



MINISTERIO
DE FOMENTO

CENTRO NACIONAL
DE INFORMACIÓN
GEOGRÁFICA

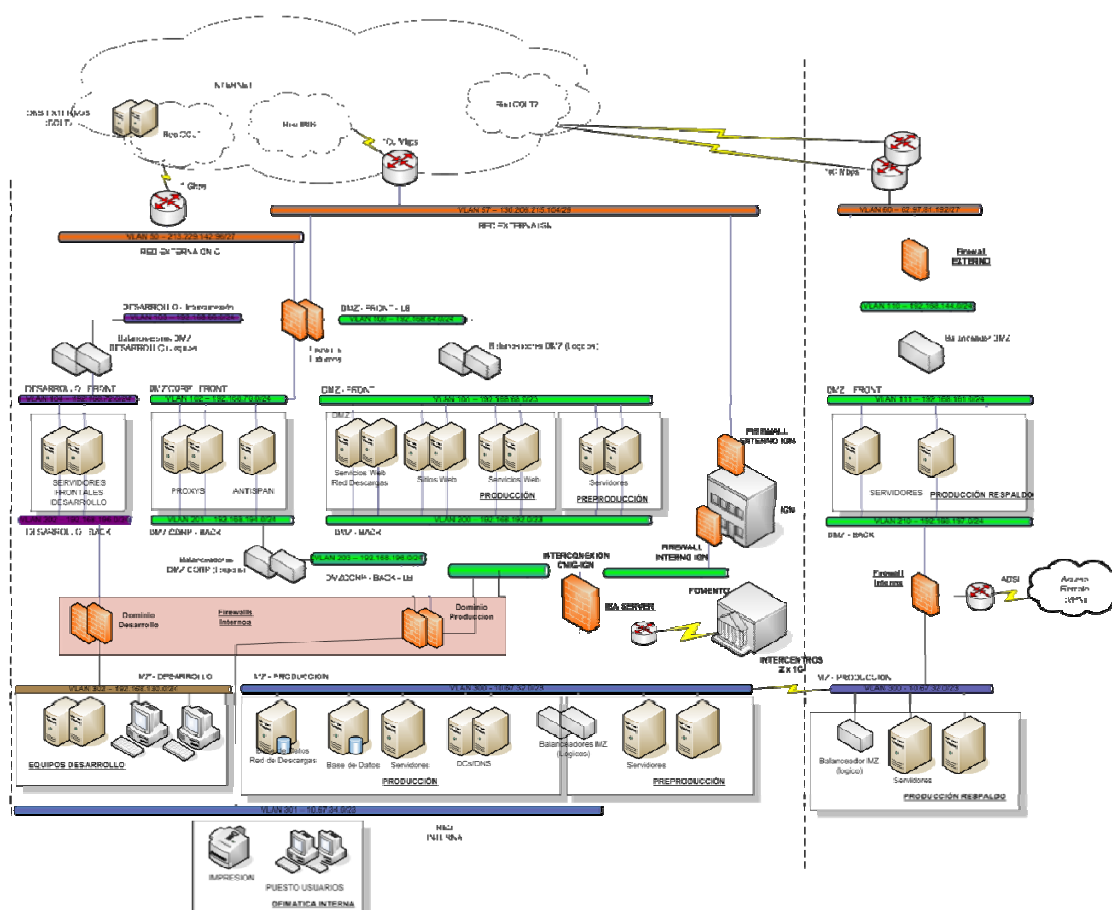
ANEXO I: ENTORNOS INFORMÁTICOS DEL CNIG

Arquitectura de Sistemas

La arquitectura de sistemas del CNIG ha sido diseñada bajo dos objetivos fundamentales:

- Construir un entorno de **Alta Disponibilidad** que permita ofrecer unos servicios de difusión de información geográfica con un nivel de servicio que facilite a los usuarios (Administraciones Públicas, empresas y ciudadanos) su utilización con una alta fiabilidad y calidad de servicio.
- Construir un entorno de **Alto Rendimiento**, con alto aprovechamiento de los recursos, con gran facilidad de escalado, que minimice tanto los costes de gestión como los esfuerzos de personal.

Bajo estos criterios de disponibilidad y rendimiento se ha llegado a la arquitectura definida en el siguiente diagrama.



Centros de Proceso de Datos

El CNIG cuenta dos centros de procesos de datos, en adelante CPD, donde reside toda la infraestructura informática que da soporte a los servicios de difusión de datos geográficos.

