

Netwerk Scan

GEMEENTE ZUTPHEN



Wij weten waar IT om draait



Documentgegevens

Opdrachtgever

Bezoekadres	Gemeente Zutphen 's Gravenhof 2 7201 DN Zutphen 14 0575
Algemeen	
Contactpersoon	Marga van Woensel M.vanWoensel@zutphen.nl

Opdrachtnemer

Bezoekadres	Lesscher IT Platinastraat 25 7554 NC Hengelo 074 240 46 46
Algemeen	
Contactpersoon	J. van Zanten@lesscher.nl

Documentrevisies

Versie	Datum	Auteur	Omschrijving/Opmerking
0.9	03-04-2013	G. Kunst	
1.0	07-04-2013	J. van Zanten	

© 2013 Lesscher IT

Niets uit dit document mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enig andere manier, zonder voorafgaande schriftelijke toestemming van Lesscher IT.

Inhoudsopgave

Inhoudsopgave	3
1. Inleiding	4
2. Opbouw netwerk gemeente Zutphen	5
2.1. Storage	5
2.2. Virtualisatie laag	5
2.3. Provisioning	5
2.4. XenApp	6
2.4.1. Web interface	6
2.4.2. Profiel	6
2.5. Workspace Manager	6
3. Bevindingen en verbeterpunten	7
3.1. Storage	7
3.1.1. Inrichting NetApp	7
3.1.2. Storage locatie gevirtualiseerde servers	7
3.1.3. Uitwijk	7
3.2. Virtualisatie platform	8
3.2.1. Centraal management	8
3.2.2. CPU over commitment	8
3.2.1. Virtuele Servers blijven hangen	9
3.3. Provisioning	11
3.3.1. Pxe boot	11
3.3.1. Cache disk performance	12
3.3.2. Cache disk grootte	13
3.3.3. SQL offline support	13
3.3.4. High availability	14
3.3.5. Traag booten geprovisionede machines	15
3.3.6. Versie Provisioning	15
3.4. XenApp	16
3.4.1. Windows activatie	16
3.4.2. Zone data collector	17
3.4.3. Applicatie Virtualisatie	17
3.4.4. Network load	18
3.4.5. Traagheid door virusscanner	18
3.4.6. Virusscanner beheer	19
3.4.7. Update/Upgrade XenApp	20
3.4.8. Citrix web interface	20
3.4.9. Kleine punten	20
3.5. Workspace manager	21
3.5.1. Veel globaal goedgekeurde executables	21
3.5.2. Dubbele en oude goedgekeurde apps	21
3.5.1. Profielen	21
3.5.2. Look and feel	22
3.5.3. Versie	22
4. Conclusie en vervolgstappen	23
4.1. Algemene conclusie	23
4.2. Vervolgstappen	23
4.2.1. Vervanging hypervisor	23
4.2.1. Upgrade XenApp omgeving	24
4.2.2. Upgrade Provisioning	25
5. Vervolg	26

1. Inleiding

Dit document beschrijft de bevindingen van de uitgevoerde netwerkscan op het Kantoor Automatisering netwerk van de Gemeente Zutphen. Deze netwerkscan is uitgevoerd om verbeterpunten binnen het KA netwerk en evt. vervolgstappen te beschrijven.

De uitgevoerde scan zal in hoofdlijnen de volgende onderdelen bevatten:

- Inrichting NetApp
- Inrichting Citrix XenApp
- Inrichting Citrix XenServer
- Inrichting Citrix Provisioning

Het speerpunt in dit onderzoek zijn de traagheidsproblemen die ondervonden worden binnen de Citrix omgeving. Het resultaat is een rapport met de bevindingen en aanbevelingen hoe de bestaande omgeving verbeterd kan worden en welke stappen gemaakt kunnen worden om de bestaande omgeving te migreren naar een nieuw platform.

De netwerkscan is uitgevoerd in overleg met de huidige beheerders. Een aantal verbeterpunten, conclusies en aanbevelingen zullen daarom binnen de organisatie reeds bekend zijn.

De opbouw van het document is als volgt, eerst wordt een situatieschets van de omgeving gegeven. Daarna een aantal verbeterpunten op de huidige installatie en configuratie. In het laatste hoofdstuk worden vervolgstappen gegeven om de problemen definitief op te lossen en de omgeving te vernieuwen zodat deze weer up-to-date is.

De omgeving ziet er qua opzet en inrichting in de basis voldoende uit. Er zijn bepaalde keuzes gemaakt m.b.t. storage, virtualisatie etc. die niet volgens de best practises zijn maar de keuzes die hierin gemaakt zijn, zijn te verklaren en lijken logisch. De gemaakte keuzes worden in dit document indien van toepassing wel ter discussie gesteld.

2. Opbouw netwerk gemeente Zutphen

Onderstaand wordt kort de bestaande omgeving beschreven om zo een vertrekpunt te creëren waarop de verbeterpunten gebaseerd zijn.

De medewerkers van de gemeente Zutphen werken voor een groot deel via Wyse thinclients op een Citrix omgeving. Zowel intern als extern loggen ze hiervoor in op een Citrix web interface (vanaf extern via een Citrix Access Gateway 5.04). Het kantoor automatisering netwerk van de gemeente Zutphen bestaat voor een gedeelte uit gevirtualiseerde servers op basis van XenServer en een aantal fysieke servers.

De omgeving van de gemeente Zutphen wordt gebruikt door maximaal 550 gelijktijdige gebruikers.

2.1. Storage

De gevirtualiseerde omgeving van de gemeente Zutphen draait op local storage op de diverse hosts, daarnaast is er een NETAPP FAS2240. Ook is er een FAS2040 aanwezig waarop de back-ups worden geplaatst.

De NetApp FAS2240 wordt momenteel alleen ingezet voor het aanbieden van ISCSI disks aan de Exchange omgeving, Oracle, SAP en SQL servers. Daarnaast wordt hij gebruikt voor het aanbieden van CIFS shares voor de gebruikers van de omgeving.

Voor fysieke machines (zoals exchange) wordt de datadisk met de exchange stores aangeboden via ISCSI. Er wordt momenteel geen gebruik gemaakt van de NETAPP om virtuele machines op te hosten omdat de XenServer 5.6 storage link hier niet goed mee overweg kan.

2.2. Virtualisatie laag

Momenteel zijn er ongeveer 24 virtualisatie hosts aanwezig binnen de omgeving van de gemeente Zutphen. Deze zijn allen voorzien van XenServer versie 5.6 build 31188p.

De virtuele machines zijn verdeeld over de hosts. Alle vm's staan op local storage. De data disk worden passthrough aangeboden via een ISCSI initiator binnen de virtuele machine richting het SAN.

De verdeling van de hosts is als volgt

Onderdeel	Aantal	Opmerkingen
Hosts t.b.v. Citrix omgeving	7	Front-end Citrix servers
Hosts t.b.v. backend omgeving	9	Overige gevirtualiseerde servers
Hosts t.b.v. testomgeving	8	

2.3. Provisioning

De Citrix Provisioning omgeving is momenteel versie 5.6.1.1045. Dit zijn 2 Windows 2008R2 servers welke in loadbalancing mode zijn geconfigureerd. De aangeboden Vdisken voor de geprovisionede servers staan op het SAN en worden via een CIFS share aangeboden aan de Provisioning servers.

De geprovisionede Citrix servers zitten in een Vlan wat specifiek voor de gevirtualiseerde servers is opgezet en de servers krijgen via PXE-boot de benodigde opstart gegevens toegestuurd.

2.4. XenApp

De XenApp omgeving is gevirtualiseerd op het XenServer hypervisor platform. De servers zijn voorzien van Windows 2008 standaard x86 (32 bit). Hierdoor zijn de server beperkt tot 4 GB werkgeheugen. Elke server is daarnaast voorzien van 4 cpu's.

De servers zijn voorzien van XenApp 5.1 voor Windows 2008 (Dit is XenApp 5.0 met rollup pack 1). De cache van Provisioning (15 tot 20 GB per geprovisionede server) wordt op de local storage van de XenServer host opgeslagen. Er zijn 30 XenApp servers beschikbaar voor de maximaal 550 gebruikers wat neerkomt op maximaal 18 gebruikers per server. Per gebruiker is ongeveer 200 MB beschikbaar per sessie indien er 550 gebruikers zijn ingelogd.

