge (Wenn Sie eine Null in der Netzwerk-ID verw angezeigt. Beispiel: Netzwerk-ID 10 erstellt 10.0 erstellt Zone 0.10.in-addr.arpa. Name der Reverse-Lookupzone: 178.168.192.in-addr.arpa | Reverse-Lookupzone an. der dieser Zone angehört. Geben Sie die nicht umgekehrt) ein. enden, wird diese im Zonennamen Zone 10.in-addr.arpa und Netzwerk-ID |
| | < Zurück Weiter > Abbrechen |

Geben unser Subnetzdaten an.



| Assistent zum Erstellen neuer Zonen |
|---|
| Dynamisches Update Sie können festlegen, dass diese DNS-Zone sichere, unsichere oder keine dynamische Updates zulässt. |
| Dynamische Updates ermöglichen DNS-Clientcomputern, sich zu registrieren und die eigenen Ressourceneinträge dynamisch mit einem DNS-Server bei Änderungen zu aktualisieren. |
| Bestimmen Sie den Typ des dynamischen Updates, der verwendet werden soll. |
| Nur sichere dynamische Updates zulassen (für Active Directory empfohlen) Diese Option ist nur für Active Directory-integrierte Zonen verfügbar. |
| Nicht sichere und sichere dynamische Updates zulassen Dynamische Updates von Ressourceneinträgen werden von allen Clients zugelassen. Durch diese Option besteht ein hohes Sicherheitsrisiko, da Updates von nicht vertrauenswürdigen Quellen angenommen werden können. |
| Dynamische Updates nicht zulassen Dynamische Updates von Ressourceneinträgen werden von dieser Zone nicht zugelassen. Diese Einträge müssen manuell aktualisiert werden. |
| < Zurück Weiter > Abbrechen |

Wählen nur sichere dynamische Updates zulassen aus.

| 1 | | | | |
|---|---------------------------------------|--------------------------|---------------------------|--------------------------------------|
| å | | | DNS-Manager | |
| Datei Aktion Ansicht ? | | | | |
| 🗢 🔿 🖄 📰 🖾 🖬 🖬 🖬 | 80 | | | |
| 👗 DNS | Name | Тур | Daten | Zeitstempel |
| ⊿ | (identisch mit übergeordnetem Ordner) | Autoritätsursprung (SOA) | [3], ads01.htdom.local., | Static |
| ⊿ 🧮 Forward-Lookupzonen | (identisch mit übergeordnetem Ordner) | Namenserver (NS) | ads01.htdom.local. | Static |
| Image: Second | 192.168.178.100 | Zeiger (PTR) | ads01.htdom.local. | 05.06.2016 11:00:00 |
| ⊿ [htdom.local | | | | |
| Imsdcs | | | | |
| isites | <u>an</u> | | Administr | ator: Eingabeaufforderung |
| ▶ 2 _tcp | Microsoft Windows [Version 6.3.9 | 600] | | |
| ⊳ 🔛 _udp | (c) 2013 Microsoft Corporation. | Alle Rechte vorbehalt | | |
| DomainDnsZones | C:\Users\Administrator>inconfig | | | |
| ForestDnsZones | er (oser s (naminiser deor vipconnig, | | | |
| ⊿ 🧾 Reverse-Lookupzonen | Windows-IP-Konfiguration | | | |
| 178.168.192.in-addr.arpa | | | | |
| ⊳ 🜍 0.in-addr.arpa | Die Kegischierung der DWS-Ressou | rcenerninage fun arre | Adapter dieses computer i | wurde inicialisiert. Fehler werden i |
| 127.in-addr.arpa | C:\Users\Administrator>_ | | | |
| 255.in-addr.arpa | | | | |
| | | | | |

Nach dem die Reverse-Lookupzone eingerichtet wurde, setzen wir den Befehl *ipconfig /registerdns* ab, um den Domaincontroller selbst in der Reverse-Lookupzone zu registrieren.



Nun können wir per **nslookup** alle Kombinationen (Computername, IP-Adresse, Domainname) testet. Wenn wir hier überall ein sauberes Ergebnis zurückbekommen, funktioniert die Namensauflösung einwandfrei.



DNSSEC einrichten (Optional zu Testzwecken)

Zu Testzwecken habe ich mal auf den DNS-Server alle Primären Zonen per DNSSec signiert. Wikipedia und Microsoft schreiben folgendes zu DNSSec.

https://de.wikipedia.org/wiki/Domain_Name_System_Security_Extensions https://technet.microsoft.com/de-de/library/dn593694(v=ws.11).aspx https://technet.microsoft.com/de-de/library/hh831411(v=ws.11).aspx

"DNSSEC verwendet ein asymmetrisches Kryptosystem. Der "Besitzer" einer Information – in der Regel der Master-Server, auf dem die abzusichernde Zone liegt – unterzeichnet jeden einzelnen Record mittels seines geheimen Schlüssels (engl. private key). DNS-Clients können diese Unterschrift mit dem öffentlichen Schlüssel (engl. public key) des Besitzers validieren und damit Authentizität und Integrität überprüfen."

Da ich in der Vergangenheit vieles darüber gelesen habe, wollte ich es mal ausprobieren und mit ein paar Screenshots dokumentieren. Nun muss ich für mich selbst noch herausfinden wieviel mehrnutzen das Ganze hat.



Um nun die Zone zu signieren, klickt man auf den Domaineintrag und wählt im Kontextmenü – **DNSSEC – Zone signieren**.

| Zonensignatur-Assistent X |
|--|
| Signierungsoptionen Vom DNS-Server werden drei Signierungsoptionen unterstützt. |
| Wählen Sie eine der Optionen für die Zonensignierung aus: |
| • Zonensignaturparameter anpassen |
| Signiert die Zone mit einem neuen Satz von Zonensignaturparametern. |
| O Zone mit den Parametern einer vorhandenen Zone signieren |
| Signiert die Zone unter Verwendung der Parameter einer vorhandenen Zone. |
| Zonenname; |
| 🔿 Standardeinstellungen für die Zonensignierung verwenden |
| Signiert die Zone unter Verwendung der Standardparameter. |
| |
| |
| < Zurück Weiter > Abbrechen |

Da es der erste Versuch ist, möchte ich gerne die Zonensignaturparameter manuell anpassen.

| Zonensignatur-Assistent | x |
|---|--------|
| Schlüsselmaster Wählen Sie den Schlüsselmaster für diese Zone aus. | |
| Der Schlüsselmaster ist ein DNS-Server, von dem kryptografische Schlüssel für eine mittels DNSSEC geschützte Zone generiert und verwaltet werden. Jeder autoritative DNS-Server, von dem eine primäre Kopie der Zone gehostet wird, kann als Schlüsselmaster fungieren. | |
| Standardmäßig wird der aktuelle DNS-Server als Schlüsselmaster festgelegt. Es kann jedoch auch ein anderer DNS-Server als Schlüsselmaster für diese Zone angegeben werden. | |
| • Der DNS-Server "ADS01" fungiert als Schlüsselmaster. | |
| O Wählen Sie einen anderen primären Server als Schlüsselmaster aus: | ~ |
| | |
| < Zurück Weiter > Abbr | rechen |

