Domain Name System

مقدمة :

يُعد نظام أسماء النطاقات (DNS) أحد الأعمدة الأساسية التي تقوم عليها شبكات الحاسوب الحديثة، سواء على مستوى الإنترنت أو داخل الشبكات المؤسسية. فبدونه لا يمكن للمستخدمين ولا للأجهزة الوصول إلى الموارد باستخدام الأسماء المفهومة للبشر.

تعتمد الأنظمة الحاسوبية على العناوين الرقمية (IP Addresses) ، بينما يتعامل الإنسان مع الأسماء (Domain Names)، وهنا يظهر دور DNS كوسيط ذكي يقوم بتحويل الأسماء إلى عناوين رقمية.

في بيئات **Active Directory**، لا يُستخدم DNS فقط للوصول إلى الخوادم، بل يُعد عنصرا أساسيا لعمل النظام بشكل صحيح، حيث يعتمد عليه:

- التحقق من هوية المستخدمين(Authentication)
- تسجيل الدخول إلى الشبكة (Logon)
- تطبيق سياسات المجموعة (Group Policy)
- اكتشاف وحدات التحكم بالمجال (Domain Controllers)

تهدف هده الجلسة الى بناء فهم علمي عميق لكيفية عملDNS ، ثم الانتقال إلى دوره المتقدم داخل Active Directory .

المفاهيم الأساسية فى DNS

DNS هو نظام موزع وهرمي يهدف إلى ترجمة أسماء النطاقات إلى عناوين IP والعكس.

المكونات الأساسية:

1. **DNS Client**
   - أي جهاز يرسل استعلام DNS (حاسوب، هاتف، خادم).
2. **DNS Server**
   - الخادم الذي يستقبل الاستعلام ويجيب عليه.

3. DNS Zone

- جزء من قاعدة بيانات DNS يحتوي على سجلات نطاق معين.

4. DNS Record

- هو سجل في DNS يُستخدم لربط اسم (مثل اسم جهاز أو نطاق) بمعلومة معينة، مثل: (عنوان IP ، خادم االبريد ، او خدمة معينة على الشبكة) .

آلية حل الاسم:

1. العميل يطلب اسما.
2. الخادم يبحث محليا.
3. إن لم يجد:
   - يستخدم Forwarder : هو خادم DNS آخر يطلب منه الخادم المحلي المساعدة عند عدم العثور على الاسم المطلوب.
   - أوRoot Hints : عند عدم وجود Forwarder ، يبدأ الخادم البحث من الأعلى (خوادم الجذر Root DNS Servers)، ثم ينتقل تدريجيا حتى يصل إلى الإجابة الصحيحة.
4. تُعاد النتيجة للعميل.

مناطق(DNS (DNS Zones

منطقة(DNS (DNS Zone :

هي وحدة إدارية وتنظيمية داخل خادمDNS ، تُستخدم لتخزين وإدارة سجلات DNS الخاصة بنطاق معين.

◆ Forward Lookup Zone

هي منطقة في DNS تُستخدم لتحويل اسم الجهاز أو اسم النطاق إلى عنوانIP ، وتُعد الأكثر استخداما في الشبكات.

◆ Reverse Lookup Zone

هي منطقة في DNS تُستخدم لتحويل عنوان IP إلى اسم الجهاز أو اسم النطاق.

تستخدم لأغراض:

- **الأمان :**التحقق من هوية الأجهزة.
- **السجلات :(Logs)** تسجيل أسماء الأجهزة بدل عناوين IP.
- **البريد الإلكتروني :**التحقق من مصدر الرسائل ومنع البريد المزعج.(Spam)

◆ Primary Zone

هي المنطقة الأساسية في DNS التي تحتوي على **النسخة الأصلية القابلة للتعديل** من سجلات DNS، وتُعد المصدر الأساسي للبيانات.

يتم إنشاء السجلات وتحديثها مباشرة داخل هذه المنطقة، ويمكن نسخها إلى خوادم DNS أخرى على شكل Secondary Zones.

◆ Secondary Zone

هي **نسخة احتياطية للقراءة فقط** من الـ Primary Zone. تُستخدم لتقليل الحمل على الخادم الأساسي وزيادة التوافر، حيث تحصل على بياناتها من الـ Primary Zone عبر **.**Zone Transfer

◆ Stub Zone

هي منطقة تحتوي فقط على الحد الأدنى من المعلومات اللازمة لتحديد خوادم DNS المسؤولة عن نطاق آخر، وتشمل:

- **SOA** (سجل بداية الصلاحية) : يحدد الخادم الأساسي المسؤول عن منطقة DNS. // من هو المسؤول الرئيسي عن المنطقة وكيف تُدار // .
- **NS** (سجل خادم الأسماء). : يحدد خوادم DNS المخولة رسميا بالإجابة عن استعلامات نطاق معين // من هم خوادم DNS التي تجيب عن استعلامات هذا النطاق // .

