

Microsoft

ACTIVE DIRECTORY



Prepared by

Matan Sigavker

Blog Website

www.Israel-IT.co.il

הקדמה | Introduction

כאנשי IT אנו מתמודדים ביום עם מספר רב של מערכות ארגוניות שעלינו לנהל. ובכדי לנהל את מערכות אלה, ראשית עלינו להכיר את סביבת הארגון בצורה הטובה ביותר. אך יש כלכך הרבה נושאים ולפעמים גם לכל נושא יש תתי נושאים אשר מספקים המון מידע שרובו אינו רלוונטי לנו, אז כיצד ניתן לדעת אילו נושאים כדאי ללמוד? אילו נושאים רלוונטים לסביבה הארגונית שלי? ואם אחרי זמן מסוים אני עובר לארגון אחר? האם אני צריך להתחיל עכשיו ללמוד הכל מחדש?

כבר בתחילת דרכי בתחום ה-IT שאלתי את עצמי את השאלות האלו וכיום לאחר מספר שנים של למידה וכתובת מאמרים מכל הסוגים, החלטתי לכתוב מאמר מקוצר על מושגי יסוד אשר קיימים כמעט בכל ארגון שתמצאו בו. כל זאת על מנת לכוון אותנו (אנשי ה-IT) כיצד ללמוד ולהכיר את הסביבה הארגונית בצורה מעמיקה ועם זאת גם מהירה.

במאמר שלפניכם מוצגים מספר מושגים ופרוטוקולים המיוחסים לסביבת Active Directory. כלומר שישנם פרוטוקולים כללים ויסודיים כמו DNS, Kerberos ו-NTP אשר ניתן לייחס לסביבות שונות, אך עם זאת תפקידם נשאר זהה ואינו משתנה כלל. מה שבכל זאת שונה מסביבה לסביבה, זו התצורה שבה מנהלים את הפרוטוקולים.

חשוב לי לציין שעל כל נושא שנכתב במאמר שלפניכם, למדתי וחקרתי לעומק בכך שקראתי מספר מאמרים שונים המספקים מידע על אותו נושא, סיכמתי את הנושאים לפי מה שרלוונטי ובמקביל לכך הקמתי מעבדה עם סביבה וירטואלית ובחנתי כיצד כל פרוטוקול עובד על מנת לאמת את מה שאני כותב.

אני מאמין ומקווה שהמאמר שכתבתי יועיל להרבה אנשי IT, בין אם הם נמצאים בתחילת דרכם ולבין אם הם כבר בעלי ניסיון. משום שבכדי להתמקצע בתחום לא מספיק ללמוד רק פעם אחת, אלא שבכל תקופה מסוימת נדרש לעבור שוב על אותם הנושאים בכדי לרענן את הזכרון ולהתעדכן האם קיימים שינויים או חידושים הקשורים לאותם נושאים.

© כל הזכויות שמורות למתן סיגבקר

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר מידע, לשדר או לקלוט בכל דרך אחרת כל חלק שהוא מהחומר במאמר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב ממחבר המאמר (מתן סיגבקר).

Table of Contents | תוכן עניינים

Active Directory Domain Services (AD DS) Overview	3
Forest and Domain Functional Levels	5
Domain Controller and Read Only Domain Controller	6
FSMO (Flexible Single Master Operations)	7
Active Directory - Sites and Services	10
Active Directory - Trust Relationships Types	11
Active Directory - Certificate Services (AD CS)	15
System Volume (SYSVOL)	17
SYSVOL - Replication Services	18
Domain Name System (DNS) in Active Directory	20
LDAP (Lightweight Directory Access Protocol)	23
Kerberos Authentication	24
Group Policy Objects (GPO)	26
Network Time Protocol (NTP) In Active Directory	28
Key Management Services (KMS)	30

Active Directory Domain Services (AD DS) Overview

Active Directory Domain Services

אלו הם שירותי הליבה של ה-Active Directory המאפשרים לנו לנהל משתמשים, מחשבים, קבוצות וגישה למשאבי הרשת בארגון כגון: שרתים, תיקיות רשת, מדפסות וכו'. השרת אשר מריץ את שירותי ה-“AD DS” נקרא Domain Controller. בדרך כלל בכל ארגון יהיה לפחות שני שרתי (Domain Controller (DC), כאשר שרת אחד מתפקד כראשי והשרת השני מתפקד כמשני לצורך גיבוי או לויסות עומסים (תלוי בהיררכיה הארגונית). כאשר משתמש מבצע Login למחשב, מאחורי הקלעים מתבצע אימות מול שרת ה-Domain Controller והוא מעניק למשתמש גישה להתחבר למחשב או לכל שירות אחר בארגון אשר דורש אימות (Authentication).

מהו Active Directory ?

Active Directory (AD) הינו שירות של מיקרוסופט אשר ניתן להתקין אותו על שרתי Windows החל מ-Windows Server 2000. המטרה של שירות זה, הוא לסייע בעת הניהול של הרשת הארגונית בצורה יעילה ונוחה. בעזרת כלי השירות שיש ל-Active Directory ניתן לנהל משתמשים, מחשבים, קבוצות, סיסמאות, הרשאות, אכיפת מדיניות ועוד. כל המידע שנשמר ב-Active Directory מאוחסן כאובייקטים.

מושגי יסוד ב-Active Directory

Schema – כוללת בתוכה את כל ההגדרות של האובייקטים אשר נוצרו ב-Active Directory, ה-Schema גם מכילה מידע לגבי כל התכונות (Attributes) שניתן להוסיף ל-Active Directory כלומר ה-Schema ניתנת להרחבה. עם זאת כדאי שתשקלו היטב כל שינוי שאתם מתכננים לבצע בסכמה, מכיוון שכל שינוי כזה עלול להשפיע על הרשת כולה.

Global Catalog (GC) – הינו מכיל רשימה חלקית של כל המידע אודות אובייקטים (Objects) ותכונות (Attributes) הנמצאים ב-Active Directory. רשימה זו מכילה מידע על אובייקטים כמו משתמשים, מחשבים, קבוצות, קונטיינרים וכל מה שנמצא ב-Active Directory כולל חלק מהתכונות של אובייקטים. כאשר יש לנו מספר Forests ב-Domains, תפקידו של ה-Global Catalog הוא למצוא מידע על אובייקטים שונים בין הדומיינים בצורה מהירה וביצוע המרת ה-SIDs (שעליו נרחיב בהמשך) של אובייקטים מסויימים לשמות. בנוסף לכך הוא גם יודע לספק מידע על קבוצות אוניברסליות (Universal Group Membership). בעבר היה ניתן להגדיר רק שרת DC אחד כ-Global Catalog וכל שאר השרתים היו מתפקדים כ-Read Only Domain Controller, שרתים אלו נקראו גם Backup Domain Controller (BDC) וזאת בכדי לחסוך ברוחב הפס. בימים אלו כבר אין מצוקה של רוחב פס ומרוב שהרשת מהירה כל כך, כל שרת Domain Controller חדש שמוקם בארגון מוגדר באופן אוטומטי גם כ-Global Catalog.

Replication Service – הוא שירות אשר אחראי על שכפול נתונים בין ה-Domain Controllers, כל שינוי שאנחנו מבצעים ב-Active Directory או בתיקיית ה-Sysvol משוכפל באופן אוטומטי אל כל שאר שרתי ה-Domain Controllers הקיימים בארגון.

Query and Index Mechanism – בעזרת שירות זה, נוכל לייצר שאילתת חיפוש אובייקטים ב-Active Directory ע"י מספר רב של קריטריונים ובכך התוצאה שנקבל תהיה די מדויקת לשאילתת החיפוש.

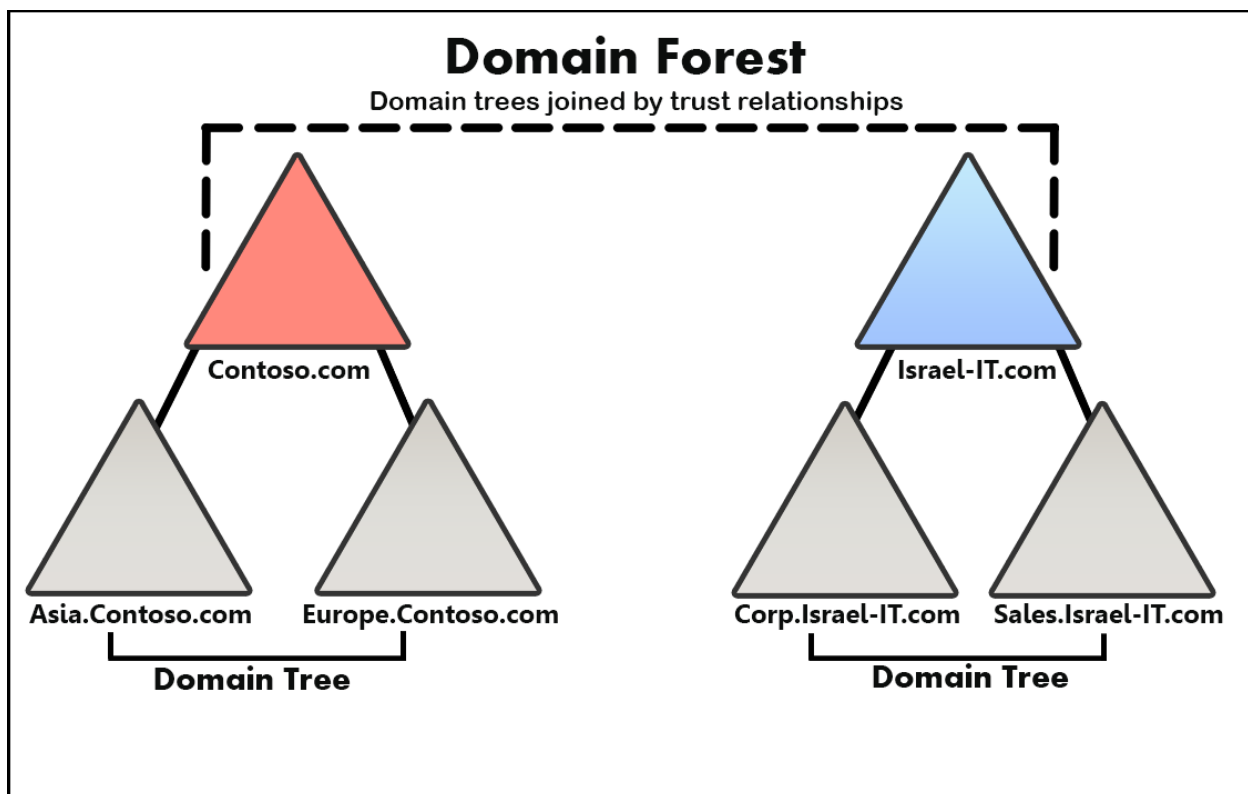
מבנה ה-Active Directory

Domain – כולל בתוכו אוסף של אובייקטים כגון משתמשים, מחשבים וקבוצות אשר חולקים את אותו מסד הנתונים (Database) של ה-Active Directory. ניתן ליצור מספר רב של Domains ו-Sub-Domains בארגון, כל Domain מדמה לנו כענף אחד של אותו העץ.

Organizational Units (OUs) – זהו קונטיינר בתוך ה-Active Directory שניתן למקם בתוכו מספר אובייקטים כגון: משתמשים, קבוצות, מחשבים ואפילו OUs נוספים. השימוש ב-OUs מסייע למנהלי הרשת לייצר סדר היררכי בארגון ולניהול המשאבים ברשת.

Tree – הינו אוסף המורכב מ-Domain אחד או מספר Domains אשר מקובצים יחד תחת היררכיה לוגית, כל Domain מדמה ענף אחד של אותו העץ (Tree) ומכיוון שענפים הם חלק בלתי נפרד מהעץ יש ביניהם יחסי אמון שנקרא "Trust".

Forest – הינו אוסף המורכב מ-Tree אחד או מספר Trees אשר חולקים את אותו Schema ו-Global Catalog, היער (Forest) משמש לצורך אבטחת הגבולות בין Forest אחד לאחר וכמובן שניתן להגדיר גם יחסי אמון בין יערות (Forests).



Forest and Domain Functional Levels

Functional Levels

כאשר מקימים Forest חדש בארגון, במהלך ההתקנה ישנה הגדרה הנקראת "Functional Level", בהגדרה זו ניתן לקבוע מה תהיה רמת של ה-Functional Level ב-Forest וברמת ה-Domain.

הגדרת ה-Functional Level קובעת באילו שירותים ניתן להשתמש ב-Active Directory Domain Services, ככל שרמתה ה-"Functional Level" תהיה גבוהה יותר כך אנחנו נקבל יותר שירותים שניתן להשתמש בהם ב-Active Directory ובנוסף לכך הסביבה תהיה הרבה יותר מאובטחת.

לכן חשוב מאוד להגדיר את רמת ה-"Functional Level" הכי מקסימלית שניתן להחיל על הארגון, נכון לשנה הזו (2024) הרמה המקסימלית היא Windows Server 2016. הגדרה זו גם קובעת אילו מערכות הפעלה (Operating System) יוכלו לתפקד בתור Domain Controller ואילו לא.

לדוגמה אם יש לנו Forest אשר ה-Functional Level שלו ברמת "Windows Server 2003", לא נוכל להגדיר שרתי Domain Controllers עם מערכות הפעלה של "Windows Server 2019" ומעלה.