Er zijn geen dedicated zone datacollectors ingericht.

Er wordt gebruik gemaakt van Trend Micro Office Scan versie 10.6 t.b.v. virusscanning op de Citrix servers.

2.4.1. Web interface

Er zijn 2 web interface servers ingericht voorzien van Citrix web interface versie 5.4. De vWeb01 werkt als web interface voor de interne omgeving. vWeb02 is nog niet volledig ingericht. Op vWeb01 staat de KMS activatie service geïnstalleerd.

2.4.2. Profiel

Er wordt gebruik gemaakt van een mandatory profile waardoor alle gebruikersinstellingen via Workspace Manager beheerd worden

2.5. Workspace Manager

Voor gebruikers instellingen en beheer wordt gebruik gemaakt van Workspace Manager 2011 SR4 Enterprise.

3. Bevindingen en verbeterpunten

In dit hoofdstuk worden per onderdeel verbeterpunten aangegeven op de bestaande installatie en configuratie.

3.1. Storage

3.1.1. Inrichting NetApp

De inrichting van de NetApp is conform de geldende best practises (althans voor zover van toepassing op deze netwerkscan). De firmware is bijgewerkt tot de laatste versie en geconfigureerde functionaliteiten (snapmirror etc.) zijn goed ingericht.

3.1.2. Storage locatie gevirtualiseerde servers

Alle virtuele servers staan op de local storage van de diverse XenServer hosts. Dit is uit het oogpunt van High Availability en disaster recovery niet wenselijk. Immers bij uitval van een host zijn de virtuele machines die erop staan niet op een andere locatie op te starten omdat de bestanden hiervan op de fysieke schijven in de host staan.

Advies

Het is raadzaam om zo snel mogelijk de **niet** XenApp servers te verhuizen van local storage naar de SAN omgeving. Gezien de huidige belasting op het SAN zouden deze extra servers niet voor problemen moeten zorgen.

3.1.3. Uitwijk

Momenteel wordt er een FAS2040 gebruikt als uitwijk/back-up unit. Deze staat in dezelfde ruimte als de productie San unit. Bij calamiteiten waarbij de serverruimte niet meer gebruikt kan worden (bijv. brand) zal zowel productie als back-up dus niet meer bruikbaar zijn en alle data die erop staat, en niet op tape buiten het pand wordt bewaard, als verloren worden beschouwd.

Advies

Het is raadzaam de back-up unit z.s.m. te verhuizen naar een andere locatie.

3.2. Virtualisatie platform

De bestaande XenServer is versie 5.6 build 31188p. Deze versie gaat 31-03-2014 end of life. Deze versie levert momenteel veel problemen op m.b.t. performance en stabiliteit. Er zal dus nu al gekeken moeten worden naar een upgrade pad/alternatieve oplossing.

3.2.1. Centraal management

De omgeving wordt op dit moment beheerd via de standaard XenCenter tooling die bij XenServer geleverd wordt. Er zijn geen resource pools etc. ingericht om failover etc. te kunnen faciliteren.

Advies

Indien het mogelijk is om virtuele machines naar centrale storage te zetten moeten ook resource pools ingericht worden van de diverse types servers zodat deze elkaars servers over kunnen nemen bij uitval etc.

3.2.2. CPU over commitment

Per XenServer host welke voor Citrix XenApp wordt gebruikt zijn 24 processor cores beschikbaar. Dit zijn 12 kernen + 12 hypertreading kernen. Bij een aantal hosts worden alle 24 kernen uitgedeeld aan virtuele machines. Hoewel dit geen probleem hoeft te veroorzaken is het geen "best practise". De oorzaak van dit probleem is dat alle vm's 4 cores tot hun beschikking hebben, indien deze allemaal zijn uitgedeeld zal het onderliggende OS (XenServer) indien het een CPU nodig heeft resources moeten lenen van een van de Citrix servers.

Technisch gezien kan dit. Echter als de Citrix servers zwaar belast worden, wat nogal eens gebeurt op de omgeving, is er geen capaciteit om de CPU aanvraag af te handelen en zal er gewacht moeten worden tot er CPU cycles vrij zijn (CPU ready time). Dit kan vertragingen veroorzaken.

advies

Het is daarom aan te raden om van Xensrv01 t/m 04 een virtuele machine af te halen en deze te plaatsen op Xensrv05 en 06. Hierdoor zijn alle hosts dan optimaal in gebruik zonder dat CPU overcommitting plaatsvindt.

3.2.1. Virtuele Servers blijven hangen

Gedurende de dag blijft er af en toe een geprovisionede Citrix server hangen. Hierop is dan niet meer in te loggen en sessies van bestaande gebruikers zitten dan vast.

Oorzaak hiervan is dat er op dat moment heel veel verkeer gevraagd wordt van de disk en dat een groot gedeelte van deze informatie op dat moment vanaf het netwerk (provisioning server) opgehaald moet worden. (let in het plaatje goed op de schaal).

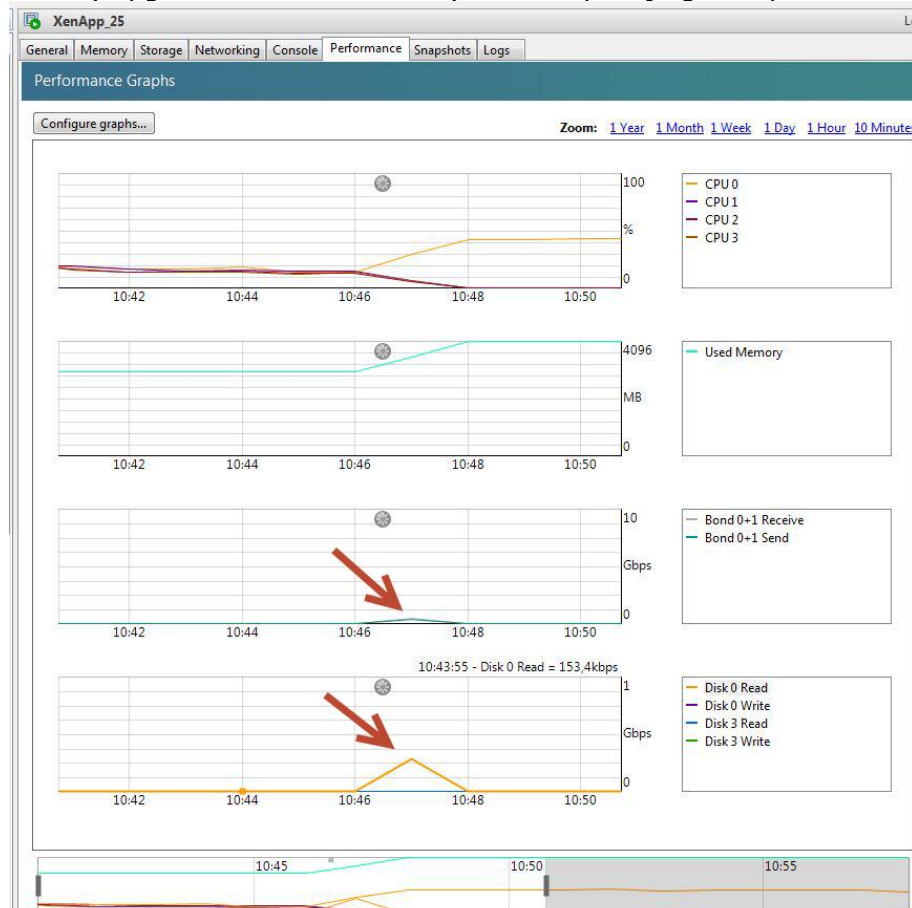


Fig. netwerkload op virtuele NIC en disk

De verbinding met de Provisioning server gaat verloren waarna de machine dus alleen nog op cache verder draait. Omdat de machine nog op informatie wacht die nooit komt zie je dit soort eventlogmeldingen voorbij komen. De server loopt dan vast en alleen een harde reset werkt dan nog.