Mein erster Domaincontroller/DNS-Server ist natürlich auch der Schlüsselmaster.

| Zonensignatur-Assistent X |
|---|
| Schlüsselsignaturschlüssel (Key Signing Key, KSK) Bei einem KSK handelt es sich um einen Authentifizierungsschlüssel zum Signieren anderer Schlüssel. |
| Der Schlüsselsignaturschlüssel (KSK) entspricht einem privaten Schlüssel zum Signieren von mindestens einem anderen Signaturschlüssel. Üblicherweise werden mit dem privaten Schlüssel, der einem KSK entspricht, andere Schlüssel zur Zonensignatur signiert. Ein KSK verfügt unter Umständen über eine längere Gültigkeitsdauer, um einen stabileren Sicherheitseinstiegspunkt in die Zone bereitzustellen. Der öffentliche Schlüssel eines KSK wird als Vertrauensanker zum Überprüfen der DNS-Antworten verwendet. |
| Klicken Sie auf "Weiter", um die Schlüsselsignaturschlüssel zu konfigurieren. |
| Diese Seite nicht mehr anzeigen |
| Weitere Informationen zum Schlüsselsignaturschlüssel (KSK) |
| < Zurück Weiter > Abbrechen |

Im nächsten Schritt erstellen wir den *Key Signing Key, KSK*, dieser private KSK Schlüssel wird benötigt um den spätere privaten *Zone Signing Keys (ZSK)* zu signieren.

https://technet.microsoft.com/de-de/library/dn593682(v=ws.11).aspx

| | | | Zonensigna | atur-Assistent | t | x |
|-----|--|--------------------------------------|--|---------------------------------------|------------------------|-----------------|
| Sch | l üsselsignatu KSKs konfigurie | r schlüssel (Ke eren | y Signing Key, K | (SK) | | |
| | Konfigurieren S Kryptografiealg | ie Parameter für jorithmen könner | mindestens einen n maximal drei KSK | KSK. Für jeden de s angegeben werd | er verfügbaren den. | |
| | Algorithmus | Schlüssellä | KSP | Replikation | Rolloverzus | Anfänglicher Ro |
| | < | | ш | | 1 | > |
| | Hinzufügen | Bearbeiten | Entfernen | | | |
| | | | | < Z0 | u rück Weiter | > Abbrechen |

Hier klicken wir auf Hinzufügen.

| GUID: | Γ | {0000000-0000-0000-000000000000}} | | |
|---|--|-----------------------------------|-------------------------------|----------|
| hlüsselgenerierung | L | | | |
| Neue Signaturschlüs | sel generieren | | | |
| O Vorab generierte So | - hlüssel verwender | 1 | | |
| Diesen Schlüssel | als aktiven Schlüss | el verwenden: | | |
| Diesen Schlüssel | als Standbyschlüss | el verwenden: | | |
| hillionada in an an ha Onar | | | | |
| niusseieigenschaften | | | | |
| Schlüssellänge (in Bits) | s: | | R5A/5HA-250 | ¥ |
| Wählen Sie einen Schlü | sselspeicheranbiet | er zum | Microsoft Software Key Storag | e Prov 🗸 |
| Generieren und Speiche | ern von Schlüsseln r für DNSKEY-RRs | aus: et (in Stunden): | 168 | ^ |
| ☑ Diesen privaten Sch (gilt nur für AD-integ | lüssel an alle autor rierte Zonen) | ritativen DNS-Server fü | diese Zone replizieren | |
| hlüssel-Rollover | | | | |
| Automatischen Roll | over aktivieren | | 1460 | * |
| Rolloverhäufigkeit | : (in Tagen): | | 0 | * |
| | erzögern um (in Ta | den). | | |

Bei den Schlüsseleigenschaften wählen wir für den Kryptografiealgorithmus mindestens **RSA/SHA 256** aus, seit dem 31. Dezember 2015 werden von allen Organisationen empfohlen den SHA-1-Hashalgorithmus durch den SHA-2 zu ersetzen, der SHA-1-Hashalgorithmus wird für ungültig erklärt.

Der **DNSSEC Good Practices Guide** schlägt bei der Schlüssellänge eine Bittiefe von 1280 Bit und maximal 4 Jahre Lebensdauer vor.

Good Practices Guide for Deploying DNSSEC

Der Automatische Rollover sollte aktiviert werden, damit der KSK Schlüssel in Regelmäßigen Abständen erneuert wird, in diesem Beispiel können wir den Standard von 755 Tagen belassen oder wir wählen nach Best Practices die vorgeschlagenen 4 Jahre.

Hier zwei Webseiten die das Thema Schlüssel Rollover beschreiben

https://securityblog.switch.ch/2013/02/05/algorithm-rollover/

http://www.heise.de/netze/meldung/DNSSEC-Verfahren-fuer-Schluesseltausch-in-der-Rootzonefestgelegt-3208629.html

| | Zonensignatur-Assistent X | | | | | | | |
|--------------------------|---|------------------------------------|--|------------------------------------|-------------------|-----------------|--|--|
| Schlüsse KSKs | Schlüsselsignaturschlüssel (Key Signing Key, KSK) KSKs konfigurieren | | | | | | | |
| Konfi <u>c</u> Krypte | jurieren Si ografiealgo | e Parameter für orithmen könner | mindestens einen KS maximal drei KSKs a | K. Für jeden der ngegeben werde | verfügbaren m. | | | |
| Algo | rithmus | Schlüssellä | KSP | Replikation | Rolloverzus | Anfänglicher Ro | | |
| RSA | /SHA-256 | 1280 | Microsoft Softw | Aktiviert | Aktiviert | 0 | | |
| < | | | III | | | > | | |
| Hinz | rufügen | Bearbeiten | Entfernen | | | | | |
| | | | | < Zur | ück Weiter | > Abbrechen | | |

Nachdem der KSK Schlüssel erstellt wurde, klicken wir auf weiter um den Zone Signing Key zu erstellen.

| Zonensignatur-Assistent 🗙 |
|---|
| Zonensignaturschlüssel (Zone Signing Key, ZSK) Bei einem ZSK handelt es sich um einen Authentifizierungsschlüssel zum Signieren der Zonendaten. |
| Der Zonensignaturschlüssel (ZSK) ist ein Authentifizierungsschlüssel, der einem privaten Schlüssel zum Signieren von Zonendaten entspricht. Üblicherweise werden ZSKs häufiger zurückgesetzt als Schlüsselsignaturschlüssel (KSKs). |
| Klicken Sie auf "Weiter", um die Zonensignaturschlüssel zu konfigurieren. |
| Diese Seite nicht mehr anzeigen |
| Weitere Informationen zum Zonensignaturschlüssel (ZSK) |
| < Zurück Weiter > Abbrechen |

