Best-Practice-Empfehlungen für die DNS-Konfiguration in einer Active Directory-Domäne

Was wollen wir?

Eine saubere und einwandfrei funktionierende DNS-Konfiguration in einer Domäne.

Warum wollen wir das?

Damit die DNS Auflösung in jedem Fall immer korrekt funktioniert und keine Probleme verursacht werden

Und wie geht das genau?

a) Hauptpunkt 1

Alle ADS-internen DNS-Server sollten in einer Art „**Selbst-Ausschluss Matrix**“ unter IPv4 DNS der Netzwerkkarte des Servers konfiguriert sein.

Jeweils mit 127.0.0.1 (dem Loopback-Adapter) als Self-Referenz IMMER am ENDE der Liste !!!

Beispiel:

DNS Konfiguration unter IPv4:	**DC1**	**DC2**	**DC3**	**DC4**
DC1	?	**?**	**?**	**?**
DC2	**?**	?	**?**	**?**
DC3	**?**	**?**	?	**?**
DC4	**?**	**?**	**?**	?
127.0.0.1	**?**	**?**	**?**	**?**

b) Hauptpunkt 2

Eine Standort-Abhängige **DNS Weiterleitung** im DNS-Server an die dortige Firewall / das Gateway / oder andere EXTERNE DNS Server muss eingerichtet sein....

c) Hauptpunkt 3

Alle anderen Server sollte ALLE AD DNS-Server in ihrer DNS-IP-CONFIG aufgeführt haben.

Dito sollte die DNS Server Liste via DHCP Options an alle Clients über den DHPC Server "Auto-verteilt" werden,

sowie bei manueller IP eines Gerätes auch die DNS-Liste auf diesem dann manuell gesetzt sein.

d) ...was generell alles zu beachten wäre...

Damit Active Directory wie vorgesehen funktioniert, ist eine korrekte Konfiguration des DNS unerlässlich. **Ein unsachgemäß konfiguriertes DNS kann eine Vielzahl von Problemen verursachen, darunter Fehler bei der Anmeldung, Probleme bei der Verarbeitung von Gruppenrichtlinien und Replikationsprobleme.** Die folgende Liste bewährter Verfahren ist nicht allumfassend, wird aber dazu beitragen, eine korrekte Namensauflösung innerhalb einer Active Directory-Domäne sicherzustellen.

- **In einer kleinen Umgebung sollte mindestens ein Domain Controller (DC) ein DNS-Server sein.** Es ist möglich, ein DNS auf Servern zu installieren, die keine DCs sind (einschließlich nicht-Windows-Servern), aber die Installation eines DNS auf DCs ermöglicht die Verwendung von AD-integrierten Lookup-Zonen (siehe unten), die die Sicherheit verbessern und die Zonen Replikation vereinfachen.
- **In einer größeren Umgebung sollten mindestens zwei Domänencontroller an jedem physischen Standort DNS-Server sein.** Dies sorgt für Redundanz für den Fall, dass ein DC unerwartet offline geht. Beachten Sie, dass Domänen angehörende Rechner dafür konfiguriert werden müssen, mehrere DNS-Server zu verwenden, um davon zu profitieren.
- **Wenn mehrere DCs als DNS-Server konfiguriert sind, sollten Sie so konfiguriert sein, dass Sie zuerst den anderen und an zweiter Stelle sich selbst für die Auflösung verwenden.** Die Liste der DNS-Server jedes DC sollte seine eine eigene Adresse enthalten, aber nicht als ersten Server in der Liste. Wenn ein DC nur sich selbst für die Auflösung verwendet, repliziert er unter Umständen nicht mehr mit anderen DCs. Dies ist offenkundig kein Problem in einer Domäne mit nur einem DC.
- **Alle einer Domäne angehörenden Computer dürfen nur interne DNS-Server verwenden.** Wenn ein einer Domäne angehöriger Computer so konfiguriert ist, dass er einen externen Server als alternativen DNS-Server nutzt, wird ein vorübergehendes Fehlen einer Verbindung zu einem internen DNS-Server dazu führen, dass dieser Rechner den externen Server für die Auflösung verwendet. Dieser externe Server wird keine Abfragen innerhalb der AD-Domäne auflösen können und der

Client-Rechner wird nicht automatisch zum internen DNS-Server zurück wechseln, wenn die Verbindung wieder hergestellt wird. Dies wirkt sich in der Regel so aus, dass vom betroffenen Rechner nicht auf Ressourcen in der Domäne zugegriffen werden kann.