Fig. foutmelding in eventlog

Oorzaak hiervan is de netwerkkaart driver van de XenServer.

Er zijn 2 relevante issues bekend met de gebruikte versie van XenServer onderstaand staan ze beschreven.

Hotfix XS56E009 not installed	
Description:	A number of security vulnerabilities have been identified in Citrix XenServer. These vulnerabilities affect all currently supported versions of Citrix XenServer up to and including version 5.6 Service Pack 2.
Citrix Recommendations:	Please refer to CTX130292 and upgrade to hotfix XS56E009
Extra Information:	None
Severity:	Severe
Category:	General
Issue detected on:	xensrv10, XENSrv17, xensrv02, xensrv08, XENSrv13, xensrv09, xensrv04, XENSrv18, XENSrv20, XENSrv12, XENSrv16, XENSrv15, xensrv07, xensrv03, XENSrv14, XENSrv-TEST01, xensrv01, xensrv05, XENSrv-UPDATE, XENSrv-TEST02, XENSrv19, xensrv06, XENSrv11
bnx2 drivers are out of date	
Description:	An out of date bnx2 driver has been found. This driver can cause network instability
Citrix Recommendations:	You can download an updated driver from CTX129215 or CTX129216 if you have applied Hotfix006 for XenServer 5.6.
Extra Information:	None
Severity:	Medium
Category:	Runtime Error
Issue detected on:	XENSrv17, xensrv02, xensrv08, XENSrv13, xensrv09, xensrv04, XENSrv18, XENSrv20, XENSrv16, XENSrv15, xensrv07, xensrv03, XENSrv14, XENSrv-TEST01, xensrv01, xensrv05, XENSrv-UPDATE, XENSrv-TEST02, XENSrv19, xensrv06

advies

Voer bovenstaande updates z.s.m. uit op de omgeving.

3.3. Provisioning

3.3.1. Pxe boot

Momenteel staan de DHCP scope options ingesteld om de geprovisionede servers te voorzien van een image. De scope options verwijzen keihard naar een van de twee Provisioning servers (optie 066 boot server host name)

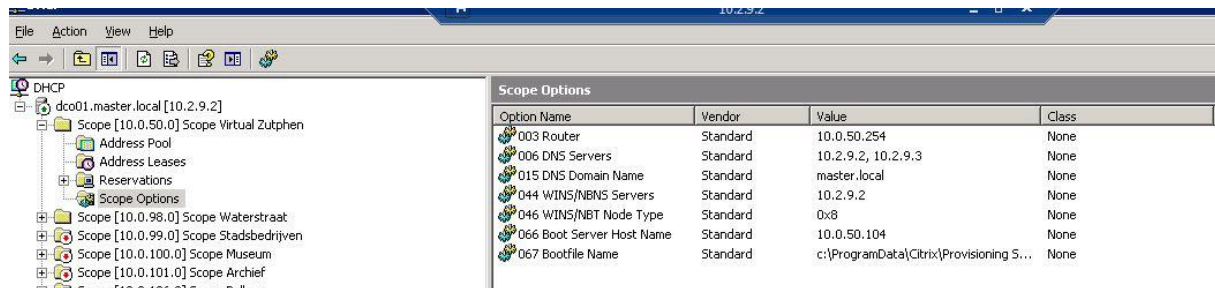


Fig. instelling dhcp scope options

Mocht deze niet bereikbaar zijn dan kunnen de servers dus niet gestart worden omdat ze via de Pxe boot options niet bij het boot image kunnen komen.

Daarnaast staan binnen Provisioning de bootstrap settings van de beide Provisioning servers niet goed geconfigureerd:

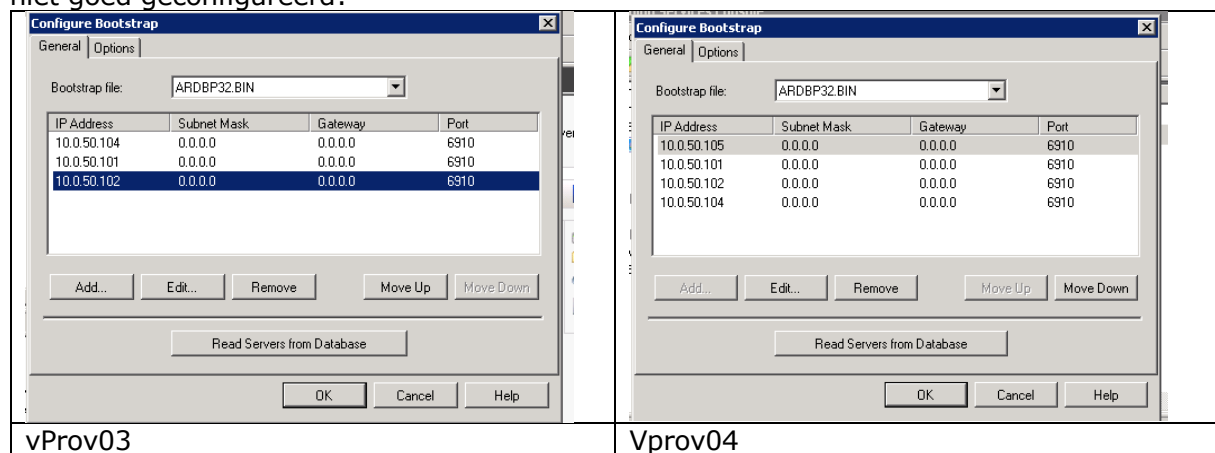


Fig. bootstrap options

Op de vProv03 staan de bootstrap settings zo ingesteld dat deze altijd vanaf vProv03 opstarten. Op vProv04 staat ingesteld dat deze altijd van Vprov04 opstarten. Echter staan op beide servers de IP-adressen van de reeds uit gefaseerde Provisioning servers ingesteld.

Advies

Laat de XenApp servers Pxe booten naar een round robin DNS adres (bijv. pvs.master.local). maak dit DNS a record 2x aan en verwijst het naar de beide Provisioning servers. Pas daarna in de bootstrap de settings aan zodat op beide servers alleen de huidige Provisioning servers erin staan. Hierdoor kan bij uitval van vProv03 d.m.v. round robin DNS toch de 2^e host gevonden worden en kan de omgeving herstart worden.

Het advies is om bovenstaand door te voeren. Mocht dit niet wenselijk zijn, zijn de volgende alternatieven mogelijk

Alternatieven

Ook kan er gekozen worden voor het booten vanaf een ISO file. Deze kan aangemaakt worden binnen de Provisioning server en kan daarna gekoppeld worden aan de virtuele machines.

In de ISO boot file worden de Provisioning servers beide aangegeven en er kan dan bij uitval van één van de Provisioning hosts via de andere geboot worden. Ook wordt hierdoor wordt een gedeelte van de PXE boot sequence overgeslagen en kan de bootsnelheid van de virtuele machines versneld worden.

Ander alternatief kan zijn: Implementeer een loadbalancing oplossing voor het tftp boot gedeelte van de provisioning servers. Dit zou de gratis versie van de Netscaler kunnen zijn (netscaler VPX). Deze is relatief simpel te installeren en zorgt ervoor dat de pxe boot aanvragen verdeeld worden over beide servers. Voor een nog hogere uptime zouden er zelfs 2 van deze netscalers geloadbalanced kunnen worden.