Hier klicken wir ebenfalls auf Weiter, um den Zone Signing Key (ZSK) zu erstellen.

| | Zonensignatur-Assistent × | | | | | | |
|-----|--|-------------------------------------|--|------------------------------------|-------------------|----------------|--|
| Zon | Zonensignaturschlüssel (Zone Signing Key, ZSK) ZSKs konfigurieren | | | | | | |
| | Konfigurieren S Kryptografiealg | ie Parameter für orithmen können | mindestens einen ZS maximal drei ZSKs a | K. Für jeden der ngegeben werde | verfügbaren n. | | |
| | Algorithmus | Schlüssellä | KSP | Rolloverzus | Anfänglicher Ro | Rolloverhäufig | |
| | < | | | | | > | |
| | Hinzufügen | Bearbeiten | Entfernen | | | | |
| | | | | < Zur | ück Weiter > | Abbrechen | |

Wir klicken auf Hinzufügen.

| Neuer Zonensigna | turschlüssel (Zone | Signing Key, ZSK) | x |
|---|----------------------|---|----------|
| GUID | | | |
| GUID: | {00000000-0000-0000- | 0000-0000000000000000000000000000000000 | |
| Schlüsseleigenschaften | | | _ |
| Kryptografiealgorithmus: | | RSA/SHA-256 | ~ |
| Schlüssellänge (in Bits): | | 1024 | ~ |
| Wählen Sie einen Schlüsselspeicheranbie Generieren und Speichern von Schlüssel | ter zum n aus: | Microsoft Software Key Storage Prov | ~ |
| Signaturgültigkeitsdauer für DNSKEY (in | Stunden): | 168 | * * |
| Signaturgültigkeitsdauer für DS (in Stund | len): | 168 | ^ ~ |
| Gültigkeitsdauer für Zoneneintrag (in St. | inden): | 240 | * * |
| Schlüssel-Rollover | | | |
| Automatischen Rollover aktivieren | | | ~ |
| Rolloverhäufigkeit (in Tagen): | | 365 | v |
| Ersten Rollover verzögern um (in T | agen): | 0 | ~ |
| | OK Abbr | echen | |

In diesem Wizard wählen wir ebenfalls den Kryptografiealgorithmus **RSA/SHA 256** aus mit einen Schlüssellänge von 1024 Bit.

Der Schlüssel Rollover sollte einmal im Jahr stattfinden.

Die Schlüssellänge die wir hier konfigurieren, beeinflusst das zu sendende UDP-Packet, dies darf derzeit die Größe von 512 Byte nicht überschreiten. Umso Größer also die Schlüssellänge, umso größer die Datenmenge die das UDP-Packet senden muss.

| Zonensignatur-Assistent | : |
|--|---|
| Next Secure (NSEC) NSEC- und NSEC3-Ressourceneinträge ermöglichen eine authentifizierte Bestätigung der Abwesenheit. | 1 |
| Wählen Sie "NSEC" oder "NSEC3" für authentifizierte Abwesenheit. NSEC3 verwenden Iterationen: | |
| < Zurück Weiter > Abbrechen | |

NSEC wird benötigt, um nicht-vorhandene DNS Einträge zu beweisen.

https://de.wikipedia.org/wiki/NSEC_Resource_Record

| Zonensignatur-Assistent X |
|---|
| Vertrauensanker (Trust Anchors, TAs) Konfigurieren Sie die Verteilung von Vertrauensankern und Rolloverschlüsseln. |
| ✓ Verteilung von Vertrauensankern für diese Zone aktivieren Ist dieser DNS-Server auch ein Domänencontroller, werden Vertrauensanker für diese Zone an alle anderen DNS-Server verteilt, die auf Domänencontrollern in der Gesamtstruktur ausgeführt werden. Ist dieser DNS-Server kein Domänencontroller, wird ein Vertrauensanker für diese Zone nur dem lokalen Vertrauensankerspeicher hinzugefügt. Die Auswahl dieser Option aktiviert die DNSSEC-Überprüfung für diese Zone auf allen Servern, an die Vertrauensanker verteilt werden. |
| < Zurück Weiter > Abbrechen |

Um das Ganze abzuschließen, klicke ich den Wizard durch.



Vertrauensanker (Trustanchors) im Netzwerk verteilen

Um den Vertrauensanker im Netzwerk verteilen zu können, muss das Verzeichnis *C:\Windows\System32\dns* im Netzwerk freigegeben werden.



Die Freigabeberechtigungen ändere ich wie folgt, die Benutzergruppe Jeder wird gelöscht.

| L | Eigenschaften von dns |
|---|--|
| | Envoitorto Eroigobo X |
| | 🕨 Berechtigungen für "dns" 🛛 🗙 |
| | Freigabeberechtigungen |
| | Gruppen- oder Benutzemamen: |
| | & Authentifizierte Benutzer |
| | |
| | |
| | |
| | |
| | Hinzufügen Entfemen |
| | Berechtigungen für "Authentifizierte Benutzer" Zulassen Verweigem |
| | Vollzugriff |
| | Ändem 🗌 🗌 |
| | Lesen 🗹 🗌 |

Und dafür füge ich die Authentifizierten Benutzer mit "Lesen" Recht hinzu.



Danach öffne ich die DNS Management Konsole und navigiere zu den Punkt "Vertrauenspunkte"

| å. | | | | | | |
|------------------------|---------------|-----------------------------|----|--------|------------|-----|
| Datei Aktion Ansicht ? | | | | | | |
| 🗢 🄿 🙍 🖬 🖉 | | | | | | |
| 🚊 DNS | | Name | | | Status | |
| ⊿ 🚆 ADS01 | | 🚞 local | | | Initialisi | ert |
| Zwischengespeichert | e Lookupvorgä | | | | | |
| ⊿ | en 🛛 | | | | | |
| msdcs.htdom.log | cal | | | | | |
| htdom.local | | | | | | |
| Reverse-Lookupzone | n | | | | | |
| ⊿ 📔 Vertrauenspunkte | | | | 1 | | |
| 🔺 🧮 local | Hinzufügen | | ٠. | | | |
| 📔 htdom | Importieren | | + | DNSKEY | | |
| Bedingte Weiterle | Aktive Aktua | ktualisierung initiieren DS | | | | |
| | Ansicht | | ۲ | | | |

Dort Importiere ich einen neuen DNSKEY.