Los siguientes recursos se encuentran trabajando en modo Activo-Activo (CPD Principal – CPD Respaldo):

- Firewall FortiGate.
- Balanceadores Radware
- Servidores de Aplicaciones
- Servidores de Bases de Datos.
- Servicio de Ficheros EFS

Los siguientes recursos no se encuentran trabajando en modo activo-activo.

- Granja servidores VMware.

CPD Principal

El CPD Principal se encuentra en la calle General Ibáñez de Ibero, nº 3, en las dependencias de la Subdirección General de Aplicaciones Geográficas, quienes realizan la gestión y operación diaria del mismo.

Para saber más detalles de la infraestructura con que cuenta dicho CPD, se remite al Servicio de Sistemas de la Subdirección General de Aplicaciones Geográficas.

CPD Respaldo

El CNIG ha contratado con *Colt Technology Services Group*, un servicio de alojamiento externo y de gestión de la instalación de respaldo de los servicios de difusión de datos geográficos que presta el CNIG.

En este Centro de Respaldo, se encuentran redundados y activos todos los servicios de difusión de datos geográficos, en una relación de efectivos de aproximadamente un 20% de los recursos localizados en el CPD Principal sito en las instalaciones del CNIG.

Plataforma Hardware

La plataforma hardware del CNIG, detallada en el Anexo B, está compuesta aproximadamente por las siguientes plataformas:

- HP Proliant DL y ML (10%)
- HP Blade (90%)

Las distribuciones indicadas son aproximadas.

Arquitectura Lógica

La configuración de las infraestructuras informáticas del CNIG, tanto del CPD Principal como del CPD Respaldo, se ha diseñado conforme a los objetivos especificados anteriormente, de modo que todos los sistemas tienen un respaldo.

Servidores de aplicaciones

Los servidores de aplicaciones están configurados en granjas de servidores, balanceados por *appliances* Radware ODS2 1016. Dichos balanceadores cuentan con la consola de gestión Apsolute Insight. Este balanceo se realiza a nivel 7 o de aplicación, aplicando políticas distintas para cada servicio.

La mayoría de las aplicaciones no requieren de mantenimiento de sesión, pero existen algunas que sí requieren de esta funcionalidad, siendo balanceadas a través de *cookies* de aplicación.

Servidores de base de datos

Los servidores de BBDD forman un clúster distribuido en ambos CPD, de tipo ORACLE RAC 10.2 en configuración Activo/Activo, clusterizado íntegramente a nivel de software de base de datos.

Toda la información reside en sistemas de almacenamiento HP EVA 8400 en CPD Principal y HP EVA 8000 en CPD Respaldo.

Este clúster está formado por cinco nodos distribuidos de la siguiente manera:

- Nodo 1: CPD Principal
- Nodo 2: CPD Principal
- Nodo 3: CPD Principal
- Nodo 4: CPD Respaldo
- Nodo 5: CPD Respaldo

Servidores de Ficheros

Existen servidores de ficheros de instancia única que dan servicio a los usuarios internos del CNIG.

Además existe un sistema de ficheros en clúster en modo de trabajo Activo-Activo, denominado HP Cluster File System (Polyserve Matrix Server).

Este servicio se encuentra localizado en CPD Principal.

Sistema de almacenamiento

Existen dos cabinas de discos en las instalaciones del CNIG:

- HP StorageWorks EVA 8400: En CPD Principal.
- HP StorageWorks EVA 8000: En CPD Respaldo

Los datos que contienen estas cabinas pueden estar replicados a nivel de trama *fiber channel* a través del software HP Continuous Access y usando un canal de fibra directa entre los dos CPD.

Entorno de virtualización.

Existen entornos de virtualización VMware ESX y VMware ESXi en las instalaciones del CNIG.

Estos servidores se encuentran en configuración de alta disponibilidad a nivel de CPD, pero no tienen mecanismo de disponibilidad entre ambos CPD.

Otros elementos de sistemas

Todos los elementos de sistemas que intervienen: Directorio Activo, Firewall, etc., gestionados por el CNIG se encuentran redundados en ambos CPD.

Arquitectura de Red

La red está formada por switches HP Procurve. Todos los elementos principales son gestionables vía SNMP y se cuenta con HP Procurve Manager Plus como herramienta de gestión, la cual debe de estar actualizada y mantenida.

