TYÖKALUJA VANHENTUEIDEN KÄYTTÄJÄ- JA TIETO-KONETILIEN LÖYTÄMISEEN JA POISTAMISEEN ACTIVE DIRECTORYSSA

Kari Lintunen

Tietojenkäsittelyn koulutusohjelma
huhtikuu 2006
Työn ohjaaja: Harri Hakonen

TAMPERE 2006
Tekijä: Kari Lintunen

Koulutusohjelma: Tietojenkäsittely/Tietoverkkopalvelut

Tutkintotyön nimi: Työkaluja vanhentuneiden käyttäjä- ja tietokonetilien löytämiseen ja poistamiseen Active Directoryssa

Työn valmistumis- kuukausi ja -vuosi: 04/2006

Työn ohjaaja: Harri Hakonen

Sivumäärä: 52

TIIVISTELMÄ


Tavoitteena oli saada vastaus seuraaviin kysymyksiin: mitä työkaluja on olemassa vanhentuneiden käyttäjä- ja tietokonetilien löytämiseen ja poistamiseen, ja onko ylipäätään olemassa yhtään hyvää työkalua tähän tarkoituksseen.


Tutkimuksen työkaluja voidaan mahdollisesti hyödyntää asiakasyritysten palvelimilla. Jokainen ympäristö on kuitenkin erilainen. Ylläpitäjän tulee arvioida tarkasti hyöty- ja haitantanäkökohdat, jos halutaan käyttää ulkopuolisten valmistajien ohjelmia Active Directoryn hallinnassa.

Avainsanat:
- Active Directory
- Hakemistopalvelu
- Virtuaalitietokone
- Windows-verkot
ABSTRACT

This study deals with finding and deleting outdated user- and computer accounts in Active Directory. I found the subject for this study during my practical training at Neuvos Tietojärjestelmät. Sometimes at work I have found outdated objects in Active Directory, both in Windows 2000 and 2003 environments. It came into my mind to look for tools for finding and deleting outdated accounts.

In Active Directory, you don’t see when users’ passwords will expire, nor when a computer has last authenticated itself with Domain Controller. Tools that are being compared in this study help administrators to solve these things. Being compared there’s one commercial program and two programs that are freeware. Furthermore, Windows 2003 commands for modifying objects were also studied.

The aim for this study was to clarify the following matters: what kinds of tools are there for finding and deleting outdated user- and computer accounts and are there any good ones in the first place.

For this study, a virtual test environment was created using Microsoft Virtual PC 2004. On this environment, Microsoft 2000 Server and Active Directory were installed. These were equivalent to customer’s environment. Virtual user- and computer accounts were created. The virtual Active Directory simulated the real Active Directory. The programs being compared on this study were installed on the virtual server. After the comparison, one program was installed also on the customer’s server. A separate virtual environment was created for testing Windows 2003 commands.

Tools being studied in this thesis may possibly be used on customer’s servers. However, every environment is different. The administrator must carefully evaluate all advantages and disadvantages when considering using third-party programs for managing Active Directory.

Keywords

Active Directory
Directory service
Virtual computer
Windows networks
Sisällysluettelo

1 TAUSTAA ..............................................................................................................................6
  1.1 Toimeksiantaja .................................................................................................................6
  1.2 Asiakasyrityksen järjestelmät ...........................................................................................6
  1.3 Etähallinta .........................................................................................................................7
  1.4 Ristiriidat ..........................................................................................................................8

2 TESTAUSYMPÄRISTÖ.....................................................................................................10
  2.1 Microsoft Virtual PC 2004 .............................................................................................10
  2.2 Virtuaalisen ympäristön luominen .................................................................................11

3 ACTIVE DIRECTORY ......................................................................................................14
  3.1 Mikä Active Directory on? .............................................................................................14
  3.2 Active Directoryn taustaa ...............................................................................................15
  3.3 Active Directoryn komponentit ......................................................................................16
  3.4 Active Directory Users and Computers ..........................................................................19

4 TESTATUT OHJELMAT ..................................................................................................21
  4.1 Active Directory Janitor 2.0 ...........................................................................................21
    4.1.1 Yleistä ......................................................................................................................21
    4.1.2 Testaus .....................................................................................................................22
  4.2 OldCmp 1.5.0 .................................................................................................................28
    4.2.1 Yleistä ......................................................................................................................28
    4.2.2 Testaus .....................................................................................................................28
  4.3 Network Account Password Age 1.3.0 ..........................................................................33
    4.3.1 Yleistä ......................................................................................................................33
    4.3.2 Testaus .....................................................................................................................33
  4.4 Vertailu ja päätös ............................................................................................................35
    4.5 Ohjelman asennus ja ajaminen asiakkaan palvelimella ..................................................36

5 WINDOWS 2003 KOMENTOJA ......................................................................................38
  5.1 Dsget ...............................................................................................................................38
  5.2 Dsmod .............................................................................................................................39
  5.3 Dsrm ...............................................................................................................................39
  5.4 Dsquery ...........................................................................................................................40
  5.5 Support Tools ja Resource Kit .......................................................................................40

6 TAVOITTEIDEN TOTEUTUMINEN ..............................................................................41

7 POHDINTAA .......................................................................................................................42
8 LÄHDELUETTELO ...........................................................................................................43
9 SANASTOA .........................................................................................................................45
10 LIITTEET ..........................................................................................................................46
1 Taustaa

1.1 Toimeksiantaja

Tutkimuksen toimeksiantaja on Neuvos Tietojärjestelmät, jossa suoritin myös työharjoittelun. Vuonna 1998 perustettu yritys tarjoaa asiakkailleen kaiken aina työasemien rakentamisesta koko IT-infrastruktuurin kokonaisvaltaiseen suunnitteluun ja ylläpitoon.

Kaikki ratkaisut räätälöidään asiakkaalle sopivaksi. Asiakas saa haluessaan esim. palvelimien ja työasemien ylläpidon ja VPN-ratkaisut (Virtual Private Network). Yritys on mm. Microsoftin, Ciscon ja F-Securen partneri ja toteuttaa laajalti näiden tarjoamia järjestelmää ja tietoturvaratkaisuja.