כאשר רוצים להגדיר או לשדרג את רמת ה-FFL וה-DFL של הארגון, יש לבצע בדיקות תאימות בין רמת ה-Functional Level לבין הגרסאות של המערכות השונות בארגון. כלומר שבמידה ויש לנו בארגון שרתים של Exchange, SharePoint וכו', או שירותים צד שלישי המתממשים אל שירותי ה-Active Directory, עלינו לוודא כי שירותים אלו אכן נתמכים ב-Functional Level שאנחנו רוצים להגדיר.

את ה-Domain Functional Level (DFL) ניתן להגדיר בגרסה גבוהה יותר ממה שמוגדר ב-Fores (functional level (FFL), אך לא ניתן להגדיר ב-DFL גרסה שהיא נמוכה יותר מה-FFL. חשוב לזכור שמהרגע שמעלים את גרסת ה-DFL החזרה לאחור תהיה קשה ומסובכת מאוד ובמקרים מסויימים בכדי לחזור לגרסה הקודמת, נצטרך לבנות את ה-Domain מחדש או לבצע שחזור מגיבוי.

Domain Controller and Read Only Domain Controller

Domain Controller (DC)

Domain Controller הוא השרת אשר מותקן עליו ה-Role של Active Directory Domain Services (ADDS). ה-DC אחראי על ניהול האבטחת הרשת הארגונית כגון: אימות הזהות של משתמשים, ניהול קבוצות ומדיניות הרשת, ביצוע בדיקה לאילו משאבים כל משתמש מורשה לגשת בסביבת ה-Domain ועוד. חשוב להבין כי בכל Forest קיים רק שרת Domain Controller אחד אשר מתפקד כ- Primary Domain Controller, והוא השרת הראשי של הארגון אשר מחזיק בחמשת חוקי ה-FSMO שעליהם נרחיב בהמשך.

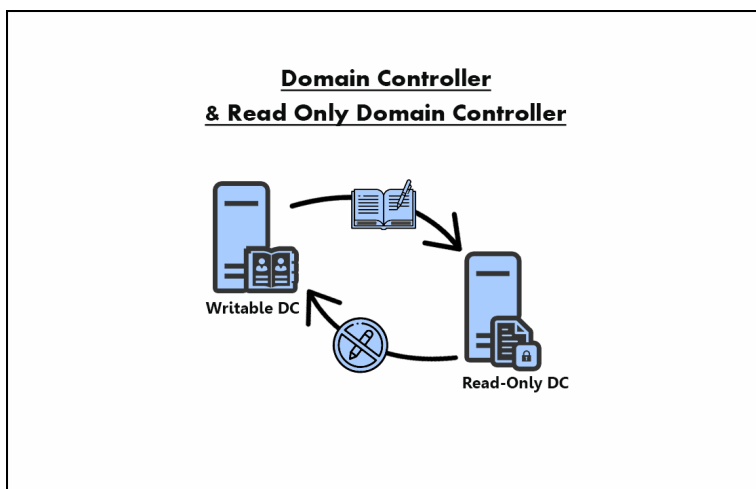
Read Only Domain Controller (RODC)

RODC זה שרת Domain Controller נוסף בארגון שמחזיק בתוכו העתק מלא של ה-Active Directory Database המוגדר בתצורת קריאה בלבד (Read-Only). כלומר, שרת המוגדר כ-RODC מאפשר לקרוא ממנו מידע אך לא לכתוב אליו מידע. הכוונה היא שכל המחשבים והמשתמשים ברשת אכן יכולים לבצע אימות מול שרת ה-RODC, לקבל את מדיניות הארגון (Group Policy) או כל מידע אחר אשר מאוחסן ב-Database של ה-Active Directory. אך עם זאת לא ניתן לבצע שום שינויים ב-Active Directory או בכל מה שמה שיושב על ה-AD Database של שרת ה-RODC.

לכן ניתן להבין כי כל שרתי ה-DC אשר אינם מוגדרים כ-Read-Only, יכולים לשכפל (Replicate) מידע על השינויים שמתבצעים ב-AD Database אל שרתי ה-RODC, אך לא ניתן לשכפל מידע משרתי ה-RODC אל שרתי ה-DC רגילים.

בדרך כלל, מגדירים שרתי DC בתצורת Read-Only במקרים שבהם רוצים לחסוך ברוחב הפס ועם זאת לשמור גם על האבטחה והסדר של הארגון. כאשר יש סניף שנמצא די רחוק מה-Domain Controller, כל פנייה של משתמשים, מחשבים או שרתים אל שרת ה-DC המרוחק עלולים להעמיס על רוחב הפס וכתוצאה מכך זמן התגובה (Latency) יהיה ארוך יותר.

לכן הפתרון היעיל ביותר הינו להגדיר Domain Controller נוסף באותו סניף, כמובן שהוא לא חייב להיות מוגדר כ-Read-Only אך במידה והשרת אכן מוגדר כך, דבר זה משפר את אבטחת הארגון מכיוון שכל הסיסמאות של המחשבים, המשתמשים והאפליקציות אינם נשמרים ב-Cache של שרתי ה-RODC. מה גם שלא ניתן להתקין על שרתים אלו אפליקציות שמתמסקות מול ה-Active Directory ומבצעות שינויים ב-AD Database.



FSMO (Flexible Single Master Operations)

מהו FSMO ?

FSMO אלו הם ראשי תיבות של "Flexible Single Master Operation", המייצגים חמישה תפקידים שקיימים על שרתי ה-Domain Controller בארגון. שניים מהתפקידים חלים ברמת ה-Forest והשלושה האחרים חלים ברמת ה-Domain.

שני התפקידים שחלים ברמת ה-Forest הם ייחודיים, כלומר שלא ניתן להחיל את תפקידים אלו על מספר שרתי DC. כן ניתן לפצל את שני התפקידים בכך שכל תפקיד יהיה על DC אחר, אך לא ניתן להגדיר את אותו התפקיד על 2 שרתי Domain Controller שנמצאים באותו ה-Forest, גם אם הם נמצאים בדומיינים נפרדים.

לעומת זאת, את שאר התפקידים שחלים ברמת ה-Domain ניתן להגדיר על כל שרת DC אשר נמצא ב-Domain נפרד. ניתן להעביר את חוקי ה-FSMO משרת DC אחד לשני, בתנאי שכל הרפליקציות בין שרתי ה-DCs אכן תקינות.

משמעות השם FSMO

- Flexible: תפקידים אלו הם גמישים וניתן להעביר אותם משרת Domain Controller אחד לאחר.
- Single: כל תפקיד הוא ייחודי ואינו תלוי בתפקיד אחר ולפי כך ניתן לפזר את תפקידים אלו בכמה שרתי DCs.
- Master Operation: אלו הם חמשת התפקידים (RID Master, PDC, Domain Naming Master, Emulator, Infrastructure Master)

חמשת התפקידי ה-FSMO

1. Schema Master

בכל Forest יכול להיות רק שרת Domain Controller אחד המתפקד כ-Schema Master, ה-Schema מכילה את כל האובייקטים (Objects) והשדות (Attributes) של האובייקטים אשר קיימים ב-Active Directory כגון: משתמשים (AD Users), מחשבים (AD Computers), קבוצות (AD Groups), קונטיינרים (Organizational Units) ועוד. לכל אובייקט יש מספר שדות שניתן להגדיר.

אם תיכנסו אל ה-Active Directory ולאחר מכן אל המאפיינים של אחד מהאובייקטים, תוכלו לראות את כל השדות של אותו אובייקט. מה גם שניתן לשנות או להוסיף אובייקטים ושדות חדשים ל-Schema הקיימת ולזה קוראים "הרחבת ה-Schema". ישנם מקרים רבים בהם אנחנו נדרשים להרחיב את ה-Schema. לדוגמה כאשר מתקינים שרת Exchange חדש בארגון, מאחורי הקלעים מתבצעת הרחבה ל-Schema מפני של-Active Directory נוספים אובייקטים ושדות חדשים.

אותו הדבר קורה גם כאשר משדרגים שרת Domain Controller מגרסת Windows Server ישנה לגרסה חדשה. עם זאת חשוב מאוד להזהר בכל עדכון או עריכה של ה-Schema, מכיוון שכל שינוי שמתבצע ב-Schema הינו חל על כל ה-Forest ובמידה ולא עושים זאת בדרך הנכונה, הארגון כולו עלול להיפגע.

Domain Naming Master .2

בכל Forest יכול להיות רק שרת Domain Controller אחד המתפקד כ- Domain Naming Master, תפקיד זה אחראי על הקמה או הסרה של Domains בתוך ה-Forest. זאת אומרת שאם נקים Domain חדש וננסה להעניק לו שם Domain שכבר קיים באותו Forest, ה- Domain Naming Master לא יאשר זאת מפני ששם הדומיין חייב להיות ייחודי.

Relative ID (RID) Master .3

בכל Domain שנמצא תחת אותו ה-Forest יכול להיות שרת Domain Controller אחד המתפקד כ- RID Master, תפקיד זה אחראי על הניהול של כל SID אשר קיים ב-Active Directory. כאשר אנו יוצרים אובייקט חדש ב-AD, מאחורי הקלעים נוצר לאותו אובייקט "SID" הייחודי לו.

בימינו אוהבים להשוות את המונח SID לתעודת זהות, מכיוון ש-SID הוא מספר ייחודי שיש לכל אובייקט ב-Active Directory. לכן אין אפשרות שיהיו שני אובייקטים בעלי אותו ה-SID. ה-Domain Controller הראשון שמקימים, מקבל Pool של 500 מספרי SIDs שהוא יכול לחלק. הספירה מתחילה מ-1,000 וכל DC נוסף אשר מקימים בארגון יקבל גם הוא Pool נוסף של SIDs.

בכדי שלא תהיה התנגשות של SIDs כל DC מקבל טווח שונה של SIDs. לדומה, ה-Domain Controller השני שתקימו בארגון יקבל טווח חלוקה החל מ-1,501 ועד 2,000 וכך גם כל DC נוסף שתקימו בארגון.

במידה ולשרת DC מסוים נגמרו כל ה-SIDs, תפקידו של ה-RID Master הוא לספק לו עוד כ-500 SIDs נוספים. במצב שה-RID Master לא עובד ול-DC נגמרו כל ה-SIDs, לא יהיה מי שיספק ל-DC טווח חדש של SIDs.

PDC Emulator Master .4

בכל Domain שנמצא תחת אותו ה-Forest יכול להיות רק שרת Domain Controller אחד המתפקד כ- Primary Domain Controller (PDC). בעבר היה רק שרת DC אחד שתפקד כ-Primary והיה ניתן לכתוב אליו. כל שאר שרתי ה-DC היו מתפקדים כ-Read Only ונקראו גם Backup Domain Controller (BDC). כיום המצב הוא שונה וניתן לכתוב למספר שרתי Domain Controllers בו זמנית. אם השרת שמתפקד כ-PDC Emulator Master לא עובד במשך זמן רב, ישנו סיכוי שלארגון תהיה בעיה של סנכרון שעונים.

תחומי האחריות של ה-PDC

- **סנכרון השעונים** - המחשבים שמצורפים ל-Domain מסונכרנים מול השעון של ה-DC שהכי הקרוב אליהם, כל שאר שרתי ה-Domain Controllers אשר לא מתפקדים כ-PDC Emulator מסונכרנים באופן אוטומטי מול השעון של שרת ה-DC שמתפקד כ-PDC Emulator.
- **החלפת סיסמאות** – כאשר מתבצעת החלפה של סיסמה לאחד מהמשתמשים או כאשר משתמש מסוים טעה מספר רב של פעמים בהקלדת הסיסמה, באותו הרגע השרת שמתפקד כ-PDC Emulator הוא תמיד יהיה הראשון לדעת על שינויים אלו. גם אם החלפת הסיסמה בוצעה מול שרת DC אשר אינו PDC, אותו שרת DC יעדכן באופן מיידי את השרת שמתפקד כ-PDC. זה אומר שהוא השרת הכי מעודכן מבין שרתי ה-DCs. אם עובד מזין את שם המשתמש והסיסמה שלו בכדי להתחבר למחשב והאימות מתבצע מול שרת Domain Controller אשר אינו מתפקד כ-PDC, אותו שרת DC יאמת מול שרת ה-PDC שהסיסמה שהוזנה היא אכן עדכנית.
- **מדיניות (Group Policy)** – בתוך תיקיית ה-SYSVOL המקומית שבכל שרתי ה-Domain Controllers אשר אינם מתפקדים כ-PDC, קיים העתק עם כל הגדרות של ה-Group Policies. ההיררכיה היא כזאת, כל שינוי אשר מתבצע ב-Group Policy מחלחל היישר משרת ה-Domain Controller המתפקד כ-PDC אל שאר שרתי ה-DCs האחרים ולאחר מכן למחשבים ולשרתים בארגון. גם אם נפתח את Group Policy דרך כלי הניהול שלו (MMC) על שרת DC אשר אינו מוגדר כ-PDC, באותו רגע שרת ה-PDC יעודכן בדבר וזאת בכדי למנוע התנגשויות.