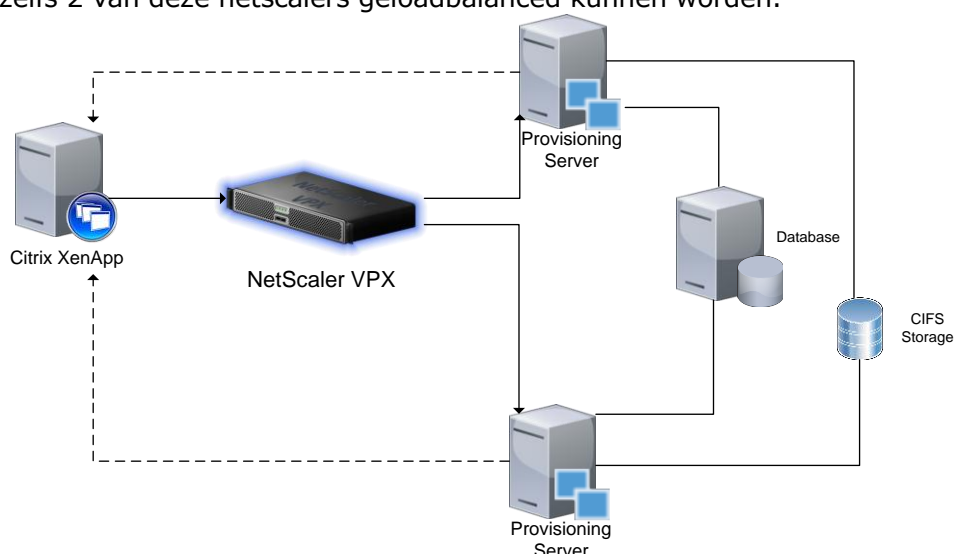


Fig. implementatie Netscaler tftp boot

3.3.1. Cache disk performance

De cache disks staan op local storage op de XenServer hosts. Wat opvalt is de slechte Read performance van deze disk. Onderstaand een test uitgevoerd op een virtuele machine op een XenServer host en een test van dezelfde virtuele machine maar dan binnen een Hyper-V host met nagenoeg gelijke hardware. Tijdens deze test is via de tool lanspeed een bestand van 2 GB geschreven naar de cache disk en daarna weer teruggelezen.

XenServer

	---Writing---	---Reading---
Packet length :	2,000,000,000	2,000,000,000
Time to complete:	28.5907275	84.5612002
Bytes per second:	69,952,750	23,651,509
Bits per second :	559,622,000	189,212,072
	-----	-----
Mbps:	559.6220000	189.2120720

Hyper-V

	---Writing---	---Reading---
Packet length :	2,000,000,000	2,000,000,000
Time to complete:	12.5444192	34.0351737
Bytes per second:	159,433,448	58,762,738
Bits per second :	1,275,467,584	470,101,904
	-----	-----
Mbps:	1,275.4675840	470.1019040

n.b. deze test is uitgevoerd door systeembeheer gemeente Zutphen

n.b2. Write is hoger omdat er write caching wordt toegepast op de harde schijven. De read snelheid is de daadwerkelijke snelheid van de disk

Hoewel deze test puur indicatief is laat het zien dat de read performance van de machine veel lager is op de XenServer omgeving dan op de Hyper-v omgeving. Daarnaast zijn ook acties met het kopiëren van grote bestanden naar de virtuele machine gedaan. Wat hierbij opvalt is dat de volledige virtuele machine onwerkbaar is tijdens deze kopie slag. Oorzaak hiervoor is de manier waarop XenServer 5.6 omgaat met local storage repository's.

Advies

Upgrade de hypervisor om bovenstaande problemen te verhelpen. De performance van XenServer 6.1 is veel beter dan de performance van XenServer 5.6. Daarnaast kan gekeken worden of een alternatieve hypervisor bijvoorbeeld Hyper-V niet een betere oplossing is)

3.3.2. Cache disk grootte

Cache disken van enkele XenApp servers zijn bijna vol (< 1gb vrije ruimte) dit kan caching problemen gaan geven indien de schijven vol raken. Oorzaak hiervoor is dat bij een harde reboot van een server (bijv. vanwege een vastlopende server) de server de cache file niet leeg maakt en deze op de cache disk blijft staan. Er wordt dan een nieuwe naast gezet tijdens de volgende boot. Dit kan problemen gaan geven zodra er geen vrije ruimte meer is.

Ook valt op dat niet alle geprovisionede servers een cache disk hebben van dezelfde grootte.

Advies

Inventariseer welke geprovisionede servers te weinig vrije ruimte hebben en maak ruimte vrij op deze machines of vergroot de disk. Zorg ervoor dat alle geprovisionede virtuele machines cache disk hebben van gelijke grootte.

3.3.3. SQL offline support

Binnen de Provisioning farm staat de optie Offline database support niet aan. Mocht onverwachts de SQL server offline gaan zullen de Provisioning hosts ook niet meer functioneren waardoor de Citrix omgeving offline zal gaan.

Indien dit vinkje is aangezet wordt de database lokaal gecached op de Provisioning hosts is de Provisioning farm nog steeds bereikbaar. Er kunnen dan geen wijzigingen worden doorgevoerd maar de geprovisionde servers gaan niet offline.

Advies

Zet offline database support aan

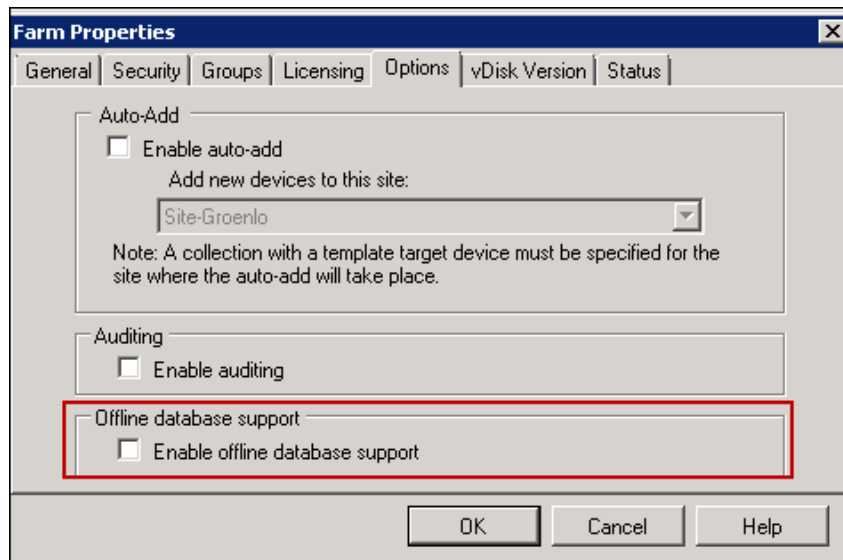


Fig. offline database support

3.3.4. High availability

Op de productie images staat momenteel High Availability niet wat betekent dat bij uitval van een van de Provisioning hosts de andere de taken niet overneemt.

Advies

Zet dit vinkje aan op de Vdisk

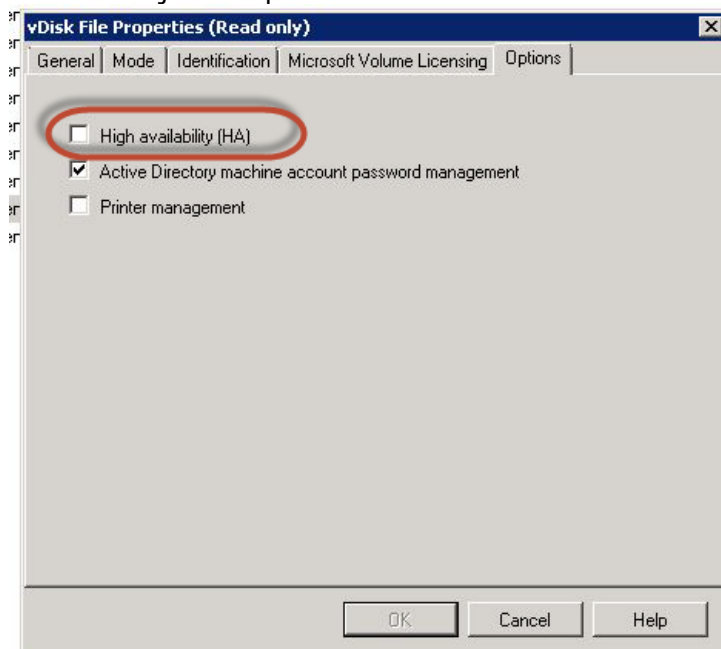


Fig. high availability vdisk

3.3.5. Traag booten geprovisionede machines

Het lijkt dat het booten van een geprovisionede virtuele machine ongeveer 10 minuten duurt waarbij er enkele minuten een zwart scherm te zien is waarbij er geen waarneembare activiteit is op de virtuele machine anders 1 CPU die op 50% van de capaciteit draait.