1.2 Asiakasyrityksen järjestelmät

Palvelin  
Tutkimuksessa mukana olevalla Neuvoksen asiakasyrityksellä on käytössään Windows 2000 Server -palvelin. Palvelimelle on asennettu seuraavat järjestelmät ja palvelut:

- Active Directory
- DNS (nimen selvityspalvelu)
- DHCP (dynaaminen osoitteiden jakamispalvelu)
- WINS (nimen selvityspalvelu)
- Microsoft SQL Server 2000 (tietokannan hallinta)

Prosessorina toimii Intel Xeon 2,4 GHz. Muistia palvelimella on tutkimusta tehtäessä 1 Gt.

Virustorjunta  

Työasemille on asennettu F-Secure Anti-Virus Client Security 6.0x. Palvelimella virustorjunnan puolesta hoitaa Anti-Virus for Windows Servers 5.6x.

Varmuuskopiointi  
Kyseisellä järjestelmällä tallennetaan kaikki yrityksen kannalta kriittinen tieto nauha-asemalle päivittäin.

Sähköposti


Turvallisuus saavutetaan siten, että yrityksen sisäisen sähköpostin ei tarvitse kulkea julkisen Internetin kautta, vaan ne kulkevat työntekijältä toiselle yrityksen oman Exchange-palvelimen kautta.

1.3 Etähallinta

Tietoturva

Asiakasyrityksen verkon ylläpito on toteutettava tietoturvallisilla etäyhteyksillä. Tämä toteutetaan siten, että Ciscon VPN Client -ohjelmalla avataan VPN-putki asiakasyrityksen verkkoon. Tällöin ylläpitäjän työasema saa IP-osoitteen samasta avaruudesta kuin asiakkaan verkkolaite. Tämän jälkeen ylläpitäjä voi ottaa yhteyden laitteeseen etäyöpöydällä tai esim. VNC-ohjelmalla (Virtual Network Computing).

Palvelin

Ylläpitäjä ottaa VPN-putken avaamisen jälkeen terminaalityöpöydylleen palvelimeen etäyöpöytäohjelmalla ja kirjautuu normalisti sisään.

Työasemat

Asiakkaan työasemilla on otettu käyttöön etäyöpöytäyhteyden mahdollisuus. Tämä on tehty Active Directoryssä (jäljempänä AD) ryhmästä, joka on liitettänyt työasemien organisaatioysikköön. Etäyöpöytäyhteyttä käyttäessä asiakkaan työasema lukittuu, eikä henkilö näe, mitä hänen työasemallaan tehdään.

Etätyö

Asiakkaan työntekijät liikkuvat ympäri Suomea, joten he tarvitsevat turvallisen etäyhteyden yrityksen verkkoresursseihin. Kannettaville tietokoneille on asennettu Cisco VPN Client, jota käyttämällä turvallinen yhteys Internetin yli mahdollistetaan.

Yrityksessä käytössä oleva sähköpostiohjelman Outlookin Internet-versio OWA (Outlook Web Access) mahdollistaa työssähköpostin käytön missä tahansa, missä on Internet-yhteys. OWA:a käytetään selaimen kautta.

1.4 Ristiriidat

Työssäni olen silloin tällöin törmännyt vanhoihin AD-objekteihin asiakkaiden palvelimilla. Vanhat tietokonetilit ja käyttäjätilit aiheuttavat ristiriitoja muiden palvelimella toimivien järjestelmien kanssa.

Muut järjestelmät


F-Secure Policy Manager Console (PMC) näyttää kaikki keskitetyissä hallinnassa olevat työasemat ja palvelimet. Kun koneen poistaa verkosta, se tulisi aina poistaa myös PMC:stä. Jos näin ei tehdä, syntyy esimerkiksi seuraava tilanne:

Ongelmatilan


Jos ylläpitäjä ei tarkistaisi työaseman statusta AD:stä, hän ryhtyisi ratkomaan virustorjunnan ongelmaa yrittämällä ottaa etäyhteyttä työasemaan. Ylläpitäjän tulee aina dokumentoida poistetut tietokoneet ja käyttäjätilit, jotta pystytäisiin tehokkaampaan ylläpitoon kaikkien järjestelmien osalta.
PMC:ssä on normaalia, että työasemat silloin tällöin saavat ”Disconnected”-statuksen. Näin tapahtuu erityisesti kannettavilla tietokoneilla, jotka tämän takia konfiguroidakaan hakemaan viruspäivitykset Internetistä suoraan F-Securen palvelimelta, kun yhteyttä yrityksen Policy Manager -palvelimeen ei ole.
2 Testausympäristö

2.1 Microsoft Virtual PC 2004

Perusteet käytölle

Oikeaan tuotantoympäristöön ei voi asentaa suoraan mitä tahansa ohjelmia, mitä Internetistä on löydetävissä. Vakoiluohjelmia voi tällaisen ohjelmien mukana tulla palvelimelle todella helposti, joten ajettavat ohjelmat tulee testata sellaisessa ympäristössä, jossa niiden mahdollinen toimimattomuus tai järjestelmän kaatuminen ei aiheuta mitään haittaa.

Yleistä


Virtual PC 2004 -ohjelmalla luodulle virtuaaliselle tietokoneelle asennetut palvelut ja ohjelmat eivät ole virtuaalisia, vaan ne on tässä tutkimuksessa asennettu todellisilta asennusmedioilta. AD:ssa luodut objektit eivät sen sijaan ole todellisia, ts. ne ovat virtuaalisia. Ne kuitenkin käyttäytyvät kuten todellisessa ympäristössä.

Asennus


Muutostyöt

Jos järjestelmä kaatuu, ja muutokset on tallennettu, uusi virtuaalinen PC on helppo luoda. Tosin kaikki siihen mennessä tehdyt asennukset ja konfiguraatioit täytyy tehdä uudestaan. Vanhankin virtuaali-PC:n voi yrittää korjata, riippuen siitä, kuinka pahasti järjestelmä on vioitunut.