| DNS △ ADS01 ▷ Zwische △ Forward ▷ _ ms ▷ ♠ htdd ▷ Reverse △ Vertraut △ loca | ngespeicherte Lookupvorga DNSKEY i Zu importierende Datei | lame local mportieren Durchsuchen | Status Initialisiert | Туре | Algorithm | us Gültig |
|---|--|--|---|--|--|-------------------------------------|
| i i i I i i i i i i i i i i i i i i i i | Å ⓒ ⓒ ✓ ↑ 💽 №a Organisieren → Neur | DNSKEY ir | nportieren | ✓ Ċ "dns | " durchsuchen 8ु☷ ▼ | × م |
| | ★ Favoriten ■ Desktop ▶ Downloads >> Zuletzt besucht remote Computer Netzwerk | Name backup samples CACHE.DNS dns.log dsset-178.168.192.in-addr.arpa set-htdom.local keyset-178.168.192.in-addr.arpa | Ä 1! 2! 1! 0! 1! 0! 1! | nderungsdatum 9.06.2016 11:39 5.05.2016 17:24 9.06.2016 17:24 9.06.2016 11:39 5.06.2016 13:55 9.06.2016 14:13 5.06.2016 14:13 | Typ Dateiordner DNS-Datei Textdokument ARPA-Datei LOCAL-Datei LOCAL-Datei LOCAL-Datei | Größe 4 0 1 1 2 2 |

Wir klicken auf Durchsuchen, in der Adresszeile wählen wir den UNC Pfad zu der eben erstellen DNS Freigabe und dort wähle wir die passende *keyset* Datei aus.

\\ads01\dns\keyset-htdom.local

Nun sollte man in der Ordnerstruktur seine DNSKEYs finden.

| å. | | | DNS-Manager | | |
|----------------------------------|---|--------|------------------|-------------|---------------------|
| Datei Aktion Ansicht ? | | | | | |
| 🗢 🄿 🙇 🖬 🗙 🖬 🍳 🕞 🚺 🖬 | | | | | |
| 🛔 DNS | Name | Status | Туре | Algorithmus | Gültig ab |
| ⊿ | 📒 (identisch mit übergeordnetem Ordner) | Gültig | DNS KEY (DNSKEY) | RSA/SHA-256 | 19.06.2016 15:15:00 |
| Zwischengespeicherte Lookupvorgä | 📒 (identisch mit übergeordnetem Ordner) | Gültig | DNS KEY (DNSKEY) | RSA/SHA-256 | 19.06.2016 15:15:00 |
| ⊿ I Forward-Lookupzonen | | | | | |
| Imsdcs.htdom.local | | | | | |
| htdom.local | | | | | |
| Reverse-Lookupzonen | | | | | |
| ⊿ 🚞 Vertrauenspunkte | | | | | |
| ⊿ 🚞 local | | | | | |
| 📔 htdom | | | | | |
| | 1 | | | | |
| | | | | | |



Um das Ganze nun testen zu können, öffnen wir eine PowerShell Sitzung und können mit folgenden Befehlen den DNS Server auf DNSSEC überprüfen.

| Σ | | | | HTD | OM - Powers | hell | _ _ × |
|--|------------------|-----------------------------|------------|--------------------|--|---|--------------|
| HTDOM D:\PowershellScripte> Resolve-DnsName -N | ame ht | dom.local | -Server a | ds01 -Dns: | sec0k | | ^ |
| Name | Туре | TTL S | ection | IPAddress | | | |
| htdom.local | A | 600 A | nswer | 192.168.1 | 78.100 | | |
| Name : htdom.local QueryType : RBSIG TTL : 600 Section : Answer TypeCovered : A Algorithm : 8 LabelCount : 2 OriginalTtl : 600 Expination : 29,06.2016 12:13:01 Signed : 19.06.2016 11:13:01 Signer : htdom.local Signer : {133, 204, 217, 12} Name : . QueryType : OPT TTL : 32768 Section : Additional Data : {} | | | | | | | |
| HTDOM D:\PowershellScripte> Resolve-DnsName -N | ame ht | dom.local | .trustanch | ors -Type | DNSKEY -Serv | er ads01 | |
| Name Type | TTL | Section | Flags | Protocol | Algorithm | Key | |
| htdom.local.trustanchors DNSKE htdom.local.trustanchors DNSKE | Y 3600 Y 3600 | Answer Answer | 257 257 | DNSSEC DNSSEC | 8 8 | {3, 1, 0, 1} {3, 1, 0, 1} | |
| HTDOM D:\PowershellScripte> Get-DnsServerTrust | Anchor | -Name ht | dom.local | | | | |
| TrustAnchorName TrustAnchorType | | TrustAnch | orState | TrustAnd | chorData | | |
| htdom.local. DNSKEY htdom.local. DNSKEY HTDOM D:\PowershellScripte> Get-DnsServerResou | rceRec | Valid Valid ord -Zone | Name htdom | [29657] [11540] | [DnsSec][RsaS [DnsSec][RsaS RType DnsKey | ha256][AwEAAelcwejG06HytUdg ha256][AwEAAef/BuuFECT/WTxK -ComputerName ads01 | ~ |

- └→ Resolve-DnsName -Name htdom.local -Server ads01 -DnssecOk
- └→ Resolve-DnsName -Name htdom.local.trustanchors -Type DNSKEY -Server ads01
- └→ Get-DnsServerTrustAnchor -Name htdom.local
- Get-DnsServerResourceRecord -ZoneName htdom.local -RRType DnsKey -ComputerName ads01
- └→ Get-DnsClientNrptPolicy
- → Resolve-DnsName -Name htdom.local -Type SOA -Server ads01 -DnssecOk
- → Resolve-DnsName -Name htdom.local -Type DNSKEY -Server ads01 –DnssecOk



Mehr Sicherheit mit SocketPoolSize und CacheLockingPercent

Um noch ein bisschen mehr Sicherheit in die DNS Konfiguration zu bringen, verändern wir zwei Standardwerte in der DNS Einstellungen.

Nach der Grundinstallation eines DNS Servers ist die SocketPoolSize Standardmäßig auf einen Wert von 2500. Dies hat anscheinend in der Vergangenheit dazu geführt das DNS Spoofing Attacken stattfanden, weil Anwendungen und Dienste den gleichen Socketpool benutzten.

Folgender Microsoft Artikel beschreibt das Sicherheitsproblem

- → dnscmd /info /socketpoolsize (2500)
- → dnscmd /config /socketpoolsize 4000

Mit folgendem Befehl kann man sehen wie viele offene UDP Ports auf einen Server mit installierter DNS Server Rolle sind.

netstat –anb

| | | HTDOM - Powershell |
|---|-------|--------------------|
| [dns.exe] UDP 0.0.0.0:55830 [dns.exe] | | |
| UDP 0.0.0.0:55831 [dns.exe] | | |
| UDP 0.0.0.0:55832 [dns.exe] | | |
| UDP 0.0.0.0:55833 [dns.exe] | | |
| UDP 0.0.0.0:55834 [dns.exe] | | |
| UDP 0.0.0.0:55835 [dns.exe] | | |
| UDP 0.0.0.0:55836 [dns.exe] | | |
| UDP 0.0.0.0:55837 [dns.exe] | | |
| UDP 0.0.0.0:55838 [dns.exe] | | |
| UDP 0.0.0.0:55839 [dns.exe] | | |
| UDP 0.0.0.0:55840 [dns.exe] | | |
| UDP 0 0 0 0.55841 | * • * | |

Um auszurechnen um wie viel genau es sich handelt, kann man folgendes Statement absetzen.

