Escola Universitària
Politècnica de Mataró

Centre adscrit a:

UNIVERSITAT POLITÈCNICA
DE CATALUNYA

Enginyeria Tècnica de Telecomunicacions: Especialitat Telemàtica

ESTUDI PER PROVA DE CONCEPTE D'ESCRIPTORIS VIRTUALS

Memòria

JOSÉ JUAN DÍAZ PÉREZ
JOSEP MARÍA GABRIEL SOLANILLA

PRIMAVERA 2015

TecnoCampus
Mataró-Maresme

Agraïments

Agrair al meu ponent Josep María Gabriel l'ajuda prestada i sobretot a la meva parella, família i amics el suport i comprensió.

Resum

S'ha fet un estudi de les opcions existents en el mercat de la virtualització d'escriptoris i s'ha triat la solució de Citrix perquè era la que millor cobria les necessitats heterogènia de la informàtica d'usuari de la universitat.

S'ha definit i desenvolupat els punts crítics i les peces necessàries per crear una prova de concepte de virtualització d'escriptoris i s'han dimensionat les necessitats hardware d'aquesta prova de concepte donat uns 50 usuaris tipus.

Índex.

Índex de figures.

Índex de taules.

Glossari de termes.

Appliance	Dispositiu hardware amb un sistema operatiu i unes funcionalitats tancades.
DNS	De l'anglès *Domain Name Server*, servidor de resolució de noms
Citrix XML	Servei emprat pels controladors de XenApp o XenDesktop per comunicar-se amb altres servidors
Citrix AppDNA	Software propietari de Citrix que donat un software instal·lador dóna com a resultat les plataformes on serà compatible
Director	Consola de XenDesktop encarregada de la monitorització de la plataforma
EMM	De l'anglès *Enterprise Mobile Management,* solució de gestió de dispositius mòbils on podrem gestionar el funcionament de les aplicacions mòbils (on poden escriure, amb quines altres aplicacions poden interactuar, etc.)
EUPMT	Escola Universitària Politècnica de Mataró
Flexcast	Nomenclatura Citrix per definir que des d'un punt d'accés es pot servir múltiples tipus de recursos: aplicacions, escriptoris compartits, escriptoris dedicats, etc.
FQDN	De l'anglès *Fully Qualified Domain Name*, nom complert resolt pels DNS
GPO	De l'anglès *Group Policy Object,* es tracta d'una política de grup de directori actiu
GSLB	De l'anglès *Global Site Load Balancing,* sistema mitjançant el qual un balancejador de càrrega permet el balanceig de serveis entre dos centres de càlcul diferents

HDX	De l'anglès *High Definition Experience*, és el nom que rep el protocol ICA de Citrix amb les noves funcionalitats de monitorització i rendiment multimèdia.
Heartbeat	Transaccions destinades a monitoritzar si un altre servei està funcionant correctament
Hipervisor	Capa de software que permet aïllar els recursos hardware de les màquines virtuals que s'estan executant a sobre del servidor
Host	En entorn virtual es refereix al servidor físic que allotja màquines virtuals
HSD	De l'anglès *Hosted Server Desktop,* entorn de virtualització de l'escriptori o aplicacions en la qual l'usuari fa servir una sessió dins d'un servidor compartit amb més usuaris
ICA	De l'anglès *Independent Computing Architecture,* és el protocol propietari d'aplicació i presentació de Citrix
IOPS	De l'angès *Input Output Operations Per Second,* és una de les mesures més importants a tenir en compte durant el dimensionament d'un emmagatzematge
IP	Direcció d'un dispositiu a una xarxa informàtica
LDAP	De l'anglès *Lightweight Directory Access Protocol,* es tracta d'un sistema de directoris
MCS	De l'anglès *Machine Creation Services*, es tracta d'un sistema de creació de màquines virtuals a partir d'una plantilla propietari de Citrix
MDM	De l'anglès *Mobile Device Management*, solució de gestió de dispositius mòbils on podrem gestionar són les funcionalitats pròpies del dispositiu. (paraules clau, encriptació, xarxes wifi, comptes de correu, aplicacions prohibides/obligatòries, etc.)
NAS	De l'anglès *Network Area Storage,* sistema d'emmagatzematge basat en fitxers

PFC	Projecte Final de Carrera
PoC	De l'anglès *Proof of Concept,* prova de concepte
PowerShell	Es tracta d'un interfaç de consola inclòs per el sistema operatiu Windows Server que permet l'execució i encadenació de comandes
PVS	Referència a Provisioning Server com a sistema de gestió d'imatges
PXE	De l'anglès *Preboot eXecution Environment,* és un sistema per arrancar, servir o instal·lar un sistema operatiu sobre un equip client
RADIUS	De l'anglès *Remote Authentication Dial-In User Service,* és un protocol de validació i autorització
Site	Nomenclatura específica de Citrix per definir una agrupació lògica de recursos per oferir un servei d'escriptori virtual
Studio	Consola de XenDesktop encarregada de la configuració i gestió de la plataforma
TFC	Treball Final de Carrera
Token	Dispositiu electrònic de seguretat que dóna a un usuari autoritzar un password variable
SaaS	De l'anglès *software as a service,* oferir una aplicació com un servei sense infraestructura local
SSL VPN	De l'anglès *Secure Socket Layer Virtual Private Network,* es tracta d'un protocol que permet comunicar remotament de forma segura les aplicacions que vagin encriptades sobre ell
URL	De l'anglés *Uniform Resource Locator,* en referència a la cadena de caràcters que fan que hem d'escriure en el navegar per arribar a una pàgina web en especial

VDA	De l'anglès *Virtual Delivery Agent,* es tracta de l'agent que s'instal·larà als escriptoris virtuals o servidors d'aplicacions per poder registrar contra els servidors i puguin ser accessibles remotament mitjançant el client.
VDI	De l'anglès *Virtual Desktop Infraestructure,* entorn de virtualització d'escriptoris en el que cada usuari rep una màquina completa per ell.
VLAN	De l'anglès *Virtual Local Area Network,* es tracta d'una xarxa virtual marcada per una etiqueta que els equips de xarxa detecten per separar les xarxes virtuals

3. Objectius.

Propòsit:

Disseny d'un pilot de virtualització d'escriptoris per la EUPMT.

Finalitat:

Definir un pilot de virtualització d'escriptoris per millorar la gestió informàtica de les aules i el personal de la EUPMT.

Objecte:

Documentació necessària per dur a terme un pilot de virtualització d'escriptoris.

Abast:

El dimensionament del pilot està orientat a 50 usuaris.

2. Anàlisis inicial.

Una universitat es tracta d'un entorn amb un parc molt heterogeni a nivell informàtica d'usuari. Ens trobem que tenim uns usuaris amb unes necessitats molt diferenciades, com pot ser el professorat de l'entorn que segurament necessitarà un parc d'aplicacions comú entre tots els departaments però que segurament cada professor necessitarà aplicacions específiques que la resta no necessitarà, ja sigui perquè les funcionalitats no escauen o perquè simplement no coneix de la seva existència, i per aquest professor és una eina molt important ja sigui de forma permanent o momentàniament per un quadrimestre donat.

Trobarem també el grup que segurament serà el més homogeni dins de les seves funcions com seria el departament d'administració, però les seves necessitats no tindran res a veure amb les necessitats del professorat.

I per altra banda trobarem l'alumnat que serà un grup d'usuaris amb unes necessitats més diverses, ja que les seves necessitats no variaran només entre les diferents carreres, sinó que variarà segons les assignatures i pràctiques que hagin de realitzar.

Per poder gestionar de forma més eficient aquest parc tan heterogeni, es decideix definir una prova de concepte de virtualització d'escriptoris, per testejar la viabilitat d'una solució d'aquest estil en l'entorn de la EUPMT-Tecnocampus.

S'ha escollit Citrix com la solució de virtualització d'escriptoris degut a que es tractava de la que millor s'adaptava a les necessitats abans esmentades.

S'han definit i explicat els components claus en un projecte d'aquest estil i els punts claus a tenir en compte en cadascun d'ell i s'ha dimensionat les necessitats per una proba de concepte acotada a 50 usuaris.

3. Plataforma Citrix. Motius de l'elecció.

3.1. Estudi de possibilitats.

Quan normalment es parla de virtualització de l'escriptori la majoria de les vegades la gent associa aquesta solució a un projecte de VDI pur. En aquest terreny les dues grans solucions en aquest terreny serien Citrix XenDesktop i VMWare View. Seguint les comparatives existents per internet i les enquestes que fan com ara Gartner, els dos fabricants estan molt propers en quan a valoració, com ara aquesta enquesta entre empreses assistents a un esdeveniment de Gartner:

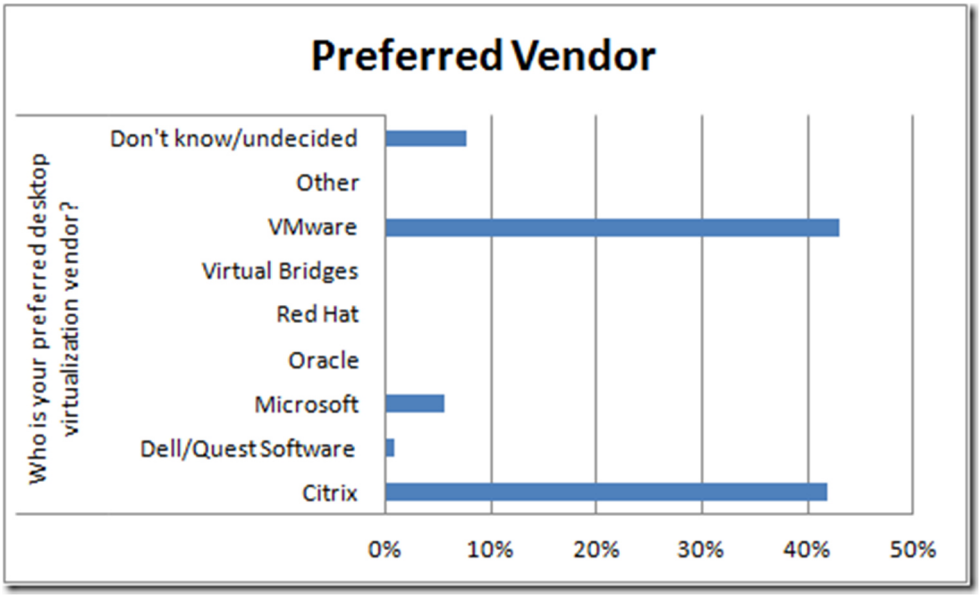

Fig. 3.1. Enquesta Gartner sobre fabricant VDI preferit

Si bé em de tenir en compte que aquest tipus d'enquestes acostumen a incloure participants que no coneixen la tecnologia o simplement tenen preferències per un fabricant per motius històrics.

Una altra forma d'avaluació seria agafar taules de funcionalitats i comparar-les una a una:

Feature	Citrix	VMware
XenApp published apps for secure access to 6 versions of Windows apps on any device	✔	✔
XenApp published desktops for 6eliber IT control and lowest cost	✔	✔
VDI desktops for 6eliber personalization	✔	✔
VDI w/Personal vDisk for 6eliber personalization with single 6elibe management	✔	
Hosted physical desktops when hypervisors aren't required	✔	
Remote PC access for secure, direct connections to office PCs	✔	
Offline client virtualization for disconnected user requirements	✔	
HDX™ user experience optimization for 6elibers6a redirection, and latest USB peripherals	✔	Limited
HDX 3D Pro™ performance optimization for 2D and 3D graphics, design, and engineering apps	✔	Limited
HDX™ Mobile optimizes Windows apps for 6elibe 6elib screen environments	✔	Limited
WAN optimized networking for long distance, limited bandwidth, high latency connections	✔	✔

Unified Communications optimization reduces latency with local 7elib and 7elib media processing	✔	Limited
Any 7elibe access with "follow-me apps" from over a billion devices including Windows, Mac, iOS, and Android or any HTML5-enabled browser	✔	Limited
Enterprise app 7elib for user self-service selection of authorized apps	✔	✔
Universal Printing services 7elibers a bandwidth optimized, print-anywhere solution eliminating the need for native drivers	✔	Limited to VDI
Support for 16-, 32-, 64-bit apps on WS 2008R2/2012R2 and WinXP/7/8	✔	Limited

Taula 3.1. Comparativa funcionalitats XenDesktop vs View

Però aquestes comparatives són complicades de fer perquè tot depèn de les funcionalitats que agafis, i al final poden ser partidistes fins i tot sense voler-ho.

Si tornem a l'enquesta realitzada en l'esdeveniment de Gartner sobre virtualització d'escriptoris, una de les preguntes tenia la finalitat de veure de totes les avantatges de la virtualització d'escriptoris quines eren les que més importaven a les empreses que estaven interessades en dur a terme un projecte d'aquest estil i aquest és el resultat:

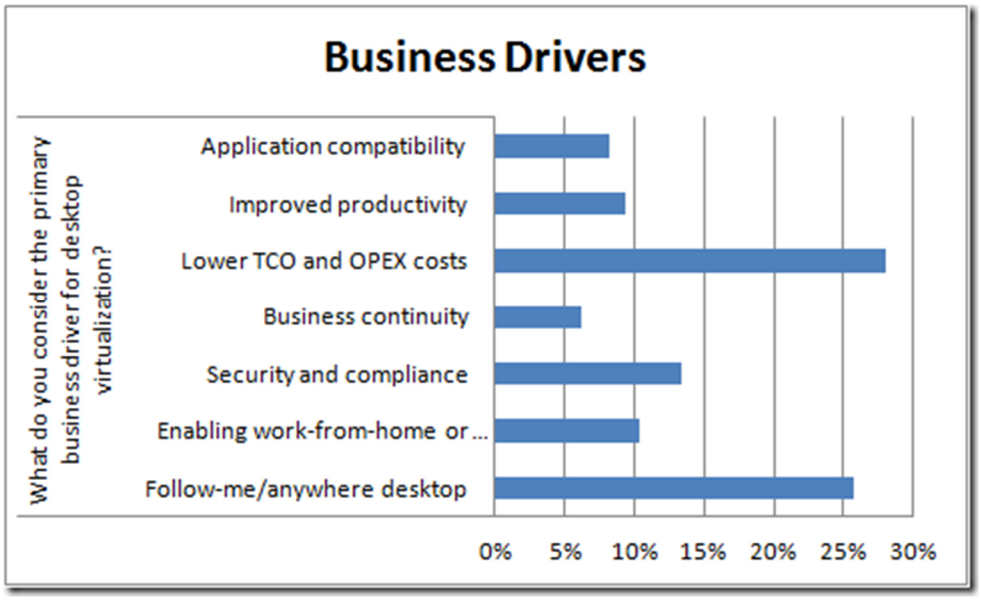

Fig 3.2. Enquesta Gartner motiu adopció virtualització d'escriptoris

On veiem que el més important per les empreses que adopten aquestes solucions és la reducció de costos, seguit de poder obrir l'escriptori des de qualsevol dispositiu i que et segueixi.

Si tenim en compte aquesta premissa, un entorn VDI pur no seria la solució més adient per la majoria d'empreses perquè l'adopció d'aquesta solució de virtualització de l'escriptori amb un ROI i TCO més gran, degut al fet de què al donar un sistema operatiu complert a cada usuari, els requisits de hardware, tant de processador, memòria e IOPs, són els més grans. A part de les necessitats de llicències en la majoria dels casos també és més elevada.

Llavors la solució amb un TCO més baix i que ens permetria en la majoria dels casos seria una solució tipus HSD, en la qual es comparteix un sistema operatiu servidor perquè múltiples usuaris puguin obrir sessió i accedir a les aplicacions publicades de forma concurrent.

En aquest sistema de publicació d'escriptoris els productes millors posicionats serien *Microsoft Remote Desktop Services, Dell Quest i Citrix XenApp.*

La gestió i aprovisionament d'imatges de sistema operatiu, el protocol de connexió ICA/HDX, la gestió granular de polítiques, la gestió avançada de perfils o els informes de

compatibilitats d'aplicacions amb Citrix AppDNA són alguns dels motius pels quals Citrix XenApp continua sent el líder en aquest sector de virtualització d'escriptoris.

Però amb cap d'aquestes dues solucions podem aprofitar les capacitats de hardware de l'equip client, en cas de què volguéssim aprofitar el hardware dels equips clients tenim dos tipus de solucions:

1) Fer servir un hipervisor a l'equip client per muntar màquines virtuals en el mateix equip i poder gestionar-les de forma centralitzada i sincronitzades en el nostre centre de càlcul. Dins d'aquesta solució els dos màxims exponents serien l'integració de *VMWare Workstation* amb *VMWare View* i la solució de *Citrix XenClient.* Cadascuna de les solucions té avantatges i desavantatges, la solució de Citrix XenClient al ser un hipervisor de capa 1, és a dir que s'isntal·la directament sobre el hardware el rendiment de les màquines virtuals és major i té un major accés al hardware del dipositiu, en canvi la solució de VMWare és un hipervisor tipus 2, s'instal·la sobre un sistema operatiu, que és el que té accés al hardware, i llavors el rendiment de la màquina virtual és més baix, però estarà suportat en la majoria de dispositius, no així el de Citrix que ha de seguir una matriu de compatibilitat de hardware.

   Una solució d'aquest estil està pensada sobretot per entorns amb portàtils que han de treballar fora de línia, sense accés a internet.

2) Fer servir una solució d'arrancat per xarxa i rebre el sistema operatiu, per exemple, per PXE, sense haver-lo d'instal·lar. Existeixen multitud de solucions d'aquest estil, per exemple, de la majoria de fabricants de hardware com ara Fujitsu, HP, Dell, Wyse, nComputing, etc. el problema d'aquestes solucions és que acostumen a ser dependents de hardware propietari de la mateixa empresa. Citrix disposa de la solució Provisioning Services que es tracta d'una solució agnòstica del hardware i que pot treballar contra entorn físic o entorn virtual com a complement o substitut de MCS.

   Aquest tipus de solucions està pensat per gestionar parcs homogenis de equips clients, com podria ser una aula informàtica de laboratori i poder aprofitar les capacitats físiques dels equips, com ara les targetes de vídeo, gravadores, etc.

Un altre opció virtualització de l'escriptori, seria la virtualització d'aplicacions, que es tractaria de l'empaquetament d'aplicacions per guardar-les en un recurs de xarxa compartit i desplegar-les als equips sense haver-les d'instal·lar, per evitar interferències amb les aplicacions instal·lades en els dispositius. En aquest àmbit tenim tres opcions principals: AppV de Microsoft, ThinApp de VMWare i Application Streaming de Citrix. El punt feble d'aquest tipus de solucions és que estan pensats per entorns de xarxa local i no posseeixen per sí mateix un control de l'escriptori de l'usuari.

3.2. Conclusions de l'estudi.

Cap de les possibilitats estudiades, per ella mateixa, ens cobreix totes les necessitats que havíem esmentat en el anàlisis inicial ni ens cobreix davant de totes les possibilitats que ens poden anar sorgint en el futur.

Però hem vist que en totes les opcions Citrix aportava una solució, que es trobava entre les millors opcions, si no la millor, i és el principal motiu pel qual s'escull Citrix com a solució per dur a terme la prova de concepte o pilot.

Sota el paraigües de la llicència de XenDesktop podem tenir una solució per totes les opcions de virtualització d'escriptori de les quals hem parlat: VDI, HSD, virtualització d'aplicacions, hipervisor client i gestió d'imatges per PXE.

Aquestes opcions es poden fer servir per separat o combinades com podria ser l'opció de mitjançant Provisioning Server gestionar imatges de uns escriptoris Linux i mitjançant XenApp publicar un connector cap a aquestes màquines virtuals.