Yleisimmissä käyttöjärjestelmissä Virtual PC 2004:n asennus asettaa fyysiselle tietokoneelle seuraavat vaatimukset:

<table>
<thead>
<tr>
<th>OS</th>
<th>Kovalevy (Gt)</th>
<th>Muisti (Mt)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 98</td>
<td>0,5</td>
<td>32</td>
</tr>
<tr>
<td>Windows Me</td>
<td>2</td>
<td>96</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>2</td>
<td>96</td>
</tr>
<tr>
<td>Windows XP</td>
<td>2</td>
<td>128</td>
</tr>
</tbody>
</table>

_Kaavio 1: Microsoft Virtual PC 2004 järjestelmävaatimukset._

(Lähde: Virtual PC Product Overview 2003)

### 2.2 Virtuaalisen ympäristön luominen


Todellista tuotantoympäristöä ei voida täysin simuloida virtuaalisesti. Erillisellä varsinaisesta toimialueesta eristetyllä testitoimialueella voitaisiin paremmin simuloida todellista ympäristöä. AD:n rakenteesta luotiin kuitenkin asiakkaan ympäristöä vastaava Users and Computers -komponentin osalta.

Kuvakaappauksen osalta virtuaalinen ympäristö on oikeaa palvelinta parempi, koska tällöin kuvista ei tarvitse poistaa työasemien, palvelimiin, ym. AD-objektien nimää. Virtual PC:llä otettuja kaappauksia voidaan käyttää sellaisenaan ilman riskiä salaisten tietojen paljastumisesta. Tästä oli apua tutkimuksessa tehtäessä.

Kuva 1: Virtuaalisen AD:n käyttäjät.

Tietokoneet-organisaatioyksikköön luotiin työasemia (kuva 2). Näitä, kuten käyttäjätilejäkin, muokattiin enable- ja disable-toimintoilla testausvaiheessa eri ohjelmilla.
Kuva 2: Virtuaalisen AD:n työasemat.

Tutkimuksen tarkoituksena ei ole vain toteuttaa jokin ”siivoamisohjelma” asiakkaan palvelimella, vaan myös testata useamman työkalun toimivuutta virtuaaliympäristössä. Näistä kaikista käsitellään niiden toiminnallisuus ja konfigurointimahdollisuudet. Työkaluista valittiin yksi, joka otettiin käyttöön oikealla asiakkaan palvelimella.
3 Active Directory

3.1 Mikä Active Directory on?

Perustietoa
AD on aktiivihakemistopalvelu, jonka avulla hallitaan kaikkia Windows-toimialueen objekteja. Näitä ovat mm. tietokoneet, käyttäjät, tuollostimet, organisaatioyksiköt ja ryhmäkäytännöt (Spealman: 36).

Asennus


AD näkymä
Työasema | AD
---|---
Objektit | tiedostot, kansiot, työasemat, käyttäjät, organisatsioyksiköt, jne.
Vaikutus | paikallinen/verkkoresurssi, toimialue
Sijainti | paikallinen/verkkoresurssi, kaikilla AD-palvelimilla

**Kaavio 2: AD:n kautta hallitaan isompia kokonaisuuksia kuin työasemalta tai palvelimelta, johon ei ole asennettu AD:ta.**

### 3.2 Active Directoryn taustaa


AD:ssa uutta oli mm. se, että toimialueen muutokset replikoituivat toisille AD-palvelimille (= DC-koneille). Tällöin kaikilla toimialueiden ohjauskoneilla on samat tiedot (Cross ym: 3). Ylläpitäjän tarvitsee tehdä muutokset vain yhdelle koneelle.


3.3 Active Directoryn komponentit

AD on monimutkainen kokonaisuus, jonka perusteelliseen selvittämiseen tarvittaisiin useampi tutkintotyö. Aikarajoitusten vuoksi tässä tutkimuksessa käydään läpi yleisten asioiden lisäksi vain ne komponentit, jotka ovat tutkimuksen kannalta avainasemassa.

Yleistä

AD muodostuu seuraavista hierarkkisista komponenteista (Cross ym: 19):

- Toimipaikat
- Toimialueet
- Puut
- Metsät
- Objektit
- DC-koneet

Toimipaikat

Toimipaikka (site) muodostuu tietokoneista, jotka ovat yhteydessä toisiinsa LAN-verkon (Local Area Network) välityksellä. Yleensä nämä tietokoneet sijaitsevat fyysisesti samassa paikassa tai samassa IP-verkossa.


Toimipaikka edustaa verkon fyysisistä rakennetta, kun taas toimialueet, puut, metsät ja objektit edustavat verkon loogista rakennetta (Cross ym: 21, 433).

Toimialueen komponentteja voi fyysisesti sijaita eri toimipaikoilla. (Cross ym. 21) Toimipaikat ja toimialueet voivat kuitenkin olla nivoutuneena toisiinsa (ks. kaavio 3). Halutut AD-objektit saadaan samaan toimialueeseen, vaikka ne sijaitsevatkin fyysisesti eri paikkakunnilla.

Toimialue (domain) on AD:n peruskomponentti. Objetit, kuten tietokoneet ja käyttäjät luodaan toimialueeseen. Ylläpitäjä voi luoda sääntöjä ja toimintatapoja koko toimialueelle määrittelemällä ne toimialueelle. Tällöin kaikki objektit perivät kyseiset toimintatavat, eikä niitä tarvitse erikseen määrittää jokaiselle organisaatioyksikölle.


Toimialueita hallitaan Active Directory Domains and Trusts-konsolilla. Täällä työkalulla hallitaan myös toimialueiden välisiä luottosuhteita.

Puu

Puu muodostuu useasta toimialueesta AD:ssa. Erityisesti kansainvälisillä yrityksillä saattaa olla oma toimialue jokaisessa maassa, jossa toimii.


Replikointia voidaan kontrolloida paremmin puu-ympäristössä. Kun luodaan alitoimialueita päätoimialueen alle, niille saadaan omat DC-konneensa, jotka replikoivat keskenään toimialueessa tapahtuvat muutokset (esim. käyttäjät- ja tietokonetilit).

Alitoimialueet kommunikoivat päätoimialueen kanssa. Niiden välille luodaan automaattisesti luottosuhde, joka mm. sallii käyttäjien päästä toisen toimialueen resursseihin käsiksi (Cross ym: 24).