Adicionalmente se incluye dentro de la infraestructura de red los switches de los chasis de blade HP P-Class y C-Class. Los modelos actuales son Gbe1 y Gbe2.

Red de Área Local (LAN)

La red LAN del CNIG se encuentra organizada como una infraestructura de portal WEB con segmentos físicos definidos claramente, desplegados independientemente en dos ubicaciones físicas (CPD's).

En CPD Principal los segmentos presentes son los siguientes (DMZ-FRONT, DMZ-BACK, DMZ-CORP, MZ, Red iLO, Usuarios) cada uno de estos segmentos de red cuentan con electrónica de red independiente y redundada a 1 Gbps, basada en la interconexión a 10 Gbps entre dos switches Procurve 2910al-48G por segmento, con cada uno de estos segmentos, securizados mediante equipos de seguridad perimetral.

En CPD Respaldo los segmentos presentes son los siguientes (DMZ-FRONT, DMZ-BACK, MZ, Red iLO) cada uno de estos segmentos de red cuentan con electrónica de red independiente a 1 Gbps mediante switches Procurve 2910al-48G.

El segmento MZ se encuentra extendido entre las dos ubicaciones físicas mediante dos enlaces de fibra a 1Gbps cada uno.

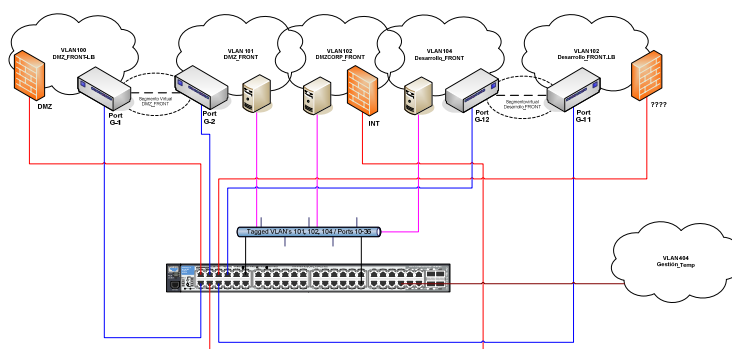


Ilustración 1: Diagrama DMZ Front

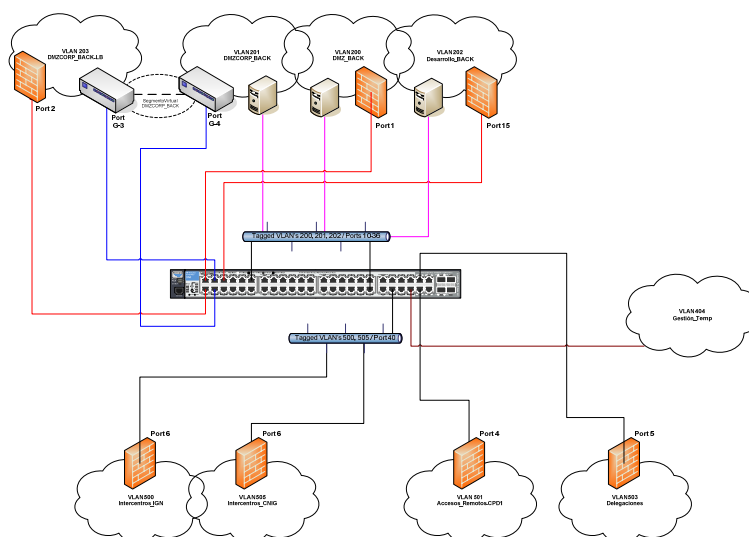


Ilustración 2: Diagrama DMZ Back

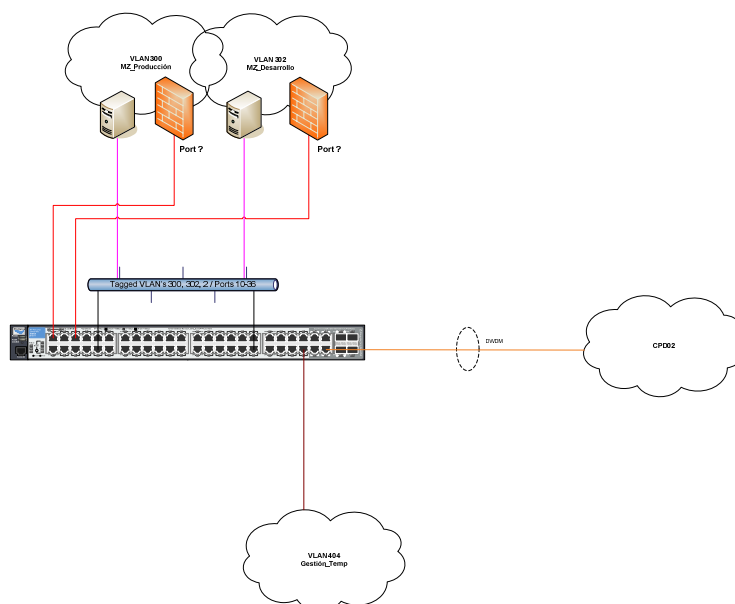


Ilustración 3: Diagrama MZ

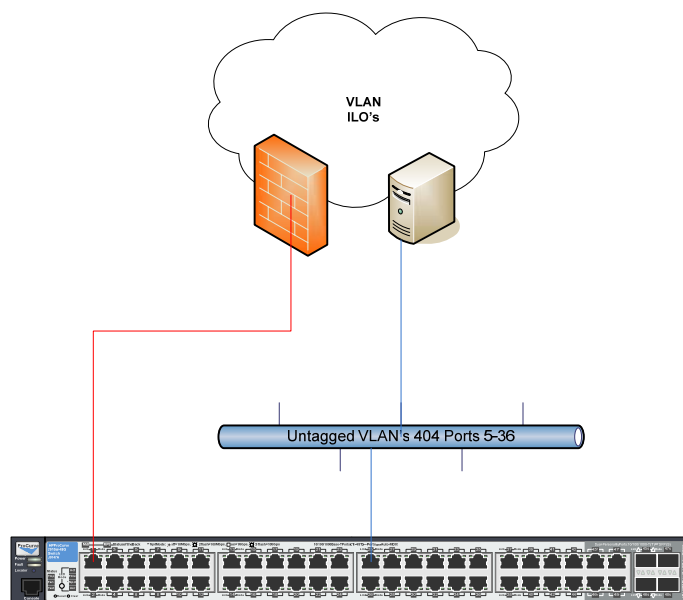


Ilustración 4: Diagrama Red iLO

Acceso a Internet

El acceso a internet está restringido en todas las redes, y permitido solamente el tráfico de salida de tipo http, https y ftp mediante cuatro servidores Proxy Squid que permiten el acceso vía http de las aplicaciones de publicación que lo requieran.

Estos servidores Proxy están distribuidos en CPD Principal y CPD Respaldo del siguiente modo.

