Opmerkingen bij het concept voorstel ontwerp LWP

Aan: LWP inventarisatie groep

Van: H. Paas, IWI

Datum: 27 sep 2006

Distributie (zie pag 3 LWP)

- Zoals reeds opgemerkt, ik laat de keuze voor een Linux distributie leverancier voorlopig in het midden. Eén en dezelfde distributie voor een RuG Linux werkplek ligt uiteraard voor de hand, maar het is niet wezenlijk van belang voor de winst die te behalen valt in het beheer en de distributie van werkplekken. Het enige voordeel is dat overal hetzelfde inlogscherm en desktop wordt gepresenteerd. De rest van de cosmetica wordt door de gebruiker zelf aangebracht via zijn profilering.
  IWI heeft op dit moment meerdere distributies / packages van Linux installaties in gebruik, tot en met de file en distributie servers zelf toe. Het biedt de gelegenheid om meerdere versies aan te bieden (afgezien van de direct nodige 32/64 bit distributies en de nodige pre-release versies), eenmaal gebundeld tot een distribueerbaar pakket levert het verder weinig extra werk aan de beheerderskant op. De winst zit altijd in een vanuit gebruikersoptiek simpele install en de uit handen genomen systeem onderhoud die de gebruiker zelf moet plegen: hij kan zich volledig op zijn werk richten en is blij voor altijd verlost te zijn van het installatie- en beheerderscorvee.
- Van belang is dat er tijdens de install een configuratiemogelijkheid bestaat om de client optimaal in te stellen voor hardware inpassing etc., niet altijd is binnen Linux een autoconfiguratie mogelijk van alle instellingen. In het boot/opstartproces bij IWI zijn voorzieningen aanwezig om niet- autoconfigureerbare onderdelen en instellingen alsnog uit te voeren.
- Er dienen waarborgen te zijn ten aanzien van de snelheid van distribuering: snelle installs zijn zeer wervend voor potentieel

nieuwe gebruikers ! Voor een indruk, op dit moment wordt bij IWI voor een full install, op een installed software base van 5.7 GB. een installatiesnelheid van 6 min. gehaald (100 Mb link). Voor grotere verzamelingen van clients is de installatiesnelheid nog meer van belang.

Samengevat moet het distribueringssysteem in staat zijn distributies te verspreiden naar clients waarna client specifieke configuratie vanuit één en dezelfde bundle plaatsvindt tijdens het bootproces. Servers, locaties en clients moeten kunnen verschillen : het is onverstandig om alle werkplekken op 1 centrale server te willen uitvoeren, diversificatie binnen 1 distributie is om die reden alleen al nodig. We moeten niet vergeten dat we een LWP ontwerpen voor een categorie gebruikers die hoge eisen stelt aan betrouwbaarheid, software content en snelheid (zie het bijgevoegde attachment).

Accounts (Pag. 4)

- De authenticatie dient terdege uitgewerkt en overdacht te worden voordat met de implementatie begonnen wordt. Er moet niet de fout gemaakt worden dat de huidige, zich tot Windows en Novell servers beperkende authenticatie voor Linux gebruikt wordt. Op dit moment is deze onbruikbaar, het is te beperkt. Extra authenticatie informatie en access regulering dient in de LDAP base opgenomen te worden om groepen systemen (clients) al dan niet toegankelijk te maken voor een gebruiker.
- De technische implementatie met drie "knooppunt"servers vind ik onvoldoende. Data server(s) die de clients van data voorzien dienen een replica van de master-server of in RC-jargon "RuG-brede" LDAP server op te vragen waarna gebruikersauthenticatie via de dataserver kan plaatsvinden op de verbonden client. Een "slave server"pushing mechanisme (vergeef me de NIS terminologie, er zal zeker een LDAP equivalent zijn) zorgt voor oplijnen van deze slave-databases. Omgekeerd dient de master server in staat te zijn wijzigingen van passwords te accepteren van een client (ja, dit zijn eisen voor een Linux werkplek, niet wat er nu al aan LDAP Novell authenticatie voorhanden is):

Wat nu onder NIS gebruikelijk is, moet ook zeker onder het veel nieuwere LDAP mogelijk zijn.

