Configuring and Troubleshooting Windows Server 2008 Application Infrastructure

1. Configuring Storage for Windows Server 2008 Applications

Storage, opslag van data kan op meerdere manieren:
- Direct Attached Storage, built in storage, decentraal
- Network Attached Storage, goedkoop, centraal, traag door NAS eigen OS dat per file de data afhandeld
- Storage Area Network, snel door access op block level, het is wel duurder en vereist meer expertise. Het is centraal en gedeeld over meerdere servers.
    * Fiber Channel: meestal over glas, op OSI 1 en 2 niveau, nadeel nieuwe lijnen en routers leggen, heel snel
    * ISCSI: meestal op koper, op TCP/IP OSI 3 en 4 niveua, kan op bestaand netwerk. veelal gebruikt.
        + ISCSI initiator is een server, die praat en mapt als netwerk drive Z:\
        + ISCSI target is datacenter storage, geeft LUN gedeelte gekoppeld aan Z:\ van een server
        + ISCSI store fabric, zijn de tussenliggende lijnen en routers

OSI model lagen:
7 application
6 presentation
5 session
4 transport TCP
3 netwerk IP
2 datalink ethernet / 802.11
1 physiek

dubbele netwerk kaart voor server:
- multipath i/o voor failover, dubbel uitvoeren voor uitval
- teaming is 2 netwerkkaarten als 1 beschouwen, voor performance en load balancing

een virtuele harddisk (.vhd bestand) kan fixed (meteen 100MB) en dynamically expanding zijn (startend bij 1MB), allebei ingesteld op 100MB maximaal
daarnaast heb je een read only base disk en meerdere wijzigbare differencing disks, dus meerdere kleine differencing disks kunnen gebaseerd zijn op 1 grote base disk met het OS erop.
windows server 2008 R2 backup schrijft ook naar .vhd bestanden.
op de enterprise editie kun je native booten vanaf een .vhd bestand

De PC opstart cyclus is:
1 bios /uefi
2 master boot record
3 bootsector

en dan voor XP / Windows 2003:
4 ntldr
5 boot.ini
6 ntdetect.com
7 ntoskrnl.exe

en dan voor Win7 / Windows 2008R2:
4 bootmanager
5 bcdedit
6 winload op physieke schijf of .vhd

Op Windows 7 kun je in XP mode draaien. deze start vpc 2007 op met XP erop. met daarop weer je legacy XP applicatie erop. de start knop van de XP applicatie integreerd met de menu structuur van de onderligende Windows 7

RAID is Redundency op Disk
0 is striping, extra availibility door stukken data te verdelen over disks (stripes)
1 mirroring, het dubbel wegschrijven van data op 2 disks
5 striping + parity, de laatste disk is de parity disk, waar een hash stripe wordt weggeschreven om data te kunnen terugrekenen van een data stripe van een andere disk

2. Configuring High Availability for Windows Server 2008 Applications

Hoe een client zich aanmeldt in een netwerk:
Een client start op en doet een broadcast naar een DHCP server.
Van de DHCP server krijgt de client een ip adres en de naam en het ip adres van de DNS server.
De client meldt zijn nieuwe ip adres aan bij de DNS server.
De client vraagt aan de DNS server de naam en het ip adres van de DC, de domain controller.
De client meldt zich aan aan de domain controller voor authenticatie van de gebruiker middels AD, Active Directory.
De client is beschikbaar op het netwerk met een ingelogde gebruiker.

High Availability kan bereikt worden door 3 zaken:
- fault tolerance = dubbel uitvoeren van servers ter voorkoming van uitval
- load balance = werkload verdelen over meerdere servers
- wan links = geografische spreiding voor plaatselijke goede performance

Network Load Balancing kan met een Network Load Balancing Cluster
1 virtueel ip adres voor tot en met 32 machines met elk een physiek ip adres.
als er een call van de client komt, gaat die naar alle 32 servers.
alle nodes hebben node software om te beredeneren of hij het oppakt, of de node ernaast, als die UP is en minder druk is.
voor deze onderlinge communicatie hebben ze veelal een extra netwerkkaart met een eigen prive netwerk verbonden met elkaar met een switch.
gezamenlijk bereiken ze dan 1 database of storage server.

Een HUB connect meerdere clients aan elkaar en stuurt informatie van iedereen naar iedereen.
Een Switch is slimmer dan een HUB en knoopt 2 clients tijdelijk point 2 point aan elkaar indien de Switch ziet dat ze verkeer met elkaar willen hebben.

Network load balancing is stateless, voor schaalbaarheid van processen, alle nodes draaien met gelijke workload.
data van de state delen kan bijvoorbeeld wel met asp.net door de session state op te slaan op een aparte state server of in een sql server state database,
maar dan wordt de state behoud opgelost op applicatief niveau.
Met het standaard state bijhouden in-process, kan de data van de state niet gedeeld worden.

