מושגים

active directory

טכנולוגיה שפותחה על ידי Microsoft המספקת שירותי רשת. הוצגה לראשונה בשנת 1999 בגרסת Windows Server 2000. בגרסא Windows Server 2008 R2 שונה השם להיות Active Directory Domain Services או בקצרה ADDS.

שירותי רשת

- Directory Services המבוססים על LDAP
- אימות באמצעות Kerberos
- שירותי DNS
- SSO

אובייקט

כל רכיב המנוהל על ידי AD נקרא אובייקט. לכל אובייקט יש Attributes שהם למעשה שדות המציינים איזה מידע מוכל בתוך האובייקט. ה Database של ה AD נמצא בשרת הנקרא Domain Controller או בקצרה DC. כאשר בונים ארכיטקטורה מבוזרת של מספר שרתי DC, ניתן להגדיר שהם יסנכרנו ביניהם אוטומטית באמצעות מנגנון Replication.

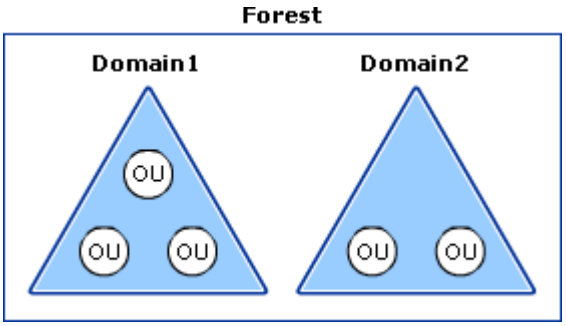
אובייקט יכול להיות אחד מהבאים, כאשר ישנה חלוקה לשלוש קבוצות עיקריות:

- משאבים
  - מדפסת
  - מחשב
  - שירות
- שירותים
- משתמשים
  - משתמש
  - קבוצה
  - חשבון משתמש