Infrastructure Master .5

- בכל Domain שנמצא תחת אותו ה-Forest יכול להיות רק שרת Domain Controller אחד המתפקד כ-Infrastructure Master, שתפקידו הוא לתרגם את ה-SIDs של המשתמשים לשמות בכדי שתחומים (Domains) אחרים יוכלו לעבוד עם שמות ולא עם SIDs. זהו תפקיד אשר שימש אותנו בעבר וכיום קיבלנו אותו בתורשה.
- הכוונה לכך שבמידה ונוסיף לאחת מקבוצות ה-AD Group משתמשים מ-Domain אחר או להפך, אנחנו נראה את ה-SID של המשתמש ובכדי שנוכל לעבוד בצורה שהיא נוחה ה-Infrastructure Master ממיר את ה-SIDs לשמות. כיום מי שאחראי על המרת SIDs לשמות הינו ה-Global Catalog (GC) ואסור שהשרת אשר מתפקד כ-GC יתפקד גם כ-Infrastructure Master, אך במידה וזה כן קורה כמו למשל בימים אלו, מה שיקרה זה שה-Infrastructure Master לא יעבוד כנדרש.
- האמת שאין לנו עוד צורך ב-Infrastructure Master מכיוון שה-Global Catalog מבצע עבודה הרבה יותר טובה והסיבה שעדיין התפקיד הזה קיים הוא מפני שקיבלנו אותו בהורשה מזמנים בהם היה ניתן להגדיר רק GC אחד בכל Domain וזאת בכדי להקל על רוחב הפס, וכיום מרוב שרוחב הפס מהיר כלכך כל Domain Controller שיש בארגון מתפקד גם כ-Global Catalog.

Active Directory Sites and Services

AD Sites and Services

הינו שירות האתרים והשירותים של ה-Active Directory, זהו כלי ניהול המאפשר לאנשי IT לשלוט על הרפליקציות בין שרתי ה-Domain Controllers והאתרים (Sites) אשר חברים באותו ה-Forest כגון: תזמון רפליקציות לפי לוחות זמנים, הגדרת טופולוגיה של סנכרון בין שרתי ה-DCs, הפנייה של טווחי כתובות IP לעבוד מול שרת ה-DC הקרוב ביותר ועוד.

למעשה בעזרת שירות האתרים והשירותים, כל שרת Domain Controller בארגון יודע מול איזה DC הוא צריך להסתנכרן ומתי. חשוב להבהיר כי אלו הגדרות שמאוד חיוניות לארגון ובמידה ולא מגדירים כהלכה את ה-Sites and Services, ככל הנראה שכל הרשת הארגונית תושפע מהגדרות אלו בכך שתחנה לא תדע לזהות מי ה-DC שהכי קרוב אלייה וכתוצאה מכך התחנה עלולה לבצע אימות מול שרת DC מרוחק, שדבר זה כמובן יאט מאוד את תהליך האימות.

אותו הדבר תקף גם לגבי Domain Controllers כאשר אין להם את היכולת לזהות מי ה-DC הקרוב אליהם מבחינה גאוגרפית, הם עלולים לנסות להסתנכרן מול שרת DC מרוחק. כמובן שדבר זה בכלל לא יעיל ורק יכול להעמיס על רוחב הפס.

AD Sites and Services מורכב ממספר תכונות:

- Active Directory Sites - נועד בכדי לסייע לארגונים אשר בבעלותם יש מספר סניפים הפרוסים ברחבי העולם ומשויכים אל אותו ה-Domain, ניתן להשוות את Sites למפה אשר עוזרת לכל Domain Controller בארגון לדעת מה המסלול הכי מהיר והכי יעיל לביצוע רפליקציות. בנוסף לכך כאשר מגדירים את ה-Sites בצורה הטובה ביותר לארגון מבחינה גאוגרפית, הניצול של רוחב הפס יהיה הרבה יותר יעיל ומה גם שהביצועים יהיו טובים יותר. ישנו Site בשם "Default-First-Site-Name" אשר נוצר באופן אוטומטי בעת הקמת ה-Forest וכברירת מחדל כל שרתי ה-DCs בארגון מוקצים אל אותו ה-Site עד שיוגדר אחרת.
- Active Directory Site Links - הינה תכונה המשמשת ליצירת חיבור לוגי בין אתרים (Sites) ובכך ניתנת לנו האפשרות לקבוע את טופולוגיית הסנכרון בין אתרים שונים כגון: כל כמה זמן יתבצע סנכרון בין ה-Sites, באילו ימים יבוצע הסנכרון ותיעדוף סדר הסנכרון בין Site ל-Site.
- Active Directory Subnets - אלו טווחי רשתות של כתובות IP אשר ניתן לשייך לכל Site, ככה כל מחשב יודע לאיזה טווח כתובות הוא משויך ומול איזה Domain Controller הוא צריך לבצע את האימות. כלומר שלפי כתובת ה-IP המוגדרת במחשב, ניתן לדעת לאיזה Subnet הוא שייך ומול איזה DC הוא צריך לתקשר.
- Sites and Replication - כאשר מתבצע שינוי על אחד משרתי ה-Domain Controllers הקשור ל-Active Directory או אל תיקיית ה-Sysvol, באופן מידי שרתי ה-DCs מקבלים עדכון על השינוי שבוצע וגם מחילים את השינוי על עצמם. ובכך מתבצעות רפליקציות בין שרתי ה-Domain Controllers בארגון.
- Knowledge Consistency Checker (KCC) – הינו רכיב אשר רץ על כל שרתי ה-Domain Controllers ב-Forest ומגדיר את טופולוגיית חיבור הרפליקציות בין שרתי ה-DCs בצורה אוטומטית.

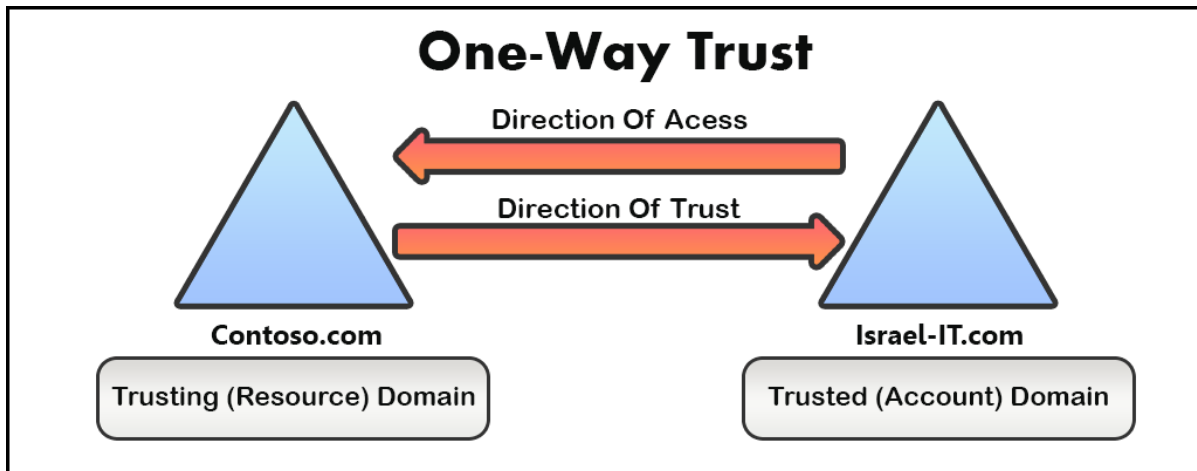
Active Directory - Trust Relationships Types

Trust Relationship

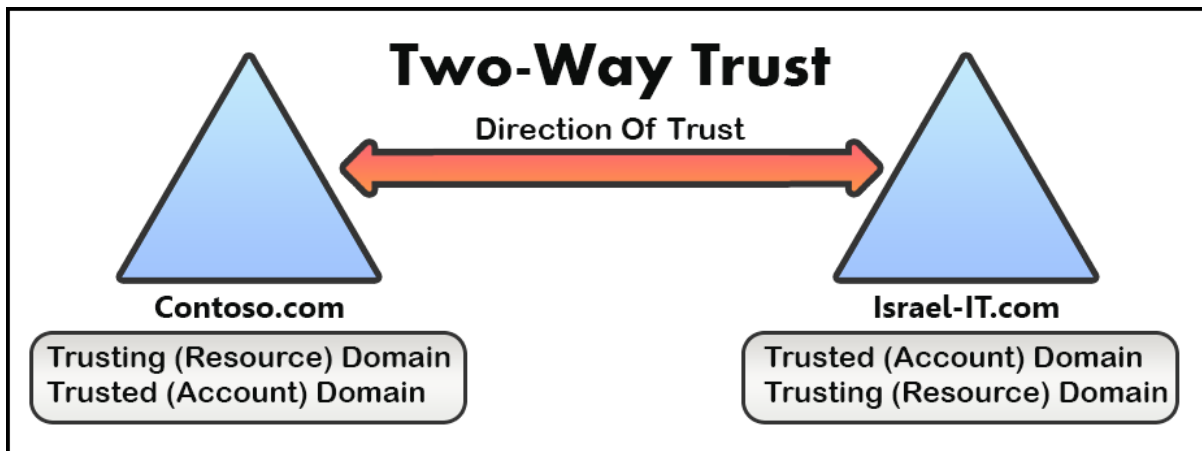
הינו חיבור לוגי בין שני Domains (תחומים) או Forests המאפשרים למשתמשים לגשת אל השירותים אחד של השני. Domain אחד נקרא "Trusting Domain" וה-Domain השני נקרא "Trusted Domain". המשתמשים אשר נמצאים בתחום שמוגדר כ-"Trusted Domain" ראשיים לגשת אל שירותים ומשאבים שנמצאים בתחום שמוגדר כ-"Trusting Domain".

סוגי יחסי אמון (Trust Type)

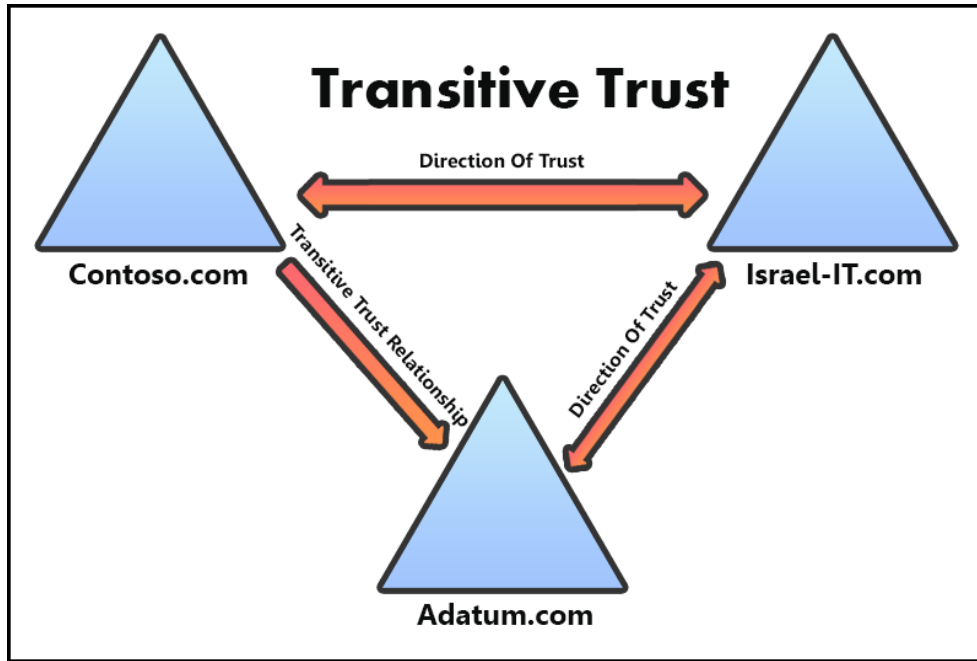
- **יחסי אמון חד-צדדי (One-Way Trust):** מאפשר ל-Domain A לגשת אל המשאבים של Domain B אך לא להפך.



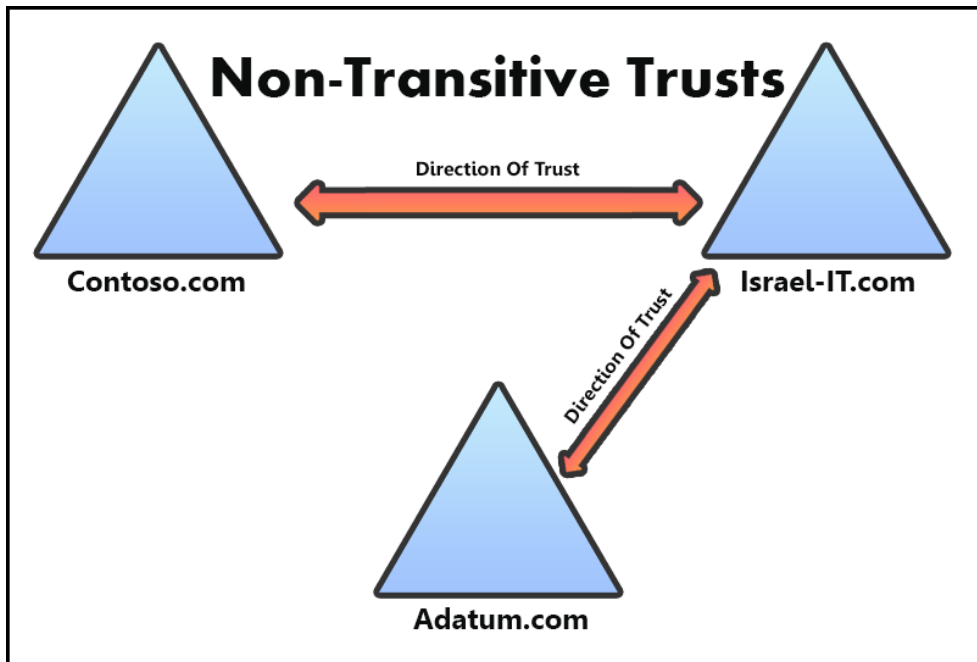
- **יחסי אמון דו-כיווני (Two-Way Trust):** הינו חיבור בין שני תחומים (Domains) שסומכים אחד על השני ומאפשרים למשתמשים מ-Domain A לגשת אל השירותים שנמצאים ב-Domain B וכך גם הפוך, Domain B יכול לגשת אל השירותים שנמצאים ב-Domain A.