Nota: cap de les solucions esmentades suportaven una solució de VDI per Linux directament, però Citrix té planificat en següents versions suportar amb XenDesktop i MCS la publicació de escriptoris Linux.

En la següent taula podem trobar una relació de funcionalitats depenent de la edició.

	XenApp Advanced	XenApp Enterprise	XenApp Platinum	XenDesktop VDI	XenDesktop Enterprise	XenDesktop Platinum
XenApp published apps (Server-based hosted apps)	✔	✔	✔		✔	✔
XenApp published desktops	✔	✔	✔		✔	✔
VDI				✔	✔	✔
VDI with Personal vDisk				✔	✔	✔
Server VDI					✔	✔
Hosted physical desktops					✔	✔
Remote PC Access (with Wake On LAN)					✔	✔
Offline client virtualization (XenClient Enterprise)					✔	✔
DesktopPlayer for Mac (Add-on*)					✔	✔
VM hosted apps		✔	✔		✔	✔
Pre-launch technology	✔	✔	✔		✔	✔
Session linger	✔	✔	✔		✔	✔

Anonymous Logon	✔	✔	✔		✔	✔
USB 3.0 ready,	✔	✔	✔	✔	✔	✔
HDX™ user experience	✔	✔	✔	✔	✔	✔
Citrix X1 Mouse	✔	✔	✔	✔	✔	✔
HDX™ Mobile,		✔	✔		✔	✔
HDX Seamless local apps			✔			✔
HDX 3D Pro™		✔	✔		✔	✔
XenServer vGPU sharing		✔	✔		✔	✔
Unified Communications optimization	✔	✔	✔	✔	✔	✔
HDX RealTime Optimization Pack for Lync		✔	✔		✔	✔
WAN optimized XenApp and XenDesktop	✔	✔	✔	✔	✔	✔
CloudBridge VPX-45 for WAN						✔
CloudBridge plug-in software-base			✔			✔
Any device access	✔	✔	✔	✔	✔	✔
Enterprise app store	✔	✔	✔	✔	✔	✔

Clientless HTML 5 Receiver	✔	✔	✔	✔	✔	✔
Universal Printing	✔	✔	✔	✔	✔	✔
Support for 16-, 32-, 64-bit apps on Windows Server 2008R2 and 2012R2 and Windows 7/8	✔	✔	✔		✔	✔

Taula 3.2. Funcionalitats XenDesktop/XenApp segons edició

4. Serveis dedicats.

4.1. StoreFront.

4.1.1. Funcionalitat

És la capa encarregada de presentar els recursos publicats a l'usuari, es tracta d'un software que s'instal•la sobre un windows i corre sobre un IIS per poder enumerar i fer accessibles els escriptoris i aplicacions disponibles dintre dels stores. Els stores es tracten de l'agrupació de recursos oferts als usuaris, en el nostre cas XenDesktop, però es pot integrar amb altres solucions com ara XenMobile, solució de gestió de dispositius mòbils oferint un entorn de MDM1 o EMM2 segons l'edició, o plataformes SaaS.

Storefront valida contra el directori actiu i guarda informació sobre les preferències de cada usuari per oferir una experiència unificada independentment del dispositiu des d'on es connecti l'usuari.

Per aquest pilot farem servir la versió 2.6 de Storefront ja que es tracta de l'última versió i perquè és l'inclosa dins de la versió 7.6 de XenDesktop, versió del producte que farem servir. Aquesta versió del producte té una serie de prerrequisits que haurem de seguir:

Requisits mínims de sistema

Hem de reservar un mínim de 2GB de RAM a part de qualsevol altre servei existent dins del servidor. L'store de subscripció necessita un mínim de 5MB d'espai en disc, més aproximadament 8MB per cada 1000 subscripcions d'aplicació. A nivell de hardware hem de seguir els mínims requeriments que tingui el sistema operatiu on hem instal•lat StoreFront.

Citrix ha testat i dóna suport per StoreFront en les següents plataformes:

- Windows Server 2012 R2 Datacenter i Standard edicions
- Windows Server 2012 Datacenter i Standard edicions
- Windows Server 2008 R2 Service Pack 1 Enterprise i Standard edicions

L'actualització del sistema operatiu en un servidor on ja està instal•lat StoreFront no està suportat. Es recomana l'instal•lació del software de StoreFront sobre una instal•lació neta de sistema operatiu. Si tenim una infraestructura amb múltiples Storefront per tenir alta disponibilitat, tots els servidors han de còrrer sobre la mateixa versió de sistema operatiu amb les mateixes característiques locals, com ara l'idioma o 32/64 bits. Encara que estiguin testats i suportats configuracions de fins a 5 servidors en un mateix grup de servidors, desde el punt de vista de prestacions a les simulacions s'ha vist que no es treu cap avantatge en crear grups de més de 3 servidors. Tots els servidors dins d'un grup han de residir dins de la mateixa localització.

Microsot Internet Information Services (IIS) i Microsoft .NET Framework són requeriments dins del servidor. Si algun d`aquests prerequisits estàn instal•lats però no habilitats, l'instal•lador l'habilitarà automàticament per nosaltres abans d'instal•lar el producte. És una recomanació permetre que l'instal•lador habiliti/instal•li aquests components per nosaltres perquè els configuri de forma correcta, ja que l'instal•lador revisa l'existència dels mateixos però no ho fa amb les característiques que tenen.

Windows PowerShell i Microsoft Management Console (MMC), els quals són components per defecte d'un servidor Windows , han d'estar instal•lats dins del web server abans de què puguis instal•lar StoreFront. La localització relativa de StoreFront dins de IIS ha de ser la mateixa dins de tots els servidors en un grup, ja que la ruta dels stores que veuran els usuaris dependrà de la mateixa.

Storefront fa servir els següents ports per comunicacions. Ens hem d'assegurar que es permetins aquests ports en els firewalls i altres dispositius a la xarxa:

- Els ports TCP 80 i 443 es fan servir per comunicacions HTTP i HTTPS, respectivament, i han de ser accessibles tant desde dins de la xarxa corporativa com desde fora pels dispositius que vulguin accedir als escriptoris i aplicacions publicades, sempre i quan es faci l'accés sense fer servir un NetScaler, llavors l'accés a aquests ports ha d'estar habilitat desde la xarxa interna i desde la direcció SNIP del NetScaler.

- El port TCP 808 es fa servir per comunicacions entre els servidors de StoreFront i han de poder ser accessibles desde la xarxa interna.

- Un port TCP aleatori seleccionat entre tots els ports sense reserva es fa servir per comunicacions entre tots els servidors de StoreFront dins d'un grup. Quan instal•les Storefront, un regla de firewall es crea dins del Firewall de Windows habilitant l'accés a l'executable de Storefront. Tot i així, ens hem d'assegurar que els dispositius de xarxa o firewalls existents entre els diferents StoreFronts dins d'un grup no bloquegin els ports TCP que no estiguin reservats.

- El port TCP 8008 es fa servir per el Receiver per HTML5, allà on estigui habilitat, per comunicacions entre els usuaris locals en la xarxa interna als servidors que ens ofereixin els escriptoris i les aplicacions. En el cas de l'accés extern via NetScaler, al fer-nos de proxy invers, aquest port haurà d'estar habilitat entre la direcció IP de SNIP del NetScaler i els servidors que serveixin els escriptoris i/o aplicacions.

StoreFront suporta tant xarxes pures IPv6 com entorns duals IPv4/IPv6.

Storefront dóna diferents opcions als usuaris per accedir als seus escriptoris i aplicacions publicats. Els usuaris poden accedir tant per el client Citrix Receiver com fent servir un navegador web per logar-se i fer servir el Receiver per web. Per els usuaris que no tenen la posibilitat d'instal•lar Citrix Receiver, ja sigui per restriccions de seguretat al dispositiu o perquè el sistema operatiu no ho soporta, però tenen un navegador compatible amb HTML5, poden accedir directament mitjançant el navegador sense l'instal•lació de cap tipus de client si s'habilita als Storefront i als Controller el Receiver per HTML5.

Usuaris amb dispositius que no estiguin units al domini poden accedir als escriptoris mitjançant els navegadors web. En el cas de dispositius units al domini i PCs reutilitzats que facin servir Citrix Desktop Lock , y clients Citrix més antics que no poden ser actualitzats, els usuaris deuen connectar-se fent servir el XenApp Services URL del store.

Si es planeja distribuir aplicacions offline als usuaris, el Plug-in Offline es requereix a més a més del Receiver per Windows. Si es volen servir entorns de Microsoft Application Virtualization (App-V) als usuaris, es requereix també una versió del client de Microsoft

Virtualization Desktop Client. Per accedir a aquestes solucions, no es pot fer servir el client web.

4.1.2. Alta disponibilitat

En el cas de què el server on estigui hospedat StoreFront no estigui disponible o el respectiu servei web, els usuaris no podran establir noves connexions contra els seus escriptoris o aplicaciones publicades. Llavors en cas de voler tenir alta disponibilitat del servei conjunt, haurem de configurar com a mínim 2 servidors de StoreFront dins de un grup, per no tenir un únic punt de fallida. L'accés a StoreFront es fa mitjançant una IP, nom NETBIOS o FQDN, llavors haurem de configurar un entorn de balanceig de càrrega d'aquests servidors per balancejar l'entrada als mateixos i que en cas de caiguda d'un dels servidors, els usuaris no pateixin una interrupció del servei. Per configurar-lo disposem de les següents opcions:

- Balancejador de càrrega hardware – Es tractarà d'un appliance amb intel·ligència, que tindrà la capacitat de verificar la disponibilitat dels servidors i activament balancejar la càrrega entre servidors de la millor forma possible. Citrix NetScaler és un exemple d'un balancejador de càrrega hardware i és una molt bona opció al tenir monitors de salut específics per StoreFront.
- DNS Round Robin – Ens proveïra d'un balanceig d'entrada rudimentari per múltiples servidors, però no faria cap tipus de comprobació de disponibilitat dels mateixos. En cas de caiguda d'un dels servidors de StoreFront la solució de DNS Round Robin continuaría dirigint peticions contra aquest servidor. Degut a això no és una opció recomanada.
- Windows Network Load Balancing – Es tracta d'un servei de Windows amb la capacitat de balancejar la càrrega i realitzar comprobacions rudimentàries de l'estat de salut d'un servidor, pot detectar si un servidor s'ha caigut completament, però no pot verificar la salut específica d'un servei. Per exemple, en el cas de què un servidor estigués bloquejat o saturat i no pogués gestionar noves peticions, aquest servei continuaría enviant peticions a aquest servidor.

En la següent imatge es mostra un disseny a alt nivell d'un NetScaler funcionant com a balancejador de càrrega d'un entorn de StoreFront, i veiem com els usaris externs farien servir NetScaler com a proxy invers a part de com a balancejador del servei.

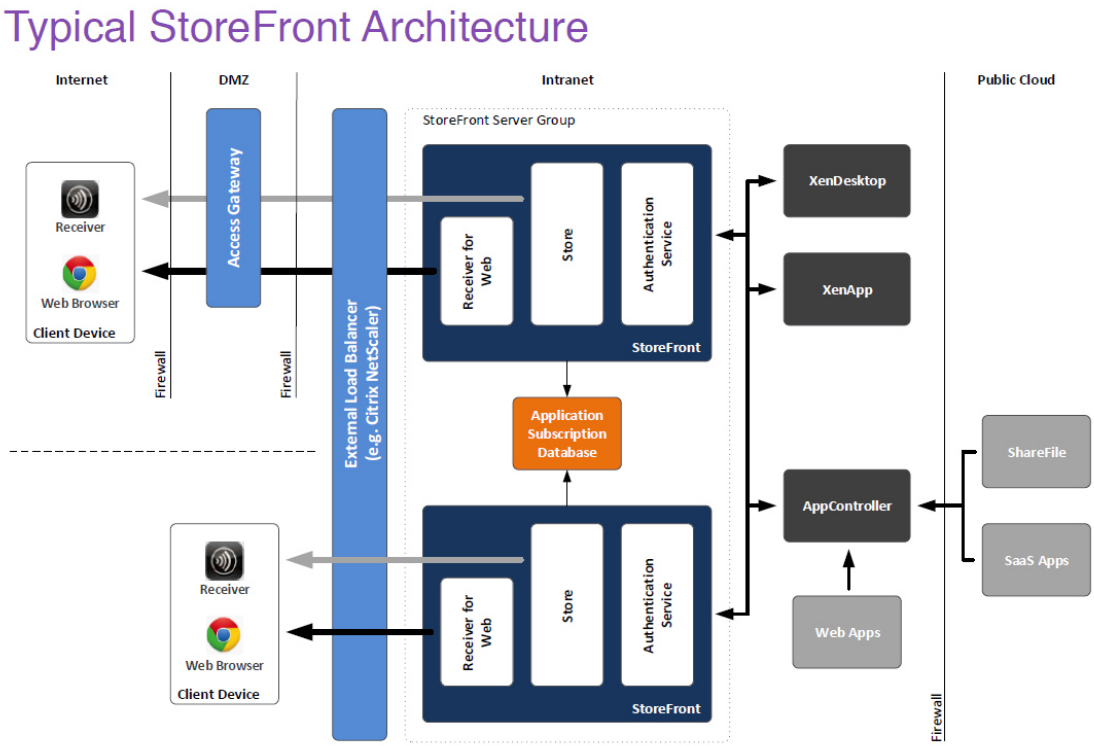

Fig 4.1. Arquitectura típica StoreFront

Per donar accés als escriptoris i aplicacions, s'ha de configurar a StoreFront com a mínim la direcció IP o el nom DNS i el port XML d'un Delivery Controller a cada site de XenDesktop/XenApp. La comunicació entre el Controller i el StoreFront es fara pel port XML. No s'han de configurar tots els controllers dins del Storefront, aquells que es configurin adquiriran el rol de XML broker. Per tolerància a fallides, s'haurien de configurar més d'un controller per cada site. StoreFront en cas de fallida del primer controller automàticament faria un failover cap al segon servidor a la llista de controllers (actiu/passiu). Per gran entorns o amb una gran càrrega de logon es recomana una distribució activa de la càrrega de logon (actiu/actiu). Això es pot aconseguir amb els monitors XML preconfigurats i persistència de sessió que ens pot oferir un balancejador com NetScaler.

4.1.3. Securització.

4.1.3.1. Tràfic d'entrada o extern.

Les comunicacions iniciades al navegador web o Receiver cap al StoreFront inclouen credencials d'usuari, configuracions de sessió i fitxers d'inicialització. El tràfic remot s'enruta per xarxes externes del nostre datacenter i fins i tot per xarxes totalment insegures (com ara internet). Per això és molt recomanable que el tràfic estigui encriptat fent servir SSL. En el cas de no disposar d'un altre solució de encriptació com ara VPN, ja siguin IPsec o SSL, NetScaler ens pot encriptar el tràfic i fer de Proxy invers per tal de tenir una connexió més segura.
Els servidor de StoreFront situats a la xarxa interna poden fer servir certificats públics o privats (domini). Els certificats han d'estar instal·lats als servidors de StoreFront i als NetScalers. Si StoreFront està balancejat per NetScaler i fem servir una connexió segura https, la següent taula explica com han d'estar instal·lats els certificats segons el tipus de certificat que fem servir. Dins del diagrama anterior estaríem parlant del tipus de connexió situada a la part baixa.

Nota: Citrix Receiver en cas de fer servir connexió encriptada SSL obliga a que la connexió sigui confiable i que el certificat sigui vàlid, és a dir, que estigui emès per la data actual, ni caducat ni vàlid per una data futura, que la connexió es faci amb el nom FQDN al qual està assignat el certificat i que confiem en la entitat certificadora.

Certificat	Tipus de certificat	Localització del certificat
Certificat public	Public	Servidor StoreFront
	Intermedi	NetScaler
Certificat privat (de domini)	Privat (domini)	Servidor StoreFront
	Arrel	NetScaler

Taula 4.1. Relació certificats segons localització

Quan fem servir un dispositiu mòbil (smartphone o tablet) o un altre tipus de dispositiu que no estigui unit al domini, de la mateixa forma que al NetScaler, el certificat arrel de la entitat certificadora del certificat servidor, ha d'estar instal·lat en aquests dispositius, per tal de poder confiar en la entitat certificadora. Per això, si el que es busca és la facilitat, un certificat públic ens pot ajudar a què aquest tipus de dispositius es puguin connectar de forma més senzilla al tenir instal·lats per defecte els certificats arrels de les entitats públiques.

Nota: Per defecte, Receiver demana encriptació SSL per poder connectar a StoreFront. Això significa que el descobriment automàtic via compte de correu o l'entrada manual del StoreFront fallarà si no tenim un certificat SSL vàlid al StoreFront i el balancejador extern (si aplica) o forcem via clau de registre que es pugui configurar la connexió via http, sense encriptació.

4.1.3.2 Tràfic intern o de backend.

Les credencials s'envien entre els StoreFronts i els Controllers configurats. Per exemple, en una sessió típica amb un Controller de XenDesktop, StoreFront envía les credencials d'usuari al servei Citrix XML del controller i el servei XML retorna informació sobre el set de recursos publicats a aquest usuari. Per defecte, es fa servir una connexió http per passar la informació entre el servidor de StoreFront i el servei XML. Les dades XML es transfereixen en texte plà, amb l'excepció dels passwords que s'envien fent servir ofuscació. En entorns amb alts estàndards de seguretat, es recomana encriptar el tràfic entre els Storefronts i els serveis de XML habilitant SSL. Tenint en compte de què es tracta de comunicacions internes i de què no hi ha interactuació amb usuaris, és senzill fer servir un certificat d'una entitat certificadora privada.

4.1.3.3 Balises.

Citrix Receiver fa servir el que anomena balises (que en realitat són llocs web) per identificar quan un usuari es connecta des de una xarxa interna o des de una xarxa externa. Els usuaris que es connecten des de una xarxa interna es connecten directament contra els recursos publicats, d'altre banda els usuaris que es connecten des de una xarxa externa via Citrix

NetScaler Gateway. És possible controlar a quins recursos té accés un usuari, restringint aplicacions o escriptoris, depenent de a quines balises té accés l'usuari en aquell precís instant.

La balisa interna no hauria de ser un lloc web que fos direccionable externament. Per defecte, la balisa interna és la URL del servei del StoreFront. La balisa externa pot ser qualsevol lloc web extern que produeixi una resposta http. Citrix Receiver monitoritza constantment l'estat de les connexions de xarxa (com ara, si hi ha o no hi ha connectivitat a nivell físic, o si ha canviat la porta d'enllaç per defecte). Quan es detecta un canvi en l'estat, Citrix intenta primer veure si pot accedir a la balisa interna abans d'intentar provar si té accés a les balises externes. D'aquesta forma pot verificar si l'usuari es troba en una xarxa interna o externa. Storefront dóna a Citrix Receiver les direccions http o https de les balises durant el procés de connexió inicial i refresca aquesta informació sempre que sigui necessari. Un cop feta la validació de connexió contra les balises, StoreFront sap si ha de donar a Citrix Receiver, que serà l'aplicació encarregada d'establir la connexió, la direcció interna del servidor que allotja el recurs publicat o si ha de donar el FQDN assignat a Citrix NetScaler Gateway.

És necessari especificar com a mínim dos balises externes com a mínim que puguin ser resoltes des de xarxes públiques.