- Proxy Primario en CPD Principal.
- Proxy Secundario (HA) en CPD Principal.
- Proxy Primario en CPD Respaldo.
- Proxy Secundario (HA) en CPD Respaldo.

Esta infraestructura de acceso a internet tiene un caudal de 1Gbps en CPD Principal y de 100Mbs en CPD Respaldo.

El acceso a internet por parte de los usuarios de la RED del CNIG se migrará de su forma actual a una infraestructura de proxies residentes en el segmento DMZ-CORP encontrándose este únicamente en CPD Principal con un ancho de banda posible de 1Gbps.

Acceso a la Red SARA

El CNIG cuenta con acceso a la Red SARA, a través del enlace administrado y gestionado por Fomento.

Servicios corporativos

CNIG proporciona sus propios servicios corporativos que son:

- Servicio de correo @cnig.es
- Servicio Antivirus y Antispam para correo electrónico.
- Servicio de Directorio Activo para dominio cnig.local
- Acceso a Internet vía Colt.

Herramientas de monitorización

Actualmente CNIG cuenta con dos tipos de monitorización:

- a) Monitorización de infraestructura de hardware: HP System Insight Manager.
- b) Monitorización de servicios: Hyperic para la supervisión del rendimiento de los servidores y HP SiteScope para la monitorización de los servicios Web de difusión de datos geográficos que presta el CNIG.

Sistemas de seguridad

El entorno de seguridad al igual que la infraestructura LAN está basado en una infraestructura de portal WEB, centrándose en dos niveles de seguridad.

- Nivel Externo: Mediante dos cortafuegos Stogate en cluster Activo-Activo y proporcionando aislamiento a los segmentos DMZ-FRONT y DMZ-CORP-BACK.
- Nivel Interno: Nivel Interno mediante dos cortafuegos Fortinet 310B en cluster Activo-Activo y proporcionando aislamiento a los segmentos DMZ-BACK, DMZ-CORP-FRONT, MZ, Usuarios, entre otros.