- יחסי אמון טרנזיטיביים (Transitive Trust): כאשר מוגדר Trust בין Domain A ל-Domain B, ול-Domain B מוגדר Trust נוסף מול Domain C, אז גם ל-Domain A יהיה Trust מול Domain C.

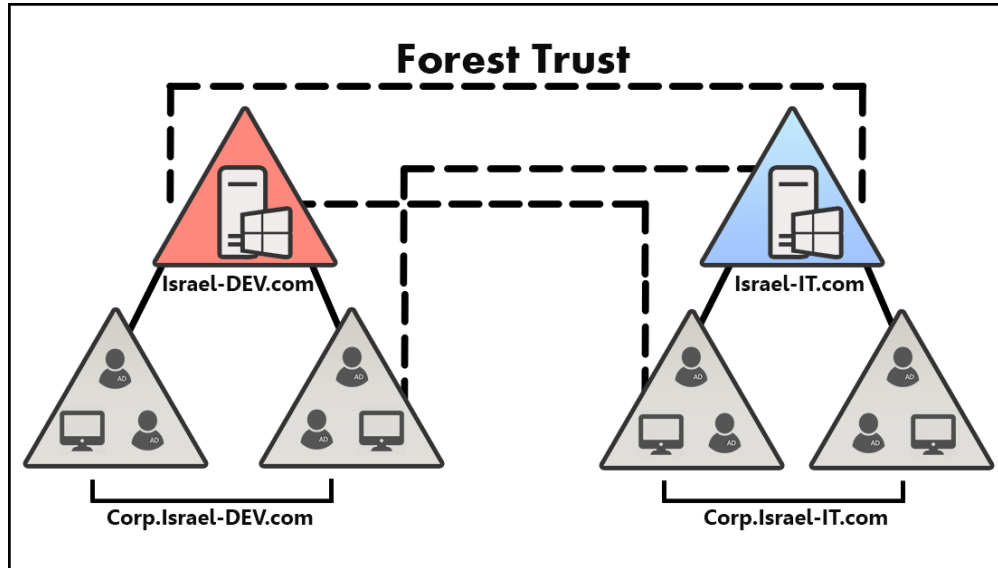


- יחסי אמון לא טרנזיטיביים (Non-Transitive Trusts): במקרה של אמון לא טרנזיטיבי, כאשר Domain A נותן אמון ב-Domain B ו-Domain B נותן אמון ב-Domain C, Domain A אינו נותן אמון ב-Domain C. את יחסי האמון הללו ניתן להגדיר בתצורת "One-Way Trust" או "Two-Way Trust".

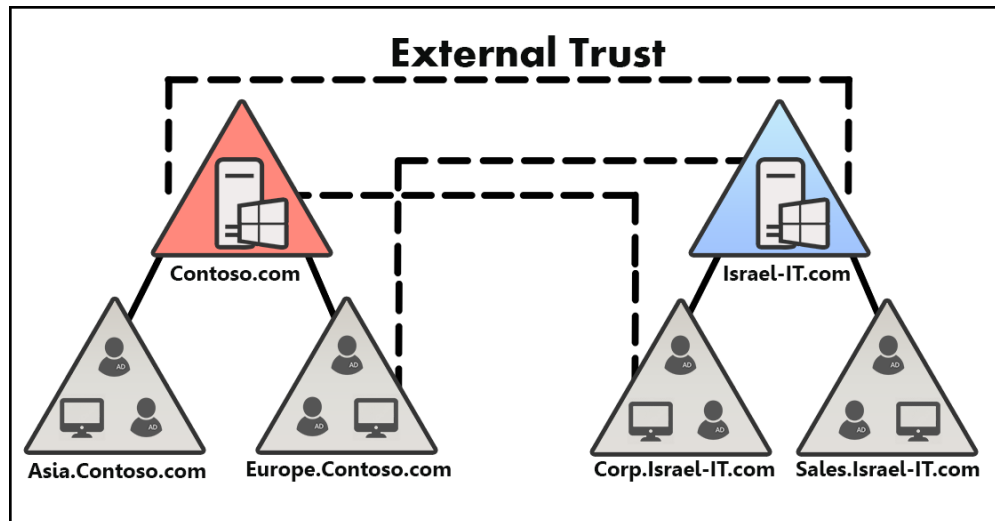


יחסי אמון בין תחומים (AD Trust)

- **יחסי אמון בין יערות (Forest Trust):** הם הגדרה מסוג "Transitive Trust", הגדרה זו מאפשרת לכל התחומים (Domains) ב-Forest A לתת אמון בכל התחומים אשר נמצאים ב-Forest B וכך גם הפוך. עם זאת, ניתן גם להגדיר את יחסי האמון הללו בתצורת "One-Way Trust".



- **יחסי אמון חיצוניים (External Trust):** הם הגדרה של Trust בין שני תחומים (Domains) אשר נמצאים ביערות (Forests) שונים. את יחסי האמון הללו ניתן להגדיר בתצורת "One-Way Trust" או "Two-Way Trust".



הגדרת ניהול יחסי האמון של Active Directory בין Domains ו-Forests דורשת מחשבה רבה, הבנה מעמיקה בתהליך ה-Trust ותכנון קפדני של כל צעד, מכיוון שהגדרות אלו משפיעות גם על אבטחת הארגון.

Trust Relationship Between Workstation to Primary Domain

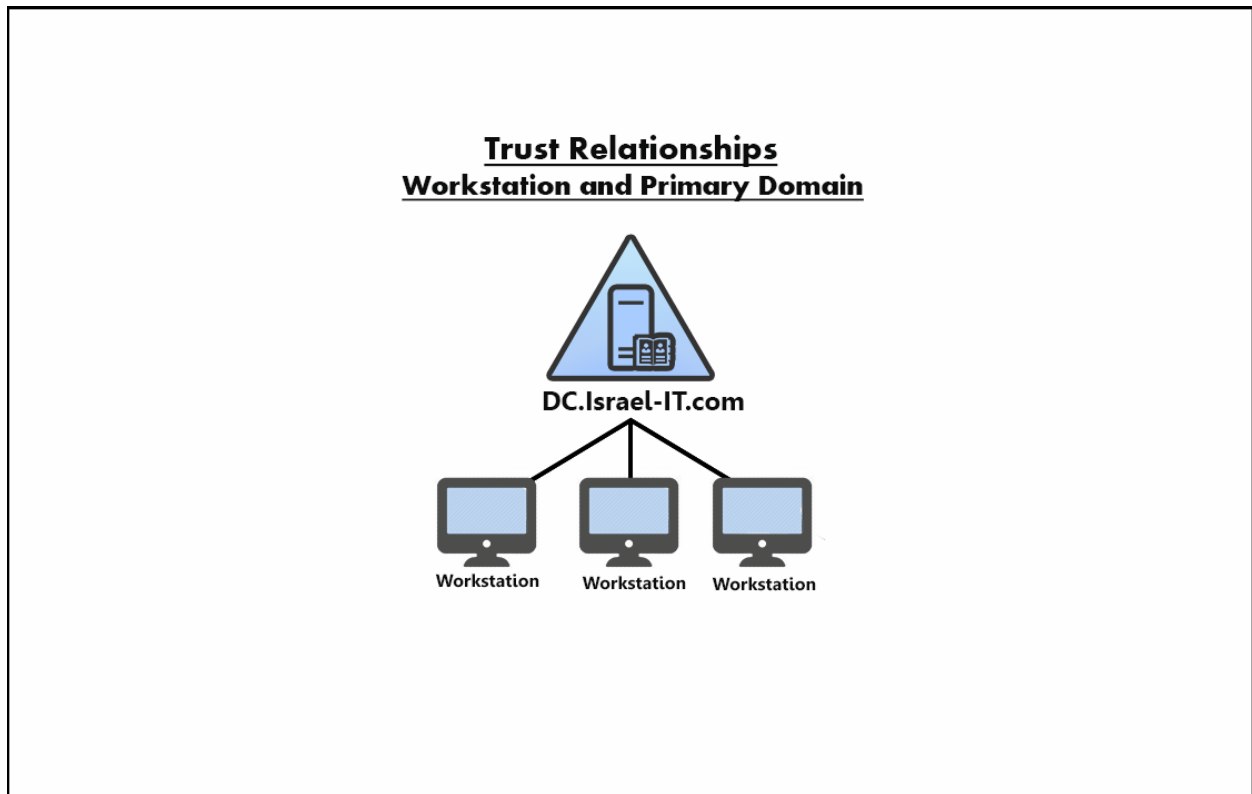
Trust Relationship הינו חיבור בין תחנות עבודה (Workstations) ל-Primary Domain, כאשר אנחנו מצרפים מחשב חדש ל-Domain נוצר ב-Active Directory אובייקט חדש הנקרא Computer Account וכמו שלכל משתמש יש סיסמה, גם לכל Computer Account ישנה סיסמה משלו אשר מתחדשת בכל 30 יום (הגדרה זו ניתנת לשינוי דרך ה-Registry או בעזרת Group Policy).

בכל פעם שאנחנו מתחברים למחשב עם Domain User, מאחורי הקלעים ה-Computer Account מבצע אימות של הסיסמה הנוכחית שלו אל מול שרת ה-Domain Controller שהכי קרוב אליו, ולכן גם חשוב לשמור על תקינות הרפלקציות בין שרתי ה-Controllers Domains בארגון.

ישנם מצבים שבהם מחשבים עלולים לקבל שגיאה לגבי Trust Relationship אשר אינו תקין, וזאת מכיוון שה-Domain אינו נותן אמון ב-Computer Account עקב ססמת המחשב אשר אינה תואמת אל ססמת המחשב שמאוחסנת ב-Active Directory וכתוצאה מכך ה-Secure Channel בין תחנת העבודה ל-Active Directory נכשל.

Secure Channel

זהו מנגנון שבאמצעותו תחנות העבודה מתחברות ל-Domain ומתקשרות בצורה מאובטחת מול שרתי ה-Domain Controllers, מנגנון זה מסתמך על הצלבת הססמאות המשוויכות לכל Computer Account מול ססמאות המחשב אשר מאוחסנות ב-Active Directory ובכך המנגנון יודע לזהות באילו מחשבים ניתן לתת אמון ובאילו לא.



Active Directory - Certificate Services (AD CS)

AD Certificate Services

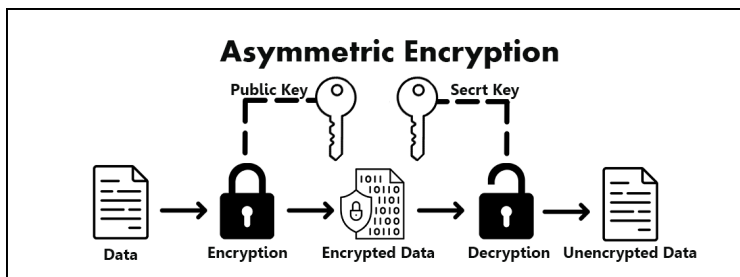
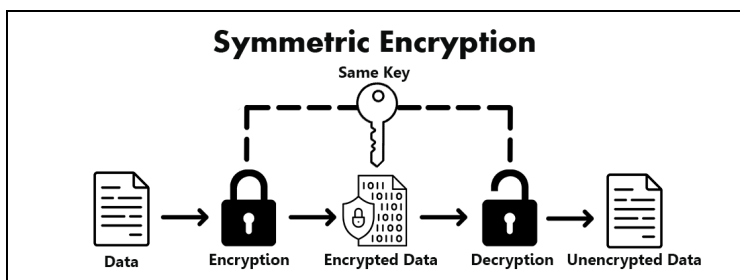
הוא אחד מה-Roles אשר כלולים בתוך מערכת ההפעלה של Windows Server ומספק תשתית מפתחות ציבוריים (Public Key Infrastructure - PKI), שזוהי הטכנולוגיה אשר עומדת מאחורי התעודות הדיגיטליות. בעזרת תשתית PKI ניתן להנפיק ולנהל תעודות דיגיטליות, להצפין מידע של מסדי נתונים (Databases), לבצע חיתום דיגיטלי על מסמכים, לאמת (Authentication) משתמשים ומכשירים בצורה מאובטחת ועוד. הצפנת המידע מתבצעת ע"י זוג מפתחות הצפנה - ציבורי ופרטי.

PKI משתמש בשני סוגי הצפנה:

1. **הצפנה סימטרית (Symmetric)** - היא הצפנה אשר משתמשת באותו המפתח הן להצפנה (Encryption) והן לפיענוח (Decryption). כלומר שבהצפנה סימטרית אנו עובדים אך ורק עם מפתח אחד.
2. **הצפנה אסימטרית (Asymmetric)** - זוהי הצפנה אשר מורכבת מ-2 סוגי מפתחות "Public Key" ו-"Private Key".
 - מפתח ציבורי (Public Key) הוא מפתח המשמש לצורך הצפנת (Encryption) המידע.
 - מפתח פרטי (Private Key) הוא מפתח המשמש לצורך פיענוח (Decryption) המידע.

ישנם מספר הבדלים בין הצפנה Symmetric ל-Asymmetric

- הצפנה Symmetric מהירה יותר מהצפנה אסימטרית Asymmetric.
- הצפנה Asymmetric מאובטחת יותר מהצפנה Symmetric.
- הצפנה Symmetric זוהי טכנולוגיה ישנה וכיום עובדים לרוב עם הצפנה Asymmetric.
- בהצפנה Symmetric אין אפשרות לדעת מי הצפין (Encryption) את המידע, לעומת זאת בהצפנה Asymmetric כן ניתן לזהות את מי שהצפין (Encryption) את המידע.