Oorzaak hiervoor is een bug in XenServer 5.6 welke met een private fix van Citrix gerepareerd kan worden. (<http://forums.citrix.com/thread.jspx?threadID=276473>)

Alternatief hiervoor is het booten vanaf bootdisk. Hierbij wordt aan de virtuele machine een ISO disk gekoppeld waarvan geboot wordt. Een gedeelte van het probleem zit in hoe de virtuele netwerkkaart het PXE boot verkeer afhandelt. Door via een ISO disk te booten wordt een gedeelte van het probleem ondervangen.

3.3.6. Versie Provisioning

Momenteel wordt Provisioning server versie 5.6 gebruikt. Hoewel deze versie goed functioneert is deze gedateerd en kan een upgrade veel voordelen opleveren.

advies

Bij een upgrade naar Provisioning 6.1 kan er gebruik wordt gemaakt van versie beheer binnen Provisioning. Hierdoor wordt het mogelijk is om verschillende versies binnen één vdisk aan te maken, dit heeft als voordeel minder schijfruimte gebruik en je kunt sneller terug naar een vorige versie dus een minder grote beheer last.

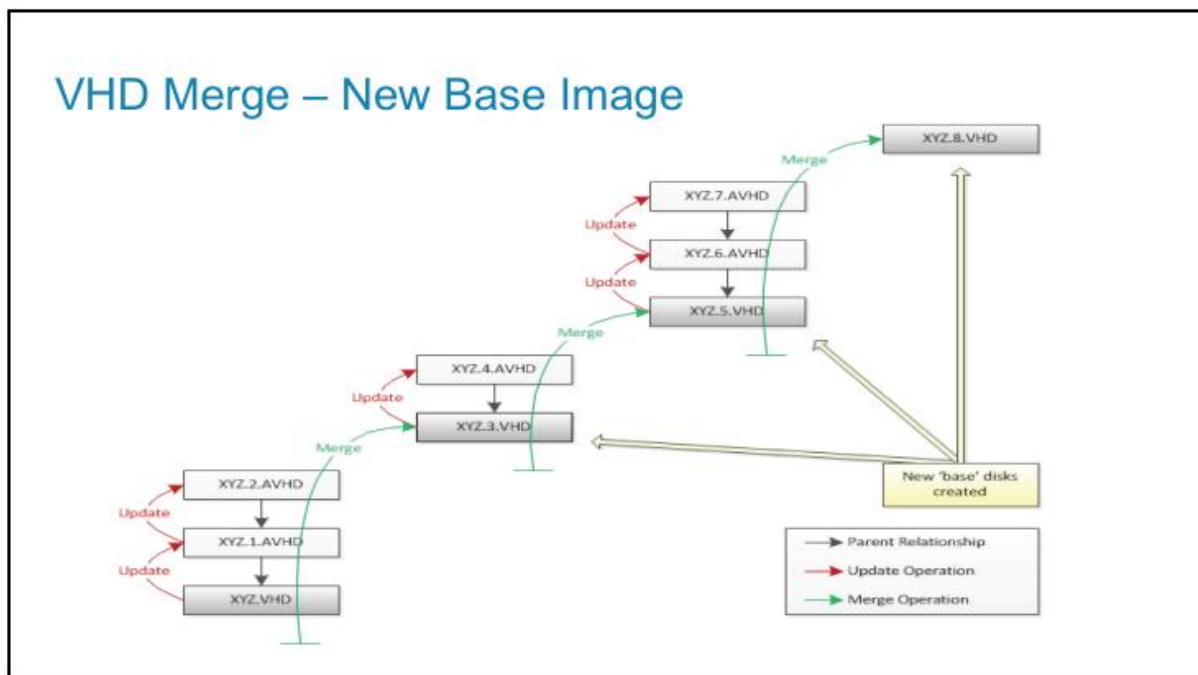


Fig. mergen vdisk

Daarnaast kan deze versie ook patchmanagement doorvoeren. Dat wil zeggen dat op gezette tijden een image automatisch voorzien kan worden van Windows updates.

Fig.

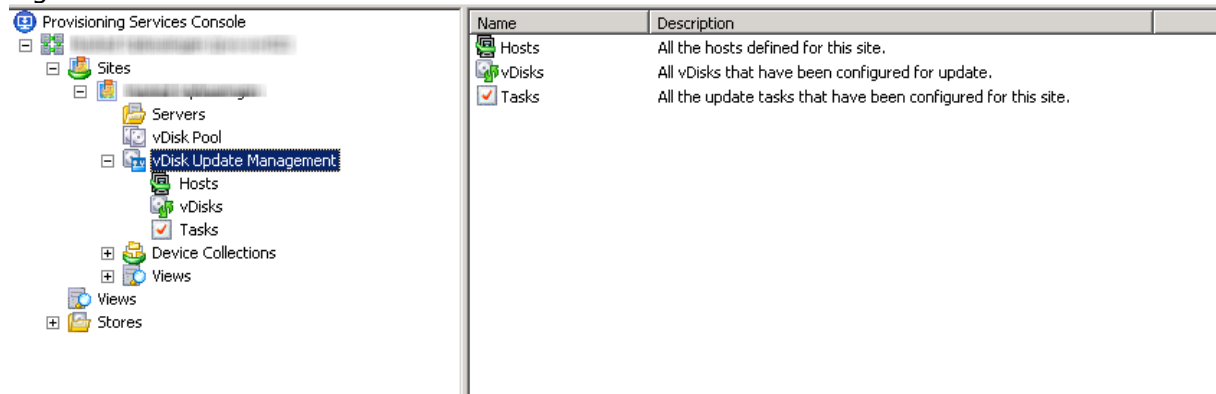


Fig. vdisk update management

Het kan zelfs zover geautomatiseerd worden dat er een nieuwe versie van de vdisk gemaakt wordt deze wordt afgepatched en vervolgens in test (en evt. in productie) gezet kan worden.

3.4. XenApp

3.4.1. Windows activatie

Momenteel wordt gebruik gemaakt van MAK activatie. Hoewel dit in veel gevallen werkt geven de servers van de gemeente Zutphen toch activatie foutmeldingen.



Fig. Windows activatie melding

Eventlog melding

Icon	Tijdstempel	Gebeurtenis	Id	Resultaat
Informatie	22-03-2013 14:26:18	Winlogon	4101	Geen
Waarschuwing	22-03-2013 14:24:52	Security-Licensing-SLC	8196	Geen
Fout	22-03-2013 14:24:51	Security-Licensing-SLC	1014	Geen
Fout	22-03-2013 14:24:51	Security-Licensing-SLC	8200	Geen
Informatie	22-03-2013 14:24:50	Security-Licensing-SLC	1011	Geen
Informatie	22-03-2013 14:24:49	Security-Licensing-SLC	1024	Geen
Informatie	22-03-2013 14:24:45	CertificateServicesClient	1	Geen

Gebeurtenis 8196, Security-Licensing-SLC

Algemeen | Details

De planner voor licentieactivering (SLUINotify.dll) kan niet automatisch activeren. Foutcode: 0xC004C020

Logboeknaam:	Toepassing	Geregistreerd:	22-03-2013 14:24:52
Bron:	Security-Licensing-SLC	Taakcategorie:	Geen
Gebeurtenis-id:	8196	Trefwoorden:	Klassiek
Niveau:	Waarschuwing	Computer:	xenapp_25.master.local
Gebruiker:	n.v.t.		
OpCode:	Info		
Meer informatie:	Online Help		

Fig. eventlog meldingen

advies

Het is raadzaam over te gaan op KMS activatie voor de Windows 2008.

3.4.2. Zone data collector

Er zijn momenteel geen dedicated zone data collectors en STA servers voor afhandelen van de aanvragen van de interne en externe webserver ingericht. De geprovisionede servers welke ook sessies hosten handelen ook dit verkeer af.