Sistema de Backup

Existe una política de backup definida por las siguientes líneas:

- Copia completa semanal.
- Copia incremental diaria

La Herramienta utilizada para realizar estas tareas es Symantec Backup Exec y HP OpenView Data Protector.

El almacenamiento de las copias de seguridad se realiza en las siguientes librerías de cintas:

- HP StorageWorks ESL 712.
- HP StorageWorks EML103

Anexo A. Relación de tecnologías presentes en el CNIG

1. Hardware

a. Servidores

- HP Proliant BL Serie C, enclosure.
- HP Proliant BL Serie P, enclosure.
- HP Proliant DL
- HP Proliant ML

2. Software

a. Sistemas Operativos

- CentOS
- RedHat
- Windows 2003 x86 y x86_64
- Windows 2008 x86 y x86_64
- VMware ESX
- VMware ESXi

b. Software Monitorización

- Hyperic
- HP Systems Insight Manager
- HP SiteScope

c. Software Cluster

- Microsoft Cluster Services
- Microsoft Distributed Filesystem
- EFS Polyserve

d. Software de Administración

- VMware vSphere vCenter, vMotion, HA.
- Sistema de Gestión Blades, RDP
- Brocade Data Center Fabric Manager
- HP Command View
- HP Ibrix

e. Software Web, FTP y DNS

- Apache Tomcat
- Apache HTTPD
- Internet Information Server
- FTP
- DNS

f. Software Servicios Infraestructura

- Squid
- Oracle RAC
- Microsoft Exchange (SMTP)

- Microsoft WSUS
- Microsoft Active Directory
- Microsoft ISA Server
- Antivirus
- HP Data Protector
- Symantec Backup Exec

Anexo B. Inventario de servidores del CNIG

Host	Modelo	Sistema Operativo
10.67.32.13	ProLiant BL685c G6	VMware ESX
10.67.32.14	ProLiant BL685c G6	VMware ESX
10.67.32.23	ProLiant BL460c G6	Red Hat Enterprise Linux
10.67.32.24	ProLiant BL460c G6	Red Hat Enterprise Linux
10.67.32.25	ProLiant BL460c G6	Red Hat Enterprise Linux
10.67.32.26	ProLiant BL460c G6	Red Hat Enterprise Linux
10.67.32.27	ProLiant BL460c G6	Red Hat Enterprise Linux
10.67.32.38	ProLiant BL460c G6	VMWare ESXi
10.67.32.39	ProLiant BL460c G6	VMWare ESXi
10.67.32.40	ProLiant BL460c G6	VMWare ESXi
10.67.32.41	ProLiant BL460c G6	VMWare ESXi
10.67.32.42	ProLiant BL460c G6	VMWare ESXi
10.67.32.43	ProLiant BL460c G6	VMWare ESXi
192.168.192.12	ProLiant BL460c G1	CentOS
192.168.192.13	VMware Virtual Server	CentOS
192.168.197.12	ProLiant BL460c G1	CentOS
192.168.197.13	VMware Virtual Server	CentOS
ufq51cnig001	ProLiant BL460c G6	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig002	ProLiant BL460c G6	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig003	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig004	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig005	ProLiant BL460c G6	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig005	ProLiant BL460c G6	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition



Host	Modelo	Sistema Operativo
		Edition
ufq51cnig006	ProLiant BL460c G6	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig007	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig008	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq51cnig008	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig001	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig002	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig003	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig004	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig005	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig006	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig007	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig008	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig009	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig010	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig012	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq52cnig013	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq55cnig001	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq55cnig002	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq55cnig003	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq55cnig004	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition



Host	Modelo	Sistema Operativo
		Edition
ufq55cnig005	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
ufq55cnig006	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq52cnig001	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig001	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig002	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig003	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig004	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig006	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig007	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig008	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig009	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig010	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig011	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig012	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig013	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig014	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig015	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig016	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig017	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
uvq61cnig018	VMware Virtual Server	Microsoft(R) Windows(R) Server 2003 Standard x64



Host	Modelo	Sistema Operativo
		Edition
wfp17cnig001	ProLiant BL460c G1	Microsoft® Windows Server® 2008 Standard
wfp34cnig001	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition
wfp34cnig002	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003 Standard x64 Edition