Een fail over cluster is statefull, de state wordt overgenomen door een andere node.
load balancing van de workload is er niet, want de applicati draait maar op 1 node.
het is pure fail over, het overnemen van de applicatie en state naar een ander beschikbare node.
om de state over te dragen naar een andere node moet er wel een shared storage zijn voor alle nodes. Alle nodes van een fail over cluster hebben een physiek ip adres en het cluster zelf heeft ook een eigen virtueel ip adres, welke aangeroepen wordt door de clients.

Elke node heeft een stem. als er genoeg stemmen / nodes (quorum) over is wordt er gefailovered.
bijvoorbeeld als de meerderheid van nodes + 1 quorum disk over zijn.
anders gebeurt er een gecontroleerde shut down van de applicatie om bijvoorbeeld corruptheid van data op disk of op de database te voorkomen bij een ongecontroleerde shut down, wanneer de laatste node klapt.
op de quorum disk staat de configuratie van het gehele cluster.

3. Configuring Remote Desktop Services, Managing Availability of Remote Desktop Services & Delivering Applications to Remote Users

WinRM: Remote Management enabelen op de server = zet de firewall poort open voor management en start een listener
WinRS: Tool op de Client voor Remote Management = om remote mangement te doen op een WinRM server

Core Server = een minimale server met een command prompt
Full Server = een volle server met een desktop

Virtualisatie kan op verschillende niveau's:
- Hardware (Hyper-V / VMWare / Citrix Xen / VPC / VDI) gehele OS met applicaties virtueel aangeboden op gevirtualiseerde hardware
- Presentation (Remote Desktop Services / Terminal Services) processing op de server, presentatie op de client
- Desktop
    * Application (App-V) gestreamed een geinstalleerde applicatie stukje voor stukje binnenhalen op de client, maar toch al beginnen te draaien, beveiligd in zijn eigen sandbox
    * Userstate (Roaming Profiles)
    * User Experience, een verzamelnaam voor virtualisatie vanaf Windows Server 2012
    * OS (VDI / VM Isolation) met desktops centraal aangeboden vanuit een datacenter
    * Netwerk (Hyper-V) virtueel een netwerk nabootsen

Elke administrator kan iedere server met 2 administrators tegelijk met windows standaard client RDP overnemen. hier is Remote Desktop Services niet voor nodig.

Remote Desktop Services bestaat uit:
- Remote Desktop Host = Hosting server voor applicaties of desktops
- Remote Desktop Client = maakt vanuit de client connectie met een host
- Remote Desktop Licensing = service die de licensing online bij Microsoft bijhoud, de License Server zelf heeft ook een eigen betaalde licentie nodig.
- Remote App = RDP windows venster voor 1 applicatie die op de host draait
- Remote Virtualisation Host = met Hyper-V complete virtuele machines aanbieden vanuit een Host
- Remote Desktop Web Access = geen .rdp file of .msi uitrollen op de client om op te starten, maar een web pagina met een menu
- Remote Desktop Gateway = over internet komen er https RDP requests binnen. deze worden uitgepakt en intern op het netwerk als RDP commando's doorgestuurd naar een Host.
- Remote Desktop Connection Broker = controller van meerdere remote desktop hosts, oftewel een farm, met ingebouwde load balancing

Je kunt iedere RDP Desktop sessie een eigen ip adres geven met ip virtualisatie.
Met Group Policies kun je voor elke remote server / user dezelfde instellingen toepassen.

4. Implementing IIS Web Applications, Implementing FTP and SMTP & Managing and Securing IIS

IIS 7.0 is standaard op Server 2008. IIS 7.5 is standaard op Server 2008 R2.

IIS is een listener de antwoord geeft op Requests van clients.
Deze requests kunnen van het type: http, https, ftp, sftp of smtp zijn.
Als web server processed IIS de web requests en zet deze om tot een response waar de client op basis van statische (html) of dynamische (asp.net met daarachter een database) data.
meerdere IIS web applicaties draaien allemaal apart op de server binnen eigen App Pools onder een ingesteld worker process account.
Worker process accounts kunnen zijn:
- local service: local user
- local system: local admin
- network service: network user account van de computer zelf

De files van een web Site staan physiek op disk, standaard op C:\inetpub\wwwroot. Ergens anders kan ook. En er een gehele ander naam aan geven ook met virtuele directories.

Clients kunnen zich authenticeren aan IIS door middel van:
- anonymous: geen authenticatie
- basic: cleartext username en password
- certificate
- digest: username en hashcode
- windows: ntlm of kerberos

Webdav server is een browser gebaseerd file systeem.