4.1.4. Dimensionament.

El número d'usuaris de Citrix Receiver suportats per un únic servidor de StoreFront depèn del número de recursos assignats i del nivell d'activitat dels usuaris:

StoreFront Scalability

StoreFront deployment	CPU usage	Simultaneous activities
• Standalone deployment • 4 CPUs • 4 GB RAM • Heavy Usage*	75%	• 291 per second
	90%	• 375 per second

• Cluster StoreFront deployment
• 2 Nodes each with:
  • 4 CPUs
  • 4 GB RAM
  • Heavy Usage*
	75%	• 529 per second

	90%	• 681 per second

Taula 4.2. Escalabilitat StoreFront

Per una òptima experiència d'usuari, Citrix recomana que hi hagin més de deu XenDesktop, XenApp o altres productes de Citrix desplegaments estiguin agregats contra un únic StoreFront.

Base de dades de sicronització: Si els usuaris es connecten a múltiples servidors de StoreFront dins d'un entorn, les seves personalitzacions (subscripció d'aplicacions) es guarden immediatament al servidor de Storefront i replicat a la resta de servidors que pertanyin al mateix grup de servidors. La base de dades de sincronització en cada servidor de StoreFront ha de ser lo suficientment gran com per encabir subscripcions d'usuari i d'aplicacions, que tenen una mida aproximada de 3 KB per usuari i per aplicació.

4.2. NetScaler Gateway.

4.2.1. Funcionalitat.

NetScaler Gateway es tracta d'un balancejador de capa 7 que pot fer les funcionalitats de SSL VPN, tallafoc d'aplicacions, GSLB i accelerador d'aplicacions principalment. Per la nostra proba de concepte, el farem servir com a balancejador dels StoreFront tant per la xarxa interna com per a la externa i com a encriptador del protocol ICA, proxy invers de les connexions externes i punt de validació contra el directori actiu, encara que el podríem fer servir altres mètodes de validació com ara RADIUS, certificats o sistemes de token de seguretat de clau variable, *one time password*, i fins i tot combinar-los.

Es pot adquirir com a hardware, que tenen la nomenclatura de NetScaler MPX, o com a software en format virtual appliance, que tenen nomenclatura NetScaler VPX, suporta els hipervisors principals Microsoft HyperV, VMWare vSphere i Citrix XenServer. A banda, existeixen els equips anomenats NetScaler SDX que el que permeten és tenir la capacitat de què es puguin executar més d'una instància de NetScaler dins del mateix appliance. En format hardware hi ha diferents models que suporten més o menys càrrega i en format virtual appliance depèn de l'ample de banda llicenciat i de les capacitats del servidor on estigui executant-se.

Existeixen diferents llicències que ens permetran tenir funcionalitats diferents. En aquesta taula podem trobar les diferents funcionalitats per versió.

Feature	Platinum Edition	Enterprise Edition	Standard Edition
Application availability			
L4 load balancing and L7 content switching	•	•	•
Microsoft SQL, MYSQL	•	•	•
AppExpert rate controls	•	•	•
IPv6 support	•	•	•
Traffic domains	•	•	•
Subscriber-aware traffic steering	•	•	•
Global server load balancing (GSLB)	•	•	◦
Carrier-Grade Network Address Translation (CGNAT)	•	•	
Dynamic routing protocols	•	•	
Surge protection and priority queuing	•	•	
Citrix TriScale® clustering	•	•	
Application acceleration			
Client and server TCP optimizations	•	•	•
Citrix AppCompress™	•	•	◦
Citrix AppCache™	•	◦	
Application security			
L4 DoS defenses	•	•	•
L7 DoS defenses	•	•	
L7 rewrite and responder	•	•	•
NetScaler Gateway™, SSL VPN	•	•	•
XenMobile® NetScaler connector	•	•	
SAML2 support	•	•	•
AAA for traffic management	•	•	
NetScaler AppFirewall™ with XML security	•	◦	
NetScaler CloudBridge™ connector	•		
Front-end Optimization*			
Content layout	•	•	
Domain sharding	•	•	
Image optimization	•	•	
Style sheets and JavaScript optimization	•	•	
TCP Protocol Optimization			
Multi-path TCP	•	•	•
BIC and cubic TCP	•	•	•
Simple manageability			
NetScaler Insight Center™-Web Insight	•	•	•
NetScaler Insight Center™-HDX Insight	•	•	
AppExpert visual policy builder	•	•	•
ActionAnalytics	•	•	•
AppExpert service callouts, templates and visualizers	•	•	•
Role-based administration and AAA for administration	•	•	•
Configuration wizards	•	•	•
Native Citrix web interface	•	•	•
Citrix command center	•	•	•

• Standard ◦ Option

Taula 4.3. Funcionalitats NetScaler per versió

En aquesta taula podem trobar una petita taula amb les prestacions per model hardware.

Models

Performance	**Entry-level**	Midrange
Version	MPX 5550, 5650	MPX 8005, 8015
HTTP Throughput	500 Mbps – 5 Gbps	5 - 15 Gbps
SSL Transactions per Second (2048-bit certificates)	1,500 to 2,800	6,500 to 11,000
SSL Throughput	500 Mbps to 2 Gbps	4 Gbps to 6 Gbps
CPU Cores	2 - 3	4
Port Configurations	6x10/100/1000 Copper	6x10/100/1000 Copper and 6xGE SFP or 6x10/100/1000 Copper and 2x10GE SFP+
Memory	8 GB	32 GB
Power Supplies	Single	Single, optional second
Rated Power	300W	450W

Models

Performance	High-end	Very High Capacity	Ultra High Capacity
Version	MPX 11515, 11520, 11530, 11540, 11542	MPX 17550, 19550, 20550, 21550	MPX 22040, MPX 22060, MPX 22080, MPX 22100, MPX 22120
HTTP Throughput	15 - 42 Gbps	20 - 50 Gbps	40 - 120 Gbps

SSL Transactions per Second (2048-bit certificates)	22,500 to 69,000	33,000 to 90,000	125,000 to 560,000
SSL Throughput	14 Gbps to 20.5 Gbps	8 Gbps to 11 Gbps	75 Gbps
CPU Cores	8 to 12	12	16
Port Configurations	8x10GE SFP+ and 4xGE SFP	8x10GE SFP+	24x10GE SFP+ and (for NEBS) 24x10GE SFP+ and 12xGE SFP
Memory	48 GB	96 GB	256 GB
Power Supplies	Dual	Dual	Dual
Rated Power	625W	650W	1100W

Taula 4.4. Capacitats hardware per model NetScaler MPX

En el nostre cas podríem optar per un model virtual i d'aquesta forma aprofitar-nos de la llicència de proves per 90 dies ampliables d'un model NetScaler VPX Platinum 3000. Més endavant en el capítol de dimensionament final veurem les necessitats reals que tindrem per aquest equip dins de la proba de concepte.

En aquesta taula podem trobar els requeriments i prestacions de les diferents edicions de NetScaler VPX.

	VPX 3000	VPX 1000	VPX 200	VPX 10
NetScaler VPX System Requirements [1,2]				
Processor [3]	2-4 vCPUs Intel VTx or AMD-V	2-4 vCPUs Intel VTx or AMD-V	2 vCPUs Intel VTx or AMD-V	2 vCPUs Intel VTx or AMD-V
Memory [4]	2 GB	2 GB	2 GB	2 GB
Hard drive	20 GB	20 GB	20 GB	20 GB
Hypervisor	XenServer 6.0, 6.1 and 6.2 VMware ESXi 4.x, 5.1, 5.5 Microsoft Hyper-V 2008 R2, 2012 R1 KVM			
Pay as you grow license upgrade	N/A	Upgrade option to VPX 3000	Upgrade options to VPX 1000 and VPX 3000	Upgrade options to VPX 200, VPX 1000 and VPX 3000
NetScaler VPX Performance [5]				
System throughput	3000 Mbps	1000 Mbps	200 Mbps	10 Mbps
SSL transaction/sec (2K key certificates)	Up to 750			
SSL throughout, Gpbs	Up to 1.0			
Compression throughput, Gbps	Up to 0.75			
SSL VPN/ICA Proxy concurrent users	Up to 1500			

1. The system requirements are in addition to hypervisor requirements.
2. Listed hardware requirements are for NetScaler VPX nCore version. NetScaler VPX classic builds are available with smaller hardware footprint and slightly reduced feature set.
3. VPX on Microsoft Hyper-V supports up to 2 vCPU.
4. The minimum memory requirement is 2GB. We recommend to add 2-4GB memory for every additional vCPU . If an enterprise or platinum VPX license is used, the minimum memory requirement is 4GB.
5. VPX performance depends on the underlying servers resources (e.g., CPU speed, CPU/memory allocated to the VPX), other guests VM running on the same server with VPX, and the hypervisor.

Taula 4.5. Capacitats per model NetScaler VPX

4.2.2. Topologia.

La selecció de la topologia de xarxa és una part central de la planificació de l'arquitectura de l'accés extern per assegurar-nos que es suportaran les funcionalitats, rendiment i seguretat necessàries. El disseny de l'arquitectura de l'accés extern s'hauria de fer conjuntament amb l'equip de seguretat per assegurar-nos que complim els requisits de seguretat de la casa, així com les necessitats de la xarxa existent. Hi ha dos topologies primàries a considerar, cadascuna de les quals ofereix un nivell més gran de seguretat.

La primera opció que podem fer servir és fer servir una topologia d'un braç, en la qual NetScaler fa servir una única targeta física o lògica, segons si es tracta d'un equip físic, SDX o MDX, o un equip virtual, VPX. En la qual portarà associat la VLAN i IP subnet, per transportar tant el tràfic frontal pels usuaris com el tràfic intern o de *backend,* contra els serveis i servidors d'escriptori o aplicacions virtuals.

1-Arm Topology

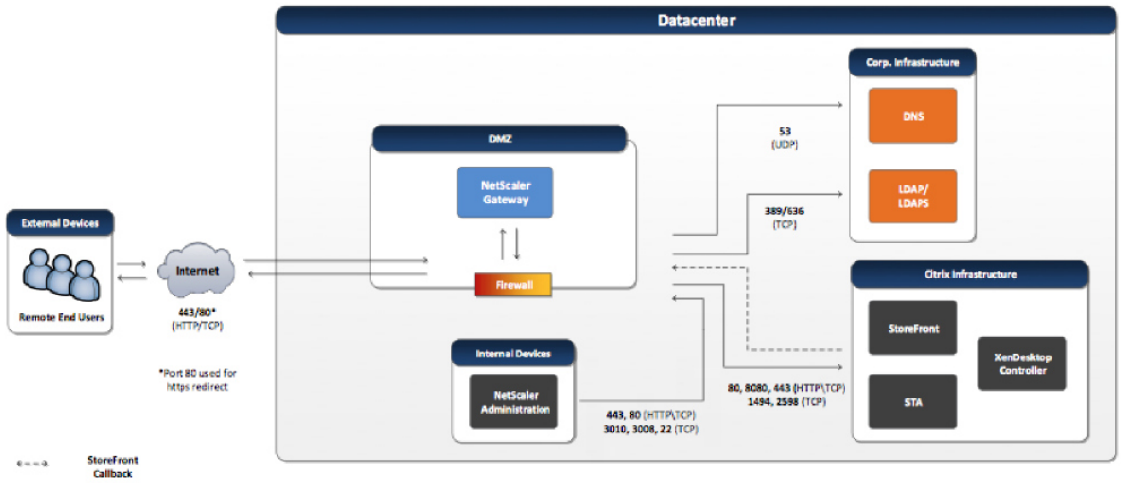

Fig. 4.2. Configuració NetScaler un braç

L'altre opció és fer servir un entorn encara més securitzat, anomenat de dos braços, en el qual NetScaler Gateway fa servir dos o més targetes de xarxa, ja siguin virtuals o físiques. D'aquesta forma el tràfic d'entrada o *frontend,* està totalment aïllat del tràfic intern o *backend,* entre els serveis i servidors de la infraestructura d'escriptori virtual, que està direccionat a una segona targeta. Això ens permet l'ús de zones desmilitaritzades separades, o *double-hop DMZs,* per aïllar el tràfic extern i l'intern amb un control i monitorització granular.

2-Arm Topology

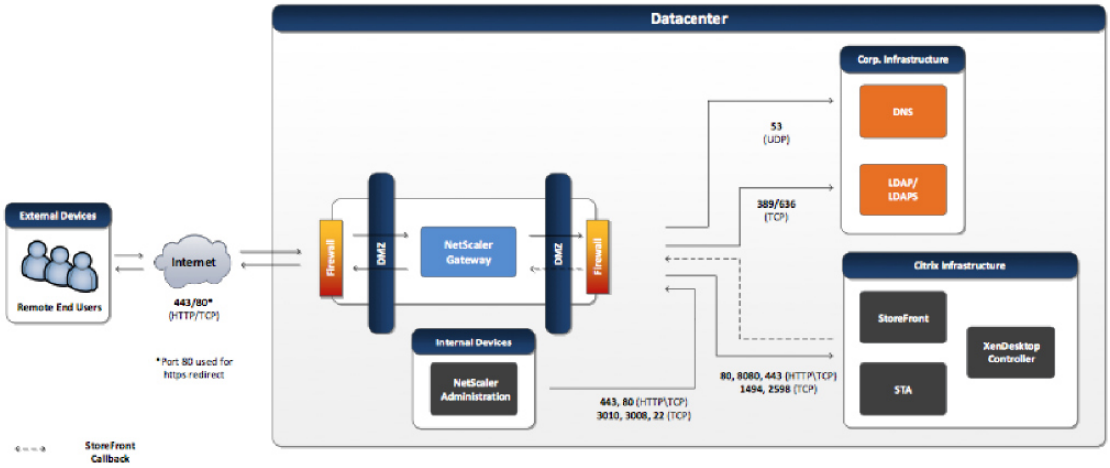

Fig. 4.3. Configuració NetScaler dos braços

4.2.3. Alta disponibilitat.

Si el NetScaler Gateway no està disponible, els usuaris remots no seran capaços d'accedir a l'entorn de virtualització d'escriptoris o aplicacions. Llavors seria recomanable el desplegament de com a mínim dos NetScaler Gateway perquè no es converteixi en un únic punt de fallida.

Quan es configura un NetScaler Gateway en una parella d'alta disponibilitat, el NetScaler Gateway secundari monitoritza el primari enviant missatges periòdics esperant resposta, també coneguts com heartbeats o probes de salut, per determinar si el primer aparell està acceptant peticions de connexió. Si un dels tests de salut falla, el NetScaler Gateway secundari intenta connectar de nou un temps determinat per l'administrador, un cop passat aquest temps si no ha hagut resposta el secundari determina que el primera no està funcionant. Un cop això succeeix el NetScaler Gateway secundari agafa precedència sobre el primari i comença a agafar el control. El secundari té una taula amb totes les connexions i totes aquelles que no necessitin una reconnexió continuaran sense haver-se de reiniciar.

Els dos NetScaler Gateway han de tenir la mateixa versió de software i el mateix nivell de llicència.

4.2.4. Dimensionament.

Per poder identificar la plataforma correcta de NetScaler que cobreixi els requisits del projecte, hem d'identificar els colls d'ampolla més importants. Com tots els accessos remots estaran securitzats fent servir *Secure Socket Layer* (SSL) transportat per *Hypertext Transfer Protocol* (HTTP) en la forma HTTPs, tenim dues mètriques que són les que haurem de tenir en compte:

- Throughput SSL – El throughput SSL són els gigabits de tràfic SSL que pot ser processat per segon (Gbps)
- Transaccions SSL per segon (TPS) – La mètrica de TPS identifica quantes vegades per segon un *Application Delivery Controller* (ADC), en el nostre cas NetScaler Gateway, pot executar una transacció SSL. La capacitat varia primàriament per la

longitud de la clau requerida per encriptar/desencriptar. TPS és una capacitat a tenir en compte primàriament durant la fase de negociació de la connexió SSL i no tant durant la resta del procés de la encriptació/desencriptació, el qual és la major part de la vida de la sessió. Encara que TPS és una mètrica important a monitoritzar, la experiència de camp ha demostrat que throughput de SSL és encara més important i marca més la experiència de usuari. Les targetes acceleradores SSL que porten els NetScalers físics on marquen la diferencia és precisament en la mètrica de TPS.

El sobre cost d'ample de banda de les capçaleres de SSL es considera normalment negligible relativament al volum del tràfic del virtual desktop i no s'acostuma a tenir en compte com a part del throughput de SSL. Tot i així, fer una provisió per aquesta necessitat ens ajudarà a que el throughput estimat sigui suficient. L'ample de banda fixe afegit a les capçaleres dels paquets pot variar depenent als algoritmes d'encriptació i el total a la mida dels paquets. En absència d'aquestes dades reals en un pilot, s'acostuma a incrementar las necessitats de throughput un 2%. D'aquesta forma, per determinar el throughput SSL requerit per un NetScaler, s'ha de multiplicar el màxim ample de banda que s'haurà de consumir per 1,02.

*Throughput SSL = Màxim ample de banda concurrent * 1,02*

El throughput SSL hauria de ser comparat amb les capacitats de throughput dels models de NetScaler per determinar el més apropiat per l'entorn. Com ja hem comentat existeixen tres grups principals de plataformes, cadascun dels quals ens ofereixen una gran escalabilitat entre ells com hem vist en les taules de prestacions.

- **VPX** – Un NetScaler virtual VPX ens ofereix les mateixes funcionalitats que un NetScaler hardware. Tot i així, hem de tenir en compte que hem de reservar recursos suficients del servidor que albergarà els VPX i que pot afectar a la resta de màquines virtuals que es trobin en el servidor, ja que l'encriptació és un procés d'ús intensiu de CPU. Llavors, són recomanables per entorns petits o mitjans.
- **MDX** – Un NetScaler MDX és la versió hardware del dispositiu. Un MDX serà més potent que un NetScaler virtual i pot suportar optimitzacions de xarxa per grans corporacions, a part de disposar de components específics per aquestes tasques com ara targetes acceleradores SSL.

- **SDX** – Un NetScaler SDX és un mix entre un dispositiu físic i un de virtual. Un SDX és un dispositiu físic que té la capacitat d'allotjar múltiples NetScalers virtuals. Estan especialment indicats per entorns d'operadors o empreses d'allotjament de serveis per la seva capacitat de consolidació.

4.2.5. Tipus de connexió.

Existeixen dos tipus de perfils de sessió que ens permeten escollir els mètodes d'accés que tindran els usuaris cap a l'entorn de virtualització d'escriptori.

- **SSLVPN** – Els usuaris creen una xarxa privada virtual i tunelitzen tot el tràfic configurat per direccions IP a través de la xarxa interna. El dispositiu del client pot accedir als recursos interns permesos tal i com si estiguessin dins de la xarxa interna. Això inclou llocs de XenDesktop, carpetes compartides o intranets. Aquest sistema és considerat menys segur degut que queden oberts cap a l'exterior serveis i ports interns que podrien ser susceptibles d'atacs.
  Un altre consideració a tenir en compte alhora de configurar l'accés via SSLVPN és decidir si habilitarem *Split tunneling* per al tràfic al dispositiu client. Habilitant *Split tunneling,* el tràfic dirigit cap a la intranet del dispositiu client estarà restringit a només alguns ports o serveis especificats. Deshabilitant Split tunneling, tot el tràfic generat des del dispositiu client estarà dirigit cap a la intranet, tant el tràfic destinat cap a serveis externs com el tràfic destinat cap a serveis externs (internet) travessarà la xarxa corporativa. L'avantatge d'habilitar *Split tunneling* és que la exposició de la xarxa interna serà més limitada i que protegirem l'ample de banda de la nostra xarxa corporativa. L'avantatge de deshabilitar *split tunneling* és que el tràfic del dispositiu client podrà ser monitoritzat i controlat mitjançant sistemes com ara filtrat web o sistemes de detecció d'intrusions.