Storage (Pag. 4)

- Centrale dataopslag ligt voor de hand. Maar er is meer dan alleen een centrale SAN en data storage.
  Centrale storage creëert meteen het probleem van user data security, dit afgewogen tegen de winst van het administratieve opschalen van de installatie.
  Het probleem onstaat meteen al doordat user authenticatie alleen niet meer voldoende is, maar er ook client authenticatie plaats moet vinden. Unix (dus ook Linux) servers vertrouwen (identificeren) clients aan de hand van IP adressen. Een intruder heeft in dit geval genoeg aan een server-trusted IP adres om ongeauthoriseerd data van een server te halen, met alle gevolgen van dien.

  Bij IWI kan alleen door een strak security en client authenticatiebeleid tot op heden NFS V3 als client-server datatransport gebruikt worden.

  NFS V3 client access valt echter meteen af in het RUG-brede Linux client-server concept : NFS security staat en valt bij voldoende client authenticatie (en security). Client authenticatie (ofwel het vertrouwen dat de server kan stellen in het IP adres van de machine die zich aanmeldt onder dat adres) valt vrijwel onmogelijk voldoende te handhaven over het totale RUG domein.
  NFS-V4 lijkt een uitweg te bieden in dit probleem. Binnen NFS-V4 is host identificatie geïmplementeerd en wordt voor user authenticatie gebruik gemaakt van UID en GID remapping naar een nfs-domein. Kerberos authenticatie zorgt voor netwerk-authenticatie waarop host-access gevalideerd wordt.

- Er moet worden onderzocht hoe de NFS V4 security-context na herladen van de systeem software instellingen van een client automatisch hersteld kan worden.

Applicatiedistributie en patching (pag 5)

- Instellingwijzingen / software toevoegingen in lopende systemen moet mogelijk zijn. Deze wens komt zowel in onderzoeks- als onderwijs clients bij IWI vaak voor. Samenhangend is een snelle respons van de beheerders op vragen naar toevoegingen van programmatuur en software modulen vereist. Zij moeten daarvoor dan ook de nodige gereedschappen voorhanden hebben.

Installatie (pag 5)

- Imaging alleen is onvoldoende. Het proces is te star en biedt te weinig mogelijkheden om tijdens het opstartproces checks en configuratieinstellingen op de clients door te voeren. IWI heeft daarom eigen startup/boot extensies in het bundle systeem die dit proces sturen. Unattended install, een must-have, (al dan niet remote opgestart) is daardoor meteen mogelijk. Een bijkomend voordeel van deze aanpak is dat de data transport tijdens de PXE / TFTP boot fase zeer beperkt gehouden kan worden waardoor het laadproces zeer versneld wordt.
- ARP requests / TFTP transporten over de gehele RUG backbone moeten mogelijk zijn. Willen we een werkelijk RUG brede Linux werkplek invoeren die overal gebruikt wordt, dan staan clients in diverse domains opgesteld. De mogelijkheden van transport van deze IP pakketten over RUGnet dient nader te worden onderzocht.

Standaardsoftware (pag5)

- Uiteraard mag het (La)TeX pakket, het de-facto wetenschappelijke tekstpakket, niet in de standaardsoftware ontbreken.

Aanvullende opmerkingen / aandachtspunten

- Dataservers kunnen op een gelijkelijke manier geïnstalleerd worden als de geschetse client-install vanuit aparte dataserver software bundles. Dit maakt het toevoegen van extra servers eenvoudig.
- Authenticatie op clients met groepsgewijze toekenning over clients aan gebruikers dient terdege uitgezocht te worden.
- Een goede test-configuratie en bundle mechanisme dient aanwezig te zijn voor het creëeren van nieuwe releases.
- Software install, onderhoud, updates en patches installeren kunnen volledig worden geautomatiseerd.
  Een snelle bediening van gebruikers na vragen om wijzigingen en toevoegingen is een veel groter probleem en zal de kwaliteit van de dienstverlening voornamelijk bepalen. Onderzoekers (en soms ook docenten) hebben behoefte aan een snelle reactie op de nodige aanpassingen en uitbreidingen. Er dienen daarom methodieken aanwezig te zijn om snel en adekwaat aan deze vraag te kunnen voldoen.