- **In einer Umgebung mit mehreren Standorten sollten Domänenmitglieder so konfiguriert sein, dass Sie die DNS-Server an ihrem lokalen Standort bevorzugt vor denen an einem anderen Standort nutzen.** Dies minimiert die DNS-Datenmenge, in langsameren WAN-Verbindungen.
- **Verwenden Sie Active Directory-integrierte DNS-Zonen, um die Sicherheit zu verbessern und die DNS-Replikation zu vereinfachen.** AD-integrierte DNS-Zonen werden in Verzeichnispartitionen innerhalb von Active Directory gespeichert. Diese Verzeichnispartitionen replizieren zusammen mit dem Rest von AD. Daher ist für die DNS-Replikation keine zusätzliche Konfiguration (z. B. Zonentransfer-Setup) erforderlich. Darüber hinaus ermöglichen AD-integrierte Zonen den Einsatz sicherer dynamischer Aktualisierungen. Dies verhindert Aktualisierungen von DNS-Datensätzen von Rechnern, die sich nicht mit der Domäne authentifizieren können.
- **DNS-Zonen sollten nur sichere dynamische Aktualisierungen zulassen, es sei denn, zwingende Gründe sprechen dagegen.** Das Zulassen von nicht sicheren dynamischen Updates kann dazu führen, dass Rechner, die nicht Teil der Domäne sind, Datensätze auf den DNS-Servern der Domäne ändern können, was ein Sicherheitsrisiko darstellt. Das Deaktivieren sämtlicher dynamischer Updates hingegen sichert zwar die DNS-Datensätze, erschwert aber die Verwaltung der Domäne.
- **Konfigurieren Sie die Weiterleitung oder Root-Hinweise für die externe Namensauflösung in einer mit dem Internet verbundene Umgebung.** Weiterleitungen können eine schnellere Reaktion auf externe Abfragen bieten, aber Sie sind weniger redundant als die 374+ weltweit verteilten Root-DNS-Server. **Root-Hinweise sind standardmäßig auf Windows-Servern vorhanden, aber Weiterleitungen müssen manuell konfiguriert werden.**
- **DNS-Server innerhalb einer Domäne sollten sich nicht gegenseitig als Weiterleitung verwenden.** Weiterleitungen sind Server, an die ein DNS-Server Abfragen sendet, die er nicht beantworten kann (d.h. Abfragen für Datensätze in Zonen, die er nicht hostet). DNS-Server innerhalb einer Domäne hosten in der Regel die gleichen Zonen, wenn also einer von Ihnen nicht in der Lage ist, eine bestimmte Abfrage zu beantworten, werden Sie alle nicht in der Lage sein, dies zu tun, und die Weiterleitung dieser Abfrage von einem Server zu einem anderen wird nur zu Verzögerungen führen.
- **Konfigurieren Sie Fälligkeit und Scavenging, um veraltete DNS-Datensätze zu vermeiden.** Die richtige Konfiguration von Fälligkeit und Scavenging sorgt dafür, dass veraltete Datensätze (die ein bestimmtes, konfigurierbares Alter überschreiten) automatisch vom DNS entfernt werden.
- **Verwenden Sie den DNS Best Practice Analyzer.** Der DNS BPA führt eine Überprüfung auf mehr Elemente als hier dokumentiert durch und bietet Richtlinien für die Lösung von Problemen, die er findet. Weitere Informationen über den DNS BPA finden Sie unter Best Practices Analyzer für Domain Name System.

Eltern haften für ihre Kinder.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!