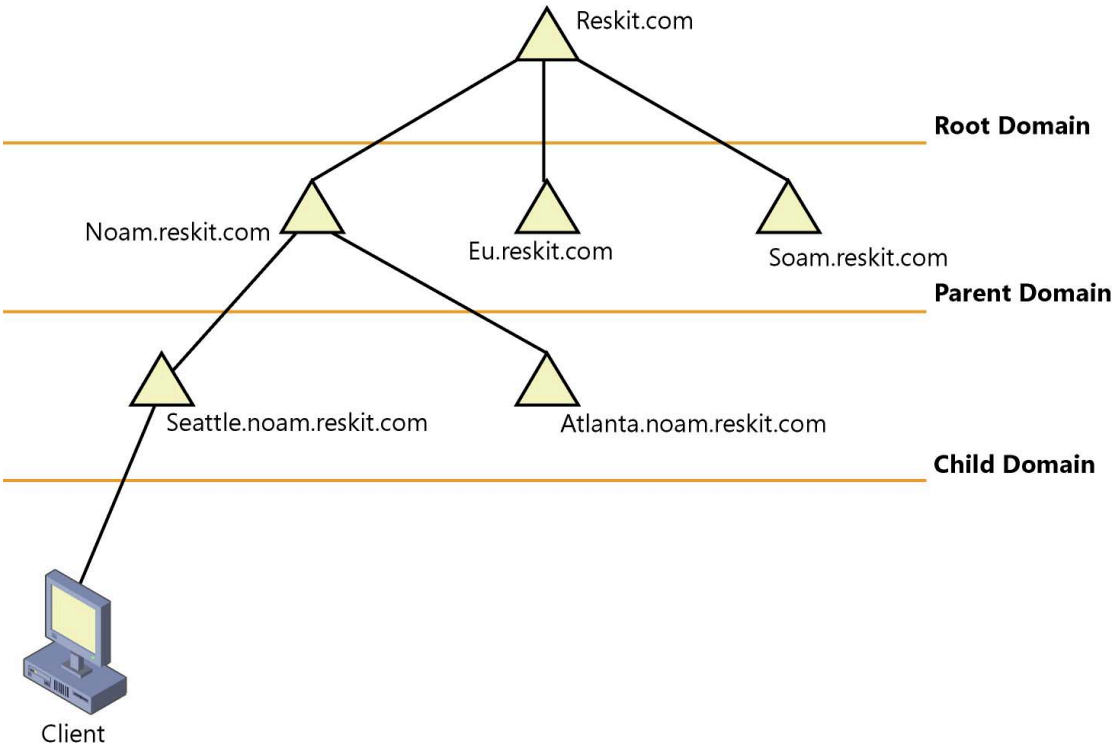
מבנה ה AD

מערכת AD בנויה בצורה היררכית כך שבראש ההיררכיה יש אובייקט הנקרא forest, תחתיו יש tree המורכב מ Domain-ים שגם בהם ניתן לייצר היררכיה של domain אב ו domain בן וכן הלאה. תחת כל Domain יש אוסף של אובייקטים המחולקים לקבוצות הנקראות Organizational Unit או בקצרה OU. ה OU משמש לחלוקת הרשת לאזורים גיאוגרפיים ולמחלקות ארגוניות. ניתן להגדיר מספר OU בתוך OU. לכל אובייקט יש מזהה ייחודי הנקרא GUID.

תרשים המתאר היחס בין forest ו domain:



תרשים המתאר היררכיה של domain:



site

כל סגמנט IP ברשת מוגדר ב site. קיימת הגדרה של site coverage המאפשרת להגדיר site בתוך site כך שכאשר אוביקט לא נמצא ב site שלי אני אחפש אותו ב site שמעלי.

LDAP

Light Weight Directory Access Protocol.

SSO

.Single Sign On

Kerberos

ראה בהרחבה.

kerberos הינו מנגנון אימות והצפנה של תחנות ושרתים אל מול שירותי רשת כגון שרתי קבצים, WEB, AD וכו'. האימות מבוצע מול שרת שלישי שגם התחנה וגם השרת שמריץ את שירות הרשת הרצוי סומכים עליו. שרת זה נקרא KDC (ר"ת Key Distribution Center) והוא רץ פיזית רק בשרתי ה DC. ה KDC מורכב משני תתי שרתים:

AS - ר"ת Authentication Server. אחראי על אימות התחנה המבקשת. במידה ותקין מייצר עבור התחנה TGT (ר"ת Ticket Granting Ticket) שמאשר שביצעה בהצלחה אימות מול ה KDC. התחנה צריכה TGT עבור כל domain ממנו היא רוצה שירות.

TGS - ר"ת Ticket Granting Server. לאחר שתחנה קיבלה TGT, היא יכולה לפנות ל TGS שייצר עבורה service ticket המתאים ספציפית עבור השירות אליו היא מעוניינת לפנות. שים לב ש TGS לא מבצע אף פנייה לשרת איתו התחנה מעוניינת לתקשר אלא מייצר את ה service ticket עצמאית.

התחנה שומרת ב cache את כל ה ticket-ים שקיבלה (הן TGT והן service ticket).

kerberos מגדיר שני סוגי חשבונות:

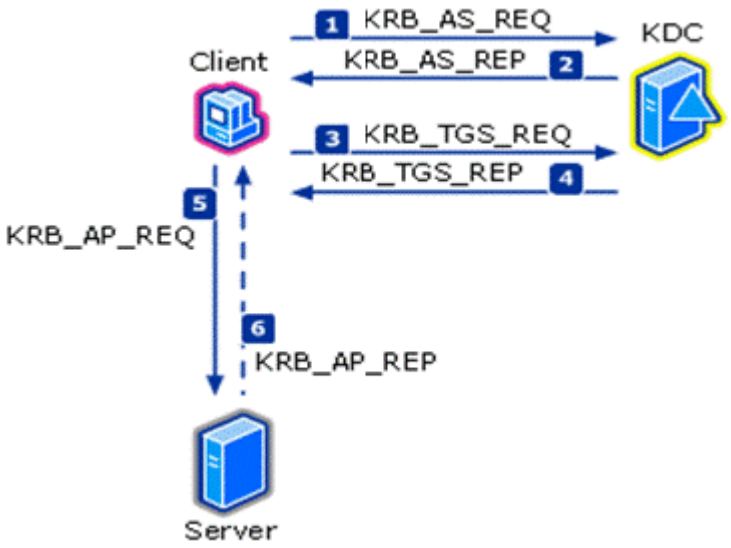
UPN - ר"ת user principal name. מזהה ייחודי של user account.