Hoewel dit vanuit Citrix niet direct als best practise wordt aangegeven bij een farm met de hoeveelheid servers welke bij de gemeente Zutphen in gebruik zijn, wordt het gebruik van dedicated zone data collectors en STA servers wel geadviseerd om de onderstaande redenen

- Remote inlogmogelijkheden voor beheer bij uitval Provisioning omgeving
- Scheiding tussen workers en management servers
- Rol kan samen met webserverrol op dezelfde machine geïnstalleerd worden dus geen extra licenties noodzakelijk
- Makkelijker troubleshooten bij problemen

3.4.3. Applicatie Virtualisatie

Momenteel wordt gebruik gemaakt van Citrix application streaming. Hoewel dit applicatie virtualisatie pakket wel werkt zijn er veel klachten over snelheid vanuit de gebruikers. De beheerders hebben reeds de keuze gemaakt om het bestaande application streaming te vervangen door APP-V 5. Dit naast de verbetering in snelheid ook meer applicaties kan virtualiseren dan Citrix Application Streaming

advies

Let bij uitvoering van de transitie van Citrix Application Streaming naar Microsoft APP-V 5 dat dit pas ondersteund wordt vanaf RES Workspace Manager 2012 SR3 welke eind mei gereleased wordt.

3.4.4. Network load

Er gaat veel verkeer over de virtuele netwerkkaart van de Citrix servers.

Netwerk 133 Mbps 7% netwerkgebruik					
Image	Proc...	Adres	Verzenden (byte...	Ontvangen (byte...	Totaal (bytes/min)
uniface.exe	7672	vdboracle	1.844.397	7.534.793	9.379.190
System	4	vfilerfsr	1.084.634	7.660.374	8.745.008
System	4	vappsrv02	423.810	2.175.658	2.599.468
...

Fig. network load

Gezien de hoge load waarbij gewoon verkeer en het stream verkeer over dezelfde netwerkkaart lopen kan een hoge belasting van de netwerkkaart ervoor zorgen dat de server traag reageert. Dit omdat de pakketjes van de Provisioning servers op hun beurt moeten wachten en er ook niet direct door komen.

Waarschijnlijk ligt de oorzaak voor de traagheid en instabiliteit in de netwerkkaart driver. En zal dit opgelost zijn door een upgrade van de netwerkkaartdriver of de vervanging van de hypervisor.

Advies

Indien na upgrade/vervanging van de hypervisor nog steeds problemen optreden met traagheid kan de oplossing zijn om een apart streaming netwerk te maken (apart VLAN op de switches en hosts). via dit netwerk zal dat al het verkeer voor het provisionen van de servers gestuurd wordt terwijl de LAN interface alleen voor LAN verkeer gebruikt wordt.

3.4.5. Traagheid door virusscanner

Op alle XenApp servers staat de trend micro officescan client. Wat opvalt is zodra de virusscanner zich bemoeit met het besturingssysteem lopen de reactietijden van de processen binnen de virtuele machines op tot tijden in secondes. Zodra de virusscanner klaar is met scannen zakken de tijden weer terug naar "normale" waardes.

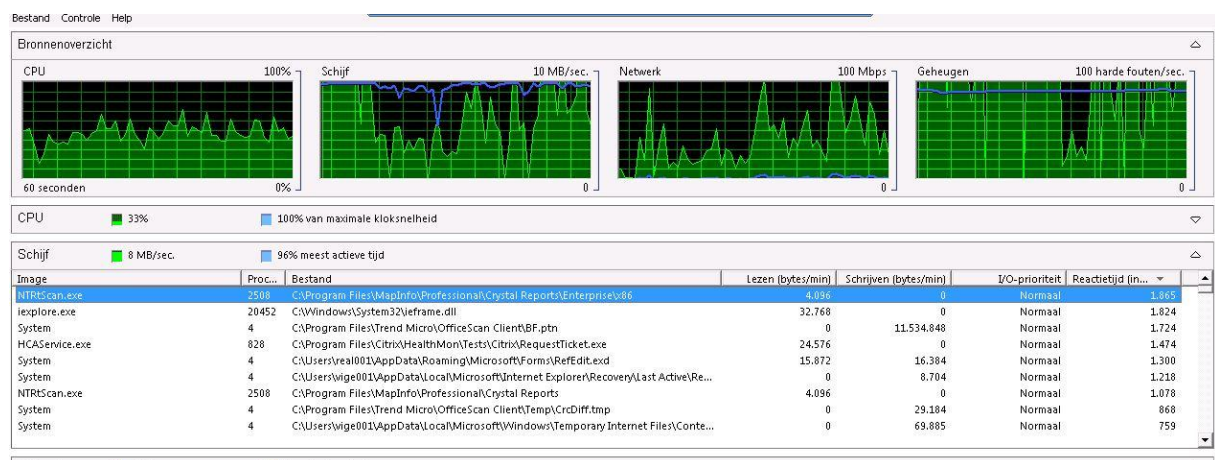


Fig. reactietijd die ntrscan.exe veroorzaakt.

De instellingen van de virusscanner zijn wel aangepast zodat deze niet alles zou moeten scannen alleen werken de exclusions die aangegeven zijn niet goed waardoor uitgesloten onderdelen van het systeem toch gescand worden.

Advies

Er zijn een aantal oplossingsrichtingen voor dit probleem.

1. Uitzoeken waarom de virusscanner dit soort gedrag vertoond.
2. Deinstalleer uit een kopie van de vdisk image de virusscanner en laat 1 server op dit image meedraaien in productie. Indien mensen op deze server minder klagen over traagheid kan hier verder naar gekeken worden
3. Stel de virusscanner in voor minimaal scannen (alleen Writes in de Documents and settings map, lees en schrijf USB en Writes op de netwerkdrives)

Vanwege de grote vertraging die het scannen heeft op de werking van de XenApp omgeving is de-installatie van de virusscanner de optie die de meeste performancewinst oplevert. Echter dit creëert weer een security risk, immers de usb sticks en de CIFS shares worden niet gescand op virussen. Dit is op te lossen door een Trend Micro Serverprotect for storage systems appliance te installeren welke de taken van de virusscanning op de CIFS shares overneemt. Indien dit een te grote aanschaf is kan ook overwogen worden toch weer een Windows machine (of meerdere) als fileserver in te gaan zetten en hier een virusscanner op te zetten.

Gezien de impact die bovenstaand heeft op de omgeving is het uitzoeken van de oorzaak voor het niet goed functioneren van de virusscanner ook een optie samen met het aanpassen van de scanfunctie zodat alleen het hoogstnoodzakelijke wordt gescand.

3.4.6. Virusscanner beheer

Momenteel wordt gebruik gemaakt van CIFS om bestanden aan te bieden aan gebruikers. Er wordt geen gebruik gemaakt van Trend Micro Deep Security om de bestanden die van en naar de CIFS shares gaan te scannen. Dit is opgelost door op alle servers (waaronder Citrix) een virusscanner te installeren. Een van de problemen is dat elke geprovisionede server aanmeldt het hetzelfde GUID heeft omdat ze geprovisioned zijn (en dus gelijk).

advies

los dit op door onderstaand uit te voeren (gebaseerd op deze blogpost:

<http://www.michelsteveldmans.com/installing-trend-micro-officescan-vdisk/>)

- Installeer de Trend Micro OfficeScan client in de vDisk.
- kies voor Unload OfficeScan.
- zet de Trend Micro services op "manual".

Maak een startupscript met onderstaande waardes

```
REG ADD HKLM\SOFTWARE\ TrendMicro\PC-cillinNTCorp\CurrentVersion /v GUID /t  
REG_SZ /d "0d8ffd52-a5a7-48c5-9313-ecd%COMPUTERNAME%" /f
```

net start tmlisten

net start ntrtscan

Dit script verandert de waarde van de guid in iets waar de pc naam in staat. Deze is uniek! Zorg dat dit script autostart elke keer als je een server start. En de servers zullen zich allemaal met een unieke guid online aanmelden.

3.4.7. Update/Upgrade XenApp

Momenteel wordt binnen de Citrix omgeving gewerkt met hotfix rollup pack 01. Ondertussen heeft Citrix diverse updates/upgrades en featurepacks uitgebracht voor XenApp 5 voor Windows 2008. Hoewel de hotfixes niet allemaal geïnstalleerd hoeven te worden is de installatie van Feature Pack 3 wel aan te raden omdat hiermee de mogelijkheid tot hotplug gebruik van USB sticks mogelijk wordt gemaakt.