AD CS מספק את השירותים (Services) הבאים :

- **Public Key Certificates (CA) Certificate Authority** : הינו שירות לניהול ולהנפקת תעודות מסוג .שנים שני סוגי תצורות שבהן ניתן להגדיר את תשתית ה-PKI :
 - (1) **Enterprise CA** - הינה תצורה אשר מתממשת מול ה-Active Directory ולכן השרת שעליו מותקן ה-CA מחויב להיות חבר ב-Domain. עם סיום תהליך ההגדרה של Enterprise CA, יונפקו ויחולקו תעודות Root CA לכל השרתים והמחשבים בארגון בצורה אוטומטית ובכך התחנות אשר חברות ב-Domain יוכלו לסמוך על שרת ה-CA מהימן. ישנם עוד פעולות אשר ניתן לבצע בצורה אוטומטית לדוגמה, משתמש רגיל יכול להנפיק תעודות אבטחה ללא צורך באישור של המנהל. כלומר שכבר מראש מנהל השרת מגדיר לשרת ה-CA אילו תעודות אבטחה ניתן להנפיק ללא צורך באישור מנהל ולאילו תעודות אבטחה לא ניתן להנפיק מבלי אישורו של המנהל.
 - (2) **Stand Alone CA** - זוהי תצורה אשר אינה מתממשת מול Active Directory ולא ניתן לחבר את שרת ה-CA לסביבה ארגונית (Domain). כאשר שרת ה-CA מוגדר כ-Stand-alone, לא ניתן להנפיק תעודות אבטחה בצורה אוטומטית והמשתמשים אינם יכולים להנפיק תעודות דיגיטליות ללא אישורו של מנהל המערכת. כלומר כל בקשה להנפקת תעודת אבטחה לא תאושר עד שמנהל המערכת יאשר את הבקשה בצורה ידנית.
- **Certification Authority Web Enrollment** : שירות זה מאפשר למשתמשים להתחבר אל שרת ה-CA הארגוני דרך דפדפן האינטרנט (Browser), ודרכו ניתן להם האפשרות לבקש ולהנפיק תעודות אבטחה דיגיטליות. גם למשתמשים החברים ב-Domain וגם למשתמשים חיצוניים אשר אינם חברים ב-Domain.
 - **Online Responder** : שירות זה מפענח במהירות רבה את הסטטוס של אישורי תעודות האבטחה אשר בוטלו (CRL certificate) ובכך תחנות יכולות לבדוק במהירות את הסטטוס של אישורים ספציפיים אשר בוטלו, שירות זה נקרא גם (OCSP (Online Certificate Status Protocol).
 - **Network Device Enrollment Service** : שירות המבוסס על (Simple Certificate Enrollment Protocol) SCEP המאפשר להנפיק תעודות אבטחה להתקני רשת מבלי לבקש אישורי דומין (Domain Credentials) כגון : Firewalls, Routers, Switches.
 - **Certificate Enrollment Web Service** : הינו שירות המאפשר למשתמשים ולמחשבים לבצע רישום וחידוש של תעודות אבטחה בצורה אוטומטית באמצעות פרוטוקול HTTPS. כלומר כאשר מחשב שולח בקשה לקבלה או לחידוש של תעודת אבטחה משרת ה-CA, הבקשה לתעודה תאושר ותונפק למחשב בצורה אוטומטית.
 - **Certificate Enrollment Policy Web Service** : בעזרת שירות זה למשתמשים ולמחשבים בארגון יש אפשרות לקבל מידע אודות מדיניות רישום האישורים (Certificate Enrollment Policy).

System Volume (SYSVOL)

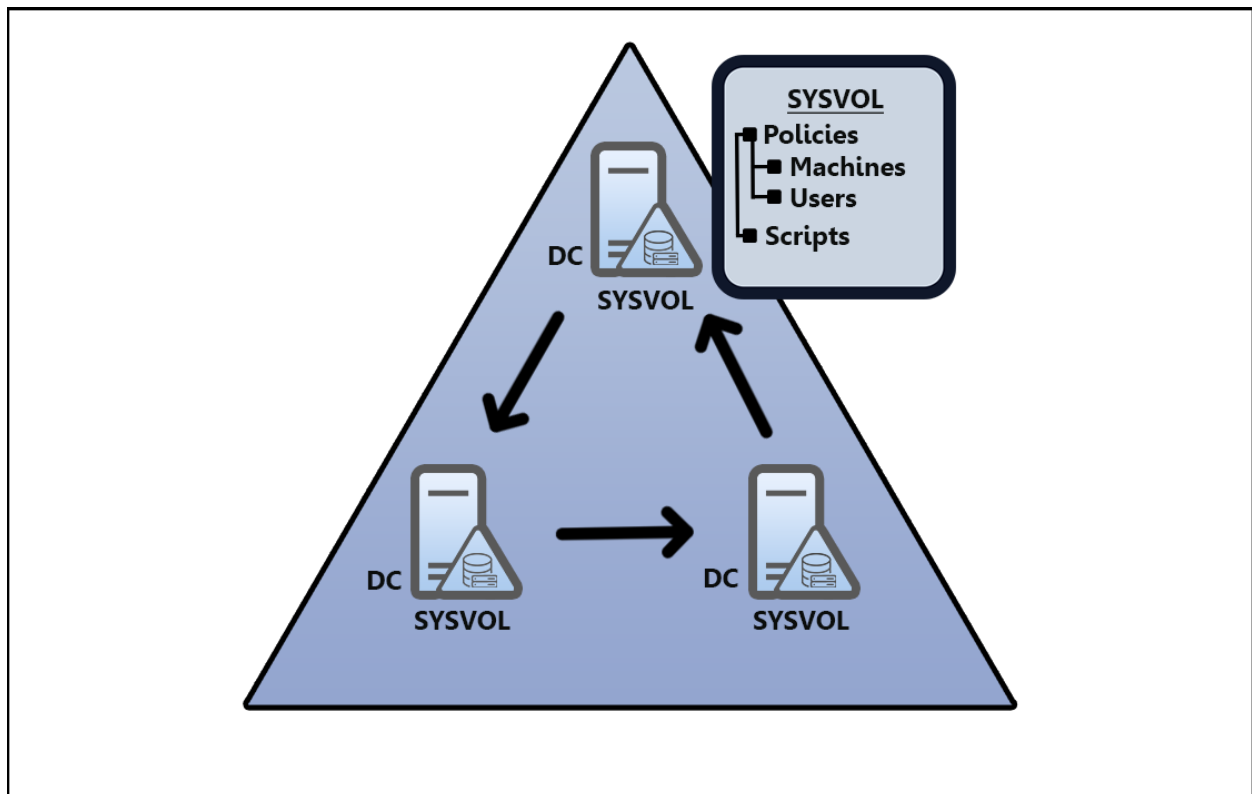
מהו (SYSVOL) System Volume ?

SYSVOL היא תיקייה מקומית אשר קיימת בכל שרת Domain Controller תחת התיב "C:\Windows", תיקייה זו נוצרת כאשר מתקינים על אחד מהשרתים את התפקיד של Active Directory Domain Services (AD DS) וזאת בכדי להפוך את השרת לתפקד כ-DC.

תיקיית ה-SYSVOL משתכפלת ומסתנכרנת בין כל שרתי ה-Domain Controllers אשר חברים לאותו Domain. כברירת מחדל, תיקיית ה-SYSVOL כוללת מספר אובייקטים כגון: Active Directory, Group Policy ו-NETLOGON Folder.

בסביבה תקינה, תיקיית ה-SYSVOL וכל הקבצים שמאוחסנים בתוכה יהיו זהים בכל שרתי ה-DCs בארגון. אל תיקייה ה-SYSVOL, ניתן לגשת מכל תחנת קצה שחברה ב-Domain. כאשר יש שרת DC שכובה או שאין תקשורת אליו, כל תחנה שתנסה לגשת אל תיקיית ה-SYSVOL של אותו שרת תופנה באופן אוטומטי לתיקיית ה-SYSVOL של שרת DC אחר. בדרך כלל, תחנת הקצה תופנה לשרת ה-DC הקרוב ביותר לתחנה (מבחינה גאוגרפית). כמובן שהכל תלוי בהגדרות של טופולוגיית הסנכרון שהוגדר בארגון (Site And Services).

כיום ישנם שני סוגים של מנגנונים (אחד ישן ואחד חדש) האחראים על השכפול של תיקיית ה-SYSVOL בין שרתי ה-Domain Controllers, מנגנון השכפול הישן נקרא "File Replication Service (FRS)" ומנגנון השכפול החדש נקרא Distributed File System Replication (DFSR). חשוב לדעת שניתן לעבוד אך ורק עם מנגנון שכפול אחד, וכדי לעבור משיטת השכפול של FRS ל-DFSR נדרש לבצע מיגרציה מסודרת.



SYSVOL - Replication Services

Replication Services

כפי שציינתי קודם לכן, ישנם שני מנגנוני שכפול (FRS ו-DFSR) אשר ניתן להשתמש בהם בכדי לבצע סנכרון של תיקיית ה-SYSVOL בין שרתי ה-Domain Controllers שבארגון. וכעת אפרט על כל מנגנון בנפרד ולאחר מכן אערוך השוואה בין FRS ל-DFSR.

File Replication Service (FRS)

כברירת מחדל תיקיית ה-SYSVOL כוללת סקריפטים (Logon Script) ואת הגדרות מדיניות הארגון (GPO). במידה וה-Service של מנגנון השכפול אינו פעיל על אחד משרתי ה-Domain Controllers ובאותו DC ביצעתם מספר שינויים בהגדרות ה-GPO, Active Directory או כל דבר אחר אשר מאוחסן בתיקיית ה-SYSVOL המשותפת, השינויים לא יוכלו להשתכפל אל תיקיות ה-SYSVOL אשר נמצאות בשאר שרתי ה-DCs, וכנראה שחלק מהמשתמשים, המחשבים והשרתים בארגון לא יקבלו את ההגדרה החדשה אלא אם כן הם פונים אל ה-DC הספציפי אשר עליו השינויים בוצעו.

קובץ ההפעלה אשר מריץ את ה-Service של מנגנון השכפול נקרא "NTFRS.exe" והוא נמצא בתיקיית System32. כל שינוי שמנהל הרשת מבצע במדיניות (GPO) או בכל אובייקט הקשור לתיקיית ה-SYSVOL, באותו רגע ה-Service מבצע שכפול באופן מידי לשאר תיקיות ה-SYSVOL. בנוסף לכך, שירות זה יודע לפתור התנגשויות של קבצים ותיקיות בכדי שהמידע יהיה עקבי בין השרתים.

Distributed File System Replication (DFSR)

זוהי טופולוגיית שכפול חדישה יותר מ-FRS, טופולוגיה זו משתמשת באלגוריתם דחיסה בשם RDC, לצורך שכפול תיקיות וקבצים של תיקיות ה-SYSVOL בין שרתי ה-DCs בארגון.

Remote Differential Compression (RDC) •

הינו פרוטוקול המשמש ליעילות רבה בעדכון קבצים על גבי רשתות שרוחב הפס שלהן מוגבל, כמו כן אלגוריתם זה יודע לזהות שינויים של תיקיות או קבצים ולשכפל אותם לשאר שרתי ה-DCs הנוספים בארגון, מה שמאפשר ל-DFSR לשכפל דלתאות ולא לבצע סנכרון מלא בכל פעם שיש שינוי בתיקייה.

DFSR הינו Service ב-Windows אשר משמש לשכפול תיקיות וקבצים המאוחסנים בתיקיית ה-SYSVOL. במידה וה-Service אינו פעיל על אחד משרתי ה-DCs, השינויים אשר בוצעו באובייקטים הקשורים לתיקיית ה-SYSVOL לא יוכלו להשתכפל אל תיקיות ה-SYSVOL הנמצאות בשאר שרתי ה-DCs.

שירות ה-DFSR משתמש ב-RPC בכדי לתקשר בין השרתים ומבצע סנכרון של תיקייה ה-SYSVOL לפי נתיב, כברירת מחדל הנתיב של תיקיית ה-SYSVOL נמצא תחת: "C:\Windows" ולכן במידה ורוצים לשנות את מיקומה של התיקייה, ישנו תהליך מסודר אשר נדרש לבצע.

Replication Services - FRS vs DFSR

FRS - אינו תומך באופן מלא בסביבה שבה יש שרתי RODC ודבר זה עשוי לגרום לבעיות סנכרון נתונים בין תיקיות ה-SYSVOL בארגון.

DFSR - תומך באופן מלא בשכפול של תיקיית ה-SYSVOL גם בסביבות הכוללות שרתי RODC.

FRS - משתמש באלגוריתם כתיבה אחרונה מנצחת. כאשר המערכת מזהה שינוי בקובץ באחת מתיקיות SYSVOL, התיקייה שעליה התבצע השינוי האחרון הופכת לשרת הסמכותי ותשכפל את השינוי הקובץ לכל ה-DCs האחרים. זה לא משנה כמה השינוי הוא מינורי, תמיד תתבצע העתקה מלאה של הקובץ, מה שעשוי לגרום לבעיות בביצועים.

DFSR - מאפשר לשכפל את השינויים החלקיים (Delta) בקובץ באמצעות שכפול ברמת הבלוק. כלומר, כאשר ניצור קובץ חדש בתיקיית ה-SYSVOL בפעם הראשונה הקובץ ישוכפל במלואו לתיקיות ה-SYSVOL האחרות ובפעמים הבאות יבוצע סנכרון דלתאות של שינויים אחרונים.