SPN - ר"ת service principal name. כל שירות שרץ בשרת מסוים ונדרש לבצע עבורו תהליך kerberos, צריך להיות מזוהה חד ערכית על ידי SPN ייחודי.

רק ל user account יש UPN ועליו להיות ייחודי ברמת ה forest. תהליך ה KDC מבצע את אימות המשתמש באמצעות ה UPN. אם מוצא יותר מחשבון משתמש אחד עם אותו UPN ההזדהות נכשלת. המבנה של UPN הוא user@contoso.com.

גם SPN חייב להיות ייחודי ברמת ה forest והוא מוגדר אוטומטית עבור computer account. ניתן לשייך SPN גם ל user accounts. מתי נעשה זאת? לכל שירות שנדרש לרוץ במחשב נדרש SPN ייעודי. שירותים לדוגמא הם: CIFS, LDAP, AD Replication, FRS וכו'.

להלן תיאור כללי של תהליך אימות באמצעות kerberose:



הסבר לגבי התהליך הנ"ל:

1. תחנת הקצה מייצרת בקשה ל KDC לקבלת TGT. הבקשה מוצפנת באמצעות הסיסמא של ה user account. הבקשה כוללת את ה UPN של התחנה והשעה של התחנה.
2. ה KDC פותח את ההצפנה כיוון שמכיר את הסיסמא של התחנה. כעת מבוצעת בדיקה של השעה ובמידה ויש פער של 5 דקות בין השעון של התחנה לשעון של KDC, הבקשה נדחית. במידה ותקין, מייצר עבור התחנה TGT ושולח אליה. בנוסף הוא מייצר עבור התחנה TGT session key שמשמש אותה בעת פנייה לקבלת service ticket.
3. התחנה מעבירה ל KDC את ה TGT שקיבלה בשלב הקודם ואת ה SPN של השירות בו היא מעוניינת ומבקשת service ticket שיאפשר לה לפנות לשירות. המידע מוצפן באמצעות ה TGT session key שהתקבל בשלב הקודם.
4. ה KDC פותח את ההצפנה באמצעות ה TGT session key ומוודא שאכן ה TGT שבבקשה מתאים ל TGT service key. בנוסף, מבוצעת שוב בדיקת שעון. כעת ה KDC מבצע שאילתת LDAP עבור ה SPN הרצוי ומייצר service session key שבו ישתמשו התחנה והשרת בתהליך התקשורת ביניהם. השלב האחרון הינו יצירת ה service ticket עצמו שמכיל את הפרטים הבאים: ערך ה service session key ומידע נוסף הנקרא PAC ר"ת Priviledged Attribute Certificate.
5. התחנה פונה לשרת ומעבירה אליו את ה service ticket שקיבלה מ KDC.
6. לאחר שהשרת מאמת את התחנה באמצעות ה service ticket הוא מבצע בדיקה נוספת מול ה DC באמצעות NetLogon ש PAC אכן חוקי.

לסיכום, ה KDC מהווה שרת צד שלישי המוסכם על שני הצדדים כדי לאפשר תקשורת מוצפנת ומאומתת.

קיימת אפשרות לבצע kerberose delegation. הכוונה היא לבקש משרת אחר שיבצע את תהליך ה

kerberose עבורי. הנ"ל נפוץ כאשר הלקוח פונה לשרת WEB שכדי לשרת את הלקוח נדרש לבצע פנייה לשרת DB. הפנייה לשרת ה DB דורשת גם היא תהליך kerberose וניתן להגדיר לשרת ה WEB שיבצע עבור הלקוח תהליך kerberose מול ה DB וכך ניתן לממש מנגנון מידור ב DB.

איך נבחר שרת ה KDC?