- → \$DNSProcess = Get-Process DNS
- → netstat -ano -P UDP | Select-String \$DNSProcess.Id | Select-String "0.0.0.0:" | Measure-Object

| Σ | | | | | | | HTDOM - Powershell | |
|----------|----------|------------|------------|--------|-----------|-----------------|--|---|
| [HTDOM | D:\Power | shellScrip | te> \$DNSP | rocess | | | | |
| Handles | NPM(K) | PM(K) | WS(K) | VM(M) | CPU(s) | Id Process | Name | |
| 16308 | 11821 | 150292 | 148656 | 197 | 0,70 | 1372 dns | | |
| | | | | | | | | |
| HTDOM D: | \Powersh | ellScripte | > netstat | -ano - | P UDP S | elect-String \$ | DNSProcess.Id Select-String "0.0.0.0:" Measure-Objec | t |
| Count | : 4001 | | | | | | | |
| Average | | | | | | | | |
| Sum | | | | | | | | |
| Maximum | | | | | | | | |
| Minimum | | | | | | | | |
| Property | - | | | | | | | |

Quelle: http://www.foxguardsolutions.com/resources/details/a-closer-look-at-windows-dns-ports



Die zweite Einstellung ist der CacheLockingPercent, diese überschreibt einen gecachden Eintrag wenn die TTL (Time to Life) zu 100% erreicht ist, Best Practice sagt, wir sollen einen Wert von 90 % setzen.

- └→ dnscmd /info /cachelockingpercent (100)
- └→ dnscmd /config /cachelockingpercent 90

oder

- └→ (Get-DnsServerCache).LockingPercent
- └→ Set-DnsServerCache -LockingPercent 90

Gruppenrichtlinie für DNSSEC aktivieren

| E . | | Gruppenrichtlinie | nverwaltung |
|---|--|--|---|
| 📓 Datei Aktion Ansicht Fenster ? | | | |
| 🗢 🔿 🚾 🗙 🖬 📓 🖬 | | | |
| Croupentichtlinienerveitung Croupentichtlinienerveitung Croupentichtlinienerveitung Croupentichtlinienebigkte Domain Cortollers Domain Cortollers Domain Cortollers Computerkond Starter-Groupentichtlinienobigkte Starter-Groupentichtlinienobigkte Computerkond | sicht ? Clicy (ADS01.HTDOM.LOCAL) Far Gyration reeinstellungen vs-Einstellungen pts (Start/Heuntefahren) httinenbasierter QoS stative Vorlagen: Vom lokaler en guration guration gen | G menselfisurgeschtline benicht in der Richtlerstabel für ür Securly und DireckCoses Richtline ist das Geschly und DireckCoses Southy und DireckCoses Geschly und DireckGose Geschl | In Page Provide Server Verwenden In Starten Poly Table. NPPT) worden de Konfguzetionseinstellungen für DNSSEC (DNS af DNS Claristom Verwenden Verschlussen verwenden verden können. ISSEC myssellen Grünzer verwenden verden können im Verschlusselungs verwenden verden können. ISSEC DNS-Einstellungen für DirectAccess. Allgemeiner DNS Server Coderung INSSEC: DNS-Einstellungen für DirectAccess. Allgemeiner DNS Server Coderung INSSEC: DNS-Einstellungen für DirectAccess. Allgemeiner DNS Server Verwenden Verschlüsselungstp:::::::::::::::::::::::::::::::::::: |

Mit der Richtlinie "*Name Resolution Policy Table, NRPT*" wird die Namensauflösung mit DNSSEC Überprüfung erforderlich gemacht.

Entweder wir erstellen eine komplett neue Gruppenrichtlinie oder ändern die Default Domain Policy,

Da es hier eine Testdomain ist ändere ich die **Default Domain Policy**, in einer Live Umgebung würde ich hier eine eigene Server Policy anlegen und mit der Domain verknüpfen.



Auch hier bitte aufpassen beim Konfigurieren der Einstellung, hier muss ganz nach unten gescrollt werden, damit die Einstellung auch angewandt werden.

| | | | | | | - | | | | |
|-----------------|-------------|--------------|--------|----------|----------|----------|--------------|---------------------------------|------------------------|----------------------|
| Richtlinientabe | lle für die | Namensauflör | 8100 | | | | Aktualisiere | en Erstelle veiterte globale | en Lö Richtlinienei | schen nstellungen |
| Namespace | Zerti | DNSSE | DNSSEC | DNSSEC (| DirectAc | DirectAc | DirectAc | DirectAc | DNS-Se | Codierung |
| nuomioca | | 00 | INCIT | | | | | | | |
| | | | | | | | | | | |

| Gesamtstruktur: htdom.local | ereich Details Einstellungen Delegierung | | | | | | | |
|--|---|--|--|------------------------|--|--|--|--|
| ⊿ ji htdom.local | Lokale Richtlinien/Sicherheitsopti | onen | | | | | | |
| J Default Domain Policy | Netzwerksicherheit | Netzwerksicherheit | | | | | | |
| Gruppenrichtlinienobjekte | Richtlinie | | Einstellung | | | | | |
| b i WMI-Filter b i Starter-Gruppenrichtlinienobjekte | Netzwerksicherheit: Abmeldung nac Netzwerksicherheit: Keine LAN Mar | h Ablauf der Anmeldezeit erzwingen ager-Hashwerte für nächste Kennwortänderung speichem | Deaktiviert Aktiviert | | | | | |
| 🙀 Standorte | Netzwerkzugriff | | | | | | | |
| Gruppenrichtlinienmodellierung | Richtlinie | | Einstellung | | | | | |
| Couppendentinenergeonisse | Netzwerkzugriff: Anonyme SID-/Nar | mensübersetzung zulassen | Deaktiviert | | | | | |
| | Richtlinien öffentlicher Schlüssel/ | Verschlüsselndes Dateisystem | | | | | | |
| | Zertifikate | | | | | | | |
| | Ausgestellt für | Ausgestellt von | Ablaufdatum | Beabsichtigte Zwecke | | | | |
| | Administrator | Administrator | 01.05.2116 17:33:30 | Dateiwiederherstellung | | | | |
| | Regeleinstellungen | | | | | | | |
| | Namespace | | | | | | | |
| | .htdom.local | | | | | | | |
| | Richtlinie | | Wert | | | | | |
| | Namespace | | .htdom.local | | | | | |
| | Zertifizierungsstelle | | Leer | | | | | |
| | Konfiguration | | DNSSEC | | | | | |
| | DNSSEC (Uberprutung) | | Ja | | | | | |
| | DNSSEC (IPsec) | | Nen Keise Verschlüsselung (sur leterstillt) | | | | | |
| | Direct Access (IPsec) |) | None verschlusseung (nur integritat) | | | | | |
| | Direct Access (IPeac.Verschlüssel | (123) | Nicht konfiguriert | | | | | |
| | |) | Nicht konfigureit | | | | | |
| | Direct Access (Provisingtellungen) | | T WOOT IS INCOMING CALIFORNIA | | | | | |
| | DirectAccess (Proxyeinstellungen) |) | Nicht konfiguriert | | | | | |
| | DirectAccess (Proxyeinstellungen) DirectAccess (Webproxy) DirectAccess (DNS-Server) | | Nicht konfiguriert | | | | | |
| | Direct Access (Proxyeinstellungen Direct Access (Webproxy) Direct Access (DNS-Server) Allaemeine DNS-Server | , | Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert | | | | | |
| | DirectAccess (Proxyeinstellungen DirectAccess (Webproxy) DirectAccess (DNS-Server) Allgemeine DNS-Server Coderung | , | Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert Nicht konfiguriert | | | | | |