FRS - אין מנגנון שידוע לתקן קבצים פגומים באופן אוטומטי.

DFSR - יש מנגנון שידוע לזהות ולתקן קבצים פגומים באופן אוטומטי.

FRS - אינה מדווחת על תקלות ולכן קשה מאוד להפיק דוחות ולאבחן תקלות במידת הצורך. שירות זה מתבסס רק על Event Viewer.

DFSR - תומך ביצירת דוחות ע"י ביצוע Health Check ומאפשר לייצא את אותם הדוחות בפורמט XML או HTML.

FRS - הינו פרוטוקול מיושן שלא היה מאפשר לתקן באגים באופן ידני ובנוסף לכך לא שוחררו עדכוני וינדוס שמתקנים את אותם הבאגים. פרוטוקולים מיושנים יכולים לגרום לאיומי אבטחה למערכות בארגון.

DFSR - כולל בתוכו המון שיפורים וגם בימים אלה ממשיכים להשקיע בפרוטוקול זה ומתבצעים בדיקות הגנה כנגד פגיעויות האבטחה של ה-Windows.

Domain Name System (DNS) in Active Directory

Domain Name System (DNS)

הינו פרוטוקול אשר מבצע מיפוי בין שמות של מחשבים ב-Domain לבין כתובות IP. כאשר נותנים שם למחשב ומחברים אותו ל-Domain, שרת ה-DNS יוצר רשומה חדשה של שם המחשב עם כתובת ה-IP המשוייכת לאותו מחשב.

כלומר שתפקידו העיקרי של שרת ה-DNS הוא לבצע תרגום משמות תחום (Domains) לכתובות IP. דבר זה מספק למנהל הרשת גמישות רבה בניהול המשאבים בארגון, מכיוון שבעזרת שרת ה-DNS ניתן להתחבר אל משאבי הרשת (לדוגמה: מחשבים \ שרתים \ אתרים) גם ע"י שם תחום וגם ע"י כתובת IP. שירות ה-DNS מותקן בצורה אוטומטית על כל שרת Domain Controller בארגון, מפני ששירות הינו חלק מהתקנת ה-Active Directory Domain Services.

DNS Forwarding

זהו תהליך המורכב ממספר שירותים אשר מבצעים הפניה של בקשות DNS משרת DNS אחד אל שרת DNS אחר. במידה ושרת ה-DNS מסוים מקבל מאחד המשתמשים בקשה לשאילתת DNS אשר אינה נמצאת באותו שרת, בעזרת DNS Forwarding מנהל הרשת יכול להגדיר לאיזה שרת DNS תופנה הבקשה.

סוגי Forwarders

- **Conditional Forwarders** - מבצע הפניות של בקשות DNS מ-Domain A אל שרת ה-DNS של Domain B. כלומר כאשר מגדירים הפנייה מסוג Conditional forwarders מדומיין Contoso.local אל שרת DNS שנמצא בדומיין Israel.local, משתמשים מדומיין Contoso.local יוכלו לגשת אל מחשבים הנמצאים בדומיין Israel.local ע"י שימוש בשם ה-DNS של המחשבים (FQDN). במידה ולא מוגדרת הפנייה של Conditional forwarders, הבקשה תשלח לשרתי ה-DNS החיצוניים שהוגדרו בארגון.
- **Forward Lookup Zone** - זהו ה-Zone הראשי של שרת ה-DNS אשר תחתיו נמצאים כל שאר ה-Zones מלבד Reverse lookup zone. תפקידו של ה-Zone הוא לקבל מהמשתמשים שאילתות DNS עם שמות מחשב ולהפנות אותם אל כתובות ה-IP המשוייכות אליהם.

DNS Zone

בשרת ה-DNS ישנה חלוקה מסויימת לאזורים אשר נקראים "DNS Zone". כל בקשה ששרת ה-DNS מקבל מהמשתמשים, מועברת אל ה-Zone המתאים על פי מה שהוגדר בשרת ה-DNS הראשי.

סוגי Zone

- Primary zone - זהו ה-Zone הראשי של הארגון אשר משמש כמקור מידע לכל שאר שרתי ה-DNS, ה-Primary zone הוא העתק של ה-"Zone Data" עם יכולת של קריאה וכתובה (read/write) ב-Zone. בכדי להוסיף או לערוך רשומות DNS, כל שינוי חייב להתבצע בתוך ה-Primary zone.
Zone Data - זה קובץ Text מקומי אשר נמצא על שרת ה-DNS תחת הנתוב: `"c:\windows\system32\dns"`
- Secondary zone - הינו Zone משני אשר מחזיק העתק של ה-Primary zone עם יכולת של קריאה בלבד (read-only). רשומות ה-DNS אשר נמצאות ב-Secondary zone, מתעדכנות מול ה-Primary zone אך עם זאת ב-Secondary zone לא ניתן לבצע שינויים ברשומות ה-DNS.
- Stub zone - הוא Zone אשר מכיל בתוכו העתק של רשומות DNS ספציפיות כגון: SOA, NS ו-A Records של שרתי ה-DNS הסמכותיים (Authoritative Servers), תפקידו של ה-Stub zone הוא להפנות בקשות DNS בין ארגונים שונים, כלומר לבצע הפניה של בקשות DNS מ-Domain A אל שרתי ה-DNS הסמכותיים של Domain B. ובכך משתמשים מ-Domain A יכולים לגשת אל משאבים אשר נמצאים ב-Domain B.
- Reverse lookup zone - הינו Zone אשר משמש להמרה של כתובות IP ל-Hostnames, כלומר שניתן לגלות שמות מחשבים (Hostnames) ב-Domain דרך כתובות ה-IP שלהם.

DNS Records (רשומות DNS)

ישנם מספר רשומות DNS אשר לכל רשומה יש תפקיד ייחודי

- **A Record**: רשומת מסוג "A" מורכבת משם וכתובת IP, תפקידה של רשומה זו היא לבצע תרגום בין שמות המחשבים ב-Domain לכתובות ה-IPv4 המשויות להם.
 - **CNAME Record**: רשומה שבעזרתה ניתן להעניק שמות נוספים לרשומת A Record. כלומר כאשר קיימת רשומת A Record עם שם וכתובת IP, ניתן ליצור רשומת CNAME עם שם אחר ולהגדיר שכל מי שפונה לרשומת ה-CNAME, ינותב בצורה אוטומטית אל רשומת ה-A Record.
 - **Mail Exchange (MX) Record**: זוהי הפניה אשר אחראית על הקישור בין הדומיין לבין שרת הדואר הארגוני. כאשר משתמש רוצה לשלוח מייל מדומיין "x.com" אל דומיין "y.co.il" (כלומר שליחת מייל בין שני שרתי דואר שונים) השולח מ-"x.com" בודק מול הדומיין "y.co.il" האם קיימת אצלו רשומה מסוג MX Record, במידה והרשומה אכן קיימת השולח יוכל לגלות מהי הכתובת של שרת הדואר החיצוני ולשלוח אליו את המייל.
 - **TXT Record**: היא רשומה שכל מטרתה היא לאמת את בעלות הדומיין. לדוגמה כאשר רוצים להגדיר בארגון את Microsoft365 כשרת דואר, מיקרוסופט מייצרת במיוחד בשבילנו רשומה ייחודית מסוג TXT אשר אותה צריך להוסיף בשרת ה-DNS שבו מנוהל ה-Domain ובכך מיקרוסופט מאמתת את בעלות הדומיין.
 - **Name Server (NS) Record**: רשומה זו מציינת את שרתי ה-DNS הסמכותיים בארגון. כלומר כל שרת DNS שנמצא ב-Domain, מופיע ב-DNS Zone כרשומת NS.
 - **Start Of Authority (SOA) Record**: זוהי רשומה ייחודית אשר קיימת בכל Zone של שרת DNS, כלומר שבכל Zone יכולה להיות רק רשומה אחת מסוג SOA אשר מציגה למנהל הרשת מידע אדמיניסטרטיבי חיוני על ה-Zone של שרת ה-DNS, מידע זה מסייע למנהל הרשת אבחן ולפתור תקלות בשרתי ה-DNS.
- רשומת SOA כוללת את הפרטים הבאים:
- מיהו שרת ה-DNS הראשי (Authoritative Server) אשר מנהל את שאר שרתי ה-DNS ב-Zone.
 - מי המנהל אשר אחראי על הדומיין.
 - כל כמה זמן שרתי ה-DNS המשניים מתעדכנים מול ה-Zone של שרת ה-DNS הראשי.
 - מהו זמן ההמתנה מהרגע ששרת DNS נכשל בקבלת עדכון מהשרת הראשי ועד הרגע שיוכל לבצע ניסיון נוסף לקבלת העדכון.
 - ישנם עוד מספר שדות נוספים כמו מספר סידורי, זמן ריענון וזמן תפוגה.
- **SRV Record**: מפרסם ב-Active Directory שירותים כגון Kerberos, ldap, Global Catalog ועם איזה פורט ניתן לגשת אל שירותים אלו. לדוגמה כאשר מצרפים מחשב חדש ל-Domain, המחשב מתשאל את שרת ה-DNS האם ל-Domain קיים שירות בשם "Ldap" אשר ניתן לפנות אליו בפורט 389.
 - **Pointer Record (PTR) Record**: הינה רשומה שתפקידה הוא לבצע מיפוי בין כתובות IP לשמות מחשב ב-Domain, כלומר שבעזרת רשומת PTR ניתן לגלות שמות מחשבים דרך כתובות ה-IP אשר משויכות להם (שזוהי פעולה הפוכה מרשומת "A Record").

LDAP (Lightweight Directory Access Protocol)

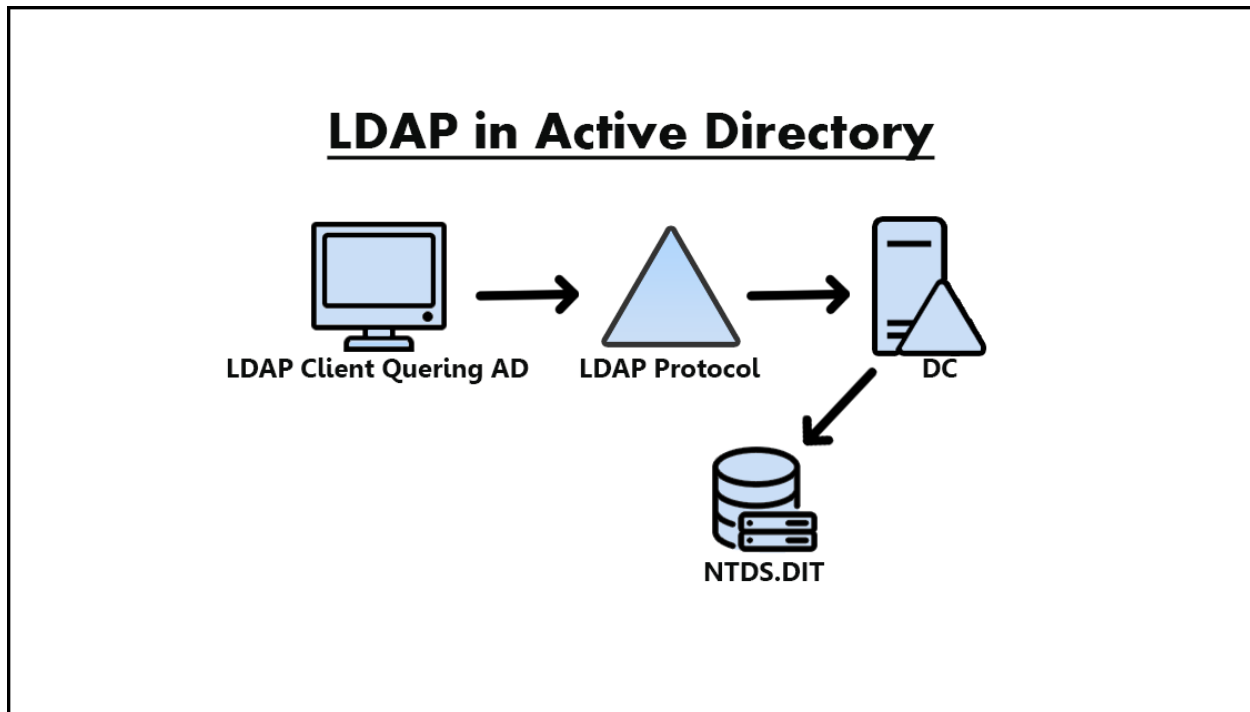
LDAP

הינו פרוטוקול המספק למשתמשים גישה אל ספריות מידע מרוחקות (כגון Active Directory) על גבי הרשת. בדרך כלל, משתמשים ב-LDAP כאשר רוצים לייצר ניהול אחיד של הרשאות המשתמשים בין שירותים שונים הקיימים בארגון, כמו לדוגמה Single Sign On (SSO) המאפשר למשתמשים להזדהות מול מספר מערכות צד שלישי עם אותו שם משתמש וסיסמה.

כלומר, שאין צורך להקים לכל עובד משתמש נוסף לכל מערכת, אלא ניתן לספק לעובד משתמש אחד ולתת לו הרשאת התחברות אל מספר מערכות צד שלישי. אפילו אם המערכות אינן חלק מהארגון, ע"י הגדרת LDAP ניתן לאפשר למשתמשים את הגישה אל מערכות אלו ובכך השימוש בפרוטוקול זה מספק למנהלי ה-IT ניהול אחיד של הרשאות המשתמשים בארגון.