מה נדרש כדי שתהליך ה kerberos יפעל כראוי:

- ההצפנה והפענוח מבוצע באמצעות שמות המשתמש והסיסמא המוגדרים ב AD. נדרשת רפליקציה תקינה של AD וסיסמאות.
- נדרשת תשתית DNS ו NetBIOS תקינה כדי לבצע name resolution של KDC והשירות הנדרש. הרשומות הנדרשות הן מסוג SRV הנקראות kerberos_ והן נדרשות להיות תחת שני ה SND domain הבאים: tcp_ ו udp_.
- כל המכונות המעורבות בתהליך ה kerberos נדרשות להיות עם הפרש שעון שלא עולה על 5 דקות.
- פורטים 88 udp ו 88 tcp צריכים להיות פתוחים בין התחנות ושרתי ה DC.
- שרת ה KDC לא זורק הודעות UDP שבוצע להם fragmentation ברשת. ניתן להכריח את ה KDC לעבוד ב TCP בלבד באופן הבא.
- ה KDC מבצע שאילתת LDAP כדי למצוא את ה SPN של השירות אותו התחנה מחפשת. במידה ויש שני שירותים עם אותו SPN תרשם הודעת שגיאה ב DC שביצע את השאילתא בפועל.

istg

אחד ה DC-ים בכל domain נבחר להחזיק את המידע לגבי טופולוגיית ה site-ים ב domain.

GPO

Group Policy היא תכונה של מערכות הפעלה השייכות למשפחת NT 5.0 מדיניות זו מאפשרת לנהל קבוצות של מחשבים על פי מדיניות הנקבעת בידי מנהל המחשוב ומוחלת על המחשבים המנוהלים. המדיניות הנאכפת על המחשב קובעת הגבלות ואפשרויות שימוש במחשב (לדוגמה: מניעת שינוי השעה בשעון, הגבלה של סמלים בלוח הבקרה, הגבלות על שינוי תיקיות במחשב ועוד).

global catalog

עקרונית, כדי למצוא אובייקט הנמצא ב domain אחר, נדרש לעבור סדרתית על כל ה DC-ים עד למציאת האובייקט הרצוי. כדי להאיץ את החיפוש, מגדירים בכל forest שרת DC אחד או יותר שתפקידו להחזיק מידע לגבי כל ה domain-ים ב forest כאשר כולם מסונכרנים ומחזיקים מידע זהה. תפקיד זה נקרא global catalog. שרת DC המשמש כ global catalog מחזיק עבור ה

domain שלו DB מלא ועבור domain-ים אחרים רק מידע חלקי המכיל רק את ה attributes של האובייקטים ולא את כל ה DB-ים. מידע של שאר ה domain-ים זמין עבורו רק עבור גישות read only. המטרה בבניית global catalog היא שכאשר מבוצע חיפוש על אובייקט ב forest, יהיה מקום מרכזי שהחיפוש יתחיל בו והוא יציין באיזה domain האובייקט נמצא. כאמור, ייתכן והאובייקט קיים ב forest אבל ה global catalog לא ימצא אותו כי רק חלק מהמידע נמצא אצלו. מייקרוסופט בנו רשימת ברירת מחדל ש global catalog מקבל הנקראת PAS ר"ת partial attribute set. ניתן להגדיר מספר שרתי DC כ global catalog ב domain.

FSMO

לרוב, כאשר מבצעים פעולה מסוימת ב domain, ניתן לבצע אותה בכל אחד משרתי ה DC והמידע מרופלק לכל האחרים כיצד? אולם, ישנן פעולות שחייבים לבצע דווקא ב DC מסוים כיוון שהוא המחזיק בתפקיד זה. תפקידים אלו מכונים FSMO ר"ת של Flexible Single Master Operationsקיימים חמישה תפקידים כאלו, כאשר כל אחד מהם מחויב להיות על DC יחיד ברמת ה forest או ברמת ה domain. קישור למסמך של מייקרוסופט בנושא best practice לתכנון AD.

להלן חמשת התפקידים:

1. schema master

יחיד ב forest. אחראי על עדכונים ושינויים של הסכימה. הסכימה מכילה את ההגדרות והמבנה של כל האובייקטים ב forest אך לא מכיל את המידע עצמו. זהו למעשה ה meta data של כלל האובייקטים. הסכימה מרופלקת לכל ה DC-ים ב forest. כל כמה זמן?