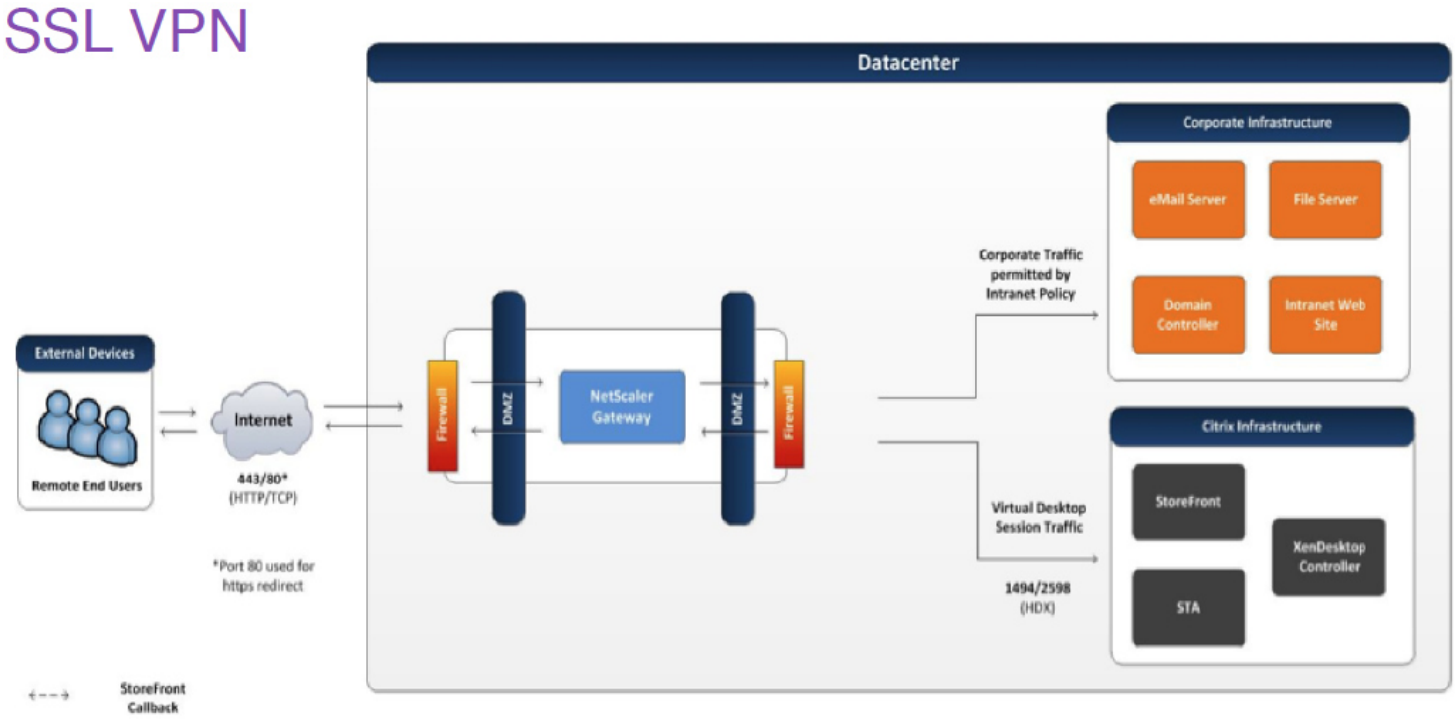

Fig.4.4. Esquema SSL VPN

- **Proxy HDX –** Amb HDX Proxy, els usuaris connecten amb els seus escriptoris virtuals i aplicacions a través de NetScaler Gateway sense exposar adreces internes externament. Amb aquesta configuració, el NetScaler Gateway actua com una micro VPN i només maneja tràfic HDX. Altres tràfics dins del dispositiu client, com ara el correu privat o navegació privada per internet no farà servir NetScaler Gateway i farà servir la xarxa on estigui connectat el dispositiu client.

  Basat en el dispositiu client i en el Citrix Receiver fet servir, s'ha de fer una decisió per veure si aquest mètode està suportat per tots els grups d'usuaris. Proxy HDX està considerat com un mètode d'accés segur per escriptoris virtuals remots degut a què només tràfic específicament destinat cap a la sessió de l'escriptori virtual està permès que travessi l'infrastuctura corporativa. La majoria de Citrix Receivers suporten Proxy HDX, llavors és el mètode preferit d'accés:

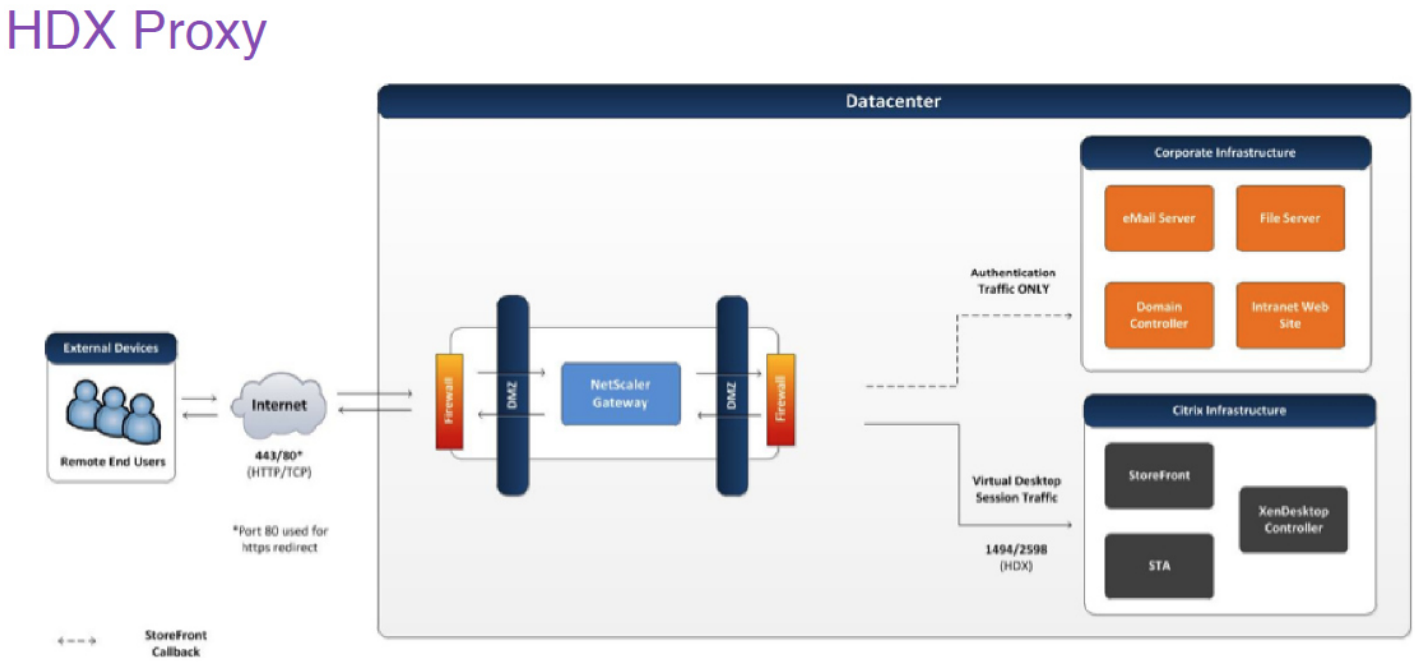

Fig.4.5. Esquema HDX Proxy

4.3. Base de dades.

4.3.1. Funcionalitat.

L'ús d'una base de dades per guardar les configuracions ajuda a simplificar l'administració perquè permet que les configuracions s'apliquin a la vegada sobre tots els objectes del mateix tipus. La majoria de productes Citrix una base de dades nova que ja existeixi dins de l'entorn per guardar els canvis administratius que es produeixin dins de la plataforma. A part, XenDesktop gestiona un base de dades compartida per guardar el canvis d'execució que es van produint, per exemple usuaris connectats o escriptoris disponibles. En aquest escenari, la base de dades es converteix en un canal de comunicació entre els diferents controladors dintre del mateix grup, anomenat site. Degut a aquestes dependències, el disseny de la base de dades es converteix en una peça clau del disseny de l'arquitectura.

4.3.2. Edicions.

Citrix XenDesktop suporta com a motor de base de dades diferents versions de SQL. Hi ha cinc edicions de base de dades Microsoft SQL Server: Express, Web, Standard, Business Intelligence i Enterprise. La taula que es mostra més endavant mostra les diferents

funcionalitats de cada edició, que tenen més relació a les necessitats que podem tenir en un projecte de virtualització d'escriptoris.

Feature	Enterprise	Busines Intelligence	Standard	Web	Express
Scalability and Performance					
Compute capacity	OS maximum	4 Sockets or 16 cores	4 Sockets or 16 cores	4 Sockets or 16 cores	1 Sockets or 4 cores
Maximum memory utilized	OS maximum	128 GB	128 GB	64 GB	1GB
Maximum database size	524 PB	524 PB	524 PB	524 PB	10GB
High Availability					
AlwaysOn failover cluster instances	Yes (Node support: OS maximum)	Yes (2 nodes)	Yes (2 nodes)	-	-
AlwaysOn availability groups	Yes	-	-	-	-
Database mirroring	Yes	Yes (Safety Full Only)	Yes (Safety Full Only)	Witness Only	Witness Only

Taula 4.6. Capacitats SQL per edició

Basat en les capacitats de les diferents versions de SQL normalment es recomana l'edició Standard per allotjar la base de dades en un entorn de Citrix XenDesktop. L'edició Standard inclou les funcionalitats adequades per cobrir les necessitats de la majoria d'entorns. És molt important revisar la matriu de compatibilitat de versions segons producte de citrix de les bases de dades, s'adjunta aquesta taula a l'annex.

4.3.3. Dimensionament de la base de dades i el log de transaccions

Quan es dimensiona una base de dades SQL, hi han dos aspectes molt important a tenir en compte:

- **Fitxer de base de dades:** Conté les dades i objectes com ara les taules, índexs, procediments i vistes guardats a la base de dades.
- **Fitxer de log de transaccions:** Conté una gravació de totes les transaccions i modificacions de base de dades fet per cada transacció. El log de transacció és un component crític de la base de dades i, i si hi ha una fallida del sistema, el log de transaccions pot ser necessari per poder recuperar la base de dades a un estat consistent. L'ús del fitxer de transaccions varia segons el tipus de model de recuperació de base de dades que es fa servir:
    - **Recuperació simple:** No es requereixen logs de còpia de seguretat. L'espai de log es reclamat automàticament, per mantenir els requeriments d'espais el més petit possible, essencialment eliminant la necessitat d'administrar l'espai

del log de transaccions. Els canvis a la base de dades des de l'última còpia de seguretat es trobaran desprotegits. En cas de un desastre, els canvis s'haurien de refer.

- **Recuperació complerta:** Requereix logs de còpia de seguretat. No es perdria cap tipus d'informació en cas de pèrdua o malmesa del fitxer de base de dades. Les dades de qualsevol punt arbitrari en el temps es pot recuperar. Recuperació complerta és un requeriment en el cas de voler fer servir *mirroring* de base de dades.
- **Bulk-logged-** Aquest sistema és un adjunt al sistema de recuperació complerta i permetria un alt rendiment de les operacions de còpia. Aquest és un sistema que no s'acostuma a fer servir per entorns Citrix.

4.3.4. Tipus de bases de dades a XenDesktop i dimensionament.

Les versions de Citrix XenApp o XenDesktop 7.x fan servir tres tipus diferents de bases de dates:

- **Base de dades de configuració de site:** Conté la configuració estàtica i les dades dinàmiques d'execució.
- **Base de dades de monitorització:** Conté dades de monitorització que són accessibles mitjançant la consola Citrix Director.
- **Base de dades de *Configuration logging:*** Conté una gravació de tots el canvis administratius que s'han executat en el site. Aquesta informació és accessible fent servir la consola Citrix Studio.

4.3.4.1. Base de dades de configuració de site

Com que la base de dades de site de XenApp o XenDesktop conté tant dades estàtiques com informació dinàmica d'execució, la mida del fitxer de base de dades no depèn només del espai físic de l'entorn si no també dels patrons d'utilització dels usuaris. Tots els següents factors impacten en la mida del fitxer de base de dades.

- Número de sessions connectades.

- Número de VDAs configurats i registrats.
- Número de transaccions que succeeixen durant el procés de inici de sessió.
- Transaccions de hertbeat del VDA.

La mida de la base de dades de site es basa en el nombre de VDAs i sessions actives. La següent taula mostra el màxim típic de la mida de la base de dades de site quan s'han realitzat tests de càrrega amb un número donat d'usuaris, aplicacions i diferents mètodes de presentació.

XenDesktop Site DB sample size calculations

Users	Applications	Desktop Types	Expected Maximum Size (MB)
1,000	50	Hosted Shared	30
10,000	100	Hosted Shared	60
100,000	200	Hosted Shared	330
1,000	N/A	VDI	30
10,000	N/A	VDI	115
40,000	N/A	VDI	390

Taula 4.7. Exemples de mides de BBDD site

Determinar la mida del fitxer de log de transaccions és complicat degut als múltiples factors que poden influenciar en la mida del mateix, com poden ser:

- El mètode de recuperació de la base de dades
- Els temps de apertura de sessió en els moments de màxima càrrega
- El número d'escriptoris o aplicacions que s'estan publicant

Durant els tests d'escalabilitat, Citrix va observar que el fitxer de transaccions creixia una mitja de 3,5MB per hora sense connexions, i per usuari/dia una mitja de 32KB. Llavors és recomanable, sobretot en entorns grans, que es porti un manteniment d'aquest fitxer amb còpies de seguretat periòdics per tal que el fitxer no creixi d'una forma descontrolada.

4.3.4.2. Base de dades de monitorització

De les tres bases de dades és la base de dades de la qual s'espera que tingui una mida més gran, degut al fet que conté informació històrica del site. La seva mida depèn de múltiples factors incloent:

- Nombre d'usuaris
- Nombre de sessions i connexions
- Configuració del període de retenció – amb la llicència Platinum es pot mantenir dades per sobre de l'any (per defecte són 90 díes). La resta de llicències només permeten guardar informació de fins a 7 díes (per defecte 7 díes).
- Nombre d'usuaris de VDI o HSD.
- Nombre de transaccions per segon. El servei de monitorització acostuma a agrupar les actualitzacions d'informació. És estrany trobar un número de transaccions per segon que estigui per sobre de les 20.
- Transaccions en *background* causats per les trucades de consolidació del servei de monitorització.
- Processament nocturn d'eliminació de les dades que estiguin fora del període de retenció.

La següent taula mostra una mida estimada de la base de dades de monitorització en diferents escenaris. Aquestes dades són un test estimant una setmana laboral de cinc dies.

Monitoring DB Size Estimations

Estimates with 1 connection and 1 session per user with a 5 day work week					
Users	**Type**	**1 week (MB)**	**1 month (MB)**	**3 months (MB)**	**1 year (MB)**
1,000	HSD	20	70	230	900
10,000	HSD	160	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500

Taula 4.8. Exemples de mides de BBDD monitorització

La mida del fitxer de transaccions de la base de dades de monitorització és molt complicada de mesurar, però els tests d'escalabilitat mostren una mitja de creixement sense connexions aproximadament de 30,5 MB per hora i per usuari/dia de aproximadament 9 KB.

4.3.4.3. Base de dades de *Configuration logging*

La base de dades de *configuration logging* és típicament la més petita de les tres bases de dades. La seva mida i la mida del fitxer de transaccions relacionat depèn les activitats i canvis administratius diaris realitzats via les consoles Citrix Studio, Citrix Director o Microsoft PowerShell, i per aquest motiu és complicat preveure la seva mida. Quantes més modificacions administratives es realitzin, més gran es farà el fitxer de base de dades. Alguns components que poden influir en la mida d'aquesta base de dades són:

- El nombre d'accions realitzades a Studio, Director i PowerShell.
- Transaccions mínimes que es produeixen a la base de dades quan no s'estan realitzant canvis.
- El temps de transacció que es produeix durant actualitzacions.
- Dades esborrades manualment de la base de dades. Les dades a la base de dades de *Configuration Logging* no estan subjectes a cap tipus de retenció i només s'esborraran en cas de què un administrador ho faci manualment.
- Activitats que tenen impacte a les sessions dels usuaris, com ara tancaments de sessió o reinicis forçats.
- El mecanisme fet servir per crear escriptoris

En entorns de XenApp on no es faci servir MCS, la mida de la base de dades té una tendència a tenir entre 20 i 40MB. En entorns en els que es faci servir MCS, la base de dades pot fàcilment excedir els 200MB degut a que es guardaran tots el canvis de creació de màquines virtuals.

4.3.5. Alta disponibilitat.

En cas de caiguda d'alguna de les bases de dades ens trobem amb les següents conseqüències:

- **Caiguda de la base de dades de site:** els usuaris no podran connectar-se o reconnectar-se als seus escriptoris o aplicacions.
  Els administrador no podran fer servir les consoles Studio o Director.
  En canvi els usuaris amb sessions actives no es veuran afectats.

- **Caiguda de la base de dades de monitorització:** Director no mostrarà cap data històrica i Studio no podrà arrencar. Les noves connexions d'usuaris es continuaran servint.
- **Caiguda de la base de dades de *Configuration logging:*** si es permeten realitzar canvis quan la base de dades està desconnectada, és una de les opcions a escollir durant la seva configuració, la caiguda de la base de dades no afectarà, més enllà de què els canvis administratius realitzats durant la seva caiguda no es guardaran. En canvi ni no s'han permès els canvis quan la base està desconnectada, durant la caiguda de la mateixa els administradors no podran fer canvis al site. Els usuaris no es veuen afectats.

Més enllà de les opcions per disseny de redundància que ofereix Citrix a nivell de base de dades, Microsoft SQL Server i l'hipervisor (en entorns virtuals), ofereixen diferents opcions d'alta disponibilitat. Això permet als administradors assegurar que la caiguda d'un únic servidor impacte el mínim possible a la infraestructura. Els següents opcions d'alta disponibilitat estan disponibles:

- **Alta disponibilitat a nivell de màquina virtual:** Aquesta opció d'alta disponibilitat estarà disponible per servidors SQL Server virtuals, els quals hauran d'estar marcats per alta disponibilitat a la capa de l'hipervisor. En cas d'una apagada inesperada a nivell de màquina virtual o servidor físic, el hipervisor intentarà arrencar la màquina virtual en un servidor físic diferent. Encara que l'alta disponibilitat a nivell de màquina virtual minimitza el temps de caiguda en cas d'apagaments inesperats, no pot protegir davant de corrupcions a nivell de sistema operatiu. Aquesta solució és

més econòmica comparada amb opcions com *mirroring o clustering,* perquè fa servir una utilitat inclosa en el propi hipervisor i necessita de emmagatzemament compartit. Però el procés de restitució de servei és més lent, perquè porta un temps detectar que ha ocorregut un problema i arrencar la màquina virtual SQL en un altre servidor físic. Aquest sistema pot suposar una interrupció en el servei als usuaris.