Päätoimialue jakaa saman nimiavaruuden alitoimialueiden kanssa. Niiden välille luodaan automaattisesti luottosuhde, joka mm. sallii käyttäjien päästä toisen toimialueen resursseihin käsiksi (Cross ym: 24).

Metsä


Objektit

Kuten aikaisemmin on mainittu, AD:ssa hallitaan toimialueiden objekteja keskitetysti. Tietokone- ja käyttäjätilien lisäksi AD 2000:n objekteja ovat (Spealman: 343):

- kontaktit (henkilöiden yhteystietoja)
- ryhmät (ryhmä käyttäjät- tai tietokonetileja)
- jaetut kansiot (osoite, tietyyyn resurssiin)
- jaetut tulostimet
- DC-koneet (AD asennettu)
- organisaatioyksiköt (sisältää muita organisaatioyksiköitä ja objekteja)

Myös AD 2003:sta löytyvät vastaavat objektit.
DC-koneet

DC-koneet ovat palvelimia, joihin on asennettu AD. Ne ohjaavat toimialuetta. AD:n ylläpitäjä muokkaa hakemistopalvelua DC-koneella ja muutokset replikoidaan muille toimialueen DC-koneille. Redundanssin luomiseksi on hyvä ylläpitää kahta DC-konetta. Tällöin toisen koneen kaaduttua käyttäjät voivat edelleen kirjautua toimialueelle.


Global Catalog sisältää kopion oman toimialueen jokaisesta objektista ja osittaisen kopion muiden toimialueiden objekteista metsässä. Tämä tarkoittaa, että kaikkia attribuutteja ei kopioida. GC mahdollistaa hakupalvelujen käytön miltä tahansa metsän toimialueelta. (Cross ym: 540,541) Metsässä on vain yksi GC-kone.

Myös toimialueen DC-koneilla on omat roolinsa. Näitä ovat Crossin ja kumppaneiden (s.29) mukaan:

- RID Master (luo jokaiselle objekille uniikin ID:n)
- PDC Emulator (NT DC emulaattori; tarvittaessa)
- Infrastructure Master (ryhmäjäsenyyksien päivitys)

3.4 Active Directory Users and Computers


Yleensä näihin säiliöihin ei jätetä objekteja, koska niihin ei voi liittää ryhmäkäytäntöobjekteja (group policy). Tietokoneille ja käyttäjille tehdään mieluummin omat organisaatioyksikkönsä, joissa niitä on helppo hallita.

Ylläpitäjä voi luoda myös muokatun konsolin MMC:n (Microsoft Management Console) avulla. Kyseisellä työkalulla voidaan liittää automaattisten palveluiden lisäksi myös muita palveluita samaan konsoлинäkymään.

Kyseiset konsolit voidaan asentaa myös työasemalle adminpak.msi-asennuspaketilla. Käyttöjärjestelmänä täytyy täältä olla vähintään Windows XP SP1 (Microsoft Technet 2005²). Tämä ei kuitenkaan tarkoita sitä, että AD olisi asennettu työasemalle. Työasema ei toimi siis DC-koneena.
4 Testatut ohjelmat

4.1 Active Directory Janitor 2.0

4.1.1 Yleistä

Special Operations Softwaren (SOS) julkaissema Active Directory Janitor 2.0 oli testattavista työkaluista ainoa jossa oli graafinen käyttöliittymä (GUI). Pienikokoinen ohjelma, vain 1,6 Mt, tarjoaa monipuoliset mahdollisuudet niin tietokonetilien, kuin käyttäjätieto- seen ja hallintaan.


<table>
<thead>
<tr>
<th>Versio</th>
<th>Hinta (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>n. 40</td>
</tr>
<tr>
<td>1.1.0</td>
<td>n. 50</td>
</tr>
<tr>
<td>2.0</td>
<td>n. 230</td>
</tr>
</tbody>
</table>

*Kaavio 4: AD Janitorin hintakehitys. (Lähente: Special Operations Software, AD Janitor, Freedownloadscenter)*

Uusimmassa versiossa on mahdollisuus skannata AD myös käyttäjä- lien osalta. Se on huomattava parannus ohjelmaan, jonka aikaisemmat versiot mahdollistivat ainoastaan tietokonetilien skannauksen.

Janitorin asennusprosessi käynnistyy normaalisti ajamalla ohjelman .exe-tiedosto. Asennusprosessi ongelmineen on kuvattu tarkemmin liitissä 2.
4.1.2 Testaus

Kuva 3: AD Janitorin avausnäkymä.

Ohjelma tarjoaa kaksi vaihtoehtoa: koneiden tai käyttäjien skannauksen (kuva 3). Skannattessa tietokoneita, käyttäjä voi valita tietyn DC-koneen tai vain yhden. Esimerkeissä on käytetty virtuaaliympäristöä, jossa on yksi toimialue, yksi DC-kone sekä työasemia ja käyttäjiä.
Kuva 4: Asetukset tietokoneiden skannaukseen.

Settings-kohdasta (kuva 4) voidaan valita, kuinka monta säätiötä (threads) voidaan yhtäaikaisesti ottaa. Mitä enemmän DC-koneita on skannauksessa mukana, sitä enemmän sääkiöitä vaaditaan optimaaliseen suoritukseen.

Kun halutaan saada selville, minkä koneiden verkkoyhteydet eivät ole kunnossa, voidaan valita ”Connect to computers that appear offline”. Skannauksesta saa lokitietoja halutessaan. Tällöin skannauksen suorituskyky alenee huomattavasti. Testauksessa käytettiin sekä loki- että offline-skannausta.
Kuva 5: Tietokoneiden haku toimialueesta.


Kuva 6: Valittujen koneiden vahvistus.
Kuva 7: Skannattavat ominaisuudet.

Scan properties -vaihtoehdolla (kuva 7) voidaan valita, mitä ominaisuuksia itse asiassa skannataan. Nopein vaihtoehto ja samalla ”kevyin” on ”From Active Directory”. Skannaus vahvistetaan kuvan 8 mukaisesti.