2. domain naming master

יחיד ב forest. אחראי על הוספה או הסרה של domain-ים ל forest.

3. primary DC Emulator , PDC

יחיד ב domain. ה DC הראשון שהוקם ב domain. ניתן להעביר את התפקיד ל DC אחר על ידי ביצוע promote.

אחראי על מספר תפקידים:

- מכיל את ה DB של כל המשתמשים וסיסמאות בגישת RW. המידע מרופלק לכל שאר ה DC-ים אך להם יש הרשאות RO בלבד.
- מספק שירותי שעון לכל ה DC-ים ב domain.
- רפליקציה של מידע לשאר ה DC-ים. יפורט בהמשך.
- כאשר משתמש מבצע שינוי סיסמא השינוי מתבצע ב DC אליו המשתמש מחובר ו DC זה מעדכן את ה PDC. מידע זה מרופלק לכל ה DC-ים ב domain.
- עריכת GPO מבוצעת ב PDC. מידע זה מרופלק לכל ה DC-ים ב domain.
- מחזיק תמונה עדכנית של namespace (לאיזה שרת להפנות כל site). מידע זה מרופלק

לכל ה DC-ים ב domain.

- משמש לתמיכה לאחור בתחנות קצה ושרתים שמריצים גרסת windows ישנה כגון winNT.

4. infrastructure master

יחיד ב domain. אחראי לעדכן את השינויים באובייקטים שהוזזו או נמחקו ב domain בשאר ה domain-ים האחרים וזאת כדי שיעדכנו את ה SID של האוביקט.

5. relative ID master

יחיד ב doamin. כדי ליצור SID ר"ת Security ID נדרש RID ר"ת Relative ID ו Domain ID. שרת ה RID master אחראי לחלק תחומי RID לכל DC כדי שיוכל ליצור SID נדרשים.

bridgehead

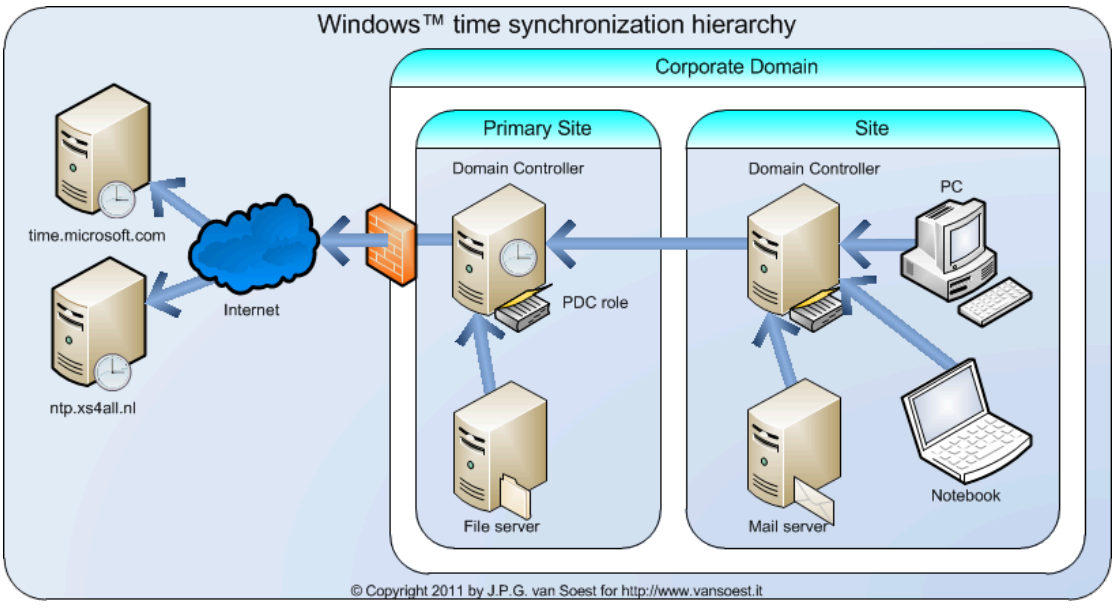
המידע שמחזיק DC מחולק ל partitions. כל partition מרופלק באופן עצמאי לשאר ה DC-ים. רפליקציה בתוך ה site מבוצע על פי intra site link ורפליקציה ל DC-ים מחוץ ל site מבוצעת על ידי DC המחזיק בתפקיד ה bridgehead. גם קבלת מידע מ site אחרים מתבצע דרך ה bridgehead.

kdc service

service שרץ ב DC שתפקידו לאמת משתמשים המבצעים logon לרשת.