- ***Mirroring:*** *Mirroring* de base de dades augmenta el nivell de disponibilitat de la base dades gairebé al nivell de recuperació de desastre gairebé instantani. *Mirroring* de base de dades pot fer-se servir per mantenir una única base de dades en *mirror* o en espera, corresponent a la base de dades principal o de producció. *Mirroring* de base de dades pot funcionar en dos modes, tant en mode operativa síncrona o alta protecció com en mode operativa asíncrona o alt rendiment. En el mode alta protecció amb recuperació automàtica (mètode recomanat per XenDesktop) es necessita una tercera instància de SQL, conegut com testimoni, el qual permet al servidor secundari actuar en mode de recuperació en calent. La recuperació del servidor principal cap a la instància *mirror,* succeeix automàticament i triga pocs segons. És una bona pràctica activar l'alta disponibilitat a nivell de màquina virtual com a mínim per al servidor de testimoni per assegurar la disponibilitat en cas de una fallida multiservidor.
- **Instàncies *AlwaysOn Failover Clúster:*** *Failover clustering* dóna suport d'alta disponibilitat per una instància sencera de Microsoft SQL Server. Un *failover clúster* és una combinació de dos o més nodes, o servidors, que fan servir un mateix emmagatzemament compartit. Una instància de *AlwaysOn Failover Clúster* apareix a la xarxa com un únic equip, però té la funcionalitat de recuperar el servei d'un node a l'altre en cas de fallida.
- ***AlwaysOn Availavility Groups:*** *AlwaysOn Availavility Groups* és una solució de recuperació de desastres i alta disponibilitat introduït amb Microsoft SQL Server 2012, el qual permet als administradors maximitzar la disponibilitat per un o vàries bases de dades. A diferència de *AlwaysOn Failover Clúster* tenir un emmagatzemament compartit no és un requisit, ja que fa servir rèpliques copiades localment en cada node del grup. Es suporta tant la còpia asíncrona com la síncrona. A diferència del sistema clúster o *mirroring,* les instàncies secundàries es poden fer servir per processar lectures, còpies de seguretat o proves d'integritat. D'aquesta forma es pot descarregar l'instància primària.

En la següent taula podem trobar les funcionalitats d'alta disponibilitat recomanades per les bases de dades:

Recommended SQL high availability options

Component	VM-Level HA	Mirroring	Failover Clustering	AlwaysOn Availability Groups
XenDesktop Site Database	◎	●	●	● 2
XenDesktop configuration Logging Database	◎	● 1	●	● 2
XenDesktop Monitoring Database	◎	●	●	● 2
Provisioning Services Farm Database	◎	●	●	● 3
XenClient Database	◎	●	●	

● Recommended ● Viable ● Not Supported ◎ Recommended for Test Enviornments Only

1 If "Allow changes when the database is disconnected" has been enabled no redundancy is required, otherwise mirroring is recommended

2 Mirroring is preferred due to the lower SQL license requirements

3 PVS 7.6 and above supports AlwaysOn for SQL Server 2012 and 2014

Taula 4.9. Recomanacions mode HA per BBDD

4.3.6. Dimensionament del servidor de base de dades

Els controladors de XenDesktop i XenApp fan servir la base de dades com una via de comunicació entre controladors, guardant les dades de configuració, les dades de monitorització i les de dades de log. Les bases de dades estan constantment en ús i l'impacte en el rendiment del servidor de SQL es pot considerar com alt.

Basats en tests d'escalabilitat interns de Citrix, aquestes són les necessitats per un servidor allotjant totes les bases de dades de XenDesktop:

- 2 cores / 4 GB de RAM per entorns de fins a 5000 usuaris
- 4 cores / 8 GB de RAM per entorns de fins a 15000 usuaris
- 8 cores / 16 GB de RAM per entorns de més de 15000 usuaris

Els fitxers de base de dades i els logs de transacció haurien d'estar allotjats en subsistemes de disc diferents per poder rendir amb un alt nivell de transaccions. Per exemple, si es registren 20000 escriptoris durant una turmenta d'inici de sistema operatiu pot causar aproximadament 500 transaccions per segon i 20000 usuaris validant durant 30 minuts en una turmenta d'inici de sessió pot suposar aproximadament 800 transaccions per segon en la base de dades de site.

4.4. Llicenciament.

4.4.1. Funcionalitat.

El llicenciament de Citrix ofereix als clients la flexibilitat de múltiples models de llicenciament que s'alineen amb escenaris d'utilització habituals. Els diferents models de llicenciament varien en base al producte Citrix utilitzat, però poden incloure per usuari/dispositiu i per usuari concurrent. Diversos productes Citrix utilitzen el servidor de llicències, mentre que d'altres requereixen una llicència que s'instal•la en el mateix producte.

En aquesta taula podem trobar la ubicació que han de tenir les llicències segons el producte:

Product	License Location
XenDesktop	Citrix License Server
XenApp	Citrix License Server
Provisioning Services	Citrix License Server
XenServer	Citrix License Server
XenClient	On the product
NetScaler	On the product
NetScaler Gateway	On the product

Taula 4.10. Ubicació fitxer de llicències per producte

4.4.2. Tipus de llicències.

Per determinar el número de llicències requerides, els clients han de determinar el model de llicenciament i el número total d'usuaris o dispositius que accediran a l'entorn Citrix. Les

llicències es poden reservar para un usuari o equip, depenent del model de llicenciament de cada producte.

Amb XenDesktop 7.6 es va introduir un període de "gràcia" suplementari. Si s'han consumit totes les llicències, es garantiran llicències de "gràcia" per un període de fins a 15 dies, permeten al administrador disposar del temps necessari per adquirir les llicències addicionals. S'alertarà al administrador que s'han consumit les llicències al Director a través de l'eina de Política de llicenciament (*License Policy Engine*).

4.4.2.1. Llicències d'usuari o dispositiu.

Amb el llicenciament per usuari/dispositiu, el servidor de llicències pot assignar la mateixa llicència a un usuari o a un dispositiu. Quan s'assigna a un usuari, la llicència permet l'accés des d'un número il•limitat de dispositius. Quan s'assigna a un dispositiu, la llicència permet l'accés des d'un dispositiu per un número il•limitat d'usuaris. El servidor de llicències determina com minimitzar el consum de llicències basant-se en el número d'usuaris i dispositius connectats.

4.4.2.2. Llicències concurrents.

Les llicències també poden ser concurrents, no subjectes a un usuari o dispositiu determinat. Quan usuari arrenca un producte, es reserva la llicència d'un ordinador o dispositiu determinat. Quan l'usuari tanca o es desconnecta de la sessió, la llicència s'allibera, restant disponible per al consum d'un altre usuari.

Es poden consumir llicències addicionals en els següents escenaris:

- Sessions múltiples en ordinadors diferents consumiran múltiples llicències. Quan un usuari arrenca un producte, es reserva una llicència fins que l'usuari tanca la sessió en aquest ordinador/dispositiu (la llicència s'allibera en aquest punt). Per exemple, si un usuari arrenca una sessió des d'un ordinador i arrenca un altre des d'un ordinador diferent sense tancar la primera sessió, es reserven dues llicències.

- Els servidors de llicències no comuniquen la informació respecte a la utilització entre si. Per tant, es poden reservar múltiples llicències que s'utilitzen múltiples servidors de llicències. Això es pot evitar assegurant que tots els productes de servidor d'un entorn apunten al mateix servidor de llicències.

- Es consumeixen múltiples llicències quan un únic dispositiu es connecta a múltiples productes de servidor configurats amb edicions diferents. Per exemple, si un usuari es connecta a una aplicació publicada en un servidor mitjançant la edició Avançada, i llavors utilitza el mateix client per connectar-se a una aplicació publicada en un servidor diferent arrencant la edició Enterprise, es consumiran dues llicències.

4.4.3. Versions.

Les noves versions de servidors de llicències són compatibles amb les prèvies, i funcionaran amb productes i fitxers de llicències més antics; no obstant, els nous productes requereixen sovint el servidor de llicències més recent per fer la reserva de llicències correctament.

4.4.4. Dimensionament.

Proves internes d'escalabilitat han demostrat que un únic servidor de llicències amb dos nuclis i 2GB de RAM poden servir aproximadament 170 llicències per segon o 360000 llicències cada mitja hora.

Citrix recomana la participació en testos d'escalabilitat adients per assegurar que el servidor de llicències és capaç de suportar la demanda de l'entorn.

4.4.5. Alta disponibilitat.

Per un entorn típic, un servidor de llicències és suficient. Quan el servidor de llicències deixa de ser accessible, s'entra en un període de "gràcia" de 30 dies, depenent del producte Citrix,

el qual ha de ser més que suficient per resoldre els problemes de connectivitat i/o restablir o tornar a muntar el servidor de llicències.

Si el servidor de llicències i el producte Citrix no tenen comunicació en 2 batecs (5-10 minuts), el producte Citrix entrarà en un període de "gràcia" que permetrà connexions fins a 30 dies. Un cop es restableixi la comunicació amb el servidor de llicències, aquesta reconciliarà les llicències reals i temporals.

Un registre CNAME al DNS és una forma adient per referir-se al servidor de llicències. L'ús de CNAMEs permet canviar el nom del servidor de llicències sense actualitzar els productes Citrix.

Si es requereix redundància addicional, Citrix suporta les següents solucions d'alta disponibilitat per al servidor de llicències.

- ***Clustering de Windows –*** Un clúster de servidors són un grup d'ordinadors que treballan conjuntament per augmentar la disponibilitat. El clustering permet que el rol del servidor de llicències commuti automàticament quan es produeix un problema. Per més informació respecte al clustering, si us plau veieu l'article Citrix eDOcs – Servidors de llicències clusteritzats.
- **Duplicació del servidor de llicències –** Crear una còpia de seguretat de la màquina virtual del servidor de llicències. Aquesta còpia de seguretat no s'hauria d'emmagatzemar al mateix servidor físic que allotja el servidor de llicències. En lloc d'això, s'hauria d'emmagatzemar en una ubicació segura, com podria ser una solució d'emmagatzemament d'alta disponibilitat, o una cinta o disc. El duplicat del servidor no estarà actiu i es trobarà en espera fins que es necessiti restablir el servidor de llicències actiu. Un cop s'hagi restaurat el servidor amb aquest còpia de seguretat, qualsevol nova llicència s'hauria de tornar a baixar al servidor.

Per XenaApp 6.5 i entorns més antics, l'arxiu *MPS-WSXICA_ MPS-WSXICA.ini* s'hauria de redireccionar a una compartició d'arxius, com es descriu a *CTX131202* – Servidors XenApp aprovisionats deixaran d'acceptar connexions si es reinicien quan el servidor de llicències no es troba disponible. Això no és problema per entorns XenApp 7.x ja que el controlador manega la reserva/alliberament de llicències.

Cada mètode permet al administrador intercanviar un únic servidor de llicències per un altre sense tall de servei; assumint que el canvi es realitza durant el període de "gràcia" i es consideren les següents limitacions:

- Els fitxers de llicències referenciaran el servidor especificat durant el procés d'assignació. Això implica que els fitxers de llicències només es poden fer servir en un servidor amb el mateix nom de màquina que el servidor especificat anteriorment.
- Dos servidors de llicències, basats en Windows, que comparteixin domini no poden compartir el mateix nom i estar actius al mateix temps.
- Dos servidors de llicències, basats en Windows, que comparteixin domini no poden compartir el mateix nom i estar actius al mateix temps.

4.4.6. Optimització.

El rendiment del servidor de llicències es pot optimitzar ajustant el número de fils "rebut" i "processant". Si el llindar de fils es fixa molt baix, les peticions es posaran a la cua fins que estigui disponible un fil. Al contrari, si el llindar de fils es fixa molt alt, el servidor de llicències es saturarà.

Els valors òptims depenen del hardware del servidor, configuració i el volum de peticions de llicències. Citrix recomana provar i avaluar diferent valors per determinar la configuració adient. Establint el número màxims de fils processant a 30 i el màxim número de fils rebuts a 15 és un bon punt de partida per desplegaments a gran escala.

Aquesta optimització millorarà la capacitat del servidor de llicències Citrix augmentant la seva capacitat per rebre i processar peticions de llicències.

4.5. Controladors XenApp/XenDesktop.

4.5.1. Optimització.

La capa de recursos dels controladors de XenApp o XenDesktops, també coneguts com *brokers o Delivery Controllers,* en nomenclatura de projectes VDI, són els encarregats de proveir els components de infraestructura per suportar els requeriments de la capa de recursos per a cada grup d'usuaris. Els controladors d'escriptoris normalment combinen tant el servei de controlador de XenDesktop i de XenApp.

Un *Site* Citrix agrupa escriptoris i aplicacions juntes per formar una única entitat arquitectònica i administrativament parlant. Totes les dades administratives i dinàmiques per el site, incloent configuració de site, assignament d'escriptoris, estat de les sessions, en guarden en la base de dades de site.

Totes les funcions pertanyents a un site es reparteixen igualitàriament entre tots el controladors dins del site. Encara que és possible assignar certes funcions específicament a un controlador, no és recomanable degut a què XenDesktop s'optimitza automàticament i les configuracions manuals poden interferir en el balanceig de càrrega automàtic i els mecanismes de recuperació.

4.5.2. Dimensionament.

Els *Delivery Controllers* autentiquen els usuaris, enumeren els recursos, direccionen les peticions d'execució dels usuaris cap als recursos disponibles i controlen els inicis, apagaments i registre dels escriptoris.

L'escalabilitat dels controladors està basat en l'ús de CPU. A més processadors disponibles, més escriptoris virtuals podrà suportar un controlador. Cada inici d'escriptori, registre,

enumeració i petició de connexió impacta en el processador del controlador. Quan la utilització de CPU del controlador arribi a màxims per sobre del 80%, el site necessitarà ampliar-se, ja sigui ampliant CPU's als controladors existents, o ampliant el número de controladors existents.

Afegint cores de CPU addicionals a un controlador minimitzarà la mitja d'ús general dels processadors, permetent d'aquesta forma augmentar el número d'escriptoris suportats per un únic controlador. Això realment només és possible quan estem parlant d'un controlador virtual, ja que llavors es pot ampliar la quantitat de cores d'una forma senzilla. L'altre alternativa és afegir un altre controlador dins de la configuració. El controlador tindria la mateixa configuració que els altres controladors, i la càrrega es repartiria i baixaria entre tots els controladors del grup.

Les proves de càrrega mostren que un controlador amb la següent configuració pot suportar fins a 5000 escriptoris.

XenDesktop Controller Specification for 5K Desktops

Component	Specification
Processor	4 vCPU
Memory	4GB RAM
Network	Bonded virtual NIC
Host Storage	40GB shared storage
Operating System	Windows Server 2012
XenDesktop	7

Taula 4.11. Dimensionament Controlador per 5K escriptoris

Llavors la següent fórmula es pot fer servir per calcular el número de controladors necessaris:

$$Number\ of\ Delivery\ Controllers = \frac{Number\ of\ Active\ Sessions\ per\ Site}{5{,}000} + 1$$

(4.1)

4.5.3. Alta disponibilitat.

Si el servidor físic que allotja el controlador no està disponible, els usuaris no podran accedir als recursos que tinguessin publicats. Per aquest motiu és recomanable disposar de com a mínim dos controladors, seguint la norma de N+1, on N és la quantitat de controladors necessaris per gestionar l'entorn, i haurien d'estar allotjats en servidors físics diferents per suportar la caiguda d'un servidor físic, sense afectar la totalitat del servei i no convertint-lo en un únic punt de fallida. Si tenim més d'un controlador, en cas de caiguda d'un dels controladors la resta podrà gestionar les connexions i administrar el site.

Les localitzacions de cada controlador està especificat en cada VDA, permetent que pugui automàticament canviar de controlador en cas de què detecti que no hi ha comunicació amb el que estava treballant. El VDA busca en les següents localitzacions per poder parar en el moment en el que troba el primer controlador que respon.

1. Una localització al emmagatzemament persistent gestionat per la funcionalitat de auto actualitzacions.
2. Les configuracions de polítiques de grup (*Delivery controllers, Delivery Controllers SIDs*)
3. L'informació sobre *Delivery Controllers* a la clau de registre sota VDA ListofDDCs. L'instal·lador emplena aquesta informació amb les dades introduïdes durant la instal·lació de la VDA.
4. Descobriment per unitat organitzativa. Tot i que aquest és un mètode que es manté per compatibilitat amb versions anteriors.
5. El fitxer *Personality.ini* creat per *Machine Creation Services.*

Des de el servei de consultoria de Citrix es recomana fer servir l'opció d'auto actualització que està habilitada per defecte, ja que simplifica l'administració i actualitza la informació sobre els controladors que existeixen automàticament quan afegim o eliminem algun controlador del nostre entorn.

4.5.4. Securització.

En una sessió típica, el servidor StoreFront passa les credencials al servei Citrix XML en un controlador de XenDesktop. El servei Citrix XML fa servir text pla per intercanviar dades, amb la excepció de les paraules clau, que es transmeten fent servir ofuscació. Si el tràfic entre els StoreFronts i els controladors és interceptat, és vulnerable als següents atacs:

- Els atacants poden interceptar el tràfic XML i robar configuració de recursos i tiquets de sessió.
- Atacants amb l'habilitat de craquejar la ofuscació podrien obtenir les credencials dels usuaris.
- Els atacants poden impersonalitzar el controlador i interceptar les peticions d'autenticació.

Per la majoria d'organitzacions, el tràfic del servei de Citrix XML estarà aïllat en un centre de processament de dades dedicat físic o virtual fent que la interceptació no sigui provable. Tot i així, per seguretat s'hauria de considerar fer servir encriptació SSL per enviar el tràfic cap als StoreFronts fent servir una connexió segura https.

4.5.5. Balanceig de càrrega.

Les polítiques de balanceig per defecte s'apliquen a tots els grups de sistemes operatius publicats, ja sigui d'aplicacions o escriptori. Les configuracions per defecte especifiquen que el màxim nivell de càrrega de un servidor serà de 250 sessions i no considera el consum de processador i memòria. Al no revisar l'ús real de recursos del servidor, pot suposar una degradació en el rendiment o una infrautilització, resultant en una gestió ineficient dels recursos si no s'ha fet un dimensionament molt correcte.

Des de consultoria es recomana la creació de polítiques de balanceig de càrrega específiques per cada grup de publicació basat en proves de càrrega reals. Diferents regles i límits superiors es poden aplicar en cada política o grup de publicació depenent de les necessitats i colls d'ampolla detectats en cada cas.

Si no es pot realitzar un estudi de càrrega adequat abans d'entrar en producció, consultoria recomana la implementació de la següent política de càrrega personalitzada que es pot aplicar a tots els servidors com a mida mitja:

- Ús de CPU – Càrrega màxima 80%
- Ús de CPU excloent prioritat del procés – Per sota de normal o Baixa
- Ús de memòria – Càrrega màxima 80%
- Ús de memòria, càrrega base – Reportar càrrega zero (MBs): 786
- Número màxim de sessions – X

Aquestes regles es poden anar afinant un cop es van veient les necessitats i colls d'ampolla reals que pateix l'entorn.

4.5.6. Pre-càrrega de sessió i persistència de sessió.

Pre-càrrega de sessió i persistència de sessió són funcionalitats de XenApp 7.6 dissenyades per ajudar als usuaris a accedir ràpidament a les aplicacions arrencant sessió prèviament a la sol·licitud d'apertura d'aplicació (pre-càrrega de sessió) i mantenint la sessió activa després que l'usuari hagi tancat totes les aplicacions en una sessió (persistència de sessió). Pre-càrrega de sessió obrirà una sessió i la mantindrà oberta per un temps especificat fins que l'usuari connecti a la sessió demanant l'apertura d'alguna aplicació. Persistència de sessió mantindrà la sessió activa durant un temps especificat un cop l'usuari ha tancat totes les aplicacions d'una sessió per si l'usuari decideix tornar a obrir una aplicació durant aquest temps i d'aquesta forma evitar la càrrega i el temps que suposa el tancament i apertura de sessió. Aquestes dues funcionalitats s'habiliten mitjançant Studio, configurant els grups de publicació.