Momenteel kunnen USB sticks in de sessie alleen gebruikt worden als deze reeds zijn ingeplugd voor de gebruiker de sessie start. Door de XenApp omgeving te upgraden naar Feature Pack 3 is het mogelijk om voor de gebruikers hotplug USB functionaliteiten aan te bieden.

Mocht de upgrade teveel impact hebben kan ook gebruik worden gemaakt van de Citrix dynamic USB tool (<http://support.citrix.com/article/CTX112588>) deze tool moet op elke thinclient geïnstalleerd worden en maakt het mogelijk via aanbieden van USB sticks als mappen binnen een bestaande map om toch een hotplug USB stick mogelijkheid aan te bieden.

Daarnaast kan na upgrade ook gebruik worden gemaakt van webcams en softphones in de Citrix sessie. Ook kan met deze upgrade gebruik gemaakt worden van HDX componenten voor bijv. het redirecten van video en flash rendering naar de thinclient. Hierdoor wordt de CPU van de thinclient gebruikt voor het renderen van een flash filmpje (van YouTube bijvoorbeeld) en wordt op deze manier de gebruikte CPU kracht en het geheugengebruik van de Citrix Server verlaagt.

Langere termijn oplossing is de upgrade van de omgeving naar Windows 2008R2 met XenApp 6.5!

3.4.8. Citrix web interface

Momenteel worden gebruikers die willen inloggen op de Citrix omgeving bediend door één webserver. Bij uitval van deze server kunnen mensen van zowel extern als intern niet meer inloggen op de omgeving.

Advies

Configureer de 2^e webserver en koppel deze via Microsoft network load balancing aan vWeb01 om hierdoor een redundante webserver oplossing te bieden.

3.4.9. Kleine punten

Adobe Acrobat

Adobe Acrobat update service deze staat aan op de Citrix servers. Deze kan uitgezet worden.

WSUS updates

De Citrix servers lopen achter qua Windows updates (laatste update oktober vorig jaar).

Taakbeheer

Momenteel wordt taakbeheer aan de gebruikers aangeboden om zelf applicaties die blijven hangen te killen. Het is verstandiger hiervoor het freeware programma Task nanny te gebruiken. Dit programma haalt alle overbodige knoppen weg waardoor gebruikers alleen nog maar applicaties kunnen killen.

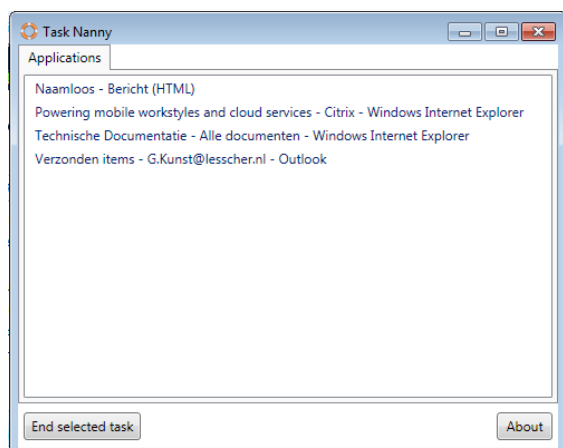


Fig. tasknanny

3.5. Workspace manager

RES Workspace Manager wordt gebruikt voor het aanbieden van de diverse applicaties en de algemene desktop aan de gebruiker. De inrichting van de Workspace Manager omgeving is goed, er zijn een paar kleine verbeterpunten

3.5.1. Veel globaal goedgekeurde executables

Er zijn veel bestanden globaal goedgekeurd (dus voor alle gebruikers en in alle sessies) terwijl deze beter op gebruikersgroepen en/of op aangeboden applicatie kunnen worden goedgekeurd. Dit zorgt voor meer overzicht en minder kans dat een medewerker per ongeluk een applicatie kan starten die hij eigenlijk niet hoor te kunnen starten.

Advies

Pas de lijst moet goedgekeurde executables aan zodat deze meer gericht per applicatie worden goedgekeurd.

3.5.2. Dubbele en oude goedgekeurde apps

Er staan in de globaal goedgekeurde applicatie lijst een groot aantal dubbel goedgekeurde applicaties en ook een aantal welke niet meer gebruikt worden. Bij elke inlog van een gebruiker moeten deze applicaties allemaal in de sessie informatie van de gebruiker geladen worden. Dit kan voor langere inlogtijden zorgen en maakt het beheer onoverzichtelijk.

Advies

Werk de lijst bij en haal dubbele en niet gebruikte applicaties uit deze lijst om de logintijd te versnellen.

3.5.1. Profielen

Momenteel wordt er gebruikt gemaakt van een mandatory profile i.c.m. Workspace Manager.

Hoewel deze combinatie in veel gevallen goed werkt zijn de medewerkers niet tevreden over de inlogsnelheid van de omgeving. Daarnaast geeft het voor de beheerders extra beheer last om bij elke nieuwe applicatie alle registerwaardes en profielinstellingen goed uit te zoeken en veilig te stellen. Ook geven de redirections foutmeldingen in de eventlogging op de Citrix servers. Dit kan ook gedeeltelijk voor de vertraging zorgen.

Advies

Kijk waar de foutmelding tijdens inloggen vandaan komt en los deze op. Kijk daarna of de inlogsnelheid verbetert is.

Upgrade de hypervisor en kijk of de verbetering van doorvoersnelheid op de disken de traagheid oplost.

Indien dit niet het geval is stap af van de mandatory profielen en ga gebruik maken van Citrix Profile Management. Deze oplossing van Citrix zorgt ervoor dat bij het inloggen van een gebruiker alleen die onderdelen van het profiel geladen worden die nodig zijn voor juiste werking van het profiel (profile streaming). Overige bestanden worden opgehaald van de profiel directory indien nodig. Indien naast de implementatie van profile management ook gekozen wordt voor slim redirecten van onderdelen uit het profiel zoals desktop, downloads, favorites etc. kan de inlogtijd verlaagt worden.

3.5.2. Look and feel

Het bureaublad van de gebruikers kan een andere look and feel krijgen door gebruik te gaan maken van themes (thema's) waardoor een Windows vista/7 uiterlijk gecreëerd kan worden. Dit geeft de gebruiker een betere beleving doordat het uiterlijk overeenkomt met wat (meestal) thuis ook te zien is. Hiervoor zal overgestapt moeten worden van de RES Workspace Manager shell naar de Windows shell

3.5.3. Versie

Momenteel wordt gebruik gemaakt van Workspace Manager 2011. De laatste release van dit moment is Workspace Manager 2012 SR2. Binnenkort komt SR3 uit (eind mei).

Advies

Upgrade naar de SR3 versie van Workspace Manager zodra deze uit is. Hierin is ook de ondersteuning van APP-V 5 meegenomen.

4. Conclusie en vervolgstappen

In dit hoofdstuk worden de stappen aangegeven die n.a.v. de gevonden verbeterpunten uitgevoerd kunnen worden.

4.1. Algemene conclusie

Hoewel de omgeving van de gemeente Zutphen in de basis goed is ingericht zijn er een aantal verbeterpunten. De belangrijkste is het zo snel mogelijk vervangen van het huidige virtualisatie platform (XenServer). Deze is de oorzaak van de meeste instabiliteit en traagheidsproblemen binnen de omgeving.

Daarnaast is het upgraden van de XenApp omgeving van Windows 2008 32 bit naar Windows 2008R2 64 bit i.c.m. XenApp 6.5 de volgende stap om winst te boeken. De meeste applicaties ondersteunen momenteel een 64 bit architectuur. Omdat de limiet van 4 GB geheugen voor 64 bit machines niet meer gelden zullen veel problemen veroorzaakt door geheugentekort op de virtuele machines dan voorbij zijn.

Daarnaast zijn er nog enkele nice to have verbeterpunten zoals het upgraden van Provisioning en het aanpassen van de gebruikersprofielen.

4.2. Vervolgstappen

4.2.1. Vervanging hypervisor

Gezien de problemen met de huidige versie van XenServer is het noodzakelijk deze te vervangen. Hierbij kan gekozen worden om de huidige versie te upgraden naar 6.1 of te kiezen voor een ander virtualisatie platform (Hyper-V of VMWare).

