ICT4Events

Versienummer: 1.0

Datum: 27-11-2014

Namen:

Hein Dauven  
Jordy Guzak  
Kenneth Reijnders

Onderzoeksopdracht Active Directory

Groep: S22-D

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Status | Datum | Wijziging |
| 0.1 | Concept | 31-10-2014 |  |
| 0.2 | Concept | 27-11-2014 |  |
| 1.0 | Definitief | 27-11-2014 |  |

1. Inhoudsopgave

[2. Samenvatting 3](#_Toc402535156)

[3. Inleiding en probleemstelling 4](#_Toc402535157)

[4. Opdrachtsformulering 5](#_Toc402535158)

[5. Onderzoeksvraag en -aanpak 6](#_Toc402535159)

[6. Onderzoeksresultaten 7](#_Toc402535160)

[7. Conclusie en evaluatie 10](#_Toc402535161)

[8. Bijlagen 11](#_Toc402535162)

[9. Literatuurlijst 12](#_Toc402535163)

# 2. Samenvatting

Active Directory is geïnstalleerd op een server, die de domain controller genoemd wordt. Deze zorgt ervoor dat de gegevens van alle netwerkobjecten ergens op het netwerk worden opgeslagen. De domain controller kan bestaan uit een domeinen, sites, trees, forests en trusts. Waarbij een domein een verzameling is van gebruikers en computers met hetzelfde beveiligingsbeleid. Sites een geografische eenheid is die fysieke computers en randapparatuur verdeeld. Trees een verzameling is van domeinen met parent – child relatie. Een forest bestaat uit een of meerdere trees en/of domeinen met een of meerdere trusts. Een trust is een vertrouwensrelatie tussen domeinen.  
Waarbij het makkelijk is om het te beheren, het beheer te verdelen en overzichtelijker is. Maar waarbij wel een complete afhankelijkheid is van het Active Directory.  
Het kan geïmplementeerd worden door via de Server Manager de rol Active Directory Domain Services uit te rollen. Waarbij er eerst een forest-root-domain aangemaakt dient te worden. Als deze is uitgerold kunnen er gebruikers en computers toegevoegd worden aan het domein.  
Active Directory is van zichzelf al goed beveiligd maar kan nog extra beveiligd worden door bijvoorbeeld gebruikers van een domein verplichten om sterke wachtwoorden te gebruiken of ze te verplichten om na een bepaalde tijd hun wachtwoord te wijzigen.

# 3. Inleiding en probleemstelling

In dit rapport wordt onderzoek gedaan naar wat Active Directory inhoud, wat de voor- en nadelen hiervan zijn, hoe het geïmplementeerd kan worden in het project ICT4Events en wat er gedaan kan worden om het zo goed mogelijk te beveiligen.   
  
De gemaakte applicaties voor het ICT4Events project maken momenteel gebruik van een database om dingen zoals het inloggen van gebruikers en het opslaan van verschillende media te regelen. Dit kan vervangen worden door Active Directory. Om er achter te komen of dit beter en veiliger is, wordt er onderzoek gedaan, aan de hand van een aantal deelvragen.

# 4. Opdrachtsformulering

In het 2e gedeelte van de proftaak PTS2 is een van de klanteisen dat er verschillende gebruikersrollen met verschillende rechten aanwezig zijn binnen de applicatie(s) die jullie ontwikkelen. Zoiets kun je op verschillende manieren implementeren. Voor PTS2 ga je een geavanceerde en in de “echte wereld” veelgebruikte aanpak verkennen en daadwerkelijk gebruiken: de Microsoft Active Directory-technologie.

Bij IN2 hebben jullie kennisgemaakt met “Microsoft Active Directory”. Het beheren van users, groepen, computers en printers in een AD-domein ging met de tool ADUC

Het voordeel van deze aanpak is dat we gebruik kunnen maken van standaardfunctionaliteit die al aanwezig is. Dit scheelt ontwikkeltijd en ontwikkelkosten: we kunnen bijvoorbeeld gebruik maken van functionaliteit die de Active Directory-technologie al voor ons implementeert.

Om inzicht te krijgen in de mogelijkheden van AD, moet eerst een grondig onderzoek worden uitgevoerd.