Kuva 8: Skannauksen vahvistus.
Ping-komento, jota AD Janitor käyttää verkkoyhteyden testaukseen, ei luonnollisesti ole mennyt läpi virtuaaliympäristössä (kuva 9), koska vain DC-koneella on IP-osoite. Nähdakseen työaseman nimen täytyisi rekisteröityä käyttäjänä.

Myös IP-osoitteen näkeminen ja työasemien enable- tai disable-toiminnon käyttäminen vaativat rekisteröitymisen. Tuloslista näyttää tiedot mm. viimeisestä kirjautumisesta, käyttöjärjestelmästä ja siitä, onko työasema poistettu käytöstä. Erityisesti viimeiseksi mainittu on tärkeä tämän tutkimuksen kannalta.

Testausympäristö ei anna vastausta seuraaviin kysymyksiin:

- kuinka nopeasti skannaminen todellisuudessa tapahtuu
- kuinka paljon se kuormittaa palvelinta
- hidastaako se ratkaisevan paljon loppukäyttäjien verkkosoveluksia (mm. sähköposti, Internet, jaetut resurssit)

Em. seikkojen vuoksi skannaus oikeassa tuotantoympäristössä, rajattaisiin aluksi muutamaan työasemaan. Lopullinen skannaus, johon kuuluu n. 50 työasema, tehtäisiin työajan ulkopuolella klo 16 jälkeen. Tällöin siitä on mahdollisimman vähän haittaa loppukäyttäjille.
Käyttäjät valitaan samalla tavalla kuin tietokoneetkin. Kuitenkin Scan properties -vaihtoehto antaa erilaiset vaihtoehdot skannaukseen. Näitä ovat mm. salasanojen vanheneminen/uusiminen, profiilipolku, sähköposti ja edellisen kirjautumisen tiedot.

Kuva 10: Käyttäjien skannauksen tulos.

Kun valitsee organisaatioryksikön sijasta koko toimialueen, saa myös järjestelmänvalvojan (administrator) tunnuksen ja käytöstä poistettujen käyttäjätiedot samaan tuloslistaan. DC-koneen saa mukaan vastaavasti tietokoneiden skannaukseen, kun valitsee koko toimialueen.

Koko toimialueen skannaus olisi alkuvaiheessa järkevää, koska objekteja saattaa sijaita useissa, ehkä jopa täysin vääränlaisissa, organisaatioryksiköissä. Esim. tilien siirron yhteydessä tietokonetila saattaa jäädä vanhaan organisaatioryksiköön.

Jotta testautilanteessa saatiin jonkin verran tietoaakin skannauksien hyödyntämiseen, virtuaali käyttäjä Mikko Mallikas liitettiin Domain Admins -ryhmään (kuva 10). Näin hän pystyi kirjautumaan DC-koneelle ja hänen tietoni näkyi Janitorin tuloksissa.

AD Janitorin demoversio ei anna paljonkaan mahdollisuuksia skannauksen hyödyntämiseen. Jos skannaus todentaisi useita vanhoja objekteja, niitä olisi vaikea tunnistaa, koska rekisteröimätön versio ei näytä niiden nimää.
4.2 OldCmp 1.5.0

4.2.1 Yleistä


Ohjelma saattaa toimia täydellisesti, puutteellisesti tai sitten se ei tee mitään AD:ssa. Viimeisin ohjelmistoversio on ilmestynyt joulukuussa 2004. (Joeware 2005)


4.2.2 Testaus

Kun ohjelman yritti käynnistää pikakuvakkeesta, OldCmp vain välähti näytöllä. Komentokehoteesta se sen sijaan toimi, tosin virheilmoituksen kera (kuva 11). Tämä sen vuoksi, koska en ollut ensikertalaisena määriteltyä tarkempia parametreja.
Peruskomentoina ohjelma tarjoaa seuraavat vaihtoehdot:

- report
- disable
- delete


Raportointi

Ylläpitäjä voi määritellä, haluaako raporttiin objektin viimeisen kirjautumisajan (-llts) vai objektit, jotka eivät ole uusineet salasanaansa tiettynä aikana (-pwd <väli>).

Eri parametreilla voidaan määritellä, halutaanko hakuun mukaan esim. tietokonetilit, jotka ovat yli 90 päivää vanhoja, vai halutaanko kaikki tietokonetilit raporttiin.


Tietokonetilit


-Upsafe-parametrilla (kuva 13) kaiken ikäiset käytöstä poistetut tietokonetilit tuhotaan rajattomasti. Vaikka ko. kriteerit täyttävää objekteja olisi kymmeniä, ne tuhottaisiin kaikki. –Safety 20 -parametrilla päivyys rajattaisiin 20 koneeseen. Raja on oletusarvoisesti määritelty 10 koneeseen.


**Kuva 15: Tietokonetilien disable-toiminto.**


Käyttäjätilit


Kuva 16: Safety-parametri.

Kuva 17: Järjestelmän käyttäjäilejä ei voi poistaa.
4.3 Network Account Password Age 1.3.0

4.3.1 Yleistä

Network Account Password Age 1.3.0 (kuva 18) kertoo salasanojen iän niin tietokoneiden kuin käyttäjien osalta. Kyseessä on OldCmp:n tapaan tekstipohjainen ohjelma.

*Kuva 18: NetPWAge 1.3.0 avausnäkymä.*


4.3.2 Testaus

Komennolla `netpwage /users` käyttäjä saa näytölle kaikkien toimialueen käyttäjien salasanojen iät. Tuloste (kuva 19) näyttää myös järjestelmän sisäiset (built-in) tilit Administrator, Guest sekä IUSR_FIRMANSERVERI, joka on anonyymin käyttäjän tilin IIS:n (Internet Information Services) käyttöön.
Kuva 19: netpwage /users.


Tietokoneet firma003 ja firma006 ovat tulosteen mukaan (kuva 20) autentikoineet itsensä. Koneita ei kuitenkaan ole olemassa, eikä virtuaalista tietokonetta (firmanserveri) ole käynnissä niiden aikana viikon. Salasanojen iästä ei siten saa varmuutta ainakaan virtuaaliympäristössä. Oikeassa tuotanto- ja yritystilassa tuloksiin ei voisi suoraan luottaa, vaan täytyisi käyttää muita työkaluja.