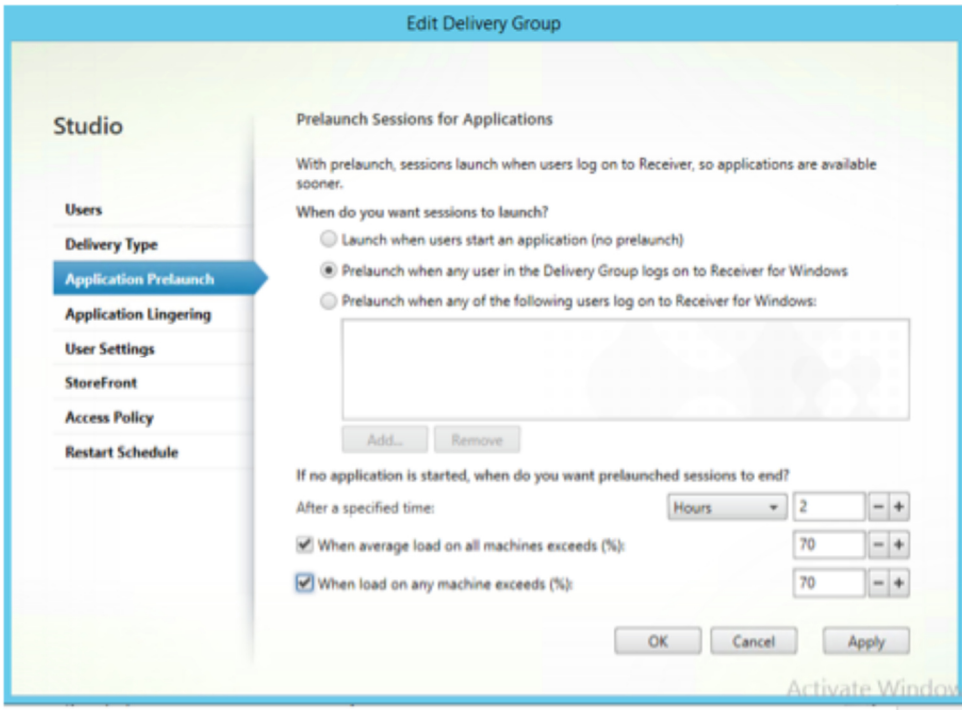

Fig.4.6. Configuració pre-càrrega i persistència de sessió

La mida de temps que una sessió sense fer-se servir pot mantenir-se activa ja sigui perquè ha estat pre-càrregada o mantinguda, es pot definir en base a:

- Un interval de temps especificat (1-99 dies, 1-2376 hores, o 1-142, 560 minuts). Si aquest interval es defineix massa curt, una sessió pre-carregada es tancarà abans de donar cap tipus de benefici a l'usuari.
- Quan la càrrega mitja en totes les màquines d'un grup de publicació excedeix un tant per cent especificat (1-99%) el controlador terminarà una sessió pre-carregada entre tots els VDAs del grup. Per defecte aquest límit està definit a un 70%.
- Quan la càrrega en una de les màquines dins del grup de publicació excedeix un tant per cent especificat (1-99%) el controlador terminarà una sessió pre-carregada en aquest VDA. Per defecte aquest límit està definit a un 70%.

Quan s'excedeix un d'aquests límits el controlador escollirà les sessions pre-carregades que portin més temps obertes. Les sessions es van tancant d'una en una fins que es baixa del nivell de càrrega configurat com a límit. Si el límit està excedit, no s'obriran noves sessions de pre-càrrega.

Els servidors amb VDA que no s'han registrat o els servidors que estan en mode de manteniment es consideren com a càrrega completa i no es poden fer servir ni per pre-càrrega de sessió ni per persistència de sessió.

S'han de tenir les següents consideracions quan s'està planificant la configuració fent servir pre-càrrega de sessions o persistència de sessió:

- Pre-càrrega de sessió augmentarà, de mitja, la quantitat de recursos necessaris. Les sessions s'obriran en grups d'aplicacions encara que no siguin necessàries.
- Pre-càrrega i persistència de sessió consumeixen una llicència Citrix.
- Pre-càrrega de sessió es fa servir per millorar el temps de càrrega d'aplicacions publicades dins d'un escriptori VDI.

4.6. Imatges base.

En seleccionar un sistema operatiu per a cada grup d'usuaris, els arquitectes tenen que considerar les necessitats dels usuaris i les seves aplicacions així com la solució d'imatge seleccionada. Les consideracions inclouran la versió del sistema operatiu, l'arquitectura, l'estratègia de lliurament, polítiques apropiades i com els usuaris i les imatges estan alineats en diferents conjunts de grups de publicació i catàlegs de la màquina.

4.6.1. Sistema operatiu.

Per seleccionar un sistema operatiu adequat per a cada grup d'usuaris, els arquitectes han d'entendre les necessitats de l'usuari i els requisits de les aplicacions així com les capacitats del model *FlexCast* elegit. La següent taula ens recomana quins sistemes operatius a XerDesktop 7 al model *FlexCast*:

Sistemes operatius per model *FlexCast:*

FlexCast Model	Windows 7	Windows 8	Windows Server 08 R2	Windows Server 2012
Hosted Shared			●	●
VDI: pooled-random	●	●		
VDI: pooled-static	●	●		
VDI: pooled w/ PvD	●	●		
VDI: dedicated	●	●		
VDI: Existing	●	●		
VDI: physical / remote PC	●	●		
VDI: Streamed	●	●		
VDI: streamed with PvD	●	●		
Streamed VHD	●	●	●	●
Local VM	●	●	●	●
On demand apps			●	●
VM local apps	●	●		

● Recommended ● Viable

Taula 4.12. SO recomanat per sistema FlexCast

Una decisió clau durant el disseny XenDesktop és si s'ha d'utilitzar un Windows XP de 32 bits (x86) o la versió de 64 bits (x64), Windows 7 o Windows 8. Windows Server 2008 R2 i Windows Server 2012 són només 64 bits.

El principal avantatge d'un sistema operatiu de 64 bits és que significativament

mes memòria física es pot assignar a cada ordinador - 128GB per a Windows XP, 192 GB per a Windows 7 Professional i 512 GB per Wndows 8. Per contra els sistemes operatius de 32 bits es limiten a 4 GB de memòria física.

Una dels desavantatges de l'elecció d'un sistema operatiu d'escriptori de 64 bits

es que es necessitaran controladors de 64 bits. Trobar controladors de 64 bits pot ser difícil, especialment per perifèrics i programes antics. No obstant, el

principal desavantatge dels sistemes operatius de 64 bits es que no poden donar suport a aplicacions de 16 bits i moltes empreses encara fan servir aplicacions de 16 bits. Fins i tot les aplicacions de 32 bits sovint inclouen elements de codi de 16 bits.

Citrix AppDNA es pot utilitzar per verificar si les aplicacions utilitzen codi de 16 bits o no, a més d'una gran quantitat de informació de compatibilitat addicional.

Si es necessiten aplicacions de 16 bits, consideri una de les següents opcions

1. Implementar un sistema operatiu de 32 bits limitat a 4 GB de RAM per la majoria dels usuaris. Proporcionar als usuaris avançats amb un sistema operatiu de 64 bits de manera que puguin ser assignats més de 4 GB de RAM.

Windows 8 està disponible en les versions de 32 bits i 64 bits.

2. Implementar un sistema operatiu de 64 bits per a tots i fer servir Microsoft Windows 2008 x86 amb Citrix XenApp 5.0 per lliurar aplicacions de16 bits.

XenApp 5.0 serà l'última versió de XenApp que suporta 32 bits Microsoft Server (Microsoft Server 2008). Windows 2008 R2 o Windows Server 2012 per a XenDesktop 7 i són només 64 bits.

3. Implementar un sistema operatiu de 64 bits i utilitzar aplicacions VM Hosted per lliurar aplicacions de 16 bits amb sistemes operatius d'escriptori de 32 bits.

4. Implementar un sistema operatiu de 64 bits i substituir o refer totes les aplicacions perquè siguin de 32 bits o 64 bits.

4.6.2. Polítiques d’equip.

Les polítiques de Citrix proporcionen la base per a configurar i afinar el entorn de XenDesktop, que permeten les organitzacions controlar la connexió, seguretat i ample de banda basat en diversos combinacions d'usuaris, dispositius o tipus de connexió.

Definir una política base inicial i assignar directives addicionals basat en els requisits de seguretat i escenaris específics d'accés és un aspecte important en lliurar una experiència d'usuari excepcional.

En prendre decisions de política és important considerar tant polítiques de Microsoft Windows i de Citrix com que cada un té un impacte en l'experiència de l'usuari i optimització de l'entorn.

El desenvolupament d'una política d'equip per l'arquitectura general inclou el mateix conjunt de decisions de disseny es defineix en la política de l'usuari. Aquestes inclouen:

- Motor de polítiques preferida
- La integració de polítiques
- Política de filtrat
- Política de precedència
- Política base

4.6.3. Catàlegs de màquina.

Catàlegs de màquines són una col•lecció de màquines virtuals o físiques administrades com una sola entitat. Els catàlegs de màquines especifiquen:

- Les màquines virtuals o físiques disponibles per allotjar aplicacions o ordinadors o ambdós.
- Les comptes d'Active Directory assignats a les màquines virtuals o ordinadors.
- El tipus de màquina virtual assignada (estàtica o aleatoria)
- El mètode d'aprovisionament utilitzat per generar la màquina virtual
- El sistema operatiu instal•lat a la màquina
- En alguns casos, la imatge principal que es copia per crear les màquines virtuals.

Com un catàleg és simplement una definició dels recursos d'escriptoris virtuals,

un únic catàleg pot estendre a través de múltiples hosts o grups d'hipervisors i associada recursos com ara emmagatzematge. Si un catàleg es pot estendre en diversos hosts, és important assegurar-se que els host tenen l'accés a les plantilles apropiades per a la clonació i les imatges, depenent del model FlexCast de l'ordinador on s'està lliurant.

Els arquitectes també hauran de considerar els mètodes utilitzats per assegurar aquesta imatge de l'ordinador de base s'actualitza en tots els hosts dins del catàleg, com es requereix.

Generalment, per tal de simplificar la gestió de l'entorn, cada catàleg creat ha de proporcionar màquines del mateix tipus (Per exemple, estàtica o aleatòria). Encara que aquest no és una restricció del producte base, limitant catàlegs per tipus de màquina permetrà una gestió simplificada i una estructura del catàleg més fàcil d'entendre.

4.6.3. Grups de publicació.

Grups de publicació són col•leccions de màquines que especifiquen què grups d'usuaris poden accedir als ordinadors o aplicacions. Per lliurar aplicacions i ordinadors, els usuaris de Directori Actiu o grups d'usuaris s'assignen a grups de publicació. La assignació de grups de publicació als usuaris es pot realitzar 1: 1 o 1 a molts, i els grups de publicació poden tenir múltiples catàlegs. Aquest procés permet als arquitectes poder definir millor les seves assignacions d'ordinadors amb els requisits de l'usuari úniques. Per exemple, si un grup de desenvolupadors necessita un d'un ordinador d'escriptori per el dia a dia , i un conjunt d'escriptoris dedicats per al desenvolupament i la prova, aquests equips es podem assignar d'un sol grup de publicació

És important que els següents elements es consideren al definir els grups d'usuaris:

- Catàlegs de màquines poden tenir diverses grups d'hipervisor
- Els usuaris poden assignar a diversos catàlegs de màquines.
- Un catàleg màquina pot estar associada amb un o més grups de publicació
- Catàlegs de màquines múltiples poden fer referència al mateix grup de publicació

- Una màquina no es pot utilitzar a més d'un grup de publicació
- Els grups de publicació es poden crear a partir de múltiples catàlegs de màquines amb les mateixes característiques.
- Grups de publicació Mixta no es poden crear a partir de catàlegs de màquines amb diversos tipus de màquines.

Els grups de publicació també permeten a una organització per a configurar una administració delegada permetent a específics administradors poder gestionar un grup dels escriptoris virtuals. Per exemple, un grup de publicació pot ser configurat per a ús executiu, amb un conjunt definit d'administradors delegats amb suport VIP.

4.6.3. Carpetes d'aplicació.

Carpetes d'aplicació és una característica XenApp 7.6 que permet a els administradors organitzar les aplicacions en grups lògics. Al organitzar les aplicacions en carpetes, els administradors tindran més facilitats per gestionar aplicacions, sobretot en grans ambients que poden tenir centenars d'aplicacions publicades.

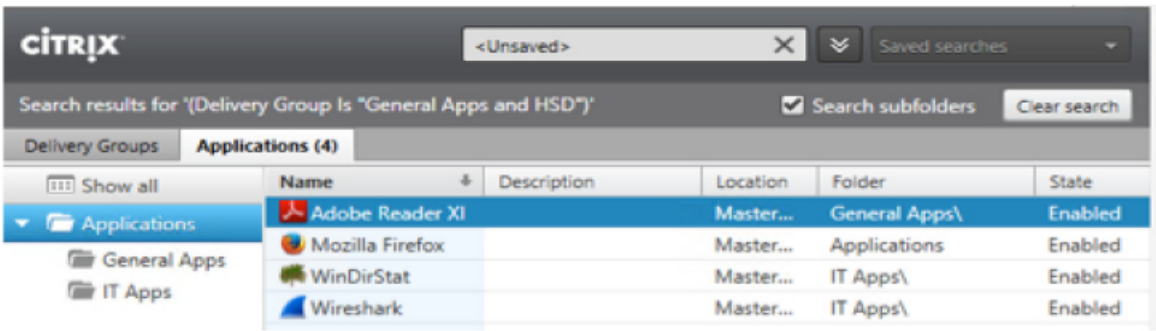

Fig.4.7. Configuració carpetes d'aplicació

Per defecte, totes les aplicacions es col•loquen en una sola carpeta anomenada Aplicacions en Citrix Studio. Les carpetes es poden crear en el mateix moment que els grups de publicació o es poden afegir més tard. Les carpetes també es poden crear en el moment les aplicacions es publiquen.

Per veure les carpetes d'aplicacions en Citrix Studio, els administradors tenen que tenir permís per "Veure Aplicacions". El permís d'edició de aplicacions s'ha de eliminar, canviar

el nom o suprimir la carpeta que conté les aplicacions. Els administradors que tenen els drets d'administrador de grup publicació són capaços de crear i modificar aplicacions dins de carpetes de l'aplicació, però no poden crear, canviar el nom o suprimir carpetes de l'aplicació.

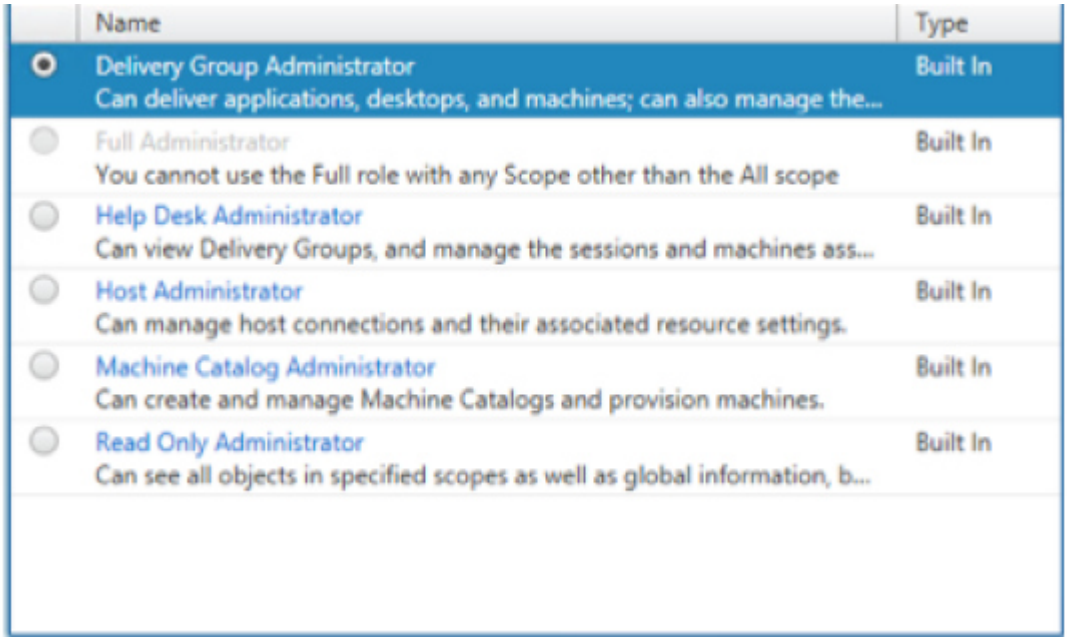

Fig.4.8. Rols administratius Citrix

Hi ha diversos casos d'ús per agrupar les aplicacions en carpetes:

Use case	Examples
Applications grouped by department use	Finance Apps Sales Apps Marketing Apps
Applications grouped by region	Americas Apps EMEA Apps
Applications grouped by product version	MS Office 2013 Apps MS Office 2010 Apps
Hosting provider with multiple tenants	Tenant1 Apps Tenant2 Apps

Taula 4.13. Exemple agrupació de carpetes

4.6.3. Assignació de recursos.

L'assignació de recursos determina el processador, la memòria i el disc de les màquines virtuals. Aquestes decisions tenen un impacte directa en els requisits de hardware i d'emmagatzematge calculats al capa de hardware.

La clau per a l'assignació de recursos és assegurar que els escriptoris virtuals i aplicacions poden oferir nivells similars de rendiment a escriptoris físics. Altrament, la productivitat i la satisfacció l'usuari general es veurà afectada. L'assignació de recursos a les màquines virtuals per sobre de les seves necessitats, però és ineficient i per al negoci.

Els recursos assignats s'han de basar en la càrrega de treball característica de cada grup d'usuaris, identificats durant fase d'avaluació.

4.6.3.1. Assignació de processador virtual (vCPU).

Per als sistemes operatius basats en escriptori (XenDesktop), Citrix normalment recomana dues o més CPU virtuals per màquina virtual perquè els múltiples fils es poden executar simultàniament. Una sola CPU virtual podria ser assignat per a càrregues de treball lleugeres, però, aquests escriptoris són més propensos a experimentar bloquejos de sessió. Addicionalment, càrregues de treball lleugeres són més apropiats per sistemes (XenApp), que ofereixen majors nivells d'escalabilitat.

Per als sistemes operatius basats en servidor (XenApp), Citrix Consulting normalment recomana quatre CPU virtuals per a Microsoft Windows Server 2008 R2 i vuit CPU virtuals per a Microsoft Servidor 2012/2012 R2.

Proves d'escalabilitat interna ha demostrat que el nombre d'usuaris allotjat en Microsoft Windows Server 2012/2012 R2 pot ser doblat quan el nombre de processadors s'incrementa de quatre a vuit. Les mateixes proves van mostrar que 2008 R2 no proporciona el mateixa escalabilitat lineal que 2012/2012 R2. Menys, d'alta densitat màquines virtuals són típicament preferits simplificar l'administració.

La següent taula proporciona orientació sobre la CPU virtuals que hauria de ser assignat a la base de la càrrega de treball i el model FlexCast.

Assignació de CPU virtual

Workload	Host Shared/Application Servers[1]	Pooled/Assinged VDI[2]	
		Configure For Density	Configure For User Experience
Light	Windows Server 2008 R2 = 4 Windows Server 2012/2012 R2 = 8	1	2
Medium		2	2-4
Heavy		2-4	4+

Taula 4.14. vCPU per usuari VDA

4.6.3.2. Assignació de memòria virtual (vRAM).

L'assignació de memòria insuficient per a les màquines virtuals causarà paginació excessiva. Si les màquines virtuals s'aprovisionen mitjançant Provisioning Services, la memòria insuficient causarà una major tràfic de xarxa i que menys dades es poden emmagatzemar en memòria local. Si la funció "desbordament de cache RAM" recomanada s'utilitza, memòria addicional s'ha d'assignar per permetre una reducció significativa en IOPS.