De .Netomgeving bevat functionaliteit (System.DirectoryServices en System.DirectoryServices.ActiveDirectory) waarmee dit te realiseren is.

Het onderzoek moet zich dus richten op het gebruik van Active Directory. De bovenstaande beschrijving moet worden omgezet in een onderzoeksvraag en in de showroom wordt d.m.v. een demonstratie de gevraagde functionaliteit getoond.

Gevraagde functionaliteit

• Een gebruiker authentiseren via het domein

• Informatie over gebruikers weergeven

• Zoek een gebruiker

• Groepen aanmaken

• Gebruiker in groep zetten

• Update een gebruiker

• Gebruiker toevoegen

• Gebruiker verwijderen

# 5. Onderzoeksvraag en -aanpak

## Onderzoeksvraag:

Hoe kan Active Directory de functionaliteit het ICT4Events project bevorderen?

## Deelvragen:

Wat is Active Directory? En wat zijn hier de voor- en nadelen van?

Hoe implementeer je Active Directory?

Hoe kunnen we Active Directory beveiligen?

# 6. Onderzoeksresultaten

## Wat is Active Directory? En wat zijn de voor- en nadelen?

Active Directory zorgt ervoor dat de gegevens van alle netwerkobjecten ergens op het netwerk worden opgeslagen. Meestal worden deze gegevens opgeslagen op een server, waarop Active Directory is geïnstalleerd. Deze server wordt dan ook wel een domain controller genoemd. Als de gegevens niet worden opgeslagen kan er niet worden geverifieerd of geautoriseerd en werkt de netwerk beveiliging niet. Deze gegevens worden bewaard in een bestand. Dit bestand wordt de NTDS.DIT genoemd, ook wel bekend als Active Directory. Waarbij NTDS staat voor New Technology Directory Service en DIT voor Data Information Table. Het NTDS.DIT bestand is een database bestand wat onder Windows server bewerkt wordt door een databaseprogramma, namelijk directories. Deze twee samen worden ook wel de Directory Service genoemd. En het is zo ontworpen dat naadloos aansluit op geldende internetstandaarden.  
De domain controller kan bestaan uit:

* Domeinen
* Sites
* Trees
* Forests
* Trusts

Een domein is een groep van gebruikers en computers met hetzelfde beveiligingsbeleid. Een domein wordt dan ook als een eenheid beheert.  
Een site is een geografische eenheid die fysieke computers en randapparatuur verdeeld. Dit kan voorkomen dat een gebruiker kan inloggen op locatie a terwijl de werknemer op locatie b werkzaam is.   
Een tree is een hiërarchische domeinstructuur, waarin een parent – child relatie bestaat tussen domeinen, en er altijd een root domein bestaat. Een forest is niets anders dan een verzameling van domeinen die door middel van trusts een relatie met elkaar hebben. En een trust is een vertrouwensrelatie tussen domeinen.

Voordelen:

* Het beheer wordt makkelijker.
* Beheer is overzichtelijker.
* Beheer kan verdeeld worden.

Nadelen:

* Compleet afhankelijk van het Active Directory.

## Hoe implementeer je Active Directory?

Een Active Directory kan geïmplementeerd worden op een server door naar de “Server Manager” te gaan en vervolgens voor “Roles” en “Add Roles” te kiezen. Er verschijnt dan een installatiescherm waar een aantal services geselecteerd kunnen worden. Selecteer “Active Directory Domain Services” en doorloop vervolgens de installatie wizard.   
  
Vervolgens dient er een “forest-root-domain” te worden gemaakt. Een nieuwe domein kan aangemaakt worden door naar “Start” -> “Run” -> “dcpromo” te gaan. Hierbij is er de keuze om een domein in een bestaand of in een nieuwe forest aan te maken. Vervolgens kan er het functioneel niveau van de forest en domein geselecteerd worden (Windows Server 2000, 2003, 2008). Kies hier voor Windows Server 2008. Op het volgende scherm wordt er gevraagd of naar extra opties. Zorg ervoor dat de optie “DNS server” is aangevinkt en ga verder.