Je kunt op 3 manieren IIS instellingen managen:
- met de IIS manager schermen, hiermee kun je ook andere IIS web servers remote beheren
- met appcmd.exe, dit is een legacy command line tool, niet meer gebruiken
- powershell, ook command line, veel uitgebreider, en hier gaan Microsoft naar toe.

dism.exe is een command line tool om windows features te enablen / disabelen op de server core, zoals windows onderdelen of het .Net framework.
want, windows bestaat uit modules, die normaliter beheerd worden in de server manager bij roles & features.
dus bestaat windows auto updates met losse files niet meer.

Encryption moet vertrouwelijk zijn (envelope) en betrouwbaar zijn (signature)
Er zijn 3 manieren:
- Hash: 1 way / fast
  Er wordt een niet omkeerbare hash gecreerd vanuit data behorende bij die data. de data is leesbaar, maar wel te controleren op correctheid.
- Symmetrisch: 2 way / 1 key / fast
  1 key om te encrypten, en dezelfde key om te decrypten, is op lange termijn kraakbaar (huidige datacenter kracht: 2 jaar), maar wordt maar tijdelijk (10 minuten) gebruikt.
  de vraag is alleen: hoe krijg je die 1e key met elkaar gedeeld, zonder dat iedereen hoort wat de key is.
- A- Symmetrisch: 2 way / 2 keys / slow
  public key en private key horen bij elkaar
  private key heb je alleen zelf, public key share je met de hele wereld, een public key is een .cer certificaat.
  je kunt ook over de public key van een ander beschikken

Internet bankieren:
de communicatie is symmetrisch op basis van 1 key.
het uitwisselen van die 1e key is a-symmetrisch.

het uitwisselen van de sleutels is a-symmetrisch:
de bank heeft een IIS server met een eigen private en public key.
een public key certificaat kan gesigned zijn door een 3e partij, bijvoorbeeld diginotar, om voor de betrouwbaarheid van de afkomst van de bank te garanderen.
de public key gaat naar de klant van de bank.
de klant van de bank versleutelt zijn eenmalige wachtwoord (gegenereerd vanuit zijn reader met zijn pasje en zijn voorafgesproken pincode) met de public key van de bank.
de bank decrypt / ontsleuteld de het wachtwoord van de klant van de bank met zijn private key.
de bank constateerd aan de code van het pasje en de pincode dat het echt die 1e klant van de bank is.

de rest van de communicatie is symmetrisch:
de financiele data wordt versleuteld, met de gezamenlijke key en aan de andere kant met dezelfde key weer ontsleuteld. dit gaat veel sneller.

Een certificaat is uitgegeven door een certificate authority (CA), en daarna weer door een hogere CA. tot en met een te vertrouwen ROOT CA, zoals Verisign of de staat der Nederlanden.
Een browser controleert een certificaat op:
- naam, klopt het certificaat naam met de web site naam?
- experition date, is het certificaat niet verlopen?
- trustable root, staat de root CA, zoals verisign, of de staat der Nederlanden wel in de browser zijn trusted root CA's?
- CRL, staat het ceritficaat of de root CA ondertussen niet op een zwarte lijst?

9. Implementing SharePoint Foundation 2010

Share Point is een centraal punt om data te delen. Voor Communication, Sharing en Collaboration.
De beschikbare versies zijn Foundation (gratis), Server Standaard en Server Enterprise.
SharePoint Foundation 2010 is gebaseerd op IIS 7.0, ASP.Net, Server 2008 en Sql Server 2008.
SharePoint integreert met:
- Microsoft Active Directory Right Management Services, om te voorkomen dat data buiten het bedrijf komt, niet gemailt en niet geprint kan worden.
- Microsoft Active Directory Federation Services, ten behoeve van single sign on op het gehele internet.
- Office en Exchange
- Databases

Een SharePoint Site kan een boomstructuur van meerdere Site Collections hebben, en uiteindelijk daaronder bestaan uit Web Applications.
SharePoint biedt het delen van informatie en bestanden, het zoeken en bestand versiebeheer.

10. Windows Streaming Media Services

In plaats van het downloaden van data, bijvoorbeeld video's, kun je data ook streamen.
Wanneer de eerste data binnenkomt wordt de video al getoond. Niet pas wanneer de gehele video gedownload is.
Er wordt wat reeds binnengehaald is aan video op de client vooruit gebuffered om netwerk delays op te kunnen vangen door dan tijdelijk uit de buffer de video af te spelen.
Multicast streaming betekent dat meerder gebruikers dezelfde media stream kunnen aftappen.

De Windows Media Services Center kan video's op disk gestreamed aanbieden.
De Encoder kan alle formaten omzetten naar het Windows Media Format.
De End User of Client kan met Windows Media Player de stream afspelen.

Protocollen voor Streaming Media zijn:
- RealTime Streaming Protocol (RTSP): vanaf Windows Media Player 9
- Hypertext Transfer Protocol (HTTP): alle versies Windows Media Player, op poort 80 door firewalls heen

Protocol Rollover betekent dat er tussen de client en de server afhankelijk van de omstandigheden het maximaal mogelijke beste protocol kiest.