Hoewel de XenServer licenties reeds in het licentiepakket van de gemeente Zutphen aanwezig zijn is het, gezien de hypervisors die in de markt worden aangeboden en de keuzes die andere bedrijven en instellingen hierin maken, verstandig om nogmaals de keuze van hypervisor te heroverwegen.

Dit is het tijdstip voor de Gemeente Zutphen om de hypervisor keuze te heroverwegen omdat de huidige virtualisatie omgeving nog relatief in de beginfase zit:

- Er is geen centrale storage voor de gevirtualiseerde servers
- Momenteel is er geen management omgeving ingericht anders dan XenCenter en Zabbix.
- Hosts zijn niet in pools gezet of anderszijds samengevoegd

Kortom elke host staat in principe op zichzelf.

De mogelijkheden van Hyper-V worden vooral aangeboden vanuit Microsoft System Center die als apart product aangeschaft en geïmplementeerd moet worden.

Microsoft System Center 2012 bestaat uit zestal onderdelen. Hieronder worden een drietal onderdelen die relevant zijn voor een gevirtualiseerde omgeving kort beschreven:

System Center Operations Manager (SCOM)

Deze monitoring tool is de overkoepelende laag die de complete infrastructuur kan monitoren. Op deze manier zal de beheer organisatie altijd op de hoogte zijn van de health status en tijdig actie kunnen ondernemen. De health status is op te vragen vanuit SharePoint Dashboards en Dynamische Visio tekeningen. Microsoft is daarnaast voortdurend aan het (door)ontwikkelen van management packs om zoveel mogelijk 3rd party software te kunnen ondersteunen.

System Center Virtual Machine Manager (SCVMM)

Dit onderdeel wordt gebruikt voor het daadwerkelijk beheren van de virtuele machines en is te vergelijken met XenCenter. Grote verschil is dat XenCenter werkt vanuit een client en dat de intelligentie in de hypervisor zit (pool master regelt alle zaken). Bij VMM wordt dit vanuit een aparte beheer virtuele machine gedaan. VMM heeft een aantal voordelen de belangrijkste is:

- Gebruikers (bijvoorbeeld applicatieontwikkelaars) kunnen via toegang tot de VMM client de eigen servers herstarten en beheren maar niet de overige servers.
- Makkelijk opzetten OTAP straat
- Beheren virtuele omgeving (servers aanmaken en verwijderen)

Conclusie

Hyper-V is met de komst van Windows 2012 en Hyper-V 3 technisch een volwassen alternatief voor VMWare VSphere en XenServer. Mede door de gunstige pricing is het een interessante oplossing om in te zetten als virtualisatie oplossing. In combinatie met System Center 2012 kan vanuit één productlijn een totale oplossing gevirtualiseerd, beheerd, gemonitord en gebackuppeld worden. Hierdoor kan een hoge mate van zekerheid en up-time gegarandeerd worden. Hyper-V in combinatie met System is zeer voordelig geprijsd wanneer het gecombineerd wordt met Windows Server Datacenter licenties.

Daarnaast lijkt Citrix de focus verloren te hebben op het XenServer platform. Dit omdat er momenteel weinig nieuwe ontwikkelingen bekend gemaakt worden en ook is het vanaf versie 6.0 mogelijk de XenServer hosts te beheren via Microsoft System Center Virtual Machine Manager. Dit wijst op verdere intensieve samenwerking met Microsoft op hypervisor gebied.

4.2.1. Upgrade XenApp omgeving

De huidige XenApp omgeving is gebaseerd op een X86 platform (32 bit). Dit is een verouderd platform en heeft geheugenbeperkingen waar binnen de bestaande omgeving problemen mee ondervonden worden.

Hoewel Windows 2012 recentelijk is uitgekomen, is het niet aan te bevelen om voor wat betreft de XenApp omgeving al op dit nieuwe platform over te stappen:

- Applicatie compatibiliteit
- Citrix software nog niet beschikbaar voor Windows 2012
- Veranderde look and feel
- RES Workspace Manager nog niet geschikt voor Windows 2012

Bij het merendeel van de XenApp omgevingen (ook binnen overheidsinstellingen) wordt op dit moment gebruikt gemaakt van Windows 2008R2 en XenApp 6.5. Ondertussen zijn bijna alle applicaties geschikt voor 64 bit installatie en indien ook gebruik gemaakt wordt van APP-V en een silo server voor enkele legacy applicaties is de omgeving van de Gemeente Zutphen prima geschikt om over te gaan.

Omdat Windows 2008R2 niet ondersteund wordt binnen XenApp 5.0 zal er een nieuwe farm geïnstalleerd moeten worden. XenApp 6.5 is de laatste versie en Windows 2008R2 wordt ondersteund door deze versie. Met XenApp 6.5 zijn er 2 rollen die ingezet gaan worden nl. de controller rol en de session-host rol. Hieronder de verschillen in rollen:

XenApp Server Mode	Can host user sessions?	Can be used as a data collector?	Can run XML service?	Can participate in elections?
Default Install (Controller)	✓	✓	✓	✓
Session-Host (Session-only)	✓	✗	✗	✗

De server met de controller rol zal niet voorzien worden van applicaties. De server zal de aanvragen van de Web interface en de CAG afhandelen en zal tevens verantwoordelijk zijn voor de management taken van de XenApp farm. Deze server zal niet meegenomen worden in Provisioning.

De server met de session-host rol heeft een versie van XenApp die alleen maar sessies van gebruikers bevat. Het voordeel i.c.m. Citrix Provisioning is dat de servers veel minder XenApp-data (Local Host Cache) moeten kopiëren en dat er minder database transacties gedaan moeten worden. Tevens zal een geprovisionede server veel sneller starten en afsluiten in de session-host rol.

Er kan wel gebruik gemaakt worden van de bestaande web interface. Gebruikers moeten alleen op een ander icoontje klikken tijdens de testfase.

Stappenplan migratie

1. Aanschrijven leveranciers of software ondersteund wordt op basis van 2008R2 en/of APP-V
2. Bepalen basis installatie (welke applicaties moeten geïnstalleerd worden in basis image)
3. Installatie basis omgeving
4. Printerdrivers X64 geschikt
5. Nieuwe RES Workspace Manager omgeving opzetten
6. APP-V packages maken van overige applicaties
7. Pilot
8. Uitrol

Let op dat ook de Citrix license server geüpgraded wordt naar de laatste versie voorafgaand aan de upgrade.

4.2.2. Upgrade Provisioning

Zoals eerder beschreven kan een upgrade van Citrix Provisioning naar versie 6.1 veel beheer voordelen opleveren. De upgrade van de omgeving kan relatief simpel gedaan worden. De installatie kan volledig naast de bestaande servers gedaan worden op een tweetal nieuwe servers. Hierna kan de van een kopie van het bestaande image de Provisioning Client software geüpgraded worden en kan de omgeving in productie worden gezet.

Installeer Citrix Provisioning versie 6.1.16 (<http://support.citrix.com/article/CTX135672>). Deze heeft een aantal bugfixes welke belangrijk kunnen zijn voor de omgeving. Tijdens de installatie van de nieuwe servers wordt de bestaande database geüpgraded waardoor de oude Provisioning servers niet meer kunnen connecten en deze op cache gaan draaien. Er kunnen dan dus geen updates op de Provisioning omgeving worden doorgevoerd!

Let op dat ook de Citrix license server geüpgraded wordt naar de laatste versie voorafgaand aan de upgrade!

5. Vervolg

In deze netwerkscan rapportage komen een aantal belangrijke verbeterpunten naar voren. De verbeterpunten met de grootste impact zijn het vervangen van de Hypervisor en de upgrade naar de laatste versie van Citrix XenApp. Lesscher IT kan hier indien gewenst in ondersteunen. Een eerste stap zou het opstellen van een Technisch Ontwerp kunnen zijn. Doormiddel van een Technisch ontwerp wordt duidelijk wat de impact van de netwerkaanpassingen zijn. Een technisch ontwerp beschrijft de huidige en nieuwe situatie die in samenwerking met de Gemeente Zutphen vastgesteld wordt, de logische stappen daarnaartoe en de benodigde middelen en doorlooptijd.