LDAP in Active Directory

המערכת של ה-Active Directory מבוססת LDAP ולכן היא מורכבת מספרייה המאחסנת בתוכה משתמשים, מחשבים, קבוצות וסיסמאות הניתנים לשיתוף עם מכשירים אחרים ברשת. פרוטוקול ה-LDAP יודע לקשר בין ספרייה ה-AD לבין מערכות שונות. כברירת מחדל, כל בקשות האימות אשר נשלחות מה-Active Directory מגיעות אל שרת ה-LDAP כטקסט רגיל (Plain Text). דבר זה יוצר בעיית אבטחה מאוד גדולה בארגון. בכדי להתעלות על הבעיה, ניתן להיעזר בפרוטוקולים נוספים אשר משמשים להצפנת מידע כגון: "Transport Layer Security (TLS)" או "LDAP over SSL (LDAPS)".



Kerberos Authentication

Kerberos

זהו פרוטוקול המשמש לאימות זהויות (Authentication) והצפנה של תעבורה ברשת. יעודו של ה-Kerberos הוא למנוע דליפת מידע מהרשת הארגונית, בכך שהוא מצפין את התקשורת בין המחשבים לשרתים. כבר ב-Windows 2000 מיקרוסופט אימצה את פרוטוקול ה-Kerberos ועד היום זוהי שיטת האימות הזוהיות אשר מוגדרת כברירת מחזל ב-Active Directory.

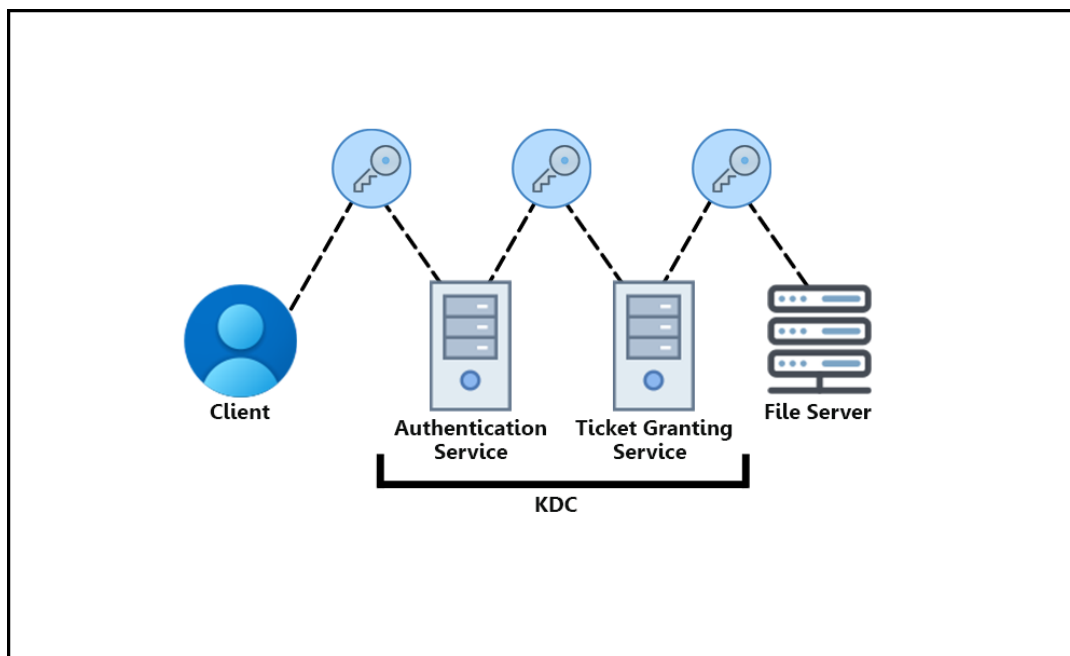
ה-Kerberos כולל בתוכו מנגנון בשם מרכז הפצת מפתחות (Key Distribution Center (KDC), אשר כלול ב-Active Directory Domain Services ואחראי לספק מפתחות למשתמשים ולמחשבים בכדי לאפשר להם לגשת אל שרתי היעד כגון: Application, SQL, File Server.

ה-KDC בנוי משני שירותים (Services) עיקריים AS + TGS:

1. **Authentication Service (AS)** – הינו שירות שתפקידו הוא לבצע את האימות הראשוני בין המחשב לשרת. כלומר כאשר משתמש מזין את פרטי ההתחברות שלו במחשב, שירות ה-AS מאמת את זהותו של המשתמש או המחשב מול ה-Active Directory ובמידה והאימות בוצע בהצלחה יונפק למשתמש כרטיס מסוג Ticket Granting Ticket (TGT) אשר מוכיח שהמשתמש עבר את האימות הראשוני ומאפשר לו להגיש בקשה להנפקת כרטיס משירות הנפקת הכרטיסיות (TGS) Granting Service בצורה מאובטחת.

2. **Ticket Granting Service (TGS)** – הינו שירות להנפקת כרטיסיות, TGS מנפיק כרטיס למשתמש או למחשב ובכך מאפשר לו להתחבר אל משאבי הרשת.

דוגמה למשאבים ברשת: File Server, SQL Server, Application Server, Web Server.



Kerberos Authentication Process in AD

תהליך האימות של ה-Kerberos כולל בתוכו שלושה גורמים מרכזיים:

1. משתמש או מחשב אשר מנסה לגשת אל אחד ממשאבי הרשת.
2. משאב הרשת שהמשתמש רוצה לגשת אליו.
3. מרכז הפצת המפתחות (KDC) אשר מותקן על שרת ה-Domain Controller.

שלב א' (שלב האימות):

המשתמש שולח בקשת אימות בשם "KRB_AS_REQ" אל ה-KDC אשר מותקן על ה-Domain Controller. בקשת האימות כוללת כמה פרטים ובניהם שם משתמש (Username) וחותרמת זמן נוכחי (Timestamp) עם ה-HASH שהוצפן ע"י סיסמת המשתמש.

ה-KDC מקבל את הבקשה ובכדי לאמת את זהותו של המשתמש הוא מנסה לפענח את הבקשה עם ה-HASH של סיסמת המשתמש אשר מאוחסנת ב-Active Directory, בנוסף לכך ה-KDC מוודא שהזמן הנוכחי אכן תואם לזמן שהבקשה הגיעה אליו.

אם שלב האימות עבר בהצלחה ה-KDC ינפיק עבור המשתמש כרטיס מוצפן מסוג Ticket Granting (TGT), שם הבקשה תשנה ל-"KRB_AS_REP" ותשלח ביחד עם כרטיס ה-TGT בחזרה אל המשתמש. במידה והמשתמש הצליח לפענח את ההצפנה בהצלחה, הוא יוכל להמשיך בתהליך.

חשוב לזכור שבמידה והסיסמה אכן תואמת אבל הזמן חורג וזוהה כלא תקין, כבר בשלב זה בקשת האימות לא תמשיך בתהליך מטעמי אבטחה ולכן סנכרון השעונים בארגון הוא נושא מאוד חשוב שצריך הקפיד עליו.

שלב ב' (הנפקת כרטיס מסוג TGS):

המשתמש שולח בקשה בשם "KRB_TGS_REQ" אל שירות ה-KDC עם כרטיס ה-TGT שהוענק לו בצירוף שם שרת היעד אשר אליו הוא רוצה לגשת, כל זאת בכדי לקבלת כרטיס משירות ה-Ticket Granting Service (TGS). במידה והבקשה אכן תקינה, ה-KDC מנפיק למשתמש כרטיס מסוג TGS, מצפין אותו עם מפתח סודי (Secret Key), משנה את שם הבקשה ל-"KRB_TGS_REP" ולבסוף הכרטיס נשלח אל המשתמש.

שלב ג' (הענקת גישה לשרת):

המשתמש שולח בקשה בשם "KRB_AP_REQ" אל משאב הרשת שאליו הוא רוצה לגשת. בבקשה זו המשתמש מצגי לשרת את כרטיס ה-TGS שקיבל מה-KDC, השרת שקיבל את הבקשה מפענח את הצפנת ה-TGS בעזרת סיסמת ה-HASH של המשתמש, שם הבקשה משתנה ל-"KRB_AP_REP" והמשתמש מקבל גישה לשרת.

Group Policy Objects (GPO)

Group Policy

זוהי תכונה (Feature) אשר קיימת ב-Windows, המאפשרת מגוון רחב של הגדרות מתקדמות שמנהלי הרשת יכולים להשתמש בהן בכדי לשלוט על סביבת העבודה של משתמשים ובחשבונות המחשבים ב- Active Directory. כלומר Group Policy מספק לאנשי ה-IT מקום מרכזי שדרכו ניתן לנהל הגדרות המדיניות של מערכות ההפעלה (Operating Systems), יישומים (Applications), מחשבים ומשתמשים.

כאשר יוצרים Policy חדש, ניתן לראות שיש יותר מ-1000 הגדרות זמינות אשר ניתן להחיל על המשתמשים והמחשבים בארגון ובעזרת הגדרות המדיניות ניתן להגביל את הגישה של המשתמשים אל מקומות מסוימים ברשת, לחסום את הגישה ל-CMD ול-PowerShell, לשלוט על הגדרות ה-Firewall במחשבים ועוד.

הגדרות אלו מסייעות לארגון להתגונן מפני הרבה תקיפות Cyber ולשפר משמעותית את אבטחת הרשת הארגונית בחברה, כל הגדרות המדיניות הן חלק מאובייקט שנקרא Group Policy Objects.

Group Policy Objects (GPO)

כברירת מחדל מערכת הפעלה של Windows כוללת בתוכה הגדרות GPO אשר מותאמות לכל גרסה של מערכות ההפעלה כגון: Windows 10\11, Windows Server 2012\2016\2022, כלומר שלכל מחשב או שרת ישנם הגדרות שונות של Group Policy, את הגדרות המדיניות ניתן להגדיר באופן ידני דרך "Group Policy Object Editor" של אותו מחשב ובכך להחיל את המדיניות על המחשב המקומי בלבד. בכדי להחיל הגדרות מדיניות של Group Policy על משתמשים או מחשבים ב-Domain, ניתן ליצור "Group Policy Objects" דרך ממשק גרפי שנקרא "Group Policy Management Console".

Group Policy Management Console (GPMC)

GPMC הינו ממשק גרפי אשר ניתן לגשת אליו דרך MMC. ממשק ה-GPMC מציג למנהלי הרשת את כל ה-Group Policy אשר קיימים בארגון לפי סדר היררכי, כולל כל הגדרות הנמצאות ב-Group Policy Objects. דרך ממשק ה-GPMC ניתן לנהל את המשתמשים והמחשבים אשר קיימים ב-Active Directory.

בעזרת GPMC ניתן לבצע את הפעולות הבאות:

- ליצור \ לערוך \ לבטל או למחוק הגדרות של Group Policy.
- להפיק דוחות מ-Group Policy.
- לשייך Group Policy ל-Site ל-Domain או ל-Organizational Unit (OU) מסוים.
- ביצוע אבחון דרך "Group Policy Modeling" המציג כיצד Group Policy מסוים ישפיע על אחד מהמשתמשים או מהמחשבים בארגון וזאת עוד לפני החלת המדיניות.
- גיבוי של כל ה-Group Policy Objects.

Default Group Policy Settings

כברירת מחדל, כאשר משייכים Group Policy ל-Domain או ל-Organizational Unit (OU), המדיניות (GPO) חלה על כל המשתמשים והמחשבים שנמצאים בקבוצת "Authenticated Users". כלומר, במידה ומשייכים GPO ל-OU מסוים, המדיניות תחול על כל המשתמשים והמחשבים הנמצאים באותו OU.

Authenticated Users - היא קבוצה ב-Active Directory המכילה את כל המחשבים והמשתמשים שקיימים ב-Domain. במידה ואינכם רוצים להחיל Group Policy על קבוצת "Authenticated Users" או במידה ואתם רוצים להחיל את Group Policy רק על כמה מחשבים מסוימים, ישנם שתי דרכים שבהן ניתן לסנן את אופן החלת המדיניות בארגון: Security Filtering או WMI Filtering.

GPO Security Filtering

מסנן האבטחה זוהי פונקציה ב-Active Directory, המאפשרת להחיל את Group Policy על קבוצות שונות ב-AD או על מספר מחשבים או משתמשים אשר ניתן להוסיף ל-Security Filtering באופן ידני. במידה ומחשב או משתמש נמצא ב-OU שעליו חל GPO אך אינו נמצא ב-Security Filtering, ה-GPO אינו יחול עליו ובכך מסנן האבטחה מאפשר לנו לבצע סינון של החלת המדיניות בארגון.

Windows Management Instrumentation (WMI) Filtering

WMI זוהי טכנולוגיה שפותחה ע"י Microsoft ומיועדת למערכות הפעלה של Windows, טכנולוגיה זו מסייעת לאנשי ה-IT לנטר את המערכות בארגון בכך שה-WMI אוסף את כל המידע לגבי החומרה של המחשבים. כלומר שבעזרת WMI אני יכול להריץ פקודות ב-PowerShell על מספר מחשבים ולקבל את כל הפרטים על החומרה שיש במחשבים כולל איזו מערכת הפעלה מותקנת עליהם, בנוסף לכך ניתן להריץ שאילתות של WMI ב-PowerShell עם תנאים מסוימים.

לדוגמה: "במידה ועל המחשב מותקנת מערכת הפעלה מסוג Windows 10, תבצע את הפעולה הבאה". כאשר יוצרים "WMI filter" דרך GPMC ניתן להגדיר המון סוגים של שאילתות WMI, כמו לדוגמה: שאילת המחפשת אך ורק מחשבים בעלי מערכת הפעלה של Windows 11 או שאילת אשר מחפשת מחשבים בעלי חומרה מסוימת. לאחר הגדרת שאילתת ה-WMI filter ניתן לשייך אותה ל-GPO, ואז ה-Group Policy יחול על כל מי שנמצא תחת "Security Filtering" וכל מי שעומד בתנאים של שאילתת ה-WMI.