Anwenden Abbrechen

Mit gpupdate oder gpupdate /force werden die Einstellungen übernommen



Alterung der DNS Serverzonen einstellen

Um den DNS-Server automatisiert zu bereinigen, richtet man die sogenannte Alterung auf Server und Zonen ein. Diese sorgt dafür dass DNS-Einträge mit einem Zeitstempel nach einer gewissen Zeit automatisch gelöscht werden.

Gerade im Zeitalter der Mobilen Geräte, werden immer häufiger Einträge im DNS Server gemacht und diese werden nicht mehr automatisch gelöscht.

Die Einstellung kann man manuell oder per PowerShell durchführen.

| | Name |
|--------------|---|
| ADS ► 🗊 (| DNS-Server konfigurieren |
| ⊳ 📫 z | Standardanwendungs-Verzeichnispartitionen erstellen |
| ⊳ 🚞 F | Neue Zone |
| ⊳ 🛄 F | Alterung/Aufräumvorgang für alle Zonen festlegen |
| | Veraltete Ressourceneinträge aufräumen |

Als erstes klicke man auf den Servernamen und wählt im Kontext Menü "Alterung/Aufräumvorgang für alle Zonen festlegen"

| Eigenschaften für Serveralterung/Aufräumvorgang | | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|
| Veraltete Ressourceneinträge aufräumen | | | | | | | | | |
| Intervall für Nichtaktualisierung | | | | | | | | | |
| Die Zeit zwischen der letzten Aktualisierung des Zeitstempels eines Eintrags und dem Zeitpunkt, zu dem der Zeitstempel wieder aktualisiert werden kann. | | | | | | | | | |
| Intervall für Nichtaktualisierung: 7 Tage V | | | | | | | | | |
| Aktualisierungsintervall | | | | | | | | | |
| Die Zeit zwischen dem frühesten Zeitpunkt, zu dem der Zeitstempel eines Eintrags aktualisiert werden kann und dem Zeitpunkt, zu dem der Eintrag aufgeräumt werden kann. Das Aktualisierungsintervall muss länger sein als der maximale Zeitraum der Eintragsaktualisierung. | | | | | | | | | |
| Aktualisierungsintervall: 7 Tage V | | | | | | | | | |
| Serveralterung/Bestätigung des Aufräumvorgangs | | | | | | | | | |
| Standardeinstellungen für neue Active Directory-integrierte Zonen: | | | | | | | | | |
| Veraltete Ressourceneinträge aufräumen: Aktiviert | | | | | | | | | |
| Diese Einstellungen auf alle vorhandenen Active Directory-integrierten Zonen anwenden | | | | | | | | | |
| OK Abbrechen | | | | | | | | | |

Wir setzen das Häkchen und klicken auf OK, danach müssen wir noch das Häkchen für alle vorhandenen Active Directory Integrierten Zonen aktivieren und ebenfalls mit OK bestätigen.

| B DNS | | E | igenschaften vor | htdom.loo | al ? | x |
|--|--|--|--|----------------------------------|---|-----------------|
| ⊿ ADS01 | | | | | | |
| Globale Protokolle | | WINS | Zonenübertragu | ingen | Sicherhei | Ł |
| Zwischengespeicherte Look | upvorgänge | Allgemein | Autoritätsursprung | (SOA) | Namenserv | er |
| ✓ Forward-Lookupzonen ▷ ③ _msdcs.htdom.local ◇ ④ _msdcs ▷ ③ _msdcs ▷ ③ _tcp ▷ ④ _udp ▷ □ _oretDnsZones ▷ □ ForestDnsZones | | Status: Wird au Typ: Active I Replikation: Alle Daten werden in A | isgeführt Directory-integriert DNS-Server in dieser D | lomäne shert. | Anhalte Ändem Ändem | n |
| Foreitoniszones Reverse-Lookupzonen Fill Vertrauenspunkte | | Dynamische Upda | ates: Nur | sichere | | ~ |
| ▷ 🦳 Bedingte Weiterleitungen | Zonenalteru Veraltete Re Interval für N Die Zeit zwis Entrags und aktualisiert w Interval für Nichtaktualis Aktualisierung Die Zeit zwis eines Eintraga der Eintraga muss länger Eintragsaktu | ng/Eigenschafter ssourceneinträge aufrää ichtaktualisierung chen der letzten Aktuali dem Zeitpunkt, zu dem verden kann. zierung: sinterval chen dem frühesten Zei saktualisiert vereden kan sen als der maximale Ze alleierung. | h für Aufräumvor umen sierung des Zeitstempe der Zeitstempel wieder Tage tpunkt, zu dem der Zeit ann und dem Zeitpunkt, n. Das Aktualisierungsin sitraum der | tstempel , zu dem ntervall | ates bestehl auenswürdige Alterung an H 3 (NSEC3) r (RRSIG) | : ein :n |
| | Aktualisierun Die Zone steht f Datum und U | gsintervall: 7 für den Aufräumvorganı Ihrzeit: 26.06.20 | g zur Verfügung nach: 016 17:00:00 | Abbrechen | 2 3 (NSEC3) r (RRSIG) 2 3 (NSEC3) r (RRSIG) 2 3 (NSEC3) r (RRSIG) 2 3 (NSEC3) | |
| | | | | | r (RRSIG) | |