La majoria dels hypervisor suporten l' assignació de memòria dinàmica per proporcionar automàticament la memòria addicional per a les màquines virtuals que ho requereixin mitjançant la limitació dels que no ho fan. La forma en què la memòria dinàmica es maneja és especifica hypervisor i està cobert a la capa de hardware.

La següent taula proporciona orientació sobre la vRAM que s'hauria d'assignar basat en el model FlexCast. Aquests són directrius recomanades, però, si un model de hardware que ja estat seleccionat, revertir la mida es pot utilitzar per assignar de manera òptima vRAM.

Assignacions de Memòria (GB)

Workload	Host Shared/Application Servers[1,3]	Pooled/Assinged VDI[2,3,4]	
		Configure For Density	Configure For User Experience
Light	Windows Server 2008 R2 = 12 Windows Server 2012/2012 R2 = 24	1-2	2-3
Medium		2	3-4
Heavy		4	5+

Taula 4.15. vRAM per usuari VDA

4.6.3.3. Assignació d'espai d'emmagatzematge.

La quantitat d'emmagatzematge que cada màquina virtual requereix variarà en funció en la càrrega de treball i el tipus d'imatge. Si es creen màquines VDI dedicades sense aprofitar una solució de gestió d'imatges, cada màquina virtual requereix suficient emmagatzematge per a tot el sistema operatiu i les aplicacions instal•lades localment.

. Desplegament de màquines a través de MCS o PVS pot reduir substancialment els requisits d'emmagatzematge per a cada màquina virtual.

Els requisits d'espai en disc per a la memòria cau d'escriptura en disc i diferència dependrà d'ús de l'aplicació i el comportament de l'usuari. No obstant això, la següent taula proporciona un punt de partida per a l'estimació d'espai en disc ,requisits basats en la mida de la màquina de amb vCPU i de vRAM segons les pautes anteriors:

Requeriments d'espai de disc:

Workload	Pooled VDI	Assigned VDI	Hosted Shared
	Windows 7/8	Windows 7/8 with Personal vdisk[3]	2012/2008 R2
Provisioning Services - Write Cache[1,2]			
Light	5 GB	15 GB	40 GB / 25 GB
Medium	7 GB	17 GB	
Heavy	10 GB	20 GB	
Machine Creation Services - Difference Disk[4,5]			
Light	5 GB	15 GB	40 GB / 25 GB
Medium	7 GB	17 GB	
Heay	10 GB	20 GB	

Taula 4.16. Espai en disc per usuari VDA

4.6.3.4. Reserva d'IOPs.

La següent taula proporciona una guia sobre el nombre de IOPS generada per màquina virtual basada en la càrrega de treball, sistema operatiu i model FlexCast. Les IOPS calculades en la següent taula són una mitjana de l'estat estacionari i no són una mitjana de pic que porta els processos d'arrancada, els inicis de sessió i tancaments de sessió.

Nota: Els números de IOPS en aquesta taula representen les operacions d'E / S dins d'una màquina virtual. El nombre de IOPS finals variarà en funció de les tecnologies de nivell de RAID i d'optimització d'emmagatzematge elegits en la capa de hardware.

Requeriments IOPS per carrega de treball:

Workload[1]	Pooled VDI		Assigned VDI (Personal vDisk)[1]		Hosted Shared	
	Windows 8	Windows 7	Windows 8	Windows 7	Windows 2012 -Per User	Windows 2008 R2 - Per User
Installed[2] (Steady State Read/Write Ratio 50/50)						
Light	7	7	n/a	n/a	5	3
Medium	13	13	n/a	n/a	9	6
Heavy[3,4]	26+	26+	n/a	n/a	17+	12+
Provisioning Services (Steady State Cache on HDD) (Read/Write Ratio 20/80)						
Light	5	5	4	4	3	2
Medium	10	10	10	10	6	4
Heavy[3,4]	20+	20+	20+	20+	12+	8+
Provisioning Services (Steady State Cache in RAM with overflow) (Read/Write Ratio 40/60)						
Light	1	1	TBD	TBD	1	1
Medium	1	1	TBD	TBD	1	1
Heavy[3,4]	1+	1+	TBD	TBD	1+	1+
Machine Creation Services (Steady State Read/Write Ratio 20/80)						
Light	7	7	5	5	5	3
Medium	13	13	12	12	9	6
Heavy[3,4]	26+	26+	26+	26+	17+	12+

Taula 4.17. IPOs per usuari VDA

4.6.3.5. Necessitats gràfiques (GPU).

Una unitat de processament gràfic (GPU), es pot aprofitar per millorar escalabilitat del processador i l'experiència de l'usuari o permetre l'ús de aplicacions gràfiques intensives. Durant el disseny d'escriptori és important decidir com la GPU (si s'utilitza) s'assignarà a la màquines virtuals. Hi ha tres mètodes disponibles.

- De pas a través de la GPU - Cada GPU física es passa a través d'un única màquina virtual XenDesktop (usuari individual) o màquina virtual XenApp (diversos usuaris).
- Hardware GPU virtualitzat - Usant la tecnologia XenServer vGPU, un GRID NVIDIA es virtualitza i es comparteix entre múltiples màquines. Cada màquina virtual té totes les funcions de controladors de NVIDIA i accés directe a la GPU.
- Programa GPU virtualitzat - La GPU està gestionat per la peticions de hipervisor i intercepta les sol•licituds fetes pel XenDesktop o màquines virtuals XenApp. Les màquines no tenen l'accés directa a la GPU fent d'aquest el mètode menys preferit. Programa virtualitzat GPU és intrínsecament diferent de programa renderitzat pel processador gràfics dins de la CPU.

	Pass-Through GPU	Hardware Virtualized GPU	Software Virtualized GPU
XenServer			
XenDesktop	O	O	X
XenApp	O	•	X
Hyper-V			
XenDesktop	X	X	•[1]
XenApp	X	X	•[1]
ESX			
XenDesktop	O	X	X
XenApp	O	X	X

"O": Recommended "•": Viable "X": Not Supported

Taula 4.18. Opcions d'assignació GPU

4.7. Personalitzacions.

4.7.1. Perfils d'usuari.

Un perfil d'usuari juga un rol fonamental en determinar quant de satisfactori és la experiència de l'usuari amb un escriptori virtual o un escenari d'aplicació virtual. Fins i tot aquelles solucions d'escriptori virtual ben dissenyades poden no resultar satisfactòries degut a llargs períodes d'inici de sessió o pèrdues d'ajustaments.

L'elecció de la solució de perfil d'usuari ha d'alinear-se amb les característiques de personalització del grup d'usuaris captats durant la fase d'avaluació, així com del model FlexCast seleccionat.

Existeixen tres tipus principals de perfils i veurem quin és el més adient per cada tipus de model de Flexcast.

Perfils locals: Els perfils locals estan emmagatzemats en cada servidor o escriptori del sistema operatiu i estan inicialment creats basant-se en el perfil d'usuari per defecte. Per tant, l'accés d'un usuari a aquests recursos crearia un perfil independent a cada sistema. Els usuaris poden mantenir els canvis del seu perfil local a cada sistema individual, però els canvis son només accessibles a les futures sessions a aquest sistema. Els perfils locals no requereixen de configuració; si l'inici de sessió d'un usuari a un servidor o escriptori de sistema operatiu no té una ruta de perfil administrativament definit, un perfil local es creat per defecte

Perfils itinerants: els perfils itinerants estan emmagatzemats en un repositori de xarxa centralitzat per a cada usuari. Els perfils itinerants són diferents respecte als perfils locals en que la informació en el perfil (tant si és una impressora, un ajust de registre, o un arxiu emmagatzemat a la carpeta d'arxius) pot ser feta disponible a les sessions d'usuari accedides des de tots els sistemes de l'entorn. Configurar un usuari per a un perfil itinerant requereix de l'administrador una designació de ruta de perfil d'usuari (per a escriptoris virtuals) o ruta de perfil per escriptori remot cap a una concreta compartició de xarxa. El primer cop que l'usuari realitza un inici de sessió cap a un servidor o escriptori de sistema operatiu, el perfil d'usuari per defecte s'utilitza per generar el perfil d'usuari itinerant. En el procés de tancament de sessió, el perfil es copia a la ubicació de xarxa especificada per l'administrador .

Perfils obligatoris: els perfils obligatoris estan normalment emmagatzemats en una ubicació central per a molts usuaris. No obstant, els canvis no es mantenen durant el tancament de sessió. Configurar un usuari per a un perfil obligatori requereix de l'administrador de crear un arxiu de perfil obligatori (NTUSER.MAN) d'un perfil existent itinerant o local i assignar a l'usuari amb una ruta de perfil d'escriptori remot. Això es pot aconseguir gràcies a la Política de Grups de Microsoft, personalitzant les propietats d'usuari de Director Actiu o Perfil de Gestió de Citrix.

Perfils Híbrids: els perfils híbrids combinen un fort nucli de perfil (un perfil obligatori o un perfil local per defecte) amb claus o arxius específics de registre que s'uneixen durant l'inici de sessió. Aquesta tècnica habilita als administradors a controlar estretament quins canvis es mantindran i disminuir la mida dels perfils d'usuari. A més, els perfils híbrids apliquen la tècnica de l'últim canvi guanya,

utilitzant tècniques de gestió de cues que automàticament detecten i prevenen canvis simultanis que podrien sobreescriure canvis realitzats en altres sessions. Minimitzen d'aquesta manera la possible frustració de pèrdua de canvis a un perfil quan s'accedeix simultàniament des de varis servidors o escriptoris virtuals. A més capturen i guarden només els canvis dintre del perfil, en comptes guardar tot el perfil en el procés de tancament de sessió.

La següent taula compara les especificacions clau per cada tipus de perfil:

Feature	Local	Roaming	Mandatory	Hybrid
Central management / roams with user	●	●	●[1]	●
User settings are stored persistently	●	●	●	●
Granular configuration	●	●	●	●
Logon performance and stability enhancements	●	●	●	●

[1] *When configured as Mandatory Roaming*

● Functionality available ● Optional ● Functionality not available

Taula 4.19. Especificacions per tipus de perfil

Per poder seleccionar el tipus de perfil òptim per a cada grup d'usuaris és important entendre les necessitats de personalització a més del model assignat de FlexCast. La següent taula ens serveix de guia en la elecció del tipus de perfil òptim:

Feature	Local	Roaming	Mandatory	Hybrid
User setting persistence required (personalization characteristic: basic / complete)				
Hosted VDI – random	●	●	●	●
Hosted VDI – dedicated / static with PVD	◎	●	●	◎
Hosted shared	●	●	●	●
XenClient	●	●	●	●
User setting persistence not required or not desired (personalization characteristic: none)				
Hosted VDI – Random	●	●	●	●
Hosted VDI – dedicated / static with PVD	●	●	●	●
Hosted shared	●	●	●	●
XenClient	●	●	●	●

● Recommended ● Viable ● Not Recommended ◎ Recommended for users who use a single virtual desktop only ◎ Recommended for users who use more than one virtual desktop

Taula 4.20. Tipus de perfil recomanat segons model Flexcast

4.7.2. Redirecció de carpetes.

Inicialment redireccionar carpetes del perfil, com ara documents de l'usuari i favorits, cap a un recurs de xarxa compartit és una bona pràctica per a minimitzar la mida del perfil, els arquitectes necessiten ser conscients que les aplicacions poden escriure i llegir dades a les carpetes de perfil com ara *AppData* , causant càrrega en la utilització del servidor de fitxers. És important fer un test a fons de la redirecció al perfil abans de de la implantació a producció per evitar aquestes qüestions. Per tant, és important realitzar una recerca d'aquelles activitats d'escriptura/lectura al perfil i realitzar un pilot abans de traslladar a producció. Microsoft Outlook és un exemple d'una aplicació que regularment realitza activats de lectura al perfil com quan la signatura de l'usuari es llegida del perfil de l'usuari cada cop que s'escriu un correu.

La següent taula mostra recomanacions generals per ajudar a identificar aquelles carpetes apropiades a redireccionar :

Folder	Local	Roaming	Mandatory	Hybrid
Application Data	●	●	●	●
Contacts	●	●	●	●
Desktop	●	●	●	●
Downloads	●	●	●	●
Favorites	◎	●	●	●*
Links	●	●	●	●
My Documents	◎	●	●	●*
My Music	◎	●	●	●
My Pictures	◎	●	●	●
My Videos	◎	●	●	●
Saves Games	●	●	●	●
Searches	●	●	●	●
Start Menu	●	●	●	●

● Recommended ● Optional ● Not Recommended ◎ Recommended for backup purposes

Taula 4.21. Recomanacions redirecció de carpetes segons tipus perfil

4.7.3. Exclusió de carpetes.

Excluir carpetes de ser emmagatzemades contínuament com a part d'un itinerant de perfil híbrid pot ajudar a reduir la mida dels perfils i els temps d'inici de sessió. Per defecte Windows exclou les carpetes AppData\Local i AppData\Local\Low, incloent totes les subcarpetes, com ara History,

Temp i Temporary Internet Files. A més, les carpetes de descàrregues i jocs guardats haurien de ser excloses també.

4.7.4. Perfils en cache.

El cache local dels perfils d'usuari itinerants o híbrids en un servidor o escriptori virtual és per defecte el del comportament de Windows i pot reduir els temps d'inici de sessió i el tràfic d'utilització i xarxa al servidor de fitxers. Amb el perfil en cache, el sistema únicament ha de descarregar els canvis realitzats al perfil. L'inconvenient del perfil en cache és que pot consumir grans quantitats d'emmagatzematge al disc local en sistemes multiusuari, com ara un servidor d'escriptori compartit.

Citrix recomana no esborrar els perfils en cache locals per als següents escenaris:

Per optimitzar el temps d'inici de sessió:

. VDI allotjat – Dedicat/Existent/Físic

. VDI allotjat – Estàtic amb PVD

. VDI allotjat – PC remot

. Màquina Virtual Local

Per optimitzar els temps de tancament de sessió:

. Escriptoris virtuals no persistents i servidors *Hosted Shared Desktops*, amb reinici en tancament de sessió o reinici diari

Citrix recomana esborrar els perfils en cache locals en tancament de sessió en els següents escenaris per evitar la proliferació de perfils viciats:

. Allotjament compartir proveït per servidors persistents d'escriptori compartit.

. Agrupació VDI allotjada sense reinici necessari en tancament de sessió.

Configurant el "Retard abans d'esborrar perfils en cache", la política de Citrix permet una possible extensió al retard de l'esborrament dels perfils en cache en el tancament de sessió. Augmentar el

retard és útil si un procés manté fitxers o el registre d'usuari s'obre durant el tancament de sessió. Això també pot reduir els temps de tancament de sessió per a perfils grans.

4.7.5. Permisos als perfils.

Per raons de seguretat, els administradors, per defecte, no poder accedir als perfils d'usuari. Mentre que aquest nivell de seguretat pot ser requerit per organitzacions que treballin amb dades molt sensibles, és innecessari per a la majoria d'entorns i pot complicar l'operativa i el manteniment. Per tant, és recomanable habilitar la opció "Afegir el grup de seguretat dels Administradors al perfil d'usuaris itinerants". La configuració d'aquesta política hauria de ser alineada amb les característiques de seguretat del grups d'usuaris captats durant la fase d'avaluació.

4.7.6. Ruta de perfil.

Determinar la ruta de xarxa per als perfils d'usuari és una de les decisions més significants durant el procés de disseny d'un perfil d'usuari. Generalment està fortament recomanat planificar un servidor de fitxers o dispositiu NAS d'alt rendiment i redundat.

Existeixen 3 tòpics que han de ser considerats en el perfil compartit:

. Actuació – L'actuació del servidor de fitxers afectarà als temps d'inici de sessió. Per a grans infraestructures d'escriptori virtual , un únic clúster de servidor de fitxers pot no ser suficient per gestionar els períodes d'activitat alta. Per a poder distribuir la càrrega a múltiples servidor de fitxers, l'adreça del servidor de fitxers i el nom compartit necessitaran ser ajustats

. Ubicació – Els perfils d'usuari són transferits per la xarxa sota el funcionament del protocol SMB, que no treballa òptimament en connexions amb alta latència. A més, les connexions WAN poder ser limitades en ample de banda, el que pot ocasionar afegir més retard al procès de càrrega del perfil. Per tant, el servidor de fitxers hauria d'estar ubicat pròxim als servidors i escriptoris virtuals per minimitzar el temps d'inici de sessió.

. Plataformes de sistema operatiu – Els perfils d'usuari tenen una estreta integració amb el sistema operatiu subjacent i no està suportat reutilitzar un usuari en diferents sistemes operatius o diferents plataforma com 64-Bit i 32-Bit. Per a més informació es pot consultar l'article KB2384951 de la base de dades de Microsoft. Windows 2008 i Windows Vista una nova estructura de perfil d'usuari, que pot ser identificat per un sufix .V2 al directori de perfil, que fa als perfils d'usuari antics incompatibles amb sistemes operatius més nous com Windows 2012, 7 i 8. Per a assegurar-se que un perfil separat és utilitzat per plataforma, el directori de perfil ha de ser adaptat.

Existeixen 2 mètodes que poden ser utilitzats per garantir aquests compromisos i estan basats en tecnologia pròpia de Windows:

. Objecte d'usuari: per cada objecte d'usuari al Directori Actiu, una ruta individual de perfil, que conté el nom del servidor de fitxers i directori de perfil, pot ser especificat. Com una única ruta de perfil pot ser especificada per objecte d'usuari, no és possible garantir que un perfil separat es carregarà per a cada plataforma de sistema operatiu.

. Política de grup de màquines o variables de sistema: la ruta de perfil d'usuari pot també ser configurada depenent de polítiques específiques de grup de màquines o variables de sistema. Això habilita als administradors a assegurar-se de que un perfil d'usuari es dedicat a la plataforma. Com que les configuracions específiques de les màquines afecten a tots els usuaris d'un sistema, tots els perfils d'usuari seran escrits sobre el mateix servidor de fitxers. Per balancejar càrrega dels perfils d'usuari a través múltiples servidors dedicats, grups d'entrega XenDesktop han de ser creats per servidor de fitxers.

Quan s'utilitza el Perfil de Gestió de Citrix, una tercera opció està disponible per garantir aquests compromisos:

. Atributs i variables d'objecte d'usuari: el Perfil de Gestió de Citrix habilita a l'administrador a configurar la ruta de perfil depenent de la política de grup de màquines utilitzant atributs de l'objecte d'usuari al Directori Actiu per especificar el servidor de fitxers dinàmicament. Per poder aconseguir-ho són necessaris 3 passos:

1 Generar un àlies de DNS (per exemple, fileserver1) que es refereixi a l'actual servidor de fitxers.

2 Genera un atribut de LDAP buit de l'objecte d'usuari (per exemple, I o UID) amb l'àlies de DNS.

3 Configura amb la Gestió del Perfil de Citrix depenent de GPO a utilitzar una ruta de perfil que es refereixi a l'atribut LDAP (per exemple, si l'atribut UID està utilitzat la ruta de perfil és converteix en \\#UID#\Profiles\profiledirectory)

A més, la Gestió del Perfil de Citrix genera automàticament variables per especificar rutes de perfil dinàmiques basades en la plataforma de sistema operatiu. Variables vàlides de la gestió de perfil són:

. !CTX_PROFILEVER! – Amplia la v1 o v2 depenent de la versió del perfil.

. !CTX_OSBITNESS! – Amplia a x86 o x64 depenent del nivell de bit del sistema operatiu.