Voidaan olettaa, että jos oikeat työasemat eivät ole kuukausiin autentikoineet itseään DC-koneen kanssa, kyseiset koneet eivät ole käytössä toimialueella.
4.4 Vertailu ja päätös


Tekstipohjaiset ohjelmat OldCmp ja NetPWAge ovat ilmiasia, kun taas GUI:n omaava AD Janitor on kallis. Se sopineekin parhaiten huomattavasti suurempiin ympäristöihin, joissa vanhat objektit aiheuttavat enemmän ongelmia. AD Janitor olisi kuitenkin selvästi monipuolisempi ohjelmisto, käyttäen monipuolisiin testatuista ohjelmista. Demoversio ikävä kyllä jätti pois olennaisimmat tiedot, eli objektien nimet. Tämän vuoksi AD Janitoria ei valittu ajettavaksi oikealla palvelimella.

NetPWAge toimi samaan tapaan kuin OldCmp:kin, teki juuri sen, minkä pitkin. Eri syntyivät siinä, että OldCmp oli huomattavasti uudempi ohjelma ja sisälsi enemmän toimintoja. NetPWAge ilmoittaa ainoastaan objektien nimet ja salasanat.


OldCmp valittiin asennettavaksi asiakkaan palvelimelle. Tähän saatiin suostumus sekä Neuvoksen toimitusjohtajalta että asiakasyrityksen kehitysjohtajalta.
4.5 Ohjelman asennus ja ajaminen asiakkaan palvelimella

Asennus
OldCmp asennettiin asiakkaan palvelimelle työajan päättymisesti. Mahdollisten ongelmien vuoksi ohjelmaa ei kannattanut asentaa ja ajaa täysin työajan ulkopuolellessa. Oli hyvä varmistaa, että joku on paikalla asiakasyrityksessä.

Ohjelman asennus ei vaatinut uudelleenkäynnistystä ja se oli hyvin nopeasti suoritettu. Ennen ohjelman ajamista tarkistin, että Veritas Backup Exec oli ottanut nauhalle kaikki varmuuskopiointikiistäisiä järjestelmiä.

Ajattelin etukäteen, että ohjelman ajaminen saattaisi kuormittaa palvelinta ja verkkoa vaikuttaen myös loppukäyttäjien työskentelyyn. Tietoinen, että virtuaaliympäristössä ohjelma skannasi AD:n läpi sekunnissa, mutta oikeassa AD:ssa skannaus saattaisi kestää kauemmin.

Raportin luonti

Työasemat


Ainoastaan yksi epäselvä seikka ilmeni raportissa. Eräs pöytäkone ei ollut vaihtanut salasanansa 47 päivään. Kuitenkin kone oli hallittavissa AD:ssa ja vastasi pingiin.
5 Windows 2003 komentoja


5.1 Dsget

Dsget-komennon avulla voidaan tiedoja mm. objektien jäsenyyksistä ja levytilan rajoituksista. Tämän tutkimuksen kannalta olennaisimmat dsget-parametrit, jotka liittyvät käyttäjä- ja tietokoneobjekteihin, ovat -user ja -computer.

Dsget computer -komennolla voi etsiä tietoja yhdestä tai useammasta koneesta. Tällaisia tietoja ovat mm. tietokoneen kuvaus (-desc), sijainti (-loc) ja jäsenyyystiedot (-memberof).

Seuraava komento antaa tietoa kyseisen tietokonetilin (firma001) staattisesta:

Dsget computer cn=firma001, ou=Tietokoneet,
dc=ekadomain,dc=fi –disabled

Jos arvoksi saadaan “yes”, tili on poistettu käytöstä, jos taas “no”, niin tili on käytössä. Lisää optioita saa näkyviin komennolla /?.

(TechCenter 2005¹)
5.2 Dsmod

Dsmod-komennolla voidaan muokata AD:n objekteja, tietokone- ja käyttäjätien lisäksi mm. organisaatioyksiköitä, ryhmiä ja DC-koneita. Komento tukee vain osaa yleisimmistä attribuuteista. Esimerkissä työasemat firma002 ja firma003 poistetaan käytöstä:

dsmo computer cn=firma002, ou=Tietokoneet, dc=ekadomain,dc=fi cn=firma003, ou=Tietokoneet, dc=ekadomain,dc=fi –disabled yes

Jos ko. koneet halutaan ottaa käyttöön, käytettäisiin parametria –disabled no.

Dsmod user -komennolla voidaan muokata objektin attribuutteja, kuten yhteystietoja ja salasanoja. Esimerkiksi käyttäjätilin käyttöönontaminen tapahtuisi seuraavasti:

dsmo user ”cn=Mikko Mallikas, ou=Käyttäjät, dc=ekadomain,dc=fi” –disabled yes

Kuten tietokonetileissäkin, myös käyttäjätilissä täytyy määritellä jokin muokattava DN (Distinguished Name) erikseen, kun haluaa muokata useita objekteja. DN muodostuu esimerkeissä seuraavasti:

- CN (Common Name)
- OU (Organizational Unit)
- DC (Domain Component)

Muita attribuuttityyppejä voisivat olla esim. C (Country, maa), STREET (katu) tai UID (User ID, käyttäjätunniste). (TechCenter 2005³, MSDN Library 2005³)

5.3 Dsrm

Dsrm on toinen työkalu, jolla voi muokata AD-objekteja. Sillä voidaan tuhota esim. käyttäjiä ja organisaatioyksiköitä. Seuraavalla komennolla tuhottaisiin Työasemat-organisaatioyksikkö ja sen sisältämät objektit: (TechCenter 2005³)

dsm –subtree –noprompt –c ou=Työasemat, dc=ekadomain,dc=fi
5.4 Dsquery


dsquery computer domainroot -stalepwd 35

Em. komentoja voidaan yhdistellä esim. seuraavasti:

- dsget:lla löydetään vanhat objektit ja ne poistetaan käytöstä dsmod:lla
- dsget ensin ja sen jälkeen dsrm:lla tuhotaan objektit

Microsoftin komentotyökalujen ei ainakaan periaatteessa pitäisi aiheuttaa ongelmia. Kuten muihin työkaluihin, ds-komentoihin (erityisesti dsmod ja dsrm) pätee se, että ylläpitäjä toimii omalla vastuullaan.