Wenn man sich nun die Eigenschaften der Forward und Reverse Lookupzonen ansieht, wurden hier die Alterungen der Zone aktiviert. (*Bitte kontrollieren*)

| DNS | Eigenschaften von ADS01 | ? | x |
|-------------------------------------|---|--------------|---------|
| Globale Protokolle | Debugprotokollierung Ereignisprotokollierung Überwa | achen Sic | herheit |
| Zwischengespeicherte Lookupvorgänge | Schnittstellen Weiterleitungen Erweitert | Stammhin | weise |
| ⊿ 🧮 Forward-Lookupzonen | | | |
| Imsdcs.htdom.local | Serverversionsnummer: | | |
| ⊿ 📳 htdom.local | 6.3 9600 (0x2580) | | |
| ▷ [] _msdcs ▷ [] _sites | Serveroptionen: Rekursionsvorgang (und Weiterleitungen) deaktivieren | 1 | |
| jo _ucp | BIND-Sekundärzonen aktivieren | | |
| upDomainDnsZonesEnrestDnsZones | □Beim Laden unzulässiger Zonendaten einen Fehler zun Roundrobin aktivieren | ückgeben | ≡ |
| Reverse-Lookunzonen | Netzwerkmaskenanforderung aktivieren | | |
| | ✓ Cacrie voi beschaugungen sichem ✓ DNSSEC-Übernr | , | \sim |
| Bedingte Weiterleitungen | | | |
| | Namensüberprüfung: Multibyte (UTF8) | | ~ |
| | Zonendaten beim Start laden: Von Active Directory un | nd Registrie | rur ∨ |
| | Aufräumvorgang bei veralteten Einträgen automatisch | aktivieren | |
| | Zeitraum des Aufräumvorgangs: 7 Tage | ; | ~ |
| | 2 | Zurücksetzer | n |
| | OK Abbrechen Übernehm | ien H | lilfe |

Die letzte Einstellung die gesetzt werden muss, ist die Einstellung das der Server nach einer gewissen Zeitspanne die Einträge auch löscht.

Diese Bereinigungsaktion kann man im Ereignisprotokoll (2501/2502) überprüfen.

- → Event ID 2501 = Welche Einträge wurden erfolgreich gelöscht.
- └→ Event ID 2502 = Es wurde nichts bereinigt



Mit Powershell und dnscmd kann man die Alterung ebenfalls einrichten, diese Befehle sind auf einem Server Core sehr nützlich.

Was unbedingt zu beachten ist, besonders wenn mehrer DNS Server im Einsatz sind, das nur ein einziger DNS Server die bereinigung vornimmt, diese Einstellung kann man entweder über PowerShell -ScavengeServers 192.168.178.100 oder dnscmd Servername /ZoneResetScavengeServers Zone IP-Adresse setzen.

Server Aging und Scavening für alle Zonen einrichten

- Set-DnsServerScavenging -ApplyOnAllZones -ScavengingState \$true -RefreshInterval 7.00:00:00 -NoRefreshInterval 7.00:000
- → dnscmd /config /scavenginginterval 168 (168 / 24 Stunden = 7 Tage)

Scavening Server für die Zonen einrichten

- → Set-DnsServerZoneAging -ComputerName \$env:COMPUTERNAME -Name htdom.local -RefreshInterval 7.00:00:00 -NoRefreshInterval 7.00:00:00 -ScavengeServers 192.168.178.100 -PassThru -Verbose
- Set-DnsServerZoneAging -ComputerName \$env:COMPUTERNAME -Name 178.168.192.inaddr.arpa -RefreshInterval 5.00:00:00 -NoRefreshInterval 5.00:00:00 -ScavengeServers 192.168.178.100 -PassThru −Verbose
- → Restart-Service DNS

Was bedeuten denn die angebenden Werte?

"Intervall für Nichtaktualisierung": Diese Zeitspanne gibt an, wie lange ein Eintrag vom Client nicht aktualisiert werden kann. Wenn ein Client seinen A-Record in der DNS-Zone einträgt, dann wird dieser Eintrag mit einem Zeitstempel versehen. Dieser Zeitstempel kann bis nach Ablauf dieser Frist nicht aktualisiert werden. Wenn aber ein Client z.B. eine andere IP-Adresse erhalten hat, dann kann er diese natürlich im DNS ändern. Diese Einstellung wirkt sich also nur auf den Aktualisierungsintervall des Zeitstempels aus. Den Zeitstempel der DNS-Records kann man in der Standardansicht nicht einsehen. Wenn man den Zeitstempel eines DNS Eintrages einsehen möchte, so muss man vorher in der DNS-Konsole unter "Ansicht" die "Erweiterte Ansicht" aktivieren. Danach kann man durch Doppelklick auf einen Eintrag den entsprechenden Zeitstempel einsehen.

"Aktualisierungsintervall": Innerhalb dieses Intervalls hat der Client die Möglichkeit, den Zeitstempel zu aktualisieren. Wenn dieses Intervall abgelaufen ist, dann wird der Eintrag als veraltet markiert und letztendlich durch den Aufräumvorgang aus der DNS-Zone entfernt.

"Aufräumvorgang bei veralteten Einträgen": Dieser Wert gibt an, wie oft der Server das Aufräumen veralteter Einträge vornimmt.



Active Directory Objekte vor versehentlichen löschen schützen.

Der Best-Practice Analyser von Active Directory, klagt nach der Grundinstallation an das alle Objekte vor dem versehentlichen löschen geschützt werden müssen.

Dies realisiert man mit folgenden PowerShell Befehlen.

- Get-ADOrganizationalUnit –Filter * -Properties ProtectedFromAccidentalDeletion | where {\$_.ProtectedFromAccidentalDeletion –eq \$false} | Set-ADOrganizationalUnit -ProtectedFromAccidentalDeletion \$true
- Get-ADObject –Filter * -Properties ProtectedFromAccidentalDeletion | where {\$_.ProtectedFromAccidentalDeletion –eq \$false} | Set-ADObject -ProtectedFromAccidentalDeletion \$true -ErrorAction SilentlyContinue

| = | Ac | tive Directory-Benut |
|--|---|-------------------------|
| Datei Aktion Ansicht ? | | |
| (+ +) 🗾 🔣 🖬 🖉 🖗 +) | · 🛿 🖬 🔧 🖄 🍞 🗾 🍇 | |
| Active Directory-Benutzer und -Compute | Name Typ | |
| Gespeicherte Abfragen | Eigenschaften von Computers ? X | e - Lokal (in Domäne) I |
| ⊿ III htdom.local | | ۱ ۱ |
| Builtin | Allgemein Objekt Sicherheit Attribut-Editor | e - Lokal (in Domäne) 🕧 |
| Computers Domain Controllers | Kanonischer Name des Objekts: | e - Global I |
| ForeignSecurityPrincipals | htdom.local/Computers | e - Global i |
| LostAndFound | | e - Global |
| Managed Service Accounts | Objektklasse: Container | - Global / |
| Program Data | Erstellt am: 25.05.2016 17:25:12 | - Global |
| System | Geändet am: 05.06.2016.12:22:36 | |
| Users | | - Global |
| In TDM Davies | Aktualisierungssequenznummem: | |
| P IPW Devices | Aktuelle: 49459 | - Universal |
| | Ursprüngliche: 5822 | e - Global I |
| | | e - Lokal (in Domäne) |
| | Objekt vor zufälligem Löschen schützen | e - Global I |
| | | e - Universal I |
| | | e - Global I |
| | | e - Universal I |
| | | e - Lokal (in Domäne) |
| | | e - Lokal (in Domäne) |
| | | e - Lokal (in Domäne) |
| | OK Abbrechen Übernehmen Hilfe | |



Zeitserver für den PDC Emulator konfigurieren

Um auf dem ersten Domaincontroller (PDC Emulator) die Zeitsynchronisation mit einer externen Quelle zu konfigurieren, sollte man sich im Internet kurz schlau machen welche Zeitquellen sind den so verfügbar.