. !CTX_OSNAME! – Amplia a el nom curt del sistema operatiu , per exemple Win7

Combinat les dues capacitats de la Gestió del Perfil de Citrix, una ruta de perfil completament dinàmica pot ser creada, que pot ser carregada balancejant entre múltiples servidors de fitxers i garantint que perfils de diferents plataformes de sistemes operatius no es barregen. Un exemple d'una ruta d'un perfil d'usuari completament dinàmic podria ser:

\\#UID#\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!

4.7.7. Perfils en streaming.

Amb un perfil d'usuari en streaming, fitxers i carpetes contingudes en un perfil son lliurats des de el servidor de fitxers a la màquina local quan un usuari accedeix a aquesta. En el procés d'inici de sessió, la Gestió del Perfil de Citrix, informa immediatament que el procés de càrrega de perfil s'ha completat, reduint el temps de càrrega de perfil a gairebé zero.

Citrix recomana habilitar el streaming de perfil per a tots els escenaris. Si es desitja mantenir una còpia local en cache del perfil d'usuari, es recomana habilitar la opció "Cache Sempre"

i configurar amb un valor de 0. Això assegura que la descàrrega del perfil d'usuari en *background* de la màquina i permet al sistema utilitzar aquesta còpia en cache en endavant.

4.7.8. Opció tornar a escriure.

Activant la opció de tornar a escriure, la Gestió del Perfil de Citrix detecta quan una aplicació ha escrit i tancat un fitxer i copia un altre cop el fitxer a la còpia de perfil de xarxa quan es troba en moments sense activitat. A escenaris on un únic usuari té múltiples escriptoris virtuals o simultanis escriptoris compartits, aquesta opció pot ser altament beneficiosa. No obstant, la Gestió del Perfil de Citrix no torna a copiar qualsevol registre a la xarxa, exceptuant un tancament de sessió marcat com tal. Llavors existeix un risc de que el registre i els fitxers quedin fora de sistemes aprovisionats, on el perfil en cache local es esborrat en els reinicis. Per tant es recomana deshabilitar aquesta opció en escenaris amb serveis de aprovisionament i creació de màquines.

4.8. Directori Actiu.

El Directori Actiu és necessari a la autentificació y a la autorització d'usuaris en un entorn Citrix. S'utilitza la implementació Kerberos al Directori Actiu per a garantitzar l'autenticitat i confidencialitat de les comunicacions amb els Delivery Controllers així com per mantenir sincronitzats els servidors.S'ha de destacar que Kerberos depèn dels Service Principle Names (SPNs) i DNS. Els SPN es defineixen al AD i s'utilitzen al procés d'identificació de Kerberos.

Els dominis Multi-bosc permeten separar un entorn per seguretat dins de la xarxa corporativa. Exemples d'això podrien ser la separació per ubicació, actius aïllats, o per departaments de l'empresa, és a dir, la separació del finançament i els recursos humans en boscos independents o la col·locació d'una fusió corporativa recentment adquirida en el seu propi bosc.

4.8.1. Administració del bosc de directori actiu.

És molt important definir correctament la gestió del bosc de directori actiu

Els desplegaments multi-bosc, per defecte, no tenen relació de confiança amb diferents dominis entre els boscos. Un administrador AD pot establir relacions de confiança entre els diversos boscos, el que permet que els usuaris i equips d'un bosc s'identifiquin i accedeixin a recursos d'un altre bosc.

Per a boscos que tenen confiança inter-domini, es recomana configurar-los de manera que permeti als Delivery Controllers comunicar-se amb tots dos dominis. Si no s'ha configurat la confiança, s'hauran de configurar diversos sites XenDesktop per a cada bosc.

4.8.2. Administració del site de directori actiu.

Un disseny adequat del site AD implica garantir que el controlador de domini està altament disponible per als Delivery Controllers i els Virtual Desktop Agents (VDA). Això es pot aconseguir deixant un controlador de domini instal·lat en local o bé un controlador de domini accessible per múltiples connexions WAN redundants. Citrix recomana que cada lloc tingui almenys dos controladors de domini per a proporcionar una alta disponibilitat. Els sites s'han de configurar de manera que els usuaris s'identifiquin contra el controlador de domini més apropiat. Normalment el que queda físicament més proper. En general, com més lluny es troba un Delivery Controller del controlador de domini, més lent serà el procés d'autenticació. Un administrador pot obligar aquesta acció configurant els sites AD amb afinitat de subxarxa.

Els Operation master roles proporcionen un mètode per evitar conflictes d'actualització d'AD especificant quins servidors realitzen certes actualitzacions AD. Tots els controladors de domini són tractats per igual en un entorn. El primer controlador de domini del bosc AD tindrà tots els operation master roles per defecte. Si el controlador de domini principal es satura a causa de gestionar tots els rols es recomana repartir els rols als altres controladors de domini.

4.8.3. Administració de les unitats organitzatives de directori actiu.

Tots els components de la infraestructura de Citrix per XenApp i XenDesktop així com els equips dels treballadors han de residir dins de la seva pròpia Unitat Organitzativa (UO); separant els treballadors i controladors per motius de gestió. En tenir el seu propi OU, els objectes interiorment tindran una major flexibilitat de gestió.

Als administradors de Citrix també se'ls pot concedir el control delegat de les unitats organitzatives específiques de Citrix. Una estructura bàsica d'UO Citrix tindrà tots els

servidors Citrix en la seva pròpia estructura d'unitats organitzatives, separant la infraestructura i els components VDA. Una estructura de Citrix OU de mostra es pot veure a continuació.

Fig.4.9. Exemple estructura OUs

4.8.3. Administració dels grups d'usuari de directori actiu.

Sempre que sigui possible, els permisos s'han d'assignar a grups d'usuaris grups en lloc de a usuaris individuals. Els grups han de ser creats per funcions específiques i úniques perquè els permisos es puguin assignar a un gran nombre d'usuaris simultàniament. Seguint els principis de Microsoft de Role-based Access Controls (RBAC) i Account, Global, Universal, Domain local, Permission (AGDLP), els administradors de sistema no assignen permisos directament a comptes d'usuaris individuals, i així s'elimina la necessitat d'editar una gran quantitat de permisos i drets d'usuari quan es creen, modifiquen o esborren comptes d'usuari.

Exemple d'aplicació de permisos:

- Una aplicació publicada a un grup de 1.000 usuaris requereix la validació d'un sol objecte per a tots els 1.000 usuaris.
- La mateixa aplicació publicada a 1.000 comptes d'usuari individuals requereix la validació de tots els 1.000 objectes.

4.8.4. Comptes de servei.

Els comptes de serveis són comptes especials que una aplicació o un servei utilitza per interactuar amb el sistema operatiu. Els administradors poden crear comptes de serveis i gestionar-les de forma centralitzada amb Directori Actiu. Es recomanen els comptes de servei ja que seran útils per evitar problemes amb els permisos i qüestions que afecten administradors i usuaris.

4.8.5. Control de directives.

4.8.5.1. Herència de directives.

Les directives de grup es poden aplicar a usuaris i equips en un site, domini o nivell d'unitat organitzativa. Quan les GPO s'apliquen a una unitat organitzativa “pare”, les GPO s'hereten pel contenidor “fill” per defecte. La prioritat de les GPO heretades està determinat per l'ordre de processat de les GPOs. Bloquejar l'herència en un contenidor “fill” impedirà que totes les GPO del contenidor “pare” s'apliquin als contenidors “fill”. Atès que les directives heretades poden afectar la usabilitat i el rendiment de l'entorn Citrix, es recomana documentar i testejar les directives en un entorn de prova abans de passar a producció.

4.8.5.2. Dimensionar les directives.

Un administrador pot aplicar una única GPO a tot l'entorn, o utilitzar diverses GPO més específics i més petits per aconseguir el mateix objectiu. En general, Citrix recomana tenir les mínimes GPOs possibles, fusionant GPO petites sempre que sigui possible. Una única GPO es pot vincular a diverses unitats organitzatives, cosa que redueix la quantitat de GPOs

en l'entorn, i millora la coherència entre múltiples entorns. Si hi ha una gran quantitat de GPO que necessitin ser processades empitjorarà el temps d'inici de sessió.

4.8.5.3. Herència en bloc.

Aquesta configuració de directiva evitarà que les configuracions de directives de OUs de nivells superiors, s'apliquin a una OU "filla". S'ha de remarcar que una OU de nivell superior pot tenir una configuració de directiva tipus "No reemplaçar", de manera que s'evita que s'apliqui l'herència en bloc.

4.8.5.4. Política de bucle invertit.

Hi ha una sèrie de directives d'usuari de Citrix específiques per a l'experiència d'usuari i seguretat que s'han d'aplicar a cada sessió d'usuari de Citrix. A causa de que els comptes d'usuari poden estar ubicades a qualsevol lloc de l'AD d'una empresa, pot arribar a ser difícil assegurar que s'estan aplicant aquestes directives d'usuari. L'aplicació de les polítiques de Citrix a nivell de domini afectaria a tots els usuaris que iniciessin sessió a l'entorn, ja sigui a través d'una connexió Citrix o no. Aplicar les directives de Citrix a la unitat organitzativa que conté el servidor Citrix XenDesktop / XenApp o escriptoris virtuals tampoc funcionaria, ja que els usuaris haurien d'estar ubicats dins d'aquesta unitat organitzativa. Habilitar una política de bucle invertit permetria que les configuracions de directives d'usuari d'una unitat organitzativa s'apliquessin a usuaris ubicats en qualsevol unitat organitzativa.

4.8.5.5. Política de filtrat de Directori Actiu.

La directiva de filtrat es pot utilitzar per a casos en què una directiva ha d'aplicar-se a un petit subconjunt d'usuaris, com ara administradors Citrix. Habilitar l'opció de processat de bucle invertit no funcionaria perquè s'aplicarà la configuració de directiva d'usuari per a qualsevol usuari que entrés al sistema, en lloc del grup desitjat d'usuaris. La directiva de filtrat de AD pot establir-se utilitzant les propietats de seguretat de la política que volguem filtrar.

5. Dimensionament de la prova de concepte.

5.1. Opció prova de concepte sense HA.

En aquesta opció mantindrem la prova de concepte al mínim sense pensar en entrar a producció degut a que tindríem múltiples únics punts de fallida, per mantenir al mínim les necessitats de hardware en la prova de concepte.

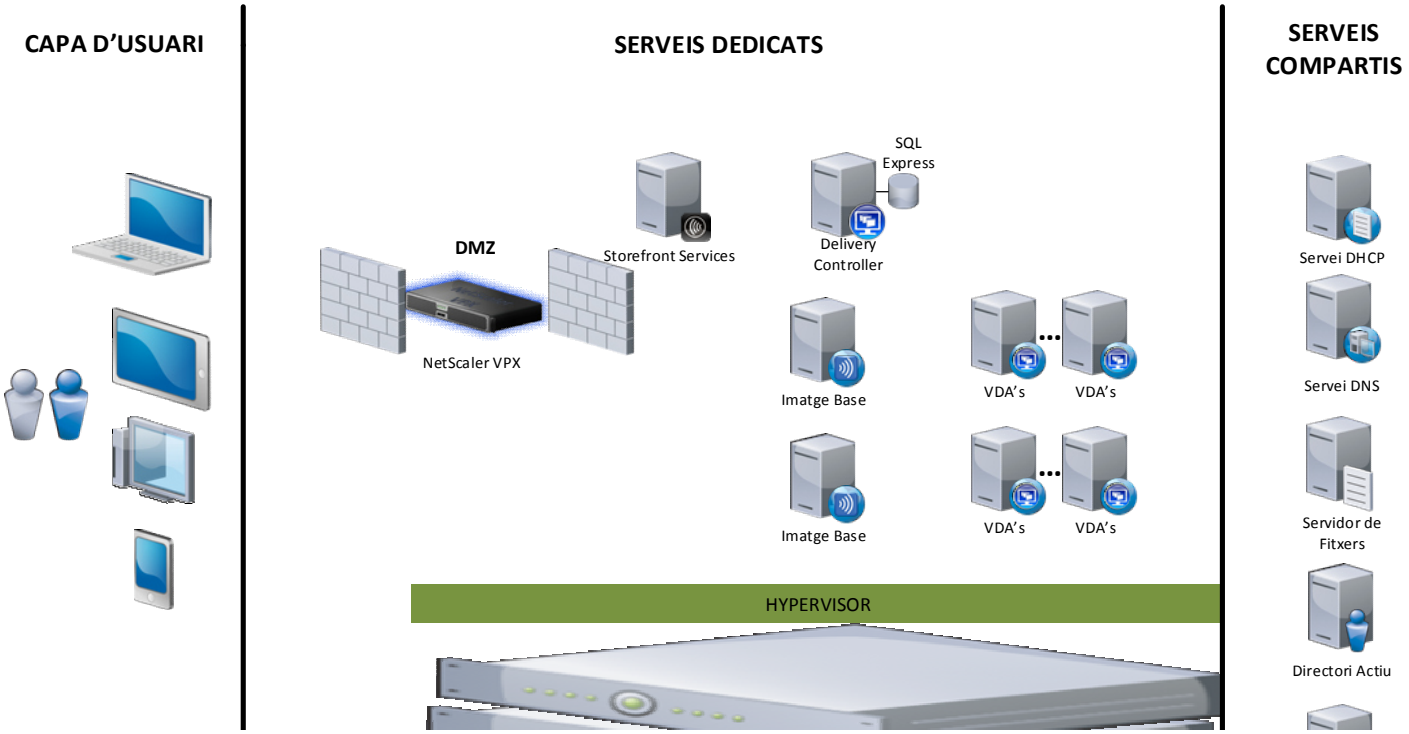

Fig. 5.1. Visio PoC sense HA

Disposaríem de un únic NetScaler VPX, un StoreFront i un Delivery Controller amb la base de dades local en SQL Express. I mesurarem les necessitats de les VDAs suposant que serviríem escriptoris per 50 usuaris tant de VDI com de HSD. Els usuaris s'han definit d'utilització mitja.

Servei	Quantitat	vCPU	vRAM	IOPs
NetScaler VPX	1	2	3	20
StoreFront	1	4	4	30
Delivery Controller	1	4	4	30
VDAs VDI Win8.1	50	2	2	21
VDAs HSD Win2K12R2	2	8	16	100
Total		126	143	1330

Taula 5.1. Dimensionament recursos per PoC sense HA

5.2. Opció prova de concepte amb HA.

En aquesta opció tots els components estan redundats i està pensat per poder testejar les recuperacions en cas de caiguda del servei i per poder mantenir la plataforma en cas de voler passar-la a producció.

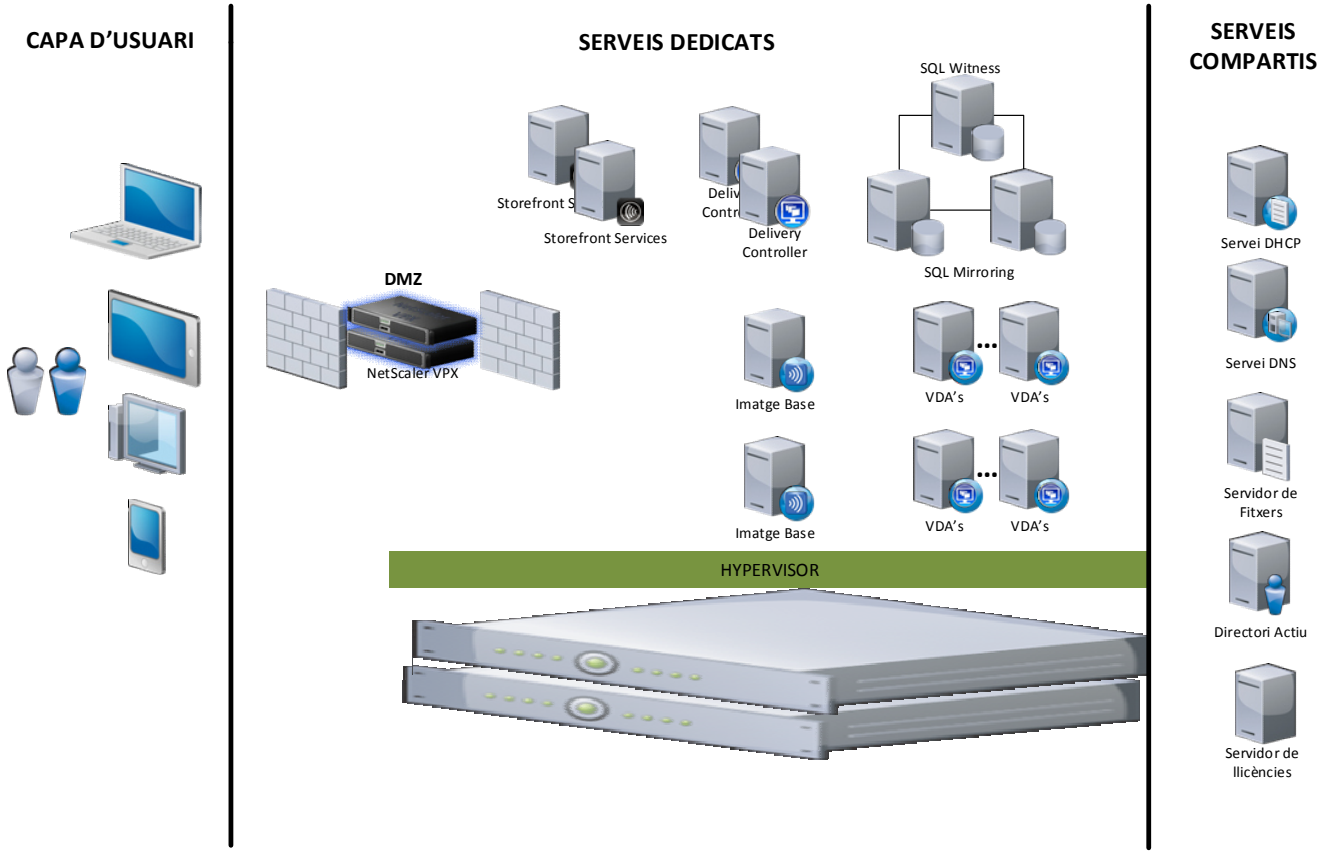

Fig. 5.2. Visio PoC amb HA

En aquesta opció disposem de dos NetScaler VPX, dos StoreFront, dos delivery controllers i tres instàncies de SQL en mirroring (primari, secundari i testimoni) i als servidors VDAs s'ha aplicat la regla de N+1 per suportar la caiguda d'un d'ells.

Taula 5.2. Dimensionament recursos per PoC amb HA

6. Conclusions.

En aquest estudi hem pogut veure les necessites existents a la EUPMT en cas de voler dur a terme un projecte de virtualització d'escriptoris.

S'ha definit la millor opció alhora de dissenyar aquesta proba de concepte entre les diferents opcions existents en el mercat.

S'han estudiat les parts crítiques del disseny de la proba de concepte i s'han apuntat les claus alhora de configurar cadascuna d'aquestes parts.

Finalment s'han dimensionat els requisits hardware necessaris per dur a terme aquesta proba de concepte.

7. Referències.

[1] http://blogs.gartner.com/chris-wolf/2012/12/10/desktop-virtualization-trends-at-gartner-data-center/

[2] https://www.citrix.com/products/xendesktop/how-it-helps/compare.html

[3] https://www.citrix.es/go/products/xendesktop/feature-matrix.html

[4] http://edocs.citrix.com

[5] http://www.virtualizationpractice.com/microsoft-windows-2012-rdsh-vs-citrix-xenapp-pv-to-get-its-own-murderball-18179/

[6] http://support.citrix.com/article/CTX139331

[7] http://www.virtualizationmatrix.com/matrix.php?category_search=all&free_based=1