5.5 Support Tools ja Resource Kit


Resource Kit puolestaan on niin ikään kokoolma työkaluja, mutta ne eivät tule asennuspaketin mukana. Näiden työkalujen avulla ylläpitäjä selvittää käyttöjärjestelmä-, AD-, verkkoyhteydet-, tai tietoturvaan liittyviä ongelmia (Dowload Center 2003). Resource Kit -työkaluja on todella runsaasti, enkä ajan puitteissa eh tinkyt pererhymään niihin kaikki.

6 Tavoitteiden toteutuminen

Tutkimuksen tavoitteena oli selvittää, minkälaisia työkaluja on saatavilla vanhojen objektien etsimiseen ja poistamiseen AD:ssa ja toisaalta, onko ylipääätään yhtään hyvää työkalua tarjolla tähän tarkoitukseen. Vaihtoehtoja ei ole tällä hetkellä monta.

Vastaus tutkimusongelmaan on, että hyviä työkaluja objektien löytämiseen on olemassa. OldCmp ja NetPWAge toimivat hyvin tässä tarkoituksessa. Työkalun hyvyys määritellään kuitenkin aina ympäristökohtaisesti. Jokainen AD on oma kokonaisuutensa. Ei voida taata, että yhdellä palvelimella menestyksekkäästi ajettu ohjelma toimii vastaavalla tavalla toisen asiakkaan palvelimella.


Kun ohjelmallisesti poistetaan tietyt parametrit omaavat objektit, riskiä on, että pienen konfiguraatio- tai ohjelmavirheen vuoksi tuhoutuvat haluttua suurempi määrä objekteja

7 Pohdintaa

Voidaan kysyä, tarvitaanko tässä tutkimuksessa mukana olevia ohjelmia. Pienissä tuotantoypäröistöissä tarve ei ole suuri. Kuitenkin tällaiset työkalut tarjoavat nopeasti lisätietoja objekteista. Olennaisia tietoja ovat mm. tietokoneiden käyttöjärjestelmät ja käyttäjien salasanojen uusimistieheys.

Pienen yrityksen ei ole välttämättä järkevää sijoittaa maksulliseen työkaluun, kuten AD Janitor. Se, kuten muutkin vastaavat työkalut, tarjoavat ylläpitäjille nopeasti lisätietoja objekteista. Pienessä ympäristössä siihen riittävät kuitenkin ilmaisohjelmat OldCmp tai NetPWAge.


Isommassa ympäristössä maksulliset työkalut tulisivat kyseeseen. Ylläpidettävänä saattaa olla tuhansia objekteja ja tällöin AD:hen jää helpommin vanhoja objekteja. Globaaleissa suuryrityksissä, joissa saattaa olla satoja tuhansia objekteja, maksulliset työkalut ovat välttämättömyyks.

Kaiken kaikkiaan, mitä ohjelmia tai komentoja ylläpitäjä käyttääkin, hänen tulee arvioida huolellisesti, mitä hyötyä toimenpiteestä käytännössä on ja mitä riskejä siinä sisältää.

Tulevaisuudessa, kun tietojärjestelmät ovat keskenään yhä enemmän yhteensoipivia ja mahdollisesti AD-integroituja, tässä tutkimuksessa mainittuja työkaluja voitaisiin käyttää myös muiden järjestelmien objektien hallintaan.

OldCmp:n luojan Joe Richardsin lukuusis AD-työkalut olisivat jatkotutkimuksen aihe, kuten myös vanhentuneiden objektien taloudellisten vaikutusten selvitys.
8 Lähdeluettelo

Kirjat:


Internet:

Microsoft Exchange Product Information 2004 [online] [viitattu 29.11.2005].
http://www.microsoft.com/exchange/evaluation/whatis.mspx

Virtual PC Product Overview 2003 [online] [viitattu 31.12.2005].

Microsoft Active Directory Glossary 1999 [online] [viitattu 29.1.2006].

Microsoft Windows Server Technet 2005 [online] [viitattu 29.1.2006]¹.


Special Operations Software [online] [viitattu 31.12.2005].
http://www.specopsoft.com/default.asp

AD Janitor [online] [viitattu 28.12.2005].
http://www.adjanitor.com/purchase/default.asp

Freedownloadscenter [online] [viitattu 28.12.2005].
Joeware [online] [viitattu 28.12.2005].
http://www.joeware.net/win/free/tools/oldcmp.htm

MSDN Library [online] [viitattu 7.1.2006]¹.


OptimumX [online] [viitattu 7.1.2006].
http://www.optimumx.com/download/#NetPWAge

Microsoft Technet Security Center 2006 [online] [viitattu 7.1.2006].

Microsoft Windows Server TechCenter [online] [viitattu 14.1.2006]¹.
http://technet2.microsoft.com/WindowsServer/en/Library/96a4a5ee-ee72-44d5-845f-71b2de33d4411033.mspx


Microsoft Knowledge Base [online] [viitattu 28.1.2006].
http://support.microsoft.com/kb/892777