סנכרון זמנים

להלן תרשים המתאר את אופן סנכרון הזמנים:



אופן פעולה

כל ה DC-ים באותו ה domain מחזיקים DB אחד מסונכרן של כל האובייקטים ב domain. לכל ה DC-ים יש הרשאות קריאה וכתיבה ל DB של ה domain שלהם.

FRS

ר"ת File Replication Service. מערכת שתפקידה לסנכרן מספר תיקיות הנמצאות בשרתים שונים ברשת כך שכל שינוי של קובץ בשרת א' מועבר מיידית לשאר השרתים אליהם מוגדר סנכרון. הנ"ל תקף גם כאשר השינוי נובע מסנכרון של שרת אחר. כלומר, נניח תצורה בה מוגדר לשרת A לסנכרן את שרת B ולשרת B מוגדר לסנכרן את שרת C. כאשר יהיה שינוי באחד הקבצים של שרת A, הוא יעדכן את שרת B שבתורו יעדכן את שרת C.

הנ"ל משמש לסנכרון תקיית SYSVOL המשמשת את שרתי ה DC לשמירת מידע וכך שומרת על סנכרון בין כל ה DC-ים. תהליך זה נקרא גם AD Replication או DC Promo.

קיים FRS Database שמכיל מידע לגבי העדכניות של כל אחד מהקבצים. לכל קובץ מוגדר file version שמשתנה על ידי השרת בו בוצע שינוי לקובץ.

הערות:

- יש לוודא כי הפרש השעון בין שרתים שנדרש לסנכרן ביניהם אינו עולה על 30 דקות

DFS

ר"ת Distributed File System. מאפשר למנהל הרשת ליצור שם אחד, namespace, המסתיר מאחוריו מספר shared folders הממוקמות בשרתים שונים, כאשר הלקוח יקבל שירות מהשרת ה"קרוב" אליו ביותר.

מושגים:

- root

root server / root server - שרת פיזי המארח את ה namespace. ניתן להגדיר מספר שרתים כאלה.

- link

- link target

ה metadata של ה DFS מכיל את רשימת השרתים, התקיות, namespace, הגדרות סנכרון בין שרתים וכו'. מידע זה נשמר ב AD. אחת לפרק זמן, כל שרת DFS פונה ל Primary DC לקבלת מידע זה ושמירתו בזיכרון ה RAM שלו. מידע זה מסונכרן בין כל שרתי ה DC באמצעות AD Replication (שמשתמש ב FRS).

הערות:

- נדרש לאפשר ב AD את האופציה bridge all site links. הגדרה זו מאפשרת ל DFS להשתמש בעלויות המרחקים בין site-ים שונים שהוגדרו ב AD.

ADFS

ר"ת AD Federation Services.

מבוא

המטרה - גישה למשאבים (אתר, אפליקציה, קבצים וכו') הנמצאים בארגון אחר.