כיצד ה-GPO עובד?

ישנו תהליך היררכי מסודר של החלת ה-Policy, הנקרא LSDOU.

תהליך ה-LSDOU מתבצע באופן הבא:

- L = Local Policy
- S = Site Policy
- D = Domain Policy
- OU = OU Policy

כלומר, ה-Policy של המחשב המקומי מושך את הגדרות ה-Policy מה-Site Policy, לאחר מכן מה-Domain Policy ולבסוף מה-OU Policy. במידה ויש סתירה בין ה-Policies, מי שיכריע יהיה ה-Policy אשר ביצע את השינוי האחרון. לדוגמה, אם ב-Site Policy יש הגדרה אשר מתנגשת עם הגדרה אחרת שביצעו ב-OU Policy (כלומר אותה הגדרה אך עם ערך שונה), מי שיכריע במצב כזה יהיה ה-OU Policy, מכיוון שהוא מבצע את ההגדרה לאחר ה-Site Policy. אז גם אם קיימת סתירה בין ה-Policies, ההגדרה האחרונה שבוצעה היא זו שתנצח.

Network Time Protocol (NTP) In Active Directory

“נדידת זמן” (Time Drift)

הינו מושג הבא לתאר סטייה בשעונים כאשר שרתים ותחנות קצה לא מקבלות עדכון כל מחזור זמן מסוים. ישנה חשיבות גבוהה לעדכון שעונים בארגון על מנת להבטיח פעילות תקינה של מערכות הארגון. וכאן נכנס לתמונה פרוטוקול ה-NTP שהוא חלק מתפקיד ה-PDC (אחד מתוך חמשת תפקידי ה-FSMO). שרת ה-DC המחזיק בתפקיד זה, הוא המקור הראשי בארגון אשר מולו כל שאר התחנות יסונכרו (“PDC operations masters”).

NTP (Network Time Protocol)

הינו פרוטוקול שאחראי על סנכרון הזמנים בין המחשבים והשרתים בארגון, כלומר שבעזרת פרוטוקול ה-NTP ניתן לוודא כי כל השעונים של המחשבים בארגון אכן מסונכרנים ומכוונים לאותה השעה וללא חריגות. חשוב מאוד להבין שסנכרון השעונים בארגון הינו דבר חשוב מאוד!

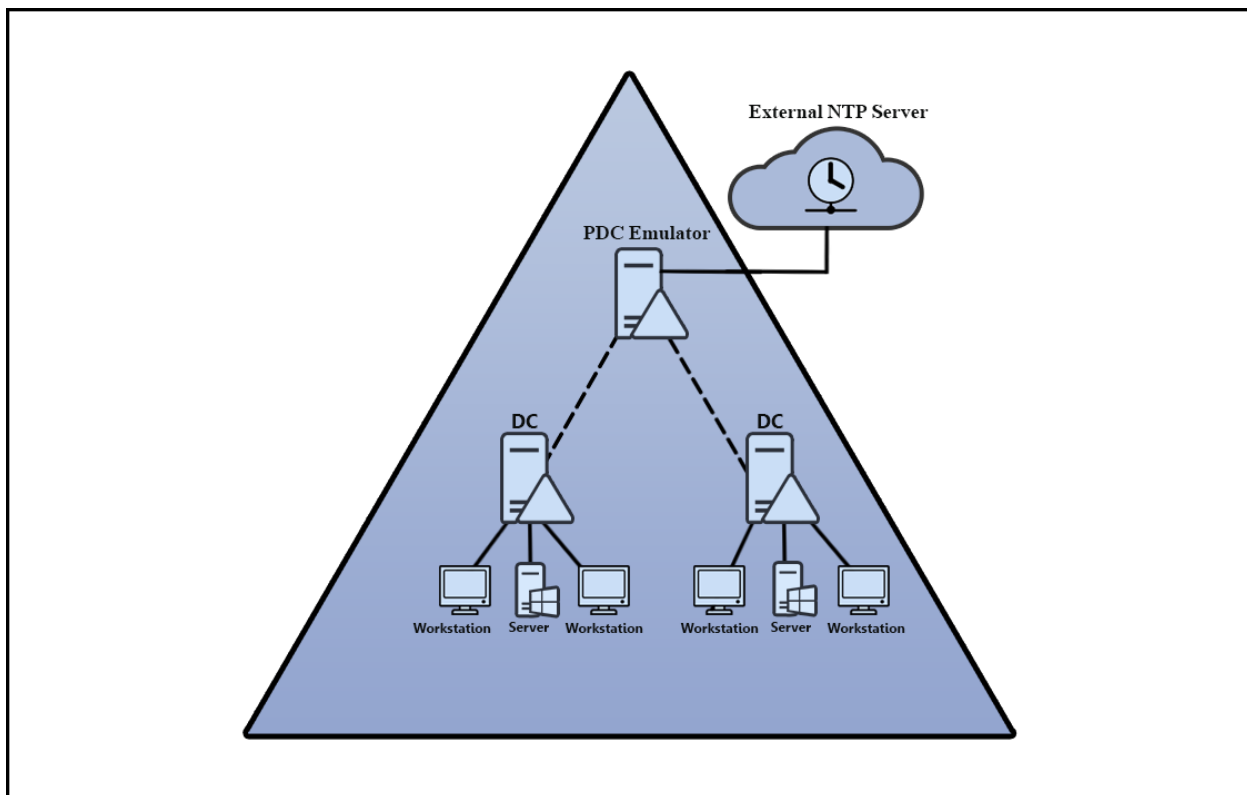
כאשר יש סטייה בשעונים, עלולות להיווצר הבעיות הבאות:

- בעיית רפליקציה בין שרתי DC - מצב של חוסר סנכרון מידע ואף איבוד מידע. “חותמת זמן” (Timestamp) הוא ערך המסייע לשרתי DCs לקבוע האם יש לבצע רפליקציה כאשר ה-Update Sequence Number (USN) זהה בין שני שרתים. כאשר חותמת הזמן משובשת, סנכרון המידע עלול להשתבש.
- Kerberos - שירות זה שאחראי על אימות הזהויות ב-Domain, מתבסס על פרוטוקול ה-NTP. כאשר שירות ה-Kerberos מנפיק “כרטיסים” (Tickets) כהרשאות גישה למשתמשים או לשירותים שונים בארגון, אותם כרטיסים מוגבלים בזמן ולכן חוסר סנכרון שעונים בין מערכות יכול להוביל לבעיות בהרשאות גישה.
- בעיות של יחסי אמון “Trust Relationship” - במצב שהשעונים אינם מסונכרנים כראוי אל מול ה-Domain Controller, עלולות להופיע תקלות מסוג Trust Relationship מספיק שלמחשב או לשרת ישנה חריגת זמן של יותר מ-5 דקות אל מול השעון של שרת ה-DC, שירות ה-Kerberos יזהה את אותו מחשב כתוקף ויוציא אותו מה-Domain, כל זאת בכדי למנוע התקפות מסוג “Replay Attacks”.

כיצד NTP עובד בסביבת AD?

שרת ה-Domain Controller הראשי של הארגון מתפקד כ-PDC Emulator ומסנכרן את השעון שלו מול מקור זמן אמין. כברירת מחדל במערכת ההפעלה של Windows ה-Time Server שמוגדר כמקור זמן אמין הינו "time.windows.com" שזהו שרת הזמן החיצוני של Microsoft.

1. שאר שרתי ה-Domain Controllers מסנכרנים את השעונים אל מול שרת ה-Primary Domain Controller (PDC).
2. כל המחשבים והשרתים החברים ב-Domain מסנכרנים את השעונים אל מול שרת ה-Domain Controller שהכי קרוב אליהם.
3. כברירת מחדל, כל מחשב או שרת בעל מערכת הפעלה מסוג Windows כולל בתוכו Service שנקרא Windows Time service (W32Time), שירות זה מסנכרן את התאריך והשעה של כל המחשבים אשר מנוהלים ב-Active Directory.



Key Management Services (KMS)

KMS

הינו שירות לניהול מפתחות בארגון. שירות זה, מבצע אקטיבציה למערכות ההפעלה של Windows המותקנות על מחשבים (Computers) ושרתים (Servers). כלומר במקום שנעבור בצורה ידנית על כל המחשבים והשרתים בארגון ונבצע להם אקטיבציה, ברגע שיש שרת KMS בארגון, האקטיבציה תבוצע בצורה אוטומטית על גבי הרשת הארגונית.

עוד ייתרון שיש ב-KMS הוא שניתן להטמיע אותו גם בסביבות מאובטחות בהן למחשבים ולשרתים אין גישה לרשת העולמית. אף על פי שהם אינם יכולים לתקשר מול שרתי Microsoft האקטיבציה מול שרת ה-KMS תתבצע בהצלחה, מכיוון שהאקטיבציה מתבצעת אך ורק ברשת המקומית בין שרת ה-KMS לבין המחשבים והשרתים.

עם זאת לשרת ה-KMS חייבת להיות גישה אל השרתים של Microsoft. כאשר רוצים להקים שרת KMS בארגון, ראשית צריך לרכוש מפתחות KMS מ-Microsoft.

סוגי מפתחות של KMS:

- Windows Client (10,11)
- Windows Server (2016-2022)
- Office LTSC 2021, Office 2019, and Office 2016 (including Project and Visio)

במידה ורוצים לבצע אקטיבציה גם למחשבים, לשרתים ולאופיס צריך לרכוש את כל שלושת סוגי הרישיונות מ-Microsoft. אך במידה ורוצים לאקטב רק שרתים, רוכשים רישיונות KMS רק של שרתים וכו'. את הרישיונות מזינים בתוך שרת ה-KMS ולאחר מכן הכלי יתחיל לבצע אקטיבציה על כל המחשבים והשרתים ב-Active Directory.

כאשר רוצים לבצע אקטיבציה גם למערכות Windows 10 וגם ל-11 Windows, מספיק לרכוש KMS Key של Windows 11 והוא ידאג לאקטב גם את מערכות ההפעלה של Windows 10, אותו הדבר תקף גם לשרתים.

כלומר, שבמידה ורוכשים רישיון KMS למערכת הפעלה מסוימת לדוגמה Windows Server 2022, תתבצע אקטיבציה גם למערכות ההפעלה הקודמות של אותה הגרסה, כגון: 2016, 2019. וזאת בתנאי שמערכת הפעלה אכן נתמכת ע"י Microsoft. שירות ה-KMS הינו Role ב-Windows Server הנקרא (Volume Activation Services) אשר ניתן להתקין אותו בכל שרת בארגון.

ניתן להגדיר את Volume Activation בשני תצורות שונות:

1. **Key Management Service (KMS)** - מבצע אקטיבציה למערכות הפעלה של Windows ולתוכנות Office בתוך הרשת הארגונית. שירות ה-KMS דורש מספר מינימלי של פניות בכדי להתחיל לבצע את האקטיבציה למערכות בארגון. המספר המינימלי הוא: 25 מחשבים ו-5 שרתים, כלומר שירות ה-KMS לא יבצע אקטיבציה לשום מחשב עד שהארגון יעמוד בדרישות האקטיבציה של ה-KMS.

דרישות אקטיבציה של KMS:

- **מחשבים** - בכדי ששירות ה-KMS יבצע אקטיבציה למחשבים, צריך שיהיו לפחות 25 פניות אל שירות ה-KMS ממחשבים אשר אינם מאוקטבים.
- **שרתים** - בכדי ששירות ה-KMS יבצע אקטיבציה לשרתים, צריך שיהיו לפחות 5 פניות אל שירות ה-KMS ממחשבים אשר אינם מאוקטבים.

כל אקטיבציה אשר תבצע ע"י שירות ה-KMS תקפה ל-180 יום בלבד, כברירת מחדל כל 7 ימים המחשב או השרת מתקשרים מול שירות ה-KMS בפורט 1688 וזאת בכדי לחדש את האקטיבציה במידה והיא הסתיימה. מחשב שקיבל אקטיבציה פעם אחת ולא תקשר מול שירות ה-KMS בכדי לבצע חידוש לאקטיבציה, הרישיון של אותו מחשב יחולק למחשב אחר.

2. **Active Directory-Based Activation (ADBA)** - מבצע אקטיבציה למערכות הפעלה של Windows ולתוכנות Office בתוך הרשת הארגונית. שימוש בתצורה זו מהווה יציבות רבה יותר מאשר השימוש ב-KMS, הגדרה זו הינה משולבת עם ה-Active Directory ולכן תבצע אקטיבציה באופן אוטומטי לכל מחשב המחובר ל-Domain.

בניגוד להגדרת ה-KMS, כאשר מגדירים את ה-Volume Activation כתצורת ADBA אין דרישה למספר מינימלי של פניות. כלומר שתבוצע אקטיבציה מיידית לכל מחשב או שרת החבר לדומיין. ADBA תומך באקטיבציה של מערכות הפעלה Windows 8 או Windows Server 2012 ומעלה.

במידה והינכם רוצים לבצע אקטיבציה למערכות ישנות יותר (Windows 7, Windows Server 2008 R2), תצטרכו להגדיר בארגונכם את תצורת ה-KMS. שימו לב כי אין דבר המונע מכם מלהגדיר את שני התצורות לעבוד במקביל ובכך תבצע בארגונכם אקטיבציה לכל מערכות הפעלה של וינדוס.