تُستخدم للربط بين أنظمة DNS المختلفة وتسهيل توجيه الاستعلامات.

◆ AD-Integrated Zone

هي منطقة DNS مخزنة داخل **Active Directory** بدلًا من ملف نصي.

تدعم:

- التكرار التلقائي عبرActive Directory
- التحديثات الديناميكية الآمنة
- التوافر العالي(High Availability)

وتُعد الخيار **الأفضل والمُوصى به** في بيئات.Active Directory

ملاحظة ☜: يساهم اختيار نوع المنطقة المناسب في تحسين أداء DNS وزيادة الأمان وضمان استقرار الشبكة، خاصة في البيئات المؤسسية.

سجلات(DNS Records) DNS

السجلات (DNS Records) تُعد جوهر نظامDNS ، إذ تخزن المعلومات التي تمكن الخوادم والعملاء من الوصول إلى الموارد داخل الشبكة. ومن أهم هذه السجلات:

- **A Record:**

يربط اسم النطاق أو اسم الجهاز بعنوان **IPv4**.

- **AAAA Record:**

يربط اسم النطاق أو اسم الجهاز بعنوان **IPv6**.

- **PTR Record:**

يربط **عنوان IP** باسم الجهاز، ويُستخدم في **Reverse Lookup Zones**لأغراض التشخيص، والأمان، والتحقق في أنظمة البريد الإلكتروني.

- **CNAME (Canonical Name):**

يوفر اسما مستعارا يشير إلى اسم نطاق آخر.(Alias)

- **MX (Mail Exchanger):**

يحدد خوادم البريد المسؤولة عن استقبال الرسائل لنطاق معين.

- **NS (Name Server):**

يحدد خوادم DNS المخولة رسميا بإدارة النطاق والإجابة عن استعلاماته.

- **SRV (Service Locator):**

يحدد موقع الخدمات داخل الشبكة مثل LDAP وKerberos ، ويُعد الأساس الذي يعتمد عليه **Active Directory** لاكتشاف وحدات التحكم بالمجال(Domain Controllers) .

DNS وActive Directory :

Active Directory يعتمد اعتمادا كليا على DNS .

لأن AD يحتاج إلى:

- اكتشاف Domain Controllers
- العثورعلى خدمات المصادقة
- توجيه العملاء للخادم الأقرب

مجلد_msdcs (Microsoft Domain Controller Services)

هو مجلد خاص داخل DNS يحتوي على سجلات تُستخدم من قبل Active Directory لاكتشاف وحدات التحكم بالمجال (Domain Controllers) وتشغيل خدماته الأساسية.

يحتوي على سجلات خاصة بخدمات:

- التكرار (Replication) بين وحدات التحكم بالمجال
- Global Catalog لاكتشاف خوادم الدليل العام
- المصادقة (Authentication) داخل المجال

سجلات SRV الأساسية في msdcs_

- **_ldap:**

تُستخدم للاستعلام عن الدليل النشط والعثور على وحدات التحكم بالمجال.

- **_kerberos:**

تُستخدم لخدمة المصادقة باستخدام بروتوكول.Kerberos

- **_kpasswd:**

تُستخدم لخدمة تغيير كلمات المرور.

- **_gc (Global Catalog):**

تُستخدم لاكتشاف خوادم **Global Catalog** وإجراء عمليات البحث على مستوى ال(Forest).

ملاحظة ☜ : تعتمد Active Directory اعتمادا كليا على هذه السجلات، وأي خلل أو حذف فيها يؤدي إلى فشل تسجيل الدخول وتعطل خدمات المجال.

DNS Delegation :

التفويض في DNS يعني إسناد إدارة نطاق فرعي إلى خادم DNS آخر.

يساعد في :

- فصل الصلاحيات
- توزيع الحمل
- الأمان
- إدارة مستقلة للأقسام

Aging & Scavenging :

هي آلية تُستخدم في DNS لتنظيف السجلات القديمة وغير المستخدمة بشكل تلقائي، بهدف الحفاظ على دقة سجلات DNS ومنع تضخمها.

- **Aging:**

تتبع عمر سجل DNS باستخدام الطابع الزمني.(Timestamp)

- **Scavenging:**

حذف سجلات DNS التي لم يتم تحديثها خلال فترة زمنية محددة.

الفترات الزمنية:

- **No-refresh Interval:** فترة لا يُسمح خلالها بتحديث الطابع الزمني للسجل.
- **Refresh Interval:** فترة يُسمح خلالها بتحديث الطابع الزمني، وإذا لم يحدث ذلك يصبح السجل قديما.(Stale)

تُعد هذه الآلية **مهمة جدا في بيئات DHCP** حيث تتغير عناوين IP باستمرار.

ملاحظة ☜ : يجب تفعيل Aging & Scavenging بحذر لتجنّب حذف السجلات الثابتة المهمة.

..... انتهت الجلسة مع تمنياتي لكم بالتوفيق والنجاح .....