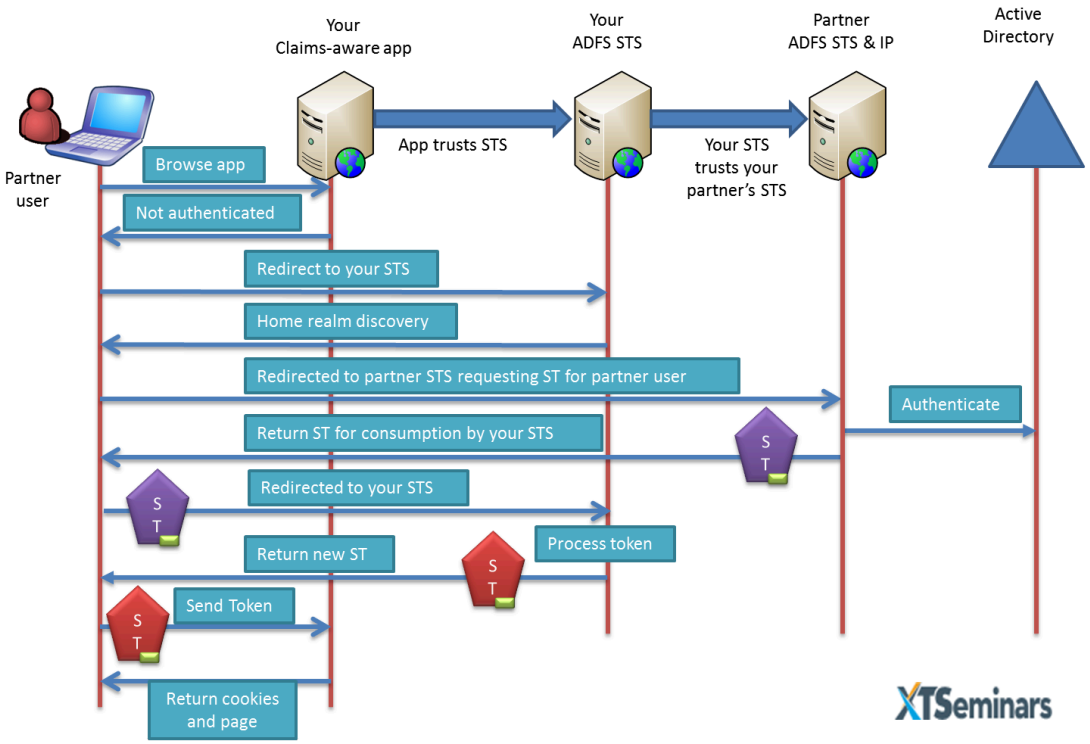
הרעיון - שיתוף נתוני זהות הרלוונטיים לטובת גישה לשירות הרצוי בלבד.

עקרונות בסיסיים:

- זיהוי, אימות והגדרת הרשאות הלקוח מתבצע בארגון שלו
- הארגון המספק את השירות סומך על הזיהוי שהתבצע בארגון השני
- המשאבים אליהם ניגשים חייבים לתמוך ב ADFS
  - דוגמאות לאפליקציות תומכות בתקן: sharepoint 2010, Citrix, וכו'
- המשתמש נדרש ל Browser התומך ב Cookie ו JavaScript
- ADFS הינו יישום של שני תקנים סטנדרטיים - WS-Federation Passive Requestor Profile ו SAML

אופן פעולה

נתוני הזהות המועברים לארגון המספק את השירות נקראים claims (בעברית "תביעה"). בגין נתונים אלו, המשתמש דורש גישה למשאב הנמצא בארגון השני. האפליקציה, שהגדירה מראש איזה claims נדרשים, מוודאת כי אכן הבקשה תקינה ומספקת את השירות.



רכיבים

ADFS Server עבור Accounts

ADFS Server עבור Resource

Federation Services Proxy עבור Account

Federation Services Proxy עבור Resource

ADDS Server

מה מכיל ה claim?

מידע לגבי המשתמש - קבוצות, הרשאות, תעודות דיגיטאליות, וכו'

מהו Cookie?

מידע שהאתר שומר ב Client. ניתן להגדיר האם להסכים לקבל ואם כן לכמה זמן יישמר.

מה מכיל ה Cookie?

מידע לגבי authentication שביצע המשתמש (למניעת הזדהות מחדש), וכו'.

מהו תקן SAML?

להשלים.

ההבדל לעומת forest trust

למה לא להשתמש ב forest trust?

תשובה - הייעוד של trust הוא כאשר מעוניינים ברמת שיתוף הדוקה יותר בין הארגונים, ולכל סוגי האפליקציות. למשל, במתאר של מיזוג חברות.

פורטים בשימוש

משתמש בפורטים סטנדרטיים - 53, 80, 443, 25