Da ich weiß das in Braunschweig mehre Atomuhren stehen nutze ich auch die Quelle als externer Zeitgeber.

http://www.zeitserver.de/deutschland/deutsche-ntp-zeitserver/ http://www.zeitserver.de/deutschland/ptb-zeitserver-in-braunschweig/

- w32tm /config /computer:ads01.htdom.local /manualpeerlist:"ptbtime1.ptb.de,0x01 ptbtime2.ptb.de,0x02 ptbtime3.ptb.de,0x02" /syncfromflags:manual /update
 - o 0x01 SpecialInterval
 - 0x02 UseAsFallbackOnly
 - 0x04 SymmatricActive
 - o 0x08 Client
- → net stop w32time && net start w32time
- → w32tm /resync /computer:ads01.htdom.local /nowait
- → w32tm /query /status /verbose





Active Directory – Standort und Dienste

Um die Grundkonfiguration abzuschließen lege ich für meinen ersten Domaincontroller noch ein Subnetz an und benenne die Default Site um. Hierzu öffne ich die MMC *Active-Directory-Standorte und Dienste*.

| 82 | | | Active [| Directory-Standorte und | I -Dienste | | | |
|--|-----------------|--------------------|-----------------------|-------------------------|------------|--|--|--|
| Datei Aktion Ansicht ? | | | | | | | | |
| | | | | | | | | |
| Reference of the second | Dienste [ads01. | Name | Тур | Beschreibung | | | | |
| ⊿ 🚞 Sites | | Servers | Servercontainer | | | | | |
| Inter-Site Transports | | MTDS Site Settings | Standorteinstellunger | n | | | | |
| ⊿ 🚞 Subnets | | | | | | | | |
| 192.168.178.0/24 | | | | | | | | |
| A 📕 Site-German-Munich | 01111 | | | | | | | |
| ⊿ 🚞 Servers | Objektverwal | tung zuweisen | | | | | | |
| ⊿ ≣ ADS01 | Suchen | | | | | | | |
| NTDS Sett Services | Alle Aufgabe | n | Þ | | | | | |
| , <u> </u> | Ansicht | | • | | | | | |
| | Löschen | _ | | | | | | |
| | Umbenenner | 1 | | | | | | |
| | Aktualisieren | | | | | | | |

Hierzu klickt man den Eintrag Default-Site mit der rechten Maustaste an und wählt im Kontextmenü umbenennen.

Im nächsten Schritt legen wir für die Site-german-Munich ein neues Subnetz an, dazu klickt man auf den Eintrag Subnets mit der rechten Maustaste und wählt Neues Subnetz.

| Neues Objekt - Subnetz | x |
|--|---|
| Erstellen in: htdom.Jocal/Configuration/Sites/Subnets | |
| Geben Sie das Adresspräfix mithilfe der Netzwerkpräfix-Schreibweise an (Adressen-/Präfxlänge). Dabei zeigt die Präfxlänge die Anzahl der festen Bits an. Sie können entweder ein IPv4- oder ein IPv6-Subnetzpräfix eingeben. Wetere Informationen zum Eingeben von Adresspräfixen. | |
| IPv4-Beispiel: 157.54.208.0/20 | |
| IPv6-Beispiel: 3FFE:FFFF:0:C000::/64 | |
| Präfix: | _ |
| Difference in des Artice Directors Descinenting des | _ |
| 192 168 178 0/24 | _ |
| 102.100.170.0/24 | _ |
| Standortobjekt für dieses Präfix auswählen. | |
| Standortname | |
| Site-German-Munich | |
| | |
| | |
| | |
| | |
| OK Abbrechen Hilf | в |

Hier vergibt man sein Subnetz in dem sich der Domaincontroller befindet und wählt die passende Site aus.



Was schreibt Microsoft zu dem Thema Standorte:

Ein Standort ist ein Bereich des Netzwerkes, der über schnelle Netzwerkverbindungen mit hoher Bandbreite verfügt. Hierbei handelt es sich per Definition um eine Sammlung von Computern mit schnellen Verbindungen auf Basis von IP-Subnetzen (Internet-Protokoll). Da Standorte steuern, wie die Replikation erfolgt, haben Änderungen, die mit dem Snap-In Active Directory-Standorte und -Dienste gemacht werden, Auswirkungen darauf, wie effizient die Domänencontroller (DCs) innerhalb einer Domäne (aber über große Entfernung) miteinander kommunizieren können.

Ein Standort unterscheidet sich konzeptionell von einer Domäne unter Windows Server 2008, da ein Standort mehrere Domänen und eine Domäne mehrere Standorte umfassen kann. Standorte sind nicht Teil des Domänennamespaces. Standorte steuern die Replikation von Domänendaten und helfen, die Nähe von Ressourcen zu ermitteln. So wählt beispielsweise eine Arbeitsstation zum Zweck der Authentifizierung einen Domänencontroller (DC) innerhalb des eigenen Standortes.

Zur Sicherstellung, dass die Replikation seitens Active Directory ordnungsgemäß durchgeführt werden kann, wird auf allen DCs ein Konsistenzprüfungsdienst mit Namen Knowledge Consistency Checker (KCC) ausgeführt, der automatisch Verbindungen zwischen einzelnen Computern am gleichen Standort herstellt. Diese Verbindungen werden als Active Directory-Verbindungsobjekte bezeichnet. Der Administrator kann weitere Verbindungsobjekte erstellen oder Verbindungsobjekte entfernen. Wenn die Replikation jedoch an irgendeinem Punkt innerhalb eines Standortes unmöglich wird oder wenn sich ein einzelner Ausfallpunkt ergibt, schaltet sich die Konsistenzprüfung ein und erstellt so viele neue Verbindungsobjekte wie nötig sind, um die Active Directory-Replikation wiederaufzunehmen.....

http://openbook.rheinwerk-verlag.de/windows_server_2012r2/08_002.html#dodtpb48200d0-6b44-40ce-af46-dcdd04802812

So das war es erst mal wieder von mir, der Domaincontroller ist nun sauber eingerichtet worden und steht für den zweiten Teil der Konfiguration Serie bereit.

Viele Grüße

Helmut Thurnhofer