Microsoft Download Center [online] [viitattu 25.1.2006].
9 Sanastoa

<table>
<thead>
<tr>
<th>Sanasto</th>
<th>Defiinointi</th>
</tr>
</thead>
<tbody>
<tr>
<td>autentikoida</td>
<td>Käyttäjä tai tietokone todentaa itsensä DC-koneelle.</td>
</tr>
<tr>
<td>disable-toiminto</td>
<td>Objekti poistetaan käytöstä AD:ssa valitsemalla ”Dis- sable” tai suorittamalla tietty komento. Ei poista ob- jekttia.</td>
</tr>
<tr>
<td>enable-toiminto</td>
<td>Käytöstä poistettu objekti otetaan käyttöön AD:ssa valitsemalla ”Enable” tai suorittamalla tietty komento.</td>
</tr>
<tr>
<td>konsoli</td>
<td>Hallintanäkymä, esim. AD Users and Computers.</td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft Management Console. Työkalu, jonka laajennuksilla (snap-in) voi hallita mm. paikallisen- tai etäkoneen palveluita ja käyttäjäryhmiä.</td>
</tr>
<tr>
<td>organisaatioyksikkö</td>
<td>Eng. organizational unit, ou. AD:n objekti, johon voidaan luoda mm. käyttäjä- tai tietokonetilejä tai toisia käyttäjätilejä. Ou:hun voidaan luoda ryhmä- käytäntöjä.</td>
</tr>
<tr>
<td>replikointi</td>
<td>DC-kone, jossa AD:hen tehdään muutoksia, toistaa eli replikoi muuttuneet tiedot toisille DC-koneille.</td>
</tr>
<tr>
<td>ryhmäkäytäntö</td>
<td>Eng. group policy. AD:ssa voidaan luoda käyttäjä- tai tietokonetasolla ryhmäkäytäntöjä ja sallia tai rajottaa tiettyjä Windowsin toimintoja.</td>
</tr>
<tr>
<td>X.500</td>
<td>CCITT:n (Comite Consultatif Internationale de Telegraphie et Telephonie) osoitehakemistostandardi.</td>
</tr>
</tbody>
</table>
10 Liitteet

LIITE 1

OLD CMP RAPORTTI

2005/12/13-16:37:14

Generated by OldCmp V01.05.00cpp - http://www.joeware.net

Search Start Time 2005/12/13-16:37:14
Search Finish Time 2005/12/13-16:37:15
Host Name firmanserver.ekadomain.fi
Directory Type Windows 2000
Forest DC=ekadomain,DC=fi
Forest Mode Domain DC=ekadomain,DC=fi
Domain Mode
Search Scope subtree
Search Base DC=ekadomain,DC=fi
Search Filter ((&(objectCategory=computer)(pwdLastSet<=127789582348420000)))
DN Exclusions
Age (days) 0
Old Age Date 2005/12/13-16:37:14
Old Age Date (Int8) 127789582348420000
Max Age (days) 0
Max Old Age Date 0000/00/00-00:00:00
Max Old Age Date (Int8) 0
Action REPORT
Stamp accountExpires FALSE
Safety Setting 10
For Real Setting FALSE

Color Legend
Lisäksi raportissa näkyvät salasanan vanhenemispäivämäärä, käyttöjärjestelmä ja sen versio-numero, Service Packit sekä käyttäjätin hallinta (esim. käytöstä poistetulla tilillä MBR DISABLED PWD_NOT_REQD).
LIITE 2

ACTIVE DIRECTORY JANITOR 2.0 ASENNUS

Active Directory Janitor 2.0 Setup

User Information
Enter the following information to personalize your installation.

Full Name: Administrator
Organization: Firma Ltd

The settings for the application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for:

- [ ] Anyone who uses this computer
- [ ] Only to me (Administrator)

Next Installation Wizard

< Back  Next  Cancel

Active Directory Janitor 2.0 Setup

Destination Folder
Select a folder where the application will be installed.

The Vizee Installation Wizard will install the Janitor for Active Directory Janitor 2.0 in the following folder:

Destination Folder:
C:\Program Files\GroupsSoft\Janitor

Next Installation Wizard

< Back  Next  Cancel

Active Directory Janitor 2.0 Setup

Ready to Install the Application
Click Next to begin installation.

Click the Back button to return to the installation information or click Cancel to exit the wizard.

Next Installation Wizard

< Back  Next  Cancel
Active Directory Janitor 2.0 has been successfully installed.

Click the Finish button to exit this installation.
Asennus eteni normaalisti. Kun ohjelman yritti käynnistää, mitään ei tapahtunut. Toisella yrityskerralla sain oheisen mscoree.dll-virheilmoituksen:

Etsittyä ratkaisua Internetistä, ilmeni, että palvelimella täytyy olla .NET Framework asennettuna.

Päivityksen asennus edellytti kuitenkin uusinta versiota päivitysohjelmasta (Microsoft Windows Installer 3.1). Tämä puolestaan vaati virtuaali-PC:n uudelleenkäynnistystä.

Kun sain .NET Framework 1.1:n asennettua, ohjelma käynnisti ja ehdotti uutta päivitysversiota 2.0.2.3, jonka asensin.
LIITE 3

VIRTUAALIYMPÄRISTÖSSÄ TOIMIMATTOMAT WINDOWS 2003 -KOMENNOT

Dsget

Objektien ominaisuuksista (properties) ei näe tietoja salasanojen iästä tai siitä, milloin viimeksi on kirjaututtu sisään. Kuitenkin objektien kuvaoksissa (description) saattaa olla tietoa objektin voimassaoloajasta, esim. poistopäivämäärän muodossa. Tällaisessa tapauksessa seu-raava komento olisi hyödyllinen:

```bash
dsget computer cn=firma001,ou=Tietokoneet,dc=ekadomain,dc=fi –desc
```

Haku tulostaa kuvaoksen kyseisestä objektista ja myös tietoa voimassaoloajasta, jos se on kuvauskseen konfiguroitu.

**Dsget user** -komennolla voidaan käyttää –disabled ja –desc-parametreja, kuten `dsget computer` -komennollakin. Esimerkki:

```bash
dsget user ”cn=Mikko Mallikas,ou=Käyttäjät, dc=ekadomain, dc=fi” –desc.
```

Dsget computer ja user eivät kuitenkaan toimineet testiympäristössä, jossa ei ollut oikeita objekteja. Syynä saattoi olla myös syntaksivirhe.

Dsquery

Virtuaalisessa testiympäristössä tämä komento ei toiminut, koska toimialueen tyyppi ei tukenut sitä.

Seuraava komento tulostaa kaikkien niiden käyttäjien DN-arvot, jotka eivät ole kirjautuneet domainiin vähintään kolmeen viikkoon.

```bash
dsquery user domainroot –inactive 3
```


Dsget:n tapaan käytöstä poistettujen objektien hakeminen onnistuu – disabled-parametrilla.