Vervolgens kunnen er computer objecten worden aangemaakt, gebruikers, gebruikersgroepen etc. Als dit allemaal gebeurt is kunnen de workstations aan het domein worden toegevoegd. Hierbij is het belangrijk dat de workstation als DNS het IP-Adres van de server gebruikt.

Dit gebeurt bijvoorbeeld op een Windows 7 machine. Klik op “Start” -> rechtermuisknop op “Computer” -> “Properties” -> “Change Settings” -> “Change..” en voer vervolgens het domein naam in.

Nu is er succesvol een Active Directory opgezet, is er een domein en forest aangemaakt, zijn er computer objecten aangemaakt en gekoppeld met het domein.

## Hoe kunnen we Active Directory beveiligen?

Active Directory biedt zelf al een veilige omgeving, doordat het gebruikt maakt van ingebouwde verificatie bij aanmelding en autorisatie van gebruikers.  
In Active Directory is het een vereiste dat de identiteit van een gebruiker bevestigd wordt voordat deze toegang tot het netwerk verleent wordt. Als een gebruiker geïdentificeerd is, wordt door het LSA (Local Security Authority) een toegangstoken gegenereerd waarin de rechten van de gebruiker voor netwerkbronnen wordt aangegeven.   
  
Active Directory zorgt er niet alleen voor beveiliging op het gebied van verificatie maar ook door de machtiging van gebruikers te eenvoudige zodat de bestanden die geshared zijn, beter beveiligd zijn.  
  
Daarnaast is het mogelijk om zelf de beveiliging van Active Directory verder te verbeteren:

* Zo kun je bijvoorbeeld gebruikers van een domein verplichten om sterke wachtwoorden te gebruiken.
* Gebruikersrechten toewijzen aan gebruikersgroepen, zodat het duidelijk wordt wat de rol van een gebruiker binnen een domein is.
* De gebruikers verplichten om na een bepaalde tijd hun wachtwoord te laten wijzigen.
* Een account laten vergrendelen nadat hij meerdere malen een verkeerd wachtwoord intoetst.

# 7. Conclusie en evaluatie

Active Directory is dus een uitgebreide rol die geïmplementeerd is op de Windows servers (vanaf 2000), al dan niet geïnstalleerd. Het is een veilige omgeving die gebruikt maakt van autorisatie en verificatie. Maar toch nog verder kan beveiligingen.

Het kan de functionaliteit van het ICT4Events project bevorderen door het te implementeren over het netwerk van het ICT4Events project, zodat gebruikers de juiste toegang krijgen.

# 8. Bijlagen

# 9. Literatuurlijst

Kieviet, N. (2010). Active Directory en PHP. Geraadpleegd op Niels Kieviet (2010). Active Directory en PHP. [ONLINE] Available at: http://www.phphulp.nl /php/tutorial/data-verwerking/active-directory-en-php/745/wat-is-active-directory-en-wat-houd-het-in/1970/.

Microsoft (). So What Is Active Directory?. [ONLINE] Available at: <http://msdn.microsoft.com/en-us/library/aa746492%28v=vs.85%29.aspx>.

Leonardo Pessoa (2014). Authorize and authenticate users with AD. [ONLINE] Available at: <http://www.codeproject.com/Articles/8819/Authorize-and-authenticate-users-with-AD>

Microsoft (). Active Directory. [ONLINE] Available at: <http://msdn.microsoft.com/en-us/library/bb742424.aspx>.

thund3rstruck (2008). Howto: (Almost) Everything In Active Directory via C#. [ONLINE] Available at: <http://www.codeproject.com/Articles/18102/Howto-Almost-Everything-In-Active-Directory-via-C>.

Microsoft (). Beveiligingsinformatie voor Active Directory. [ONLINE] Available at: <http://technet.microsoft.com/nl-nl/library/cc779033(v=ws.10).aspx>.

Microsoft (). Active Directory beveiligen. [ONLINE] Available at: <http://technet.microsoft.com/nl-nl/library/cc728372%28v=ws.10%29.aspx>.

Microsoft, (2008). 'Fundementals of Network Infrastructure'. In: Don Messier (ed), Fundamentals of Winows Server 2008 Network and Applications Infrastucture. 1st ed. : Microsoft. pp.1-24, 1-30.